VERTIV

VERTIV DPP Configuration Utility Manual

Products covered by this manual:
Secure KVMs, KMs, Mini Matrixes
and Multi Viewers having DPP port

Doc No.: HDC10955
Rev.: D

Table of Contents

Introduction

This User Manual provides all the details you'll need to configure DPP functionality of your new product. The DPP feature can be managed via Configurable Device Filtering (CDF) mechanism with configuration permissions limited to authenticated administrators. This Configuration Manual provides all the details required to manage and configure 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 potential security vulnerability while installing or operating this product, we encourage you to contact us immediately in one of the following ways:

- Email: Secure@VertivCo.com
- Tel: +1-888-793-8763

Important: 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.

Intended Audience

This document is intended for the following professionals:

- System Administrators/IT Managers

Revision

A – Initial Release, 11 June 2015

B – Updated User Guidance, 21 June 2015

C – Updated for NIAP evaluation, January 28, 2016

D – Changing to VERTIV new branding, 20 May 2019

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 except for administrator credentials and log information.
   e. After RFD, the product will revert to FDF (Fixed Device Filtration) restrictive fUSB mode – in this mode enables only smart-card reader USB devices to connect to the product.

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.

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.

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.
    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, DPP 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.

Before Installation

Unpacking the Product

Before opening the product packaging, inspect the packaging condition to assure that product was not damaged during delivery.

When opening the package, inspect that the product Tamper Evident Labels are intact.

Important:

1. If the unit's enclosure appears disrupted or if all channel-select LEDs flash continuously, please remove product from service immediately and contact Technical Support at:
   http://www.VertivCo.com

2. 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.

Where to locate the Product?

The enclosure of the product is designed for desktop or under the table configurations. An optional Mount Kit is available.

Product must be located in a secure and well protected environment to prevent potential attacker access.

Consider the following when deciding where to place product:

- Product front panel must be visible to the user at all times.
- The location of the computers in relation to the product and the length of available cables (typically 1.8 m)

Warning: Avoid placing cables near fluorescent lights, air-conditioning equipment, RF equipment or machines that create electrical noise (e.g., vacuum cleaners).

User Default Active Channel & Switching

- By default, after product power-up, the active channel will be computer #1, indicated by the applicable front panel push button LED lit. In case only some of the channels operate with a USB device, it is recommended to make sure computer #1 is connected to USB device.
- Once the user switches channels, for example to channel #3, DPP functionality will move to computer #3 and be indicated by channel #3 DPP LED turning steady green.
- In case user switches to a channel that is not connected to a USB device, the previous USB connection will be terminated and no new connection will be established. No DPP LED will be lit in this case.

User Freeze DPP Functionality

- In case "Freeze DPP" slider was moved to activate DPP function for computer #1, for example, switching to a different channel would keep DPP function locked to channel #1.
- To release "Freeze DPP" function from channel #1, the user will need to move the "Freeze DPP" slider again to its original position. The release will be indicated by the channel #1 DPP LED being turned off.

User Restore Factory Default (RFD) Behavior

- 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.
- RFD action will be indicated by front panel LEDs blinking all together.
- 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.
- In case Restore-to-Default was performed while "Freeze DPP" slider was activated on a specific channel, after boot up this function will be locked to computer #1.

User Session Termination

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

Administrator Configuration

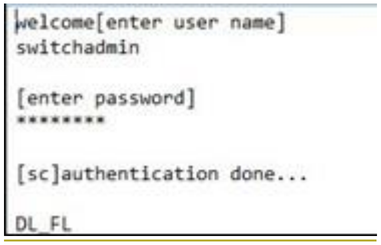
The product operates with authorized USB devices plugged into the console DPP Port, such as USB smart-card reader or Common Access Card (CAC) reader.

By default, authentication devices such as smart card readers and CACs are authorized for use. (product operate in FDF mode).

For authorizing additional USB devices to work with product, Configurable Device Filtering (CDF) mechanism is used with configuration permissions limited to identified and authenticated administrators only.

Administrator Setup

- Use the USB Device Configuration Utility (UCU) to set USB device policies.
- Use USB A-B cable to connect product to a management PC, on which the UCU is installed.
- Connect the A side of the USB A-B cable to the management PC and the B side to the appropriate channel port in panel rear product.
- Switch to the channel you wish to configure and login as administrator. To log in as administrator, proper administrator user name and password are required and should be entered from terminal as shown in the image below:



```
welcome[enter user name]
switchadmin

[enter password]
********

[sc]authentication done...

DL_FL
```

Defining the USB Device Policies

The USB device policies are configured using the USB Device Configuration Utility, which lists allowed and blocked devices. Allowed devices are listed in the white list, and blocked devices are listed in the black list.
Note: Devices on the black list will always supersede devices on the white list. Specific devices can be assigned to certain computers but not to others.

Device policy rules can be created based on:
• Class
• Sub-class
• Protocol
• VID, PID
• Serial Number

Once configured, the policy is loaded onto product.

The USB Device Configuration Utility supports the following operating systems:
• WinXP or greater

Step 1 – Installing the USB Device Configuration Utility

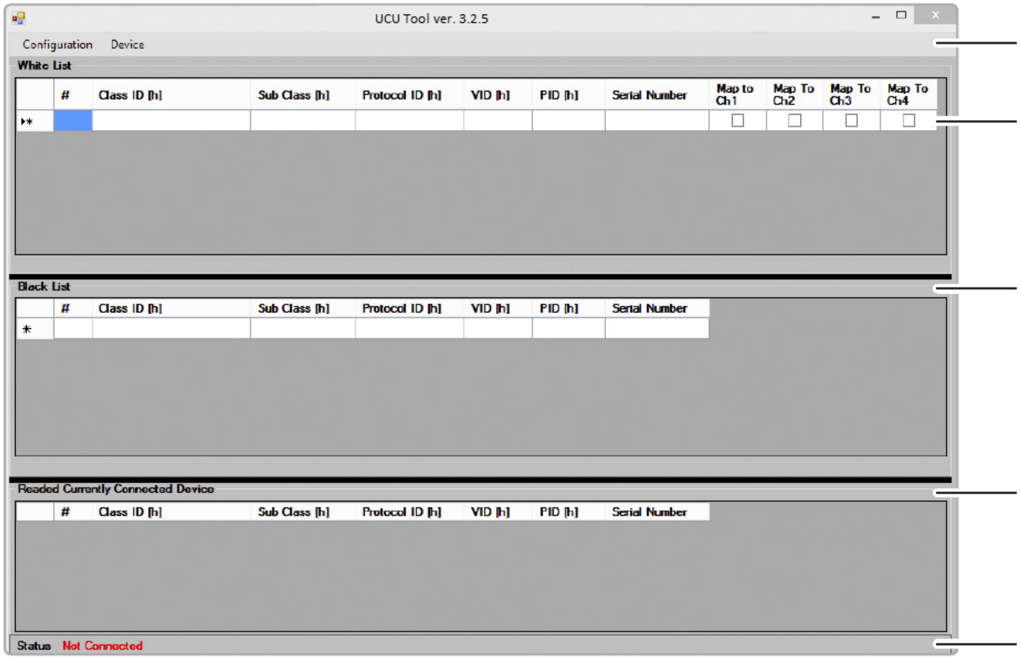
Install the USB Device Configuration Utility by following the installation wizard instructions.

Step 2 – Connect Product to management PC

The management PC can be any external laptop or desktop running WinXP or greater.
Connect a USB Cable from the computer being used to configure the policies to product rear panel.

Step 3 – Open the USB Device Configuration Utility (UCU)

The UCU GUI includes the following areas:



White List

	#	Class ID [h]	Sub Class [h]	Protocol ID [h]	VID [h]	PID [h]	Serial Number	Map to Ch1	Map To Ch2	Map To Ch3	Map To Ch4
▸*								□	□	□	□

Black List

	#	Class ID [h]	Sub Class [h]	Protocol ID [h]	VID [h]	PID [h]	Serial Number
*							

Readed Currently Connected Device

	#	Class ID [h]	Sub Class [h]	Protocol ID [h]	VID [h]	PID [h]	Serial Number

Status Not Connected

Command Bar – Performs certain commands.

White List Rules – Lists allowed devices using "or" relationship rules.

Black List Rules – Lists the blocked devices using "or" relationship rules.

Read Bar – Upon request, displays the attributes of the currently connected device.

Status Bar – Shows the status of the USB Switch and UCU.

Note: The black list rules will always supersede the white list rules.

Step 4 – Check the Connection and Secure UCU

Log on to the product using proper administrator user name and password.

Check the status bar to make sure a connection is established. There are several status options:

• Not Connected – UCU is not communicating with the product or product is not in administrator mode (administrator not currently logged on);

• Connected/Access Granted – UCU is communicating with Product

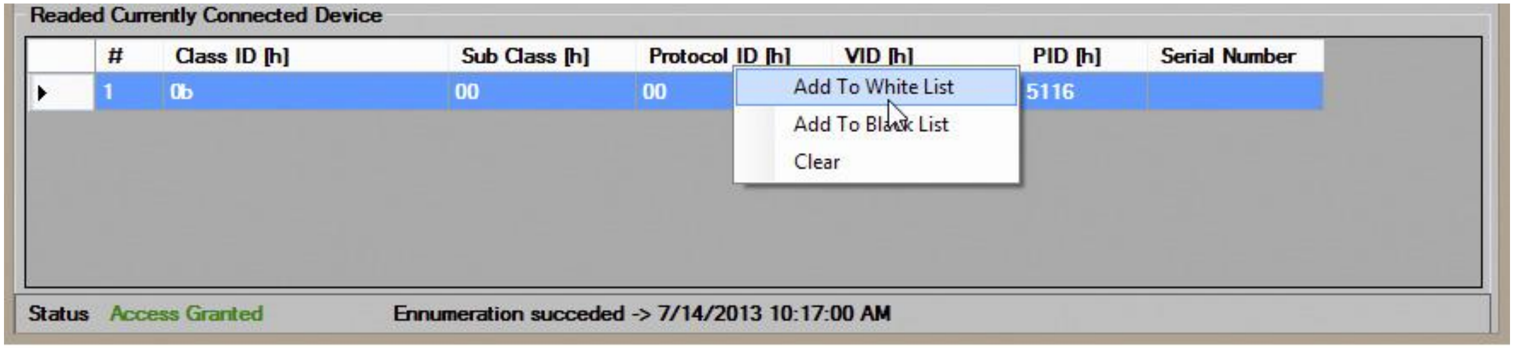
Step 5 – Create USB device rules

Once product is powered up and connected to the UCU, create your first rule.

The mechanisms to create white list and black list rules are very similar and can be done in two ways:

Method 1: Read Attributes from USB Device
You can read the attributes of a connected USB device to create the white list and black list rules.

1. Connect the USB device to the DPP port at product rear panel.
2. Select Device > Read.
The USB device attributes will appear in the Currently Connected Device pane.
3. Right-click attributes and select from the drop-down list if you Wish to add it to the white list or black list.
4. Repeat the above steps for every USB device you are configuring.



Readed Currently Connected Device

#	Class ID [h]	Sub Class [h]	Protocol ID [h]	VID [h]	PID [h]	Serial Number
1	0b	00	00		5116	

Status Access Granted Ennumeration succeded -> 7/14/2013 10:17:00 AM

Method 2: Manually Define USB Devices

1. Go to the white or black list areas and select the attributes by which you would like to define your products.

2. Double-click on a field to open a complete list of all possible attributes. Alternatively just type the value you want.

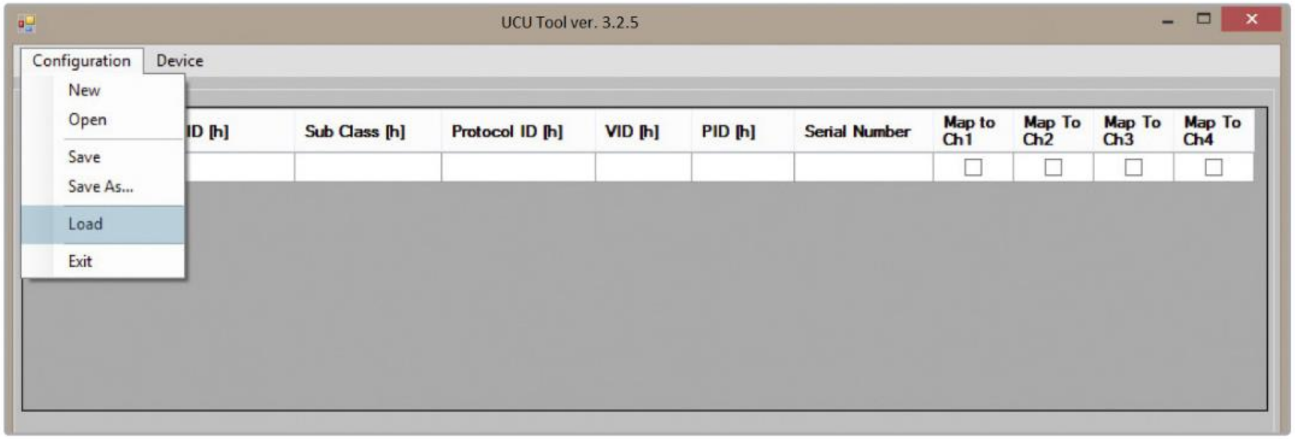
Note:

- For the white list rules, you can also define a host to which you would like to allow the device.
- All fields must be entered.
- Use "*" to define an "any" attribute in a field. * can also be used within the field to define a wild card, for example: 4765* will allow 47653, 476598, and 47650.
- You can create up to 16 white list rules and 16 black list rules in every configuration.
- To delete a rule or move it to the opposite list, right click it, and Select the desired action.

Step 6 – Load the Configuration

Once you have defined the configuration, load it to product. Note that prior to loading configuration – target must be connected and administrator must be logged on (proper username and password entered).

1. Go to Configuration > Load:



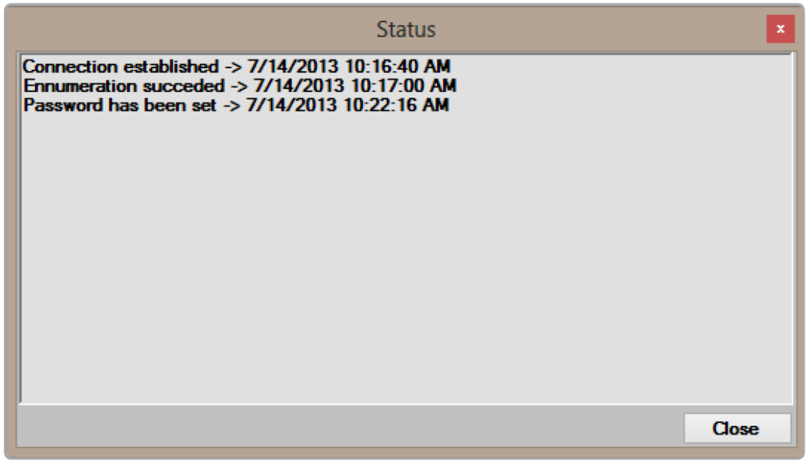
2. When the load command is received, product status LED will turn off.
3. Restart product to apply the new configuration by disconnecting and reconnecting the power supply.

Note: It is impossible to view the configuration currently loaded on product. You can Open a previously saved configuration, edit it and load it to product.

Viewing Connection Status

You can get information regarding the connection status by clicking

Connection Status at the bottom left corner of the application window.



```
Connection established -> 7/14/2013 10:16:40 AM
Ennumeration succeded -> 7/14/2013 10:17:00 AM
Password has been set -> 7/14/2013 10:22:16 AM
```

Saving, Opening and Loading Preset Configurations

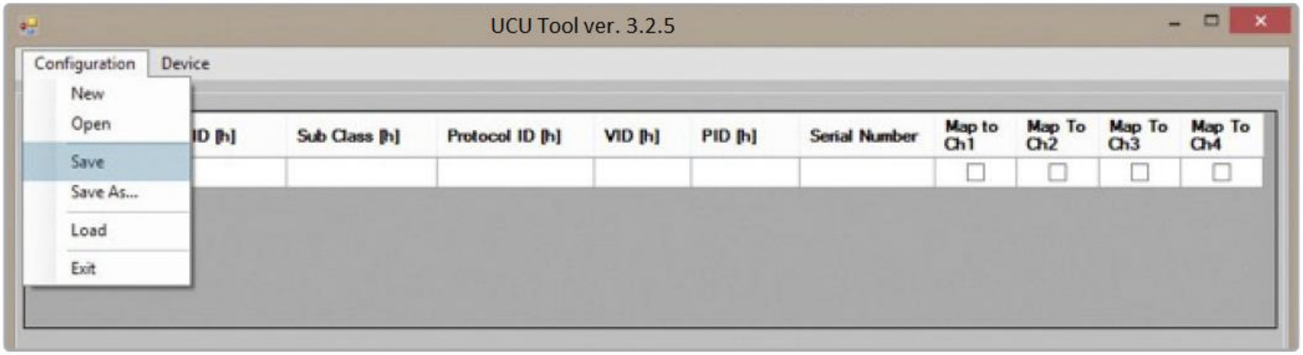
You can save defined configurations to a file and later open or load the saved configuration. When the definitions are ready, it can be either saved for later use or loaded to target if target is ready (connected and having administrator logged in).

To save the configuration:

1. In the menu bar, click Configuration > Save As...
2. Navigate to the directory where you want to save the configuration file, name the file and click Save.

To open and load a saved file:

1. In the menu bar, click Configuration > Open.
2. Navigate to the directory where the configuration file is saved, select it and click Open.
3. Connect product to the administrator PC and load the configuration to product as described in previous pages.



ID [h]	Sub Class [h]	Protocol ID [h]	VID [h]	PID [h]	Serial Number	Map to Ch1	Map To Ch2	Map To Ch3	Map To Ch4
						□	□	□	□

A saved configuration can be opened by selecting Open from the Configuration Menu. Once the saved file is opened, it can be edited as needed and then loaded to product.

Product Configuration Samples

Prior to starting the examples below make sure product is connected to the management PC and UCU is communicating with product. To properly communicate with the target device, enter terminal and log on using valid administrator user name and password.

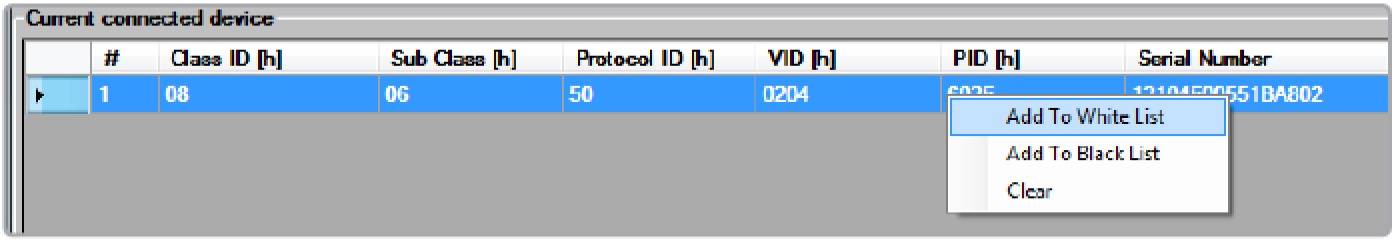
Creating White Rule: Allow using USB Flash drive on PC #3

The purpose of this example is to create a simple ‘White’ Rule in UCU to allow mapping of a USB Flash device to PC#3.

1. Connect the USB Flash Drive to product DPP port. The USB status LED will illuminate RED as at this point USB mapping is prohibited.

2. In UCU, select Device -> Read. The USB device attributes will appear in the ‘Currently Connected Device’ pane.

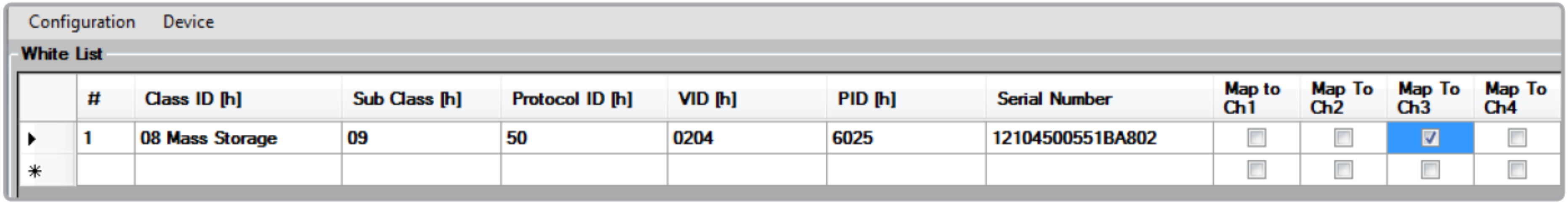
3. Right-click the attributes to add them to the White list pane. Select to map the USB Drive to channel 3 only.



Current connected device

#	Class ID [h]	Sub Class [h]	Protocol ID [h]	VID [h]	PID [h]	Serial Number
1	08	06	50	0204	6025	12104F00551BA802

In UCU, select Configuration -> Load. The USB status LED will blink and turn off indicating the new settings are stored.



	#	Class ID [h]	Sub Class [h]	Protocol ID [h]	VID [h]	PID [h]	Serial Number	Map to Ch1	Map To Ch2	Map To Ch3	Map To Ch4
▸	1	08 Mass Storage	09	50	0204	6025	12104500551BA802	□	□	☑	□
*								□	□	□	□

Disconnect the USB cable from product and power cycle device.

Testing White Rule: Allow using USB Flash drive on PC #3

As a result of the previous configuration, the USB status LED will illuminate Green indicating the connected USB Flash Drive is approved.

Use product channel port selector to navigate between the channels.

The attached USB Flash drive will be mapped to PC #3 only.
Other USB Flash Drives would not work in the current configuration as they were not approved in the UCU.

Creating ‘Black’ Rule: Block mapping of USB Flash drive.

The purpose of this test is to create a ‘Black’ Rule in UCU.

1. Connect the USB Flash Drive to product DPP port. The USB status LED will illuminate RED as at this point USB mapping is prohibited.

2. In UCU, select Device -> Read. The USB device attributes will appear in the ‘Currently Connected Device’ pane.

3. Right-click the attributes to add them to the Black list pane. Select to map the USB Drive to channel 3 only.

Testing Black Rule: Block mapping of USB Flash drive.

The USB status LED will illuminate RED indicating the connected USB Flash Drive is blocked. The channel LED indicators is turned OFF indicating the connected USB Flash Drive is prohibited.

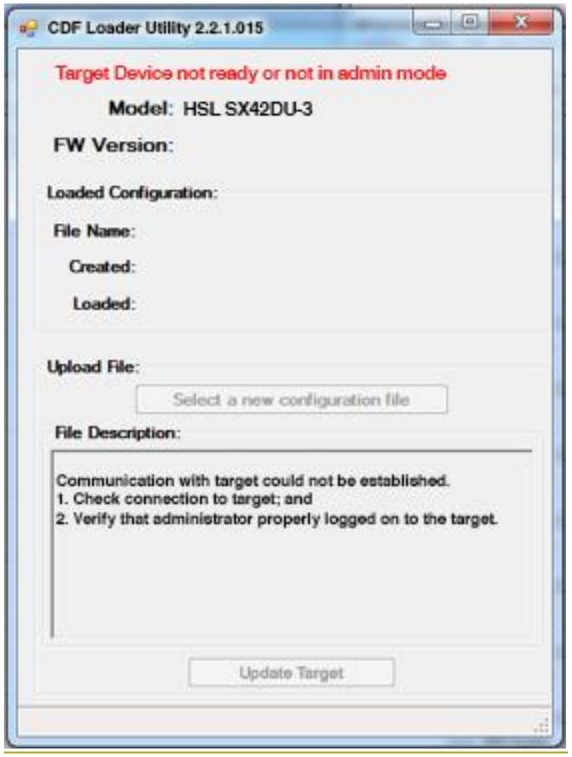
Use product port selector to navigate between the channels.

The USB Flash drive will be blocked as the ‘Black’ Rule overrides the previously configured White Rules.

Other USB Flash Drives would not work in the current configuration as they were not approved.

Loading: Send the device policy to the target product

Once the USB policy definition completed, the policy may be loaded to the target product.
Note that target product must have administrator logged on prior to loading or the following error message will be shown:



Target Device not ready or not in admin mode

Model: HSL SX42DU-3

FW Version:

Loaded Configuration:

File Name:

Created:

Loaded:

Upload File:

File Description:

Communication with target could not be established.
1. Check connection to target; and
2. Verify that administrator properly logged on to the target.

Important Security Note:

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

- Email: Secure@VertivCo.com
- Tel: +1-888-793-8763

Important: If the unit's enclosure appears disrupted or if all LEDs flash continuously, please remove product from service immediately and contact Technical Support at

http://www.Vertiv.com

Important: 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.

COPYRIGHT AND LEGAL NOTICE

Copyright and Legal Notice

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

Images are for demonstration purposes only.