



# Curtain™ e-locker 5.0

## Installation Guide

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](mailto: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 e-locker, please refer to the Curtain Software License agreement.

© 2002-2018 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**

|                                                                                                                |    |
|----------------------------------------------------------------------------------------------------------------|----|
| <b>Chapter 1 - Introduction</b>                                                                                |    |
| 1.1 - Challenges on Data Leakage                                                                               | 1  |
| 1.2 - What is the purpose of Curtain e-locker?                                                                 | 1  |
| 1.3 - Backend systems (e.g. Windows file server) also have access control.<br>Why do we need Curtain e-locker? | 1  |
| 1.4 - USB port and Internet access are blocked in my company. Why do<br>we need Curtain e-locker?              | 2  |
| 1.5 - About Curtain e-locker                                                                                   | 3  |
| 1.5.1 - Basic Controls of Curtain e-locker                                                                     | 3  |
| 1.5.2 - Architecture of Curtain e-locker                                                                       | 3  |
| 1.5.3 - Components of Curtain e-locker                                                                         | 4  |
| 1.5.4 - Curtain Protected Zone                                                                                 | 5  |
| <b>Chapter 2 - Preparation before Installation</b>                                                             |    |
| 2.1 - High-level Installation Plan                                                                             | 7  |
| 2.2 - System Requirements                                                                                      | 7  |
| 2.2.1 - System Requirements of Curtain Server Plug-in and Curtain Admin                                        | 7  |
| 2.2.2 - System Requirements of Curtain Client                                                                  | 8  |
| 2.3 - Curtain Basic Access Rights                                                                              | 8  |
| 2.4 - Open Port for Curtain e-locker                                                                           | 10 |
| 2.4.1 - Open Port 24821 and 24822 for Curtain Admin and Curtain<br>Server Plug-in                              | 10 |
| 2.4.2 - Open Port 24821 and 24822 for Curtain Client                                                           | 18 |
| 2.4.3 - Check whether Tomcat Port 8005 is occupied on Curtain Server<br>Plug-in                                | 26 |
| 2.4.4 - Change Tomcat Port 8005 for Curtain Server Plug-in                                                     | 27 |
| <b>Chapter 3 - Installation</b>                                                                                |    |
| 3.1 - Install Curtain Admin                                                                                    | 28 |
| 3.2 - Install Curtain Server Plug-in                                                                           | 31 |
| 3.3 - Install Curtain Client                                                                                   | 33 |
| <b>Chapter 4 - Product Activation</b>                                                                          |    |
| 4.1 - Product Activation                                                                                       | 37 |
| 4.2 - Activate Curtain e-locker                                                                                | 37 |
| <b>Chapter 5 - Configurations</b>                                                                              |    |
| 5.1 - Create Control Policy Group                                                                              | 41 |
| 5.2 - Configure Control Policy Group                                                                           | 42 |
| 5.3 - Set Default Policy                                                                                       | 44 |
| 5.4 - Grant control policy by user/user group                                                                  | 45 |
| 5.5 - Assign workstations/users to Control Policy Group                                                        | 49 |
| 5.6 - Define Protected Server Resources                                                                        | 51 |
| 5.7 - Protect sub-folder of a share folder                                                                     | 57 |
| 5.8 - Exception Rule                                                                                           | 61 |
| 5.8.1 - Exception Rule                                                                                         | 61 |
| 5.8.2 - Set Exception Rule                                                                                     | 63 |
| 5.9 - Disable protection temporarily                                                                           | 67 |

---

|                                                                                    |     |
|------------------------------------------------------------------------------------|-----|
| <b>Chapter 6 - Other Features</b>                                                  |     |
| 6.1 - Protect First Draft                                                          | 69  |
| 6.2 - Online/Offline Protection                                                    | 71  |
| 6.3 - Housekeeping                                                                 | 72  |
| 6.4 - Screen Capture Protection                                                    | 73  |
| 6.5 - Smart Copy-and-Paste Control                                                 | 73  |
| 6.6 - Secure Print-to-PDF                                                          | 74  |
| 6.7 - Share protected files with others                                            | 75  |
| 6.8 - Audit Trail                                                                  | 79  |
| 6.9 - Send Request                                                                 | 81  |
| 6.10 - Watermark for Printouts                                                     | 86  |
| 6.11 - Snapshot for printouts                                                      | 90  |
| 6.12 - Create shortcut for protected application                                   | 91  |
| 6.13 - Local Encrypted Drive                                                       | 93  |
| 6.14 - Set login password for Curtain Admin, Server Plug-in and Client             | 107 |
| 6.15 - Change or reset login password for Curtain Admin, Server Plug-in and Client | 109 |
| <br>                                                                               |     |
| <b>Chapter 7 - Ongoing Maintenance</b>                                             |     |
| 7.1 - Patch Management                                                             | 111 |
| 7.2 - Migrate Curtain Admin to a new machine                                       | 112 |
| 7.3 - Backup and restore Curtain Admin policies and audit log manually             | 114 |
| 7.4 - Backup Curtain Admin policies automatically                                  | 115 |
| <br>                                                                               |     |
| <b>Chapter 8 - Frequently Asked Questions</b>                                      |     |
| 8.1 - How to avoid conflict with Antivirus?                                        | 117 |
| 8.2 - Use Curtain e-locker to protect NAS through iSCSI                            | 117 |
| 8.3 - Enable/disable Curtain Debug Log                                             | 135 |
| 8.4 - Generate unique token for cloned Curtain Client                              | 136 |
| <br>                                                                               |     |
| <b>Chapter 9 - Best Practice</b>                                                   |     |
| 9.1 - Allow protected files copy/send out of protected zone                        | 138 |
| 9.2 - How to protect SolidWorks Enterprise PDM?                                    | 141 |



# 1 - Introduction

## 1.1 - Challenges on Data Leakage

In everyday operations, users have access to and work on sensitive files. However, it is difficult for companies to control how the users use the files. Once users have access rights to a piece of electronic information, in a sense they "own" the information and as such, they can easily mis-use the information or "leak" the information via different channels (e.g. email, Internet, USB disk, etc). It is difficult for companies to fully control the use of such information. There are many ways by which a user can steal a file. When a user is authorized to access a file (e.g. read/edit), it is difficult to prevent the user to copy and take the file out of the company.

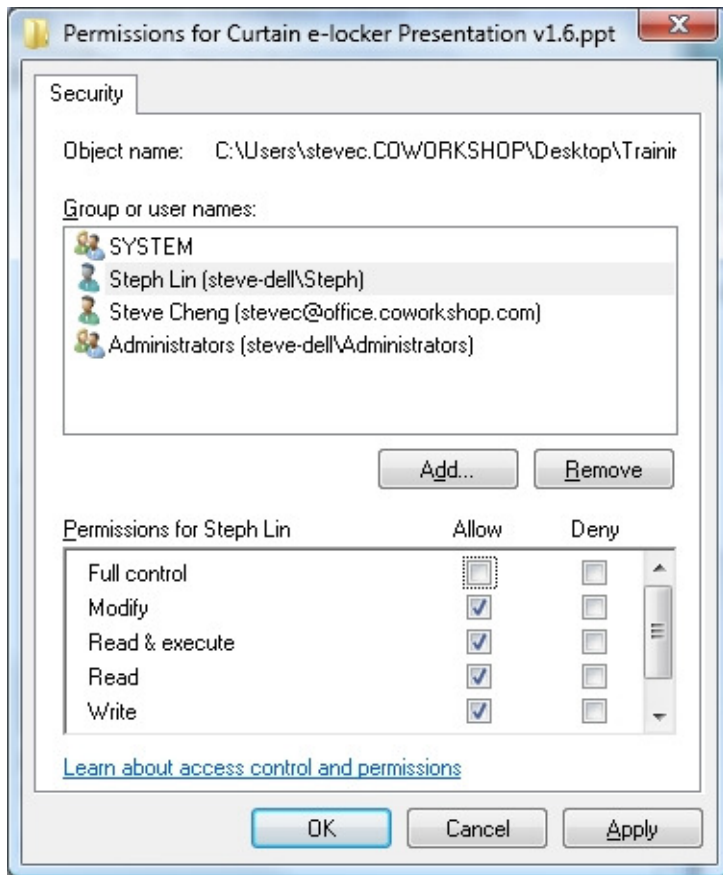
## 1.2 - What is the purpose of Curtain e-locker?

Curtain e-locker – a Data Loss Prevention (DLP) solution, which effectively prevents unauthorized leakage/usage of protected confidential information by any exit channels. By using Curtain e-locker, a company can allow authorized users to access confidential files and information. At the same time, the company can control NOT to allow the users to take the files/information out of the company during normal course of daily operations.

## 1.3 - Backend systems(e.g. Windows file server) also have access control. Why do we need Curtain e-locker?

Yes, backend systems also have access control. However, backend systems can only control permission of Read, Edit, Delete, and etc. If administrators allow users to access server information (e.g. a share folder), backend systems CANNOT stop the users to save files to local drive, USB hard-disk, or send files out through email. This area is responsible by Curtain e-locker. Therefore, Curtain e-locker is like to work with your backend systems, instead of replacing them. When a user is allowed to access server resources, administrators can adopt Curtain e-locker to prevent the user to take sensitive information out of the company.

For example: It is permission setting for a Windows folder. There is no option for controlling Print and Save.



## 1.4 - USB port and Internet access are blocked in my company. Why do we need Curtain e-locker?

Yes, blocking USB port and Internet access can reduce the risk of data leakage. However, there are so many ways for sending information out. For example:

- Print
- Print-screen or Capture-screen software
- Copy and Paste
- Email
- Wi-Fi or Bluetooth (using mobile phone as hotspot)
- Skype, Whatsapp, QQ
- and more...

Some companies are trying to block all channels to prevent data leakage. However, it is difficult for system administrators to setup and maintain so many controls. Moreover, it is inconvenient for end-users to work without email, Internet, Skype, and USB nowadays.

Curtain e-locker does not affect users' normal operations, while security is maintained. Curtain e-locker makes a good balance between convenience and security.

## 1.5 - About Curtain e-locker

### 1.5.1 - Basic Controls of Curtain e-locker

Curtain e-locker controls:

- Save Anywhere
- Send
- Print
- Print Screen
- Copy Content to Anywhere
- Copy File to Anywhere

Curtain e-locker ONLY controls files within Protected Zone. Users still can use files within Protected Zone as usual. Only unauthorized activities are blocked by Curtain. For example, if a user is not authorized to save files out of Protected Zone or even print files out, all these activities are blocked by Curtain. The user still can use email, USB hard-disk, or Internet, only files in Protected Zone are controlled by Curtain.

Administrators can define different control policy groups for different users or workstations. Please refer to related documents.

### 1.5.2 - Architecture of Curtain e-locker

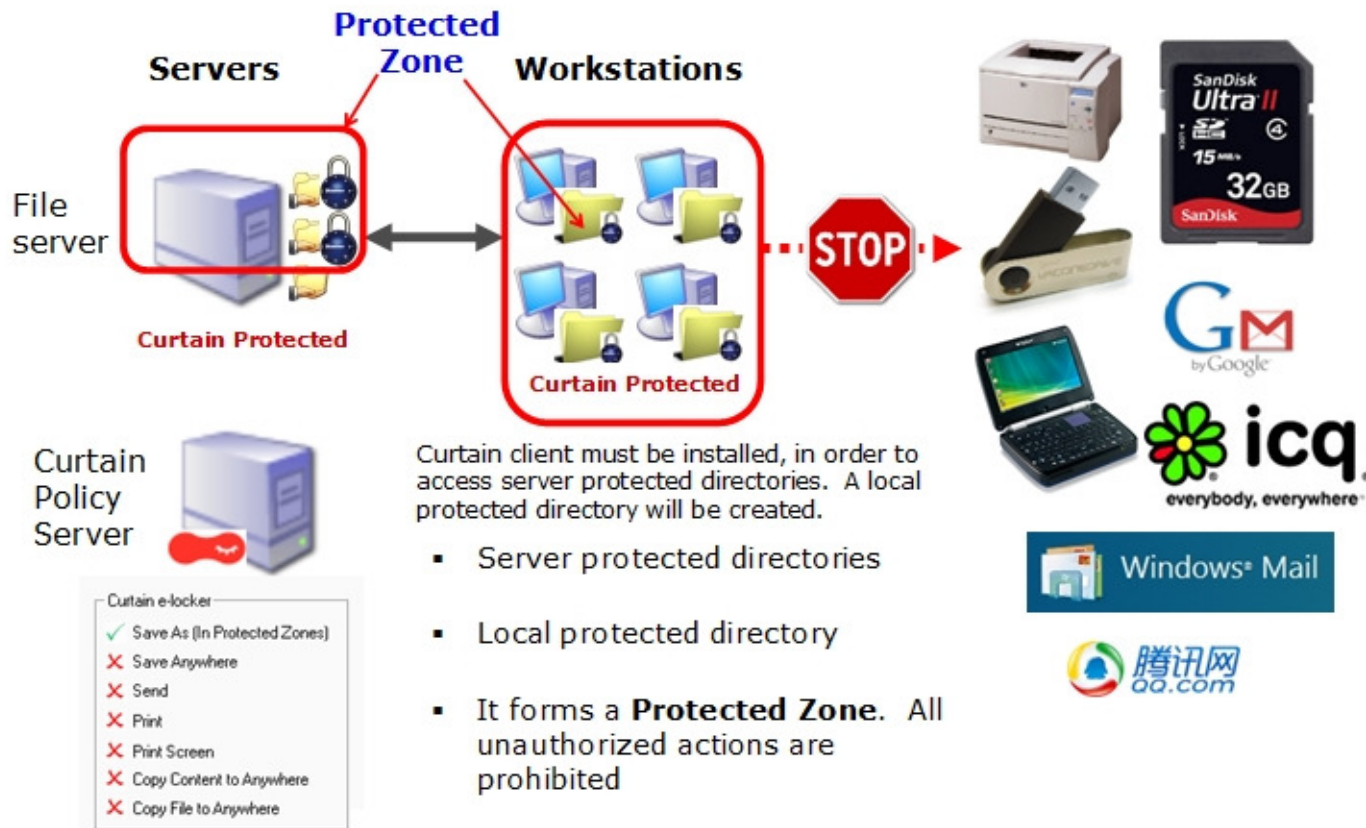
Employees have to access information to perform their roles (e.g. Sales persons need to access customer information, Engineers need to access design drawings, and etc). When they have access to share folders in Windows File Server, it is difficult to control them not to copy the information out of the company.

With Curtain e-locker, there is a Curtain Policy Server (that hosts Curtain Admin). Administrators can define which share folders in Windows File Server are protected by Curtain. In order to access Protected Share Folders, Curtain Client must be installed on users' workstations. A secure folder (i.e. Local Protected Directory) will be automatically created in user's workstation during installation of Curtain Client.

Then administrators can define different control policies centrally in Curtain Admin. The control policies are applied to control users' workstations. Curtain e-locker has a unique design called Protected Zone (i.e. combined by Protected Share Folders in file server and Local Protected Directory in user's workstation). Users can work with sensitive information within the Zone as usual (e.g. Read, Edit, etc). If they are not authorized, they cannot take the information out of the Zone. At the same time, users can still use Internet, email, and etc.



## Architecture



### 1.5.3 - Components of Curtain e-locker

There are 3 basic components of Curtain e-locker:

- Curtain Client
- Curtain Admin (for the machine having Curtain Admin, we call it Curtain Policy Server)
- Curtain Server Plug-in

**Curtain Client:**

When a user accesses Protected server resources (e.g. Protected Share Folder, Protected website, etc), Curtain Client must be installed in the user's workstation. A secure folder (i.e. Local Protected Directory) will be automatically created in user's workstation during installation of Curtain Client.

**Curtain Admin:**

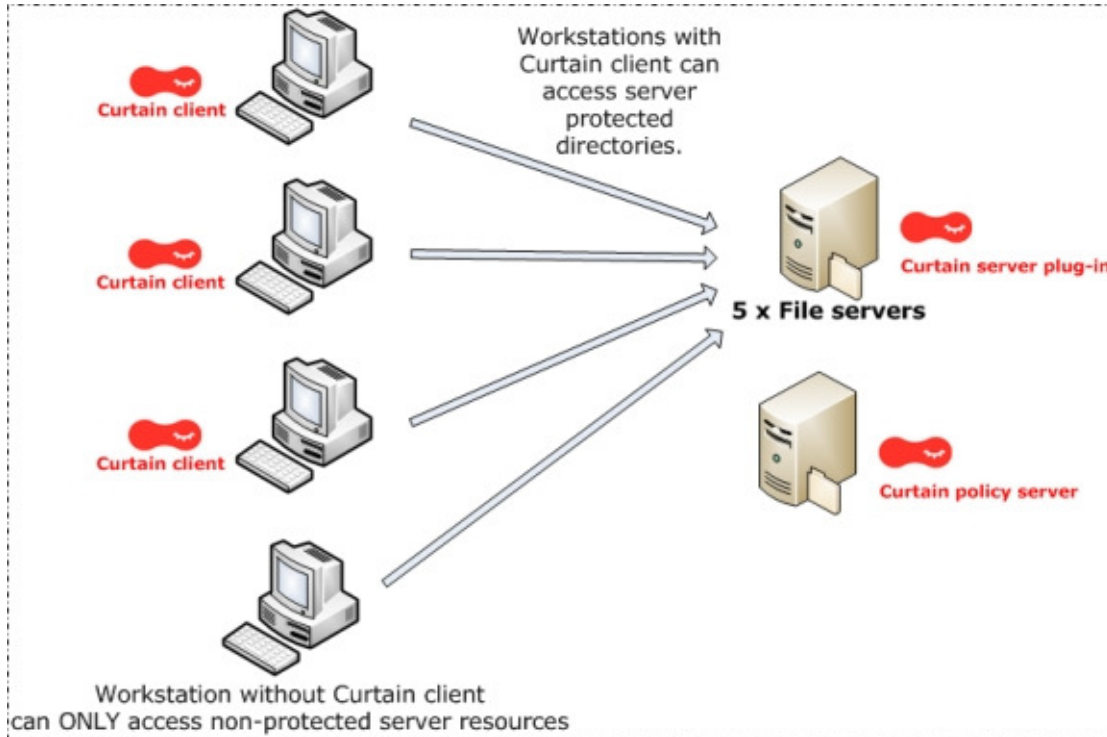
Curtain Admin is mainly for system administrators to define Curtain control policies centrally. It also stores audit log for management review. In general, only one Curtain Admin is needed in a company.

**Curtain Server Plug-in:**

Curtain Server Plug-in should be installed on all servers which need Curtain Protection. Curtain Admin will communicate with Curtain Server Plug-ins periodically, to instruct them how to protect the server resources.

Example: This company wants to protect share folders of 5 Windows File Servers. Then, they need to install Curtain Server Plug-on on those 5 file servers.

Here is the basic architecture of Curtain e-locker:



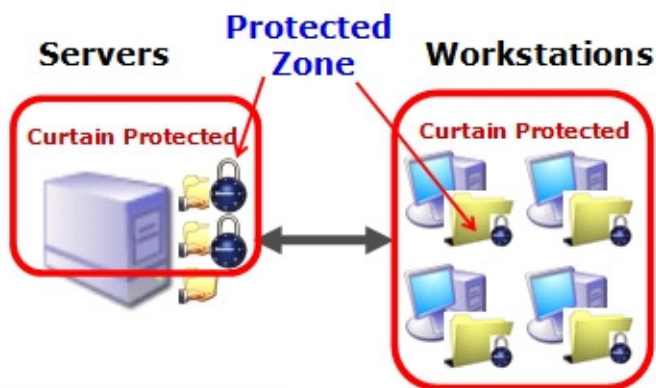
P.S.

- Curtain Admin can be installed on a separated machine or one of the File Servers.
- Administrators can use the function of "Exception" to allow workstation to access protected server resource without Curtain Client installed.

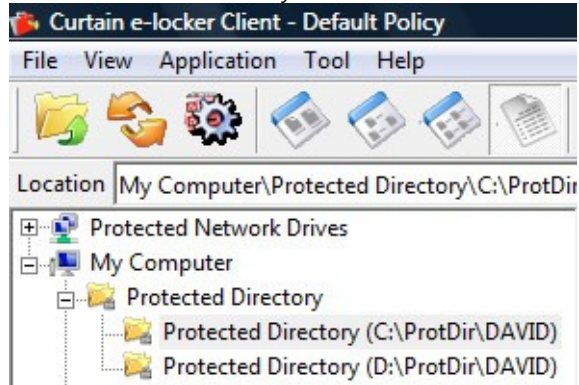
### 1.5.4 - Curtain Protected Zone

Protected Zone is formed by Protected area in server-side and Local Protected Directory in client-side. Protected area in server-side could be Share Folder in file server, SharePoint site, ERP system, self-developed system, and etc. In client-side, Local Protected Directory will be automatically created during installation of Curtain Client. The folder name is "ProtDir" that will be created in all local drives.

Protected Zone:



Local Protected Directory:



In this case, there are two local drives (i.e. C and D). Therefore, "ProtDir" will be created under C and D drive. Moreover, Local Protected Directory is personal according to login user. User cannot access Local Protected Directory of another user in the same workstation.

P.S.

- There is a setting called "Hide local protected directory" in control policy group. If administrators want to enforce users directly accessing protected files in file server, they can enable this function.
- There is a function called "Local Encrypted Drive". Administrators can use this function to encrypt Local Protected Directory in order to enhance the security.
- Administrators can set additional local protected directory if needed.

## 2 - Preparation before Installation

### 2.1 - High-level Installation Plan

Preparation:

- Which server resources do you want to protect (e.g. Share Folder, SharePoint, ERP, self-developed system, etc)?
- Who will access the Protected server resources?
- How do you want to control users to use the protected information (e.g. save anywhere, print, etc)?
- Which server will act as Curtain Policy server (i.e. Curtain Admin will be installed on that server)?
- Do you want to integrate Curtain e-locker with Active Directory (so that control policy can be granted to AD user/user group)?
- Do you want to encrypt Local Protected Directory in user's workstation?

High-level installation plan:

1. Install Curtain Admin
2. Install Curtain Server Plug-in on servers which your company wants to protect
3. Install Curtain Client on users' workstations
4. Activate Curtain e-locker
5. Create and configure control policy groups in Curtain Admin
6. Connect with Active Directory for collecting user information, if you prefer to grant control policy by user/user-group
7. Assign workstations/users to different policy groups
8. Define and apply protection to server resources
9. Done

P.S. Curtain Server Plug-in and Curtain Client should NOT be installed on the same machine simultaneously.

### 2.2 - System Requirements

#### 2.2.1 - System Requirements of Curtain Server Plug-in and Curtain Admin

System Requirements of Curtain Server Plug-in and Curtain Admin:

- Intel Pentium or above processor
- Windows XP/Server 2003/2008/2012/2012R2/2016/Vista/Win 7/Win 8/Win 8.1/Win 10 operating system
- 128MB RAM (Recommended 256MB RAM)
- 200MB Hard Disk (in NTFS) for installation
- TCP/IP network
- TCP Port 8443 (Default Enable)
- 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)

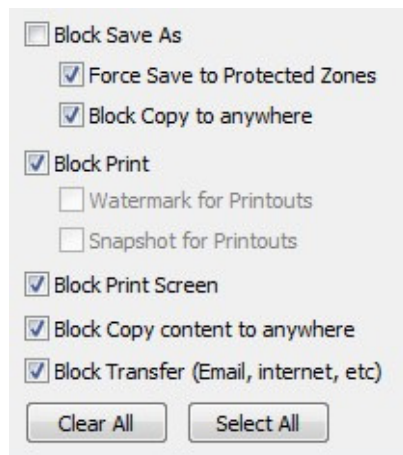
## 2.2.2 - System Requirements of Curtain Client

System Requirements of Curtain Client:

- Intel Pentium or above processor
- Windows XP/Server 2003/2008/2012/2012R2/2016/Vista/Win 7/Win 8/Win 8.1/Win 10 operating system
- 128MB RAM (Recommended 256MB RAM)
- 200MB 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)

## 2.3 - Curtain Basic Access Rights

Curtain access rights can be defined by Policy Group and Application. Here is default setting of Curtain access right.



"Force Save to Protected Zone" – When this option is selected, protected files cannot be saved out of Protected Zone (in the application, such as Word).

"Block Copy to anywhere" – When this option is selected, protected files cannot be copied out of Protected Zone (in Curtain Client).

"Block Print" – When this option is selected, "Print" and related functions in the application are blocked.

"Watermark for Printouts" – When this option is selected, watermark will be printed on the printouts (For detail information, please refer to related documents).

"Snapshot for Printouts" – When this option is selected, the system will take snapshots for printouts. The snapshots will be stored in Curtain Admin for audit purpose (For detail information, please refer to related documents).

"Block Print Screen" – When this option is selected, screen of protected files cannot be captured by Print-screen or Capture-screen software.

"Block Copy content to anywhere" – When this option is selected, copying sensitive content to non-Protected area is blocked (e.g. copying content and paste it to Gmail).

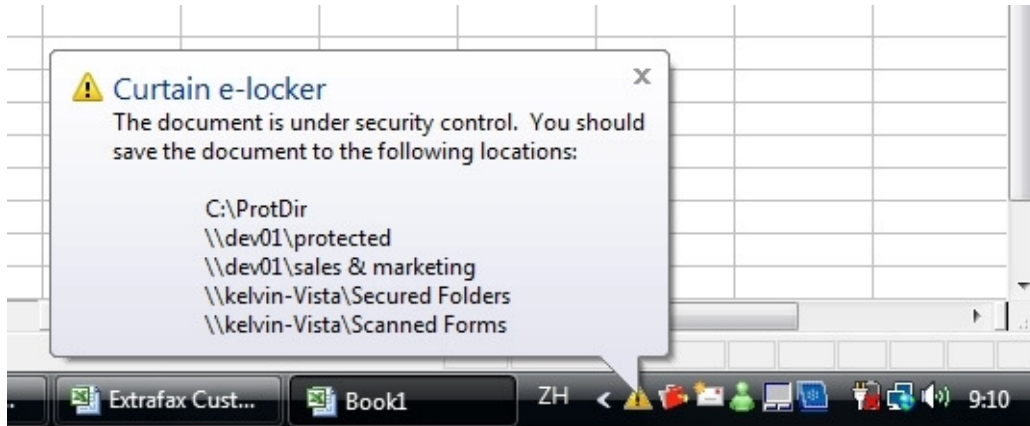
"Block Transfer (Email, Internet, etc)" – When this option is selected, "Send to" and related functions in the application are blocked.



Examples of using Curtain access rights

For scenario 1 - "Force Save to Protected Zone" is enabled for MS Word:

- When a user tries to select "File > Save As" in MS Word to save protected documents out of Protected Zone, Curtain e-locker will block it and warn the user.

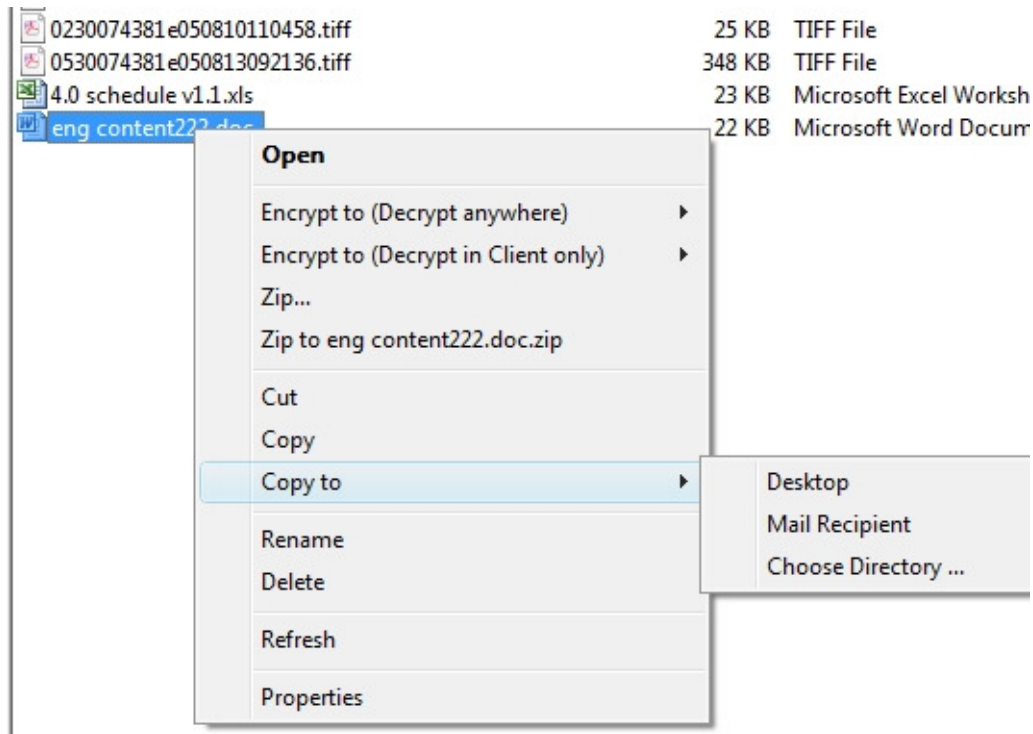


For scenario 2 - "Block Copy to anywhere" is disabled for MS Word:

- In Curtain Client, select a Word document and right-click. You can see an entry called "Copy to". You can use this function to copy Word documents out of Protected Zone.

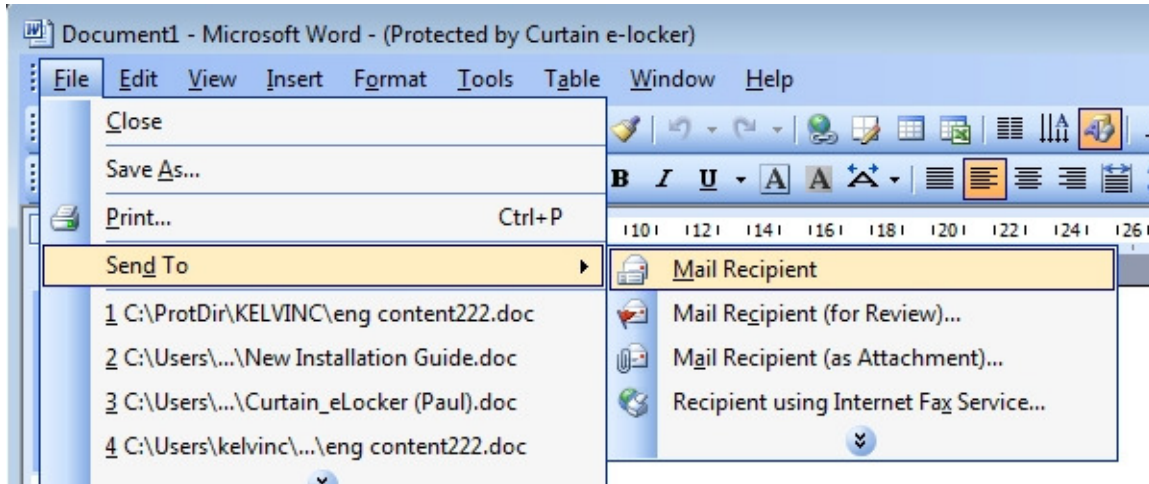
After the documents are copied out of Protected Zone:

- Curtain e-locker will not control the documents anymore.
- Curtain e-locker will log this "Copy Out" action in Audit Trail.



For scenario 3 - "Block Transfer (Email, Internet, etc)" is enabled for MS Word:

- When a user tries to select "File > Send To" in MS Word to send protected documents out of Protected Zone through email, Curtain e-locker will block it and warn the user.



## 2.4 - Open Port for Curtain e-locker

### 2.4.1 - Open Port 24821 and 24822 for Curtain Admin and Curtain Server Plug-in

If Windows Firewall is enabled, please open port 24821 and 24822 for Curtain Admin and Curtain Server Plug-in.

For Windows 2008/2012/2016/Vista/Win 7/Win 8/Win10, please add the rules as below:

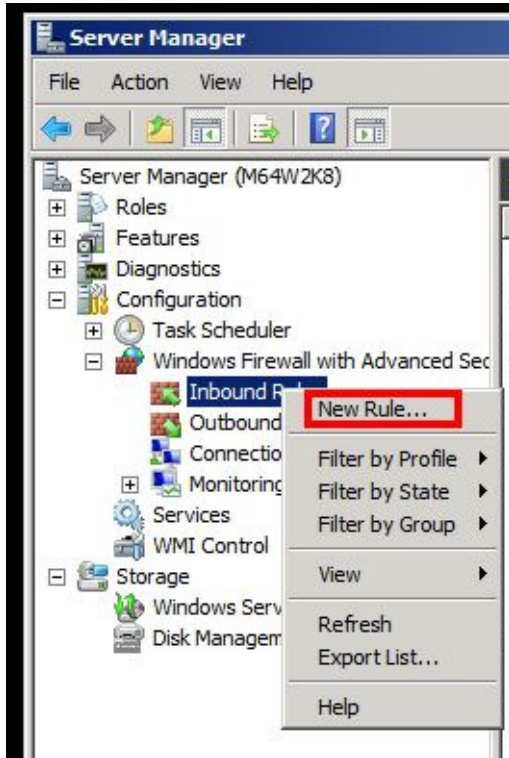
- inbound rule of 24821 port of TCP
- inbound rule of 24821 port of UDP
- outbound rule of 24822 port of TCP
- outbound rule of 24822 port of UDP

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

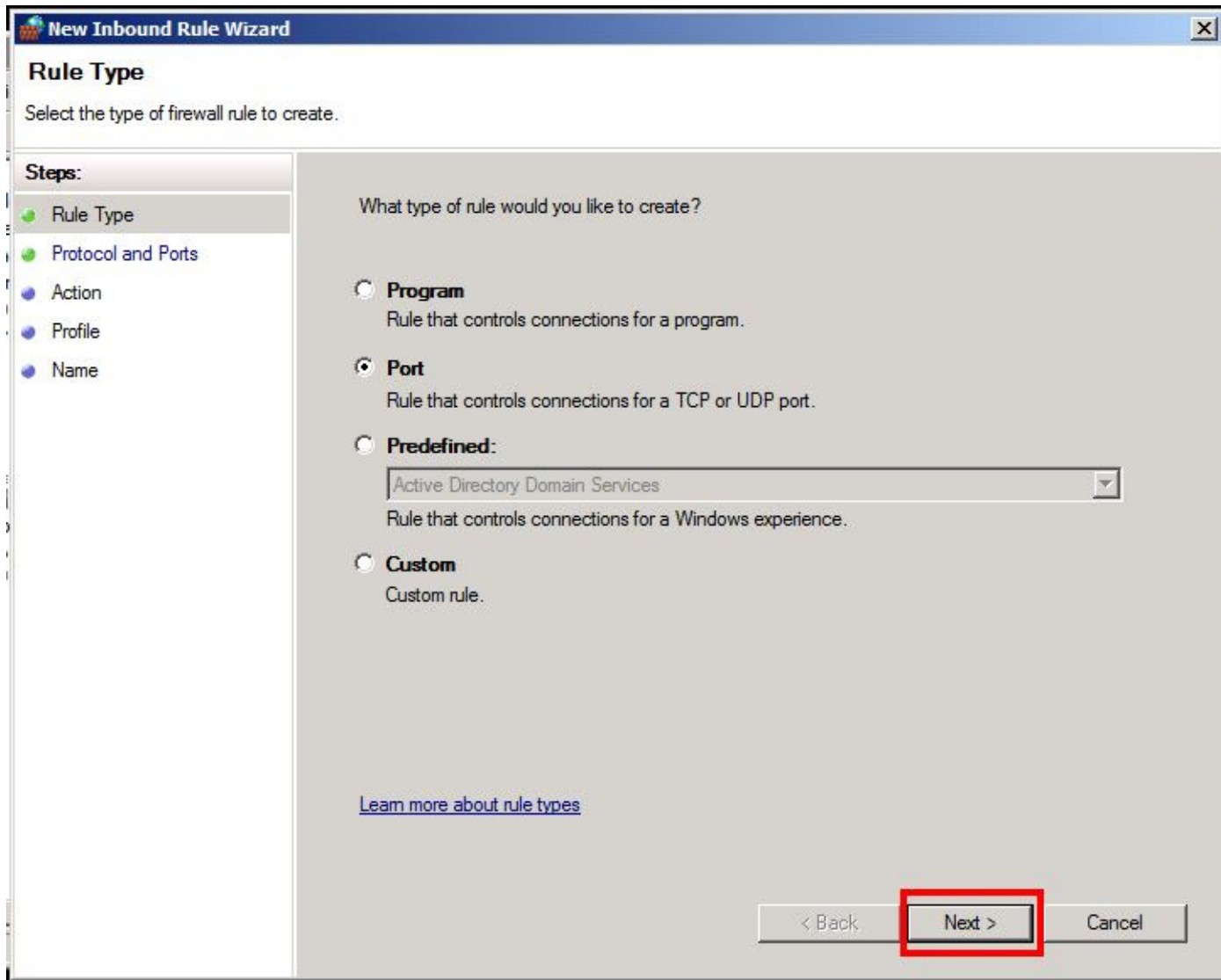
- 24821 port of TCP
- 24821 port of UDP
- 24822 port of TCP
- 24822 port of UDP

Steps to add rules for Windows 2008/2012/2016/Vista/Win 7/Win 8/Win10:

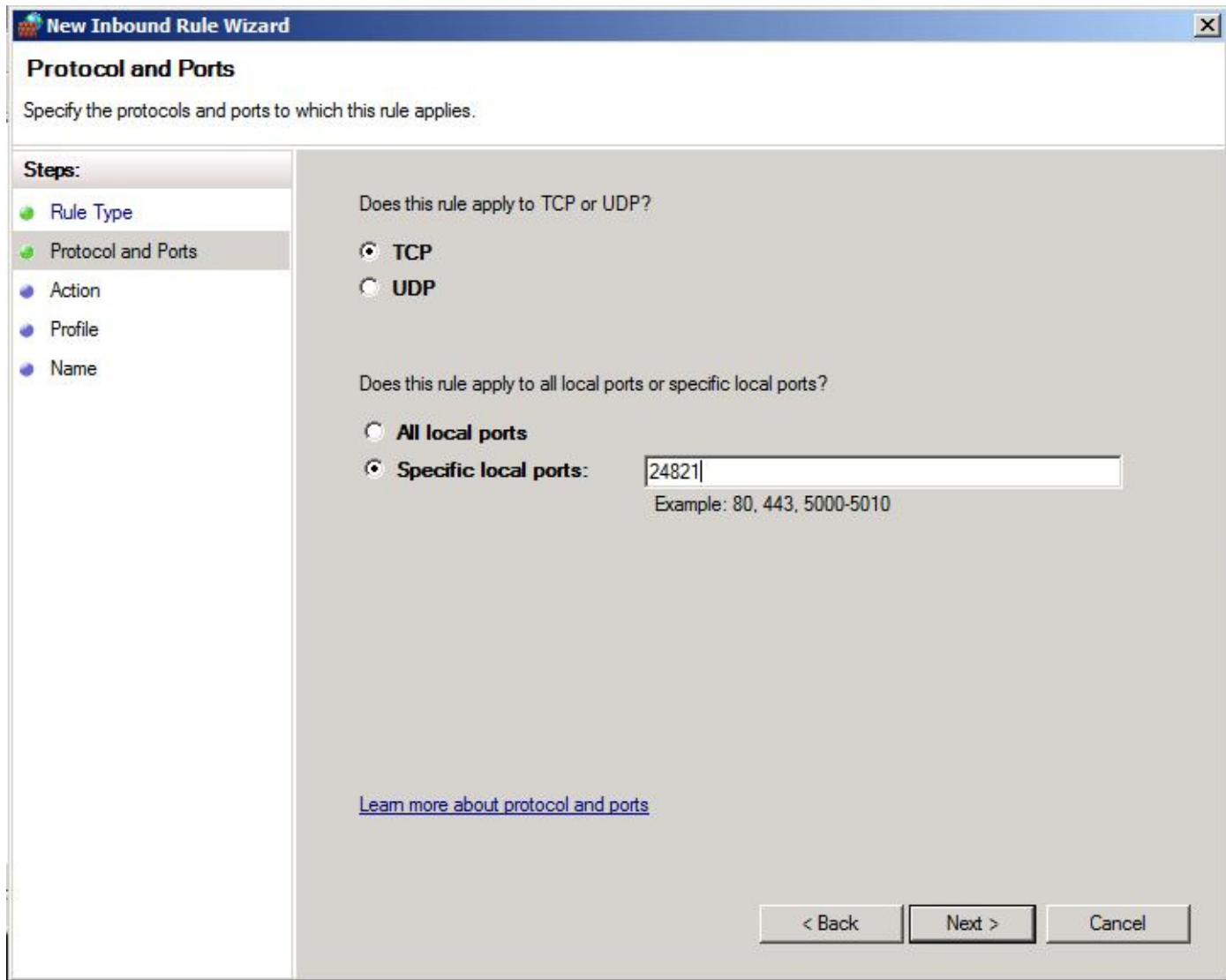
1. Select "My Computer" and right click to select "Manage"  
Then, Server Manager will be shown.
2. In Server Manager, select "Inbound Rules" as below picture and right click to select "New Rule..."



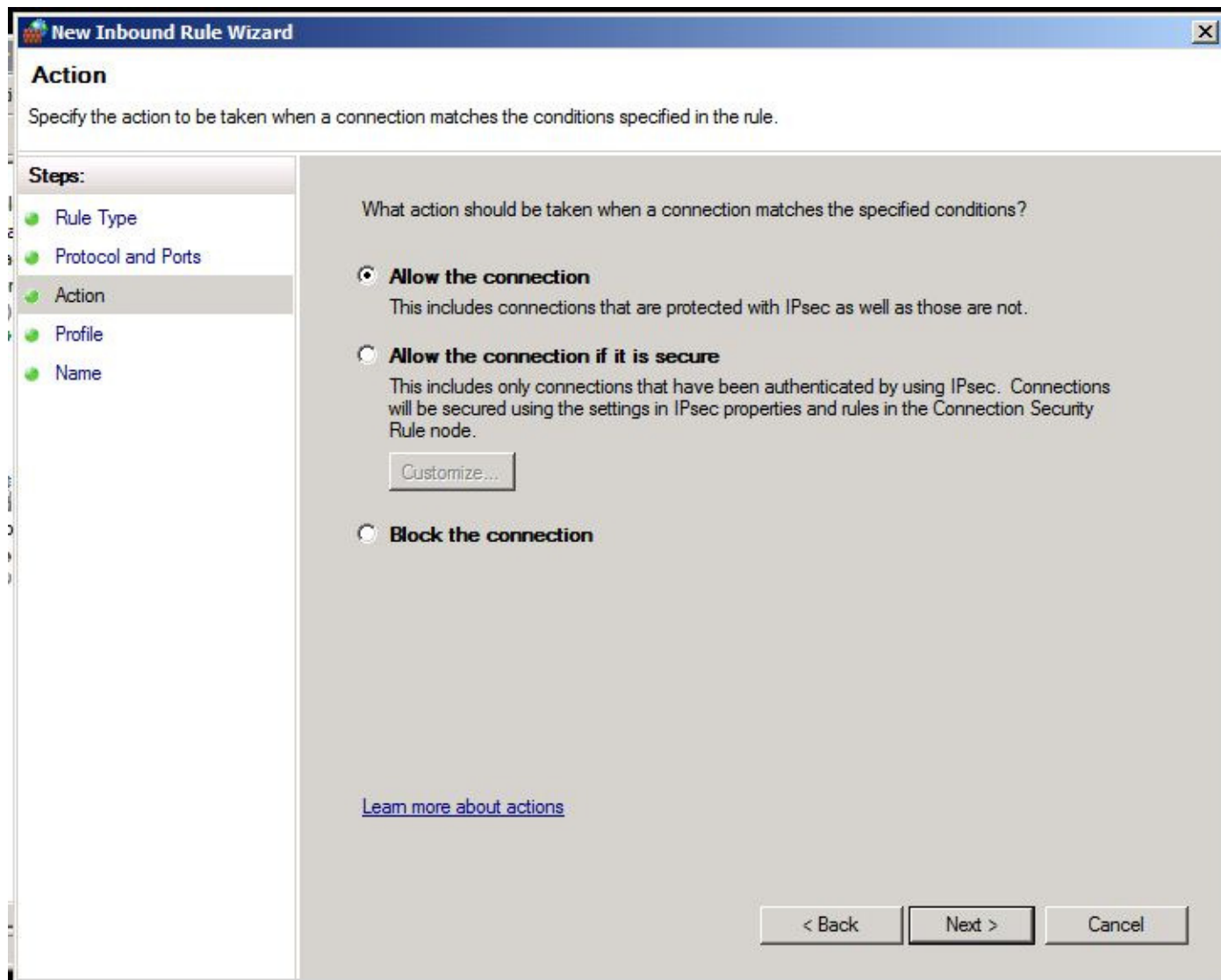
3. New Inbound Rule Wizard is shown as below, choose Port and click Next.



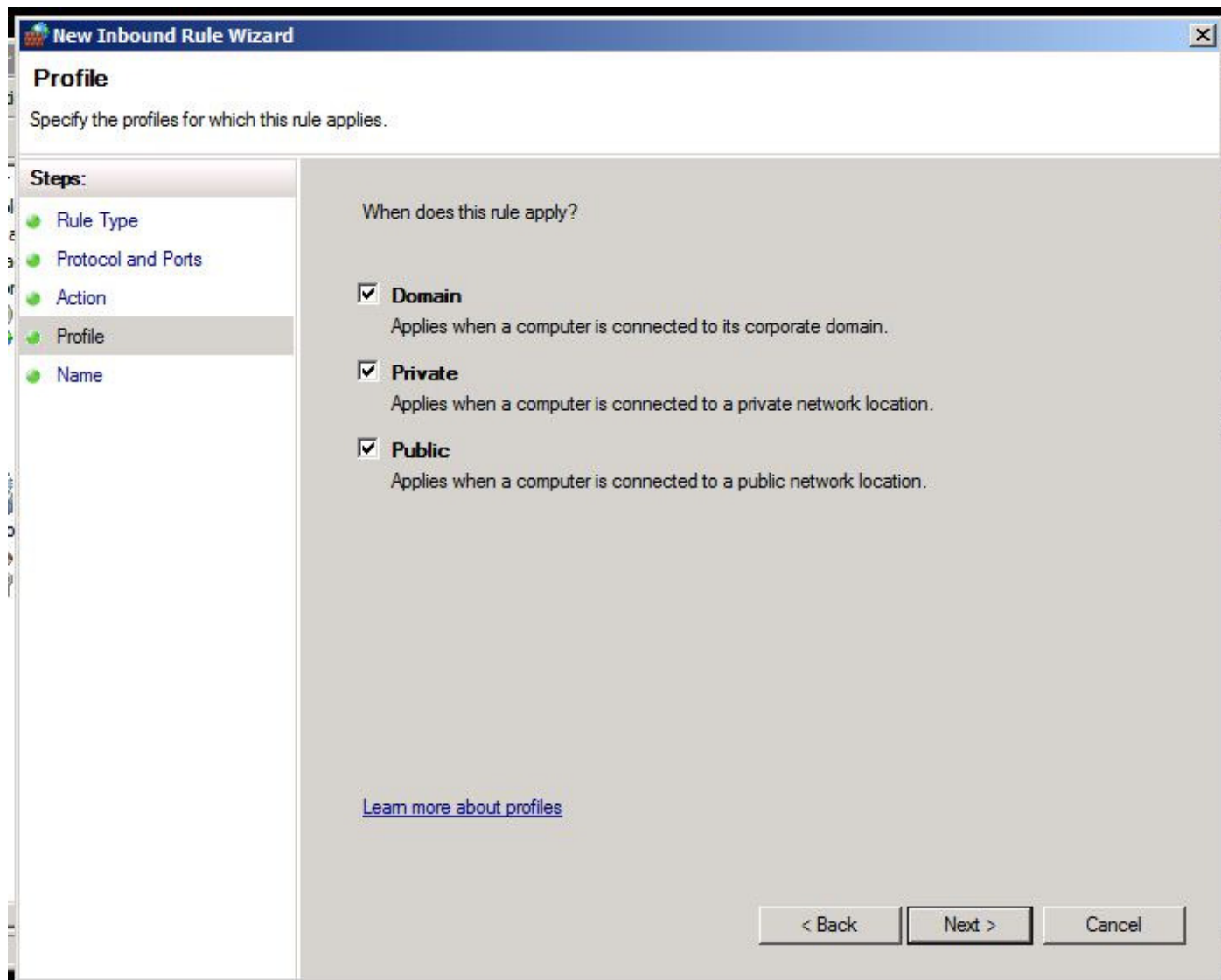
4. This rule applies to TCP and enter "24821" in Specific local ports, and click Next.



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

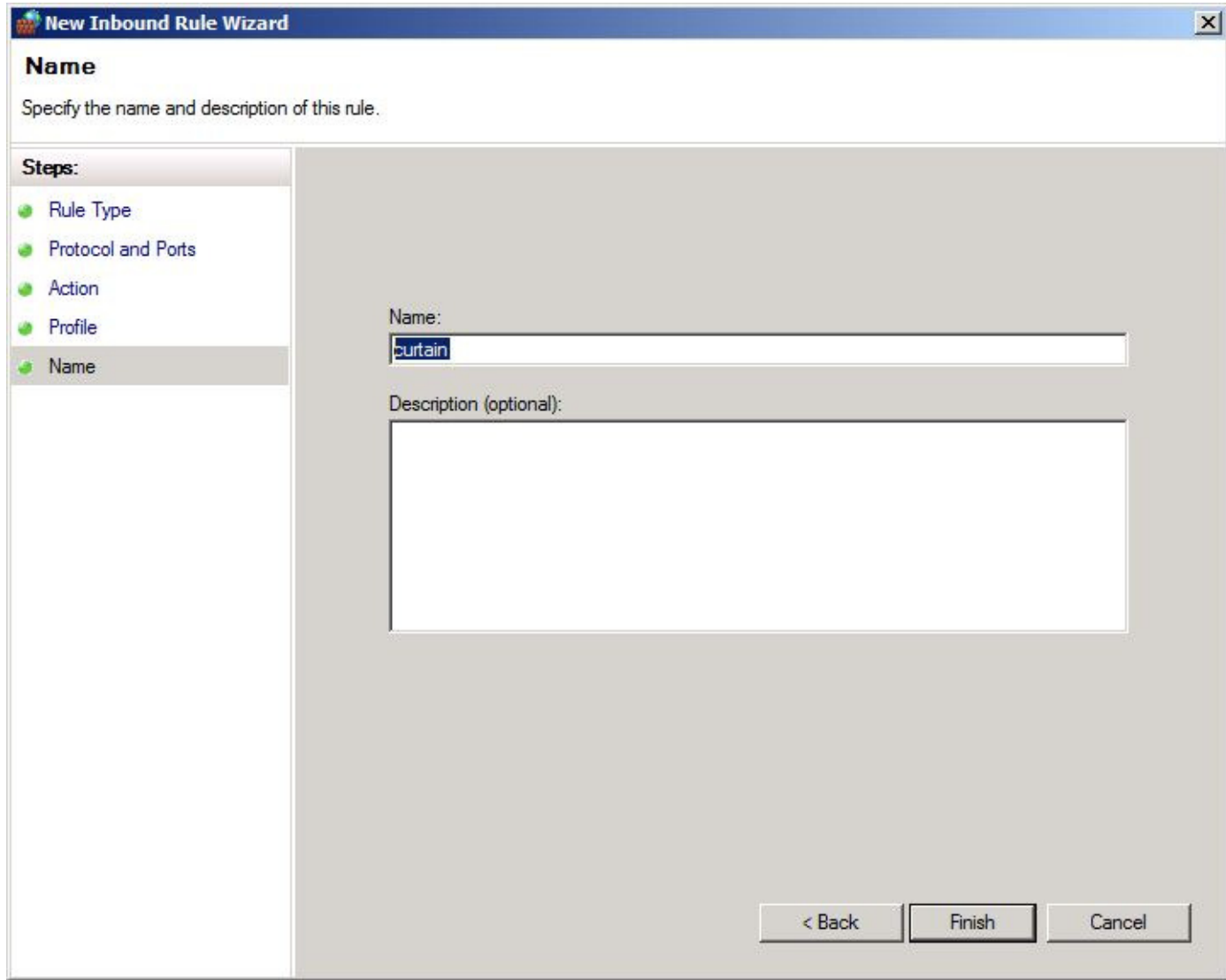


6. Check all as shown below (i.e. "Domain", "Private", and "Public") and click Next.

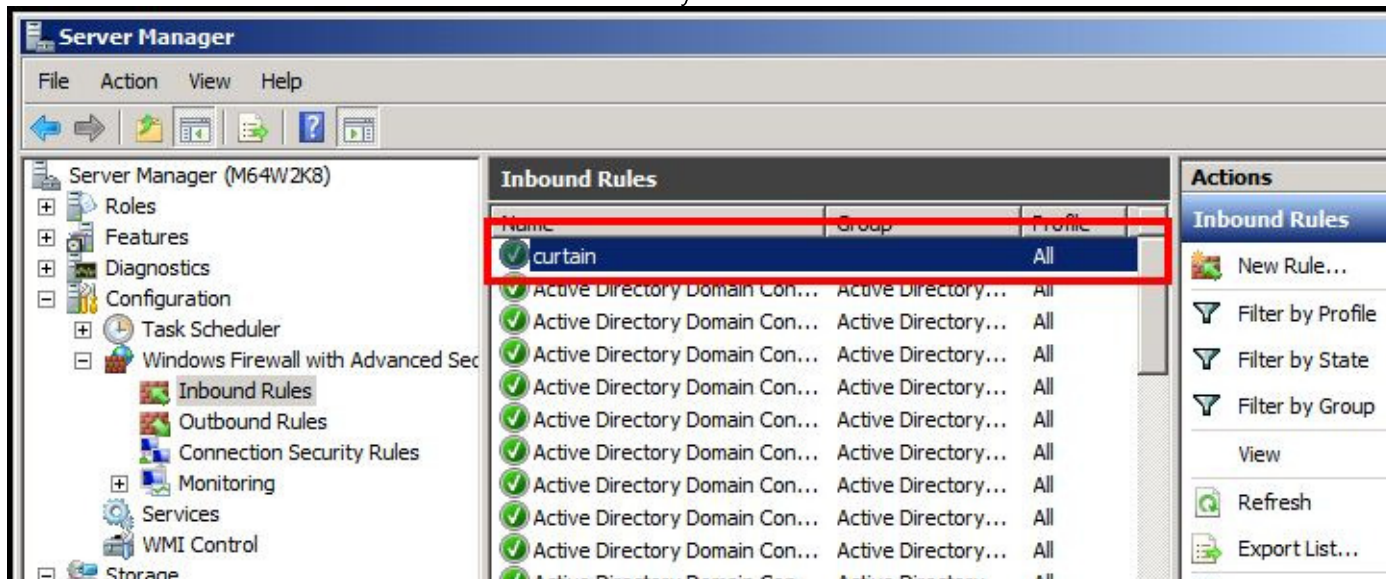




7. Enter "curtain" for the name of this rule, and click Finish.



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





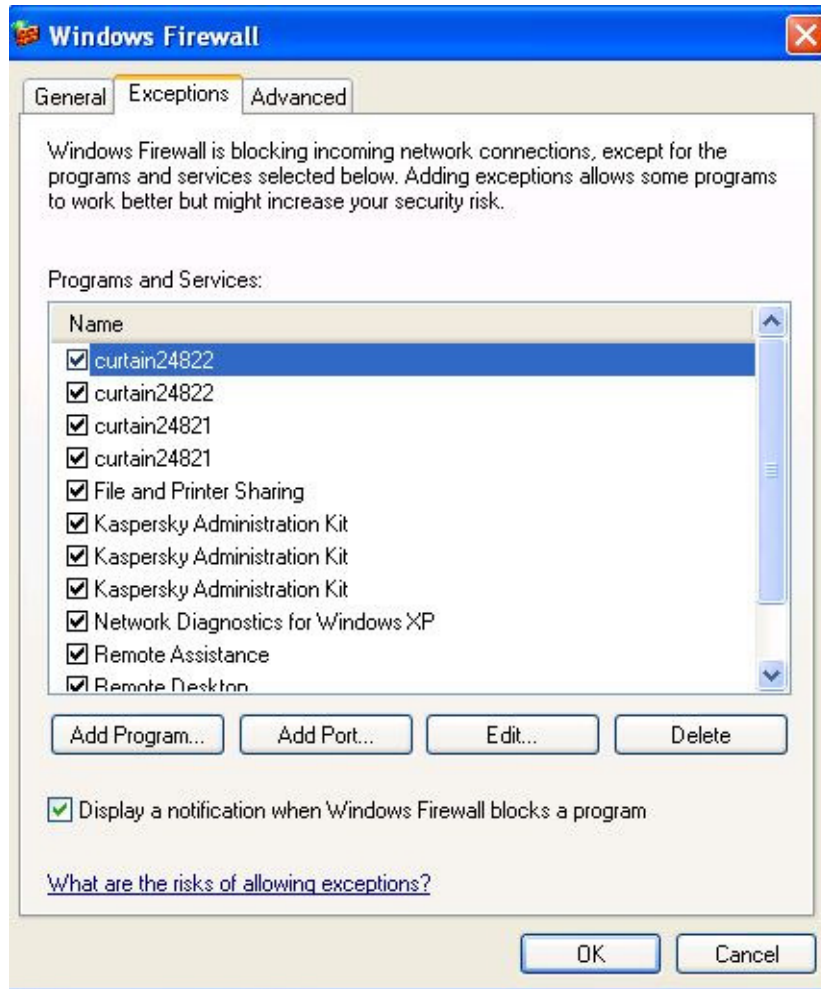
Please according to the above steps, to add 3 more rules for:

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

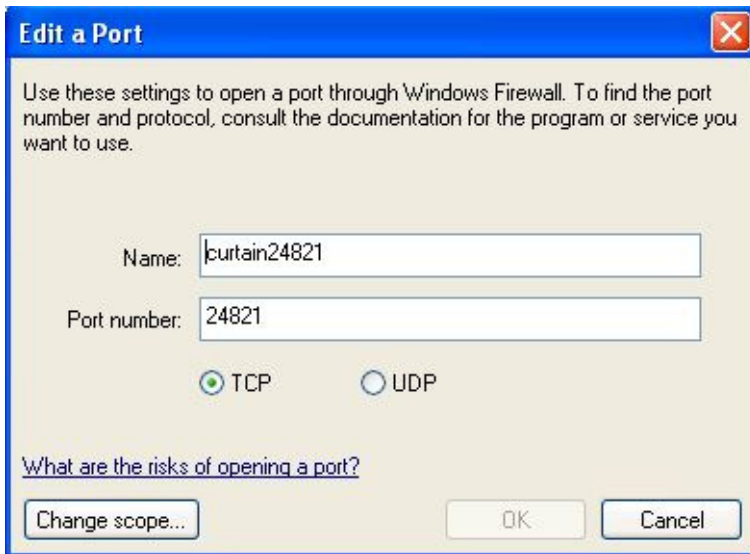
P.S. To create outbound rule, select "Outbound Rules" and right click to select "New Rule..."

[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 3 more exceptions for:

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

#### 2.4.2 - Open Port 24821 and 24822 for Curtain Client

If Windows Firewall is enabled, please open port 24821 and 24822 for Curtain Client.

For Windows 2008/2012/2016/Vista/Win 7/Win 8/Win10, please add the rules as below:

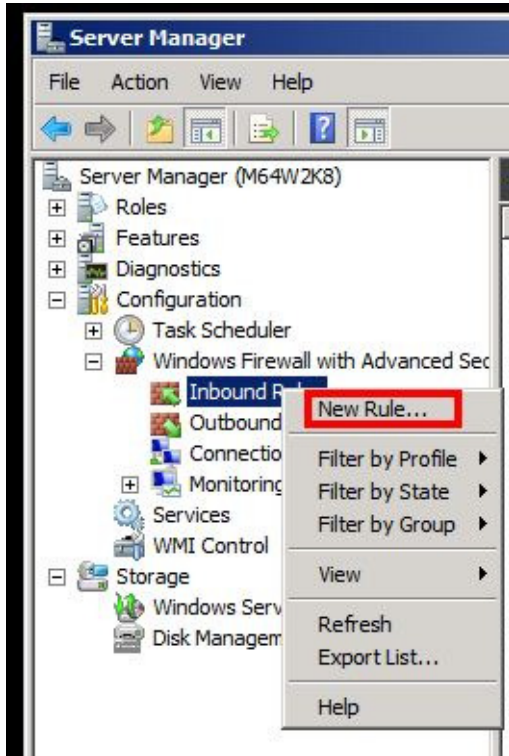
- inbound rules of 24822 port of TCP
- inbound rules of 24822 port of UDP
- outbound rules of 24821 port of TCP
- outbound rules of 24821 port of UDP

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

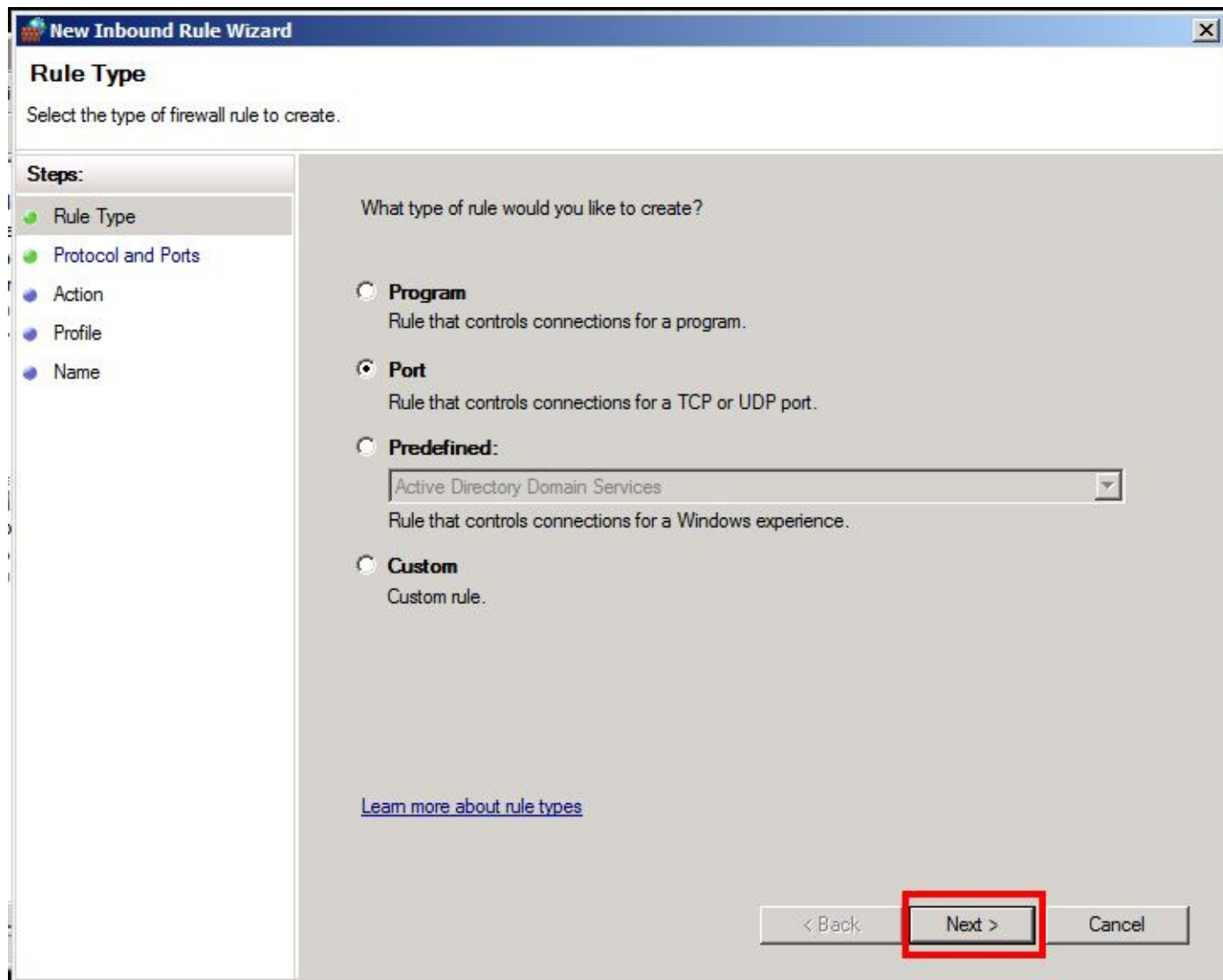
- 24821 port of TCP
- 24821 port of UDP
- 24822 port of TCP
- 24822 port of UDP

Steps to add rules for Windows 2008/2012/2016/Vista/Win 7/Win 8/Win10:

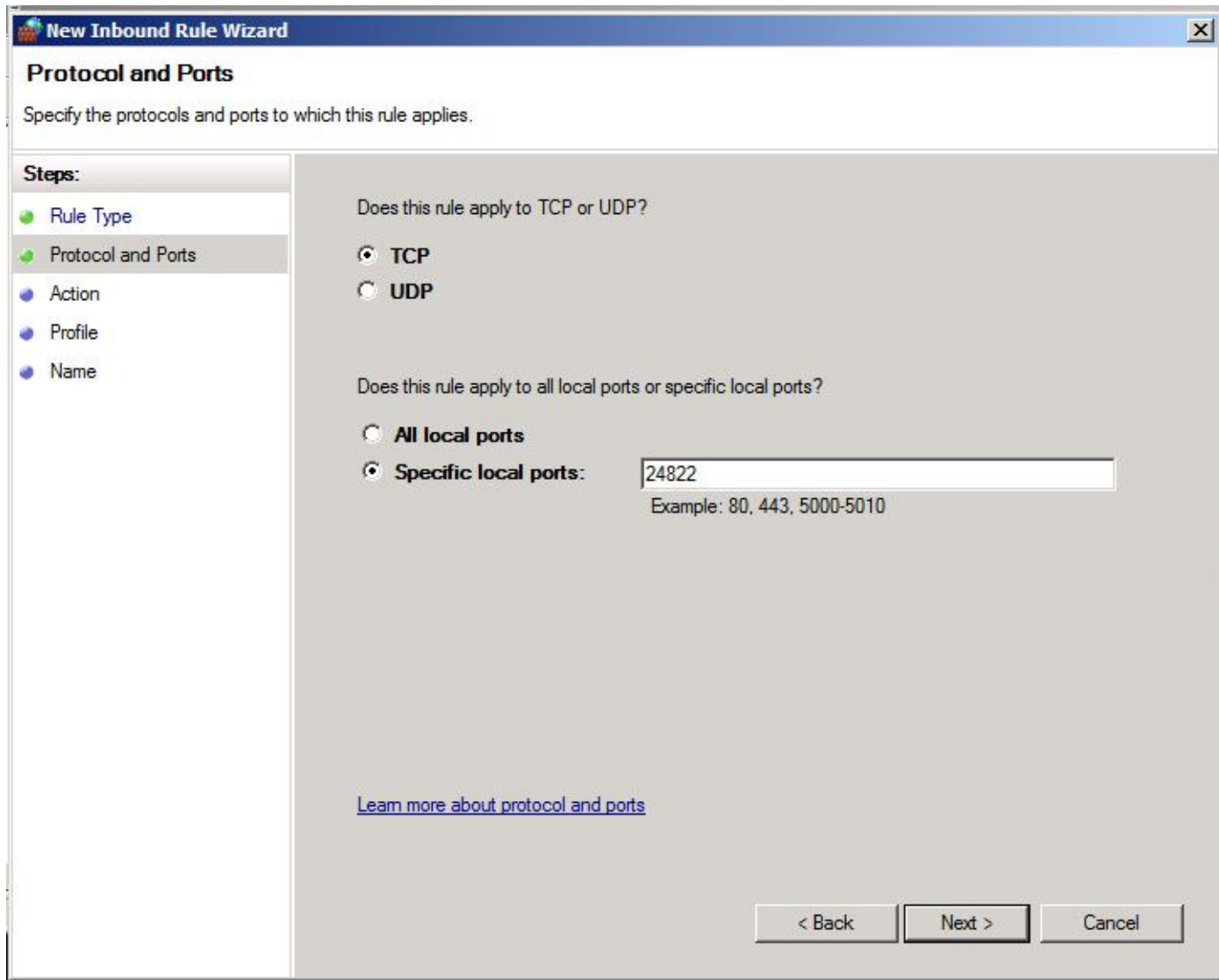
1. Select "My Computer" and right click to select "Manage"  
Then, Server Manager will be shown.
2. In Server Manager, select "Inbound Rules" as below picture and right click to select "New Rule..."



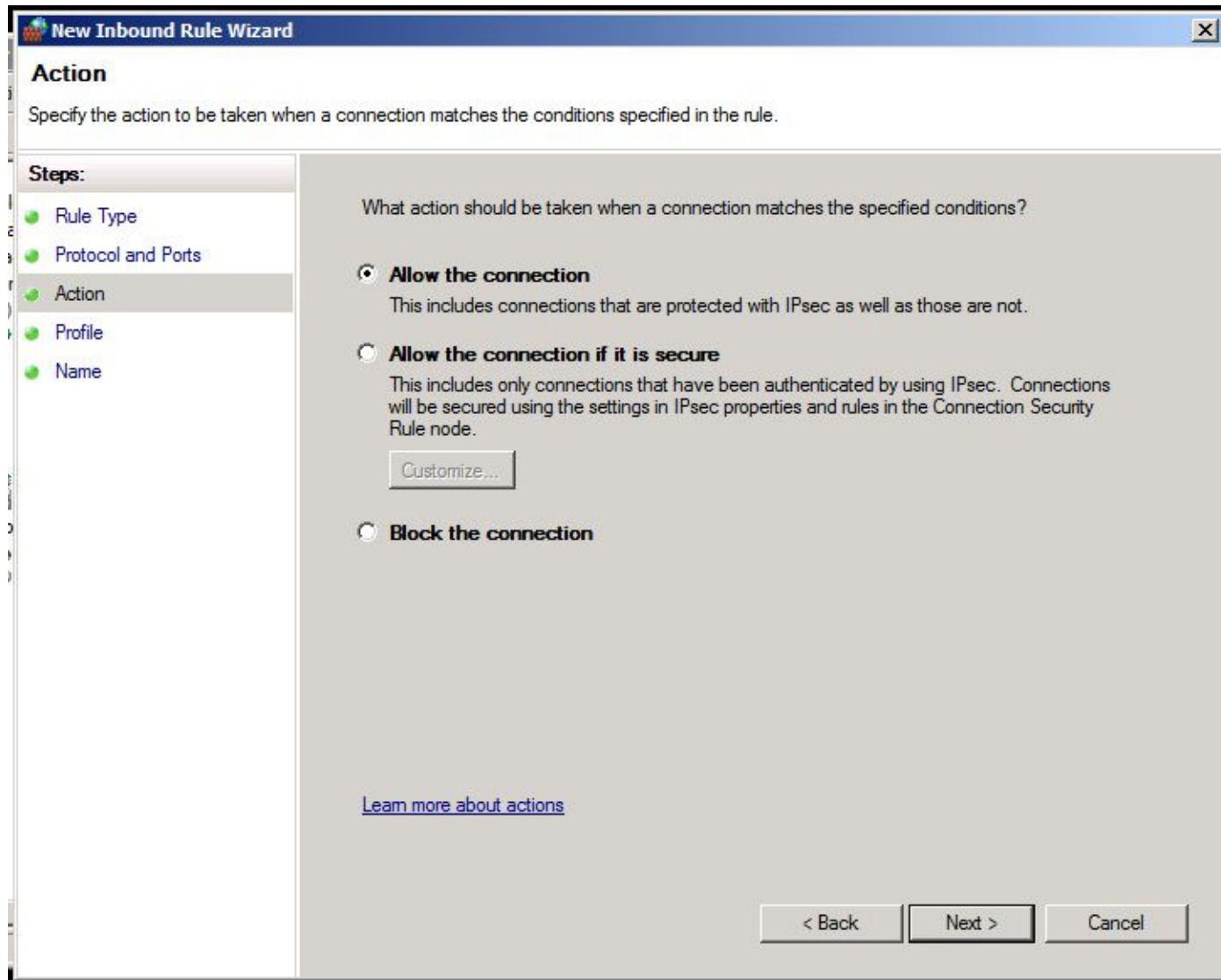
3. New Inbound Rule Wizard is shown as below, choose Port and click Next.



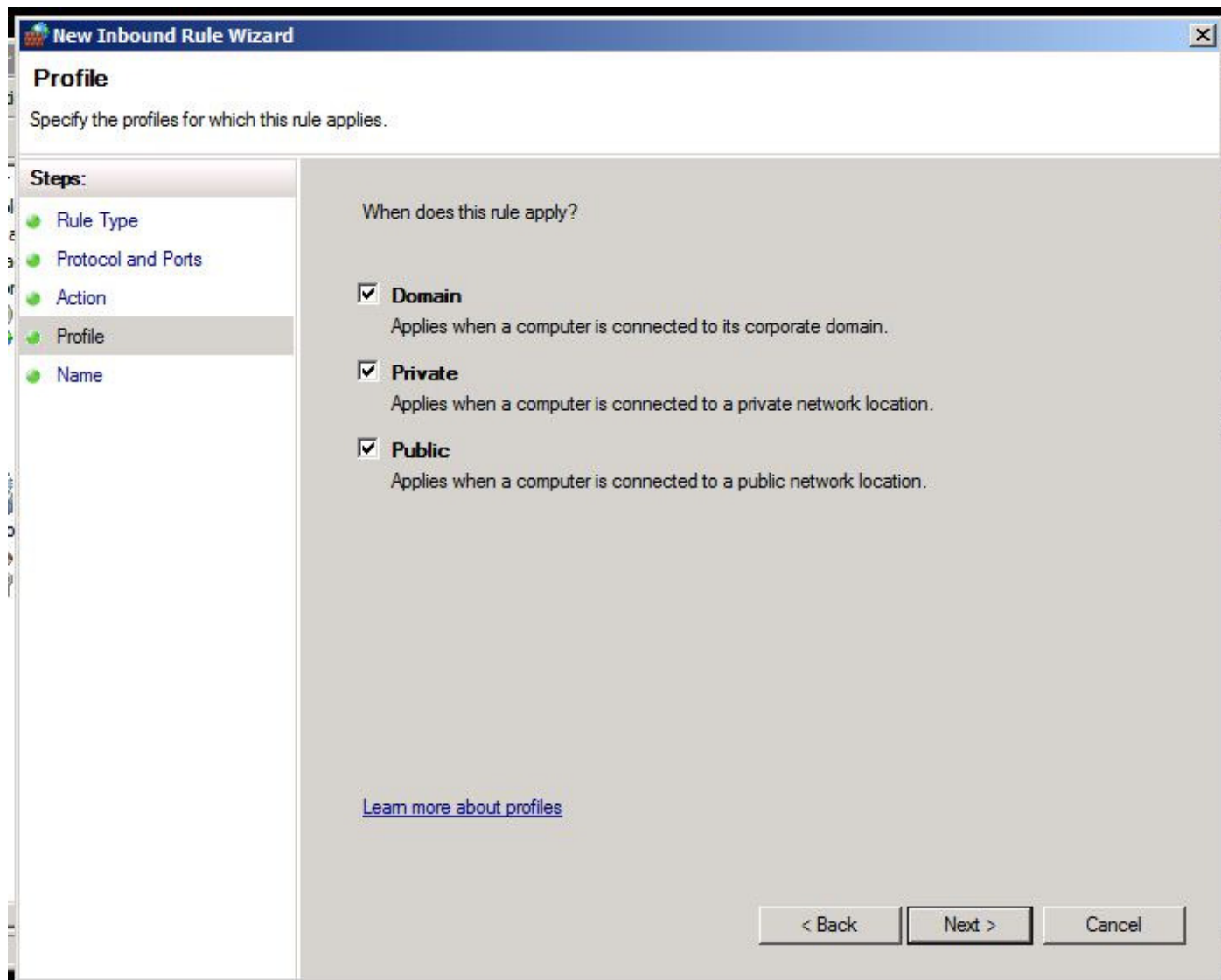
4. This rule applies to TCP and enter "24822" in Specific local ports, and click Next.



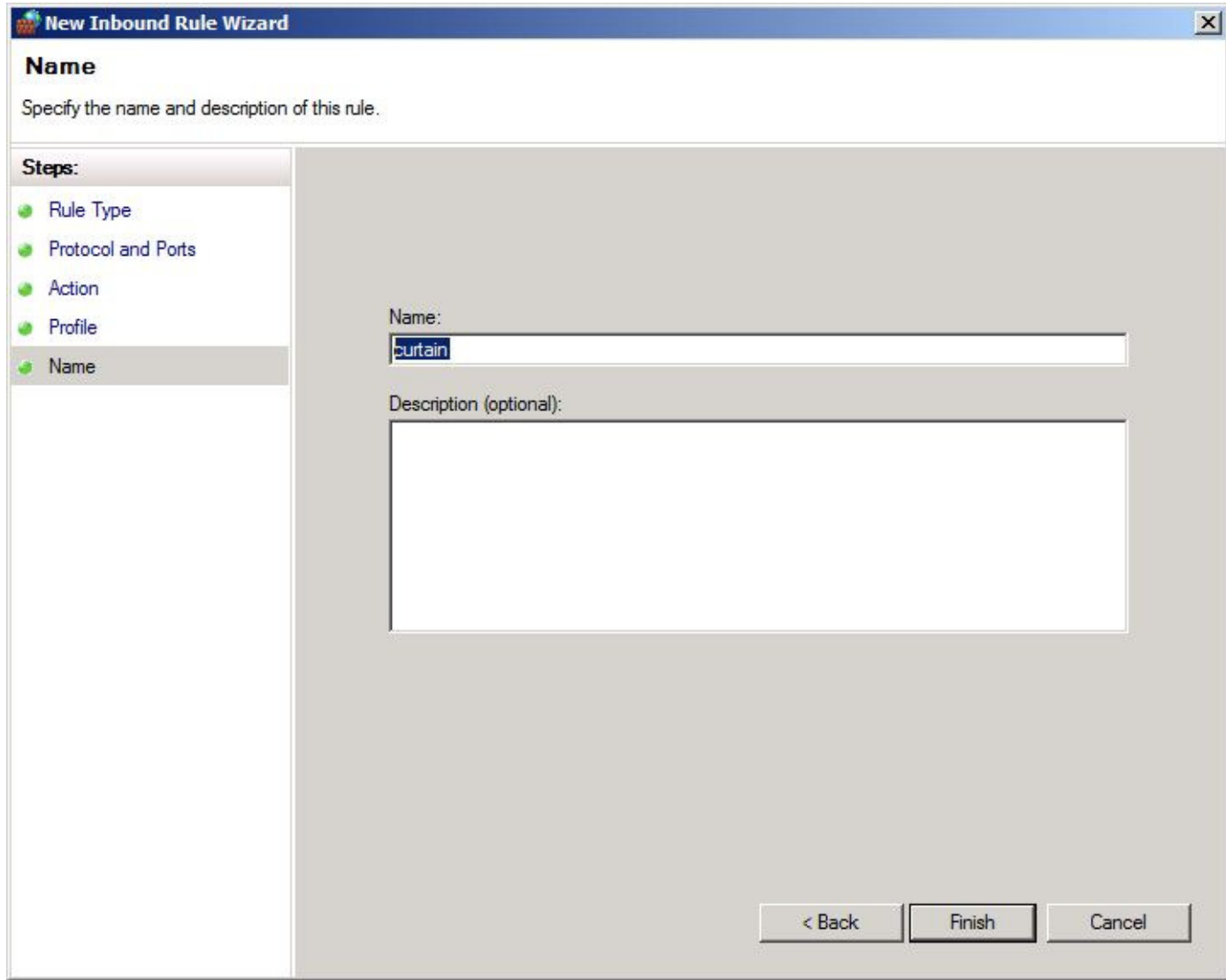
5. Select "Allow the connection", and click Next.



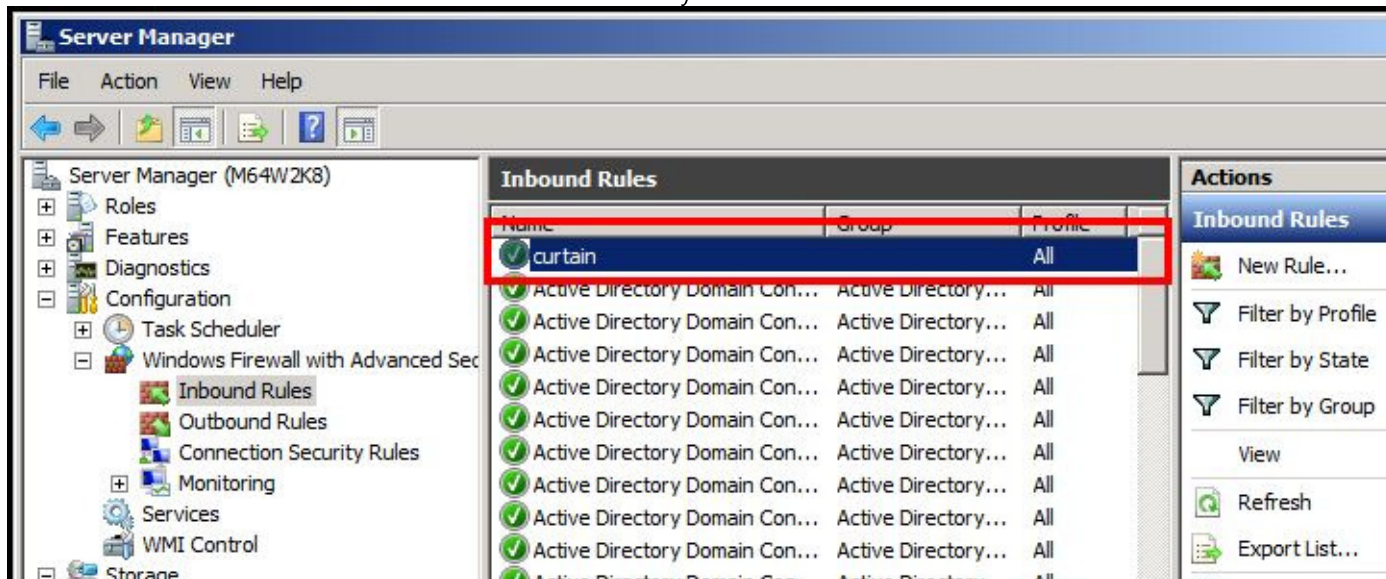
6. Check all as shown below (i.e. "Domain", "Private", and "Public") and click Next.



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 3 more rules for:

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

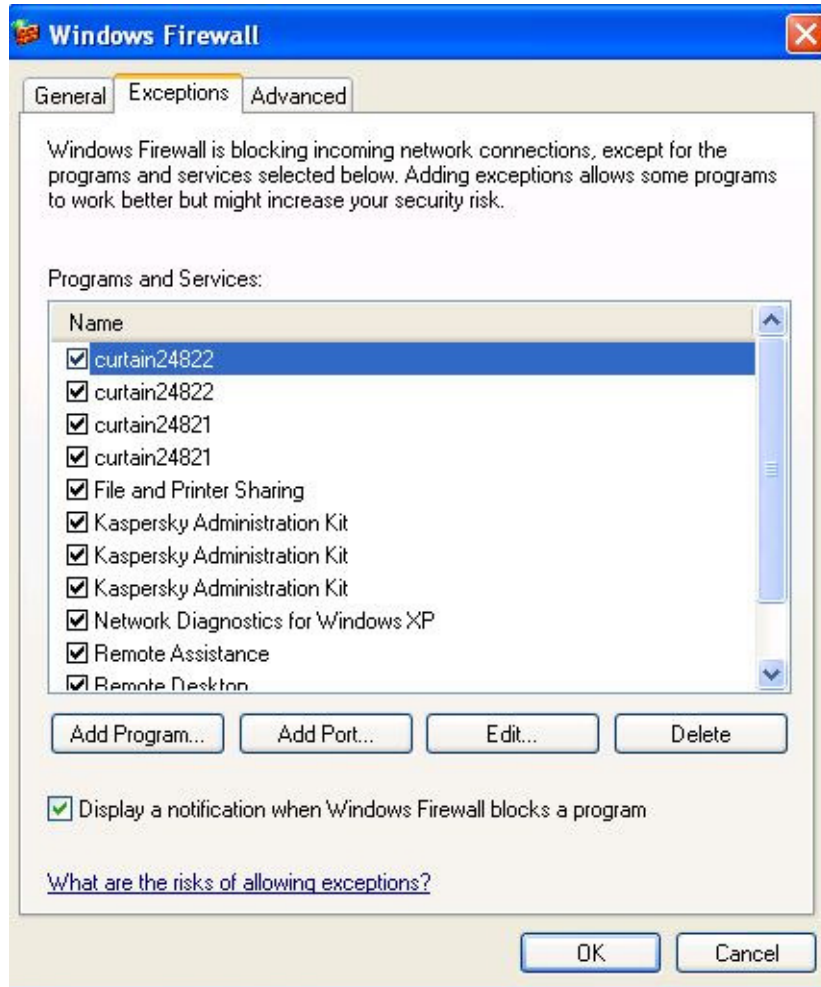
P.S.

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

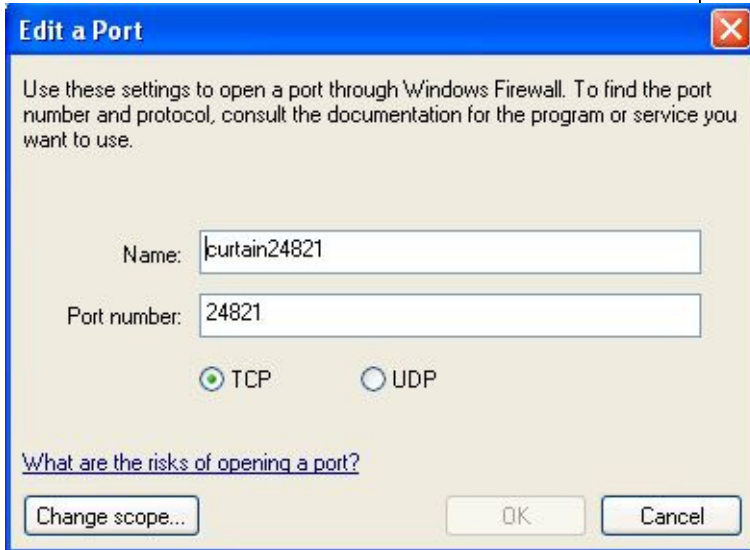
- Please be careful. The inbound rule is port 24822 for Curtain Client, while the inbound rule is port 24821 for Curtain Admin/Server Plug-in. It is easy to mix them up.

#### 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 3 more exceptions for:

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

### 2.4.3 - Check whether Tomcat Port 8005 is occupied on Curtain Server Plug-in

Tomcat will be automatically installed during installation of Curtain Plug-in Server. In order to avoid conflict of Port 8005, please check whether the port is already in use before installing Curtain Plug-in Server. If Port 8005 is already occupied, please continue to install Curtain Plug-in Server. After installation of Curtain Server Plug-in, please change Tomcat port for Curtain Plug-in Server before rebooting the server (please refer to FAQ 00193 for how to change Tomcat port).

[Steps to check the status of Port 8005:](#)

1. In Command Prompt, enter `netstat -ano|findstr "8005"`, and press Enter.

2. If port 8005 isn't occupied, it will return None. As shown below:

```

C:\Windows\system32>netstat -ano|findstr "8005"

C:\Windows\system32>

```

3. If port 8005 have been used, search results would be listed out. As shown below:

```

Administrator: Command Prompt

Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netstat -ano|findstr "8005"
TCP    127.0.0.1:8005          0.0.0.0:0              LISTENING          3956

C:\Windows\system32>tasklist|findstr "3956"
Tomcat8.exe                3956 Services           0                 40,760 K

C:\Windows\system32>

```

4. Use the listed PID to find out the application name. In Command Prompt, enter `tasklist|findstr "3956"`, and press "Enter" key (in this example, PID is 3956).
5. Modify `server.xml` file to change Tomcat Port for Curtain Plug-in Server (please refer to FAQ 00193).

#### 2.4.4 - Change Tomcat Port 8005 for Curtain Server Plug-in

If Tomcat Port 8005 is already occupied by another application, please continue to install Curtain Server Plug-in. When the installation is completed, please change Tomcat port for Curtain Server Plug-in before rebooting the server.

[Steps to modify Tomcat port 8005 for Curtain Server Plug-in:](#)

1. In Computer Management, stop "Curtain web service".
2. Go to path `C:\Program Files\Coworkshop\Curtain 3\Runtime\tomcat6.0.26\conf\.`
3. Open file "`server.xml`" by Notepad (or other text editor).
4. Locate port 8005 as shown below, change it to other available port, and then save.

```

<Server port="8005" shutdown="SHUTDOWN">
  <!--APR library loader. Documentation at /docs/apr.html -->
  <Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on"/>
  <!--Initialize Jasper prior to webapps are loaded. Documentation at /docs/jasper-howto.html -->
  <Listener className="org.apache.catalina.core.JasperListener"/>
  <!-- Prevent memory leaks due to use of particular java/javax APIs-->
  <Listener className="org.apache.catalina.core.JreMemoryLeakPreventionListener"/>
  <!-- JMX Support for the Tomcat server. Documentation at /docs/non-existent.html -->
  <Listener className="org.apache.catalina.mbeans.ServerLifecycleListener"/>
  <Listener className="org.apache.catalina.mbeans.GlobalResourcesLifecycleListener"/>
  <!-- Global JNDI resources
  Documentation at /docs/jndi-resources-howto.html
  -->

```

5. In Computer Management, start "Curtain web service" (rebooting the server is needed after installation of Curtain Server Plug-in).
6. Done.

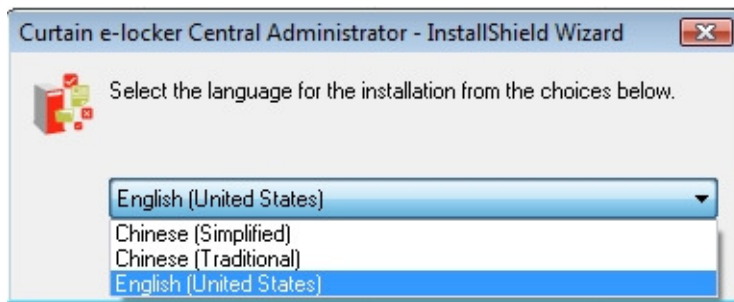
## 3 - Installation

### 3.1 - Install Curtain Admin

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

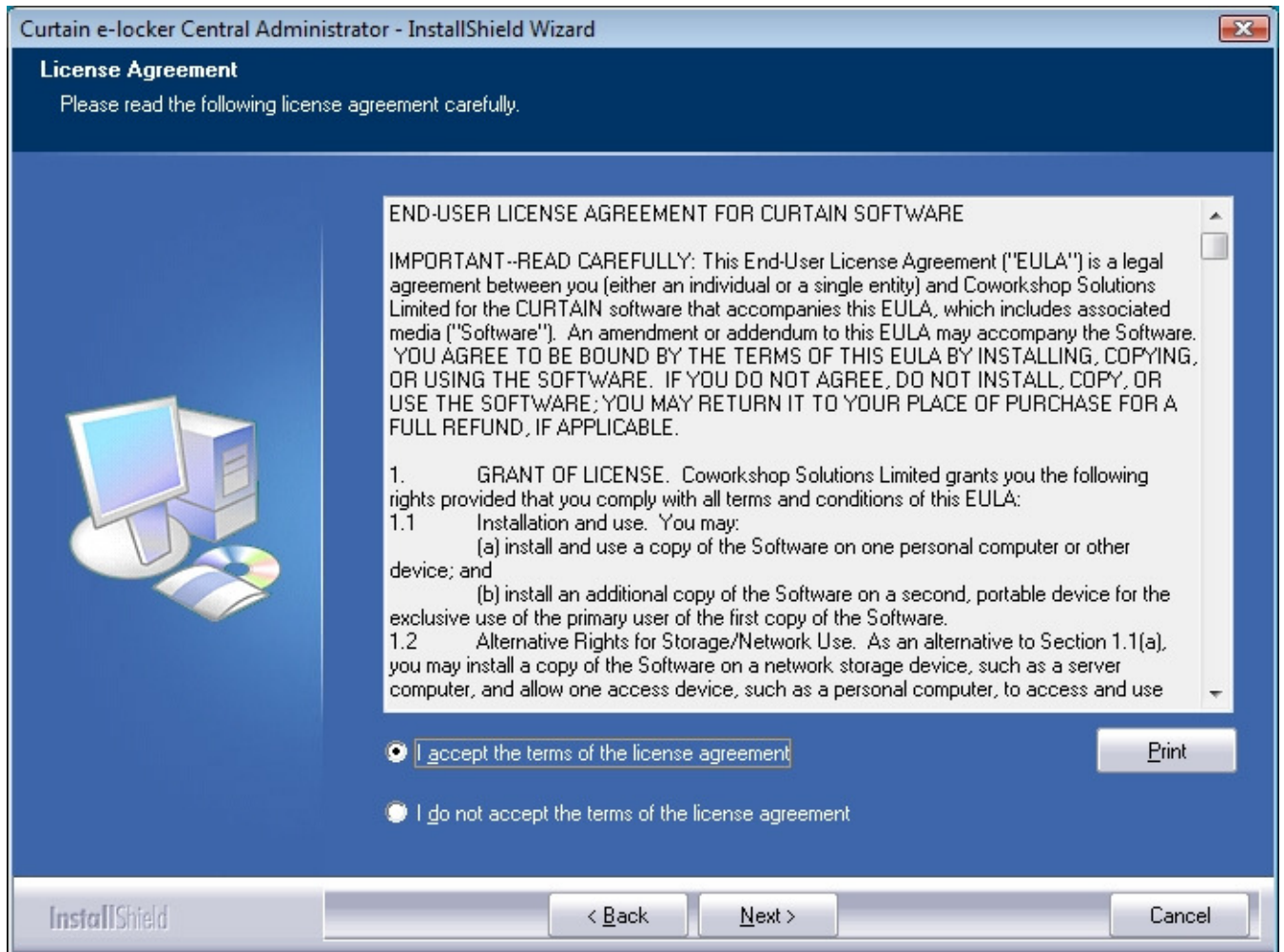
#### Steps to install Curtain Admin:

1. Copy appropriate Curtain server setup package (e.g. CurtainAdmin\_Win32(327304).zip or CurtainAdmin\_X64(327304).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.

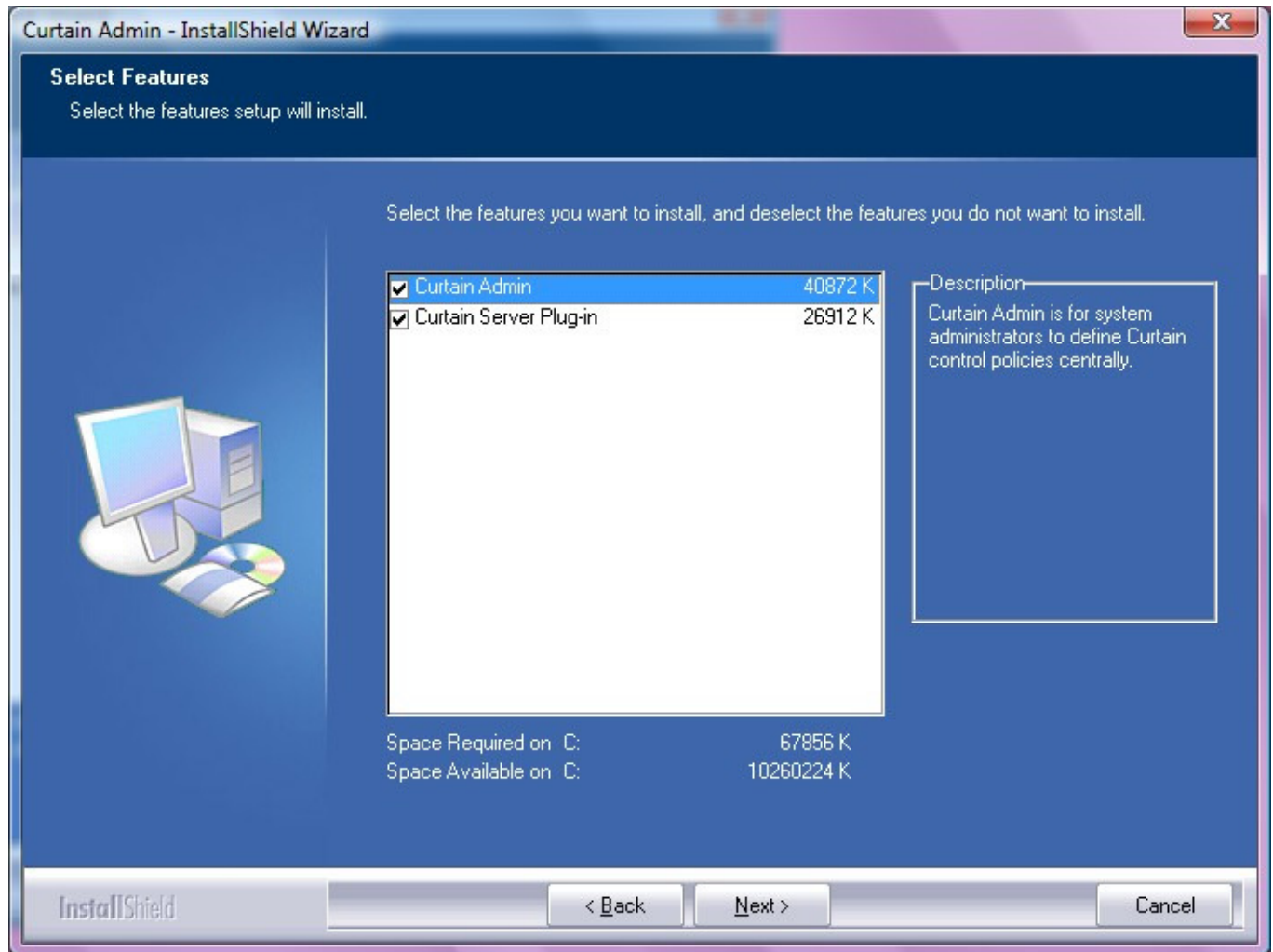


4. Select a language and click OK.

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. There are two scenarios:

(a) If you only want to install Curtain Admin on this server,  
- only select "Curtain Admin"

(b) If you also want to protect resources on this server (e.g. Protected Share Folder, Protected website, etc),  
- select "Curtain Admin" to install Curtain Admin, and  
- select "Curtain Server Plug-in" to install Curtain Server Plug-in.  
Click Next to continue.

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

8. Click Install to start the installation.

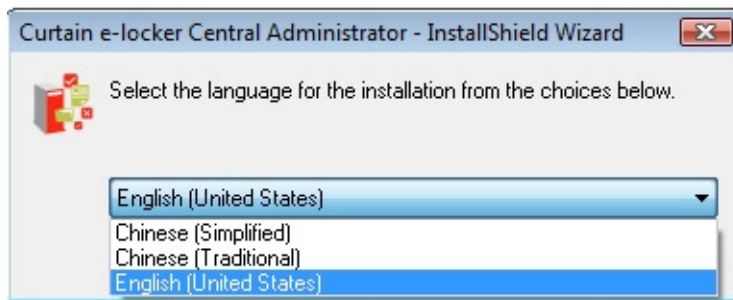
9. If you have installed Curtain Server Plug-in on this server, reboot the server after the installation.

## 3.2 - Install Curtain Server Plug-in

If you want to protect resources on a server (e.g. Protected Share Folder, Protected website, etc), you should install Curtain Server Plug-in on that server. Here are the steps.

### Steps to install Curtain Server Plug-in:

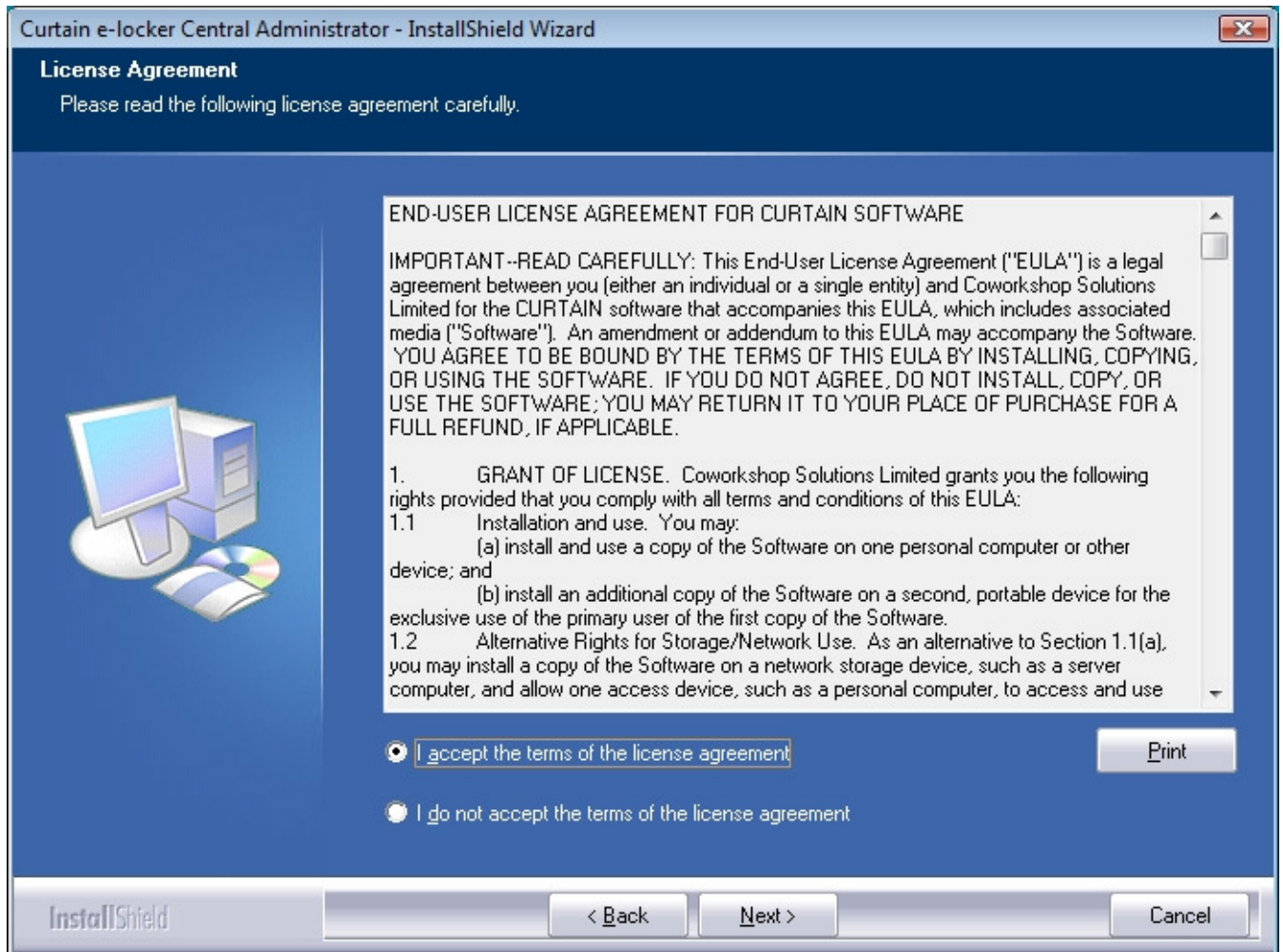
1. Copy appropriate Curtain server setup package (e.g. CurtainAdmin\_Win32(327304).zip or CurtainAdmin\_X64(327304).zip) to local hard-disk of the server.
2. Unzip the setup package.
3. Run Curtain server setup program. Make sure that you login Windows with administrator right. Then, you will be asked to select Language for the installation.



4. Select a language and click OK.

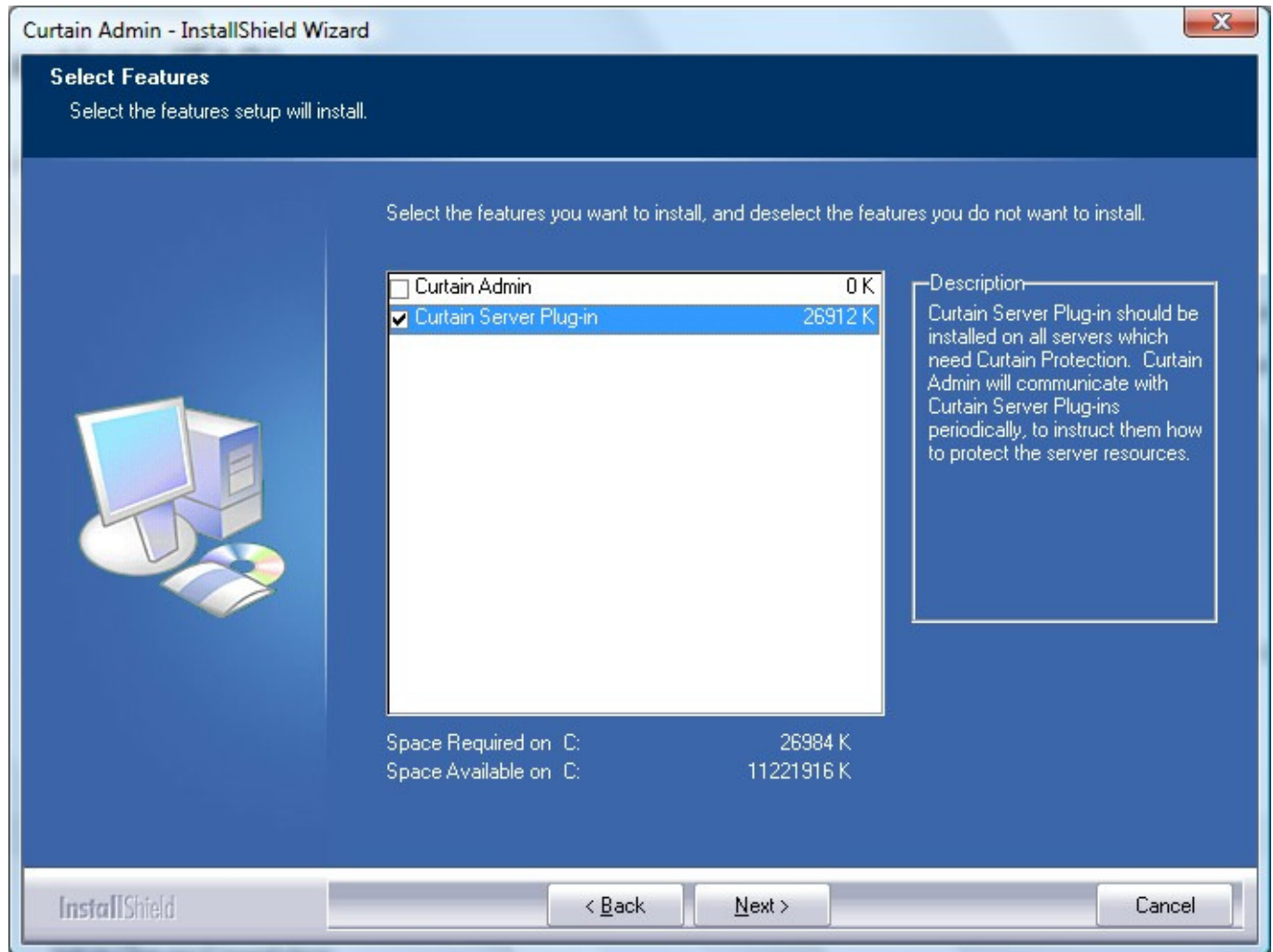


5. Read License Agreement. If you accept the agreement, select "I accept the terms of the license agreement" and click Next to continue.





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



6. ONLY Select "Curtain Server Plug-in", 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 server after the installation.

### 3.3 - Install Curtain Client

If a user needs to access Protected server resources (e.g. Protected Share Folder, Protected website, etc), you should install Curtain Client on the user's workstation. Here are the steps.

#### [Steps to install Curtain Client](#)

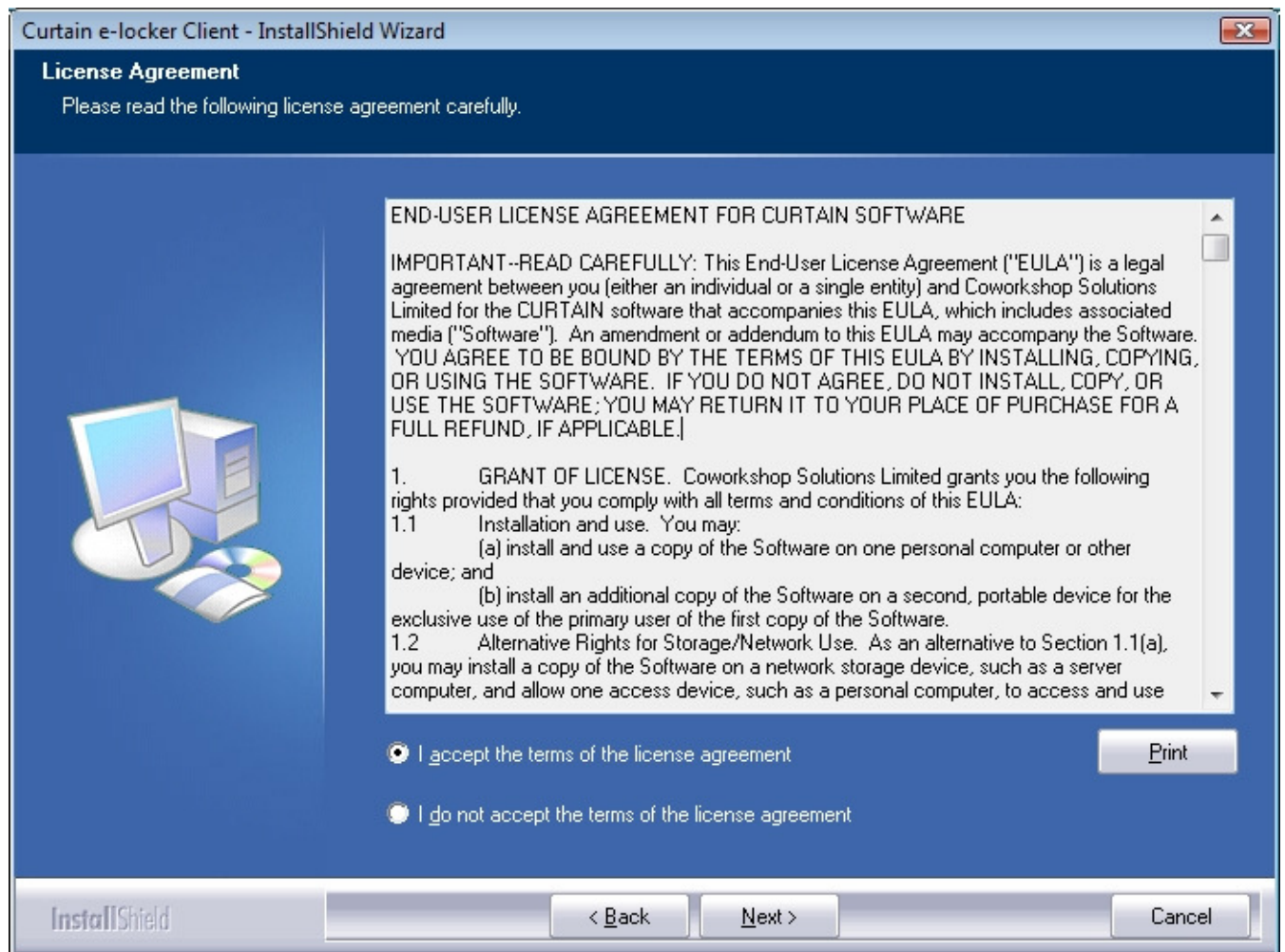
1. Copy appropriate Curtain client setup package (e.g. CurtainClient\_Win32(327304).zip or CurtainClient\_X64(327304).zip) to local hard-disk of user's workstation.
2. Unzip the setup package.

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

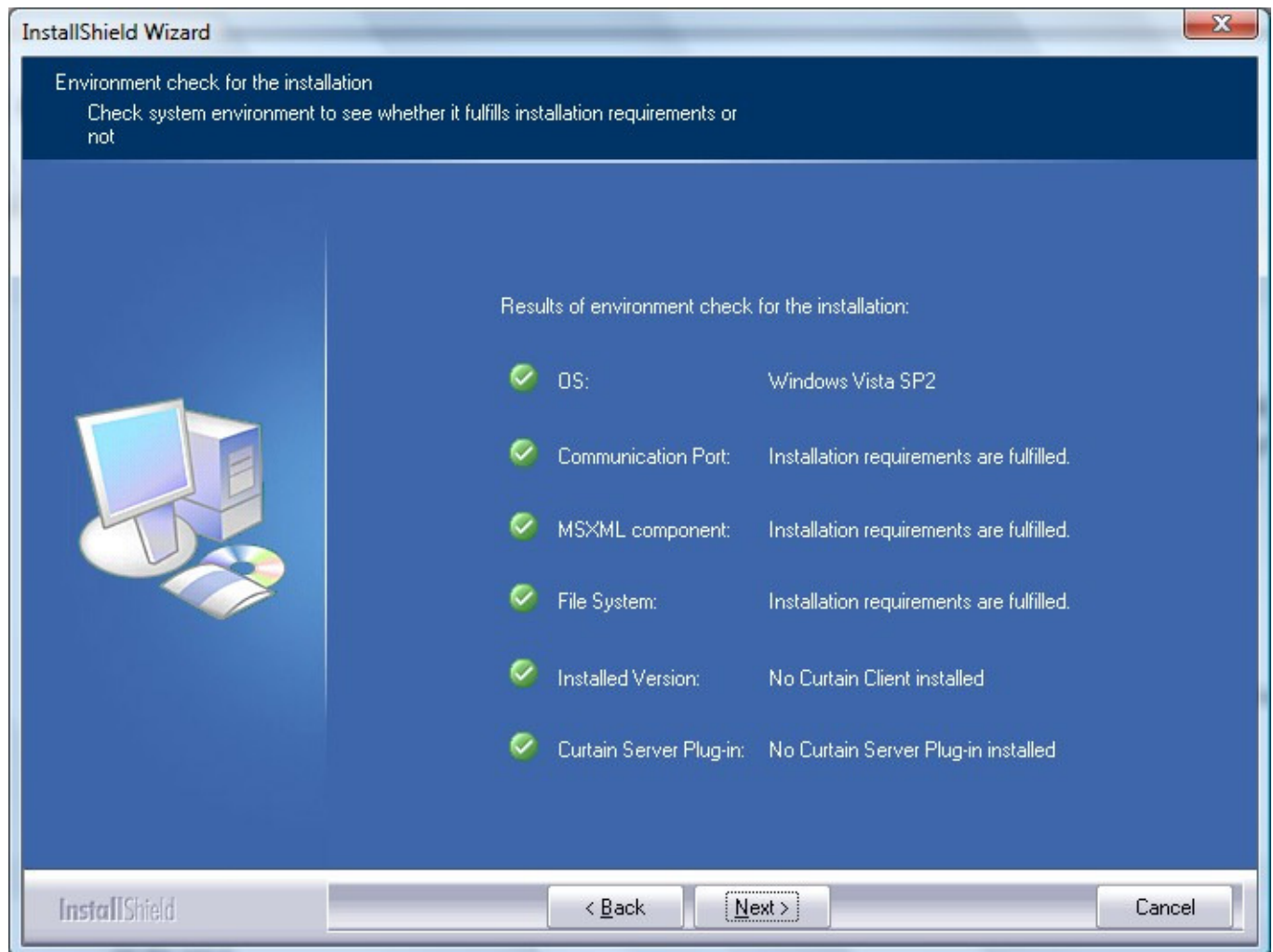


4. Select a language and click OK.

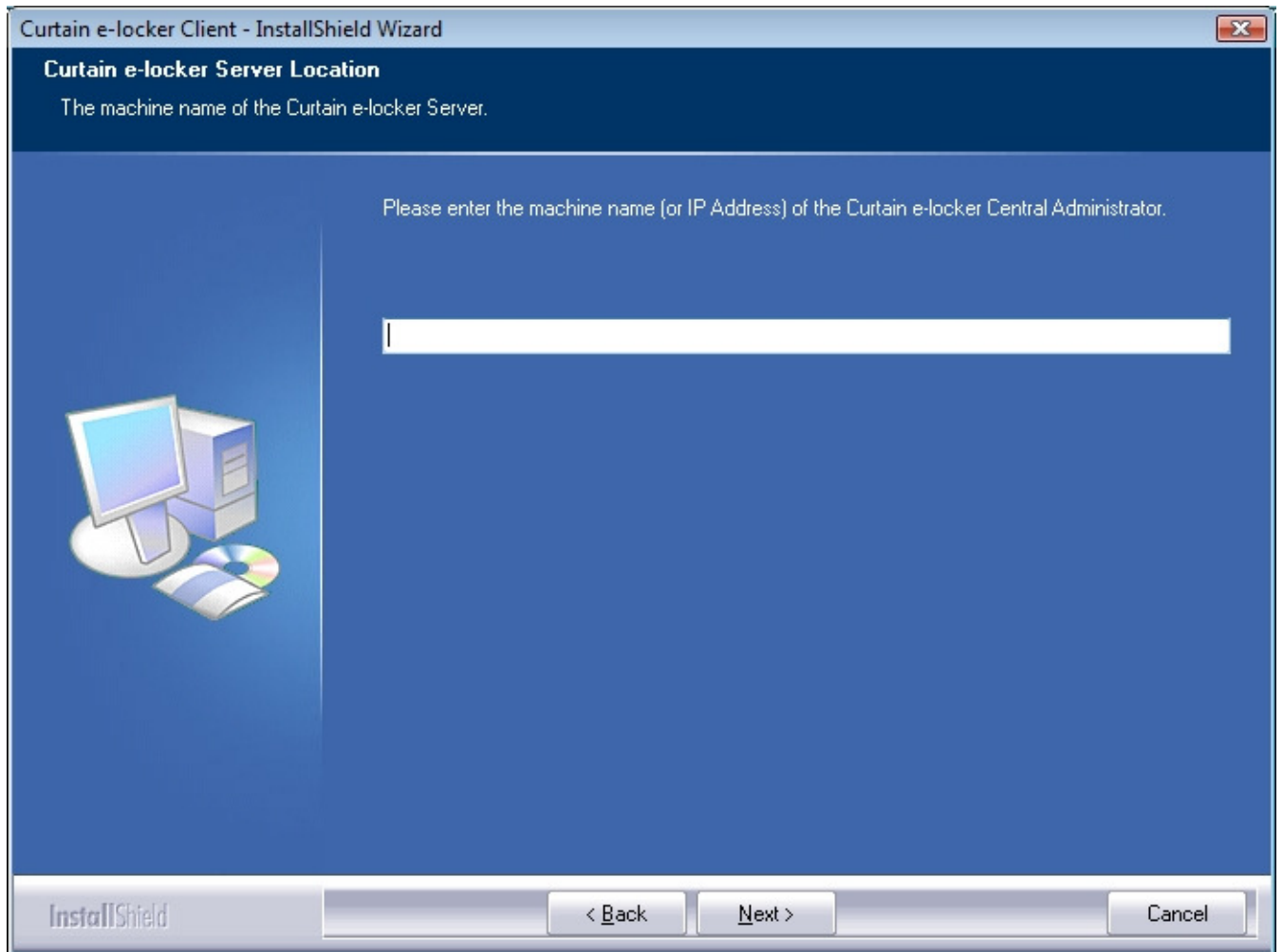
5. Read License Agreement. If you accept the agreement, select "I accept the terms of the license agreement" and click Next to continue.



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



6. Enter hostname or IP Address of Curtain 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 Client.

P.S. If you want to use Group Policy to remotely install Curtain Client, please refer to FAQ 00201.

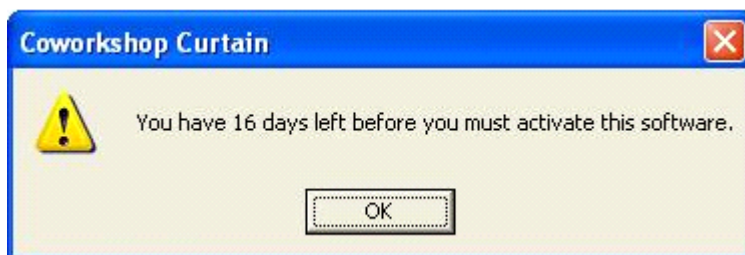
## 4 - Product Activation

### 4.1 - Product Activation

Curtain e-locker has applied Product Activation technology to control license of the software. Without product activation, companies can use Curtain e-locker for 30 days. They can try and play with the software for evaluation purpose. If companies want to extend the evaluation period, they should contact Coworkshop or its authorized resellers for the arrangement.

For Curtain e-locker existing customers, product activation should be done at initial setup. And, the software has to be reactivated every year, for the purpose of license control. Coworkshop will assist customers to reactivate the software free-of-charge, even the customers do not join the software annual maintenance. For the procedures of Product Activation, please refer to related documents.

When activation is needed, the software will prompt users to remind them every time when Curtain Client or Curtain Admin is launched. Here is the Reminding Message.



The software will start to prompt users for the activation 30 days before the expiration date. If the software is not reactivated before the date, users cannot launch Curtain Client and Curtain Admin until activation is done.

P.S. Administrators only need to do the product activation in Curtain Admin. Once Curtain Admin is successfully activated, all Curtain Clients will be activated automatically.

### 4.2 - Activate Curtain e-locker

When product activation is needed, Curtain e-locker will prompt users every time when Curtain Client or Curtain Admin is launched. Please follow steps below to activate the software.

[Steps to activate Curtain e-locker:](#)

1. In Curtain Policy Server, launch Curtain Admin. Then, you will be asked to do the activation.



2. 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 4 to continue.

**Enter Product Key**

Product Key  
Please enter the Product Key of your copy of Curtain 3.0.

Registration Information

User Name:

Organization:

OK Cancel

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

**Curtain e-locker Product Activation**

Product Activation

Step 1: Click "Generate Request..." to create the "Activation Request File".  
Send the file to Coworkshop Solutions Limited

Step 2: When you receive the Confirmation file,  
click "Import Confirm File..." to complete the activation process.

Step 1

Step 2

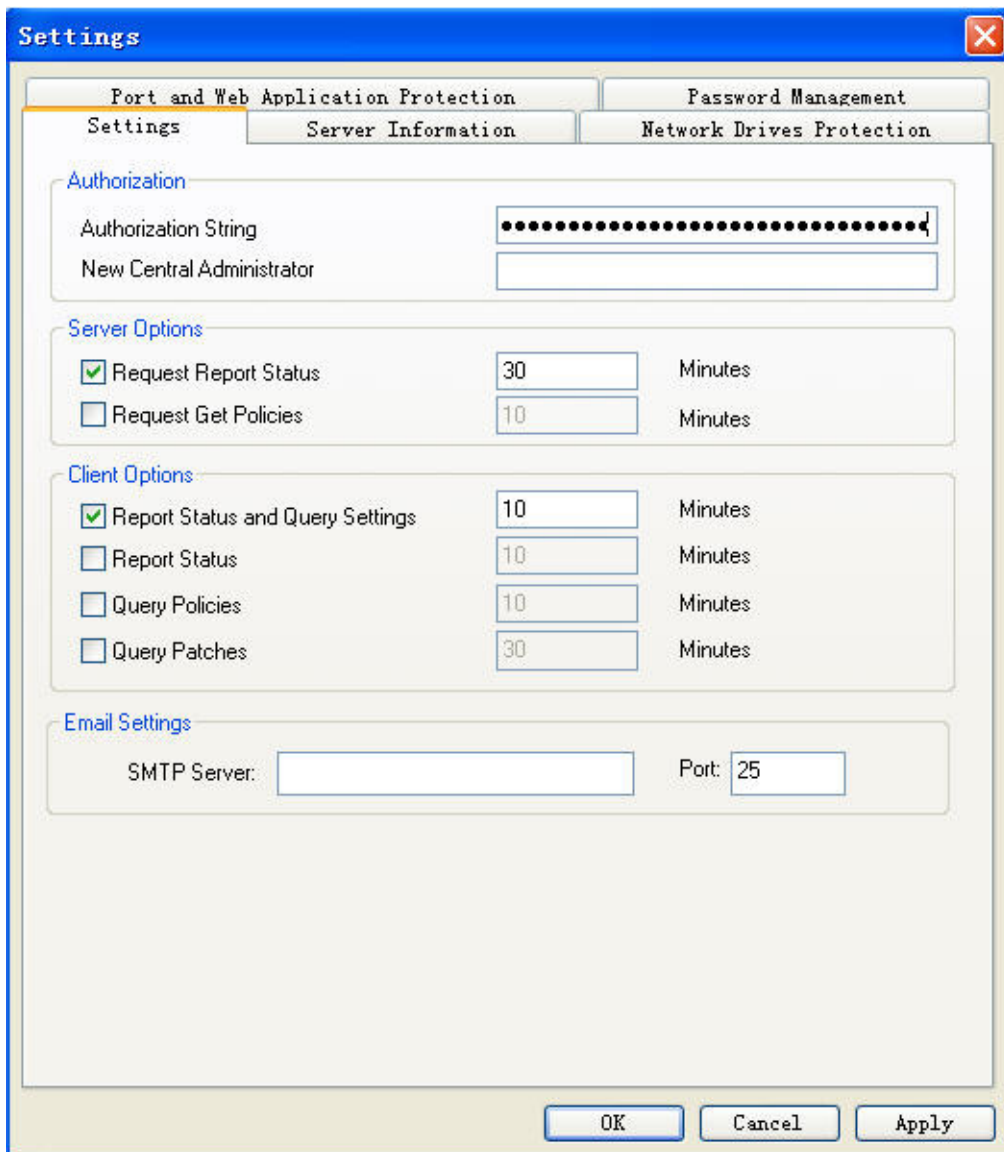
4. Click "Generate Request file..." button to generate Activation Request File, and send this file to Coworkshop (registration@coworkshop.com). After receiving your activation request, Coworkshop will send file(s) back to you.
  - If it is the first time Product Activation, you will receive two files from Coworkshop (i.e. Confirmation Code and Authorization String).
  - If it is the Annual Product Reactivation, you will receive one file from Coworkshop (i.e. Confirmation Code).

5. 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.



- If it is the first time Product Activation, please go to next step to continue.
- If it is the Annual Product Reactivation, you have completed the process of Reactivation.

6. In Curtain Admin, select "File > Settings" in the menu. Then, "Settings" window will be shown. Enter Authorization String and Click OK.

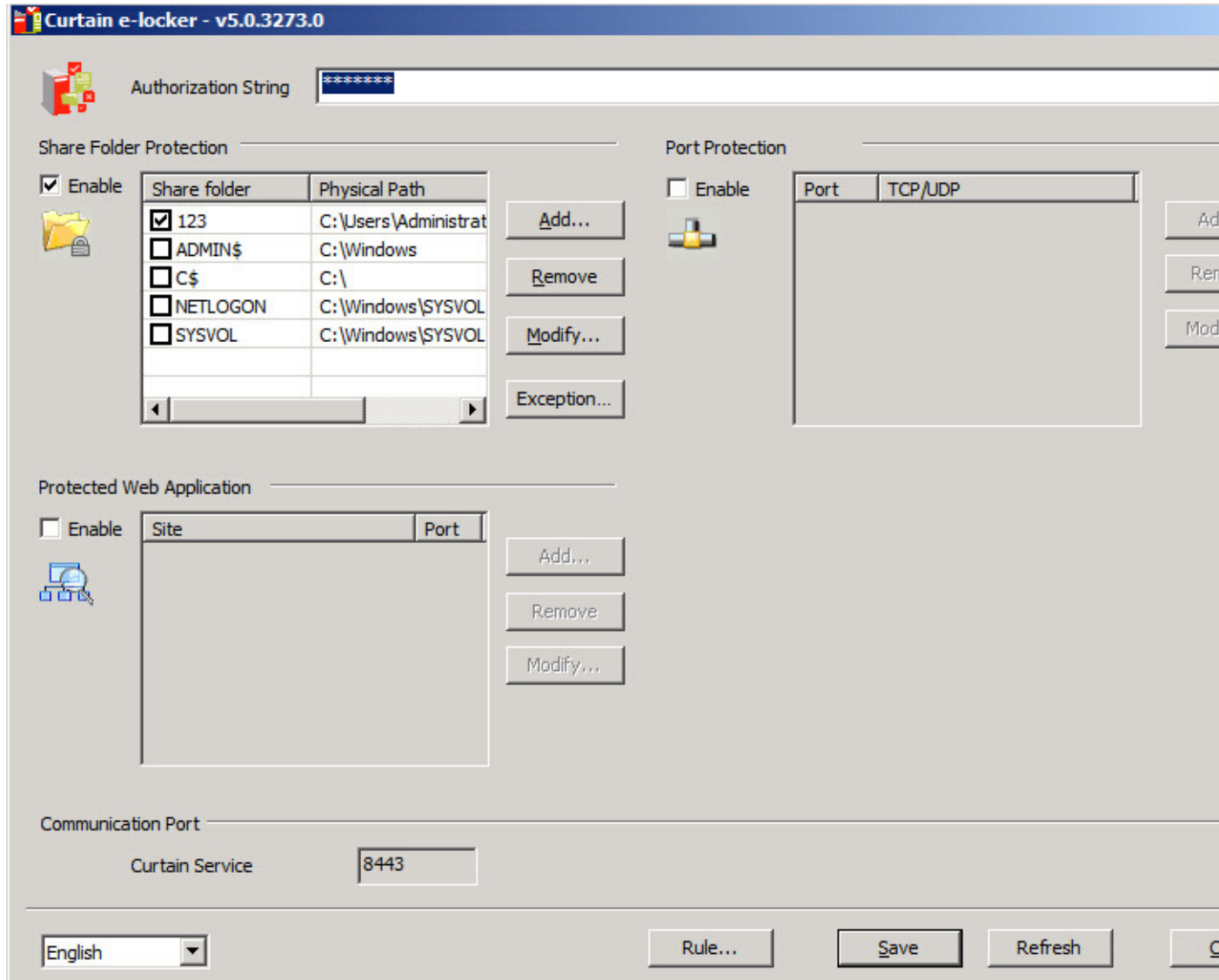


If you have installed Curtain Server Plug-in alone on other servers for protecting server's resource, please follow Step 7-10 to enter the Authorization String to Curtain Server Plug-in manually.



7. Open Curtain Server Plug-in by selecting "Start > Programs > Coworkshop Curtain e-locker > Secure Network Manager"

Then, the interface of Curtain Server Plug-in will be shown.



8. Enter Authorization String and Click "Save" button.

9. Click "Refresh" button to apply the changes.

10. Click "Close" button to quit.

Congratulations! Curtain e-locker has been activated successfully.



## 5 - Configurations

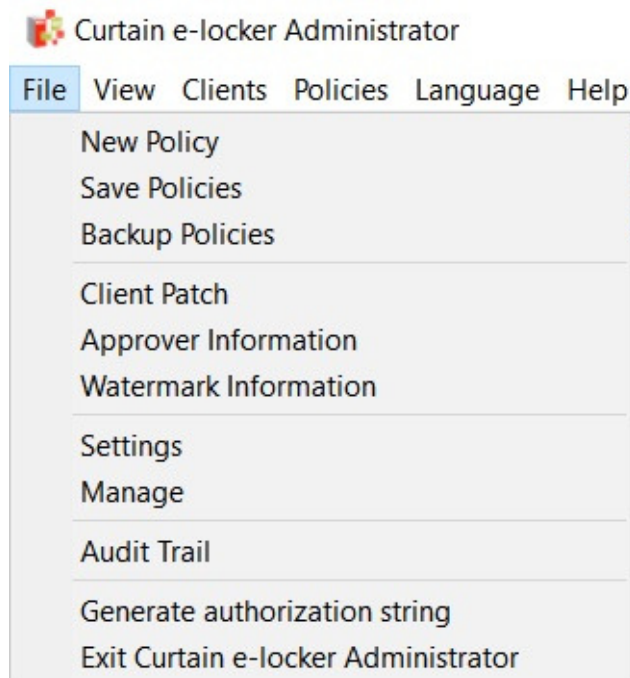
### 5.1 - Create Control Policy Group

Administrators can create many Control Policy Groups in Curtain Admin for different workstations/users. We recommend to use Default Policy for protecting the most of workstations/users. Here is an example of Control Policy Groups for reference.

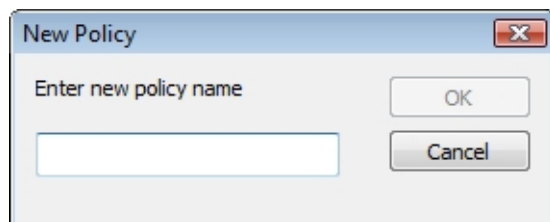
- Default Policy: for general users, disallow printing and saving protected document out of protected zone
- Managers: for senior management, allow printing and saving protected document out of protected zone
- Notebooks: for notebooks, disallow printing and saving protected document out of protected zone. Also the workstation must be online (connecting with Curtain Admin) every 72 hours in order to access files in local protected directory.

#### Steps to create Control Policy Group:

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



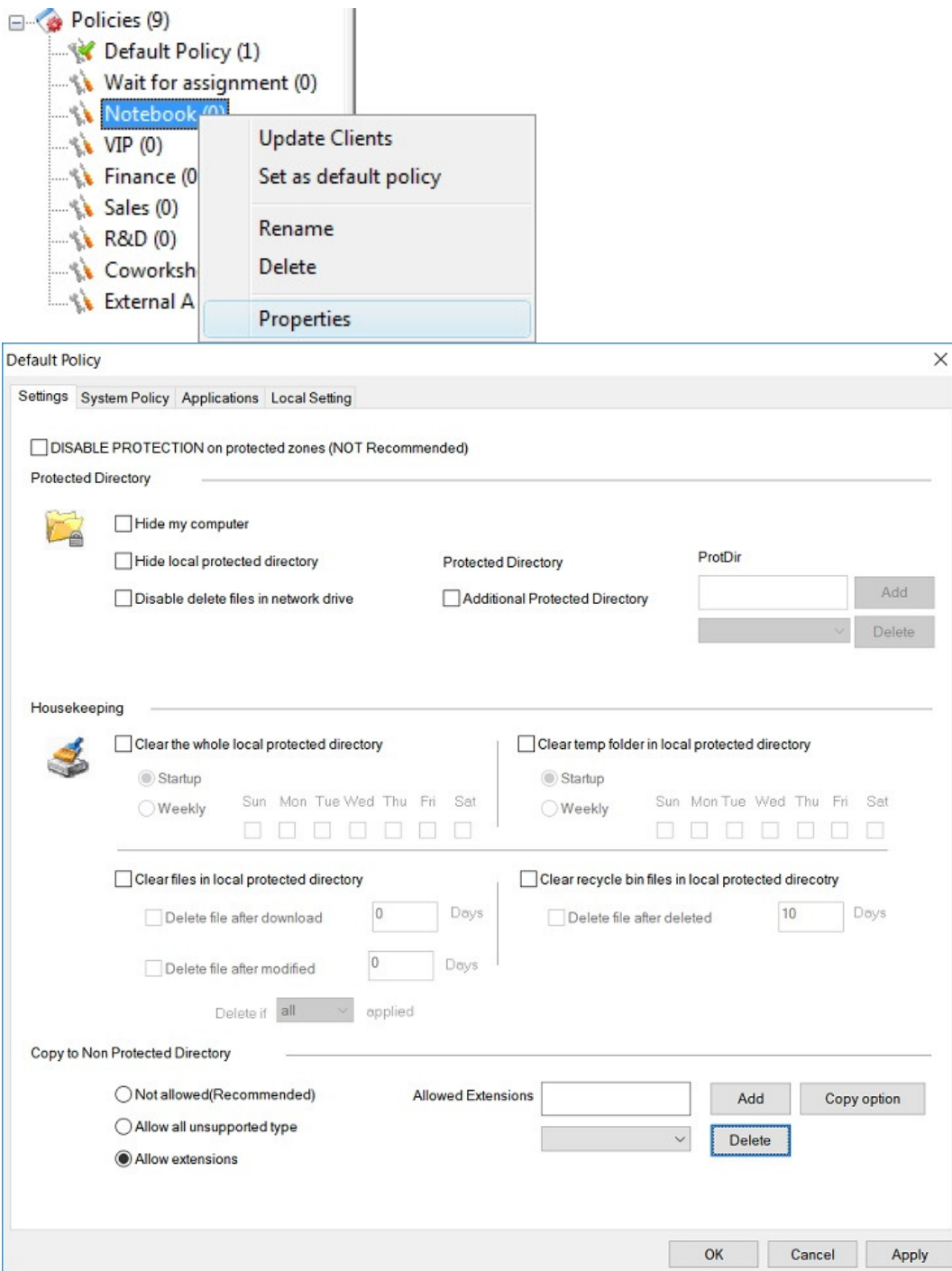
2. Enter new Policy Name and click OK to confirm.



## 5.2 - Configure Control Policy Group

Steps to configure Control Policy Group:

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



Here is a summary of settings in a Policy Group.

Settings tab

- DISABLE PROTECTION on protected zone
- Additional local protected directory
- Housekeeping of local protected directory
- "Copy out" policy by file extension
- "Encrypt out" policy

System Policy tab

- Online/offline control

Applications tab

- Control the behaviors when using protected documents in Application (e.g. disallow printing and saving protected document out of protected zone)

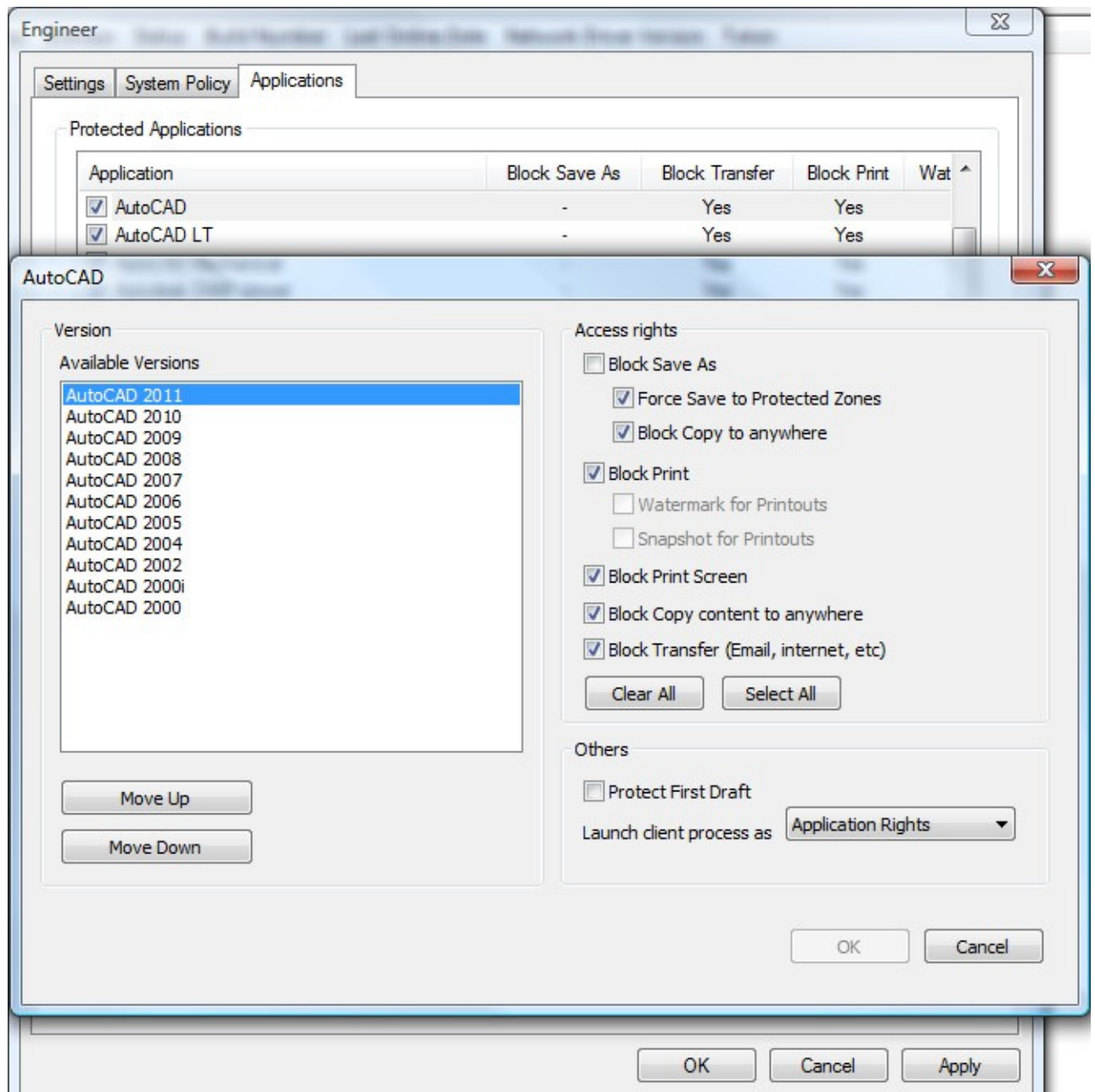
Local Settings tab

- Specify Approver(s) who is authorized to approve Send Request for this policy group
- Specify Printer(s) which is included for this policy group

We focus on Application tab here. For other settings, please refer to Chapter 6.

2. In Applications tab, double-click the application which you want to configure.

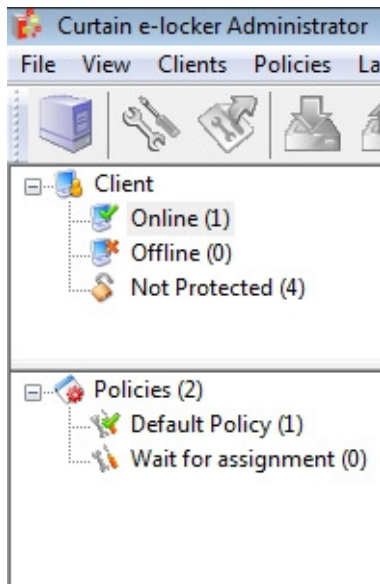
3. Define Curtain access rights and click OK to confirm.



4. Repeat Step 2-3 for different applications.

### 5.3 - Set Default Policy

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



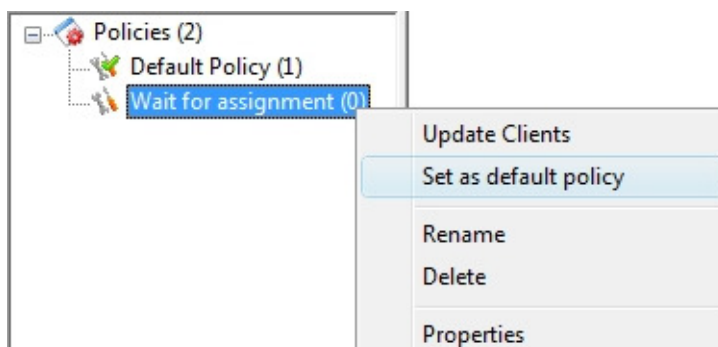
There are two built-in Control Policy Groups.

- Default Policy: With pre-defined settings of this Policy Group, users can work with sensitive documents in Protected Zone. But they cannot take the information out of the Zone.
- Wait for Assignment: With pre-defined settings of this Policy Group, users cannot read or edit sensitive documents in Protected Zone.

When Curtain Clients have been installed in users' workstations, they will connect to Curtain Admin and apply default policy. If administrators want to verify new Curtain Clients before allowing them to read/edit sensitive documents in Protected Zone, administrators could set "Wait for Assignment" to default policy. After verifying a new Curtain Client, administrators can move the Curtain Client to appropriate Control Policy Group.

#### Steps to set a Control Policy Group to default policy:

1. In Curtain Admin, select a Control Policy Group and right-click. Then a menu will be shown.
2. Select "Set as default policy"



3. Done

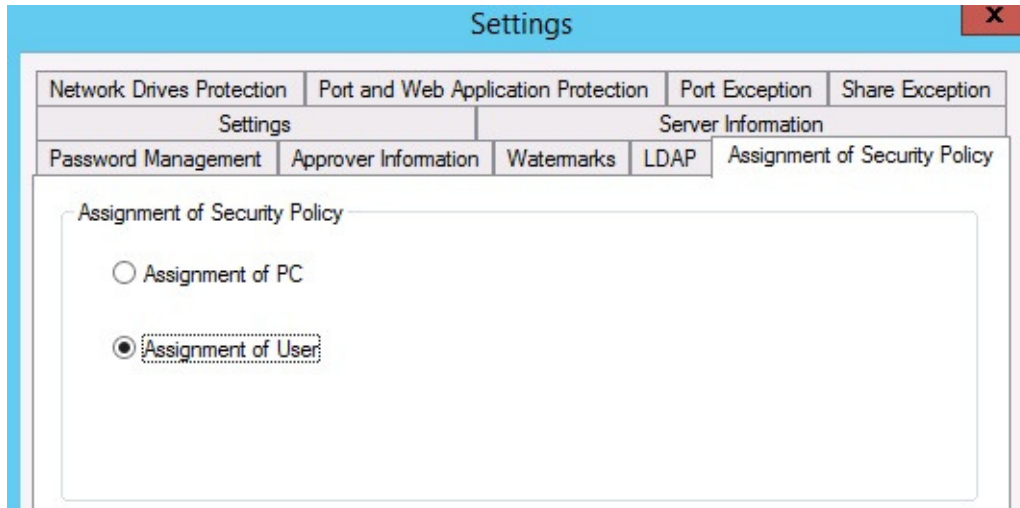
## 5.4 - Grant control policy by user/user group

Control policy of Curtain e-locker 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 Admin. When the first time Curtain 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.

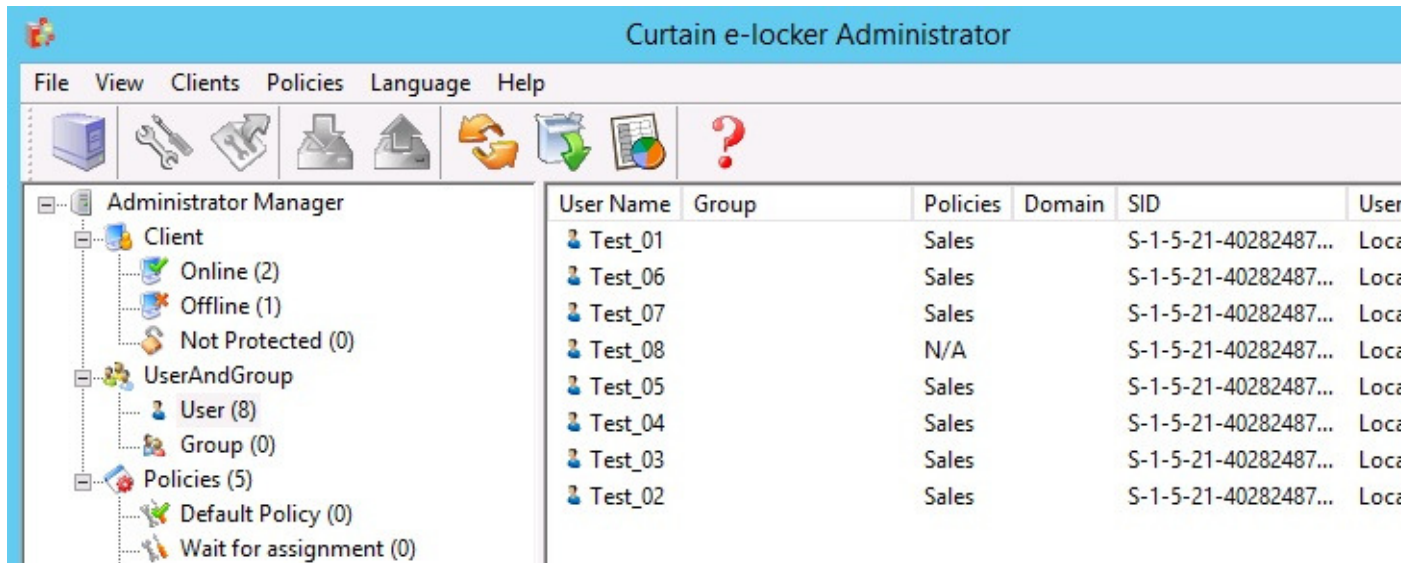
To grant control policy by user/user group, please follow steps stated below to enable "Assignment of User" in Curtain Admin.

[Steps for enabling "Assignment of User" in Curtain Admin:](#)

1. Launch Curtain 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 Admin.

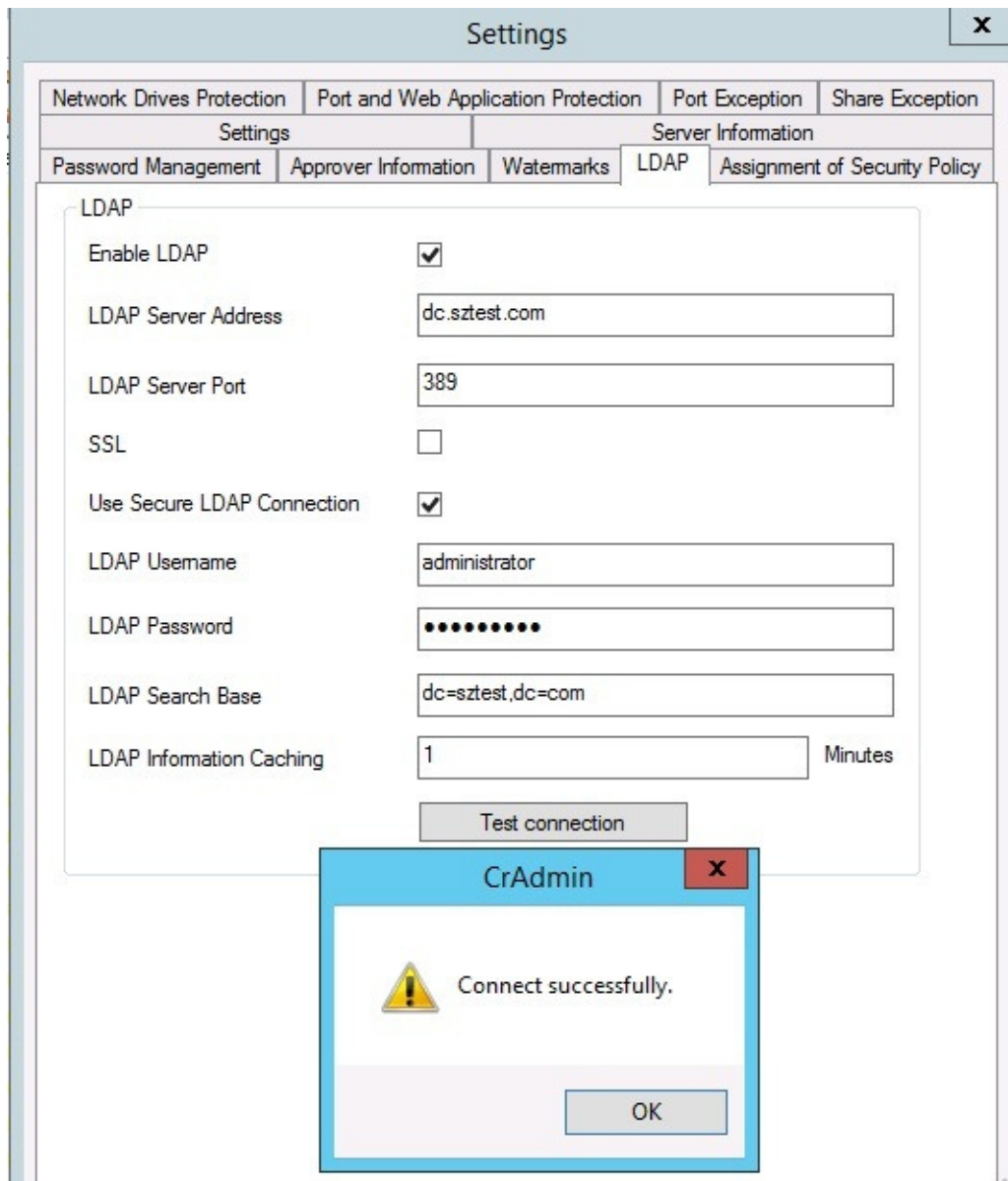


3. Done.

[Steps for importing users and user groups from AD domain:](#)

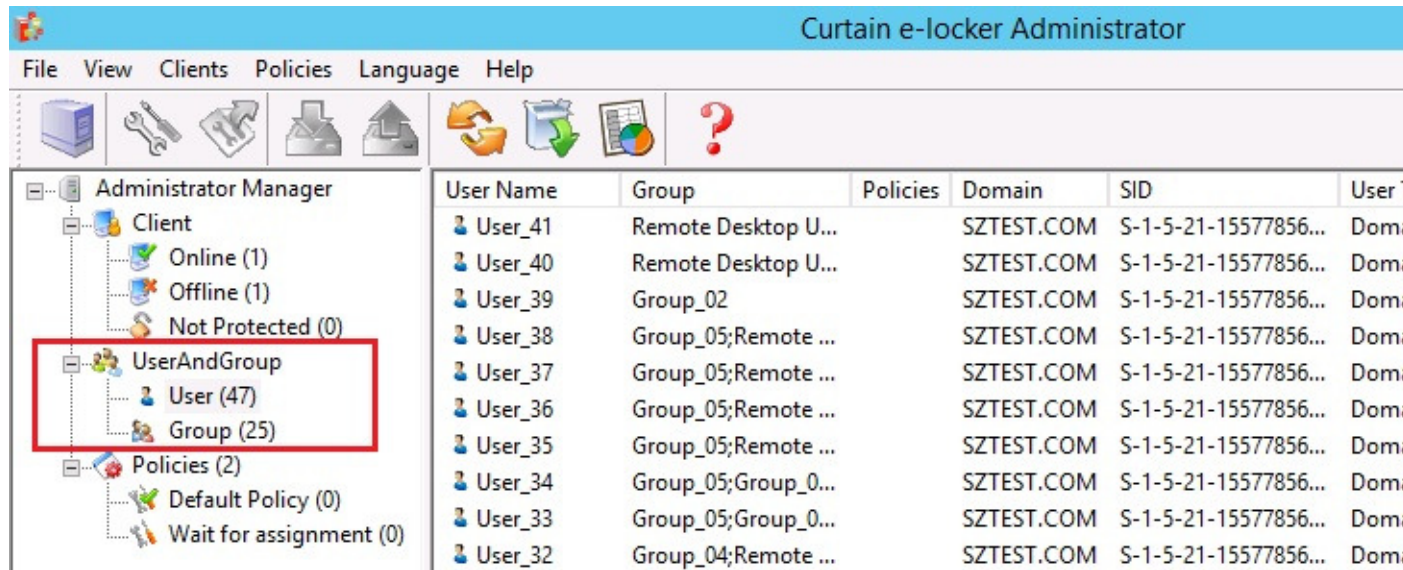
1. Launch Curtain Admin, open File -> Settings -> LDAP.
2. Check "Enable LDAP" button.
3. Enter LDAP server address, DNS or IP address on "LDAP Server Address".
4. "LDAP Server Port", default port is 389.

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 Admin successfully, they will be shown under "User And Group" in Curtain Admin as below.

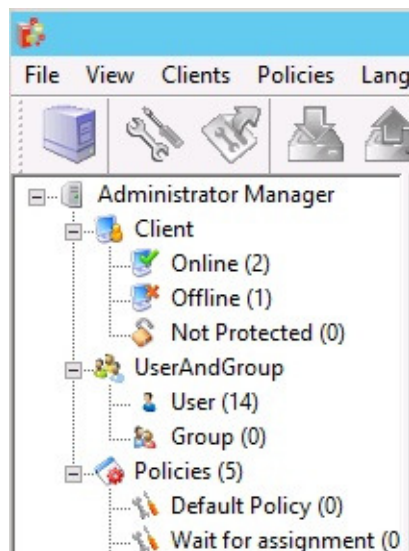


12. Done.

P.S. For local/workgroup users, they will be listed under "User And Group" once they open Curtain Client.

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

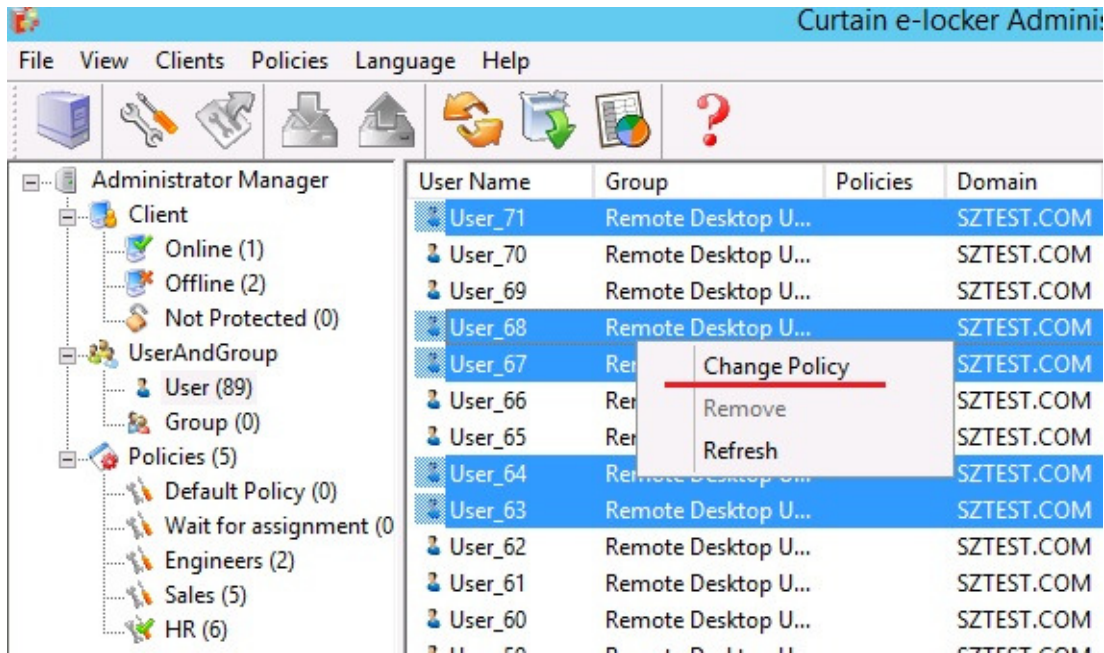
1. In Curtain Admin, select User/Group in left panel. Then, Users/Groups will be listed out in the right panel.



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.



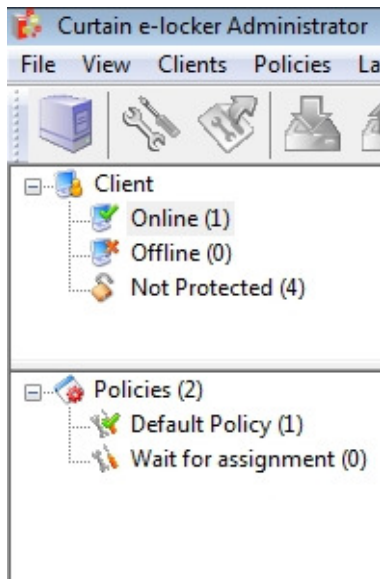


4. Repeat Step 2-3 for assigning other users/groups to appropriate policy groups.
5. Done.

## 5.5 - Assign workstations/users to Control Policy Group

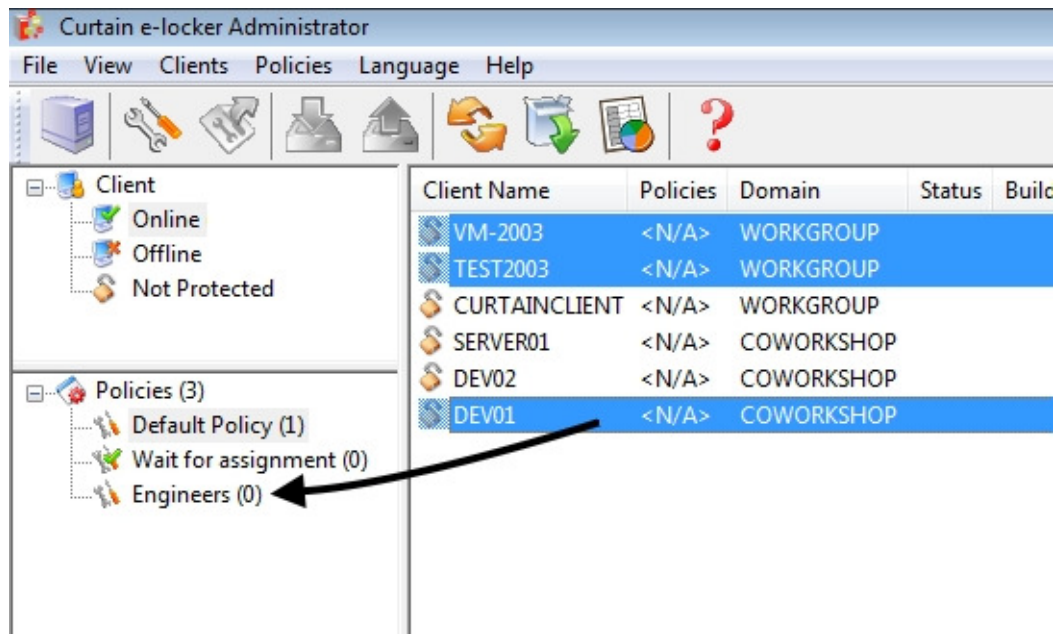
[Steps to assign workstations to different Control Policy Groups:](#)

1. In Curtain 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

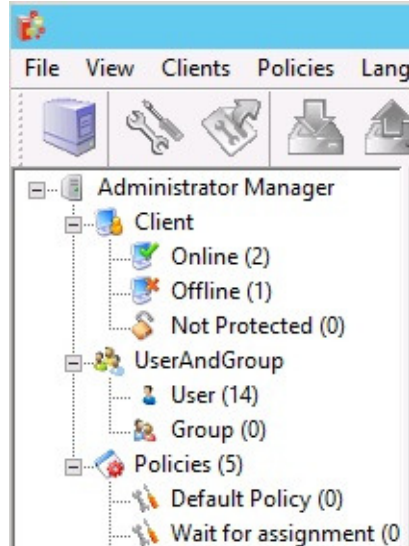


4. Repeat Step 2-3 for assigning other workstations to appropriate policy groups.

5. Done

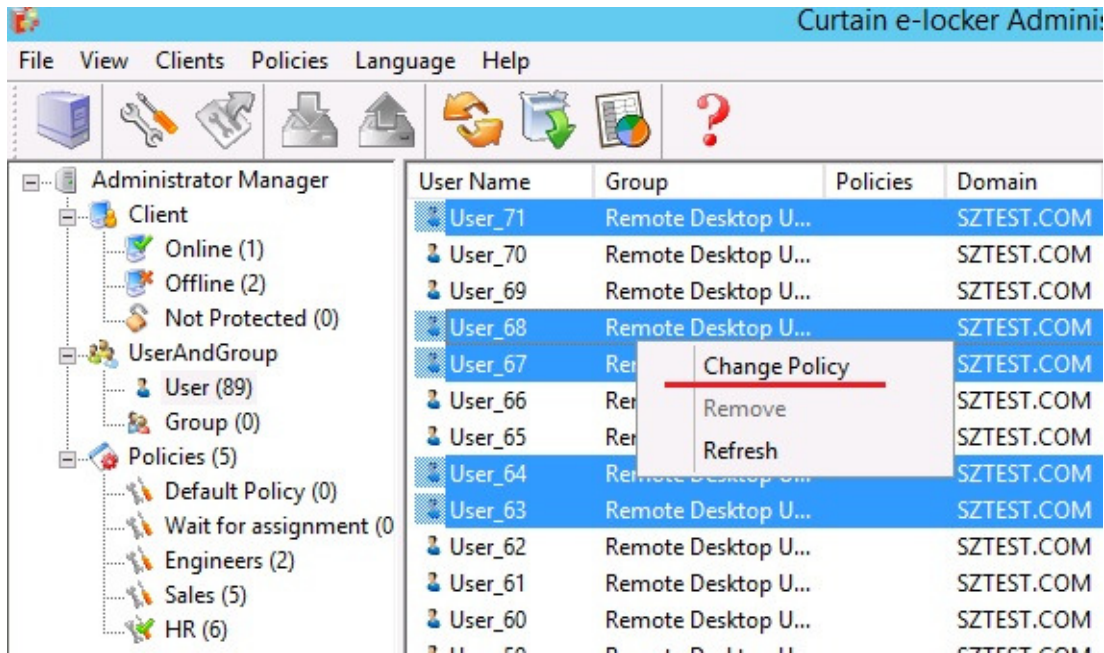
#### Steps to assign users to different Control Policy Groups:

1. In Curtain 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.



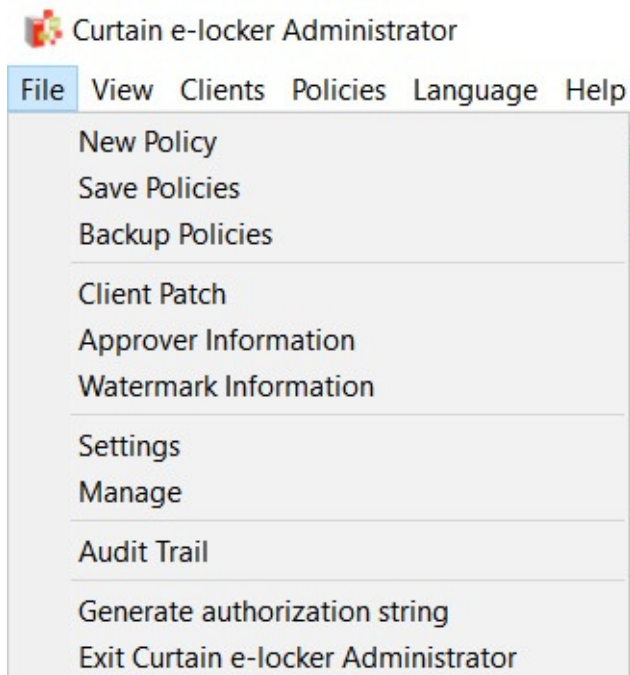
4. Repeat Step 2-3 for assigning other users/groups to appropriate policy groups.
5. Done.

## 5.6 - Define Protected Server Resources

Curtain e-locker can be used to protect different kinds of server resources, such as share folders in Windows File Server, web application, or even self developed system. Please follow below steps to define Protected server resources.

[Steps to define Protected server resources:](#)

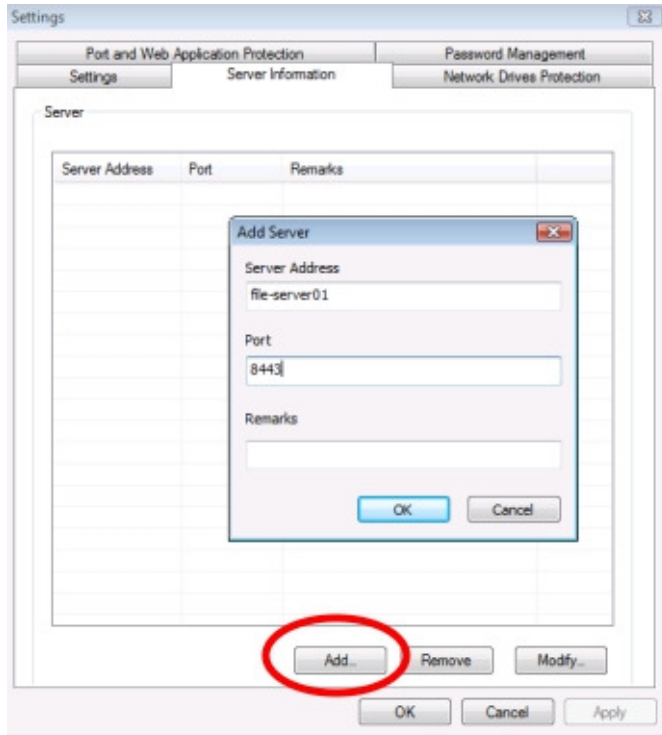
1. In Curtain Admin, select "File > Settings".



2. In Server Information tab, click Add button to add server information first. For example, if you want to protect share folders of two Windows File servers and one web application, you should add the three servers in this tab.

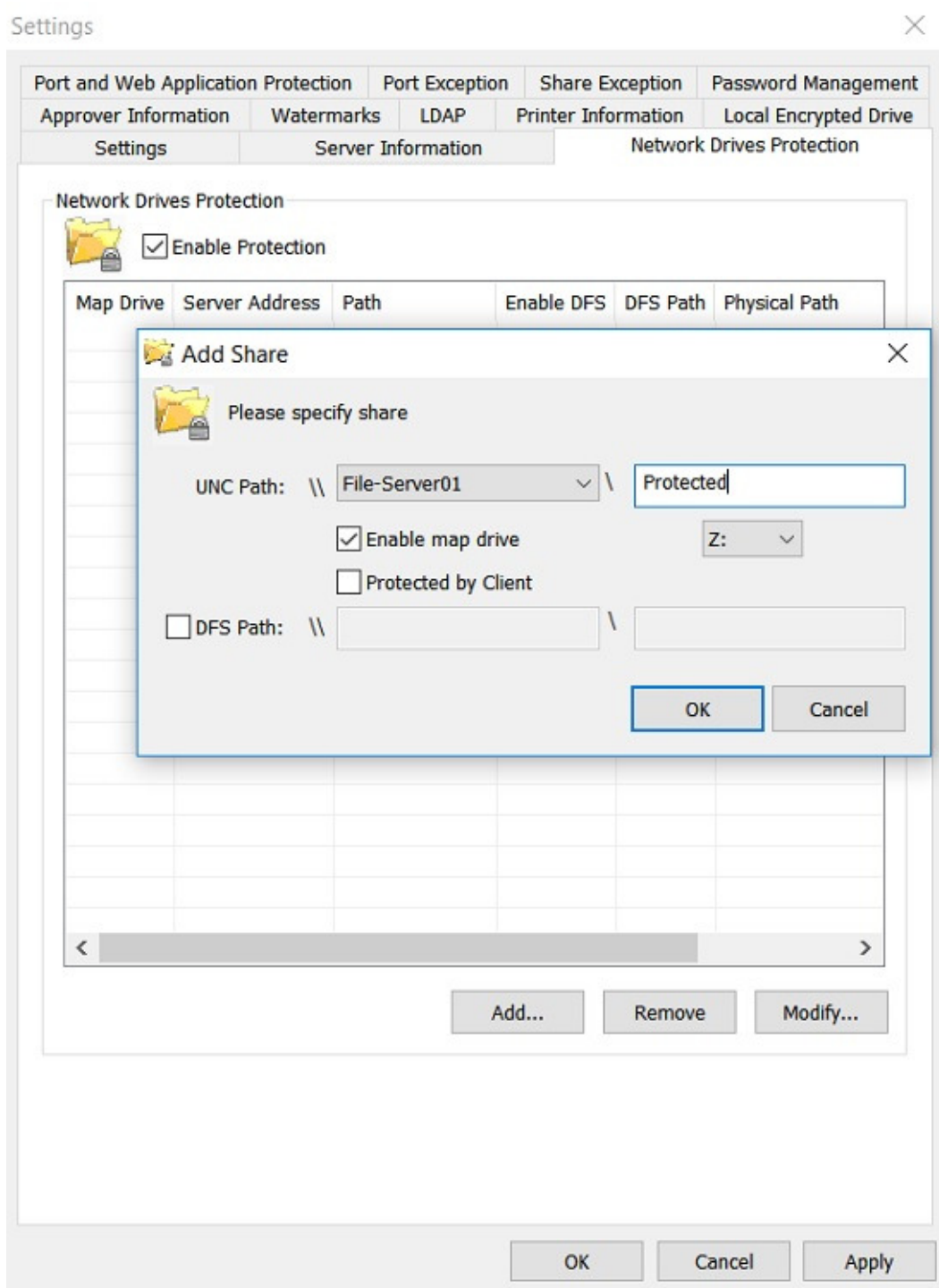
Server Address: Hostname or IP address of the server.

Port: Default value is Port 8443 (for communication between Curtain Admin and Curtain Server Plug-in).



3. Add Protected server resources.

- For scenario 1 - Protect share folder of Windows File Server
- In Network Drives Protection tab, check "Enable Protection".
  - Click "Add" button, a dialog box will be shown.



UNC Path: \\Server\Share Name

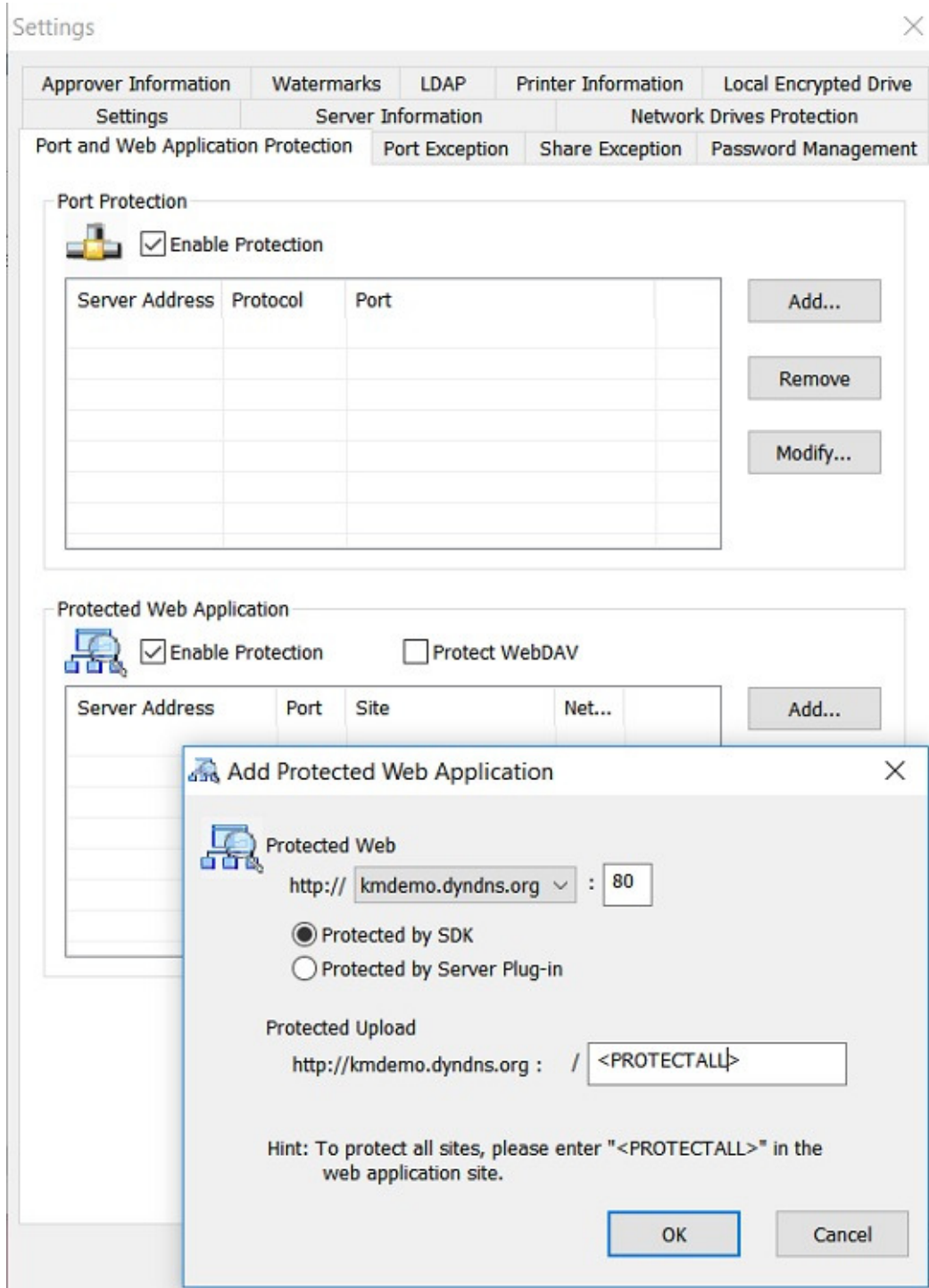
- Server - Select the server (hostname or IP address)
- Share Name - Enter name of the Share (not the folder name, unless you gave the Share the same name as the folder)

Enable map drive: Check this option and select a drive letter, if you want all Curtain Clients map themselves to this drive at startup. Otherwise, users need to do drive mapping manually or use their own logon script.

Protected by Client: Enable this option ONLY when you need to protect share folders without Curtain Server Plug-in installed on the server (e.g. NAS - Network Attached Storage).

- DFS Path: Check this option, if share folder listed above is managed by DFS (Distributed File System).
- Server - Enter server name (users should see the server name as apparent host in My Network Places)
  - Path - Enter path name (the path that users see to the share folder in My Network Places)

For scenario 2 - Protect Web Application  
 - In Protected Web Application, check "Enable Protection".  
 - Click "Add" button, a dialog box will be shown.





Protected Web: http://Hostname: Port Number

- Hostname - Select the web server (hostname or IP address)
- Port Number - Enter port number (port 80 is used by most web applications)

Protected by SDK: Select this option, if the web application has been customized for Curtain e-locker by using our SDK (software development kit).

Protected by Server Plug-in: Select this option, if the web application has NOT been customized for Curtain e-locker.

Protected Upload: http://Hostname/Path

- Path - Enter the path you want to protect

Example 1 - Microsoft SharePoint (e.g. http://SharePoint Server/Site)

- Administrators can create many SharePoint sites. If administrators want to apply Curtain e-locker to protect some of them, they can enter SharePoint Site Name for the Path. Then, users have to use Protected Internet Explorer to access the Protected Site. All resources under the Site are protected by Curtain e-locker.

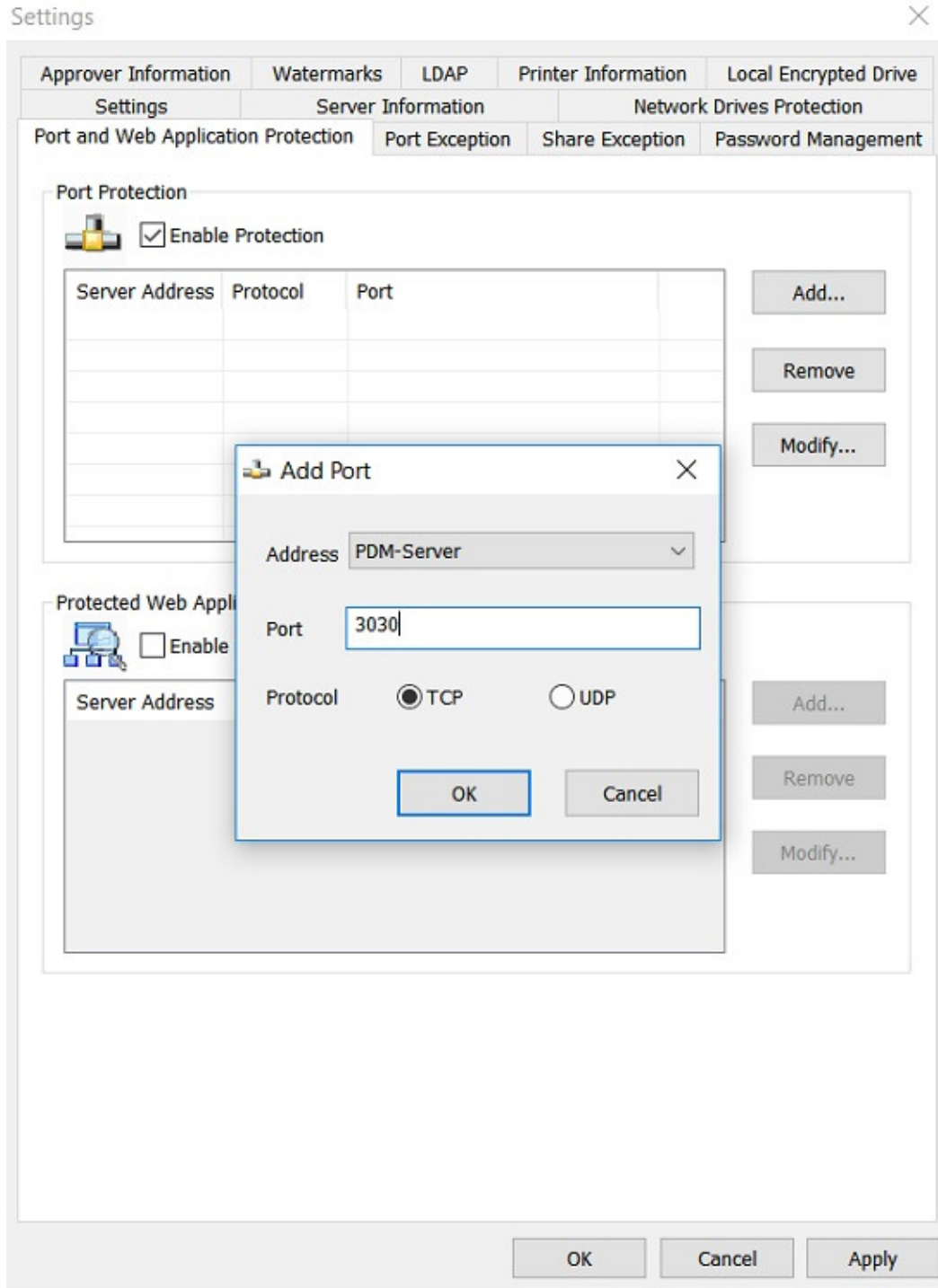
Example 2 - IBM Lotus Quickr (e.g. http://Lotus Quickr Server/Place)

- Administrators can create many Places in Lotus Quickr. If administrators want to apply Curtain e-locker to protect some of them, they can enter the full path of the Place (e.g. quickr/place1.nsf). Then, users have to use Protected Internet Explorer to access the Protected Place. All resources under the Place are protected by Curtain e-locker.

If administrators want to protect the whole web application, they should enter "<PROTECTALL>".

For scenario 3 - Protect Port (for SolidWorks PDMWorks)

- In Port Protection, check "Enable Protection".
- Click "Add" button, a dialog box will be shown.



- Address - Select the PDMWorks server (hostname or IP address)
- Port Number - Enter port number (default port for PDMWorks is 3030)
- Protocol - Select protocol (default protocol for PDMWorks is TCP)

4. Click OK to confirm.



## 5.7 - Protect sub-folder of a share folder

For example: There are 9 share folders (i.e. pro1, pro2... and pro9) in file server under a share folder called "pro". If you only want to set pro1, pro2, and pro3 as Server Protected Zone, how can we do that? There are two methods.

Method 1:

Share those sub folders (i.e. pro1, pro2, and pro3) in file server and set them as Protected Network Drive in Curtain Admin.

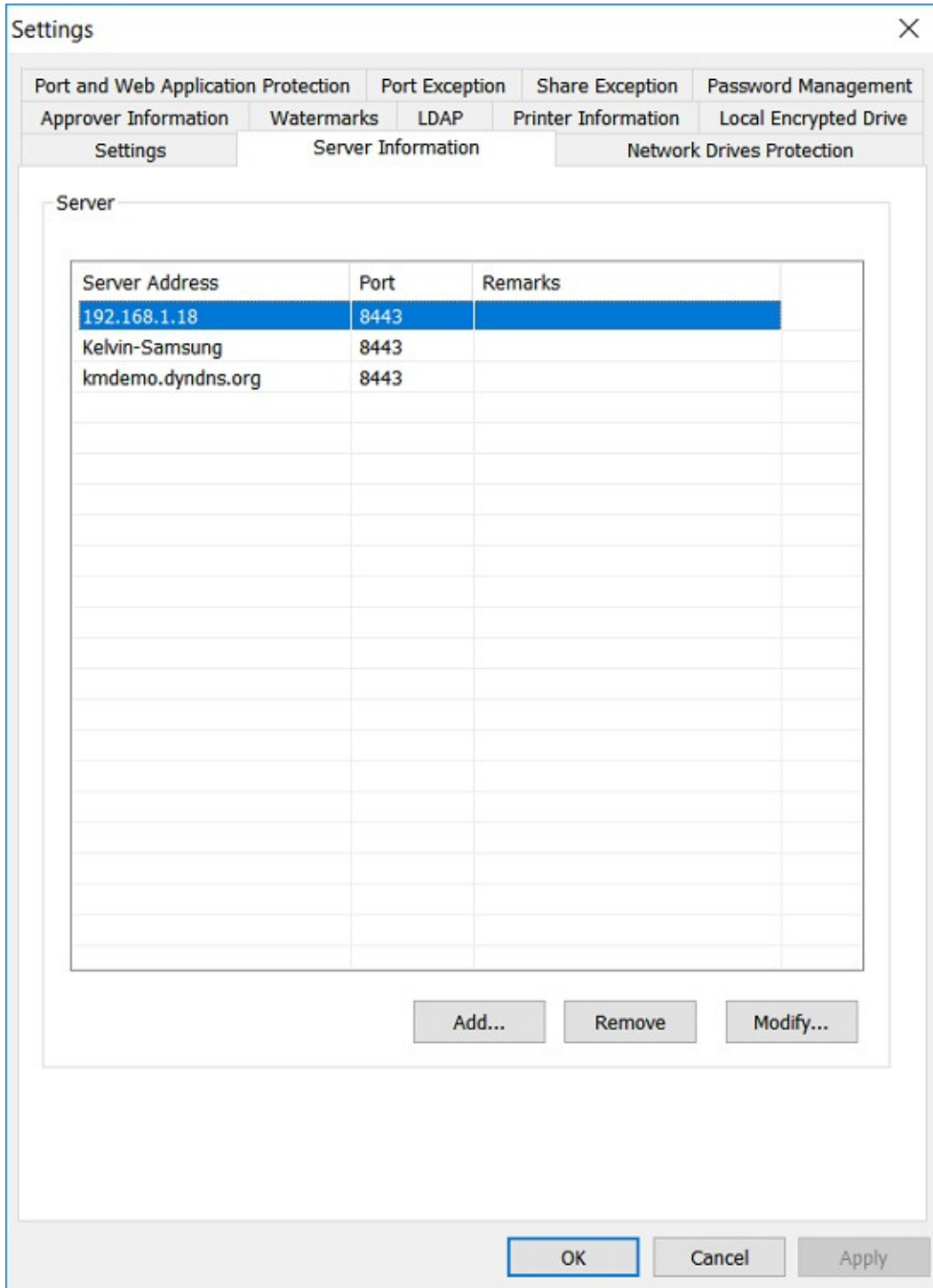
Method 2:

No need to share those sub folders (i.e. pro1, pro2, and pro3) in file server. You can set them as Protected Network Drive in Curtain Admin directly. Please follow steps stated below.

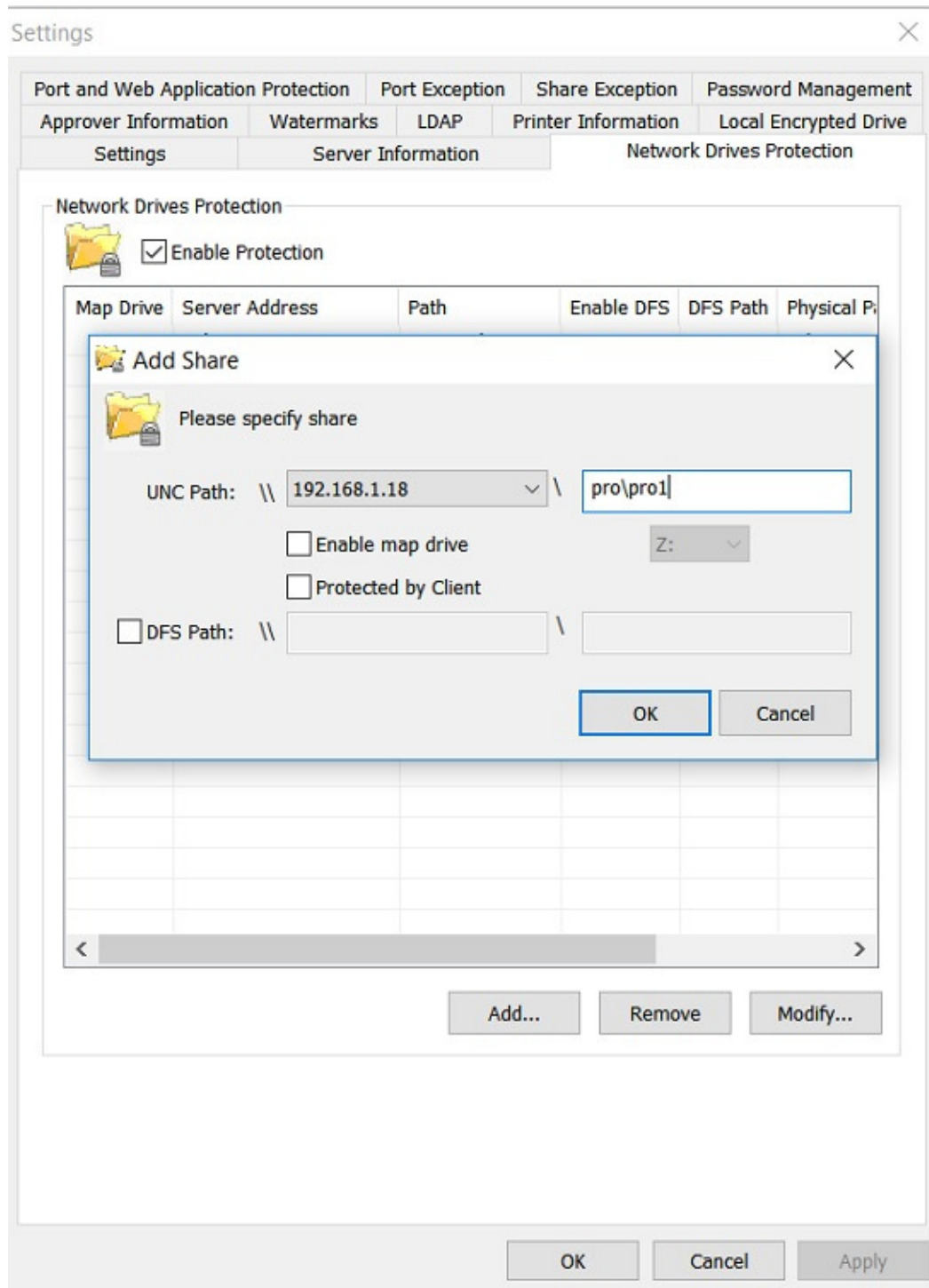
### [Steps to set protection for sub-folder](#)

1. In Curtain Admin, click "File > Settings" in the menu.

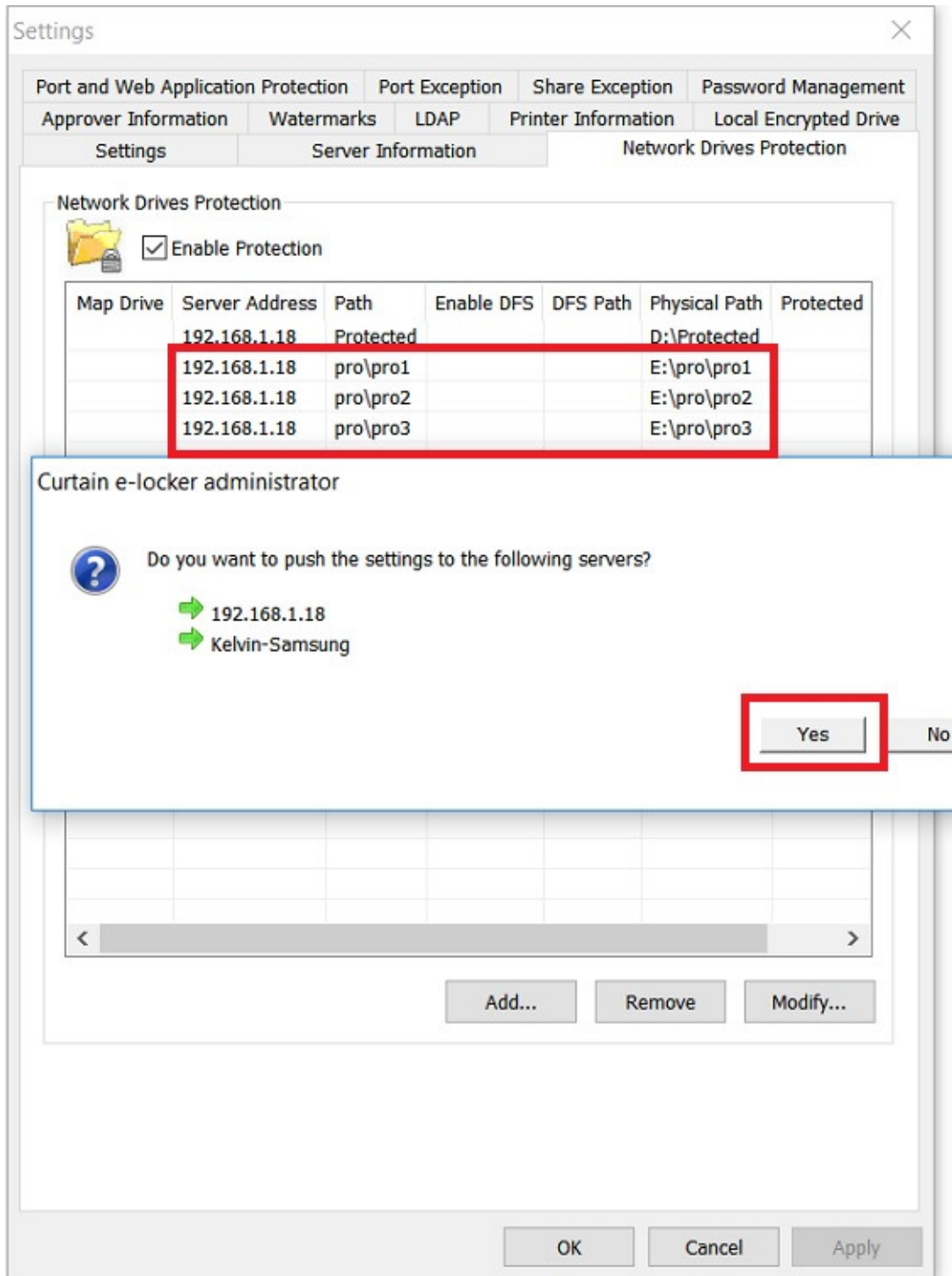
2. Add the machine name or IP address of the file server in "Server Information" tab.



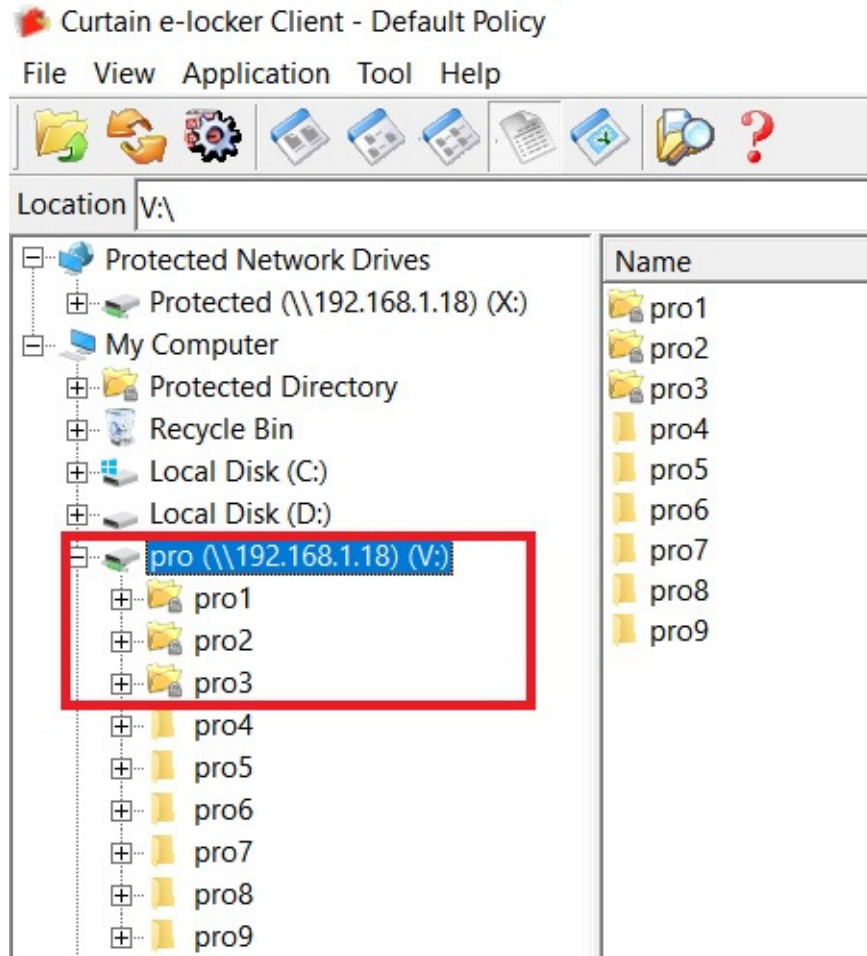
3. Add the 3 sub folders (that is pro1, pro2 and pro3 in our example) in "Network Drives Protection" tab as picture below.



4. Click OK to confirm, and click Yes to push the settings to server(s).



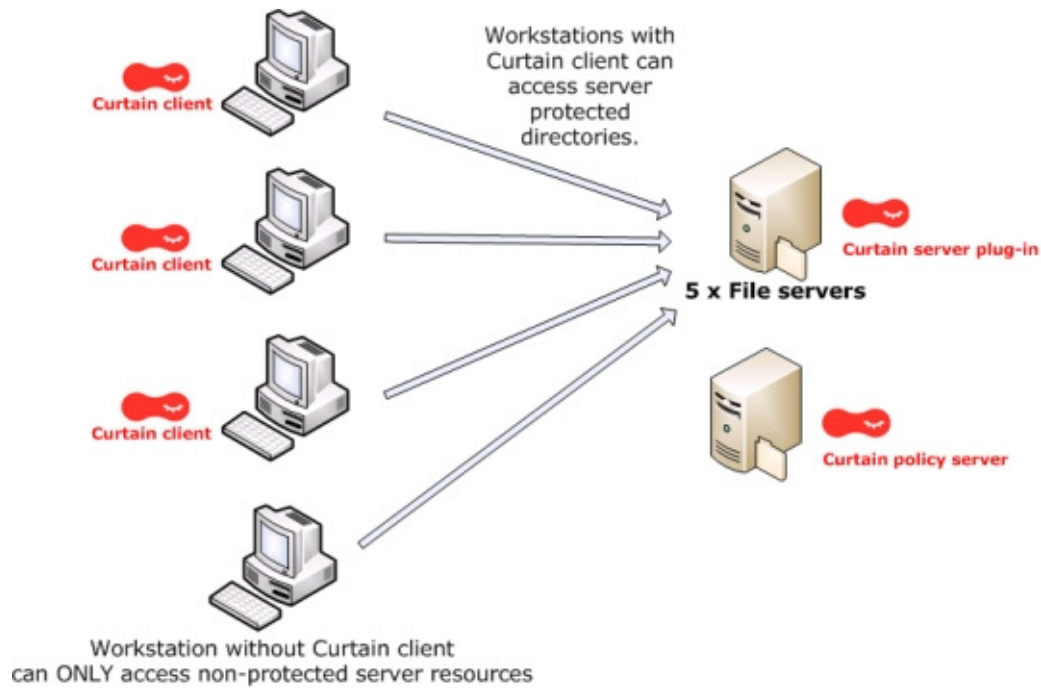
5. Open Curtain Client, you can see sub-folder pro1, pro2 and pro3 are protected by Curtain e-locker under My Computer. The folder icon of these 3 sub-folders are with lock, while other sub-folders are not protected.



## 5.8 - Exception Rule

### 5.8.1 - Exception Rule

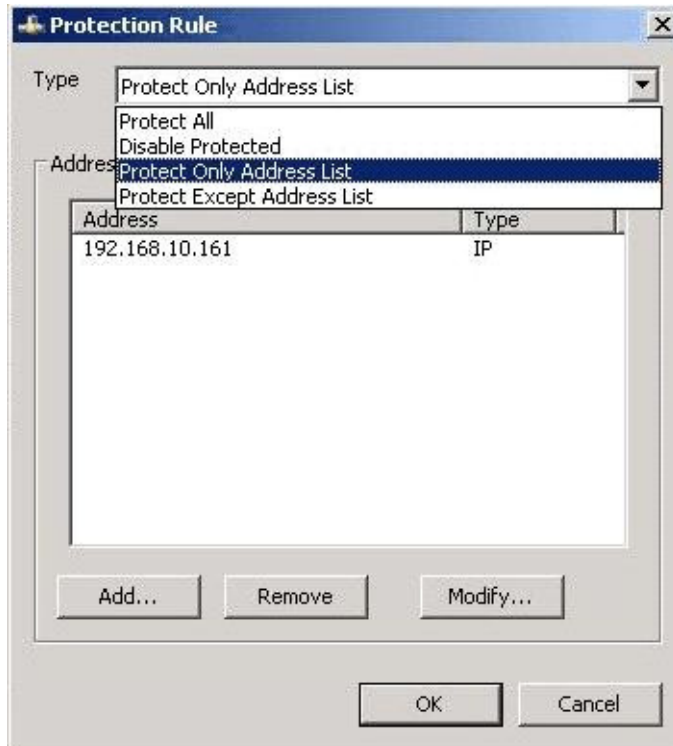
The function of Exception Rule provides the flexibility to administrators to allow some workstations without Curtain Client installed to access Protected Zone. As the picture shown below, workstations with Curtain Client can access protected server resources (e.g. protected share folders) under Curtain protection. By default, workstations without Curtain Client installed CANNOT access protected server resources. However, in some situations, administrators need to allow some workstations (e.g. top management) without Curtain Client installed to access protected server resources. Then, they can use this function to do that.



This function is also useful for setting up test environment. For example, R&D department is using SolidWorks EPDM system to manage their product information. Now, they want to implement Curtain e-locker to protect the information in EPDM. Before implementing e-locker to all workstations in R&D department, they want to install Curtain e-locker on a few workstations for testing. Then, administrators can use this function to specify which workstations are protected by e-locker. Other workstations without Curtain Client installed can still access the EPDM system without e-locker control.

There are 4 Protection Rules.

- Protect All - this rule is the default setting. Only workstations with Curtain Client installed can access Protected Zone.
- Disable Protection - this rule is not recommended. When this rule is selected, e-locker protection is temporarily disabled. All workstations can access Protected Zone without e-locker control.
- Protect Only Address List - administrators can enter a list of workstation (by IP address). Only workstations on the list are protected by e-locker.
- Protect Except Address List - administrators can enter a list of workstation (by IP address). Only workstations on the list are NOT protected by e-locker.



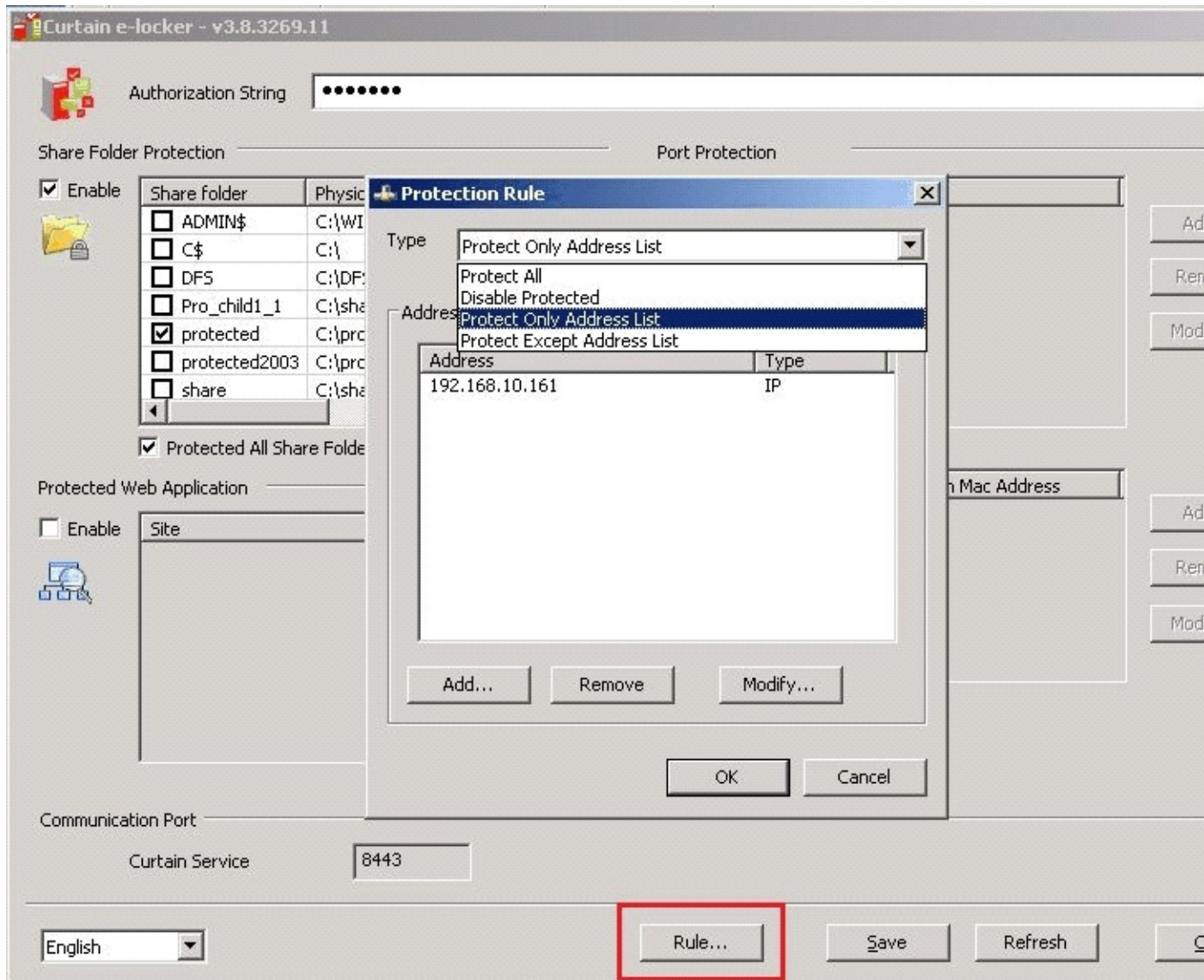
### 5.8.2 - Set Exception Rule

The function of Exception Rule provides the flexibility to administrators to allow some workstations without Curtain Client installed to access protected resources in particular server. Therefore, this function is set in Curtain Server Plug-in.

#### [Steps to set Exception Rule:](#)

1. Open Curtain Server Plug-in by selecting "Start -> Programs -> Coworkshop Curtain e-locker -> Secure Network Manager"

2. Click "Rule..." button and select appropriate protection type.



3. If "Protect Only Address List" or "Protect Except Address List" is selected, click "Add" button to add workstation's IP to the list.

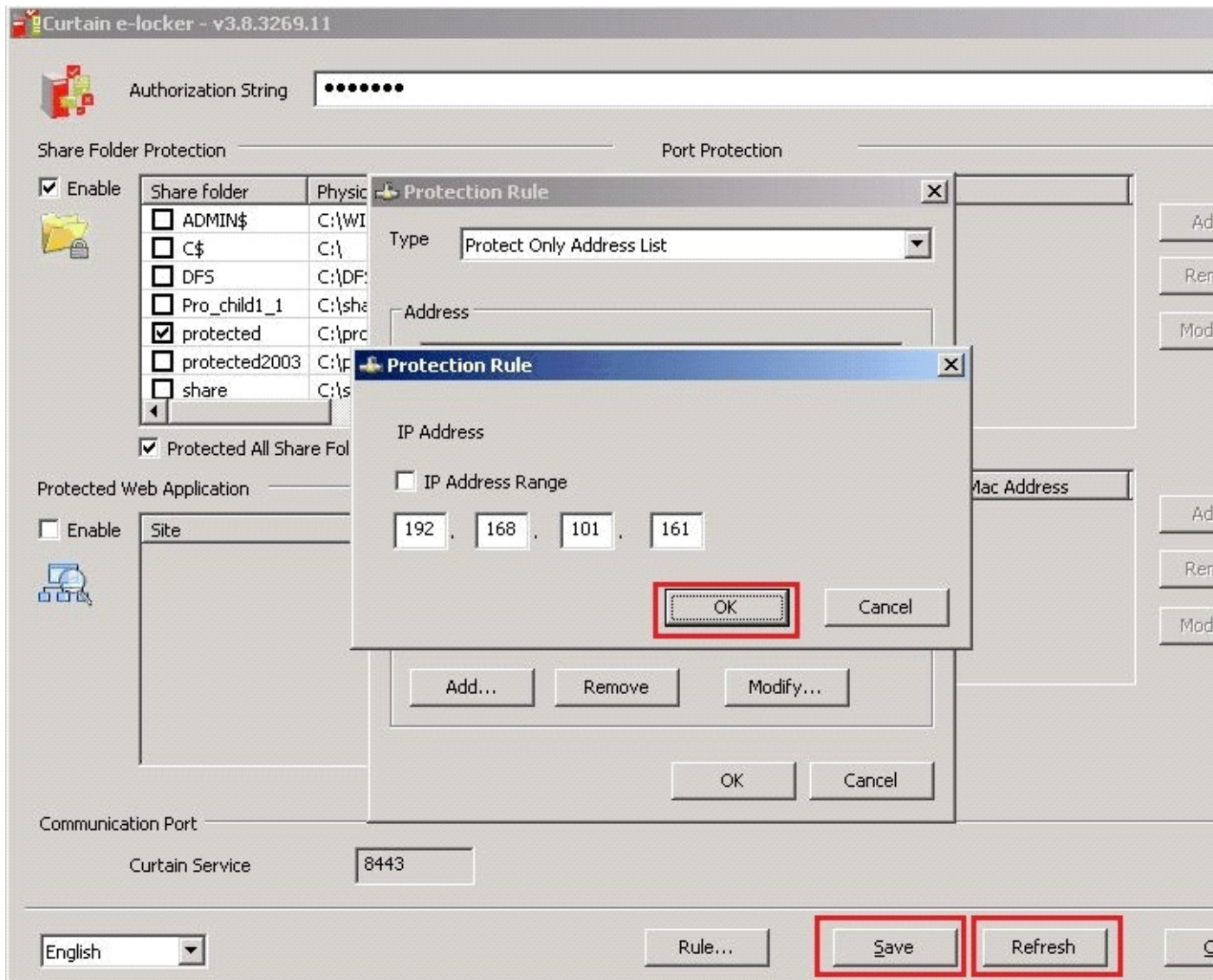


4. Choose Address Type and input the address accordingly.



5. Click "OK" to confirm.

6. Click "Save" and "Refresh" button.



P.S. When click "Close" button, the system will prompt message to ask whether to restart the server or not. Simply click "No" to exit.

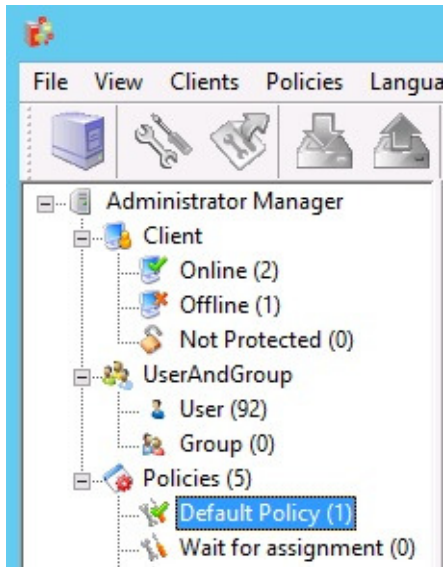
7. Done.

## 5.9 - Disable protection temporarily

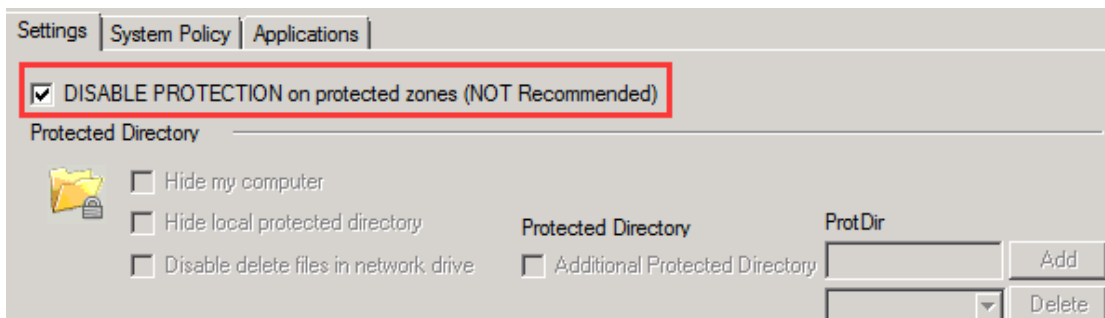
The function of Disable Protection provides the flexibility to administrators to allow workstations/users under particular policy group to access Protected Zone without e-locker protection. In general, it is not recommended to enable this function because it may cause leakage of sensitive files. However, sometimes administrators may need to disable e-locker protection temporarily. You may create a Policy Group with this function enabled. When you want to disable e-locker protection to workstations/users, you can simply assign them to this control policy group.

[Steps to disable Curtain e-locker protection:](#)

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

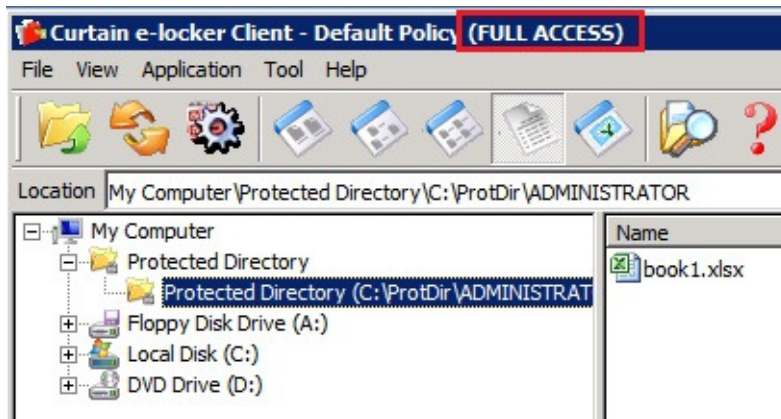


2. Select "DISABLE PROTECTION on protected zones".



3. Click OK to confirm.

If a workstation/user is disabled e-locker protection temporarily, "FULL ACCESS" will be shown in the title bar of Curtain Client as below.



4. Done.

## 6 - Other Features

### 6.1 - Protect First Draft

Protect First Draft is a feature to protect newly created files. If this feature is enabled, user must save newly created file to Protected Zone. It protects sensitive information at the point of creation.

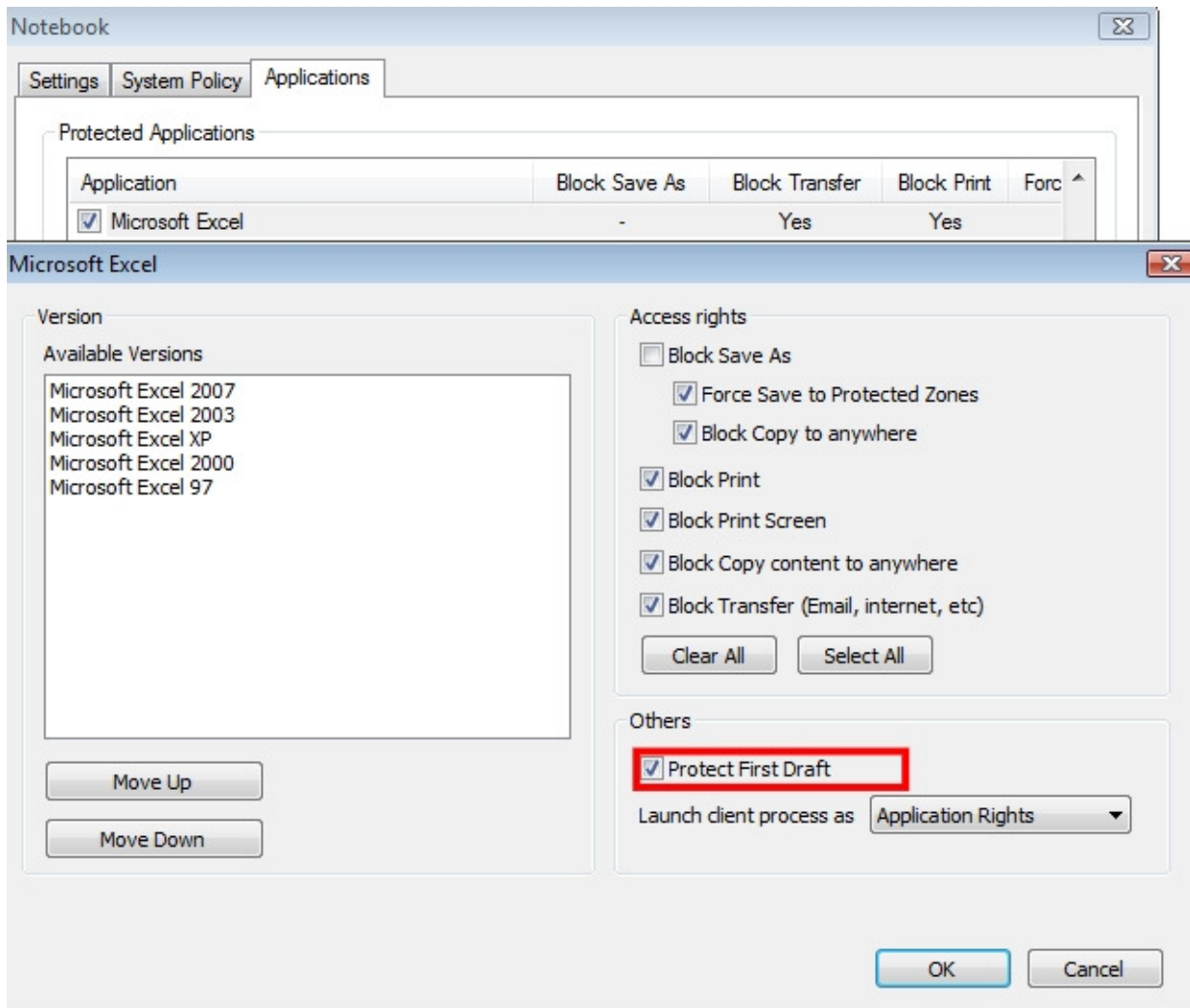
This feature can be enabled by Policy Group and Application. Here is an example of its usage.  
- Enforce engineers to save all newly created AutoCAD and Photoshop files to Protected Zone

[Steps to enable Protect First Draft for an application:](#)

1. In Curtain Admin, select a Policy Group and right-click to select "Properties".
2. In Applications tab, double-click the application which you want to enable Protect First Draft.
3. Select "Protect First Draft" and click OK to confirm.

"Launch client process as Application Rights" - This control is only applied to the selected application.

"Launch client process as Parent Process Rights" - This control is applied to the selected application and all of its child process (e.g. a Excel program is launched within AutoCAD)



P.S. When Protect First Draft is enabled for an application (e.g. Excel). ONLY Protected application can be launched. In this example, that means users cannot launch non-Protected Excel. If users try to launch it, Curtain e-locker will automatically stop the application. For non-Protected Excel files, users must copy them to Protected Zone before opening them. Users can copy them to Protected Zone by Copy-and-Paste or Drag-and-Drop.

## 6.2 - Online/Offline Protection

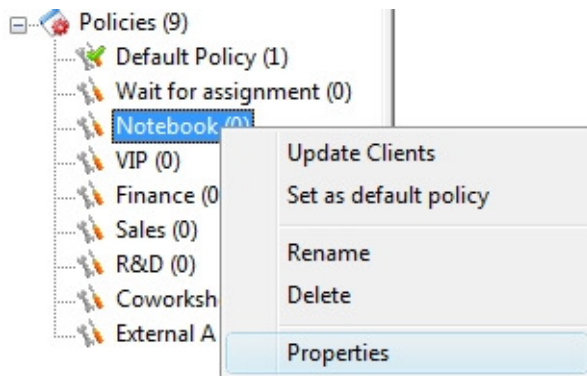
Online/Offline Protection is a feature to control how users use downloaded sensitive information.

The major purpose of this function:

- Do not want downloaded sensitive information can be used when the desktop/notebook is out of the company (it means the desktop/notebook cannot connect with Curtain Admin)

[Steps to enable Online/Offline Protection:](#)

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

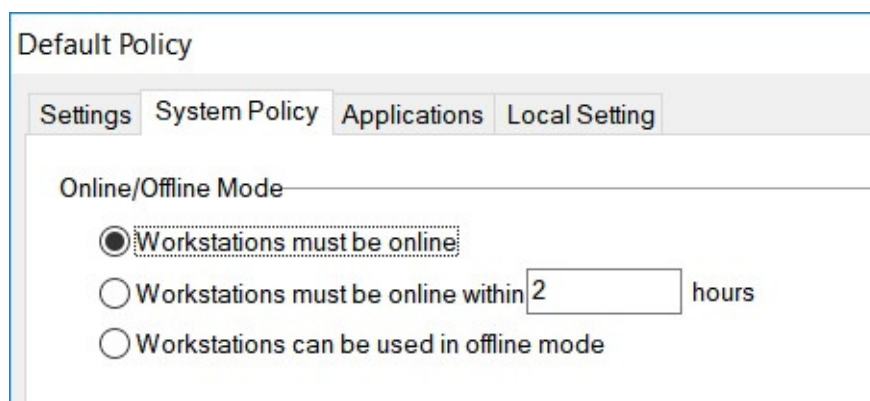


2. In "System Policy" tab, there are three options under Online/Offline Mode.

"Workstations must be online" - When this option is selected, Curtain Client CANNOT be launched if it cannot connect with Curtain Admin.

"Workstations must be online within [ ] hours" - When this option is selected, Curtain Client CANNOT be launched if it disconnected with Curtain Admin for a specified period of time.

"Workstations can be used in offline mode" - When this option is selected, Curtain Client can be launched no matter it can or cannot connect with Curtain Admin.



## 6.3 - Housekeeping

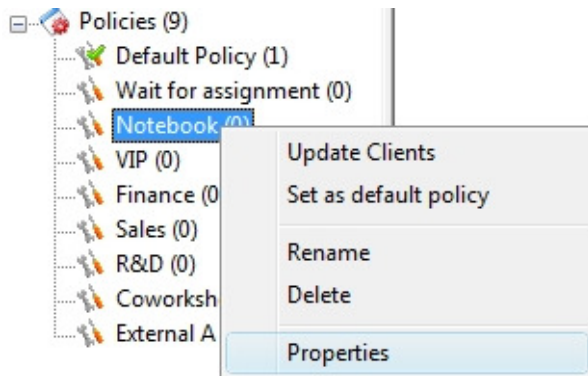
Housekeeping is a feature for clearing up files in Local Protected Directory.

There are 2 main purposes of this function:

- Do not want users to keep files in Local Protected Directory forever.
- Clean up cache, temporary files and Recycle Bin in Local Protected Directory, in order to free up disk space.

[Steps to enable Housekeeping:](#)

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



2. Select the Rules to clean up files in Local Protected Directory, and then click OK button to confirm.

### Housekeeping

|                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> <b>Clear the whole local protected directory</b><br><input checked="" type="radio"/> Startup<br><input type="radio"/> Weekly Sun Mon Tue Wed Thu Fri Sat<br><input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> | <input type="checkbox"/> <b>Clear temp folder in local protected directory</b><br><input checked="" type="radio"/> Startup<br><input type="radio"/> Weekly Sun Mon Tue Wed Thu Fri Sat<br><input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> |
| <input type="checkbox"/> <b>Clear files in local protected directory</b><br><input type="checkbox"/> Delete file after download: <input type="text" value="0"/> Days<br><input type="checkbox"/> Delete file after modified: <input type="text" value="0"/> Days<br>Delete if <b>all</b> applied                                                                    | <input type="checkbox"/> <b>Clear recycle bin files in local protected directory</b><br><input type="checkbox"/> Delete file after deleted: <input type="text" value="10"/> Days                                                                                                                                                                                         |

"Clear the whole local protected directory" - If this option is selected, all files in Local Protected Directory will be deleted.

Startup - If this option is selected, housekeeping will be done every time when user's workstation startup.

Weekly - If this option is selected, housekeeping will be done when user's workstation startup on the selected day(s).

"Clear temp folder in local protected directory" - If this option is selected, all temporary files in Local Protected Directory will be deleted.

Startup - If this option is selected, housekeeping will be done every time when user's workstation startup.

Weekly - If this option is selected, housekeeping will be done when user's workstation startup on the selected day(s).



"Clear files in local protected directory" base on Date downloaded and/or Date modified - If this option is selected, all files in Local Protected Directory which meet the criteria (i.e. Date downloaded and/or Date modified) will be deleted.

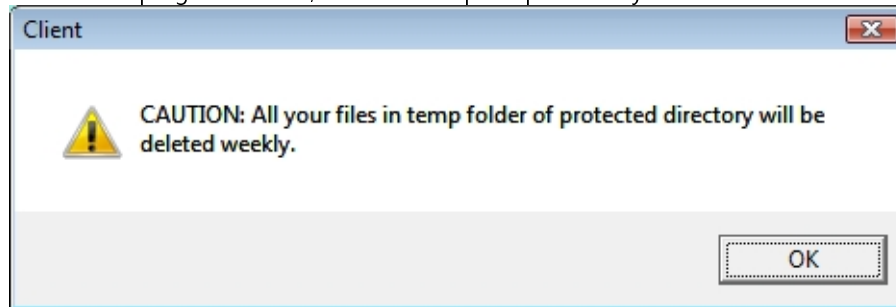
Delete file after downloaded [ ] Days - If this option is selected, files downloaded to Local Protected Directory over specified days will be deleted.

Delete file after modified [ ] Days - If this option is selected, last modified date over specified days will be deleted.

"Clear recycle bin files in local protected directory" base on Date deleted - If this option is selected, all files in Recycle Bin which meet the criteria (i.e. Date deleted) will be deleted.

Delete file after deleted [ ] Days - If this option is selected, files deleted to Recycle Bin over specified days will be deleted.

If housekeeping is enabled, users will be prompted every time when Curtain Client is launched.



## 6.4 - Screen Capture Protection

Curtain e-locker handles Print-screen or Capture-screen software in a smart way.

- Only window of sensitive data is dimmed
- Users still enjoy the convenience of screen-capture for non-sensitive data
- Screen-dump software is also blocked



## 6.5 - Smart Copy-and-Paste Control

Curtain e-locker handles Copy and Paste in a smart way.

- Copy and Paste in between documents in Protected Zone is allowed,
- Copy data from non-Protected Zone to Protected Zone is allowed,
- However, copy data from Protected Zone to non-Protected Zone is prohibited if it is not allowed.

It does not affect normal operations, while security is maintained. Curtain e-locker makes a good balance between convenience and security.

## 6.6 - Secure Print-to-PDF

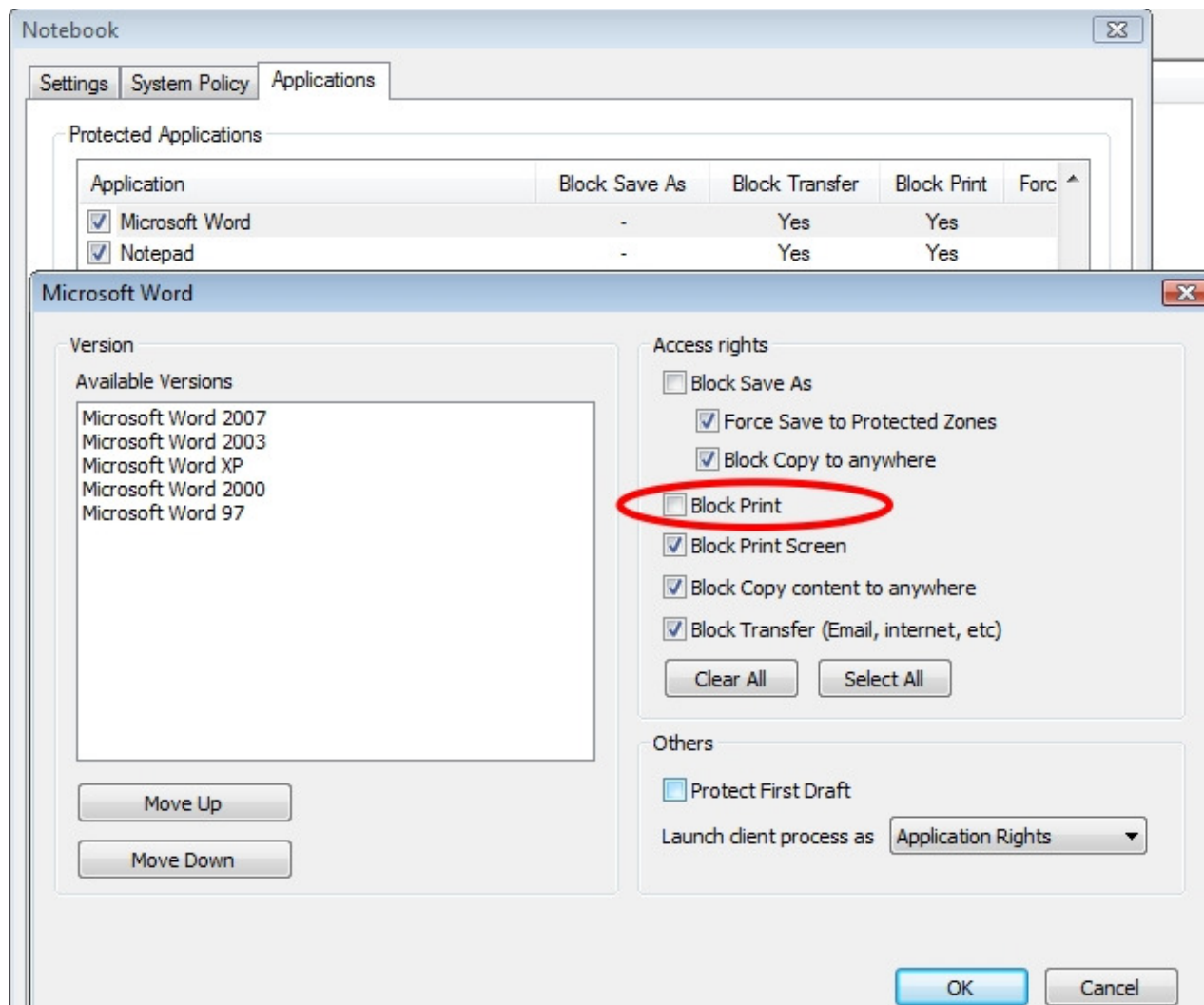
Secure "Print-to-PDF" is a feature to allow users to convert sensitive documents to PDF format in a secure way.

The major purpose of this function:

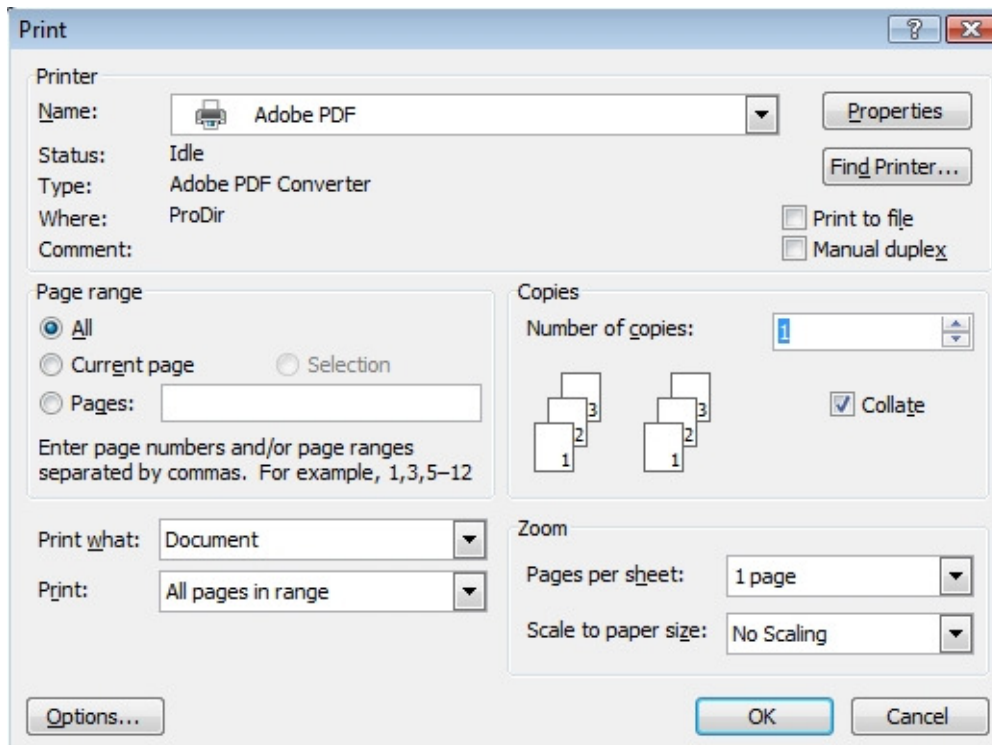
- Users can convert sensitive documents to PDF format by using the function of Print-to-PDF. However, the PDF file can be only saved to Protected Zone. It makes a good balance on convenience and security. Users can generate PDF files, but data still cannot be leaked out of the company through this channel.

### Example: Allow users to convert Protected Word documents to PDF format

If administrators allow a user to convert Protected Word documents (i.e. Word documents in Protected Zone) to PDF format, administrators should allow the user to print Word document first. Then the user can print Word documents in Protected Zone to PDF format by Print-to-PDF. All generated PDF files can be only saved to Protected Zone.



Allow users to print Word document first



Convert documents to PDF format by Print-to-PDF

## 6.7 - Share protected files with others

In general, there are three different levels of permission:

(Scenario 1) user is authorized to encrypt and save the encrypted files out of Protected Zone. The files can be ONLY decrypted in Protected Zone.

(Scenario 2) user is authorized to encrypt and save the encrypted files out of Protected Zone. The files can be decrypted anywhere with entering correct password.

(Scenario 3) user is authorized to save/send/copy files out of Protected Zone (without encrypting the files). The files are no longer under Curtain e-locker protection.

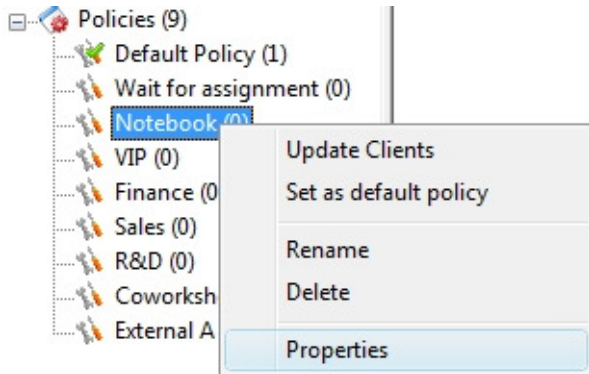
Scenario 1 - Encrypt out (Decrypt in Client only):

This function is very useful for users to share protected files within company. Therefore, you can grant this function to most of the users.

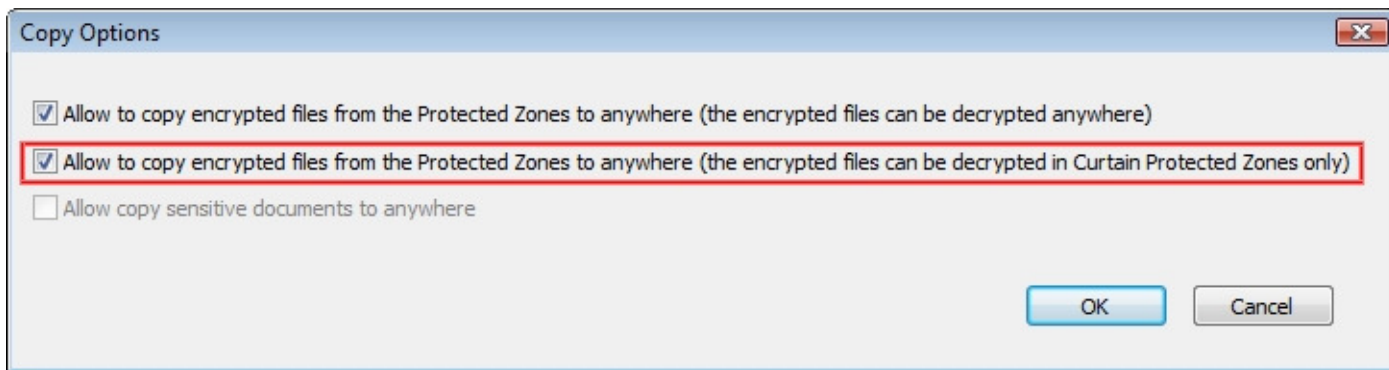
If a user is allowed to Encrypt Out (Decrypt in Client Only), the user can encrypt Protected files and share the encrypted files with others. When other users receive the files, their workstations must have Curtain Client (pointing to the same Curtain Admin) installed. The users can double-click the files to decrypt them. Files will be automatically decrypted to Local Protected Directory.

**Steps to grant the right "Encrypt Out (Decrypt in Client Only)":**

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

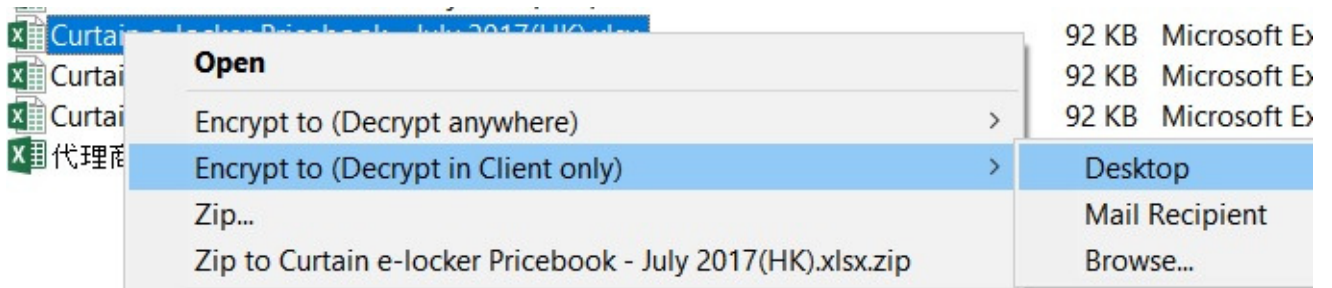


2. Click "Copy Options" button, select the second option as below and click OK to confirm.



**Steps to share encrypted files with others:**

1. In Curtain Client, select a protected file and right-click to select "Encrypt to (Decrypt in Client only)". Then an encrypted file will be copied to destination.



2. Send the encrypted file to others. Since the file is encrypted, the file is safe during transmission (e.g. USB flash drive or Email).



3. When user receives the file, the user simply double-clicks the file. It will be decrypted to Local Protected Directory.

### Scenario 2 - Encrypt out (Decrypt Anywhere):

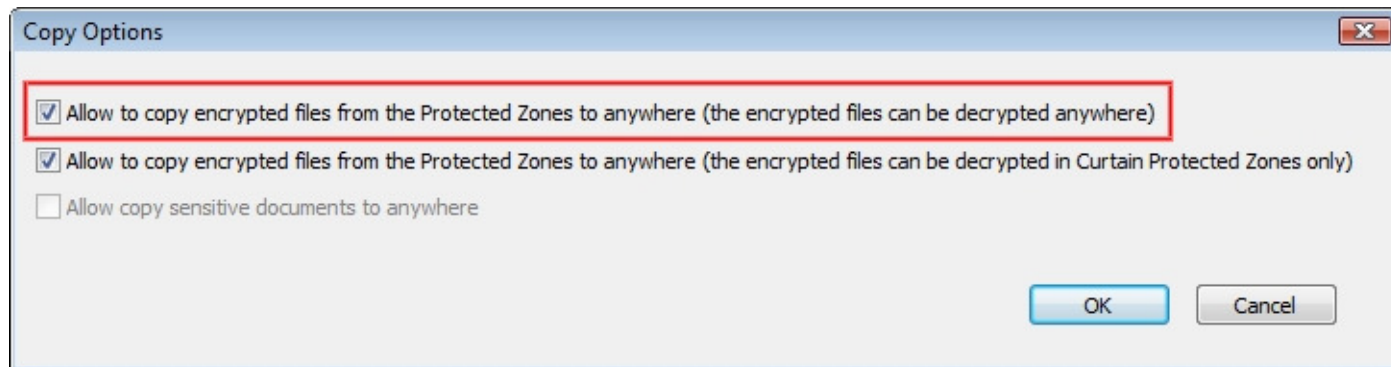
Actually the users can get the files after entering correct password. Therefore, this function should be only granted to authorized users.

If a user is allowed to Encrypt Out (Decrypt Anywhere), the user can encrypt Protected files with password and share the encrypted files with others. When other users receive the files, they can decrypt the files with entering correct password.

P.S. Curtain Client is not needed for the decryption. After the files are successfully decrypted to plain files, Curtain will not protect the plain files anymore.

#### Steps to grant the right "Encrypt Out (Decrypt Anywhere)":

1. In Curtain Admin, select a Policy Group and right-click to select "Properties"
2. Click "Copy Options" button, select the first option as below and click OK to confirm.

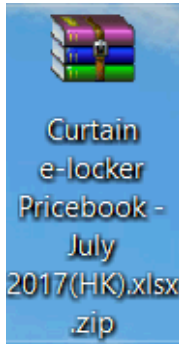


#### Steps to share password-encrypted files with others:

1. In Curtain Client, select a protected file and right-click to select "Encrypt to (Decrypt Anywhere)".
2. Set Password and click OK. Then an encrypted file will be copied to destination.



3. Send the password-encrypted file to others. Since the file is encrypted, the file is safe during transmission (e.g. USB flash drive or Email).

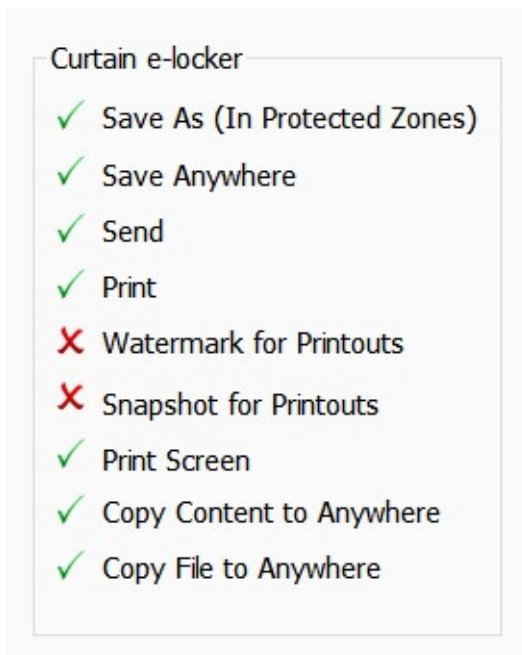


4. When user receives the file, the user simply double-clicks the file. After user enters correct password, the file will be decrypted to destination.

Scenario 3 - Save out without encryption:

When some users need to share protected files with external parties frequently or you don't need to control them to use protected files, then you can allow them to save protected files out of Protected Zone without encrypting the files. This function should be only granted to authorized users. Please refer to FAQ00084 or Section 5.2 in the Installation Guide for the setup.

If a user is allowed to Save Anywhere/Send/Copy File to Anywhere, the user can share non-encrypted files (plaint files) with others. Since the files are not encrypted, users can use the files without Curtain Protection. The major difference between Save Anywhere/Send/Copy File to Anywhere is that Curtain can keep log for Send/Copy File to Anywhere. However, there is no log for Save Anywhere.

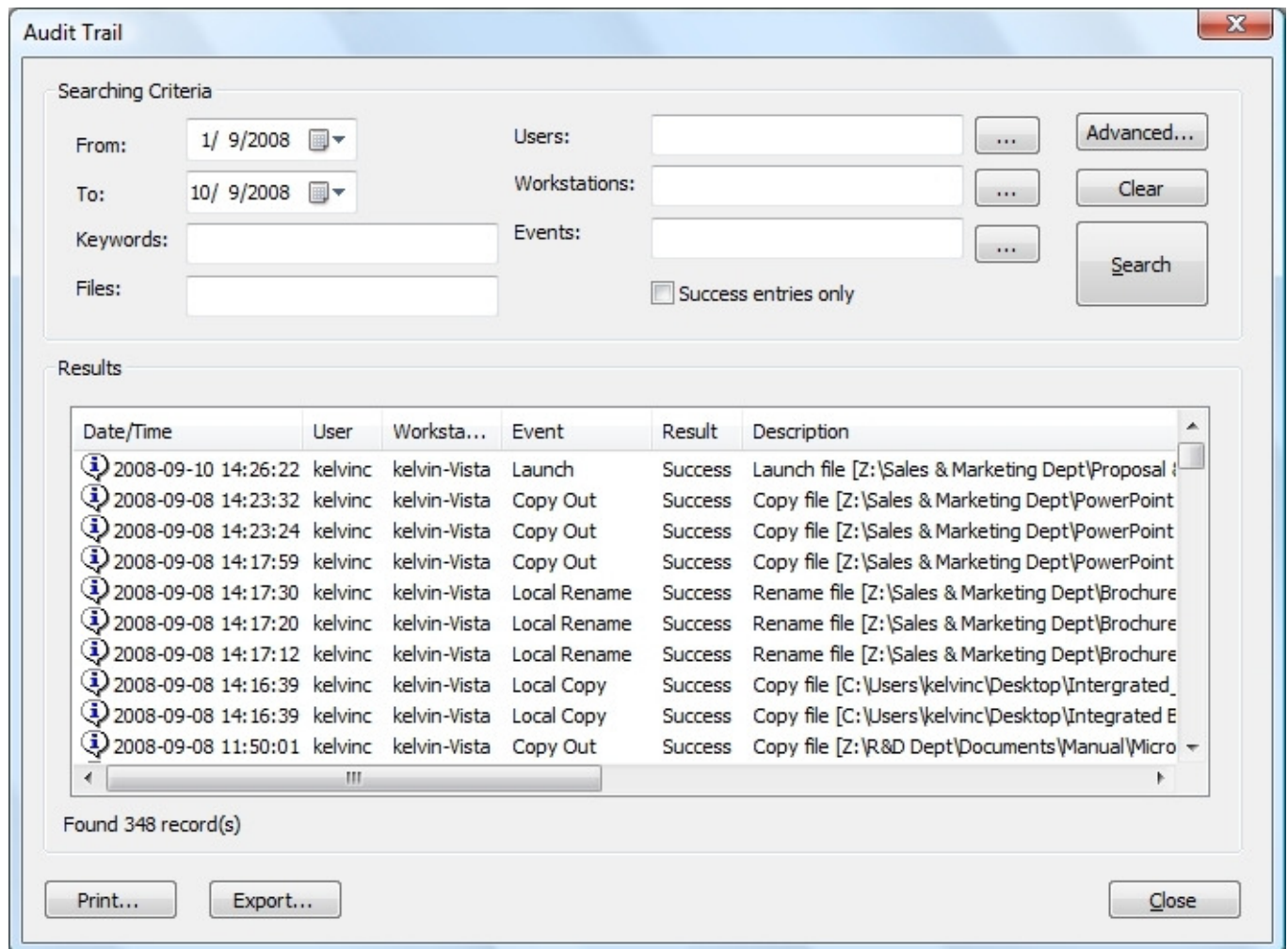


## 6.8 - Audit Trail

Yes, Curtain e-locker has system log. We call it "Audit Trail".

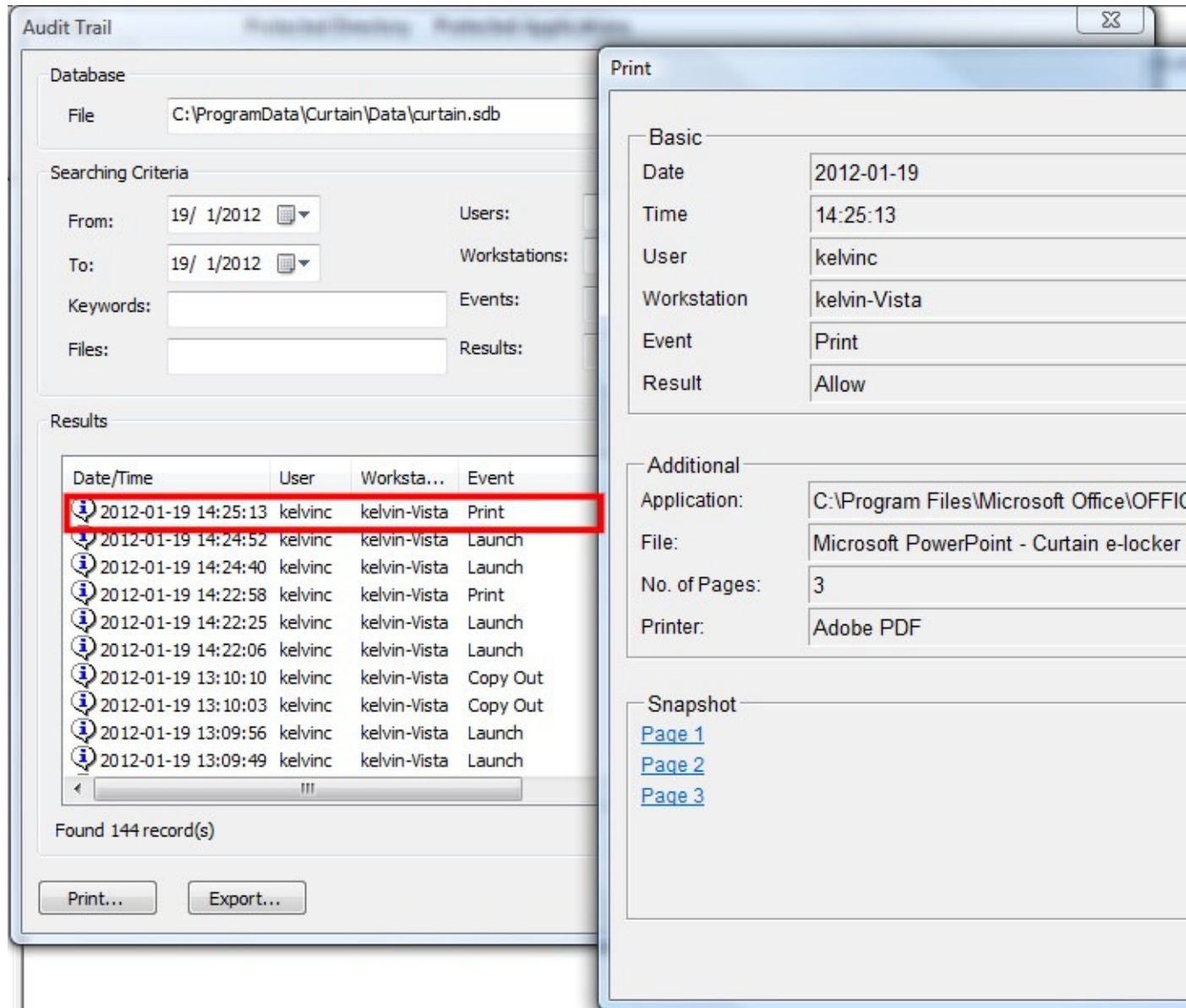
### Steps to view Audit Trail:

1. In Curtain Policy Server, launch Curtain Admin.
2. Click "Audit Trail" button in the Toolbar OR select "File > Audit Trail" in the menu. Then "Audit Trail" window will be shown.





3. If there is "Snapshot for Printouts", you can double-click the entry to view the snapshot.



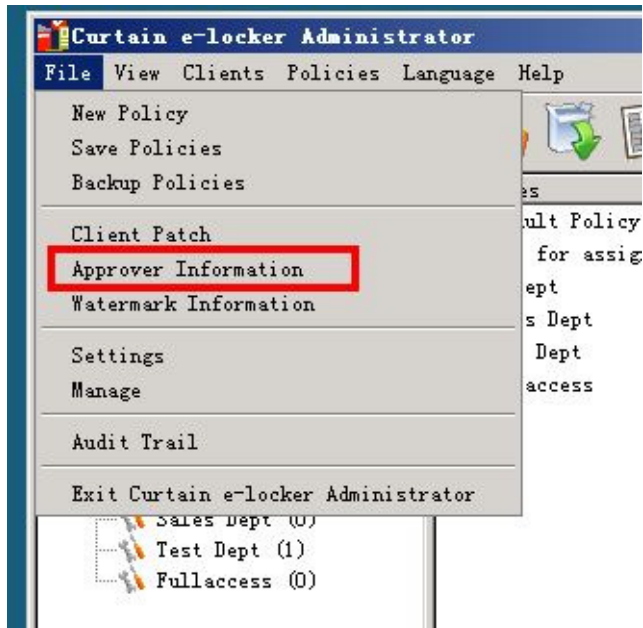


## 6.9 - Send Request

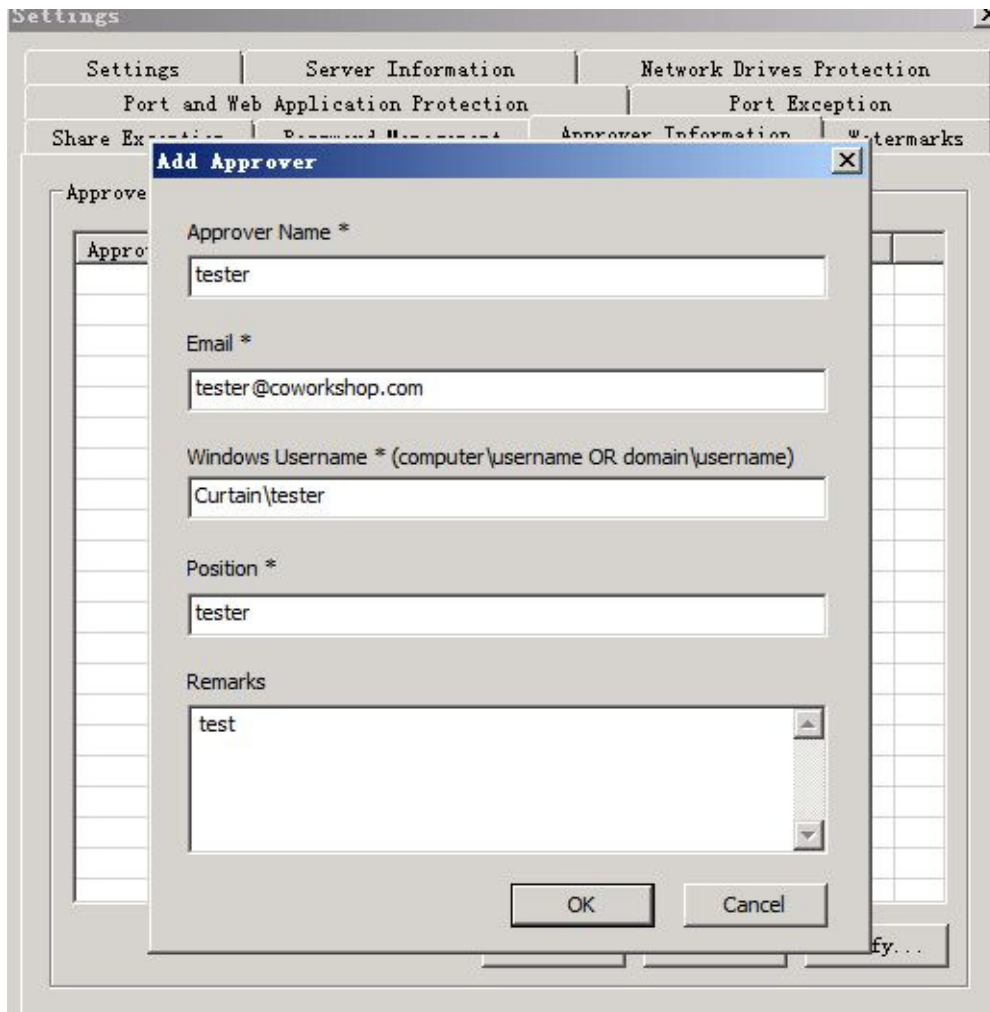
If an unauthorized user needs to share a protected document with external parties, the user can submit a Request for approval. If the request is approved, the system will send the document to requester through email. Since the document is already out of the Protected Zone and not encrypted, requester can share it with external parties without the control of e-locker. The whole approval process will be logged in Audit Trail. This function is called Send Request.

### Steps to define Approver Information:

1. In Curtain Admin, select "File > Approver Information".



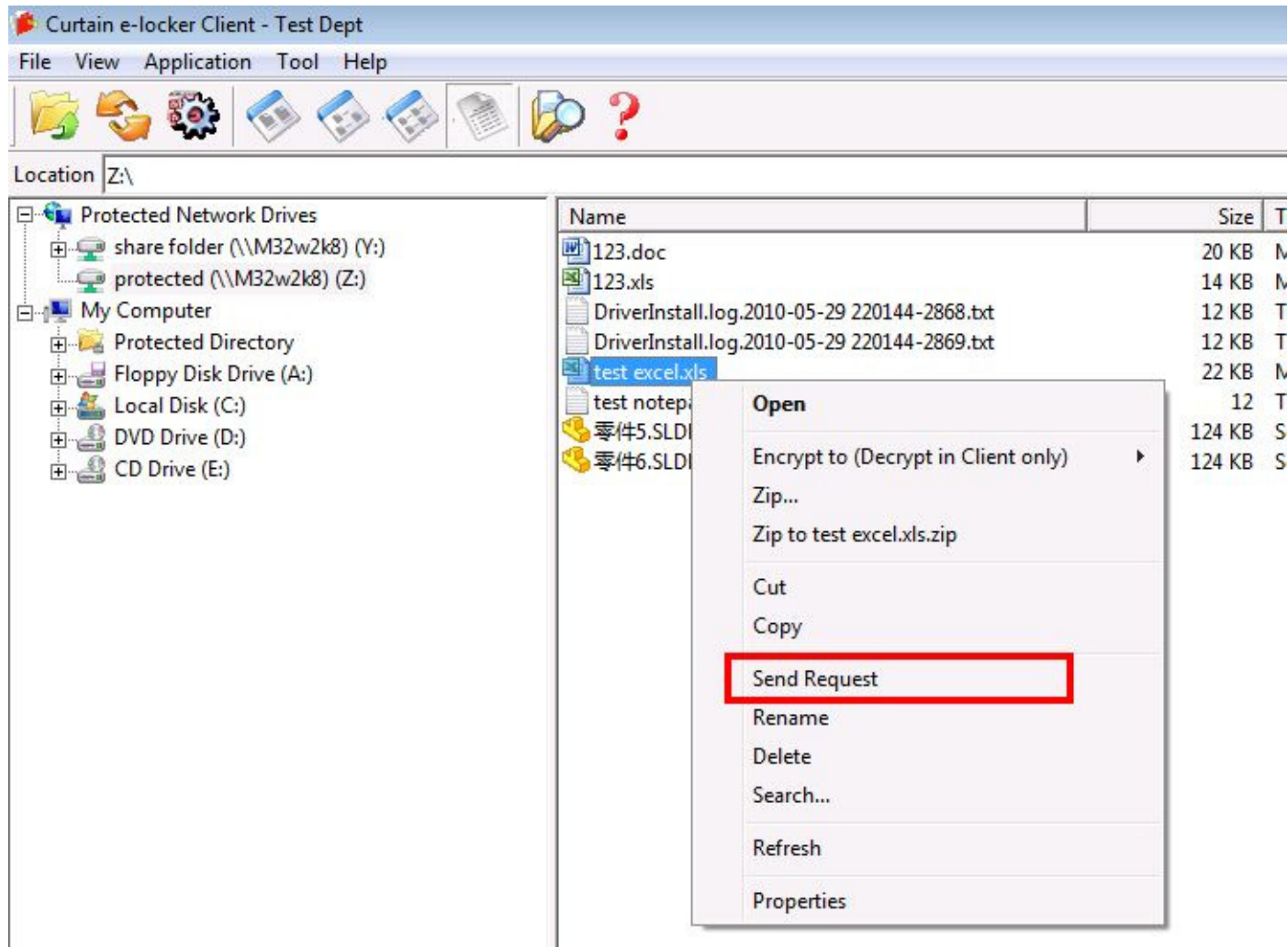
2. Click "Add" button to add approver.
  - Enter the approver's name, email, and position.
  - For the field of Windows Username, please enter "computer\username" OR "domain\username" (such as, M32w2k8-PC\Administrator and Curtain\Tester).



P.S. In order to submit/approve Request, Curtain Client must be installed on approver/requester's workstation.

### Steps to submit a Request:

1. In Curtain Client, select protected document(s) and right-click to select "Send Request"



P.S.

- selecting folder is not supported.
- multiple files are supported (using Ctrl to select more than 1 file).

2. Enter reason and select an approver.

| Approver N... | Email        | Windows U... | Position | Rem  |
|---------------|--------------|--------------|----------|------|
| tester        | tester@co... | Win732en...  | tester   | test |

3. After filling out the form, click "OK".

Then, a draft email will be created by using your default Mail client. Currently, we support Microsoft Office Outlook, Outlook Express, and Windows Mail. An attachment named "SendFile.curtain2" will be automatically attached to the draft email. User can simply click "Send" button to submit the request to the selected approver.

---

```
Requester:
    jant shen

Request Files:
    C:\ProtDir\JANT\test excel.xlsx

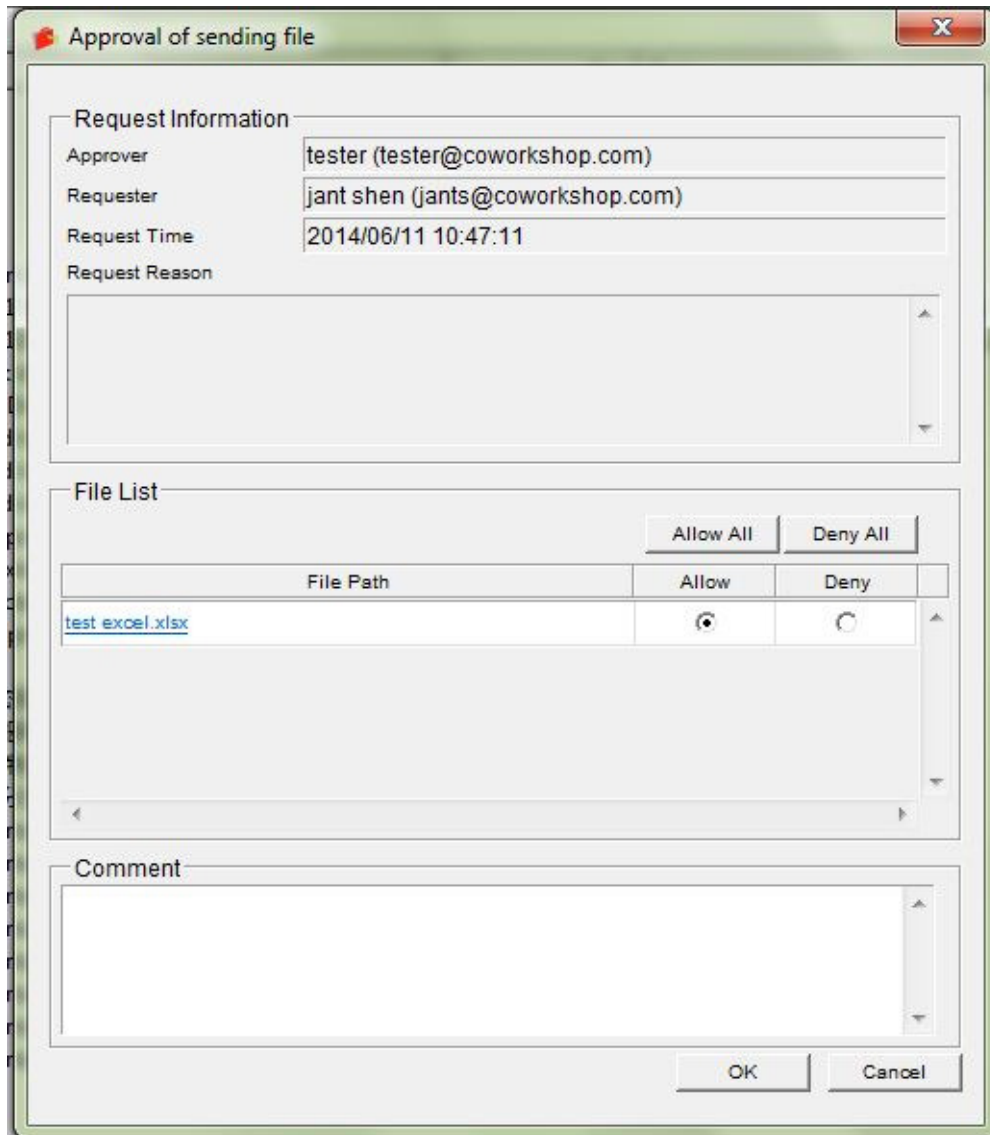
Request Reason:

    Please approval.
```



### Steps to approve/reject a Request:

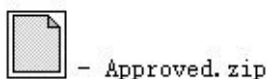
1. When approver receives the email, there is an attachment named "SendFile.curtain2". Approver can double-click this attachment. Then, a dialog box will be shown with requester information and the reason why he/she needs to get the file(s). The approve can decide to approve/reject the request.



The system will compare current Windows logon user to check approver's identity. If it is different from the record, attachment "SendFile.curtain2" cannot be opened.

2. Select Allow or Deny, and write down the comment if any.
3. Click "OK" to confirm.

Then, a draft email will be created by using the default Mail client. If the Request is approved, an attachment named "Approved.zip" will be automatically attached to the draft email. Approver can simply click "Send" button to send the result to the requester. Since the document is already out of the Protected Zone and not encrypted, requester can share it with external parties without the control of e-locker.



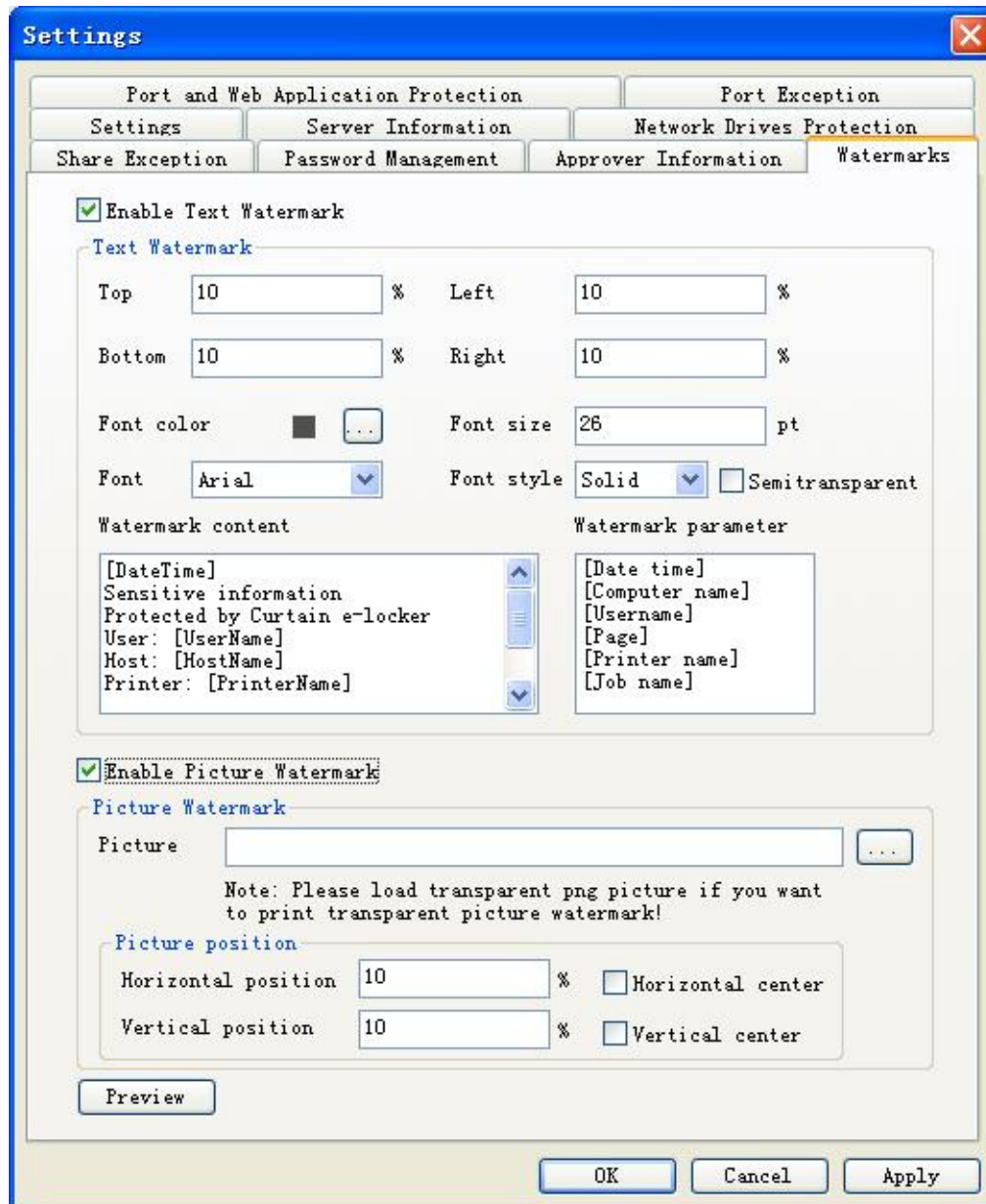
- Approved.zip

## 6.10 - 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. In Curtain Admin, select "File > Watermark Information".

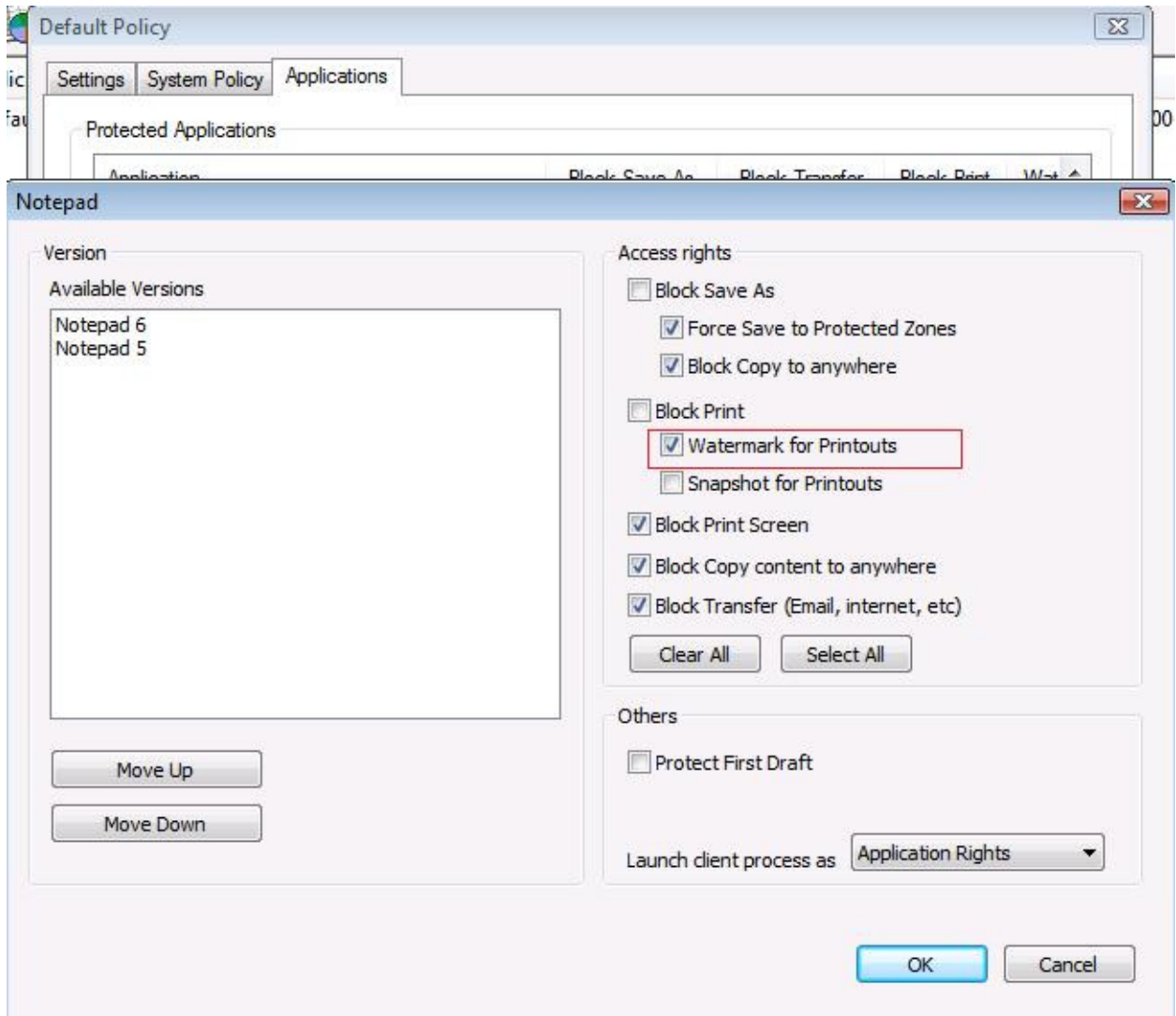


2. When finish your watermark, Click OK to confirm.

### Steps to enable Watermark for an application in a Policy Group:

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

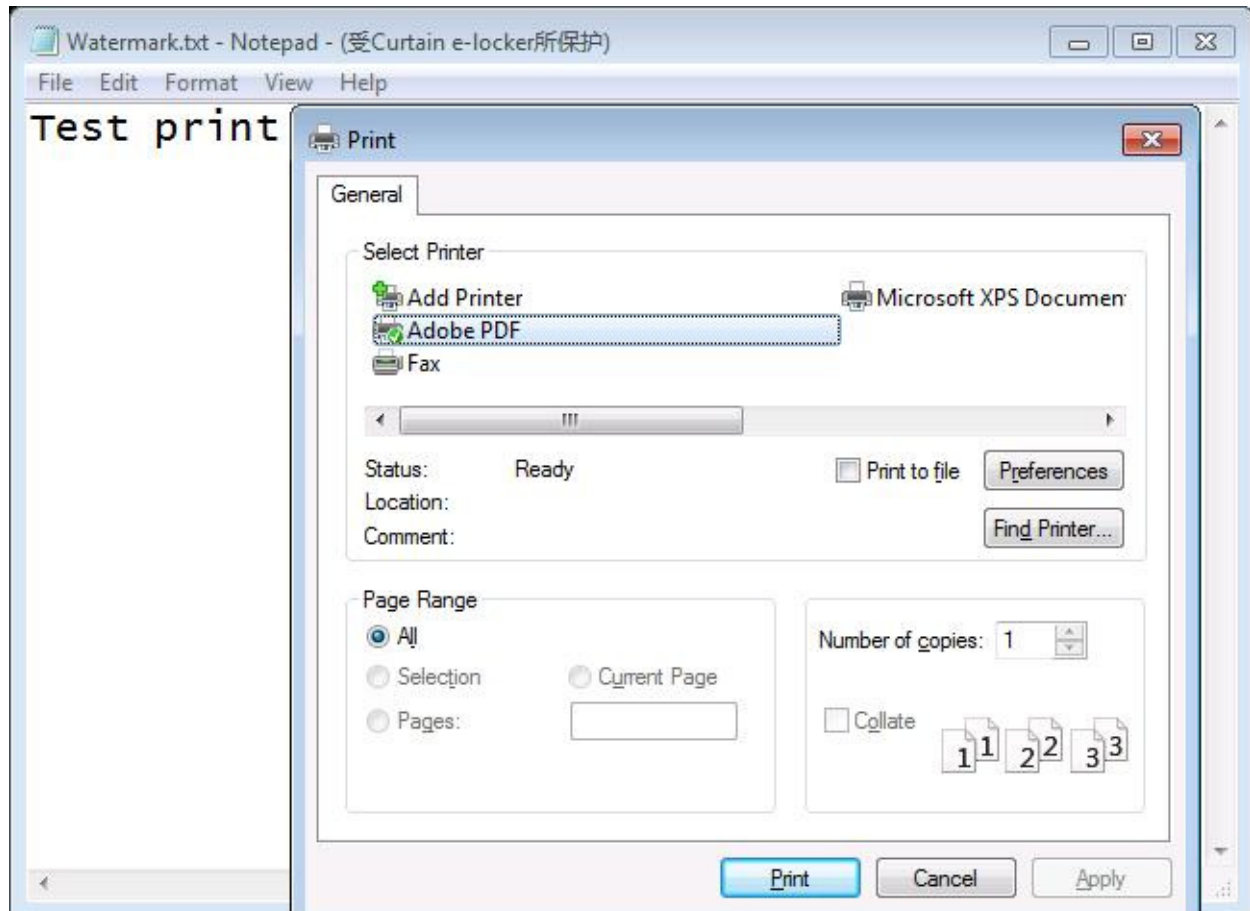
2. In Applications tab, double-click the application which you want to enable "Watermark for Printouts".



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

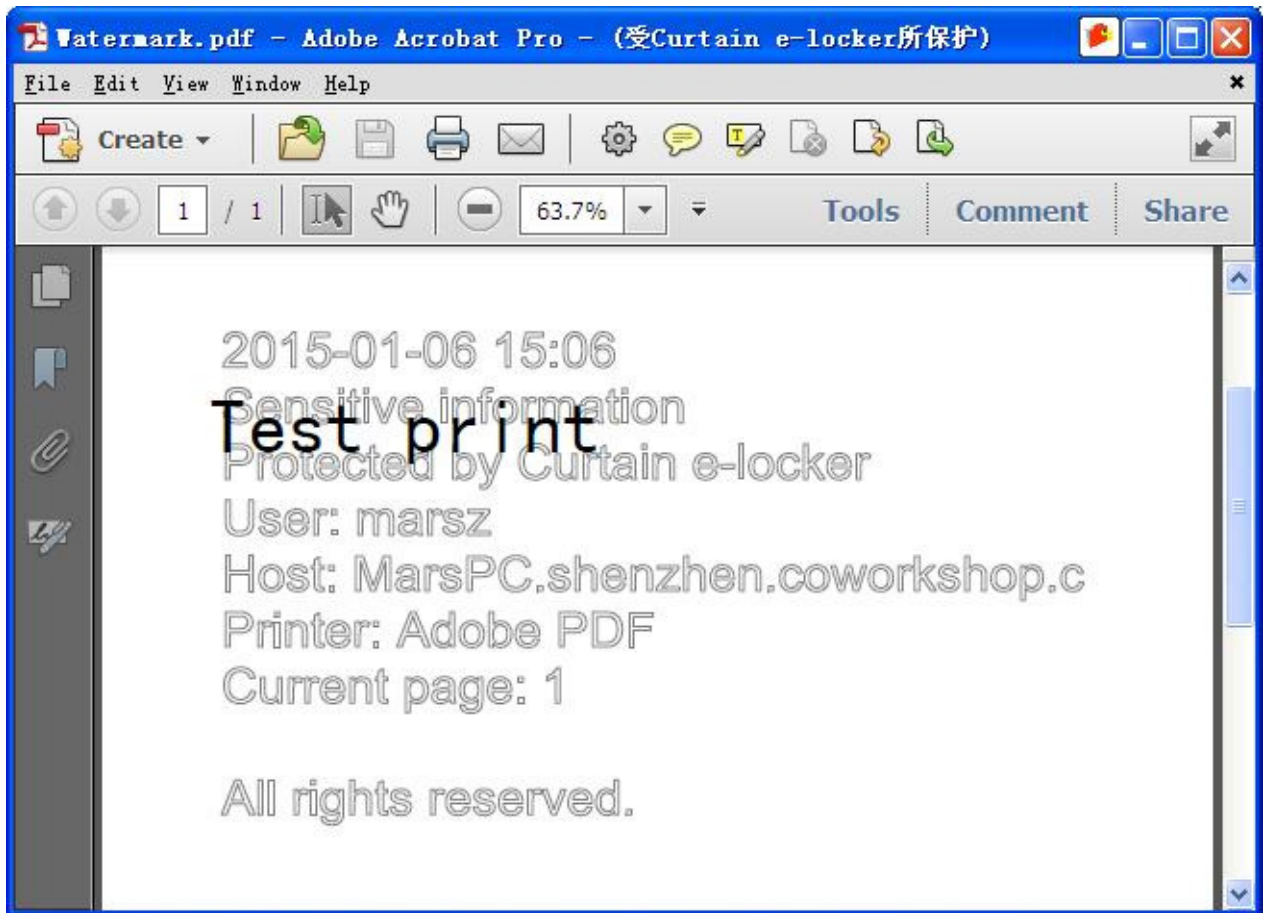
Examples of Watermark:

As a result, a watermark will be added when users use that application to print protected documents.





If "print-to-pdf" is used, watermark will be also added to the newly generated PDF document.

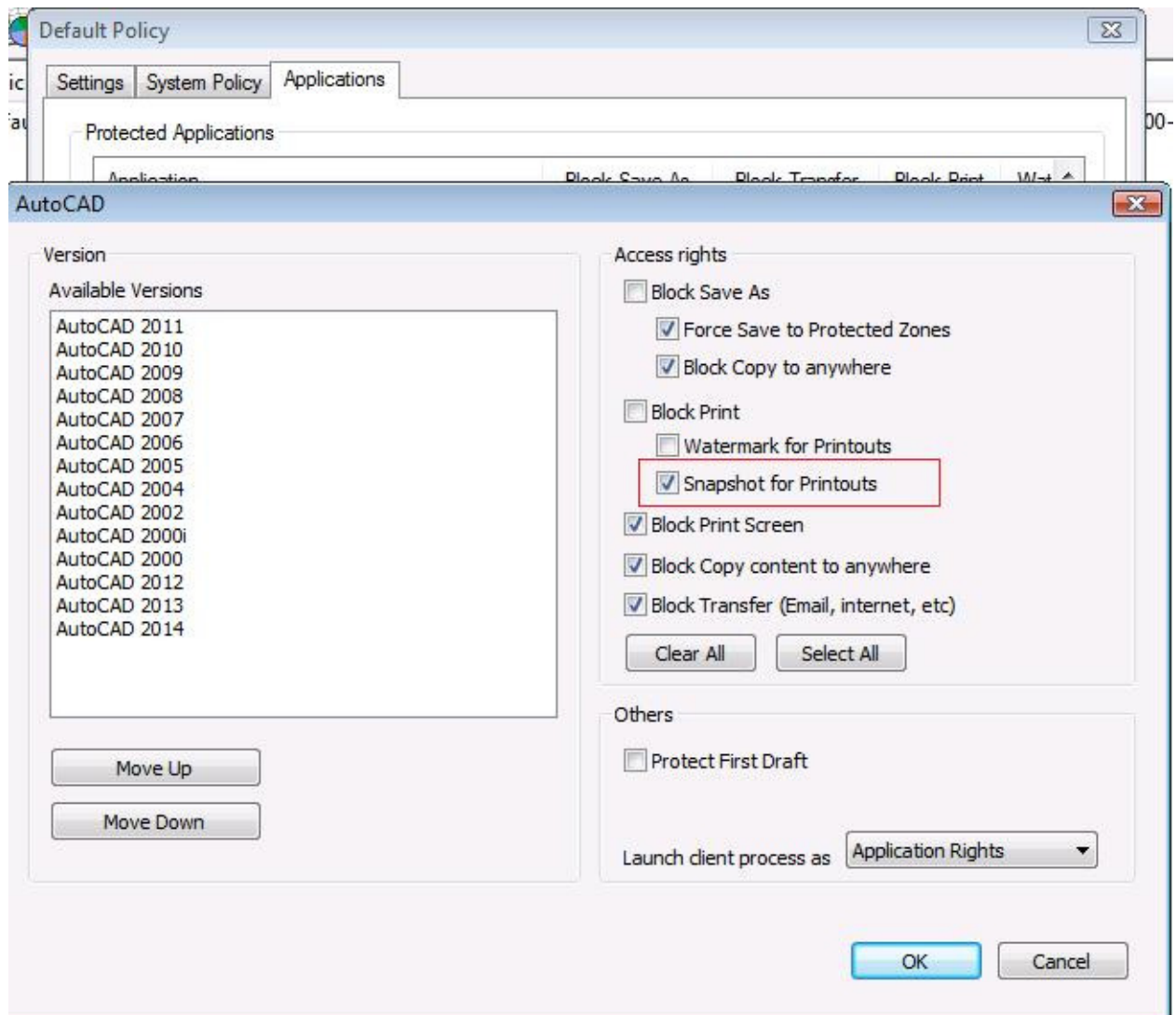


## 6.11 - Snapshot for printouts

By default, Curtain e-locker has a print log for administrators to keep track which documents users printed out. However, administrators can only guess what kind of information was printed by the filename stated in the print log. If administrators want to know exactly what contents were printed by users, they can enable this function - "Snapshot for printouts". When this function is enabled, the system will take snapshot for all printout documents and store them in the format of JPG. Administrators can see what exactly was printed in Audit Trail.

[Steps to enable Snapshot for Printouts for an application:](#)

1. In Curtain Admin, select a Policy Group and right-click to select "Properties".
2. In Applications tab, double-click the application which you want to enable "Snapshot for Printouts".



3. Select "Snapshot for Printouts" and click OK to confirm.

P.S. When this function is enabled, please be careful about the size of system log.

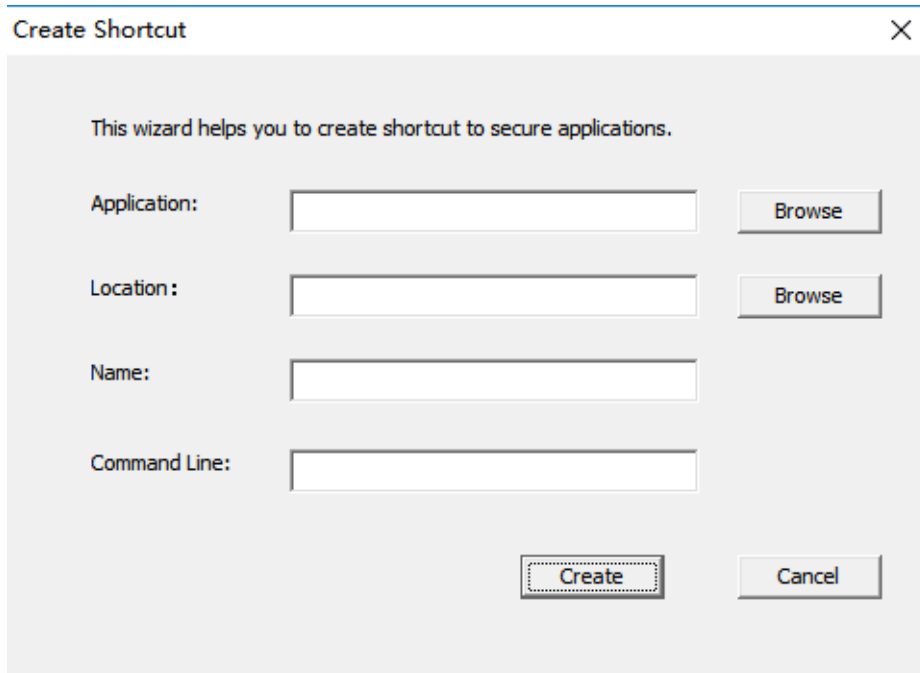
## 6.12 - Create shortcut for protected application

Users can launch Curtain e-locker protected application by using the menu in Curtain Client. Users can also create shortcut for launching a protected application. Please refer to the steps below.

[Steps to create shortcut for protected application :](#)

1. In Curtain Client, select "Tool > Create Shortcut".

Then, "Create Shortcut" dialog box will be shown as below.



**Create Shortcut** [X]

This wizard helps you to create shortcut to secure applications.

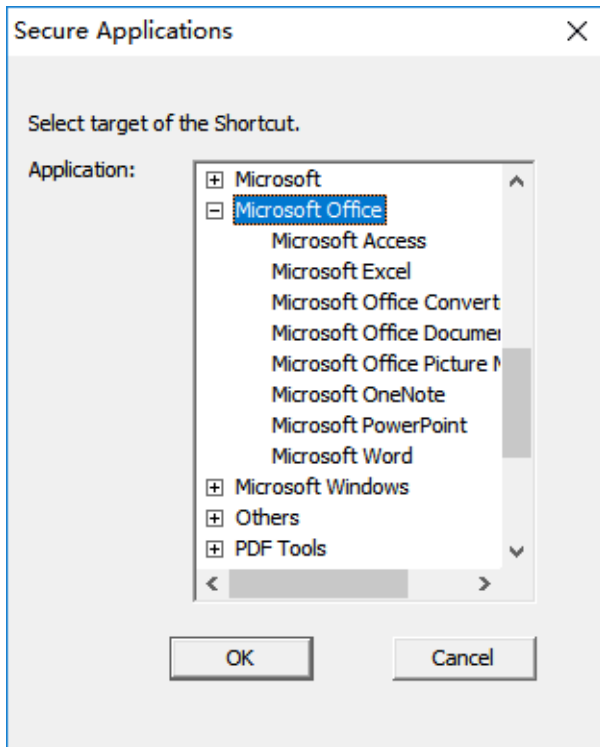
Application:

Location:

Name:

Command Line:

2. Use "Browse" button to select application for which you want to create shortcut. And then, click OK to confirm.



P.S. the selected application must be already installed on the workstation.

3. Use "Browse" button to select the location of shortcut. And then, click OK to confirm.
4. Click "Create" button to create the shortcut.
5. Done.

## 6.13 - Local Encrypted Drive

By default, Local Protected Directory is not encrypted when it is created after installation of Curtain Client. Administrators can enable the function of Local Encrypted Drive to encrypt Local Protected Directory in order to enhance the security. Once Local Encrypted Drive is applied to a workstation, it cannot be rolled-back to non-encrypted local protected directory.

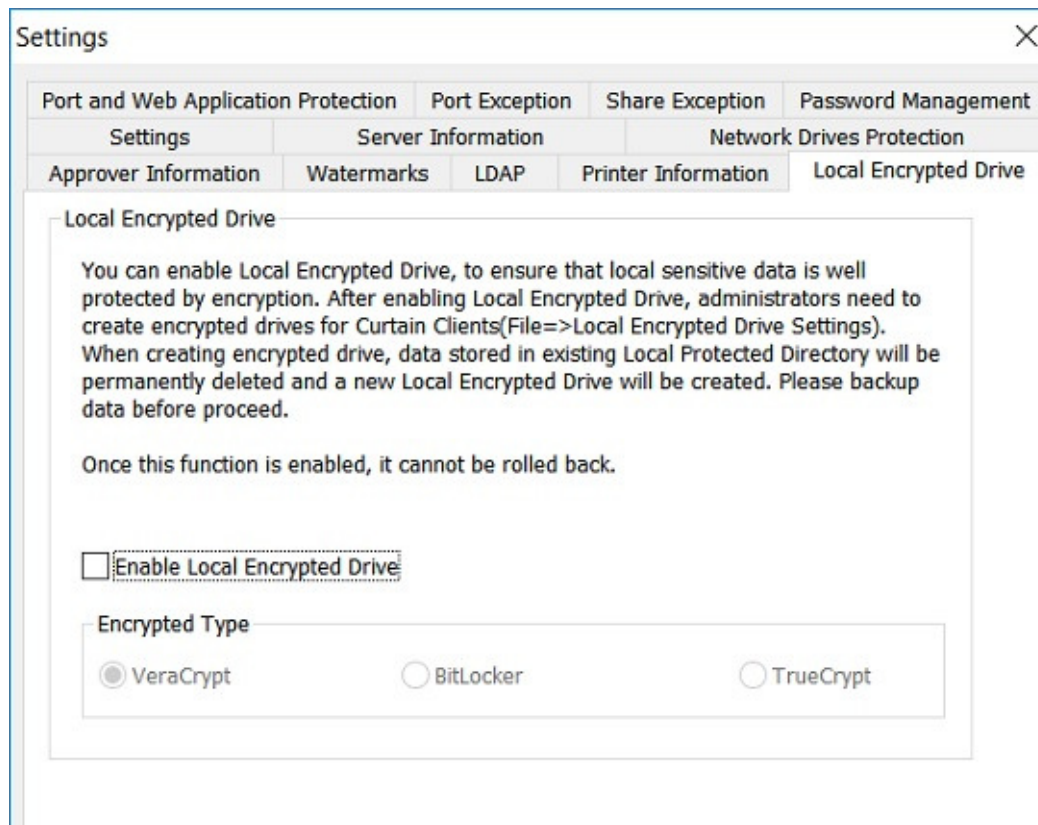
Actually Local Encrypted Drive is a virtual drive. The drive is stored as an encrypted file when the client computer is power off. When the computer startup, the encrypted file will be mounted as a virtual drive. Users can access data stored in the virtual drive normally. Since all the data in the virtual drive is stored as an encrypted file when computer is off, the data is well protected even the computer is lost or stolen. The size of the Local Encrypted Drive will be equal to the size of the encrypted file. Therefore, please make sure that the location for storing the encrypted file has enough free space for the encrypted file. That is the mechanism of Local Encrypted Drive.

[Steps to enable Local Encrypted Drive \(in Curtain Admin\):](#)

1. In Curtain Admin, select "File > Settings".

2. In Local Encrypted Drive tab, check "Enable Local Encrypted Drive" as below.

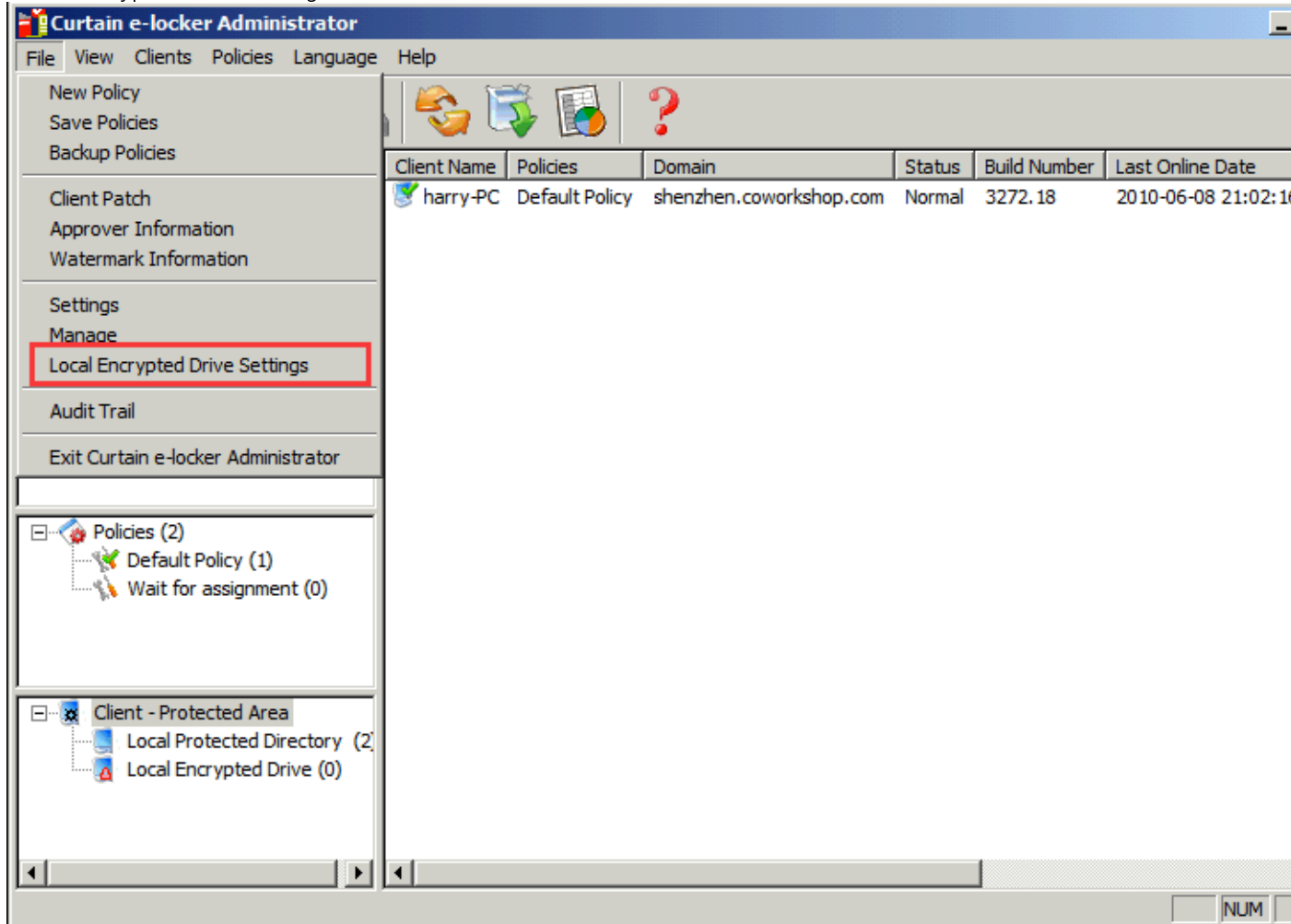
Currently Curtain e-locker supports three well-known encryption tools for encrypting the local protected directory, namely VeraCrypt, BitLocker and TrueCrypt. You can select one of them.



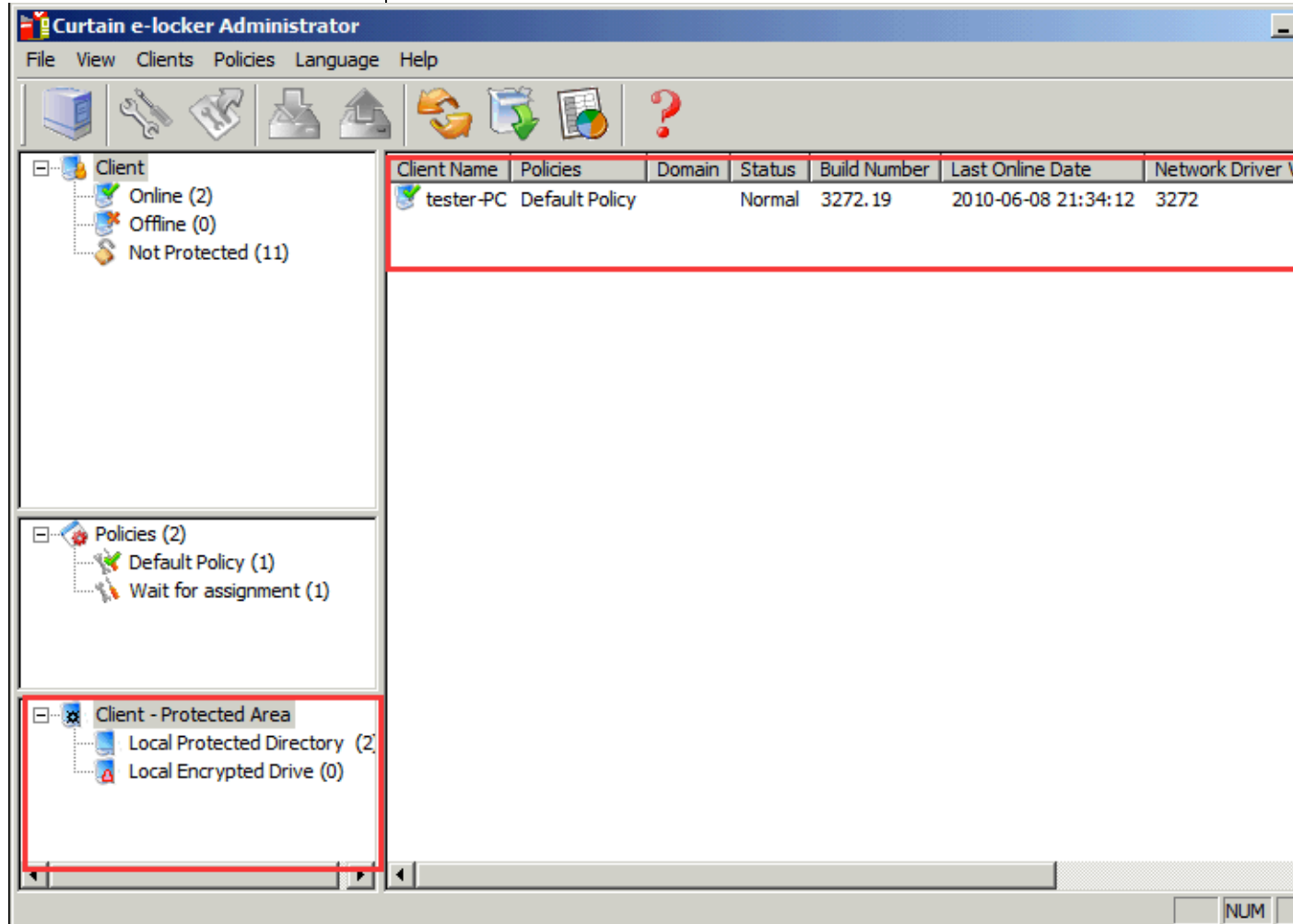
3. Click OK to confirm (Once you click OK to confirm, you cannot disable Local Encrypted Drive).

4. After Local Encrypted Drive is enabled, "Local Encrypted Drive Settings" will display in file menu. Also, "Client - Protected Area" view will be shown in left panel.

"Local Encrypted Drive Settings" in file menu



"Client - Protected Area" view in left panel



"Client - Protected Area" includes two types of clients.

Local Protected Directory - list out all Curtain Clients which are using default local protected directory. It means data in local protected directory is NOT encrypted.

Local Encrypted Drive - list out all Curtain Clients which are using local encrypted drive. It means local protected data is stored in an encrypted drive.

After enabling Local Encrypted Drive, administrators can search clients and create the encrypted drive for them. Please refer to steps below.

#### [Steps to search clients and create default Local Encrypted Drive for them \(in Curtain Admin\):](#)

1. In Curtain Admin, select "File > Local Encrypted Drive Settings".

Then, Local Encrypted Drive Settings dialog box will be shown as below. Administrators can search clients by specific criteria and apply suitable settings to those clients for creating Local Encrypted Drive. For example, you can find out clients which have more than 10GB free space in local drive and then create Local Encrypted Drive with 1GB size for those clients.

**Local Encrypted Drive Settings**

**Search Criteria**

Protected Type:  Local Protected Directory  Local Encrypted Drive

Client Name:  Operate System:

Local Drive:  ... Local Encrypted Drive:

Local Drive Total Space:  MB~  MB Local Drive Free Space:  MB~  MB

Local Encrypted Drive Total:  MB~  MB Local Encrypted Drive Free:  MB~  MB

Search:

Local Encrypted Drive:

**Client List**

| Client Name              | Local Drive | Local Drive Space | Local Encrypted Drive Space | Local Encrypted Drive Status |
|--------------------------|-------------|-------------------|-----------------------------|------------------------------|
| < <input type="text"/> > |             |                   |                             |                              |

Tips: Double click on the client item to view more details, including more local drive and encrypted drive information. Search result:0

The following is detailed description of each search criteria:

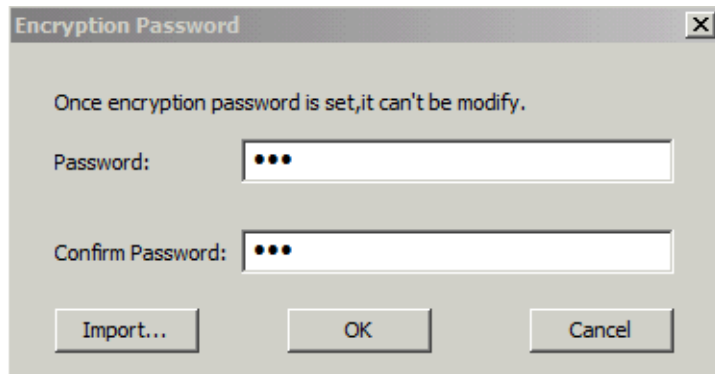
- Protected Type: Local Protected Directory or Local Encrypted Drive
- Client Name: Computer name of the client (support fuzzy search)
- Operating System: Enter the operating system keywords, such as Vista
- Local Drive: Search for clients which have specific local drive letter
- Local Drive Total Space: Search for clients which have specified range of total disk space of local drive
- Local Drive Free Space: Search for clients which have specified range of free disk space of local drive
- Local Encrypted Drive Total Space: Search for clients which have specified range of total disk space of local encrypted drive
- Local Encrypted Drive Free Space: Search for clients which have specified range of free disk space of local encrypted drive



- Local Encrypted Drive Status: Status of local encrypted drive, including:
  - "All": all status
  - "Have not got settings": clients have not received the settings about creating local encrypted drive from Curtain Admin
  - "Have got settings": clients have received the settings about creating local encrypted drive from Curtain Admin
  - "Create failed": clients failed to create local encrypted drive
  - "Create success": clients created local encrypted drive successfully
  - "Mount failed": clients failed to mount local encrypted drive
  - "Mounted success": clients mounted local encrypted drive successfully
  - "To be delete": administrator has submitted request to delete local encrypted drive (only for extend encrypted drive)
  - "Delete failed": clients failed to delete local encrypted drive (only for extend encrypted drive)
  - "Delete success": clients deleted local encrypted drive successfully (only for extend encrypted drive)

2. Click "Encryption Password..." to set password for encryption.

Before you can configure encrypted drive for clients, you must set a password for the encryption.



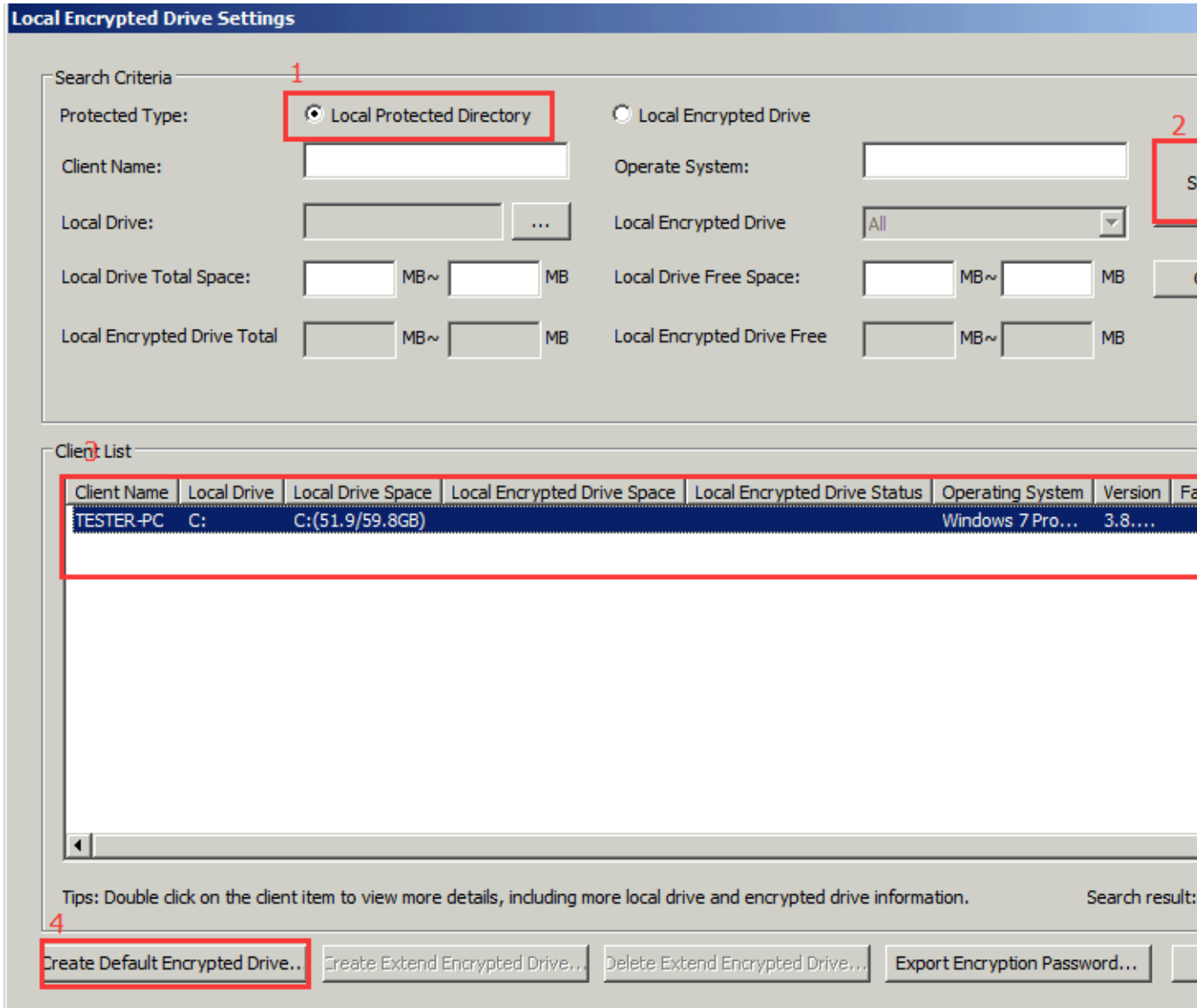
3. Enter password and click OK to confirm.

After click "OK", the system will ask you to back up the password file. Please keep the password file carefully.

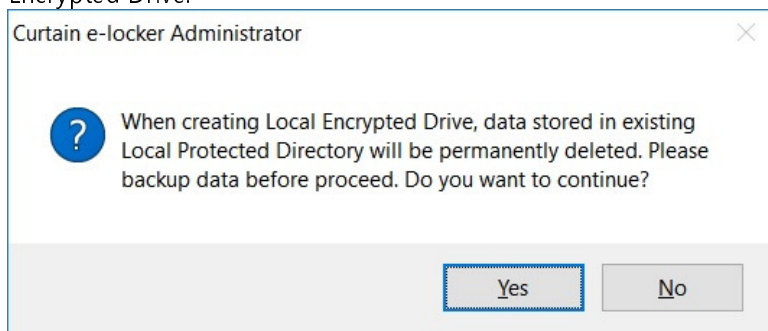
Now, you can find out clients and apply suitable settings to those clients for creating Local Encrypted Drive (described above). For example, you can select Local Protected Directory to search for clients that have not adopted local encrypted drive. Or, you can select Local Encrypted Drive to search for clients that have created local encrypted drive.

4. Select "Local Protected Directory" and click Search button.

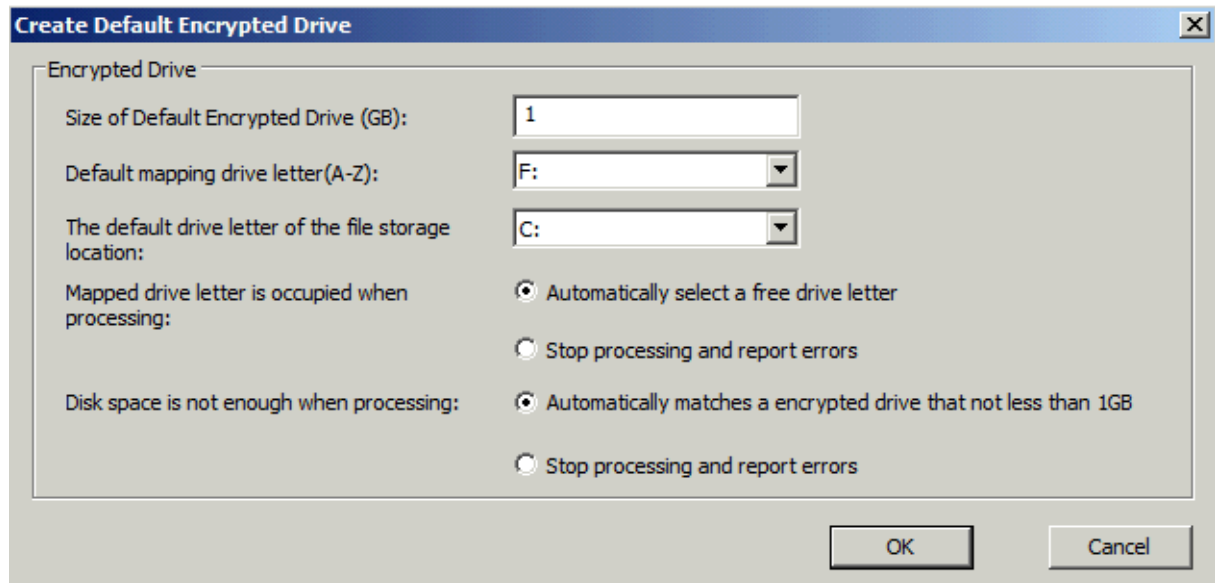
The system will list out all clients which have not adopted Local Encrypted Drive (still using default Local Protected Directory).



5. Select clients and click "Create Default Encrypted Drive..." (use Ctrl button for multiple selection)  
 The system will alert you to backup data stored in Local Protected Directory before upgrading to Local Encrypted Drive.



6. Click Yes to proceed, when you have already backup your data in local protected directory. Then, "Create Default Encrypted Drive" dialog box will prompt as below. You can define suitable settings for creating Local Encrypted Drive for the selected clients.



Settings in "Create Default Encrypted Drive" dialog box:

- Size of Default Encrypted Drive (GB): size of the local encrypted drive you want to create
- Default mapping drive letter (A-Z): default drive letter for mapping the local encrypted drive
- The default drive letter of the file storage location: default drive location for storing the encrypted file of Local Encrypted Drive. Please make sure that the local drive has enough free space for storing the encrypted file.
- Mapped drive letter is occupied when processing: specify the way how to proceed if the Default mapping drive letter is occupied on the client computer
  - Automatically select a free drive letter: the system will automatically mount the local encrypted drive by using a free drive letter
  - Stop processing and report errors: the system will stop to proceed and report error to Curtain Admin
- Disk space is not enough when processing: specify the way how to proceed if the Default Drive for storing the encrypted file has not enough disk space
  - Automatically matches a drive that not less than 1GB: the system will automatically create a 1GB local encrypted drive (instead of the Size specified)
  - Stop processing and report errors: the system will stop to proceed and report error to Curtain Admin

7. Click "OK" to confirm after finishing the settings.

Next time when the Curtain Client opens, the system will prompt the user to create the Local Encrypted Drive.

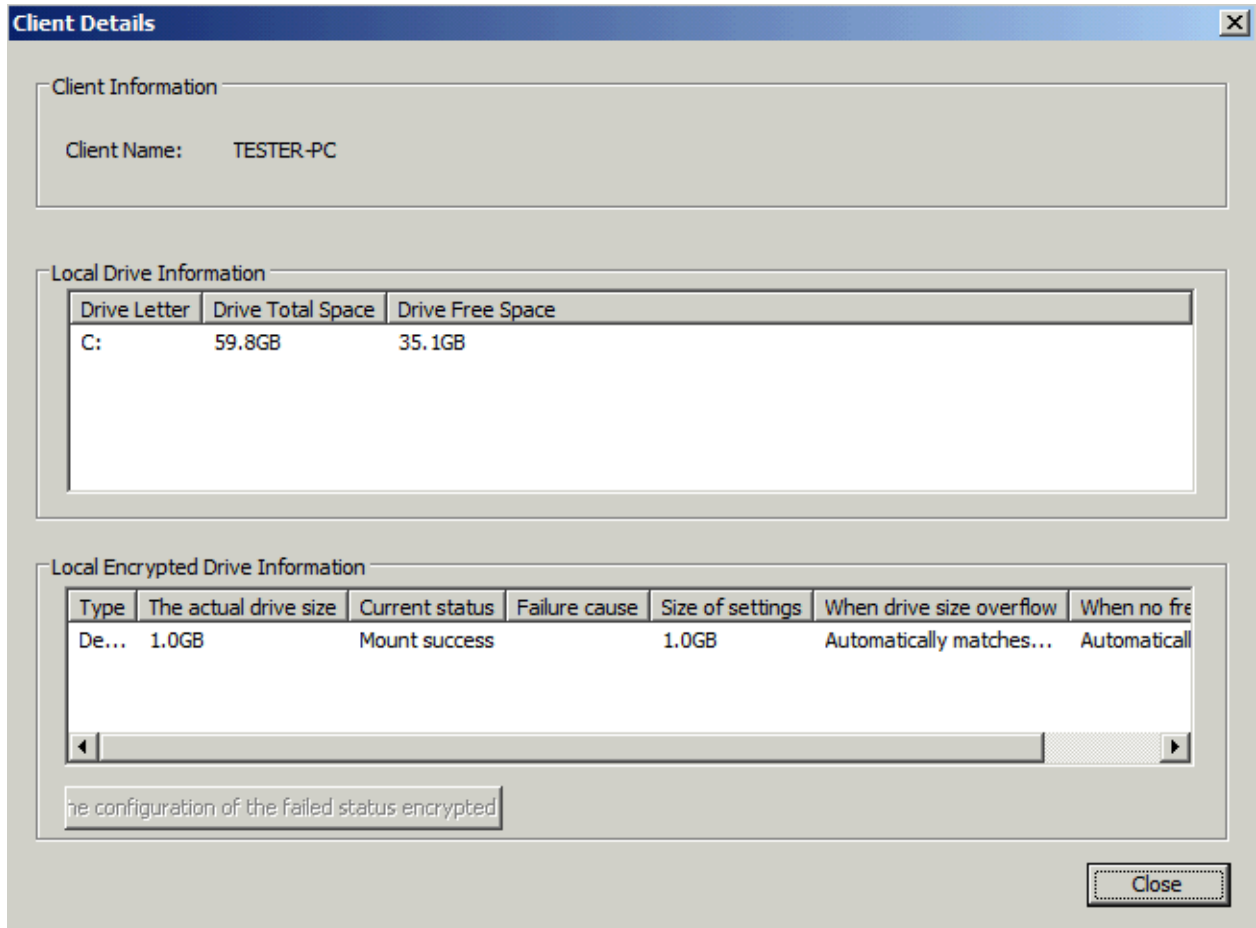
It is just an example for reference:

- Size of Default Encrypted Drive (GB): 10
- Default mapping drive letter (A-Z): F:
- The default drive letter of the file storage location: C:
- Mapped drive letter is occupied when processing: Automatically select a free drive letter
- Disk space is not enough when processing: Automatically matches a drive that not less than 1GB

This example means to create a 10GB size Local Encrypted Drive and mount with F: drive letter. When client computer is off, the encrypted file is stored in C: drive. If C: drive in client computer has no 10GB free space, the system will automatically create a 1GB local encrypted drive. If F: drive letter is occupied, the system will use another available drive letter.

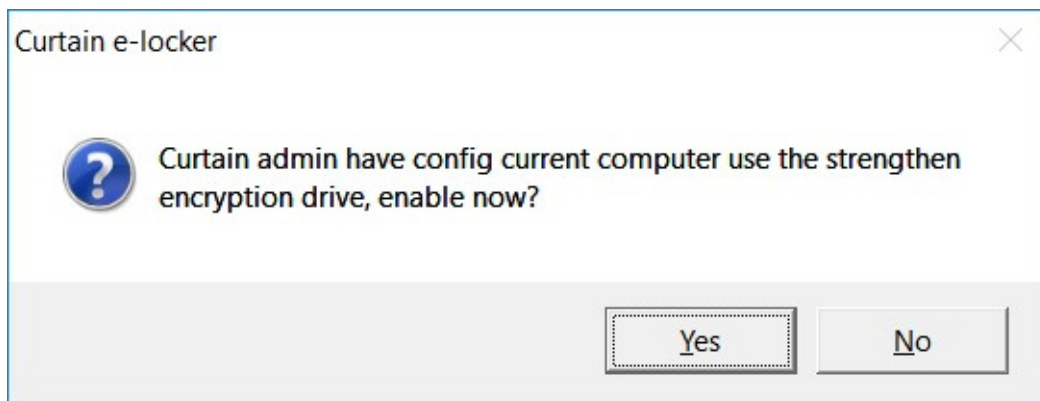
8. Double click a client in "Local Encrypted Drive settings" dialog box, to view detailed information.

This picture shows that Local Encrypted Drive has been created successfully for the client.



#### Steps to finish the creation of Local Encrypted Drive in Curtain Client:

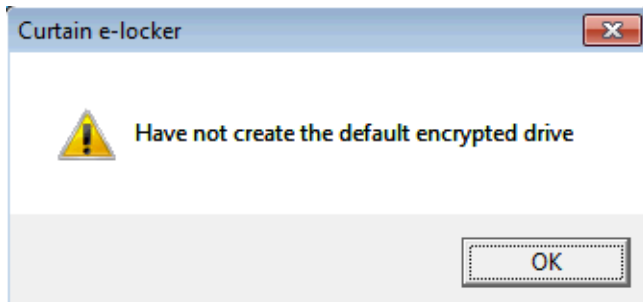
1. Next time when the selected clients open Curtain Client, the system will prompt the users to create Local Encrypted Drive.



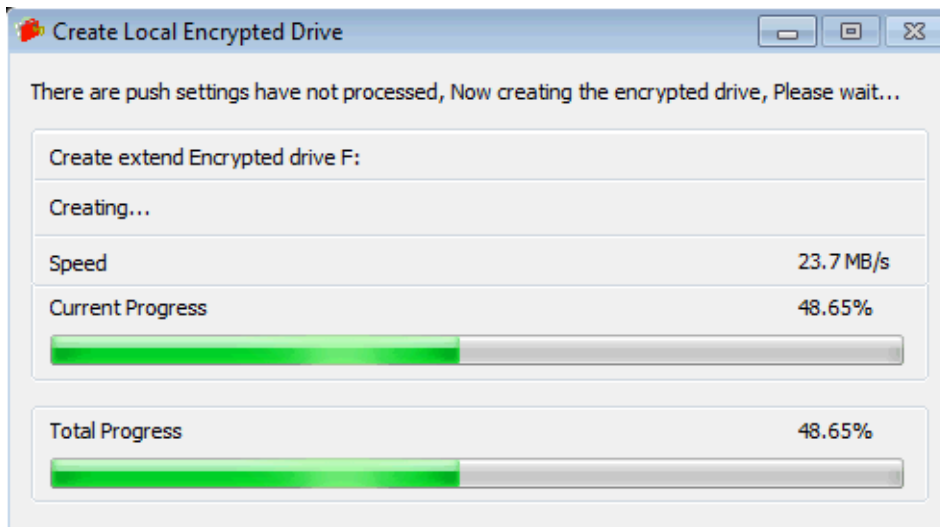
2. Click Yes to create Local Encrypted Drive, or click No to create the drive later.

After clicking Yes, the Local Encrypted Drive will be created in client after rebooting the computer. Please remember to backup data in local protected directory if needed.

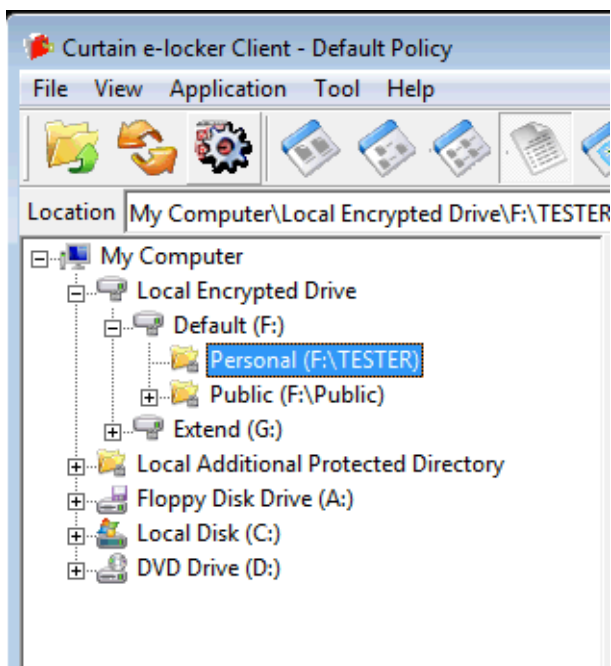
3. Open Curtain Client after rebooting the computer. Then, the system will prompt the user as below.



4. Click OK to proceed. Then, the system will create the Local Encrypted Drive immediately.



5. Done. Here is the interface of Curtain Client after creating Local Encrypted Drive.

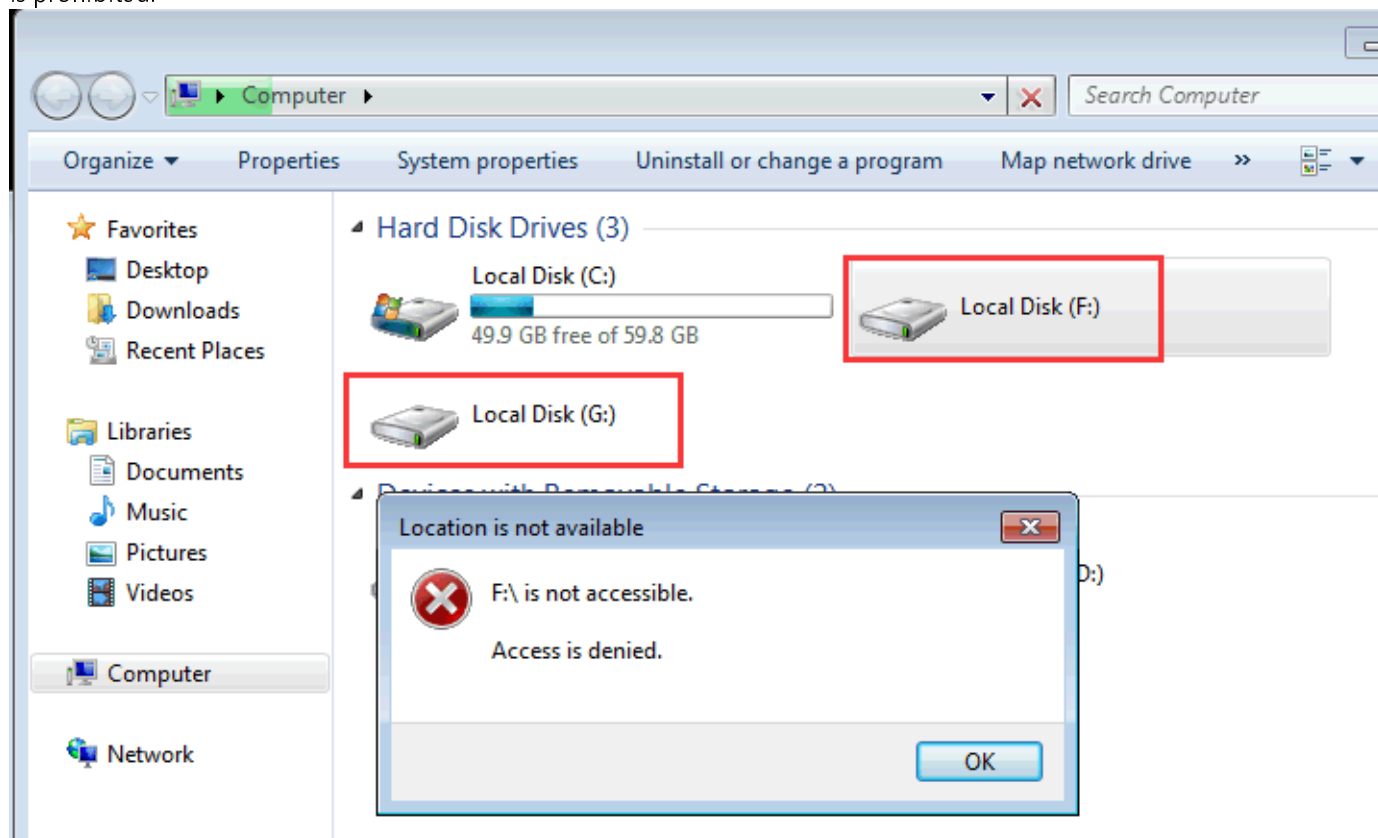


In Curtain Client, "Local Encrypted Drive" is shown under My Computer.

The first Local Encrypted Drive created must be Default local encrypted drive. Administrators can create Extend Local Encrypted Drive for clients as additional encrypted drive. Under local encrypted drive, you can see there are two folders, namely Personal and Public. The Personal folder is for the current login user only, while the Public folder can be used by other users. So, you can use Personal folder for storing your private documents and use Public folder for sharing documents in the client.

If you have Additional Protected Directory before upgrading to Local Encrypted Drive, the additional protected directory will be still there. Local Encrypted Drive is not applicable to additional protected directory.

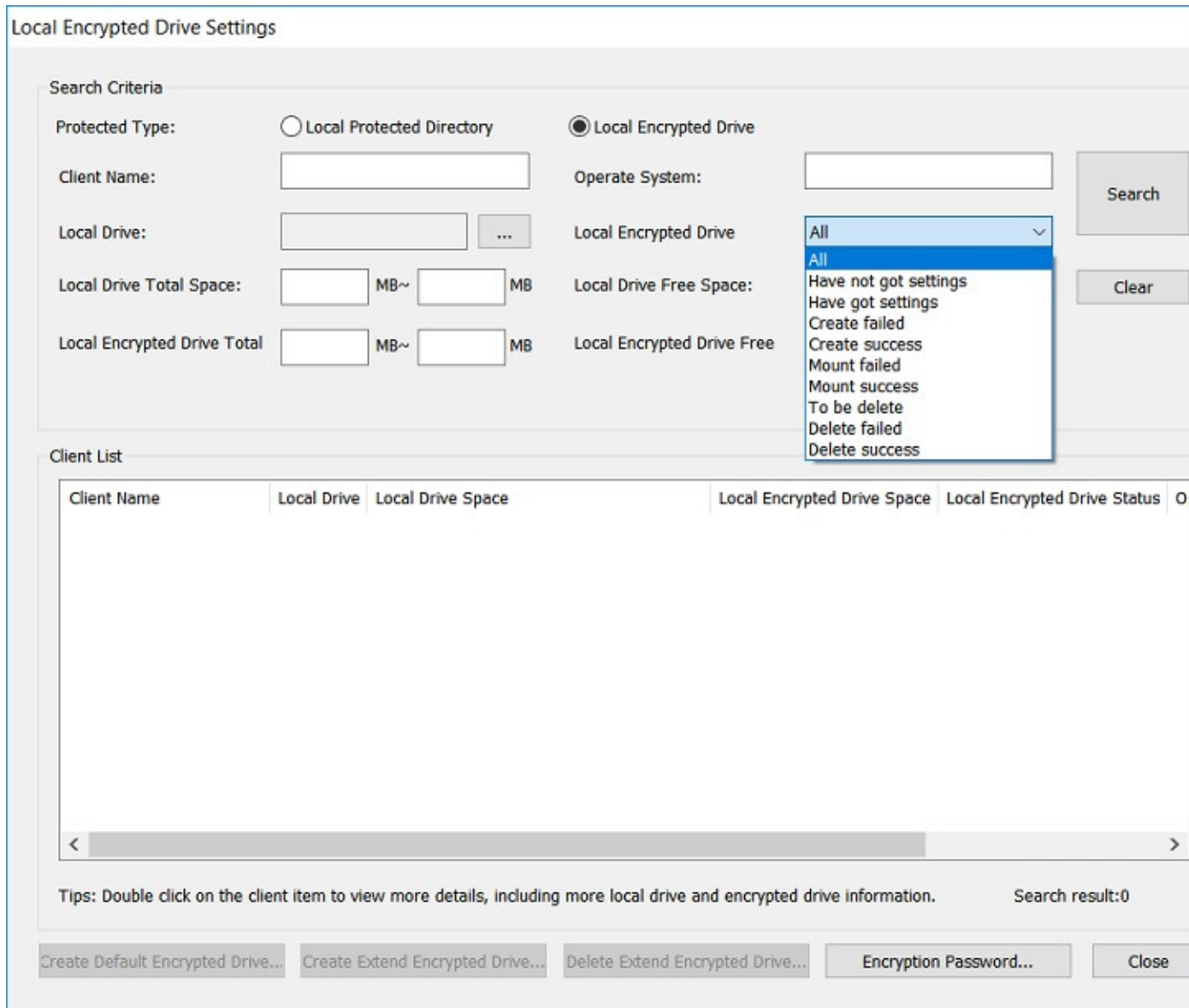
In the example stated above, Drive F: is the Default local encrypted drive, while Drive G: is the Extend local encrypted drive. Users can only access files in Protected Zone (including local encrypted drive) under Curtain e-locker environment, such as Curtain Client or protected application (e.g. Word application having Curtain icon at top right corner). If users try to access local encrypted drive directly in Windows Explorer, it is prohibited.



#### Steps to handle clients which failed to create/mount Local Encrypted Drive (in Curtain Admin):

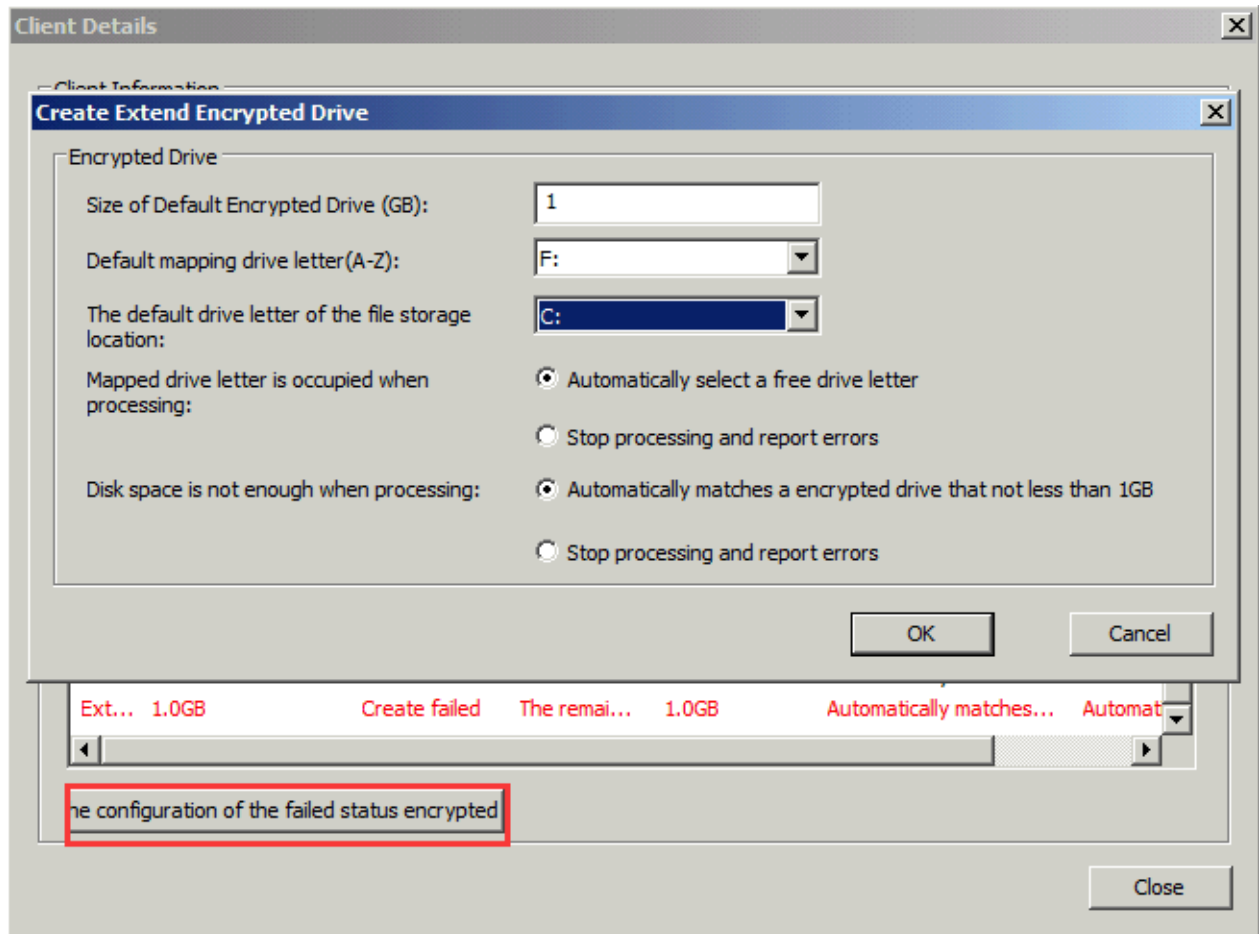
Some clients may fail to create/mount the Local Encrypted Drive, due to many reasons, such as insufficient disk space for storing the encrypted file, or assigned drive letter is occupied. Then, administrators can find out all these clients and fine-tune the settings for creating local encrypted drive again.

1. In Curtain Admin, select "File > Local Encrypted Drive Settings".



2. Select "Local Encrypted Drive" for Protected Type.
3. Select "Mount failed" or "Create failed" for Local Encrypted Drive Status.
4. Click Search to find out all clients which failed to mount/create Local Encrypted Drive.
5. Double-click a client to open Client Details dialog box.

6. Click the button as picture below, to change settings of Local Encrypted Drive.



7. Click "OK" to confirm after finishing the settings.

Next time when the Curtain Client opens, the system will prompt the user to create the Local Encrypted Drive again.

#### [Steps to search clients and create Extend Local Encrypted Drive for them \(in Curtain Admin\):](#)

Administrators may need to create Extend Local Encrypted Drive, due to many reasons, such as default local encrypted drive is almost full. Then, administrators can create extend local encrypted drive for those clients.

1. In Curtain Admin, select "File > Local Encrypted Drive Settings".

Then, Local Encrypted Drive Settings dialog box will be shown as below. Administrators can search clients by specific criteria and apply suitable settings to those clients for creating Extend Local Encrypted Drive. For example, you can find out clients which have less than 500MB free space in Local Encrypted Drive.

2. Enter criteria and click Search button.

3. Select clients and click "Create Extend Encrypted Drive..." (use Ctrl button for multiple selection)



The steps of creating extend local encrypted drive is quite similar to the steps of creating default local encrypted drive. You may refer to the procedures of creating default local encrypted drive.

**Local Encrypted Drive Settings**

Search Criteria

Protected Type:  Local Protected Directory  Local Encrypted Drive

Client Name:

Local Drive:  ...

Operate System:

Local Encrypted Drive:

Local Drive Total Space:  MB ~  MB

Local Drive Free Space:  MB ~  MB

Local Encrypted Drive Total:  MB ~  MB

Local Encrypted Drive Free:  MB ~  MB

Client List

| Client Name | Local Drive | Local Drive Space | Local Encrypted Drive Space | Local Encrypted Drive Status | Operating System | Version | Fa |
|-------------|-------------|-------------------|-----------------------------|------------------------------|------------------|---------|----|
| TESTER-PC   | C:          | C:(49.9/59.8GB)   | F:(0.9/1.0GB),G:(0.9/1.0... | F:Mount success,G:Mount...   | Windows 7 Pro... | 3.8...  |    |

Tips: Double click on the client item to view more details, including more local drive and encrypted drive information. Search result:

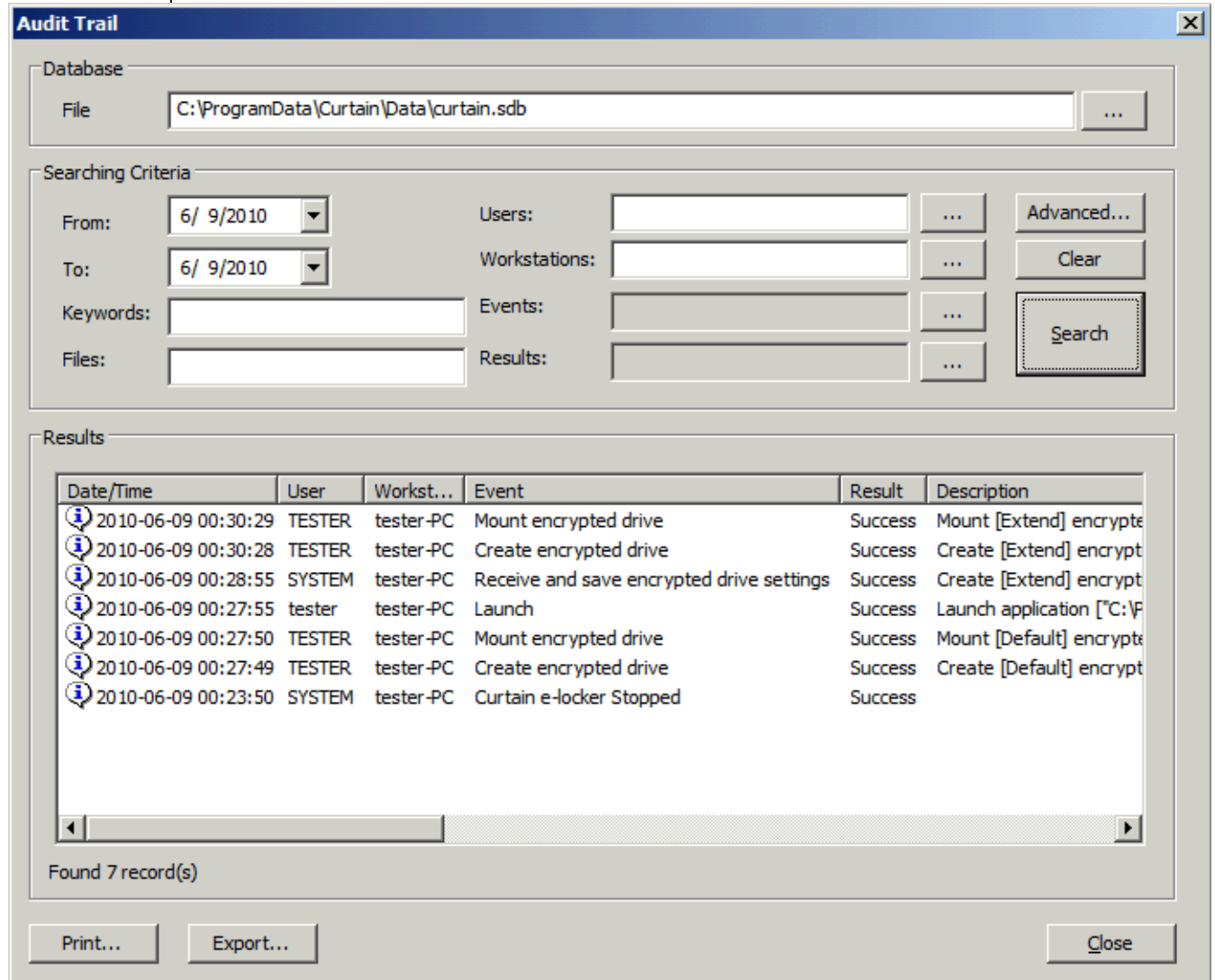
Create Default Encrypted Drive... **Create Extend Encrypted Drive...** Delete Extend Encrypted Drive... Export Encryption Password...

[Steps to review audit log for Local Encrypted Drive \(in Curtain Admin\):](#)

All the activities of Local Encrypted Drive (e.g. create/mount default local encrypted drive, remove extend local encrypted drive, and etc) will be logged for audit trail purpose.

1. In Curtain Admin, select "File > Audit Trail".
2. Enter criteria and click Search.

Here is an example.



## 6.14 - Set login password for Curtain Admin, Server Plug-in and Client

By default, users do not need to enter password for launching Curtain Admin, Server Plug-in or Client. Administrators can enable password protection to enhance the security of those programs.

[Steps to enable login password for Curtain Admin:](#)

1. In Curtain 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 Admin, a dialog box will be shown for entering new password. Otherwise, the last password will be used.

The screenshot shows the 'Settings' dialog box with the 'Password Management' tab selected. The 'Administrator Password Management' section is highlighted with a red box, showing the 'Password Protection' checkbox checked and a 'Reset Password' button below it. Other sections include 'Client Password Management' with options for 'No Password', 'By Client', 'Custom Password', and 'USB Token', and 'Server Plug-in Password Management' with options for 'No Password' and 'By Server Plug-in'. The 'Uninstall Password' section has a 'Password Protection' checkbox. The dialog box has 'OK', 'Cancel', and 'Apply' buttons at the bottom.

| Approver Information                | Watermarks         | LDAP            | Printer Information       | Local Encrypted Drive |
|-------------------------------------|--------------------|-----------------|---------------------------|-----------------------|
| Settings                            | Server Information |                 | Network Drives Protection |                       |
| Port and Web Application Protection | Port Exception     | Share Exception | Password Management       |                       |

**Client Password Management**

Login Password

No Password

By Client

Custom Password

USB Token

**Uninstall Password**

Password Protection

**Administrator Password Management**

Password Protection

Reset Password

**Server Plug-in Password Management**

No Password

By Server Plug-in

OK Cancel Apply

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



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

#### [Steps to enable login password for Curtain Server Plug-in:](#)

1. In Curtain Admin, select "File > Settings".

2. In Password Management tab, select "By Server Plug-in" and click "OK" to confirm.

If it is the first time to set password for a Curtain Server Plug-in, a dialog box will be shown for entering new password next time when launching Curtain Server Plug-in. Otherwise, the last password will be used.

#### [Steps to enable login password for Curtain Client:](#)

1. In Curtain Admin, select "File > Settings".

2. In Password Management tab, select "By Client". There are two options under "By Client".

Custom Password - Users will be asked to enter new password next time when launching Curtain Client.

USB Token - Users will be asked to insert USB Token with digital certificate next time when launching Curtain Client.

3. Click "OK" to confirm.

4. If both "Custom Password" and "USB Token" are selected, users can decide to set password or use token for signing in Curtain Client.

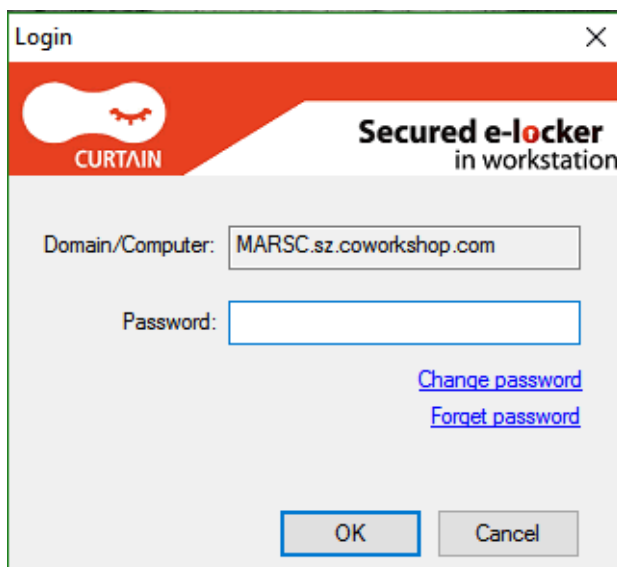


## 6.15 - Change or reset login password for Curtain Admin, Server Plug-in and Client

If administrators have enabled password protection for Curtain Admin, Server Plug-in or Client, users must enter password for launching corresponding program. If users want to change or reset the password, please refer the procedures stated below.

[Steps to change or reset password for Curtain Admin/Server Plug-in/Client:](#)

1. Click "Change password" when you are asked to enter password for launching Curtain Admin, Server Plug-in or Client.



Then, "Set Password" dialog box will be shown as below.

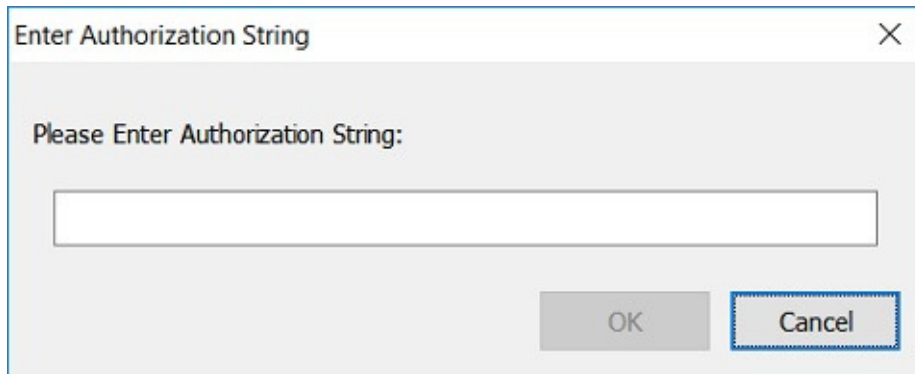


The "Set Password" dialog box features a red header with the CURTAIN logo and the text "Secured e-locker in workstation". It contains three input fields: "Old Password:", "New Password:", and "Repeat". A blue link labeled "Forget password" is positioned below the "Old Password" field. At the bottom, there are "OK" and "Cancel" buttons.

2. Enter Old Password and New Password.

3. Click OK to confirm.

4. If you do not remember the password, please contact administrators. Administrators can click "Forget password" and use Authorization String to reset the password for you.



The "Enter Authorization String" dialog box has a light gray background and a title bar with a close button. It contains the text "Please Enter Authorization String:" above a single-line text input field. At the bottom, there are "OK" and "Cancel" buttons.

## 7 - Ongoing Maintenance

### 7.1 - Patch Management

Administrators can download the latest patches from our website and apply the patches in Curtain Admin. Then all the Curtain Clients will be updated accordingly. There is no need to apply patches to users' workstations one by one.

#### Procedures of applying patch:

1. Download appropriate patch from our website. When a build is released, five patches will be provided by us. Here is an example (e.g. build number is 3273.04):

- CurtainFullPatch\_Win32(327304).zip - for Curtain Admin which is running on 32-bit OS
- CurtainFullPatch\_X64(327304).zip - for Curtain Admin which is running on 64-bit OS
- CurtainAdminPatch\_Win32(327304).zip - If you want to apply the patch only to Curtain Admin or Curtain Server Plug-in, you can run this patch. Curtain Clients will not be updated
- CurtainAdminPatch\_X64(327304).zip - If you want to apply the patch only to Curtain Admin or Curtain Server Plug-in, you can run this patch. Curtain Clients will not be updated
- CurtainClientPatch(327304).zip - If you want to apply the patch to particular Curtain Clients, you can run the patch directly on client-side

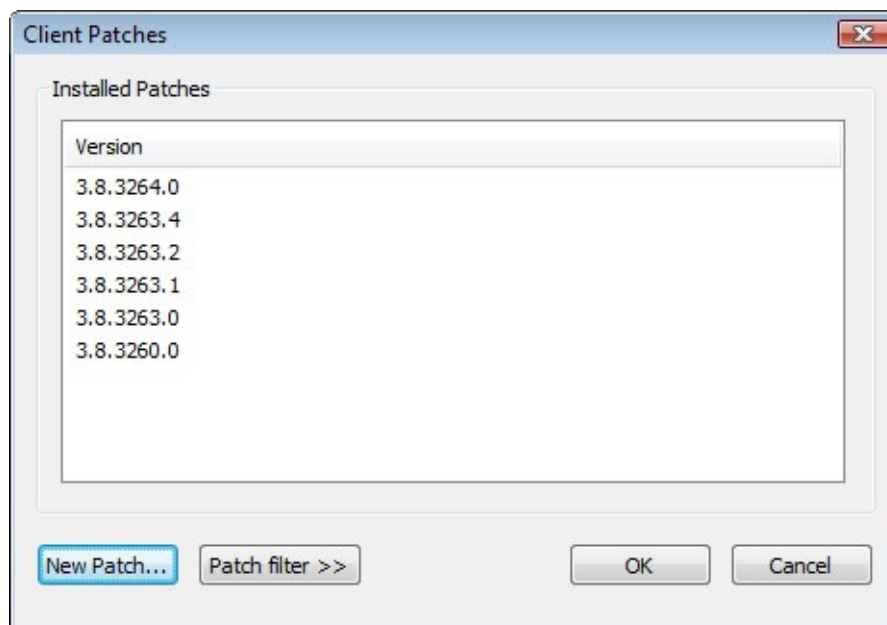
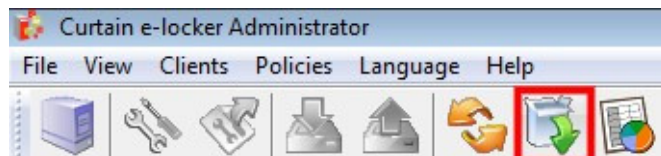
2. Unzip the patch.

3. Run the CurtainFullPatch\_Win32.exe or CurtainFullPatch\_X64.exe on Curtain Policy server (the machine which hosts Curtain Admin). Then all Curtain Clients will be updated when they connect to Curtain Admin next time.

4. Run the CurtainAdminPatch\_Win32.exe or CurtainAdminPatch\_X64.exe to update other Curtain Server Plug-ins, if needed.

#### View all installed patches in Curtain Admin:

- Click "Update Patch" button or select "File > Client Patch" in Curtain Admin



## 7.2 - Migrate Curtain Admin to a new machine

There are 2 scenarios:

- (1) Migrate Curtain Admin to a new machine : Using the same hostname and IP address
- (2) Migrate Curtain Admin to a new machine : Using different hostname and IP address

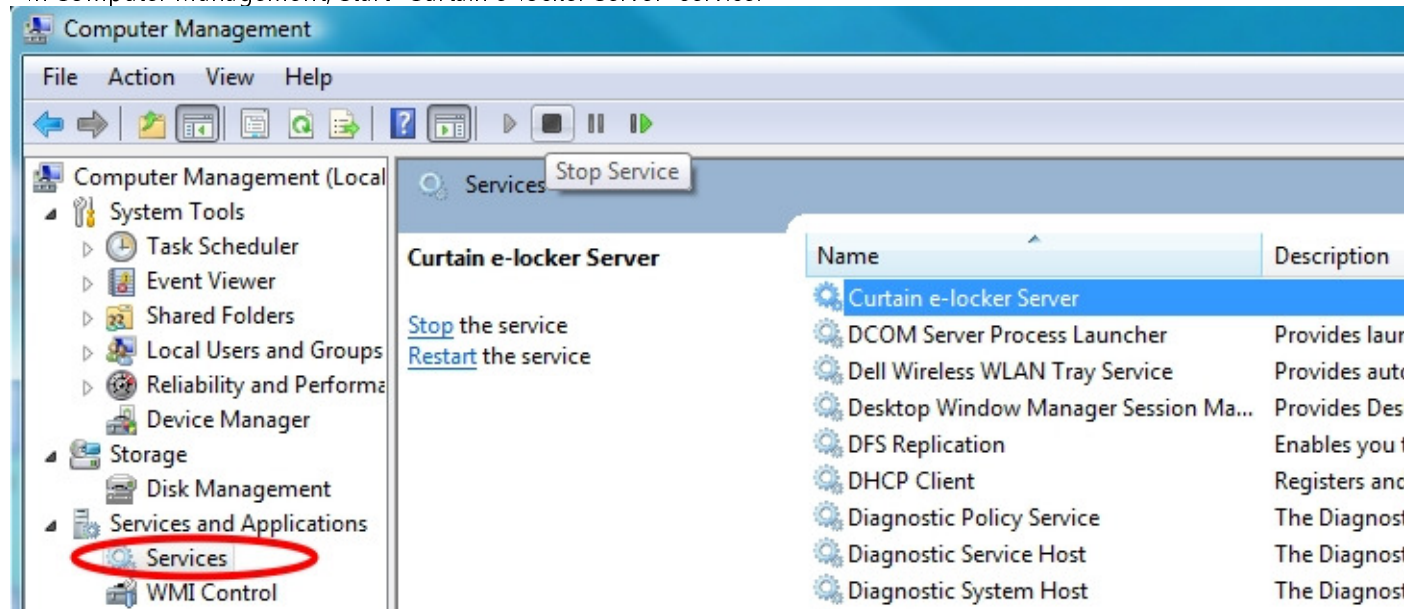
### Preparation:

1. Backup policies from existing Curtain Admin, please copy folder and files stated below.
  - C:\Program Files\Coworkshop\Curtain 3\bin\Config
  - C:\Program Files\Coworkshop\Curtain 3\bin\ServerStore.dat
  - C:\Program Files\Coworkshop\Curtain 3\bin\ServerStore.enx
2. Backup Audit Trail files from existing Curtain Admin, please copy files stated below.
  - C:\Program Files\Coworkshop\Curtain 3\bin\Curtain.mdb (it exists in old versions)
  - Backup the whole "Curtain" folder
    - for Windows 2000 / XP / 2003, this folder should be under C:\Documents and Settings\All Users\Application Data
    - for Windows 2008 / 2010 / Vista / Win7 / Win8 / Win10, this folder should be under C:\ProgramData

For scenario 1 - Migrate Curtain Admin to a new machine : Using the same hostname and IP address:

### Here are migration steps:

1. Shutdown existing Curtain Policy server (i.e. the machine which hosts Curtain Admin) or simply disconnect it from the network.
2. Install a new machine with the same hostname and IP address of the existing Curtain Policy server.
3. Install Curtain Admin on the new machine (For detail information, please refer to related documents).
4. Activate the license of Curtain e-locker (For detail information, please refer to related documents).
5. Copy Policies and Audit Trail (the folder and files backup in Preparation) to the new machine.
  - In Computer Management, Stop "Curtain e-locker Server" service.
  - Restore the folder and files to the new machine.
  - In Computer Management, Start "Curtain e-locker Server" service.



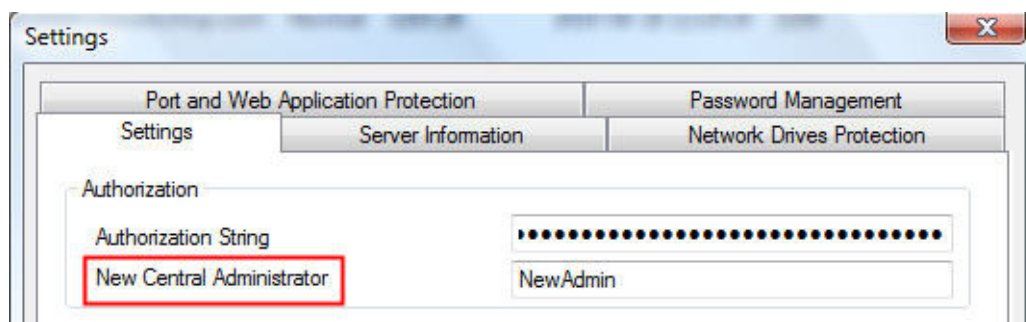
6. Since the hostname and IP address of the new machine are the same as that of old Curtain Policy server, all Curtain Clients will automatically connect to the new Curtain Admin.

7. Done



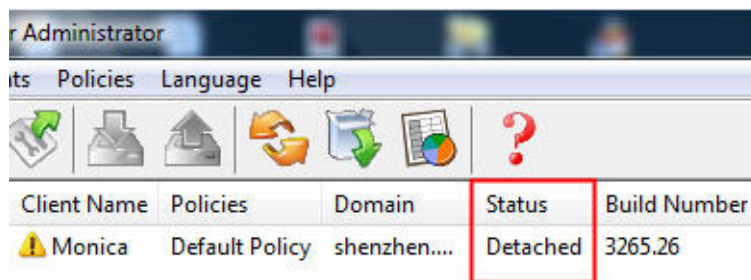
For scenario 2 - Migrate Curtain Admin to a new machine : Using different hostname and IP address:  
[Here are migration steps:](#)

1. Install a new machine with different hostname and IP address.
2. Install Curtain Admin on the new machine (For detail information, please refer to related documents).
3. Activate the license of Curtain e-locker on the new machine (For detail information, please refer to related documents).
4. Copy Policies and Audit Trail (the folder and files backup in Preparation) to the new machine.
  - In Computer Management, Stop "Curtain e-locker Server" service.
  - Restore the folder and files to the new machine.
  - In Computer Management, Start "Curtain e-locker Server" service.
5. In the existing Curtain Admin, select "File > Settings" in the menu. Then, "Settings" window will be shown.



6. Enter hostname or IP address of the new machine in "New Central Administrator", and Click OK.

When Curtain Clients connect to the existing Curtain Admin, they will be notified that there is a new Curtain Admin. Status of these Curtain Clients will change to "Detached". When status of all Curtain Clients change to "Detached", administrators can switch off (or uninstall) the old Curtain Admin. All Curtain Clients are managed by the new Curtain Admin.



7. Done

P.S. You should use the same Authorization String in the new Curtain Admin.

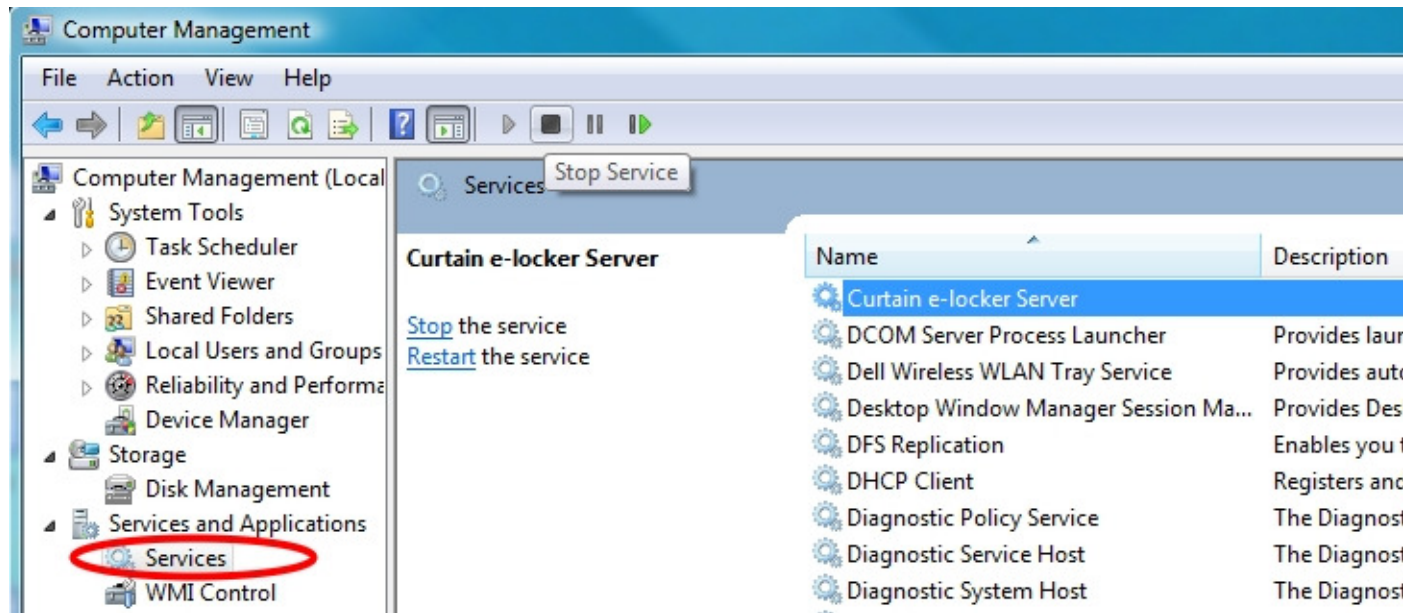
## 7.3 - Backup and restore Curtain Admin policies and audit log manually

### Backup Policies & Audit Trail:

1. Backup Policies from existing Curtain Admin, please copy folder and files stated below.
  - C:\Program Files\Coworkshop\Curtain 3\bin\Config
  - C:\Program Files\Coworkshop\Curtain 3\bin\ServerStore.dat
  - C:\Program Files\Coworkshop\Curtain 3\bin\ServerStore.enx
2. Backup Audit Trail files from existing Curtain Admin, please copy files stated below.
  - C:\Program Files\Coworkshop\Curtain 3\bin\Curtain.mdb (it exists in old versions)
  - Backup the whole "Curtain" folder
    - for Windows 2000 / XP / 2003, this folder should be under C:\Documents and Settings\All Users\Application Data
    - for Windows 2008 / 2010 / Vista / Win7 / Win8 / Win10, this folder should be under C:\ProgramData

### Restore Policies & Audit Trail:

- In Computer Management, Stop "Curtain e-locker Server" service.
- Restore the folder and files.
- In Computer Management, Start "Curtain e-locker Server" service.



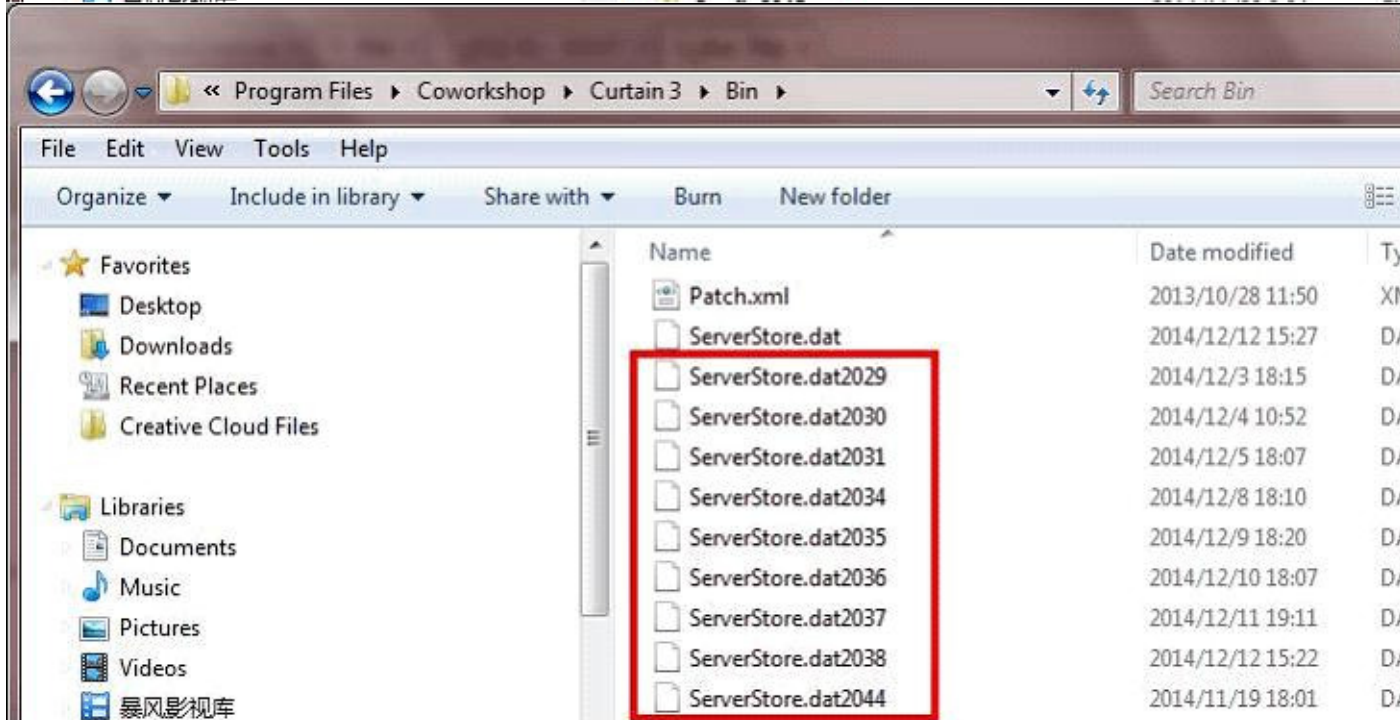
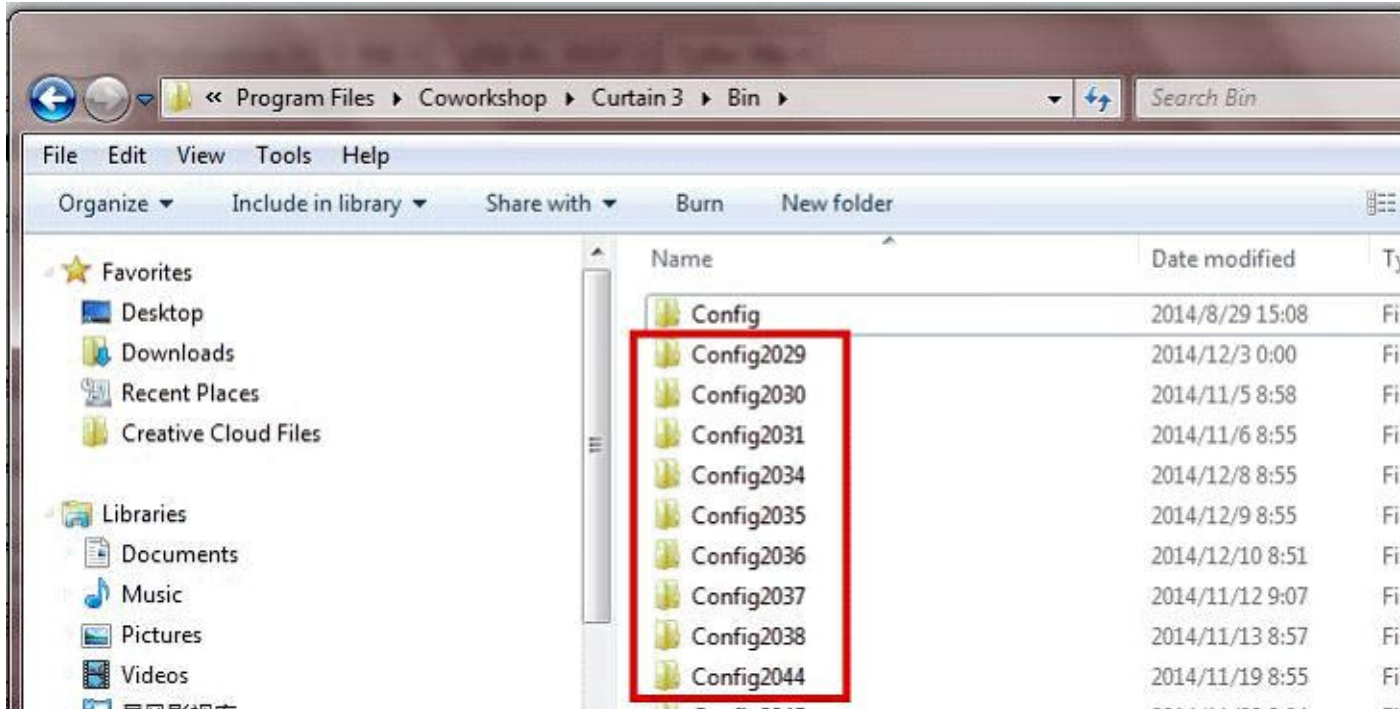
## 7.4 - Backup Curtain Admin policies automatically

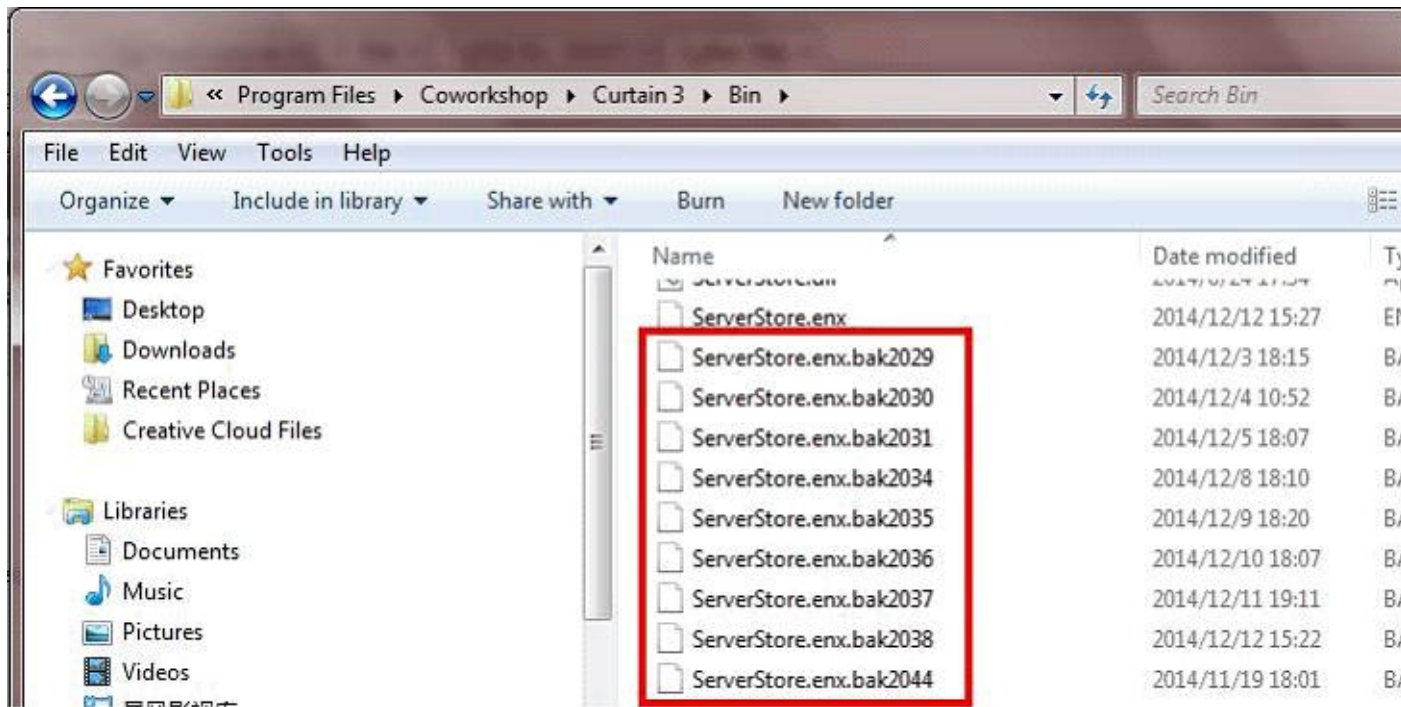
Curtain Admin will backup your control policies automatically. In case, the policies are corrupted accidentally (e.g. abnormal shutdown), you can restore the policies manually.

Control Policies are stored in folder and files as below.

- C:\Program Files\Coworkshop\Curtain 3\bin\Config
- C:\Program Files\Coworkshop\Curtain 3\bin\ServerStore.dat
- C:\Program Files\Coworkshop\Curtain 3\bin\ServerStore.enx

You can find some duplicate folders and files as below. You can use "Date modified" to find out which folder and files you want to restore.





#### Restore Policies:

- In Computer Management, Stop "Curtain e-locker Server" service.
- Rename to restore the "Config" folder, "ServerStore.dat" and "ServerStore.enx" file.
- In Computer Management, Start "Curtain e-locker Server" service.

When you open Curtain Admin again, all the control policies and settings are restored.

## 8 - Frequently Asked Questions

### 8.1 - How to avoid conflict with Antivirus ?

There are many popular antivirus in the market, such as Trend Micro, Kaspersky, McAfee, 360 Total Security, Avast, AVG and etc. Some antivirus are compatible with e-locker without any problem. However, some antivirus need to add e-locker related files and paths to "Trust list" or "Exception list". Below is the list of file and path:

Path of Curtain drivers and files:

- 32 bit system: C:\Program Files\Coworkshop\Curtain 3\CBin\
- 64 bit system: C:\Program Files\Coworkshop\Curtain 3\CBin\ and C:\Program Files (x86)\Coworkshop\Curtain 3\CBin\
- Drivers: C:\windows\system32\drivers (curtain.sys,CurtainP.sys,CurtainPM.sys,CurtainWfp.sys,CurtainRP.sys, CurtainPD.sys,CrNetFltW.sys)

If adding path is not allowed in the antivirus, please add EXE files manually:

- CrClient.exe
- CrClientSvc.exe
- CrCmd.exe
- CrCmdAppMon.exe
- CrCmdAW.exe
- CrCmdW.exe
- CrCryptFormat.exe
- CrFileDialog.exe
- CrProcMonSvc.exe
- CrShellExecProxy.exe
- CrUtilSvc.exe
- CurtainCB.exe
- CurtainParser.exe
- CurtainTips.exe
- PDMWEClient.exe
- searchmonkey.exe

P.S. Include all EXE files under path of C:\Program Files\Coworkshop\Curtain 3\CBin\ and C:\Program Files (x86)\Coworkshop\Curtain 3\CBin\

### 8.2 - Use Curtain e-locker to protect NAS through iSCSI

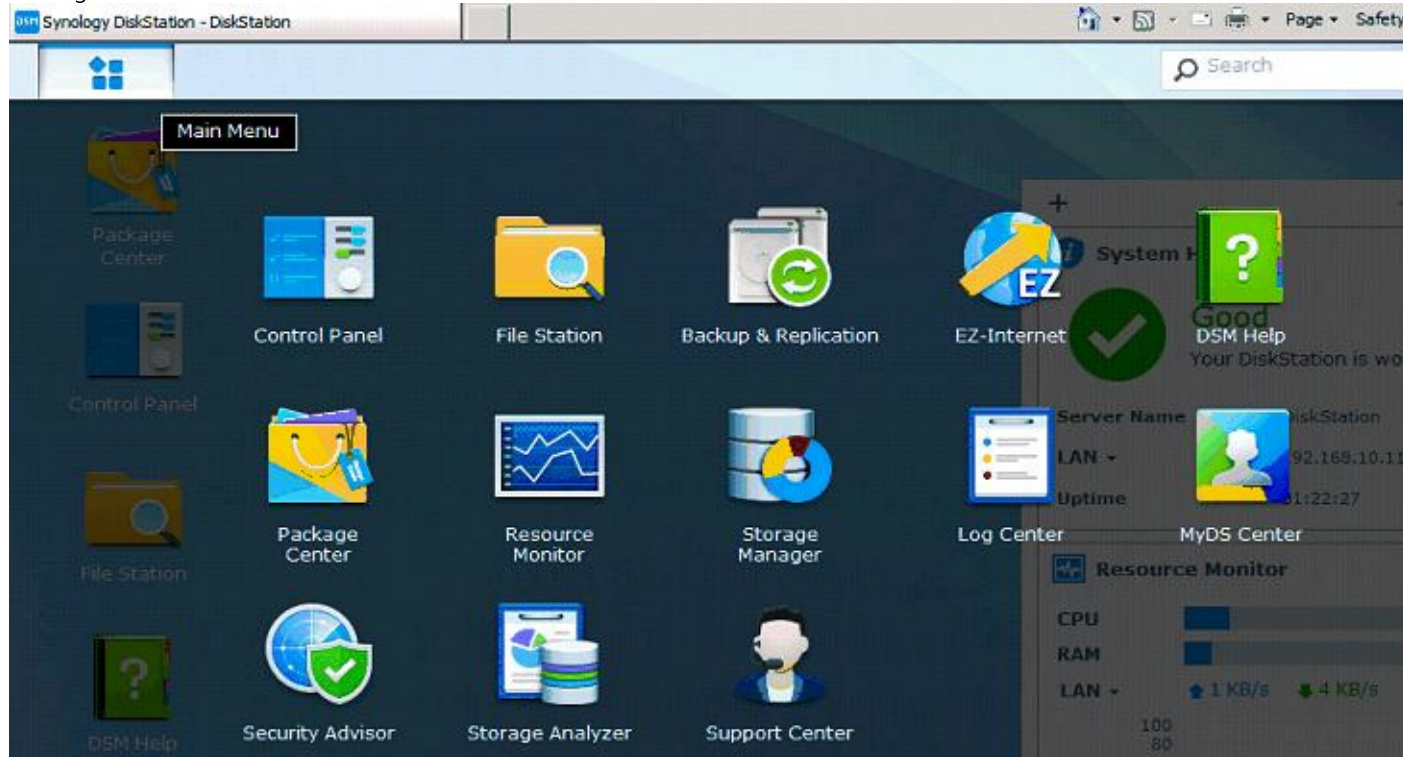
Currently most NAS storage servers are running Linux and they do not allow people to install program/software on the NAS. That means we cannot install Curtain Server Plug-in on a NAS storage server, to protect the share folders. Alternatively, we can protect the NAS by mounting it to a Windows server as local virtual disk through iSCSI. Firstly, you need to create iSCSI LUN (logical unit) on the NAS, and then use Windows iSCSI Initiator to create a virtual disk on the Windows server. Finally, you can share the virtual disk and protect it by Curtain e-locker.

P.S. We used Synology DiskStation to demonstrate how to do the setup. The interface and naming will be different if you are using other NAS servers.

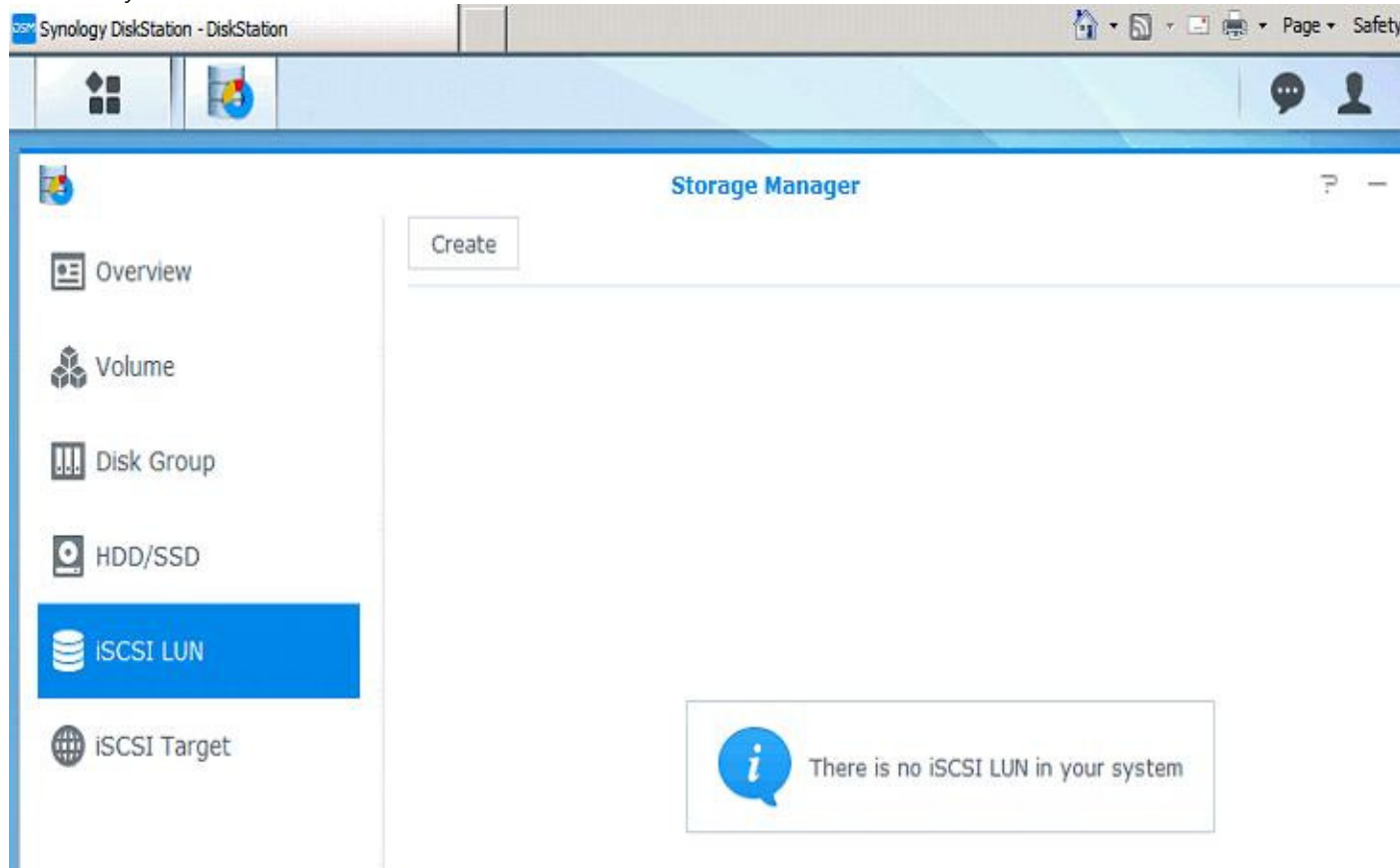


Steps to create iSCSI LUN (logical unit) on NAS:

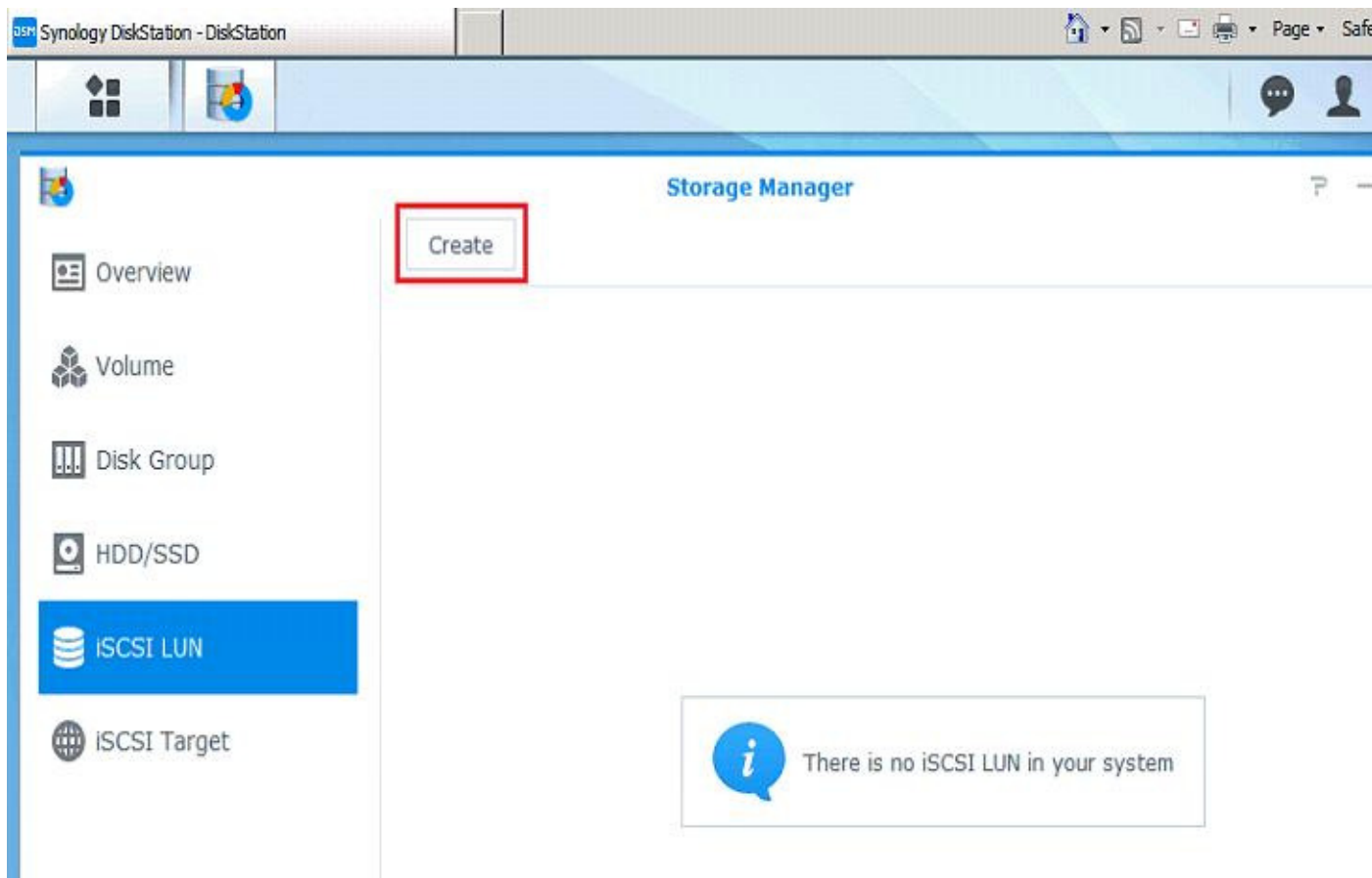
1. In my Synology DiskStation, go to DSM (DiskStation Manager), and click "Main Menu > Storage Manager" as below.



2. In the "Storage Manager" page, select the "iSCSI LUN" item as below. By default, there is no iSCSI LUN in the DSM system.



3. Click the "Create" button, it will pop the setup page. As follow figure:



4. In the "Choose a LUN type", select the "iSCSI LUN(Regular Files)" type, and click the "Next" button. As follow figure:

**Choose a LUN type**

iSCSI LUN (Regular Files)  
This type of iSCSI LUN provides flexibility of dynamic capacity management with Thin Provisioning.

iSCSI LUN (Block-Level) - Single LUN on RAID  
This type of iSCSI LUN provides the best access performance.

Name:

iSCSI Target mapping:

iSCSI LUN (Block-Level) - Multiple LUNs on RAID  
This type of iSCSI LUN is created on a Disk Group and provides flexibility of dynamic capacity management with optimized access performance.


Name:

iSCSI Target mapping:



5. Set up iSCSI LUN properties in this step, we suggest you to set up the "Capacity(GB)" property only, the capacity room is up to you. If you have already set up, click the "Next" button. As follow figure:

### Set up iSCSI LUN Properties

|                       |                                                                                                                      |
|-----------------------|----------------------------------------------------------------------------------------------------------------------|
| Name:                 | <input type="text" value="LUN-1"/>                                                                                   |
| Location:             | <input type="text" value="Volume 1 (Available: 912 GB)"/>                                                            |
| Thin Provisioning:    | <input type="text" value="Yes"/>  |
| Capacity (GB):        | <input type="text" value="512"/>                                                                                     |
| iSCSI Target mapping: | <input type="text" value="Create a new iSCSI target"/>                                                               |

6. In this step, you will create a new iSCSI target. Input the "Name" first, we suggest you to enable the CHAP and set up the password. To prevent anonymous use the iSCSI target, please follow figure:

**Create a new iSCSI target**

Name: Target-1

IQN: iqn.2000-01.com.synology:DiskStation

Enable CHAP

Name: Target1

Password: .....

Confirm password: .....

Enable Mutual CHAP

Name:

Password:

Confirm password:

Back Next Cancel

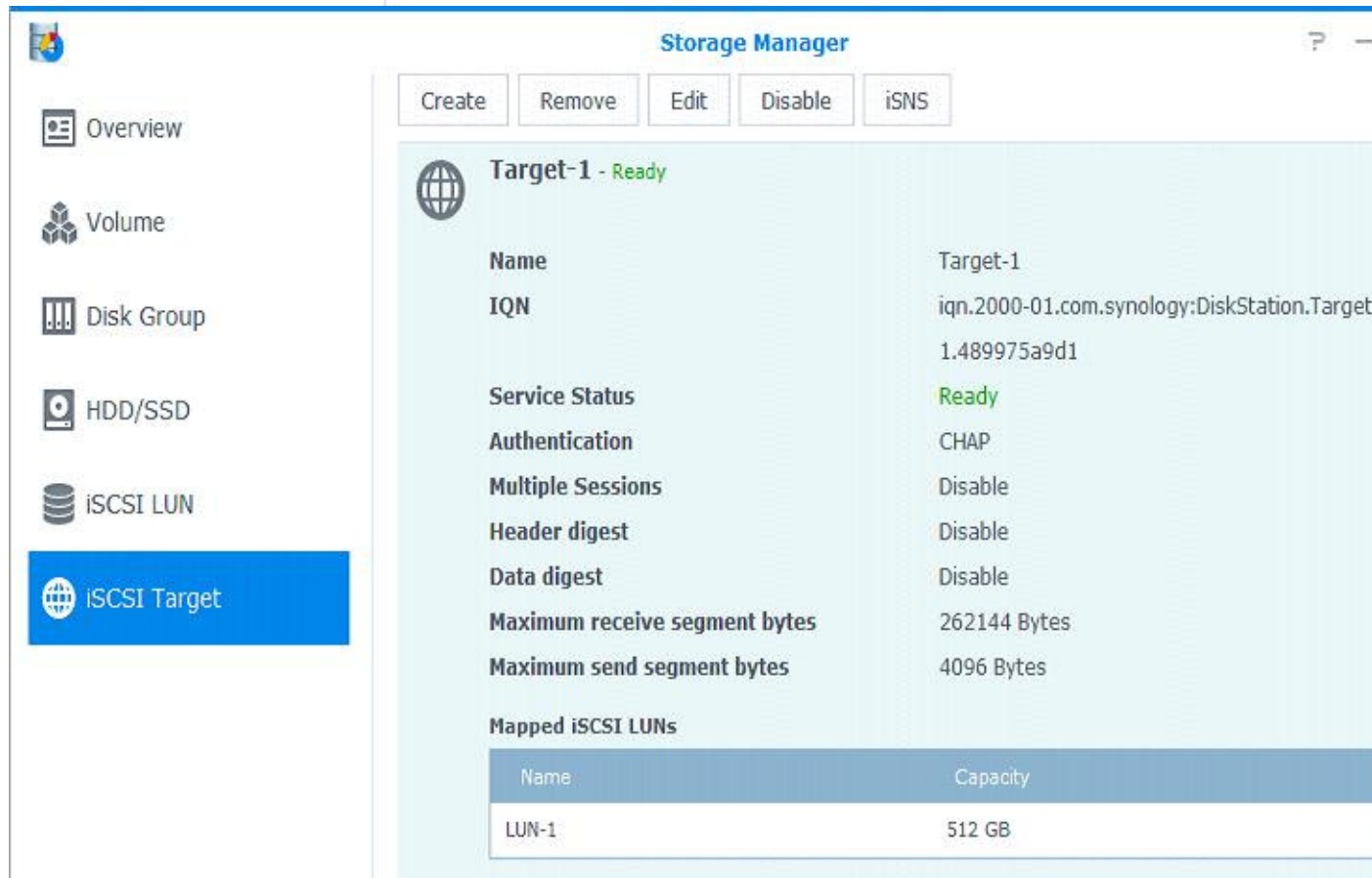
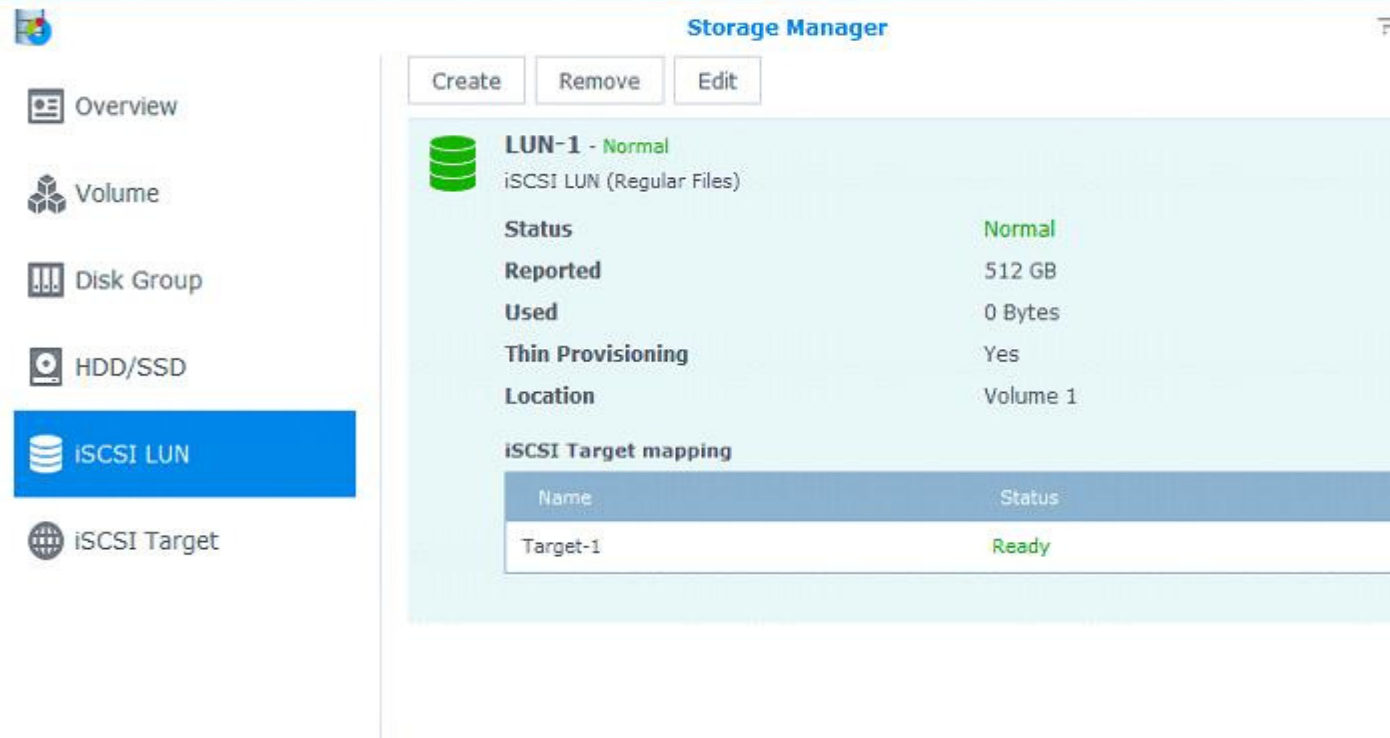
7. Confirm the settings that you have set up, if no problem, click the "Apply" button to create the iSCSI LUN. As follow figure:

### Confirm settings

The wizard will apply the following settings. The process will take a few seconds.

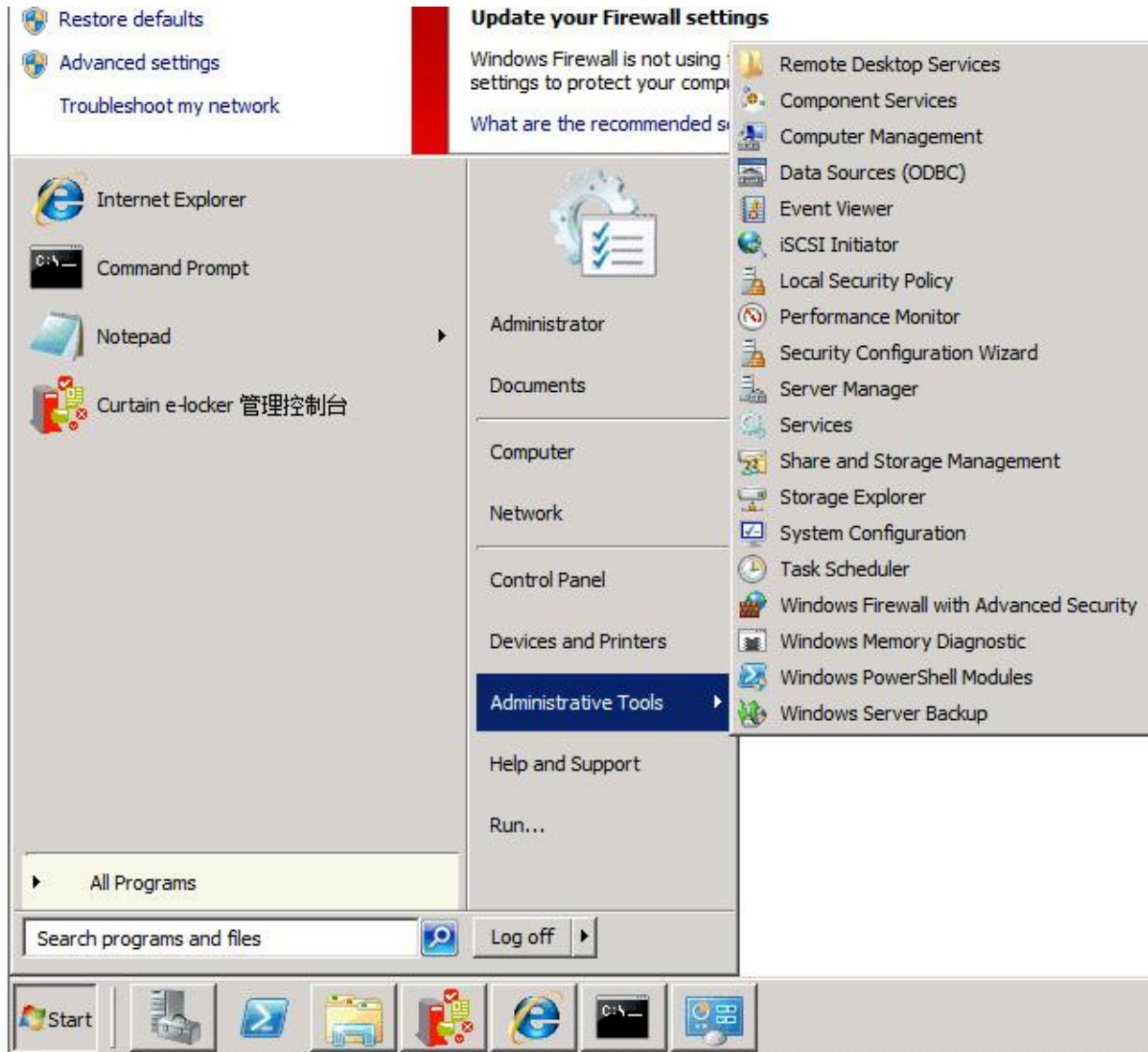
| Item                         | Value                                                    |
|------------------------------|----------------------------------------------------------|
| <b>Usage</b>                 | iSCSI LUN                                                |
| <b>Name</b>                  | LUN-1                                                    |
| <b>Location</b>              | Volume 1 (Available: 912 GB)                             |
| <b>Capacity</b>              | 512 (GB)                                                 |
| <b>Thin Provisioning</b>     | Yes                                                      |
| <b>iSCSI Target mappi...</b> | Target-1 (Create)                                        |
| <b>IQN</b>                   | iqn.2000-01.com.synology:DiskStation.Target-1.489975a9d1 |
| <b>Authentication</b>        | CHAP                                                     |
| <b>Name</b>                  | Target1                                                  |

8. Now you have created the iSCSI LUN, in the "Storage Manager" page, you can see the iSCSI LUN that you have created. As follow figure:

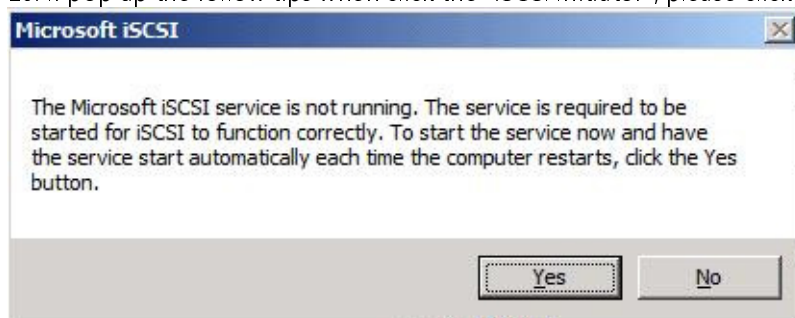


Map the iSCSI Target to a local virtual disk on the Windows

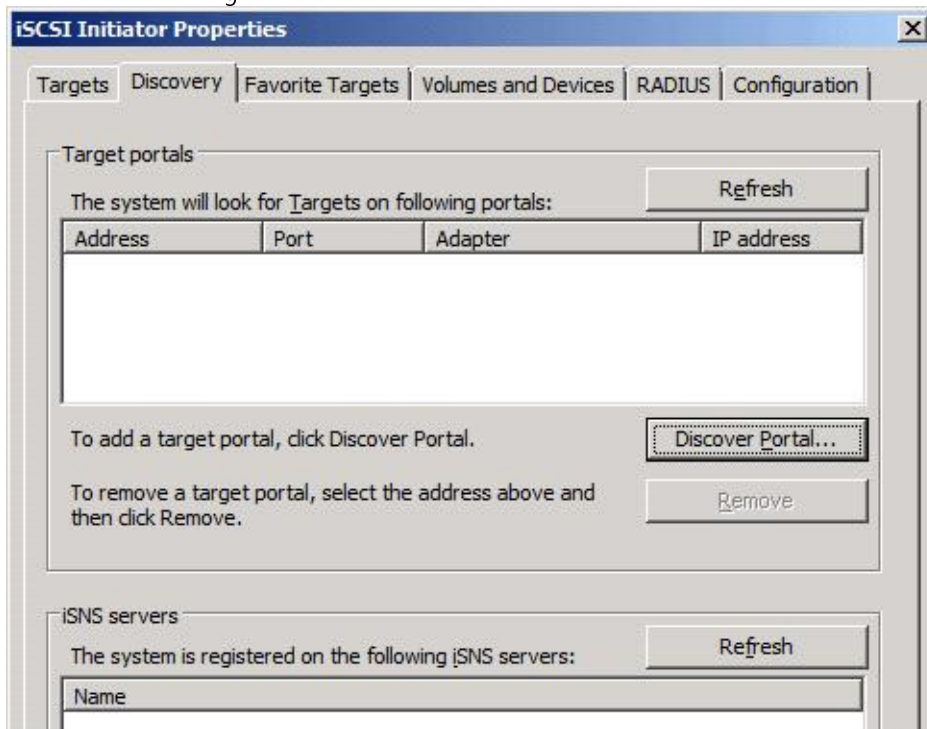
9. In the Windows start menu, click the "Start Menu" -> "Administrative Tools" -> "iSCSI Initiator". As follow figure:



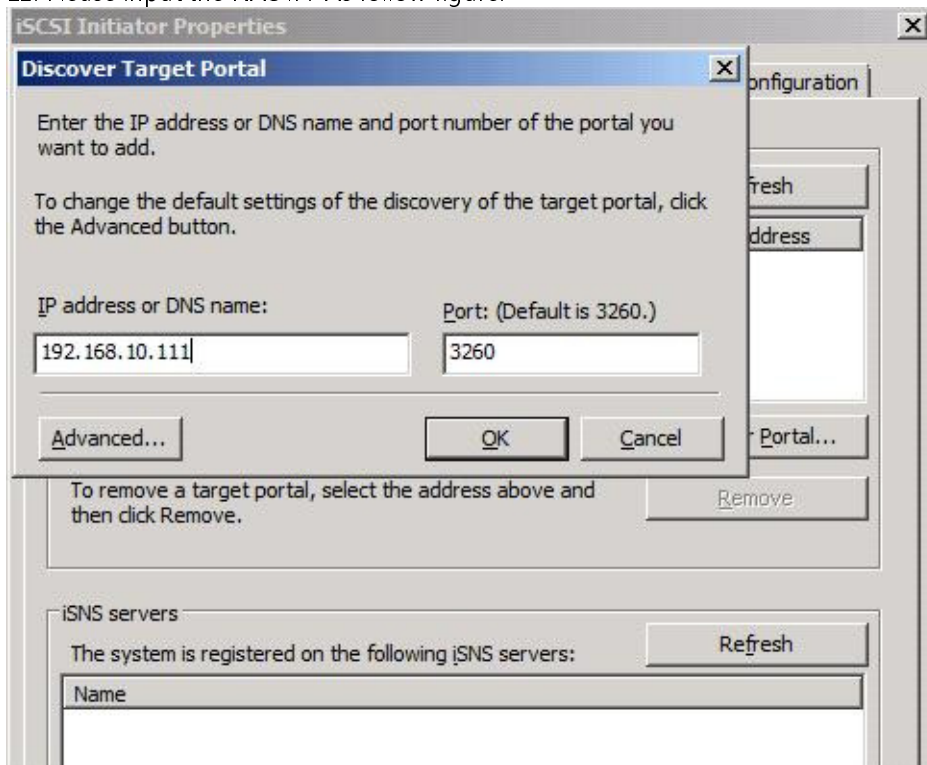
10. If pop up the follow tips when click the "iSCSI Initiator", please click the "Yes" button.



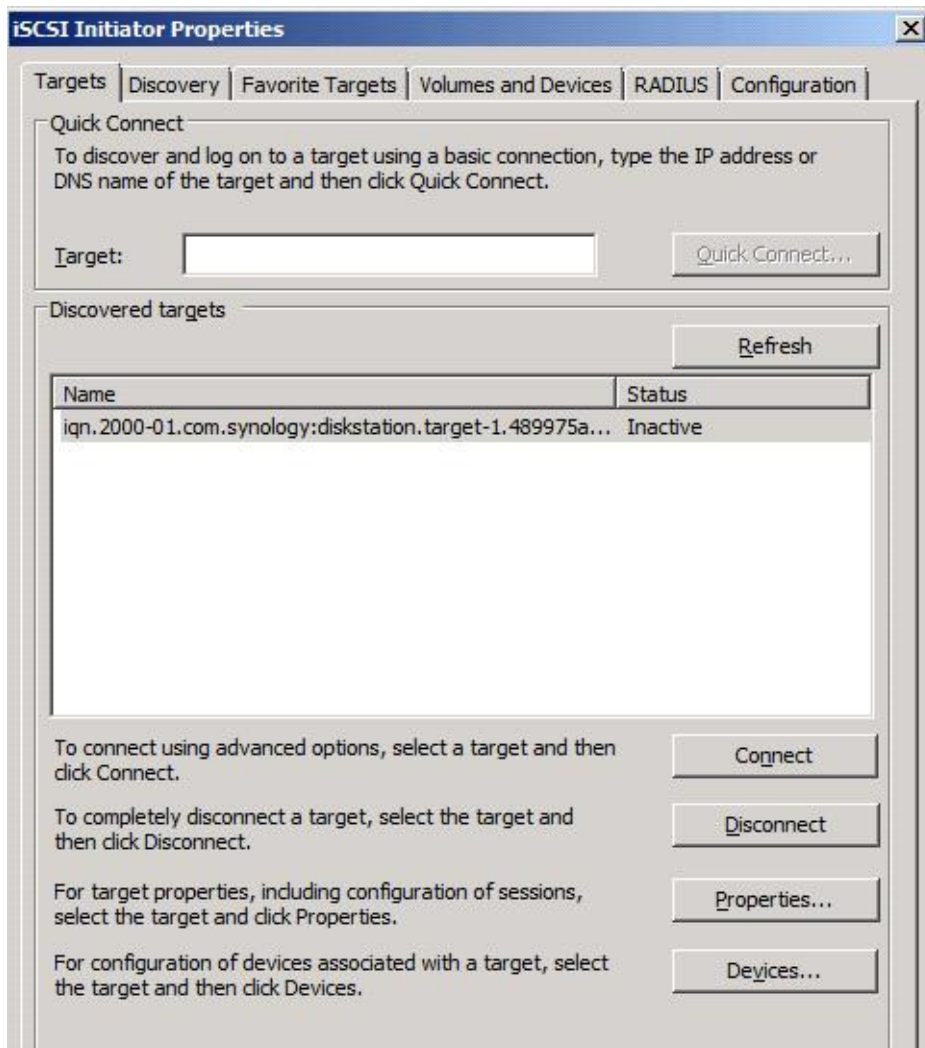
11. In the "iSCSI Initiator Properties" window, select the "Discovery" page, and click the "Discover Portal..." button. As follow figure:



12. Please input the NAS'IP. As follow figure:

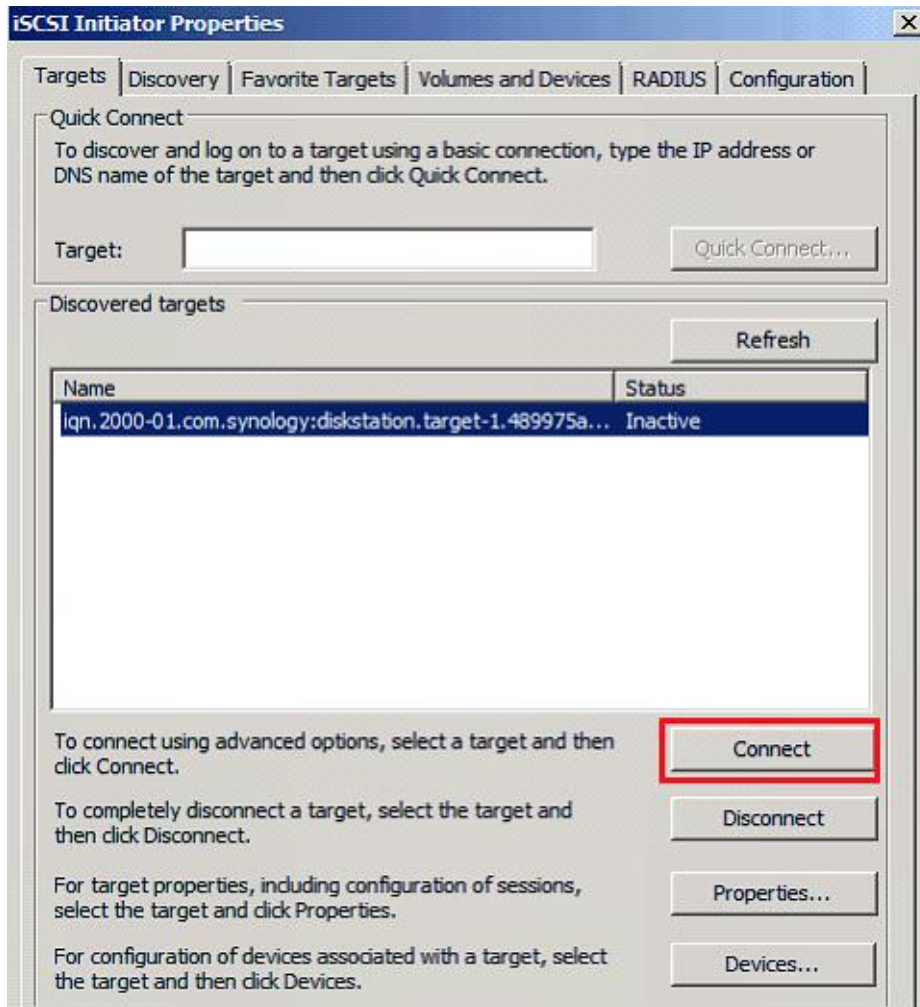


13. Click the "OK" button, and return the "Targets" page, now you can see a new target in the targets list view. As follow figure:



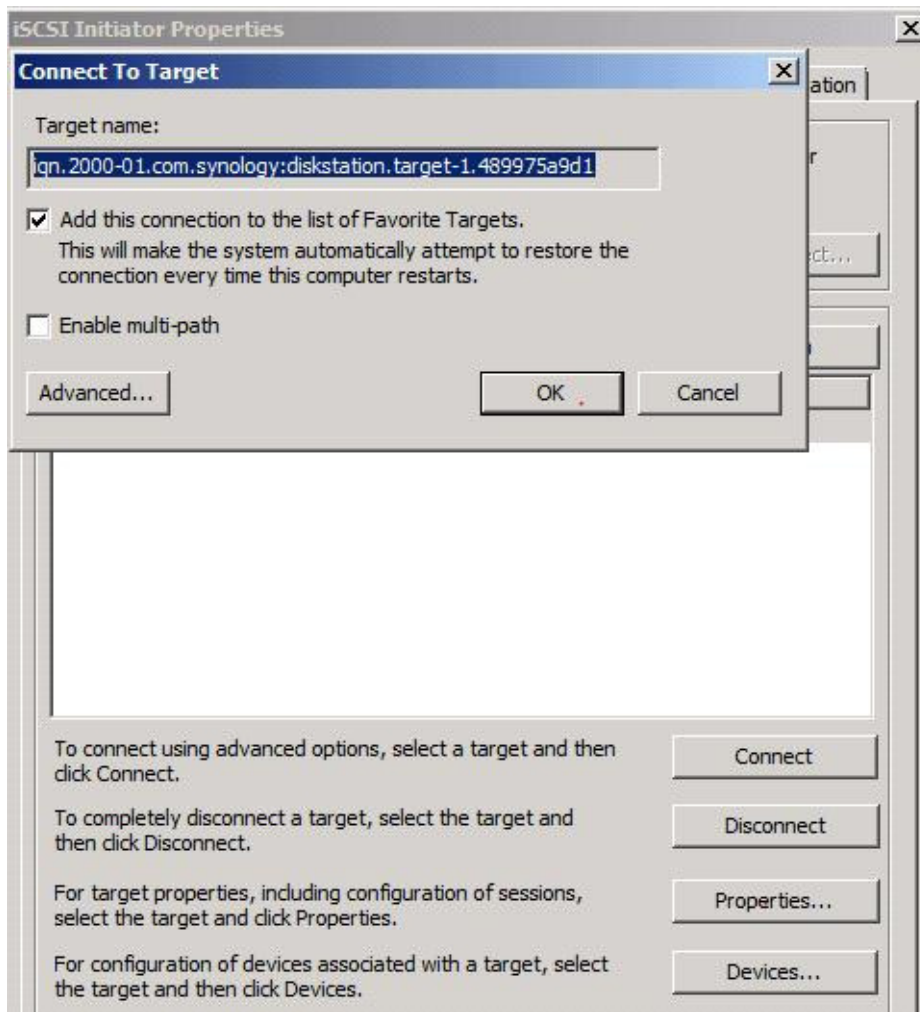


14. Select the new iSCSI target in the list view, and click the "Connect" button. As follow figure:

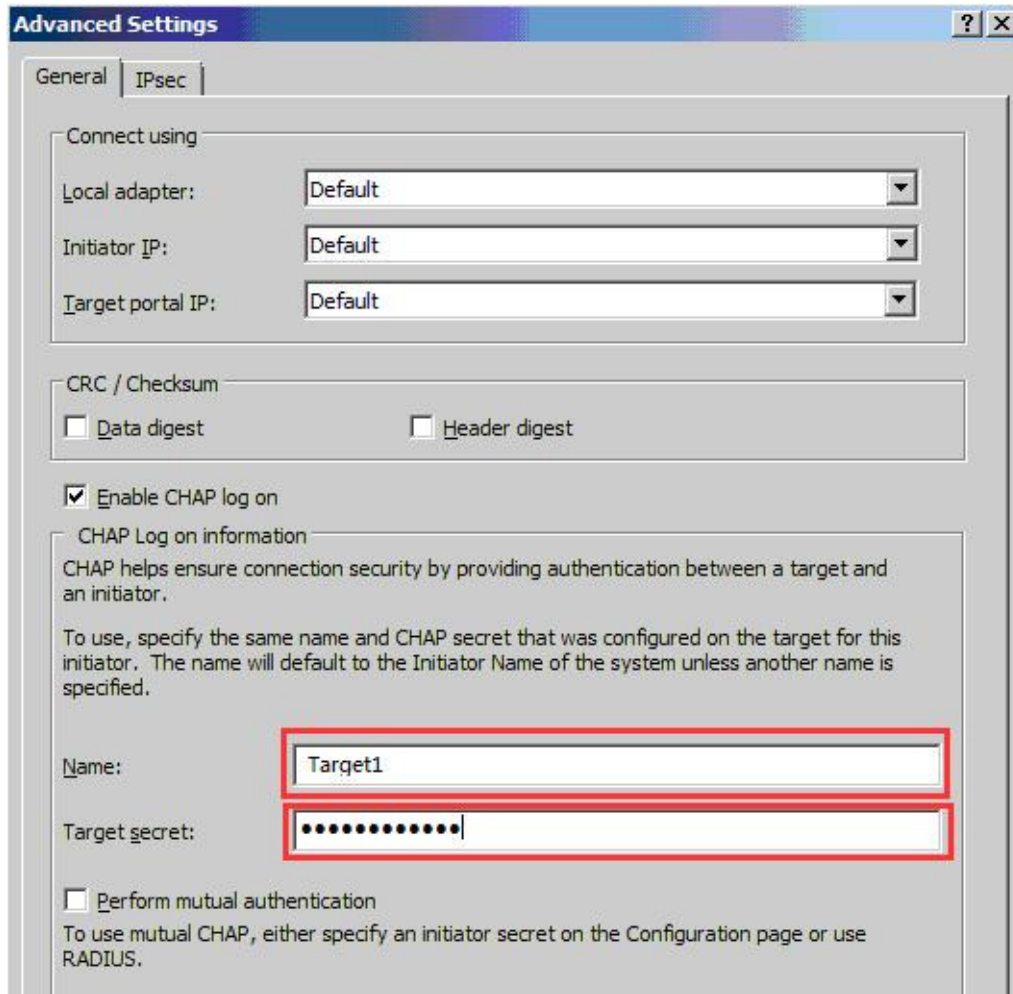




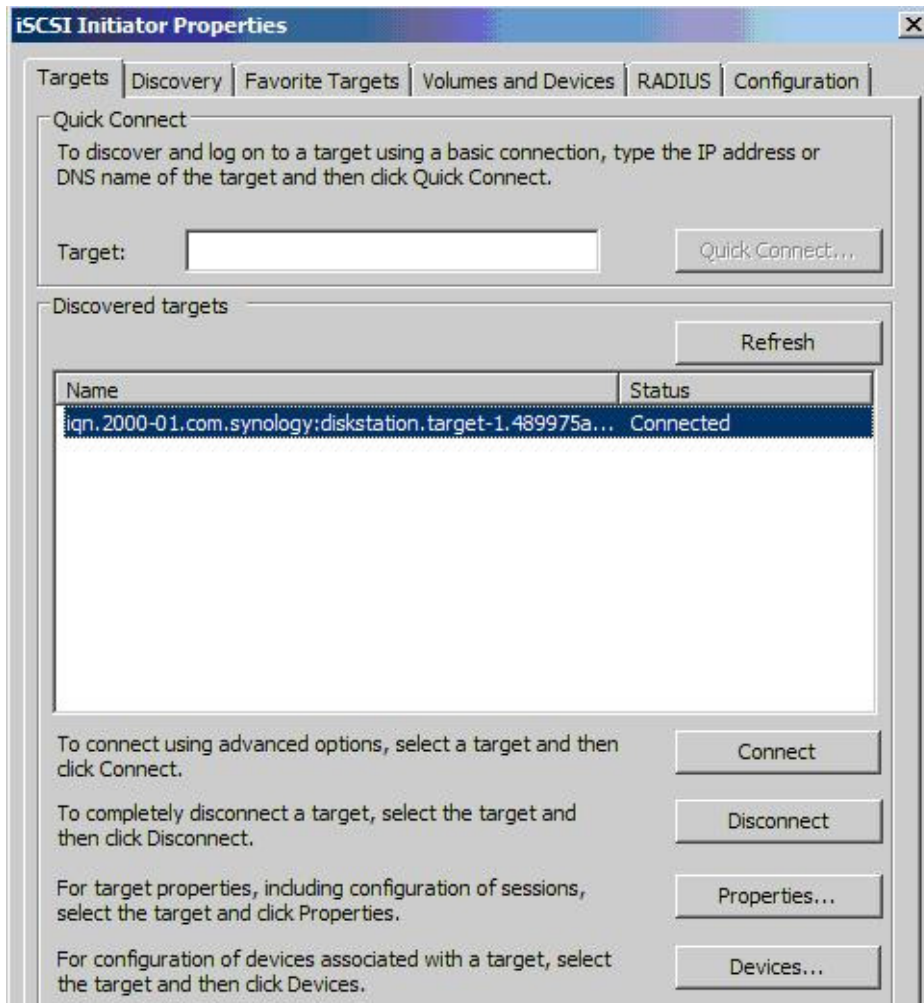
15. Click the "Advanced..."button. As follow figure:



16. In the Advanced Settings window, check the "Enable CHAP log on" button, and input the name and password that have set up in step 6. As follow figure:

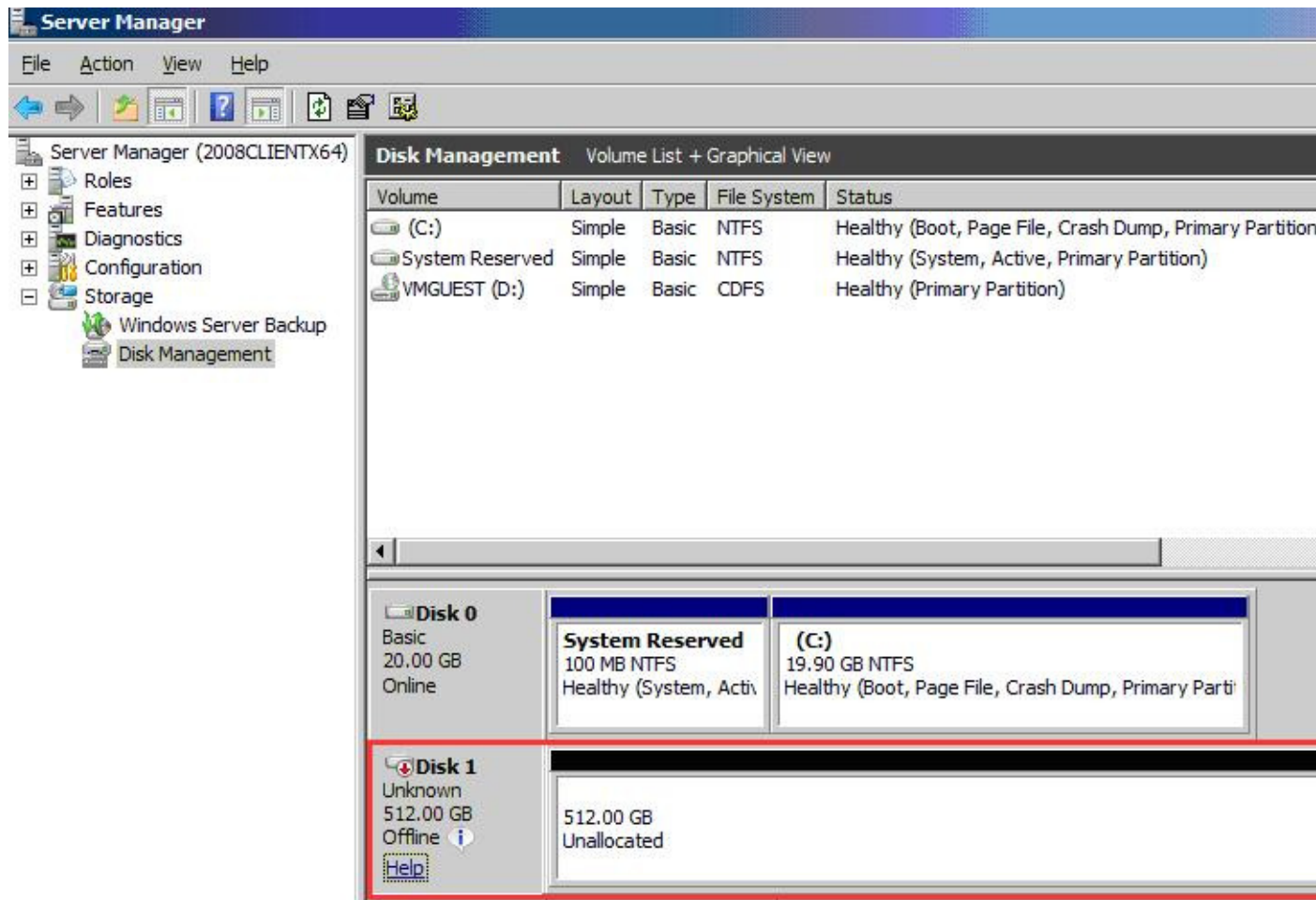


17. Click the "OK" button, it will return to "iSCSI Initiator Properties" window, you can see the new iSCSI Target's status have changed to "Connected". As follow figure:

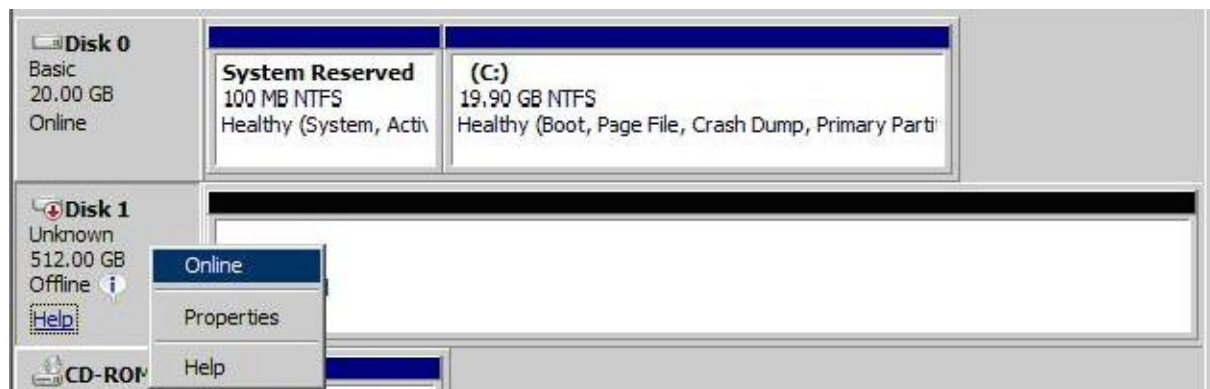


18. Click the "OK" button to exit.

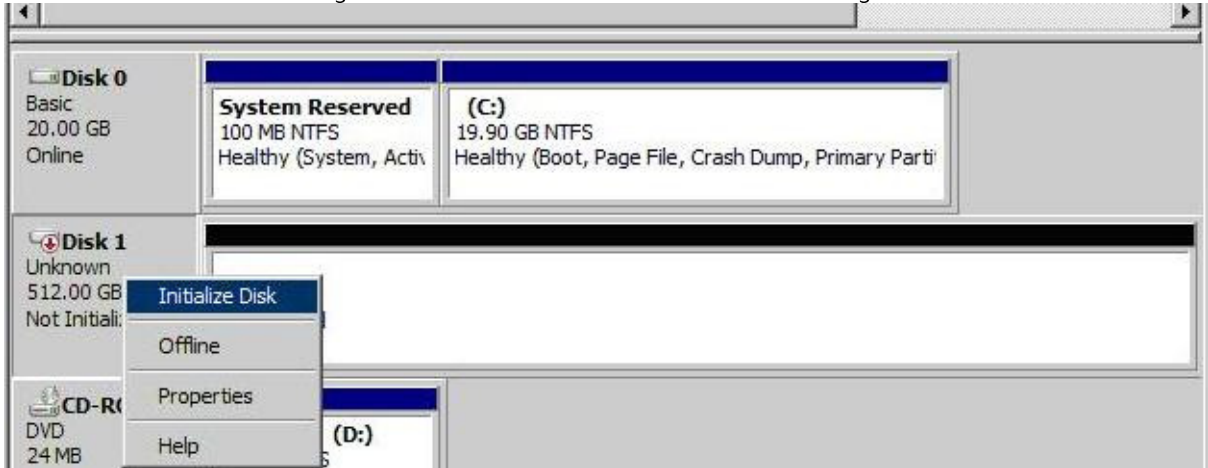
19. Open the Windows Disk Management, appears a new disk. As follow figure:



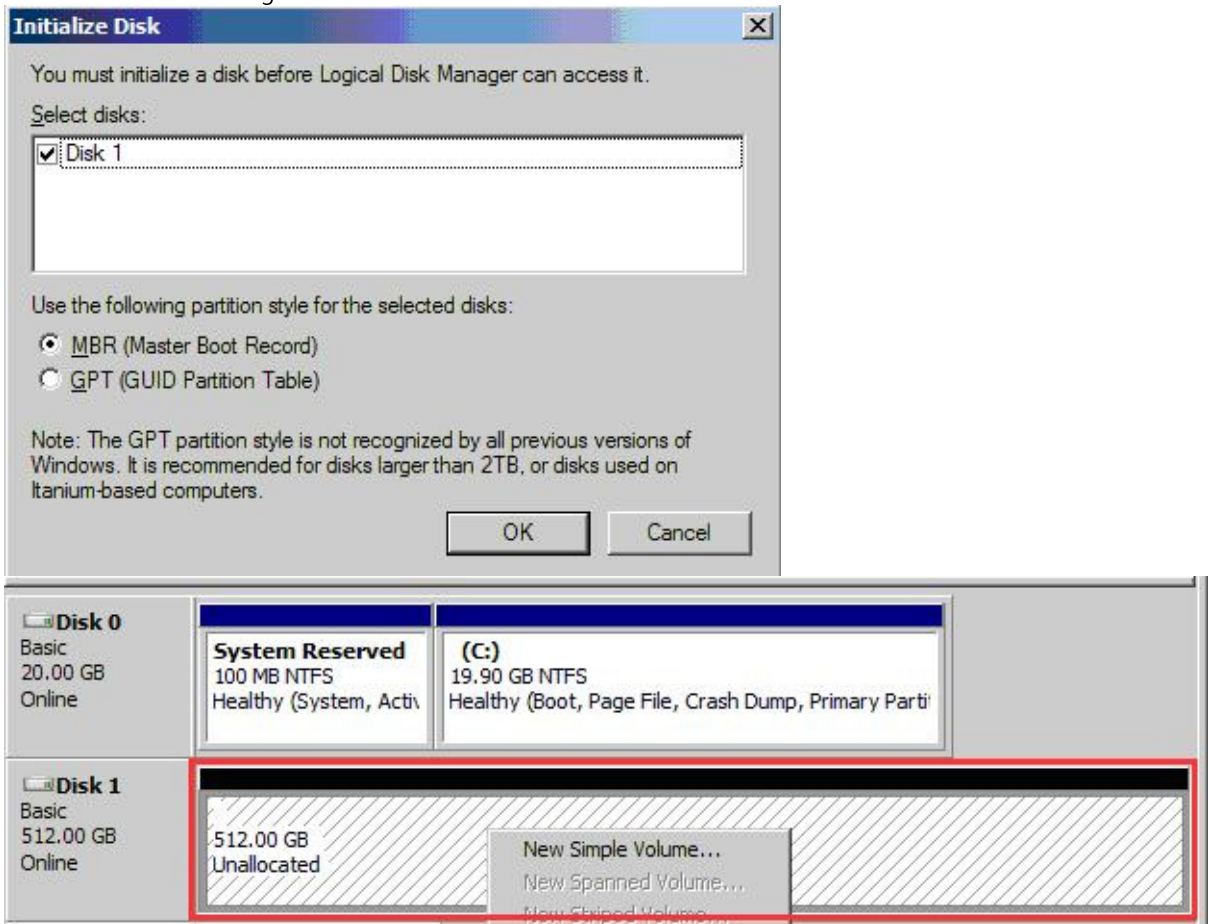
20. Select the new disk and right click, click the "Online". As follow figure:



21. Select the new disk, and right click, select the "Initialize Disk". As follow figure:



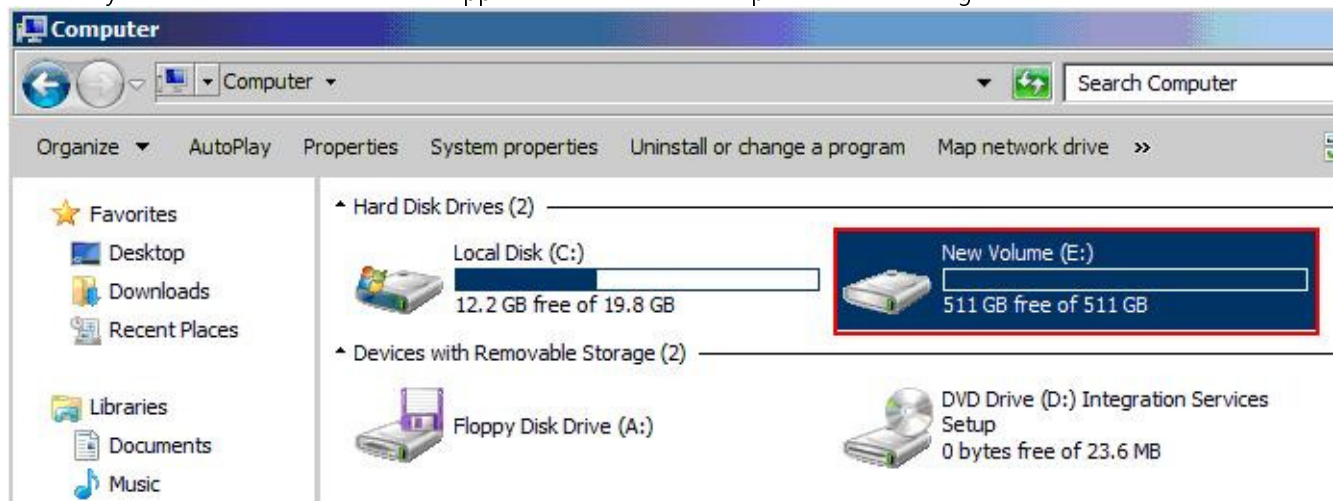
22. Select the "MBR" partition style, then click "OK", and right click the new disk, select the "New Simple Volume...". As follow figure:



23. Create "New Simple Volume", click "Next" to continue, then completing the New Simple Volume Wizard. As follow figure:



24. Now you can see a new volume "E:" appears in the Windows Explorer. As follow figure:



[Share the virtual disk and protected with Curtain e-locker](#)

25. Share the virtual disk.

26. Open the Curtain Admin, set the share virtual disk protected (Refer to FAQ 00085).

27. Now re-launch Curtain Client, and mapping protected network drive .

P.S. NAS share folder permission need to migrate to the Windows server manually by Administrators.

### 8.3 - Enable/disable Curtain Debug Log

To enable/disable Curtain Debug Log, please follow below steps:

1. Launch Command Prompt (by selecting Start menu > Programs > Accessories > Command Prompt)
2. Enter "regedit" to launch Registry Editor
3. Go to \HKEY\_LOCAL\_MACHINE\SOFTWARE\Coworkshop\Curtain 3
4. Enable Curtain Debug Log:
  - To Enable the log, Set DebugLog = a
5. Reproduce problem
6. Send log files under the locations stated below to Curtain Support Team;

Locations for Vista and above system :

- \\installation path\Coworkshop\Curtain 3\cbin\log
- \\Users\username\CurtainLog

Locations for Vista and below system :

- \\installation path\Coworkshop\Curtain 3\cbin\log
- \\Users\username\CurtainLog

For example:

C:\Program Files\Coworkshop\Curtain 3\CBin\Log  
 C:\Program Files (x86)\Coworkshop\Curtain 3\CBin\Log  
 C:\Users\tester\CurtainLog

P.S. For 64-bit operating system, please send logs under both "Program Files" and "Program Files (x86)".

7. After the completion of the operation, please remember to stop the debug log:
  - To Disable the log, Set DebugLog = 0

P.S. Please remember to disable the log after use. It is because the log may take a lot space of hard-disk.



## 8.4 - Generate unique token for cloned Curtain Client

During installation of Curtain Client, it will generate an unique token (GUID, Globally Unique Identifier) to identify each client. This token will be stored in Registry. Since cloned Curtain Clients will have same token, you need to regenerate this unique token for them.

### [Steps to generate and update Token automatically](#)

1. In workstation with Curtain Client installed, double click to run ReGenToken.exe tool.
2. You will be prompted "Generate token and set successfully".
3. Please go to Curtain Client and Curtain Admin to double check whether the token has been changed.

Checking Token on Curtain Client:

Registry Editor

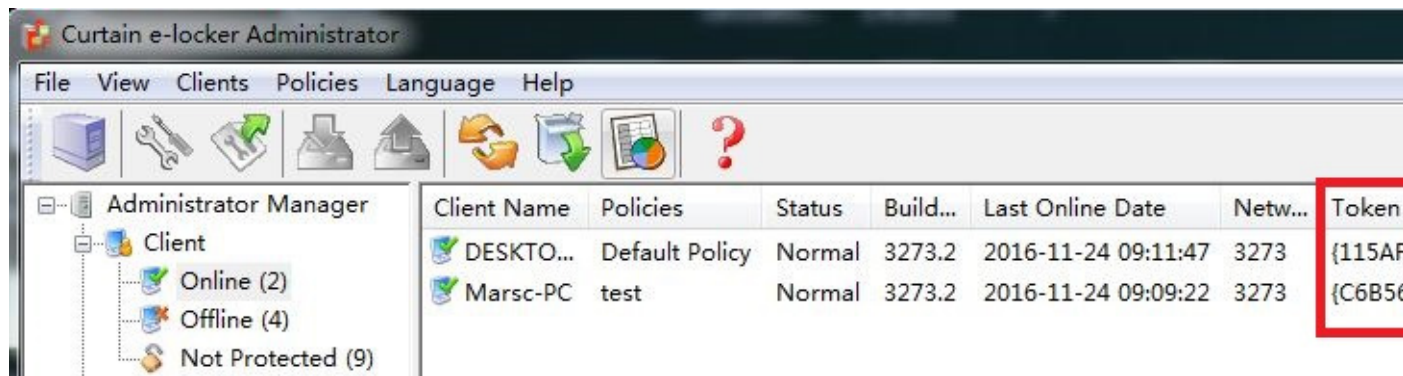
File Edit View Favorites Help

Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Coworkshop\Curtain 3

| Name              | Type      | Data                              |
|-------------------|-----------|-----------------------------------|
| ClientPath        | REG_SZ    | C:\Program Files\Coworkshop\Cu... |
| DebugLog          | REG_DWORD | 0x0000000a (10)                   |
| DebugLogSave...   | REG_DWORD | 0x0000000a (10)                   |
| DisableEFS        | REG_DWORD | 0x00000000 (0)                    |
| FileBased         | REG_DWORD | 0x00000000 (0)                    |
| FirstRun          | REG_DWORD | 0x00000000 (0)                    |
| InstallPathAdmin  | REG_SZ    | C:\Program Files\Coworkshop\Cu... |
| LocalEncryption   | REG_DWORD | 0x00000001 (1)                    |
| LsdHelpHideSta... | REG_DWORD | 0x00000000 (0)                    |
| Major             | REG_DWORD | 0x00000003 (3)                    |
| MigratedToPPD     | REG_DWORD | 0x00000001 (1)                    |
| Minor             | REG_DWORD | 0x00000008 (8)                    |
| Organization      | REG_SZ    | Kelvin-samsung                    |
| PatchPending      | REG_DWORD | 0x00000000 (0)                    |
| ProductKey        | REG_SZ    | ZP3VL-PQJ25-5HZH8-PNLB8-7T1       |
| Revision          | REG_DWORD | 0x00000000 (0)                    |
| SeqNo             | REG_DWORD | 0x0000001f (31)                   |
| Server            | REG_SZ    | 127.0.0.1                         |
| Token             | REG_SZ    | {8C1322F1-2D00-4855-ADFA-E6...    |
| UserName          | REG_SZ    | Kelvin-samsung                    |



Checking Token on Curtain Admin:



P.S. GenToken.exe tool have two versions (i.e. 3272 and 3273), please according to your Curtain Client's version to select .

Download link :

[GenToken.exe tool](#)

<http://www.coworkshop.com/download/ReGenToken.zip>

## 9 - Best Practice

### 9.1 - Allow protected files copy/send out of protected zone

Steps to authorize users to copy/send protected files out of protected zone by file extension:

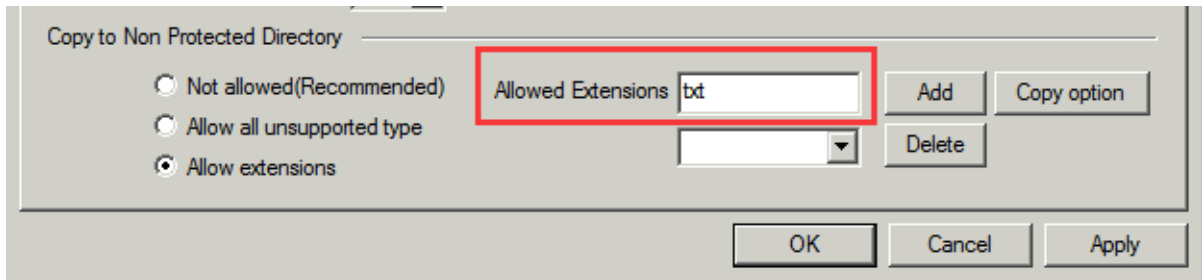
1. Launch Curtain Admin, right click Policy group -> Properties -> Copy to Non-Protected Directory .

The screenshot shows the 'Default Policy' dialog box with the following sections and options:

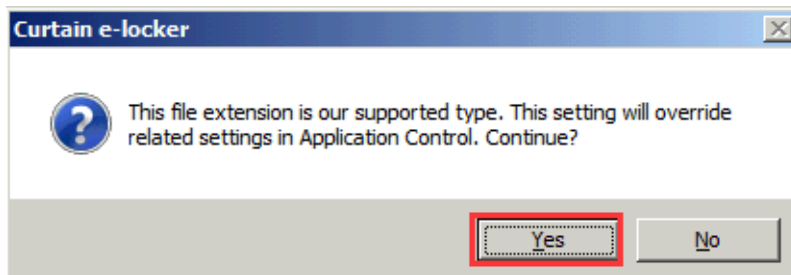
- Settings** | System Policy | Applications
- DISABLE PROTECTION on protected zones (NOT Recommended)
- Protected Directory: \_\_\_\_\_
- Hide my computer  
 Hide local protected directory  
 Disable delete files in network drive
- Additional Protected Directory: \_\_\_\_\_ ProtDir: \_\_\_\_\_ Add  
 \_\_\_\_\_ Delete
- Email**  
 Allow send sensitive documents by email  
 Audit trail for sending sensitive documents  
 Send notification to: \_\_\_\_\_ Add  
 \_\_\_\_\_ Delete
- Housekeeping**  
 Clear the whole local protected directory  
 Startup  
 Weekly Sun Mon Tue Wed Thu Fri Sat  
 Clear temp folder in local protected directory  
 Startup  
 Weekly Sun Mon Tue Wed Thu Fri Sat  
 Clear files in local protected directory  
 Delete file after download 0 Days  
 Delete file after modified 0 Days  
 Delete if all applied
- Copy to Non Protected Directory** (highlighted with a red border)  
 Not allowed (Recommended) Allowed Extensions: \_\_\_\_\_ Add Copy option  
 Allow all unsupported type \_\_\_\_\_ Delete  
 Allow extensions

Buttons: OK, Cancel, Apply

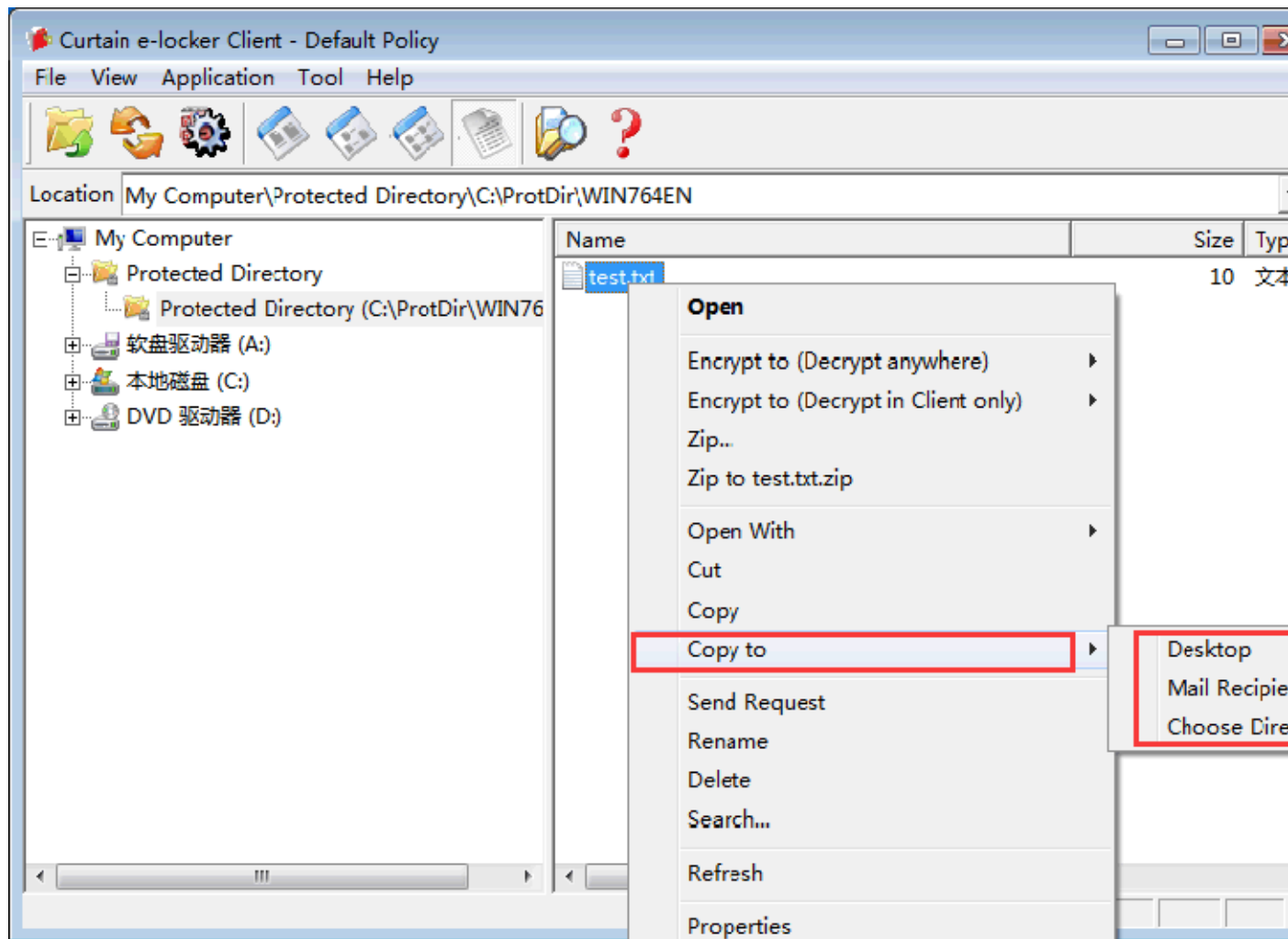
2. Enable "Allow extensions" and enter a file extension you want to allow copying (e.g. TXT)



3. Click "Add" and select "Yes" button .



4. Launch Curtain Client, Right click .txt file, select "Copy to" unprotected zone .



5. Done.

P.S. Please remember that this setting will override setting in Application Control. For example, if you do not allow this group to save/copy file out in MS Excel but allow copying XLS file out, the latter setting will override former setting.

## 9.2 - How to protect SolidWorks Enterprise PDM ?

High-level steps for setting up Curtain Protection for SolidWorks EPDM:

1. In Curtain Admin, protect the EPDM server.
2. In user's PC, use Secure EPDM View Setup to set Local File Vault to any folder under Local Protected Directory.
3. Done.

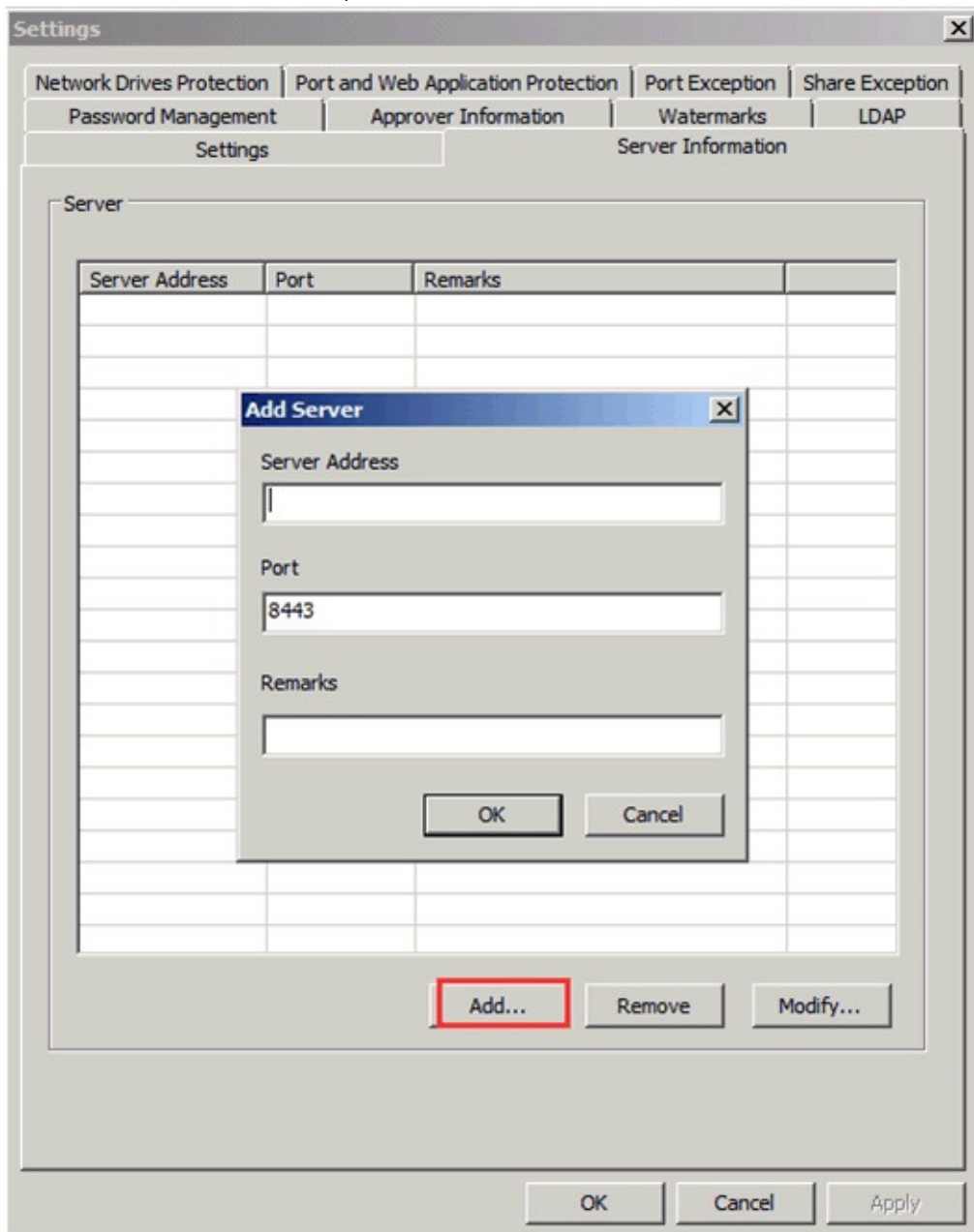
Detailed steps for the setup:

Step 1. In Curtain Admin, protect the EPDM server.

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

1.2. In Server Information tab, click Add button to add EPDM server information first.  
Server Address: Hostname or IP address of the EPDM server.

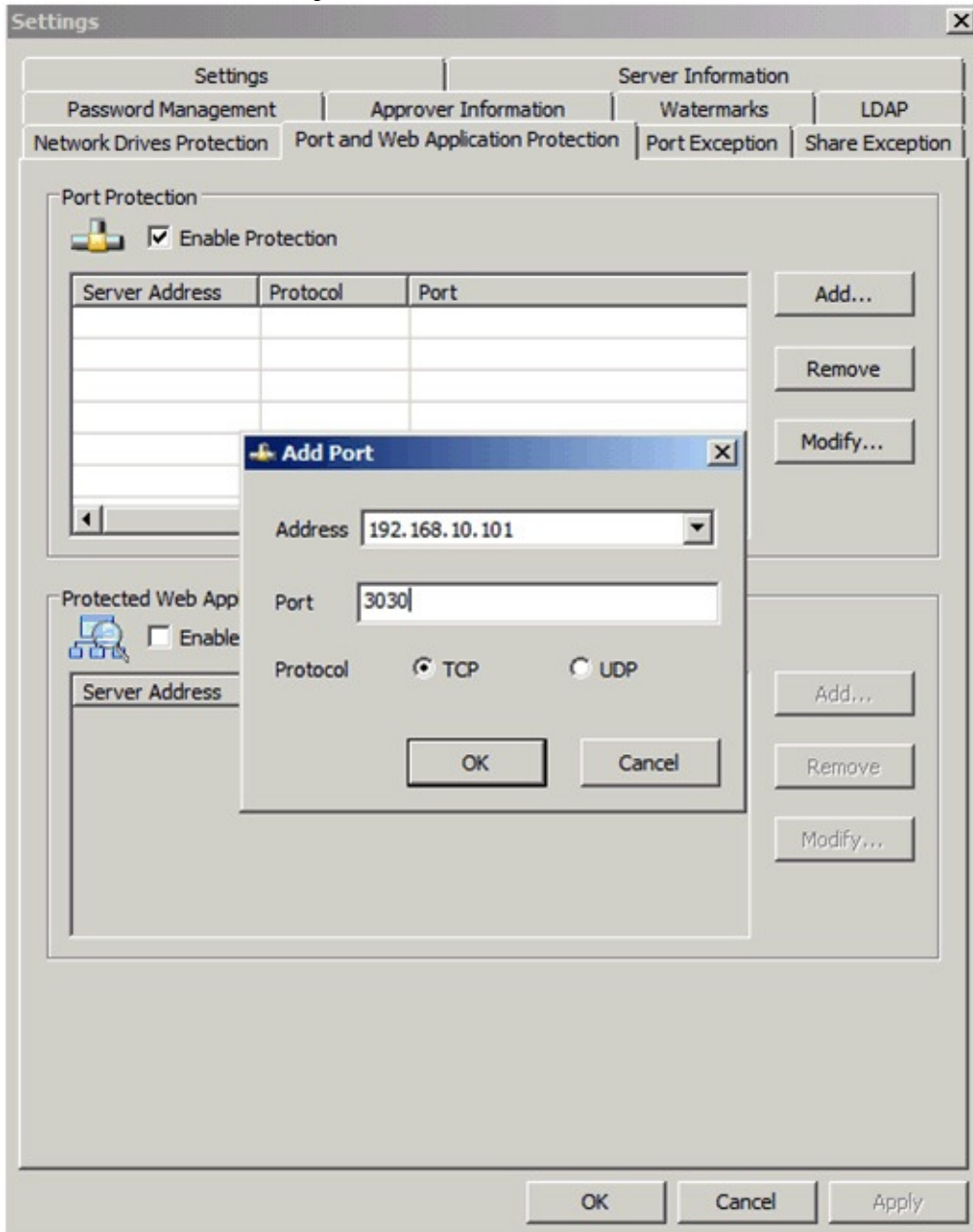
Port: Default value is Port 8443 (for communication between Curtain Admin and Curtain Server Plug-in).



1.3. Click "OK" to confirm.

## 1.4. Protect port for EPDM server.

- In Port Protection, check "Enable Protection".
- Click "Add" button, a dialog box will be shown.



- Address - Select the EPDM server (hostname or IP address)
- Port Number - Enter 3030 (default port for EPDM is 3030)
- Protocol - Select TCP (default protocol for EPDM is TCP)

## 1.5. Click OK to confirm.

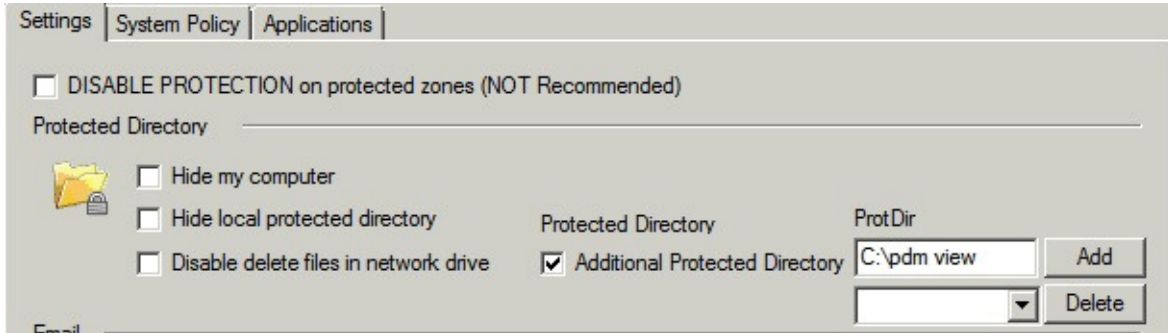
Step 2. In user's PC, use Secure EPDM View Setup to set Local File Vault to any folder under Local Protected Directory.

- If more than one user use EPDM in this PC, you need to use Additional Protected Directory because User A cannot Access Local Protected Directory of User B. Please follow Step 2.1 to continue.
- If only one user uses EPDM in this PC, please go to Step 2.4 to continue.

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

2.2. In Settings tab:

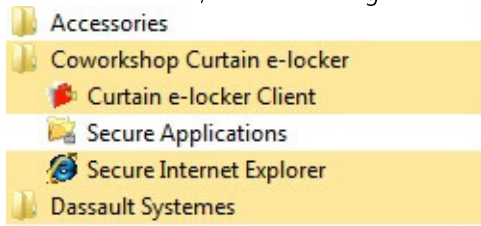
- Check "Additional Protected Directory" and enter the path.
- Click "Add" button to confirm.



2.3. The Additional Protected Directory will be shown after you restart Curtain Client.



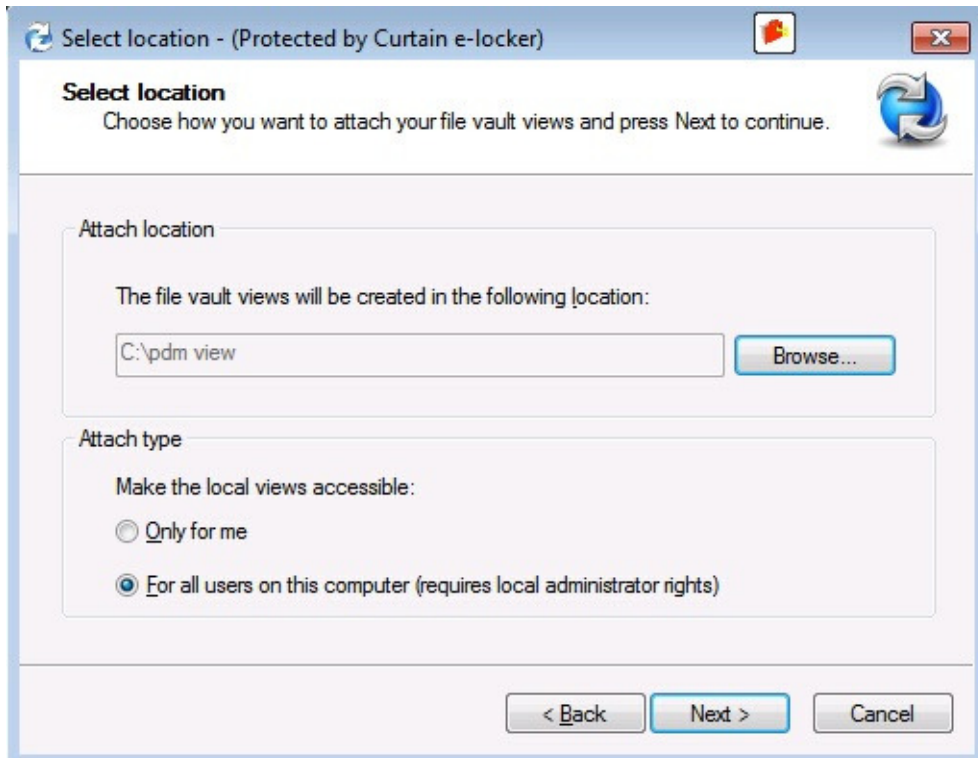
2.4. In start menu, select "All Programs > Coworkshop Curtain e-locker > Secure Applications".



2.5. Launch Secure EPDM View Setup.



2.6. Set Local File Vault to any folder under Local Protected Directory.



P.S. If more than one user use EPDM in this PC, the file vault views should be created in Additional Protected Directory.

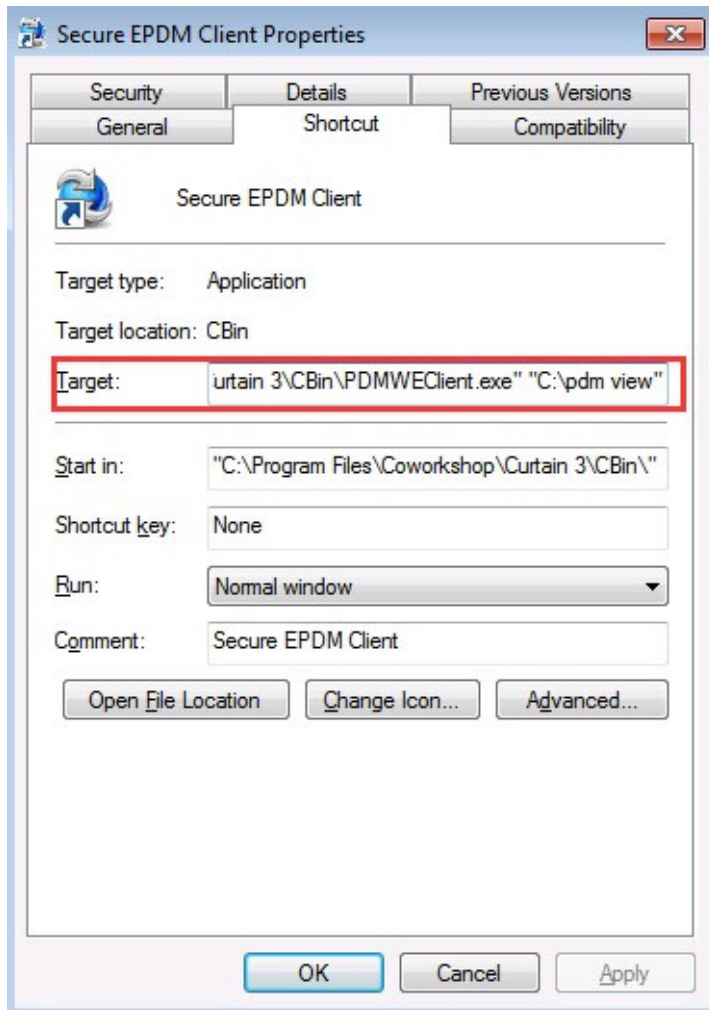
2.7. In Start menu, select "All Programs > Coworkshop Curtain e-locker > Secure Applications".

2.8. Select the shortcut of Secure EPDM Client and right-click to select "Properties".





2.9. Enter the path of EPDM local File Vault at the end of Target.



P.S. Please make sure that:

- You have used Secure EPDM View Setup to set Local File Vault to this Additional Local Protected Directory.

2.10. Access EPDM by using Secure EPDM Client.

