



2/4-Port USB DisplayPort/HDMI

Single/Dual View Universal Secure KVM Switch User Manual

GCS1512TAA4 - GCS1514TAA4 - GCS1522TAA4 - GCS1524TAA4
GCS1512TAA4C - GCS1514TAA4C - GCS1522TAA4C - GCS1524TAA4C

Table of Content

EMC Information.....	iv
User Notice.....	v
Package Contents.....	vi
About This Manual.....	vii
Overview	vii
Conventions	vii
Product Information	viii
Overview	1
Chapter 1 - Introduction	1
Features	2
Requirements.....	4
Console.....	4
Computers.....	4
Cables.....	4
Operating Systems.....	4
Front View (of IOGEAR Universal KVM Switch)	5
Rear View (of IOGEAR Universal Secure KVM Switch).....	6
Components.....	7
Front View (of IOGEAR Remote Port Selector	11
Chapter 2 – Hardware Setup.....	13
Before You Begin	13
Tampering prevention and detection.....	13
Always use qualified and authorized peripheral devices	14
Secure Installation	15
Secure Operation and Administration.....	15
Stacking.....	15
Rack Mounting	15
Installation.....	16
Rear View	19
Front View	19
Chapter 3 – Operation	20

Powering On	20
During the self-test	20
Self-test failure	20
Manual Switching	21
Port ID Numbering	21
LED Display	21
Chassis Intrusion Detection	23
Smart Card and CAC Reader (CAC models only)	24
Appendix	25
Specifications	26
Limited Warranty	28

EMC Information

FEDERAL COMMUNICATIONS COMMISSION 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 when the equipment is operated in a commercial environment. This equipment generates, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

Warning: Operation of this equipment in a residential environment could cause radio interference

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.



Industry Canada Statement

This Class A digital apparatus complies with Canadian ICES-00

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

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 service, 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

The IOGEAR Universal Secure KVM package consists of:

1 x Universal Secure KVM Switch

1 x Power Adapter

1 x Foot Pad Set

1 x Port Name Labels

1 x User Manual*

1 x HDMI Cable Lock Set**

Check to make sure that all the components are present and in good order. If anything is missing, or was damaged in shipping, contact your dealer.

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 the Universal Secure KVM installation.

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

** The HDMI Cable Lock is specifically designed for DisplayPort/HDMI combo connectors to ensure a secure connection between the HDMI cable and the Universal Secure KVM switch. Several HDMI Cable Locks are included in the package contents. Please visit our website for installation instructions.

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 Universal Secure KVM Switch (except Power) flash continuously, all Remote Port Selector (RPS) LEDs flash, or either enclosure appears breached, avoid using this product and contact your IOGEAR dealer.

The Universal Secure KVM Switch, and the 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/RPS, and void the warranty.



Tamper-evident seal

About This Manual

This user manual is intended for system administrators and end users.

This user manual is provided to help you get the most from your IOGEAR Universal Secure KVM Switch system. It covers all aspects of installation, configuration, and operation. An overview of the information found in the manual is provided below.

This user manual covers the following IOGEAR Universal Secure KVM Switches

Configuration (with CAC function)			2-Port	4-Port
PC Video Connection	Console Video Connection	No. of Displays		
DisplayPort / HDMI	DisplayPort / HDMI	Single	GCS1512TAA4C	GCS1514TAA4C
		Dual	GCS1522TAA4C	GCS1524TAA4C

Configuration (without CAC function)			2-Port	4-Port
PC Video Connection	Console Video Connection	No. of Displays		
DisplayPort / HDMI	DisplayPort / HDMI	Single	GCS1512TAA4	GCS1514TAA4
		Dual	GCS1522TAA4	GCS1524TAA4

Overview


Chapter 1, Introduction, introduces you to the IOGEAR Universal Secure KVM Switch system. Its purpose, features, and benefits are presented, and its front and back panel components are described. **Chapter 2, Hardware Setup**, provides step-by-step instructions for setting up your installation.

Chapter 3, Operation, explains the concepts involved in operating the IOGEAR Universal Secure KVM Switch.

An Appendix provides specifications and other technical information regarding the IOGEAR Universal Secure KVM Switch.

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 chorded, 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 <i>Start</i> menu, and then select <i>Run</i> .
	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 Universal Secure KVM Switch series is NIAP¹-certified and compliant with NIAP PPv4.0 (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) Reader³ between multiple computers. Conformity with Protection Profile v4.0 certifies that other USB peripherals cannot be connected to the console ports of the Universal Secure KVM Switch, and that only a keyboard and mouse are accommodated, therefore providing high-level security, protection, and safekeeping of data.

The IOGEAR Universal Secure KVM Switch hardware security includes tamper-evident tape, chassis intrusion detection, and tamper-proof hardware, while software security features include restricted USB connectivity – non-HIDs (Human Interface Devices) or non-predefined CAC/HIDs are ignored when switching, an isolated channel per port that makes it impossible for data to be transferred between secure and unsecure computers, and automatic clearing of the keyboard and mouse data when switching port focus.

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

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. It is operated by the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST).
2. The IOGEAR Universal Secure KVM Switch series additionally satisfies 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.

Features

FEATURES		BENEFITS
■	2/4-Port USB DisplayPort/HDMI Single/Dual Display Universal Secure KVM Switch	Reduces the costs involved in controlling up to 4 Single/Dual Display computers while offering data isolation between shared peripherals and computers
■	DisplayPort/HDMI combo connectors ¹	Support DisplayPort and HDMI video interfaces (both PC and Console sides)
■	Superior ultra-high video resolution to 5K UHD 5120 × 2880 ²	Supports resolutions to 5120 × 2880 with crystal clear image quality
■	Video DynaSync™ – exclusive IOGEAR technology	IOGEAR Video DynaSync™ eliminates boot-up display problems and optimizes resolutions when switching between ports
■	DisplayPort AUX channel filtering	Non-qualified auxiliary channel traffic such as MCCS and EDID write is rejected
■	NIAP PP PSD v4.0 certified	Provides the most advanced security features required by the latest Protection Profile (PP) v4.0 for Peripheral Sharing Device (PSD)
■	Pushbutton / Remote Port Selector (RPS) ³ port selection and secure port switching	Port selection via pushbutton / Remote Port Selector (RPS) only to enhance security. Keyboard, Mouse, Video, Audio and CAC readers switch together for secure switching.
■	Channel Isolation	Isolated channel per port — makes it impossible for data to be transferred between computers
■	Shared peripherals and computer isolation	The always-on keyboard, mouse, and display EDID emulation ensures isolation between peripherals and connected computers.
■	Restricted USB connectivity	Non-authorized HID (Human Interface Devices) or non-predefined CAC/HIDs will be rejected / ignored.
■	Unidirectional data flow	Secure design enables unidirectional data flow between devices and connected computers.
■	Administrative configuration and event log functions	Secure access for authorized administrators to audit KVM operation logs and secure configuration. (Please refer to the Administrator guide.)
■	Supports analogue audio (speaker only) ⁴	Only unidirectional speaker data is allowed preventing the passage of the analogue audio by microphone input or line input.
■	Active always-on chassis intrusion detection	If physical tampering is detected, the switch or the Remote Port Selector becomes permanently inoperable.
■	Clears keyboard data when switching	Keyboard data is automatically purged when switching KVM port focus.

■	Configurable Port LED color and Port Name Labels	Easier identification between ports connected to different security classification levels.
■	Tamper-proof hardware	All integrated circuits are soldered directly to the circuit board to prevent tampering with the components.
■	Tamper-evident tape	Provides a visual indication of any attempt to gain access to the switch (or RPS) internal components.
■	Firmware non-reprogrammable	Prevents tampering and attempts to reprogram the switch's firmware.
■	Metal enclosure	Rugged metal enclosure.

Note:

1. Connect the DisplayPort cable to the DisplayPort section (upper side) of the DisplayPort/HDMI combo connector or connect the HDMI cable to the HDMI section (lower side) of the DisplayPort/HDMI combo connector.
2. Supports video output resolutions to 5120 × 2880 @60Hz, 5120 x 2160 @60Hz, 5120 x 1440 @60Hz, 120Hz, 144Hz, 3840 x 2160 @60Hz, 120Hz, 144Hz.
3. Remote Port Selector is not supplied in the package and requires a separate purchase
4. Only analogue speaker data input is supported. The IOGEAR Universal Secure KVM Switch does not convert digital audio to analogue audio.

Requirements

Console

- HDMI or DisplayPort monitor capable of the highest resolution that you will be using on any computer in the installation
- USB mouse
- USB keyboard
- Speaker (Optional)
- USB Smart card or CAC (Common Access Card) reader (Optional)*
- Remote Port Selector (Optional)**

Computers

- A HDMI/DisplayPort video output connector
- A USB Type A port for keyboard and mouse
- A USB Type A port for Smart Card or CAC reader (Optional)*
- A 3.5 mm jack Audio port for speaker (Optional)

Cables

- The KVM cable sets which are specifically designed to work with this switch are not supplied in the package and require a separate purchase.
- For security, do not connect any cable that has a microphone audio input or line in audio input.

Note:

* Only applicable on the models with CAC function

** Remote Port Selector is not supplied in the package and requires a separate purchase

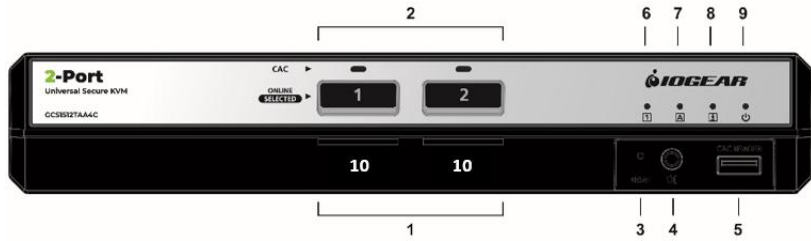
Operating Systems

Suggested operating systems are shown in the table below:

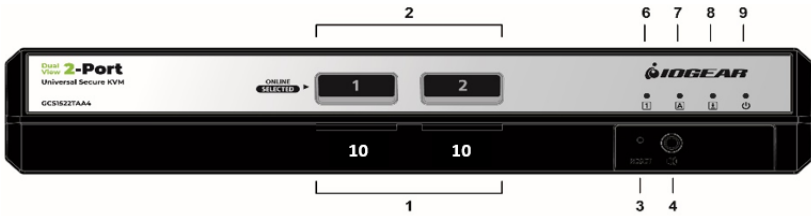
OS		Version
Windows		7 / 10 / 11
Linux	Ubuntu	24.04
	CentOS	9
	openSUSE	15.3 Leap
macOS		14

Front View (of IOGEAR Universal KVM Switch)

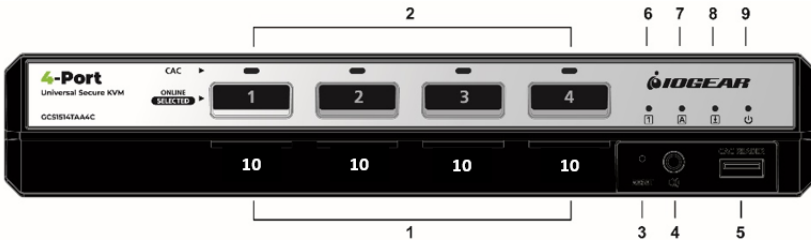
GCS1512TAA4C



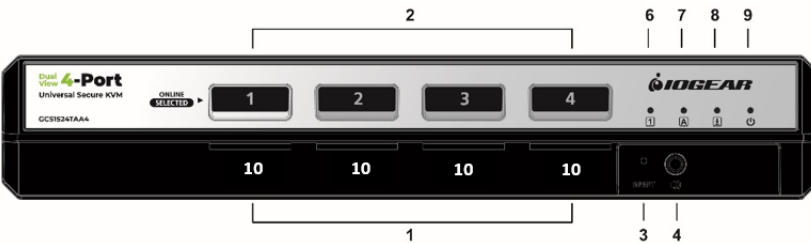
GCS1522TAA4



GCS1514TAA4C

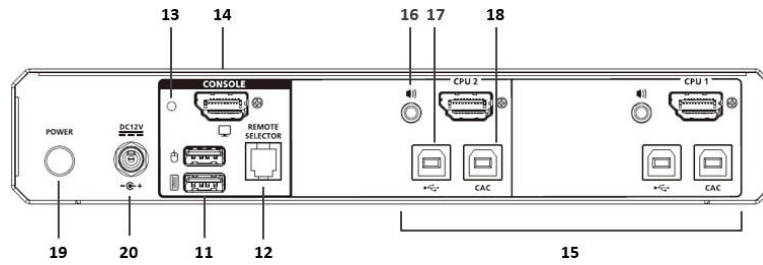


GCS1524TAA4

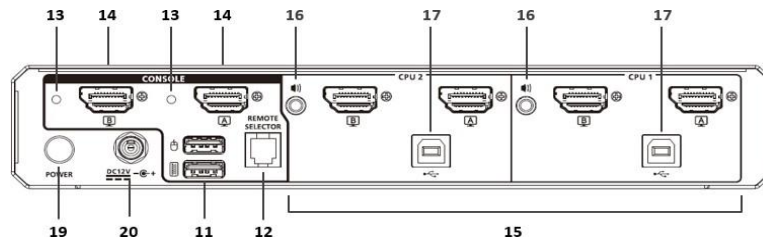


Rear View (of IOGEAR Universal Secure KVM Switch)

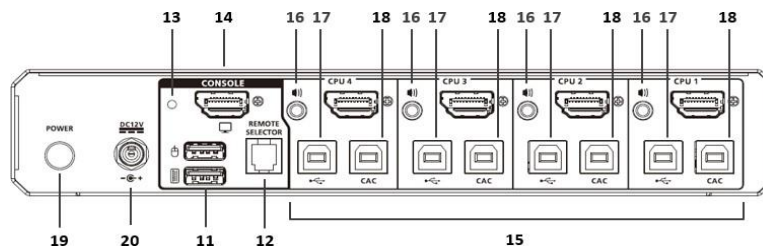
GCS1512TAA4C



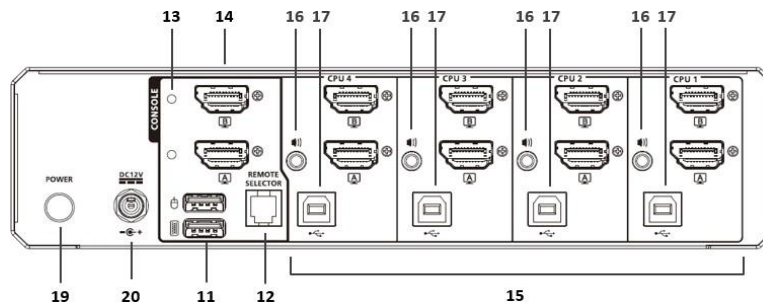
GCS1522TAA4



GCS1514TAA4C



GCS1524TAA4



Components

Note:

This user manual uses GCS1514TAA4C, GCS1522TAA4, GCS1514TAA4C, GCS15124TAA4 to demonstrate each port number (2/4- Port), CAC support (Yes/No), and number of displays (single/dual) supported by the IOGEAR Universal Secure KVM Switch series.

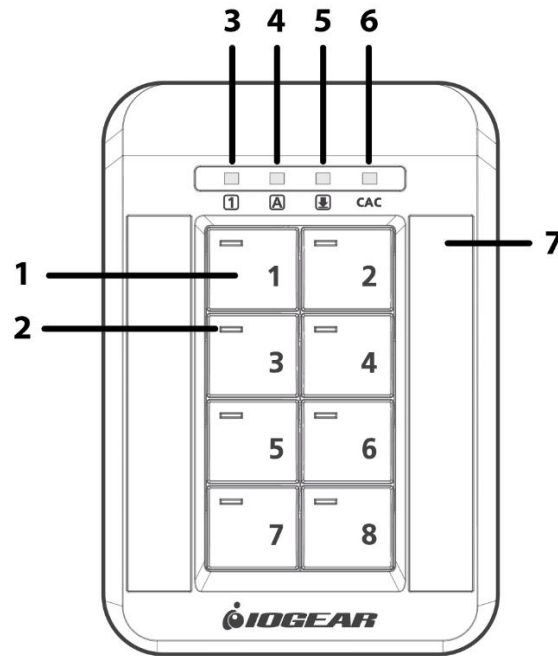
No.	Component	Description
1	Port Selection Pushbuttons	Pressing a Port Selection Pushbutton brings together the keyboard, mouse, video, audio, and CAC reader focus to the computer attached to its corresponding port.
2	Port and CAC LEDs	<p>The Port / CAC LEDs are located on the front panel to indicate Port / CAC reader selection or connection status.</p> <p>Port LEDs (Lower row)</p> <p>Selected – Lights bright green (default) to indicate that the computer attached to its corresponding port has the KVM focus.</p> <p>Online – Lights orange to indicate that the computer attached to its corresponding port is connected and powered on.</p> <p>Warning - Flashes to indicate that a non-qualified USB HID device is connected to the console USB keyboard port or mouse port when the corresponding port has the focus.</p> <p>CAC LEDs (Upper row, CAC models only)</p> <p>Selected – Lights bright green to indicate that the CAC function is enabled, and the computer attached to its corresponding port has the CAC focus.</p> <p>Online – Lights orange to indicate that the computer attached to its corresponding port has a USB CAC reader cable connection and the CAC function is enabled.</p> <p>None – No lights indicate that the cable is not connected, or CAC has been disabled.</p> <p>Warning - Flashes to indicate that a non-qualified USB smart card / CAC reader is connected when the corresponding port has the focus.</p> <p>Note:</p> <ol style="list-style-type: none"> The Port LED color (for the selected computer) can be configured by authorized administrators for identification (default is bright green). Please refer to the Administrator Guide for details. CAC function of each port can be enabled or disabled by pressing the port selection pushbutton for more than 3 seconds (this is a toggle feature). Please refer to the operation section of this user manual for more information. All front panel LEDs (except the Power LED) will flash continuously when a chassis intrusion or self-test failure (except for Pushbutton jam) is detected. See Chassis Intrusion Detection section for further details. Port and CAC LEDs also indicate the status of the Universal Secure KVM self-test status. See Operation section for further details

3	Reset Button	<p>Press this button to reset the IOGEAR Universal Secure KVM Switch.</p> <p>Note:</p> <p>When you perform a reset by pressing the reset button for more than 5 seconds, the keyboard/mouse data will be purged, and the switch will reboot and perform a self-test. After a successful self-test, port focus will switch to Port 1, and the CAC function of each port will be set to factory default setting (enabled).</p> <p>If the Universal Secure KVM fails to generate video on the monitor after a reset, please power off the installation, check the cables, and follow the instructions found in this manual to power on the installation.</p>
4	Audio Port	<p>The cables from your speakers plug in here.</p> <p>Note: Only standard analogue speaker connections are allowed. The use of an analogue microphone or line-in audio device is strictly prohibited.</p>
5	USB Smart Card / CAC Reader Port (CAC models only)	<p>Only qualified USB authentication devices (e.g., standard smart card and CAC reader) can be plugged into this port.</p> <p>Note: USB authentication device filter is configurable by authorized administrators for trusted devices (e.g. USB token, USB Biometric reader). Please refer to the Administrator Guide for details.</p>
6	Num Lock LED	<p>Lights green to indicate the Num Lock function has been turned on.</p> <p>Note: The Num Lock LED on the keyboard will be disabled due to security requirements.</p>
7	Caps Lock LED	<p>Lights green to indicate the Caps Lock function has been turned on.</p> <p>Note: The Caps Lock LED on the keyboard will be disabled due to security requirements.</p>
8	Scroll Lock LED	<p>Lights green to indicate the Scroll Lock function has been turned on.</p> <p>Note: The Scroll Lock LED on the keyboard will be disabled due to security requirements.</p>
9	Power LED	<p>Lights green to indicate that the IOGEAR Universal Secure KVM Switch is powered on.</p>
10	Port Name Label Area	<p>Port names can be written on labels and placed on this area for easier port identification.</p>

11	USB Console Ports	<p>The USB keyboard and mouse plug into these ports. The USB console keyboard port (lower port) and mouse port (upper port) support the following – standard USB keyboards/mice, standard USB keyboards/mice via a USB hub, and the HID functions of a composite device.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. The console USB keyboard and mouse ports are interchangeable, meaning you can connect a keyboard to the mouse port and vice versa. However, for optimal operation, it is recommended to connect the USB keyboard to the console USB keyboard port and the USB mouse to the console USB mouse port. <p>For security purposes, do not attempt to connect a wireless keyboard or mouse to the switch.</p>
		<ol style="list-style-type: none"> 2. Non-standard keyboards/mice with integrated USB hubs and/or other USB-integrated devices may not be fully supported due to the strict security standards and policy of the IOGEAR Universal Secure KVM Switch. If supported, only basic (HID) keyboard/mouse operations will function. 3. Multimedia keys on the keyboard will not function due to the security policy. 4. The Num Lock, Caps Lock, and Scroll Lock LED on keyboards will not function due to the security policy. 5. USB HID device filter is configurable by authorized administrators for trusted devices (only the USB console mouse port is applicable for setting specific blocked devices). Please refer to the Administrator Guide for details.
12	Remote Port Selector Port	<p>The cable on the Remote Port Selector plugs in here. (Remote Port Selector is not supplied in the package)</p>
13	Video LED(s)	<p>The LED will light up green when the video connection is up and running. The LED flashes when a non-qualified monitor is connected.</p> <p>Note: With the dual-display model, each console video connection has a video LED.</p>
14	Console Monitor Port(s)	<p>The cable from your console monitor plugs in here.</p> <p>Note: The dual-display model has two console monitor ports.</p>
15	KVM Port Section	<p>The custom KVM cables that attach to your computers plug into this section.</p>

16	KVM Audio Port	The audio cable that attaches to your computer plugs in here. Note: Only speaker connections are allowed. The use of an analog microphone or line-in audio device is strictly prohibited.
17	KVM USB Port	The USB cable that attaches to your computer's keyboard / mouse plugs in here.
18	KVM USB Smart Card / CAC (Common Access Card) Reader Port	The USB cable that attaches to your computer's USB Smart Card / CAC reader plugs in here.
19	Power Pushbutton	This power pushbutton powers the IOGEAR Universal Secure KVM Switch on and off.
20	Power Jack	The power adapter cable plugs in here

Front View (of IOGEAR Remote Port Selector



No.	Component	Description
1	Port Selection Pushbuttons	<p>Pressing a Port Selection Pushbutton brings together the keyboard, mouse, video, audio, and CAC reader focus to the computer attached to its corresponding port.</p> <p>Note: When attached to a 2-Port Universal Secure KVM Switch, only pushbuttons numbered 1 and 2 will be detected and functional. When attached to a 4-Port Universal Secure KVM Switch, only pushbuttons numbered 1, 2, 3, and 4 will be detected and functional.</p>
2	Port LEDs	<p>The Port LEDs are located on the upper-left side (of each pushbutton) to indicate port selection and connection status.</p> <p>Port LEDs</p> <p>Selected – Lights bright green to indicate that the computer attached to its corresponding port has the KVM focus.</p> <p>Online – Lights orange to indicate that the computer attached to its corresponding port is connected and powered on.</p> <p>Warning - 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.</p>

3	Num Lock LED	Lights green to indicate the Num Lock function has been turned on. Note: The Num Lock LED on the keyboard will be disabled due to security requirements.
4	Caps Lock LED	Lights green to indicate the Caps Lock function has been turned on. Note: The Caps Lock LED on the keyboard will be disabled due to security requirements.
5	Scroll Lock LED	Lights green to indicate the Scroll Lock function has been turned on. Note: The Scroll Lock LED on the keyboard will be disabled due to security requirements.
6	CAC LED	<p>The CAC LED is located on the far right of the upper bar (on the panel) to indicate CAC reader selection status.</p> <p>CAC LED (CAC models only)</p> <p>Selected/Online – Lights bright green to indicate that the CAC function is enabled and the computer attached to its corresponding port has a USB CAC reader cable connection and has the CAC focus.</p> <p>None – No lights indicate that the cable is not connected, or CAC has been disabled.</p> <p>Warning – Flashes to indicate that a non-qualified USB smart card / CAC reader is connected when the corresponding port has the focus.</p> <p>Note:</p> <p>All panel LEDs on the RPS will flash continuously when a chassis intrusion (except for Pushbutton jam) is detected. See Chassis Intrusion Detection section for further details.</p>
7	Port Name Label Area	Port names can be written on labels and placed on these two areas covered with mylar panels for easier port identification.

Chapter 2 – Hardware Setup

Before You Begin

ATTENTION

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

If all front panel LEDs on the Universal Secure KVM Switch (except Power) flash continuously, all Remote Port Selector (RPS) LEDs flash, or either enclosure appears breached, avoid using the product and contact your IOGEAR dealer.

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



Tamper-evident seal

Tampering prevention and detection

1. The IOGEAR Universal Secure KVM Switch, and the optional Remote Port Selector (RPS) include tamper-evident tape to provide visual indications of intrusion to the switch / RPS enclosure. If the tamper-evident seal is missing, peeled, or looks as if it has been adjusted, avoid using the product and contact your IOGEAR dealer.
2. The IOGEAR Universal Secure KVM Switch and IOGEAR RPS are equipped with active always-on chassis intrusion detection:
 - If a mechanical intrusion is detected on the switch, the switch (without RPS connected) will be permanently disabled, and all the front panel LEDs (except the 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 itself and the switch, and all LEDs (on RPS) and the front panel LEDs except the Power LED (on switch) will flash continuously.

If the switch or RPS enclosure appears breached or all the LEDs are flashing continuously, stop using it, remove it from service immediately and contact your IOGEAR dealer.

3. Any attempt to open the switch or RPS enclosure will activate the chassis intrusion detection security, which will render it inoperable and void the warranty.
4. The IOGEAR Universal Secure KVM Switch cannot be upgraded, serviced, or repaired.
5. The IOGEAR Universal Secure KVM Switch and IOGEAR RPS contain an internal battery

which is non-replaceable. Never attempt to replace the battery or open the switch / RPS enclosure.

Always use qualified and authorized peripheral devices

1. For security, the IOGEAR Universal Secure KVM Switch supports only standard USB devices (or pointing device). Do not connect a wireless keyboard/mouse, or any keyboard/mouse with an internal USB hub or composite device with non-HID functions to the switch.
2. If a non-qualified keyboard is connected, the keyboard will not function. No keystrokes will be seen on the screen.
3. If a non-qualified mouse is connected, the mouse will not function. No cursor movement will be seen on the screen.
4. For security, the 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 the security policy.
6. Special multimedia keys on the keyboard will be disabled due to the security policy.
7. For security, the IOGEAR Universal Secure KVM Switch does not support an analogue microphone or line-in audio input. Never connect a microphone or headset microphone to the audio output port. Standard analogue speakers and headsets are supported.
8. For security, the USB CAC port by default only supports authorized user authentication devices such as USB Smartcard or CAC readers. Do not connect other USB devices to the USB CAC port. Non-qualified or non-authorized USB devices will be rejected. For administrative configuration, please refer to the Administrator 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 a qualified monitor. 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 the Universal 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 the IOGEAR Universal 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 23. Please review it before proceeding.
3. Before installation, make sure the power sources to all devices connected to the installation are turned off. You must unplug the power cords of any computers that have the Keyboard Power On function.
4. For optimal display output, it is recommended to power off the Universal Secure KVM Switch and the monitor before changing the console monitor.
5. A computer connected to the Universal Secure KVM Switch should only be powered on after all the connections to the device are made (video, USB and audio).

Secure Operation and Administration

Please refer to the Administrator Guide for Universal Secure KVM Switch configuration and event log auditing functions.

Stacking

The IOGEAR Universal Secure KVM Switch features a rugged metal enclosure which provides stability and allows the unit to be stacked on a desktop. The unit can be placed on any level surface that can safely support its weight and the weight of the attached cables. Ensure that the surface is clean and free of materials that can block the exhaust vents or otherwise interfere with the normal operation of the KVM switch.

Rack Mounting

Mounting kits specifically designed to work with Universal Secure KVM switches are not supplied in the package and require a separate purchase. Please visit our website for more details.

Installation

To set up your IOGEAR Universal Secure KVM Switch installation, refer to the installation diagram on page 22 (the numbers in the diagram correspond to the steps below), and do the following:

1. Plug your USB keyboard and USB mouse into the USB console ports located on the unit's rear panel. (The console USB keyboard/mouse ports are only compatible with standard USB keyboards/mice).

Note:

1. The console USB keyboard and mouse ports are interchangeable, meaning you can connect a keyboard to the mouse port and vice versa. However, for optimal operation, it is recommended to connect the USB keyboard to the console USB keyboard port and the USB mouse to the console USB mouse port.
2. For security purposes, do not attempt to connect a wireless keyboard/mouse to the switch.
3. During KVM operation, non-standard keyboards with integrated USB hubs and/or other USB-integrated devices may not be fully supported due to the strict security standards and policy of the IOGEAR Universal Secure KVM Switch. If supported, only basic (HID) keyboard/mouse operations will function.
4. When the Universal Secure KVM Switch is powered on, if the keyboard or mouse is rejected, the keyboard and mouse will be inoperable (mouse cursor freezes and/or no keystrokes will respond).

2. Plug your console monitor(s) into the console video port(s) located on the unit's rear panel and power on the monitor.

Note:

1. When the IOGEAR Universal Secure KVM Switch is powered on, the Video LED lights green when the video connection is up and running. The Video LED flashes when a non-qualified monitor is connected.
2. For optimal display output, it is recommended to power off the Universal Secure KVM Switch and the monitor before changing the console monitor.
3. Connected monitors will be filtered when the IOGEAR Universal Secure KVM Switch is powered on. Non-qualified monitors will be rejected (Video LED flashes). Please refer to the LED Display for detailed visual identification.

3. Plug your speakers into the console speaker jack located on the unit's front panel.

Note:

Only speaker connections are allowed. The use of an analogue microphone or line-in audio connection is strictly prohibited.

4. With a single-display Universal Secure KVM Switch, using a KVM cable set (not supplied

with this package and must be purchased separately), plug the video connector into any available video socket in the KVM port section of the switch, then plug the accompanying USB (keyboard/mouse or CAC) and speaker connectors into their corresponding USB and speaker sockets.

With a dual-display Universal Secure KVM Switch, using a KVM cable set (not supplied with this package and must be purchased separately), plug the video connector for your primary monitor into any available video socket A in the KVM port section of the switch. Using another video cable and plug the video connector for your secondary monitor into video socket B on the same KVM port section of the switch, then plug the accompanying USB (keyboard/mouse or CAC) and speaker connectors into their corresponding USB and speaker sockets.

Note:

1. Verify that all the plugs are in the same KVM port sockets (all in Port 1, all in Port 2, etc.). Each socket is marked with an appropriate icon.
2. If the CAC reader function is to be disabled for certain PCs, it's advised not to connect a USB CAC cable in the installation.

5. At the other end of the KVM cable set, plug the USB, video, and speaker cables into their respective ports on the computer.

With a dual-display Universal Secure KVM Switch, at the other end of the other video cable, plug this video cable into its respective port on the computer.

Note:

1. Verify that the second video plug is in the same KVM port section as the first video plug (all in Port 1, all in Port 2, etc.). Each socket is marked with an appropriate icon.
2. Repeat steps 4, 5 for each computer you are installing.
3. With a dual-display installation, for easier cabling at your site, you can also connect all the primary video connectors to video sockets B, and secondary video connectors to video

6. Plug the USB Smart Card / CAC reader to the console CAC port on the front panel. (Optional)

Note:

1. Only appropriate qualified USB authentication devices (e.g., Smart Card and CAC readers by default) can be plugged into this port. During KVM operation, non-qualified or non-authorized USB devices will be filtered and rejected (the CAC LED that has the port focus will flash). Please refer to the LED display for visual indications.
2. The CDF (Configurable Device Filtration) function can only be operated by authorized administrators. Please refer to the Administrator Guide and Port Authentication Utility Guide for details.
3. An active session on the selected computer is immediately terminated upon removal of the CAC card.

7. Plug the cable on the RPS into the console RPS port. (Optional)

Note:

1. Be sure to connect the RPS before the IOGEAR Universal Secure KVM Switch is powered on.
2. Any connection of RPS after the IOGEAR Universal Secure KVM Switch is powered on will not be detected by the switch.

8. Plug the power cord into the IOGEAR Universal Secure KVM Switch power socket.

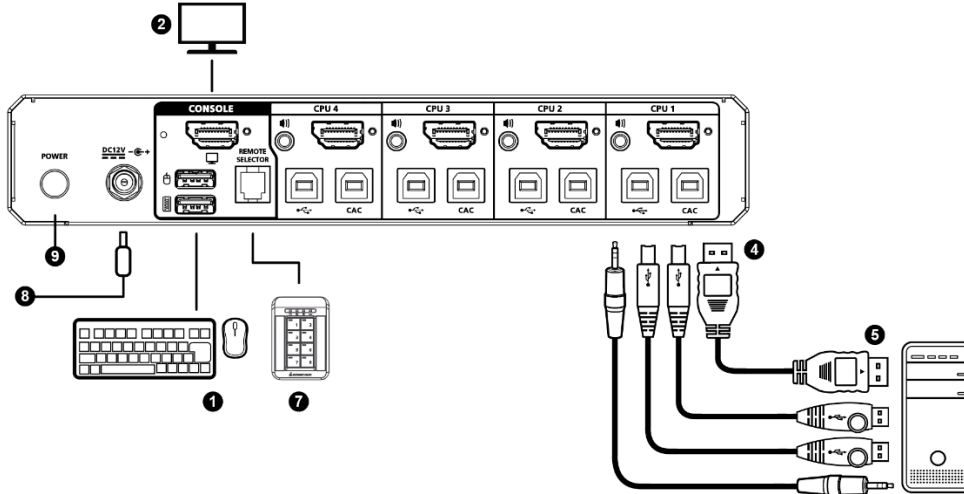
9. Turn on the IOGEAR Universal Secure KVM Switch and check that the LEDs light up. The IOGEAR Universal Secure KVM Switch will start a self-test.

Note:

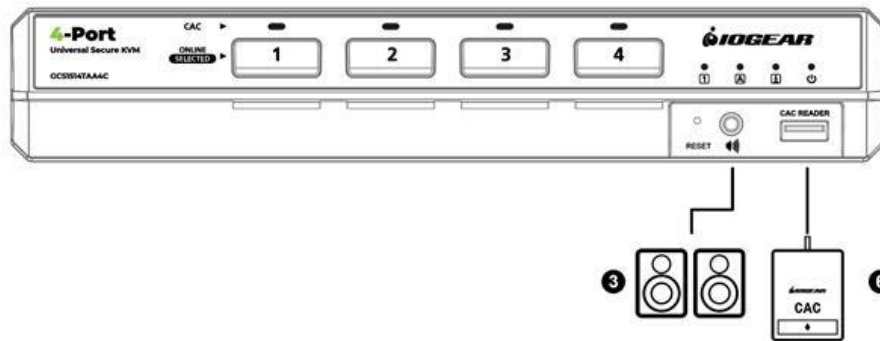
The IOGEAR Universal Secure KVM Switch performs a security self-test at power-on and at each power cycle. Front panel LEDs will indicate the self-test status and test result. Please refer to the operation section and LED Display section for visual identification details.

Installation Diagram

Rear View



Front View



Chapter 3 – Operation

Powering On

When you power on, reset, or power cycle the IOGEAR Universal 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 LEDs, all CAC LEDs (if supported), Num Lock LED, Caps Lock LED, and Scroll Lock LED on the Universal Secure KVM will turn ON and then OFF.

The KVM focus will be switched to Port 1 when the self-test is completed successfully (Port 1 LED lights bright green).

Self-test failure

In the case of a self-test failure, the Universal Secure KVM Switch becomes inoperable, with front panel LED combinations (on the Universal Secure KVM) indicating the potential cause of the failure (such as button jam or KVM integrity compromise)

A pre-defined combination of the Port and CAC LEDs indicates the cause of the failure.

If all front panel LEDs on the Universal Secure KVM (except the Power LED) flash continuously, it means 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's LEDs (Port LED and CAC LED) will flash.

For security, the IOGEAR Universal Secure KVM Switch becomes inoperable if the self-test fails. Please verify your KVM installation by checking that the front panel pushbuttons are not stuck and then power cycle the Universal Secure KVM Switch. If the self-test failure remains, stop using the IOGEAR Universal Secure KVM Switch immediately, remove it from service and contact your IOGEAR dealer.

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

The IOGEAR Universal Secure KVM Switch filters and emulates both a mouse and keyboard on each port after the unit is powered on. If the keyboard, mouse, monitor, or Smart card / CAC reader fails to operate properly, make sure that you are using the appropriate peripherals (qualified and authorized peripherals); then power off the IOGEAR Universal Secure KVM Switch, check all the cable connections, and power on the unit again.

Manual Switching

For enhanced security, the IOGEAR Universal Secure KVM Switch offers manual port switching only. This is achieved by pressing the port selection pushbuttons located on the switch front panel or pressing the port selection pushbuttons located on the RPS panel (if RPS is 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, audio, and USB CAC reader ports will be switched together. The Selected Port LED lights bright green (on Switch and/or RPS) 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 should be able to detect the peripherals after port switching. If the PC fails to detect the keyboard, mouse, or the CAC reader:

- Verify that the keyboard, mouse, and/or CAC reader are qualified.
- Verify that the keyboard, mouse, or CAC reader hasn't failed.
- For USB CAC reader (USB authentication device), please make sure that the USB CAC cable has been securely connected, and the CAC function is enabled.
- For USB CAC reader port, please contact your administrator to verify if the device has been authorized.

Port ID Numbering

Each KVM port on the IOGEAR Universal Secure KVM Switch is assigned a port number (1~2 for the 2-Port models; 1~4 for the 4-Port models). The port numbers are marked on the rear of the switch. See Rear View, page 7. The port ID of a computer is derived from the KVM port number it is connected to.

LED Display

In addition to the Power LED, the IOGEAR Universal Secure KVM Switch (and IOGEAR RPS) has Port LEDs (Online and Selected), keyboard lock (Num Lock/Caps Lock/Scroll Lock) LEDs and CAC LEDs that are built into the front panel to indicate port / keyboard / CAC reader operating status. A video LED is located on the back panel (of the switch) to indicate the operating status of the video connection. These LEDs also serve as the alarm notification for KVM security issues.

LED	Indication
Power LED (on the Universal Secure KVM switch)	The Power LED is on the front panel lights green to indicate that the KVM switch is powered on.
Video LED (on the Universal Secure KVM switch)	The Video LED is located on the back panel next to each video connector. The LED lights are green when the video connection is up and running. The LED flashes when a non-qualified monitor is connected.
Port LED (on the Universal Secure KVM switch and the RPS)	<p>Port LEDs are located on the front panel (of the switch) and the upper-left side of each pushbutton (of the RPS) to indicate the port selection or connection status.</p> <p>Selected – Lights bright green (default) to indicate that the computer attached to its corresponding port has the KVM focus.</p> <p>Online – Lights orange to indicate that the computer attached to its corresponding port is connected and powered on.</p> <p>Warning - 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.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. The Port LED color (for the selected computer) can be configured by authorized administrators for identification (default is bright green). Please refer to the Administrator Guide for details. 2. Port and CAC LEDs (on the Universal Secure KVM switch) also indicate the status of the Universal Secure KVM self-test status. See Operation section for further details.

<p>CAC LED (on the Universal Secure KVM switch and the RPS) CAC models only</p>	<p>The CAC LEDs are located on the front panel (of the switch) and the far right of the upper bar on the panel (of the RPS) to indicate CAC reader selection or connection status.</p> <p>Selected – Lights bright green to indicate that the CAC function is enabled, and the computer attached to its corresponding port has the CAC focus.</p> <p>Online – Lights orange to indicate that the computer attached to its corresponding port has a USB CAC reader cable connection and the CAC function is enabled.</p> <p>None – No lights indicate that the cable is not connected, or CAC has been disabled.</p> <p>Warning - Flashes to indicate that a non-qualified USB Smart card / CAC reader is connected when the corresponding port has the focus.</p> <p>Note:</p>
	<ol style="list-style-type: none"> 1. The CAC function of each port can be enabled or disabled by pressing the port selection button (on the switch) for more than 3 seconds (this is a toggle feature). 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.
<p>Num Lock LED (on the Universal Secure KVM switch and the RPS)</p>	<p>Lights green to indicate the Num Lock is enabled</p>
<p>Caps Lock LED (on the Universal Secure KVM switch and the RPS)</p>	<p>Lights green to indicate the Caps Lock is enabled</p>
<p>Scroll Lock LED (on the Universal Secure KVM switch and the RPS)</p>	<p>Lights green to indicate the Scroll Lock is enabled</p>

Chassis Intrusion Detection

To help prevent malicious tampering with the IOGEAR Universal Secure KVM Switch, the switch (or the RPS) becomes inoperable and all front panel LEDs on the Universal 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).

The intrusion detection protection is an always-on function. If all front panel LEDs on the Universal Secure KVM Switch (except Power) flash continuously, all Remote Port Selector (RPS) LEDs flash, or either enclosure appears breached, avoid using the product and contact your IOGEAR dealer.

Smart Card and CAC Reader (CAC models only)

The USB Smart Card / CAC reader function of each port can be enabled or disabled (enabled by default). Press the port selection pushbutton (on the switch) for more than 3 seconds then release it, to enable/disable the CAC reader function for that port (this is a toggle feature). The CAC LEDs are used to indicate the CAC reader operation status.

If the CAC reader function is to be disabled for certain PCs, it's advised not to connect a USB CAC cable to the installation.

Appendix

General Safety Instructions

- This product is for indoor use only.
- Read all 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 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.

Specifications

IOGEAR DP/HDMI Single Display Universal Secure KVM (CAC and Non-CAC models)

Function		GCS1512TAA4C	GCS1512TAA4	GCS1514TAA4C	GCS1514TAA4	
Computer Connections	Direct	2	2	4	4	
	Max.	2	2	4	4	
Console Connections		1 Direct		1 Direct		
Port Selection		Pushbutton, Remote Port Selector		Pushbutton, Remote Port Selector		
Connectors	Console Ports	Keyboard	1 x USB Type A Female		1 x USB Type A Female	
		Video	1 x DisplayPort/HDMI Female		1 x DisplayPort/HDMI Female	
		Mouse	1 x USB Type A Female		1 x USB Type A Female	
		Speaker	1 x Mini Stereo Jack Female		1 x Mini Stereo Jack Female	
		Microphone	N/A		NA	
		CAC	1 x USB A Female	NA	1 x USB A Female	NA
	KVM Ports	Keyboard/ Mouse	2 x USB-B Female		4 x USB-B Female	
		Video	2 x DisplayPort/HDMI Female		4 x DisplayPort/HDMI Female	
		CAC	2 x USB-B Female	NA	4 x USB-B Female	NA
		Speaker	2 x Mini Stereo Jack Female		4 x Mini Stereo Jack Female	
		Microphone	N/A		NA	
	Power	1 x DC Jack		1 x DC Jack		
	Remote Port Selector	1 x RJ-11		1 x RJ-11		
Switches	Port	2 x Pushbuttons		4 x Pushbuttons		
	Reset	1 x Semi-recessed Pushbutton		1 x Semi-recessed Pushbutton		
	Power	1 x Pushbuttons		1 x Pushbuttons		
LEDs	Selected / Online	2 (Green / Orange)		4 (Green / Orange)		
	CAC activated	2 (Green)	NA	4 (Green)	NA	
	Power	1 (Green)		1 (Green)		
	Key Lock LED	3 (Green; Num Lock, Caps Lock, Scroll Lock)		3 (Green; Num Lock, Caps Lock, Scroll Lock)		
	Console Video	1 (Green, rear panel)		1 (Green, rear panel)		
Emulation	Keyboard/Mouse	USB		USB		
Video		5120 x 2880 @ 60 Hz		5120 x 2880 @ 60 Hz		
Housing		Metal		Metal		

IOGEAR DP/HDMI Dual Display Universal Secure KVM (CAC and Non-CAC models)

Function		GCS1522TAA4C	GCS1522TAA4	GCS1524TAA4C	GCS1524TAA4	
Computer Connections	Direct	2	2	4	4	
	Max.	2	2	4	4	
Console Connections		1 Direct		1 Direct		
Port Selection		Pushbutton, Remote Port Selector		Pushbutton, Remote Port Selector		
Connectors	Console Ports	Keyboard	1 x USB Type A Female		1 x USB Type A Female	
		Video	2 x DisplayPort/HDMI Female		2 x DisplayPort/HDMI Female	
		Mouse	1 x USB Type A Female		1 x USB Type A Female	
		Speaker	1 x Mini Stereo Jack Female		1 x Mini Stereo Jack Female	
		Microphone	N/A		NA	
		CAC	1 x USB A Female	NA	1 x USB A Female	NA
	KVM Ports	Keyboard/ Mouse	2 x USB-B Female		4 x USB-B Female	
		Video	4 x DisplayPort/HDMI Female		8 x DisplayPort/HDMI Female	
		CAC	2 x USB-B Female	NA	4 x USB-B Female	NA
		Speaker	2 x Mini Stereo Jack Female		4 x Mini Stereo Jack Female	
		Microphone	N/A		NA	
	Power		1 x DC Jack		1 x DC Jack	
	Remote Port Selector		1 x RJ-11		1 x RJ-11	
	Switches	Port	2 x Pushbuttons		4 x Pushbuttons	
Reset		1 x Semi-recessed Pushbutton		1 x Semi-recessed Pushbutton		
Power		1 x Pushbuttons		1 x Pushbuttons		
LEDs	Selected / Online	2 (Green / Orange)		4 (Green / Orange)		
	CAC activated	2 (Green)	NA	4 (Green)	NA	
	Power	1 (Green)		1 (Green)		
	Key Lock LED	3 (Green; Num Lock, Caps Lock, Scroll Lock)		3 (Green; Num Lock, Caps Lock, Scroll Lock)		
	Console Video	2 (Green, rear panel)		2 (Green, rear panel)		
Emulation	Keyboard/Mouse	USB		USB		
Video		5120 x 2880 @ 60 Hz		5120 x 2880 @ 60 Hz		
Housing		Metal		Metal		

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 3 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

