# 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 .............................................................................................................18
Figure 15: Restore Factory Defaults .................................................................................................18
List of Tables

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

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

<table>
<thead>
<tr>
<th>Menu Function</th>
<th>User</th>
<th>Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log-in</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Change User Access Credentials</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Change Admin Access Credentials</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>View Registered CAC Device*</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Register New CAC Device*</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Auditing - Dump Log</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Select Mode - KVM/KM**</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Restore Factory Default (reset)</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Terminate Session</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Table 1: User/Administrator Function Permissions

*for models that support USB authentication devices only (‘C’ in model name)

**Tripp-Lite 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. If the product does not behave in the manner specified by this document, please contact Tripp Lite technical support at intlservice@tripplite.com.
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 Tripp Lite technical support at [www.tripplite.com/support](http://www.tripplite.com/support).
3. **System Requirements**

- The Tripp-Lite 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:

<table>
<thead>
<tr>
<th>Console Port</th>
<th>Authorized Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keyboard</td>
<td>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.</td>
</tr>
<tr>
<td>Display</td>
<td>Display, Projector, Video or KVM extender.</td>
</tr>
<tr>
<td>Audio out</td>
<td>Analog amplified speakers, Analog headphones, Digital audio appliance.</td>
</tr>
<tr>
<td>Mouse / Pointing Device</td>
<td>Any wired mouse or trackball without internal USB hub or composite device functions, Touch-screen, Multi-touch or digitizer, KVM extender.</td>
</tr>
<tr>
<td>User Authentication Device</td>
<td>Smart-card reader, PIV/CAC reader, Token or Biometric reader.*</td>
</tr>
</tbody>
</table>

*Table 2: Peripheral Devices supported by the KVM TOE

*TOE ‘C’ models only*
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.tripplite.com/pages/niap-secure-kvm](https://www.tripplite.com/pages/niap-secure-kvm)
- 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](image-url)
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](image)

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](image)

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:
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:

6.4. User – Terminate Session

- Press “Esc Esc”.
- Figure 6 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 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.

![Figure 7: Administrator Log-In](image)

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:
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:

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.
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.

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:

<table>
<thead>
<tr>
<th>No</th>
<th>Event</th>
<th>Date &amp; Time</th>
<th>Pass/Fail</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>ALO</td>
<td>10/26/16 15:58:49</td>
<td>PASS</td>
</tr>
<tr>
<td>10</td>
<td>P01</td>
<td>10/26/16 15:59:10</td>
<td>PASS</td>
</tr>
<tr>
<td>11</td>
<td>PWU</td>
<td>10/26/16 15:59:11</td>
<td>PASS</td>
</tr>
<tr>
<td>12</td>
<td>STS</td>
<td>10/26/16 15:59:11</td>
<td>PASS</td>
</tr>
<tr>
<td>13</td>
<td>ALO</td>
<td>10/26/16 15:59:41</td>
<td>PASS</td>
</tr>
<tr>
<td>14</td>
<td>AFD</td>
<td>10/26/16 15:59:47</td>
<td>PASS</td>
</tr>
<tr>
<td>15</td>
<td>ALF</td>
<td>10/26/16 16:00:12</td>
<td>PASS</td>
</tr>
<tr>
<td>16</td>
<td>PWU</td>
<td>10/26/16 16:00:26</td>
<td>PASS</td>
</tr>
<tr>
<td>17</td>
<td>STS</td>
<td>10/26/16 16:00:26</td>
<td>PASS</td>
</tr>
<tr>
<td>18</td>
<td>ALO</td>
<td>10/26/16 16:00:47</td>
<td>PASS</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>#</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ALO</td>
<td>Administrator Log On</td>
</tr>
<tr>
<td>2</td>
<td>ALF</td>
<td>Administrator Log Off</td>
</tr>
<tr>
<td>3</td>
<td>ARM</td>
<td>Arming A/T System</td>
</tr>
<tr>
<td>4</td>
<td>CAC</td>
<td>CAC Configuration</td>
</tr>
<tr>
<td>5</td>
<td>EDL</td>
<td>EDID Learn</td>
</tr>
<tr>
<td>6</td>
<td>LGD</td>
<td>LOG Dump</td>
</tr>
<tr>
<td>7</td>
<td>PWU</td>
<td>Power Up</td>
</tr>
<tr>
<td>8</td>
<td>PXX</td>
<td>Select Mode 01(KVM), 02(KM), 03(Custom)... Uploaded</td>
</tr>
<tr>
<td>9</td>
<td>RCA</td>
<td>Rejected CAC Device</td>
</tr>
<tr>
<td>10</td>
<td>AFD</td>
<td>Restore Factory Default</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>11</td>
<td>RKM</td>
<td>Rejected Keyboard or Mouse</td>
</tr>
<tr>
<td>12</td>
<td>STS</td>
<td>Self-Test</td>
</tr>
<tr>
<td>13</td>
<td>TMP</td>
<td>Device Tampered, Review by MFR only</td>
</tr>
<tr>
<td>14</td>
<td>ULO</td>
<td>User Log On</td>
</tr>
<tr>
<td>15</td>
<td>ULF</td>
<td>User Log Off</td>
</tr>
</tbody>
</table>

**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):

- Select option 1 for KVM mode, or option 2 for KM mode. The device will reset after mode selection. Note that Tripp Lite 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](image)

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”.