2/4/8-Port USB DVI/HDMI/DisplayPort

Single/Dual View Secure KVM Switch
Admin Log Audit Code

GCS1212TAA4 - GCS1214TAA4 - GCS1218TAA4 - GCS1222TAA4 - GCS1224TAA4 - GCS1228TAA4
GCS1312TAA4 - GCS1314TAA4 - GCS1322TAA4 - GCS1324TAA4
GCS1412TAA4 - GCS1414TAA4 - GCS1418TAA4 - GCS1422TAA4 - GCS1424TAA4 - GCS1428TAA4
GCS1212TAA4C - GCS1214TAA4C - GCS1218TAA4C - GCS1222TAA4C - GCS1224TAA4C - GCS1228TAA4C
GCS1312TAA4C - GCS1314TAA4C - GCS1322TAA4C - GCS1324TAA4C
GCS1412TAA4C - GCS1414TAA4C - GCS1418TAA4C - GCS1422TAA4C - GCS1424TAA4C - GCS1428TAA4C

www.iogear.com

Table of content

EMC Information

FEDERAL COMMUNICATIONS COMMISSION INTERFERENCE STATEMENT: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. Any changes or modifications made to this equipment may void the user's authority to operate this equipment. This equipment generates and can radiate radio frequency energy. If not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measure:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio / TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) this device may not cause harmful interference, and
(2) this device must accept any interference received, including interference that may cause undesired operation

RoHS

This product is RoHS compliant.

Important. Before proceeding, download the Installation and Operation Manual by visiting the website, www.iogear.com and navigating to the product page. The manual includes important warnings, loading specifications and grounding instructions.

User Notice

User Information

All information, documentation, and specifications contained in this manual are subject to change without prior notification by the manufacturer. The manufacturer makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties as to merchantability or fitness for any particular purpose. Any of the manufacturer's software described in this manual is sold or licensed *as is*. Should the programs prove defective following their purchase, the buyer (and not the manufacturer, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair and any incidental or consequential damages resulting from any defect in the software.

The manufacturer of this system is not responsible for any radio and / or TV interference caused by unauthorized modifications to this device. It is the responsibility of the user to correct such interference.

The manufacturer is not responsible for any damage incurred in the operation of this system if the correct operational voltage setting was not selected prior to operation. PLEASE VERIFY THAT THE VOLTAGE SETTING IS CORRECT BEFORE USE.

Product Information

For information about all IOGEAR products and how they can help you connect without limits, visit IOGEAR on the Web or contact an IOGEAR Authorized Reseller. Visit IOGEAR on the Web for a list of locations and telephone numbers:

www.IOGEAR.com

Manual Version: v1.03

Manual Date: 2021-05-05

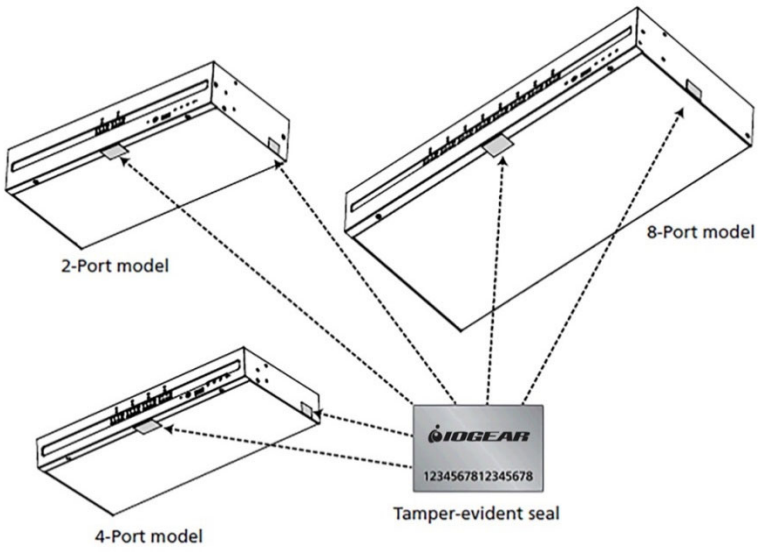
ATTENTION

If the tamper-evident seals are missing or peeled, avoid using the product and contact your IOGEAR dealer.

If all front panel LEDs on the Secure KVM switch (except for Power LED), all Remote Port Slector(RPS) LEDs flash, flash continuously or the switches' enclosure appears to be breached, avoid using this product and contact your IOGEAR dealer.

This Secure KVM Switch and Remote Port Selector (RPS) are equipped with active always-on chassis intrusion detection security. Any attempt to open the enclosure will permanently damage, disable the Switch and Remote Port Selector(RPS), and void the warranty.

To maximize security and to prevent unauthorized access to Secure KVM, please do change default logon password after your first successful logon.



Tamper-evident seal

About This Admin Log Audit Code

This Admin Log Audit Code is intended for authorized administrators only.

- This Admin Log Audit Code is provided to help authorized administrators audit logs/events and perform administrator functions
- Please refer to the IOGEAR Secure KVM Administrator's Guide for basic administrator functions
- If the Secure KVM Switch becomes inoperable, Log/Event data logs can only be decoded by the Secure KVM Switch manufacturer*

Notes:
* The following audit codes are generated which result in the Secure KVM Switch becoming inoperable. These Log/Event data logs can only be decoded by the Secure KVM Switch manufacturer.

- ADML – KVM locked due to Administrators' failed login
- IHWN – H/W integration test failed
- SUMN – Checksum test failed
- MEMN – Memory test failed
- ISON – Self-test port data check failed (different from jammed button BTNJ)
- TMPH – Anti-Tamper triggered
- TMPR – Anti-Tamper triggered by RPS

This Administrator Guide covers the following IOGEAR Secure KVM:

Configuration (without CAC function)			2-Port	4-Port	8-Port
PC Video Connection	Console Video Connection	Number of Displays			
DisplayPort	DisplayPort	Single	GCS1412TAA4	GCS1414TAA4	GCS1418TAA4
		Dual	GCS1422TAA4	GCS1424TAA4	GCS1428TAA4
HDMI	HDMI	Single	GCS1312TAA4	GCS1314TAA4	n/a
		Dual	GCS1322TAA4	GCS1324TAA4	n/a
DVI	DVI	Single	GCS1212TAA4	GCS1214TAA4	GCS1218TAA4
		Dual	GCS1222TAA4	GCS1224TAA4	GCS1228TAA4

Configuration (with CAC function)			2-Port	4-Port	8-Port
PC Video Connection	Console Video Connection	Number of Displays			
DisplayPort	DisplayPort	Single	GCS1412TAA4C	GCS1414TAA4C	GCS1418TAA4C
		Dual	GCS1422TAA4C	GCS1424TAA4C	GCS1428TAA4C
HDMI	HDMI	Single	GCS1312TAA4C	GCS1314TAA4C	n/a
		Dual	GCS1322TAA4C	GCS1324TAA4C	n/a
DVI	DVI	Single	GCS1212TAA4C	GCS1214TAA4C	GCS1218TAA4C
		Dual	GCS1222TAA4C	GCS1224TAA4C	GCS1228TAA4C

How does the Administrator Logon Function Work?

- After the authorized Administrator successfully logs on to the Secure KVM switch, the Secure KVM Switch can dump the necessary information (text only) in a text editor on the authorized Administrator's management computer.
- All Administrator configuration options will be displayed in the text editor upon the Administrator's key stroke command.
- When the Administrator selects an option, the result of this execution will also be displayed in text editor.
- If the Administrator chooses to display available logs to audit, those logs will be displayed within the text editor.

Setup and Operation of Administrator Logon Functions

Please refer to the IOGEAR Secure KVM Switch **Administrator's Guide** for details.

Format for Information displayed in Text Editor

Administrator Logon Mode

ID: Administrator

Please enter password: ********

Logon ok.

LIST

DATE-TIME= 25-12-2021_17:23:05_UTC

MFG_DATE= 23-12-2021

TAMP_TEST= PASS

HW_TEST= PASS

FW_TEST=PASS

KVM_BATT_TEST=3.0V

RPS_BATT_TEST=3.0V

RPS_TEST=PASS

FW_CHECKSUM= xxxx

AUDT_ST 23-12-2021_17:23:05_UTC

AUDT_SP NA

FW_VER= v1.1.101

TTL_LOGS= 8

No.	Cat.	DATE-TIME	Code	Crit
01	ADM	25-12-2021_17:23:05_UTC	ADIO	
02	CAC	25-12-2021_17:25:02_UTC	ADCWO	
03	CAC	25-12-2021_17:26:12_UTC	ADCBO	
04	ADM	25-12-2021_17:30:27_UTC	ADOO	

Operation ok

Administrator Configuration Menu

The Administrator can press a numbered option to perform the configuration.

For example: If the Administrator wants to audit logs and events, then he/she can press “1” to access Text Menu Level 2. If the Administrator presses “2” when Text Menu Level 2 is displayed, then all critical logs & events will be shown in the text editor.

Text Menu Level 1	Text Menu Level 2
1. Show logs and events	[1-2] Display logs & events. Please choose an option
	1. Show all logs & events
	2. Show critical logs & events
	3. Show non-critical logs & events
	7. Return
2. Configure CAC filter*	[2-2] Configure CAC filter of Admin session. Please choose an option
	1. Allow currently connected device on all Ports
	2. Block currently connected device on all Ports
	3. Show info of currently connected device
	4. Show info of all added devices**
	5. Reset Admin CAC Allow list
	6. Reset Admin CAC Block list
	7. Return
3. Configure KB_MS filter***	[3-2] Configure KB_MS filter of Admin session. Please choose an option
	1. Block currently connected device on all Ports
	2. Show info of currently connected device
	3. Show info of all added devices
	4. Reset Admin KB_MS Block list
	7. Return
4. Change Password	[4-2] Change Admin password. Please choose an option
	1. Continue
	7. Return
5. Check FW version	[5-2] FW version: vx.x.xxxx
	7. Return
6. Reset KVM to Default	[6-2] Reset KVM, CAC filter, & KB_MS filter to factory default. Please choose an option
	1. Continue
	7. Return
8. Exit logon session	

Note:

* This function will also be shown on Non-CAC models, but the statement would be changed to “Configure CAC filter (CAC Models Only)

The “Show info of all added devices” option lists only devices added by the Administrator on the KVM switch through the Administrator Logon Function. It does not show the devices blacklisted or whitelisted by IOGEAR **Port Authentication Utility

*** Only the HID devices plugged into the Secure KVM console mouse port could be blocked. Once the certain device is blocked, it will be effective on both Secure KVM console keyboard/mouse ports.

Log / Event Audit Code

Cat. (Category)	Code	Description	Critical Event Area
ADM (Administrator Tasks)	ADIO	Administrator login OK	
	ADIN	Administrator login failed. (Critical area only keeps the last login fail event. This event will also be logged in non-critical areas)	**Yes**
	ADOO	Administrator logout	
	ADIL	Administrator last login ok	**Yes**
	APIO	AP connection login ok for Blacklist/Whitelist update	
	APIN	AP connection login fail for Blacklist/Whitelist update (Critical area only keeps the last AP login fail event. This event will also be logged in non-critical areas.)	**Yes**
	APOO	AP connection terminated	
	APIL	AP last connection login ok	**Yes**
	PWCO	Administrator password change (Critical area only keeps the last password change event. This event will also be logged in non-critical areas.)	**Yes**
	RSTO	Administrator performs Reset to Factory Default (Critical area only keeps the last Administrator Reset to Factory Default event.)	**Yes**
	ADML	KVM locked due to Administrator's failed attempts to login	**Yes**
CAC (CAC Related)	ADCWO	Administrator changed CAC port Whitelist	
	ADCBO	Administrator changed CAC port Blacklist	
	APCTO	AP changed CAC port Blacklist/Whitelist	
	USBCO	USB CAC port accepted the connected device	
	USBCR	USB CAC port rejected the connected device	**Yes**
KM (KB/MS Related)	ADMBO	Administrator changed KB/MS ports Blacklist	
	USBMO	USB KB/MS ports accepted the connected device	
	USBMR	USB KB/MS ports rejected the connected device	**Yes**
VI	VIO	Console video port accepted the connected device	
	VIR	Console video port rejected the connected device	**Yes**
RPS (Remote Port Selector Related)	RPSO	This event will be logged when RPS_TEST = PASS	
	RPSR	This event will be logged when RPS_TEST = REJ or connecting the Remote Port Selector to KVM after KVM is powered on (This event will also be logged in non-critical area.)	**Yes**
TST* (KVM Test Related)	IHWN	H/W integration test failed	**Yes**
	SUMN	Checksum test failed	
	MEMN	Memory test failed	
	ISON	Self-test port data check failed	
	BTNJ	Button jam detected	

TMP (Anti-tampering)	TMPH	Anti-tampering triggered	**Yes**
	TMPR	Anti-tampering triggered by RPS being tampered	**Yes**
SYS (KVM System)	PWR	KVM power cycle	
	RST	Reset by front panel	

*Note:
IOGEAR Secure KVM Switch self-test includes the hardware integration test, firmware checksum test, memory test, port data test, and pushbutton jam test. Only the pushbutton jam test failure can occur more than once.

Appendix

General Safety Instructions

- ❑ This product is for indoor use only.
- ❑ Read all of these instructions. Save them for future reference.
- ❑ Follow all warnings and instructions marked on the device.
- ❑ Do not place the device on any unstable surface (cart, stand, table, etc.). If the device falls, serious damage will result.
- ❑ Do not use the device near water.
- ❑ Do not place the device near, or over, radiators or heat registers.
- ❑ The device cabinet is provided with slots and openings to allow for adequate ventilation*. To ensure reliable operation, and to protect against overheating, the cabinet must never be blocked or covered.
- ❑ The device should never be placed on a soft surface (bed, sofa, rug, etc.) as this will block its ventilation openings*. Placing the device without slots or openings on a soft surface will affect the heat dissipation.
- ❑ The device should not be placed in a built-in enclosure unless adequate ventilation has been provided.
- ❑ Never spill liquid of any kind on the device.
- ❑ Unplug the device from the wall outlet before cleaning. Do not use liquid or aerosol cleaners. Use a damp cloth for cleaning.
- ❑ The device should be operated from the type of power source indicated on the marking label. If you are not sure of the type of power available, consult your dealer or local power company.
- ❑ The device is designed for IT power distribution systems with 230V phase-to-phase voltage.
- ❑ To prevent damage to your installation, it is important that all devices are properly grounded.
- ❑ The device is equipped with a 3-wire grounding type plug. This is a safety feature. If you are unable to insert the plug into the outlet, contact your electrician to replace your obsolete outlet. Do not attempt to defeat the purpose of the grounding-type plug. Always follow your local / national wiring codes.
- ❑ Do not allow anything to rest on the power cord or cables. Route the power cord and cables so that they cannot be stepped on or tripped over.
- ❑ If an extension cord is used with this device, make sure that the total of the ampere ratings of all products used on this cord does not exceed the extension cord ampere rating. Make sure that the total of all products connected to the wall outlet does not exceed 15 amperes.
- ❑ To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- ❑ Position system cables and power cables carefully; Be sure that nothing rests on any cables.
- ❑ Never push objects of any kind into or through cabinet slots. They may touch dangerous voltage points or short out parts resulting in a risk of fire or electrical shock.
- ❑ Do not attempt to service the device yourself. Refer all servicing to qualified service personnel.
- ❑ If the following conditions occur, unplug the device from the wall outlet and bring it to a qualified service personnel for repair:
    - The power cord or plug has become damaged or fried.
    - Liquid has been spilled into the device.
    - The device has been exposed to rain or water.
    - The device has been dropped, or the cabinet has been damaged.
    - The device exhibits a distinct change in performance, indicating a need for service.
    - The device does not operate normally when the operating instructions are followed.
- ❑ Suitable for installation in Information Technology Rooms in accordance with Article 645 of the National Electrical Code and NFPA 75

CAUTION: Never attempt to replace battery or open the switches' enclosure.

*Note: Not all devices have slots or openings to allow for ventilation.

Limited Warranty

IN NO EVENT SHALL THE DIRECT VENDOR'S LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, DISK, OR ITS DOCUMENTATION.

The direct vendor makes no warranty or representation, expressed, implied, or statutory with respect to the contents or use of this documentation, and especially disclaims its quality, performance, merchantability, or fitness for any particular purpose.

The direct vendor also reserves the right to revise or update the device or documentation without obligation to notify any individual or entity of such revisions, or update. For further inquiries, please contact your direct vendor.

This Secure KVM carries a 4 Year Limited Warranty. For the terms and conditions of this warranty, please visit https://www.iogear.com/support/warranty

Register your IOGEAR Secure KVM Switch online at https://www.iogear.com/register

For further assistance with IOGEAR Secure KVM Switch series, please contact IOGEAR Technical Support department at GovSupport@iogear.com