# Vertiv™ Cybex™ SC/SCM Switching System Additional Operations and Configuration

Technical Bulletin

**Technical Support Site**

If you encounter any installation or operational issues with your product, check the pertinent section of this manual to see if the issue can be resolved by following outlined procedures. For additional assistance, visit https://www.VertivCo.com/en-us/support/

# TABLE OF CONTENTS

# 1 INTRODUCTION

The Vertiv™ Cybex™ High Performance Secure Desktop Matrix switch can be configured to enable dedicated peripheral port (DPP) functionality and send log and audit data to the administrator. The DPP feature can be managed via the configurable device filtering (CDF) feature and configuration permissions limited to authenticated administrators. This document provides system administrators and IT managers the information necessary to enable and manage these features on any qualified switch.

**WARNING! This product is equipped with active intrusion protection and tamper-evident seals. Tampering with the switch or breaking/removing the seals permanently disables it and voids the warranty. If the enclosure appears to be tampered with or if all the port LEDs flash continuously, contact Technical Support.**

This page intentionally left blank.

# 2 USB DEVICE CONFIGURATION UTILITY

The switch supports authorized USB devices such as smart card readers or common access card (CAC) readers. USB devices are plugged into the console DPP port. By default, authentication devices are authorized for use; however, only authenticated administrators can authorize additional USB devices through the CDF feature and configuration permissions.

The CDF feature allows administrators to create lists of allowed and blocked devices, which are referred to as the white list and black list, respectively. You can also assign authorized USB devices to specific computers and create policy rules based on the USB device's class, sub-class, protocol, vendor id (VID), product ID (PID) and serial number.

### 2.0.1 Installing the UCU on a management computer

Before you can access the CDF feature to configure or manage USB device policies, you must download and install the USB device Configuration Utility (UCU) on a designated management computer. The management computer can be a laptop or desktop and must be equipped with at least Microsoft® Windows® XP to run the UCU.

To install the UCU:

1. From the Vertiv web site, access the Software Downloads section and download the UCU onto a management computer.

   -or-

   Contact Technical Support.

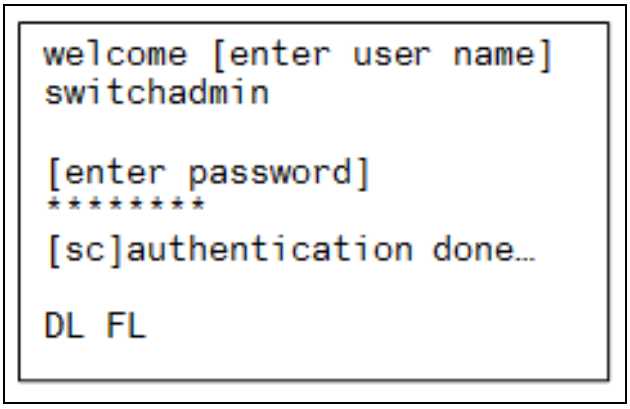
2. Launch the UCU installation wizard and follow the provided instructions.

### 2.0.2 Connecting the management computer to the switch

To connect the management computer to the switch:

1. Using a USB Type-A and B cable, connect the A side of the cable to the management computer and the B side to the appropriate channel port on the switch.
2. Using the channel select LED buttons, switch to the channel to be configured.
3. Log in as administrator.

**Figure 1.1 Administrator Log-in Terminal**




## 2.1 Launching the UCU User Interface

After downloading and installing the UCU to the management computer and connecting the management computer to the switch, you can launch the UCU user interface. The following figure and table include the UCU user interface sections and each item's description.

Figure 1.2 UCU User Interface

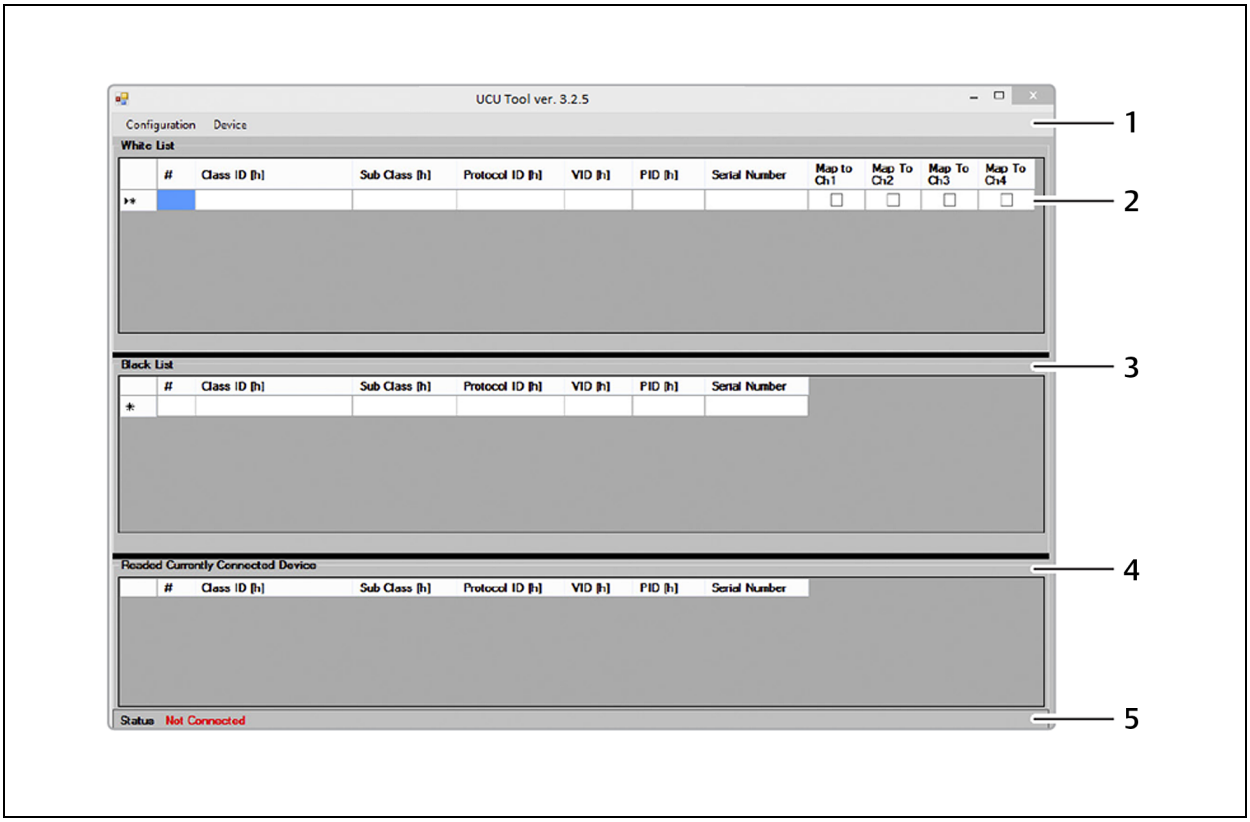



Table 1.1 UCU Interface Sections

| ITEM | NAME | DESCRIPTION |
|---|---|---|
| 1 | Command bar | Enables you to perform system commands. |
| 2 | White list rules | Displays a list of authorized devices using OR relationship rules. |
| 3 | Black list rules | Displays a list of unauthorized blocked devices using OR relationship rules. |
| 4 | Read bar | Displays the attributes of the currently connected device upon request. |
| 5 | Status bar | Displays the connection status of the USB switch and the UCU. |

**NOTE: Black list rules established for blocked devices always supersede white list rules established for authorized devices.**

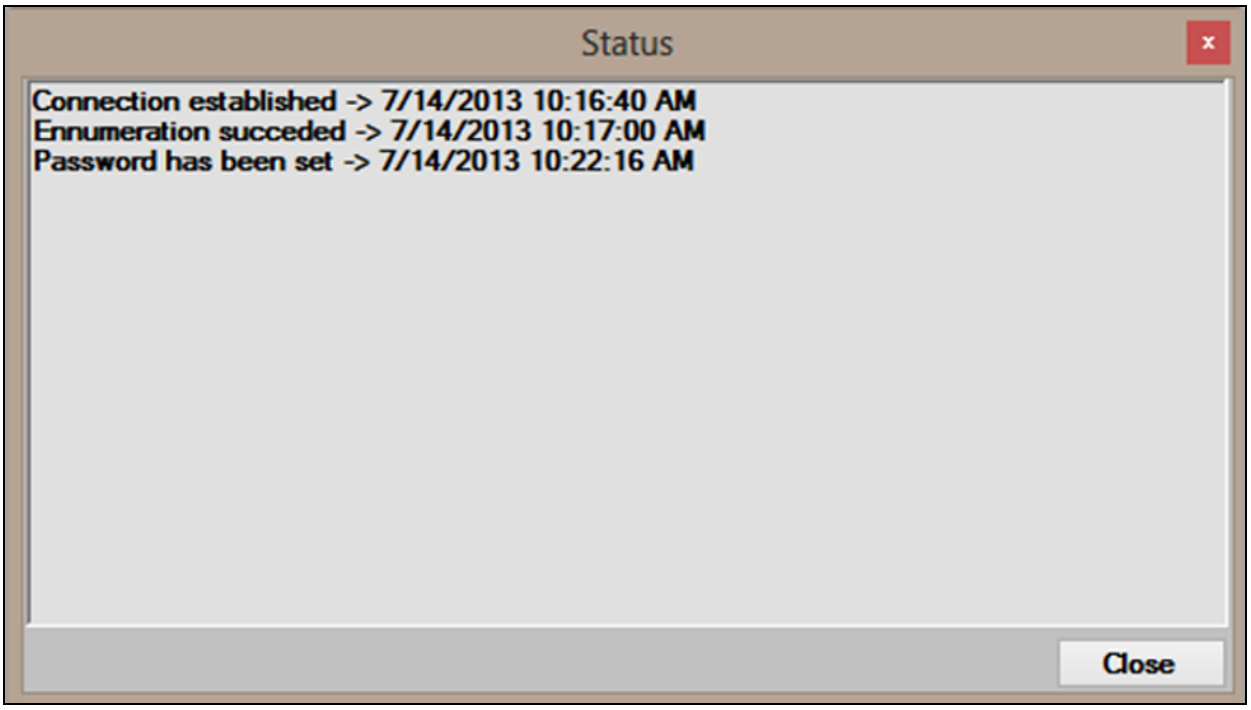
The status bar indicates if the switch is connected to the management computer. It displays one of two statuses:

- Not Connected - If the UCU is not communicating with the switch or if the administrator is not logged on and the switch is not in administrator mode, this status is red.
- Connected/Access Granted - If the UCU is communicating with the switch and the switch is in administrator mode, this status is green.

### To view connection status details:

In the UCU interface window, click *Connection Status* to display a Status window.

Figure 1.3 Status Window



This page intentionally left blank.

# 3 CONFIGURING DEVICE RULES

You can create device policies through the UCU by reading the attributes from the connected USB device to generate white and black list rules. You can also manually select attributes to customize white and black list rules. Rules can be created based on the device's class, sub-class, protocol, vendor id (VID), product ID (PID) and serial number. Each configuration supports up to 16 rules each for the white list and black list.

### To read attributes from a USB device:

1. On the switch's back panel, connect the USB device to the console DPP port.
2. In the UCU interface, click *Device - Read* to display a list of the USB device attributes that appear in the Currently Connected Device window.
3. To add an attribute to the white list, right-click the attribute and select *Add To White List* from the drop-down menu.

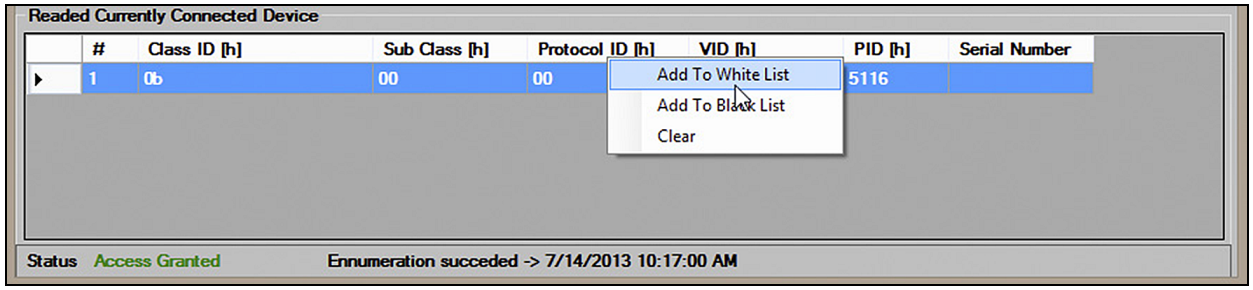
   -or-

   To add an attribute to the black list, right-click the attribute and select *Add To Black list* from the drop-down menu.

   -or-

   To delete the attribute, right-click the attribute and select *Clear* from the drop-down menu.

**Figure 2.1 Currently Connected Device Window and Drop-down Menu**




4. Repeat for every USB device to be configured.

### To manually define attributes for a USB device:

1. Scroll to the White List or Black List section of the UCU interface.
2. Double-click a field to open a complete list of possible attributes and click to select an attribute.

   -or-

   Click to select a field and enter the value of the attribute in the field.

**NOTE: All fields must be completed. Entering * in a field indicates that any value is acceptable and entering * after a value indicates a wild card.**

## 3.1 Loading Configurations

After the configuration is defined, it must be loaded onto the switch.

### To load the configuration:

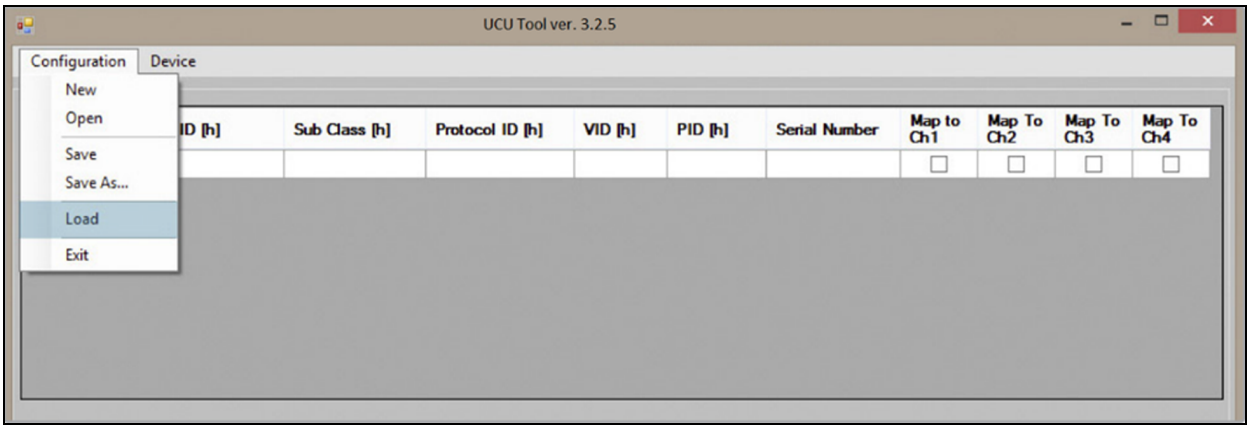
1. In the command bar, click *Configuration - Load*.

**NOTE: When the load command is received, the switch LED status turns off.**

2. Disconnect and reconnect the power supply cable to restart the switch and apply the new configuration.

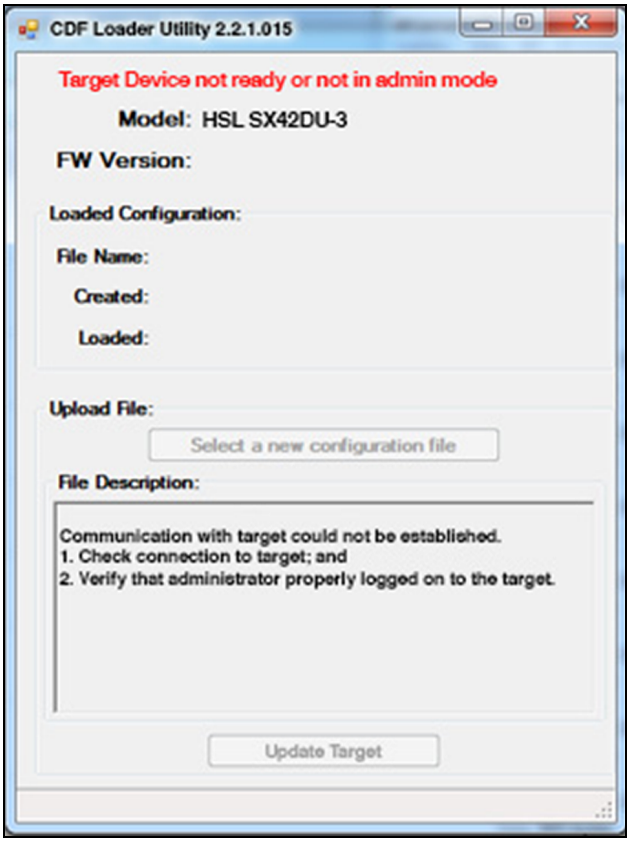
**NOTE: You cannot view a current configuration after it is loaded on the switch. You can only open, edit and re-load previously saved configurations.**

Figure 2.2 UCU Tool Configuration




Ensure the management computer is connected to the switch and you are logged on as administrator. If you are not logged in as administrator, a loader utility error message appears.

Figure 2.3 Loader Utility Error Message



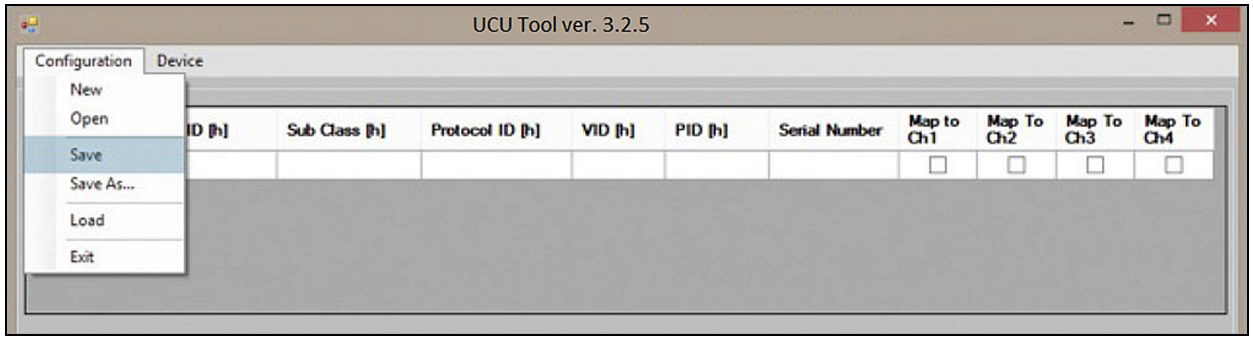

## 3.2 Saving Configurations

Defined configurations can be saved to a file and later edited or loaded onto a connected target that is in administrator mode. Configuration files are saved to the management computer through the UCU.

To save a configuration:

1. In the UCU command bar, click *Configuration - Save As*.
2. In the Save As window, browse to the directory where the file will be saved.
3. In the File Name field, enter the name of the file and click *Save*.

**Figure 2.4 Saving a Configuration**




To open, edit or load a saved configuration:

1. In the UCU command bar, click *Configuration - Open*.
2. Browse and select the directory containing the saved configuration file and click *Open*.
3. Update the configuration settings in the White List and Black List sections and click *Configuration - Save*.

   -or-

   Connect the switch to the management computer and load the configuration onto the switch.

## 3.3 Configuration Examples

Before implementing the example procedures, ensure the switch is connected to the management PC and the UCU is communicating with the switch. You must be logged in as administrator to properly communicate with the target device. The following procedures provide steps for creating and testing a white list and black list rule.

### 3.3.1 Creating and testing a white list rule

The steps in the following example procedures enable you to add a rule to the white list that allows you to map a USB flash device to computer 3 and verify the rule is successfully added.

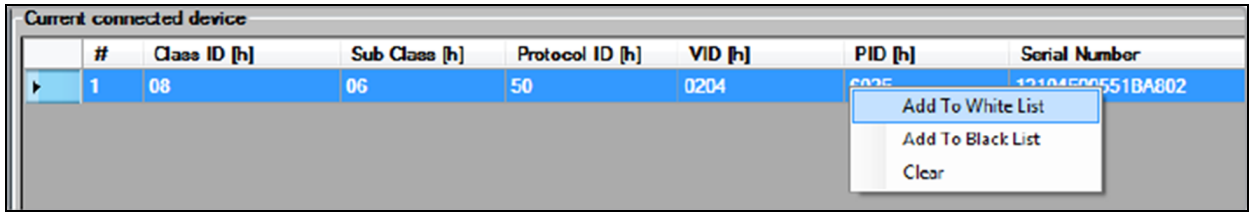
To add a white list rule for mapping a USB flash drive to computer 3:

1. Connect the USB flash drive to the switch's DPP port.

**NOTE: The USB status LED illuminates red because the USB mapping is prohibited at this point.**

2. In the UCU command bar, click *Device - Read* to display the USB device attributes in the Currently Connected Device pane.
3. In the White list section, right-click on each attribute, select *Add To White List* from the drop-down menu and select the Map to Ch3 checkbox.

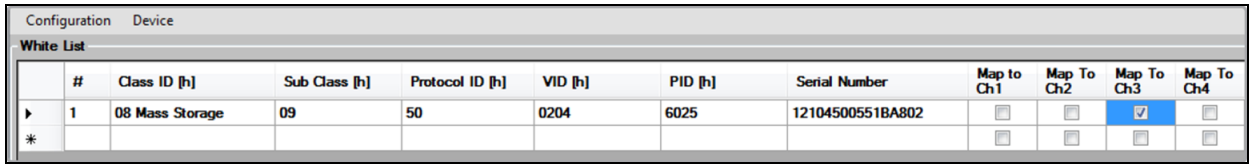
**Figure 2.5 Current Connected Device**



4. In the UCU command bar, click *Configuration - Load*.

**NOTE: The USB status LED will blink and turn off to indicate the new settings are stored.**

**Figure 2.6 White List**




5. Disconnect the USB cable and turn the switch's power off and on.

### To verify the white list rule is added:

1. Verify the USB status LED illuminates green to indicate the connected USB flash drive is approved.
2. Using the front panel channel select LED button, select channel 3 and verify the attached USB flash drive is mapped to computer 3.
3. Select channels 1, 2 and 4 and verify the attached USB flash drive is not mapped to computers 1, 2 or 4.

## 3.3.2 Creating and testing a black list rule

The steps in the following example procedures enable you to add a rule to the black list that allows you to block USB flash devices to any computer and verify the rule is successfully added.

### To add a black list rule to block USB flash drives on all computers:

1. Connect the USB flash drive to the switch's DPP port.

**NOTE: The USB status LED illuminates red since USB mapping is prohibited at this point.**

2. In the UCU command bar, click *Device - Read* to display the USB device attributes in the Currently Connected Device pane.
3. In the Black list section, right-click on each attribute and select *Add To Black List* from the drop-down menu.
4. In the UCU command bar, click *Configuration - Load*.
5. Disconnect the USB cable and turn the switch's power off and on.

### To verify the black list rule is added:

1. Verify the USB status LED illuminates red to indicate the connected USB flash drive is blocked and the channel LED indicators are turned off to indicate the connected USB flash drive is prohibited.
2. Using the front panel channel select LED button, select each channel and verify the USB flash drive is blocked on all channels.

**NOTE: The USB flash drive is blocked on channel 3 because the black list rules override white list rules.**

# 4 ADMINISTRATOR CONFIGURATION

The switch allows authenticated administrators to download event log files and audit histories. Log functions cannot be disabled and log data cannot be erased by users or administrators. You must set up an administrator username and password and log in to the account to view event logs and audit histories.

## 4.1 Administrator Setup

The default username is admin1234 and the default password is 1234ABCDefg!@#. You can use the default credentials to log in to the switch and change the username and password. When creating a new username and password, adhere to the following criteria:

- The username must be at least four characters in length and composed of letters and numbers only. Special characters are not supported for the username. For confirmation, the username must be entered twice.
- The new password must be at least eight characters in length but no longer than 24 characters, and contain at least one capital and one lowercase letter, one number and one symbol. For confirmation, the password must be entered twice.

**NOTE: The password can be changed at any time and resetting the switch to factory default settings does not reset the username or password.**

When logging in, you are allowed three failed attempts. After three failed attempts, the administrator console is inaccessible for 15 minutes. After nine failed log-in attempts, the administrator console is permanently locked and you must contact Technical Support for assistance.

From the terminal menu, you can create up to nine additional administrator accounts per switch.

## 4.2 Administrator Log-in

You must log in to the switch as an administrator to have access to event logs, audit histories and the UCU. See USB Device Configuration Utility on page 3 for more information about the UCU. Before logging in, ensure the computer is connected to a keyboard and mouse and that the switch and computer are turned on. The following figure and table include items that appear in the terminal window and each item's description.

Figure 3.1 Authenticated Administrator Event Log Report

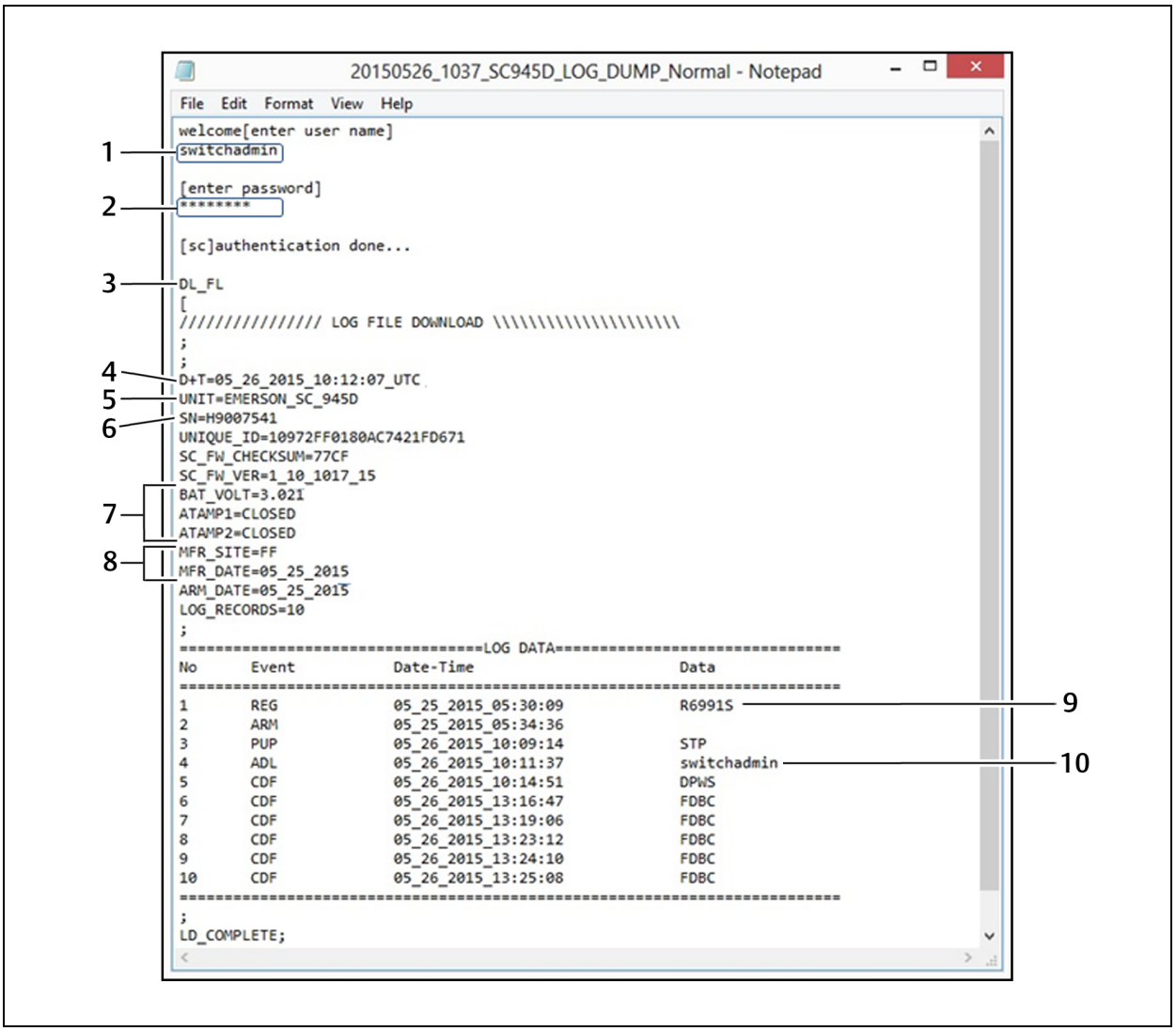



Table 3.1 Administrator Report Items

| ITEM | DESCRIPTION |
|---|---|
| 1 | Administrator username. |
| 2 | Administrator password. |
| 3 | Command to dump the log files into Notepad. |
| 4 | Date and time of the administrator's log-in in Coordinated Universal Time (UTC) format. |
| 5 | Switch's model number. |
| 6 | Switch's serial number. |
| 7 | Anti-tampering system state to indicate if the switch was compromised. |
| 8 | Manufacturer information including manufactured date (MFR date) and anti-tampering system arming (ARM) date. |
| 9 | Registration information. |
| 10 | Administrator account that is logged in and the time and date of the log in. |

To log on as an administrator:

1. Open Microsoft® Notepad or any other text editor on the connected computer.
2. Enter L CTRL+R CTRL+T to access admin mode.
3. Enter the administrator username and password.
4. In the terminal, enter DL_FL to dump the log file into Notepad.

The following table includes the fields that are displayed in the data log file dump and each item's description:

**Table 3.2 Data Log File Fields**

| FIELD NAME | DESCRIPTION | NOTE |
|---|---|---|
| T+D= | Date and time (in UTC format) when the dump file was downloaded. | The time and date are set during production. |
| UNIT= | Switch's manufacturer and model number. | N/A |
| SN= | Switch's serial number. | N/A |
| UNIQUE_ID= | ROM based identification string from controller silicon. | The identification string can be used to identify inactive or dead products. |
| SC_FW_CHECKSUM= | System controller firmware checksum. | Verifies the integrity of the SC firmware. |
| SC_FW_VERSION= | System controller firmware version number. | N/A |
| BAT_VOLT= | Anti-tampering battery voltage. | The battery voltage is measured once every 24 hours. The minimum voltage is 2.45 Volts (V). The nominal value is 3.2 V. |
| ATAMP1= | Status of the left anti-tampering switch. | The switch is closed by default. If the switch is open, the product has been tampered with. |
| ATAMP2= | Status of the right anti-tampering switch. | The switch is closed by default. If the switch is open, the product has been tampered with. |
| MFR_SITE= | Switch's manufacturing site code. | N/A |
| MFR_DATE= | Switch's manufacturing date. | N/A |
| ARM_DATE= | Switch's anti-tampering arming date. | N/A |
| LOG_RECORDS= | Number of log lines in the switch's memory. | N/A |

## 4.3 Log Data Information

Log data is categorized into two types: Critical and non-critical. Critical and non-critical information appears in the designated log area.

The following information appears in the critical log area:

- Product registration information
- Anti-tampering arming event
- Tampering events detected (up to six possible events with date and time information)
- Last administrator log-in
- Last self-test failure information including error codes

The non-critical log area can display up to 32 lines of data. As new events are created, the oldest event is deleted to display the newest event. The following information appears in the non-critical log area:

- Administrator log-in with changes
- Changes to the administrator password
- Rejected USB devices
- Self-test failures
- Black list and white list information
- Power on and off cycles

This page intentionally left blank.

VertivCo.com | Vertiv Headquarters, 1050 Dearborn Drive, Columbus, OH, 43085, USA

© 2017 Vertiv Co. All rights reserved. Vertiv and the Vertiv logo are trademarks or registered trademarks of Vertiv Co. All other names and logos referred to are trade names, trademarks or registered trademarks of their respective owners. While every precaution has been taken to ensure accuracy and completeness herein, Vertiv Co. assumes no responsibility, and disclaims all liability, for damages resulting from use of this information or for any errors or omissions. Specifications are subject to change without notice.

590-1741-501A