TruMonitor

User's Guide

Rev. 1.0.5

D.O.I-Net Co., Ltd.

Disclaimers

1. D.O.I-Net Co., Ltd. shall not take responsibility for any direct and indirect damage caused by the descriptions stated in this document or other injustices.
2. It is not intended to consent to any rights including the patent rights of any third party or our company with this document.
3. It is prohibited to reprint or reproduce some or all parts of this document without permission.
4. D.O.I-Net Co., Ltd. may change the specifications listed in this document without a notice for the purpose of improvement.

Company names and product names listed in this document are the trademarks of the companies or the registered trademarks.
When you export these products, please follow the necessary procedures by confirming the foreign exchange, foreign trade methods, and regulations such as the U.S. export control laws.

Revision History

Rev.	Date	Details
1.0.0	2010/11/11	Issued.
1.0.1	2012/04/17	Removed Windows 2000 from Supported OSs due to version up.
1.0.2	2013/05/01	Added Windows 8, Windows Server 2012 to Supported OSs. Changed Trial Period.
1.0.3	2014/12/04	Modified descriptions of Supported OSs.
1.0.4	2015/07/22	Added Windows 10 to Supported OSs.
1.0.5	2023/11/07	Changed Supported Oss.

Index

Figure Index

1. Introduction

This User's Guide explains the operation of TruMonitor and the TruMonitor Configuration (Configuration Wizard) utility that configures TruMonitor operation, produced by D.O.I-Net Co., Ltd. (D.O.I-Net).

2. Operating Conditions

a. Supported OSs

Windows 10 32bit/64bit
Windows 11
Windows Server 2016
Windows Server 2019

3. TruMonitor Functionality

a. Product Summary

TruMonitor is launched as an OS service, and monitors the status change of USB ports and disk connections. It also takes predefined protective actions such as Logoff when it detects that an inhibitive device is attached.

In addition, TruMonitor also executes a predefined protective action when the USB device is detached.

The event at execution of a protective action is recorded to the log file, and will be helpful for analysis when a problem occurs.

i. Single License Edition

This is a package mainly for personal users. It comes with the exe installer package. The trial period is 1 month. No restrictions are set during the trial period.

ii. Volume License Edition

This is a package mainly for corporate users. It comes with the msi installer package. You cannot uninstall it from "Apps and Features" of the OS installed on the PC. Uninstall it from “Active Directory server” or “re-launched msi installer”. Either 32bit version or 64bit version is available. The trial period is 3 months. No restrictions are set during the trial period.

b. Targeting Detected Devices

i. USB Devices (except USB HUB)

1) Devices without Serial Numbers

If the devices are attached to different USB ports, TruMonitor will recognize

them as different individuals even though they are identical.

2) Devices with Serial Numbers

If your OS is upgraded from one earlier than Windows 2000 Service Pack 2 with the devices attached, TruMonitor will recognize them as different individuals, even though they are identical, if the devices are attached to different USB ports.

After Windows 2000 Service Pack 3, TruMonitor will recognize them as identical even though they are attached to different USB ports.

ii. Disk Devices (including IDE, PCMCIA, etc.)

1) Devices without Serial Numbers

TruMonitor will recognize them as different individuals, even though they are identical, if the devices are connected at different places.

2) Devices with Serial Numbers

If your OS is upgraded from one earlier than Windows 2000 Service Pack 2 with the devices connected, TruMonitor will recognize them as different individuals, even though they are identical, if the devices are connected at different places.

After Windows 2000 Service Pack 3, TruMonitor will recognize them as identical even though they are connected at different places.

c. Detecting Method

i. White List

TruMonitor detects the devices based on a white list that accepts specific USB devices and disk devices. Refer to the White List Configuration section below for more details.

ii. Filter

1) White Filter

TruMonitor permits attachment and detachment based on the VID&PID (Vendor ID and Product ID) of USB devices and disk devices. Refer to the White Filter Configuration section below for more details.

2) Device Filter

TruMonitor can optionally filter the USB devices and disk devices that you want to attach or detach by class. Refer to the Device Filter Configuration section below for more details.

iii. Application Order

The following shows the order (high to low) of application of the filter and white list.

1. Disk Device Filter
2. USB Device Class Filter

3. White Filter
4. White List

Devices that do not match the filter and white list will be detected as unauthorized devices.

d. Detecting Event

i. At OS Booting

Statically attached unauthorized devices to the PC.

ii. After OS Booted

Dynamically attaching unauthorized devices to the PC.

Dynamically detaching authorized devices from the PC.

You can optionally use the Configuration Wizard to assign devices which detection should ignore.

e. Protective Action at Event Detection

i. At OS Booting

1) At Detection of Unauthorized Device Statically Attached

TruMonitor executes one of the predefined actions listed below.

Workstation Lock
Log Off
OS Shutdown
PC Power Off
Reboot
Detach (logically detach the unauthorized device)
Nothing

ii. After OS Booted

1) At Detection of Unauthorized Device Dynamically Attached

TruMonitor executes one of the predefined actions listed below.

Workstation Lock
Log Off
OS Shutdown
PC Power Off
Reboot
Detach (logically detach the unauthorized device)
Nothing

2) At Detection of Authorized Device Dynamically Detached

TruMonitor executes one of the predefined actions listed below.

Workstation Lock
Log Off
OS Shutdown
PC Power Off
Reboot
Nothing

f. Event Logging

If one of the events mentioned before is detected, the event log data is stored to the client PC.

Note: You can view the event log data with the dedicated log viewer, and can also keep the event log data in another PC on the network if both use TruLog Service produced by D.O.I-Net. The volume license edition assumes the combined use of TruLog Service. Please refer to the TruLog Service Client/Server Configuration User's Guide for the installation of TruLog Service.

i. Register Authorized Devices at Once

You can create a device list from the event log data. It is possible to register the entire white list at once by using the device list.

① Run TruMonitor temporarily, with each protective action configured as "Nothing" after installation.
② After the temporary operation, import the collected device list with the "Import List" function of the "White List Configuration" page.
③ Select and/or delete the devices, and configure the filter as required.
④ Configure each protective action as you prefer.

ii. Asset Management

You can grasp the usage situation of authorized devices with the dedicated viewer mentioned above if you have enabled the "Asset Management" function on the Configuration Wizard.

g. Manage Access to Removable Storage

You can manage writing and access to removable devices.

i. Supporting OS

Windows XP Service Pack 2 or later
    Supports some devices
Windows Vista or later
    Supports all devices

h. Administrator Authentication

You can specify registered administrative users to use the Configuration Wizard.

Note: It is possible for the Configuration Wizard to authenticate administrators with authentication devices such as biometrics if you also use TruGate produced by D.O.I-Net. Further, if TruLog Service (mentioned before) is used as well, authentication log data will be kept.

4. Warnings

1. If either Logoff, Shutdown, Reboot, or Power Off is selected as the protective action, when the protective action is executed, the running applications are forced to close and the data will be lost if not saved.
2. Event detection is suspended while the Configuration Wizard is running.
3. The delay time from the attachment/detachment to the protective action execution depends on the PC and Windows Plug and Play operation.
4. TruMonitor does not support multiple USB2.0 host controllers.
5. Never install a single license edition and a volume license edition together on the same PC.
6. There will be a possibility that the protective action is not performed as expected, depending on the edition of the OS and/or Service Pack. In that case, perform Windows Update.

5. Installation and Uninstallation Procedure

Note: In installing and uninstalling, please log on with the administrator privilege of the local computer. For the installation of Volume License Edition, please refer to the TruMonitor Client Setup Guide.

a. Installation

A dialog box shown below appears when you execute TruMonitor Trusted Stackware Illegal Device Interceptor.exe. Click the "Next" button.

Figure 1 Setup Wizard Welcome Dialog Box

Read "SOFTWARE LICENSE AGREEMENT" shown in the dialog box carefully, and click the "I accept the terms in the license agreement" radio button if you agree, then click the "Next" button.

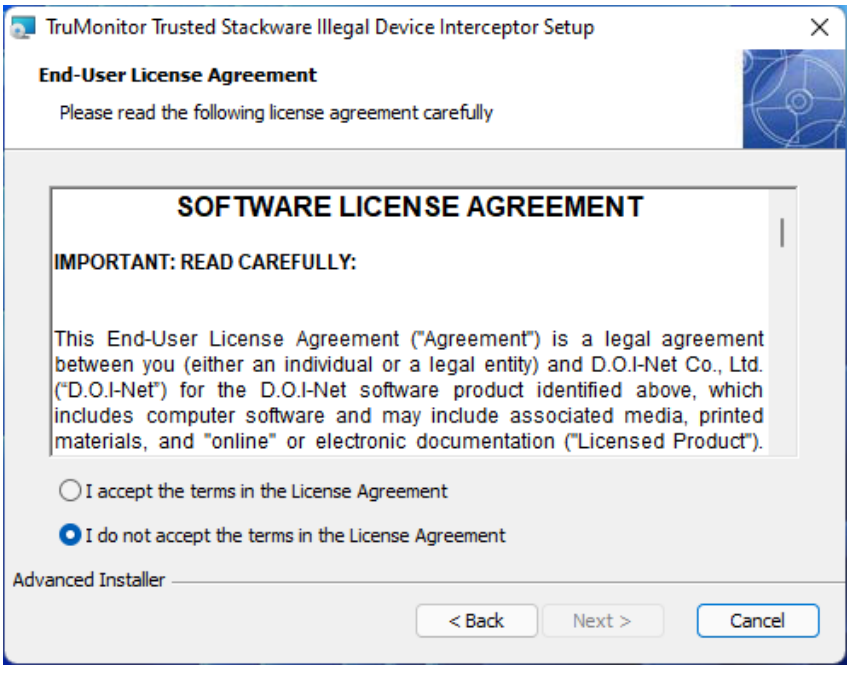

Figure 2 SOFTWARE LICENSE AGREEMENT

When the Setup Type dialog box is displayed, select the setup type according to your usage environment.

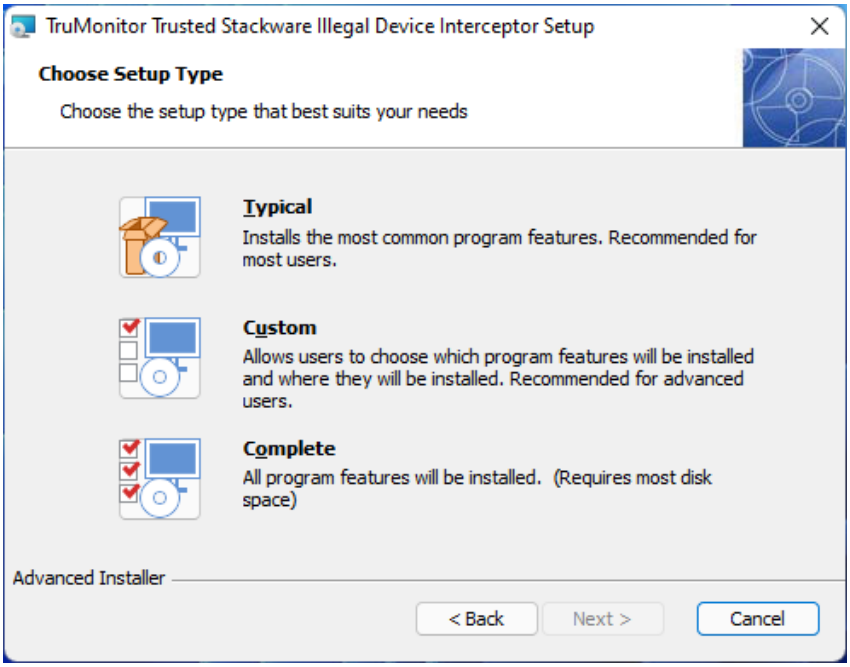

Figure 3 Setup Type Selection Dialog Box

Click the "Install" button unless you need to change. If you need to make some changes, click the "Back" button and return to the dialog box where you want to make changes.

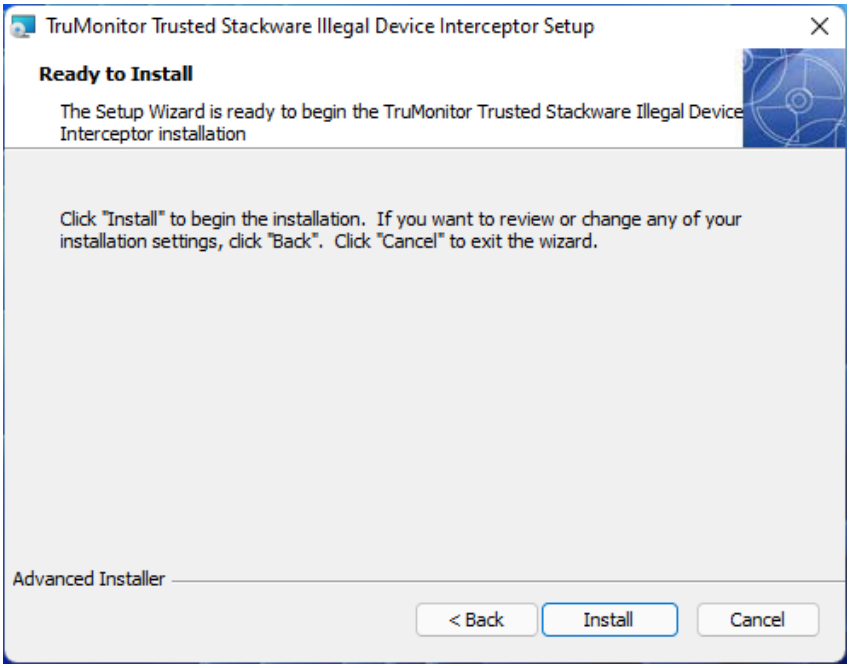

Figure 4 Ready to Install Dialog Box

During installation, the following indicator dialog box will be displayed.

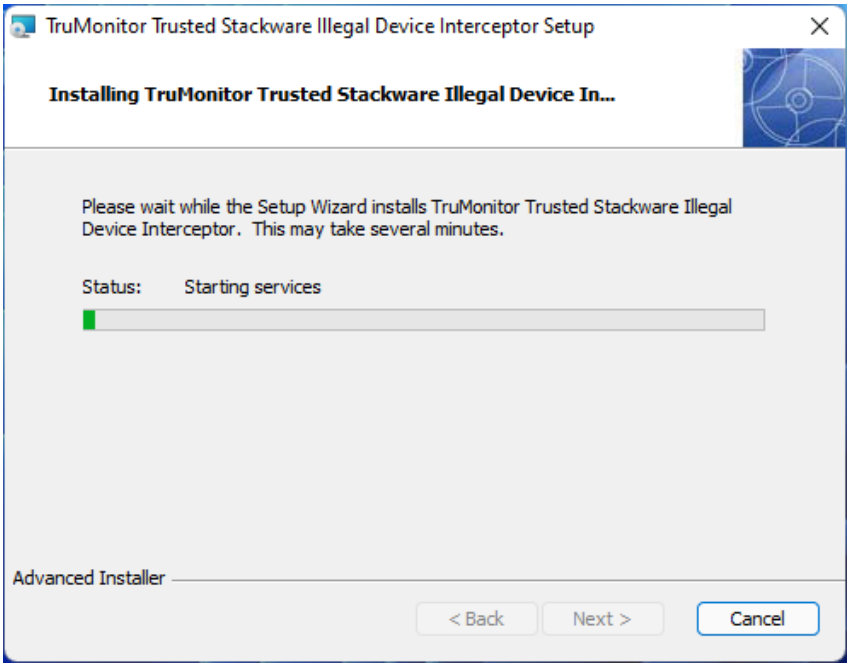

Figure 5 Installation Indicator Dialog Box

When installation is finished, the following installation completion dialog will be displayed. Click the "Finish" button.

Figure 6 Installation Complete Dialog Box

b. Uninstallation

Note: If you are using "Removable Storage Access Configuration" function

mentioned below, please put them back before uninstallation, and uninstall TruMonitor after reflecting them.

Select “TruMonitor Trusted Stackware Illegal Device Interceptor” from "Apps and Features" of the OS.

The following is an operation example with Windows 11.

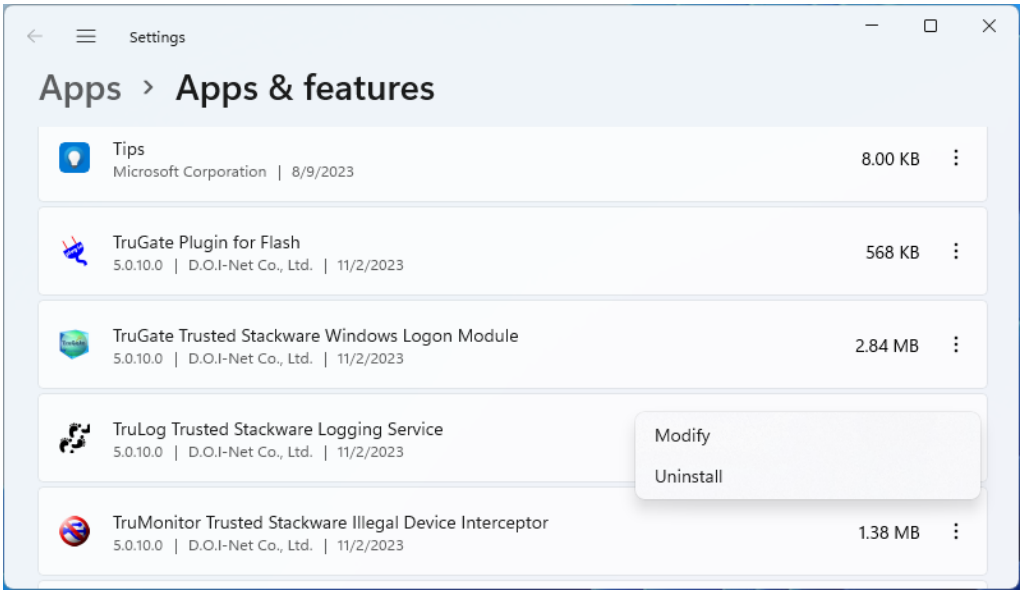

Figure 7 Apps and Features Dialog Box

Then click “Uninstall”, and uninstall TruMonitor following the message.

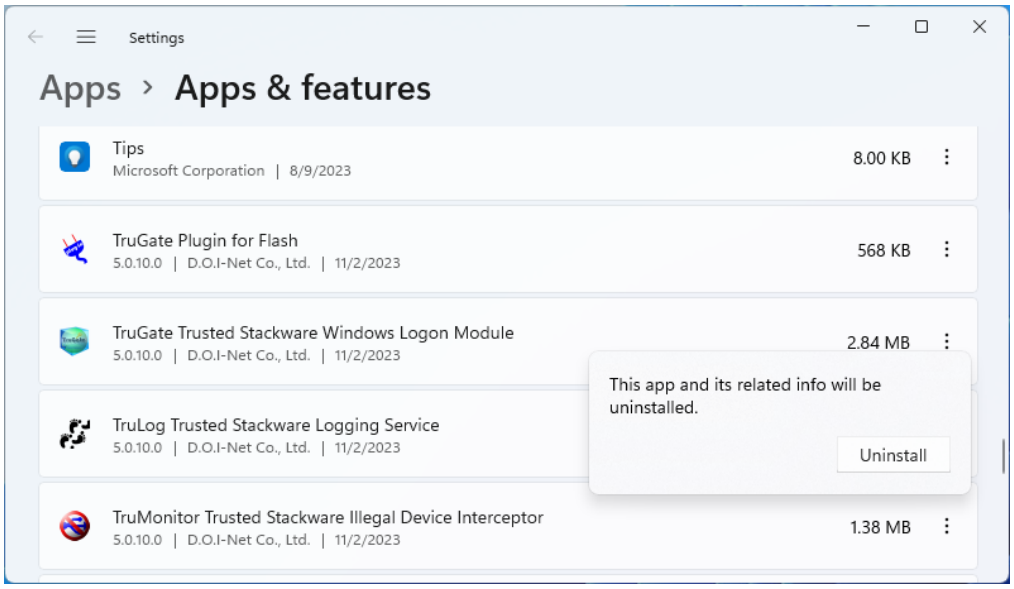

Figure 8 Confirmation of Program Uninstallation Dialog Box

During uninstallation, the following indicator dialog box will be displayed.

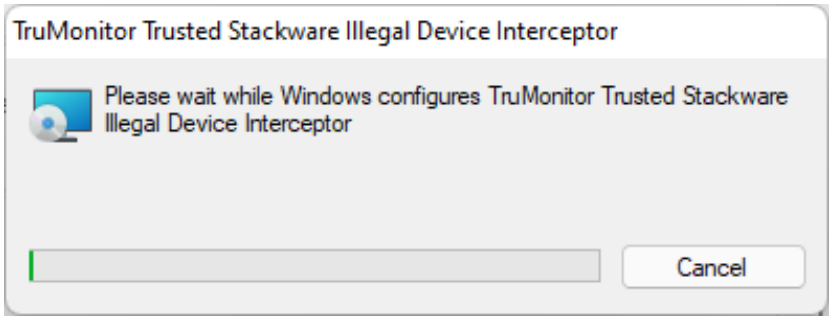

Figure 9 Uninstall Indicator Dialog Box

When uninstallation is completed, the indicator dialog box will disappear.

6. Operation Method

In order for TruMonitor to perform protective actions, it must be configured with the Configuration Wizard.

Note: Please log on with the administrator privilege of the local computer to operate the Configuration Wizard. Also, the event detection is suspended while the Configuration Wizard is running. If you want to add authorized devices, please attach them to the PC after the Configuration Wizard is launched.

a. Preparation

When using TruMonitor for the first time, after installation, attach all the devices you want to authorize before launching the Configuration Wizard. You can leave or detach them as you prefer.

b. Launch Configuration Wizard

Click in the order of “Start” – “All Apps” – “TruStack” – “TruMonitor Configuration”.

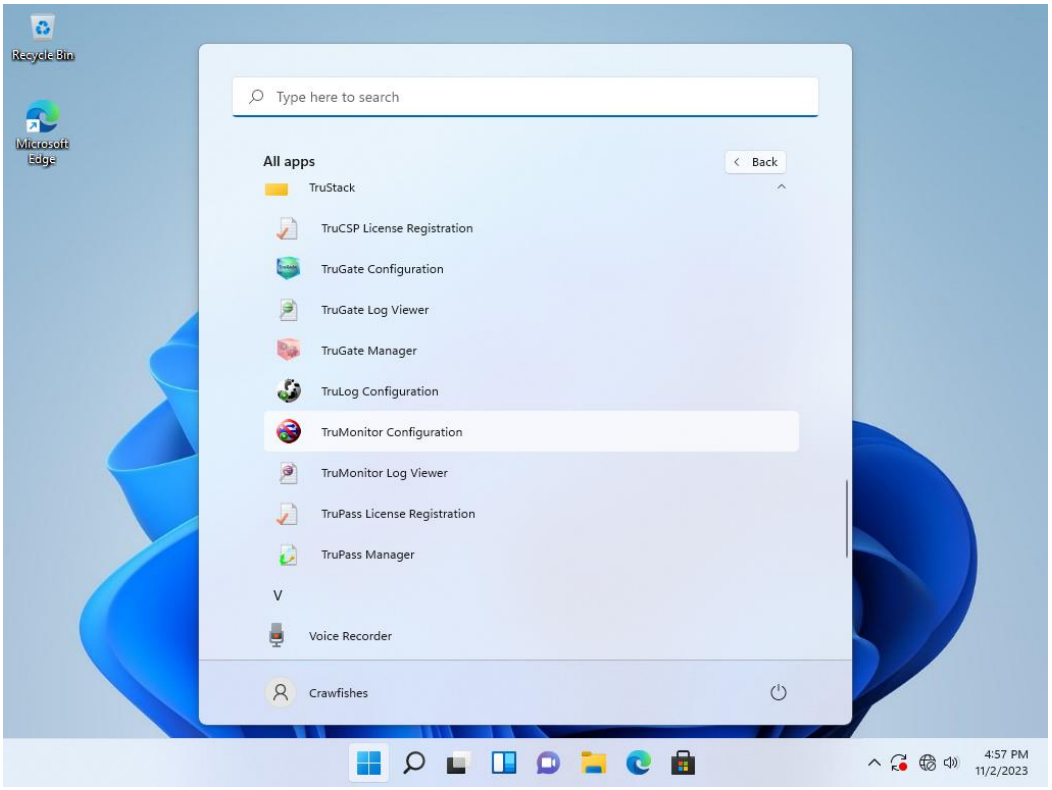

Figure 10 Launch Configuration Utility

i. License Verification

The following popup message will be displayed during the trial period. If the message is shown, click the “OK” button.

Figure 11 Trial Period Message

Note: Trial period is 1 moth for the single license edition, and 3 months for the volume license edition. TruMonitor will not perform the protective action after the trial period expires. Please register the product key to use TruMonitor continuously.

When the trial period is over, the dialog box as follows will be displayed. To keep using it, enter the product key in the edit box, then click the “OK” button. To terminate

the trial, click the “Cancel” button, and uninstall TruMonitor.

Figure 12 Trial Period Expired Warning Message

ii. Administrator Registration

If any Administrator is not registered even though the “Use Authorized Admin Function” check box is checked on the “Administrator Configuration” page mentioned below, you will be requested to register the Administrator at the next application launching.

Click the “Yes” button if the following dialog box is shown.

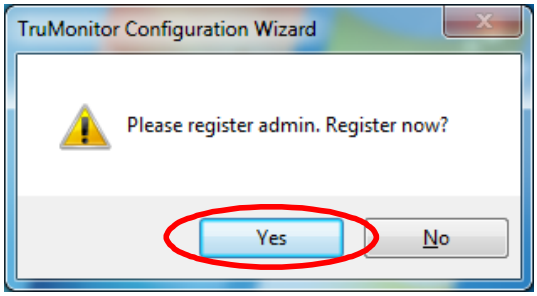

Figure 13 Request for Administrator Registration at Launch

Next, if the dialog box shown below is displayed, enter the user name to register as an administrator. After that, click the “OK” button.

Note: If you are also using TruGate produced by D.O.I-Net, the registering administrator user name should be a pre-registered user of TruGate. The “Select Device…” button in the dialog box will be available if TruGate is also used.

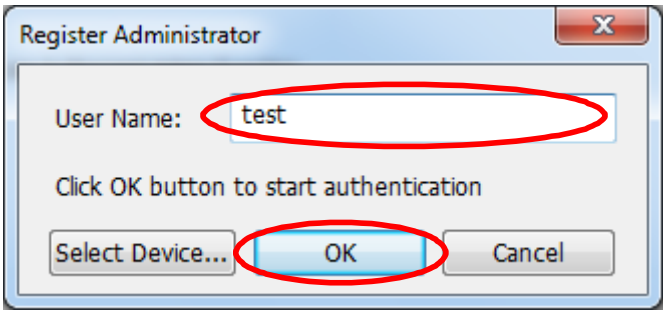

Figure 14 Administrator Registration Dialog Box

After administrator registration is completed at launching, a confirmation dialog is displayed. Click the “OK” button and perform administrator authentication as in the next section.

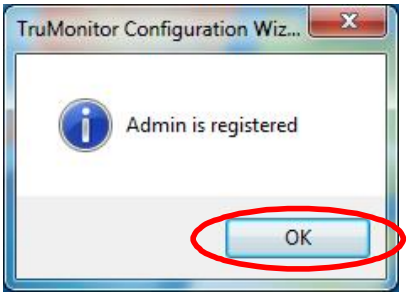

Figure 15 Completion of Administrator Registration

iii. Administrator Authentication

If the “Use Authorized Admin Function” check box is checked on the “Administrator Configuration” page mentioned below, the administrator authentication dialog box as follows is displayed.

If this dialog box is displayed, enter the registered administrator user name, and click the “OK” button to authenticate.

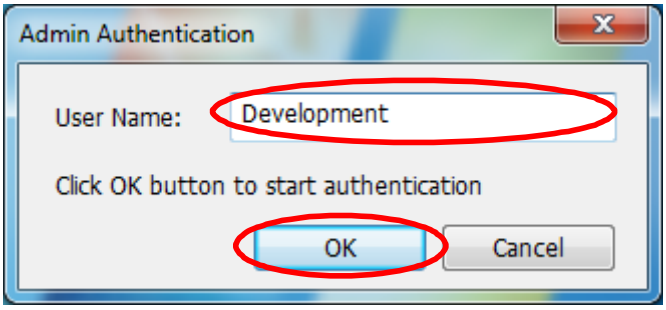

Figure 16 Administrator Authentication

If the authentication is successful, the Configuration Wizard is launched and the following page is displayed. Click the “Next” button to start configuration.

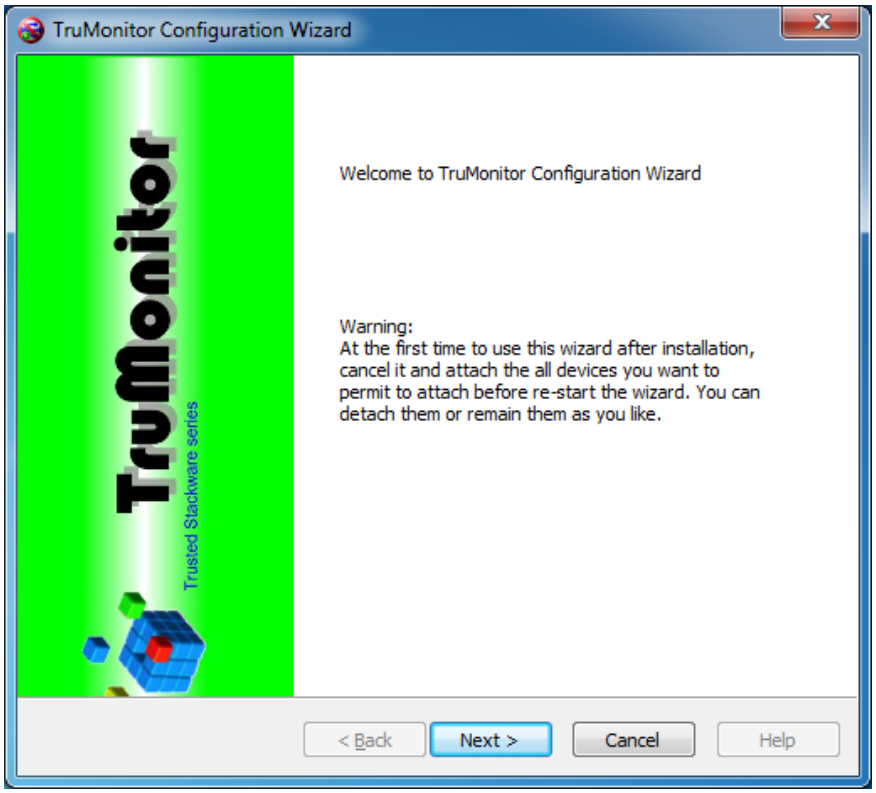

Figure 17 TruMonitor Configuration Wizard

c. Basic Configuration

When the “Basic Configuration” page is displayed, check or uncheck the following check boxes as needed.

i. Add to Existing White List

If this check box is checked, you can register multiple authorized devices to the same port.

Default: checked

ii. Restart Service at Exit

If this check box is checked, TruMonitor service is resumed after the Configuration Wizard is finished. The new configuration such as protective actions and the white list will be applied at resumption.

Default: checked

iii. Apply VID&PID Filter

If this check box is checked, the “White Filter Configuration (for Detach)” and “White Filter Configuration (for Attach)” pages mentioned below become available.

When the white filter is valid, the devices that have the same VID&PID as the one included in the White Filter list will be ignored by the protective action at the device

detection.

When importing configuration data exported from another PC, check this check box and configure the white filter. Also, if you frequently change connection places and/or USB ports, check this check box and configure the white filter.

Default: uncheck (single license edition)

Default: checked (volume license edition)

iv. Apply USB Device Class Filter

If this check box is checked, the “Device Filter Configuration” page mentioned below becomes available, as does the “USB Device Class” filter on that page.

When the USB Device Class Filter is valid, the devices that belong to the same device class as that checked by the “USB Device Class” filter will be ignored by the protective action at the device detection.

Default: uncheck (single license edition)

Default: checked (volume license edition)

v. Apply Disk Device Filter

If this check box is checked, the “Device Filter Configuration” page mentioned below becomes available, as does the “Disk Device Class” filter on that page.

When the Disk Device Class Filter is valid, the disks that belong to the same disk device class as that checked by the “Disk Device Class” filter will be ignored by the protective action at the device detection.

Default: uncheck (single license edition)

Default: checked (volume license edition)

vi. Enable Asset Log

If this check box is checked, the event log is output at detection of authorized devices statically and/or dynamically.

Default: uncheck

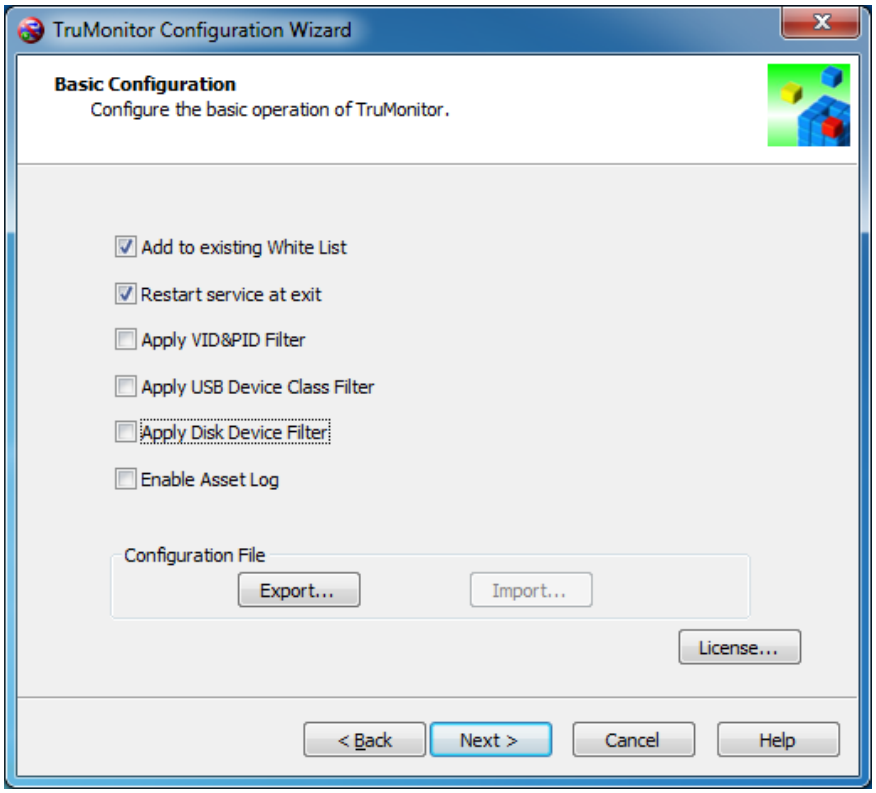

Figure 18 Basic Configuration page - in trial period

vii. Export of Configuration File

To export the configuration file, click the “Export...” button on the “Basic Configuration” page.

Note: “Export...” outputs the configuration data already configured. The data reflects the configuration that was last saved with the “Finish” button. For the normal procedure, re-launch the Configuration Wizard after executing the configuration, and export the configuration data before closing the Configuration Wizard with “Cancel”.

If the “Save As” dialog box is displayed, assign the location to which you want to export the file, enter the file name in the “File name” combo box, and click the “Save” button. If you click the “Cancel” button, the export will be cancelled.

If you use the volume license edition and want to export distributable configuration data, select “Policy Template” or “Registry File” from the “Save as type” drop down list.

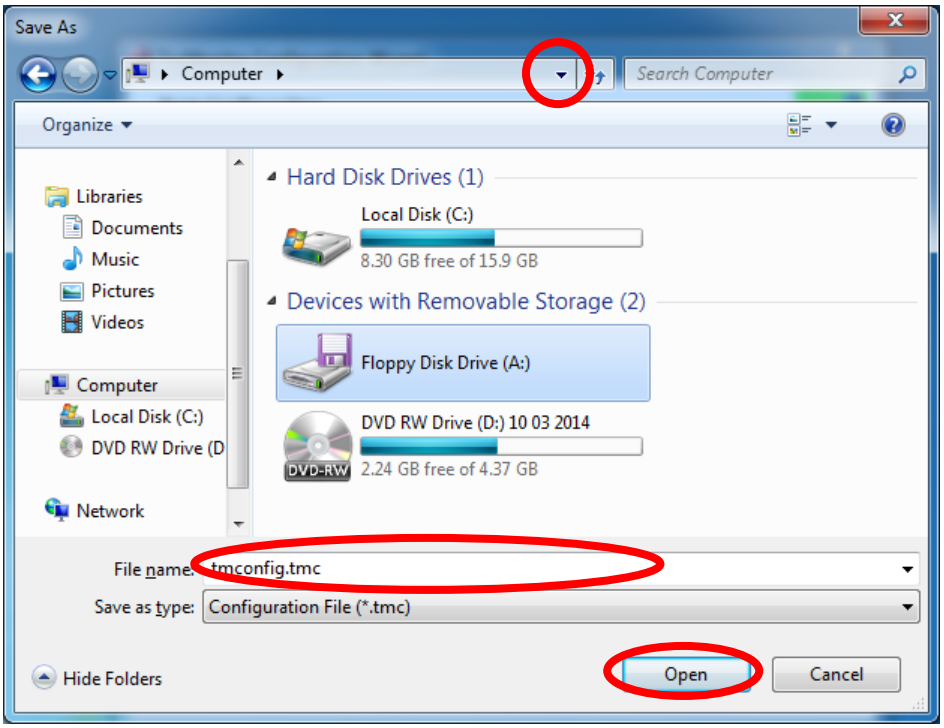

Figure 19 Export of Configuration File

If the export was successful, the “End of Export” dialog box is shown as follows. Click the “OK” button.

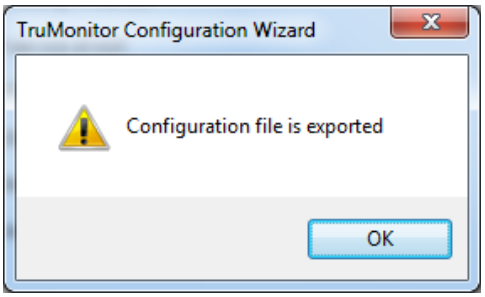

Figure 20 End of Export

viii. Import of Configuration File

To import a configuration file, click the “Import...” button on the “Basic Configuration” page.

Note: The “Import...” button will be available when both of the “Add Existing White List” and “Apply VID&PID Filter” check boxes are checked. Once the “Import...” is executed, the configuration data is overwritten immediately. Please be careful because it is impossible to bring back the earlier data with the “Cancel” button after the execution of the “Import...”.

If the “Open” dialog box is displayed, assign the location to which you want to import the file, enter the file name in the “File name” combo box, and click the “Open”

button. If you click the “Cancel” button, the import will be cancelled.

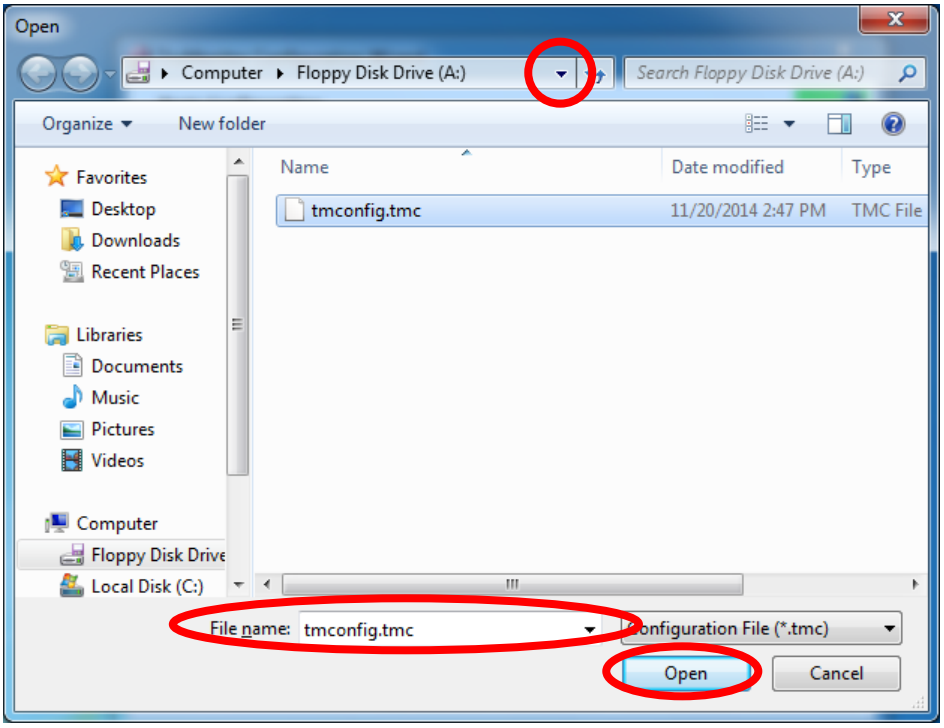

Figure 21 Import of Configuration file

If the import was successful, the “End of Import” dialog box is shown as follows. Click the “OK” button.

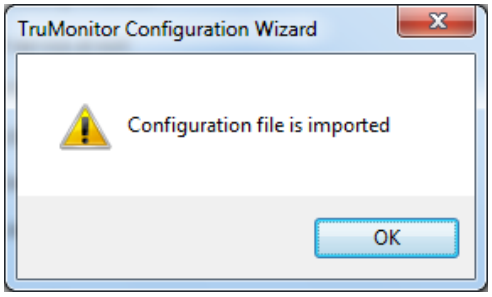

Figure 22 End of Import

ix. License Registration

To register the product license, click the “License…” button on the “Basic Configuration” page.

When License Registration dialog box appears, click the “OK” button after entering the product key you obtained separately in the edit box. If the “Cancel” button is clicked, the license registration will be cancelled.

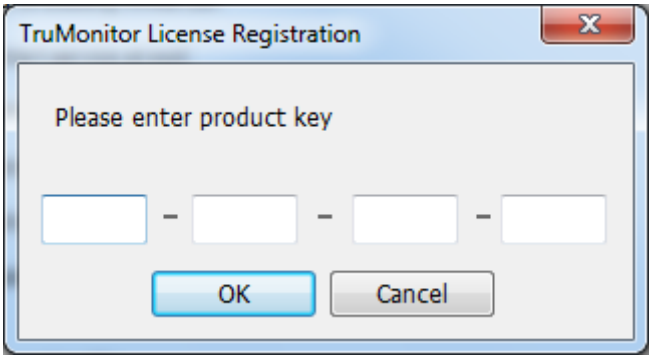

Figure 23 License Registration

If the verification of product key is successfully done, and the registration is normally complete, the “License…” button on the “Basic Configuration” page will disappear.

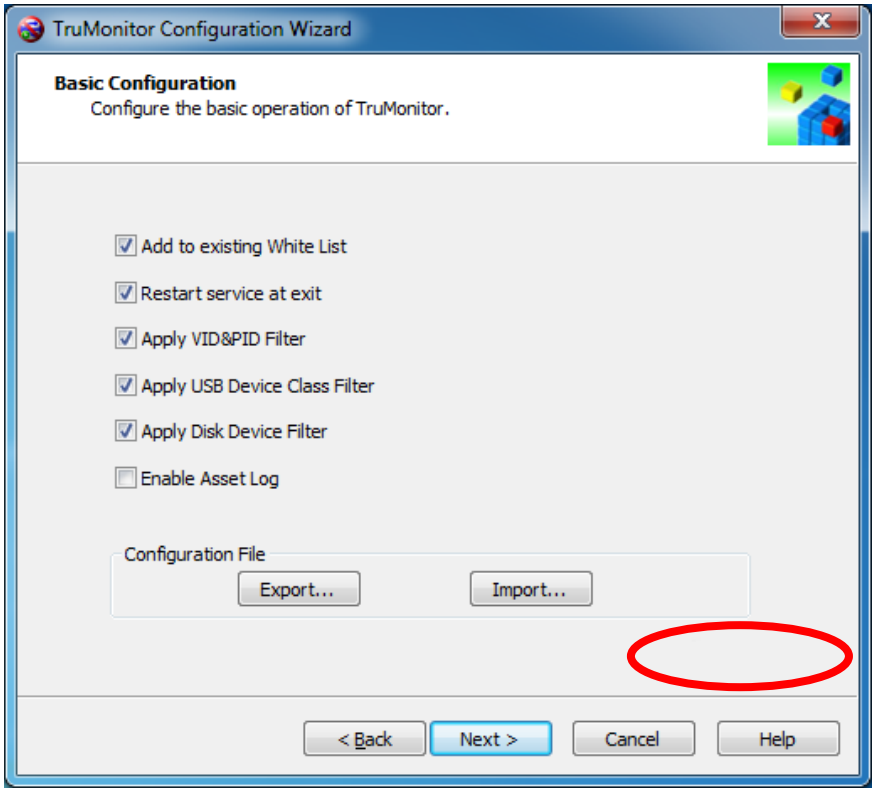

Figure 24 Basic Configuration page - after license registered

d. Administrator Management

The ”Administrator Configuration” page manages the use of the Configuration Wizard Administrator authentication function and administrator registration/unregistration.

Note: Registered administrator names will not be included in the configuration file. Therefore, they are excluded from the targets of “Export...” and/or “Import...” on

the “Basic Configuration” page.

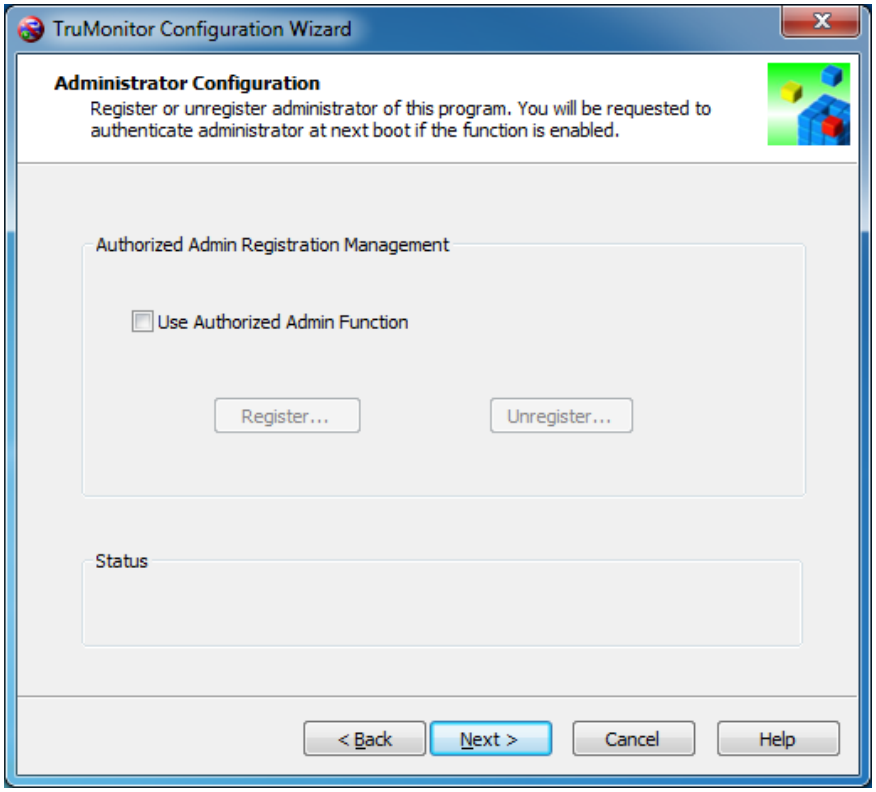

Figure 25 Administrator Configuration page

i. Use Authorized Admin Function

If you want to restrict operation of the Configuration Wizard to a specific administrator only, check this check box.

Default: uncheck

ii. Administrator Registration

The “Register...” button will be available when the “Use Authorized Admin Function” check box is checked. If this button is clicked, Administrator Registration dialog box as follows will be displayed. When the dialog box is displayed, enter the user name you want to register as an administrator. After that, click the “OK” button.

Note: If you are also using TruGate produced by D.O.I-Net, the registering administrator user name should be a pre-registered user of TruGate. The “Select Device...” button in the dialog box will be available if TruGate is also used.

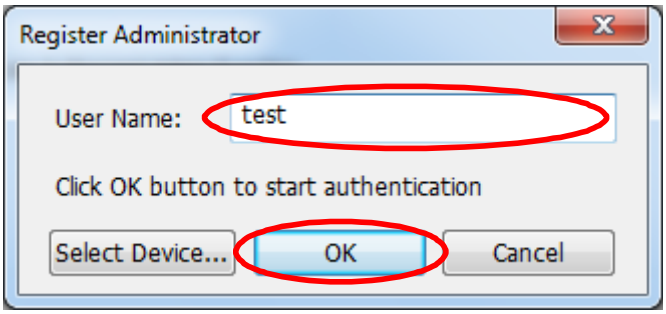

Figure 26 Administrator Registration

iii. Administrator Unregistration

The “Unregister...” button will be available when the “Use Authorized Admin Function” check box is checked. If this button is clicked, Administrator Unregistration dialog box as follows will be displayed.

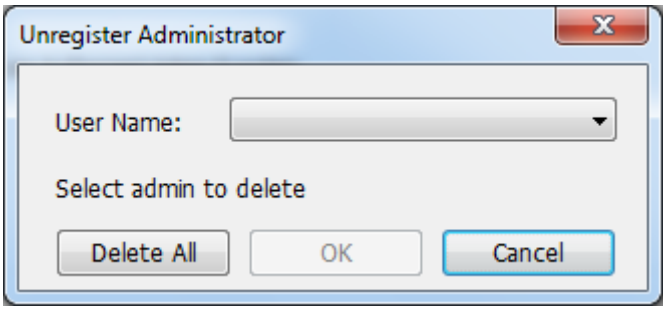

Figure 27 Administrator Unregistration

When the dialog box is displayed, select the administrator name you want to unregister from the “User Name” drop down list.

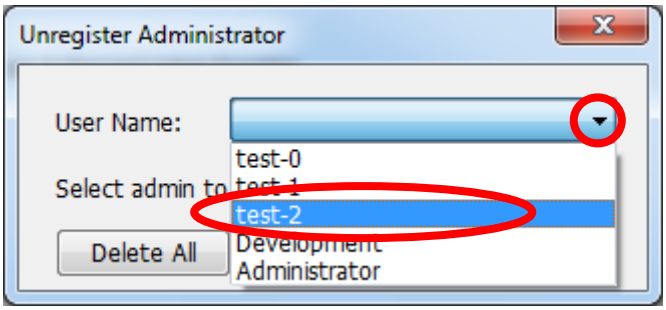

Figure 28 Administrator Unregistration - select from list

Click the “Delete” button after selecting the administrator you want to unregister.

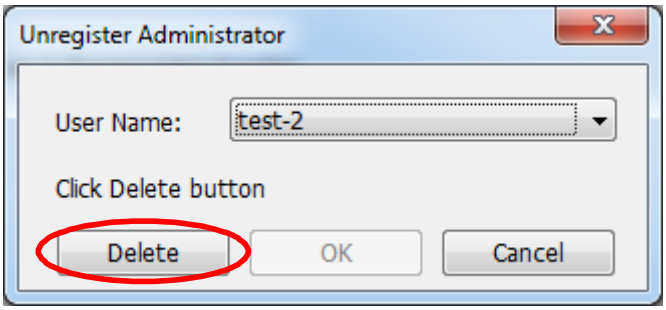

Figure 29 Administrator Unregistration - unregister

When the administrator is successfully unregistered from the shown list, a message like below will be displayed. Unregistering of the administrator will be completed when the “OK” button is clicked. If the “Cancel” button is clicked, the unregistering operation will be cancelled.

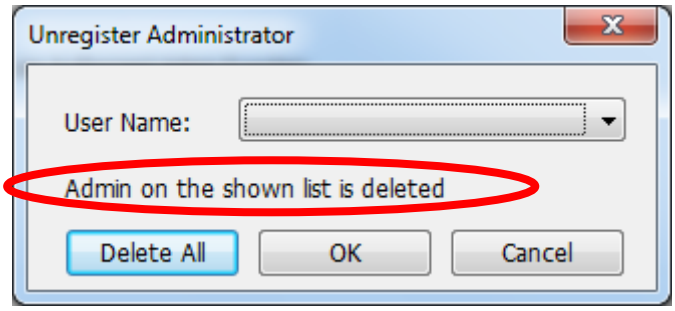

Figure 30 Administrator Unregistration - unregister from shown list

In order to unregister all of the administrators, click the “Delete All” button.

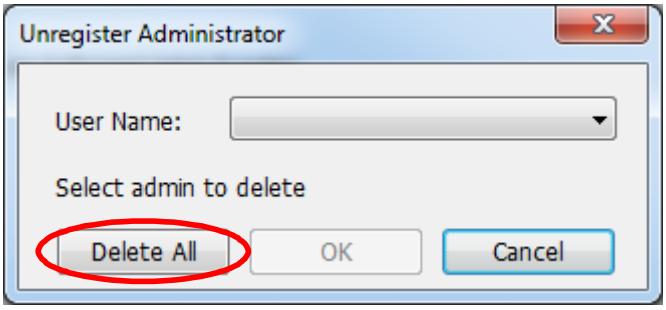

Figure 31 Administrator Unregistration - unregister all

A confirmation message like below will be displayed. Click the “Yes” button when you really want to do so.

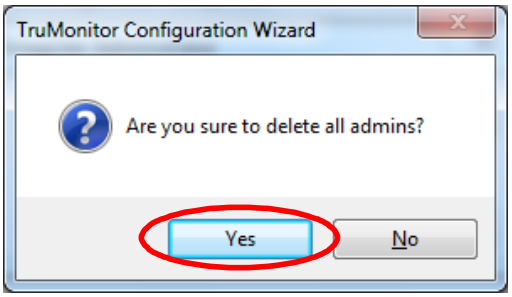

Figure 32 Confirmation for Unregistration of All Administrators

The following message will be displayed if all the administrators are unregistered from the shown list successfully. After clicking the “OK” button, unregistering of all the administrators will be completed. If you click the “Cancel” button, the unregistering operation will be cancelled.

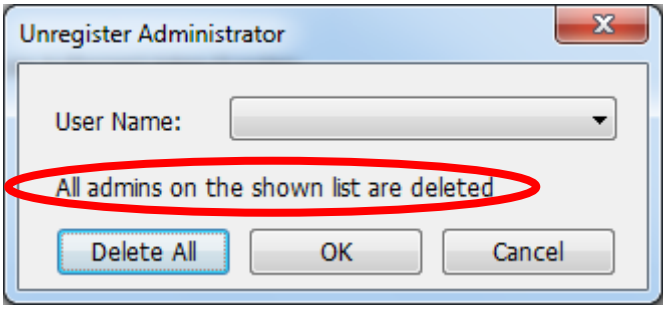

Figure 33 Administrator Unregistration - unregister all from shown list

e. Accessing Removable Storage

The “Removable Storage Access Configuration” page configures permissions for use of removable storage devices. If you want to inhibit the use of a device, check the check box of that device in the “Inhibit to Use” group. Also, if you want to write-protect, check the check box of that device in the “Write Protect” group.

Note: This function modifies the registry data that the OS refers to. The configurable and applicable items depend on what OS you use. The full items are applicable with Windows Vista or above. If you have already configured device access control with a Removable Storage Devices group policy, please set the same permission for each item. When you uninstall this program, please return the configuration and apply it, before uninstalling the program.

Default values are below.

Inhibit to Use

Default: uncheck all

Write Protect

Default: uncheck all

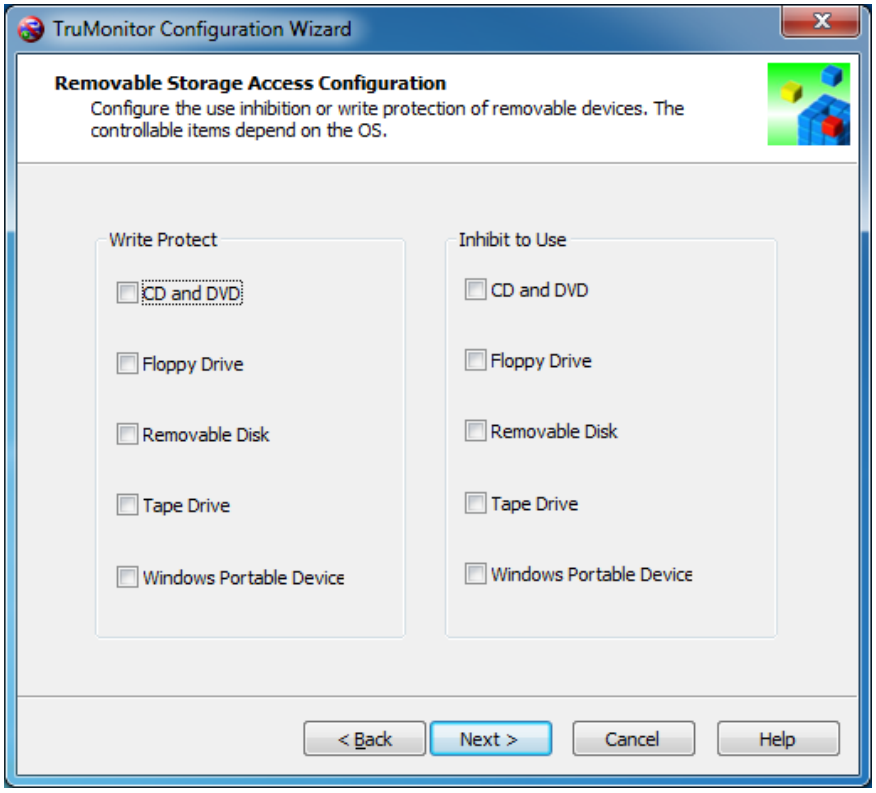

Figure 34 Removable Storage Access Configuration page

When you write to a write-protected device, the message shown below is displayed. The message varies according to OS edition and device.

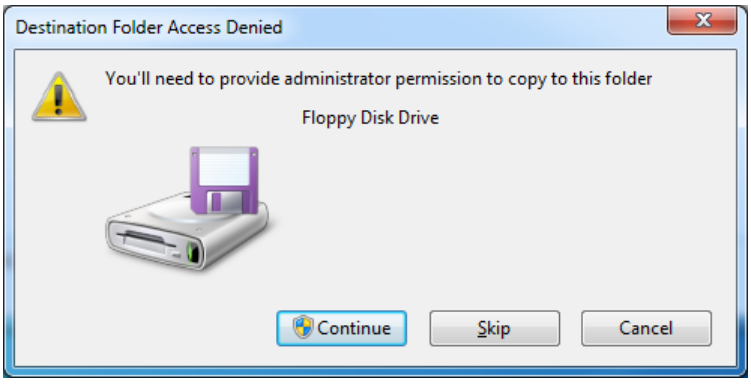

Figure 35 Write Protect Message Dialog Box

When you access an inhibited device, the message shown below is displayed. The message varies according to OS edition and device.

Note: If you use CD Writer and/or a third party application that does not use IMAPI (Image Mastering Applications Programming Interface), users can create or modify even CDs and DVDs which have been write-protected. In that case, please inhibit

the use of that application.

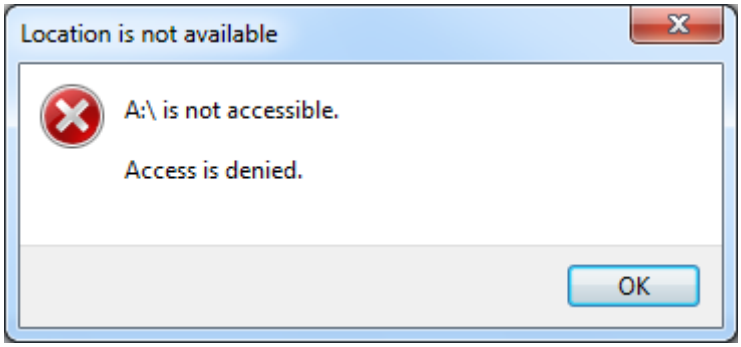

Figure 36 Access Denied Message Dialog Box

f. USB Device List

The ”USB Device List” page shows the currently attached USB device tree. You can individually specify the devices that you want to ignore from “Action at Detach” as defined on the “Protective Action Configuration” page. Check the check box of devices such as USB mice which users attach and detach frequently.

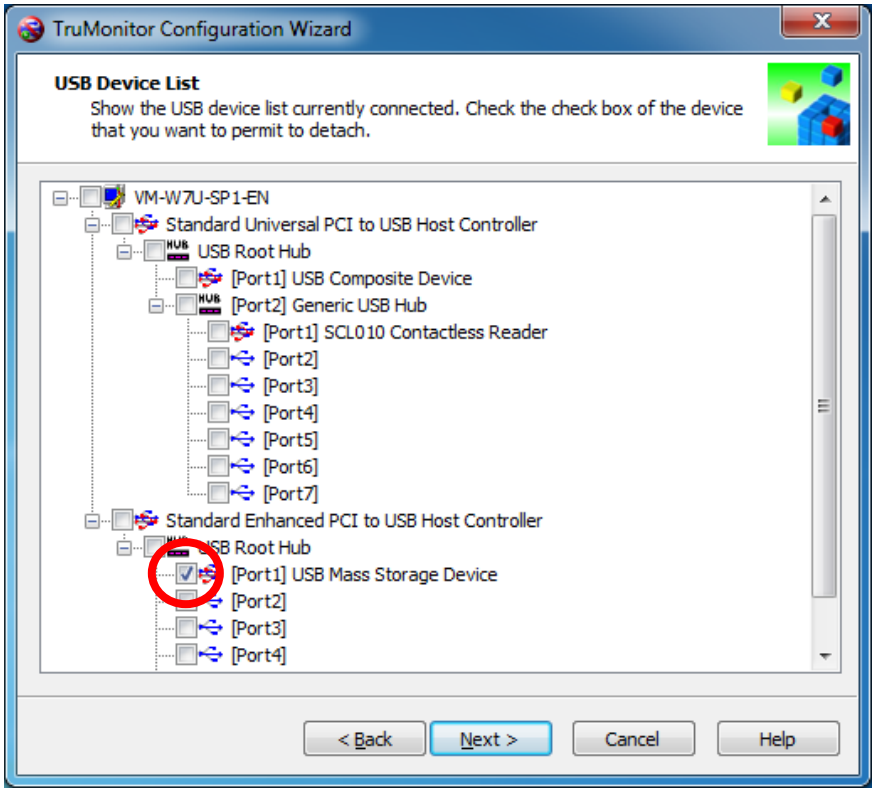

Figure 37 USB Device List page - example of exception for detach protective action

g. Protective Action Configuration

The ”Protective Action Configuration” page defines the protective actions that are performed on detection of unauthenticated devices according to the Plug and Play event caused by device attachment/detachment and OS booting. You can specify the protective action for each event: 1) when a device that is not permitted to be detached is detached; 2) when an unauthorized device is attached; 3) when an unauthorized device is detected at OS booting.

Default values are below.

Action at Detach

Default: Nothing

Action at Attach

Default: Nothing

Action at Boot

Default: Nothing

Note: If “Detach” cannot be performed during the execution of a protective action, “Workstation Lock” will be performed instead.

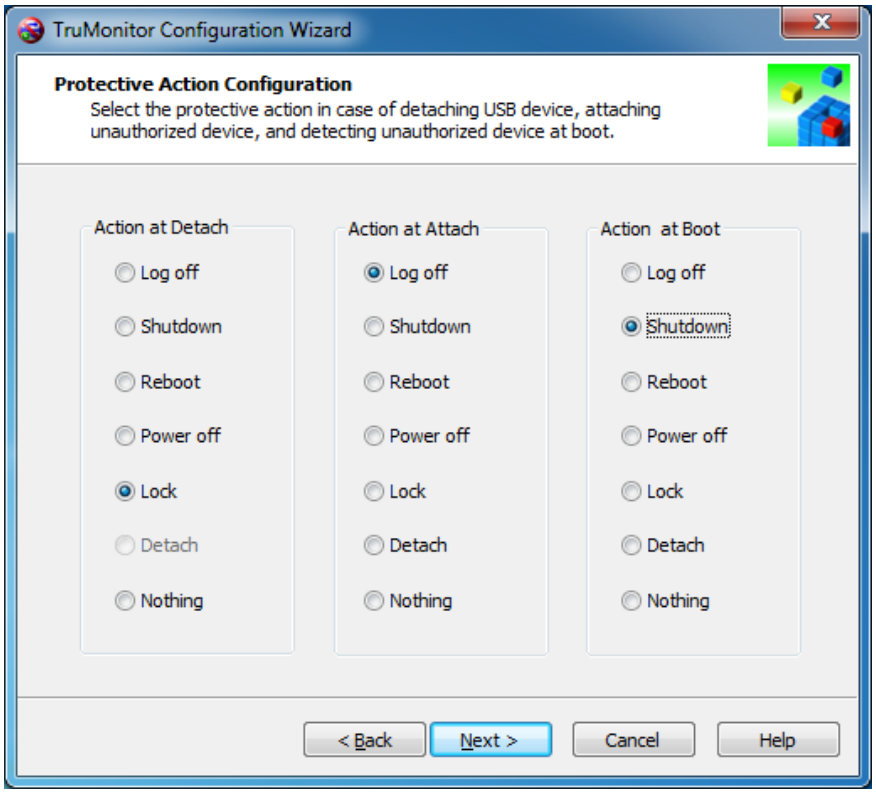

Figure 38 Protective Action Configuration page

h. White List Configuration

The “White List Configuration” page shows the list of authorized devices you want to permit to attach, and you can add/remove devices to/from the list. Also, the configuration contents of the “White Filter Configuration (for Attach)” page and “Device Filter Configuration” page mentioned below are reflected in the list.

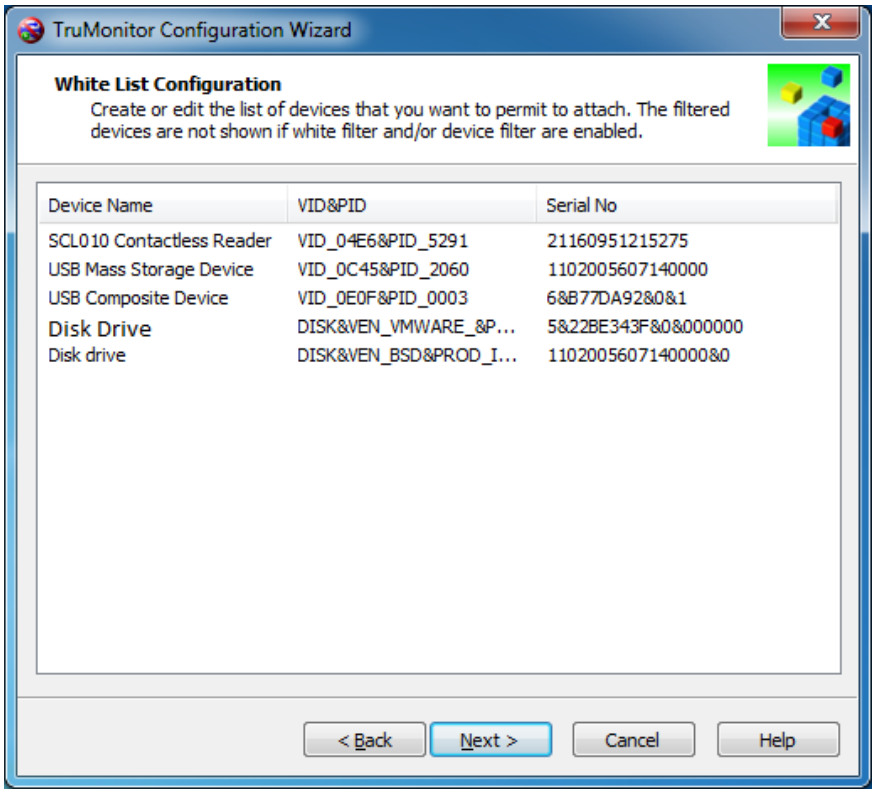

Figure 39 White List Configuration page

i. Refresh

The list will be refreshed at page creation or by single clicking the right mouse button. The refreshed list will include the currently attached devices.

ii. Delete Items

You can delete device you don’t want attached: double click the left mouse button on the device you want to delete from the list.

Note: Physically attached devices cannot be deleted.

iii. Import List

You can import the list if the “Add to existing White List” check box on the “Basic Configuration” page is checked. To import the list, double click the right mouse button within the display area of the “White List Configuration” page. The White List Import dialog box will be displayed.

Note: Perform the import at first configuration.

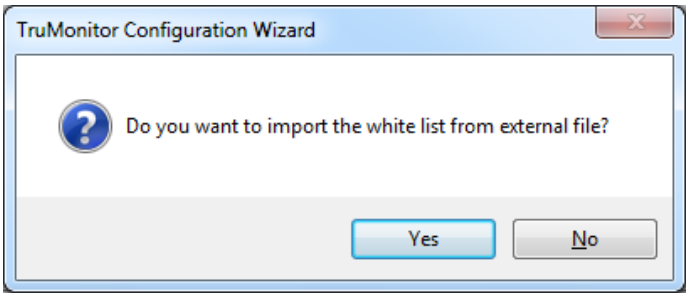

Figure 40 Import White List Dialog Box

1) For Single License Edition

Click the “No” button on the White List Import dialog box. The list will be created based on the log data that have been recorded from the installation, and be imported.

2) For Volume License Edition

Follow the procedure below if you use the volume license edition.

Note: It is possible to import the list through the same procedure as the single license edition if the Log Server and the Configuration Wizard are running on the same PC.

① Click the “Yes” button on the White List Import dialog box.

② The “Open” dialog box will be displayed. Specify the file path, and enter in the “File name” combo box the device list file name previously created by TruMonitor Log Viewer. Then click the “Open” button.

③ Delete devices according to the “Delete Items” section above if unauthorized USB devices are listed.

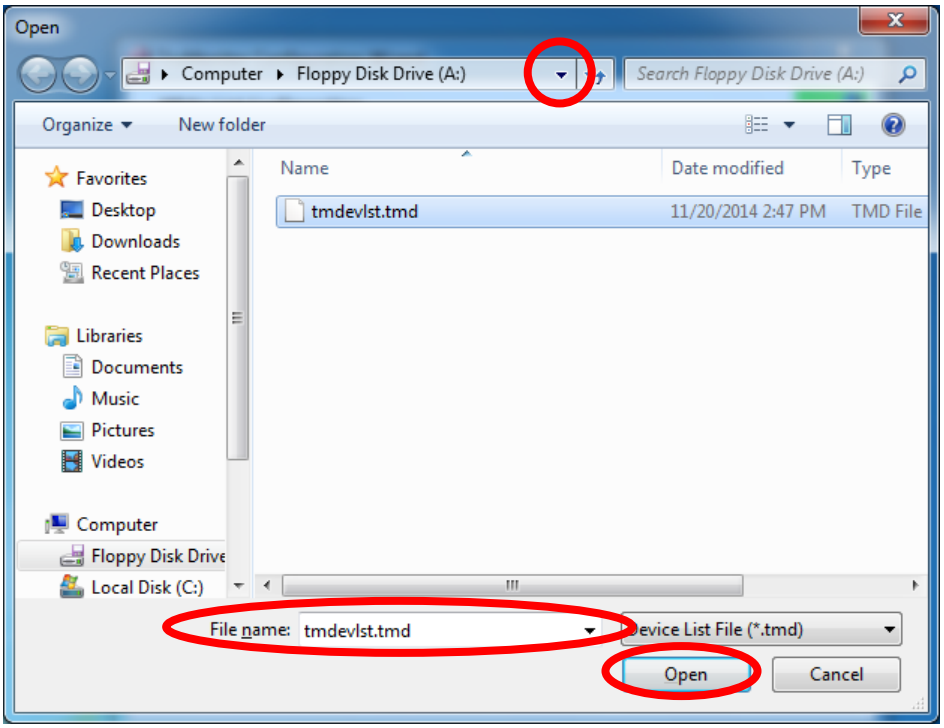

Figure 41 Import from External File

i. White Filter Configuration for Detaching

The “White Filter Configuration (for Detach)” page shows the list of authorized devices you want to permit to detach by VID&PID category; you can add/remove the devices to/from the list. Also, the configuration contents of the “Device Filter Configuration” page mentioned below will be reflected in the list.

i. Refresh

The list will be refreshed by single clicking the right mouse button. The refreshed list will include the currently attached devices.

ii. Delete Items

You can delete device you don’t want detached: double click the left mouse button on the device you want to delete from the list.

iii. Import List

You can import the list that is shown on the “White List Configuration” page to the “White Filter Configuration (for Detach)” page. Double click the right mouse button within the display area of the “White Filter Configuration (for Detach)” page. The devices in the same category will be merged.

Note: The device list on the “White List Configuration” page will be updated according to the contents of the “White Filter Configuration (for Attach)” page and/or “Device Filter Configuration” page. Be careful regarding the order of

filter configuration.

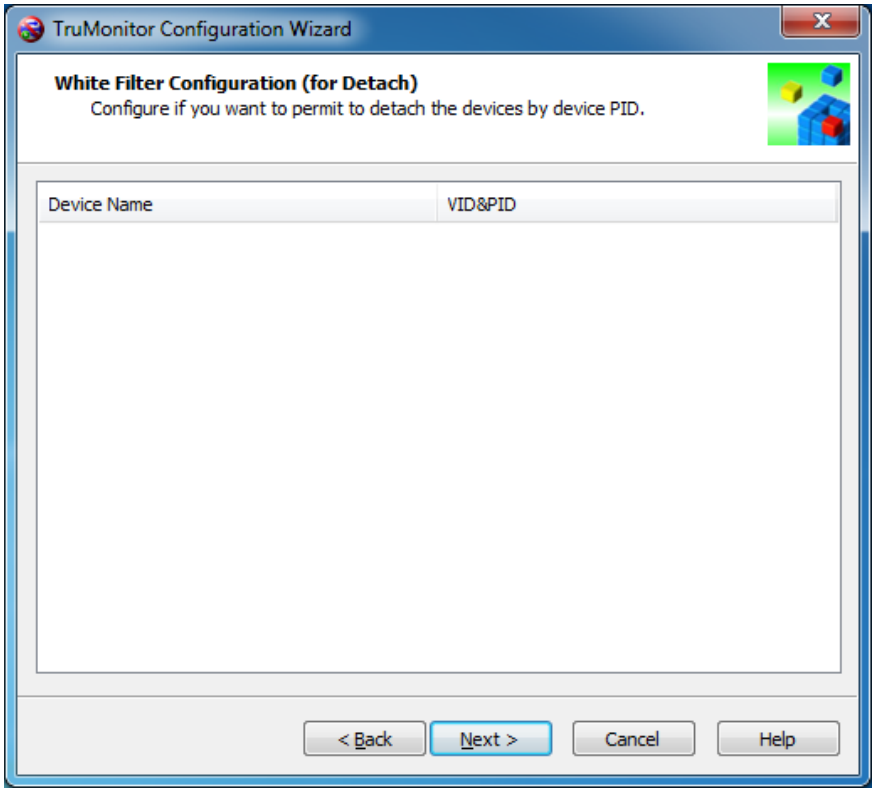

Figure 42 White Filter Configuration page - for detaching

j. White Filter Configuration for Attaching

The “White Filter Configuration (for Attach)” page shows the list of authorized devices you want to permit to attach by VID&PID category; you can add/remove devices to/from the list. Also, the configuration contents of the “Device Filter Configuration” page mentioned below will be reflected in the list.

i. Refresh

The list will be refreshed by single clicking the right mouse button. The refreshed list will include the currently attached devices.

ii. Delete Items

You can delete device you don’t want attached: double click the left mouse button on the device you want to delete from the list.

iii. Import List

You can import the list that is shown on the “White List Configuration” page to the “White Filter Configuration (for Attach)” page. Double click the right mouse button within the display area of the “White Filter Configuration (for Attach)” page. The devices in the same category will be merged.

Note: The device list on the "White List Configuration" page will be updated according to the contents of the "White Filter Configuration (for Attach)" page and/or "Device Filter Configuration" page. Be careful regarding the order of filter configuration.

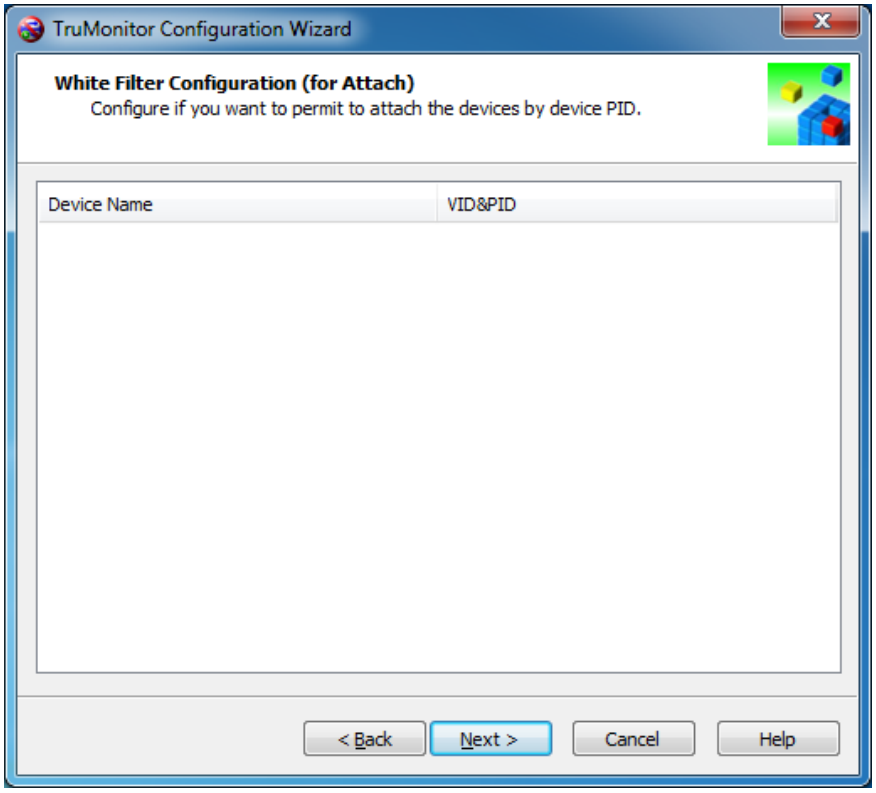

Figure 43 White Filter Configuration page - for attaching

k. Device Filter Configuration

The "Device Filter Configuration" page configures a detection filter for target devices. The devices belonging to each class will be ignored by the protective action if that class is filtered. Generally, however, this product should be used without modification.

Note: For volume license edition, filter the disk device class that is used on the client PC. Also, it is recommended that you filter the Human Interface Device in the USB Device Class.

Default values are below.

USB Device Class

Default: uncheck all

Disk Device Class

Default: uncheck all

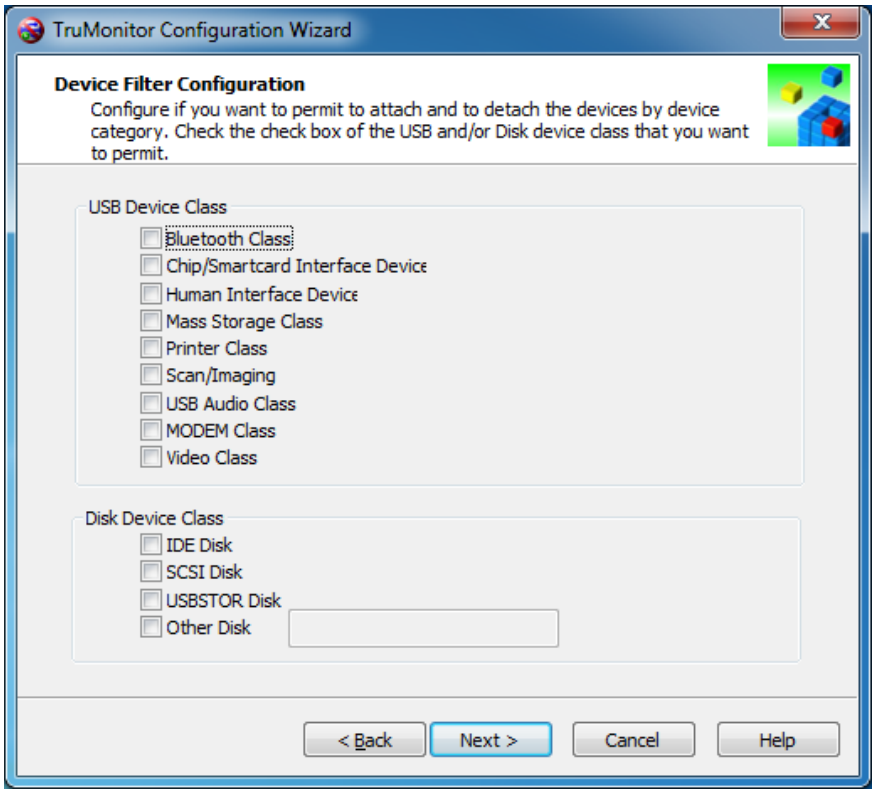

Figure 44 Device Filter Configuration page

The following procedure shows an example of HOW TO DETERMINE THE USB DEVICE CLASS. If you are not sure of the class, confirm it according to the example.

① Refer to the following registry key with the Registry Editor (regedit.exe).
HKLM¥SYSTEM¥CurrentControlSet¥Enum¥USB

② Refer to the target device key under the above registry key. Look at VID&PID in the log of TruMonitor with the TruMonitor Log Viewer for xxxx and yyyy.
VID_xxxx&PID_yyyy

③ Refer to one of the sub-keys under the above device key.

④ Refer to the value of the following name.
CompatibleIDs

⑤ Read the USB Device Class from the next table by referring to the zz portion of USB¥Class_zz.

USB Device Class	zz
Bluetooth Class	E0
Chip/Smartcard Interface Device (CCID)	0B
HUB Class	09
Human Interface device (HID)	03
Mass Storage Class (MSC)	08
Printer Class	07
Scan/Imaging (PTP)	06
USB Audio Class	01
MODEM Class (CDC)	02
Video Class (UVC)	0E

I. End of Configuration Wizard

After completing configuration, click the “Finish” button to end the Configuration Wizard.

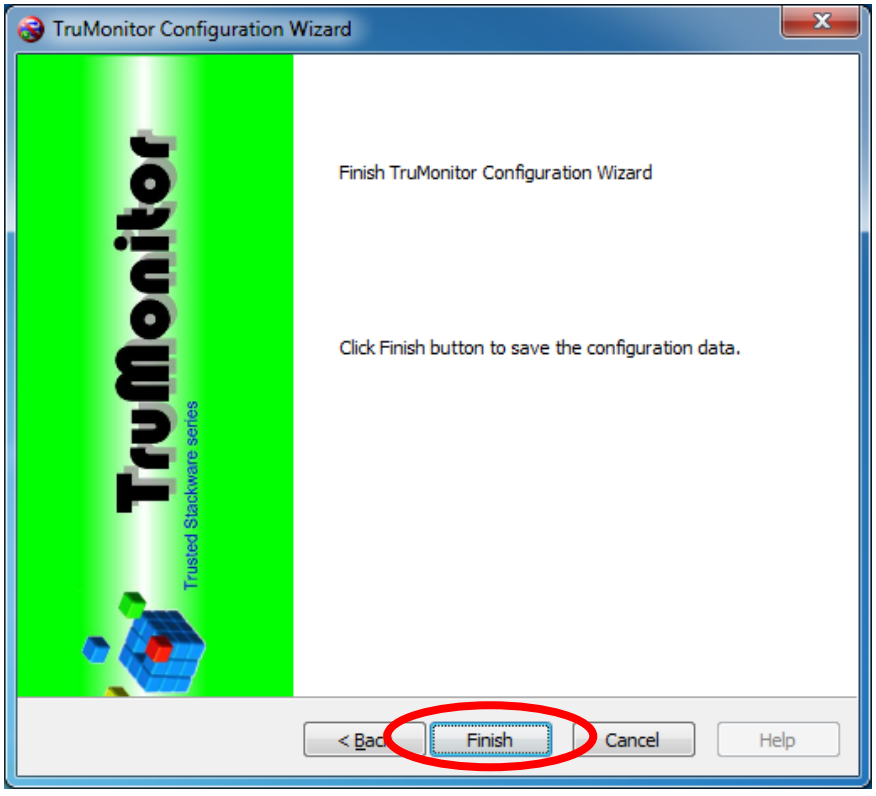

Figure 45 End of Configuration Wizard

The configured data will be discarded (however, data imported with the “Import...” button on the “Basic Configuration” page will not be discarded) if you click the “Cancel” button. The following message will be displayed as a precaution in the case of cancellation.

Confirm whether unauthorized devices are detached, then, click the “OK” button. If the unauthorized devices are still attached, the protective action (At Boot) will be performed right after the end of the Configuration Wizard.

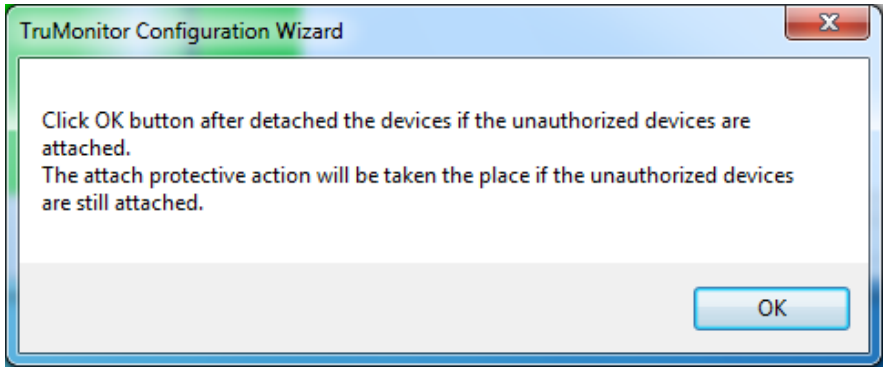

Figure 46 Warning Message at Cancel Configuration

Also, if the configuration of the “Removable Storage Access Configuration” page is modified, the following popup message will be displayed as a precaution after restarting of TruMonitor service. Click the “Yes” button to apply immediately. The OS will be rebooted if the “Yes” button is clicked. If you do not want to reboot the OS immediately, click the “No” button. In that case, the last modified configuration will not be applied until the OS is rebooted.

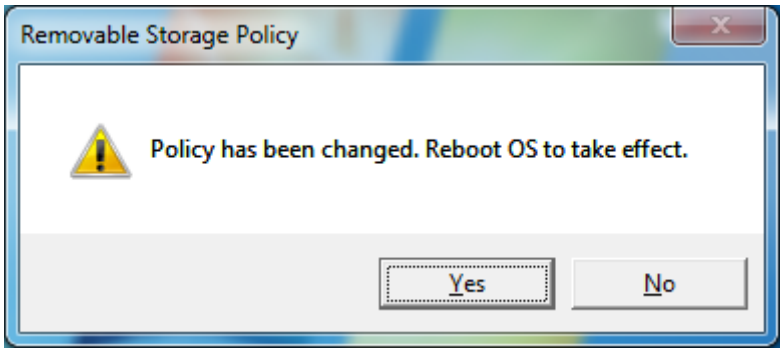

Figure 47 Warning Message at changing of Removable Storage Policy

End of document

Questions to Trusted Stackware series product
D.O.I-Net Co., Ltd.
Zip Code: 190-0011
2-25-23 Takamatsu, Tachikawa, Tokyo JAPAN
E-Mail: info@doi-net.com
URL: https://www.doi-net.com/