VERTIV™

Avocent® MergePoint Unity™ KVM over IP and Serial Console Switch

Firmware Release Notes

VERSION 2.2.4, DECEMBER, 2018

Release Notes Section Outline

1 Update Instructions

For detailed instructions on updating your switch, please refer to your user documentation.

WARNING: After upgrading to version 1.18.0.x, the Avocent® MergePoint Unity™ switch cannot be downgraded to a firmware version earlier than 1.18.0.x. For more information, contact Technical Support.

- Attaching the MPUIQ-VMC or DSRIQ-VMC module to a Windows target may require the USB CCID driver to be installed. If you are prompted by the Windows New Hardware Wizard, select the *Next* button.
- For Avocent® Power Management 2003, 2006, 2024, 3003, 3006 and 3024 Power Distribution Units (PM PDUs), version 1.10 firmware or higher is required to manage the PDU from the Avocent® MergePoint Unity™ switch.

2 Appliance Support Information

The following appliances are supported with this release.

MERGEPOINT UNITY™ SWITCH	FIRMWARE
MPU104E	FL0620-AVO-2.2.4.25378.fl
MPU108E	FL0620-AVO-2.2.4.25378.fl
MPU108EDAC	FL0620-AVO-2.2.4.25378.fl
MPU1016	FL0620-AVO-2.2.4.25378.fl
MPU1016DAC	FL0620-AVO-2.2.4.25378.fl
MPU2016	FL0620-AVO-2.2.4.25378.fl

MERGEPOINT UNITY™ SWITCH	FIRMWARE
MPU2016DAC	FL0620-AVO-2.2.4.25378.fl
MPU2032	FL0620-AVO-2.2.4.25378.fl
MPU2032DAC	FL0620-AVO-2.2.4.25378.fl
MPU4032	FL0620-AVO-2.2.4.25378.fl
MPU4032DAC	FL0620-AVO-2.2.4.25378.fl
MPU8032	FL0620-AVO-2.2.4.25378.fl
MPU8032DAC	FL0620-AVO-2.2.4.25378.fl

NOTE: For CentOS targets, use a single or dual mouse cursor with AMS disabled.

3 Fixes

- Updated Java and Active X viewer certificates; see section 8 for more information.
- Fixed issue where syslog events were not sent from the appliance (L3 #487234-840783271).
- Fixed issue where the HTML5 viewer did not support the Swiss/German keyboard layout (L3 #487234-812741935).
- Fixed issue where 32 RIP firmware download would not complete with four SNMP trap destinations.

4 Notes

If the appliance is going to be enrolled in the Avocent® DSView™ management software, firmware version 2.2.4 requires Avocent® MergePoint Unity™ switch plug-in version 2.2.0.

5 Known Issues

Sharing with stealth must be enabled to share HTML5 sessions.

6 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	70.0.3538.102 (Official Build) (64-bit)

7 Flash Update Failure Recovery

If the switch doesn't boot into the new firmware after a Flash procedure, it is possible to revert to the previous firmware version.

WARNING: After upgrading to version 1.18.0.x, the Avocent® MergePoint Unity™ switch cannot be downgraded to a firmware version earlier than 1.18.0.x. For more information, contact Technical Support.

To revert to the previous firmware version:

1. Connect a serial cable to the Setup port on the rear panel of the Avocent® MergePoint Unity™ switch.
2. Run a terminal program on the PC connected to the Setup port. The serial port settings should be: 9600 baud, 8 data bits, 1 stop bit, no parity and no flow control.
3. Turn on the Avocent® MergePoint Unity™ switch.
4. Press any key when the *Hit any key to stop autoboot* prompt appears in the terminal program.
5. Once a menu is displayed in the terminal program, press **1** to select Boot Alternate, and then press **Enter**.
6. The Avocent® MergePoint Unity™ switch will then reboot to the previous version automatically.

8 Java Viewer Session Expired Certificate Information

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

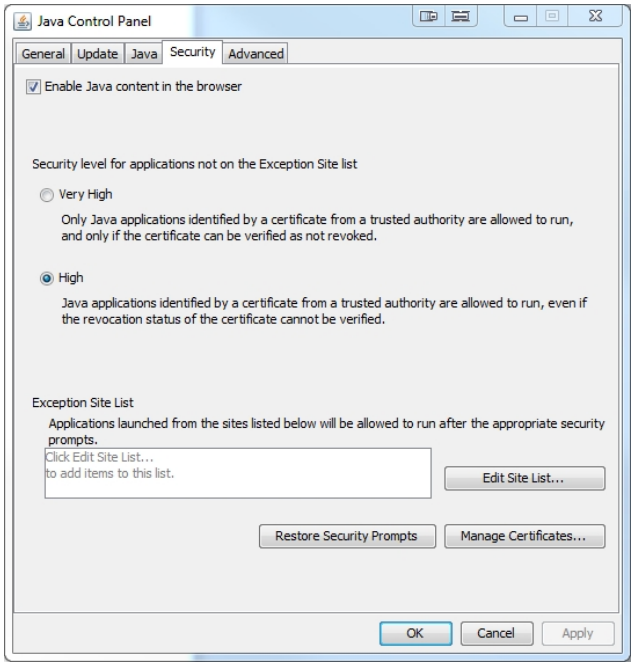
IMPORTANT NOTE: Unless you use the HTML5 viewer, update to the newest firmware or edit the Java Console Security settings on each computer client by that date, you will be unable launch KVM sessions.

NOTE: Active X users are not affected and will be able to continue using the expired certificate.

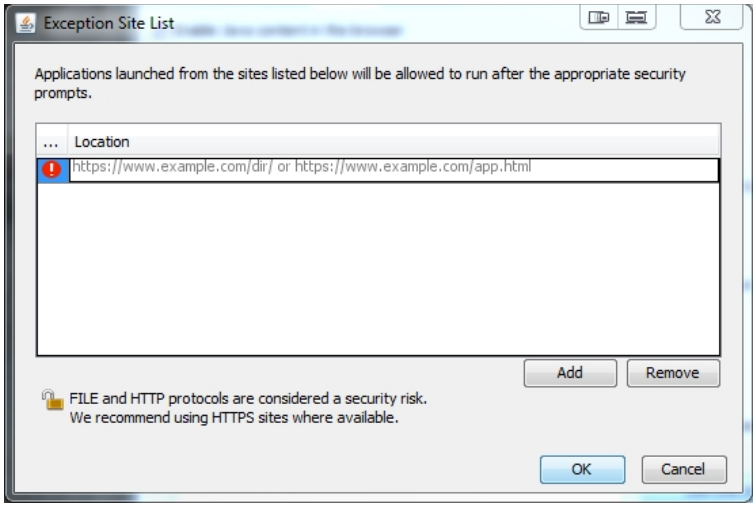
To edit the Java Console security settings:

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.