HSL ADMINISTRATOR GUIDE

Products covered by this guide:
HSL Secure Products

HighSecLabs
Highest Security Solutions Ltd.

HDC19968 Rev. C

TABLE OF CONTENTS

INTRODUCTION

This Administrator Guide provides all the details you'll need to receive log and audit data from your new product.

Important security note:
If you are aware of a potential security vulnerability while installing or operating this product, please contact Technical Support immediately in one of the following ways:
a) Web form: http://www.highseclabs.com/support/case/
b) Email: security@highseclabs.com
c) Tel: +972-4-9591191 or +972-4-9591192

INTENDED AUDIENCE

This document is intended for the following professionals:

- System Administrators/IT Managers

SAFETY PRECAUTIONS

Please read the following safety precautions carefully before using the product:

- Before cleaning, disconnect from the electrical power supply.
- Do not expose to excessive humidity or moisture.
- Do not store or use for an extensive period of time in extreme thermal conditions; it may shorten the product's lifetime.
- Install only on a clean and secure surface.
- If not used for a long period of time, disconnect it from electrical power.
- If any of the following situations occurs, have the product checked by a qualified service technician:
  - Liquid penetrates its case.
  - It is exposed to excessive moisture, water or any other liquid.
  - It is not working well even after carefully following the instructions in this Administrator Guide.
  - It has been dropped or is physically damaged.
  - The product shows obvious signs of breakage or loose internal parts.
  - If using an external power supply - if the power supply overheats, is broken or damaged, or has a damaged cable.
- It should be stored and used only in temperature and humidity-controlled environments, as defined in the product's environmental specifications.
- Never attempt to open the product enclosure. Any attempt to open the enclosure permanently damages the product.
- It contains a non-replaceable internal battery. Never attempt to replace the battery or open the enclosure.

Important: This product is equipped with an always-on active anti-tampering system. Any attempt to open the product enclosure activates the anti-tamper triggers and renders the unit inoperable and the warranty void.

SAFETY PRECAUTIONS (FRENCH)

Veuillez lire attentivement les précautions de sécurité suivantes avant d'utiliser le produit:

- Avant nettoyage, débranchez l'appareil de l'alimentation DC / AC.
- Assurez-vous de ne pas exposer l'appareil à une humidité excessive.
- Assurez-vous d'installer l'appareil sur une surface sécurisée propre.
- Ne placez pas le cordon d'alimentation DC en travers d'un passage.
- Si l'appareil n'est pas utilisé de longtemps, retirez l'alimentation murale de la prise électrique.
- L'appareil devra être rangé uniquement dans des environnements à humidité et température contrôlées comme défini dans les caractéristiques environnementales du produit.
- L'alimentation murale utilisée avec cet appareil devra être du modèle fourni par le fabricant ou un équivalent certifié fourni par le fabricant ou fournisseur de service autorisé.
- Si une des situations suivantes survenait, faites vérifier l'appareil par un technicien de maintenance qualifié:
  - En cas d'alimentation externe - L'alimentation de l'appareil surchauffe, est endommagée, cassée ou dégage de la fumée
  - ou provoque des court circuits de la prise du secteur.
  - Un liquide a pénétré dans le boîtier de l'appareil.
  - L'appareil est exposé à de l'humidité excessive ou à l'eau.
  - L'appareil ne fonctionne pas correctement même après avoir suivi attentivement les instructions contenues dans ce guide de l'utilisateur.
  - L'appareil est tombé ou est physiquement endommagé.
  - L'appareil présente des signes évidents de pièce interne cassée ou desserrée
  - L'appareil contient une batterie interne. La batterie n'est pas remplaçable. N'essayez jamais de remplacer la batterie car toute tentative d'ouvrir le boîtier de l'appareil entraînerait des dommages permanents à l'appareil.

Importante: Ce produit est équipé d'toujours-sur le système anti-sabotage active. Toute tentative d'ouvrir le boîtier du produit va activer le déclencheur anti-sabotage et de rendre l'unité vide inutilisable et garantie.

Warnings and Precautions

Please read the following User Guidance Precautions carefully before using the product:

1. As the product powers-up, it performs a self-test procedure. In case of self-test failure, for any reason, including jammed buttons, the product is inoperable. Self-test failure is indicated by the following abnormal LED behavior:
   - All channel-select LEDs are turned ON and then OFF;
   - A specific, predefined LED combination is turned ON;
   - The predefined LED combination indicates the problem type (jammed buttons, firmware integrity).

   Try to power-cycle the product. If the problem persists, contact your system administrator or technical support.
2. Product power-up and RFD behavior:
   a. By default, after product power-up, the active channel is computer #1, indicated by the lit applicable front panel push button LED.
   b. To reset the device to factory defaults, please use **Left Ctrl | Left Ctrl | f11 | r**.
   c. RFD action is indicated by all the front panel LEDs blinking together.
   d. When the product boots after RFD, the keyboard and mouse are mapped to the active channel #1 and default settings are restored, erasing all user-set definitions.
3. The appropriate usage of peripherals (e.g. keyboard, mouse, display, authentication device) is described in detail in this Administrator Guide's appropriate sections. Do not connect any authentication device with an external power source to product.
4. In any event do not connect a wireless keyboard/mouse.
5. For security reasons, if products do not support microphone/line-in audio input, in any event do not connect a microphone to the product audio output port, including headsets.
6. The product is equipped with an always-on active anti-tampering system. Any attempt to open the product enclosure activates the anti-tamper system, indicated by all channel-select LEDs flashing continuously. In this case, the product is inoperable and the warranty is void. If the product enclosure appears disrupted or if all channel-select LEDs flash continuously, remove it from service immediately and contact technical support.

Important:
For change-management tracking, it is advised to perform a quarterly log check to verify that RFD was not improperly used to override the current device policy by an unauthorized person.

7. If a connected device is rejected in the console port group, you will have the following visual indications, when connecting a non-qualified:
   a. Keyboard: the keyboard is non-functional with no visible keyboard strokes on screen when using the keyboard.
   b. Mouse: the mouse is non-functional with the mouse cursor frozen on the screen.
   c. Display: the video diagnostic LED flashes once in green and then turns off. The video does not work.
   d. USB device: The fUSB LED flashes green once and then turns off. The USB device is inoperable.
8. Do not connect product to computing devices that:
   a. Are TEMPEST computers;
   b. Include telecommunication equipment;
   c. Include frame grabber video cards;
   d. Include special audio processing cards.
9. The product has a remote-control port in the back panel labeled RCU. Do not use this port; it is inoperable and for future use.
10. Important! Before re-allocating computers to channels, it is mandatory to power-cycle the product, keeping it powered OFF for more than one minute.
11. The product log access and administrator configuration options are described in this guide.
12. The authentication session is terminated once the product power is down or you intentionally terminates the session.
13. If you are aware of any potential security vulnerability while installing or operating product, remove it from service immediately and contact us in one of the ways listed in this guide.

Important:

1. If the unit's enclosure appears disrupted, OR if the tamper-evident labels protecting the unit seem to be handled with, OR if all channel-select LEDs flash continuously, remove the product from service immediately and contact HSL Technical Support at http://highseclabs.com/support/case/
2. Do not connect product to computing devices that:
   a) Are TEMPEST computers;
   b) Include telecommunication equipment;
   c) Include frame grabber video cards;
   d) Include special audio processing cards.

Warnings and Precautions

The product enables authorized administrators to download event log files and audit the product history as well as have access to advanced settings.
This function is available only to authenticated administrators.

Note: The log data may not be erased and log functions may not be disabled by users or administrators.
RFD does not reset the administrator's password and username, but deletes the additional users that the admin has created.

Important note before deploying the product:
To comply with the product's Common Criteria evaluation and to prevent unauthorized administrative access to the product, the default administrator user name and password must be changed prior to first use.

CAUTION:
The KVM device must be installed in an environment that provides physical security appropriate for the data being processed on the attached computing devices.

Note:
Appropriately trained and trusted administrators and users must be available to administer, configure, and use the device.

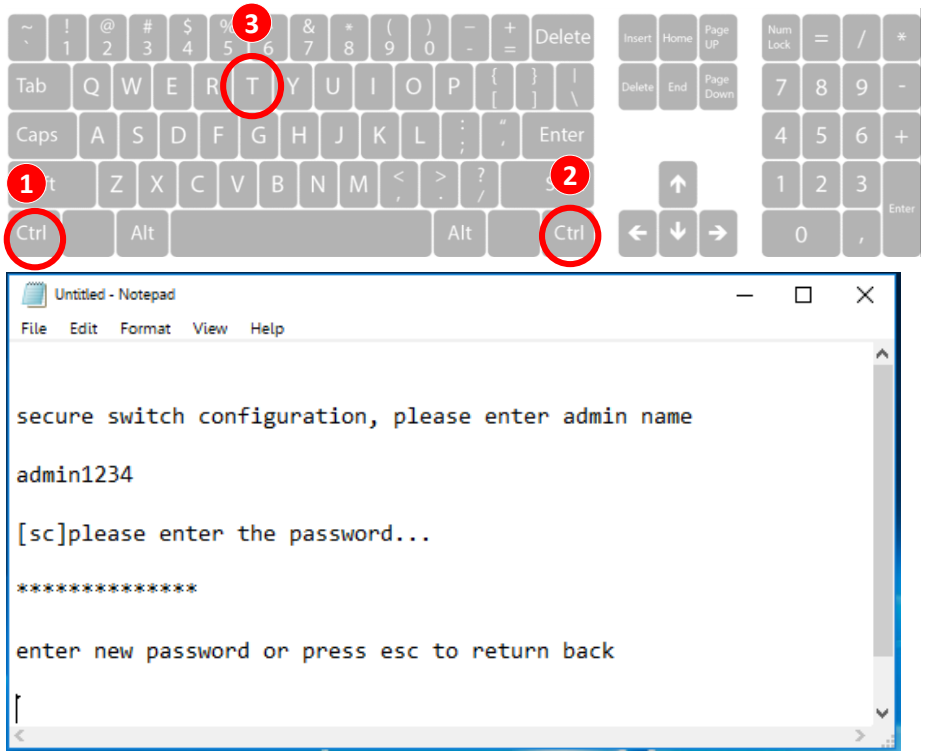
ADMINISTRATOR CONFIGURATION

Administrator Setup

a) To get to "Terminal\Admin Mode", connect the product and power up as defined by the UM.
b) Select channel #1 on the product and open Notepad on the computer that is connected to channel #1.
c) On the keyboard, hit the following key combination: **Left Ctrl | Right Ctrl | t** (press keys sequentially)
d) Text appears on the screen, asking for a user name.
e) The default user name is: "**admin1234**"
f) The default first device logon password is: "**1234ABCDefg!@#**"
g) At first logon, the administrator must set a new, non-default, password. The new password must be 8 to 15 characters long and must contain:
   i. Uppercase letters
   ii. Lowercase letters
   iii. Digits "0-9"
   iv. Any of the special characters: "!@#$%^&*()-_"
h) Password must be typed twice to confirm.
i) Password may be changed at any time.
j) RFD does not reset the main admin user name and password!
k) If the password or username are forgotten – contact HSL support.
l) After three failed logon attempts the device admin console is locked. The user may cycle the device power and try again.
m) Additional administrative user accounts can be created from the terminal menu (up to nine per switch).

Administrator Logon

a) Connect keyboard, mouse, and one KM cable to the computer and power up the product. Note that display may or may not be connected through the products.
b) Open Notepad or any other text editor on the connected computer.
c) Use the keyboard and type **Left Ctrl | Right Ctrl | t** (press keys sequentially) to enter Admin Mode. Follow the instructions on the screen to logon.



Terminal Mode Options

Once authenticated, the following menu opens:

authentication succeeded. please select operation...
0 - Asset management
1 - Firmware versions
2 - Configure DPP
3 - Configure SC (System Controller)
4 - Account management
5 - Reset to factory defaults
6 - Logs and events
7 - Configure peripheral devices
8 - Exit Terminal mode
9 - Power cycle the KVM

Select any of the options, by typing the number on the keyboard.

Make sure NOT to use the keyboard's numeric pad; it does not work. Only the main keyboard numbers work.

NOTE:

- To exit the Terminal mode, type - 8 (as seen in the menu above) or power cycle the KVM switch.
- As long as the unit is in Terminal mode, keystrokes are not sent to the target computer.

Terminal Mode Options – Explained

0 - Asset Management

Change the USB parameters that the KVM switch uses to identify itself to the connected computer. The options are:

1 - Use standard descriptor as asset container
2 - Use custom descriptor as asset container
3 - Enter new asset tag
4 - Show current asset tag
5 - Apply asset tag to DE
8 - Back
10 - Exit terminal mode

1 - Firmware Versions

Check the different firmware versions that are loaded on the different controllers of the KVM switch. The firmware-version options are:

1 - DE version
2 - SC version
3 - VC version (Video Controller)
4 - DPP version
8 - Back
9 - Exit terminal mode

2 - Configure DPP

Configure and change the devices that are allowed through the DPP (dedicated peripheral port). This is the fUSB port.
By default, all authentication devices and only authentication devices are allowed. You can also use a tool that gives you more functionality. The options are:

1 - Allow currently connected device on all channels
2 - Block currently connected device on all channels
3 - Show currently connected device
4 - Show currently approved device
5 - Show currently blocked device
6 - Reset DPP settings
7 - Upload DPP settings from the host
8 - Back
9 - Exit terminal mode

3 - Configure SC

Configure and change the SC (system controller) settings.
The options are:

1 - Enter desktop configuration [0-40] [default=0]
2 - Enter mouse speed [0-32] [default=5]
3 - Upload configuration from the host
4 - Use ctrl key as shortcut prefix
5 - Use alt key as shortcut prefix
6 - Guard mode configuration
7 – RGB FP configuration
8 - Back
9 - Exit terminal mode

Option 7 – RGB Front Panel Configuration. On choosing this option a new menu will appear with the following options:

1 – Upload FP configuration from a host
2 – Select colors for channels
8 - Back
9 - Exit terminal mode

On choosing option 1 - the user can upload an external file with RGB configuration.

Option 2 opens a dialog where user will enter his choices as follows:

1. *Select a channel [1..4] (*or 1-8 in 8 Port units) or press esc to go back*
2. *Select a color . Please select operation:*
   1.Blue
   2.Red
   3.Green
   4.Yellow
   5.Purple
   8.Back
   9.Exit terminal mode

4 - Account Management

Manage, add, and remove administrator accounts.
The options are:
1 - Change password
2 - Create admin account
3 - Delete all accounts
8 - Back
9 - Exit terminal mode

Up to nine additional administrator accounts may be created. The additional accounts can be removed or renamed by the admin and will be deleted during RFD.

Additional administrators' usernames must be 5 to 11 characters long, and must contain: Uppercase letters & Lowercase letters.

5 - Reset to Factory Defaults

Resets the device to factory default.

NOTE: Although this is a complete reset, it does not reset the main Admin username and password and the logs.

6 - Logs and Events

The options are:
1 - Show OTP log
2 - Show Critical Ram LOG
3 - Show Non-Critical RAM log
8 - Back
9 - Exit terminal

Under logs and events, all information defined as critical and sensitive is saved. There are two types of logs on the KVM switches:

- **The critical RAM log:**

Its information is never deleted, not even during the RFD. This log keeps date, time and username of all the events that defined as critical, such as: self-test failures, peripheral device rejection, tampering event, DPP configuration changes, RFD, admin password change. Stores up to 64 events in a cyclic way (overwrites the new events instead of the oldest ones).
These events are never deleted from the log.

- **The Non-Critical RAM log:**

Its information is never deleted, not even during the RFD. The events kept on this log are events like power up, peripheral device acceptance, simple configuration change, Admin logon, user add/delete, password change or password lock, and so on. The RAM log stores up to 128 latest events, and deletes the oldest ones when it is full.

- **The OTP log**

Stores critical events in parallel with the critical-RAM log, up to 64 events. Its information is never deleted and it is not renewable. All critical events starting 65 will enter the critical RAM log.

7 – Configure Peripheral Devices

Manage the peripheral devices options:

1 -Toggle Touch support
2 -Toggle consumer control support
3 - Configure absolute mouse support
4 - Toggle copy/paste support
5 - Toggle video follow mouse
8 - Back
9 - Exit terminal

Any of the above changes might require up to 10 sec. to be applied on the device.

External Configuration Tool

You have the option of using an external configuration tool. It lets you configure:

- DPP
- Presets

COPYRIGHT AND LEGAL NOTICE

This product and/or associated software are protected by copyright, international treaties and various patents.
This manual and the software, firmware and/or hardware described in it are copyrighted. You may not reproduce, transmit, transcribe, store in a retrieval system, or translate into any language or computer language,
in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, any part of this publication without express written permission from HSL.
HSL SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN; NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS MATERIAL.
The information contained in this document represents the current view of HSL on the issues discussed as of the date of publication. Because HSL must respond to changing market conditions, it should not be interpreted to be a commitment on the part of HSL, and HSL cannot guarantee the accuracy of any information presented after the date of publication.
PRODUCT DESIGN AND SPECIFICATION IS SUBJECT TO CHANGES WITHOUT NOTICE
This Guide is for informational purposes only. HSL MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

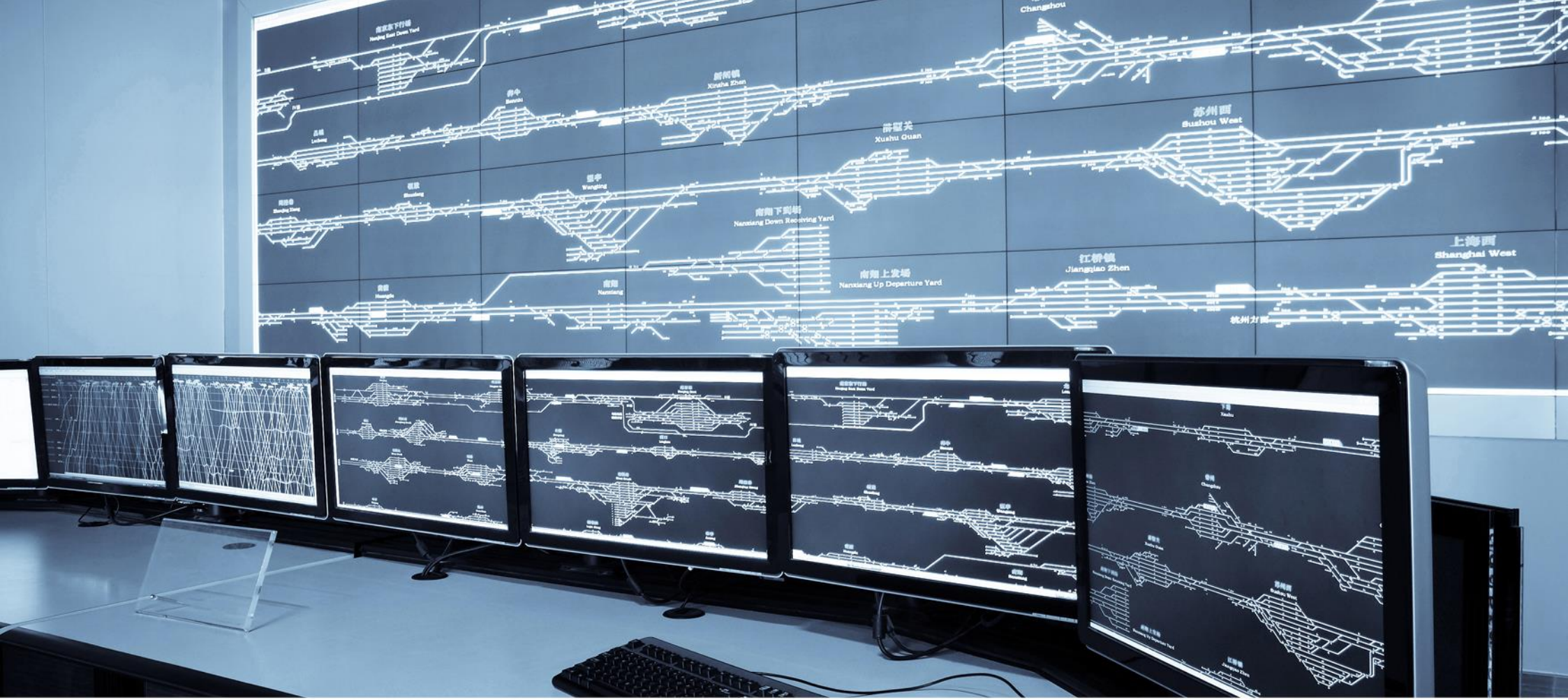
PATENTS AND TRADEMARKS

The products described in this manual are protected by multiple patents.
HSL Product/s and logo are either trademarks or registered trademarks of HSL.
Products mentioned in this document may be registered trademarks or trademarks of their respective owners.

U.S. GOVERNMENT RESTRICTED RIGHTS

The Software and documentation are provided with RESTRICTED RIGHTS.
You agree to comply with all applicable international and national laws that apply to the Software, including the U.S. Export Administration Regulations, as well as end-user, end-use and country destination restrictions issued by U.S. and other governments.

The information and specifications in this document are subject to change without prior notice.
Images are for demonstration purposes only.



HighSecLabs
Highest Security Solutions Ltd.

THANK YOU

For more information, please visit www.highseclabs.com