Adder AVS-4112, AVS-2112, AVS-4114, AVS-4214, AVS-2114, AVS-2214, AVS-4128, AVS-4124, AVS-1124, AVS-4224 Firmware Version 44404-E7E7 Peripheral Sharing Devices

Common Criteria Guidance Supplement

Doc No. 2149-001-D105D1
Version: 1.4
10 February 2022

Adder Technology
Saxon Way Bar Hill
Cambridge, United Kingdom
CB23 8SL

Prepared by:
EWA-Canada, An Intertek Company
1223 Michael Street North, Suite 200
Ottawa, Ontario, Canada
K1J 7T2

DOCUMENT HISTORY

Rev.	Issue Date	Description	Author	Reviewer
0.1draft	12 March 2020	Initial draft for developer review	Teresa MacArthur	
1.0	13 March 2020	Initial draft for evaluation	Teresa MacArthur	Dawn Adams
1.1	8 May 2020	ST Split	Teresa MacArthur	
1.2	9 February 2021	Minor correction	Teresa MacArthur	
1.3	23 November 2021	Removed 16 port device	Teresa MacArthur	
1.4	10 February 2022	Addressed ORs	Ben Buttera	

CONTENTS

LIST OF TABLES

1 PREPARATION OF THE OPERATIONAL ENVIRONMENT

1.1 OPERATIONAL ENVIRONMENT

For secure operation, users are required to ensure the following conditions are met in the operational environment:

- TEMPEST approved equipment may not be used with the secure peripheral sharing device
- The operational environment must provide physical security, commensurate with the value of the peripheral sharing device and the data that transits it
- Wireless keyboards, mice, audio, user authentication, or video devices may not be used with the secure peripheral sharing device
- Peripheral sharing device Administrators and users are trusted individuals who are appropriately trained
- Administrators configuring the peripheral sharing device and its operational environment follow the applicable security configuration guidance
- Special analog data collection cards or peripherals such as analog to digital interface, high performance audio interface, or a component with digital signal processing or analog video capture functions may not be used with the secure peripheral sharing device
- Microphones must not be plugged into the TOE audio output interfaces

2 SECURE ACCEPTANCE PROCEDURES

Adder peripheral sharing devices may be purchased directly from Adder, or through distributors and resellers / integrators.

Upon receipt of the Adder peripheral sharing device, the customer can verify the configuration and revision by comparing the part number and revision on the packing list with the label on the back of the hardware unit. The nameplate includes the product part number (CGA) which is linked directly to the revision of the hardware components and firmware. Verification of the part number provides assurance that the correct product has been received.

The customer must download product documentation from the Adder website in Adobe Acrobat Portable Document Format (PDF). The customer can confirm that the documentation matches the purchased model.

Customers are instructed to check all delivered products for package container seals, and to verify that product tampering evident labels are intact. If an issue is discovered, the customer is instructed to return the product immediately.

3 SECURE INSTALLATION PROCEDURES

This section describes the steps necessary for secure installation and configuration.

3.1 SECURE INSTALLATION

Instructions for secure installation may be found in the Quick Installation Guides.

4 SECURE OPERATION

This section describes the steps necessary for the secure operation of the Adder Peripheral Sharing Devices.

4.1 SELF TESTS

A self test is performed at power up. Self test failures may be caused by an unexpected input at power up, or by a failure in the device integrity. A self test failure may also be an indication that the device has been tampered with.

A user may enter self test failure mode by following the procedures outlined in Table 1 for the applicable device type.

Device Type	Procedure
AVS-4112 AVS-2112 AVS-4114 AVS-4214 AVS-2114 AVS-2214 AVS-4128 AVS-4124	1. To enter self test failure mode, press and hold the channel 1 button, and power on the device. The channel indicators on the front panel light up sequentially, and the audio, video, and keyboard/mouse USB ports are disabled. 2. To exit self test failure mode, cycle the power.
AVS-1124 AVS-4224	1. To enter self test mode, press and hold the channel 1 button, and power on the device. The channel indicators on the front panel light up sequentially, and the audio, video, and keyboard/mouse USB ports are disabled. 2. To exit self test mode, cycle the power.

Table 1 – Procedure to Initiate a Self Test

In the case of a self test failure, users are directed to contact Adder Technical Support.

4.2 ERROR STATE

As the product powers up, it performs a self-test procedure. Following failure of a self-test, the device will enter an error state. The error state is indicated by sequential flashing of the Light Emitting Diodes and by a clicking noise. At this point, the device will be inoperable. It will not accept input from any peripheral device or pass output to any peripheral device.

4.3 TAMPER EVIDENCE AND RESPONSE

The KVM switches are equipped with anti-tampering features. Opening the device will cause it to become permanently disabled. If the device appears to have been tampered with, or if any of the following are observed, contact Technical Support:

- One or more tamper-evident seals has been broken or removed. If removed, the word 'VOID' appears on both the label and the product surface.
- The front panel LEDs blink sequentially and continuously. This indicates that the TOE has been tampered with and the device will be permanently disabled.

The remote control is also equipped with anti-tampering features. Opening the device will cause it to become permanently disabled. If the device appears to have been tampered with, or if any of the following are observed, contact Technical Support:

- The tamper-evident seal has been broken or removed. If removed, the word 'VOID' appears on both the label and the product surface.
- The LEDs blink sequentially and continuously. This indicates that the remote control has been tampered with and the device will be permanently disabled.

4.4 SELECTED CHANNEL AT STARTUP

Channel 1 is selected by default when the peripheral sharing device is started.

4.5 NUMBER OF SUPPORTED DISPLAYS

The number of supported displays is shown in the following table:

Device	Number of Supported Displays
AVS-4112	1
AVS-2112	1
AVS-4114	1
AVS-4214	2
AVS-2114	1
AVS-2214	2
AVS-4128	2
AVS-4124	2
AVS-1124	2
AVS-4224	2

Table 2 – Number of Supported Displays by Device

4.6 AUTHORIZED AUDIO DEVICES

Most speakers and headphones connected to a 3.5 mm audio jack may be used with devices that support audio. Users are directed not to plug a microphone, or a device with a microphone (such as a headset), into the Adder secure peripheral sharing device.

4.7 AUTHORIZED HUMAN INTERFACE DEVICES

Most wired keyboard and mouse devices may be used with Adder secure peripheral sharing device.

4.8 GUARD MODE OPERATION

Users may switch the connected computer using mouse movement and a guard for devices that support two displays. The user must press the Left Ctrl button while dragging the mouse between screens to switch channels.