iPGARD Secure KVM

Administration and Security Management Tool Guide

(KVM and KM)

DESIGNED AND MADE IN USA

.

Release Date: January 14th, 2017

Document ID: DOC-IPG-2009

Version: 2.1

Prepared By: Albert Cohen

Prepared For: iPGARD

Table of Contents

TABLE OF CONTENTS

1. Overview 4
2. Intended Audience 5
3. System Requirements 5
4. System Setup 6
5. Initiate Session 7
6. User Functions 7
- User - Log-in 7
- User - CAC Port Configuration 8
- User – View Registered CAC Peripheral 8
- User – Terminate Session 9
7. Administrator Functions 9
- Administrator - Log-in 9
- Administrator - CAC Port Configuration 10
- Administrator – View Registered CAC Peripheral 10
- Administrator – Change User Credentials 11
- Administrator – Change Administrator Credentials 11
- Administrator - Event Log (auditing) 12
- Administrator - Select Mode (KVM/KM) 12
- Administrator - Restore Factory Defaults 13
- Administrator – Terminate Session 13

Table of Figures

Figure 3.1: Administration and Security Management Tool 6

Figure 4.1: Initiate Session Capture 7

Figure 5.1: User Log-in 7

Figure 5.2: User CAC Port Registration 8

Figure 5.3: User View Registered CAC Peripheral 8

Figure 5.4: Terminate Session 9

Figure 6.1: Administrator Log-in 9

Figure 6.2: Admin CAC Port Registration 10

Figure 6.3: Admin View Registered CAC Peripheral 10

Figure 6.4: Admin Change User Credentials 11

Figure 6.5: Admin Change Administrator Credentials 11

Figure 6.6: Sample Log 12

Figure 6.7: Events Codes 12

Figure 6.8: Admin Select Mode 13

Figure 6.9: Restore Factory Defaults 13

1. OVERVIEW

Administration and Security Management Tool designed by iPGARD to allow identified and authenticated users and system administrators to perform the following activities:

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	✓	✓

An authenticated User and authenticated Administrator are both considered types of administrators for the PP PSS.

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.

3. SYSTEM REQUIREMENTS

1. iPGARD Secure PSS 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 operating system XP, Win 7, Win 8 and Win 10 with framework .NET 2.0 or newer.

2. The peripheral devices that supported by the KVM/KM TOE are listed in the following table:

Console Port	Authorized Devices	KVM/KM
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;	KVM/KM
Display	Display, Projector, Video or KVM extender.	KVM
Audio out	Analog amplified speakers, Analog headphones, Digital audio appliance.	KVM/KM
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.	KVM/KM
User Authentication Device	Smart-card reader, PIV/CAC reader, Token or Biometric reader*	KVM/KM

*TOE - Models with UCAC only

4. SYSTEM SETUP

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

1. Ensure that KVM/KM power is turned off or disconnected from the unit and the computer.
2. Using USB cable Type-A to Type-B connect the PC to the KVM/KM host K/M port one. Connect a second USB cable Type-A to Type-B between the PC and the KVM/KM if CAC port configuration is also required.
3. Connect a USB keyboard and mouse in the two USB console ports.
4. For KVM – Connect the appropriate video cable between the PC and the KVM video 1 port.
5. For KVM – Connect the monitor to the KVM console video output connector.
6. For KM – Connect the monitor directly to the PC video output connector.
7. Power up the PC and the KVM/KM
8. Download the Administration and Security Management Tool from the following link to the PC - https://ipgard.com/tools-software/
9. Run the Administration and Security Management Tool executable file. Figure 3.1 below is a screenshot of the tool you should be seeing on your screen.

Figure 3.1: Administration and Security Management Tool

5. INITIATE SESSION

1. Using the keyboard, press “Alt Alt cnfg”
2. At this stage the mouse connected to the KVM/KM will stop functioning.
3. Figure 4.1 below is a screenshot of the tool you should be seeing on your screen.

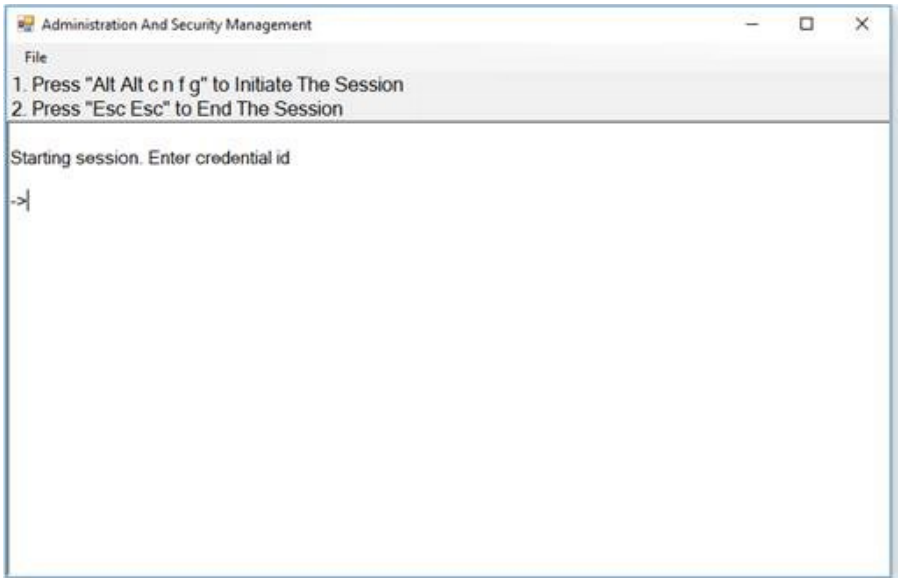

Figure 4.1:
Initiate Session Capture

6. USER FUNCTIONS

User - Log-in

1. Enter the default username “user” and press Enter.
2. Enter the default password “12345” and press Enter.
3. Figure 5.1 below is a screenshot of the tool you should be seeing on your screen.

Figure 5.1: User Log-in

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 KVM/KM. Only one peripheral can be registered and only the registered peripheral will operate with the KVM/KM. By default, when no peripheral is registered, the KVM/KM will operate with any Smart Card Reader.

1. Select option 2 from the menu on your screen and press Enter.
2. Connect the peripheral device to be registered to the CAC USB port in the console side of the KVM/KM and wait until the KVM /KM is reading the new peripheral information.
3. The KVM/KM will list the information of the connected peripheral on the screen and buzz 3 times when registration is completed.
4. Figure 5.2 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 sample:

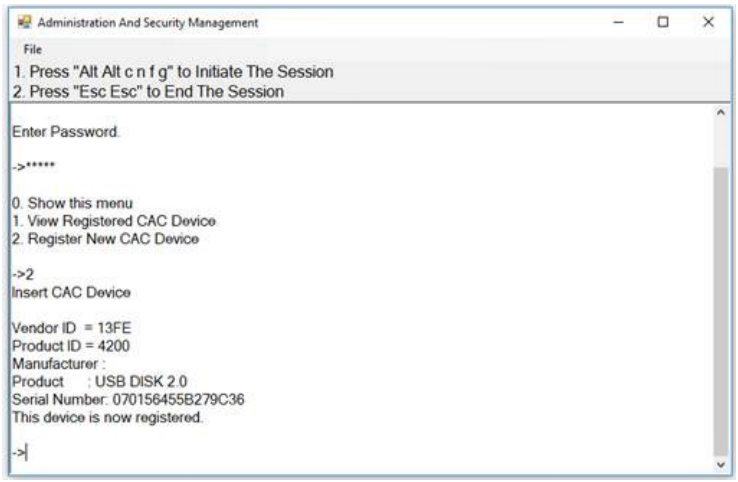

Figure 5.2:
User CAC Port Registration

User – View Registered CAC Peripheral

1. Select option 1 from the menu on your screen and press Enter.
2. Figure 5.3 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 sample:

Figure 5.3:
User View Registered CAC Peripheral

User – Terminate Session

1. Press “Esc Esc”.
2. Figure 5.4 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 sample:

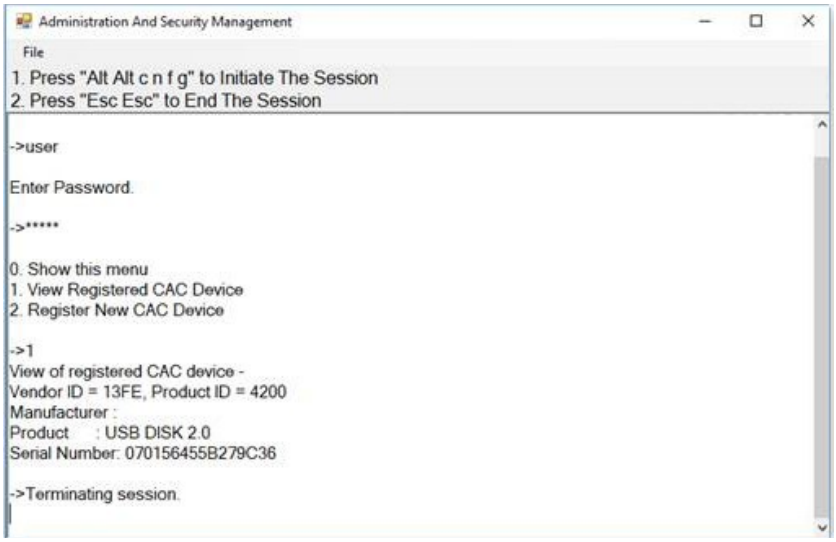

Figure 5.4: Terminate Session

7. ADMINISTRATOR FUNCTIONS

Administrator - Log-in

1. Enter the default username “admin” and press Enter.
2. Enter the default password “12345” and press Enter.
3. Figure 6.1 below is a screenshot of the tool you should be seeing on your screen.

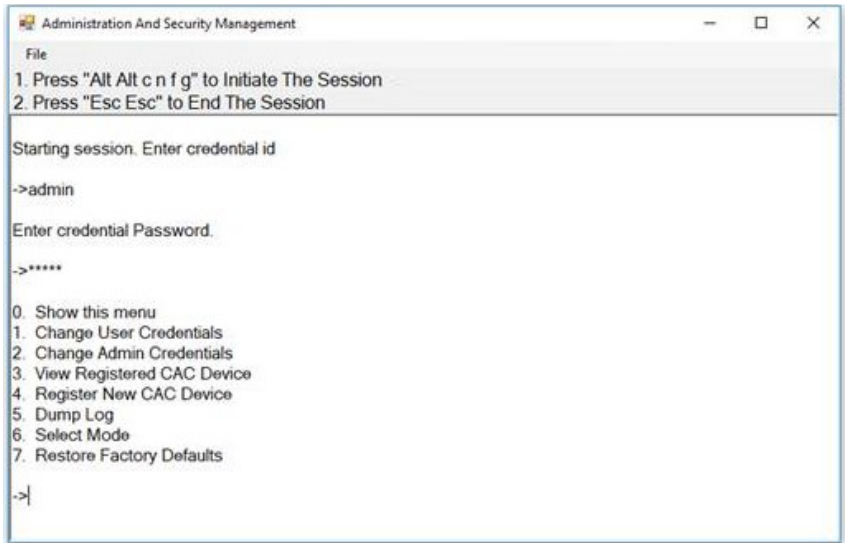

Figure 6.1: Administrator Log-in

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 KVM/KM. Only one peripheral can be registered and only the registered peripheral will operate with the KVM/KM. By default, when no peripheral is registered, the KVM/KM will operate with any Smart Card Reader.

1. Select option 4 from the menu on your screen and press Enter.
2. Connect the peripheral device to be registered to the CAC USB port in the console side of the KVM/KM and wait until the KVM /KM is reading the new peripheral information.
3. The KVM/KM will list the information of the connected peripheral on the screen and buzz 3 times when registration in completed.
4. Figure 6.2 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 sample:

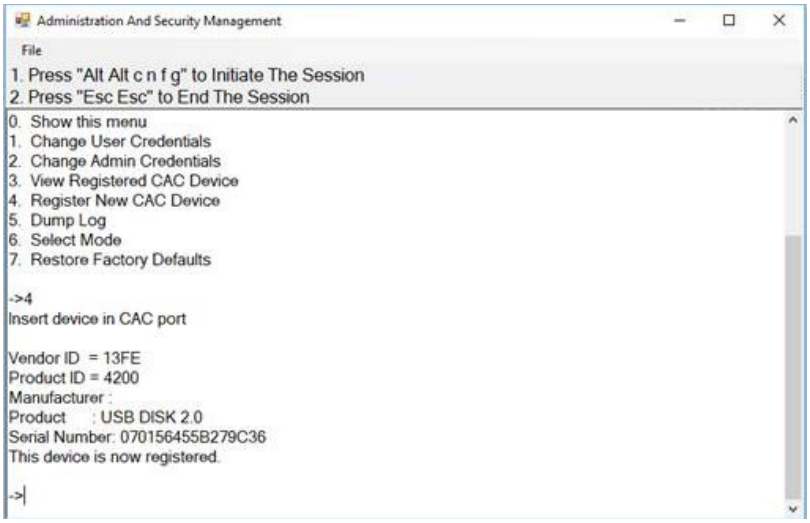

Figure 6.2:
Admin CAC Port Registration

Administrator -
View Registered CAC Peripheral

1. Select option 3 from the menu on your screen and press Enter.
2. Figure 6.3 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 sample:

Figure 6.3: Admin View Registered CAC Peripheral

Administrator – Change User Credentials

1. Select option 1 from the menu on your screen and press Enter.
2. Enter the new User ID and press Enter.
3. Enter the new User ID again and press Enter.
4. Enter the new User password and press Enter.
5. Enter the new User password again and press Enter.
6. Figure 6.4 below is a screenshot of the tool you should be seeing on your screen.

Figure 6.4:
Admin Change User Credentials

Administrator – Change Administrator Credentials

1. Select option 2 from the menu on your screen and press Enter.
2. Enter the new Administrator ID and press Enter.
3. Enter the new Administrator ID again and press Enter.
4. Enter the new Administrator password and press Enter.
5. Enter the new Administrator again and press Enter.
6. Figure 6.5 below is a screenshot of the tool you should be seeing on your screen.

Figure 6.5:
Admin Change Administrator Credentials

Administrator - Event Log (auditing)

Event Log is a detailed report of critical activities stored in the KVM memory. The following steps provide instructions for dumping the log by identified and authenticated administrator.

1. Select option 5 from the menu on your screen and press Enter.
2. The last up to 100 events will be presented in the log:
3. Press the Enter key to see the previous 10 events.
4. 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
5. The log Data may include any of the following codes:

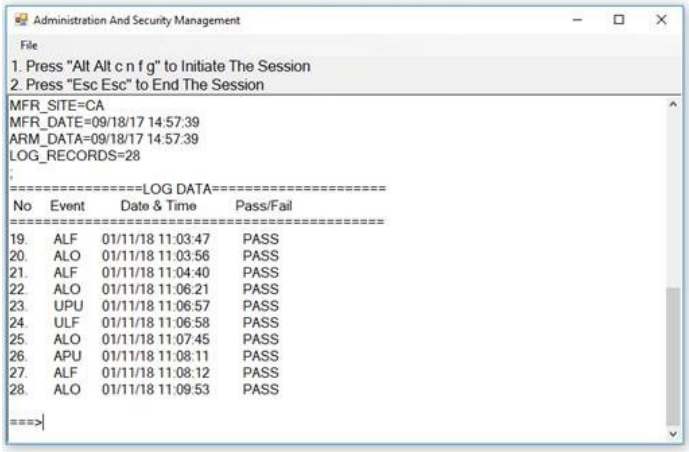

Figure 6.6: Sample Logs

#	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 6.7: Events Codes

Administrator - Select Mode (KVM/KM)

1. Select option 6 from the menu on your screen and press enter.
2. The following menu will be presented (see Figure 6.8 below):
3. Select option 1 for KVM mode, or option 2 for KM mode. The device will reset after mode selection.
4. Exit the menu by pressing the Esc key once on the keyboard.

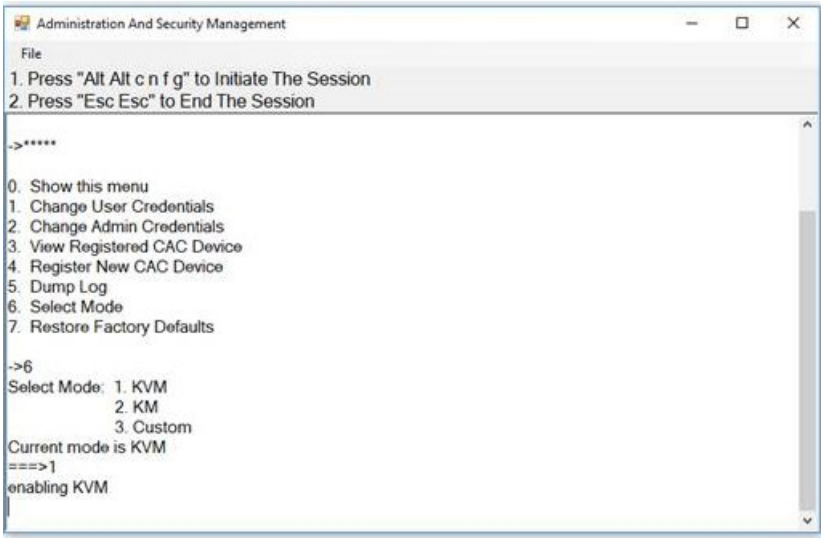

Figure 6.8: Admin Select Mode

Administrator - Restore Factory Defaults

1. Select option 7 from the menu on your screen and press enter.
2. The following menu will be presented (see Figure 6.9 below):

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

Figure 6.9: Restore Factory Defaults

Administrator – Terminate Session

1. Press “Esc Esc”.