Belkin Administrator Guide

Products covered by this manual:

Belkin Secure Products

Doc No.: HDC10957
Rev.: C

Table of Contents

Introduction

This Administrator Guide provides all the details you'll need to receive log and audit data from your new product.
This Administrator Guide provides all the details required to manage this function.

Important note before deploying the product:

In order to comply with the product's Common Criteria evaluation and in order to prevent unauthorized administrative access to the product, the default administrator user name and password must be changed prior to first product use.

Refer to the product Administrator Guide for further details.

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 at the following e-mail address: **gov_security@belkin.com**

Important: This product is equipped with an always-on active anti-tamper system. Any attempt to open the enclosure may activate the anti-tamper system and render the unit permanently inoperable. If the unit's enclosure appears disrupted or if all the port LEDs flash continuously, please call Belkin Technical Support at **1 (800) 282-2355**

Intended Audience

This document is intended for the following professionals:

- System Administrators/IT Managers

Revision

A – Initial Release, 11 June 2015

B – Detailed textual description of log events and User Guidance updates, 16 June 2015

C – Added Section on Admin Logon, 13 August, 2015

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 checked 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 user'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 damage 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 carefully before using the product:

1. As product powers-up it performs a self-test procedure. In case of self- test failure for any reason, including jammed buttons, the product will be Inoperable. Self-test failure will be indicated by the following abnormal LED behavior:
    a. All channel-select LEDs will be turned ON and then OFF;
    b. A specific, predefined LED combination will be turned ON;
    c. The predefined LED combination will indicate the problem type (jammed buttons, firmware integrity).

    Try to power cycle product. If problem persists please contact your system administrator or technical support.

2. Product power-up and RFD behavior:
    a. By default, after product power-up, the active channel will be computer #1, indicated by the applicable front panel push button LED lit.
    b. Product Restore-to-Factory-Default (RFD) function is available via a physical control button on rear panel. Use a sharp object or paper clip to hold RFD button pressed for several seconds to initiate an RFD action.
    c. RFD action will be indicated by front panel LEDs blinking all together.
    d. When product boots after RFD, 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 this User Manual's appropriate sections. Do not connect any authentication device with an external power source to product.

4. For security reasons products do not support wireless keyboards and mice. In any case do not connect wireless keyboard/mouse to product.

5. For security reasons products do not support microphone/line-in audio input. In any case do not connect a microphone to product audio output port, including headsets.

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

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 using the keyboard.
    b. When connecting a non-qualified mouse, the mouse will be non-functional with mouse cursor frozen on screen.

Important: For change management tracking, it is advised to perform a quarterly log check to verify that RFD was not improperly used to override the current device policy by an unauthorized person.

   c. When connecting a non-qualified display, the video diagnostic LED will flash green and video will not work.
   d. When connecting a non-qualified USB device, CAC LED will flash green and USB device 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. Product has a remote control port in the back panel labeled RCU. Do not use this port - it is inoperable and for future use.

10. Important! Before re-allocating computers to channels, it is mandatory to power cycle product, keeping it powered OFF for more than 1 minute.

11. Product log access and administrator configuration options are described in product Administrator Guide.

12. Authentication session will be terminated once product power is down or user intentionally terminates session.

13. If you are aware of any potential security vulnerability while installing or operating product, please remove product from service immediately and contact us in one of the ways listed in this manual.

Reporting Belkin Product Security Vulnerability.

If you are aware of potential security vulnerability with any Belkin Government product, we encourage you to contact us immediately at the following email address: **gov_security@belkin.com** or our technical support line at: TOLL FREE **1-800-282-2355**

After your communication is received, Belkin Government personnel will contact you to follow up. To ensure confidentiality, Belkin encourages you to use our PGP encryption key.

The **gov_security@belkin.com** email address is not intended to reach technical support on Belkin Government products or services.

Administrator Configuration

The product enables authorized administrators to download event log file and audit product history. This function is available only to authenticated administrators.

Note that the log data may not be erased and log function may not be disabled by users or administrators.

Important note before deploying the product:

In order to comply with the product's Common Criteria evaluation and in order to prevent unauthorized administrative access to the product, the default administrator user name and password must be changed prior to first product use.

Refer to the product Administrator Guide for further details.

Administrator Setup

a. The default first device logon password is: "1234ABCDefg!@#"
b. At first logon define an administrator account user name. The name must be typed twice for confirmation, include at least 4 characters made of letters and numbers only (special keys are not supported).
c. At first logon the administrator must also set a new, non-default, password.
The new password must be at least:

i. 8 characters long but not longer than 24 characters;
ii. Have at least one capital and one small letter
iii. Have at least one number;
iv. Have at least one symbol.

d. Password must be typed twice to confirm.
e. Password may be changed at any time.
f. RFD will not reset the user name and password!
g. If the password or user are forgotten – contact Belkin support.
h. After 3 failed logon attempts the device admin console will be inaccessible for 15 minutes.
i. After 9 failed logon attempts the device admin console will be permanently locked. Call Belkin support for assistance.
j. Additional administrative user accounts can be created from the terminal menu (up to 9 per switch).

Administrator Setup

a. Connect keyboard, mouse, and one KM cable to computer and power up the product. Note that display may or may not be connected through the products.
b. Open Notepad or any other text editor in the connected computer.
c. Use keyboard and type **CTRL (Left), CTRL (Right), T** to enter **Admin Mode.** Product shall respond by: [sc] authentication done.
d. Type your administrator user name and password to login and press Enter.
e. Type the following command: **DL_FL** to dump Log File into Notepad.

The various events' data available from Log file is described in the following image:

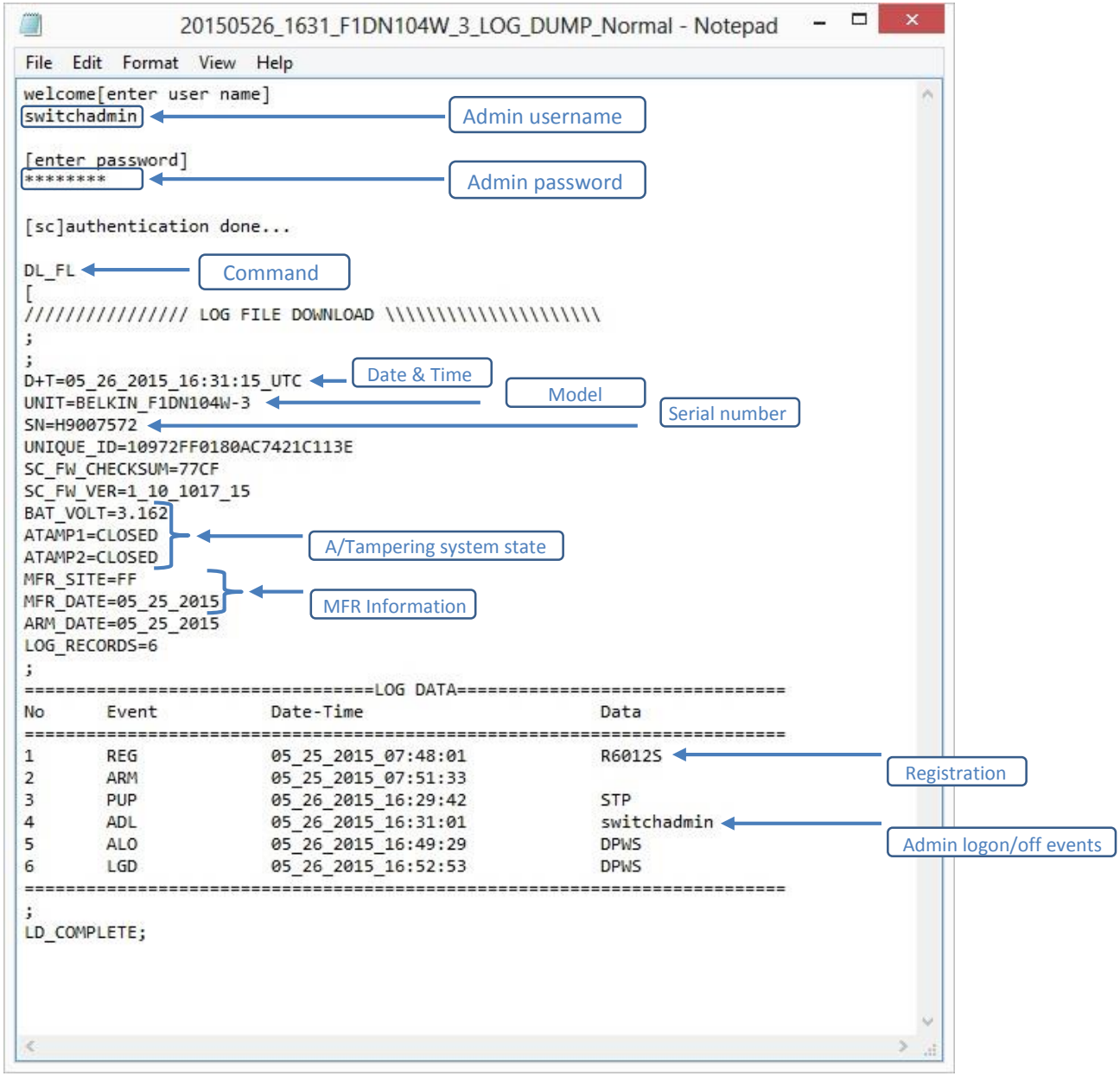

Figure 1: Authenticated Admin Event Log Report derived from product

The information provided by this dump file is explained in the following tables:

Header fields information

Title	Description	Note
D+T=	Date and time (UTC) when the dump file was downloaded	Time and date are set during production
UNIT=	Product manufacturer and model	
SN=	Product serial number	
INIQUE_ID=	ROM based identification string from controller silicon	Can be used to identify dead product
SC_FW_CHECKSUM=	System Controller firmware checksum	Used to verify the integrity of the SC firmware
SC_FW_VERSION=	System Controller firmware version number	
BAT_VOLT=	Anti-tampering battery voltage	Measured once per 24 hours. Minimum value is 2.450V.
		Nominal value is 3.200V
ATAMP1=	The status of the left side anti-tampering switch	Normally this switch must be closed. If it is opened – product is tampered
ATAMP2=	The status of the right side anti-tampering switch	Normally this switch must be closed. If it is opened – product is tampered
MFR_SITE=	Product manufacturing site code	
MFR_DATE=	Product manufacturing date (UTC)	
ARM_DATE=	Product anti-tampering arming date (UTC)	
LOG_RECORDS=	The number of log lines in product memory	

Log data lines information

Data fields can be decoded by the manufacturer.

1. **Critical log area -** This log area stores the following data in fixed structure:
   a. The product registration information (once during production);
   b. The anti-tampering arming event (once during production);
   c. Tampering events detected (may be up to 6 possible event flags, each with data and time);
   d. The last admin log-on information (one event); and
   e. The last self-test failure information (one event with error codes).

2. **Non-critical log area -** This log area holds a maximum of 32 lines of data. Every new event will delete the oldest line. This area holds the following data:

   a. Administrator log in and changes made,
   b. Changes in administrator password,
   c. Rejection of USB devices,
   d. Self-test failures,
   e. CDF (black-list / white-list) and traffic rules uploading, and
   f. Power up and down cycles.

Reporting Belkin Product Security Vulnerability.

If you are aware of potential security vulnerability with any Belkin Government product, we encourage you to contact us immediately at the following email address: **gov_security@belkin.com** or our technical support line at: TOLL FREE **1-800-282-2355**

After your communication is received, Belkin Government personnel will contact you to follow up. To ensure confidentiality, Belkin encourages you to use our PGP encryption key.

The **gov_security@belkin.com** email address is not intended to reach technical support on Belkin Government products or services.

COPYRIGHT AND LEGAL NOTICE

Windows, Windows Vista, Microsoft, and IntelliMouse are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Mac OS and Mac are trademarks of Apple Inc., registered in the U.S. and other countries.

belkinbusiness.com

The information and specifications in this document are subject to change without prior notice.

Images are for demonstration purposes only.