

Vertiv™ Avocent® DSView™ 4.5 Management Software

Service Pack 18 (SP18) Release Notes

VERSION 4.5.0.911, FEBRUARY 2025

Release Notes Section Outline

1. Software/Hardware Support
2. Install/Update Instructions
3. Database Backup and Restore Information
4. Language Support Information
5. Client Browser Support Information
6. Viewer Support and Version Information
7. Server Operation System Support Information
8. Change Log Information (Fixed Issues)
9. Known Issues
10. Devices Supported
11. Plug-In Information and Versions
12. Using a Virtual Machine
13. HTML5 Viewer Notes
14. Flash Notes
15. Third-Party Package Support Information

1. Software/Hardware Support

IMPORTANT NOTE: Before upgrading to the Vertiv™ Avocent® DSView™ 4.5 software for any service pack at SP5 or higher, you must validate that your hardware will have full integration software support with this release. The latest status list of hardware compatible with the Vertiv™ Avocent® DSView™ software, as well as links to plug-in downloads, is available here: <http://www.vertiv.com/DSViewDownloads>.

For more information, contact your appropriate Technical Support representative.

2. Install/Update Instructions

NOTE: Prior to upgrading, it is highly recommended that you make a backup of the current Vertiv™ Avocent® DSView™ database using the DSView™ Backup/Restore tool as a safeguard against potential upgrade issues.

NOTE: The Vertiv™ Avocent® DSView™ 4.5 software does not support new installation or upgrades on Linux headless servers.

Ensure you note the following information prior to performing any upgrade procedures:

- You must reboot the Vertiv™ Avocent® DSView™ software application prior to upgrading in order for the upgrade installation to proceed.
- Review this document for any specific information regarding the patches applied to the Vertiv™ Avocent® DSView™ 4.5 software since the last full release; this document is an addendum to the Vertiv™ Avocent® DSView™ 4.5 software user documentation.
- The Vertiv™ Avocent® DSView™ 4.5 software must be installed on a 64-bit server class machine. During the software installation, you have the option to install PostgreSQL or point to an existing instance of the database.

IMPORTANT NOTE: Due to PostgreSQL incompatibility between version 9.4 (used before SP16) and version 14.x (used in SP16, SP17 or later), the backup format for the database has changed. This means that any backup from SP15 or earlier versions will not work when restoring into SP16, SP17

or later. See the Database Backup and Restore Information section of these release notes for details on migrating to SP17 from previous versions (SP15 or earlier) of the Vertiv™ Avocent® DSView™ software. If you need additional support with the installation, backup and restore process, contact your Technical Support representative.

- Installation failures in a user's customized environment are possible in certain instances. For example, if you installed AlmaLinux 8.5 in Server only mode rather than in Server with GUI mode, the LZ4 compression library will be missing in the OS; this causes the Postgres database to fail execution. When that occurs, it prevents the pre-installation backup attempt by the Vertiv™ Avocent® DSView™ management software from running successfully. In this scenario, you would need to add the LZ4 library to the OS before trying the installation again.
- If you have a customized environment that includes a system/machine under the “control” of a cloud-capable provider, please be aware that your ports and “new or unknown” applications can be severely restrained.

First Time Installation

When installing the software, please ensure the following:

- For the first-time installation scenario, you must be logged in as a local administrator.
- Due to changes in the database format, ensure you create a backup of the new version upon successful installation.
- For Linux, the OS version is now required at the beginning of the installation process.

To install the Vertiv™ Avocent® DSView™ 4.5 software for the first time:

1. Begin the Vertiv™ Avocent® DSView™ software installation using one of the following methods:
 - a. For installation on a supported Windows system:
Run the *setup.exe* and then follow the on-screen instructions.
 - b. For installation on a Linux system:
From a command line, type `./install.bin`, `sh install.bin` or `bash install.bin`, then follow the on-screen instructions.
 - i. For SUSE Linux users:
Update “/etc/hosts” file with <Short-Hostname> of the server. Then, run “hostname <Short-Hostname>” from the command line before installing the Vertiv™ Avocent® DSView™ 4.5 software.
2. On the PostgreSQL Installation screen, select *Existing database* to connect to a remote installation of PostgreSQL or a pre-installed PostgreSQL, or the software will install a Vertiv™ Avocent® DSView™ software pre-included version of the PostgreSQL database.
3. Modify the following PostgreSQL configuration files before using a remote installation of PostgreSQL or an existing PostgreSQL as a Vertiv™ Avocent® DSView™ 4.5 software database:
 - a. Under the PostgreSQL Install Folder/Data folder, append “custom_variable_classes = 'symmetric'” at the end of the `postgresql.conf` file. This is only required for PostgreSQL version 9.0, and not required on version 9.4 or later.
 - b. Under the PostgreSQL Install Folder/Data folder, add “host all all <DSViewServerIP>/32 md5” to the `pg_hba.conf` file.
4. When installation is complete, the Vertiv™ Avocent® DSView™ 4.5 software may be launched from the web browser by accessing the following URL:
<https://<DSViewServerIP>:<DSViewPort>/dsview>

NOTE: If an older version of the Vertiv™ Avocent® DSView™ software was uninstalled from this server, some folders from the old installation may be left behind. To prevent these folders from interfering with the current installation, delete the DSView install folder and PostgreSQL folder before proceeding with the installation. These folders are, by default, located in C:\Program Files (Windows) or /usr/local (Linux).

NOTE: Also, ensure the following information is true on a Windows platform. These suggestions do not apply to every environment, but failed Vertiv™ Avocent® DSView™ software installations have been resolved so far using these recommended steps:

- The Vertiv™ Avocent® DSView™ software and PostgreSQL folders are exempt from all antivirus software scanning
- Secondary Login Services are enabled and started
- Postgres users (or user group) have permissions to `cmd.exe`
- You've right-clicked in the `cmd.exe` shortcut (Start menu) and changed the log in to `%windir%`

Upgrading to the New Service Pack

NOTE: Since this service pack is provided as a full installation package, you cannot manually remove it. You must be logged in as a local administrator, and the service pack needs to be applied to each Vertiv™ Avocent® DSView™ 4.5 server (hub and spoke).

IMPORTANT NOTE: This release can only be upgraded from SP17. If using an older version, upgrade the firmware to SP17 prior to applying SP18 in order to migrate the database contents to the new format.

To upgrade to this release:

1. Perform a replication on all spokes in the current system.
2. Back up the Vertiv™ Avocent® DSView™ 4.5 server.
3. Clear the existing Vertiv™ Avocent® DSView™ software installation directory by deleting all files contained in the directory (for example: /usr/local/Vertiv/DSView_4/).
4. Begin the Vertiv™ Avocent® DSView™ 4.5 software installation using one of the following methods:
 - a. For installation on a supported Windows system:
Run the *setup.exe* and then follow the on-screen instructions.
 - b. For installation on a Linux system:
From a command line, type `./install.bin`, `sh install.bin` or `bash install.bin`, then follow the on-screen instructions.
 - i. For SUSE Linux users:
Update "/etc/hosts" file with <Short-Hostname> of the server. Then, run "hostname <Short-Hostname>" from the command line before installing the Vertiv™ Avocent® DSView™ 4.5 software.

3. Database Backup and Restore Information

When performing backup and restore operations for Vertiv™ Avocent® DSView™ management software, certain criteria must be met due to the upgrade of the background PostgreSQL database.

NOTE: The Vertiv™ Avocent® DSView™ management software must be upgraded sequentially from SP15 to a later version. For example, to upgrade the management software from SP15 to SP18, you must first upgrade to SP16, then upgrade to SP17, and lastly upgrade to SP18.

Prerequisites

- The Vertiv™ Avocent® DSView™ software installation must be freshly installed. You must start with an empty directory that will house the installed Vertiv™ Avocent® DSView™ software files.
- Ensure that the only PostgreSQL database installed on the system is version 14; if other PostgreSQL versions are on the system, uninstall them.
- The Vertiv™ Avocent® DSView™ 4.5 backup and restore utility must use the default PostgreSQL port (5432) available on localhost, which is configured during the Vertiv™ Avocent® DSView™ 4.5 software installation.

Instructions

To perform backup and restore operations:

For Windows users, an error occurs during the backup and restore process using the *DsviewBackupRestore.exe* utility. Ignore this error since it will not impact the backup and restore process; it occurs due to the different database formats.

-or-

For Linux users (Red Hat/SUSE/CentOS), use the credentials provided in the Vertiv™ Avocent® DSView™ software backup .zip file during the backup and restore process (if you have not changed the credentials to your own). The file is: `sudo ./DSViewBackupRestore.sh -restore -archive /tmp/dsviewBackup.zip`

NOTE: During the restore process, you may encounter a series of TOC (TableOfContents) errors. This is expected since the TOC may be different due to variations in the PostgreSQL versions. However, even with the errors, the data should still be processed correctly.

4. Language Support Information

The languages supported by this version of the Vertiv™ Avocent® DSView™ software are English, Simplified Chinese and Japanese.

5. Client Browser Support Information

NOTE: Unless noted otherwise, both 32-bit and 64-bit browsers are supported.

- Mozilla Firefox (125.0.3)
- Google Chrome (124.0.6367.203)
- Microsoft Edge (124.0.2478.97)

6. Viewer Support and Version Information

The following table lists browser/viewer combinations successfully tested with a representative selection of client operating systems.

NOTE: Latest versions of the Mozilla Firefox browser on a Windows client no longer support ActiveX, so all ActiveX viewers are now eliminated from use on this browser.

Tested Browser and Viewer Combinations

CLIENT SYSTEMS	JAVA/SERIAL VIEWER	ACTIVE X SERIAL VIEWER	HTML5 SERIAL VIEWER	LEGACY JAVA KVM VIEWER	LEGACY ACTIVE X KVM VIEWER	JAVA KVM VIEWER	ACTIVE X KVM VIEWER	HTML5 IDRAC VIEWER*	HTML5 KVM VIEWER
Chrome 53 32-bit	YES	NO	YES	YES	NO	YES	NO	YES	YES
Chrome 53 64-bit	YES	NO	YES	YES	NO	YES	NO	YES	YES
Firefox 45 ESR 32-bit For Windows Client	YES	NO	YES	YES	NO	YES	NO	YES	YES
Firefox 45 ESR 32-bit For Linux Client	YES	NO	YES	YES	NO	YES	NO	YES	YES
Firefox 45 ESR 64-bit For Linux Client	YES	NO	YES	YES	NO	YES	NO	YES	YES
Firefox 45 ESR 32-bit For Mac OS Client	YES	NO	YES	YES	NO	YES	NO	YES	YES
Microsoft Edge	YES	NO	YES	YES	NO	YES	NO	YES	YES

NOTE: *Suitable for iDRAC 7 and 8 running firmware version 2.30.30.30 and higher.

Service Pack 18 (SP18) Viewer Versions

VIEWER	JAR/EXE	VERSION	OS PLATFORM
Video Viewer	AvctVideoViewer.exe	3.5.2.3	Win32
Virtual Media	AvctVirtualMedia.exe	3.5.1.7	Win32
VNC Viewer	avctVncViewer.exe	2.1.1.1	Win32

VIEWER	JAR/EXE	VERSION	OS PLATFORM
RDP	avctRdpViewer.exe	1.3.0.5	Win32
3rd Party/Serial	AvctSerialViewer.exe	3.7.0	Win32
Putty	AvctPuttyTel.exe	0.64	Win32
Java Video Viewer	avctvideoviewer.jar	4.16.2.7	Linux/Mac
Java Serial Viewer	avctsshtelnet.jar	4.6.1.18	Linux/Mac
Java Virtual Media	avctVM.jar	1.8.0.91	Linux/Mac
Java VNC Viewer	avctVncViewer.jar	4.6.2.12	Linux/Mac
Java 3rd Party/Serial	serialconsoleviewer.jar	4.6.1.16	Linux/Mac
New ActiveX KVM Viewer 32-bit	AvctInstall32.cab	5.04.04.406	Win32
New ActiveX KVM Viewer 64-bit	AvctInstall64.cab	5.04.04.406	Win64
New Java KVM Viewer	avctVideo.jar	5.04.04.463	Win/Linux/Mac
HTML5 KVM Viewer	N/A	1.10.22	Win/Linux/Mac
HTML5 Serial/SSH Viewer	N/A	2.0.3	Win/Linux/Mac

7. Server Operation System Support Information

- Microsoft Windows Server 2008 R2 (x64), 2012 R2 (x64), 2019 (x64), 2022
- SUSE Linux Enterprise Server 15.4 (x64), openSUSE 15.4 (x64) only
- Red Hat Enterprise Server 7.3 (x64), 7.5 (x64), 7.9 (x64), 8.2 (x64), 8.5 (x64), 8.10 (x64)
- CentOS 7.4, CentOS 7.5, CentOS 7.8, CentOS 7.9, CentOS 8.2
- AlmaLinux 8.5 (x64), 8.6 (x64), 8.8 (x64), 8.10 (x64)

8. Change Log Information (Fixed Issues)

Fixed Issues (Release: SP18)

ISSUE #	DESCRIPTION
CAS-53523-W7K0V5 / CA-000796337	Fixed issue where a user who does not belong to the Administrator or Appliance Administrator user group is able to create exclusive unit groups.
CA-0000625544	Fixed issue where a database replication between a hub and a spoke will periodically fail due to timeouts.
Enhancement	Multiple security improvements: <ul style="list-style-type: none"> • Updated cipher lists • Remediation for several CVEs
N/A	Fixed issue where the blade chassis plug-in may be uninstalled when the Vertiv™ Avocent® DSView™ 4.5 management software is upgraded to SP17 and cannot be re-added to the management software.
N/A	Fixed issue where loading of a plug-in fails when the Vertiv™ Avocent® DSView™ 4.5 management software is running on a Linux environment.

Historical Fixed Issues (Previous Release: SP17)

ISSUE #	DESCRIPTION
CAS-59241-L0P9V4 / CAS-56199-Y5C3H4 / CA-0000765063	Fixed issue where the management software stops communicating with Vertiv™ Avocent® ACS appliances if restricted to only allow the use of TLS v1.3
CA-0000796343 / CAS-53697-P8G3W9	Fixed UI issue where a user can select both "deny" and "allow" at the same time on the access rights setup page
CA-0000764754 / CAS-69280-W2D8H2	UMG Plugin: Removed residual reference to Log4j functionality within plugin
Enhancement / CA-0000617545	Updated webserver libraries
CA-0000765880 / CAS-65153-R5Z9Q1	Upgraded the PostgreSQL database to version 14.8
Enhancement / CA-0000793005	Upgraded Amazon Corretto 8 Java to version .382
Enhancement	Removed duplicate event log entries for user group "Everyone"
Enhancement	Multiple security improvements: <ul style="list-style-type: none"> • Updated cipher lists • Improved protections for data and passwords at rest • Remediation for several CVEs

ISSUE #	DESCRIPTION
Enhancement / CA-0000934387	<p>Fixed issue related to weak ciphers with the SSH server. In this case, a modification of the system.properties file is required to allow strong ciphers. The user may modify the SSH.Server.Secure.Level security setting with the following values: NONE, WEAK, STRONG, STRONG_PLUS or PARANOID</p> <p>The default level NONE (SP13) has increased to WEAK (SP14). The user has the option to increase the security level beyond the default level.</p> <p>The system.properties file is located under the folder \[DSViewInstallFolder]\etc.</p> <ul style="list-style-type: none"> On Windows, the system.properties file is located under the folder C:\Program Files\Vertiv\DSView 4\etc. On Linux, the system.properties file is located under the folder /usr/local/Vertiv/DSView_4/etc. Below is an example of how to specify the SSH server security level in the system.properties file: <pre>SSH.Server.Secure.Level=STRONG_PLUS</pre> <p>After the system.properties has been modified, you need to restart the DSView service.</p>

Historical Fixed Issues (Previous Release: SP16)

ISSUE #	DESCRIPTION
CAS-54611-M9J5X5	Fixed issue where an error message was displayed when opening the user interface (UI) page after an upgrade to SP15
CAS-53832-K6V0Z8	Fixed logic that kept remote devices such as the Vertiv™ Avocent® ACS advanced console system from authenticating users via the Vertiv™ Avocent® DSView™ management software
CAS-53984-Q9N6Q4	Addressed issue with SP15 that would not allow the user to set an expiration date for internal Vertiv™ Avocent® DSView™ management software accounts
CAS-51877-N4M0M1	Fixed error encountered during new Vertiv™ Avocent® DSView™ management software user logins when done in combination with MFA
FER CAS-48082-P4F8W9	Upgraded the PostgreSQL database to version 14.3
CAS-50606-T8T5K4	The system will now properly apply the list of customer-specified ciphers via the UI
CAS-55411-T0B8L3	HSTS headers now available for HTTPS server exchanges
CAS-54611-M9J5X5	Addressed issue where User Administrators were previously unable to view the UI page
Enhancements	<ul style="list-style-type: none"> Upgraded Java JRE to Corretto8 MFA settings are now correctly copied to a Vertiv™ Avocent® DSView™ management software spoke after initial spoke replication Windows installation now allowed to non-default locations

Historical Fixed Issues (SP15)

ISSUE #	DESCRIPTION
CAS-47411-C688W1	Mitigated log4j vulnerabilities (library updated to a newer version)
CAS-43652-C7R8X2	AD user SSH session failing when launching from a Vertiv™ Avocent® ACS8000 advanced console system
CAS-42325-X0D5F7	Ability to disable the Java client

ISSUE #	DESCRIPTION
CAS-31518-L0Q7T9	Issues launching the HTML5 Viewer for a Vertiv™ Avocent® ACS800 advanced console system
CAS-41788-K7VU9	Email notification not working
CAS-42311-D3Z456	jQuery updated to version 3.6.0
CAS-40347-J5Z8Q6	Web service API authentication and zone support
CAS-40347-J5Z8Q6	Support for Vertiv™ Leibert® GXT5 UPS
CAS-39954-W8W0D4	Notify the user of the date and time of their last successful logon
CAS-36801-V9P7G4 CAS-36801-88Z5C1	Replacement of Bulk Edit capability from Flash
CAS-40925-F6H3R7	Postgres and Java vulnerabilities mitigated
CAS-48543-M0J3D5	Vertiv™ Geist PDU SNMPv3 AES support
CAS-32035-S2L2S7	Vertiv™ Avocent® DSView™ software support for ESX 7.0
CAS-34103-Y1X8D1	User Administrators are able to create new Vertiv™ Avocent® DSView™ software administrators; limit the User Administrator role to not be able to create higher-privilege users
CAS-39544-J8H5J0	Mitigated Java vulnerabilities
CAS-46435-B3V0V1	Deleting user removes associated tasks without warning
CAS-48151-F2T1Q4 CAS-48980-H7D5S5	Serial session issue when using the Vertiv™ Avocent® DSView™ software with a Vertiv™ Avocent® Universal Management Gateway appliance
CAS-47627-V6V2J7	The Java KVM session failed with the following error message: <i>The viewer has been terminated. Reason: the network connection has been dropped.</i>
Enhancement	<ul style="list-style-type: none"> • TLS 1.3 supported as an option for internet exchanges that utilize TLS1.2 • HTML5 Viewer not launched when using MAC OSX • Updated event type for replication error and modified ordering of uploaded file type • Security headers enabled on all web pages

Historical Fixed Issues (SP14.1)

ISSUE #	DESCRIPTION
CAS-41540-P7X6S5 CAS-42312-T9N8P2	Updated the PostgreSQL database to Version 9.4.26.
CAS-45071-N4D1V2	Fixed the Vertiv™ Avocent® DSView™ Server Certificate Wizard to generate a self-signed SSL server certificate with a correct Organization field and a present Organization Unit field.
CAS-45069-R9J9Z8	Fixed SP14 issue involving Vertiv™ Avocent® DSView™ SSH authentication with passthrough. The use case: "Establish a Putty SSH connection to a Vertiv™ Avocent® DSView™ serial target device using a private key file for authentication." NOTE: Putty version 0.74 (and earlier versions) does not exhibit the issue with SP14.

ISSUE #	DESCRIPTION
CAS-42325-X0D5F7	In the Vertiv™ Avocent® DSView™ Web API, the user has the option to disable the API. The system.properties file is located at \[DSViewInstallFolder]\etc\ For example, the default Windows install folder is c:\Program Files\Vertiv\DSView 4\etc. Example setting: API.DISABLE=1
CAS-42328-Y9T2W4	SSL re-negotiation is disabled.
CAS-42306-Z4S0Q5	The SSL cipher list has been modified.
CAS-46064-G0C0B7 CAS-39332-D4Q8B5	Fixed the issue where the HTML5 KVM session was opening to a black screen.

Historical Fixed Issues (SP14)

ISSUE #	DESCRIPTION
N/A	<ul style="list-style-type: none"> Previous Vertiv™ Avocent® DSView™ software releases have used Flash-based technology for several pages; however, mainstream browsers are ending support of Adobe Flash on 12/31/2020. Beginning with SP13, the information contained in the following pages may be obtained through a different method: <ul style="list-style-type: none"> Unit Status page: The user may view the status for all units by accessing the <i>Units View</i> page and clicking on the appropriate unit filter (<i>Appliances</i> or <i>Target Devices</i>, for example) on the left navigation panel. The status for each unit is displayed in the Status column. Appliance Versions page: The user may view the list of appliance versions by creating a system task, exporting a report that contains the list of firmware versions for each appliance, and then filtering the report to the get firmware versions for each appliance type. Connections page: <ul style="list-style-type: none"> Merge targets by accessing the Unit Overview page or using the merge operation in Unit View. Launch sessions from the Unit Overview page or by using <i>Action</i> in Unit View. Perform power operations from the Unit Overview page or by using <i>Power Operation</i> in Unit View. Check the topology from the Unit View page. Renewed the CA signed certificates in the Java and ActiveX viewers for three more years. IMPORTANT NOTE: Old viewer certificates expire on 9/26/21. If you are unable to update to SP14 until after that date, you may perform a new viewer-only upgrade. See section 13 of these release notes for additional details and instructions on upgrading the viewers.
CAS-34645-M0Q1Q0	<p>This issue is in regard to weak ciphers with the SSH server. In these cases, modification of the system.properties file is allowed. The user may modify the SSH.Server.Secure.Level security setting with the following values: NONE, WEAK, STRONG or PARANOID</p> <p>The default level NONE (SP13) has increased to WEAK (SP14). The user has the option to increase the security level beyond the default level.</p> <p>The system.properties file is located at \[DSViewInstallFolder]\etc\. For example, the default Windows install folder is c:\Program Files\Vertiv\DSView 4\etc.</p> <p>Example setting: SSH.Server.Secure.Level=STRONG</p>

ISSUE #	DESCRIPTION
FERS	<ul style="list-style-type: none"> Added support to the Vertiv™ Avocent® MergePoint Unity™ KVM over IP and serial console switch plug-in to push outlet names from the Vertiv™ Avocent® DSView™ software for all Geist™ Power Distribution Units (PDUs) and Liebert® MPH PDUs. Enhanced HTML5 serial viewer that includes search functionality and expanded history. Enhanced HTML5 VMware viewer to support proxy configuration.
CAS-36099-S2F3N6 CAS-35688-M5X2M4	Added support to the remote HTTPS server to enforce HTTP Strict Transport Security (HSTS).
CAS-23996-M3H8D6	Added more detailed information to the database backup task to provide the customer with better visibility in regard to potential database failure.
CAS-24914-BOJ3T2	Fixed JRE vulnerabilities by updating the JRE version to 1.8.0 Update 202.
CAS-32717-Y8W5L8	Modified the initial MFA login process to stop during initial login and use the MFA tools (token) rather than allowing the first login to continue.
CAS-25043-C8J2J5 CAS-36205-H0J6P5 CAS-37022-R4N7W5	The Subject Alternative Name (SAN) is now included in the Certificate Signing Request (CSR).
CAS-36799-BOX5X1 CAS-37615-P5Y3B4 CAS-36507-Q9D7Z6	Upgraded PuTTY viewer to version 0.73 to resolve a cipher mismatch with Vertiv™ Avocent® ACS 6000 advanced console servers and Vertiv™ Avocent® ACS8000 advanced console systems.
CAS-43652-C7R8X2	Resolved issue where AD users launching SSH HTML5 viewer sessions experienced failing sessions.
CAS-25044-R4N8W3	Added support to allow the Vertiv™ Avocent® DSView™ software to establish an HTML5 KVM session to a Dell M1000E blade cascaded off of a Vertiv™ Avocent® MergePoint Unity™ switch.

9. Known Issues

This release contains the following known issues:

- If you are running the Vertiv™ Avocent® DSView™ 4.5 software SP17 on a Windows system and you need to uninstall DSView™ 4.5 software SP17 to perform a fresh installation of SP16, the installation might get stuck at 100% complete and not allow you to continue. To prevent this issue, uninstall the "Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.40664" package from the Windows server using the control panel.
- Launching of the Vertiv™ Avocent® DSView™ 4.5 software application from a web browser URL with only the IP address or DNS host name of the Vertiv™ Avocent® DSView™ server may display an "HTTP ERROR 404 Not Found" error message. Make sure to include the text "/dsview" after the IP address or DNS host name of the Vertiv™ Avocent® DSView™ server in the web browser URL.
- Unable to configure individual outlets from Vertiv™ Liebert® GXT4 and Vertiv™ Liebert® GXT5 outlet groups.
- Linux Environments: User must manually update the file folder permissions to avoid an error uploading appliance files via the UI.
- The Java Viewer is not supported for AlmaLinux 8.5.
- The Java Viewers (Serial, Video and VNC) may not launch when using Java Runtime Environment (JRE) versions less than 1.8.0.72.
- Legacy viewers support 32-bit browsers only.
- The RDP Viewer and Putty will not work if the client machine does not have the Microsoft Visual C++ 2010 SP1 Redistributable Package (x86) installed. While the RDP Viewer works in IE11, it does not work with Windows OS versions higher than Windows Server 2012.

- For a Vertiv™ Avocent® Universal Management Gateway appliance target, the HTML5 Proxy will not work if Use dedicated WSS port is enabled on the appliance side.
- It will be necessary to download the VMware VMRC 10.0.4 or above in order to launch the VMware Viewer.
- Prior to launching the HTML5 VMware Viewer, you must trust or accept the VMware ESX Server/VC certificate.
- The Vertiv™ Avocent® DSView™ software dial-out from Linux requires root access.
- There is a known issue when attempting to upgrade from Vertiv™ Avocent® DSView™ software version 4.5.0.190 or older versions to DSView™ software version 4.5.0.247 or newer versions on CentOS 7 and Red Hat 7. The workaround for this issue is to perform a database backup of the current Vertiv™ Avocent® DSView™ version, do a fresh install of the newer DSView™ software version and restore the database using the backup. For a spoke, delete the spoke from the hub, do a fresh install on the spoke server and re-register to the hub.
- An open Java-based viewer session will not automatically be closed by the Vertiv™ Avocent® DSView™ software if you log out of the software. This is a side effect of removing Java support from the browsers.
- You should not use hostnames (DNS defined names) for addressing appliances. Use the IP address only.
- The Vertiv™ Avocent® DSView™ software does not support NTLM SSO for Windows Server 2012 and Windows Server 2016.
- The JCE Extension Library needs to be downloaded to support Kerberos SSO on Windows 2016.
- SUSE11 installs requires at least 8GB memory.
- The Digi Rapidport/4 USB modem is not compatible with Windows Server 2016.
- The Vertiv™ Avocent® DSView™ software no longer supports Kerberos SSO in a Windows Server 2008 OS.

10. Devices Supported

Vertiv™ Devices

- Avocent® ACS 6000 advanced console servers
- Avocent® ACS8000/800 advanced console systems
- Avocent® AutoView 2108/ 2216 and 3108/3216 switches
- Avocent® MergePoint Unity™ 1016, MergePoint Unity™ 1016DAC, MergePoint Unity™ 104E, MergePoint Unity™ 108E, MergePoint Unity™ 108EDAC, MergePoint Unity™ 2016, MergePoint Unity™ 2016DAC, MergePoint Unity™ 2032, MergePoint Unity™ 2032DAC, MergePoint Unity™ 4032, MergePoint Unity™ 4032DAC, MergePoint Unity™ 8032 and MergePoint Unity™ 8032DAC KVM over IP and serial console switches
- Avocent® Power Management Distribution Unit (PM PDU) PM 1000/2000/3000 PDUs
- Avocent® SPC power control devices
- Avocent® Universal Management Gateway 2000, 4000 and 6000 appliances
- Geist™ Upgradeable PDU GU2 and R-Series (RCM, RCU) rack PDUs running firmware 5.3.0 or later.
- Liebert® GXT4/GXT5 UPS devices
- Vertiv™ MPH2™ rack PDUs (with RPC-2000 cards), Liebert® MPH rack PDUs, and Vertiv™ MPX™ rack PDUs (with RPC-1000/RPC-2000 cards)

Other Devices

- APC AP78xx, AP79xx, AP8881, AP8661 and AP8941 PDUsD
- Blade, Dell DRAC MC, Dell M1000e, FSC BX600, Generic Blade Chassis, HP BladeSystem, HP BladeSystem c-Class, HP BladeSystem p-Class, IBM BladeCenter, IBM BladeCenter H, IBM BladeCenter HT, IBM BladeCenter T
- Citrix XenServer 6.5 Standard

- Dell 2161DS-2, Dell 2321DS, Dell 4161DS and Dell 8321DS appliances
- Dell Remote Console Switch (1082DS/2162DS/4322DS) product family
- FCL Plug-in to support FW Digital KVM Switch product line FW-D1008NP, FW-D2016NP, FW-D2032NP, FW-D4016NP, FW-D8032NP
- Fujitsu KVM s4 Appliance product family KVM s4-0812, KVM s4-1622, KVM s4-3242
- HP Console Switch G2 product family Server Console Switch G2 0x2x16, Server Console Switch G2 0x2x32, IP Console Switch G2 1x1Ex8, IP Console Switch G2 2x1Ex16, IP Console Switch G2 4x1Ex32
- HP G3 KVM Console Switch 0x1x8 G3 KVM Console Switch, 0x2x16 G3 KVM Console Switch
- IBM Console Switch GCM16/32 product family
- KVM Switch product family: 1x1x8 switch, 2x1x16 switch, 8x1x32 switch
- Lenovo GCM 16/32 console switch product family
- Lenovo LCM 8/16 switch product family
- Microsoft Hyper-V2 on Windows 2008 R2
- Microsoft Hyper-V3 on Windows 2012 and 2012 R2
- MPI Intelligent PDU family
- Server Technologies Sentry Switched CDU CW-8H1*, CW-8H2*, CW-16V1*, CW-16V2*, CW-24V2*, CW-24V3*, CW-32VD1*, CW-32VD2*, CW-48V5Z454-A1P, CW-24VY-L30M, CWG-24V4Z423A9/QR, CW-8H1A413, CW-24V4K425A9, STV-4501C, STV-6502M and STV-4501C (supported models may change; contact Technical Support for current information)
NOTE: Models with an asterisk (*) must be attached to a managed appliance such as the Vertiv™ Avocent® MergePoint Unity™ KVM over IP and serial console switch.
- VMware 6.0, VMware 6.5 and VMware 6.7

11. Plug-in Information and Versions

NOTE: All plug-ins listed below are shipped with the Vertiv™ Avocent® DSView™ software. Pre-Installed plug-ins are automatically loaded into the Vertiv™ Avocent® DSView™ software and are ready for use. Optional plug-ins must be loaded into the Vertiv™ Avocent® DSView™ software to be used. It is recommended that only plug-ins that will be used be loaded.

NOTE: The minimum recommended plug-in versions to be used with this software version are listed in the table that follows.

- Please see the Vertiv™ Avocent® Universal Management Gateway appliance plug-in release notes for features affecting this plug-in in this release of Vertiv™ Avocent® DSView™ software. The release notes are available at www.vertiv.com.
- Please use the recommended Virtualization plug-in version with the Vertiv™ Avocent® DSView™ software for support for vMotion and Microsoft VMM. This version of the software supports SCVMM 2008 installed on Windows 2008 R2 and SCVMM 2012 installed on Windows 2012 R2.

PLUG-IN	VERSION	PRE-INSTALLED/OPTIONAL
Vertiv™ Avocent® ACS8000 console system	2.26.2.1	Pre-installed
Vertiv™ Avocent® ACS 6000 console server	3.7.0.5	Pre-installed
Vertiv™ Avocent® MergePoint Unity™ KVM over IP and serial console switch	2.10.0	Pre-installed
Vertiv™ Avocent® Power Management Distribution Unit (PM PDU)	2.0.1.8	Pre-installed
Vertiv™ Avocent® Universal Management Gateway appliance	4.5.0.18	Pre-installed
Blade Chassis support	1.2.0.55	Pre-installed
Vertiv™ RPC2 and Rack PDU support	1.1.2.4	Pre-installed

PLUG-IN	VERSION	PRE-INSTALLED/OPTIONAL
Infrastructure	2.0.0.20	Pre-installed
Vertiv™ Liebert® Rack PDU support	1.1.0.31	Pre-installed
Virtualization	3.0.0.701	Pre-installed
APC MasterSwitch RPDU support	4.0.0.15	Optional
Vertiv™ Avocent® AutoView™ switch	1.31.0.4476	Optional
Vertiv™ Avocent® AutoView™ switch for Dell	1.31.0.4476	Optional
Dell Remote Console Switch (1082DS/2162DS/4322DS)	2.8.3	Optional
Fujitsu KVM s4 Appliance	1.32.0.24542	Optional
Vertiv™ Geist™ rPDU	1.0.0.24	Optional
HP G2 Console Switch	2.3.7.25473	Optional
HP G3 KVM Console Switch	2.3.7.25473	Optional
IBM Console Switch GCM16/32	2.3.0.25179	Optional
Lenovo GCM 16/32 Console Switch	2.3.0.25179	Optional
Lenovo Local Console Manager (LCM) Switch	1.30.0.4476	Optional
Vertiv™ Liebert® GXT4 or GXT5 UPS devices	1.0.0.445	Optional
MPI PDU	1.0.0.22	Optional
Server Tech Sentry 3 PDU	1.0.0.43	Optional
Server Tech Sentry 4 PDU	1.0.0.12	Optional

12. Using a Virtual Machine

You may set up the Vertiv™ Avocent® DSView™ management software to run on a Virtual Machine (VM). The following specifications are recommended as baseline resources for installing the Vertiv™ Avocent® DSView™ software. Depending on the size of the Vertiv™ Avocent® DSView™ software database, these specifications may need to be increased to improve software performance.

NOTE: VMware administrators should monitor the performance of the VM to ensure that the appropriate resources are provided to support the software system.

Recommended VM Requirements for Running the Vertiv™ Avocent® DSView™ Software

NOTE: It is recommended that vMotion and Ballooning be disabled for this VM scenario.

The minimum required specifications for setting up a VM to run the Vertiv™ Avocent® DSView™ software are as follows:

- 6 GB RAM (Reserved)
- 1-2 vCPUs (1 core)
- 40+ GB HDD (<7000 target devices)/ 80+ GB HDD (>7000 target devices)
- 1 NIC dedicated 100% (VMXNET3- 1 GB or 10 GB suggested)

The following best practices are recommended for improved performance on VMs in a VMware environment:

- Verify that the Vertiv™ Avocent® DSView™ software VMs sharing a vSwitch connected via an NIC are not connected to an oversubscribed network switch.
- Verify that the Vertiv™ Avocent® DSView™ software VMs are not connected to an oversubscribed storage LUN.
- Verify that the Vertiv™ Avocent® DSView™ software VMs are not placed on oversubscribed server hardware.
- Ensure there are no issues with switches or ports that are oversubscribed due to too many VMs sharing a single port or VLAN.
- Ensure there is available spare capacity in datastores and ensure you are not queuing during peak business hours.
NOTE: Queuing is when there is not enough IO being processed by your storage unit and reads/writes are backing up (or queuing).
- Monitor all resource thresholds to ensure more hardware resources are added before your warning thresholds are breached. Allowing an ESXi host to be oversubscribed puts its VMs at a risk of poor performance.

13. HTML5 Viewer Notes

- Due to limited resources for HTML5 Viewers with Microsoft Internet Explorer browsers, the All Targets Live option in Scan mode is disabled when using Microsoft Internet Explorer browsers.
- When using the HTML5 Serial Viewer, some systems may require the following:
 - Ensure no pop-up blockers are enabled within the browser and accept the certificate when prompted.
 - Ensure the following TCP ports are not blocked by security services on the network or client:
 - TCP port 443, for use with Vertiv™ Avocent® Universal Management Gateway appliances and Vertiv™ Avocent® ACS8000 console systems
 - TCP port 4206, for use with Vertiv™ Avocent® MergePoint Unity™ KVM over IP and serial console switches
 - When using Internet Explorer (IE), enable Certificate Authentication under the Vertiv™ Avocent® DSView™ software client server Session Properties menu.

14. Flash Notes

- Although Vertiv™ Avocent® DSView™ software releases prior to SP13 used Flash-based technology within some software pages/features, mainstream browsers ended support of Adobe Flash at the end of December 2020. Beginning with SP13, information contained in the following Vertiv™ Avocent® DSView™ software pages may be obtained through a different method:
 - Unit Status page: You may view the status for all units by accessing the Units View page and clicking on the appropriate unit filter (*Appliances* or *Target Devices*, for example) on the left navigation panel. The status for each unit is displayed in the Status column.
 - Appliance Versions page: You may view the list of appliance versions by creating a system task, exporting a report that contains the list of firmware versions for each appliance, and then filtering the report to the get firmware versions for each appliance type.
 - Connections page:
 - Merge targets by accessing the Unit Overview page or using the merge operation in Unit View.
 - Launch sessions from the Unit Overview page or by using *Action* in Unit View.
 - Perform power operations from the Unit Overview page or by using *Power Operation* in Unit View.
 - Check the topology from the Unit View page.
- Links to old Flash-based pages have been removed.
- The CA signed certificates in the Java and ActiveX viewers are renewed for three more years.

IMPORTANT NOTE: Old viewer certificates expired on September 26, 2021. If you did not perform a viewer-only upgrade or update to SP14 before then, your Java and ActiveX viewers may not launch. In this case, ensure you've updated to this service pack.

15. Third-Party Package Support Information

The following table lists third-party packages and versions that are supported by the Vertiv™ Avocent® DSView™ software in different service packs.

Package Versions in Service Packs

VERTIV™ AVOCENT® DSVIEW™ SERVICE PACK	POSTGRESQL	CORRETO 8 JAVA	SSH	JQUERY	JETTY	RELOAD4J
SP16	14.4	8.342	1.7.32	3.6.0	9.2.7	1.2.18.5
SP17	14.8	8.382	1.7.32	3.6.0	9.4.48	1.2.18.5
SP18	14.14	8.432	1.7.32	3.6.0	9.4.56	1.2.18.5