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

Single/Dual View Secure KVM Switch
Administrator's Guide

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.

Package Contents

IOGEAR Secure KVM package consists of:

1 x Secure KVM Switch

1 x Power Cord

1 x User Manual*

Please check to make sure that all of the components are present and are in good order. Please contact your dealer if anything was missing or damaged in shipping.

Please read this manual thoroughly and follow the installation and operation procedures carefully to prevent any damage to the switch or to any other devices on IOGEAR Secure KVM installation.

*Please visit our website to download the most up to date version of the manual

Manual Version: v1.03

Manual Date: 2021-05-05

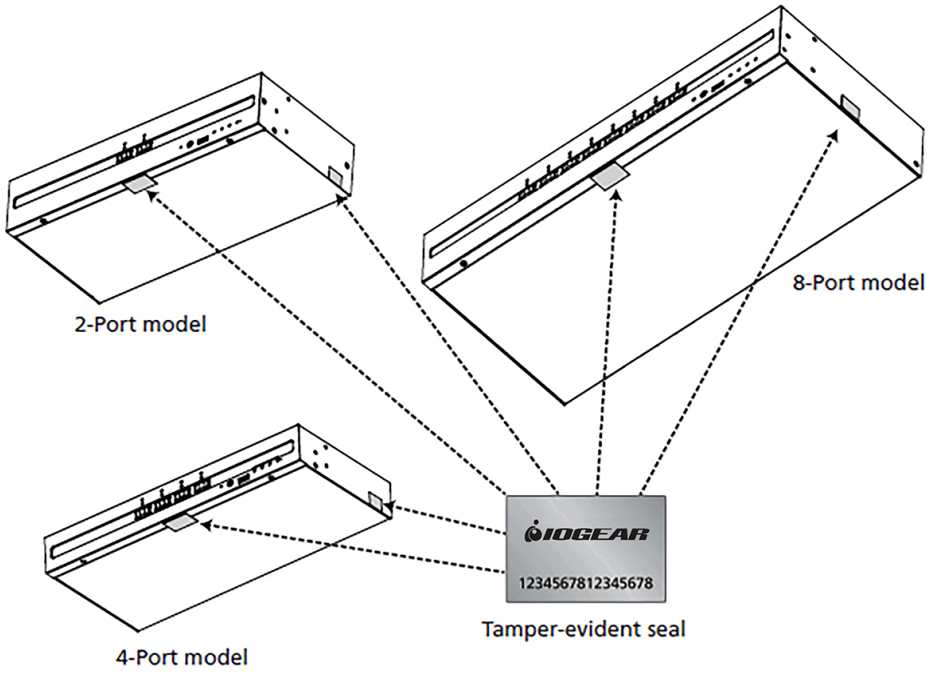
ATTENTION

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

If all front panel LEDs on Secure KVM Switch (except Power) flash continuously, all Remote Port Selector (RPS) LEDs flash, or the switch's 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 the RPS, and void the warranty.

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



Tamper-evident seal

About This Administrator's Guide

This Administrator's Guide is intended for authorized administrators only.

This Administrator Guide is provided to help authorized administrators to audit logs and configure the IOGEAR Secure KVM switch series. To maximize security, administrators are recommended to audit logs event records and the Secure KVM Switch's configuration on a routine base.

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

Conventions

This manual uses the following conventions:

Monospaced	Indicates text that you should key in
[]	Indicates keys you should press. For example, [Enter] means to press the **Enter** key. If keys need to be pressed together, they appear together in the same bracket with a plus sign between them: [Ctrl+Alt]
1.	Numbered lists represent procedures with sequential steps.
♦	Bullet lists provide information, but do not involve sequential steps.
→	Indicates selecting the option (on a menu or dialog box, for example), that comes next. For example, Start → Run means to open the *Start* menu, and then select *Run*.
	Indicates critical information

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

Chapter 1 - Introduction

Overview

The IOGEAR Secure KVM Switch series is NIAP[1]-certified and compliant with NIAP PP 4.0 (Protection Profile for Peripheral Sharing Device version 4.0)[2] requirements, satisfying the latest security requisites set by the U.S. Department of Defense for peripheral sharing devices. Compliance ensures maximum information security while sharing a single set of keyboard, mouse, monitor, speakers, and CAC (Common Access Card) Reader[3] between multiple computers. Conformity with Protection Profile v4.0 certifies that only a keyboard and a mouse are accommodated, other USB peripherals cannot be connected to the console ports of the Secure KVM; therefore, providing high-level security, protection and data safekeeping.

The IOGEAR Secure KVM Switch provides the utmost hardware and software security when switching port focus. Hardware security includes tamper-evident tapes, chassis intrusion detection, and tamper-proof hardware. Software security includes restricted USB connectivity, meaning non-HIDs (Human Interface Devices) or non-predefined CAC/HIDs are ignored when switching. This security includes channel isolation per port and automatic clearing of the keyboard and mouse buffer when switching port focus, making it impossible for data to be leaked or transferred between secure and unsecure computers.

By combining physical security with controlled USB connectivity and controlled unidirectional data flow from devices to connected computers only, the IOGEAR Secure KVM Switch series offers the means to consolidate multiple workstations of various security classification levels with one keyboard, one video monitor, and one mouse (KVM) console.

Administrative Functions

To be compliant with Protection Profile 4.0 while providing higher deployment flexibility, wider product support for new authentication devices, and maximum security, the IOGEAR Secure KVM Switch offers Port Authentication Utility. IOGEAR Port Authentication Utility allows authorized administrators to configure IOGEAR Secure KVM Switch to either accept or reject specific USB devices. Through a secured access and authentication process, authorized administrators can perform log data auditing, the Secure KVM Switch configuration, and configurable device filtering through the Port Authentication Utility.

Note:

1. The National Information Assurance Partnership (NIAP) is a United States government initiative to meet the security testing needs of IT consumers and manufacturers. NIAP is operated by the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST).
2. IOGEAR Secure KVM Switch series additionally satisfied Protection Profile version 4.0 for Peripheral Sharing Device (PSD).
3. USB 1.1 for Keyboard, mouse connections, and USB 2.0 for CAC reader connection

Chapter 2 – Precautions and Preparation

Before You Begin

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

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

This Secure KVM Switch and the PRS are equipped with active always-on chassis intrusion detection security. Any attempt to open the enclosure will permanently damage, disable the switch, and void the warranty.

To maximize security and to prevent unauthorized access to IOGEAR Secure KVM Switch, the administrator will be prompted to change the default password after the first successful logon.

Tampering prevention and detection

1. IOGEAR Secure KVM Switch and the RPS include tamper-evident tapes to provide visual indications of intrusion to the switch/RPS enclosure. If the tamper-evident seals are missing, peeled, or looks as if they have been adjusted, avoid using the product and contact your IOGEAR dealer.
2. IOGEAR Secure KVM Switch and the RPS are equipped with active always-on chassis intrusion detection. If a mechanical intrusion is detected on the switch (without RPS connected), the switch will be permanently disabled and all front panel LEDs (except for Power LED) will flash continuously. If a mechanical intrusion is detected by the RPS(connected with the switch and aligned), this will permanently disable both the RPS and the switch, and all LEDs on the RPS and the front panel LEDs except the power LED on the switch will flash continuously. If the switch/RPS enclosure appears to be breached or all the LEDs are flashing continuously, stop using this product, remove it from service immediately, and contact your IOGEAR dealer.
3. Any attempt to open the switch or the RPS enclosure will activate the chassis intrusion detection security, which will render it inoperable and void the warranty.
4. IOGEAR Secure KVM Switch cannot be upgraded, serviced, or repaired.
5. IOGEAR Secure KVM Switch and RPS are equipped with active always-on chassis intrusion detection security. Never attempt to open the enclosure. Any attempt to open the enclosure will permanently damage and disable the switch.
6. IOGEAR Secure KVM Switch and RPS contain an internal battery which is non-replaceable. Never attempt to replace the battery or open the switch or RPS enclosure.

Always use qualified and authorized peripheral devices

1. For security, IOGEAR Secure KVM Switch supports only standard USB devices (or pointing device). Do not connect a wireless keyboard/mouse, or keyboard/mouse with an internal USB hub or composite functions to the switch.
2. When connecting a non-qualified keyboard, the keyboard will not function. No keyboard keystrokes will be seen on the screen.
3. When connecting a non-qualified mouse, the mouse will not function. No mouse cursor movement will be seen on the screen.

4. For security, IOGEAR Secure KVM's USB console keyboard/mouse ports by default only support the following – standard USB keyboards/mice, standard USB keyboards/mice via a USB hub, and the HID functions of a composite device. Do not connect other USB devices to the USB console keyboard/mouse ports. Non-qualified or non-authorized USB devices will be rejected. For administrative configuration, please refer to the **Administrator Guide**.
5. Num Lock LED, Caps Lock LED, and Scroll Lock LED on the keyboard will be disabled due to security policy.
6. Special multimedia keys on the keyboard will be disabled due to security policy.
7. For security, IOGEAR Secure KVM Switch does not support analog microphones or line-in audio inputs. Never connect a microphone to the switch's audio output port, including that of a headset's. Only standard analog speakers and headsets are supported.
8. For security, IOGEAR Secure KVM Switch's USB CAC ports (by default) only support authorized user authentication devices, such as USB Smartcards or CAC readers. Do not connect other USB devices to USB CAC Port. Non-qualified or non-authorized USB devices will be rejected. For administrative configuration, please refer to the **Administrator's Guide** and **Port Authentication Utility Guide** for details.
9. For security, do not use any USB CAC authentication device or other peripherals that adopt an external power source.
10. Always use qualified monitor(s). Non-qualified monitors will be rejected.
11. Do not use wireless video transmitters or any docking device.
12. Do not connect any Thunderbolt device to IOGEAR Secure KVM Switch.
13. Any cable connector or non-IOGEAR remote controller plugged into the console RPS port will be ignored.

Secure Installation

1. Do not attempt to connect or install the following devices to the computers connected to IOGEAR Secure KVM Switch:
    - TEMPEST computers,
    - Telecommunication equipment,
    - Frame grabber video cards, or
    - Special audio processing cards
2. Important safety information regarding the placement of this device is provided on page 19. Please review it before proceeding.
3. Before installation, please make sure that the power sources to all connected devices are turned off. You must unplug the power cords of any computers that have the Keyboard Power On function.
4. Hot-swapping of the console monitor is not allowed. Power off the Secure KVM Switch and the monitor before changing the console monitor.
5. A computer connected to IOGEAR Secure KVM Switch should only be powered on after all of the device (Video, USB, and audio) are securely connected
6. Please refer to IOGEAR Secure KVM Switch **User Manual** for hardware installation instructions.

Secure Operation and Administration

1. IOGEAR Secure KVM Switch's administration functions (such as log data and configuration of authentication devices filters) can only be performed by an authorized administrator.
2. To maximize security and to prevent unauthorized access to IOGEAR Secure KVM Switch, please change the default password right after your first successful log in.
3. Administrator's session will be terminated if the administrator logs out or the Secure KVM Switch is powered off.

Please refer to the **Operation** section for details administrator functions.

Chapter 3 – Operation

Powering On

When powering on, resetting, or power cycling IOGEAR Secure KVM Switch, the switch will perform a self-test to check the unit's integrity and security functions.

During the self-test

- ❑ All Port , CAC LEDs (if supported), Num Lock LED, Caps Lock LED, and Scroll Lock LED on the Secure KVM switch will turn ON and then OFF
- ❑ The KVM focus will be switched to Port 1 when the self-test completes successfully (Port 1 LED lights bright orange)

Self-test failure

In case of a self-test failure, IOGEAR Secure KVM Switch becomes inoperable. Front panel LED combination lights up, indicating the potential cause to the failure (such as button jam or KVM integrity compromise):

- ❑ A pre-defined combination of Port and CAC LED indicates the cause to the failure.
- ❑ If all front panel LEDs (except for Power LED) flash continuously, then either KVM tampering is detected or a self-test failure has occurred (except for Pushbutton jam; see below)
- ❑ If Pushbutton jam is detected, both the Port and CAC LEDs will flash

For security, IOGEAR Secure KVM Switch becomes inoperable if self-test fails. Please verify your KVM installation, pushbuttons, and power cycle the Secure KVM Switch again if this should happen. If the self-test failure remains, stop using the Secure KVM Switch immediately, remove it from service, and contact your IOGEAR dealer.

After the IOGEAR Secure KVM Switch is powered on and ready, power on your computers. By default, the IOGEAR Secure KVM Switch will switch to Port 1 after a successful self-test.

Resetting the Secure KVM Switch (Rebooting the Secure KVM switch)

Press the Reset button on the front panel to reset IOGEAR Secure KVM Switch.

When pressing the Reset Button for more than 5 seconds, the keyboard/mouse buffer will be purged. Then, the IOGEAR Secure KVM Switch will reboot and a self-test will initiate. After a successful self-test, the port focus will be switched to Port 1, and the CAC function of each port will be set back to factory default (enabled). An administrator's **Reset KVM to Default** function is also available, please see page 18 for more details.

If the Secure KVM fails to generate video on the console monitor after a reset, please power off all connected devices, check the cables, and follow the **Operation Instructions** in the **User Manual** to power on the installation.

Manual Switching

For increased security, IOGEAR Secure KVM Switch offers manual port-switching only. This is achieved by pressing the port selection pushbutton on the switch, or on the RPS if connected and aligned. Press and release a port selection pushbutton to bring the KVM focus to the computer attached to its corresponding port (see **Port ID Numbering** below). To meet maximum security and channel isolation requirements, the keyboard, mouse, video monitor, audio, and USB CAC reader ports will be switched together.

The Selected Port LED lights orange to indicate that the computer attached to its corresponding port has the KVM focus (keyboard, mouse, monitor, audio, and CAC reader).

The PC that has the port focus on should be able to detect the peripherals after port switching. If the PC fails to detect the keyboard, mouse, or CAC reader:

- Please verify if you are using qualified Keyboard, Mouse, or CAC reader
- Please verify if your keyboard, mouse, or CAC reader has failed
- For USB CAC Card readers (USB authentication devices), please make sure that the USB CAC cable has been securely connected and the CAC function on the Secure KVM switch is enabled.
- Please verify if the USB CAC reader has been authorized for the corresponding port

LED Display

In addition to the Power LED, IOGEAR Secure KVM Switch and RPS have built-in Port LEDs (Online and Selected), keyboard lock keys (Num Lock / Caps Lock /Scroll Lock) LEDs and CAC LEDs on the front panel to indicate Port / Keyboard / CAC reader operating status. A Video LED is located on the rear panel (of the switch) to indicate the video connection operating status. These LEDs also serve as notification alarm for Secure KVM Switch security issues.

LED	Indication
Power LED (on the Secure KVM switch)	Power LED is located on the front panel ❑ Power LED lights blue to indicate that the KVM switch is powered on.
Video LED (on the Secure KVM switch)	Video LED is located on the rear panel next to each video connector. ❑ Video LED lights green when the video connection is established. ❑ Video LED flashes when a non-qualified monitor is connected.
Port LED (on the Secure KVM switch and the RPS)	Port LEDs located on the front panel (of the switch) and upper-left side of each pushbutton (of the RPS) are to indicate the Port selection or connection status. ❑ Online – Port LED lights dim orange to indicate that the computer attached to its corresponding port is connected and powered on. ❑ Selected – Port LED lights bright orange to indicate that the computer attached to its corresponding port has the KVM focus. <u>Warning:</u> Flashes to indicate that a non-qualified USB HID device is connected to console USB keyboard port or mouse port when the corresponding port has the focus. <u>Note:</u> 1. Port and CAC LEDs will flash constantly when a chassis intrusion is detected. See **Chassis Intrusion Detection** section for details. 2. Port and CAC LEDs also indicate the Secure KVM self-test status. See **Operation** section for further details
CAC LED (on the Secure KVM switch and the RPS) Models with CAC feature only	CAC LEDs located on front panel(of the switch) and the far right of the upper bar on the panel(of the RPS) are to indicate CAC reader selection or connection status: **Online** – CAC LED lights dim green to indicate that the computer attached to the corresponding port has a USB CAC reader cable connection established and that CAC function is enabled. **Selected** – CAC LED lights bright green to indicate that the CAC function is enabled and the computer attached to the corresponding port has the CAC focus **None** – No light indicates that the cable is not connected or CAC has been disabled **Warning** – CAC LED flashes to indicate that a non-qualified USB Smart card / CAC reader is connected when the corresponding port has the focus.

	Note: 1. CAC function of each port can be enabled or disabled by pressing the port selection button for more than 3 seconds (This is a toggle function). Please refer to **Operation** section for details. 2. Port and CAC LEDs will flash constantly when a chassis intrusion is detected. See **Chassis Intrusion Detection** section for further details.
Num Lock LED (on the Secure KVM switch and the RPS)	Num Lock LED lights green to indicate Num Lock is enabled
Caps Lock LED (on the Secure KVM switch and the RPS)	Caps Lock LED lights green to indicate Caps Lock is enabled
Scroll Lock LED (on the Secure KVM switch and the RPS)	Scroll Lock LED lights green to indicate Scroll Lock is enabled

Chassis Intrusion Detection

The IOGEAR Secure KVM Switch, the switch (or the RPS) becomes inoperable and all front panel LEDs on the Secure KVM switch (except Power) or all Remote Port Selector (RPS) LEDs flash constantly when a chassis intrusion (such as the cover being removed) is detected (by the switch or by the RPS). This is to prevent malicious tampering with IOGEAR Secure KVM Switch.

The Intrusion Detection is an active always-on function. If all front panel LEDs on the Secure KVM Switch (except Power) flash continuously, all Remote Port Selector (RPS) LEDs flash, or the switch's enclosure appears to be breached, avoid using this product and contact your IOGEAR dealer.

Administrator Functions

Administrator functions of IOGEAR Secure KVM Switch enable authorized administrators to configure the Secure KVM switch, configure user authenticated device filters, and audit log data generated by the Secure KVM Switch.

- **Log Data Audit**: This function enables authorized administrators to view log data and events generated by the Secure KVM Switch. The Log Data Audit function is enabled as soon as the Secure KVM Switch is manufactured. This capability cannot be terminated; it is not affected by KVM power-cycle, KVM Reset, or Reset KVM to Default.
- **User Authentication Device and HID Device Filtering Configuration**: This function enables authorized Administrators to assign a whitelist and blacklist for User Authenticated devices, and a blacklist for HID devices.
- **The Secure KVM Switch Configuration**: This function enables authorized Administrators to perform functions such as Reset to Factory Default.

Administrators must first log in and be authenticated for the Secure KVM Administrator Functions. To maximize security, before performing other administrative functions, Administrator *must set a new password* after the first successful login. The Administrator password can be changed anytime via the Administrator Configuration.

Setup for Administrator Logon

Administrators must first logon and be authenticated for the Secure KVM Administrative Operations.

This section will assist in setting up for Administrator Logon installation.

1. Please make sure that all devices, including source computer, are powered off.

2. Connect a qualified keyboard, mouse, and display to the IOGEAR Secure KVM console section. (Please refer to the Secure KVM **User Manual** for details)

3. Connect a source computer to Port 1 of the Secure KVM Switch's KVM Port section using IOGEAR KVM cable sets. The USB cable attached to the computer's keyboard / mouse must be connected to the KVM USB Port on the switch. (Please refer to the Secure KVM **User Manual** for details)

4. Turn the IOGEAR Secure KVM Switch power on, and then turn the source computer power on. The IOGEAR Secure KVM Switch will switch to Port 1 after a successful self-test.

Administrator Logon

After the IOGEAR KVM Secure Switch is set up, please follow below steps to logon:

1. Open a text editor on the source computer connected to Port 1
2. Use the console keyboard to:
    a. Press and hold down the **Ctrl** key,
    b. Press and hold down the **F12** key:
        [Ctrl + F12]
    c. First, release the **F12** key, followed by the **Ctrl** key
    d. Press and release the **[L]** key, then press and release **[Enter]**
    Please make sure not to exceed 2 second between each key

    After successful input of the key sequence above, you will be in the Administrator Logon mode and be prompted in text editor to be authenticated.

3. In the text editor, you will be prompted to input the default Administrator logon password.

ATTENTION

- The default Administrator password should only be used the first-time Administrator Log in.

- To maximize security and to prevent unauthorized access to IOGEAR Secure KVM Switch, please change default logon password after the first-time successful logon. Once changed, the default Administrator password will not be restored EVEN after Reset to Factory Default is initiated.

4. The default Administrator password for the first-time log in is:
ABCD@xyz#2468!

    - The password is case-sensitive

    - Caps lock function is disabled automatically in Administrator Logon mode. Use **[Shift]** key for upper case letters and special characters

5. A **[Logon OK]** message appears if the password input is correct; you will be prompted to input the password again if the password is incorrect.

a. With **3 (three)** failed login attempts, the Administrator Logon mode will be terminated and access to the Administrator Logon mode will be locked for 15 minutes.

b. With **9 (nine)** failed login attempts, IOGEAR Secure KVM Switch will become inoperable permanently. Please remove it from service immediately and contact your IOGEAR dealer.

6. After a **[Logon OK]** message appears, type **LIST** and press **[Enter]** to show list of the Administrator Functions
(For a complete list of administrator functions, please contact GovSupport@iogear.com . An "Admin Log Audit Code" document is available for registered customers to download)

7. For maximum security, the administrator must change the Administrator Logon password after the first successful login.

The new password should contain:

a. At least 8 characters in length, but no longer than 22 characters.

b. At least 1 lower case letter and,

c. At least 1 upper case letter and,

d. At least 1 numeric character and,

e. At least 1 special character

Do not use the default Administrator password for your new password.

The administrators will be asked to enter the new password a second time for confirmation.

Once the new Administrator password is entered, the default Administrator Logon password will not be restored even after a Reset to Factory Default. The default administrator password cannot be restored.

Log Data Audit

Log Data Audit is enabled when the IOGEAR Secure KVM Switch is manufactured and cannot be terminated.

After a successful Administrator Login, type **LIST** and press **[Enter]** for administrator functions.

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

KVM Information Area

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

Log Data Area

Appendix

Operation ok

1. KVM Information Area

This area displays the Secure KVM Switch status and critical information

a. DATE-TIME: Current Date and Time in UTC
b. MFG_DATE: Manufacturing Date (in UTC) of the Secure KVM Switch
c. TAMP_TEST: The Secure KVM Switch Tamper protection test status
d. HW_TEST: The Secure KVM Switch hardware self-test status
e. FW_TEST: The Secure KVM Switch firmware self-test-status
f. KVM_BATT_TEST: The Secure KVM Switch battery self-test status. (The battery voltage will be displayed if the battery for Secure KVM switch is still working)
g. RPS_BATT_TEST: The Remote Port Selector battery self-test status. (The battery voltage will be displayed if the Remote Port Selector is connected and detected successfully)
h. RPS_TEST: The Secure KVM Switch Remote Port Selector connection self-test status. ("PASS" will be displayed if the Remote Port Selector is successfully detected and connected)
i. FW_CHECKSUM: The Secure KVM Switch firmware checksum for firmware integrity.
j. AUDT_ST: Date and Time (in UTC) when the Secure KVM Switch activates all protection mechanism and Log Data Audit function.
k. AUDT_SP: "NA" will be displayed if the Secure KVM Switch functions normally. If events that trigger the Secure KVM Switch's protection mechanism are detected, and the switch shuts down and becomes inoperable, a Date/Time log will be recorded. (This particular Date/Time log can only be decoded by the Secure KVM manufacturer.)
l. FW_VER: Firmware version.
m. TTL_LOGS: Total number of event logs

2. Log Data Area

The Log Data Area is an area where critical and non-critical Events and Log Data can be displayed. Each Event /Log Data is recorded with time/date stamp and special codes to indicate the type and content of the event. The clock inside the KVM is used to print out timestamps for each event in the log. The internal battery inside the KVM ensures that the clock is active at all times and allows for accurate time recordings for all events. The initial date is set in each KVM manually at the time of manufacturing. These special codes can only be decoded by the Secure KVM Switch manufacturer if the device becomes inoperable.

a. Critical Log Data:
   Critical Log Data includes Administrator Logon events, Administrator password change events, Critical Administrator KVM configuration events, and Self-test / Tampering events (up to five). A maximum of 32(thirty-two) critical event logs will be kept on the Secure KVM Switch.

   For critical events that do not result in a Secure KVM Switch lockdown, only a record of the most recent occurrence will be kept, overwriting the records of prior occurrences of the same event.

b. Non-critical Log Data:
   Non-critical Log Data includes Administrator Logon records (including Administrator log in and log out events), administrator password change events, administrator configuration events, device filter configuration events, self-test events, and power cycle events.

A maximum of 32 (thirty-two) non-critical event logs will be kept in the Secure KVM Switch. The new log entries will overwrite the oldest one. For example, the 33rd (thirty-third) log entry will overwrite the 1st (first) log entry.

User Authentication Device and HID Device Filtering Configuration

Administration functions enable authorized administrators to Configure Device Filtering (CDF). This function allows the administrator to configure whether the Secure KVM Switch will accept or reject specific USB devices (for CAC port)[1], and reject specific HID devices (for Keyboard/Mouse Ports)[2].

CAC Port device filtering can also be configured via IOGEAR Port Authentication Utility. Please refer to the IOGEAR **Port Authentication Utility Guide** for details.

Reset KVM to Default (Restore KVM to Factory Default)

The Administrator function enables the authorized Administrator to reset the Secure KVM Switch configuration to the factory default settings.

1. When the administrator performs Reset KVM to Default, settings previously configured by the administrator (such as USB device whitelist/blacklist and HID device blacklist) will be cleared and reset to the factory default settings.
2. Once Reset KVM to Default has been completed, the Secure KVM Switch will terminate the Administrator Logon mode, purge keyboard/mouse buffer, and power cycle the Secure KVM Switch automatically. After a successful self-test, the KVM port focus will be switched to Port 1, and CAC function of each port will be set to the factory default (enabled).
3. Reset KVM to Default will not affect or erase Log data
4. Reset KVM to Default will not affect previously changed Administrator password
5. Reset KVM to Default will clear the whitelist/blacklist created by both the Secure KVM administrator functions and IOGEAR **Port Authentication Utility**.

Note:
1. The CAC port does not support USB hub. The USB hub cannot be added to whitelist/blacklist via either administrator functions or IOGEAR Port Authentication Utility.
2. The user can only blacklist an HID device within the default HID devices* for the Keyboard/ Mouse Ports. Please connect the HID device (you would like to blacklist) directly to the Mouse Port (do not connect it to the KVM via a USB hub), and perform the configuration via administrator functions. After configuration, the blacklisted HID device will be rejected by both Keyboard/ Mouse Ports. A USB hub cannot be added to blacklist via administrator functions.

* The default HID devices for Keyboard/ Mouse Ports could be referred to bullet 4. in the section “Always use qualified and authorized peripheral devices” on page 9.

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