

VERTIV[™] Avocent® AutoView[™]2108/2216 Switch

Firmware Release Notes

VERSION 1.30.2, DECEMBER 14, 2018

Release Notes Section Outline

- 1 Appliance Support Information
- 2 Enhancements
- 3 Fixes
- 4 Notes
- 5 Client/Browser Information
- 6 Java Viewer Session Expired Certificate Information

1 Appliance Support Information

The following appliances are supported with this release.

AUTOVIEW™ SWITCH	FIRMWARE
AV2108	FL0674-AVO-1.30.2.0.4435.fl
AV2216	FL0674-AVO-1.30.2.0.4435.fl

NOTE: Firmware updates to version 1.30.1 and higher are NOT reversible to firmware versions earlier than 1.30.1.

2 Enhancements

This release adds support for the USBIAC2 KVM cable.

3 Fixes

- Updated Java and Active X viewer certificates; see section 6 for more information.
- Fixed issue with Korean language function key not working (L3 #487234-804242745).

4 Notes

Firmware version 1.30.2 requires the Avocent® AutoView[™] switch plug-in, version 1.30.1, if the appliance is to be enrolled in Avocent® DSView[™] management software.



5 Client/Browser Information

NOTE: Microsoft Internet Explorer versions 8 and 9 are no longer supported as client browsers.

The following chart indicates the latest version tested.

SOFTWARE	VERSION
Java	10
Internet Explorer	11
Firefox	63.0.3 (64-bit)
Firefox ESR	60.3.0 ESR (64-bit)
Chrome	Version 70.0.3538.102 (Official Build) (64-bit)

6 Java Viewer Session Expired Certificate Information

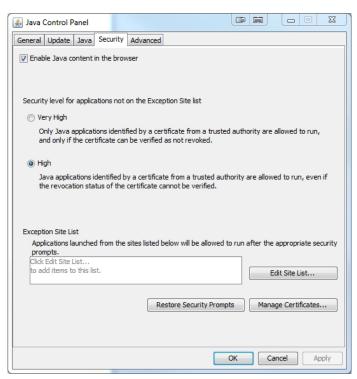
Java serial viewer session certificates existing in older firmware versions are expiring on February 17, 2019.

IMPORTANT NOTE: Unless you update to the newest firmware 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: <a href="http://<a product open-style="color: blue;">http://<a product open-style="color: blue;">http://</a prod

🔹 Exception Site List	
Applications launched from the sites listed below will be allowed to run after prompts.	r the appropriate security
Location Interpretation Interpretatio Interpretation Interpretation Interpretation Interpre	nl
FILE and HTTP protocols are considered a security risk. We recommend using HTTPS sites where available.	Add Remove
	OK Cancel

- 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 expired viewer certificate.

🔬 Java Control Panel 📃 💻 🗙 🖌
General Update Java Security Advanced
☑ Enable Java content in the browser
Security level for applications not on the Exception Site list
🔘 Very High
Only Java applications identified by a certificate from a trusted authority are allowed to run, and only if the certificate can be verified as not revoked.
e High
Java applications identified by a certificate from a trusted authority are allowed to run, even if the revocation status of the certificate cannot be verified.
Exception Site List
Applications launched from the sites listed below will be allowed to run after the appropriate security prompts.
http://10.207.27.117:80
Restore Security Prompts Manage Certificates
OK Cancel Apply

© 2018 Vertiv Co. All rights reserved. Vertiv and the Vertiv logo are trademarks or registered trademarks of Vertiv Co. All other names and logos referred to are trade names, trademarks or registered trademarks of their respective owners. While every precaution has been taken to ensure accuracy and completeness herein, Vertiv Co. assumes no responsibility, and disclaims all liability, for damages resulting from use of this information or for any errors or omissions. Specifications are subject to change without notice.