



IPGard Secure KVM Administration and Security Management Tool Guide (KVM/Matrix)

DESIGNED AND MADE IN USA

Release Date: May 10th, 2018

Document ID: ADG-OS0-ALL

Version: 2.1

Prepared By: Albert Cohen

Prepared For: IPGard

Table of Contents

TABLE OF CONTENTS.....	2
1. OVERVIEW.....	5
2. INTENDED AUDIENCE	6
3. SYSTEM REQUIREMENTS.....	7
4. SYSTEM SETUP	8
5. INITIATE SESSION.....	9
6. USER FUNCTIONS.....	10
6.1. USER – LOG-IN	10
6.2. USER – CAC PORT CONFIGURATION	10
6.3. USER – VIEW REGISTERED CAC PERIPHERAL.....	11
6.4. USER – TERMINATE SESSION	11
7 ADMINISTRATOR FUNCTIONS.....	13
7.1 ADMINISTRATOR – LOG-IN.....	13
7.2 ADMINISTRATOR – CAC PORT CONFIGURATION	13
7.3 ADMINISTRATOR – VIEW REGISTERED CAC PERIPHERAL	14
7.4 ADMINISTRATOR – CHANGE USER CREDENTIALS.....	14
7.5 ADMINISTRATOR – CHANGE ADMINISTRATOR CREDENTIALS.....	15
7.6 ADMINISTRATOR – EVENT LOG (AUDITING)	15
7.7 ADMINISTRATOR – SELECT MODE (KVM/KM)	17
7.8 ADMINISTRATOR – RESTORE FACTORY DEFAULTS	18
7.9 ADMINISTRATOR – TERMINATE SESSION	18

Table of Figures

Figure 1: Administration and Security Management Tool	8
Figure 2: Initiate Session Capture	9
Figure 3: User Log-in	10
Figure 4: User CAC Port Registration	11
Figure 5: User View Registered CAC Peripheral.....	11
Figure 6: Terminate Session	12
Figure 7: Administrator Log-in.....	13
Figure 8: Admin CAC Port Registration.....	14
Figure 9: Admin View Registered CAC Peripheral	14
Figure 10: Admin Change User Credentials.....	15
Figure 11: Admin Change Admin Credentials	15
Figure 12: Sample Log.....	16
Figure 13: Event Codes.....	17
Figure 14: Admin Select Mode	17
Figure 15: Restore Factory Defaults.....	18

List of Tables

Table 1: User/Administrator Function Permissions	5
Table 2: Peripheral Devices supported by the KVM/Matrix TOE	7

1. OVERVIEW

The Administration and Security Management Tool was designed by IPGARD to allow identified and authenticated users and system administrators to perform the following management activities on IPGARD Secure KVM/Matrix 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		✓
Select Mode - KVM/KM**		✓
Restore Factory Default (reset)		✓
Terminate Session	✓	✓

Table 1: User/Administrator Function Permissions

*for models that support USB authentication devices only (-P or -X in model name)

**IPGARD does not offer KM model but KVM devices still support KM operation mode.

An authenticated User and authenticated Administrator are both considered types of administrators for the purposes of compliance with version 3.0 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 IPGARD technical support at support@IPGARD.com.

3. SYSTEM REQUIREMENTS

- The IPGARD Secure KVM/Matrix 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/Matrix 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, KVM/KM extender.
Display	Display, Projector, Video or KVM extender.
Audio out	Analog amplified speakers, Analog headphones, Digital audio appliance.
Mouse / Pointing Device	Any wired mouse or trackball without internal USB hub or composite device functions, Touch-screen, Multi-touch or digitizer, KVM/KM extender.
User Authentication Device	Smart-card reader, PIV/CAC reader, Token or Biometric reader.*

Table 2: Peripheral Devices supported by the KVM/Matrix TOE

*TOE -P and -X models only

4. SYSTEM SETUP

Note: Only one computer connected to the KVM or Matrix 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/Matrix 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 - <http://ipgard.com/tools-software/>
- 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.

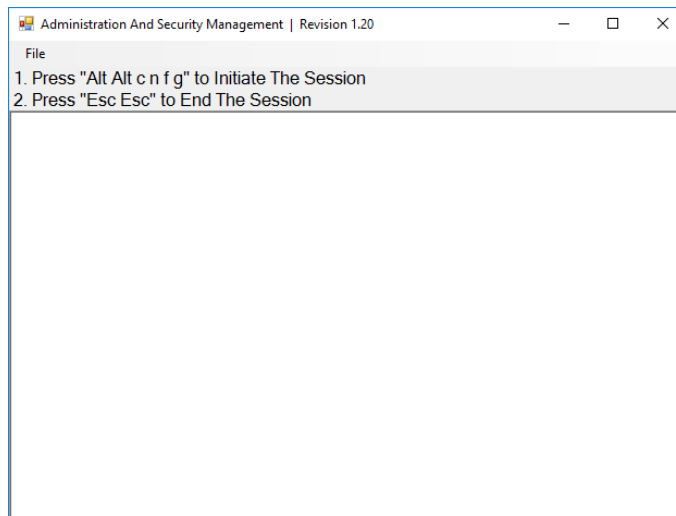


Figure 1: Administration and Security Management Tool

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.

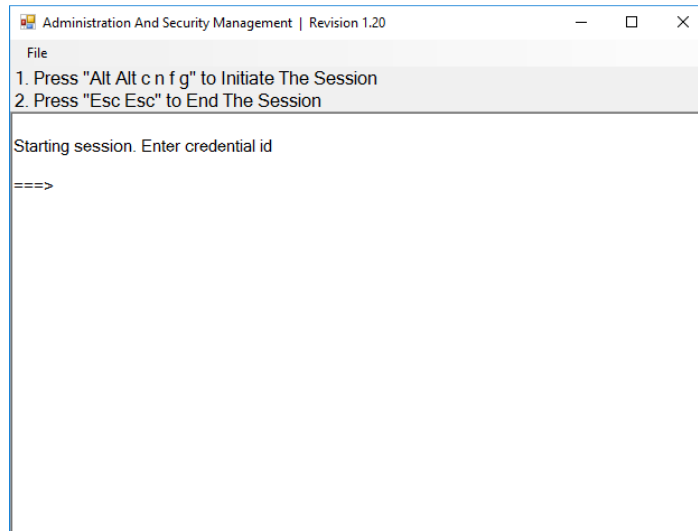
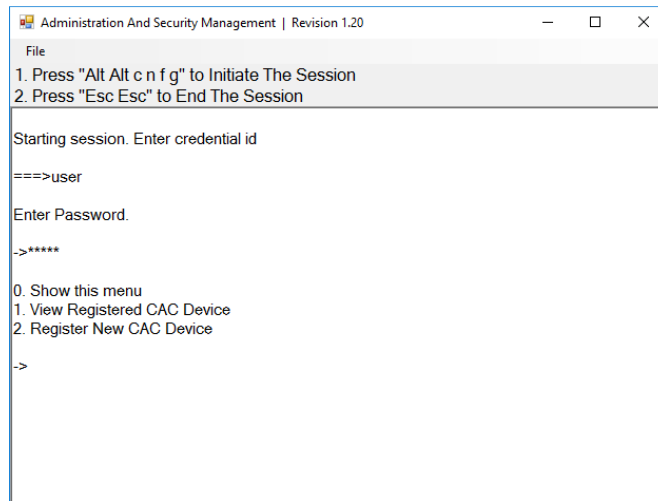


Figure 2: Initiate Session Capture

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.



```
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
===>user

Enter Password.
->*****

0. Show this menu
1. View Registered CAC Device
2. Register New CAC Device
->
```

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.

- 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:

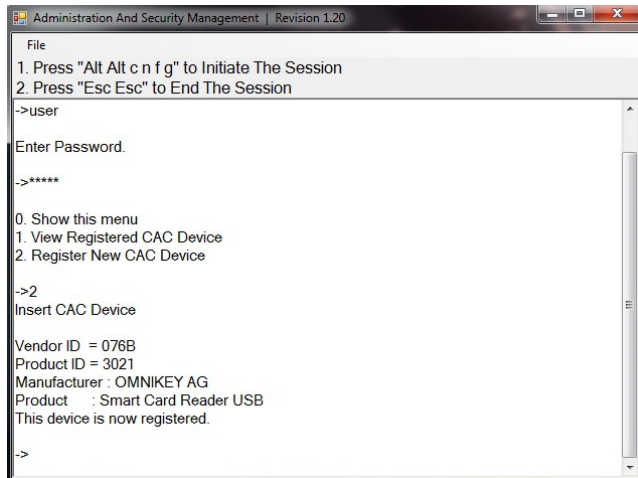


Figure 4: User CAC Port Registration

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:

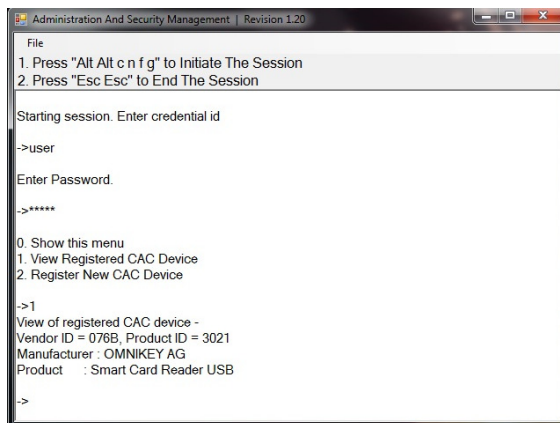


Figure 5: User View Registered CAC Peripheral

6.4. User – Terminate Session

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

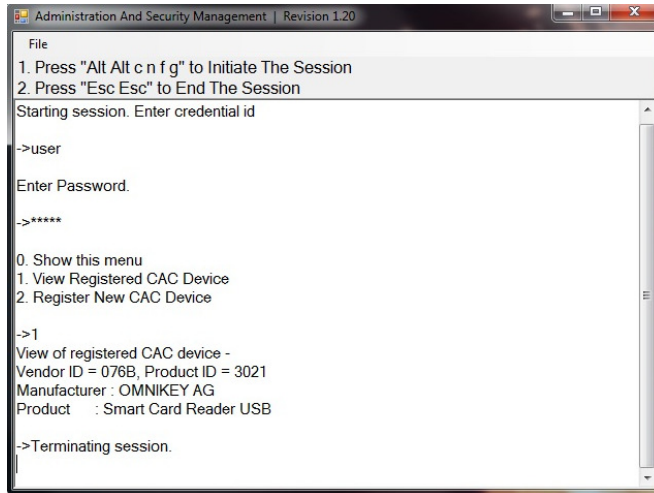
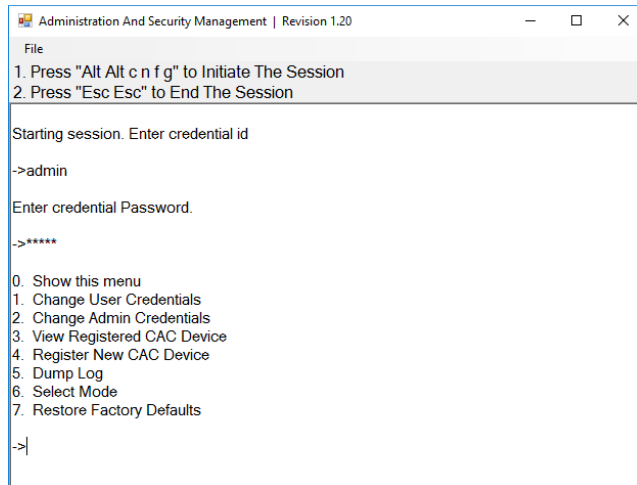


Figure 6: Terminate Session

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. Select Mode
7. 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.

- 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:

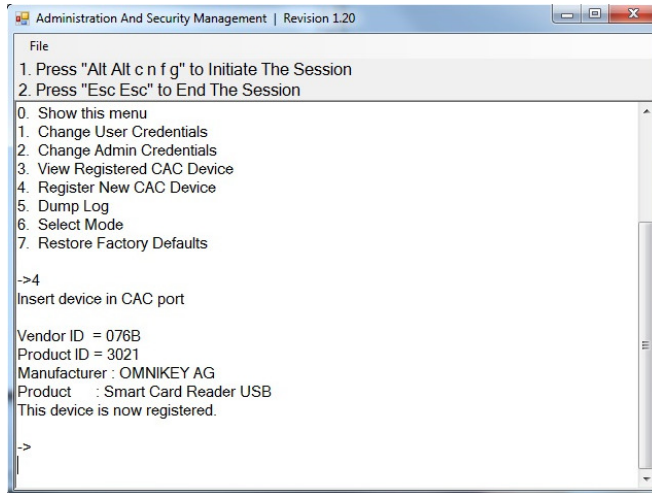


Figure 8: Admin CAC Port Registration

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:

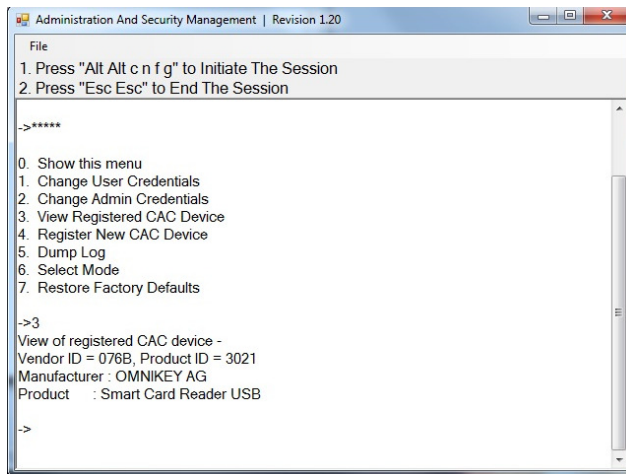


Figure 9: Admin View Registered CAC Peripheral

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.

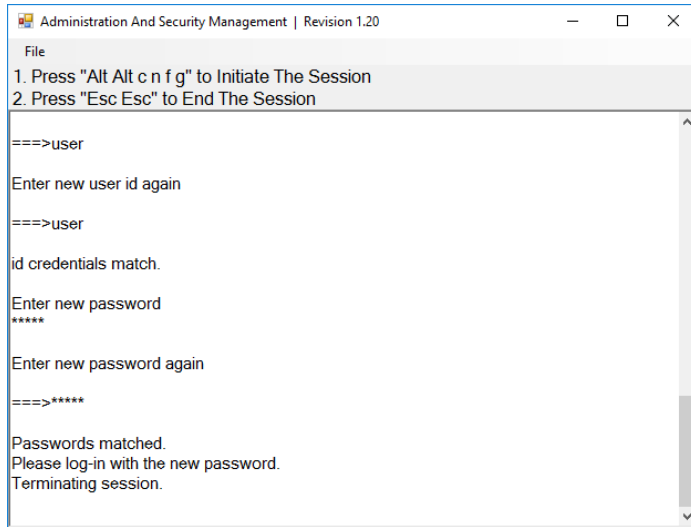


Figure 10: Admin Change User Credentials

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.

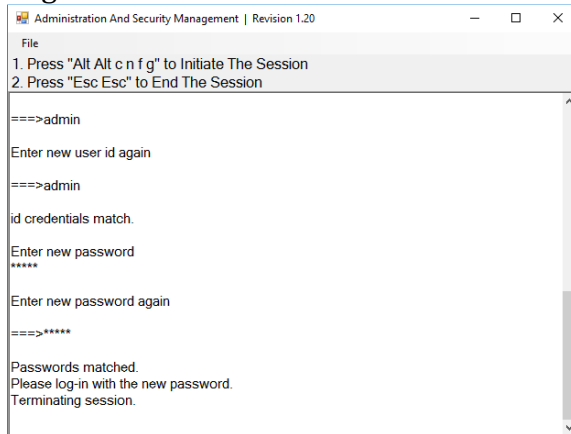


Figure 11: Admin Change Admin Credentials

7.6 Administrator – Event Log (auditing)

Event Log is a detailed report of critical activities stored in the device memory. The 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
=====
9.   ALO     10/26/16 15:58:49   PASS
10.  P01     10/26/16 15:59:10   PASS
11.  PWU     10/26/16 15:59:11   PASS
12.  STS     10/26/16 15:59:11   PASS
13.  ALO     10/26/16 15:59:41   PASS
14.  AFD     10/26/16 15:59:47   PASS
15.  ALF     10/26/16 16:00:12   PASS
16.  PWU     10/26/16 16:00:26   PASS
17.  STS     10/26/16 16:00:26   PASS
18.  ALO     10/26/16 16:00:47   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	PXX	Select Mode 01(KVM), 02(KM), 03(Custom)... Uploaded
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

Figure 13: Event Codes

7.7 Administrator – Select Mode (KVM/KM)

- Select option 6 from the menu on your screen and press enter.
- The following menu will be presented (see Figure 14 below):

```

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
U. 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. Select Mode
7. Restore Factory Defaults
->6
Select Mode: 1. KVM
              2. KM
              3. Custom
Current mode is KVM
===>2
Select KM type: 1. KM(two minute delay)
                2. KM(no delay)
->1
enabling KM_2
Terminating session.

```

Figure 14: Admin Select Mode

- Select option 1 for KVM mode, or option 2 for KM mode. The device will reset after mode selection. Note that IPGARD does not offer KM model but KVM devices still support KM operation mode. The Select Mode 3 (Custom) is only available on DisplayPort models.
- When selecting option 2, sub-menu will be displayed with two options: KM (two minute delay) and KM (no delay).
- KM (two minute delay) when selected will make the KVM unit's port switching behave like a KM unit. If the port was switched via the front panel there will be a delay of two minutes where the user won't be able to switch ports using the mouse and port switching will only be allowed via the front panel. On the other hand if the port was switch via the mouse after option KM (two minute delay) was selected, then the user won't be able to port switch via the front panel for two minutes and port switching will only be allowed via the mouse. KM (no delay) when selected will

make the KVM unit's port switching behave like a KM unit. The user will be allowed to change ports either by using the front panel or moving the mouse.

- Exit the menu by pressing the Esc key once on the keyboard.

7.8 Administrator – Restore Factory Defaults

- Select option 7 from the menu on your screen and press enter.
- The following menu will be presented (see Figure 15 below):

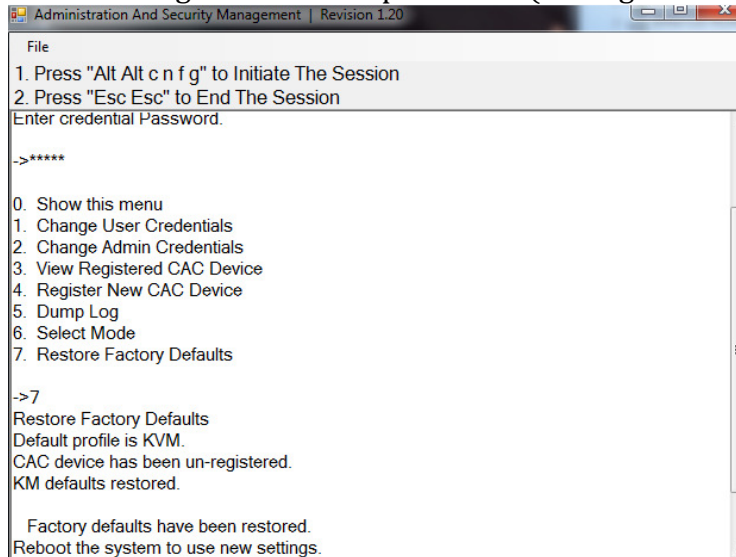


Figure 15: Restore Factory Defaults

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

7.9 Administrator – Terminate Session

Press "Esc Esc".