Belkin Administrator Guide

Products covered by this manual:
Belkin Secure KVM, KM, and Windowing KVM

Doc No: HDC10957
Rev: F

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, 11 June 2015
B – Modified Description of log events & User Guidance Updates, 16 June 2015
C – Added Section on Admin Logon, 13 August 2015
D – Terminal Mode description and clarity on menu choices, 15 February 2018
E – Grammar and Spelling edits, 18 April 2018
F - Minor Changes 30 May 2018

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 logon events can be verified.

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 DCU. Only the optional Belkin supplied desktop controller unit can be used with this port.

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

The product only maintains a log of security-related functions that can be configured. Logs can be viewed only by authenticated administrators.
Note that the one-time-programmable (OTP) log data may not be erased, and the log function may not be disabled by users or administrators.

Also note that the unit ships with a default (root) admin account and requires that the default password be changed upon first boot. Additional admin accounts can be created by the root administrator; however, an RFD will delete these accounts. Root admin account and new password will not be affected by an RFD.

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.

Note:

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

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.

Administrator Setup

a. 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.

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

c. Using keyboard, type **CTRL (Left), CTRL (Right), t** to enter **Admin Mode.**
d. Text will appear in Notepad asking for a user name.
e. The default user name is: "**admin1234"**. This account ID cannot be changed or deleted.
f. The default first device logon password is: "**1234ABCDefg!@#**"

g. **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.

h. Password must be typed twice to confirm.
i. Password may be changed at any time.
j. RFD will not reset the user name and password!
k. If the user name or password is forgotten – contact Belkin support.

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

Terminal Mode Operation

Once authenticated the following menu will be presented:

“Authentication succeeded. Please select operation...

0 - asset management

1 - firmware versions

2 - configure dpp (inoperable – used only in production)

3 - configure sc (allows configuration of KM functionality)

4 - account management

5 - reset to factory defaults

6 - logs and events

8 - back

9 - exit terminal mode

The administartor will be able to select any of the options by selecting the number on the keyboard (note that the keypad is disabled).

User can exit out of Admin mode but remain as an authenticated administrator by selecting 9 as seen in the above menu. However, to exit authenticated administrator mode, unit must be power cycled.

Important: Power cycle the unit after completing administrative tasks to exit configuration mode.

Note: As long as the unit is in Admin mode key strokes will not be sent to the target computer.

Note: Selection #2 is used during the production process to activate the unit. This has no function post production. Item #3 (SC Configuration) is used to configure Keyboard/Mouse (KM) functions for units that are programmed to be a KM switch and should not be used for KVM switches.

Asset Management (0)

The asset management section allows the administrator to change the USB parameters that the KVM switch will use to identify itself to to an asset tracking system.
Administrators can select to use a standard descriptor, a custom descriptor, enter a new asset tag, display the asset tag, or apply the asset tag.

Firmware Versions (1)

The firmware versions sections allows the administrator to check the different firmware versions loaded on the different controllers of the KVM switch. Administrators can check the Device Emulator (de) version, System Controller (sc) version, or CAC controller (dpp) version. “vc” is reserved for production use only and has no function once unit has been produced.

Account Management (4)

Add and remove administrators as well as change passwords. Account user IDs require 1 capital, 1 lower case, and 1 numeral. Passwords must be between 8 and 24 characters long and contain at least 1 capital, 1 lower case, 1 number, and one symbol. When deleting accounts, power cycle the unit before adding new accounts.

Reset to Factory Defaults (5)

Reset the device to factory default. This is a complete reset that will not reset the root Admin user name and password, and the log. It will delete all secondary admin accounts and passwords as well as reset configurable functions to factory defaults.

Logs and Events (6)

Logs consist of critical and non-critical information. Unit logs those aspects deemed by NIAP as impacting the security aspects of the product. As the Belkin secure peripheral switches are strictly restricted in their flexibility to minimize the attack surface,

1. Critical Log Information (OTP): stores and presents the following information:
    a. Administrator account creation events
    b. Password Change events
2. RAM Log
    a. Held in volatile memory that will over-write itself and delete upon power cycling.
    b. Information on USB peripheral rejection events, failed log-on events

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