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

Single/Dual View Secure KVM Switch
Port Authentication Utility 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 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.

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

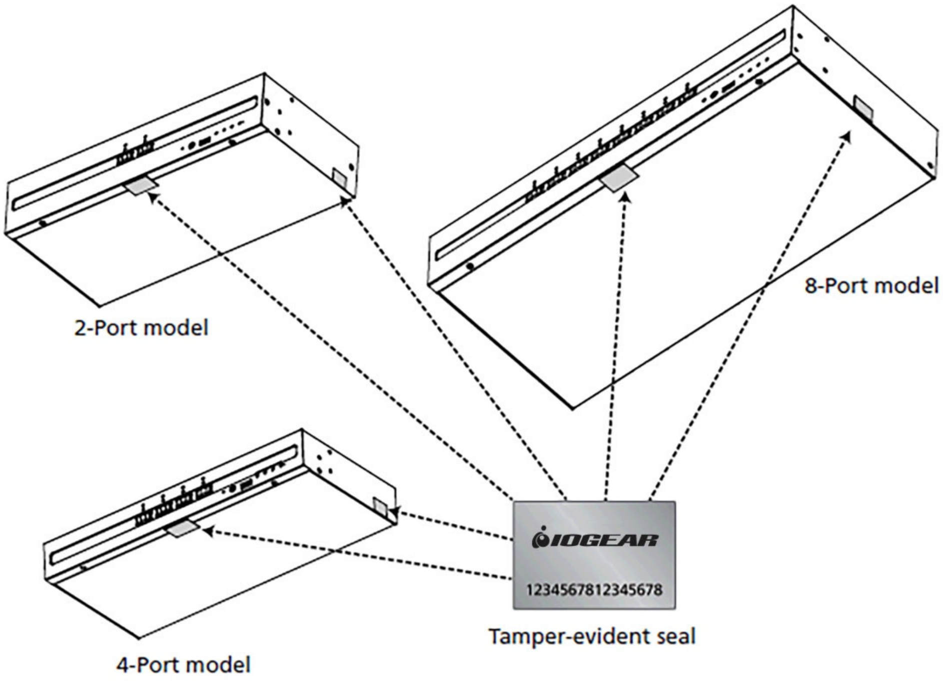
Manual Date: 2021-05-05

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 the 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 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 Port Authentication Utility Guide

This Port Authentication Utility Guide is intended for authorized administrators.

This Port Authentication Utility Guide is provided to help authorized administrators to configure authentication device filters (whitelist or blacklist) on the IOGEAR Secure KVM Switch. To maximize security, the administrator is advised to audit log events recorded by the IOGEAR Secure KVM Switch on a routine base.

This Port Authentication Utility Guide is applied to the following IOGEAR Secure KVM Switch with CAC function only.

Configuration			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 colored, 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 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.

Port Authentication Utility

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.

<u>Note:</u>

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).

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 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.

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 IOGEAR Secure KVM Switch, the administrator will be prompted to change the default password of the Port Authentication Utility after the first successful logon. The administrator is also advised to change the Port Authentication Utility password and audit event logs created by IOGEAR Secure KVM Switch on a routine base.

Tampering prevention and detection

1. IOGEAR'S Secure KVM switch and the optional Remote Port Selector (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 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 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 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 and RPS.
6. IOGEAR Secure KVM Switch contains 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, 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's 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 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 26. 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.
4. 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 LEDs, all CAC LEDs (if supported), Num Lock LED, Caps Lock LED, and Scroll Lock LED on the Secure KVM 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 (on the secure KVM) 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 on the Secure KVM (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

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).

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 located on the Secure KVM switch's front panel 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, 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 not failed.
- For USB CAC reader (USB authentication device), please make sure that the USB CAC cable has been securely connected, and that the CAC function is enabled.
- For USB CAC reader port, please contact your administrator to verify if the device you are using has been authorized.

Port ID Numbering

Each KVM port on IOGEAR Secure KVM Switch is assigned a port number (1-2 for 2-Port models; 1-4 for 4-Port models; 1-8 for 8-Port models). The port numbers are marked on the rear side of the switch. The port ID of a computer is derived from the KVM port number to which it is connected.

LED Display

In addition to Power LED, IOGEAR Secure KVM Switch and RPS have 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 rear 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 switch)	Power LED is located on the front panel ❑ The LED lights green to indicate that the KVM switch is powered on.
Video LED (on the 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 switch)	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. ❑ Online – Port LED lights dim orange to indicate that the computer attached to the corresponding port is established and powered on. ❑ Selected – Port LED lights bright orange to indicate that the computer attached to the corresponding port has the KVM focus. 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. Note: 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 status of the Secure KVM self-test status. See **Operation** section for further details

CAC (on the switch and the RPS) Models with CAC feature only	CAC LEDs are located on 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: ❑ 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 the 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 lights indicates that the cable is not connected or CAC function 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: • 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). Please refer to **Operation** section. • Port and CAC LEDs will flash constantly when a chassis intrusion is detected. See **Chassis Intrusion Detection** section for further details.
Num Lock (on the switch and the RPS)	Num Lock LED lights green to indicate Num Lock is enabled.
Caps Lock (on the switch and the RPS)	Caps Lock LED lights green to indicate Caps Lock is enabled.
Scroll Lock (on the switch and the RPS)	Scroll Lock LED lights green to indicate Scroll Lock is enabled.

Chassis Intrusion Detection

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

The Intrusion Detection Feature is an always-on function. If all front panel LEDs on the IOGEAR Secure KVM Switch (except for power LED) flash continuously, all Remote Port Selector (RPS) LEDs flash, or either 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 switch, configure user authenticated device filters, and audit log data generated by the Secure KVM Switch. Please refer to the IOGEAR Secure KVM Switch **Administrator's Guide** for detail.

Port Authentication Utility

IOGEAR Secure KVM Switch Port Authentication Utility enables authorized administrators to configure user authentication device filtering. By default, the USB CAC Port on IOGEAR Secure KVM Switch supports authorized User Authentication Device such as USB Smartcards or CAC readers. The Port Authentication Utility enables authorized administrators to assign a whitelist and a blacklist filter to the USB/CAC Port.

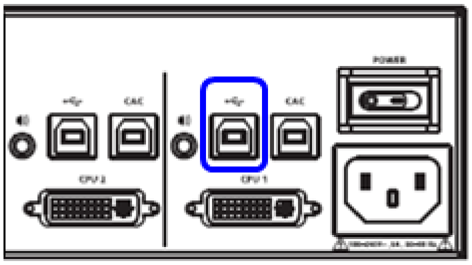
ATTENTION

- The whitelist and blacklist assigned by the Secure KVM Switch administrator functions has higher priority over the lists in the Port Authentication Utility. Please refer to IOGEAR Secure KVM Switch **Administrator's Guide** for details.
- The reset of the whitelist and blacklist assigned by the Secure KVM administrator function does not affect the whitelist and blacklist uploaded by the Port Authentication Utility.
- With the Port Authentication Utility, when a device is assigned to both the blacklist and whitelist, the device will be treated as blacklisted (**Device Filtering Rule**: blacklist always has higher priority over whitelist).
- 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.

Setup for Port Authentication Utility

This section assists with installation and setting up for the Port Authentication Utility. Only authorized administrators are allowed to perform the installation and operate the Port Authentication Utility. IOGEAR Port Authentication Utility supports Microsoft Windows®8 and higher.

1. Install IOGEAR Port Authentication Utility to a separate secure source computer following the Installation instruction. This separate secure source computer is for management only and has its own monitor, keyboard, and mouse connected for installation and operation. Power off this separate source PC after Port authentication Utility installation.
2. Connect a qualified monitor, keyboard, and mouse to the IOGEAR Secure KVM Switch's console section. (Please refer to the Secure KVM **User Manual** for details).
3. Connect the separate secure source computer (with IOGEAR Port Authentication Utility previously installed) to Port 1 (demonstrated below) of the Secure KVM Switch Port section via USB B-to-A cable of the KVM cable sets.



Port 1

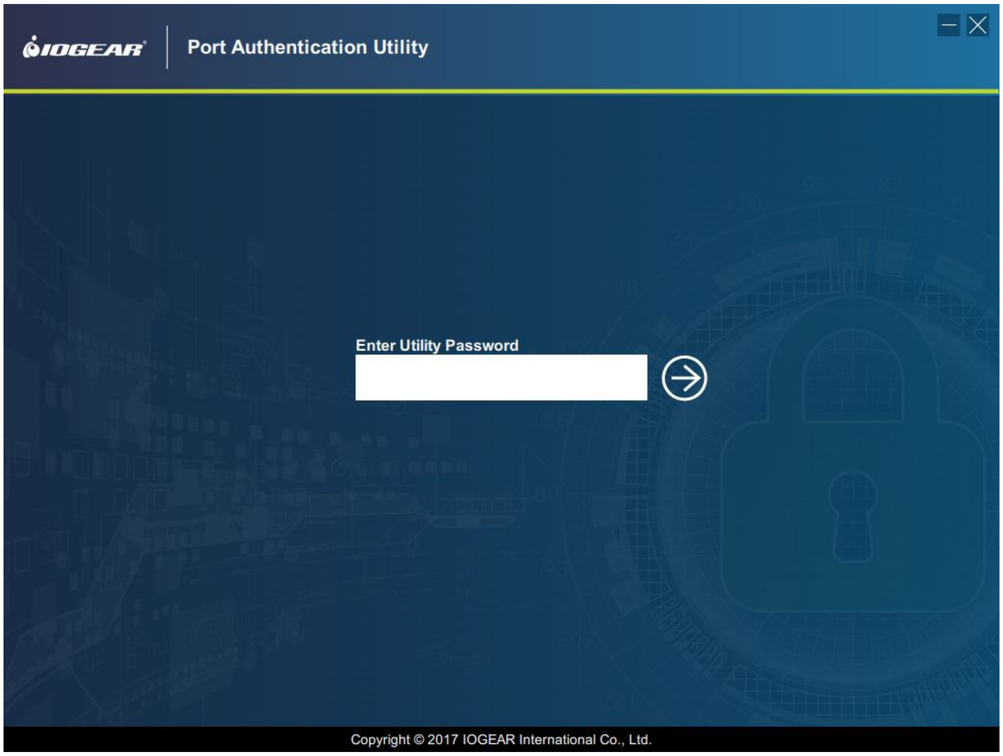
4. Power on the IOGEAR Secure KVM Switch, then power on the separate source computer (with Port Authentication Utility installed) connected to Port 1. The IOGEAR Secure KVM Switch will switch to Port 1 after a successful self-test.
5. Use the monitor, keyboard, and mouse from the source computer to operate IOGEAR Port Authentication Utility.

Port Authentication Utility Operation

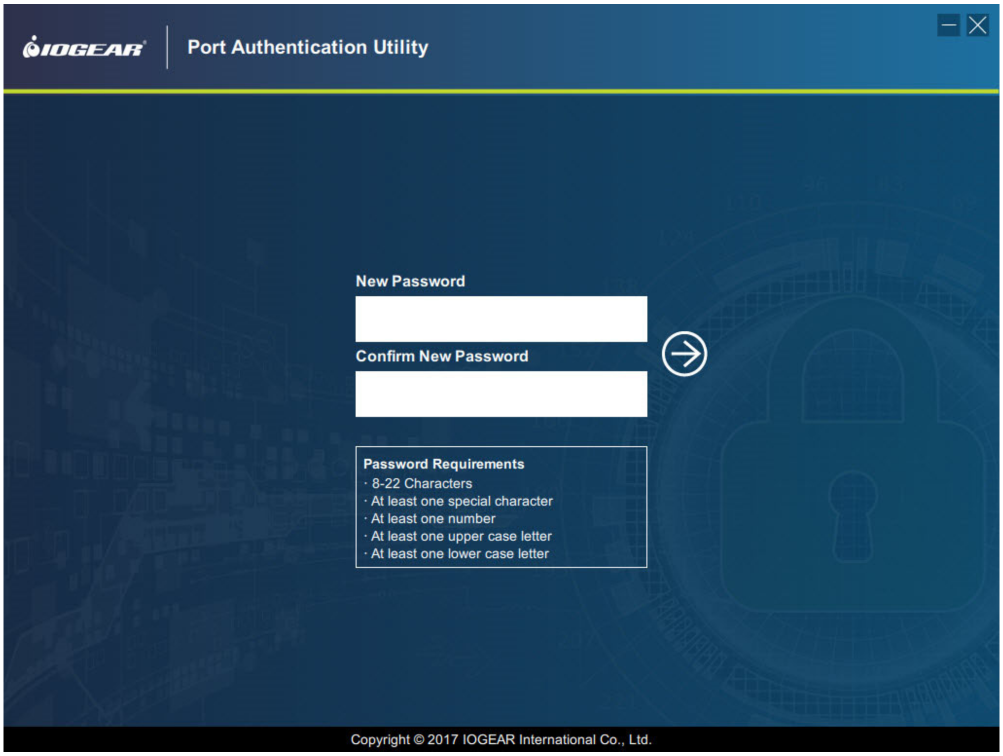
After the separate secure computer and IOGEAR Secure KVM Switch are ready, open the Port Authentication Utility installed on the separate secure computer.

1. The administrator will be prompted to enter the default password when Port Authentication Utility is opened for the first-time.
   The default password for first-time Port Authentication Utility is: abcd@XYZ#1357!

   The password is case-sensitive


IOGEAR
Port Authentication Utility
Enter Utility Password
Copyright © 2017 IOGEAR International Co., Ltd.

2. After the first-time successful password input, the administrator will be prompted to change the password.


IOGEAR
Port Authentication Utility
New Password
Confirm New Password
Copyright © 2017 IOGEAR International Co., Ltd.

Password Requirements
- 8-22 Characters
- At least one special character
- At least one number
- At least one upper case letter
- At least one lower case letter

The new password is case-sensitive. For maximum security, the new password must contain:

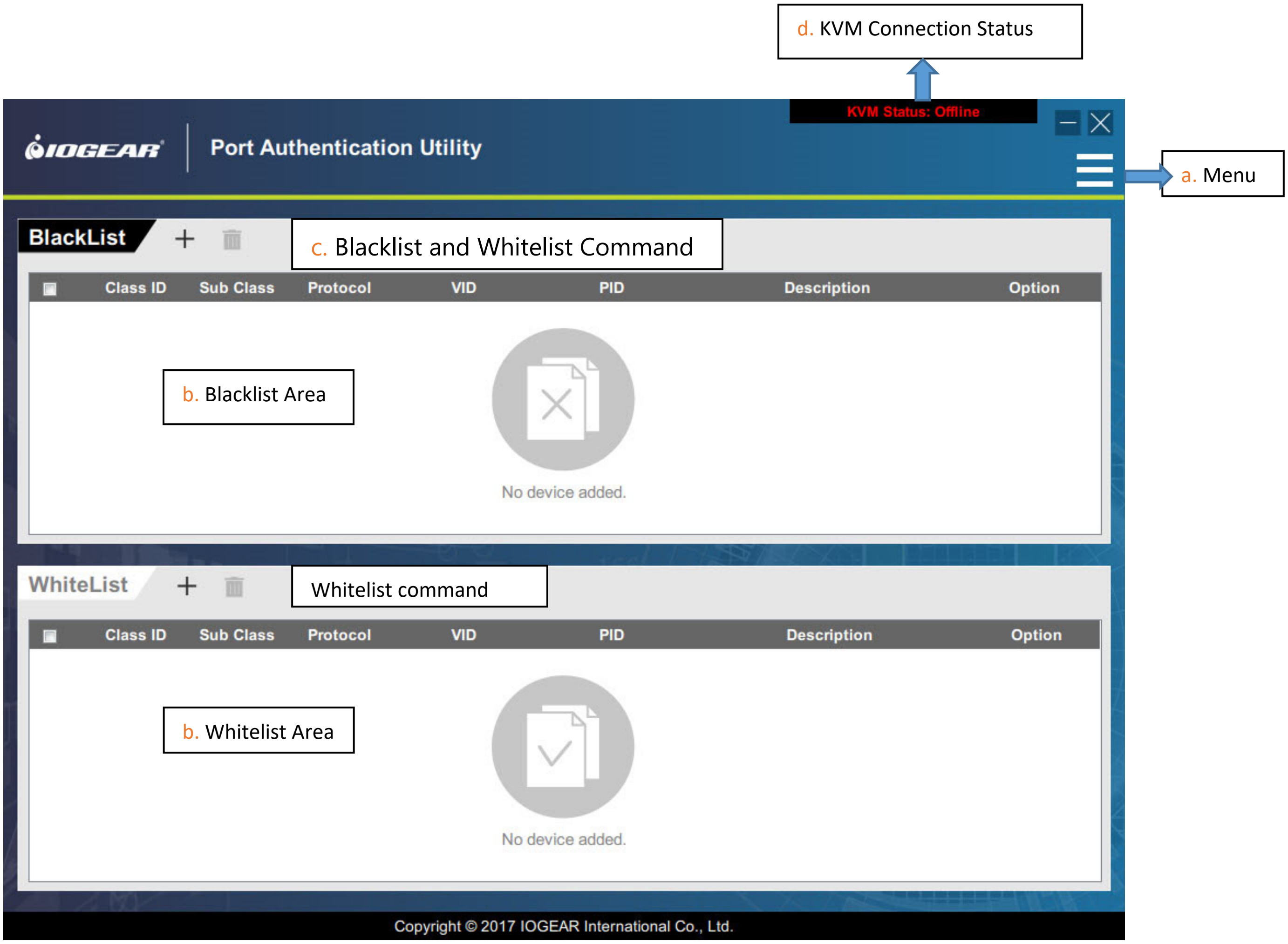
a. At least 8 characters in length, but no longer than 22 characters
b. A minimum of 1 lower case letter and,
c. A minimum of 1 upper case letter and,
d. A minimum of 1 numeric character and,
e. A minimum of 1 special character.

ATTENTION

- Do not use the default password for your new password.
- This password is for Port Authentication Utility only. Do not use the same password for Administrator Logon functions.
- The password for the Port Authentication Utility can be changed anytime via the password change option in the menu.

After the new password has been confirmed, the administrator can create a new filter list or open an existing filter list.

3. Port Authentication Utility Interface
The filter list contains a Blacklist and a Whitelist. The Port Authentication Utility's interface allows administrators to add, remove, or edit filtering rule entries to the Blacklist or Whitelist.



a. Menu

   The drop-down menu provides options to create new blacklist or whitelist filter, save an edited filter, open / import an existing filter from the source computer, or update the Secure KVM Switch filter. A password change option is also available.

b. Blacklist and Whitelist Area

   Filtering rules added to the Blacklist or Whitelist will be displayed in these areas.

c. Blacklist and Whitelist Command Area

   By clicking on the “Add” or “Delete” icons, the administrator can add new rules to, or delete selected rules from the Blacklist or Whitelist Area.

d. KVM Connection Status

   This area shows the KVM connection status.

4. Editing the Blacklist and Whitelist

   The Port Authentication Utility enables authorized administrators to edit the filtering rules to block (Blacklist) or to allow (Whitelist) specific USB devices connected to the USB CAC Port on the Secure KVM Switch.

   A filtering rule is defined by USB (Base) Class ID, Sub-Class, Protocol, VID (device Vendor ID), and PID (device Product ID) of a USB device. For example, a Base Class ID of a Smart Card device is 0Bh.

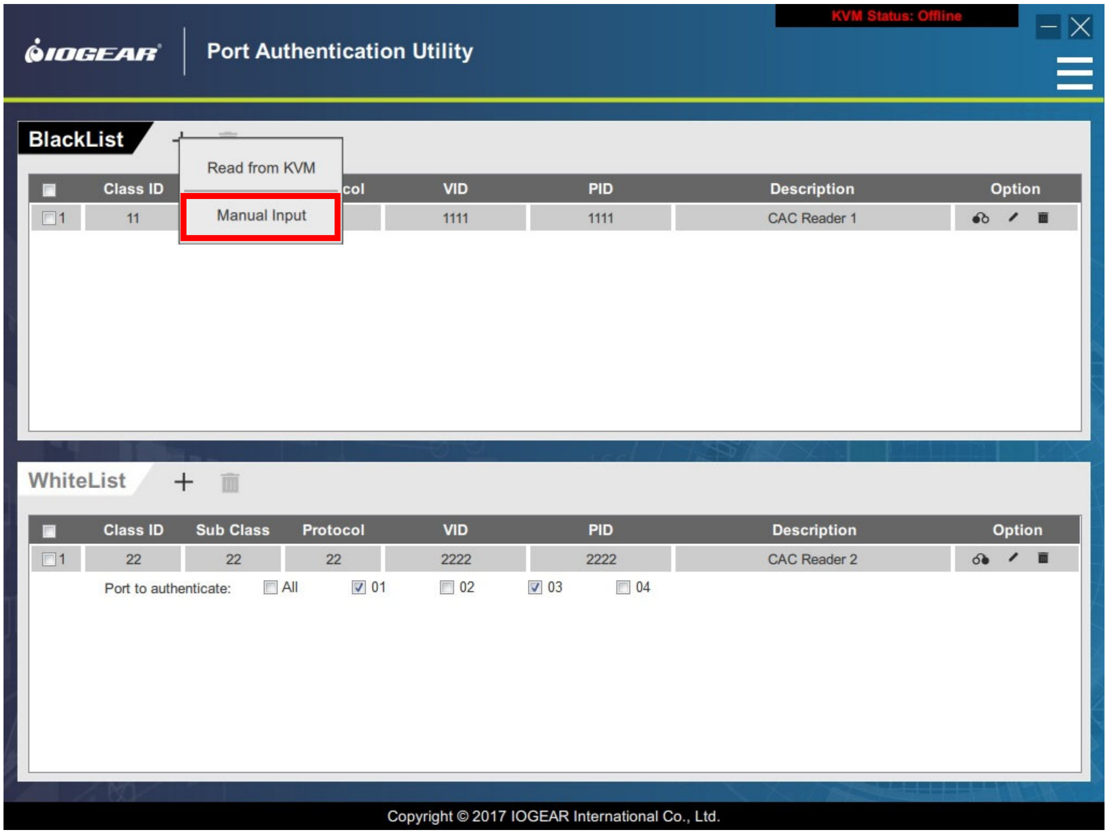
Base Class	Sub-Class	Protocol	Device
0Bh	xxh	xxh	Smart Card device

By completing the Class ID, Sub-Class, Protocol, VID and PID field of a filtering rule, the administrator can assign this filtering rule to the Blacklist or the Whitelist to block or allow a USB device.

When adding the value to Class, Sub-Class, Protocol, PID or VID field, the last digit “h” can be ignored. For example, when adding “0Bh” to the Class ID field, just type “0B”.

a. Manually adding a filtering rule to the Blacklist / Whitelist

   To add a new filtering rule to the Blacklist, click on the “+” icon in the Blacklist command area, and choose “Manual Input” from the menu to edit a filtering rule.



BlackList

□	Class ID	col	VID	PID	Description	Option
□ 1	11		1111	1111	CAC Reader 1	

WhiteList

□	Class ID	Sub Class	Protocol	VID	PID	Description	Option
□ 1	22	22	22	2222	2222	CAC Reader 2	

Port to authenticate: □ All ☑ 01 □ 02 ☑ 03 □ 04

Copyright © 2017 IOGEAR International Co., Ltd.

Manually type the value for the Class ID, Sub Class, Protocol, VID, and PID fields. For the PID value, 4 digits are required. A wildcard character asterisk "*" can be used in the field to represent one or more other characters.

For example, the PID filtering rule (5***) below would include all the devices whose PID starts with a 5.

Class ID	Sub Class	Protocol	VID	PID
0B	11	22	1234	**5*** **

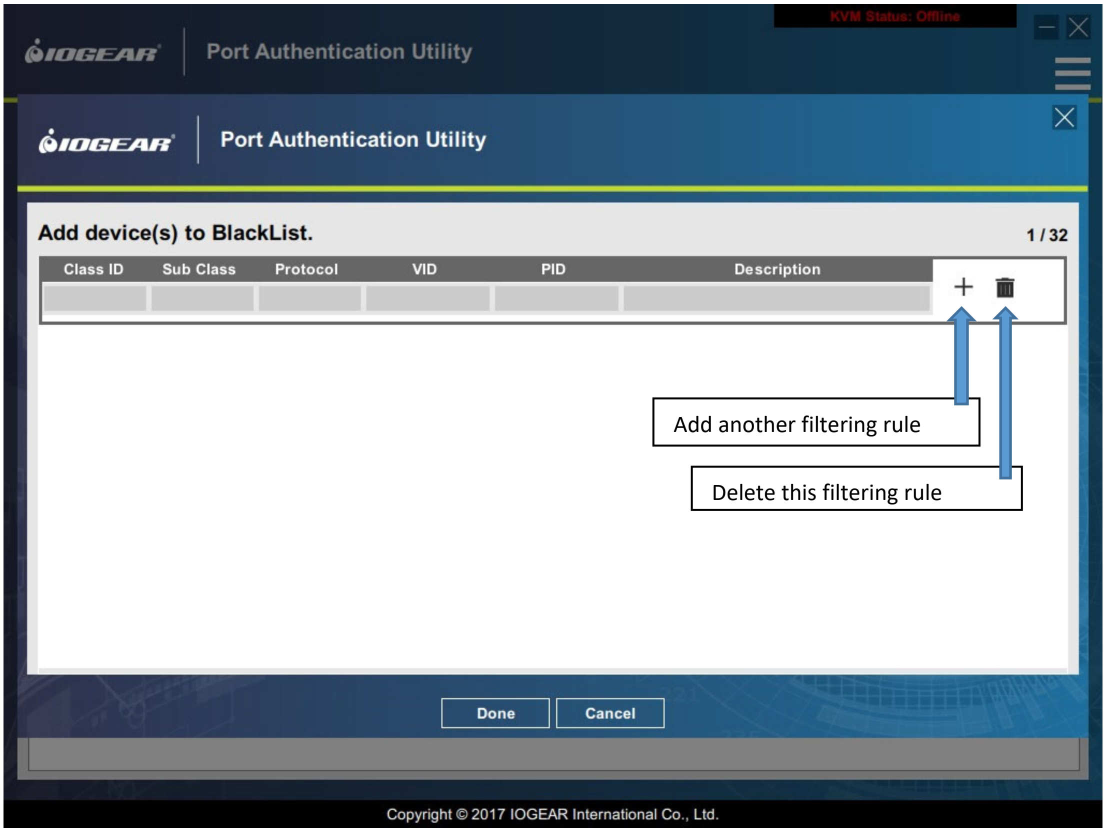
The filtering rule below includes all the devices whose PID starts with 5 and ends with 1

Class ID	Sub Class	Protocol	VID	PID
0B	11	22	1234	**5**1**

A short description can be added to Description field to describe the device.

After finishing a filter rule entry, click the "+" icon on the right to add another filter rule. Click on the recycle bin icon to discard an entry.

Click "Done" button after editing all the entries. The added filtering rules will be added to Blacklist area.



Add device(s) to BlackList.

1 / 32

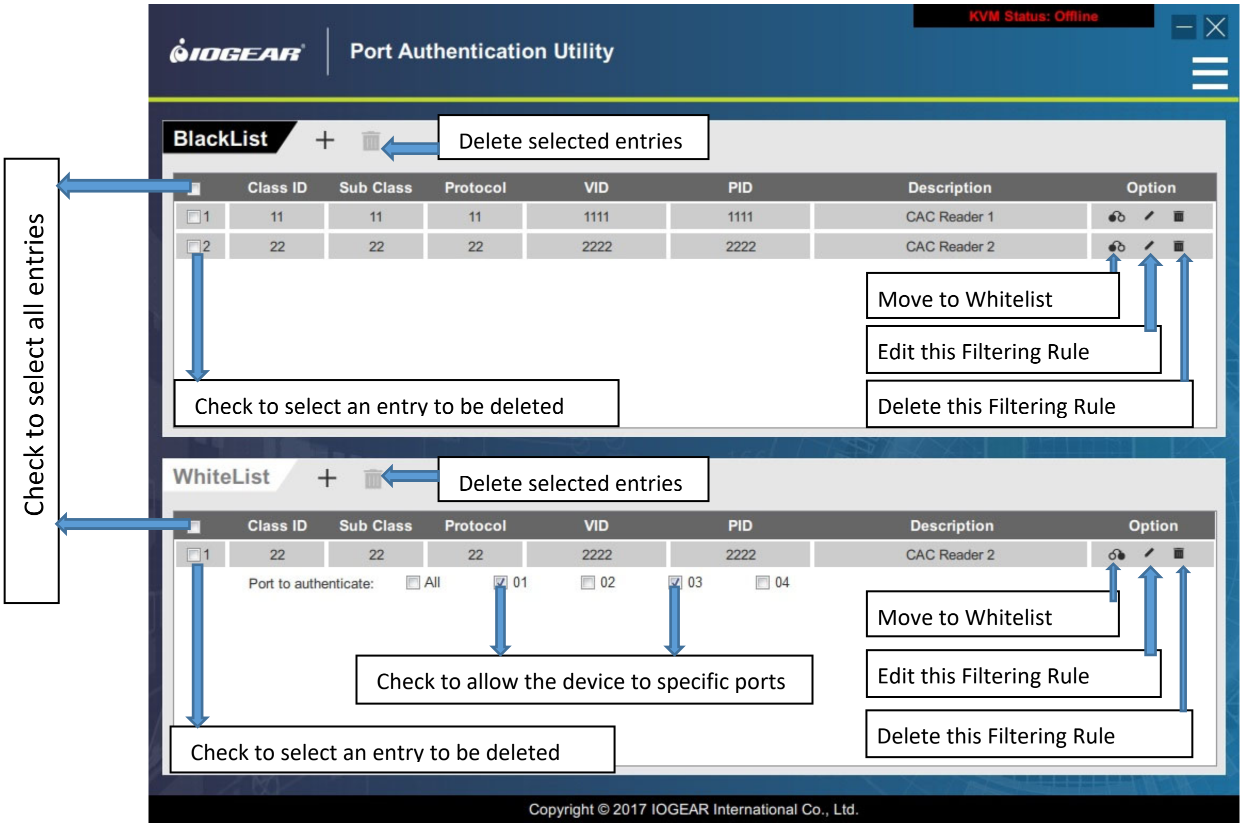
Class ID	Sub Class	Protocol	VID	PID	Description

Add another filtering rule

Delete this filtering rule

Copyright © 2017 IOGEAR International Co., Ltd.

Filtering rules added and listed in the Blacklist area can be edited, deleted, or moved to the Whitelist.



Delete selected entries

Check to select all entries

□	Class ID	Sub Class	Protocol	VID	PID	Description	Option
□ 1	11	11	11	1111	1111	CAC Reader 1	
□ 2	22	22	22	2222	2222	CAC Reader 2	

Move to Whitelist

Edit this Filtering Rule

Delete this Filtering Rule

Check to select an entry to be deleted

Delete selected entries

□	Class ID	Sub Class	Protocol	VID	PID	Description	Option
□ 1	22	22	22	2222	2222	CAC Reader 2	

Port to authenticate: □ All ☑ 01 □ 02 ☑ 03 □ 04

Check to allow the device to specific ports

Move to Whitelist

Edit this Filtering Rule

Delete this Filtering Rule

Check to select an entry to be deleted

Copyright © 2017 IOGEAR International Co., Ltd.

The Administrator can use the same approach to add filtering rules to the Whitelist.

If a device is added to the Blacklist, it will be blocked from all Secure KVM Switch ports

If a device is added to the Whitelist, it can be allowed from the ports specifically assigned by the administrator.

Blacklist filtering rules always supersede the Whitelist filtering rules.

A maximum of 32 filtering rules can be added to the Blacklist, and another maximum of 32 filtering rules can be assigned to the Whitelist.

b. Retrieving the USB device value from the device on the IOGEAR Secure KVM Switch USB CAC Port

In addition to manually typing the value to each filtering rule, administrators can retrieve the USB device information from the USB device connected to the Secure KVM Switch USB CAC Port

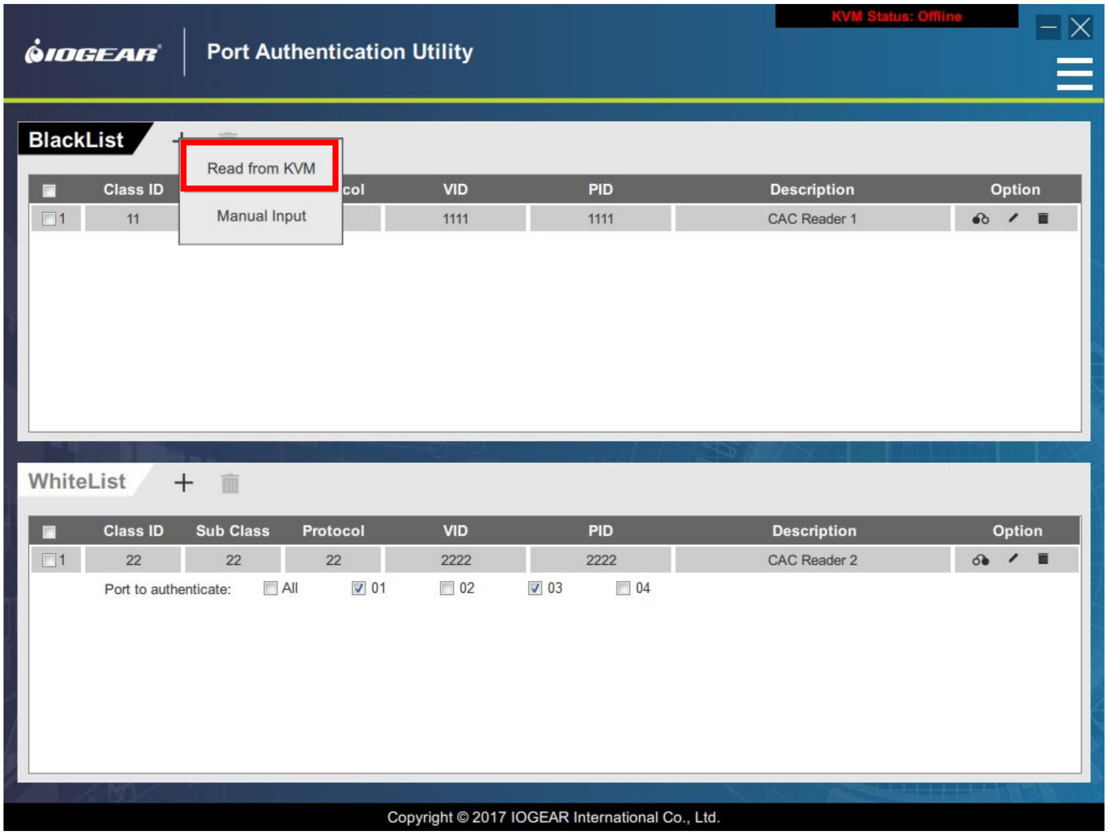
Before retrieving the USB value from the USB CAC Port device, connect the USB device to the Secure KVM Switch's USB CAC port. When the USB device has been connected to the USB CAC Port, use the Secure KVM Switch's console keyboard to:

(a) Press and hold down the **Ctrl** key
(b) Press the **F12** key: **[Ctrl+F12]**
(c) First, release the **F12** key, followed by the **Ctrl** key
(d) Press and release the **[U]** key, and then press and release **[Enter]**

Please make sure not to exceed 2 seconds between each key

The combination of key strokes enables the Secure KVM Switch to be ready for the Administrator Logon authentication and Administrator's retrieval of the device info from the USB CAC Port.

To add the values of the USB device from the USB CAC Port to filtering rules, click the "+" icon in the command area, and choose "Read from KVM"

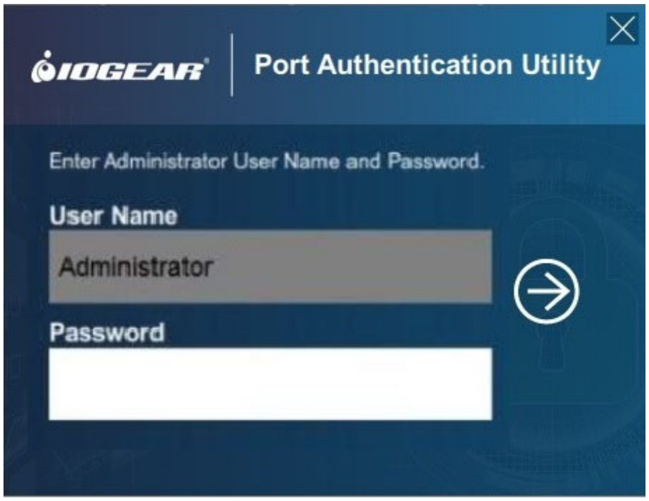


	Class ID		col	VID	PID	Description	Option
□ 1	11			1111	1111	CAC Reader 1	

	Class ID	Sub Class	Protocol	VID	PID	Description	Option
□ 1	22	22	22	2222	2222	CAC Reader 2	

Port to authenticate: □ All ☑ 01 □ 02 ☑ 03 □ 04

Administrators will be prompted to input Administrator Logon User name and password authentication



Enter Administrator User Name and Password.

User Name: Administrator

Password

ATTENTION

- The User Name and Password here refers to the ID and Password for Administrator Logon functions. Please refer to IOGEAR Secure KVM Switch **Administrator's Guide** for detail
- With 3 (three) failed attempts to logon, the Administrator Logon mode will be terminated automatically. Access to the Administrator Logon mode will blocked for 15 minutes
- With 9 (nine) failed attempts to logon, the Secure KVM Switch will become inoperable permanently. If this happens, please remove it from service immediately and contact your IOGEAR dealer.

After a successful Administrator Logon authentication, the values of USB device connected to IOGEAR Secure KVM Switch's USB CAC Port will be displayed in the filtering rule entry. The Administrator can continue to edit this entry or move on to the Blacklist or Whitelist work area.

The Administrator Logon session terminates automatically after the value of the device on the IOGEAR Secure KVM Switch USB CAC port is successfully retrieved.

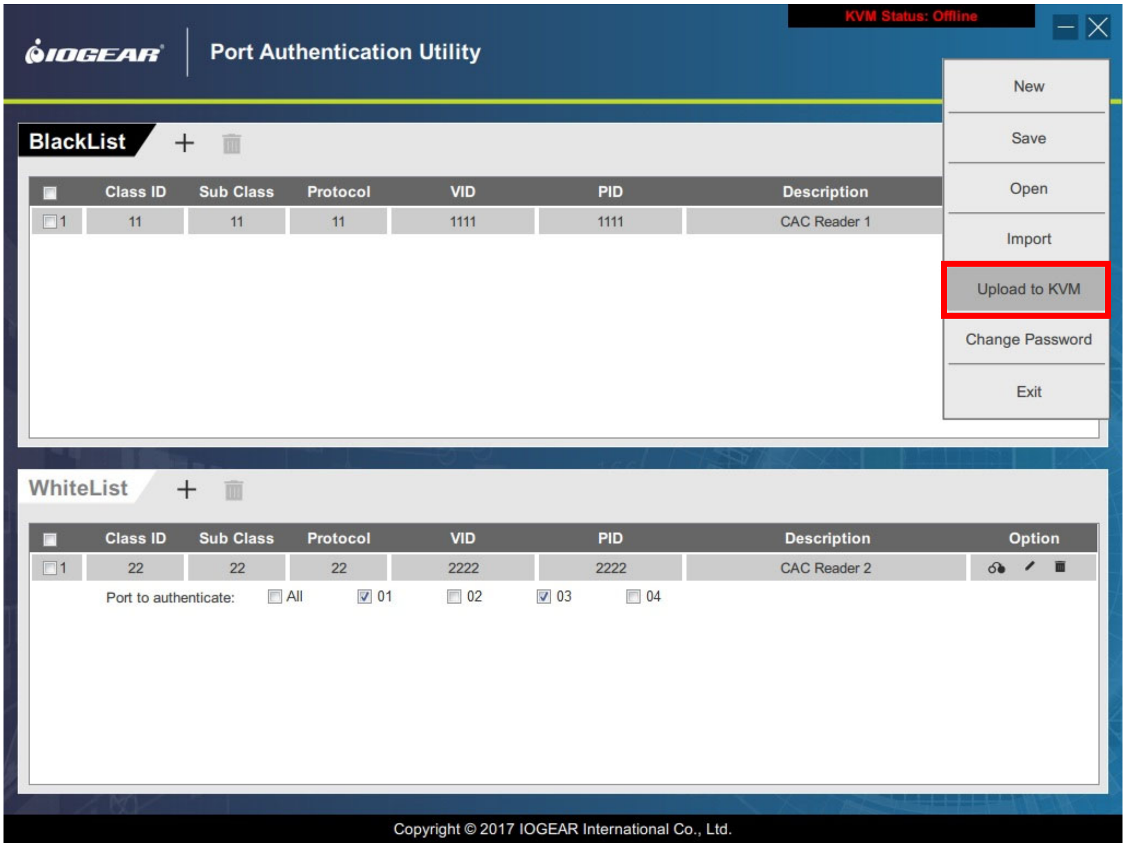
5. Upload the Filtering List

   Administrator can upload the Filtering List when finished with Filter list editing.

   a. Before uploading the Filtering list, Administrator should make the Secure KVM Switch ready for connection. Use the Secure KVM Switch's console keyboard to
      i. Press and hold down the **Ctrl** key
      ii. Press and hold down the **F12** key:
          [Ctrl+F12]
      iii. First, release the **F12** key, followed by the **Ctrl** key
      iv. Press and release the **[U]** key, then press and release **[Enter]**
          Please make sure not to exceed 2 seconds between each key

      The Secure KVM will be ready for the Filtering list upload.

   b. Choose the "Upload to KVM" option from the drop-down Menu



BlackList

☐	Class ID	Sub Class	Protocol	VID	PID	Description
☐ 1	11	11	11	1111	1111	CAC Reader 1

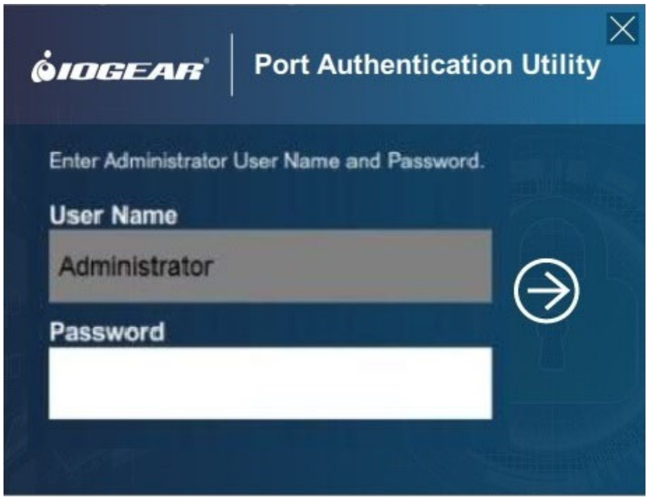
WhiteList

☐	Class ID	Sub Class	Protocol	VID	PID	Description	Option
☐ 1	22	22	22	2222	2222	CAC Reader 2	

Port to authenticate: ☐ All ☑ 01 ☐ 02 ☑ 03 ☐ 04

Copyright © 2017 IOGEAR International Co., Ltd.

After choosing “Upload to KVM” option, Administrator will be prompted to input user name and password authentication.



Enter Administrator User Name and Password.

User Name: Administrator

Password:

ATTENTION

- The User Name and Password here refers to the ID and Password for Administrator Logon functions. Please refer to IOGEAR Secure KVM Switch **Administrator’s Guide** for detail
- With 3 (three) failed attempts to logon, the Administrator Logon mode will be terminated automatically. Access to the Administrator Logon mode will blocked for 15 minutes.
- With 9 (nine) failed attempts to logon, the Secure KVM Switch will become inoperable permanently. If this happens, please remove it from service immediately and contact your IOGEAR dealer.

After a successful Administrator Logon authentication, the Filter list will upload to the Secure KVM Switch. The Secure KVM Switch will allow or block USB devices connected to the USB CAC port based on the updated Blacklist and Whitelist.

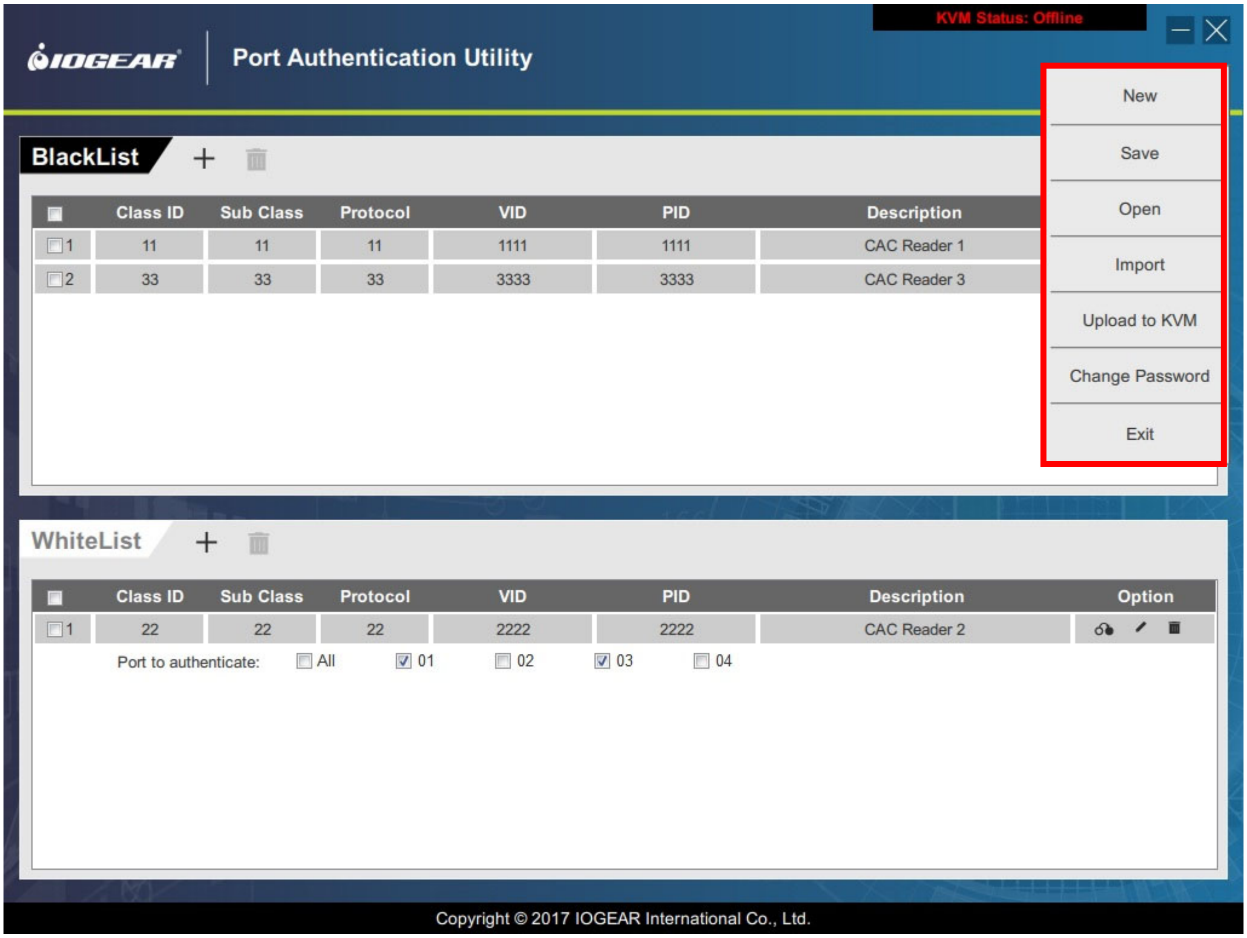
The Administrator Logon session terminates automatically after the filtering list is updated. To make the updated filtering list take effect, remove the IOGEAR Secure KVM Switch from the installation and power cycle the Secure KVM Switch.

ATTENTION

- The Blacklist and Whitelist defined by the Administrator Logon Functions always supersedes the filtering list created by the Port Authentication Utility. The administrator should make sure that there is no conflict when editing device entries.
- The updated filtering list will overwrite the one previously uploaded to the Secure KVM Switch.
- A 2-port based Filtering list can only be uploaded to 2-Port Secure KVM models. (4-Port list to 4-Port models; 8-Port list to 8-Port models). An error message shows up when uploading the wrong filtering list.
- The only way to clear the Blacklist and Whitelist updated by the Port Authentication Utility is for the administrator to perform "Reset KVM to Default" (This Reset KVM to Default also clears the Blacklist and Whitelist created by the Secure KVM administrator functions.
  Please refer to the IOGEAR **Administrator's Guide** for more details.)

6. Create, Save, Open, and Import a Filtering List

   More filtering list operations options are available from the drop-down menu



BlackList

□	Class ID	Sub Class	Protocol	VID	PID	Description
□ 1	11	11	11	1111	1111	CAC Reader 1
□ 2	33	33	33	3333	3333	CAC Reader 3

WhiteList

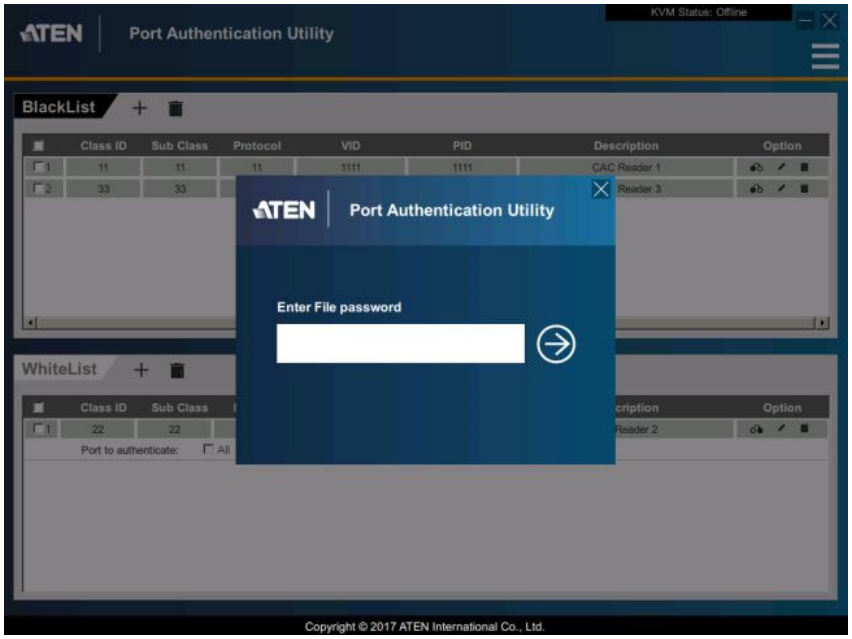
□	Class ID	Sub Class	Protocol	VID	PID	Description	Option
□ 1	22	22	22	2222	2222	CAC Reader 2	

Port to authenticate: □ All ☑ 01 □ 02 ☑ 03 □ 04

Copyright © 2017 IOGEAR International Co., Ltd.

a. New
Use this option to create a new filtering list.
When creating a new filtering list, follow the instructions in the Port Authentication Utility to choose a proper model type (2, 4, or 8-Port model) for the filtering list.

b. Save
The administrator can save a Filtering list and edit it later.
All saved Filtering list will be protected by a password. When saving a filtering list, the administrator will be prompted to assign a password to the file. The password is case-sensitive.
Do not use the same password as the Administrator Logon Functions or Port Authentication Utility.
After assigning the password, the administrator will be prompted to enter the filename, and choose a folder on the source computer to save the filtering list.



KVM Status: Offline

ATEN | Port Authentication Utility

BlackList

■	Class ID	Sub Class	Protocol	VID	PID	Description	Option
□ 1	11	11	11	1111	1111	CAC Reader 1	
□ 2	33	33				Reader 3	

ATEN | Port Authentication Utility

Enter File password

WhiteList

■	Class ID	Sub Class		cription	Option
□ 1	22	22		Reader 2	

Port to authenticate: □ All

Copyright © 2017 ATEN International Co., Ltd.

c. Open
The administrator can open a previously saved filtering list and continue with the editing. When opening a saved filtering list, the administrator will be prompted to input the password created for the file.

d. Import
The administrator can import filtering rule entries of a previously saved filtering list to a current filtering list. When importing a saved filtering list, the administrator will be prompted to input password for the file to be imported.
If the administrator is editing a 2-Port filtering list, the filtering list to be imported must also be a 2-Port based list.

7. Changing Password
The administrator can change the password for the Port Authentication utility anytime.
Choose the “Change Password” option in the drop-down menu to change the password.

The new password is case-sensitive. For maximum security, the new password should contain,

a. At least 8 characters in length, but no longer than 22 characters
b. A minimum of 1 lower case letter and,
c. A minimum of 1 upper case letter and,

d. A minimum of 1 numeric character and,

e. A minimum of 1 special character.

8. Exit the Port Authentication Utility
Choose the “Exit” option in the menu to exit Port Authentication Utility

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

IOGEAR®

www.iogear.com