SEKURYX

Sekuryx Secure KVM Administration and Security Management Tool Guide (Non-CAC)

DESIGNED AND MADE IN USA

Release Date: April 6th, 2021

Version: 1.0

Prepared By: Steve Barash

Prepared For: Sekuryx

Table of Contents

Table of Figures

List of Tables

1. OVERVIEW

The Administration and Security Management Tool was designed by Sekuryx to allow identified and authenticated users and system administrators to perform the following management activities on Sekuryx Secure KVM switch devices:

Menu Function	Administrator
Log-in	✓
Change Admin Access Credentials	✓
Auditing - Dump Log	✓
Restore Factory Default (reset)	✓
Terminate Session	✓

Table 1: Administrator Function Permissions

This guide outlines the required information to operate each function in the above table.

2. Intended Audience

The information in this document is for authorized system administrators or users. If the product does not behave in the manner specified by this document, please contact Sekuryx technical support at info@sekuryx.com.

3. SYSTEM REQUIREMENTS

- The Sekuryx Secure KVM switch is compatible with standard personal/portable computers, servers or thin-clients, running operating systems such as Windows or Linux.
  The Administration and Security Management Tool can only run on Windows. The supported versions are Windows XP, 7, 8, and 10. Version 2.0 or later of the .NET framework is also required.
- The peripheral devices that supported by the KVM TOE are listed in the following table:

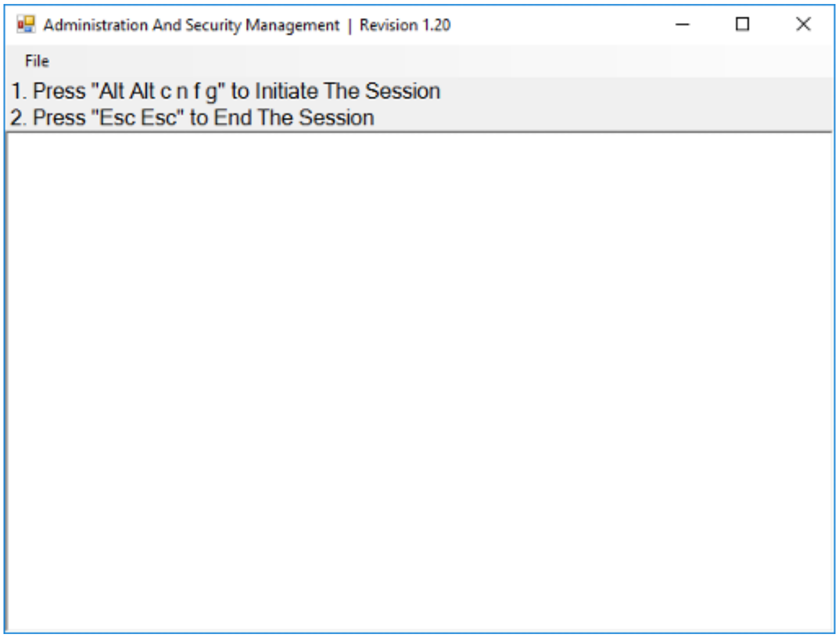
Console Port	Authorized Devices
Keyboard	Wired keyboard and keypad without internal USB hub or composite device functions, unless the connected device has at least one endpoint which is a keyboard or mouse HID class
Display	Display device (e.g., monitor, projector) that uses an interface that is physically and logically compatible with the TOE ports (DVI-I, HDMI, or DisplayPort, depending on model)
Audio out	Analog amplified speakers, Analog headphones
Mouse / Pointing Device	Any wired mouse or trackball without internal USB hub or composite device functions

Table 2: Peripheral Devices supported by the KVM TOE

4. System Setup

Note: Only one computer connected to the KVM port 1 is required for any activity in this guide.

- Ensure that device power is turned off or disconnected from the unit and the computer.
- Using USB cable Type-A to Type-B connect the PC to the device host K/M port 1.
- Connect a USB keyboard and mouse in the two USB console ports.
- Connect the appropriate video cable between the PC and the KVM video 1 port.
- Connect the monitor to the KVM console video output connector.
- Power up the PC and the device.
- Download the Administration and Security Management Tool from the following link to the PC - https://www.sekuryx.com/documentation/NIAP4
- Run the Administration and Security Management Tool executable file. Figure 1 below is a screenshot of the tool you should be seeing on your screen.

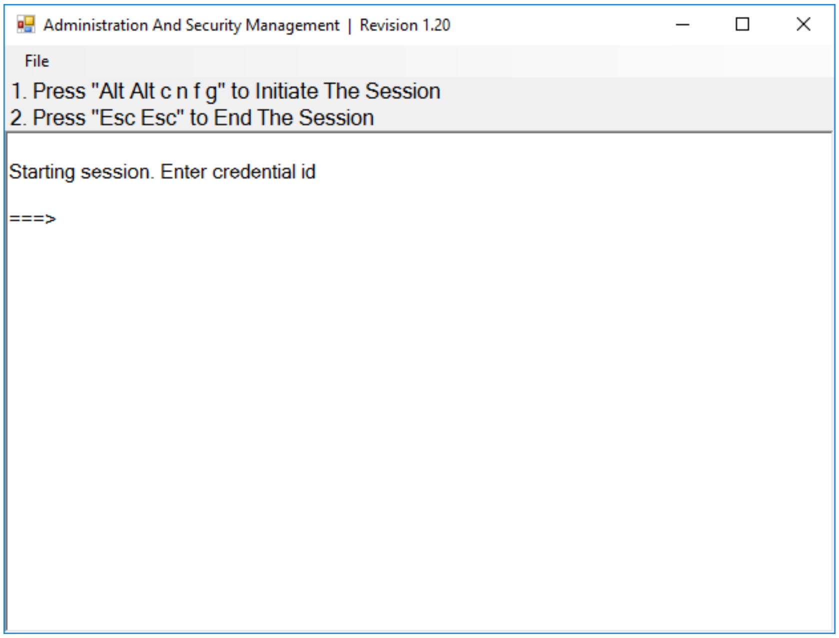


1. Press "Alt Alt c n f g" to Initiate The Session
2. Press "Esc Esc" to End The Session

Figure 1: Administration and Security Management Tool

5. Initiate Session

- Using the keyboard, press "Alt Alt cnfg"
- At this stage the mouse connected to the device will stop functioning.
- Figure 2 below is a screenshot of the tool you should be seeing on your screen.



1. Press "Alt Alt c n f g" to Initiate The Session
2. Press "Esc Esc" to End The Session

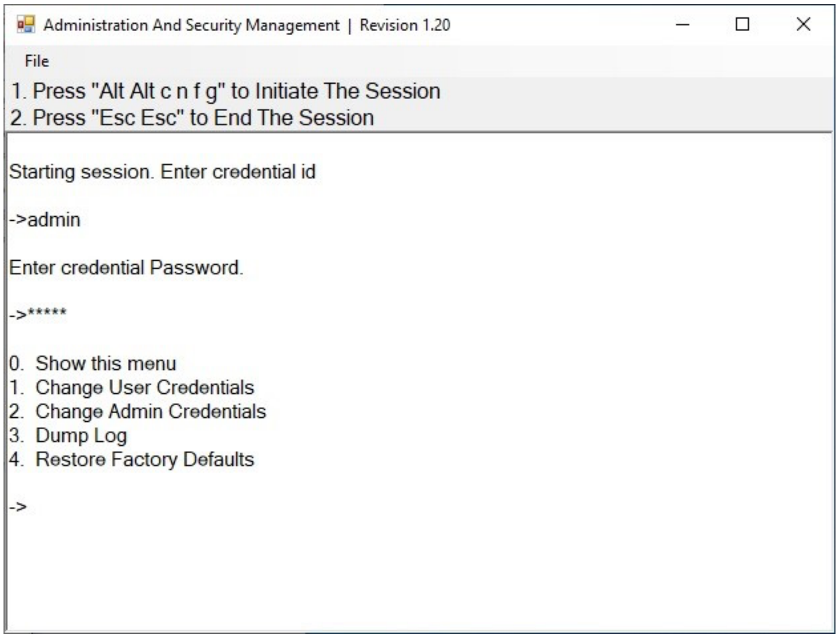
```
Starting session. Enter credential id

===>
```

Figure 2: Initiate Session Capture

7 Administrator Functions

7.1 Administrator – Log-in

- Enter the default username “admin” and press Enter.
- Enter the default password “12345” and press Enter.
- Figure 3 below is a screenshot of the tool you should be seeing on your screen.

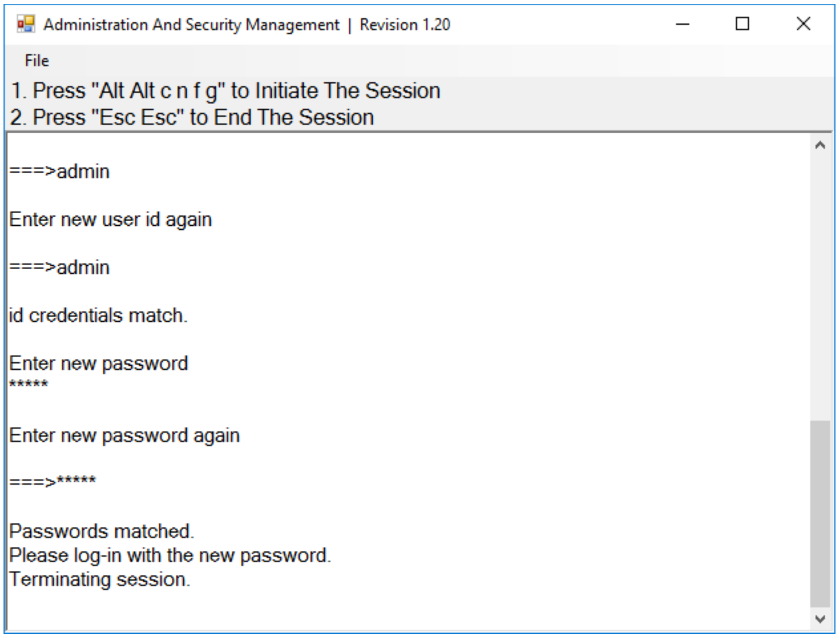


```
1. Press "Alt Alt c n f g" to Initiate The Session
2. Press "Esc Esc" to End The Session

Starting session. Enter credential id

->admin

Enter credential Password.

->*****

0.  Show this menu
1.  Change User Credentials
2.  Change Admin Credentials
3.  Dump Log
4.  Restore Factory Defaults

->
```

Figure 3: Administrator Log-in

7.2 Administrator – Change Administrator Credentials

- Select option 2 from the menu on your screen and press Enter.
- Enter the new Administrator ID and press Enter.
- Enter the new Administrator ID again and press Enter.
- Enter the new Administrator password and press Enter.
- Enter the new Administrator again and press Enter.
- Figure 4 below is a screenshot of the tool you should be seeing on your screen.



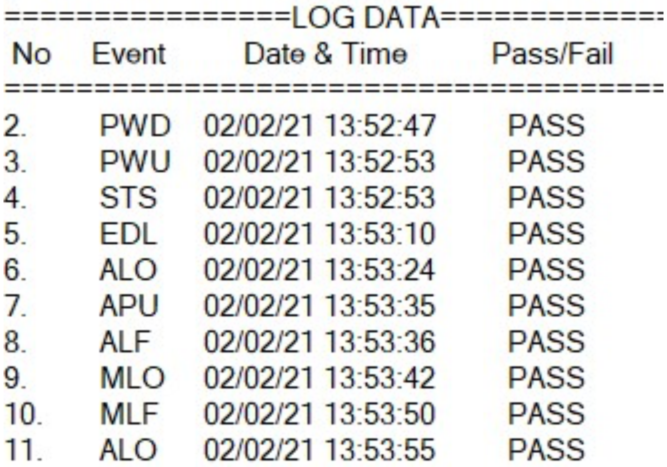
```
1. Press "Alt Alt c n f g" to Initiate The Session
2. Press "Esc Esc" to End The Session

===>admin

Enter new user id again

===>admin

id credentials match.

Enter new password
*****

Enter new password again

===>*****

Passwords matched.
Please log-in with the new password.
Terminating session.
```

Figure 4: Admin Change Admin Credentials

7.3 Administrator – Event Log (auditing)

Event Log is a detailed report of critical activities stored in the device memory. The internal clock of the KVM is used to print out timestamps for each event in the log. The internal battery of the KVM ensures the clock is always active and allows for accurate time recordings for all events. The initial date is inputted into each KVM manually at the time of manufacturing. The following steps provide instructions for dumping the log by identified and authenticated administrator.

- Select option 3 from the menu on your screen and press Enter.
- The last 10 events will be presented in the log as shown in Figure 5 below:



```
================LOG DATA=============
 No    Event      Date & Time        Pass/Fail
=======================================
2.     PWD    02/02/21 13:52:47      PASS
3.     PWU    02/02/21 13:52:53      PASS
4.     STS    02/02/21 13:52:53      PASS
5.     EDL    02/02/21 13:53:10      PASS
6.     ALO    02/02/21 13:53:24      PASS
7.     APU    02/02/21 13:53:35      PASS
8.     ALF    02/02/21 13:53:36      PASS
9.     MLO    02/02/21 13:53:42      PASS
10.    MLF    02/02/21 13:53:50      PASS
11.    ALO    02/02/21 13:53:55      PASS
```

Figure 5: Sample Log

- Press the Enter key to see the previous 10 events. This can be repeated for up to the most recent 100 events.
- The Log header includes the following information:
  - Unit's Model
  - Unit's S/N
  - Anti-tamper switch status
  - Manufacturing Site
  - Manufacturing Date
  - Anti-tamper Arming Date
  - Number of current records in the Log

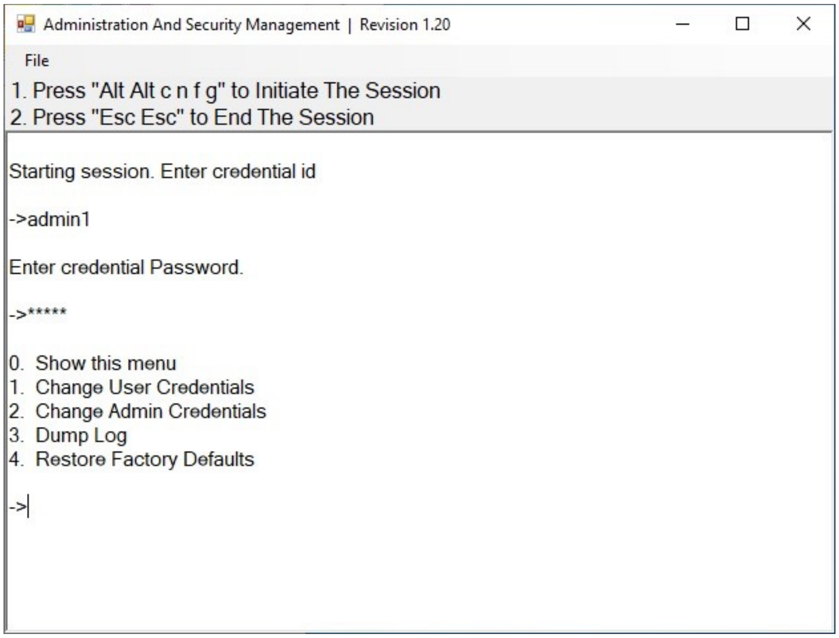
The log data may include events with any of the codes shown in Figure 6 below:

#	Code	Description
1	ALO	Administrator Log On
2	ALF	Administrator Log Off
3	ARM	Arming A/T System
4	EDL	EDID Learn
5	LGD	LOG Dump
6	PWU	Power Up
7	PWD	Power Down
8	AFD	Restore Factory Default
9	RKM	Rejected Keyboard or Mouse
10	STS	Self-Test
11	TMP	Device Tampered, Review by MFR only
12	APU	Administrator Credential Update

Figure 6: Event Codes

7.4 Administrator – Restore Factory Defaults

- Select option 4 from the menu on your screen and press enter.
- The following menu will be presented (see Figure 7 below):



1. Press "Alt Alt c n f g" to Initiate The Session
2. Press "Esc Esc" to End The Session

```
Starting session. Enter credential id

->admin1

Enter credential Password.

->*****

0.  Show this menu
1.  Change User Credentials
2.  Change Admin Credentials
3.  Dump Log
4.  Restore Factory Defaults

->
```

Figure 7: Restore Factory Defaults

The unit will perform power reset automatically. All system defaults will be restored.

7.5 Administrator – Terminate Session

Press “Esc Esc”.