Vertiv™ Avocent® Universal Management Gateway Appliance Plug-in for the Avocent® DSView™ Management Software

Release Notes

VERSION 4.6.0.18, APRIL 2023

Release Notes Section Outline

1. System Requirements
2. Language Support Information
3. Features and Enhancements
4. Known Issues

1. System Requirements

This plug-in is compatible with Vertiv™ Avocent® DSView™ management software release versions beginning with version 4.5, Service Pack 5 (SP5). Please update the Vertiv™ Avocent® DSView™ management software to version 4.5 SP5 or higher prior to installing this plug-in.

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

This plug-in is required to support Java 8-based Vertiv™ Avocent® DSView™ management software, version 4.5. SP5 (Service Pack 5) and higher, and this plug-in is not compatible with Java 7-based Vertiv™ Avocent® DSView™ software from version 4.5.0.108 to 4.5.0.247.

After upgrading the appliance to version 4.0.0.19, if KVM sessions launched via the Vertiv™ Avocent® DSView™ software display an error message, resync the appliance with the Vertiv™ Avocent® DSView™ software and try again.

For more detailed information on system requirements and other helpful reference items, please refer to the Vertiv™ Avocent® Universal Management Gateway appliance and the Vertiv™ Avocent® DSView™ software installer/user guides, as well as the Avocent® DSView™ software plug-in technical bulletin.

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™ software. Java JRE 8u191 and 10.0.2 were used in testing.

1. Upgrade the Vertiv™ Avocent® DSView™ management software to SP5 (Service Pack 5) or later. If there are Vertiv™ Avocent® DSView™ software login issues using the Internet Explorer browser after upgrading, please ensure that the SSLv2 and SSLv3 options are disabled in the browser.
2. Upgrade the Vertiv™ Avocent® Universal Management Gateway appliance plug-in to version 4.6.0.18 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 Vertiv™ Avocent® Universal Management Gateway appliance to version 4.6.0.18 or earlier.
4. Execute the appliance resync action for the Vertiv™ Avocent® Universal Management Gateway appliance within the Vertiv™ Avocent® DSView™ software.
5. If this upgrade sequence could not be followed and the Vertiv™ Avocent® Universal Management Gateway appliance cannot properly be managed using the Vertiv™ Avocent® DSView™ software, please remove the appliance from the software and then re-add the appliance again.

NOTE: There are some appliance/ Vertiv™ Avocent® DSView™ software upgrade scenarios where target sessions to the appliance cannot be launched from the Vertiv™ Avocent® DSView™ software. These sessions are still functional when launched from the appliance web user interface (UI). Contact Technical Support for the latest workaround for this issue if it occurs.

2. Language Support Information

English, Chinese and Japanese languages are supported by the Vertiv™ Avocent® Universal Management Gateway appliance plug-in.

3. Features and Enhancements

COMPONENT	DESCRIPTION
Vertiv™ Avocent® DSView™ software plug-in	The Vertiv™ Avocent® Universal Management Gateway appliance version 4.6.0.18 is now supported in the Avocent® DSView™ software.

4. Known Issues

Vertiv™ Avocent® DSView™ Software Compatibility

- If the Vertiv™ Avocent® Universal Management Gateway appliance is upgraded to 4.6.0.18 and associated plug-in currently managed by Vertiv™ Avocent® DSView™ software SP10 or later is upgraded to version 4.6.0.18, then the secure mode setting must be toggled to ensure that the 2048-bit certificate is being used in the connection. If the upgraded appliance and plug-in are newly added to Vertiv™ Avocent® DSView™ software SP10 or later, the 2048-bit certificate will automatically be used in the connection.

- An Vertiv™ Avocent® Universal Management Gateway appliance managed by Vertiv™ Avocent® DSView™ software SP9 or earlier must be added in secure mode to successfully launch target sessions.

- If an Vertiv™ Avocent® Universal Management Gateway appliance is added to Vertiv™ Avocent® DSView™ software SP10 or later, it cannot later be added to Vertiv™ Avocent® DSView™ software SP9 or earlier without factory restoring the appliance.

General

- An Vertiv™ Avocent® Universal Management Gateway appliance must have an assigned IP address prior to being added to the Vertiv™ Avocent® DSView™ software.

- The Vertiv™ Avocent® Universal Management Gateway appliance only sends SNMP type 1 traps to the Vertiv™ Avocent® DSView™ software.

- When an Vertiv™ Avocent® Universal Management Gateway appliance is managed using the Vertiv™ Avocent® DSView™ software, the appliance time should be left at UTC and not a specific time zone.

- If the Vertiv™ Avocent® DSView™ software will not accept the upload of the Vertiv™ Avocent® Universal Management Gateway appliance firmware, make the following change to the installed DSView™ software:

  - In the file location C:\Program Files\Vertiv\DSView 4\webapp\WEB-INF\struts-config.xml, update the <controller maxFileSize="1500M"/> line to <controller maxFileSize="2000M"/>, then restart the DSView™ software service or reboot the server.

- An Vertiv™ Avocent® Universal Management Gateway appliance cannot be added to the Vertiv™ Avocent® DSView™ software if the appliance is a target device (such as a terminal server) of another appliance already added to the Vertiv™ Avocent® DSView™ software.

- When the Vertiv™ Avocent® Universal Management Gateway appliance is under heavy processor load and simultaneously is added to Vertiv™ Avocent® DSView™ software, the appliance may be added without targets. Please either resync the appliance or delete and re-add the appliance after the processor load is reduced to complete the discovery of the target devices managed by the appliance.

- The display of targets in the Vertiv™ Avocent® Universal Management Gateway appliance unit view of the Vertiv™ Avocent® DSView™ software is slower when there are many targets added to the appliance.

- When connecting SSH sessions to the Vertiv™ Avocent® Universal Management Gateway appliance through the Vertiv™ Avocent® DSView™ software using the Internet Explorer browser, the PuTTY viewer must be selected in the Vertiv™ Avocent® DSView™ software. If the Chrome browser is used, then the built-in Java viewer must be selected in the Vertiv™ Avocent® DSView™ software. Firefox can use either serial viewer application, except that for browser version 21, the plugins.load_appdir_plugins value must be set to true from the about:config screen to enable the PuTTY viewer to be launched.

- Configuration performed on the *Target Settings-KVM Settings-Defaults* screen does not work correctly for appliance firmware versions 2.8.1.13 and older used with plug-in version 3.1.3.12 and newer.

- Appliance or target event handling or logging is not yet supported through the Vertiv™ Avocent® DSView™ software.

- Disabled port status update is not yet supported through the Vertiv™ Avocent® DSView™ software unless Unit Status Polling is enabled.

- Dial-up functionality is not yet supported through the Vertiv™ Avocent® DSView™ software.

- Appliance backup or restore is not yet supported through the Vertiv™ Avocent® DSView™ software.

- If a target device is moved to a different private port on the appliance, an Appliance Resync in the Vertiv™ Avocent® DSView™ software is required to update the port number in the Vertiv™ Avocent® DSView™ software.

Service Processor (SP)

- The control of Service Processor indicators using the Vertiv™ Avocent® DSView™ software is now only functional for appliance versions 2.9.0.25 and later, using plug-in versions 3.1.0.18 and later. Use the appliance web UI as needed to work around this issue.

- Serial-over-LAN sessions launched from the Avocent® DSView™ software are shown as serial sessions in the Vertiv™ Avocent® DSView™ software Active Sessions list.

- The Vertiv™ Avocent® Universal Management Gateway appliance now supports Service Processor discovery by assigning the Service Processor hostname. If the same target using a hostname is discovered in multiple appliances which are managed by the Vertiv™ Avocent® DSView™ software, the target will be presented with multiple navigation nodes and other undefined behavior. Please ensure that a Service Processor target is only managed once within the Vertiv™ Avocent® DSView™ software.

- If a blade chassis is added to the appliance with Automatic Topology Update enabled in the Vertiv™ Avocent® DSView™ software, the blades within the blade chassis do not always automatically appear in the Vertiv™ Avocent® DSView™ software. Please execute the Update Topology task within the Vertiv™ Avocent® DSView™ software to complete the discovery of the blades within the blade chassis.

- The KG value within a Service Processor cannot be saved through the Vertiv™ Avocent® DSView™ software for Vertiv™ Avocent® Universal Management Gateway appliance versions less than 2.0.0.0. Please upgrade the Vertiv™ Avocent® Universal Management Gateway appliance firmware to 2.x.x.x or later to resolve the issue.

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

- The Vertiv™ Avocent® DSView™ software does not display the Enclosure LED status for the HP iLo and iLo2 Service Processors.

- When an FSC iRMC Service Processor target is selected in the Vertiv™ Avocent® DSView™ software, the navigation label shows IPMI instead of FSC iRMC.

- The status of a Generic Service Processor is shown in the Vertiv™ Avocent® DSView™ software as *Unit Status Unknown* when it should be shown as *Idle*.

- Merged targets cannot include more than one Service Processor target.

- SPAccess vKVM sessions using HTML5 are not yet supported when using DSView™ proxy mode. Please disable the proxy mode for this function.

- The SPAccess vKVM session to the HP iLO4 Service Processor launched using DSView™ proxy mode is currently failing. Please disable the proxy mode for this function.

- An SPAccess Virtual Media session is currently not launching using the Java viewer to the iDRAC6 blade when the appliance is operating in DSView™ software proxy mode. Use the Vertiv™ Avocent® DSView™ software ActiveX viewer, the appliance web UI or DSView™ software non-proxy mode for this function.

- An SPAccess vKVM session is currently not launching to the iDRAC8/9 or iLO5 blade when the appliance is operating in Vertiv™ Avocent® DSView™ software proxy mode. Use the appliance web UI or DSView™ software non-proxy mode for this function.

- Two SoL Session tools are displayed for the Cisco UCS-B blades.

- Power information is not available from Dell M600, M605 or M805 blades. The error message *SPM_RESULT_MEMORYERROR* may be displayed.

- SSH and Telnet session launches to Service Processor chassis are currently not functional using the Vertiv™ Avocent® DSView™ software. Please use the appliance web UI for these launches.

Power Distribution Unit (PDU)

- Power Distribution Unit (PDU) firmware update is not yet supported through the Vertiv™ Avocent® DSView™ software.

- For best results, outlet power control operations from the appliance unit view and outlet unit overview should be performed slowly and only using one outlet at a time. Cycle operations should be avoided.

- For best results, outlet power control functions from the *Outlet-Properties* navigation of the outlet unit overview should be performed slowly.

- Outlet transition notifications are not always received from the appliance.

- A "PDU thresholds Configuration - Bulk Edit" operation option is unintentionally presented for any PDU managed through the Vertiv™ Avocent® Universal Management Gateway appliance. This operation is not functional and should not be used.

- If an outlet of a PDU managed by the Vertiv™ Avocent® Universal Management Gateway appliance was set to Locked Off prior to adding the appliance to the Vertiv™ Avocent® DSView™ software, the outlet state will be displayed as "Idle" in the Vertiv™ Avocent® DSView™ software.

KVM/UMIQ Module

- Use the appliance web UI to convert the UMIQ-V2 module to a UMIQ-E module.

- KVM sessions may only be launched from 32-bit browser clients when using the Vertiv™ Avocent® DSView™ software.

- Virtual media sessions are not functional within KVM sessions launched from the Avocent® DSView™ software when the client is running Java 9. For this scenario, Java 8 must be used.

- KVM sessions launched from Chrome version 42 and greater cannot be launched until the NPAPI is enabled.

  To enable NPAPI:

  1. Browse to **chrome://flags/#enable-npapi.**
  2. Click *Enable* for the Enable NPAPI configuration option.
  3. Click *Relaunch* at the bottom of the configuration page.

- If KVM viewer installation issues are seen when using the Firefox browser version 21 and later with the Vertiv™ Avocent® DSView™ software, please browse to **about:config** in the browser and change the plugins.load_appdir_plugins value to *true*.

- If KVM viewer installation issues are seen when using the Internet Explorer browser with the Vertiv™ Avocent® DSView™ software, please complete the following steps.

  To troubleshoot issues when using IE with the Vertiv™ Avocent® DSView™ software:

  1. In a separate tab, browse to **https://<DSView-IP>/DSView/applets/AvctInstall32.cab#Version=5,04,04,317**.
  2. Save the cab file to the hard disk and expand the contents into a folder.
  3. Execute the *AvctInstall32.ba*t file to complete the viewer installation.

- If KVM data is encrypted on a KVM session, the appliance must be connected to the Vertiv™ Avocent® DSView™ software in secure mode.

- If KVM data is not encrypted but a KVM session cannot be established, the appliance must be connected to the Vertiv™ Avocent® DSView™ software in secure mode.

- A KVM session launched from the Vertiv™ Avocent® DSView™ software may be preempted by a KVM session launched from the appliance, even if the preemption level of the appliance is less than the preemption level of the Vertiv™ Avocent® DSView™ software. Please avoid these conflicts.

- HTML5 KVM sessions are not yet supported when using DSView™ software proxy mode. Please disable the proxy mode for this function.

- HTML5 KVM scan mode sessions are not yet supported; use the Legacy ActiveX viewer for this function.

- Virtual Media sessions are not functional within HTML5 KVM sessions launched from the Vertiv™ Avocent® DSView™ software, unless the Use Dedicated WS Port setting is enabled in the appliance. Browse to *Administration – Targets - KVM Management - Defaults* to enable this setting.

- When using the Vertiv™ Avocent® DSView™ software Legacy Java or ActiveX viewers with the appliance, please disable mouse synchronization so that the mouse will remain available for subsequent KVM sessions launched through the Vertiv™ Avocent® DSView™ software. The current Java and ActiveX viewers in the Vertiv™ Avocent® DSView™ software do not have this limitation.

- UMIQ module offline status update is not yet supported through the Vertiv™ Avocent® DSView™ software unless Unit Status Polling is enabled.

- If UMIQ module names are not automatically pulled into the Vertiv™ Avocent® DSView™ software from the Vertiv™ Avocent® Universal Management Gateway appliance, please ensure the setup and configuration is set as follows:

  - SNMP Traps should be enabled and flowing between the Vertiv™ Avocent® Universal Management Gateway appliance and the Vertiv™ Avocent® DSView™ software.

  - SNMP traps from the Vertiv™ Avocent® Universal Management Gateway appliance should be directed to the correct Vertiv™ Avocent® DSView™ software. Check this from the appliance Unit Overview. The *Appliance Settings-Users-Authentication-Authentication Servers-DSView software* setting for Authentication server 1 should be set to the Vertiv™ Avocent® DSView™ software server IP address as seen by the appliance. If this value is incorrect, it may be manually set here, or will be automatically reset by an appliance resync.

  - The following System Settings in the Vertiv™ Avocent® DSView™ software should be enabled:

    - The *System-Global Properties-Units-Synchronization-Auto Name Pull* screen must have the "Pull Names from appliances to DSView automatically" setting enabled.

    - The *System-Global Properties-Units-Synchronization-Auto Topology Update* screen must have the "Delete target devices that no longer have connections" setting enabled.

    - The *System-Global Properties-Units-Deletion* screen must have the "Delete target devices that no longer have connections" setting enabled.

  - If there is still an issue with a name update on an appliance reboot or the adding of a UMIQ module, check the *Target Devices* view and delete any instances where the target name in the Vertiv™ Avocent® DSView™ software database matches the actual target name of the UMIQ module.

- The Vertiv™ Avocent® DSView™ software proxy mode selection overrides the UMIQ module pass-through mode setting.

Serial Port Targets

- The Vertiv™ Avocent® DSView™ software Serial Viewer will not launch using the Chrome browser version 29. Please use an older or newer version of Chrome.

- If PuTTY serial viewer installation issues are seen when using the Firefox browser version 21 and later with the Vertiv™ Avocent® DSView™ software, please browse to **about:config** in the browser and change the plugins.load_appdir_plugins value to *true*. After the appliance is factory defaulted, serial sessions launched from the Vertiv™ Avocent® DSView™ software with an Vertiv™ Avocent® DSView™ software user not defined within the appliance will display some error messages at the start of the launch in the viewer window. These error messages do not indicate a user issue and may be ignored.

- Serial session launch tools for terminal servers are currently not supported. Please use the appliance web UI for this function.

FIPS Operation

- When the appliance is operating in FIPS mode, an MD5-based certificate is used to connect the appliance to the Vertiv™ 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 Vertiv™ Avocent® DSView™ software, then re-added to the 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 Vertiv™ Avocent® DSView™ software and then re-added to the software after the appliance is removed from FIPS mode.

Accessible Targets

If sessions launched to Accessible Targets fail consistently, please resync the appliance to restore normal operation.