

SEKURYX

Sekuryx Secure KVM Administration and Security Management Tool Guide (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 CONTENTS.....	1
1. OVERVIEW.....	4
2. INTENDED AUDIENCE	5
3. SYSTEM REQUIREMENTS.....	6
4. SYSTEM SETUP	7
5. INITIATE SESSION	8
6. USER FUNCTIONS.....	9
6.1. USER – LOG-IN	9
6.2. USER – CAC PORT CONFIGURATION	9
6.3. USER – VIEW REGISTERED CAC PERIPHERAL.....	10
6.4. USER – TERMINATE SESSION	10
7 ADMINISTRATOR FUNCTIONS.....	12
7.1 ADMINISTRATOR – LOG-IN	12
7.2 ADMINISTRATOR – CAC PORT CONFIGURATION	12
7.3 ADMINISTRATOR – VIEW REGISTERED CAC PERIPHERAL	13
7.4 ADMINISTRATOR – CHANGE USER CREDENTIALS.....	13
7.5 ADMINISTRATOR – CHANGE ADMINISTRATOR CREDENTIALS	14
7.6 ADMINISTRATOR – EVENT LOG (AUDITING)	15
7.7 ADMINISTRATOR – RESTORE FACTORY DEFAULTS	16
7.8 ADMINISTRATOR – TERMINATE SESSION	17

Table of Figures

Figure 1: Administration and Security Management Tool	7
Figure 2: Initiate Session Capture	8
Figure 3: User Log-in	9
Figure 4: User CAC Port Registration	10
Figure 5: User View Registered CAC Peripheral.....	10
Figure 6: Terminate Session	11
Figure 7: Administrator Log-in.....	12
Figure 8: Admin CAC Port Registration.....	13
Figure 9: Admin View Registered CAC Peripheral	13
Figure 10: Admin Change User Credentials	14
Figure 11: Admin Change Admin Credentials	15
Figure 12: Sample Log.....	15
Figure 13: Event Codes	16
Figure 14: Restore Factory Defaults	17

List of Tables

Table 1: User/Administrator Function Permissions	4
Table 2: Peripheral Devices supported by the KVM TOE	6

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	User	Administrator
Log-in	✓	✓
Change User Access Credentials		✓
Change Admin Access Credentials		✓
View Registered CAC Device	✓	✓
Register New CAC Device	✓	✓
Auditing - Dump Log		✓
Restore Factory Default (reset)		✓
Terminate Session	✓	✓

Table 1: User/Administrator Function Permissions

An authenticated User and authenticated Administrator are both considered types of administrators for the purposes of compliance with version 4.0 of the Protection Profile (PP) for Peripheral Sharing Switch (PSS), to which this product claims conformance.

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
User Authentication Device	USB devices identified as user authentication (base class 0Bh, e.g., Smart-card reader, PIV/CAC reader, Token, or Biometric reader)

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 second USB cable Type-A to Type-B between the PC and the KVM if CAC port configuration is also required.
- 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.

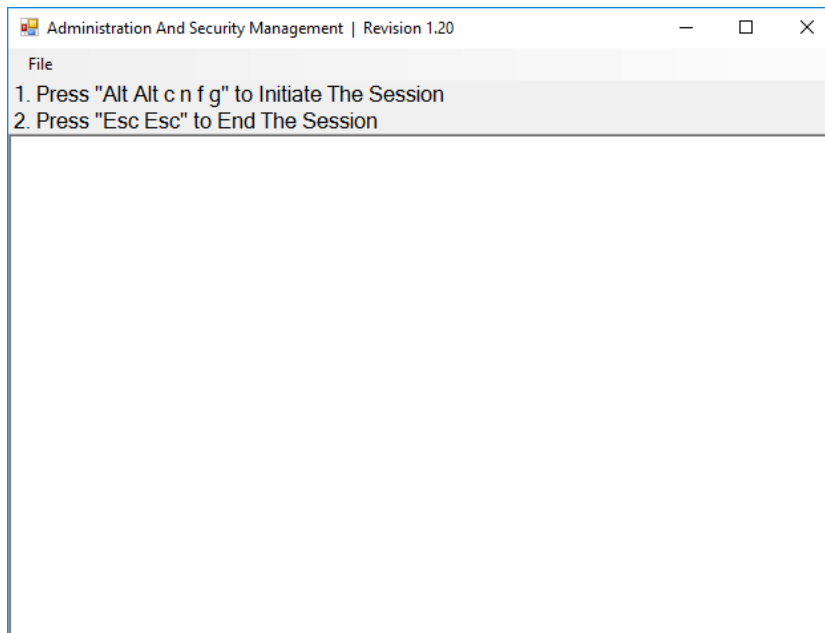


Figure 1: Administration and Security Management Tool

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.

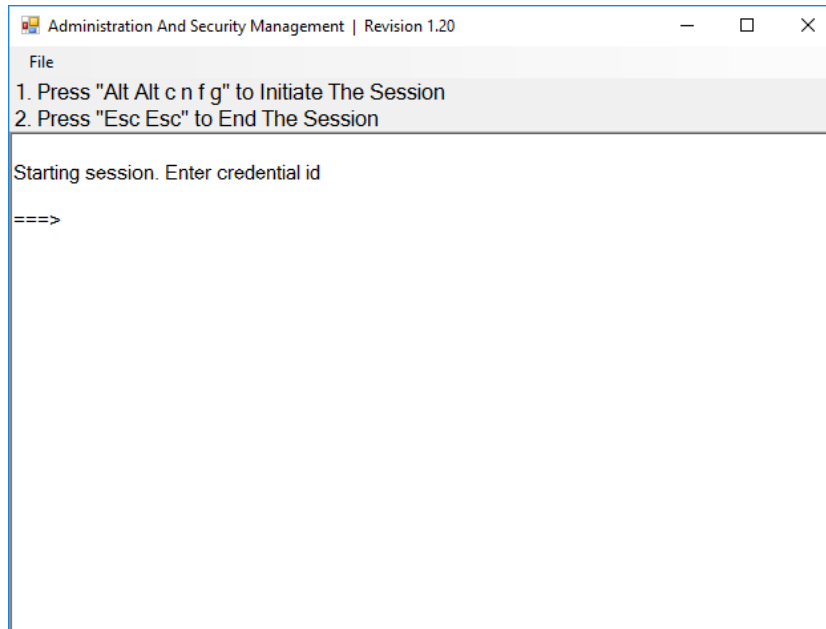


Figure 2: Initiate Session Capture

6. USER FUNCTIONS

6.1. User – Log-in

- Enter the default username “user” 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.

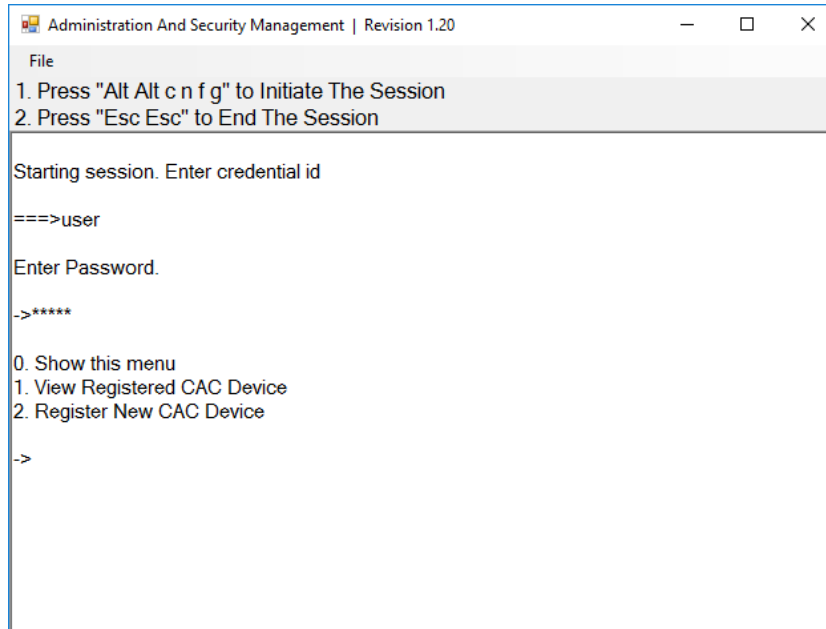


Figure 3: User Log-in

6.2. User – CAC Port Configuration

CAC (Common Access Card) port configuration is an optional feature, allowing registration of any specific USB peripheral to operate with the device. Only one peripheral can be registered at a time and only the registered peripheral will operate with the device. By default, when no peripheral is registered, the device will operate with any smart card reader or other USB authentication device. Other device types are not supported by default.

Be advised, this CAC port is intended to be used solely for specific User Authentication Devices listed in Table 2. Misusing the KVM by registering any other USB device is beyond the scope of the Protection Profile 4.0 approved by NIAP.

- Select option 2 from the menu on your screen and press Enter.
- Connect the peripheral device to be registered to the CAC USB port in the console side of the device and wait until the device is reading the new peripheral information.
- The device will list the information of the connected peripheral on the screen and buzz 3 times when registration is completed.
- Figure 4 below is a screenshot of the tool you should be seeing on your screen. A USB Smart Card Reader was registered to the CAC port in this example:

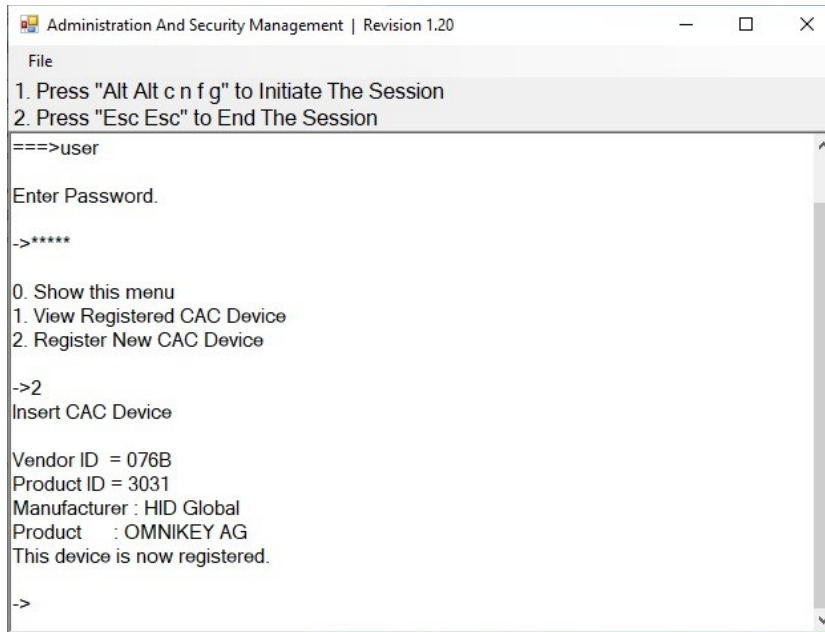


Figure 4: User CAC Port Registration

6.3. User – View Registered CAC Peripheral

- Select option 1 from the menu on your screen and press Enter.
- Figure 5 below is a screenshot of the tool you should be seeing on your screen. A USB Smart Card Reader is registered to the CAC port in this example:

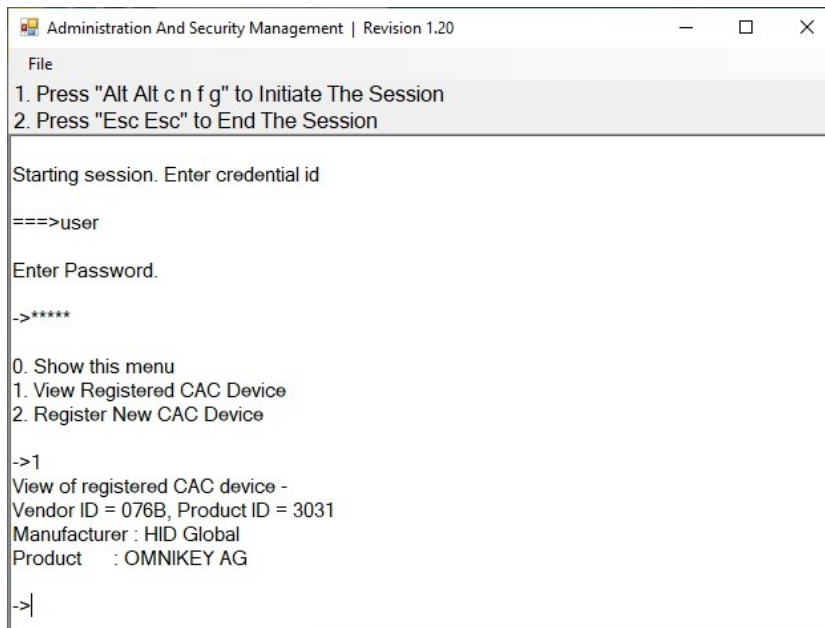


Figure 5: User View Registered CAC Peripheral

6.4. User – Terminate Session

- Press "Esc Esc".

- Figure 6 below is a screenshot of the tool you should be seeing on your screen.

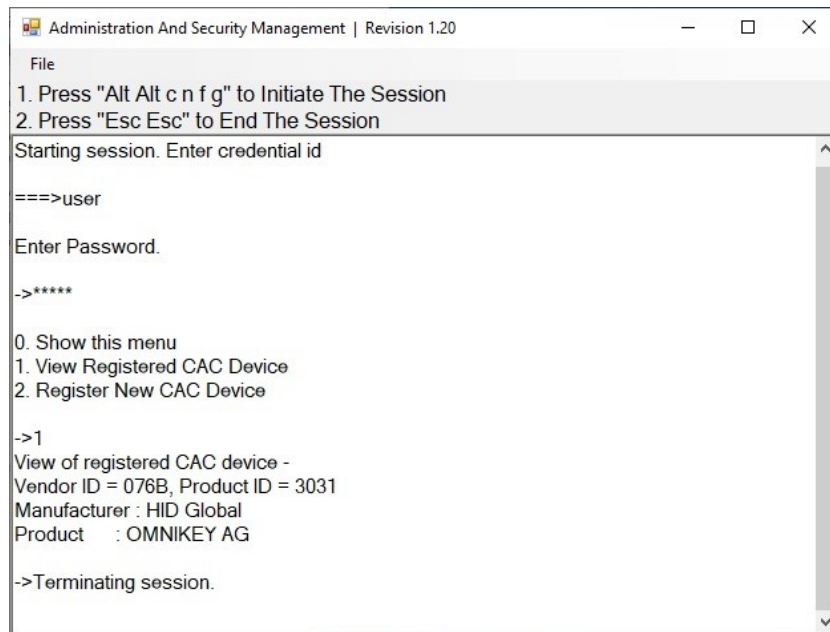
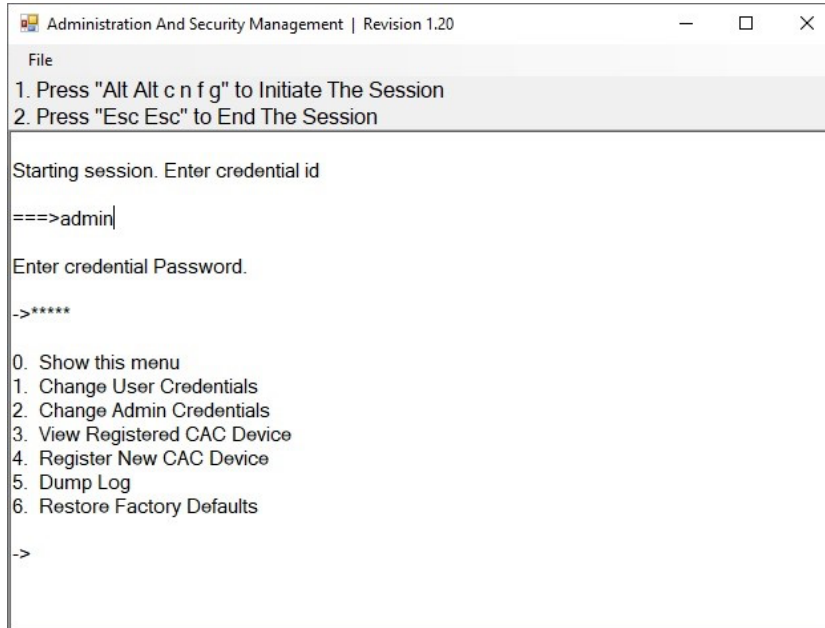


Figure 6: Terminate Session

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 7 below is a screenshot of the tool you should be seeing on your screen.



```
Administration And Security Management | Revision 1.20
File
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. View Registered CAC Device
4. Register New CAC Device
5. Dump Log
6. Restore Factory Defaults

->
```

Figure 7: Administrator Log-in

7.2 Administrator – CAC Port Configuration

CAC (Common Access Card) port configuration is an optional feature, allowing registration of any specific USB peripheral to operate with the device. Only one peripheral can be registered at a time and only the registered peripheral will operate with the device. By default, when no peripheral is registered, the device will operate with any smart card reader or other USB authentication device. Other device types are not supported by default.

- Select option 4 from the menu on your screen and press Enter.
- Connect the peripheral device to be registered to the CAC USB port in the console side of the device and wait until the device is reading the new peripheral information.
- The device will list the information of the connected peripheral on the screen and buzz 3 times when registration is completed.
- Figure 8 below is a screenshot of the tool you should be seeing on your screen. A USB Smart Card Reader was registered to the CAC port in this example:

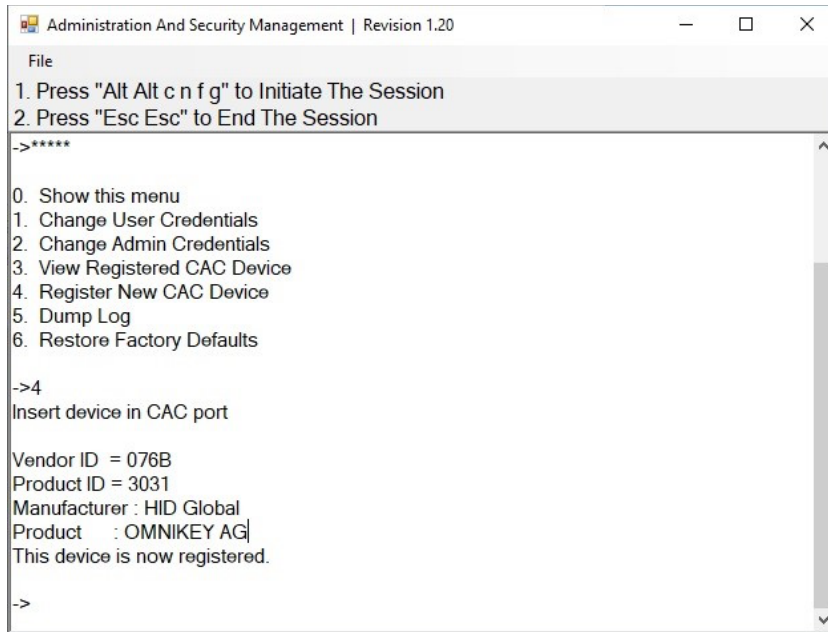


Figure 8: Admin CAC Port Registration

7.3 Administrator – View Registered CAC Peripheral

- Select option 3 from the menu on your screen and press Enter.
- Figure 9 below is a screenshot of the tool you should be seeing on your screen. A USB Smart Card Reader is registered to the CAC port in this example:

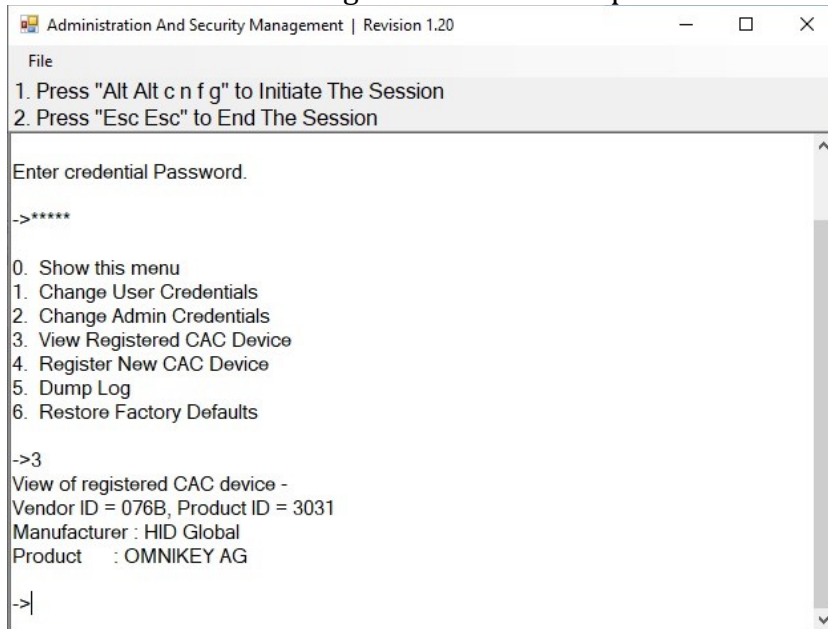


Figure 9: Admin View Registered CAC Peripheral

7.4 Administrator – Change User Credentials

- Select option 1 from the menu on your screen and press Enter.
- Enter the new User ID and press Enter.

- Enter the new User ID again and press Enter.
- Enter the new User password and press Enter.
- Enter the new User password again and press Enter.
- Figure 10 below is a screenshot of the tool you should be seeing on your screen.

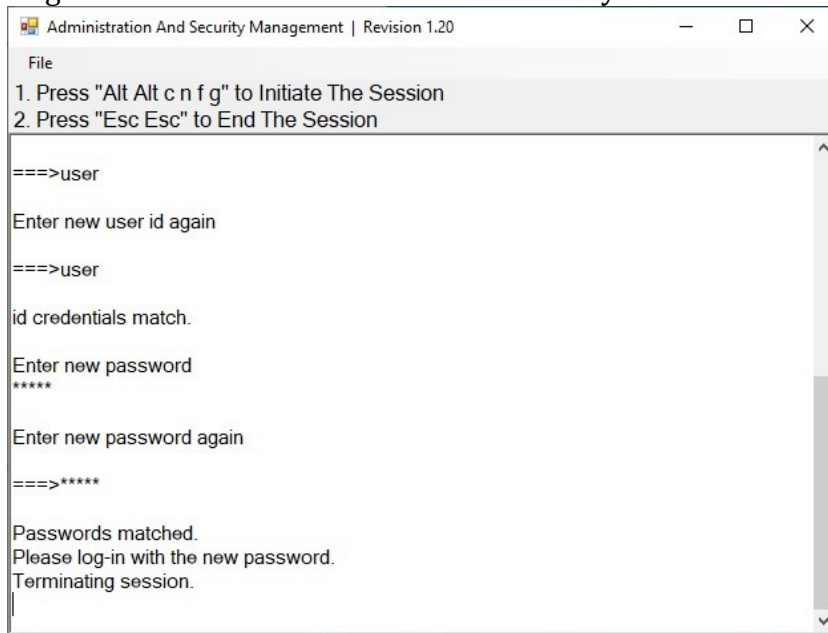


Figure 10: Admin Change User Credentials

7.5 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 11 below is a screenshot of the tool you should be seeing on your screen.

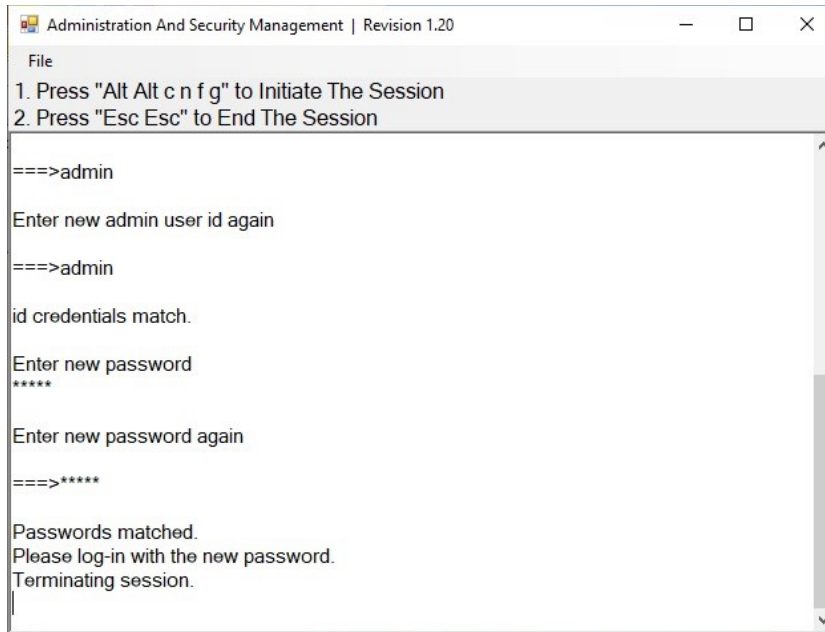


Figure 11: Admin Change Admin Credentials

7.6 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 5 from the menu on your screen and press Enter.
- The last 10 events will be presented in the log as shown in Figure 12 below:

```

=====LOG DATA=====

```

No	Event	Date & Time	Pass/Fail
28.	ALF	02/02/21 12:45:27	PASS
29.	ALO	02/02/21 12:46:51	PASS
30.	LGD	02/02/21 12:47:01	PASS
31.	PWD	02/02/21 12:47:26	PASS
32.	PWU	02/02/21 12:47:32	PASS
33.	STS	02/02/21 12:47:33	PASS
34.	ALO	02/02/21 12:50:56	PASS
35.	LGD	02/02/21 12:51:05	PASS
36.	ALF	02/02/21 12:56:15	PASS
37.	ALO	02/02/21 13:00:54	PASS

Figure 12: 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 13 below:

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

Figure 13: Event Codes

7.7 Administrator – Restore Factory Defaults

- Select option 6 from the menu on your screen and press enter.
- The following menu will be presented (see Figure 15 below):

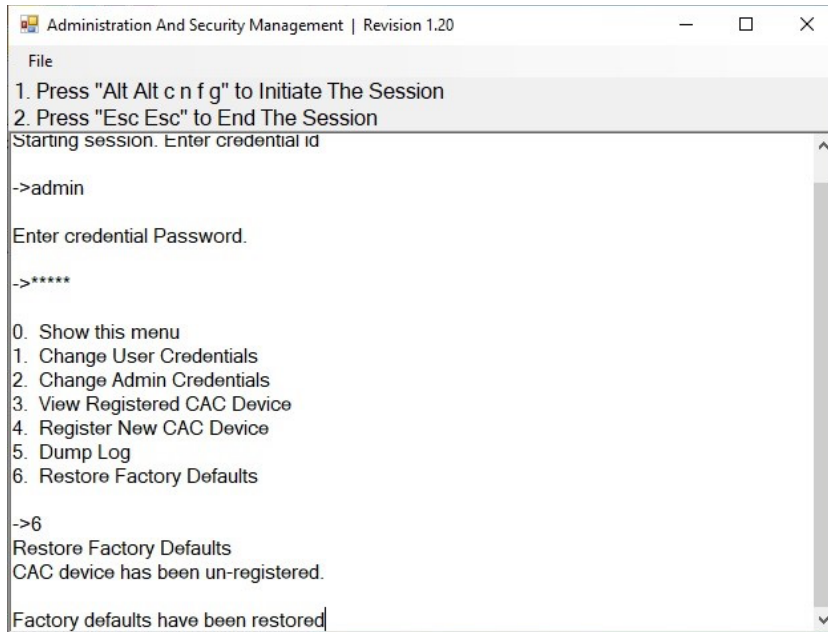


Figure 14: Restore Factory Defaults

The unit will perform power reset automatically. All system defaults will be restored and any registered CAC devices will be cleared.

7.8 Administrator – Terminate Session

Press "Esc Esc".