Curtain™ e-locker 3.8

Installation Guide

Release date: May 1, 2010
Copyright (c) 2002-2010. Coworkshop Solutions Limited

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

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

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

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

© 2002-2010 Coworkshop Solutions Ltd. All Rights Reserved. Curtain belongs to Coworkshop Solutions Ltd. All other brand names, product names, or trademarks belong to their respective holders.

Table of Contents

1 - Introduction

1.1 - 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 or remove an electronic 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.

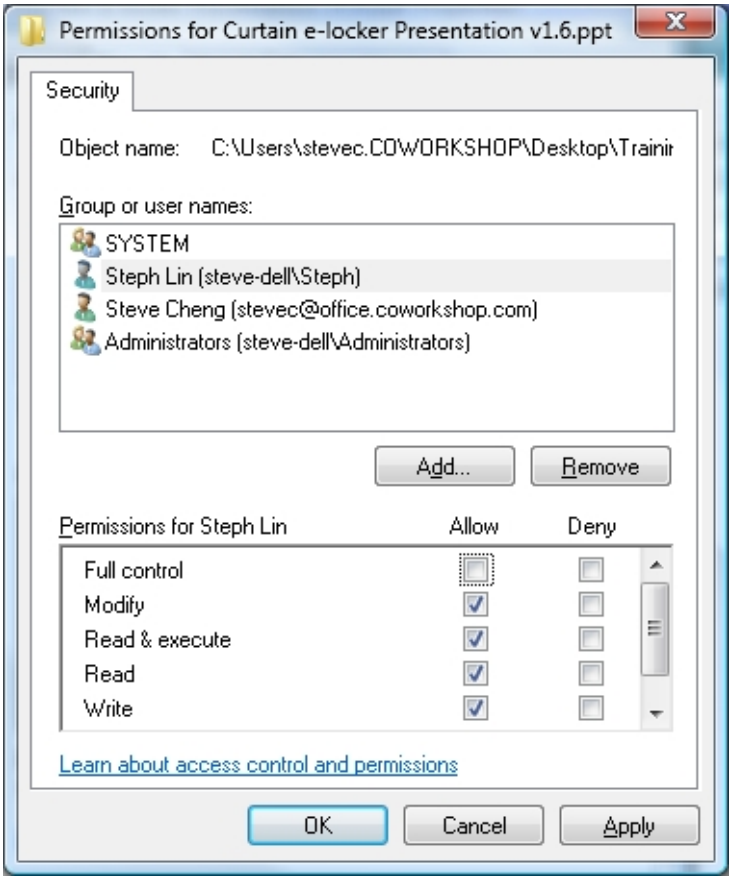
1.2 - What is the purpose of Curtain e-locker?

Curtain e-locker – an Information Rights Management 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
- Infra-red or Bluetooth
- ICQ, MSN, 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, MSN, 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.

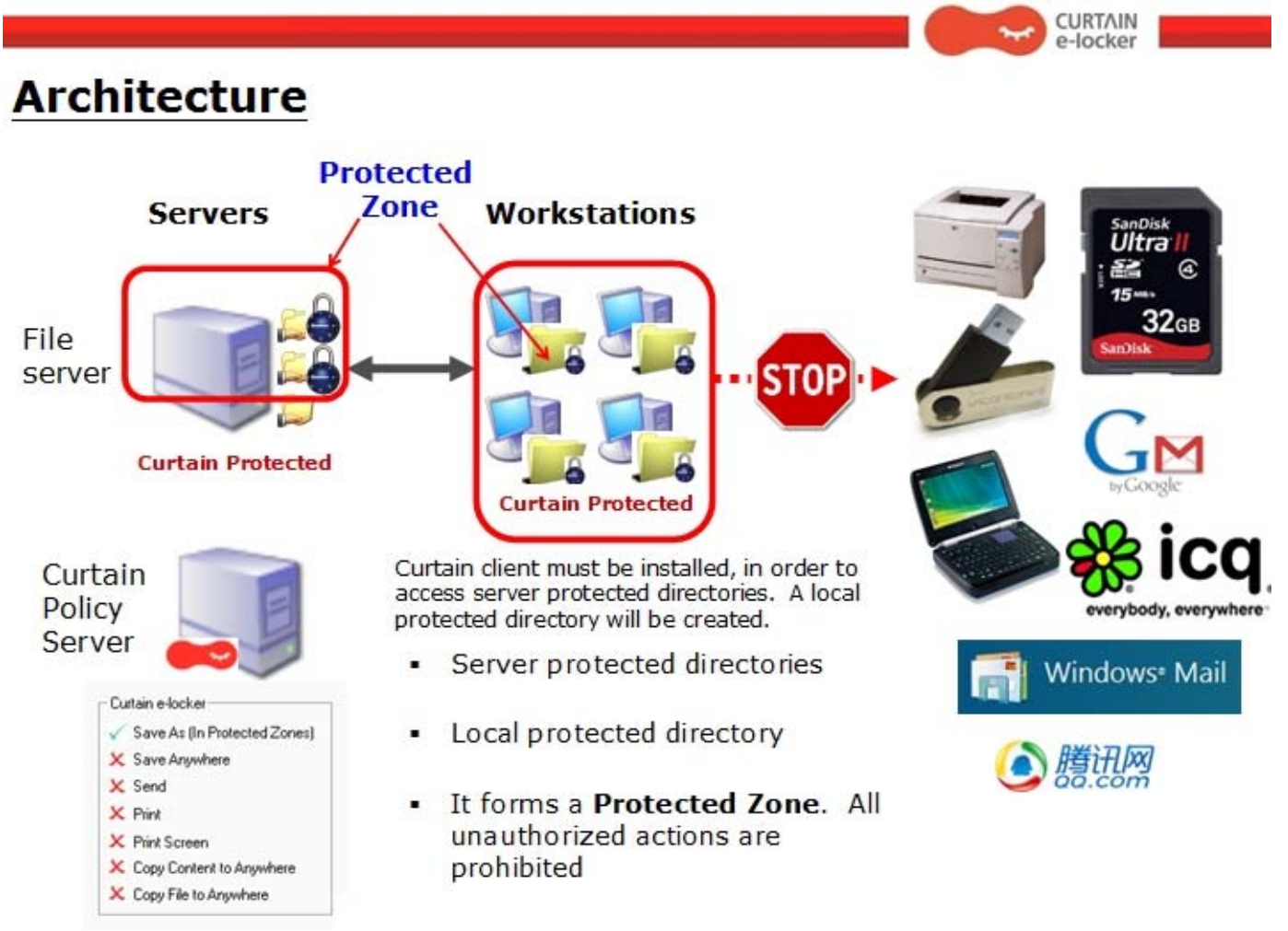
Administrators can define different control policy groups. Please refer to related documents.

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. 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. An encrypted folder (i.e. Local Protected Directory) will be automatically created 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. 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, etc.



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

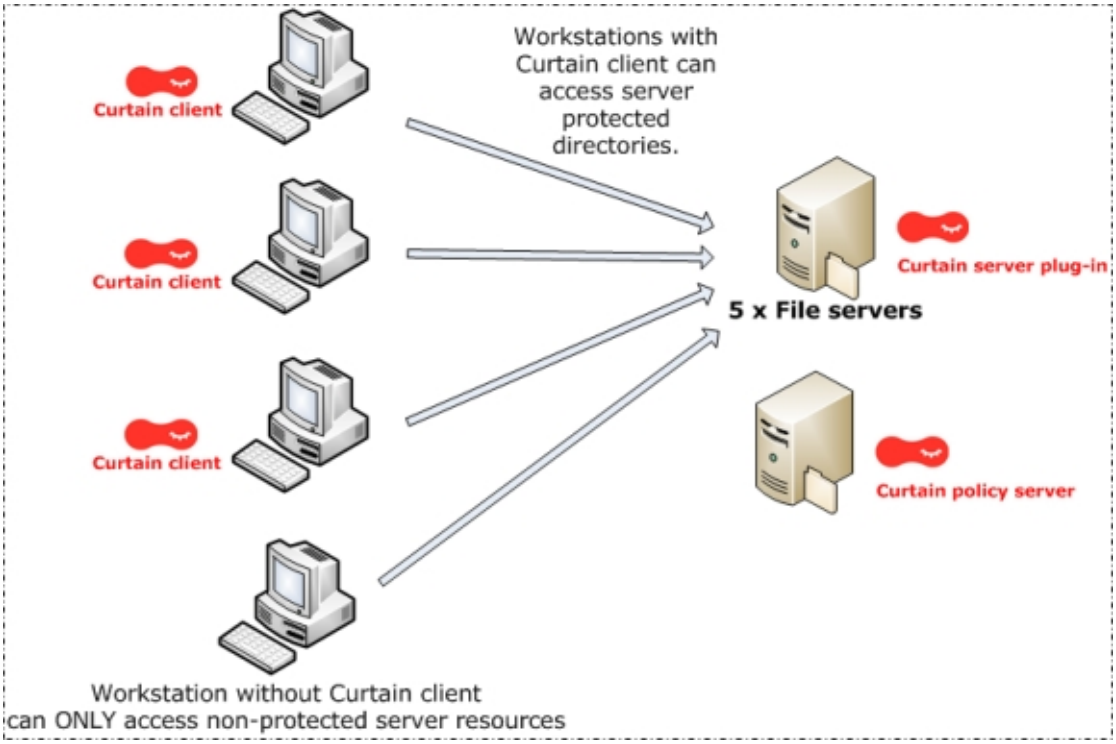
Curtain Client:
When a user accesses Protected server resources (e.g. Protected Share Folder, Protected website, etc), Curtain Client must be installed in the user's workstation. An encrypted folder (i.e. Local Protected Directory) will be automatically created during installation of Curtain Client.

Curtain Admin:
Curtain Admin is for system administrators to define Curtain control policies centrally. 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.

Here is the basic architecture of Curtain e-locker:

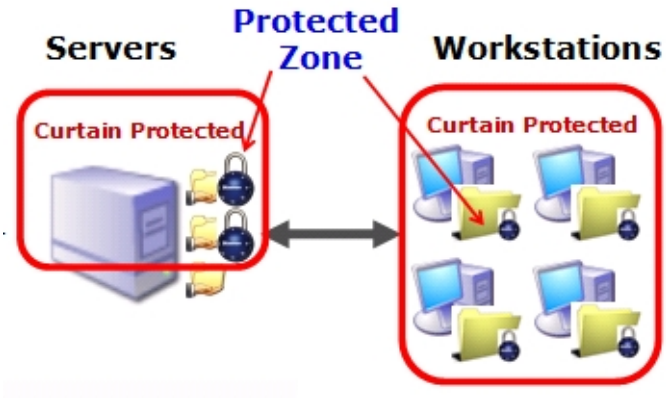


P.S. Curtain Admin can be installed on a separated machine or one of the File Servers.

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 Protected Share Folder in file server, Protected website, 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.

2 - Preparation before Installation

2.1 - High-level Installation Plan

Preparation:

- Which server resources does your company want to protect (e.g. Protected Share Folder, Protected website, etc)?
- Who will access the Protected server resources?
- Which server will act as Curtain Policy server (i.e. Curtain Admin will be installed on that server)?

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. Define Protected server resources
6. Configure control policy groups in Curtain Admin
7. Assign users' workstations to different policy groups
8. 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 2000 SP4 or above/XP Professional/2003/Vista operating system
- 128MB RAM (Recommended 256MB RAM)
- 60MB Hard Disk (in NTFS) for installation
- TCP/IP network
- TCP Port 24821 and 24822 are open for communication (Note: if firewall exists in the network, please make sure these two communication ports are not disabled)
- For 64-bit OS, MSXML 6 is required (It can be download from Microsoft website)

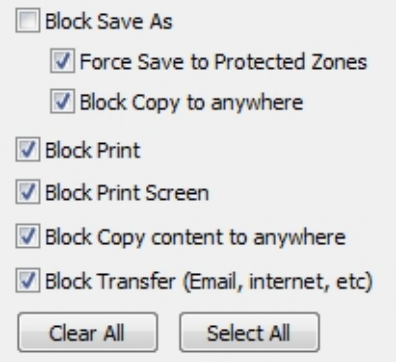
2.2.2 - System Requirements of Curtain Client

System Requirements of Curtain Client:

- Intel Pentium or above processor
- Windows 2000 SP4 or above/XP/2003/Vista/Windows 7 operating system
- 128MB RAM (Recommended 256MB RAM)
- 50MB Hard Disk (in NTFS) for installation
- TCP/IP network
- TCP Port 24821 and 24822 are open for communication (Note: if firewall exists in the network, please make sure these two communication ports are not disabled)
- For 64-bit OS, MSXML 6 is required (It can be download from Microsoft website)

2.3 - Curtain Basic Access Rights

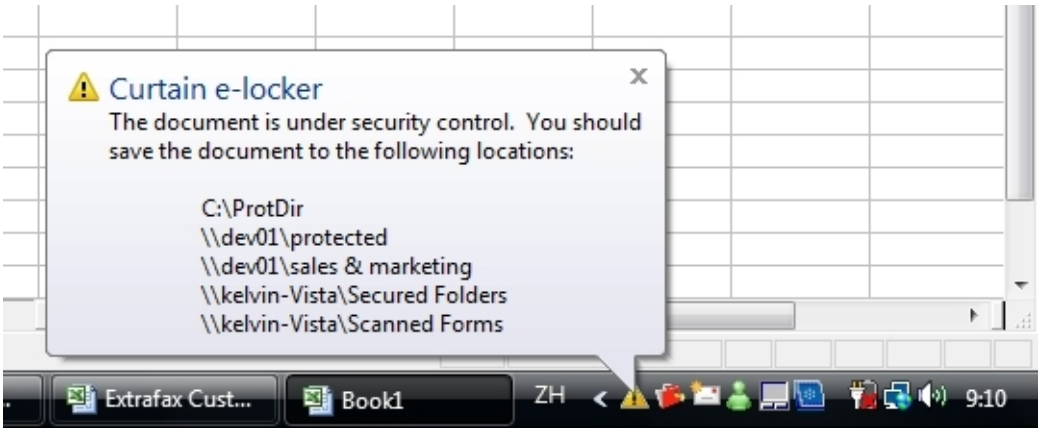
Curtain access rights can be defined by Policy Group and Application. Here is default setting of Curtain access right.



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

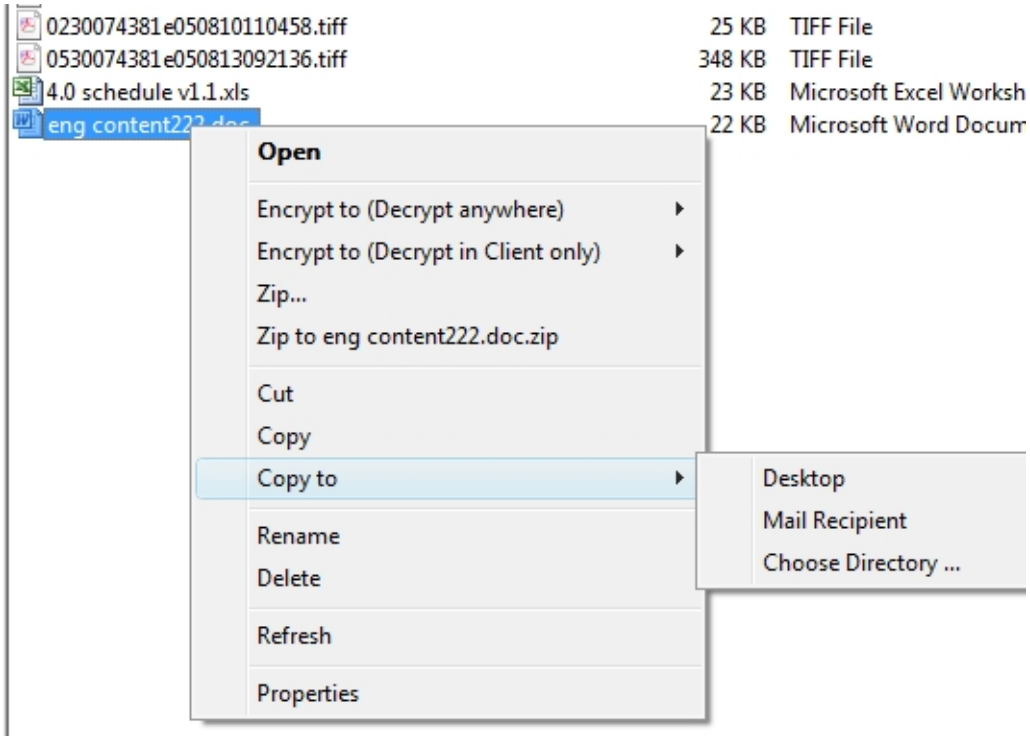
Examples of using Curtain access rights

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.

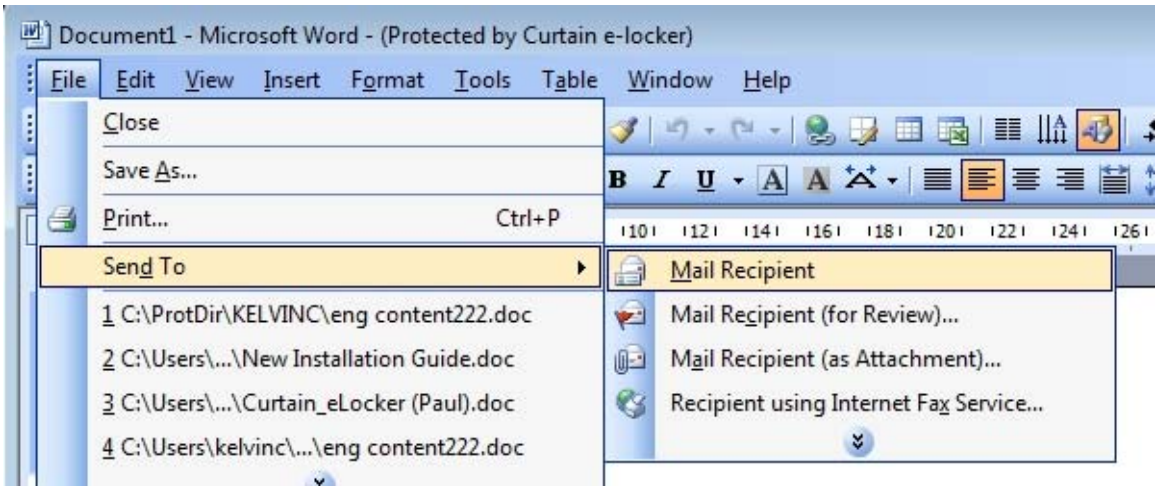


For scenario 2 - "Block Copy to anywhere" is disabled for MS Word:
- In Curtain Client, select a Word document and right-click. You can see an entry called "Copy to". You can use this function to copy Word documents out of Protected Zone.

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.



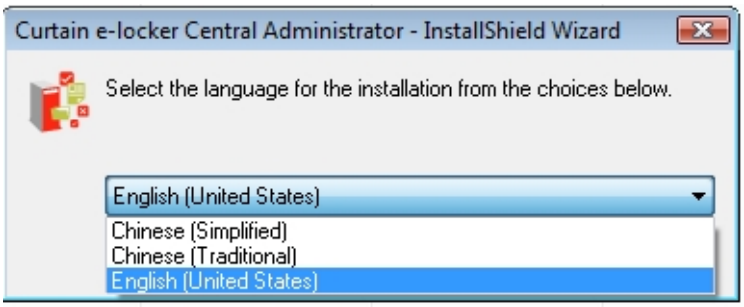
3 - Installation

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.

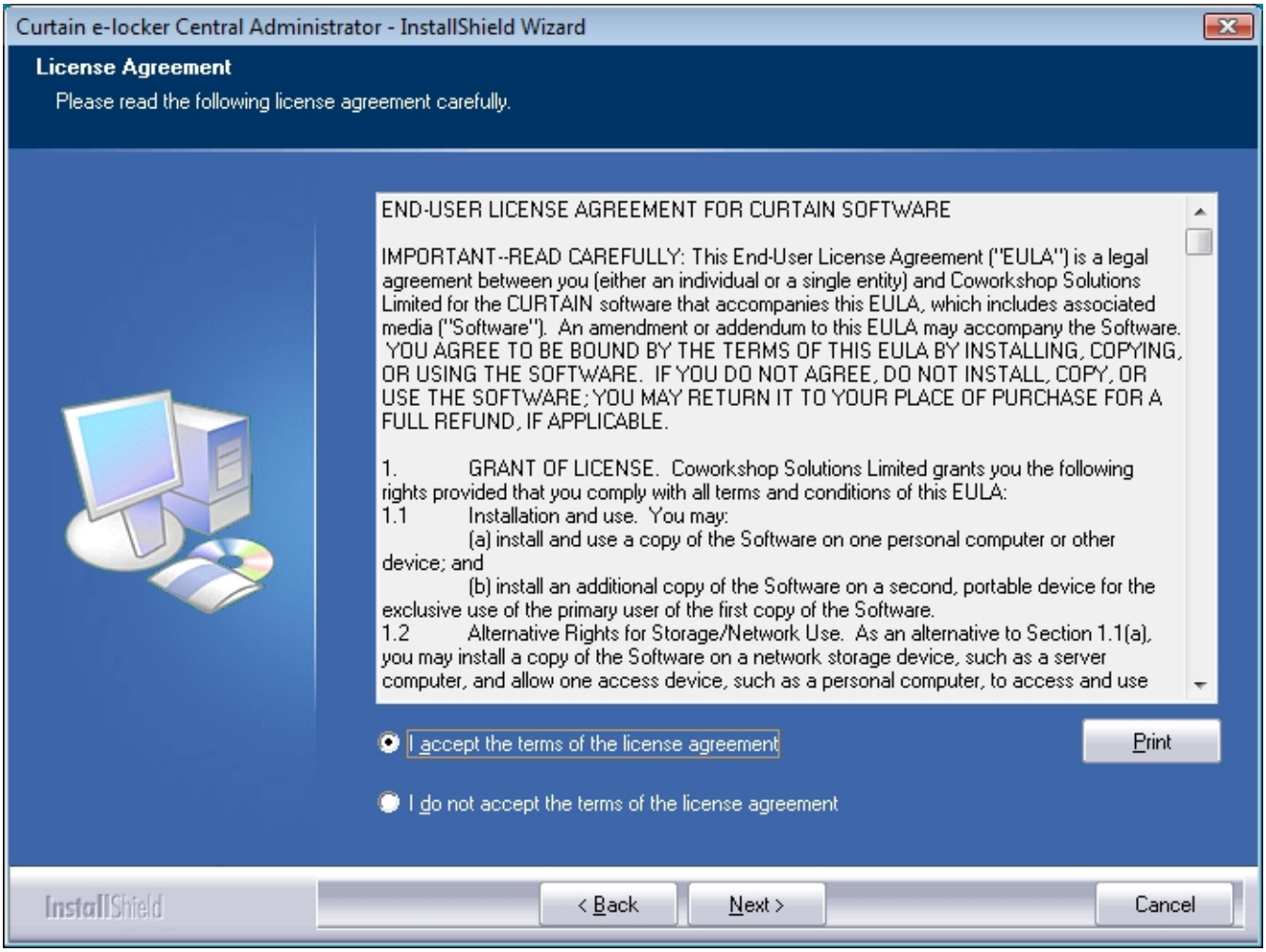
Steps to install Curtain Admin:
1. Copy Curtain server setup program (i.e. Curtain3Admin.exe) to local hard-disk of the server.

2. Run Curtain server setup program (i.e. Curtain3Admin.exe). Make sure that you login Windows with administrator right.
Then, you will be asked to select Language for the installation.

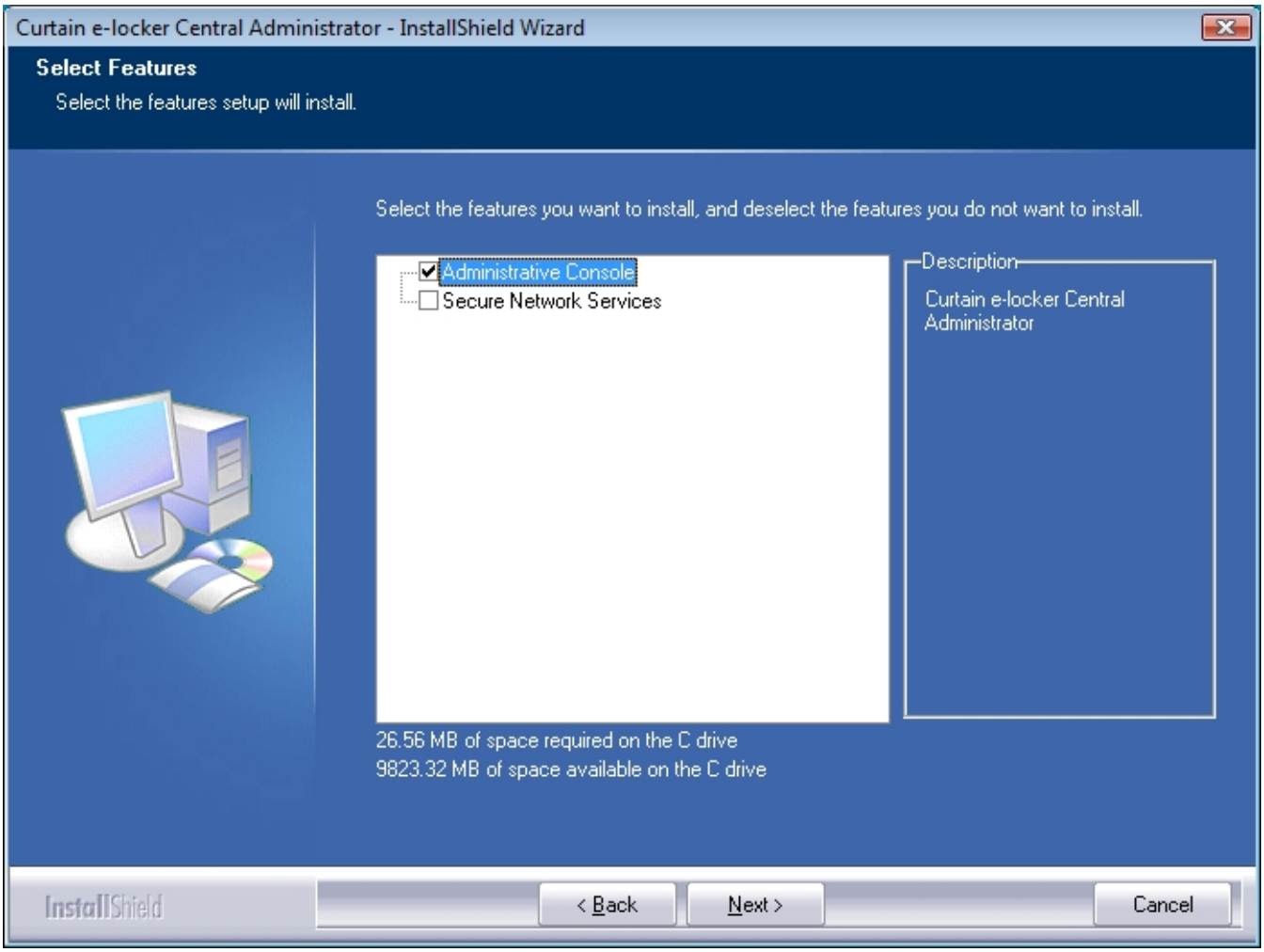


3. Select a language and click OK.

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


Curtain e-locker Central Administrator - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
END-USER LICENSE AGREEMENT FOR CURTAIN SOFTWARE
IMPORTANT--READ CAREFULLY: This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and Coworkshop Solutions Limited for the CURTAIN software that accompanies this EULA, which includes associated media ("Software"). An amendment or addendum to this EULA may accompany the Software. YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA BY INSTALLING, COPYING, OR USING THE SOFTWARE. IF YOU DO NOT AGREE, DO NOT INSTALL, COPY, OR USE THE SOFTWARE; YOU MAY RETURN IT TO YOUR PLACE OF PURCHASE FOR A FULL REFUND, IF APPLICABLE.
1. GRANT OF LICENSE. Coworkshop Solutions Limited grants you the following rights provided that you comply with all terms and conditions of this EULA:
1.1 Installation and use. You may:
(a) install and use a copy of the Software on one personal computer or other device; and
(b) install an additional copy of the Software on a second, portable device for the exclusive use of the primary user of the first copy of the Software.
1.2 Alternative Rights for Storage/Network Use. As an alternative to Section 1.1(a), you may install a copy of the Software on a network storage device, such as a server computer, and allow one access device, such as a personal computer, to access and use
I accept the terms of the license agreement
I do not accept the terms of the license agreement
Print
InstallShield
< Back
Next >
Cancel

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



5. There are two scenarios:
(a) If you only want to install Curtain Admin on this server,
- only select "Administrative Console" to install Curtain Admin.

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

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

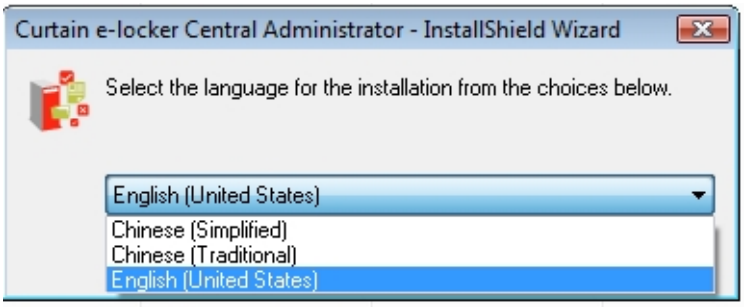
7. Click Install to start the installation.

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.

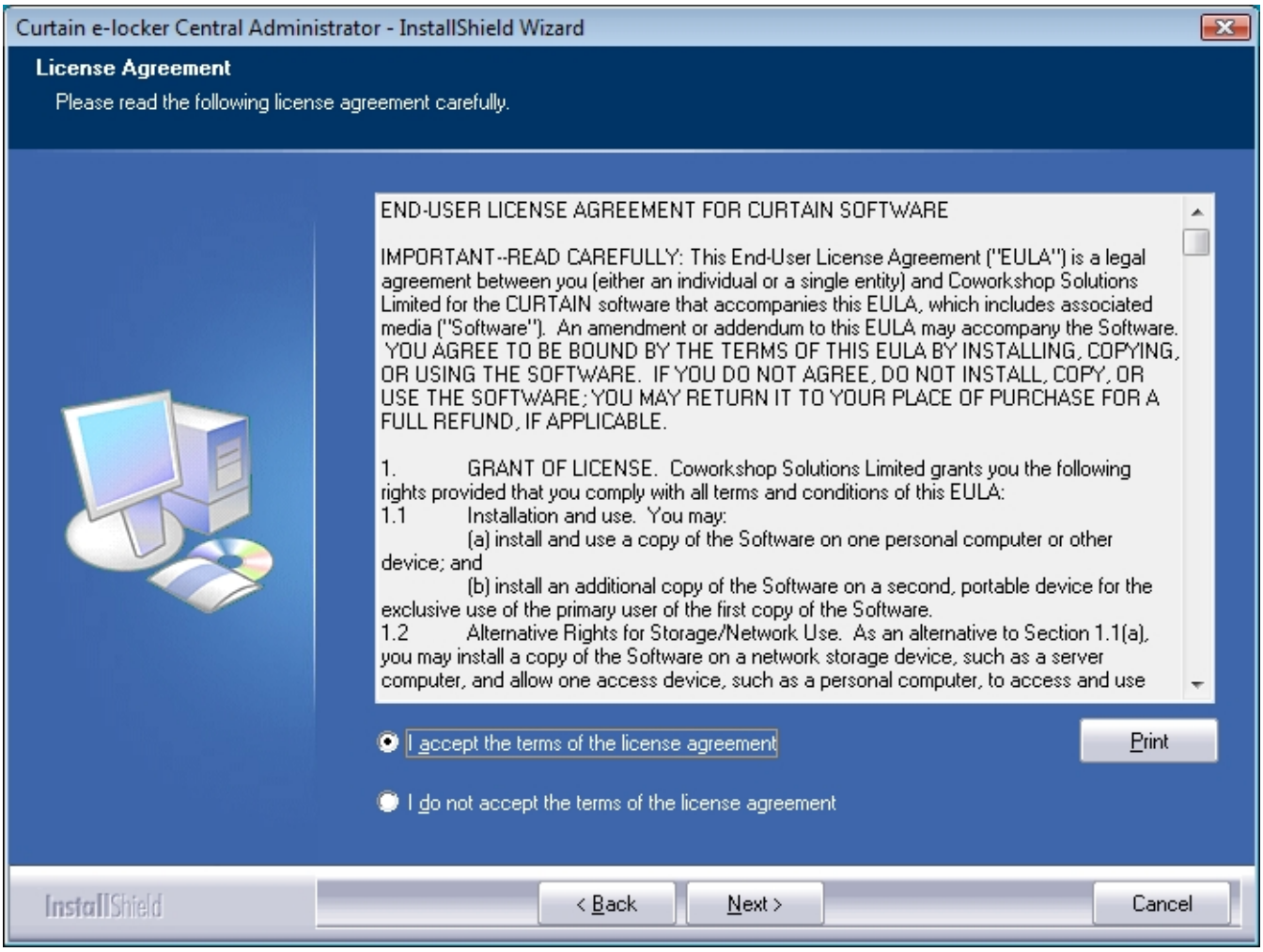
Steps to install Curtain Server Plug-in:
1. Copy Curtain server setup program (i.e. Curtain3Admin.exe) to local hard-disk of the server.

2. Run Curtain server setup program (i.e. Curtain3Admin.exe). Make sure that you login Windows with administrator right.
Then, you will be asked to select Language for the installation.

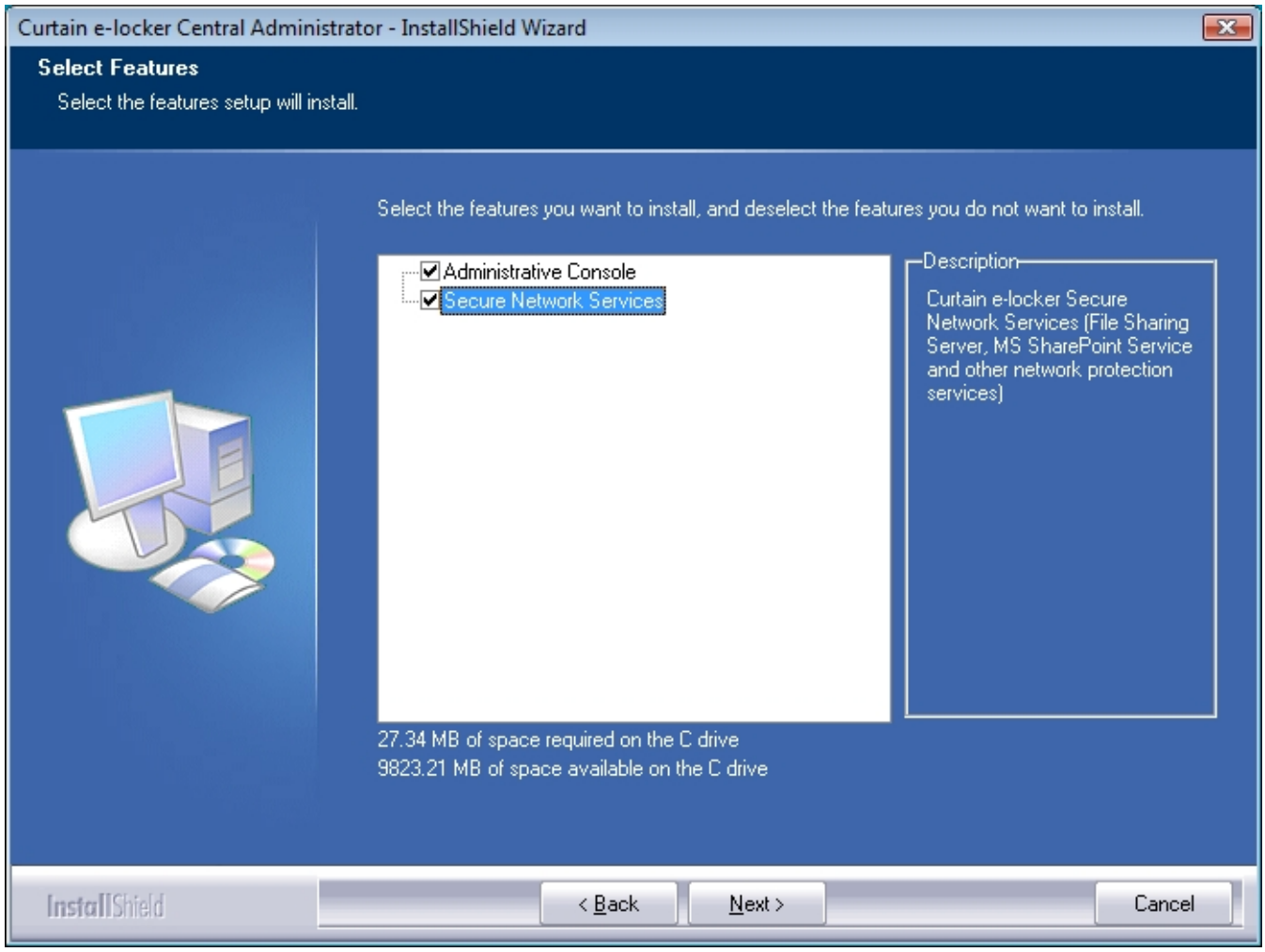


3. Select a language and click OK.

4. 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.



5. ONLY Select "Secure Network Services" to install Curtain Server Plug-in, and click Next to continue.

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

7. Click Install to start the installation.

3.3 - Install Curtain Client

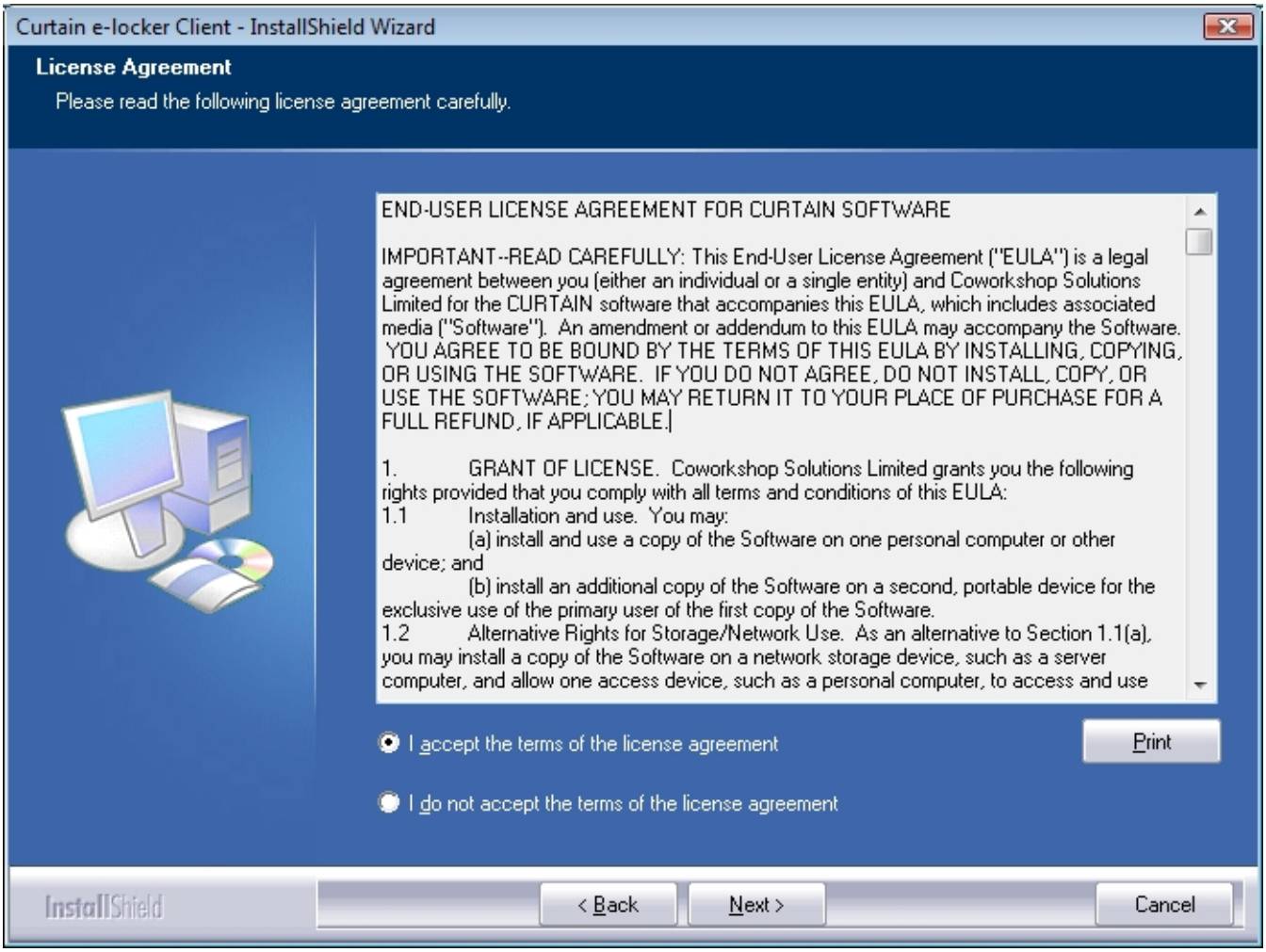
If a user needs to access Protected server resources (e.g. Protected Share Folder, Protected website, etc), you should install Curtain Client on the user's workstation. There are two ways to install Curtain Client:
(1) Run Curtain Client setup program on user's workstation
(2) Install Curtain Client remotely from Curtain Admin

Method 1 - Run Curtain Client setup program on user's workstation:
1. Copy Curtain client setup program (i.e. Curtain3Client_SA.exe) to local hard-disk of user's workstation.

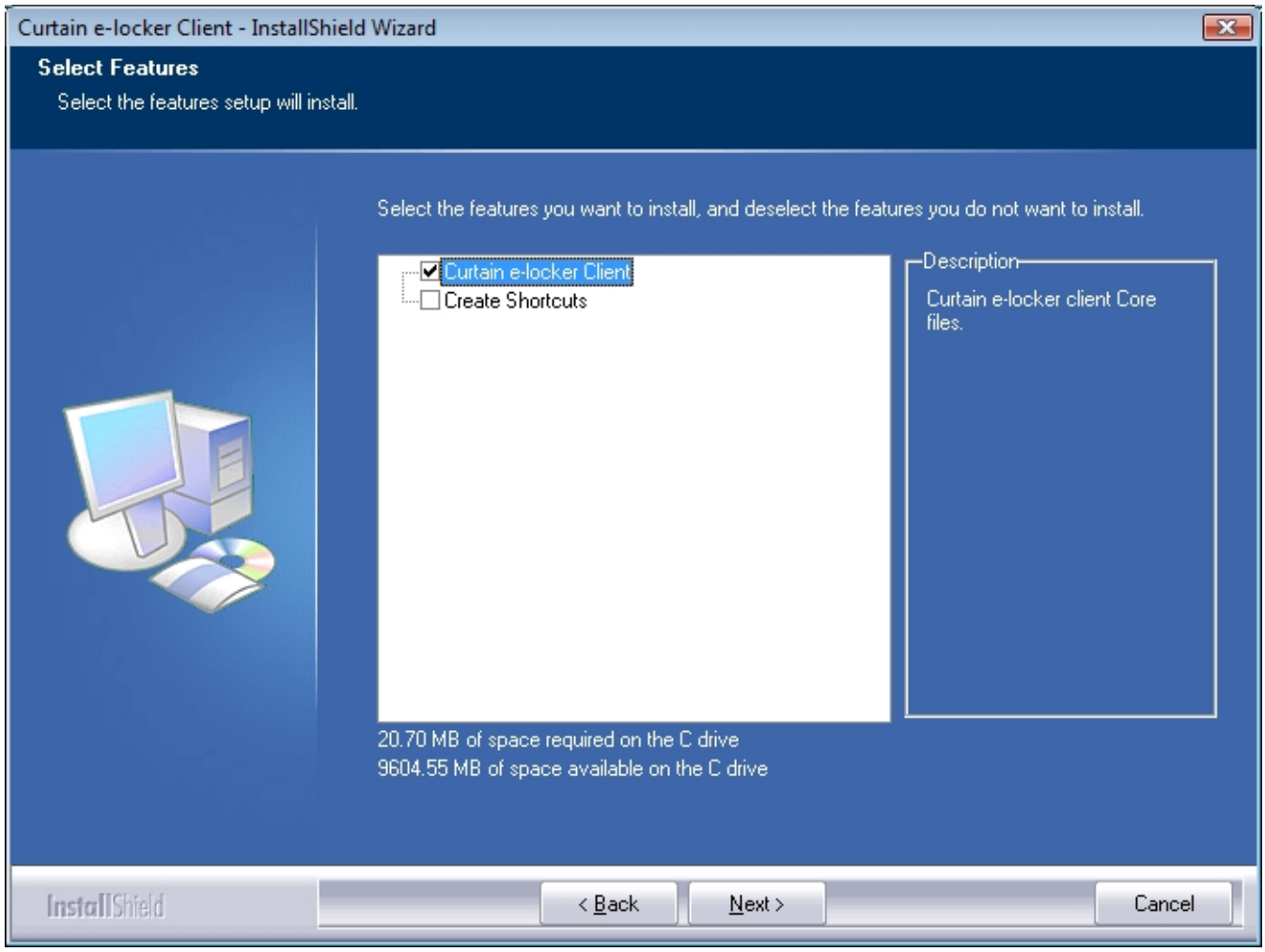
2. Run Curtain client setup program (i.e. Curtain3Client_SA.exe). Make sure that you login Windows with administrator right.
Then, you will be asked to select Language for the installation.

3. Select a language and click OK.

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

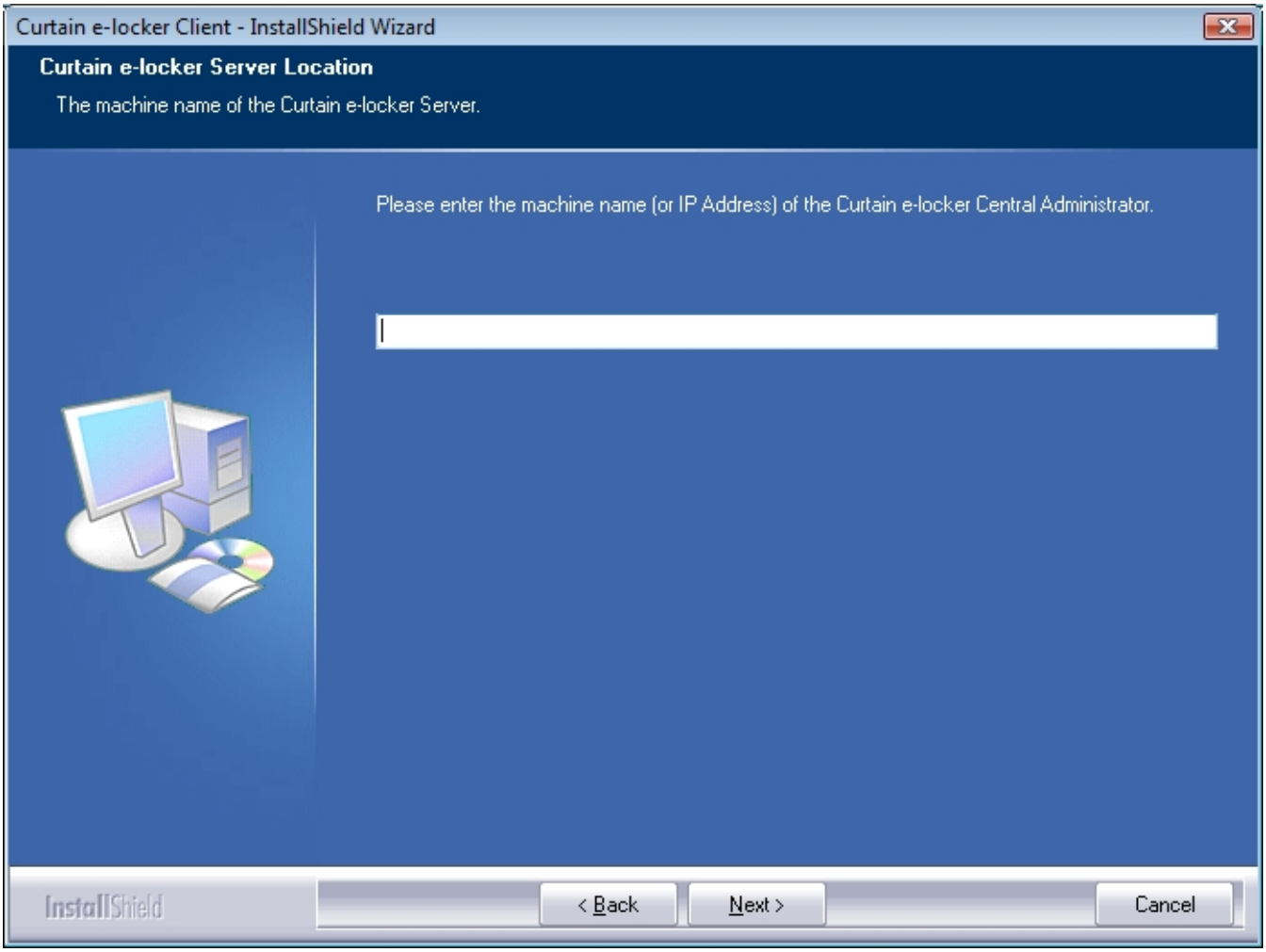

Curtain e-locker Client - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
END-USER LICENSE AGREEMENT FOR CURTAIN SOFTWARE
IMPORTANT--READ CAREFULLY: This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and Coworkshop Solutions Limited for the CURTAIN software that accompanies this EULA, which includes associated media ("Software"). An amendment or addendum to this EULA may accompany the Software. YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA BY INSTALLING, COPYING, OR USING THE SOFTWARE. IF YOU DO NOT AGREE, DO NOT INSTALL, COPY, OR USE THE SOFTWARE; YOU MAY RETURN IT TO YOUR PLACE OF PURCHASE FOR A FULL REFUND, IF APPLICABLE.
1. GRANT OF LICENSE. Coworkshop Solutions Limited grants you the following rights provided that you comply with all terms and conditions of this EULA:
1.1 Installation and use. You may:
(a) install and use a copy of the Software on one personal computer or other device; and
(b) install an additional copy of the Software on a second, portable device for the exclusive use of the primary user of the first copy of the Software.
1.2 Alternative Rights for Storage/Network Use. As an alternative to Section 1.1(a), you may install a copy of the Software on a network storage device, such as a server computer, and allow one access device, such as a personal computer, to access and use
I accept the terms of the license agreement
I do not accept the terms of the license agreement
Print
InstallShield
< Back
Next >
Cancel

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



5. If you also want to create Shortcuts for Curtain Protected Applications,
- select "Curtain e-locker Client" to install Curtain Client, and
- select "Create Shortcuts" to create shortcuts for Curtain Protected Applications.
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.

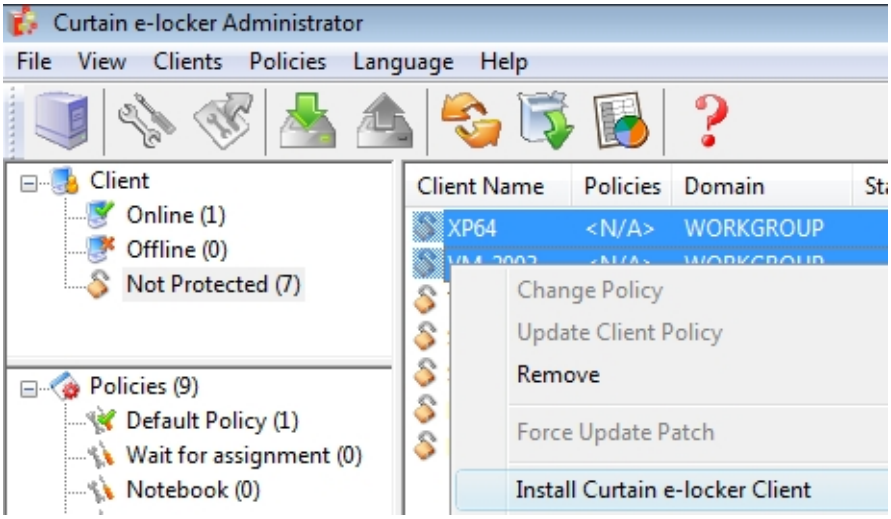
8. Click Install to start the installation.

9. Reboot the workstation after installing Curtain Client.

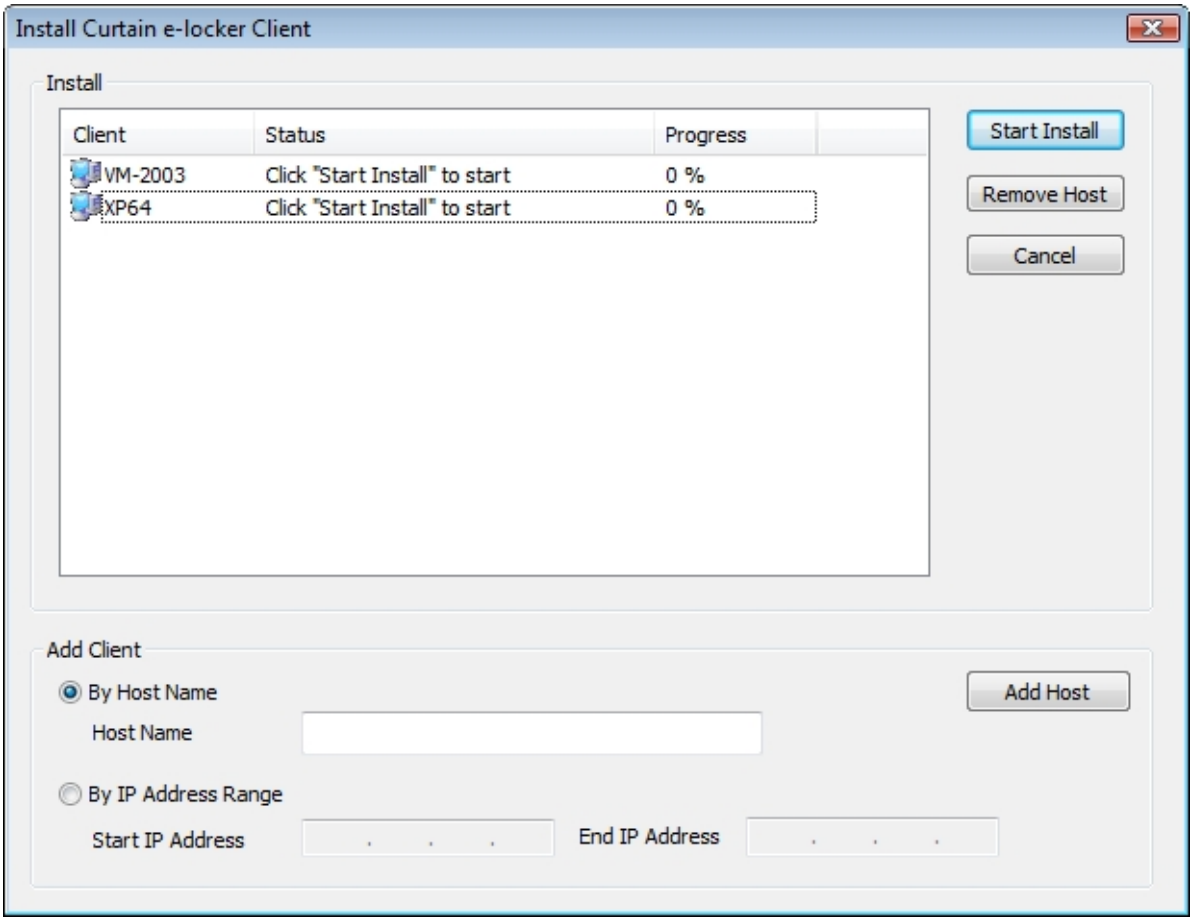
Method 2 - Install Curtain Client remotely from Curtain Admin:

Before starting Remote Installation, please make sure requirements below are fulfilled.
(a) Must be a domain environment (this feature is not available for workgroup environment)
(b) Login Windows with domain administrator right
(c) TCP Port 24821 and 24822 are open for communication (Note: if firewall exists in the network, please make sure these two communication ports are not disabled)

1. In Curtain Admin, select "Not Protected". Then the system will explore and show all machines in your network.



2. Select a machine (or press Ctrl for multi-selection) and right-click to select "Install Curtain e-locker Client".



3. You can include more machines to the installation by hostname or a range of IP address.

4. Click "Start Install" button to continue. Then, Curtain Admin will start to install Curtain Client program to the selected workstations.

5. Reboot the workstations after finishing remote installation.

4 - Product Activation

4.1 - What is 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.

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

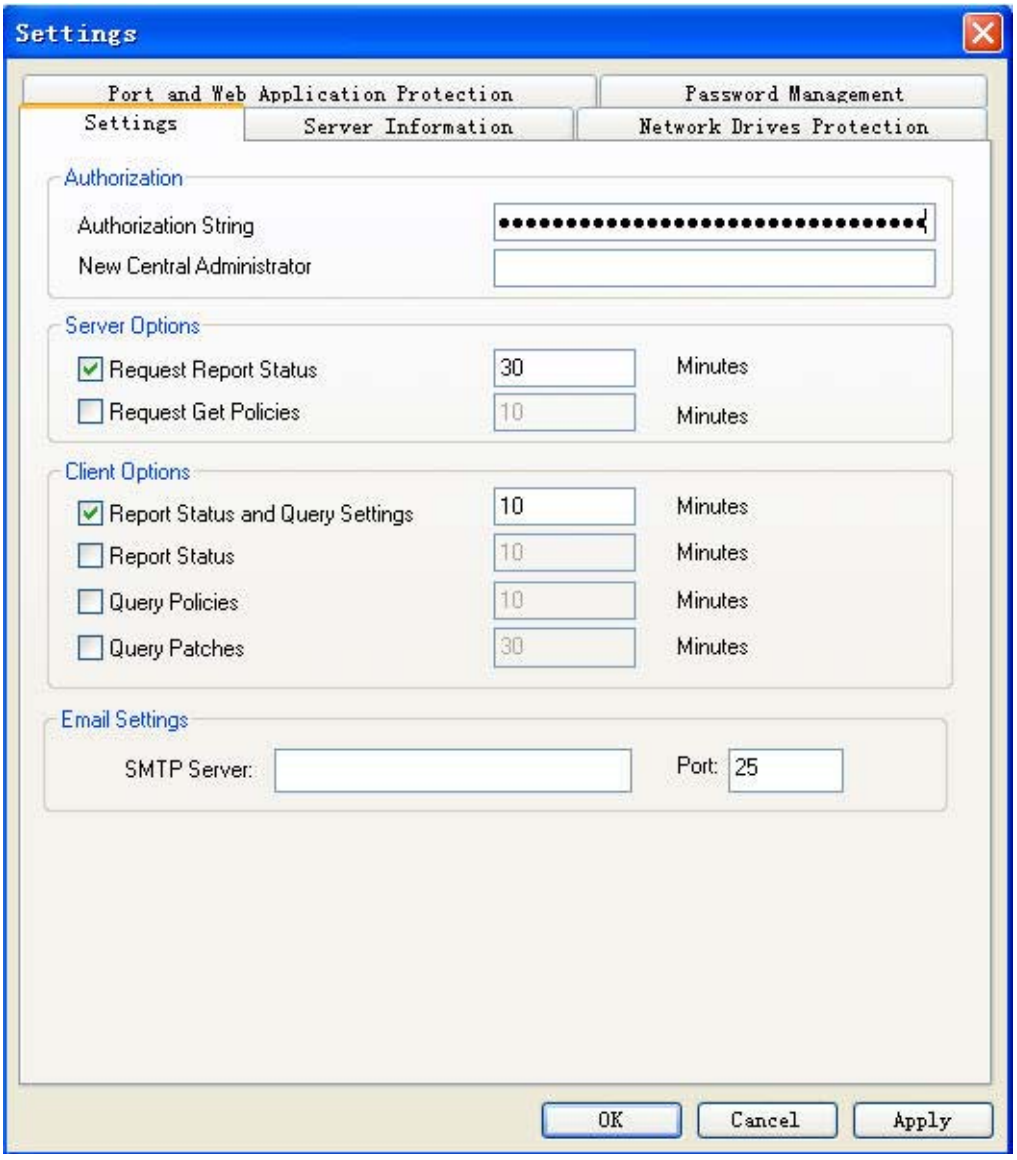
4. Click "Generate Request file..." button to generate Activation Request File, and send this file to Coworkshop (registration@coworkshop.com). After receiving your activation request, Coworkshop will send file(s) back to you.

- 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.



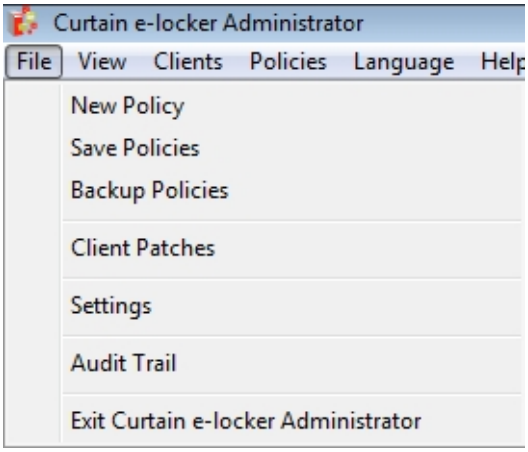
Congratulations! Curtain e-locker has been activated successfully.

5 - Configurations

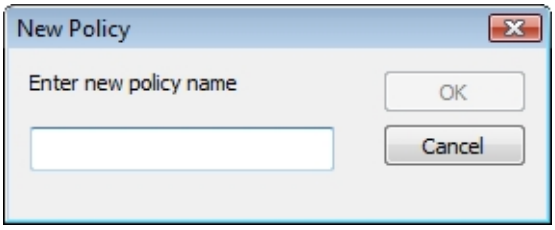
5.1 - Create Control Policy Group

Administrators can create many Control Policy Groups in Curtain Admin for different workstations. Here are some sample Control Policy Groups for reference.
- Top Management: Loose controls for management's workstations
- Notebook: Tight controls for notebooks
- Engineers/Sales/Designers: Appropriate controls for target groups

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.

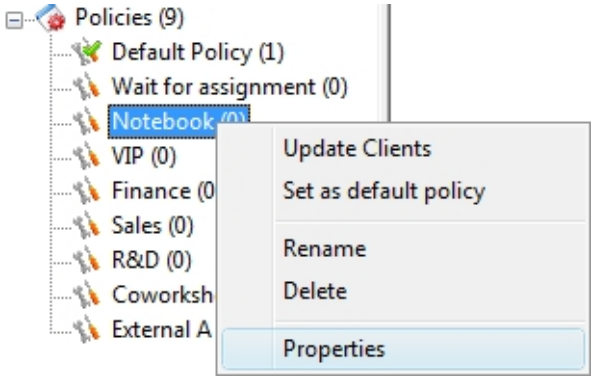


2. Enter new Policy Name and click OK to confirm.



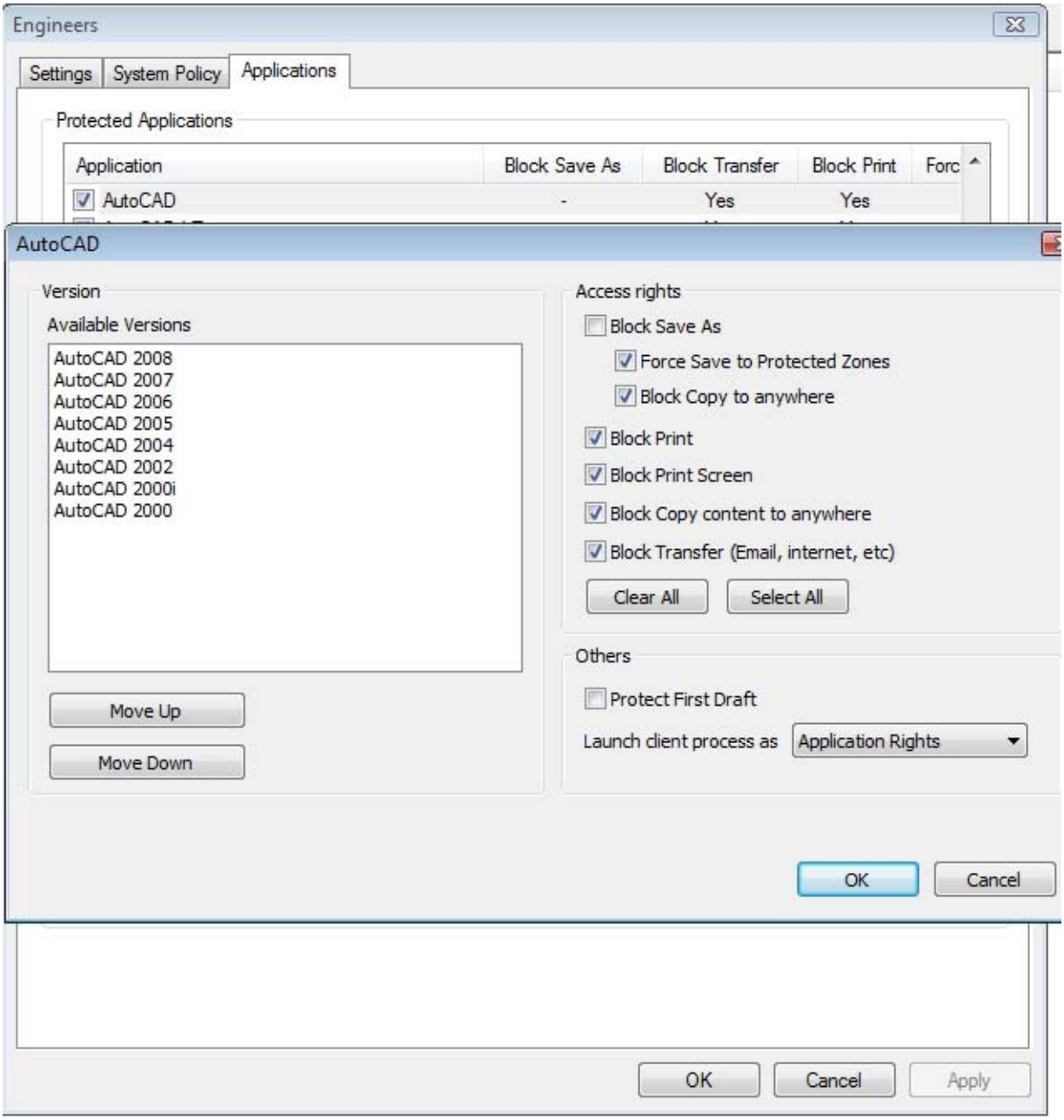
5.2 - Configure Control Policy Group

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



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

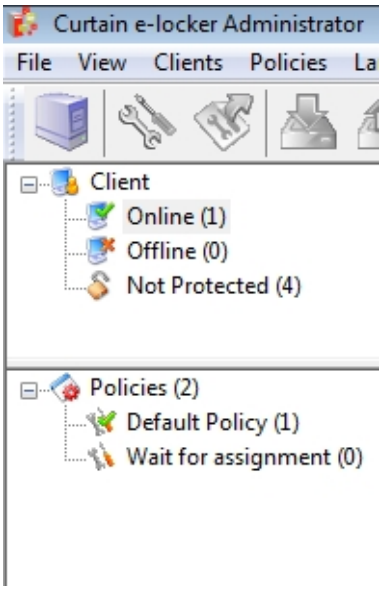
3. Define Curtain access rights and click OK to confirm.



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.

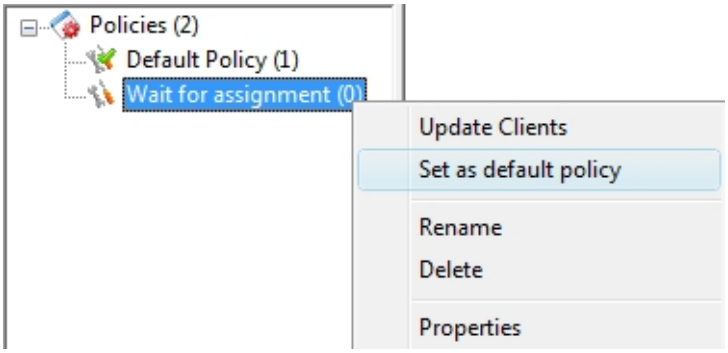


There are two built-in Control Policy Groups.
- Default Policy: With pre-defined settings of this Policy Group, users can work with sensitive documents in Protected Zone. But they cannot take the information out of the Zone.
- Wait for Assignment: With pre-defined settings of this Policy Group, users 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.

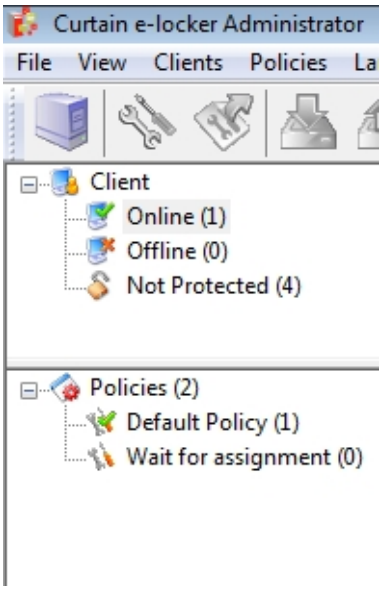
2. Select "Set as default policy"



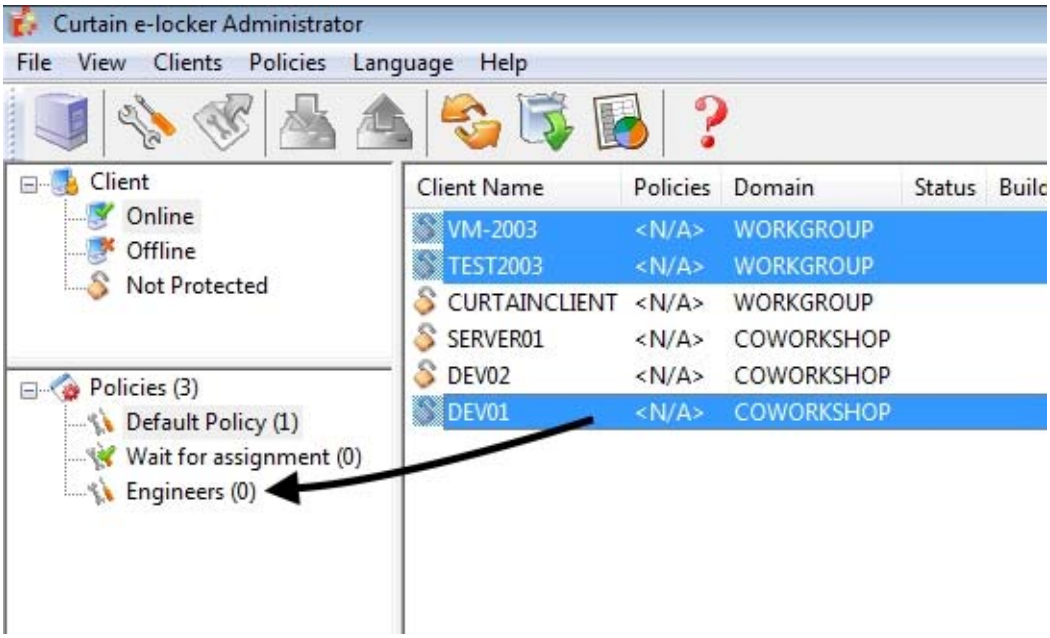
3. Done

5.4 - Assign workstations 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

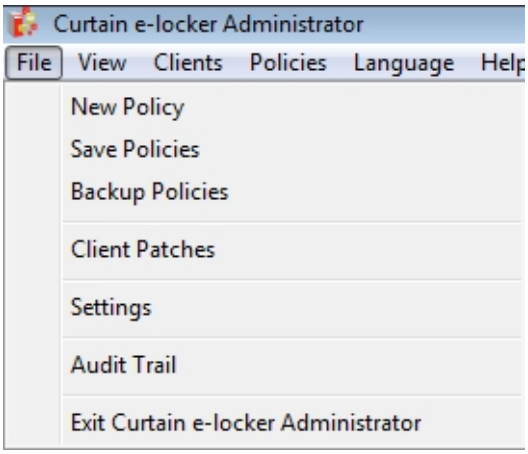


4. Repeat Step 2-3 for assigning other workstations to appropriate policy groups.
5. Done

5.5 - Define Protected Server Resources

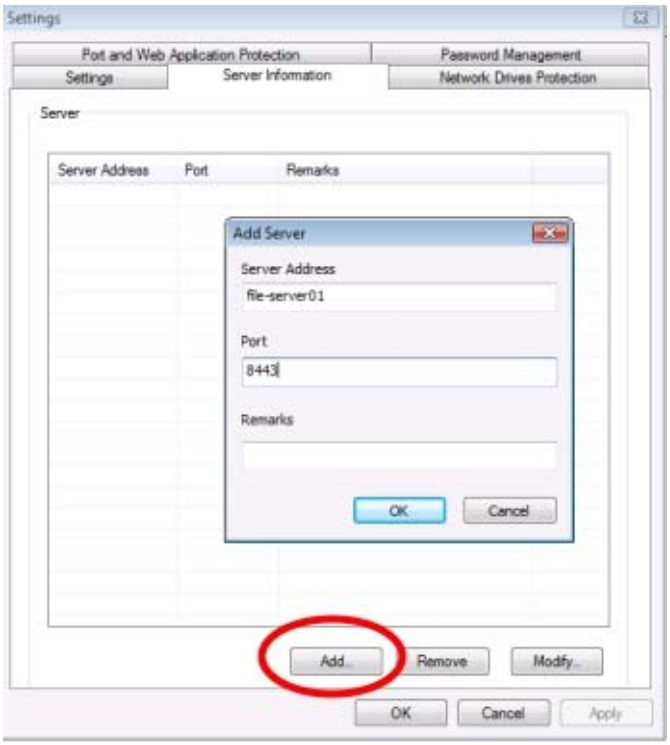
Curtain e-locker can be used to protect different kinds of server resources, such as share folders in Windows File Server, web application, or even self developed system. Please follow below steps to define Protected server resources.

Steps to define Protected server resources:
1. In Curtain Admin, select "File > Settings".



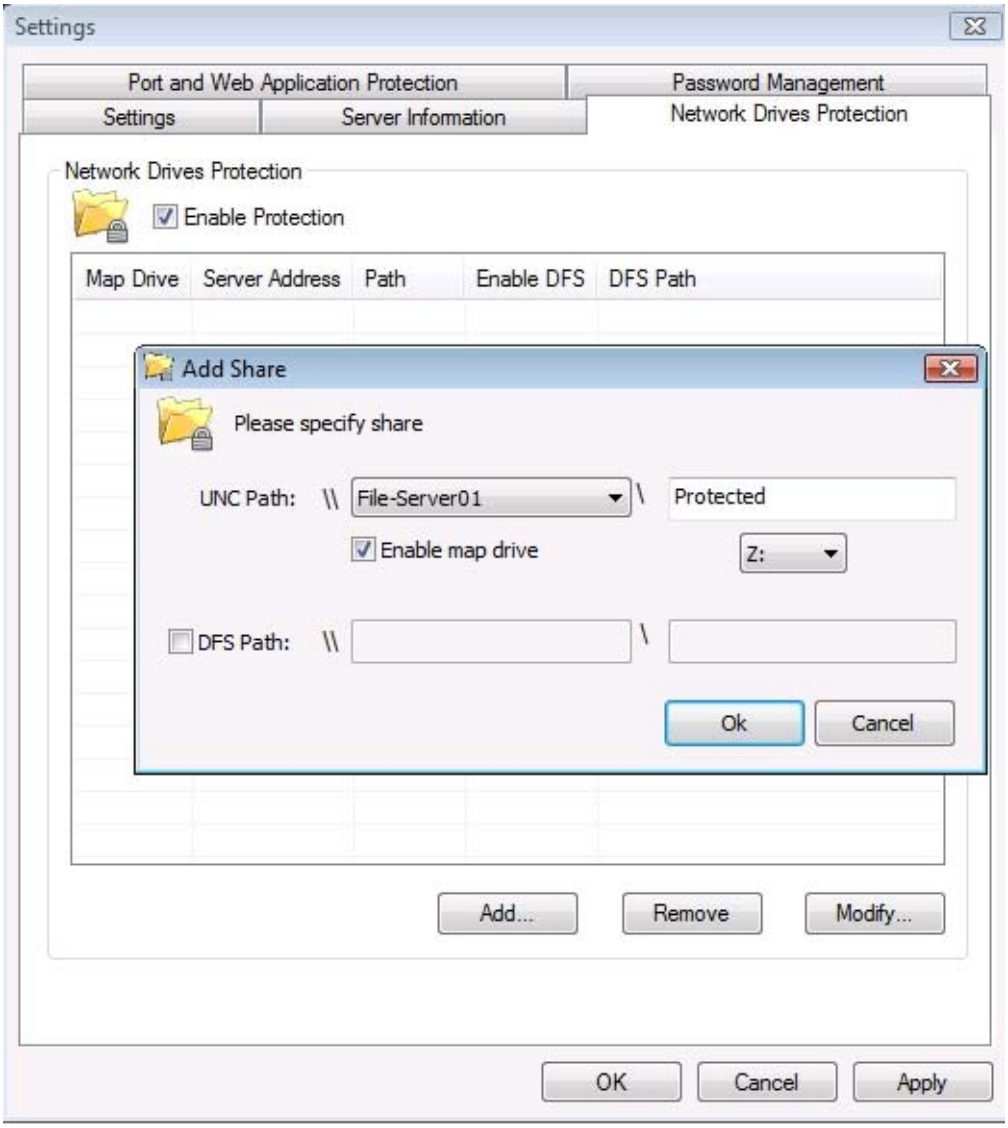
2. In Server Information tab, click Add button to add server information first. For example, if you want to protect share folders of two Windows File servers and one web application, you should add the three servers in this tab.

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.

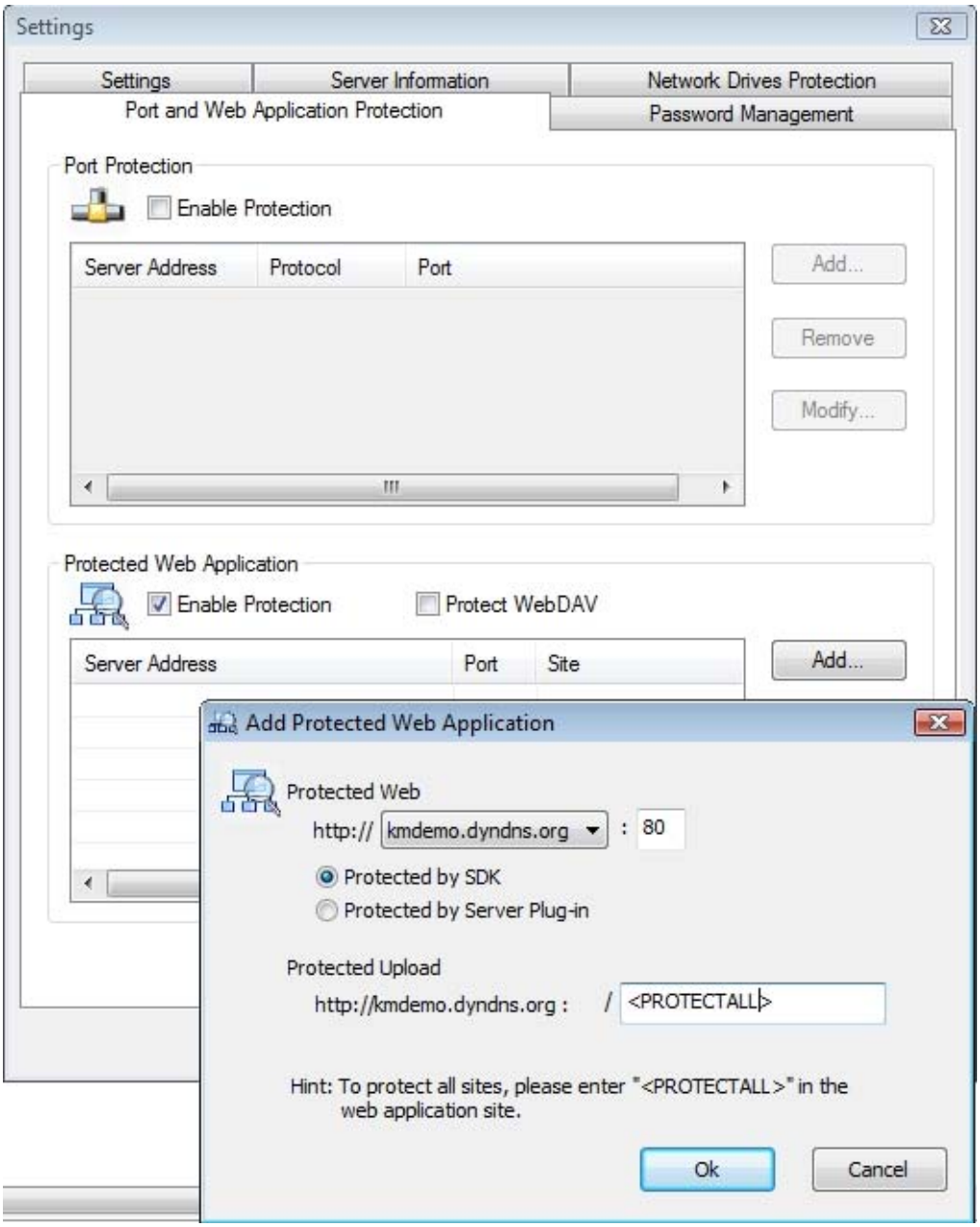


UNC Path: \\Server\Share Name
- Server - Select the server (hostname or IP address)
- Share Name - Enter name of the Share (not the folder name, unless you gave the Share the same name as the folder)

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.

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.

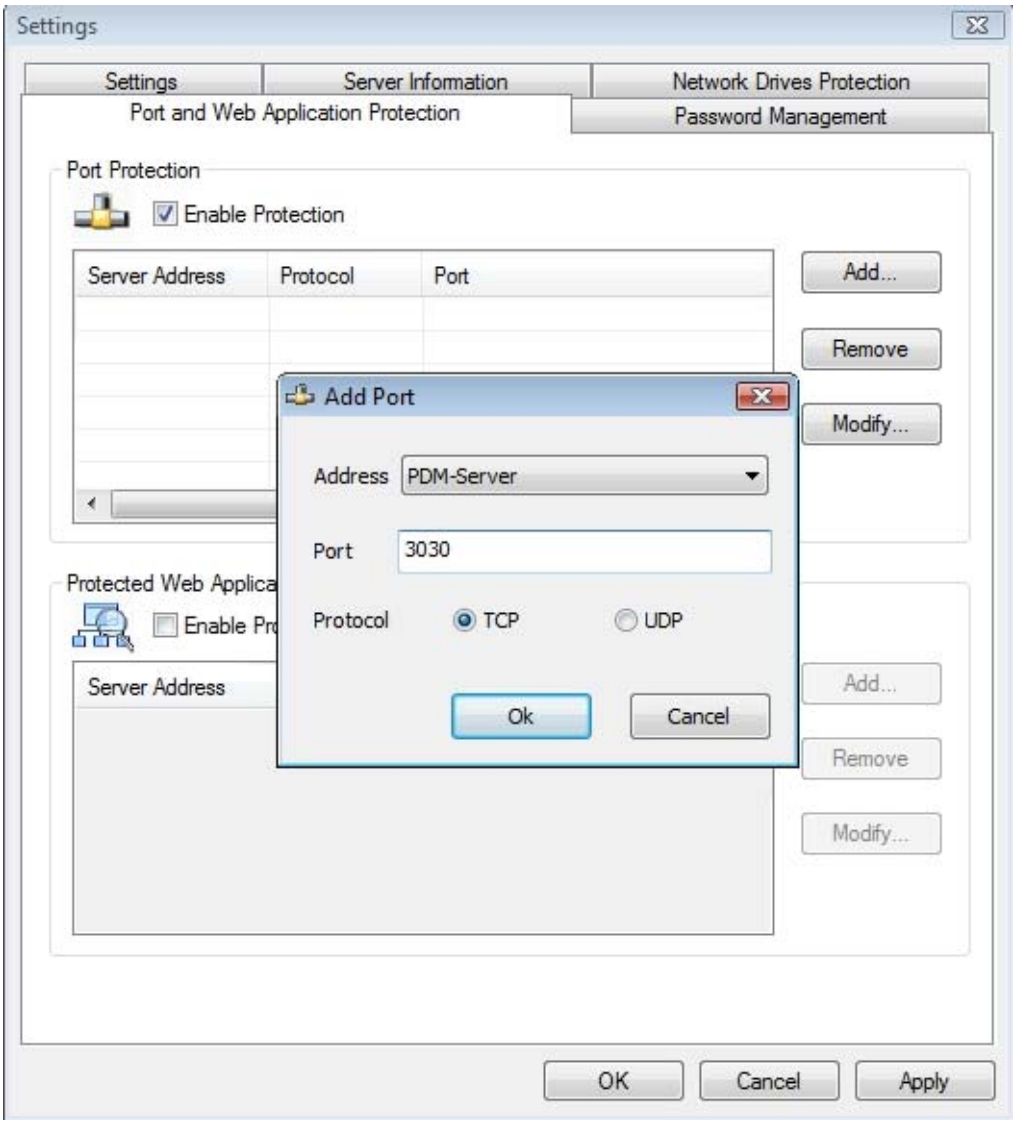
Protected Upload: http://Hostname/Path
- Path - Enter the path you want to protect

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.

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.

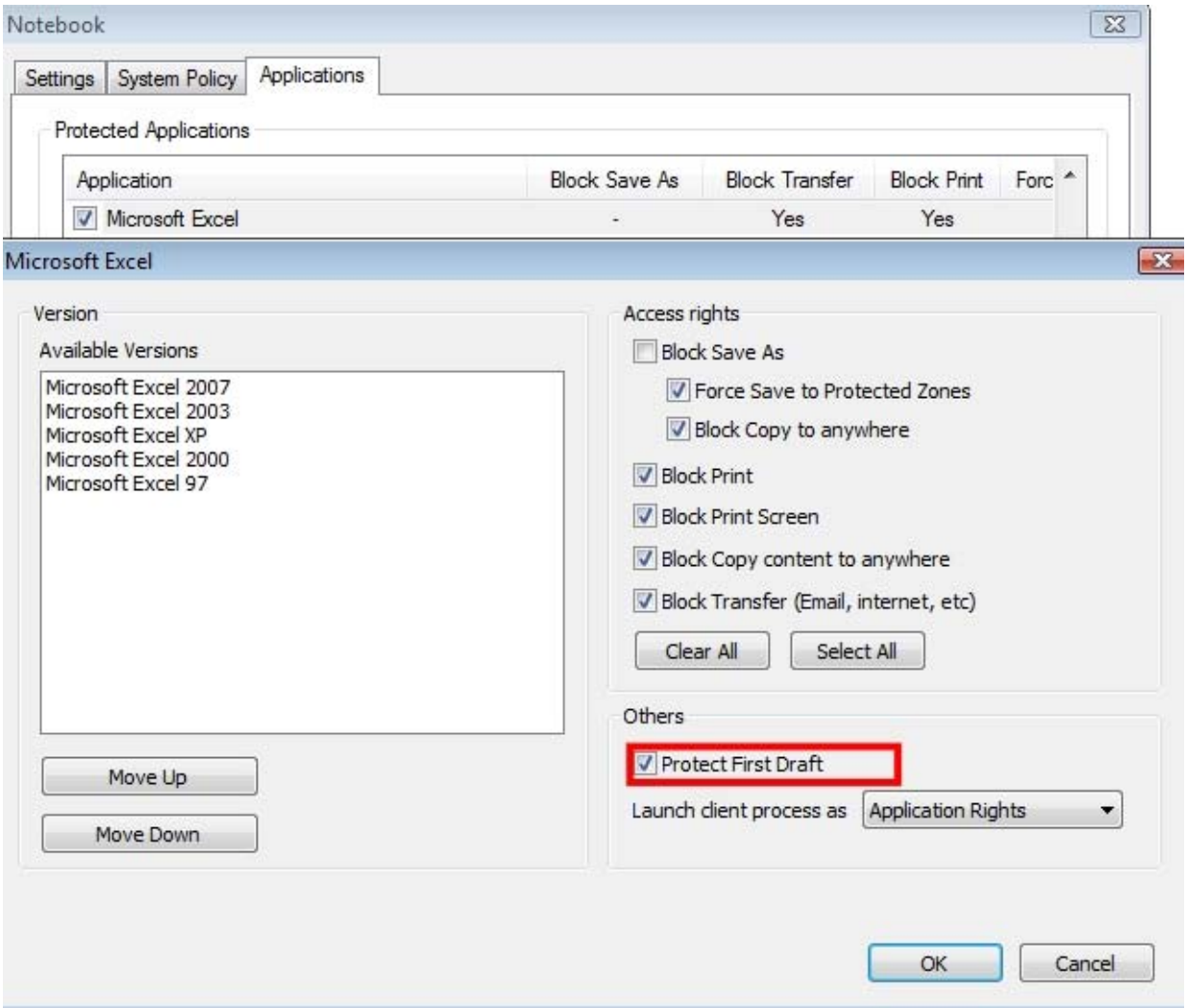
This feature can be enabled by Policy Group and Application. Here is an example of its usage.
- Enforce engineers to save all newly created AutoCAD and Photoshop files to Protected Zone

Steps to enable Protect First Draft is enabled 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)



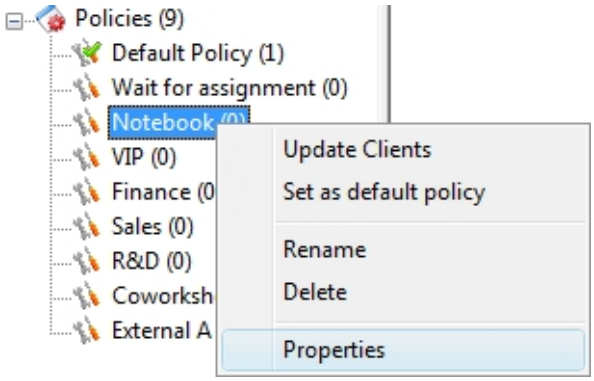
P.S. When Protect First Draft is enabled for an application (e.g. Excel). ONLY Protected application can be launched. In this example, that means users cannot launch non-Protected Excel. If users try to launch it, Curtain e-locker will automatically stop the application. For non-Protected Excel files, 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.

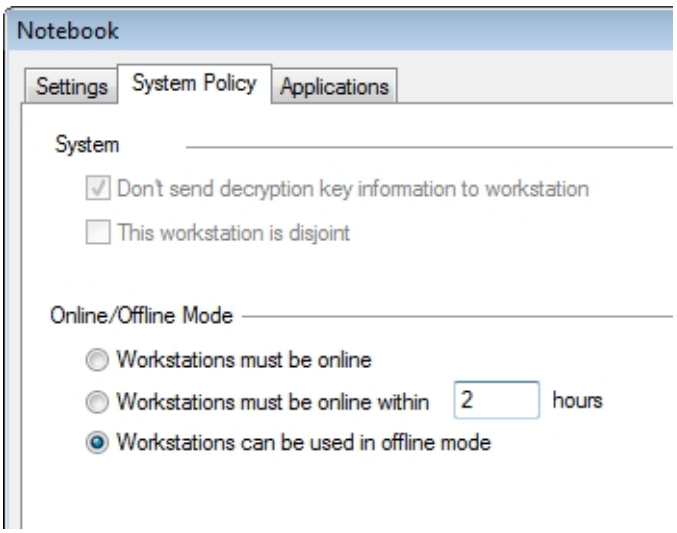
The major purpose of this function:
- Do not want downloaded sensitive information can be used when the desktop/notebook is out of the company (it means the desktop/notebook cannot connect with Curtain Admin)

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.

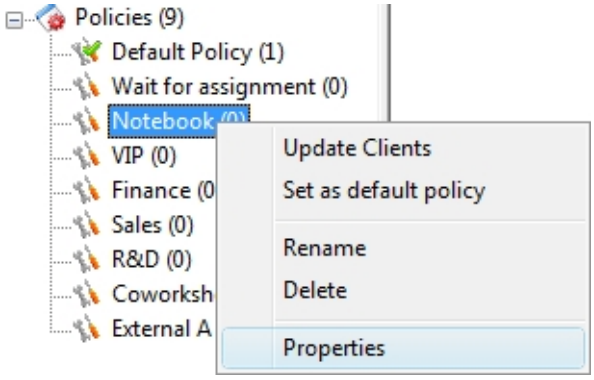


6.3 - Housekeeping

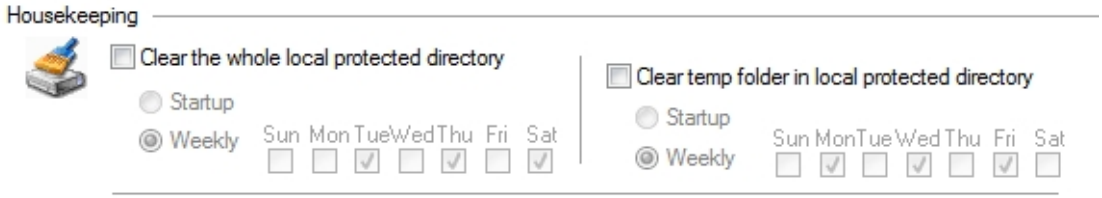
Housekeeping is a feature for clearing up files in Local Protected Directory.

There are 2 main purposes of this function:
- Do not want users to keep files in Local Protected Directory forever.
- Clean up cache and temporary files 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".

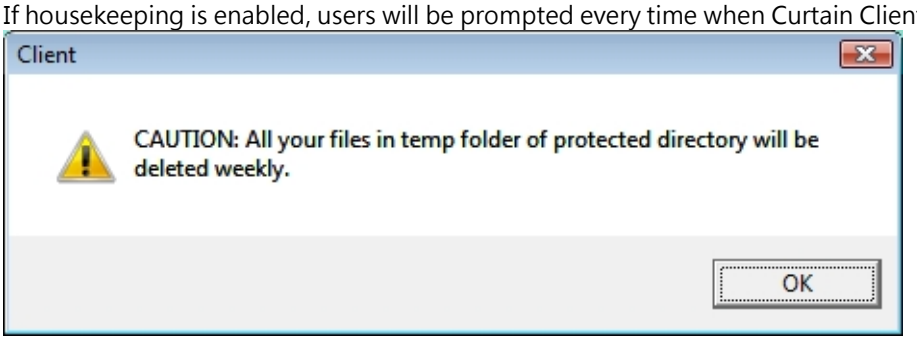


2. Select the Rules to clean up files in Local Protected Directory, and then click OK button to confirm.



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

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.

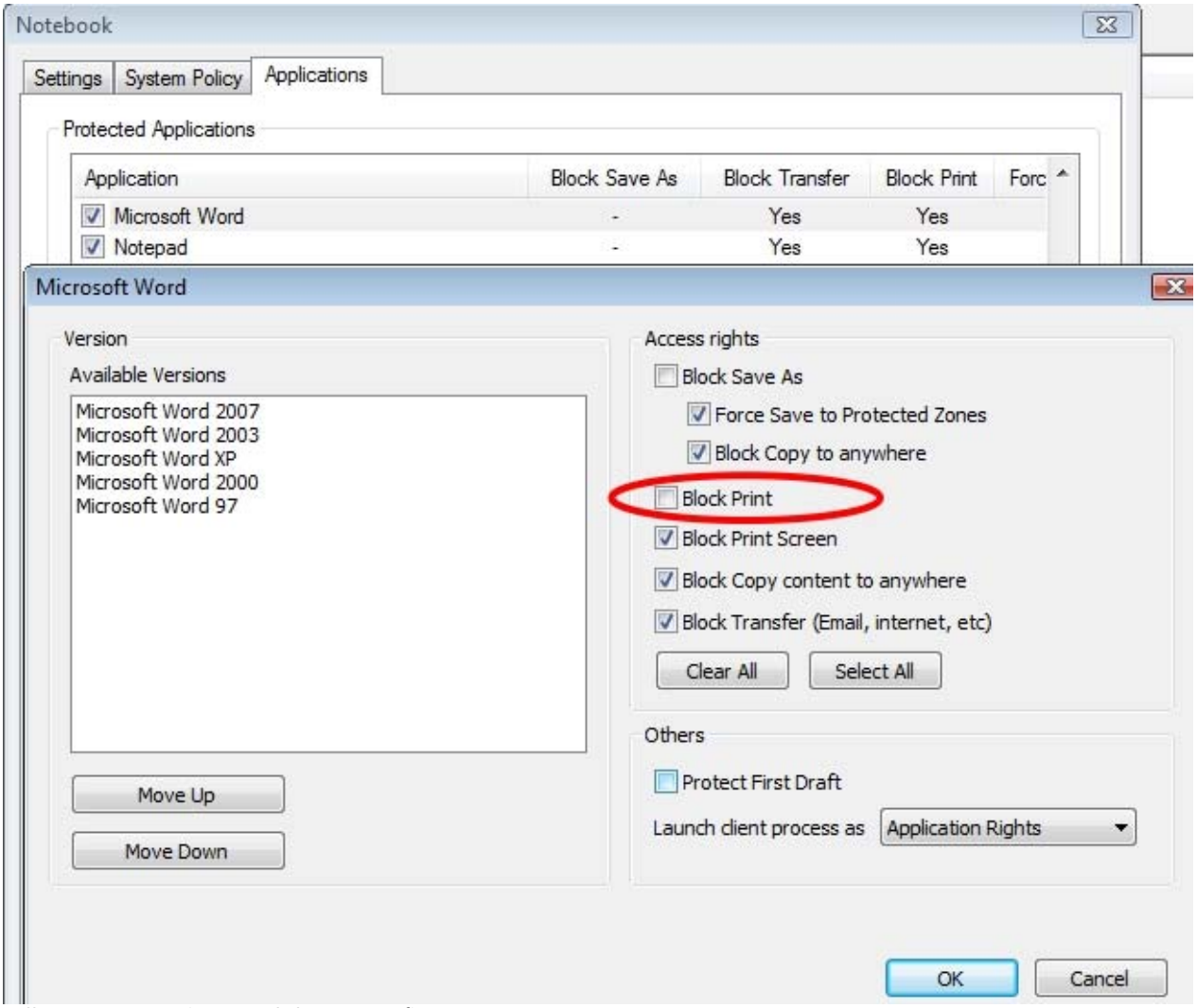
It does not affect normal operations, while security is maintained. Curtain e-locker makes a good balance between convenience and security.

6.6 - Secure Print-to-PDF

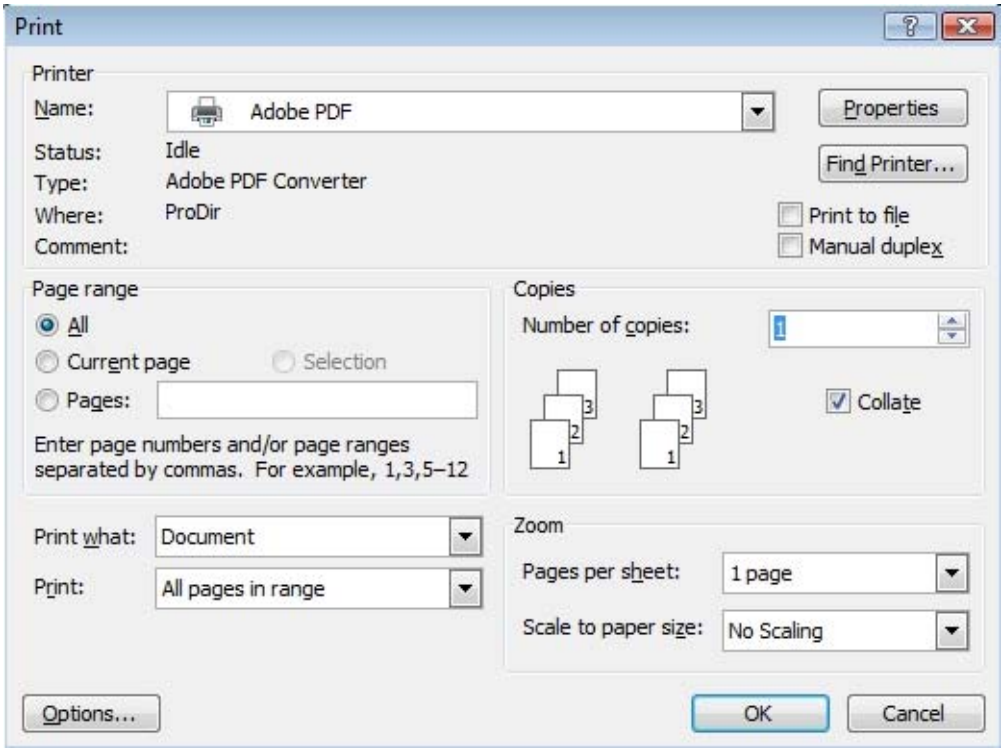
Secure "Print-to-PDF" is a feature to allow users to convert sensitive documents to PDF format in a secure way.

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

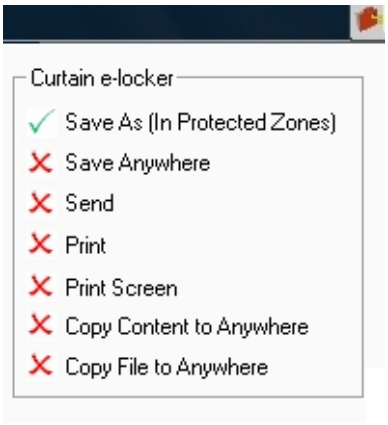


Convert documents to PDF format by Print-to-PDF

6.7 - Secure File Sharing

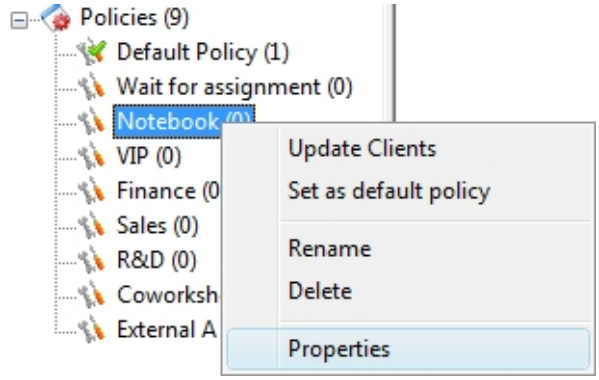
In general, there are three scenarios:
(1) user is authorized to share non-encrypted files with others.
(2) user is authorized to share encrypted files with others. But the files can be only decrypted in Protected Zone.
(3) user is authorized to share password-encrypted files with others. The files can be decrypted anywhere with entering correct password.

Scenario 1:
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.

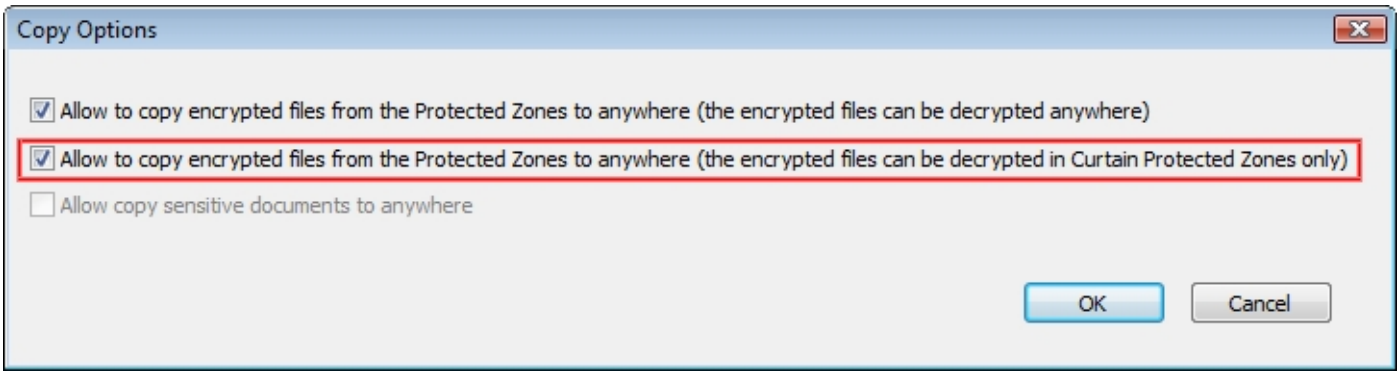


Scenario 2:
If a user is allowed to Encrypt Out (Decrypt in Curtain Only), the user can encrypt Protected files and share the encrypted files with others. When other users receive the files, their workstations must have Curtain Client (pointing to the same Curtain Admin) installed. The users can double-click the files to decrypt them. Files will be automatically decrypted to Local Protected Directory.

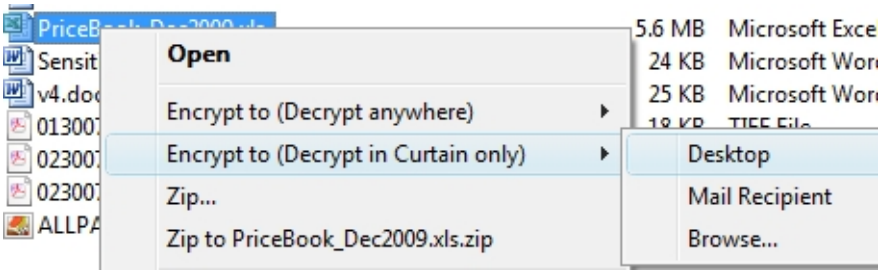
Steps to grant the right "Encrypt Out (Decrypt in Curtain Only)":
1. In Curtain Admin, select a Policy Group and right-click to select "Properties".



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 Curtain only)". Then an encrypted file will be copied to destination.



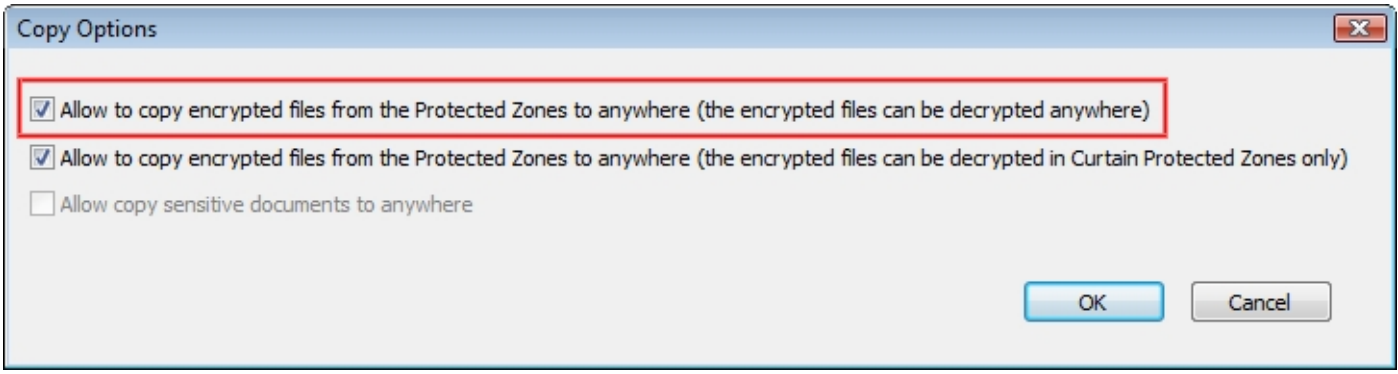
2. Send the encrypted file to others. Since the file is encrypted, the file is safe during transmission (e.g. USB flash drive or Email).

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

Scenario 3:
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 plaint files, Curtain will not protect the plaint 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 Desktop.

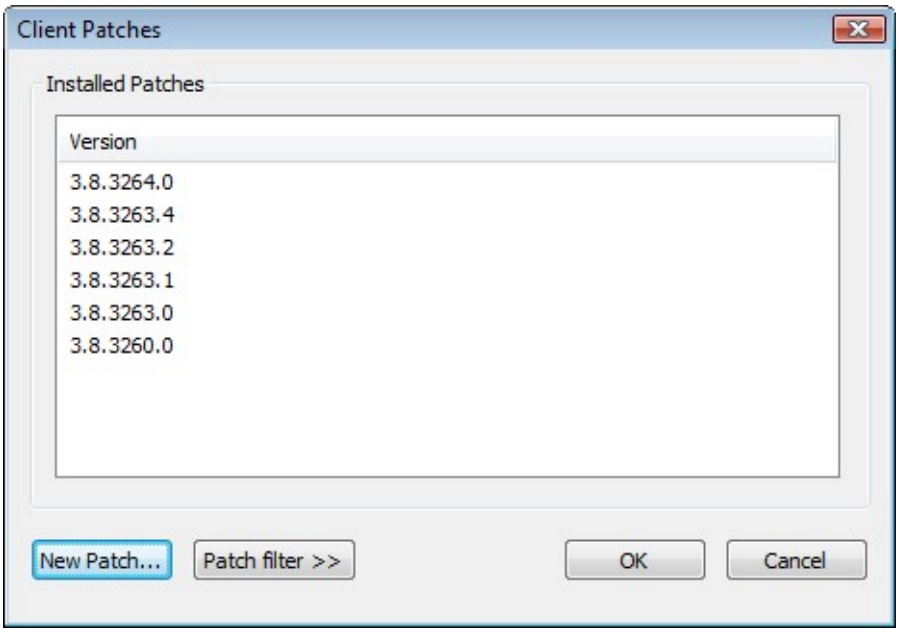
6.8 - Patch Management

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

Click "Update Patch" button

2. Click "New Patch..." button to insert the patch. Then Curtain Clients will be updated when they connect to Curtain Admin next time.



6.9 - 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.