Belkin Administrator Guide

Products covered by this guide:
Belkin Secure KVM – NIAP PP4.0

LNKPG-00666
Rev. B00

Table of Contents

Introduction

This Administrator Guide provides details to configure, administer, and audit your new product.

Important Security Note:

If you are aware of a potential security vulnerability while installing or operating this product, we encourage you to contact us immediately in one of the following ways:

- Email: gov_security@belkin.com
- Tel: +1 (800) 282-2355

Note that gov_security@belkin.com is not intended for technical support.

Important Anti-Tamper Indications:

This product has tamper-evident security tape that will provide visual indication of attempts to open the enclosure. Further, the product is equipped with an always-on active anti-tamper mechanism. Any attempt to open the enclosure will activate the anti-tamper trigger and render the unit permanently inoperable.

If the product's anti-tamper security tape appears disrupted or if all the channel LEDs flash continuously, do not install the unit and call Belkin Technical support at +1 (800) 282-2355

Intended Audience

This document is intended for the following professionals:

- System Administrators/IT Managers/Information Assurance Managers

Revision History

A – Initial Release, 1 March 2020

Important note before deploying the product:
To comply with the product's Common Criteria requirements and to prevent unauthorized administrative access, the default administrator password must be changed prior to first use.

Refer to Administrator Setup section for further details.

Safety Precautions

Please read the following safety precautions carefully before using the product:

- Before cleaning, disconnect the product from any electrical power supply.
- Do not expose the product to excessive humidity or moisture.
- Do not store or use for extensive period of time in extreme thermal conditions – it may shorten product lifetime.
- Install the product only on a clean, secure surface.
- If the product is not used for a long period of time, disconnect it from electrical power.
- If any of the following situations occurs, have the product inspected by a qualified service technician:
    - **Liquid penetrates the product's case.**
    - **The product is exposed to excessive moisture, water, or any other liquid.**
    - **The product is not working well even after carefully following the instructions in this administrator's manual.**
    - **The product has been dropped or is physically damaged.**
    - **The product shows obvious signs of breakage or loose internal parts.**
    - **In case of external power supply – If power supply overheats, is broken or damaged, or has a damaged cable.**
- The product should be stored and used only in temperature and humidity-controlled environments as defined in the product's environmental specifications.
- Never attempt to open the product enclosure. Any attempt to open the enclosure will permanently disable the product.
- The product contains a non-replaceable internal battery. Never attempt to replace the battery or open the enclosure.
- This product is equipped with always-on active anti-tampering system. Any attempt to open the product enclosure will activate the anti-tamper triggers and render the unit inoperable and warranty void.

Safety Precautions (French)

Veuillez lire attentivement les précautions de sécurité suivantes avant d'utiliser le produit:

- Avant nettoyage, débranchez l'appareil de l'alimentation DC /AC.
- Assurez-vous de ne pas exposer l'appareil à une humidité excessive.
- Assurez-vous d'installer l'appareil sur une surface sécurisée propre.
- Ne placez pas le cordon d'alimentation DC en travers d'un passage.
- Si l'appareil n'est pas utilisé de longtemps, retirez l'alimentation murale de la prise électrique.
- L'appareil devra être rangé uniquement dans des environnements à humidité et température contrôlées comme défini dans les caractéristiques environnementales du produit.
- L'alimentation murale utilisée avec cet appareil devra être du modèle fourni par le fabricant ou un équivalent certifié fourni par le fabricant ou fournisseur de service autorisé.
- Si une des situations suivantes survenait, faites vérifier l'appareil par un technicien de maintenance qualifié:

- **En cas d'alimentation externe - L'alimentation de l'appareil surchauffe, est endommagée, cassée ou dégage de la fumée ou provoque des court circuits de la prise du secteur.**
- **Un liquide a pénétré dans le boîtier de l'appareil.**
- **L'appareil est exposé à de l'humidité excessive ou à l'eau.**
- **L'appareil ne fonctionne pas correctement même après avoir suivi attentivement les instructions contenues dans ce guide de l'utilisateur.**
- **L'appareil est tombé ou est physiquement endommagé.**
- **L'appareil présente des signes évidents de pièce interne cassée ou desserrée**
- **L'appareil contient une batterie interne. La batterie n'est pas remplaçable. N'essayez jamais de remplacer la batterie car toute tentative d'ouvrir le boîtier de l'appareil entraînerait des dommages permanents à l'appareil.**
- **Ce produit est équipé d'toujours-sur le système anti- sabotage active. Toute tentative d'ouvrir le boîtier du produit va activer le déclencheur anti-sabotage et de rendre l'unité vide inutilisable et garantie.**

User Guidance & Precautions

Please read the following User Guidance & Precautions before using the product:

1. As the product powers-up it performs a self-test procedure. In case of a self-test failure, including jammed buttons, the product will be Inoperable. A Self-test failure will be indicated by the following LED behavior:

    a. **Unit's anti-tamper mechanism has been activated:**

Unit will rapidly and continuously switch channels

    b. **Jammed button or other failure to boot: Unit will slowly switch between channels.**

To exit a self-test failure state, power cycle the unit. If the problem persists, contact your system administrator or Belkin technical support.

2. Product power-up and Reset to Factory Defaults:

    a. **By default, after product power-up, the active channel will be computer #1, indicated by the applicable front panel button LED being lit.**

    b. **Product restore to factory defaults (RFD) function is available by pressing the following keyboard key sequence: Left CTRL | Left CTRL | f11 | r.**

    c. **RFD action will be indicated by a single click**

    d. **When the product reboots after RFD, the console keyboard and mouse will be mapped to the active channel #1 and default settings will be restored, erasing all user-set definitions.**

3. The appropriate usage of peripherals (e.g. keyboard, mouse, display, authentication device) is described in detail in the User Manual's appropriate sections. Do not connect any authentication device with an external power source to the product.

4. For security reasons and per NIAP and Common Criteria environmental requirements, product should never be used with wireless keyboards and mice.

5. For security reasons and per NIAP and Common Criteria environmental requirements, products should never be connected to a microphone input. Do not connect a microphone to the product audio output port, including headsets with microphone inputs. The KVM is designed to prevent audio input signal flow.

6. The Product is equipped with always-on active anti- tampering system. Any attempt to open the enclosure will activate the anti-tamper trigger, indicated by all channel- select LEDs flashing rapidly from one channel to the other. In this case, product will be inoperable. If the product's anti-tamper evidence tape appears disrupted or if all channel-select LEDs flash continuously, remove product from service immediately and contact technical support.

Important: For change management tracking, it is advised to perform a quarterly log check to verify that administrator accounts and log on events can be verified.

User Guidance & Precautions

7. In case a connected device is rejected in the console port group the user will have the following visual indications:
   a. **When connecting a non-qualified keyboard, the keyboard will be non-functional with no visible keyboard strokes on screen when typing.**
   b. **When connecting a non-qualified mouse, the mouse will be non-functional with mouse cursor frozen on screen.**
   c. **When connecting a non-qualified display, the video diagnostic LED will flash green once and turn off, and video will not display on monitor.**
   d. **When connecting a non-qualified CAC reader (on models with a dedicated CAC port), the USB LED will flash green once and turn off, CAC reader will be inoperable.**
8. Do not connect product to computing devices:
   a. **That are TEMPEST computers**
   b. **That include telecommunication equipment**
   c. **That include frame grabber video cards**
   d. **That include special audio processing cards**
9. The product has a remote-control port on the back panel labeled remote. This port can be used with various remote controls and if connected the operation must be verified and secured.
10. Important! After re-allocating computers to channels, it is mandatory to power cycle the product, keeping it powered OFF for more than 1 minute.
11. The product log access and administrator configuration options are described starting in the next section.
12. Administrator authentication session is terminated only when unit is power-cycled. Once all administrative tasks have been completed, power cycle the unit to exit administrator-authenticated mode.

Reporting Belkin Product Security Vulnerabilities:

1. **If the product's anti-tamper evidence tape appears disrupted or if all channel-select LEDs flash continuously, please remove product from service immediately and contact Belkin Technical Support.**
2. **If you are aware of potential security vulnerabilities with any Belkin secure KM/KVM product, we encourage you to contact us immediately at gov_security@belkin.com or our technical support line at +1-800-282-2355.**

Note: The Gov_Security@belkin.com email address is not intended for technical support.

Administrator Configuration

Warnings and Precautions

The product enables authorized administrators to download event log files and audit the product history as well as have access to advanced settings.

This function is available only to authenticated administrators.

Note: the log data may not be erased and log functions may not be disabled by users or administrators. Also note that RFD does not reset the administrator's password and user name.

Once a new Admin user has been created, there is no way to reset or delete that user.

Important note before deploying the product:

To comply with the product's Common Criteria requirements and to prevent unauthorized administrative access, the default administrator password must be changed prior to first use.

Caution:

The KVM device must be installed in an environment that provides physical security appropriate for the data being processed on the attached computing devices.

Note:
Appropriately trained and trusted administrators and users must be available to administer, configure and use the device.

Administrator Setup / Log On

1. Connect keyboard, mouse and one USB cable between the KVM and the computer and power up the product. Note that the display may or may not be connected through the product.

2. Select channel #1 on the product and open Notepad on the computer connected to channel #1.

3. Using keyboard, type CTRL (Left), CTRL (Right), t to enter Admin Mode.

4. Text will appear in Notepad asking for a user name.

5. The default user name is: “admin1234”. This account ID cannot be changed or deleted.

6. The default first device logon password is: “1234ABCDefg!@#”

7. At first logon the administrator must set a new, non- default, password.

   The new password must be at least:

   a. **8 characters long but not longer than 24 characters;**

   b. **Have at least one capital and one lower-case letter**

   c. **Have at least one number;**

   d. **Have at least one symbol.**

8. Password must be typed twice to confirm.

9. Password may be changed at any time.

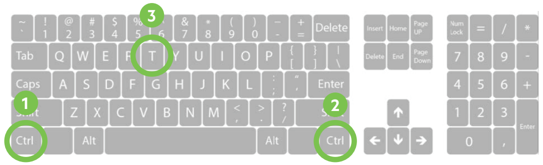
10. RFD will not reset the user name and password!

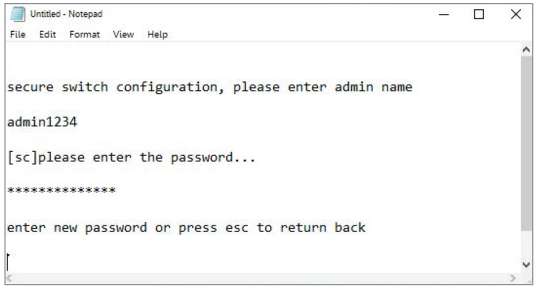
11. If the user name or password is forgotten – contact Belkin support.

12. Note: The unit will enter tamper mode after 4 failed attempts to login. To reset, power cycle the unit and attempt again.

13. Additional administrative user accounts can be created from the terminal menu (up to 8 more in addition to the default admin account per unit).

    a. **Admin names need to include at least 1 capital and 1 lower case letter and 1 number.**





```
secure switch configuration, please enter admin name

admin1234

[sc]please enter the password...

**************

enter new password or press esc to return back
```

Terminal Mode Options

Once authenticated, the following menu opens:
authentication succeeded. please select operation...

```
0-  asset management
1-  firmware versions
2-  configure dpp
3-  configure sc
4-  account management
5-  reset to factory defaults
6-  logs and events
7-  configure peripheral devices
8-  back
9-  exit terminal mode
10- power cycle the KVM
```

Select any of the options, by typing the number on the keyboard.

Make sure NOT to use the keyboard's numeric pad; it does not work. Only the main keyboard numbers work.

NOTE:

- **To get out of Admin mode, type 8 (as seen in the menu above) or power cycle the KVM switch.**
- **As long as the unit is in Admin mode, keystrokes are not sent to the target computer.**

Terminal Mode Operation

Once authenticated the following menu will be presented:
“Authentication succeeded. Please select operation…

0 – Asset Management

Change the USB parameters that the KVM switch uses to identify itself to the connected computer. The options are:

- **1- use standard descriptor as asset container**
- **2- use custom descriptor as asset container**
- **3- enter new asset tag**
- **4- show current asset tag**
- **5- apply asset tag to de**
- **8- back**
- **10- exit terminal mode**

1 - Firmware Versions

Check the different firmware versions that are loaded on the different controllers of the KVM switch. The firmware-version options are:

- **1- de version**
- **2- sc version**
- **3- vc version**
- **4- dpp version**
- **8- back**
- **9- exit terminal mode**

2 - Configure DPP (if equipped)

Configure and change the devices that are allowed through the DPP (dedicated peripheral port). This is the CAC port.

By default, all authentication devices and only authentication devices are allowed. You can also use a tool that gives you for more functionality. The options are:

- **1- allow currently connected device on all channels**
- **2- block currently connected device on all channels**
- **3- show currently connected device**
- **4- show currently approved device**
- **5- show currently blocked device**
- **6- reset dpp settings**
- **7- upload dpp settings from the host**
- **8- back**
- **9- exit terminal**

3 - Configure SC (allows configuration of KM functionality)

Configure and change the SC (system controller) settings.

The options are:

- **1- enter desktop configuration [0-40] [default=0]**
- **2- enter mouse speed [0-32] [default=5]**
- **3- upload configuration from the host**
- **4 - use ctrl key as shortcut prefix**
- **5- use alt key as shortcut prefix**
- **6- guard mode configuration**

3 - Configure SC (cont.)

Terminal Mode Operation

3 - Configure SC (cont.)

7- rgb fp configuration

8- back

9- exit terminal mode

Option 7 – RGB Front Panel Configuration. On choosing this option a new menu will appear with the following options:

1- Upload FP configuration from a host

2- Select Colors for Channels

8- Back

9- Exit terminal mode

On choosing option 1 - the user can upload an external file with RGB configuration.

Option 2 opens a dialog where user will enter his choices as follows:

1. Select a channel [1..4] (*or 1-8 in 8 Port units) or press esc to go back

2. Select a color. Please select operation:

l- Blue

2- Red

3- Green

4 - Yellow

5 - Purple

8 - Back

9 - Exit terminal mode

4 - Account Management

Manage, add, and remove administrator accounts. The options are:

1- change password

2- create admin account

3- delete all accounts

8- back

9- exit terminal mode

Up to nine additional administrator accounts may be created. The additional accounts can be removed or renamed by the admin and will be deleted during RFD.

Additional administrators' usernames must be 5 to 11 characters long, and must contain:

i. Uppercase letters

ii. Lowercase letters

5 - Reset to Factory Defaults

Reset the device to factory default.

NOTE: Although this is a complete reset, it does not reset the main Admin user and the OTP log.

Terminal Mode Operation

6 - Logs and Events

The options are:

1- **show otp log**
2- **show ram log**
3- **show non-critical RAM log**
8- **back**
9- **exit terminal**

Under logs and events, all information defined as critical and sensitive is saved. There are two types of logs on the KVM switches:

- The OTP log:
  Its information is never deleted, not even during the RFD. This log keeps date, time and username of all the events that defined as critical, such as: self-test failures, peripheral device rejection, tampering event, DPP configuration changes, RFD, admin password change.

  These events are never deleted from the log.

- The RAM log:
  Its information is never deleted, not even during theRFD. The events kept on this log are events like power up, peripheral device acceptance, simple configuration change, Admin logon, user add/delete, password change or password lock, and so on. The RAM log stores up to 100 latest events and deletes the oldest ones when it is full.

- The Non-Critical RAM log:
  Its information is never deleted, not even during the RFD. The events kept on this log are events like power up, peripheral device acceptance, simple configuration change, Admin logon, user add/delete, password change or password lock, and so on. The RAM log stores up to 128 latest events, and deletes the oldest ones when it is full.

7 - Configure Peripheral Devices

Manage the peripheral devices options:

1- **Toggle Touch support – add/remove touch device interface from DE**
2- **Toggle Consumer (keyboard) support - add\ remove consumer device interface from DE**
3- **Add/Remove an ABS mouse interface to/from DE**
4- **Add/Remove Copy/Paste (for standard units only) - per active channel (not on secure devices)**
5- **Video Follow Mouse**
8- **Back**
9- **Exit terminal**

Any of the above changes might require up to 10 sec. to be applied on the device.

External Configuration Tool

You have the option of using an external configuration tool. It lets you configure:

- **DPP**
- **Presets**

Terminal Mode Operation

Important Anti-Tamper Indications:

This product has tamper-evident security tape that will provide visual indication of attempts to open the enclosure. Further, the product is equipped with an always-on active anti-tamper mechanism. Any attempt to open the enclosure will activate the anti-tamper trigger and render the unit permanently inoperable.

If the product's anti-tamper security tape appears disrupted or if all the channel LEDs flash continuously, do not install the unit and call Belkin Technical support at +1 (800) 282-2355 belkin