TruMonitor

Client
Setup Guide

Rev. 1.0.3

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	2015/04/09	Updated Distribution Example using Policy Template section based upon Windows Server 2008.
1.0.3	2023/11/07	Changed Supported OSs.

Index

1. Introduction 7
2. Required Environment 7
   a. TruLog Service 7
   b. TruMonitor 7
3. Setup Summary 7
4. How to Create Configuration Data 8
   a. TruLog Service 8
      i. TruLog Service Installation 8
      ii. TruLog Service Client/Server Settings 8
      iii. Create TruLog Service Configuration Data 8
   b. TruMonitor 8
      i. TruMonitor Installation 8
      ii. TruMonitor Settings 8
      iii. Create TruMonitor Configuration Data 9
5. How to Distribute Installer 9
   a. TruLog Trusted Stackware Logging Service.msi Installer Distribution 9
   b. TruMonitor Trusted Stackware Illegal Device Interceptor.msi Installer Distribution 9
6. How to Distribute Configuration Data 9
   a. Distribute TruLog Service Configuration Data 9
   b. Distribute TruMonitor Configuration Data 9
7. Distribution Example using Group Policy 10
   a. Create Distribution Point 10
   b. Create Group Policy Object for Distribution 10
      i. Launch Active Directory Users and Computers 10
      ii. Create New OU 11
      iii. Registration of Distribution Target Client PCs 12
      iv. Create New Group Policy Object 13
   c. Create Group Policy for Distribution 14
      i. Software Settings 14
      ii. Template Configuration 17
         1) Add Template 17
         2) Template Settings 19
   d. Distribution 21
   e. Create White List 22
      i. USB Device Sampling 22
      ii. Create Device List 22

iii. White List Settings 22
iv. Create White List 22
f. White List Distribution 22
i. Template Configuration 22
1) Add Template 22
2) Template Settings 24
ii. Distribution 26
g. How to Change Service Startup Type 26
i. Template Configuration 27
1) TruLog Service service 27
2) TruMonitor service 28
ii. Apply Changes 30
h. Procedure of Policy Template Update 30

Figure Index

Figure 1 Active Directory Users and Computers - launch 11
Figure 2 Active Directory Users and Computers - create new OU 11
Figure 3 Create OU 12
Figure 4 Active Directory Users and Computers - register PCs to new OU 12
Figure 5 Group Policy Management - create new GPO 13
Figure 6 New GPO - designate Name 13
Figure 7 Group Policy Management - edit Policy 14
Figure 8 Group Policy Management Editor - software installation 15
Figure 9 Group Policy Management Editor - create the package 15
Figure 10 Designate Distribution Installer File 16
Figure 11 Select Software Deployment Method 17
Figure 12 Group Policy Management Editor - add Template 18
Figure 13 Add/Remove Templates - launch 18
Figure 14 Select TruLog Service Policy Template 19
Figure 15 Add/Remove Templates - TruLog Service Policy Template added 19
Figure 16 Group Policy Management Editor - TruLog Service settings 20
Figure 17 TruLog Service Properties 21
Figure 18 Group Policy Management Editor - add Template 23
Figure 19 Add/Remove Templates - launch 23
Figure 20 Select TruMonitor Policy Template 24
Figure 21 Add/Remove Templates - TruMonitor Policy Template added 24
Figure 22 Group Policy Management Editor - TruMonitor settings 25
Figure 23 TruMonitor Properties 26
Figure 24 Group Policy Management Editor - TruLog Service service settings 27
Figure 25 TruLog Service service Properties 28
Figure 26 Group Policy Management Editor - TruMonitor service settings 29
Figure 27 TruMonitor service Properties 30

1. Introduction

This Setup Guide explains the procedure of network client configuration for TruMonitor produced by D.O.I-Net Co., Ltd.

For the network client configuration, you need to use the volume license edition of TruMonitor and TruLog Service.

2. Required Environment

a. TruLog Service

TruLog Service volume license edition installer package
Client PC for test
Server PC for logging
Windows Active Directory Server
Client PC for users

b. TruMonitor

TruMonitor volume license edition installer package
Client PC for test
Windows Active Directory Server
Client PC for users

It is assumed that the PCs are all connected to the same domain network.

3. Setup Summary

The settings will be roughly processed according to the following steps. The TruMonitor's Protective Action distributed at the last step, will be applied after rebooting each user's Client PC (restarting service).

① Create the setting data of TruLog Service on the Client PC for test.
② Distribute the setting data of the TruLog Service to the user's Client PC.
③ Distribute both of TruLog Service and TruMonitor installers to the user's Client PC.
④ Tentatively operate after distributing the installers correctly.
⑤ After operating for a while, output the connected device table as the Device List by using the TruMonitor Log Viewer for the logging Server PC.
⑥ Import the output Device List by using the "Import List" function on "White List Configuration" page of the TruMonitor Configuration Wizard on the Client PC for test.

⑦ Configure the filter, each protective action, and device selection by using the TruMonitor Configuration Wizard.

Note: The detection processing time becomes longer if the White List's registered device is increased. Please consider to reduce the White List's registered device by applying the White Filter and Device Filter.

⑧ Create the setting data of TruMonitor on the Client PC for test.

⑨ Distribute the setting data of TruMonitor to the user's Client PC.

4. How to Create Configuration Data

a. TruLog Service

Create the setting data of the TruLog Service to distribute it to the user's Client PC, according to the following steps.

i. TruLog Service Installation

Install the TruLog Service to the Client PC for test.

Similarly, install the TruLog Service to the Server PC for logging.

Note: You have to select the "Complete" on the Setup Type Selection Dialog Box (Silent Installation is not acceptable).

ii. TruLog Service Client/Server Settings

On the Client PC for test, launch the TruLog Service Configuration Wizard and configure it. Refer to the "Use on Client/Server System" section of TruLog Service Client/Server Configuration User's Guide for configuration detail.

iii. Create TruLog Service Configuration Data

Export the configuration data in "Policy Template" (In the case of using group policy) or "Registry File" (in the case of using other management tool) type by using the TruLog Service Configuration Wizard on the Client PC for test.

b. TruMonitor

Create the setting data of the TruMonitor to distribute it to the user's Client PC, according to the following steps.

i. TruMonitor Installation

Install the TruMonitor to the Client PC for test.

Note: You have to select the "Complete" on the Setup Type Selection Dialog Box (Silent Installation is not acceptable).

ii. TruMonitor Settings

On the Client PC for test, launch the TruMonitor Configuration Wizard and configure it. Refer to the TruMonitor User's Guide for configuration detail.

iii. **Create TruMonitor Configuration Data**

Export the configuration data in "Policy Template" (In the case of using group policy) or "Registry File" (in the case of using other management tool) type by using the TruMonitor Configuration Wizard on the Client PC for test.

Note: Please export after registering the product key in the real operating.

5. How to Distribute Installer

a. TruLog Trusted Stackware Logging Service.msi Installer Distribution

Distribute and install TruLog Trusted Stackware Logging Service.msi to each user's Client PC via the group policy on the Windows Active Directory Server or other network management tool.

To perform the silent installation, execute the following command on the user's Client PC.

msiexec.exe /i "TruLog Trusted Stackware Logging Service.msi" /qn

Note: TruLog Trusted Stackware Logging Service will be installed as "TruLog Service" with auto start type service program.

b. TruMonitor Trusted Stackware Illegal Device Interceptor.msi Installer Distribution

Distribute and install TruMonitor Trusted Stackware Illegal Device Interceptor.msi to each user's Client PC via the group policy on the Windows Active Directory Server or other network management tool.

To do the silent installation, execute the following command on the user's Client PC.

msiexec.exe /i "TruMonitor Trusted Stackware Illegal Device Interceptor.msi" /qn

Note: TruMonitor Trusted Stackware Illegal Device Interceptor will be installed as "TruMonitor" with auto start type service program.

6. How to Distribute Configuration Data

a. Distribute TruLog Service Configuration Data

Distribute the policy template made in section 4.a.iii to each user's Client PC via the group policy on Windows Active Directory Server, or distribute the registry file to HKLM of each user's Client PC by using other network management tool.

b. Distribute TruMonitor Configuration Data

Distribute the policy template made in section 4.b.iii to each user's Client PC via the group policy on Windows Active Directory Server, or distribute the registry file to HKLM of each user's Client PC by using other network management tool.

7. Distribution Example using Group Policy

Note: Please log on with the administrator privilege of the domain to operate the following application.

a. Create Distribution Point

If there is not the existing shared folder for accessing from each user's Client PC, create the network shared folder to keep the MSI installer files. When creating that shared folder, grant the access right of "Read & execute", "List folder content" and "Read" to "Administrators", "Authenticated users" and "Domain users" group.

Next, copy TruLog Trusted Stackware Logging Service.msi and TruMonitor Trusted Stackware Illegal Device Interceptor.msi to this folder.

b. Create Group Policy Object for Distribution

In this section, you make the group policy object, and link it to the Active Directory Container containing the MSI installer distribution target client PCs.

i. Launch Active Directory Users and Computers

On Active Directory Server, click in the order of "Start" – "Windows Administrative Tools" – "Active Directory Users and Computers".

If it is launched normally, Active Directory Users and Computers console as follows will be displayed.

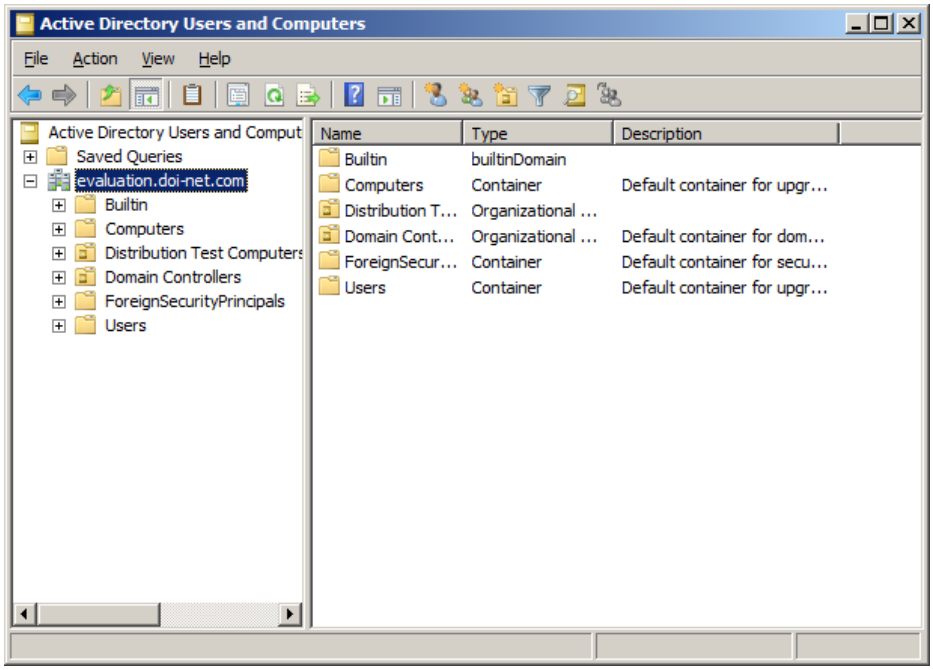

Figure 1 Active Directory Users and Computers - launch

ii. Create New OU

When Active Directory Users and Computers console is displayed, click the right mouse button on the distribution target domain in the left pane, and select “New” – “Organizational Unit”.

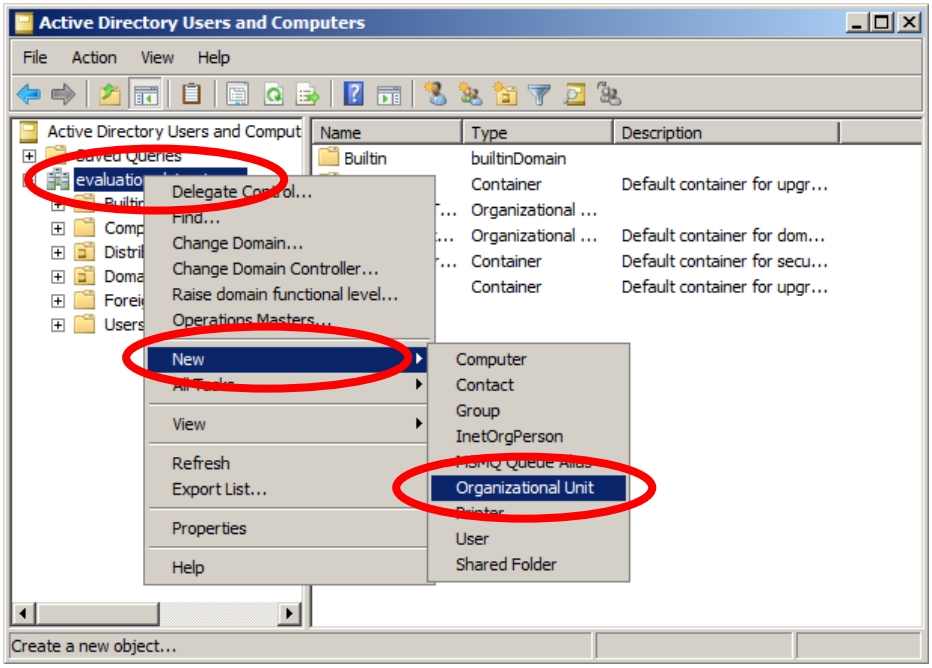

Figure 2 Active Directory Users and Computers - create new OU

When New Object - Organizational Unit dialog box as follows is displayed, enter any

OU name in “Name” edit box, and click the “OK” button.

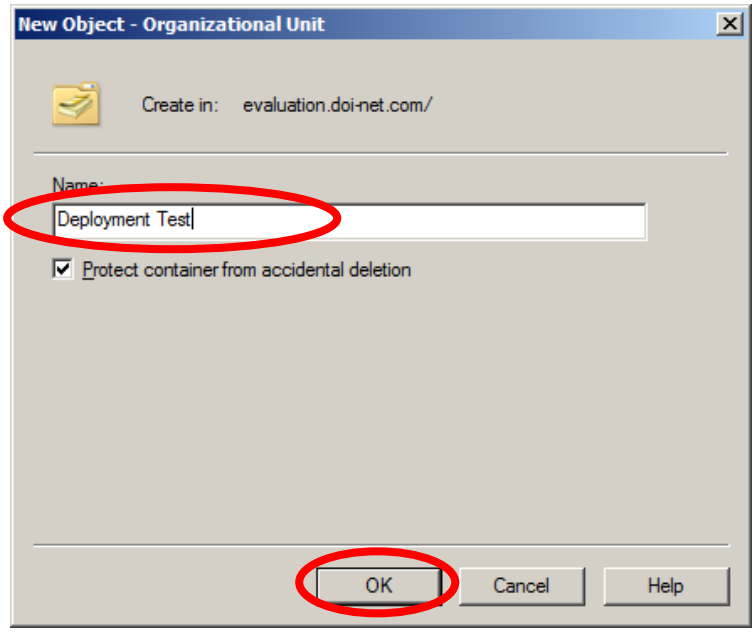

Figure 3 Create OU

iii. Registration of Distribution Target Client PCs

When it brings back to Active Directory Users and Computers console, select the created OU in the left pane, and register the distribution target client PCs in the right pane. Then, close Active Directory Users and Computers console.

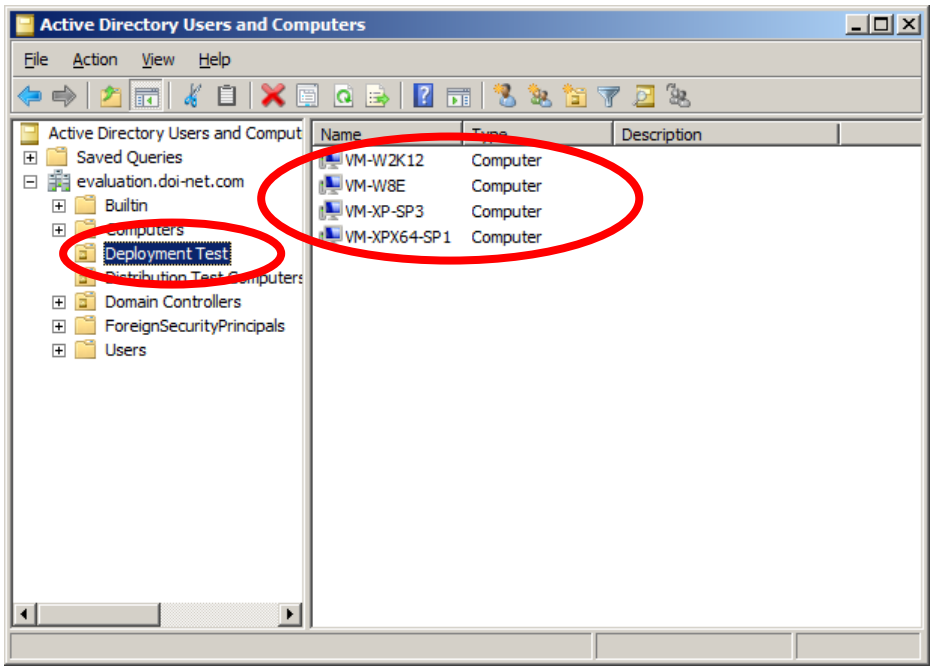

Figure 4 Active Directory Users and Computers - register PCs to new OU

iv. Create New Group Policy Object

Next, click in the order of “Start” – “Windows Administrative Tools” – “Group Policy Management”.

When Group Policy Management console as follows is displayed, click the right mouse button on the newly created OU in the left pane, and select “Create a GPO in this domain, and Link it here...”

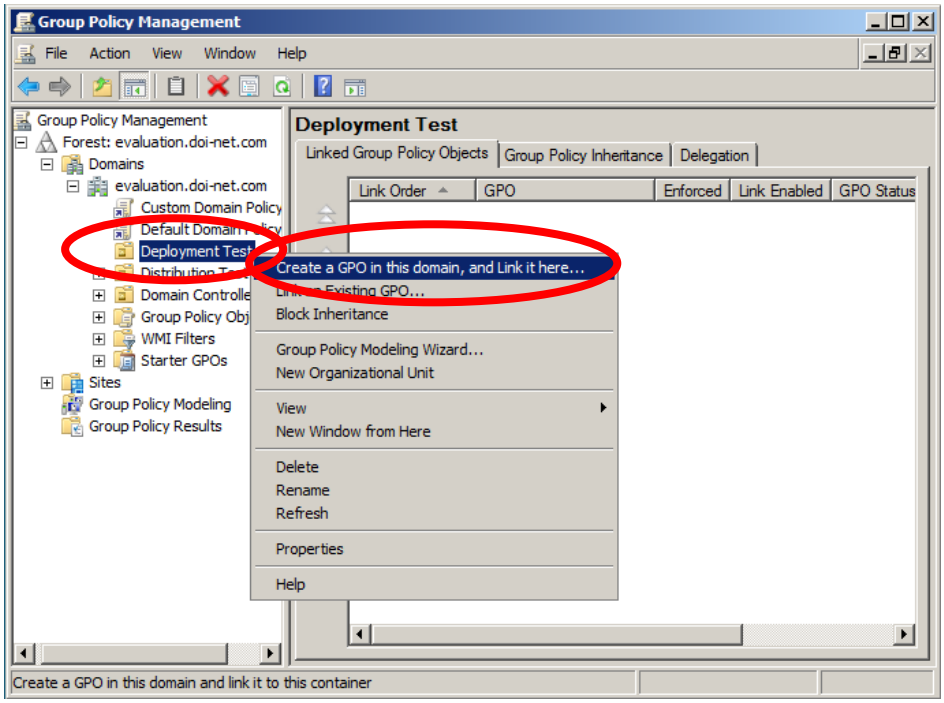

Figure 5 Group Policy Management - create new GPO

When New GPO dialog box as follows is displayed, enter any Policy Name in “Name” edit box, and click the “OK” button.

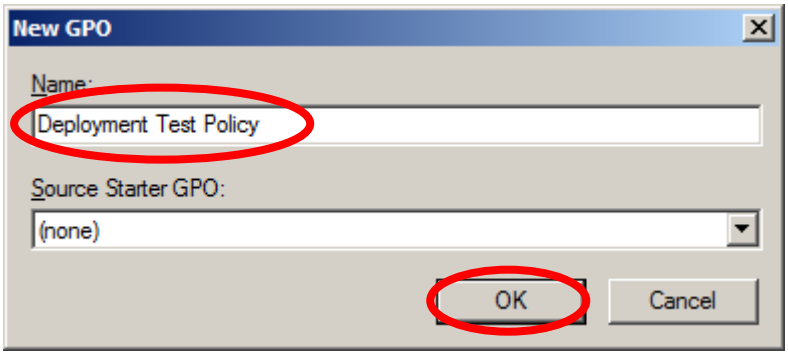

Figure 6 New GPO - designate Name

When it brings back to the Group Policy Management console, click the right mouse button on the newly created policy in the left pane, and select “Edit...”

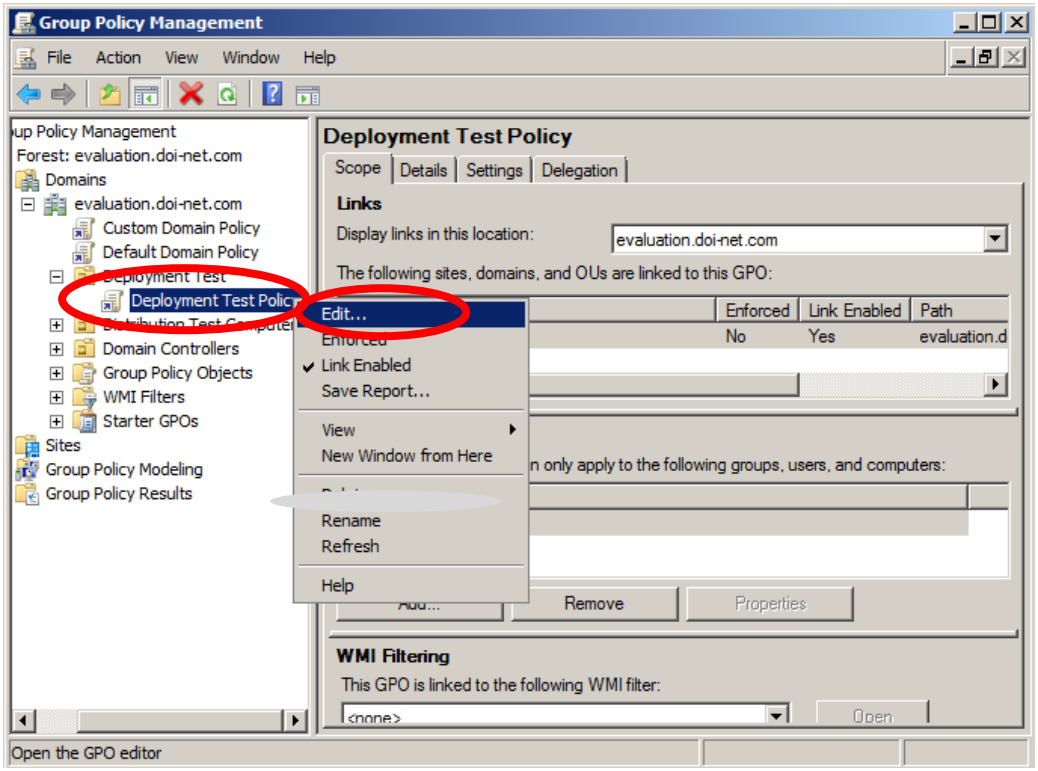

Figure 7 Group Policy Management - edit Policy

c. Create Group Policy for Distribution

After creating the group policy object, create the distribution group policy.

i. Software Settings

When Group Policy Management Editor console is displayed, click the right mouse button on “Software Installation” in the left pane.

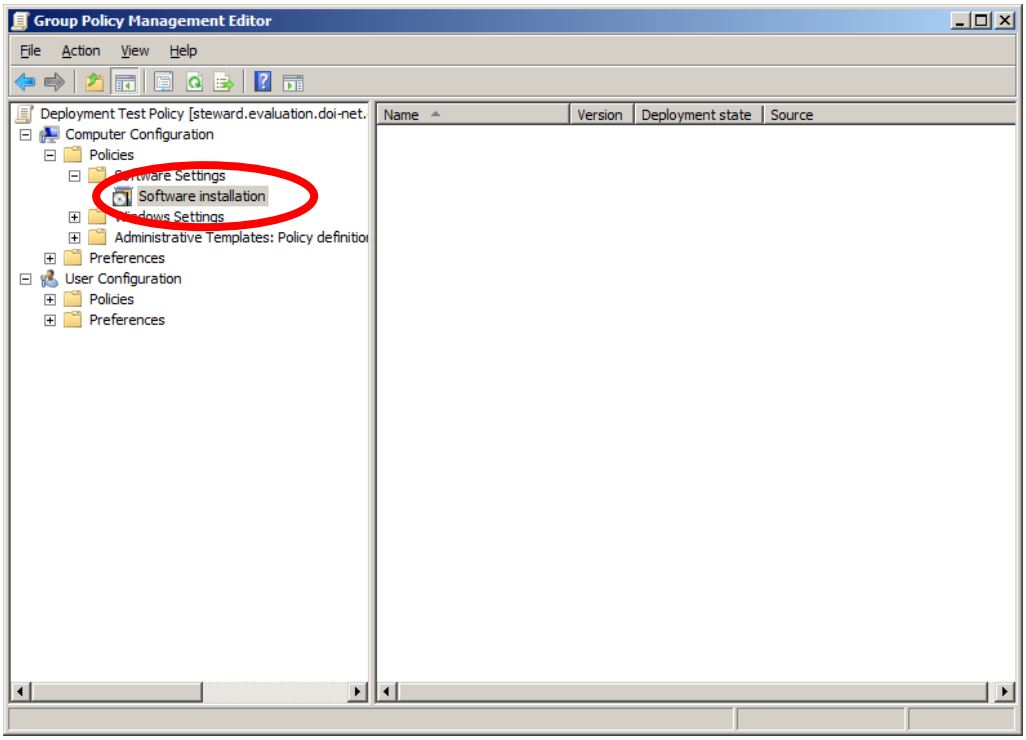

Figure 8 Group Policy Management Editor - software installation

Next, click in the order of “New” – “Package…”.

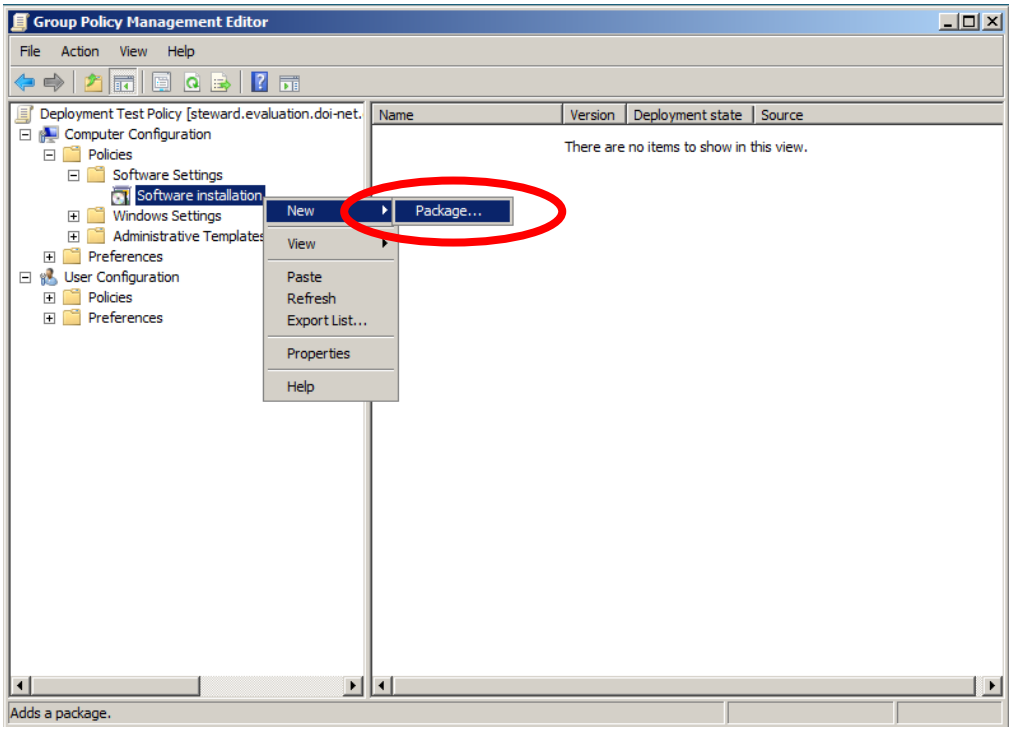

Figure 9 Group Policy Management Editor - create the package

When the Open dialog box is displayed, follow to the previously created distribution point from “Network” in the left pane, specify the copied MSI installer file, and click the “Open” button. Repeat this process for TruLog Trusted Stackware Logging Service.msi and TruMonitor Trusted Stackware Illegal Device Interceptor.msi respectively.

Note: You have to follow from “Network” since the file should be specified in UNC path.

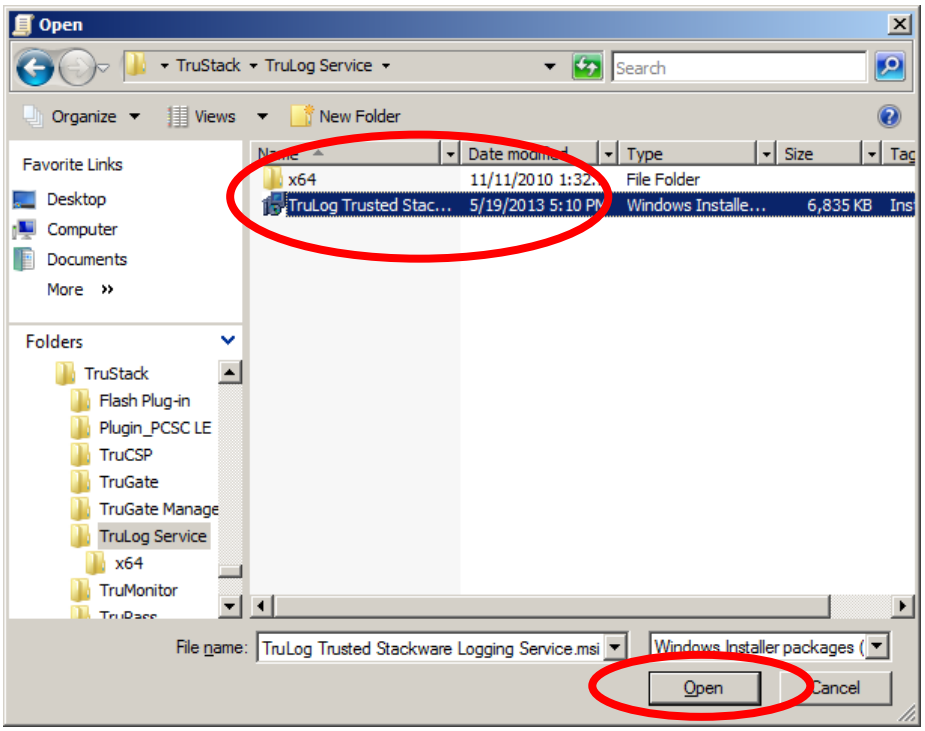

Figure 10 Designate Distribution Installer File

Next, the Deploy Software dialog box is displayed, click the “OK” button.

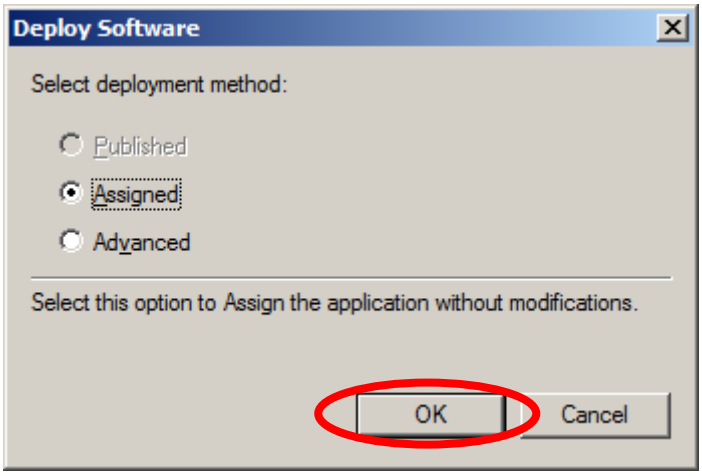

Figure 11 Select Software Deployment Method

ii. Template Configuration

1) Add Template

After creating the group policy object, import the administrative template. First, copy the TruLog Service policy template (ADM file) to the <OS folder name>¥inf folder of Active Directory Server. Then, on Group Policy Management Editor console, click the right mouse button on “Administrative Templates: Policy definitions” in the left pane, and select “Add/Remove Templates...”

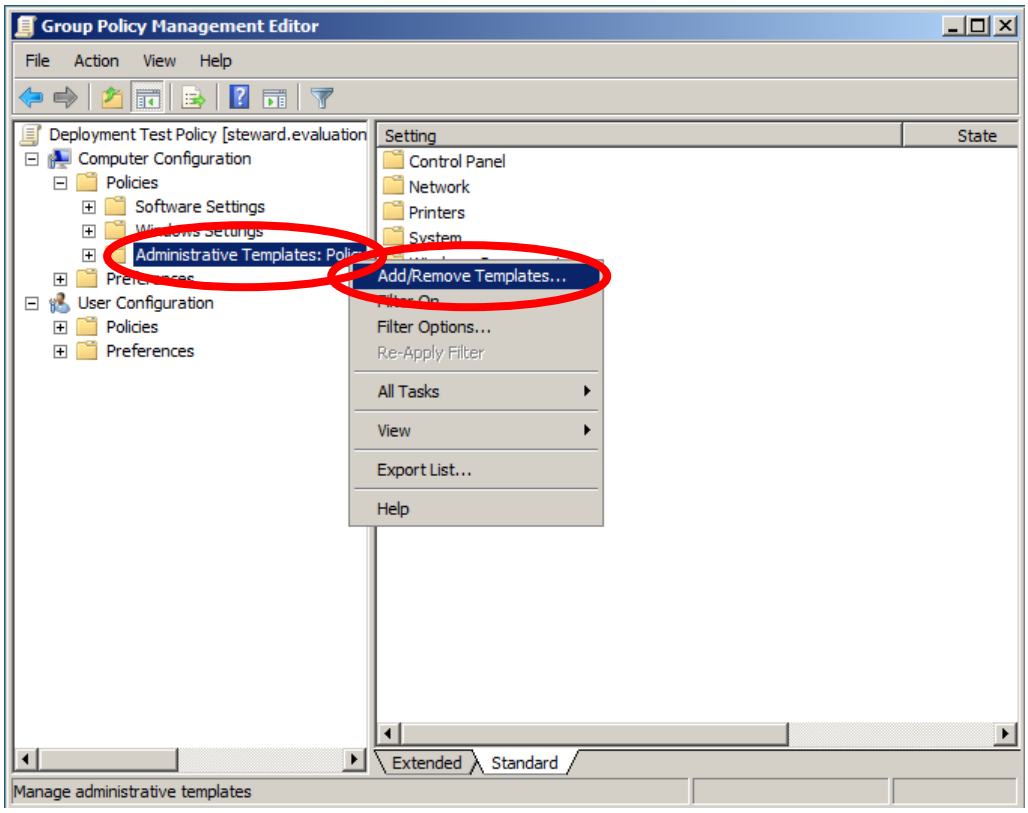

Figure 12 Group Policy Management Editor - add Template

When Add/Remove Templates dialog box as follows is displayed, click the "Add..." button.

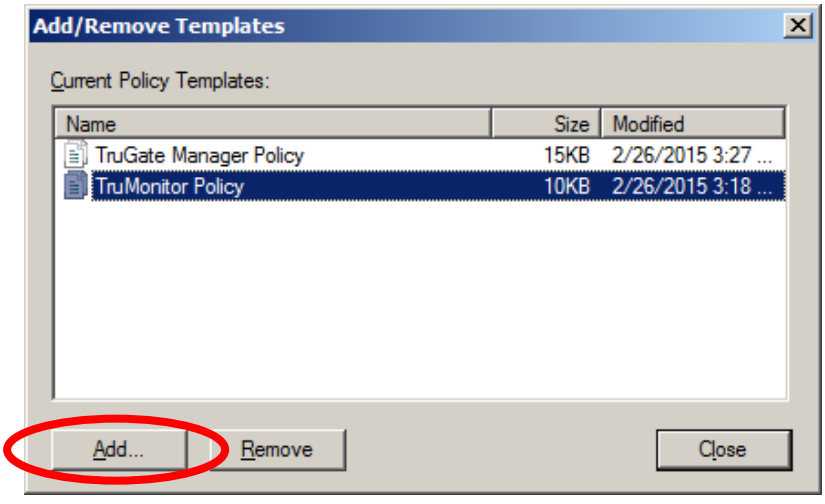

Figure 13 Add/Remove Templates - launch

If Policy Templates dialog box is displayed, select the copied TruLog Service policy template, and click the "Open" button.

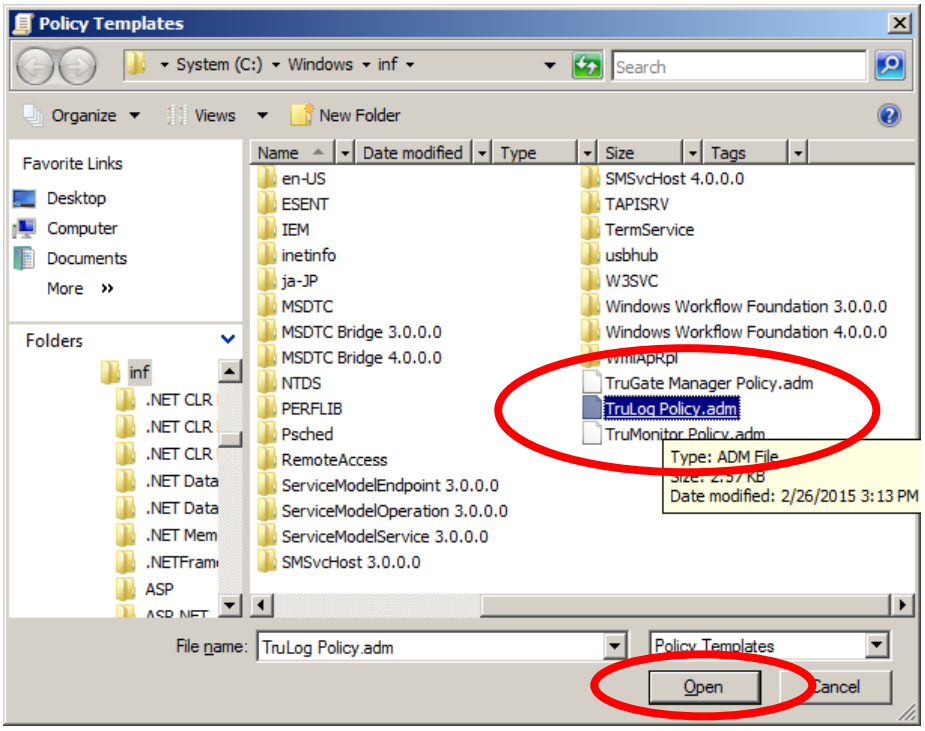

Figure 14 Select TruLog Service Policy Template

After completing to add the template, click the “Close” button on Add/Remove Template dialog box.

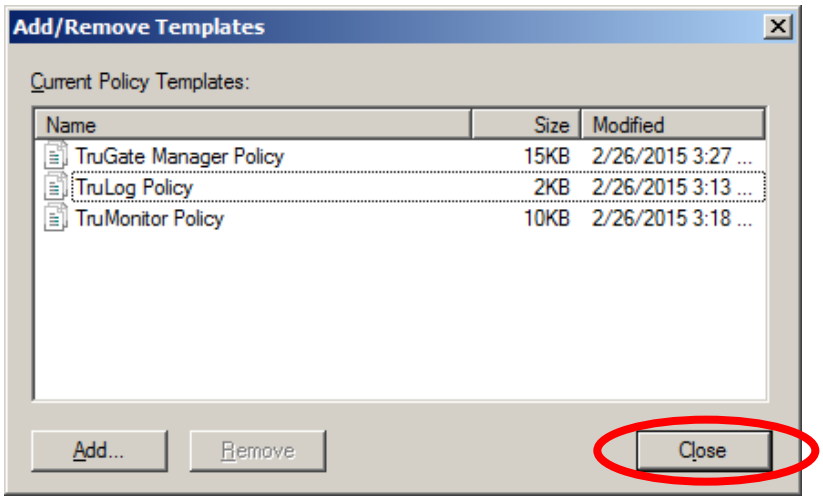

Figure 15 Add/Remove Templates - TruLog Service Policy Template added

2) Template Settings

When it returns to the Group Policy Management Editor console, select in the order of “Administrative Templates: Policy definitions” – “Classic Administrative Templates” – “TruStack” – “TruLog Service ver.x.x.x” in the left pane, and

double click “TruLog Service” in the right pane.

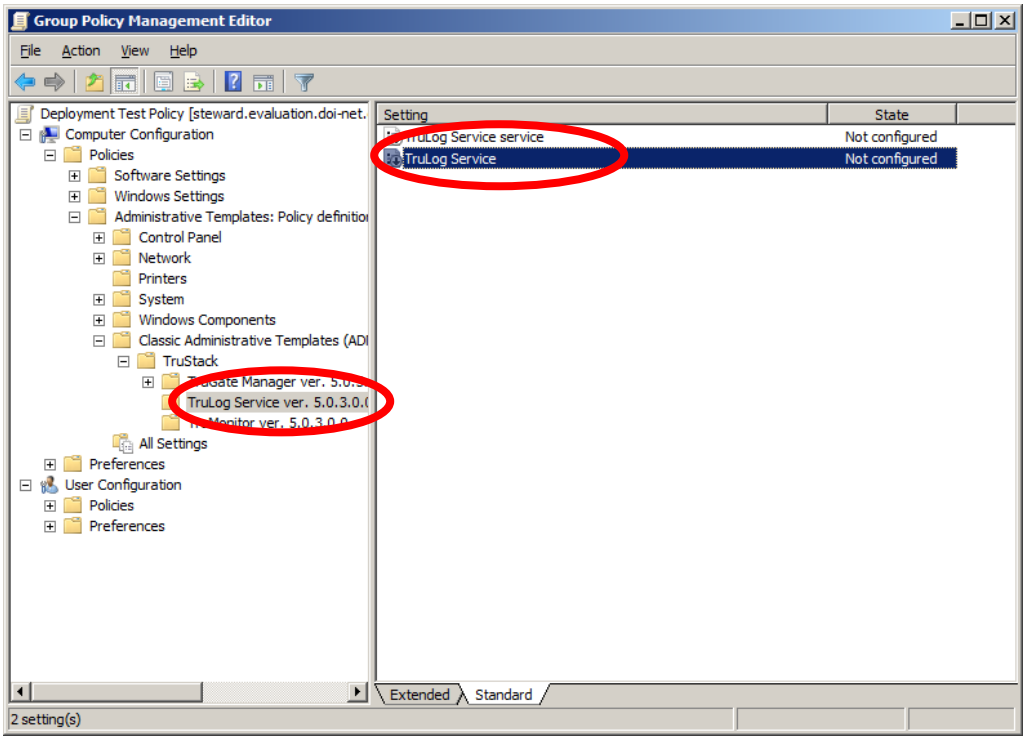

Figure 16 Group Policy Management Editor - TruLog Service settings

When TruLog Service Properties dialog box as follows is displayed, select the “Enabled” radio button and enter the setting data in the lower pane. Generally, however, this product should be used without modification. Click the “OK” button after completing.

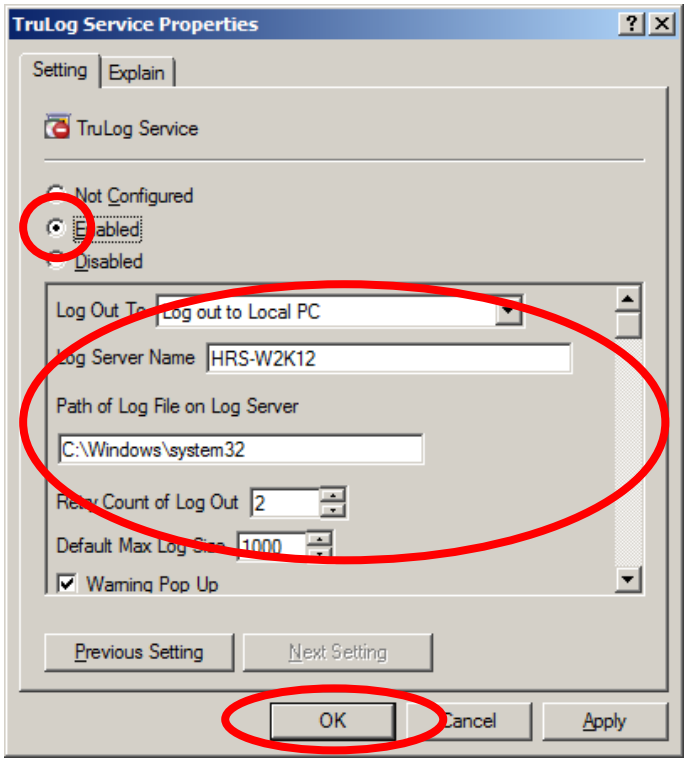

Figure 17 TruLog Service Properties

When you return to the Group Policy Management Editor console, click in the order of "File" – "Exit" to complete.

d. Distribution

After the distribution group policy is created, that group policy will be applied when the distribution target client PC is rebooted.

If you want to apply the group policy immediately, execute the following command within the command prompt on the client PC.

gpupdate.exe /force

Note: For rapid application and management of the policy, it is recommended to utilize the following policy at the same time.

① "Computer Configuration" – "Policies" – "Administrative Templates: Policy definitions" – "System" – "Logon" – "Always wait for the network at computer startup and logon".

② "Computer Configuration" – "Policies" – "Administrative Templates: Policy definitions" – "Network" – "Network Connection" – "Windows Firewall" – "Domain Profile" – "Windows Firewall: Allow inbound remote administration exception".

e. Create White List

Create the settings of TruMonitor to distribute it to the user's Client PC according to the following procedure.

i. USB Device Sampling

After distributing the software normally, operate it temporarily in a while.

ii. Create Device List

After that, create the table of devices that were connected with that period by using the TruMonitor Log Viewer for the logging Server PC, and output it as the Device List.

iii. White List Settings

Launch the TruMonitor Configuration Wizard on the Client PC for test, import the above Device List by using the "Import List" function on "White List Configuration" page. For more detail of Import, refer to the TruMonitor User's Guide.

Note: Use the filter functions according to the necessity in setting together. It is recommended to apply USB HID class, IDE and SCSI disk device filtering also.

iv. Create White List

Export the configuration file in "Policy Template" type by TruMonitor Configuration Wizard on the testing Client PC. The White List will be included in the configuration file with other settings data.

f. White List Distribution

After creating the White List, add it to the distribution group policy, and distribute it to the user's Client PC.

i. Template Configuration

1) Add Template

After creating the group policy object, import the administrative template. First, copy the TruMonitor policy template (ADM file) to the <OS folder name>¥inf folder of Active Directory Server. Then, on Group Policy Management Editor console, click the right mouse button on "Administrative Templates: Policy definitions" in the left pane, and select "Add/Remove Templates..."

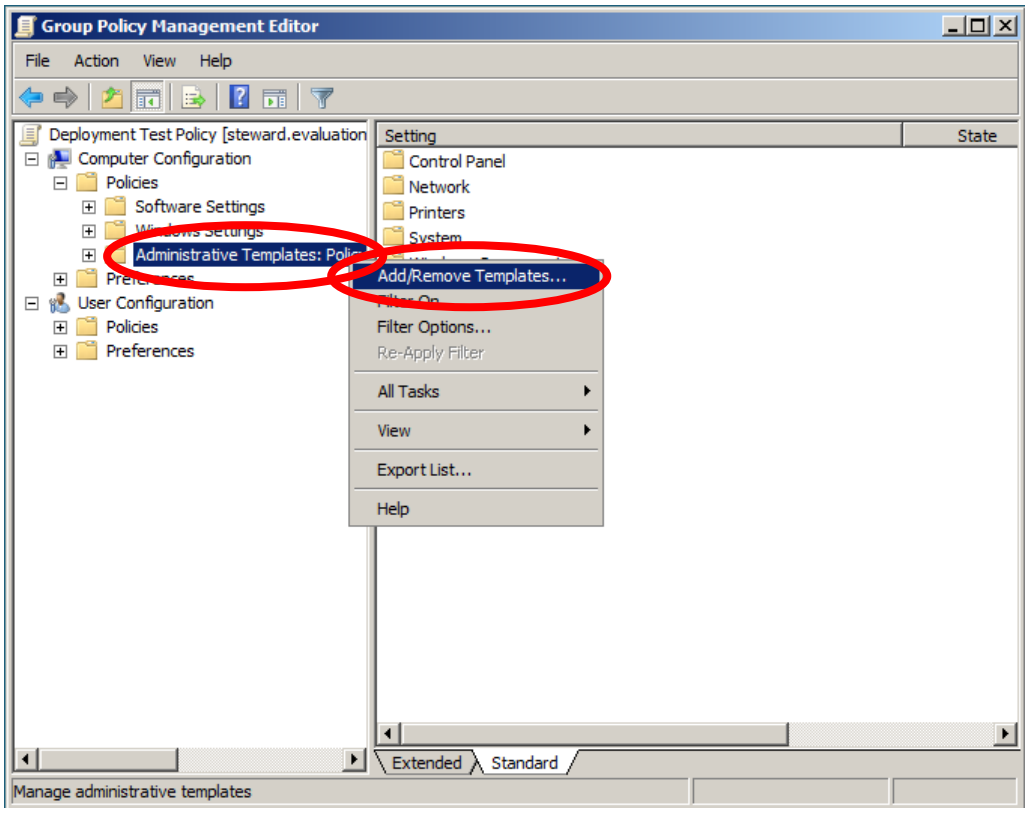

Figure 18 Group Policy Management Editor - add Template

When Add/Remove Templates dialog box as follows is displayed, click the "Add..." button.

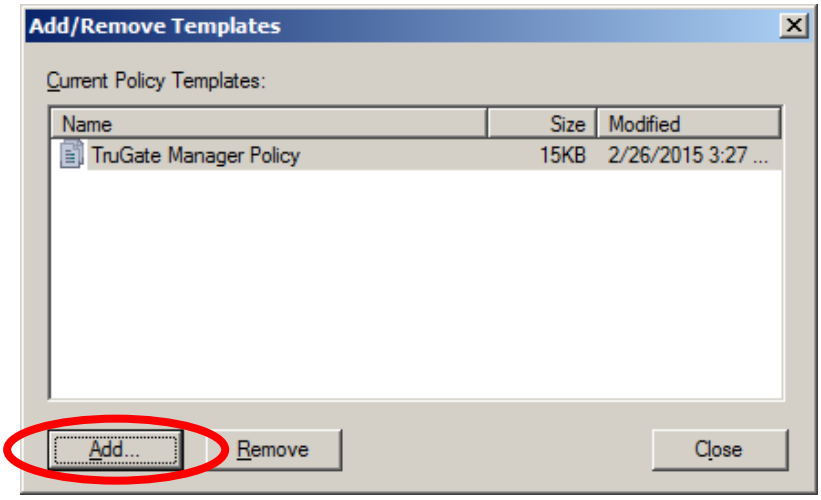

Figure 19 Add/Remove Templates - launch

If Policy Templates dialog box is displayed, select the copied TruMonitor policy template, and click the "Open" button.

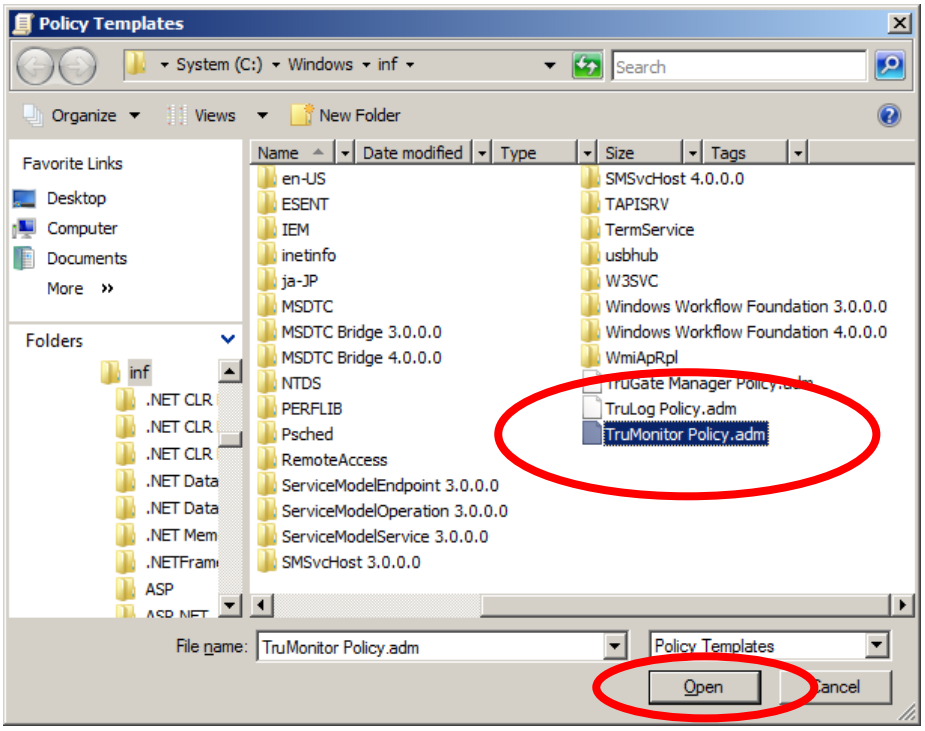

Figure 20 Select TruMonitor Policy Template

After completing to add the template, click the “Close” button on Add/Remove Template dialog box.

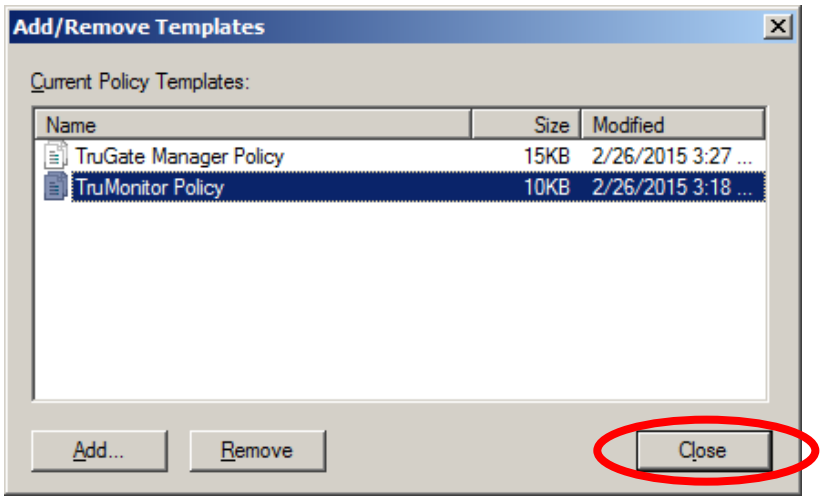

Figure 21 Add/Remove Templates - TruMonitor Policy Template added

2) Template Settings

When it returns to the Group Policy Management Editor console, select in the order of “Administrative Templates: Policy definitions” – “Classic Administrative Templates” – “TruStack” – “TruMonitor ver.x.x.x” in the left pane, and double

click “TruMonitor” in the right pane.

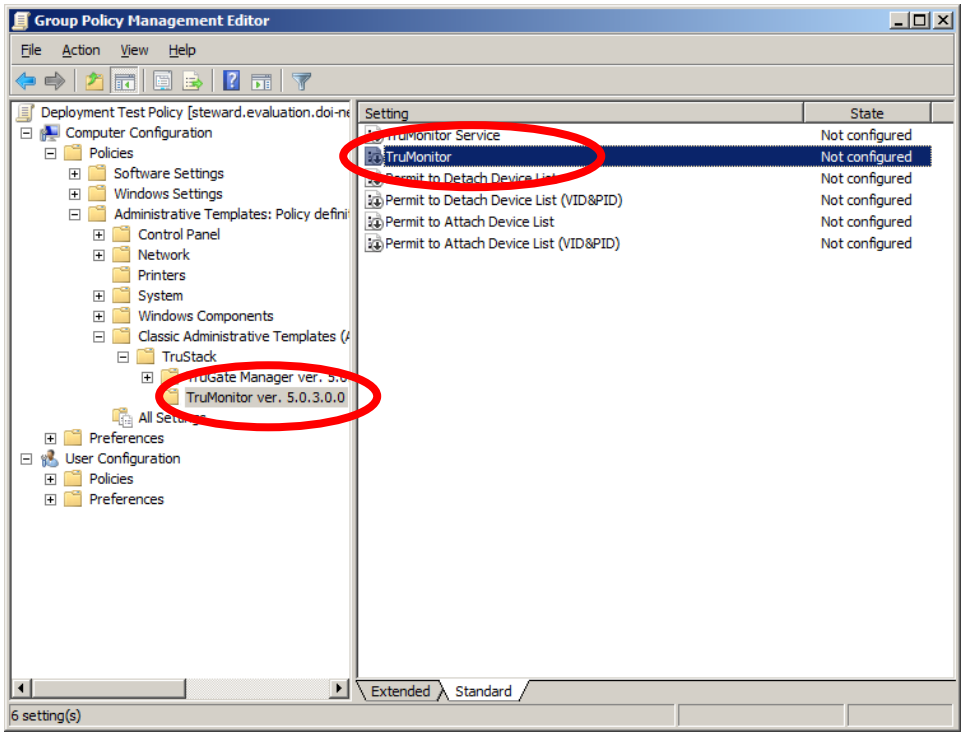

Figure 22 Group Policy Management Editor - TruMonitor settings

When TruMonitor Properties dialog box as follows is displayed, select the “Enabled” radio button and enter the setting data in the lower pane. Generally, however, this product should be used without modification. Click the “OK” button after completing.

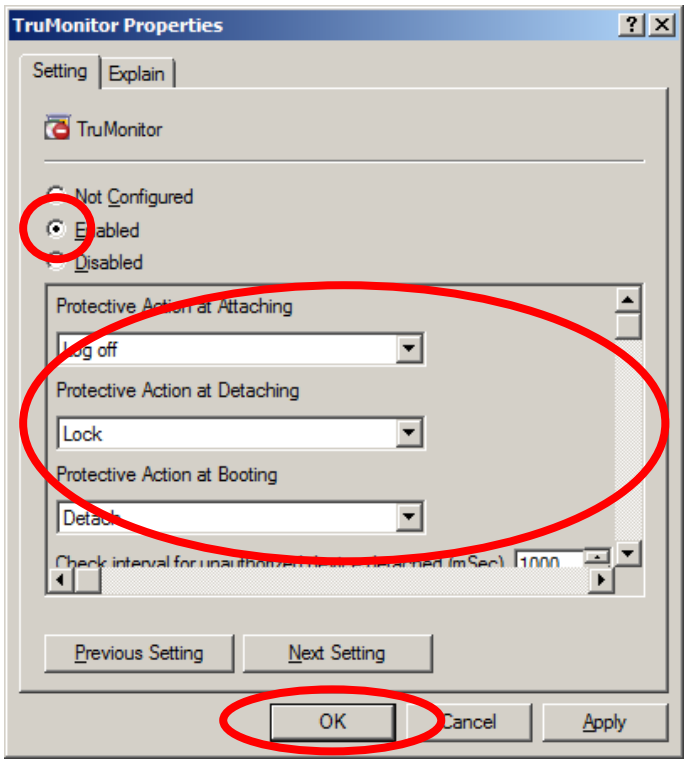

Figure 23 TruMonitor Properties

Also, select the “Enabled” radio button and click the “OK” button for “Permit to Detach Device List Properties”, “Permit to Detach Device List (VID&PID) Properties”, “Permit to Attach Device List Properties” and “Permit to Attach Device List (VID&PID) Properties” respectively.

When you return to the Group Policy Management Editor console, click in the order of “File” – “Exit” to complete.

ii. Distribution

After the distribution group policy is updated, and the group policy for user’s Client PC belonging to OU created above is updated, the updated group policy for that PC will be applied.

g. How to Change Service Startup Type

Please follow the below operation If you want to change the startup type of the service. Also, the below operation should be taken after confirming the distribution of the program to the targeted user’s Client PC is complete.

i. Template Configuration

1) TruLog Service service

Launch the Group Policy Management Editor console, select in the order of “Administrative Templates: Policy definitions” – “Classic Administrative Templates” – “TruStack” – “TruLog Service ver.x.x.x” in the left pane, and double click “TruLog Service service” in the right pane.

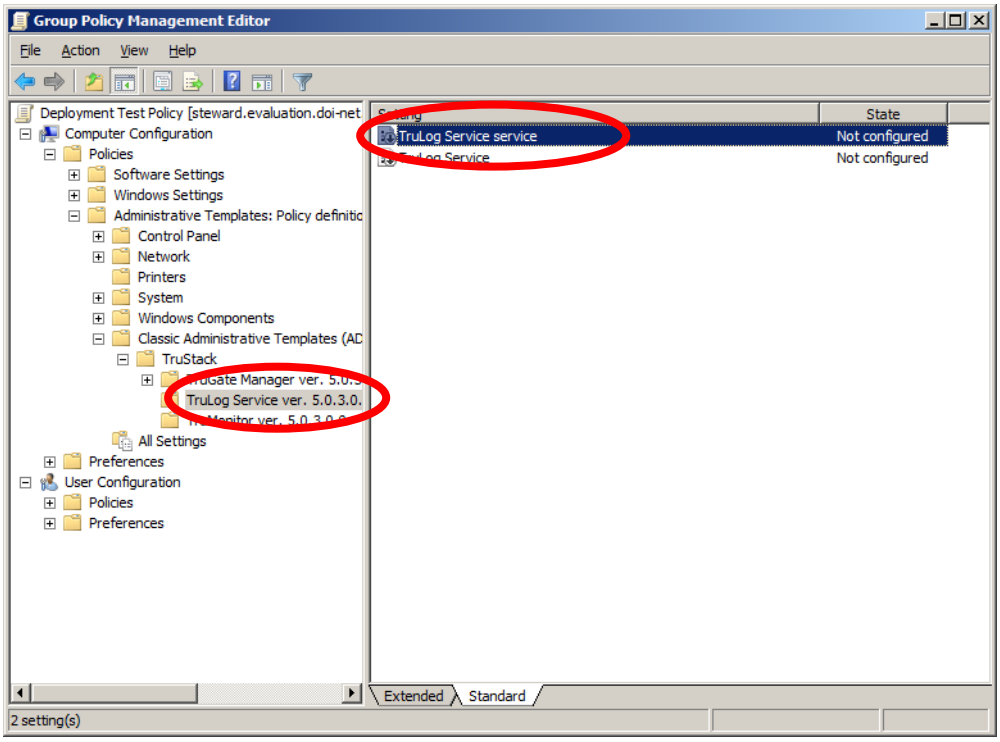

Figure 24 Group Policy Management Editor - TruLog Service service settings

When TruLog Service service Properties dialog box as follows is displayed, select the “Enabled” radio button and select the desired type from the “Start Up Type” drop down list in the lower pane. When you have finished the settings, click the “OK” button.

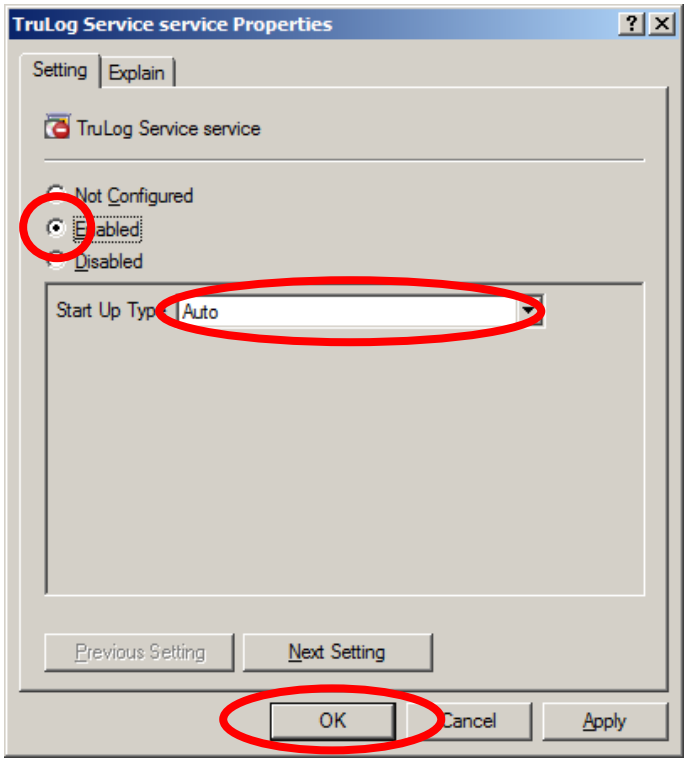

Figure 25 TruLog Service service Properties

When you return to the Group Policy Management Editor console, click in the order of “File” – “Exit” to complete. Subsequently, it returns to Group Policy Management console, close it as well.

2) TruMonitor service

Launch the Group Policy Management Editor console, select in the order of “Administrative Templates: Policy definitions” – “Classic Administrative Templates” – “TruStack” – “TruMonitor ver.x.x.x” in the left pane, and double click “TruMonitor Service” in the right pane.

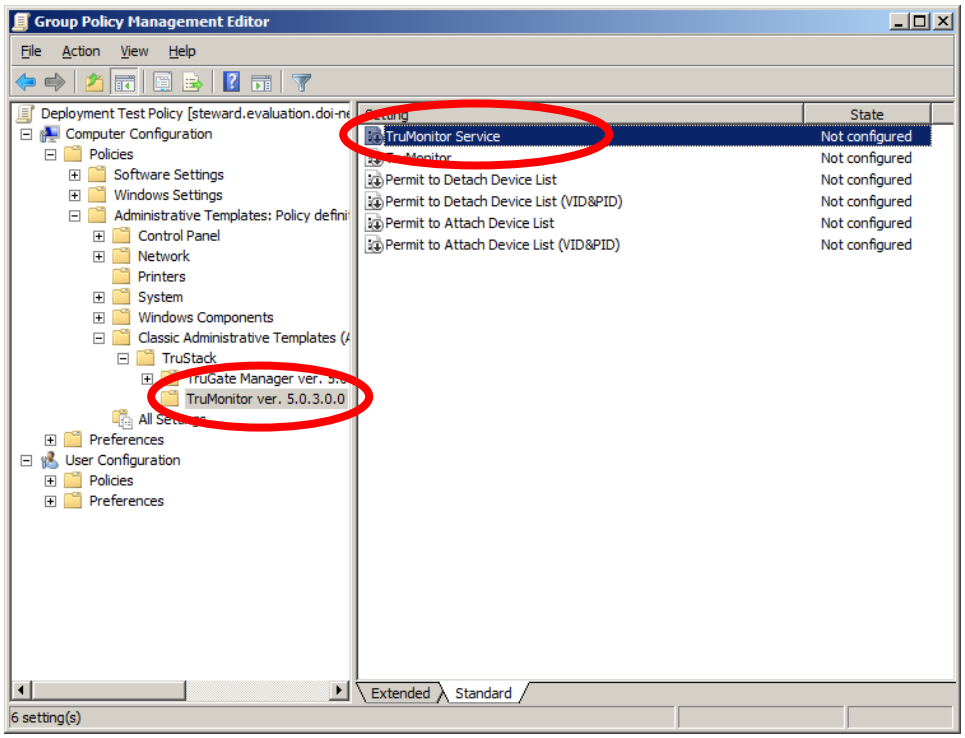

Figure 26 Group Policy Management Editor - TruMonitor service settings

When TruMonitor Service Properties dialog box as follows is displayed, select the “Enabled” radio button and select the desired type from the “Start Up Type” drop down list in the lower pane. When you have finished the settings, click the “OK” button.

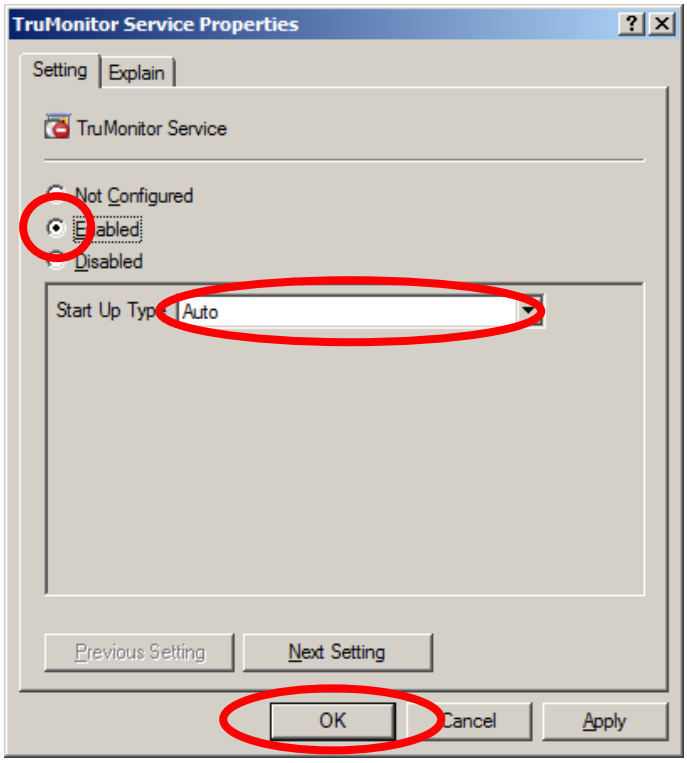

Figure 27 TruMonitor service Properties

When you return to the Group Policy Management Editor console, click in the order of “File” – “Exit” to complete. Subsequently, it returns to Group Policy Management console, close it as well.

ii. Apply Changes

After the distribution group policy is updated, that updated startup type will be applied when the distribution target client PC is rebooted.

h. Procedure of Policy Template Update

To update the policy template, follow the procedure below.

① Temporarily change the using template to “Disabled”. If the settings data are empty, it will be changed to “Not Configured” after applying “Disabled”.

② Copy the renewal template to <OS folder name>¥inf folder of Active Directory Server with a different name from existing.

③ Add the renewal template.

Note: The Configuration Wizard increments the internal revision number of the policy template when the configuration is changed.

④ Select the “Enabled” radio button after confirming the setting data of renewal template.

⑤ Change the previous template to “Not Configured” after the renewal template is distributed with all target PCs.

⑥ When the previous template becomes no more necessary, delete it from Add/Remove Templates dialog box, after that delete the previous template file from <OS folder name>¥inf folder of Active Directory Server.

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/trustack/