Curtain™ LogTrace 5.0

Installation Guide

Release date: Jul 1, 2024
Copyright (c) 2002-2024. Coworkshop Solutions Limited

Contact your Authorized Curtain Reseller or Service Provider to report problems and/or provide feedback.

Additional help resources or updates will be available by emailing info@coworkshop.com

Coworkshop Solutions Ltd. reserves the right to make changes to this document and to the product described herein without notice. The software described in this manual is furnished under the terms and conditions of the Curtain Software License Agreement and may be used or copied only in accordance with the terms of the agreement.

For information about your legal rights concerning the use of the Curtain LogTrace, please refer to the Curtain Software License agreement.

© 2002-2024 Coworkshop Solutions Ltd. All Rights Reserved. Curtain belongs to Coworkshop Solutions Ltd. All other brand names, product names, or trademarks belong to their respective holders.

Table of Contents

1 - Introduction

1.1 - Challenge of tracing user's file activities

In the daily work environment, companies often need to authorize their employees to access and use sensitive company data. However, most companies lack visibility into how their employees are actually utilizing this data, and whether any misuse is occurring.

At the same time, companies have to meet internal audit requirements and comply with various data security regulations and policies. This creates a need for the IT department to find ways to effectively monitor and record how employees are accessing and using the company's data resources.

Additionally, management is seeking proactive security alerts that can detect abnormal user behavior, allowing them to take immediate action to minimize potential risks and damages to the organization.
While Windows does have built-in logging capabilities, these logs can be difficult to read and interpret. Furthermore, the logs are stored locally on individual user machines, making it challenging for administrators to centrally review and analyze user activity records.

There are enterprise-grade solutions like SIEM (Security Information and Event Management) systems that provide comprehensive user activity monitoring and reporting. However, these sophisticated tools can be cost-prohibitive, especially for small to medium-sized businesses.

The key security challenge lies in finding a simple, user-friendly and cost-effective logging solution that can satisfy the company's requirements for visibility into employee file activities, compliance reporting, and proactive security monitoring - all within a centralized platform accessible to IT and management.

1.2 - What is the purpose of Curtain LogTrace?

Curtain LogTrace provides IT system administrators with a simple, easy-to-use, and cost-effective logging solution. LogTrace can record various file operations performed by users, such as creating, copying, moving, deleting, renaming, printing, opening, closing, and saving files. For copy and move operations, the software also records the source and destination paths, as well as the disk type, allowing administrators to generate reports specifically for files copied to USB devices.

The log records are automatically uploaded from the user's computer to the central management console, enabling administrators to filter the records based on different criteria and view the user's activities from various perspectives. For large enterprises, the software offers features like AD system integration, password management, anti-uninstallation protection, support for large-scale databases, and MSI-based bulk installation.

The software comes in both Free version and Paid version. The free version provides excellent basic functionality, capable of recording the majority of user file operations. The paid version offers more comprehensive logging capabilities and supports additional enterprise-level features, such as AD system integration and MSI-based bulk installation. The price of the paid version is very reasonable, possibly only a tenth of the cost of a SIEM solution, but it still provides excellent logging capabilities.

1.3 - Components of Curtain LogTrace

There are 2 basic components of Curtain LogTrace:
- Curtain Lite Client
- Curtain Lite Admin (for the machine having Curtain Lite Admin, we call it Curtain Policy Server)

Curtain Lite Client:
When administrators want to trace user's file activities, Curtain Lite Client must be installed in user's computers.

Curtain Lite Admin:
Curtain Lite Admin is mainly for administrators to define Curtain control policies centrally. In general, only one Curtain Lite Admin is needed in a company.

P.S.
- Curtain Lite Admin can be installed on physical machine or virtual machine (VM).
- For standalone computer, Curtain Lite Admin and Client can be installed on the same machine. It is recommended to enable password protection for Curtain Lite Admin for preventing users to change control policy.

2 - Preparation before Installation

2.1 - High-level Installation Plan

Preparation:
- Which computers do you want to trace user's file activities?
- What kind of user's file activities do you want to log (e.g. create file, delete file, copy file, etc)?
- Which server will act as Curtain Policy server (i.e. Curtain Lite Admin will be installed on that server)?
- Do you want to integrate Curtain LogTrace with Active Directory (so that control policy can be granted to AD user/user group)?

High-level installation plan:
1. Install Curtain Lite Admin
2. Install Curtain Lite Client on user's workstations
3. Activate Curtain LogTrace (for Paid version)
4. Create and configure control policy groups in Curtain Lite Admin
5. Connect with Active Directory for collecting user information, if you prefer to grant control policy by user/user-group
6. Assign workstations/users to different policy groups
7. Done

Related FAQs:
FAQ00357 - What are the basic components of Curtain LogTrace?
FAQ00359 - How to activate Curtain LogTrace?
FAQ00361 - How to configure Control Policy Group for Curtain LogTrace?
FAQ00363 - How to grant control policy by user/user group?

2.2 - System Requirements of Curtain MonGuard and Curtain LogTrace

System Requirements of Curtain Lite Admin and Client:

- 1.6 GHz or faster, 2-core; 2 GHz or greater recommended
- 2GB RAM (Recommended 8GB RAM)
- 2GB Hard Disk (in NTFS) for installation
- TCP/IP network
- TCP Port 24821 and 24822 are opened for communication (Note: if firewall exists in the network, please make sure these two communication ports are not disabled)
- For 64-bit OS, MSXML 4 or 6 is required (It can be download from Microsoft website)

P.S.: Curtain Lite program includes features of Curtain MonGuard and Curtain LogTrace

Operating System	32-bit	64-bit
XP	Supported	Not Supported
Win Server 2003	Supported	Not Supported
Win Server 2003 R2	Supported	Not Supported
Vista	Supported	Not Supported
Win Server 2008	Supported	Must have SP2 installed
Win Server 2008 R2	Supported	Must have SP1 & KB3033929 installed
Win 7	Supported	Must have SP1 & KB3033929 installed
Win 8	Supported	Supported
Win 8.1	Supported	Supported
Win Server 2012	\	Supported
Win Server 2012 R2	\	Supported
Win 10	Supported	Supported
Win Server 2016	\	Supported
Win Server 2019	\	Supported
Win 11	\	Supported
Win Server 2022	\	Supported

2.3 - Open Port 24821 and 24822 for Curtain Lite Admin

If Windows Firewall is enabled, please open port 24821 for Curtain Lite Admin and Curtain Lite Client.

For Windows 2008/2012/2016/2019/2022/Vista/Win 7/Win 8/Win 10/Win 11, please add the rules for Curtain Lite Admin as below:

- inbound rule of 24821 port of TCP
- inbound rule of 24821 port of UDP
- outbound rule of 24822 port of TCP
- outbound rule of 24822 port of UDP

For Windows 2003 and XP, set the port exception as below:

- 24821 port of TCP
- 24821 port of UDP
- 24822 port of TCP
- 24822 port of UDP

For Windows 2008/2012/2016/2019/2022/Vista/Win 7/Win 8/Win 10/Win 11, please add the rules for Curtain Lite Client as below:

- outbound rules of 24821 port of TCP
- outbound rules of 24821 port of UDP
- inbound rules of 24822 port of TCP
- inbound rules of 24822 port of UDP

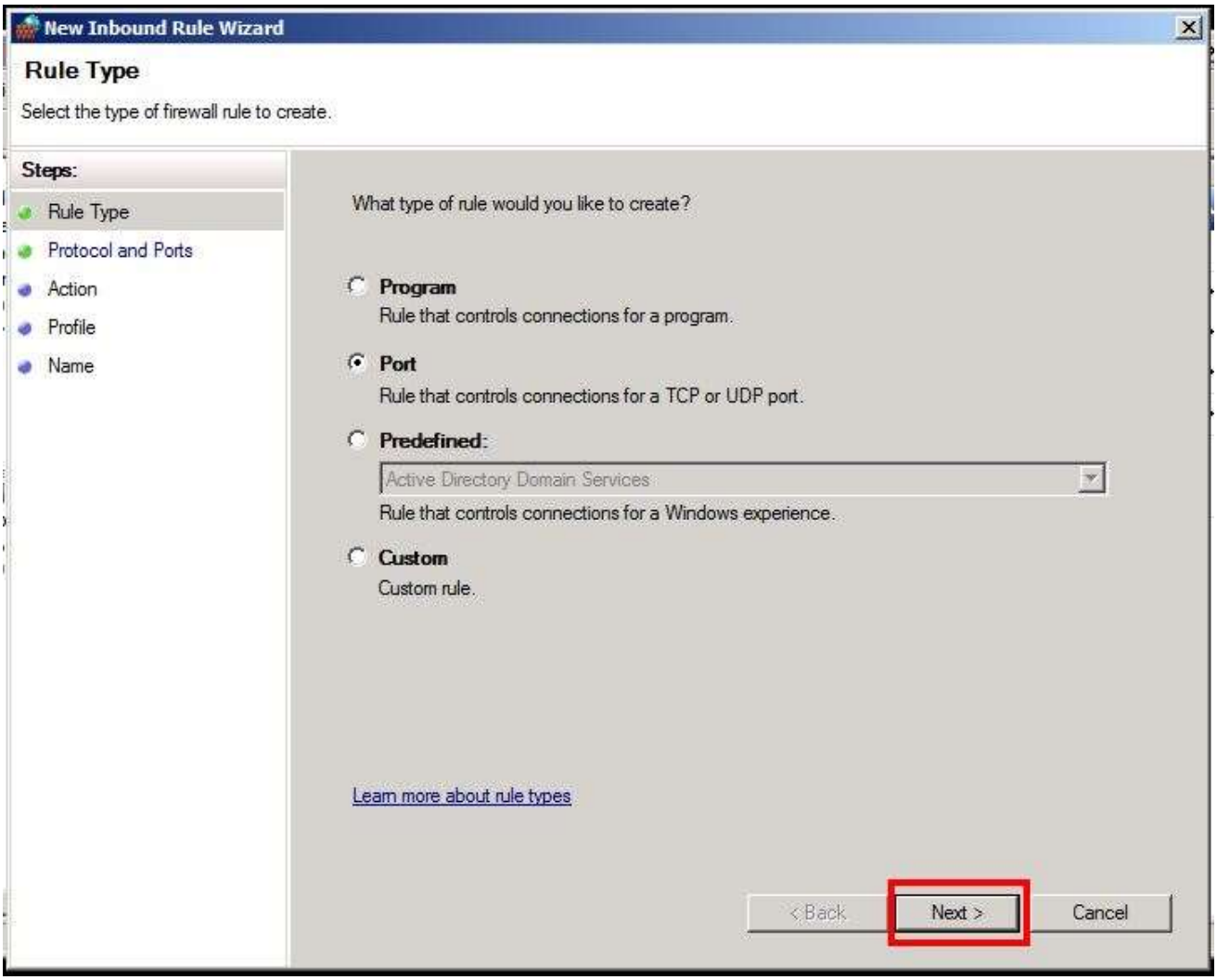
For Windows 2003 and XP, set the port exception as below:

- 24821 port of TCP
- 24821 port of UDP
- 24822 port of TCP
- 24822 port of UDP

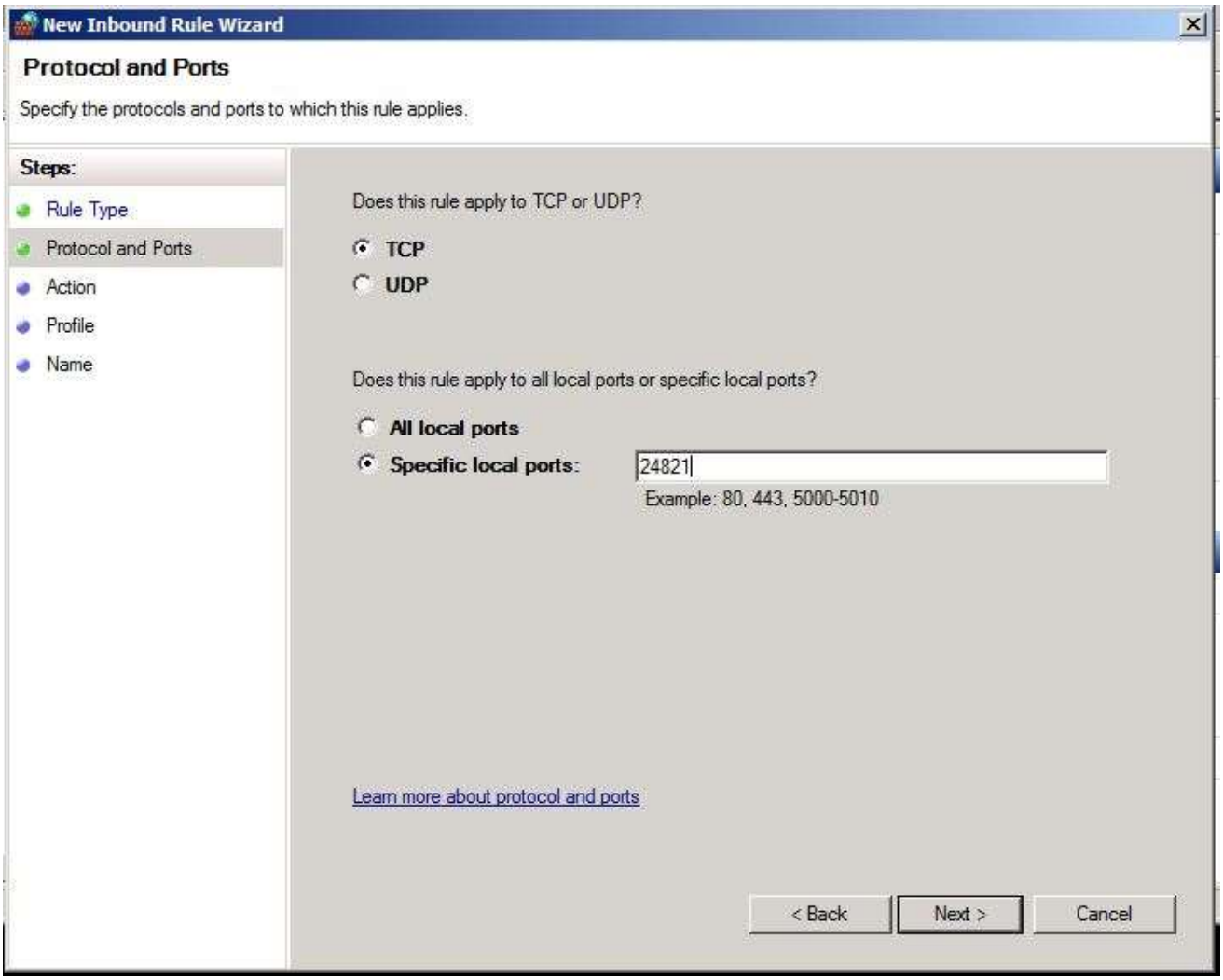
Steps to add rules for Windows 2008/2012/2016/2019/2022/Vista/Win 7/Win 8/Win 10/Win 11:
1. Select "My Computer" and right click to select "Manage"
Then, Server Manager will be shown.

2. In Server Manager, select "Inbound Rules" as below picture and right click to select "New Rule..."

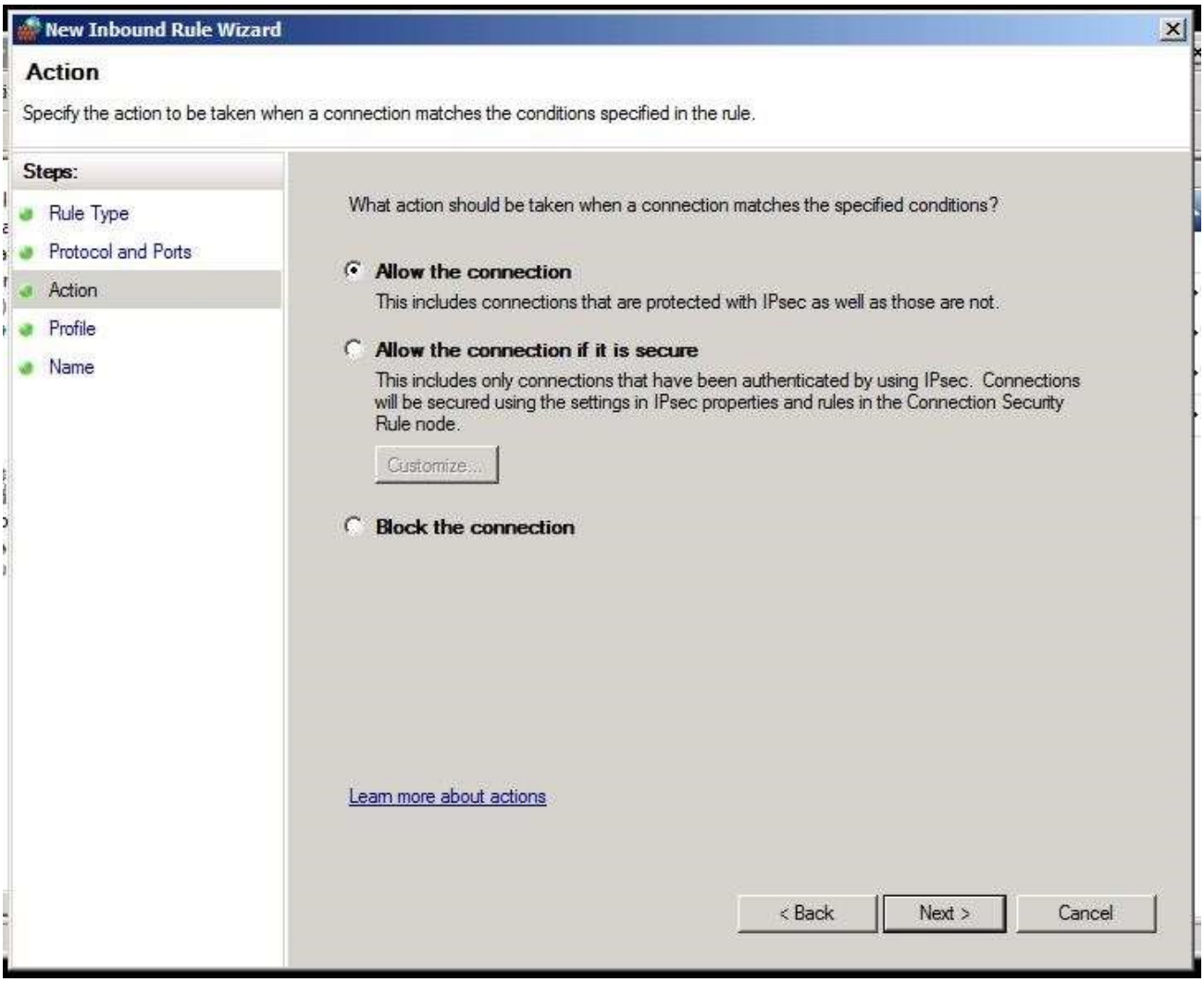
3. New Inbound Rule Wizard is shown as below, choose Port and click Next.



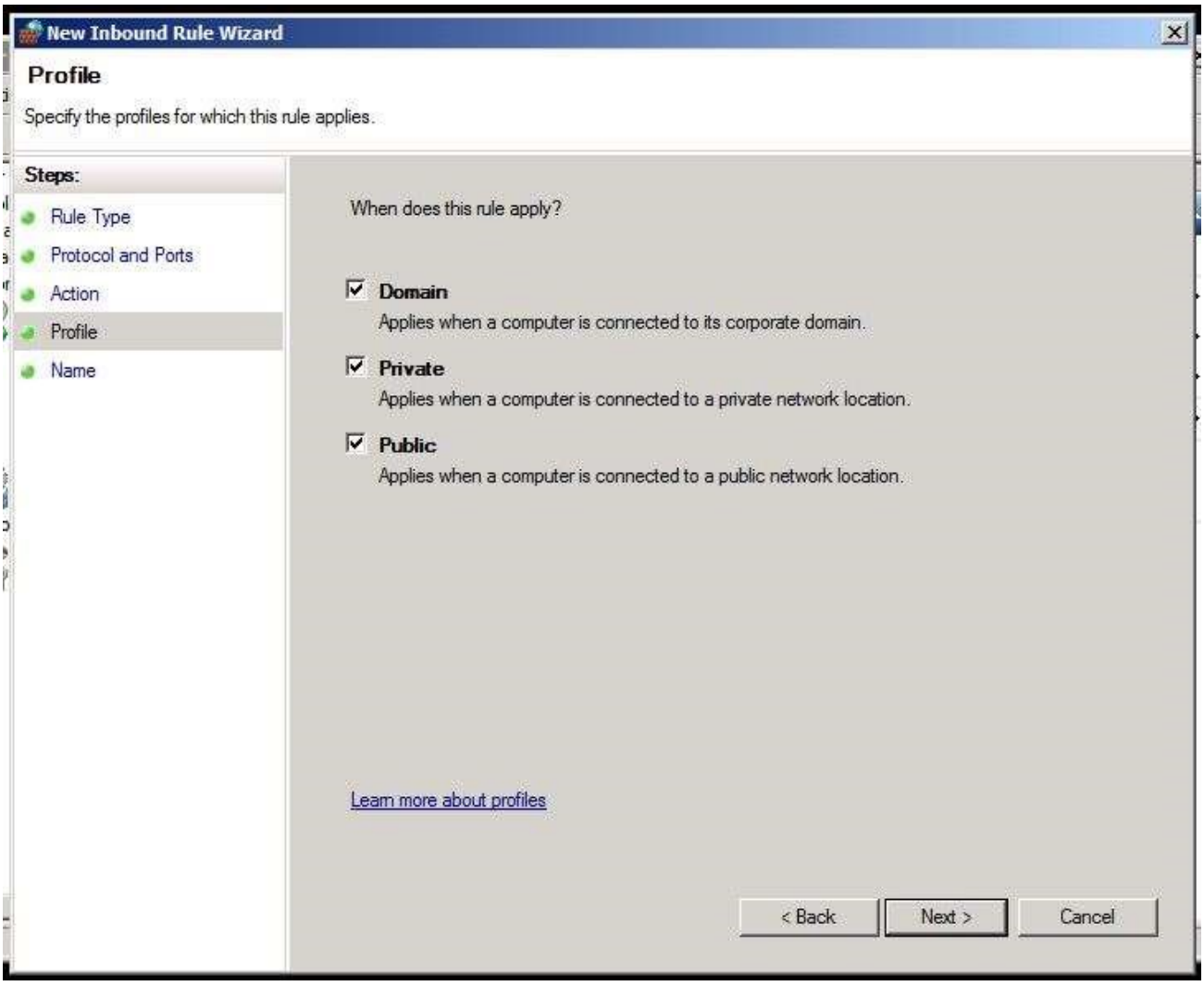
4. This rule applies to TCP and enter "24821" in Specific local ports, and click Next.



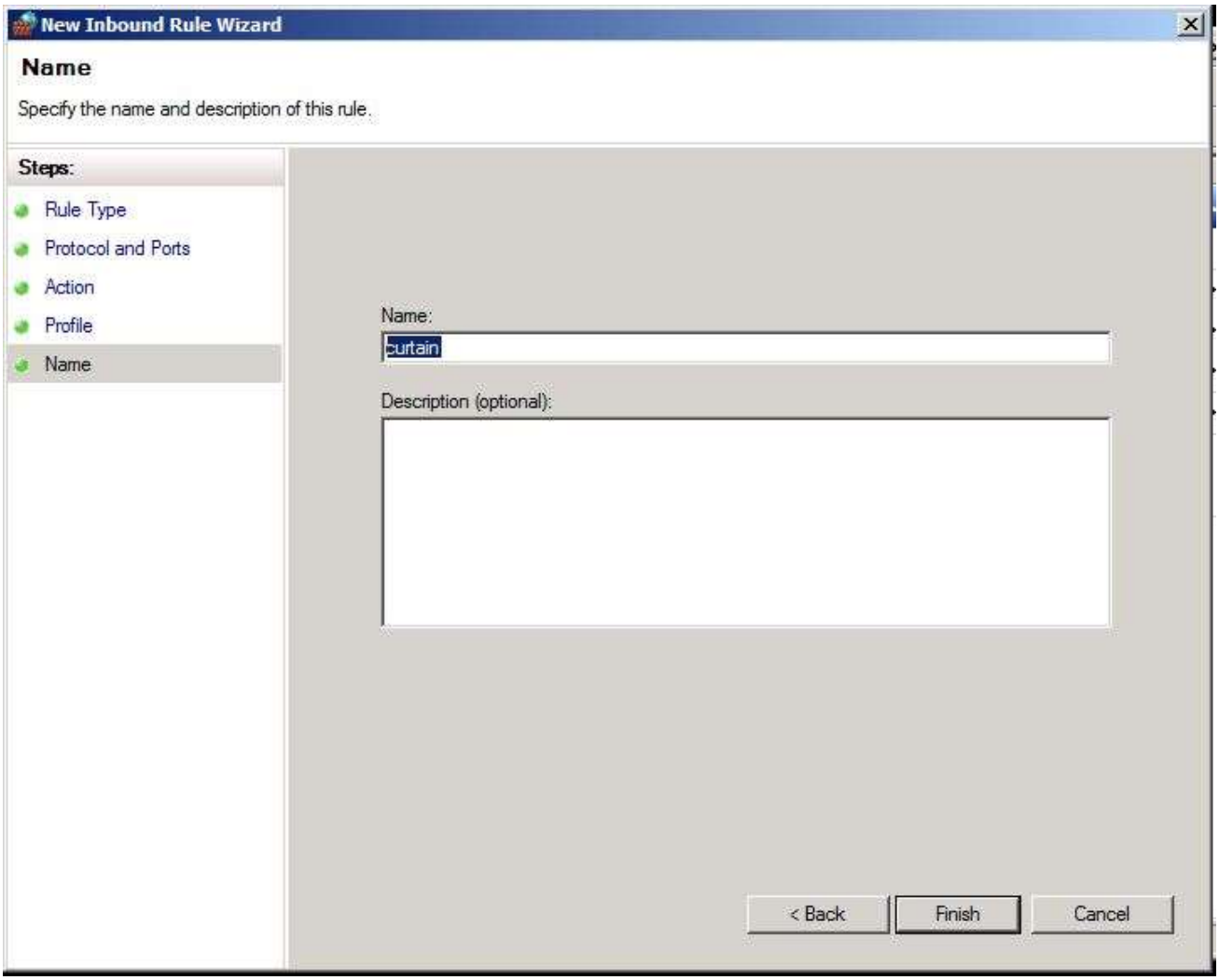
5. Select "Allow the connection", and click Next.



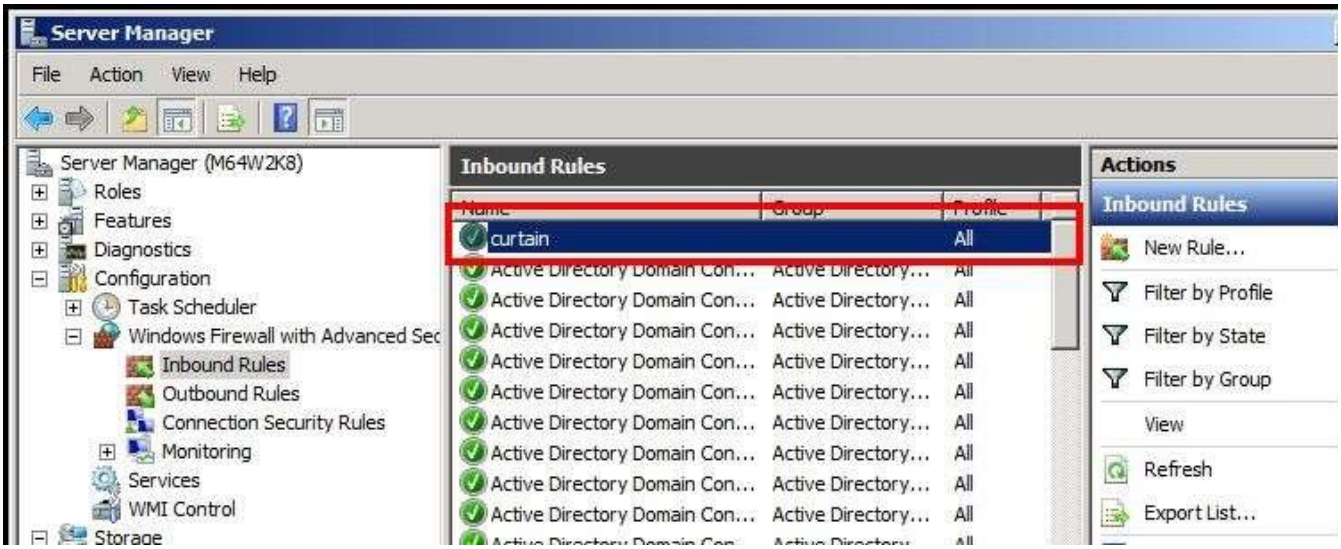
6. Check all as shown below (i.e. "Domain", "Private", and "Public") and click Next.



7. Enter "curtain" for the name of this rule, and click Finish.



8. A new inbound rule named "curtain" is created successfully.



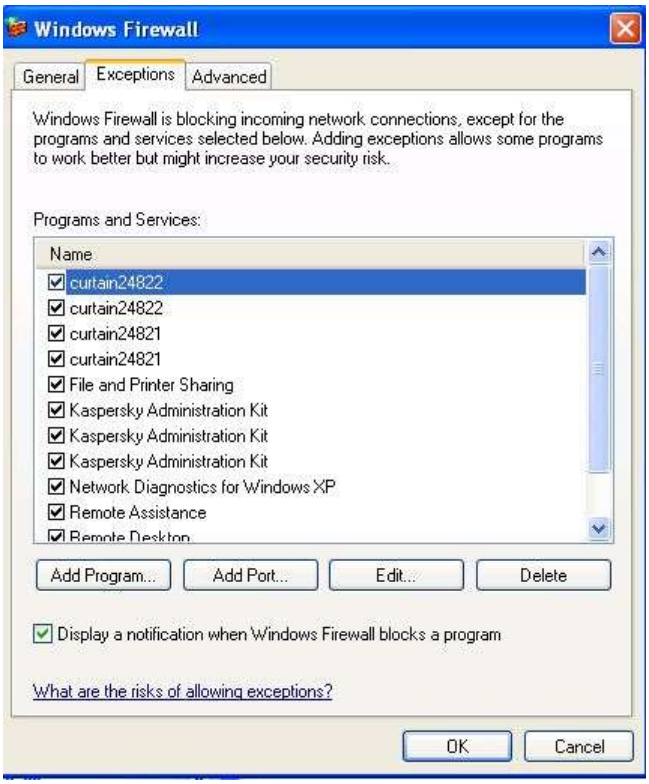
Please according to the above steps, to add more rules for:

- inbound rule of 24821 port of UDP
- outbound rule of 24822 port of TCP
- outbound rule of 24822 port of UDP
- outbound rules of 24821 port of TCP (Curtain Lite Client)
- outbound rules of 24821 port of UDP (Curtain Lite Client)
- inbound rules of 24822 port of TCP (Curtain Lite Client)
- inbound rules of 24822 port of UDP (Curtain Lite Client)

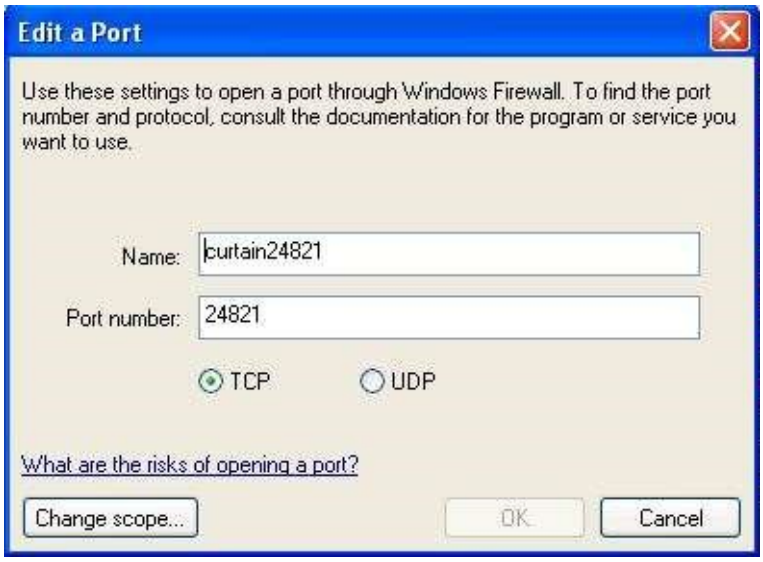
P.S. To create outbound rule, select "Outbound Rules" and right click to select "New Rule..."

Steps to set Port Exception for Windows 2003 and XP:

1. Click "Add Port..." button in Control Panel > Windows Firewall > Exceptions



2. Enter 24821 and select TCP. Then, enter a name for this exception and click OK.



Please according to the above steps, to add more exceptions for:

- 24821 port of UDP
- 24822 port of TCP
- 24822 port of UDP
- 24821 port of TCP (Curtain Lite Client)
- 24821 port of UDP (Curtain Lite Client)
- 24822 port of TCP (Curtain Lite Client)
- 24822 port of UDP (Curtain Lite Client)

3 - Installation

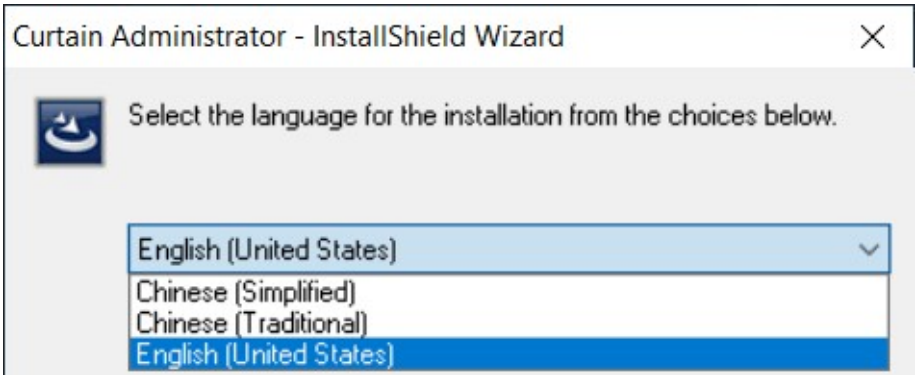
3.1 - Install Curtain Lite Admin

After you decide which server acts as Curtain Policy server, you should install Curtain Lite Admin on that server. Here are the steps.

Steps to install Curtain Lite Admin:
1. Copy appropriate Curtain server setup package (e.g. CurtainLiteAdmin_Win32(327400).zip or CurtainLite Admin_X64(327400).zip) to local hard-disk of the server.

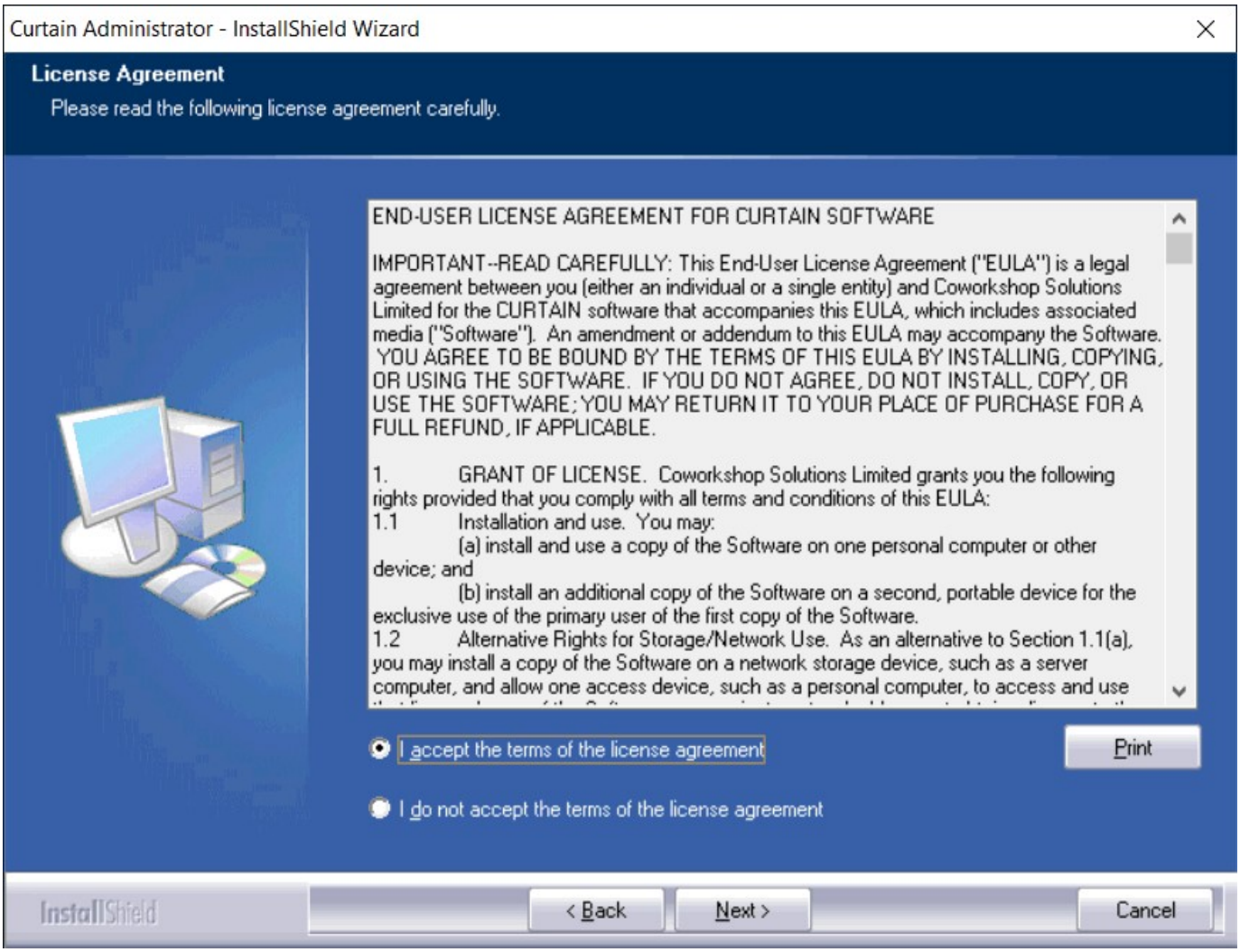
2. Unzip the setup package.

3. Run Curtain server setup program. Make sure that you login Windows with administrator right.
Then, you will be asked to select Language for the installation.

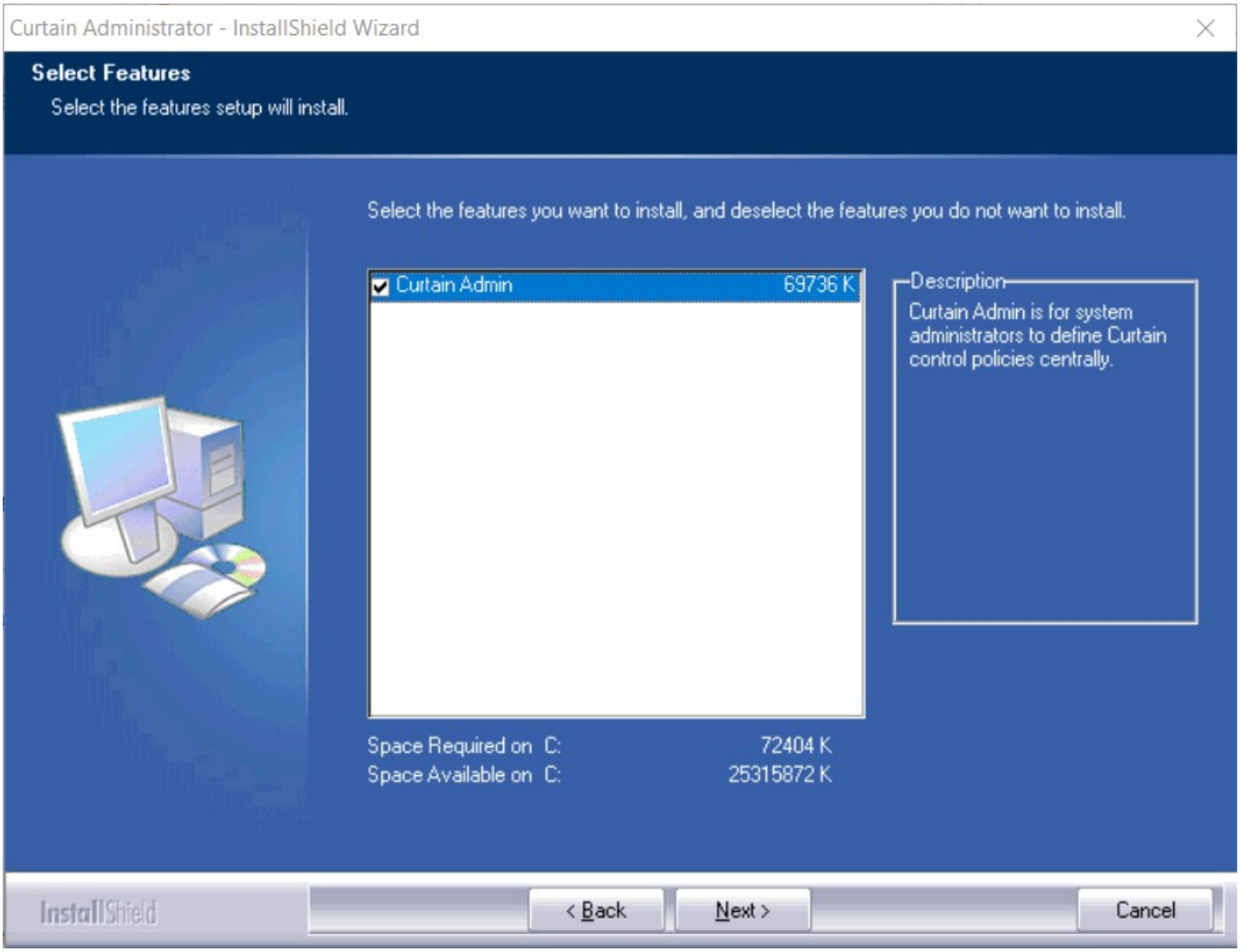


4. Select a language and click OK.

5. Read License Agreement. If you accept the agreement, select "I accept the terms of the license agreement" and click Next to continue.



Then, you will be asked to select Curtain components to install.



6. By default, "Curtain Admin" is selected. Click Next to continue.

7. Select Destination Folder for the installation, and click Next to continue.

8. Click Install to start the installation.

9. Please reboot the server after the installation.

3.2 - Install Curtain Lite Client

If you want to display watermark on screen in a user's workstation, you should install Curtain Lite Client on that. Here are the steps.

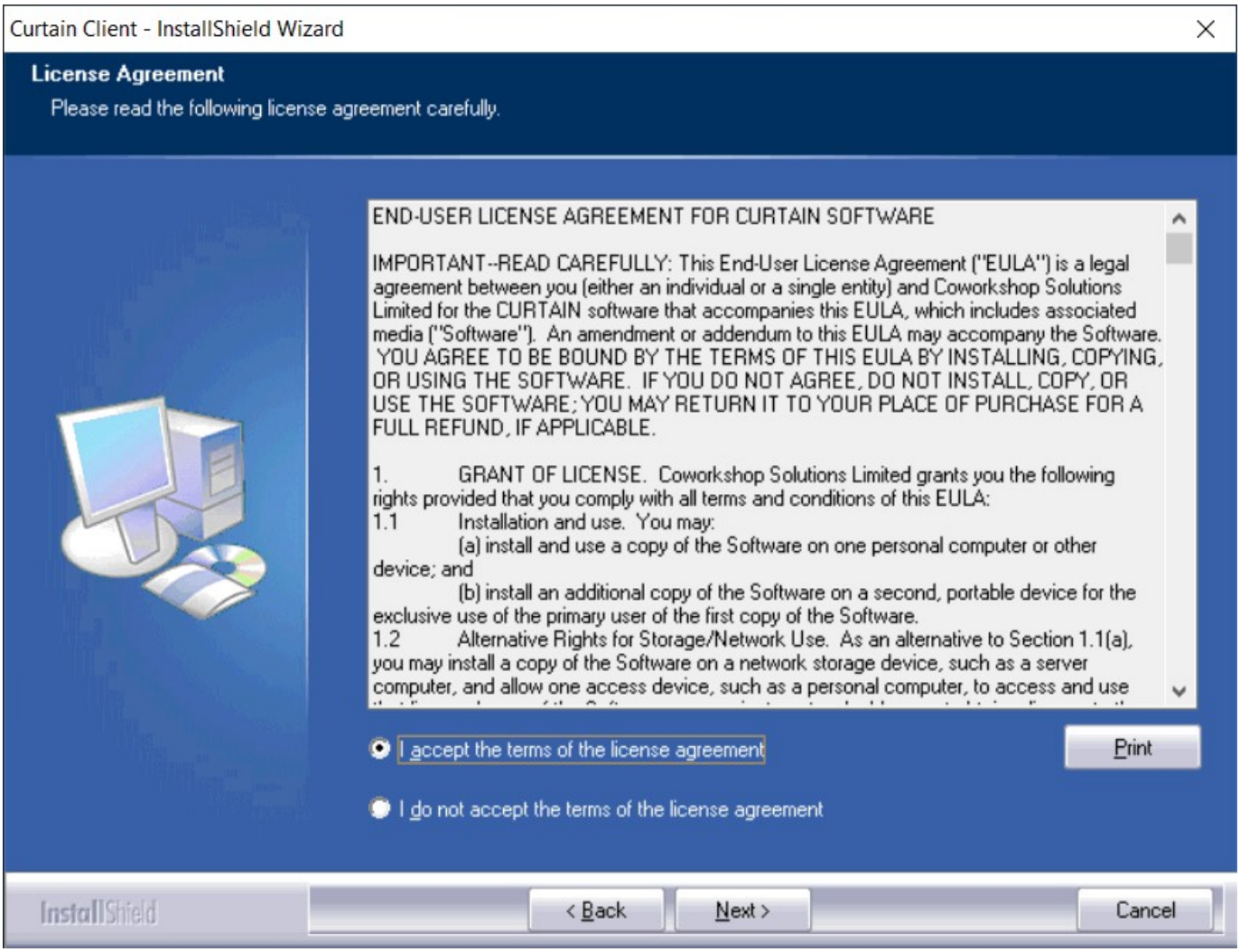
Steps to install Curtain Lite Client:
1. Copy appropriate Curtain Lite client setup package (e.g. CurtainLiteClient_Win32(327400).zip or CurtainLiteClient_X64(327400).zip) to local hard-disk of user's workstation.

2. Unzip the setup package.

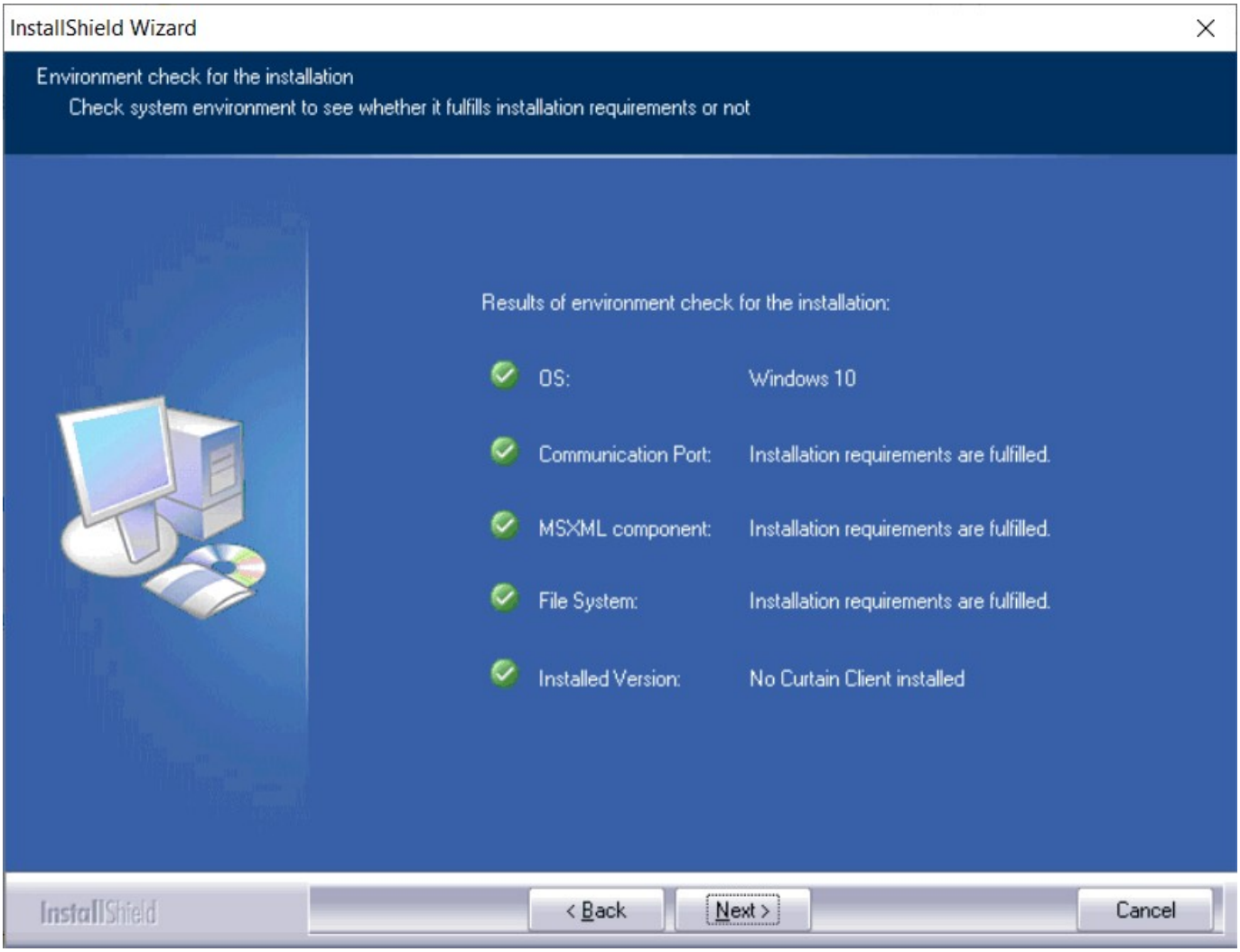
3. Run Curtain Lite client setup program. Make sure that you login Windows with administrator right. Then, you will be asked to select Language for the installation.

4. Select a language and click OK.

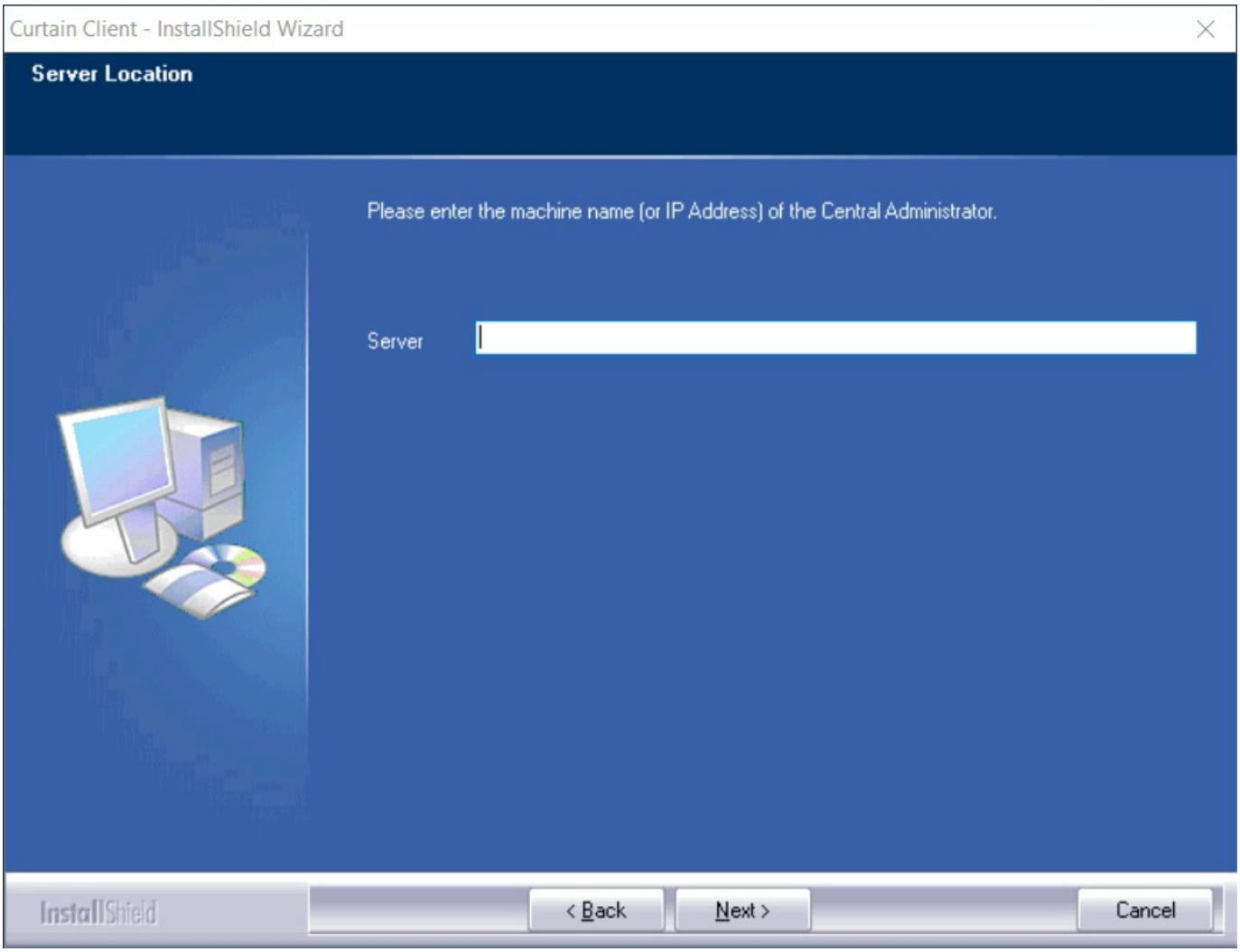
5. Read License Agreement. If you accept the agreement, select "I accept the terms of the license agreement" and click Next to continue.



Then, the setup program will check your system environment for the installation, click Next to continue.



6. Enter hostname or IP Address of Curtain Lite Admin (Please make sure that it is entered correctly), and click Next to continue.



7. Select Destination Folder for the installation, and click Next to continue.

8. Click Install to start the installation.

9. Reboot the workstation after installing Curtain Lite Client.

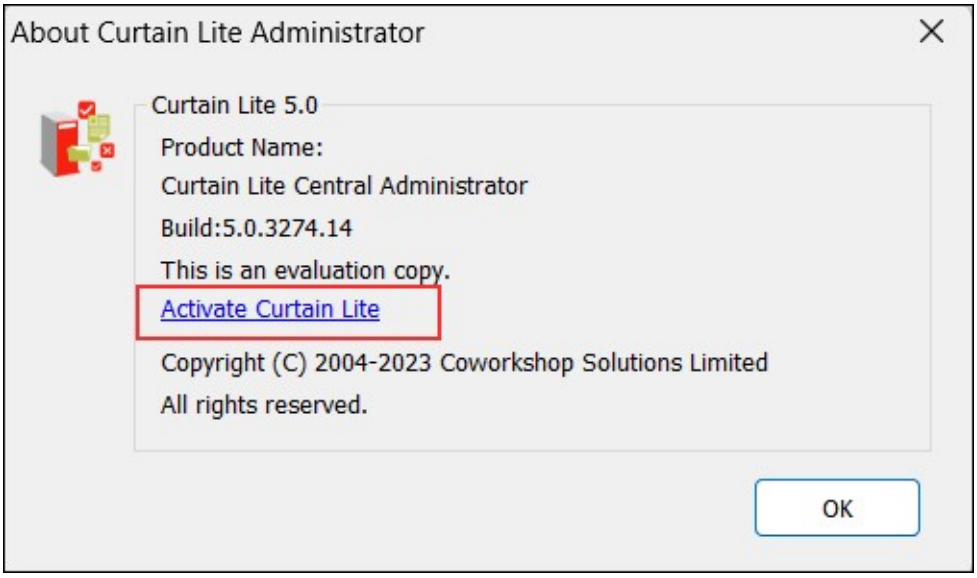
P.S. There is no user interface for Curtain Lite Client. You can find it in Windows control panel.

4 - Product Activation

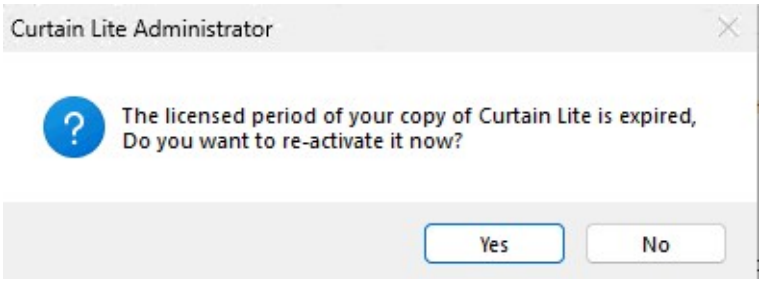
4.1 - Activate Curtain LogTrace

Curtain LogTrace is a shareware. You can download and use the software for free on a trial basis or commercial use. If you want to log more file events (e.g. print, rename, save, open and close) and some advanced features, you need to activate the software to paid version.

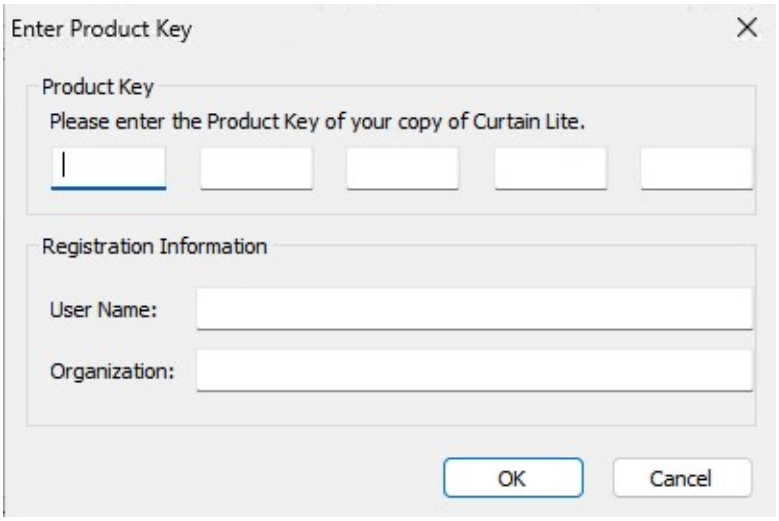
Steps to activate Curtain LogTrace:
1. In Curtain Lite Admin, select "Help > About Curtain Lite Administrator". Then, the following dialog will appear.



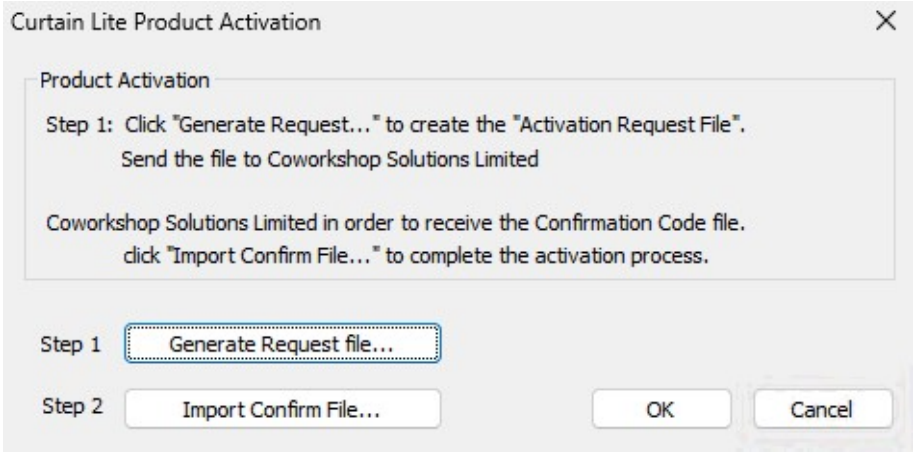
2. Click "Activate", you will be asked to do the activation.



3. Click Yes to start Product Activation (or click No to skip the Activation).
   - If it is the first time you activate the software, you will be asked to enter a 25-character Product Key.
   - If it is the Annual Product Reactivation, please go to Step 5 to continue.

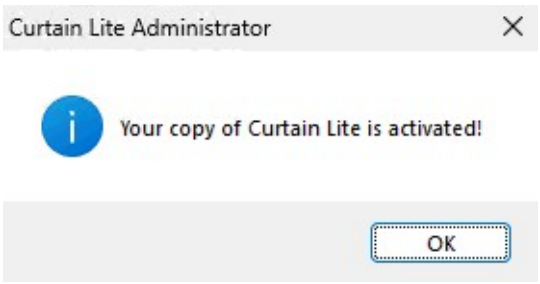


4. Enter Product Key (which is case sensitive) and company information, and click OK to continue. Then, the following dialog will appear.



5. Click "Generate Request file..." button to generate Activation Request File, and send this file to Coworkshop (registration@coworkshop.com). After receiving your activation request, Coworkshop will send Confirmation Code file back to you.

6. After receiving Confirmation Code file from Coworkshop, click "Import Confirm File..." button and select the file. After you click OK, the following message box will appear.



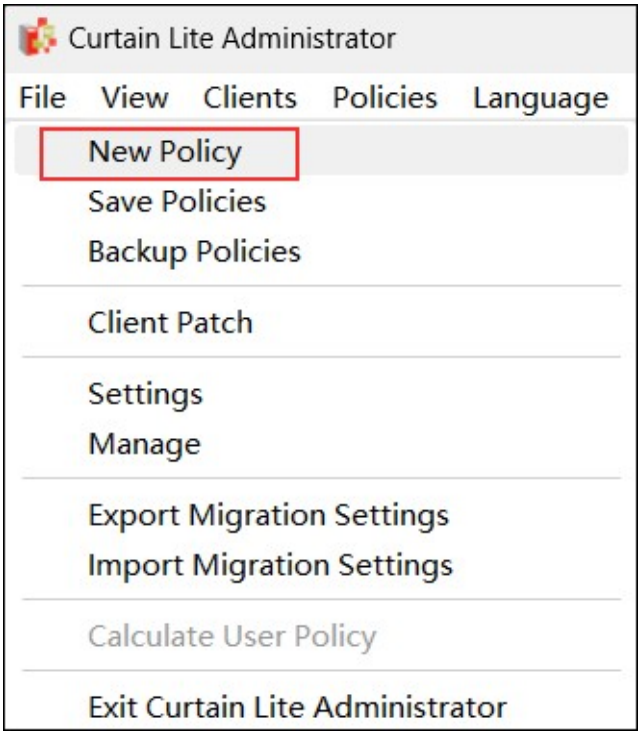
Congratulations! Curtain LogTrace has been activated successfully.

5 - Configurations

5.1 - Create Control Policy Group

Administrators can create many Control Policy Groups in Curtain Lite Admin for different workstations/users. Here is an example of Control Policy Groups for reference.
- Default Policy: for general users, only log File Operations (i.e. New, Copy, Move, Delete, Rename and Print)
- R&D: for R&D team, log both File Operations and Application Operations (i.e. Open, Save, Save As and Close)

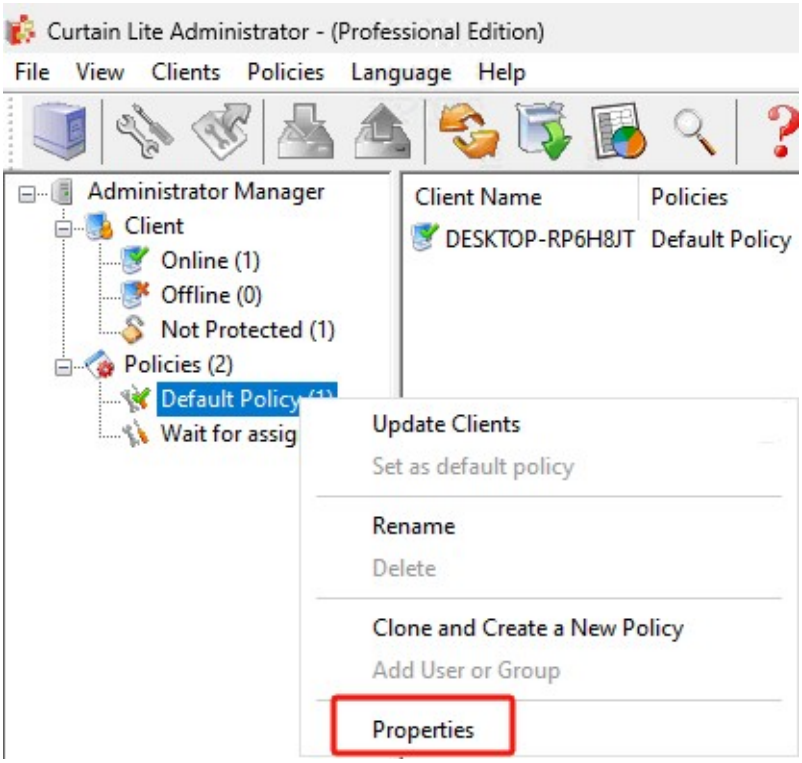
Steps to create Control Policy Group:
1. In Curtain Lite Admin, select "File > New Policy" in the menu. Then you will be asked to enter new Policy Name.



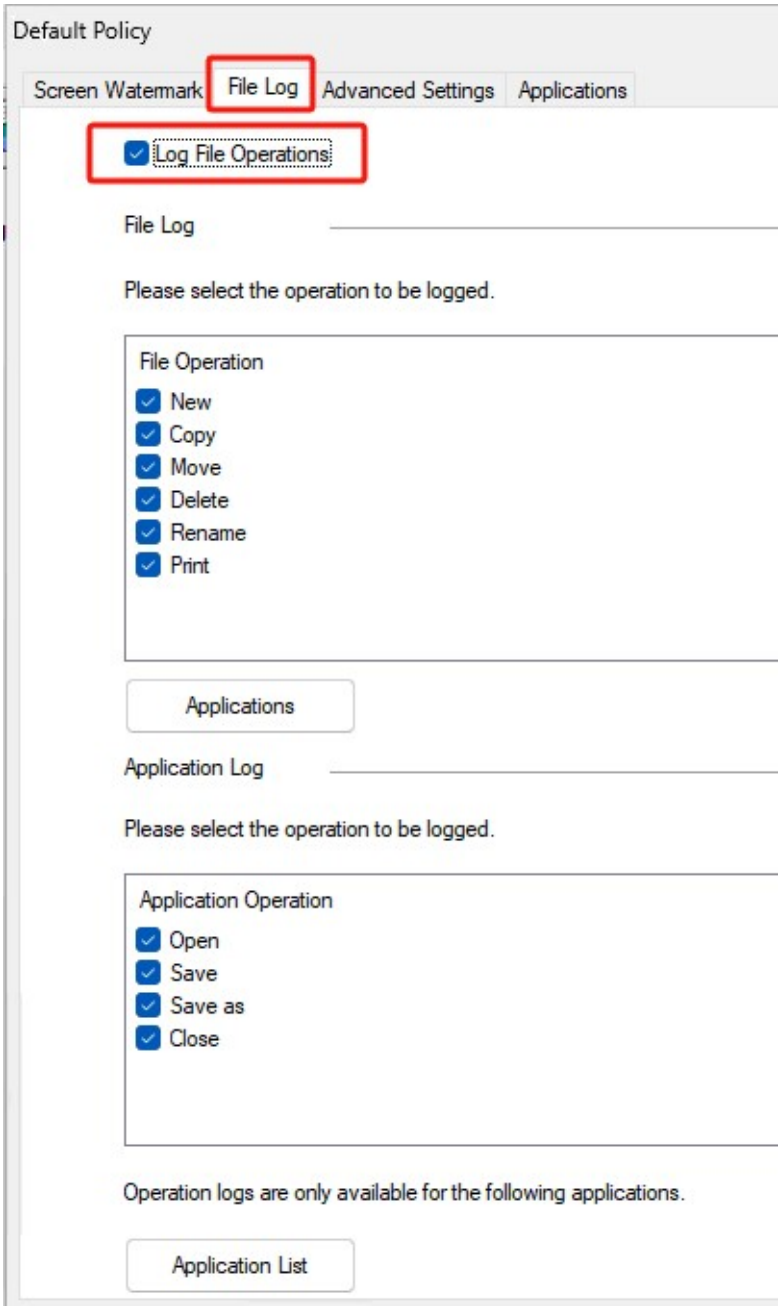
2. Enter new Policy Name and click OK to confirm.

5.2 - Configure Control Policy Group

Steps to configure Control Policy Group:
1. In Curtain Lite Admin, select a Policy Group and right-click to select "Properties".



2. Select "File Log" and enable the "Log File Operations"

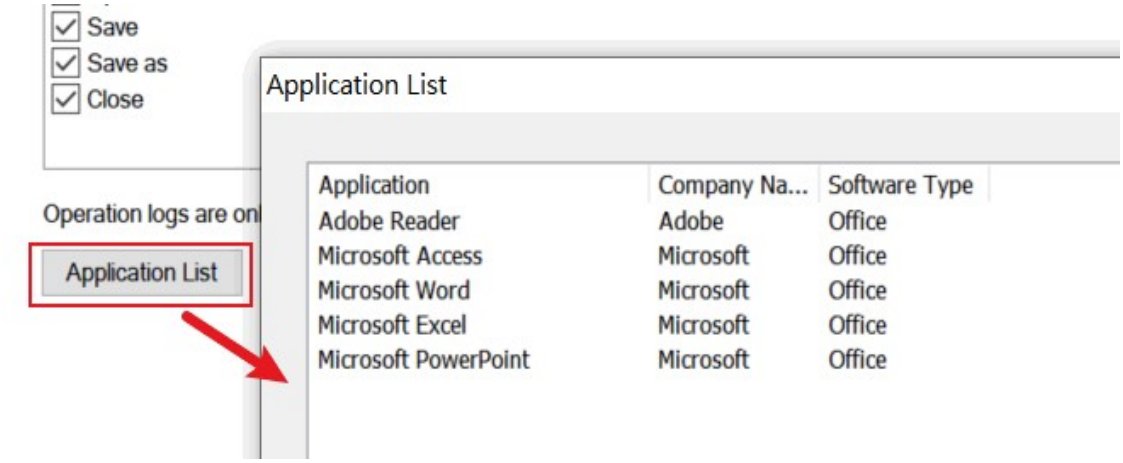


There are 2 types of Log operations:

- File Log : It logs below operations.
  - New
  - Copy
  - Move
  - Delete
  - Rename
  - Print

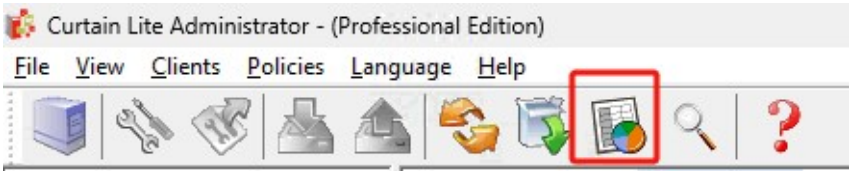
- Application Log : It logs below operations in specific applications (i.e. Adobe Reader, Microsoft Access, Word, Excel, and PowerPoint)
  - Open
  - Save
  - Save As
  - Close

3. Click the "Application List" to see which applications are supported for logging.

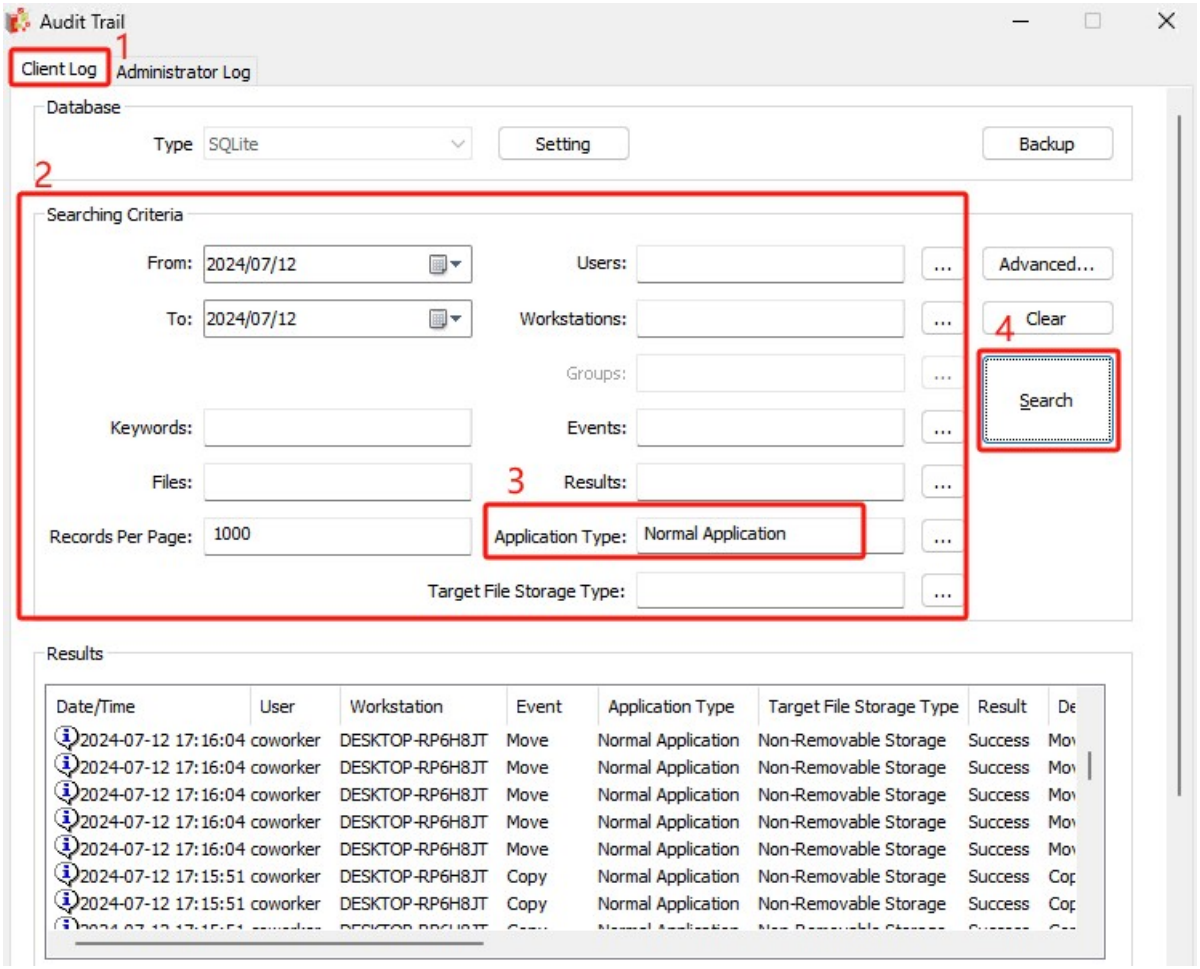


Steps to view the file log:

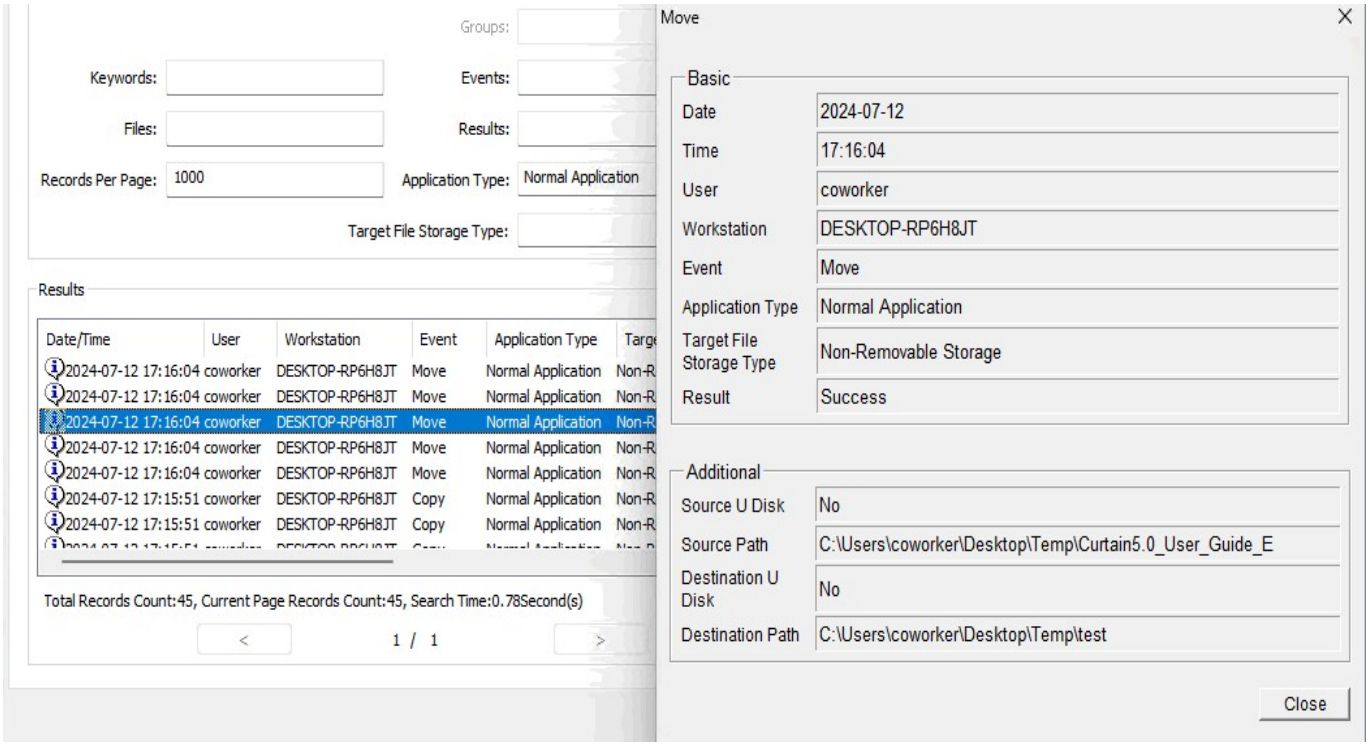
1. In Curtain Lite Admin, Click the "Audit Trail" button in the toolbar, or select "File > Audit Trail" from the menu. The "Audit Trail" window will be displayed.



2. Select " Client Log " . Input "Searching Criteria" (e.g. Application Type -> normal application) and click the "Search" button.

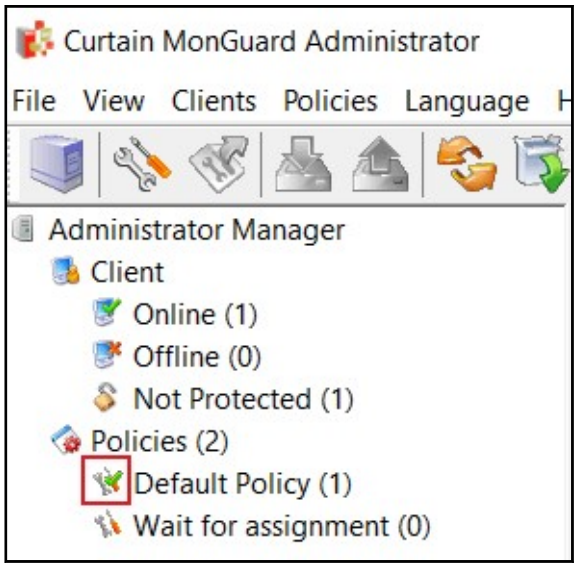


3. You can double-click on a record to view details.



5.3 - Set Default Policy

If it is the first time to launch Curtain Lite Admin (after the installation), "Default Policy" is set as default policy. If a Control Policy Group is set as default policy, all newly installed Curtain Lite Clients will fall into that Policy Group. A green tick indicates which Policy Group is default policy.

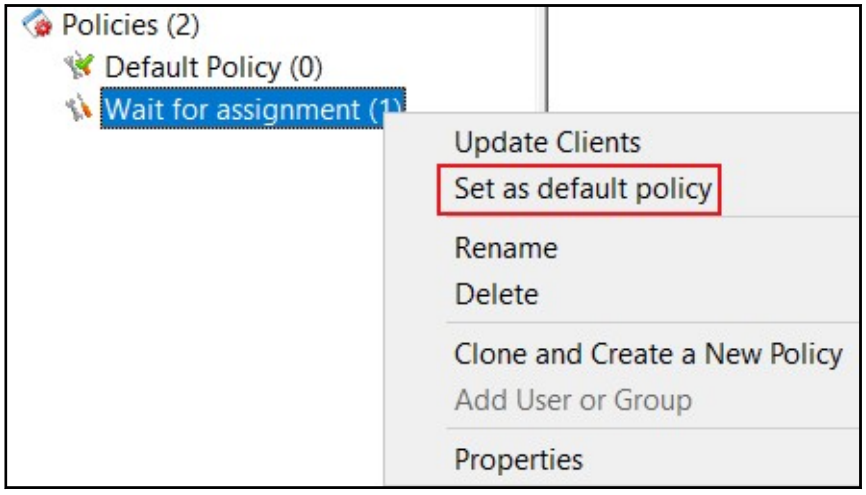


There are two built-in Control Policy Groups.
- Default Policy
- Wait for Assignment

When Curtain Lite Clients have been installed in user's workstations, they will connect to Curtain Lite Admin and apply default policy.

Steps to set a Control Policy Group to default policy:
1. In Curtain Lite Admin, select a Control Policy Group and right-click. Then a menu will be shown.

2. Select "Set as default policy"



3. Done

5.4 - Grant control policy by user/user group

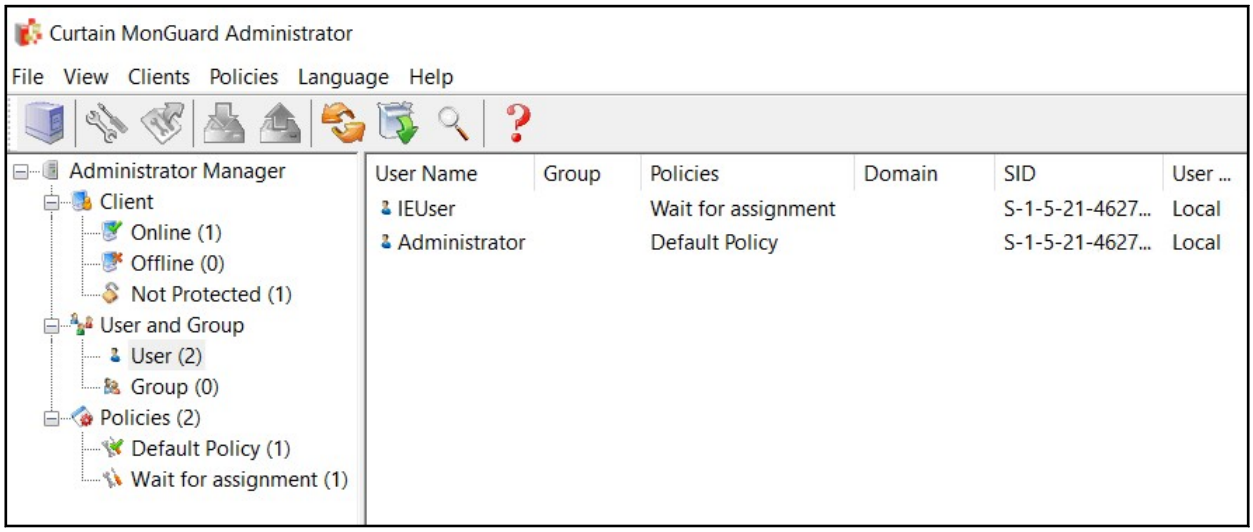
Control policy of Curtain LogTrace can be applied to computer or user/user group. If you prefer to grant control policy by AD user/user group, you need to connect with AD for importing user information to Curtain Lite Admin. When the first time Curtain Lite Admin gets a user information, the system will use default control policy for controlling that user/user group. Administrator needs to assign the user/user group to appropriate control policy group manually.

To grant control policy by user/user group, please follow steps stated below to enable "Assignment of User" in Curtain Lite Admin.

Steps for enabling "Assignment of User" in Curtain Lite Admin:
1. Launch Curtain Lite Admin, open File -> Settings -> Assignment of Security Policy.

2. Choose "Assignment of User", and click "OK" button.

Then "User And Group" will be shown in Curtain Lite Admin.



3. Done.

Steps for importing users and user groups from AD domain:

1. Launch Curtain Lite Admin, open File -> Settings -> LDAP.

2. Check "Enable LDAP" button.

3. Enter LDAP server address, DNS or IP address on "LDAP Server Address".

4. "LDAP Server Port", default port is 389.

5. Recommend to enable "Use Secure LDAP Connection", it means to use secure LDAP connection to AD (default is disable).

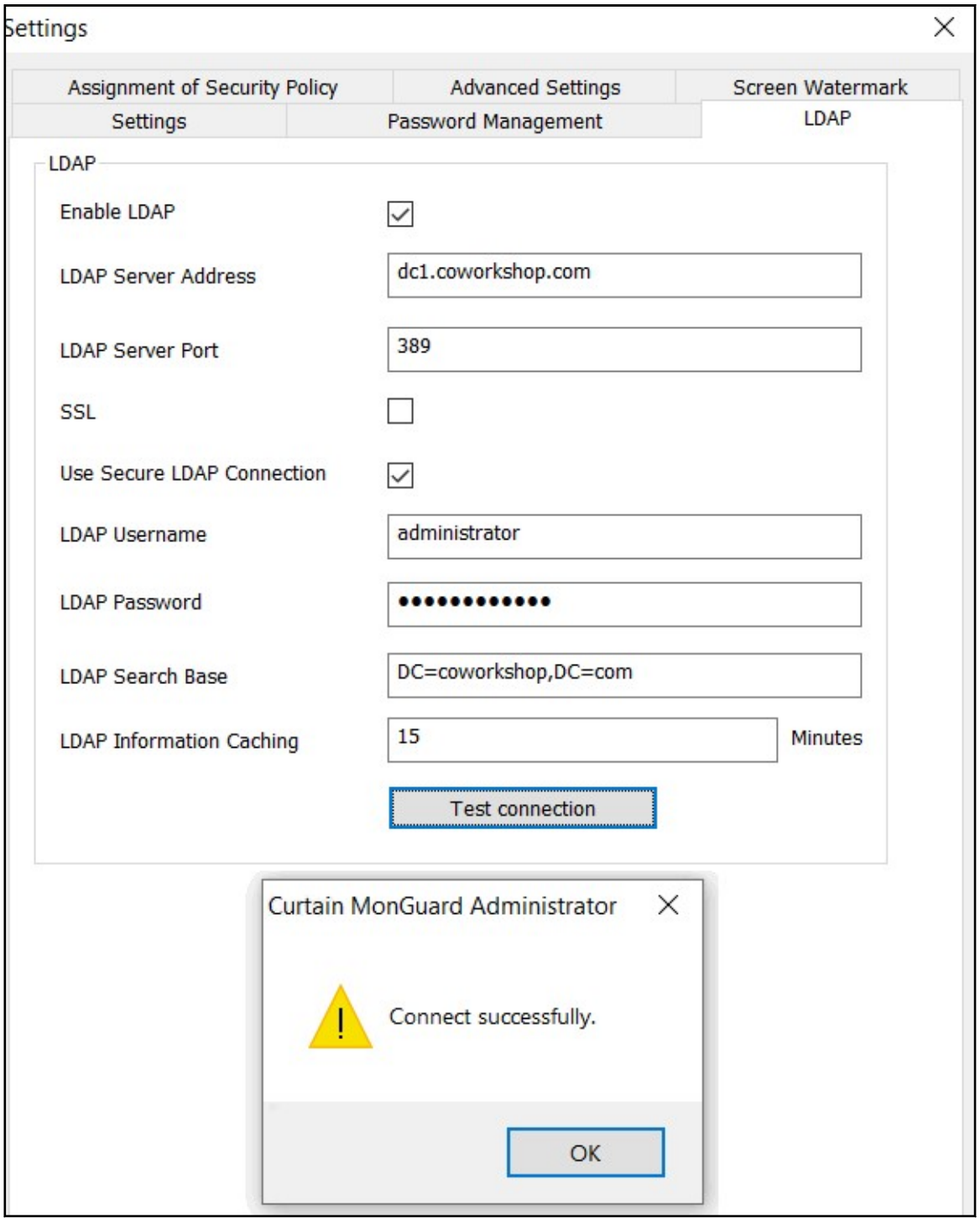
6. Enter user name on "LDAP Username" to connect LDAP server.

7. Enter password on "LDAP Password".

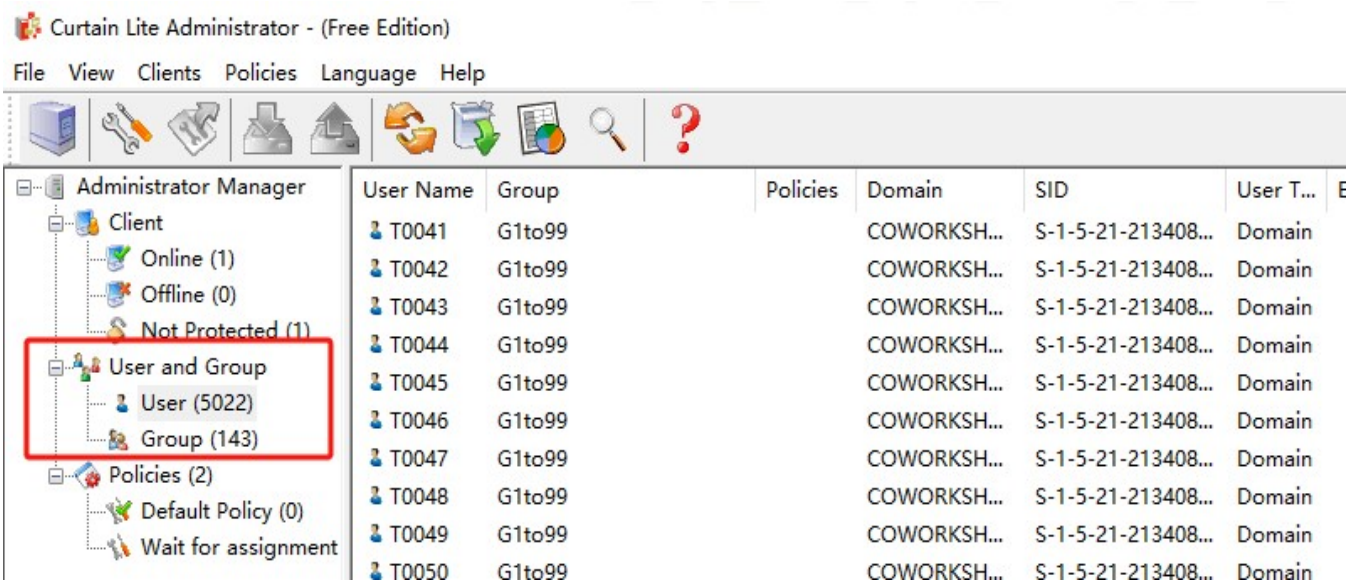
8. "LDAP Search Base", enter the root of user or group , should enter CN, OU and DC .
   - for search the whole domain, enter "dc=domain name,dc=domain suffix" (e.g. "dc=test,dc=com")
   - for search the whole group, enter "ou=organizational unit name,dc=domain name,dc=domain suffix" (e.g. "ou=it,dc=test,dc=com")
   - for search single user, enter "cn=username,ou=organizational unit name,dc=domain name,dc=domain suffix" (e.g. "cn=tester,ou=it,dc=test,dc=com")

9. "LDAP Information Caching", for setup caching information of AD (default is 15 minutes).

10. While setting is finished, click "Test connection" button to see whether connect to AD successfully or not.



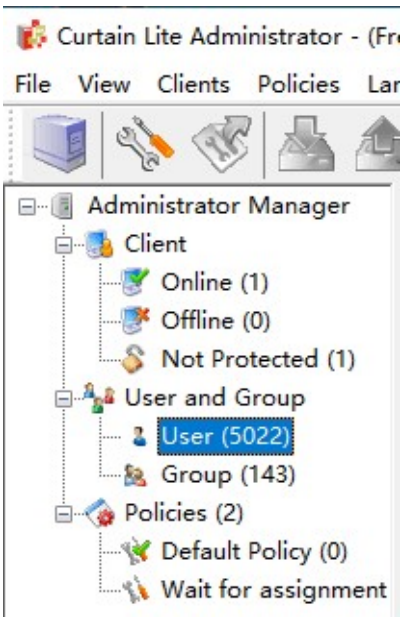
11. If AD user/user group is imported to Curtain Lite Admin successfully, they will be shown under "User And Group" in Curtain Lite Admin as below.



12. Done.

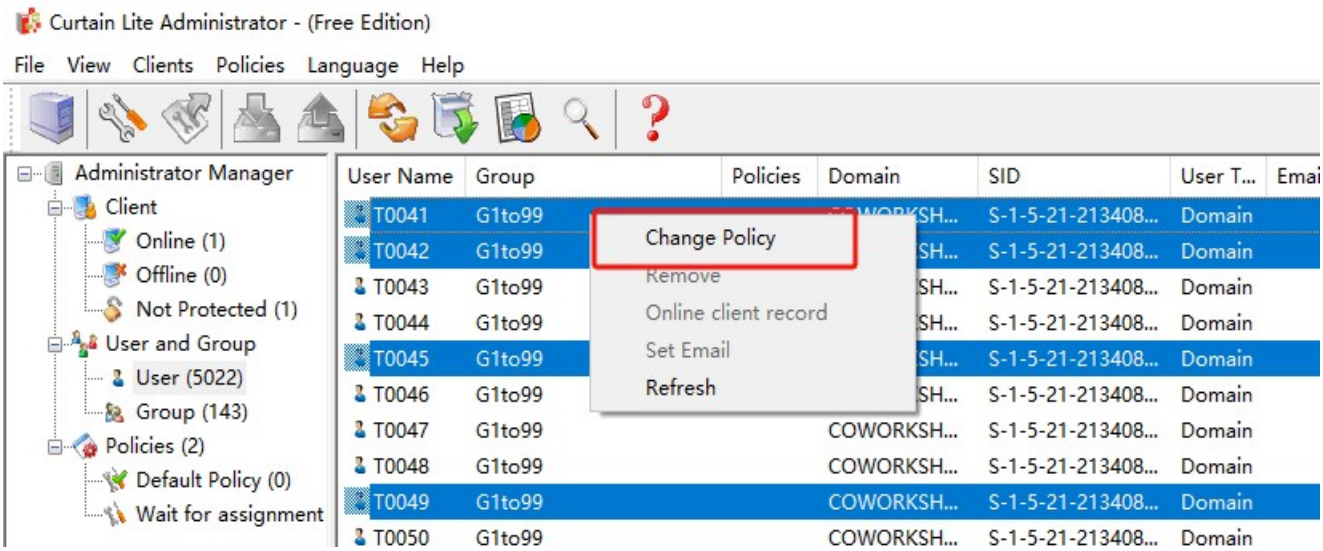
Steps to assign users/user groups to different Control Policy Groups:

1. In Curtain Lite Admin, select User/Group in left panel. Then, Users/Groups will be listed out in the right panel.



2. Select users/groups (press Ctrl button for multiple selection).

3. Right click and select "Change Policy" to assign users/groups to appropriate Control Policy Group.

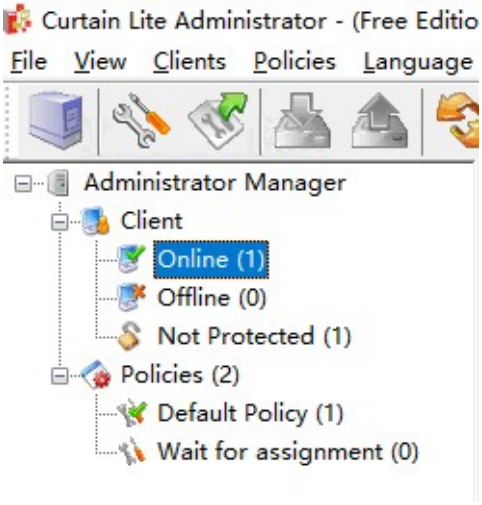


4. Repeat Step 2-3 for assigning other users/groups to appropriate policy groups.

5. Done.

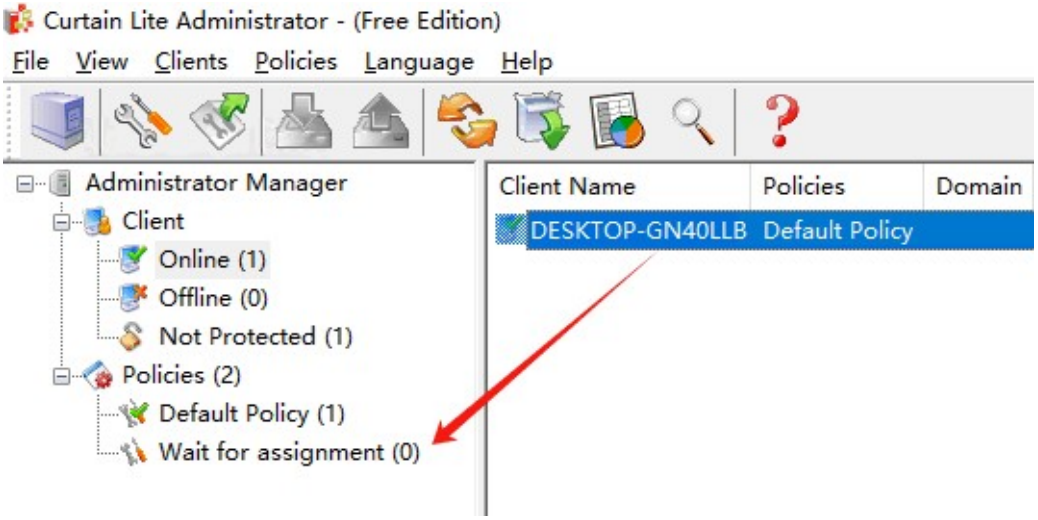
5.5 - Assign workstations/users to Control Policy Group

Steps to assign workstations to different Control Policy Groups:
1. In Curtain Lite Admin, select Online/Offline in left panel. Then, workstations will be listed out in the right panel.



2. Select workstations (press Ctrl button for multiple selection)

3. Drag and Drop selected workstations to appropriate Control Policy Group

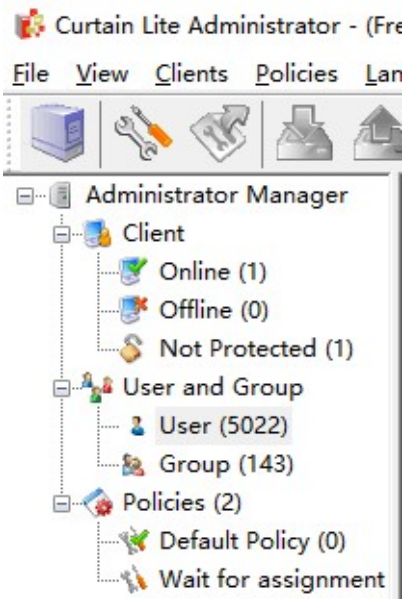


4. Repeat Step 2-3 for assigning other workstations to appropriate policy groups.

5. Done

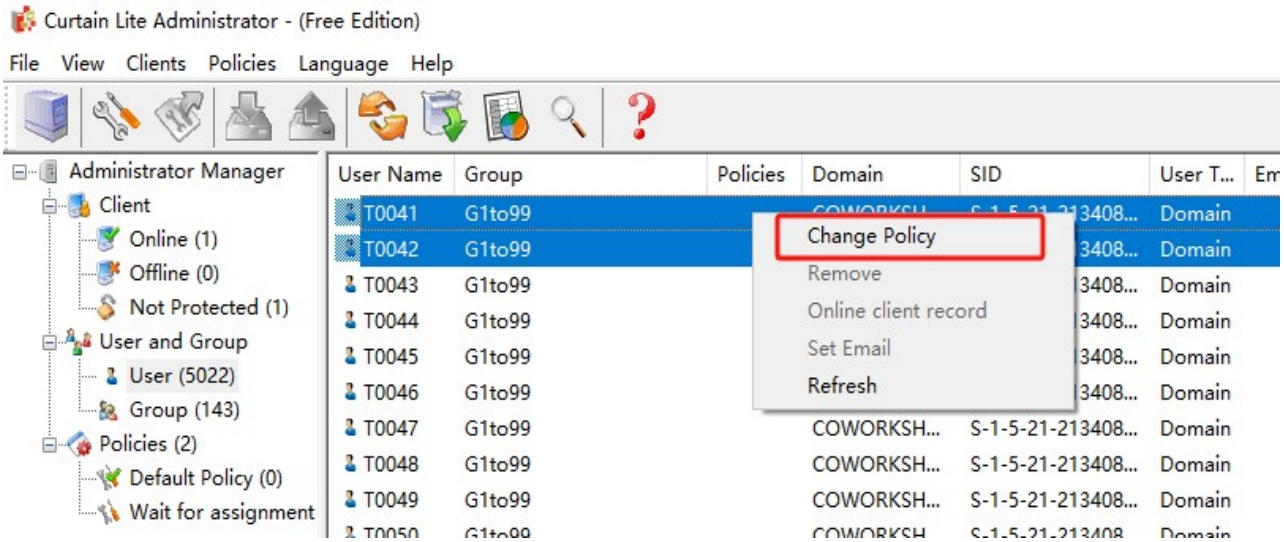
Steps to assign users to different Control Policy Groups:

1. In Curtain Lite Admin, select User/Group in left panel. Then, Users/Groups will be listed out in the right panel.



2. Select users/groups (press Ctrl button for multiple selection).

3. Right click selected users/groups, choose "Change Policy" and assign users to appropriate Control Policy Group.



4. Repeat Step 2-3 for assigning other users/groups to appropriate policy groups.

5. Done.

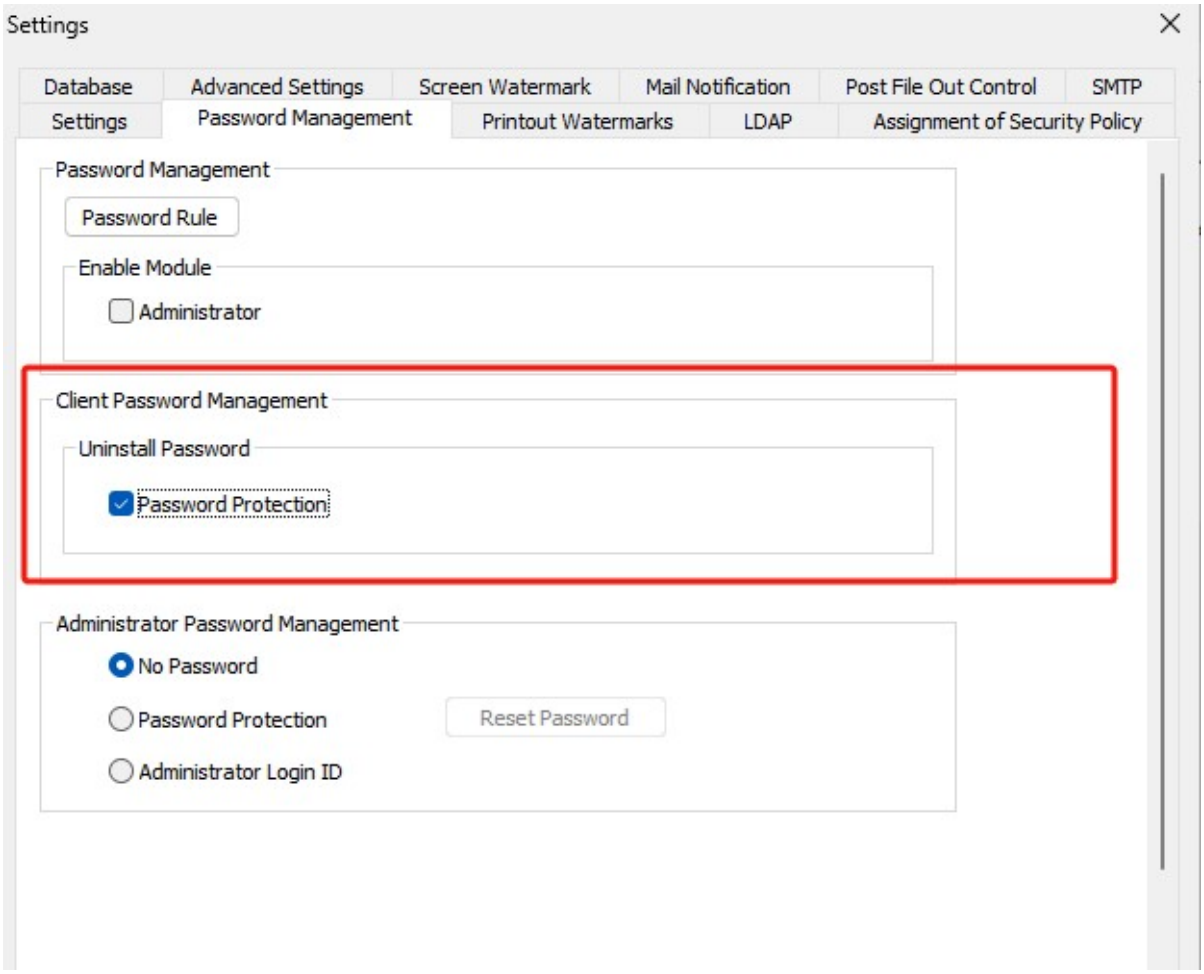
6 - Other Features

6.1 - Password protection for uninstalling Curtain Lite Client

By default, users do not need to enter password for uninstalling Curtain Lite Client. Administrators can enable Password Protection for removing Curtain Lite Client to enhance the security.

Steps to enable Password Protection for uninstalling Curtain Lite Client:
1. In Curtain Lite Admin, select "File > Settings".

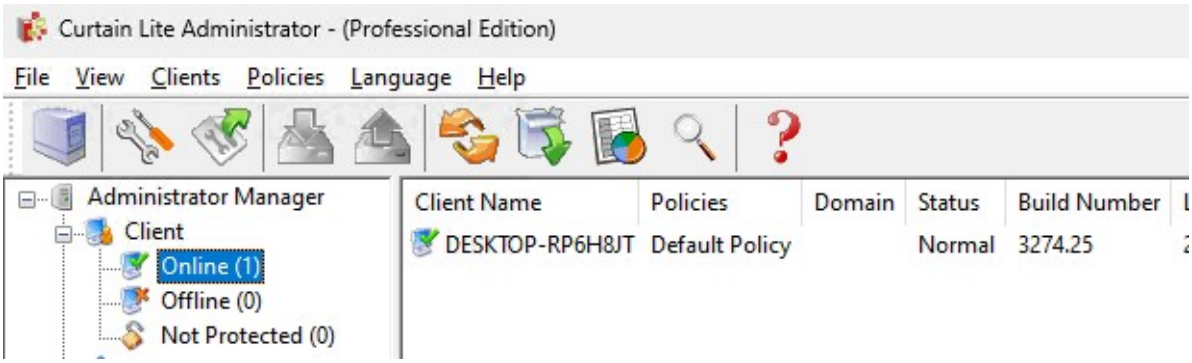
2. In Password Management tab, check "Password Protection" of Uninstall Password Under Client Password Management as below.



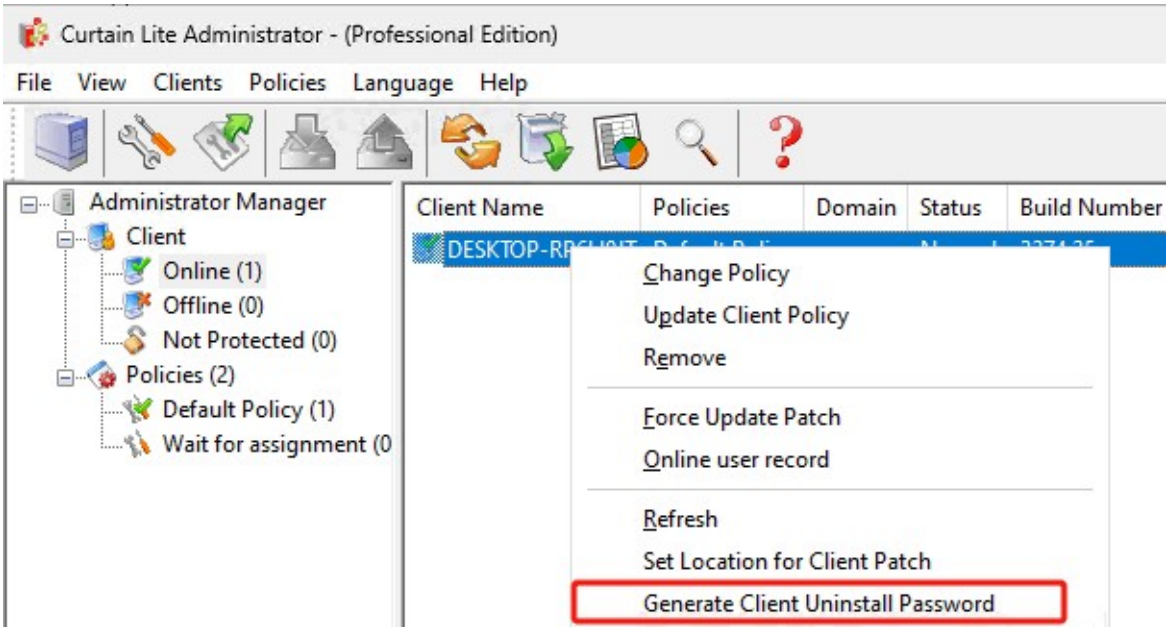
3. Enter "OK" to confirm.

Steps to Uninstall Curtain Lite Client with password protection :

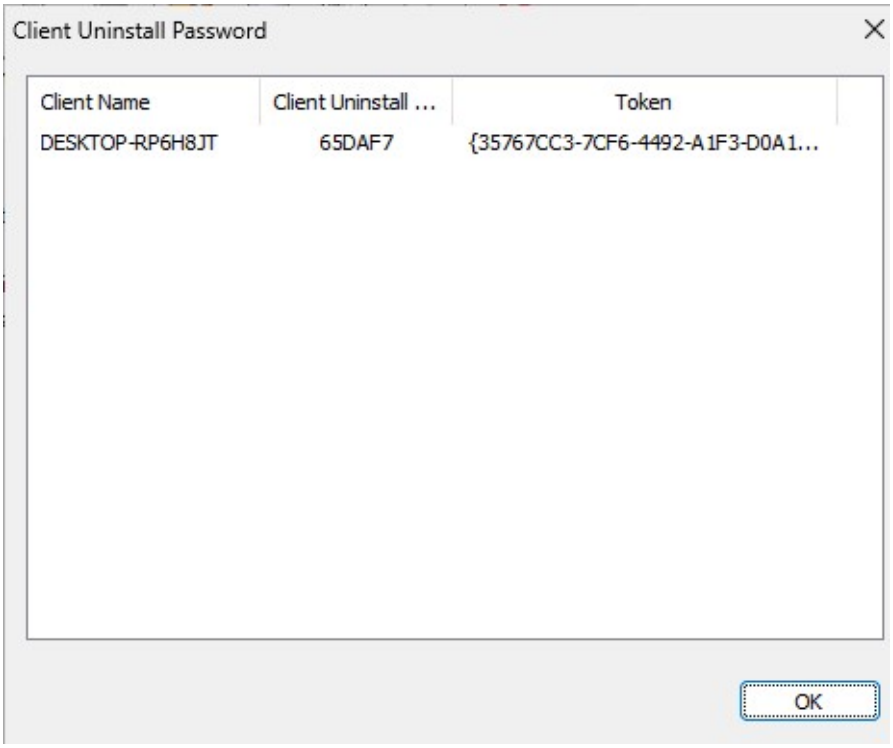
1. In Curtain Lite Admin, select Online/Offline in left panel. Then, workstations will be listed out in the right panel.



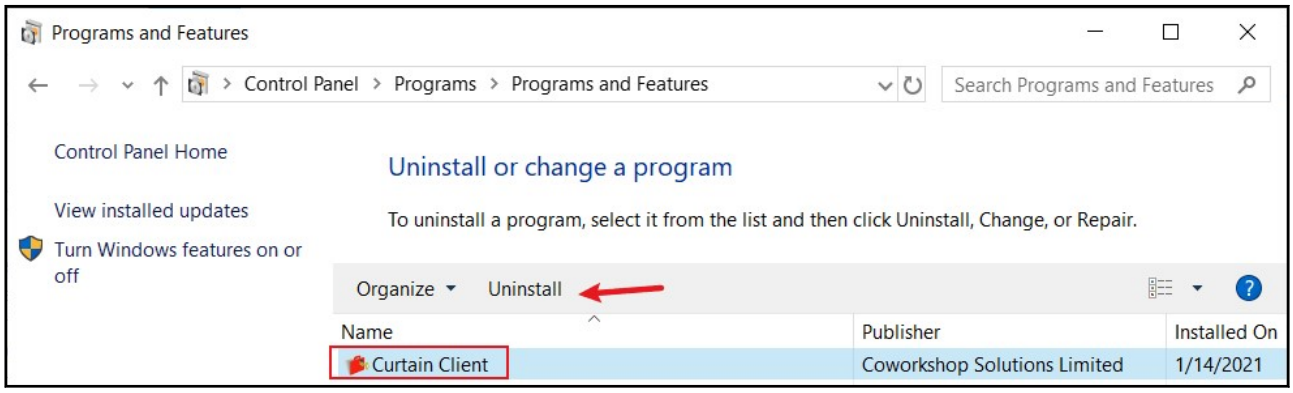
2. Select workstations and right click to choose "Generate Client Uninstall Password"



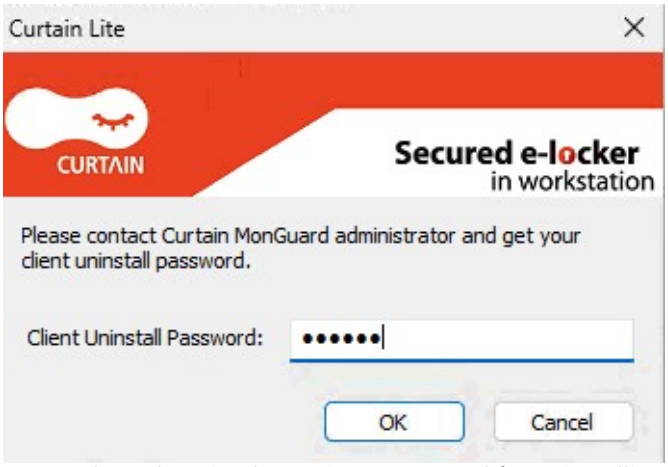
Then unique password will be generated for each client. These passwords are used for uninstalling Curtain Lite Client in specific workstation.



3. In workstation (e.g. MSEDGEWIN10), uninstall Curtain Lite Client in Windows Control Panel.



4. Enter the uninstall password and Click "OK" to proceed.



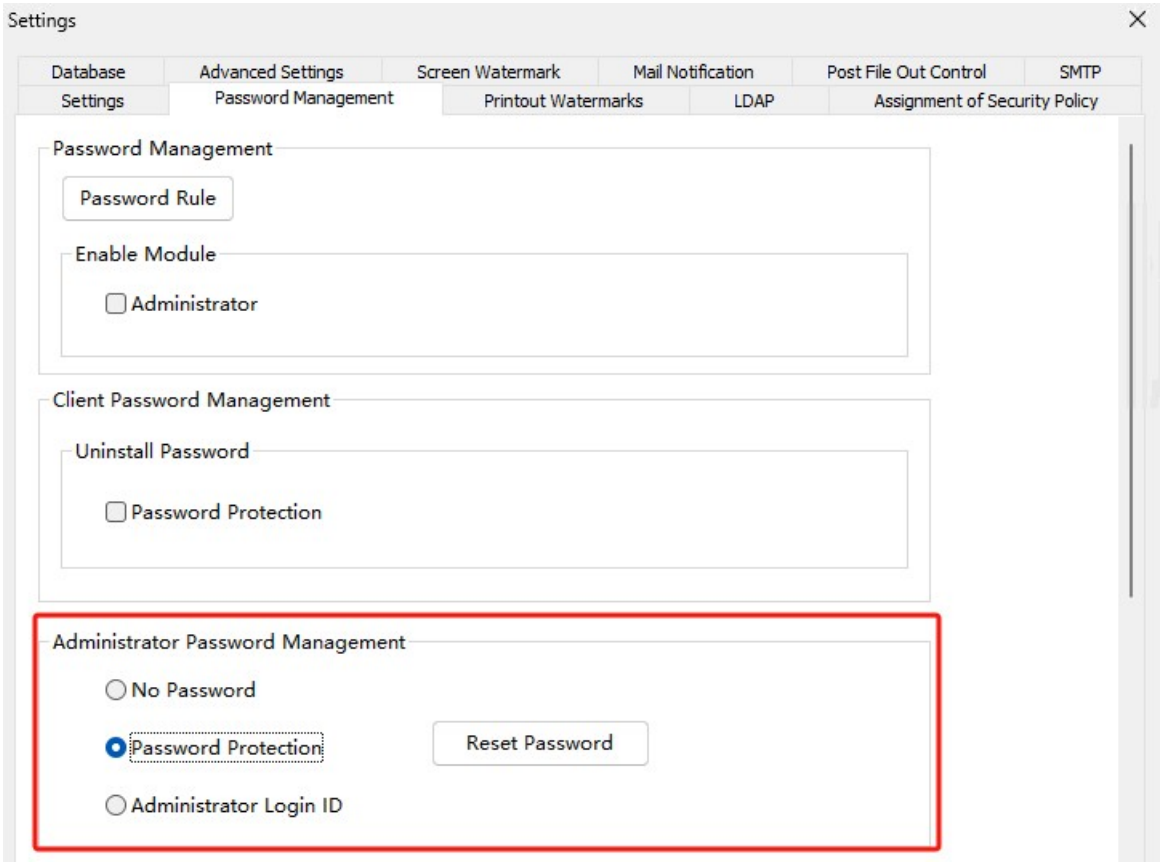
P.S. Each workstation has unique password for uninstalling Curtain Lite Client.

6.2 - Set login password for Curtain Lite Admin

By default, users do not need to enter password for launching Curtain Lite Admin. Administrators can enable password protection to enhance the security.

Steps to enable login password for Curtain Lite Admin:
1. In Curtain Lite Admin, select "File > Settings".

2. In Password Management tab, check "Password Protection" under Administrator Password Management as below. If it is the first time to set password for Curtain Lite Admin, a dialog box will be shown for entering new password. Otherwise, the last password will be used.



3. Enter password and click "OK" to confirm.

4. Done. Next time administrators have to enter correct password when they open Curtain Lite Admin.

P.S.
1. The password management function can only be used after activation.
2. For Administrator Login ID, please refer to FAQ00310.

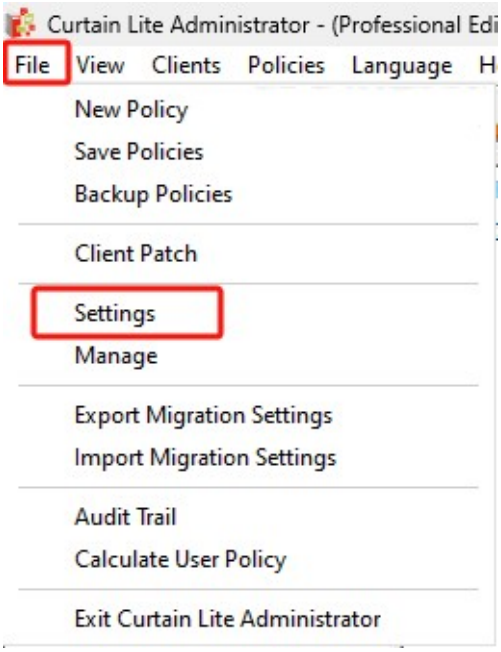
6.3 - Watermark for Printouts

If you want to add watermark to printouts, you can use this function. Text (e.g. username or disclaimer) or Picture (e.g. company logo) can be used for watermark.

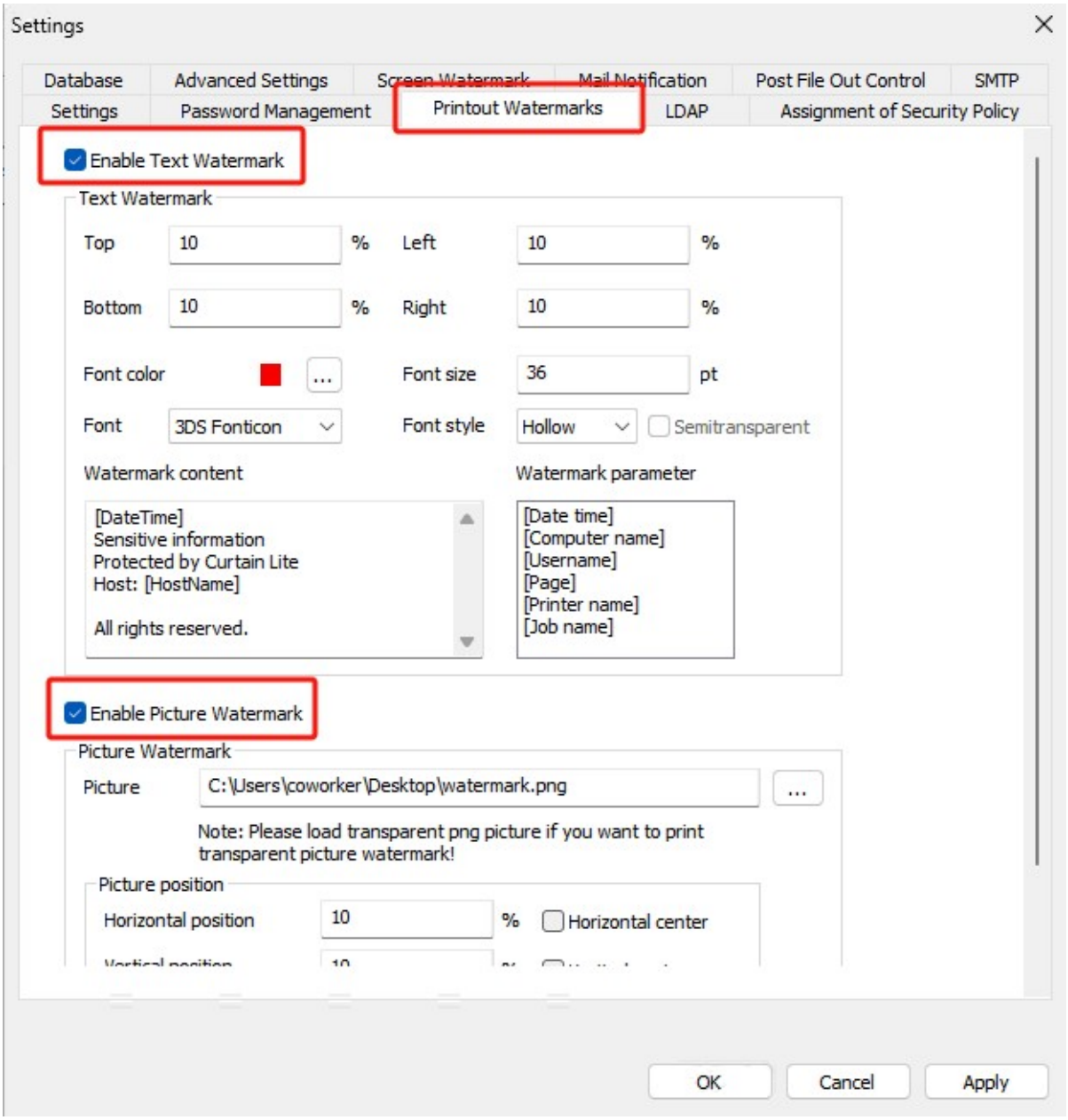
Steps to define Watermark:
1. Enable the watermark function (text watermark and image watermark) in Curtain Lite Admin global settings.
2. Select the application and enable the "Watermark for Printouts" function in a policy group of Curtain Lite Admin .
3. View the effect of "Watermark for Printouts" in user's PC.

Detailed steps of Watermark:
Step 1. Enable the watermark function (text watermark and image watermark) in Curtain Lite Admin global settings.

1.1. In Curtain Lite Admin, select "File > Settings".



1.2. Check "Enable Text Watermark" or "Enable Picture Watermark" as needed.



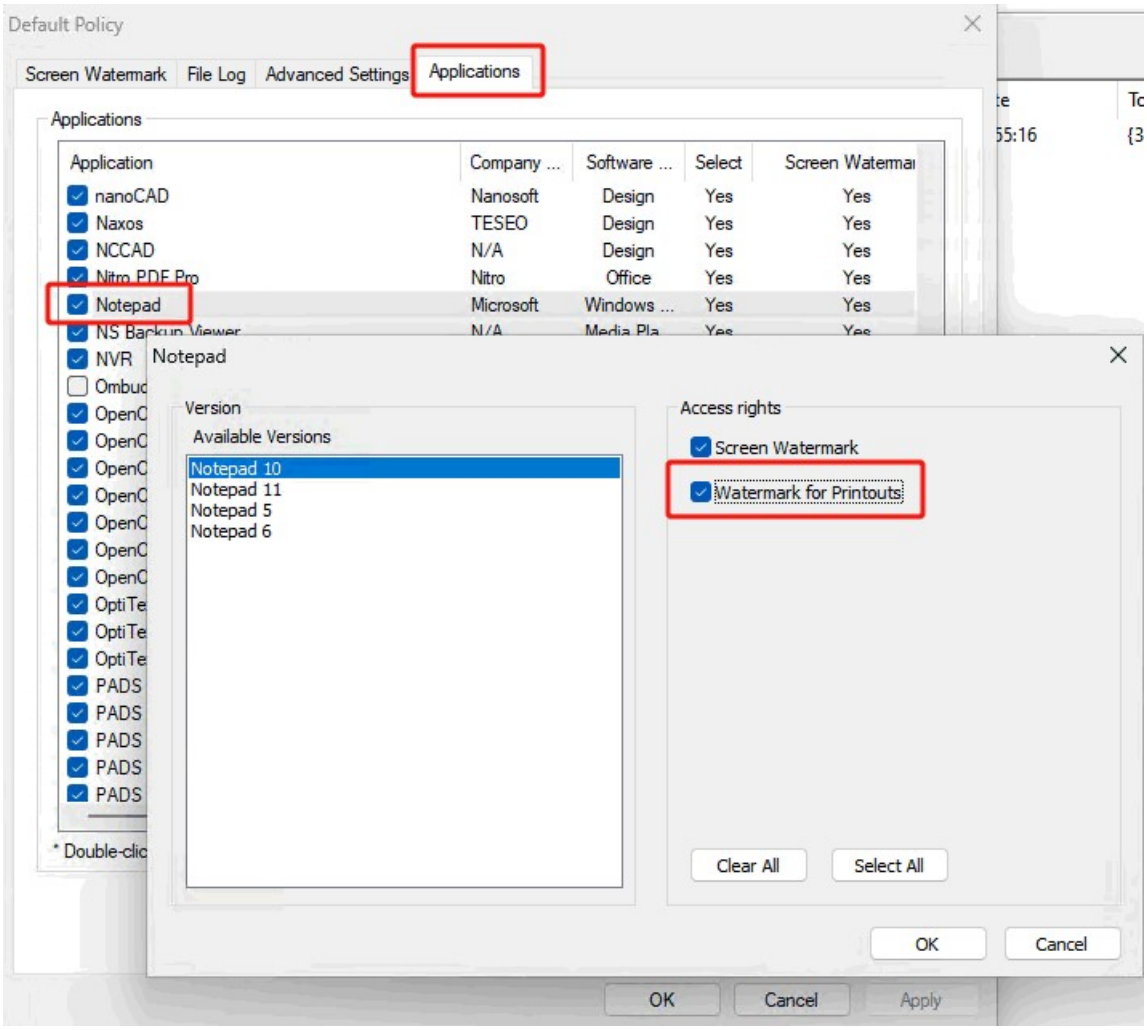
1.3 Click OK to confirm.

Step 2. Select the application and enable the "Watermark for Printouts" function in a policy group of Curtain Lite Admin .

2.1. In Curtain Lite Admin, select a Policy Group and right-click to select "Properties".

2.2. In Applications tab, double-click the application which you want to enable "Watermark for Printouts".

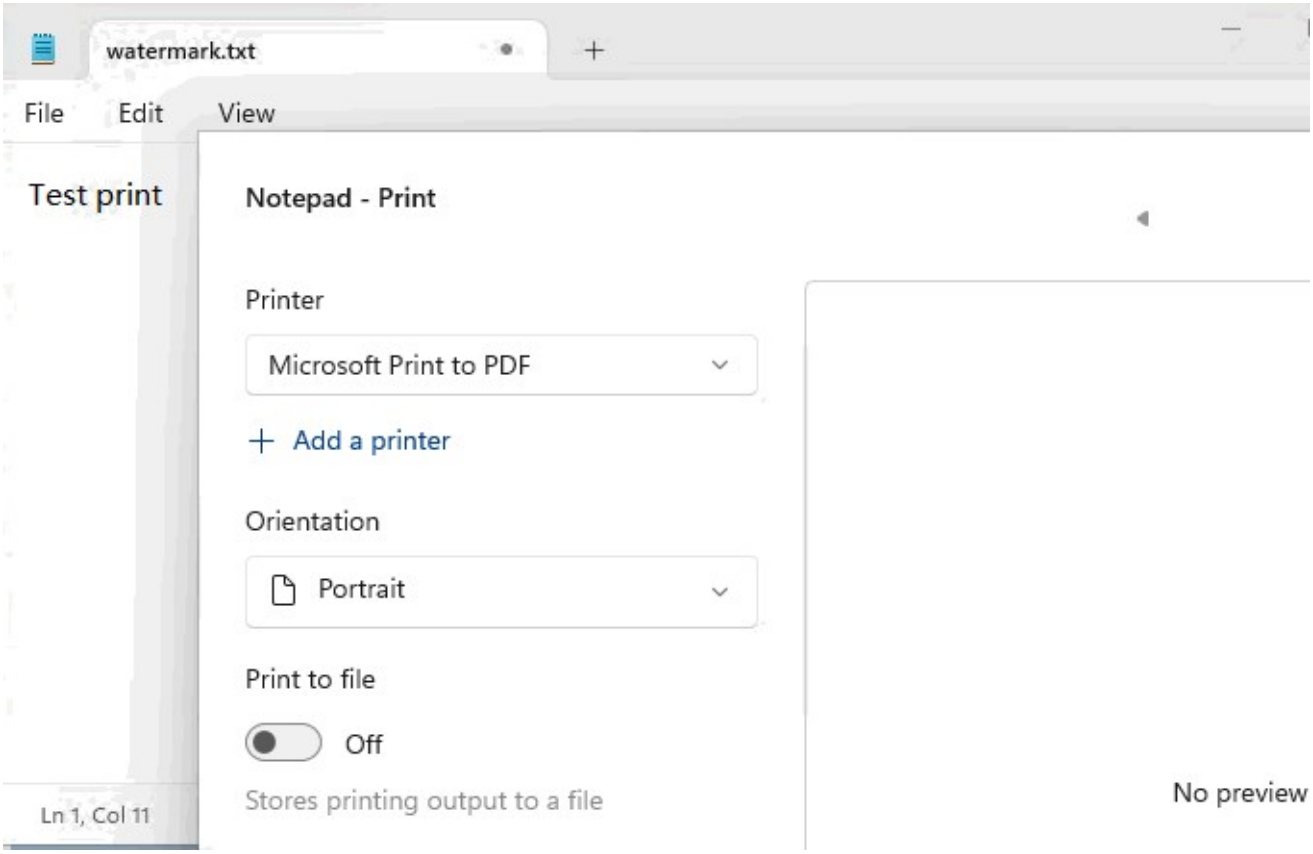
2.3. Select "Watermark for Printouts" and click OK to confirm.



Step 3. View the effect of "Watermark for Printouts" in user's PC.

3.1 In user's PC, open the application with the function of "Watermark for Printouts" , such as Notepad software or txt documents.

3.2 Print documents to a real printer, or "Microsoft print to PDF".



3.3 If "Microsoft print to PDFf" is used, watermark will be also added to the newly generated PDF document.