SEP User Manual

CONTENTS

Foreword

Thank you for choosing Smart Extend Protocols (SEP), a proprietary software product developed by Centerm Information Co., Ltd. Before suing this product, please carefully read through this User Manual.

Please understand that due to the continual upgrade of software version, the illustrations given herein may differ from the actual software interface, and we do appreciate your kind understanding.

1. Product Introduction

1.1 Overview

SEP is an application developed by Centerm for running in the virtual office environment. It mainly consists of the following six modules:

- TWAIN mapping: optimized image display and transmission of devices supporting TWAIN protocol;
- Webcam mapping: optimized image display of video devices on the server side;
- USB mapping: to map local USB devices to the server side;
- MMR (Multimedia Redirection): optimized playback of cloud video;
- Serial/parallel port mapping: to map local serial/parallel port to the server side;
- Disk mapping: to map local USB storage device (flash disk or mobile HDD) to the server side.

1.2 Operating Environment

- Operating systems supported on the server side

  Windows XP 32-bit, Windows Server 2003, Windows 7, Windows Server 2008 R2

- Operating systems supported on the client side

  Windows XP 32-bit, Windows 7 32-bit, XPe, WES7, COS, COSA

- Operating systems supported by the license & policy server

  Windows Server 2003, Windows Server 2008, Windows Server 2008 R2

1.3 Protocols Supported

- ICA Protocol

  Client supported:

  Windows system: Citrix Receiver 13.x or above versions

  COS/COSA system: Citrix Receiver12.x, 13.x

- PCoIP Protocol

  Client supported:

  Windows system: VIEW 5.1 or above versions

  COS/COSA system: All versions of CT Vision Client

- RDP Protocol

  Client supported:

  Windows system: Windows' built-in remote desktop connection tool

  COS/COSA system: the built-in remote desktop connection tool

- Xred 2.0 Protocol

  Windows system: Xred 2.0 or above versions

  COS/COSA system: Xred 2.0 or above versions

1.4 Port Resources

- License & Policy Server

  License service: port 7825

  Policy service: port 7816

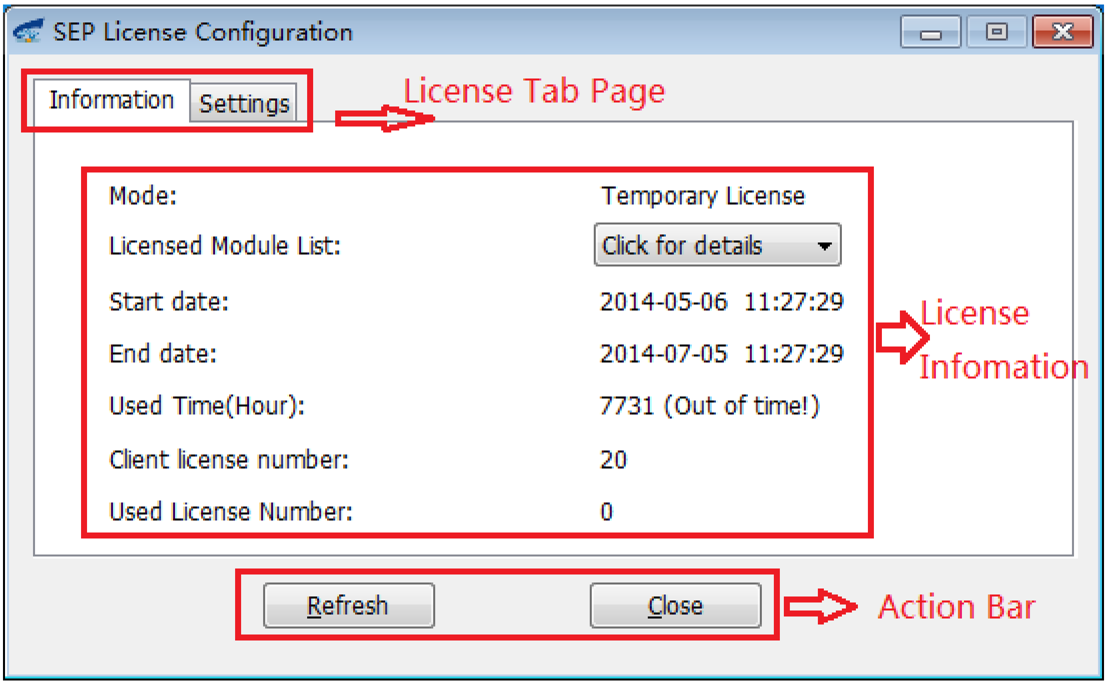
2. License & Policy Server

2.1 License Server

2.1.1 User interface

The main user interface for license server configuration is shown below:

There are two tabs in the license window: "Information" and "Settings". In the "Information" tab, you can view the current license information of the license server. In the "Settings" tab, you can configure license settings.



Mode: Temporary License
Licensed Module List: Click for details
Start date: 2014-05-06 11:27:29
End date: 2014-07-05 11:27:29
Used Time(Hour): 7731 (Out of time!)
Client license number: 20
Used License Number: 0

※ **License information tab**

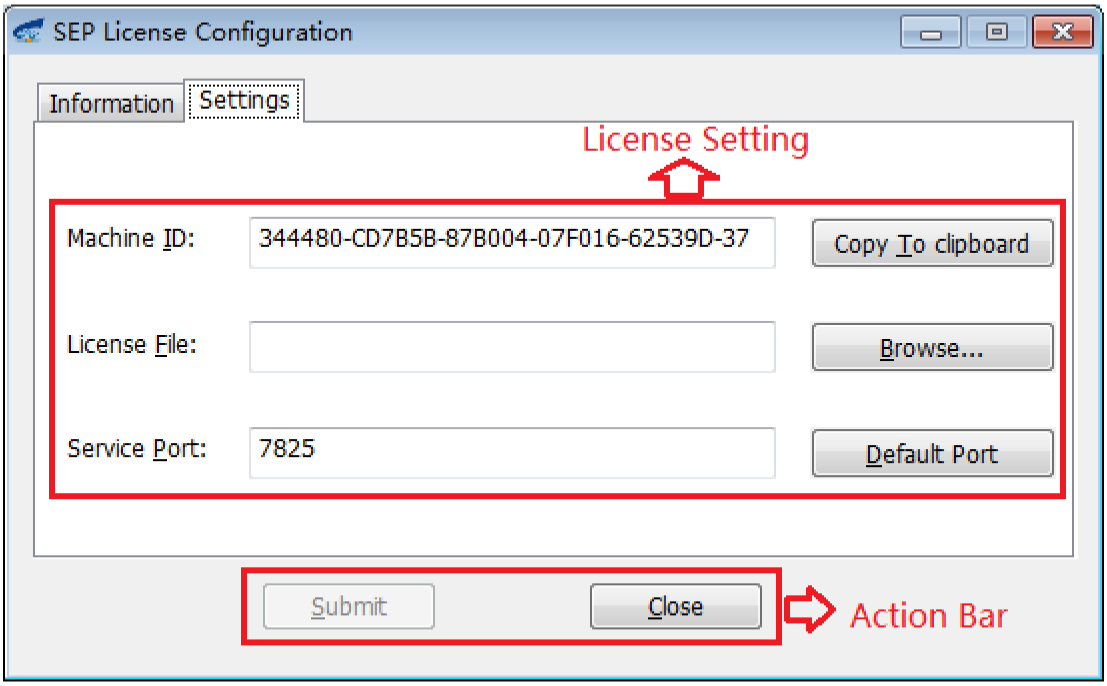
- License information

The license information area shows detailed license information about this license server.

- Action bar

Click "Refresh" button to get the latest license information; click "Close" button to close the license configuration window.

※ **License settings tab**



Machine ID: 344480-CD7B5B-87B004-07F016-62539D-37

License File:

Service Port: 7825

- Machine ID

The unique ID generated based on a specific algorithm to identify the current license server. This character string will be used during license application.

- License File

SEP license file: You will get a license file after applying to Centerm. Import this file to activate the license.

- Server Port

The listening port of this license server (default: 7825). To change into another port, you need to include this port into firewall exceptions.

- Copy to clipboard

To copy the machine ID to clipboard (facilitating your operation).

- Browse

To browse and import the license file.

- Default Port

To set the listening port of license server as the default port.

- Submit

After browsing and selecting the license file, click "Submit" button to import and activate the license file.

- Close

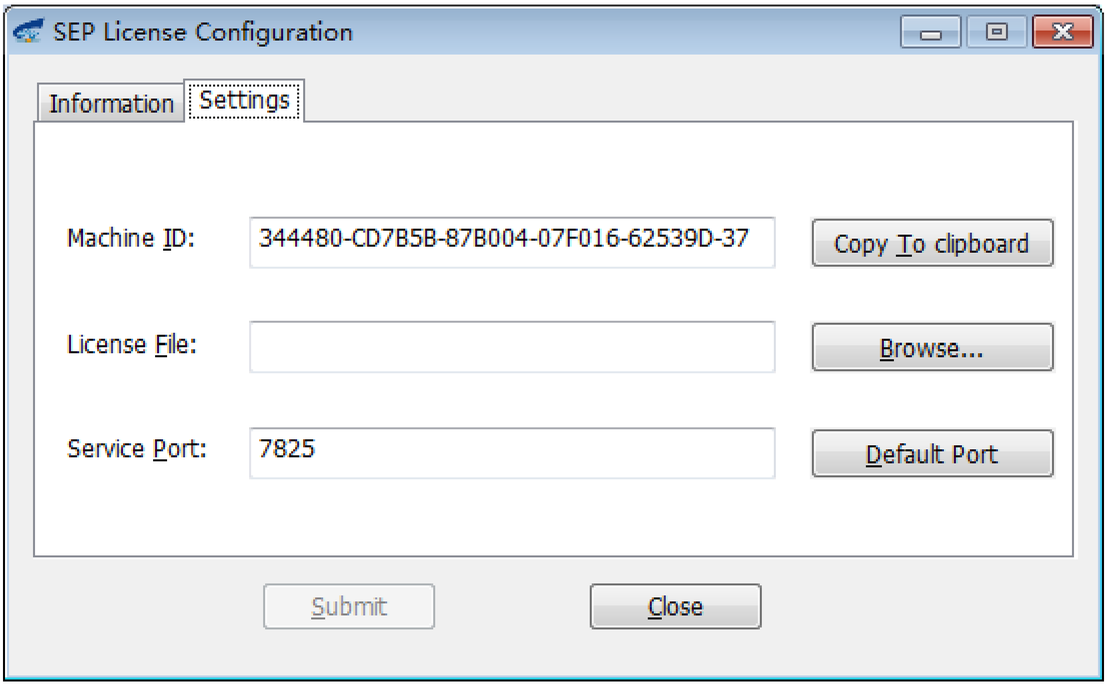
Close the license configuration window.

2.1.2 Apply for license

Follow the following steps to apply for SEP license:

1. Get registration ID

On the license server, open SEP license configuration window, as shown below:



SEP License Configuration

Machine ID: 344480-CD7B5B-87B004-07F016-62539D-37

License File:

Service Port: 7825

The machine ID here is the registration ID. Click "Copy to clipboard" to copy this ID.

2. Apply for license file

Send the machine ID to Centerm's licensing department and explain your specific licensing needs.

After proper communication, the user will receive from Centerm a ".key" license file.

3. Register license file

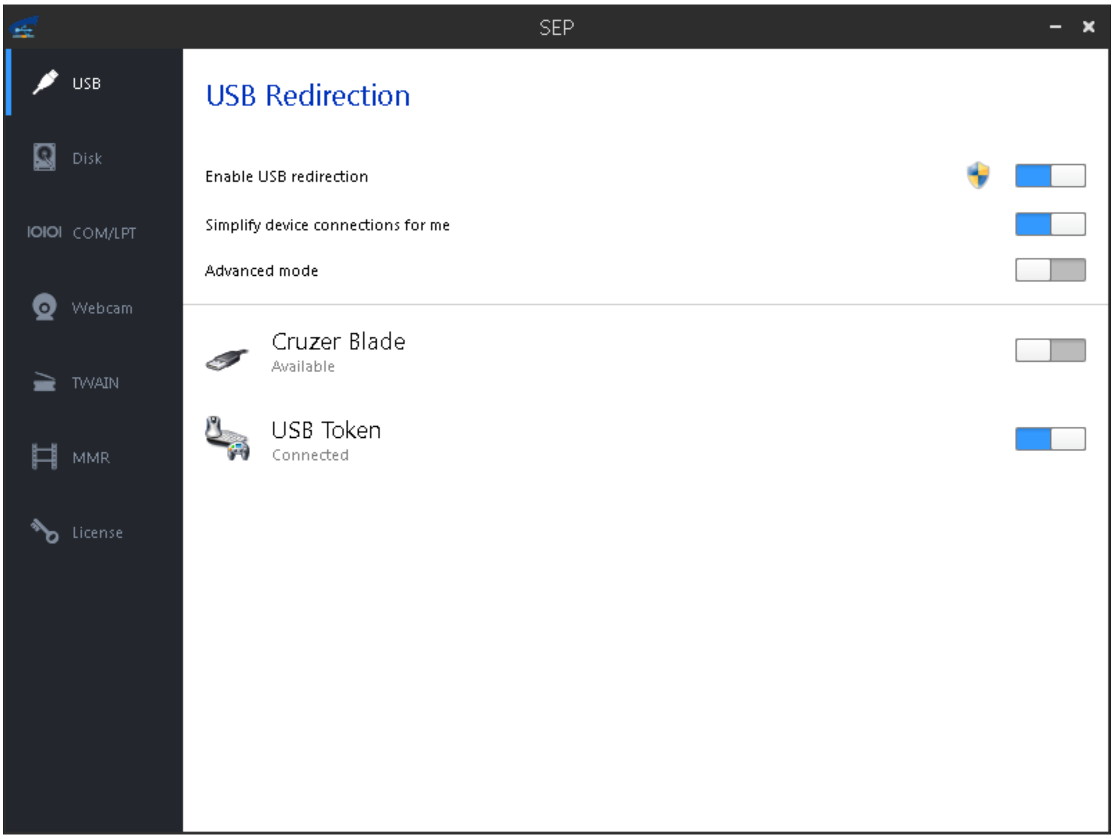
Click "Browse" button to select the license file received. Configure the server port and click "Submit" button.

4. Licensing successful

A prompt message indicating successful operation means you have got licensed successfully.

2.1.3 Configure license

1. Open the main program window of SEP, as shown below:

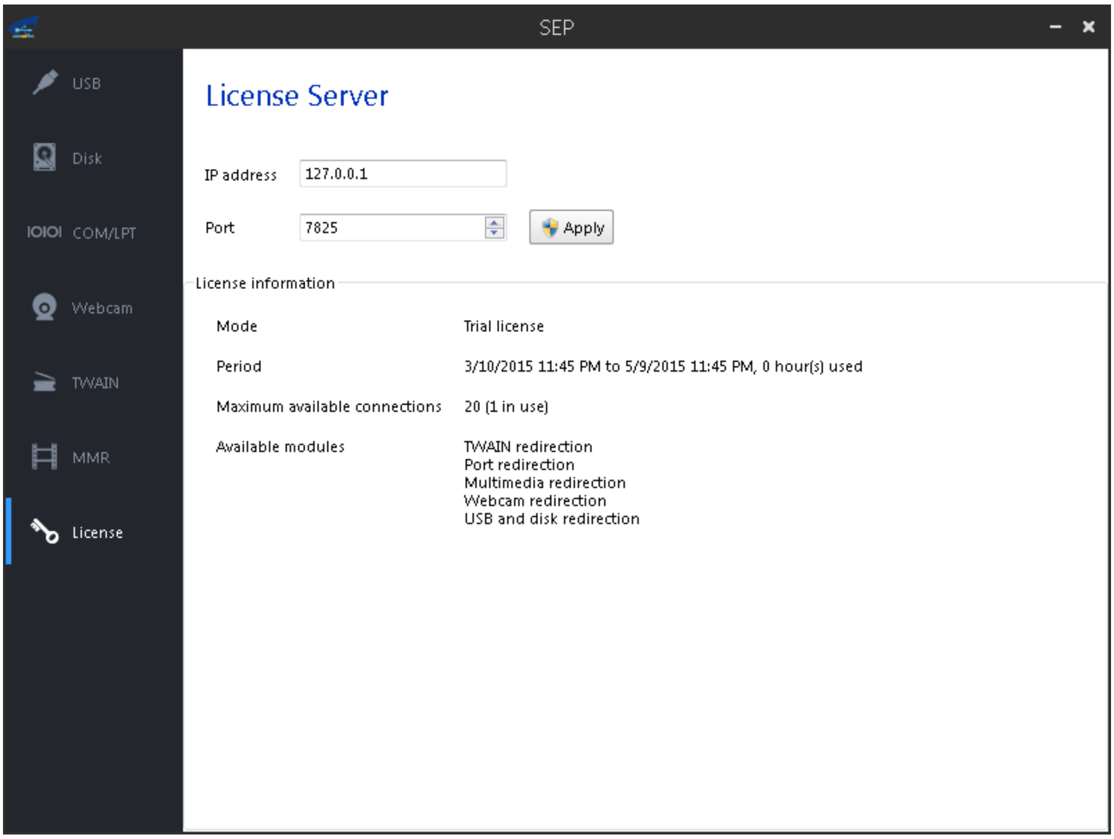


Enable USB redirection

Simplify device connections for me

Advanced mode

2. In the main program window of SEP, click "License", as shown below:



License Server

IP address 127.0.0.1

Port 7825

License information

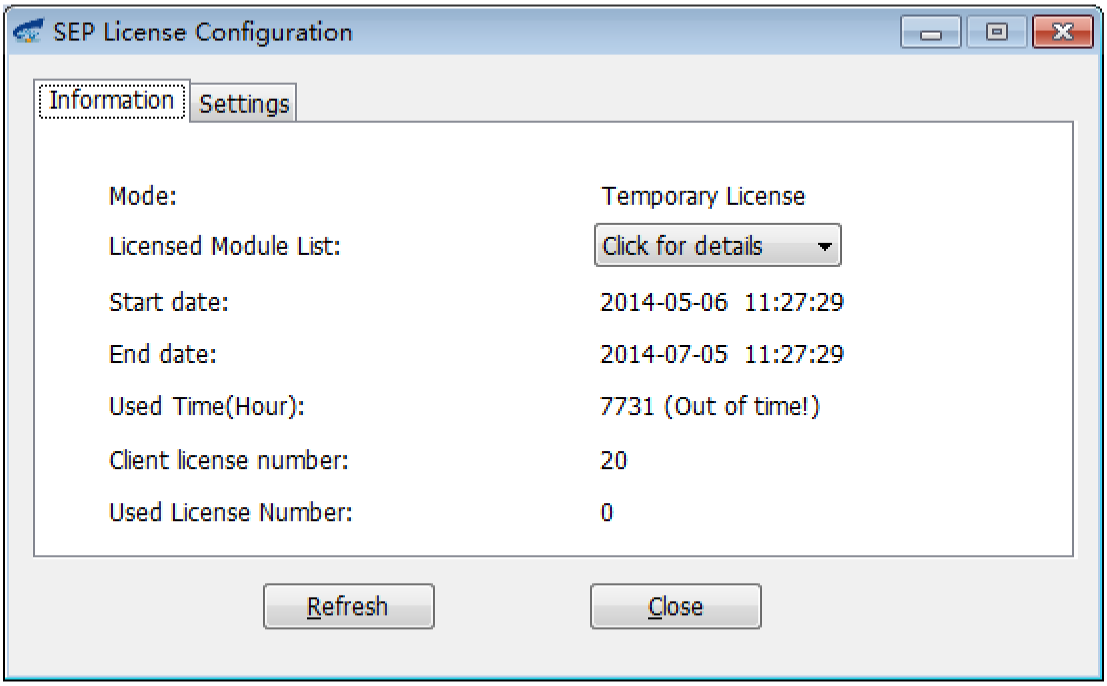
Mode	Trial license
Period	3/10/2015 11:45 PM to 5/9/2015 11:45 PM, 0 hour(s) used
Maximum available connections	20 (1 in use)
Available modules	TWAIN redirection Port redirection Multimedia redirection Webcam redirection USB and disk redirection

3. Enter the IP address and port number of license server, click "Apply" button and reconnect to the remote desktop.

2.1.4 View license

- View license on the license server

1. On the license server, open license configuration window, as shown below:



Mode: Temporary License

Licensed Module List: Click for details

Start date: 2014-05-06 11:27:29

End date: 2014-07-05 11:27:29

Used Time(Hour): 7731 (Out of time!)

Client license number: 20

Used License Number: 0

2. You can view detailed license information. To view the licensed modules, click "Click for details" button and then click "Refresh" button to see the real-time license information.

- View license on the virtual desktop

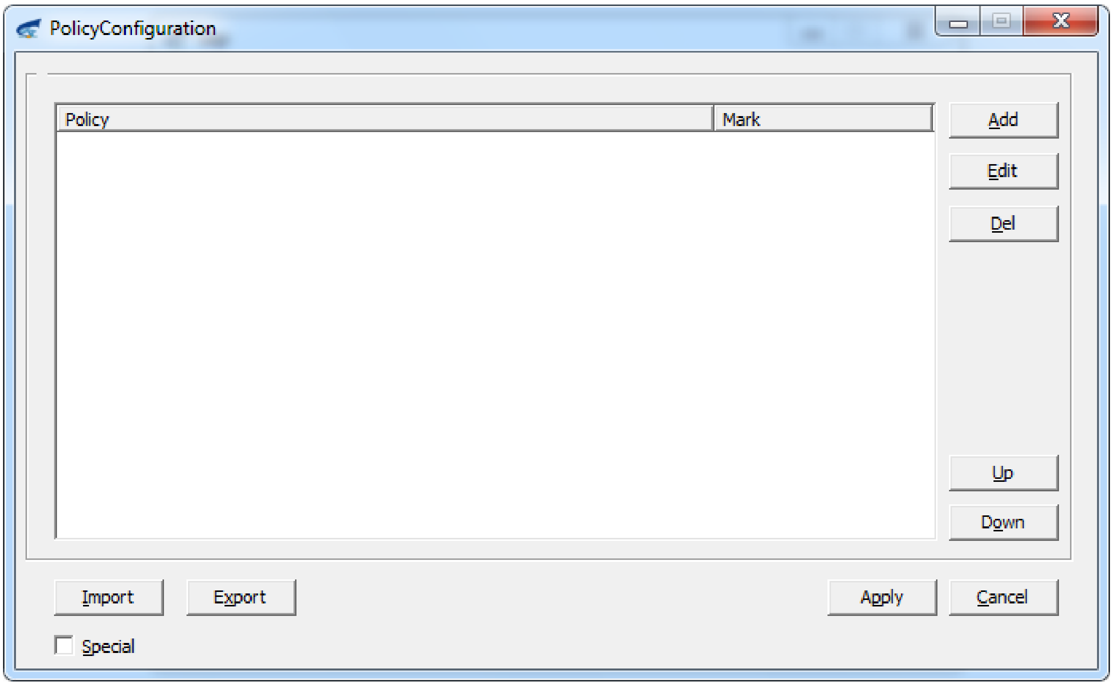
See 2.1.3.

2.2 Policy Server

2.2.1 Description

※ **Main Interface**

The main interface for policy server configuration is shown below:



- Policy list

The policy list shows the policies added by the user and consists of "Policy" and "Mark". The "Mark" field identifies the policy entries so that the user can quickly locate specific entries instantly.

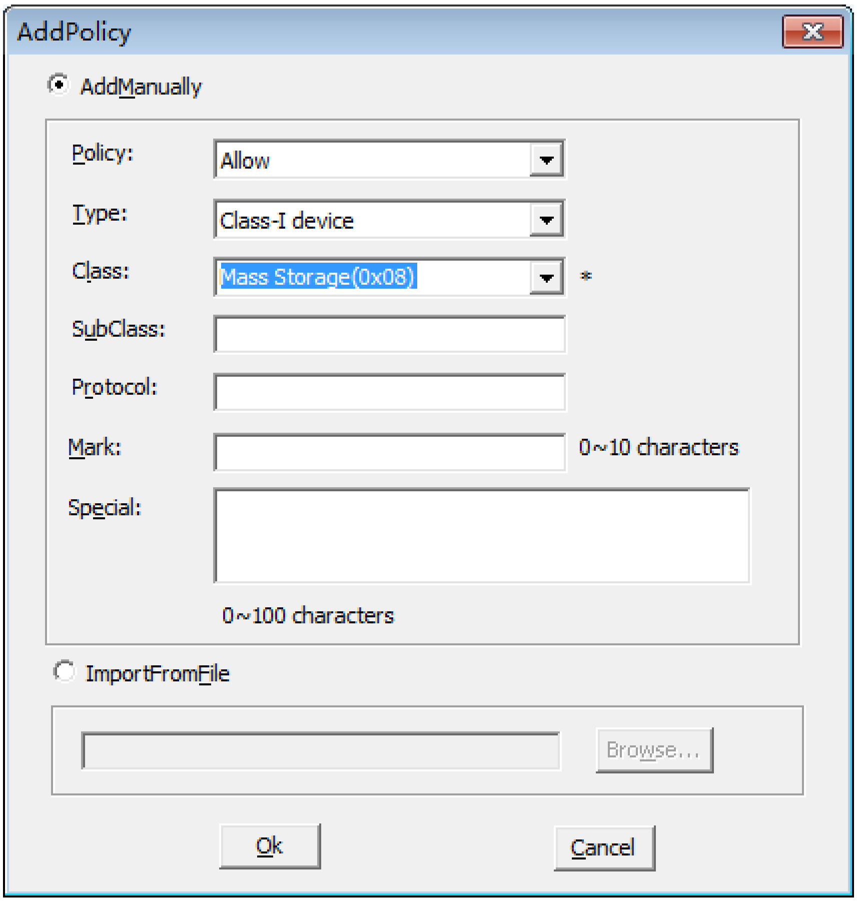
- Function buttons

The window consists of multiple function buttons. "Add", "Edit" and "Del" buttons are used to add, edit and delete policy entries; "Up" and "Down" buttons are used to adjust the sequence of policy entries; "Import" and "Export" buttons are used to import the existing policy files into the policy list or export all policies from the policy list into a policy file. Click "Apply" button to apply and save all changes to the current policies, or click "Cancel" button to ignore all changes and exit the program.

- Special

User may forget the purpose of adding the policy entry after a long time. Therefore, the "Special" field is provided to describe the policy when user adds it, so that the user can view details and purpose of this policy anytime. Select one policy entry and check "Special" to show a textbox below, which will show detailed information about this entry.

※ "Add Policy" window



● AddManually

Policy: Allow

Type: Class-I device

Class: Mass Storage(0x08) *

SubClass:

Protocol:

Mark:

Special:

○ ImportFromFile

There are two ways to add a new policy: "Add By Hand" and "Add By File".

- Add By Hand

In such a case, the user needs to configure detailed settings, including "Policy", "Type", "Mark", "Special", etc. Policy: including "Allow", "Prohibit", "Default Allow" and "Default Prohibit".

Type: including "Specific device" and "Class-I device". Different selections will lead to different options below. When user selects "Specific device", "PID", "VID" and "BCD" information of the device must be specified. When user selects "A kind of device", "Class", "SubClass" and "Protocol" information of the device must be specified.

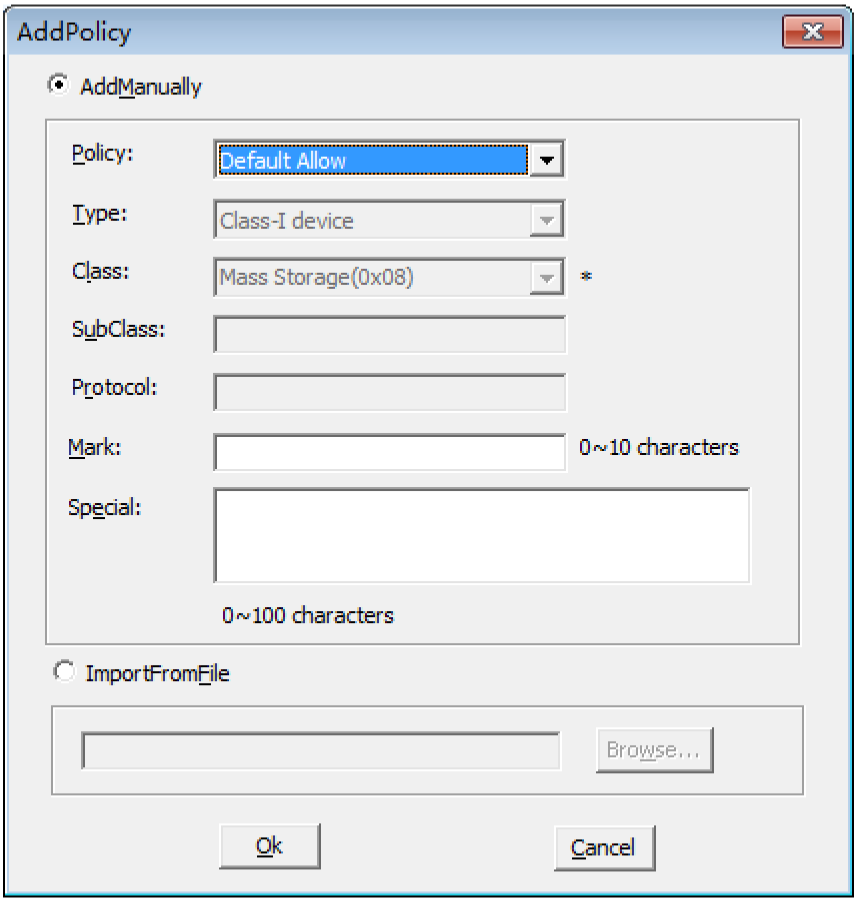
Mark: for identifying policy entry and facilitating entry finding.

Special: including detailed description about the policy. The user may describe here the purpose for adding this policy.

- Add By File

Adding policy by this way requires the user to use the USB policy tool to generate a policy file first.

※ **"Edit Policy" window**



AddPolicy

● AddManually

Policy: Default Allow

Type: Class-I device

Class: Mass Storage(0x08) *

SubClass:

Protocol:

Mark: 0~10 characters

Special:

0~100 characters

○ ImportFromFile

"Edit Policy" window is basically the same as the "Add Policy" window. However, certain functions are grey and unavailable, such as the adding method. While editing one policy entry, the user can only edit "Policy", "Mark" and "Special" fields.

2.2.2 Instructions for Configuration

1. Add policy

A. In the main window of "Policy Configuration", click "Add" button to pop up "Add Policy" window.

B. Select "Add By Hand" or "Add By File" to add the policy.

C. If you choose "Add By Hand", you will need to specify and fill in the corresponding "Policy", "Type", "Mark", "Special" and other fields. When the policy is "Default Allow" or

"Default Prohibit", you only need to fill in "Mark" and "Special". If you select "Specific device" from "Type", you will need to specify "VID", "PID" and "BCD" of the corresponding device. Such information can be obtained from the device. If you select "A kind of device" from "Type", you will need to specify "Class", "SubClass" and "Protocol".

D. If you choose "Add By File", you will need to import the specific policy file. This file must be the policy file generated using USB policy tool.

E. After filling in necessary information or specifying the policy file, click "OK" button and the new policy will appear in the policy list of "Policy Configuration" window.

2. Edit policy

A. Select the policy entry to be edited and click "Edit" button to edit.

B. Change policy settings. The user is only allowed to edit "Policy", "Mark" and "Special".

C. After editing, click "OK" button to save the changes.

3. Change policy sequence

Policy sequence is critical, as the upmost policy will be matched first. To change policy sequence, select the policy entry to be changed and click up/down buttons: "Up" button to move the selected entry up one position in the list, or "Down" to move down one position.

4. Import/export policy

Policies can be exported and saved, or can be imported for policy configuration. Click "Import" or "Export" button to complete the corresponding operations. Please note that it's impossible to export any file if there is no policy in the policy list.

5. Notes for policy

A. When the policy server hasn't been specified or the communication with policy server fails, the local policies on the server will be used.

B. When the server communicates normally with the policy server and if no policy has been configured on the policy server, it's deemed this server is not bound to any policy and can be mapped by all devices.

C. On the policy server, the default policy is "Default Prohibit". For any USB device, if there is 1 or more polices, the policies will be matched from top to bottom, and this process will end if any policy is matched. If no policy is matched, the default policy will take effect, namely this USB device will be Deny from mapping.

D. To add one new policy, the new policy will be placed above all existing policies and will be given first priority.

E. To prevent "Default Prohibit" policy from taking effect, you may add a "Default Allow" policy, which will be matched prior to "Default Prohibit".

F. When importing policy file through the "Import" button, the original policies will all be overwritten. When clicking "Add" button and then importing policy by selecting "Import By File", the policy will be added to the policy list without deleting the original policies.

C. The newly added policy will take effect upon the establishment of next session. It won't apply to the current session.

3. Product Features

3.1 TWAIN Mapping

TWAIN mapping can significantly enhance the image display and transmission effect when the image capture device (such as document camera and scanner) supporting TWAIN protocol is used on the virtual desktop.

TWAIN mapping supports the optimized display and transmission of images captured in "Native", "File" or "Memory" mode.

3.1.1 Environment preparation

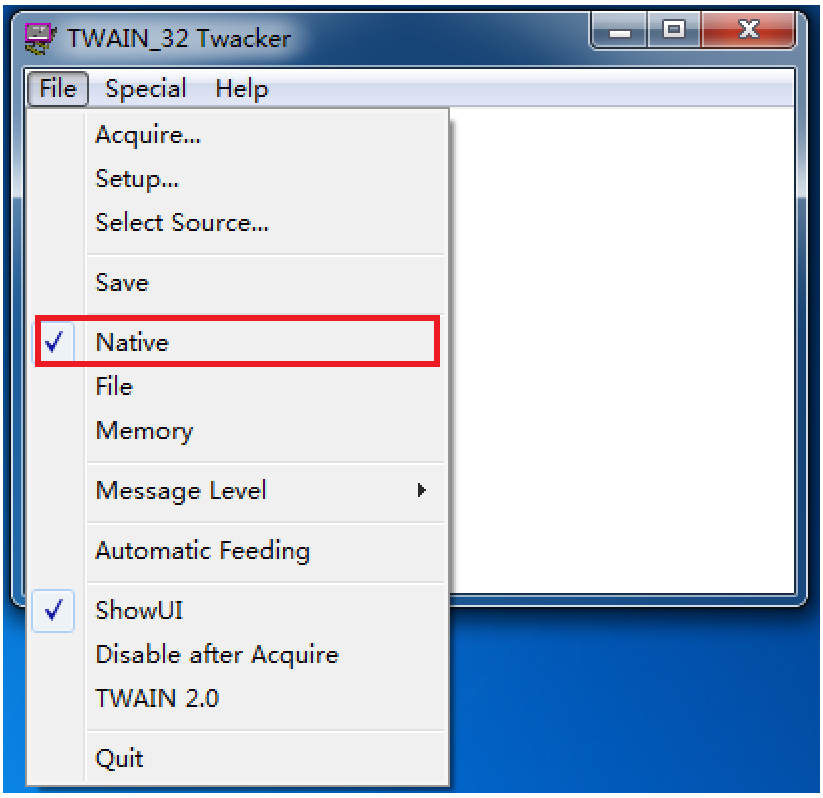
Server side: install image capture application program supporting TWAIN protocol (taking Twack_32 as the example);

Client side: install device driver.

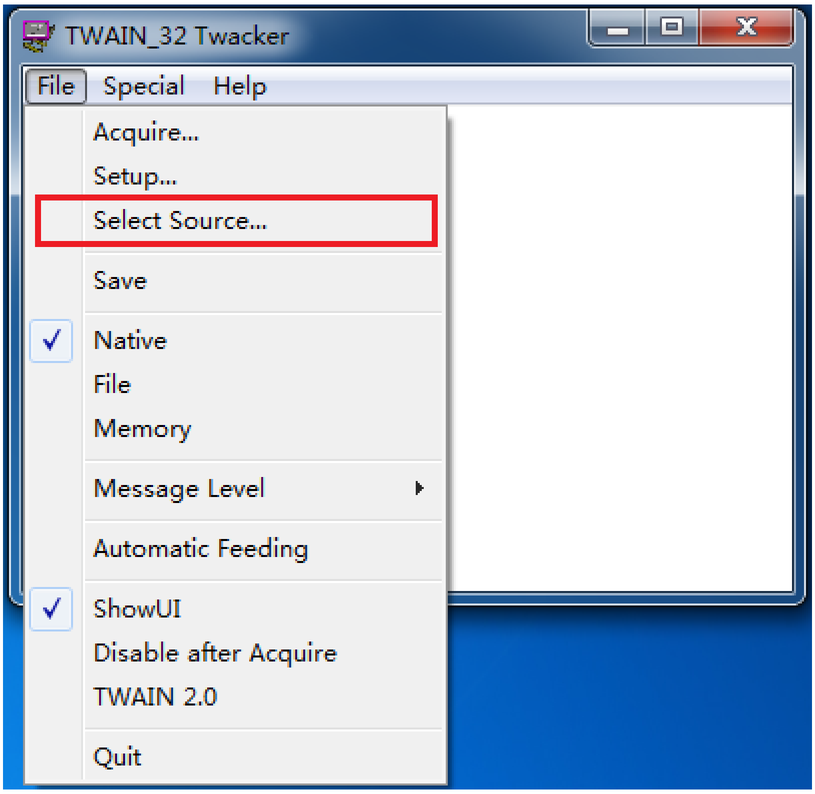
3.1.2 Using TWAIN mapping to capture image

1. Connect to virtual desktop.

2. On the server side, open Twack_32 program and select “Native”, “File” or “Memory” mode from the "File" menu.

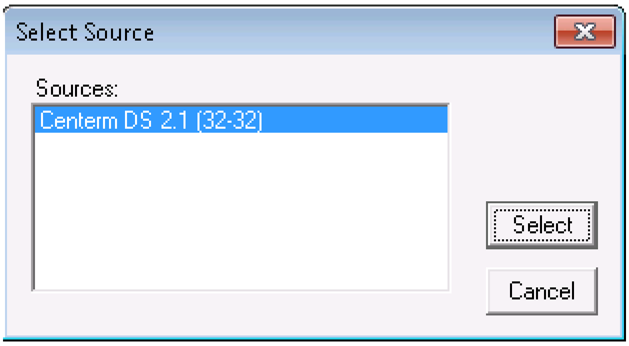


3. Select "Select Source" from the "File" menu.

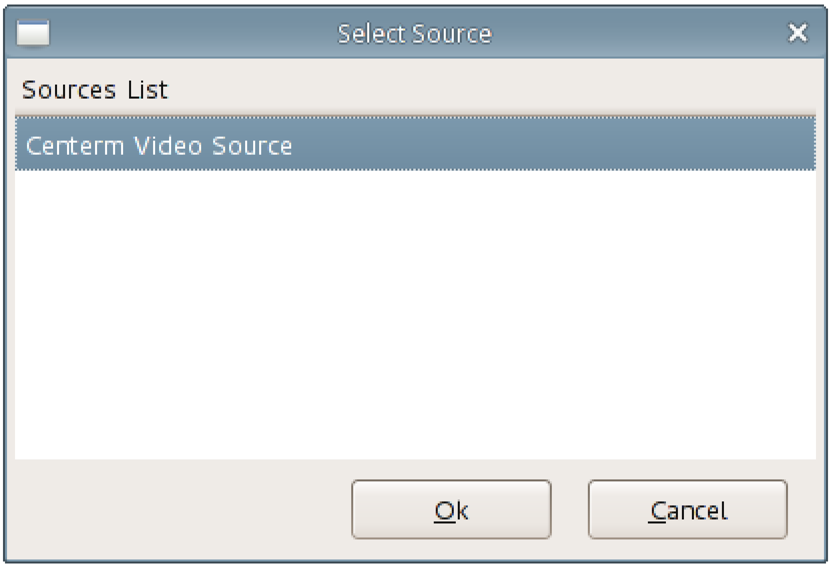


4. From the pop-up source dialog box (which varies from OS to OS), select the source and then click "Select" (Windows)" or "OK" (Linux).

※ "Select Source" dialogue box in Windows



※ "Select Source" dialogue box in Linux



5. Select "Acquire" from the "File" menu to pop up the image preview screen.

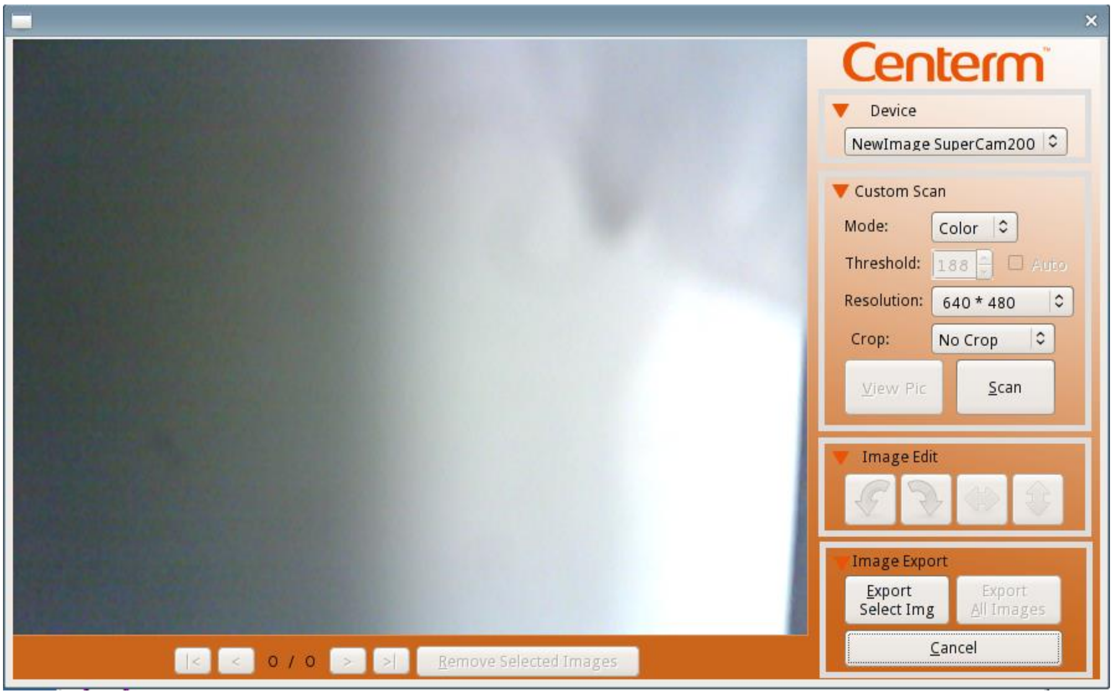
※ On Windows client, the user interface of the image preview screen is related to the driver for the corresponding device and is not fixed.

※ On COS/COSA client, Centerm TWAIN mapping image preview dialogue box will pop up. The corresponding features are described in 4.1.5.

Capture the image by performing the corresponding operations on the image preview screen.

3.1.3 Image preview screen in COS/COSA system

On COS/COSA client, the following TWAIN mapping image preview screen will be displayed.



NewImage SuperCam200

Mode: Color

Threshold: 188 □ Auto

Resolution: 640 * 480

Crop: No Crop

- Device

Select the image device for preview.

- Mode

Select the image scanning mode, including color, grey and black & white.

- Threshold

Manually adjust the threshold from 0 to 255. It will take effect immediately when the mode is black & white. You can also check "Auto" to automatically calculate the best threshold.

- Resolution

All resolutions supported by the current image device.

Crop

Crop the image to the custom dimensions.

- Scan type

Including "Default" and "Custom". The "Custom" mode contains crop feature.

- View Pic

To edit the image when there is a scanned image.

- Back

The preview screen can dynamically display the image.

- Scan

Scan the image and preview the image on the preview screen. If there are multiple images, you can switch or remove the image underneath the preview screen.

- Image Edit

From left to right: counterclockwise, clockwise, left-right and up-down rotation.

- Image Export

Only export one image currently displayed on the preview screen.

- Export All Images

Export all images on the preview screen.

- Cancel

Close the window.

3.1.4 Notes

NA.

3.2 Webcam Mapping

Webcam mapping can significantly enhance the display and transmission effect of captured video when the video device is used on the virtual desktop.

3.2.1 Environment Preparation

Server side: install the video capture application program (taking AMCap as the example)

Client side: install device driver.

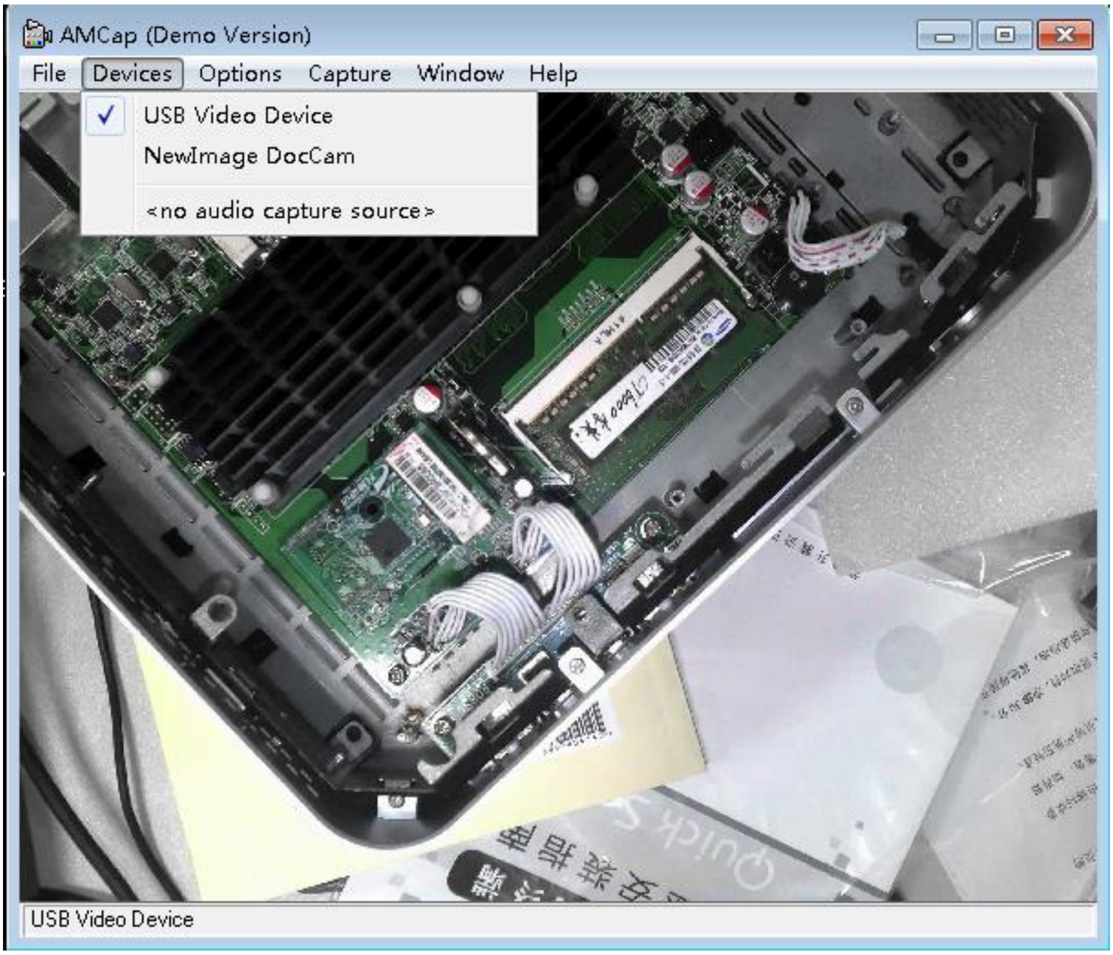
3.2.2 Use Webcam mapping to capture video

1. Insert USB camera into the USB port of terminal.

2. Open SEPConfig program and find the inserted camera device in the device list. Switch the device to "Native" mode.

3. Connect to virtual desktop.

4. On the server side, open AMCap program and select the video device to be mapped from the "Devices" menu to capture video.



3.2.3 Notes

※ While using WebCam, please switch the USB mapping mode of USB video device to "Local".

3.3 USB Mapping

USB mapping allows you to map local USB devices to the server side, including flash disk, USB printer, etc.

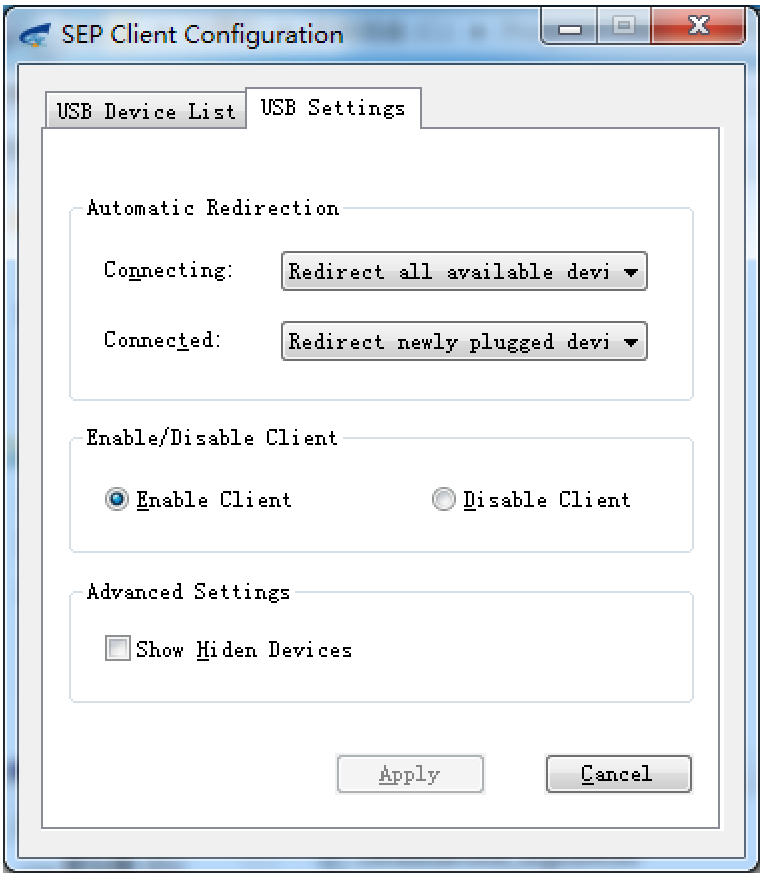
Multi-user isolation of USB storage device, HDD, printer and smart card reader are supported.

On Windows Service 2008 R2 server, multi-user isolation of webcam, scanner, digital camera, music player, USB-to-serial adapter, ergonomic device and biological device are also supported.

3.3.1 Automatic mapping of USB device

Automatic mapping will map the device to the virtual desktop automatically after inserting USB device into the client device.

1) Open SEP Config program and configure the corresponding settings, as shown below:



SEP Client Configuration

USB Device List | USB Settings

Automatic Redirection

Connecting: Redirect all available devi

Connected: Redirect newly plugged devi

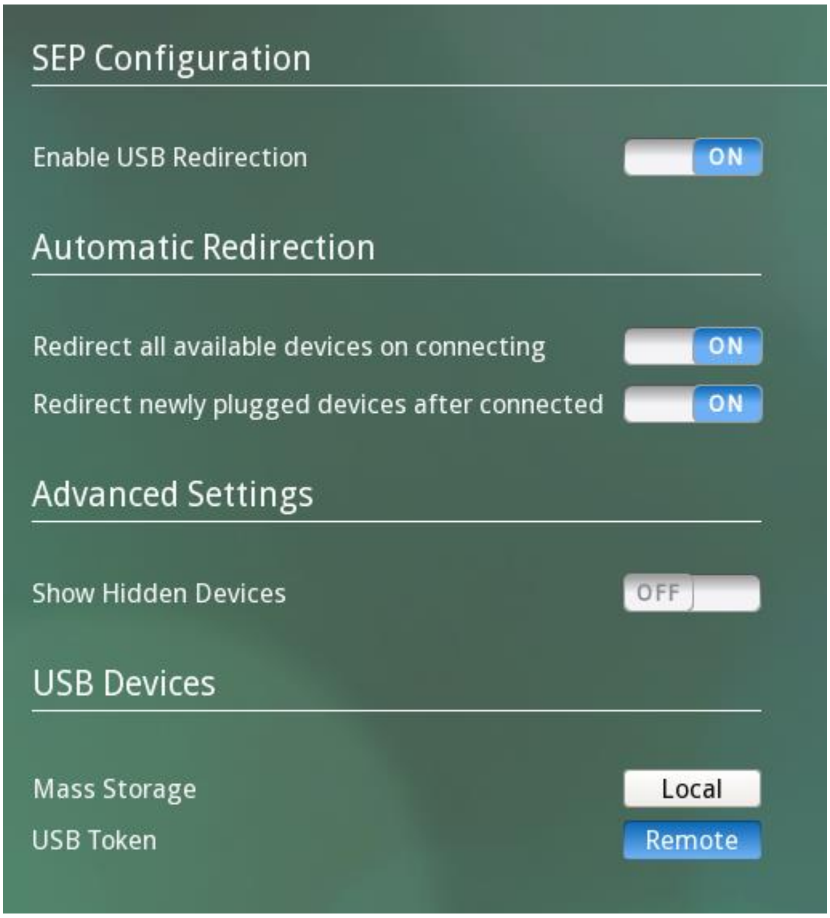
Enable/Disable Client

● Enable Client ○ Disable Client

Advanced Settings

□ Show Hiden Devices

User interface of the client for ordinary terminals



SEP Configuration

Enable USB Redirection: ON

Automatic Redirection

Redirect all available devices on connecting: ON

Redirect newly plugged devices after connected: ON

Advanced Settings

Show Hidden Devices: OFF

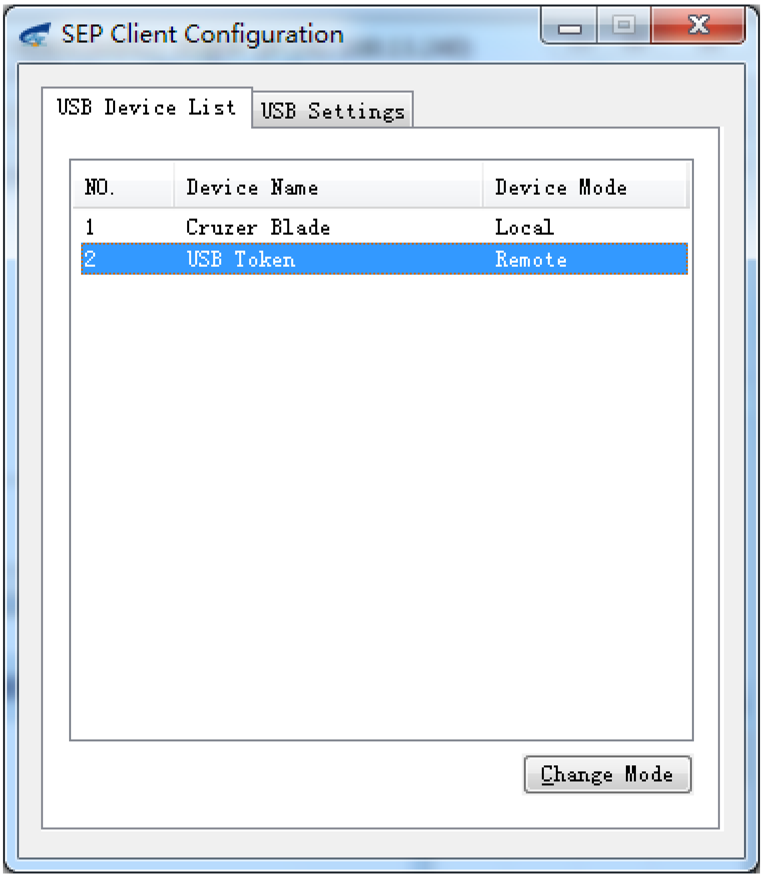
USB Devices

Mass Storage: Local

USB Token: Remote

User interface of the client for cloud terminals

2) In the device list, set the device to "Remote" mode.



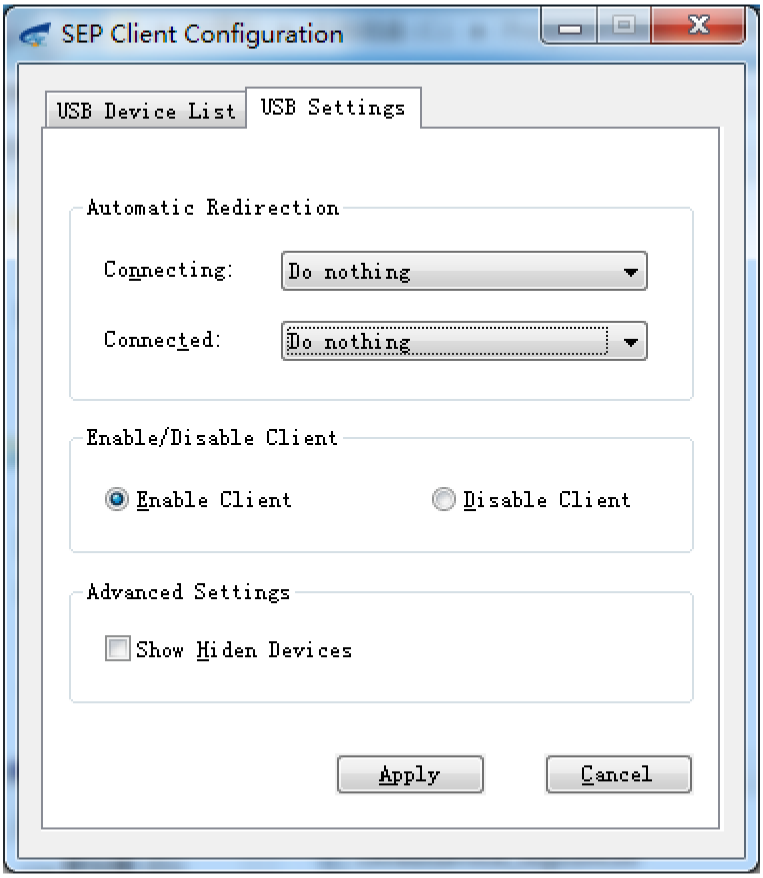
NO.	Device Name	Device Mode
1	Cruzer Blade	Local
2	USB Token	Remote

3) The next time you insert the corresponding device, if the user is currently engaged in a remote session or initiating a remote session, this device will be automatically mapped to the virtual desktop.

3.3.2 Manual mapping of USB device

Manual mapping requires you to manually map the device to the virtual desktop after inserting USB device into the client device.

1) When manual mapping is needed, configure SEP Configure as follows:



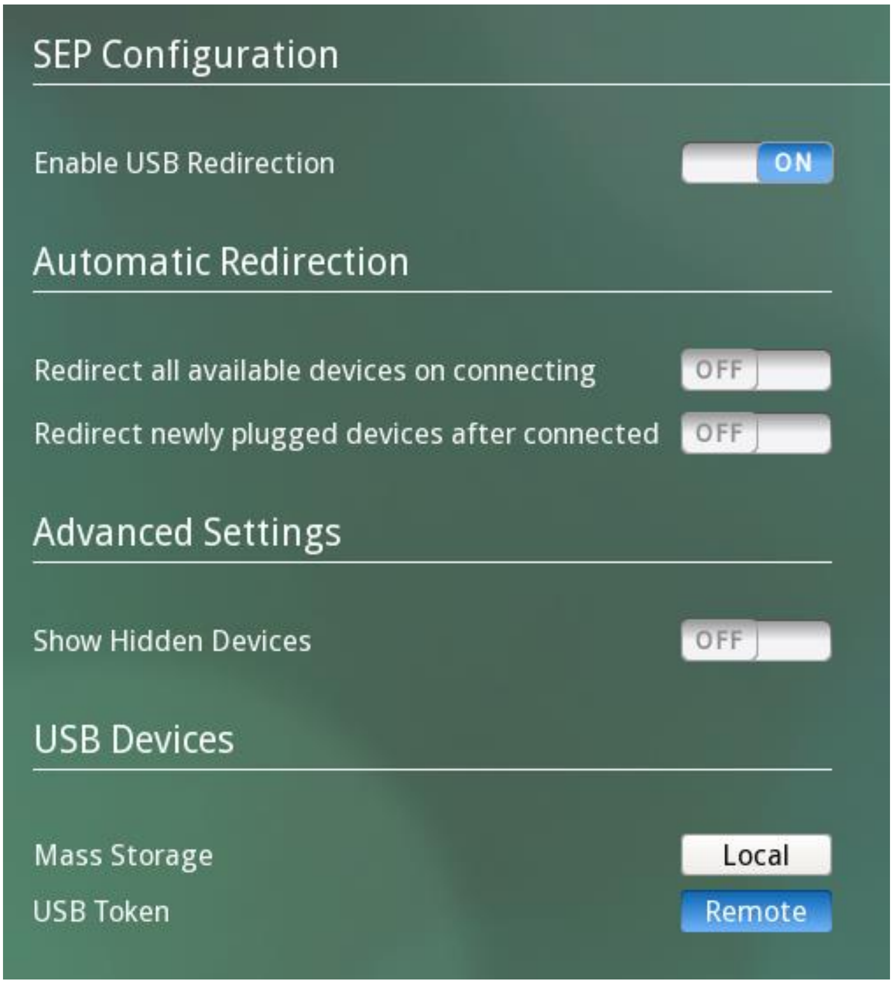
Connecting: Do nothing

Connected: Do nothing

● Enable Client ○ Disable Client

□ Show Hiden Devices

User interface of the client for ordinary terminals



SEP Configuration

Enable USB Redirection ON

Automatic Redirection

Redirect all available devices on connecting OFF

Redirect newly plugged devices after connected OFF

Advanced Settings

Show Hidden Devices OFF

USB Devices

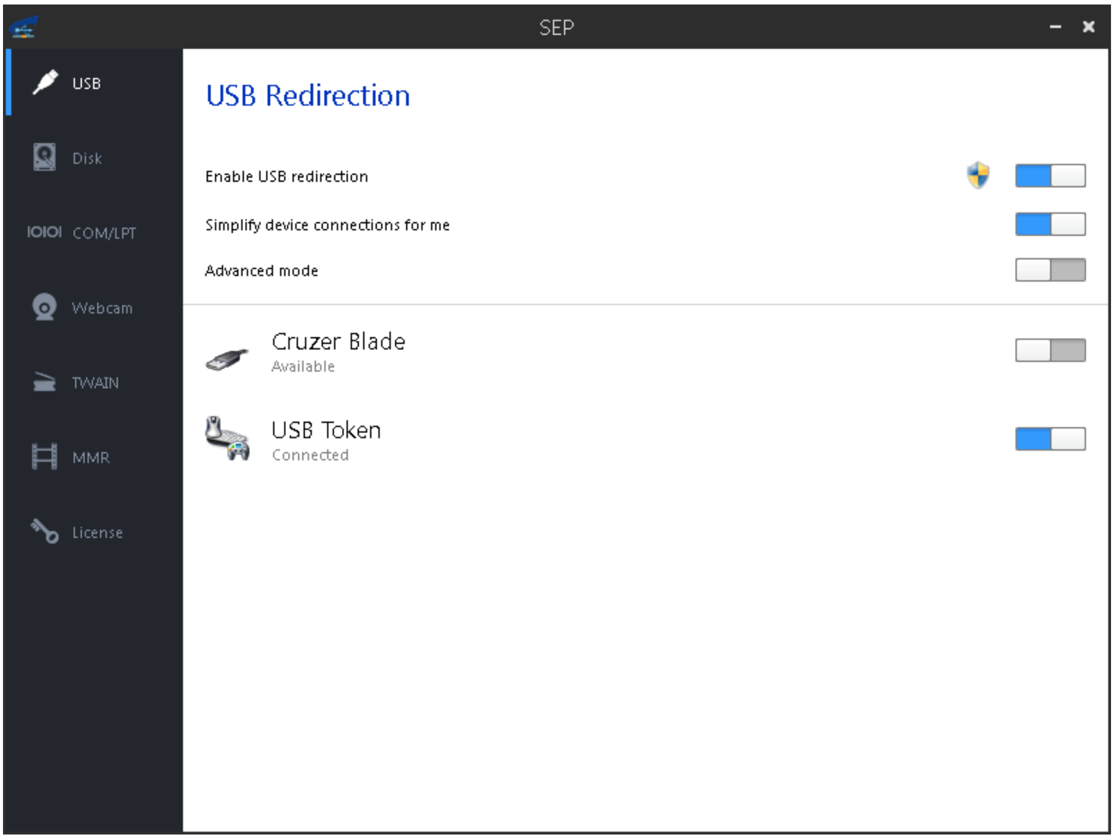
Mass Storage Local

USB Token Remote

User interface of the client for cloud terminals

2) Device is in "Local" mode.

3) Click "Change Mode" button to set the device to "Remote" mode. Mapping is only possible after connecting to the virtual desktop, or you can open SEPApp on the server and click the corresponding switching button.



Enable USB redirection: on

Simplify device connections for me: on

Advanced mode: off

Cruzer Blade
Available: off

USB Token
Connected: on

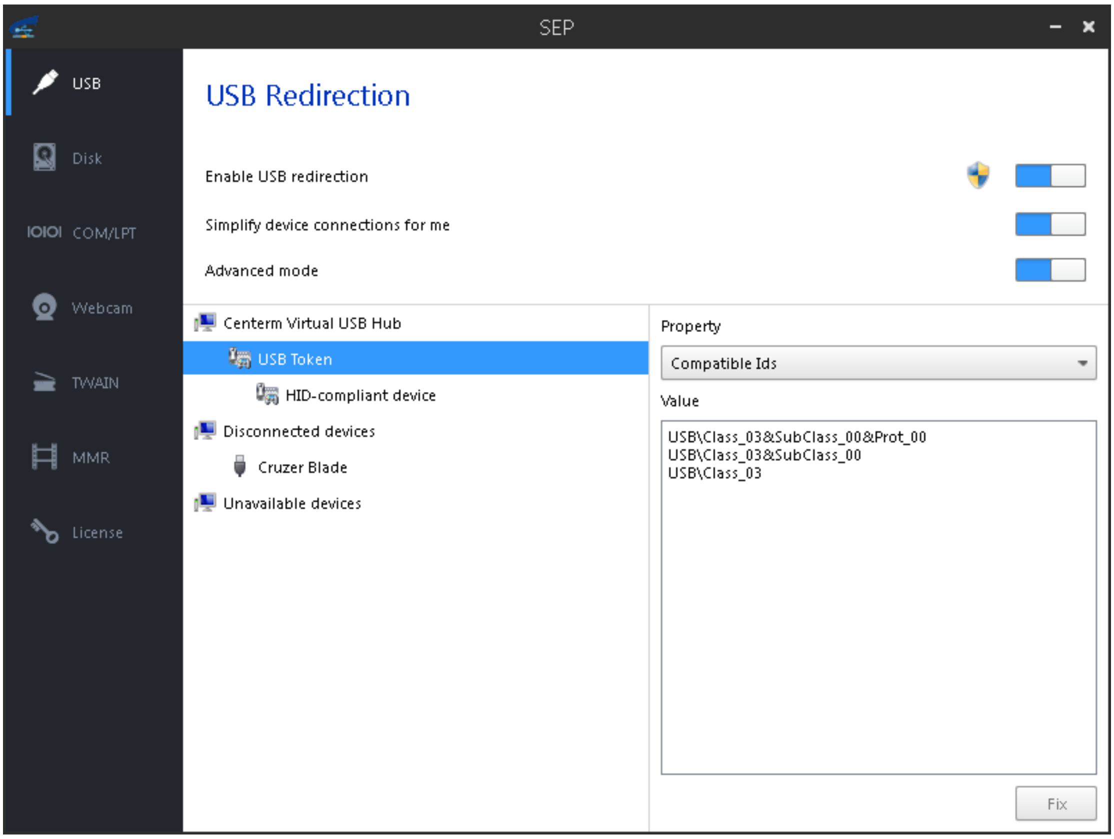
4) "Connected" status indicates successful mapping.

3.3.3 Show hidden devices

Devices hidden by default can be displayed, such as mouse, keyboard, etc. The device mode of hidden devices displayed needs to be switched to "Remote" to allow normal mapping (Note: Switching the device mode of mouse and keyboard must result in local malfunction of mouse/keyboard. You may consult with after-sales engineers for support).

3.3.4 Advanced mode of use mapping

USB-mapped device restoration and display of detailed device information are also supported. Click "Advanced mode" button to switch to the advanced mode, as shown below:



USB\Class_03&SubClass_00&Prot_00
USB\Class_03&SubClass_00
USB\Class_03

3.3.5 Notes

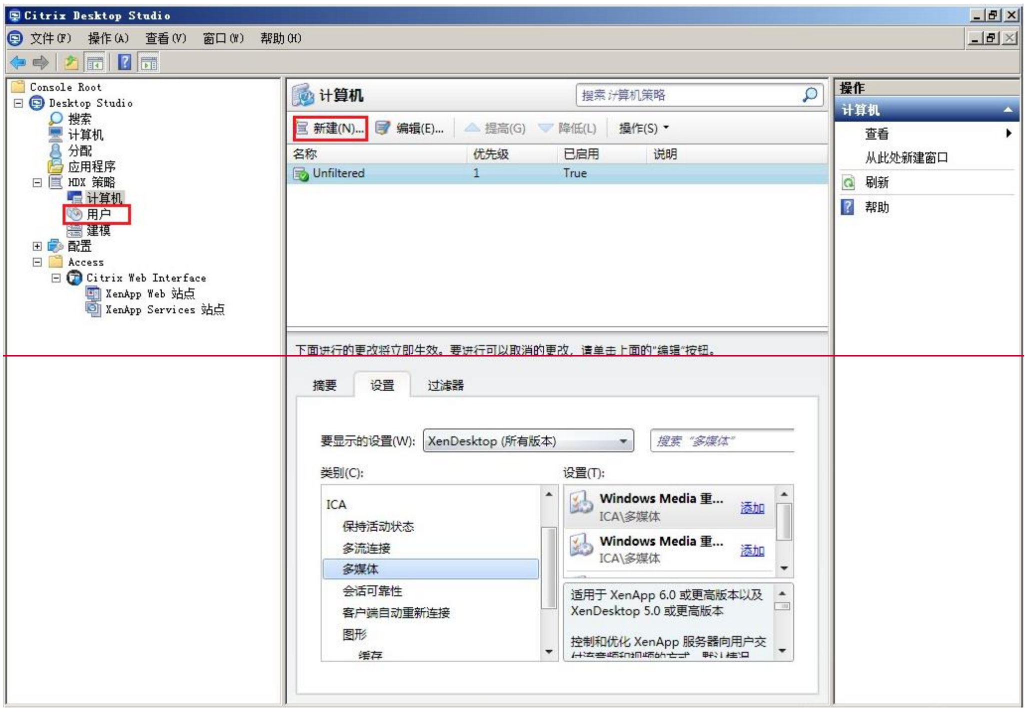
※ USB mapping is not recommended for devices which may transmit excess data within a short period of time, such as USB webcam.

※ It's not recommended to map mouse/keyboard, as this may result in local malfunction of mouse/keyboard. You may consult with after-sales engineers for support.

~~※ Before using the USB mapping of SEP on Citrix virtual desktop, the system administrator must disable the USB redirection policy of Citrix server through the following steps:~~

~~1. Log in Citrix server as system administrator;~~

~~2. Go to "Desktop Studio -> HDX Policy -> User" and click "New";~~



名称	优先级	已启用	说明
Unfiltered	1	True	

下面进行的更改将立即生效。要进行可以取消的更改，请单击上面的"编辑"按钮。

要显示的设置(W): XenDesktop (所有版本)

搜索 "多媒体"

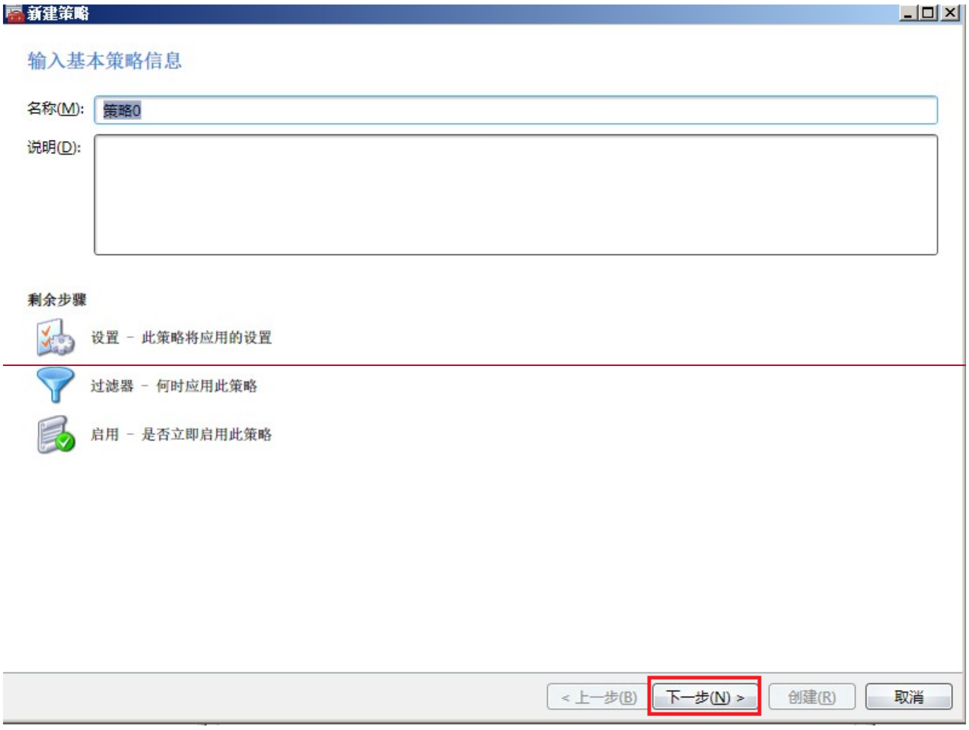
类别(C):

设置(T):

适用于 XenApp 6.0 或更高版本以及 XenDesktop 5.0 或更高版本

控制和优化 XenApp 服务器向用户交付流音频和视频的方式。默认情况

~~2. Click "Next";~~



输入基本策略信息

名称(M): 策略0

说明(D):

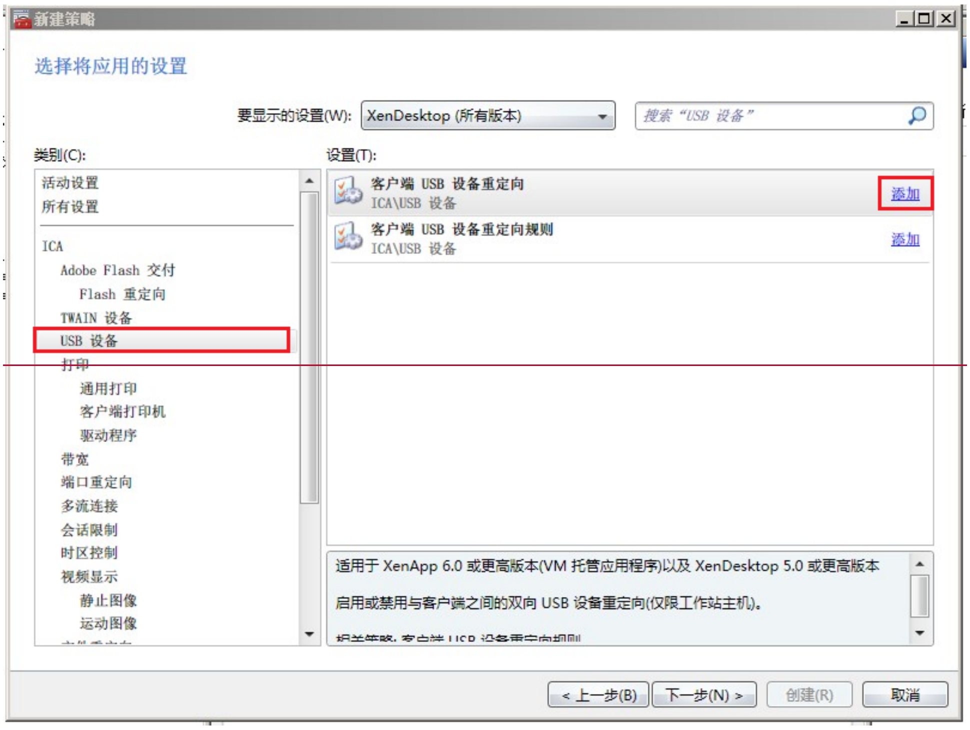
剩余步骤

设置 － 此策略将应用的设置

过滤器 － 何时应用此策略

启用 － 是否立即启用此策略

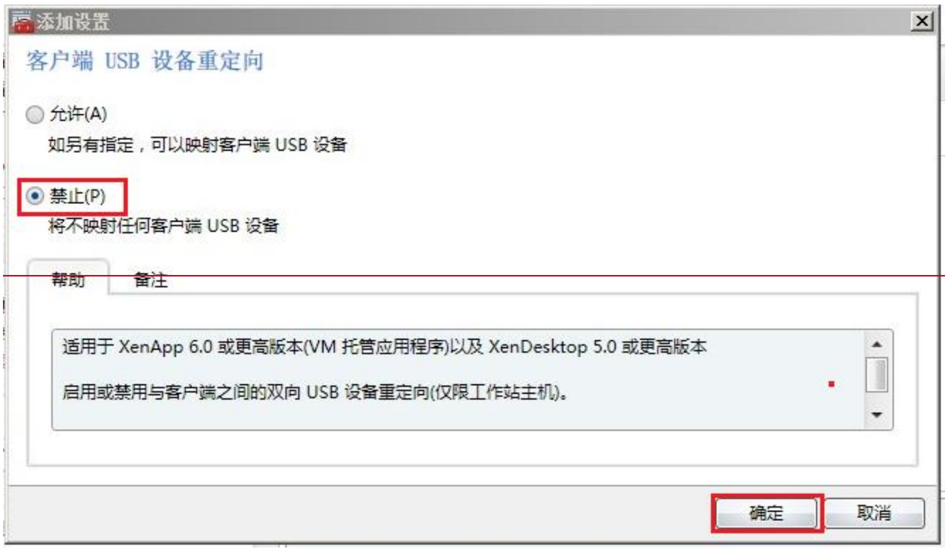
~~3. Select "USB Device" tab and click "Add";~~



适用于 XenApp 6.0 或更高版本(VM 托管应用程序)以及 XenDesktop 5.0 或更高版本

启用或禁用与客户端之间的双向 USB 设备重定向(仅限工作站主机)。

~~Select "Disable" and click "OK";~~



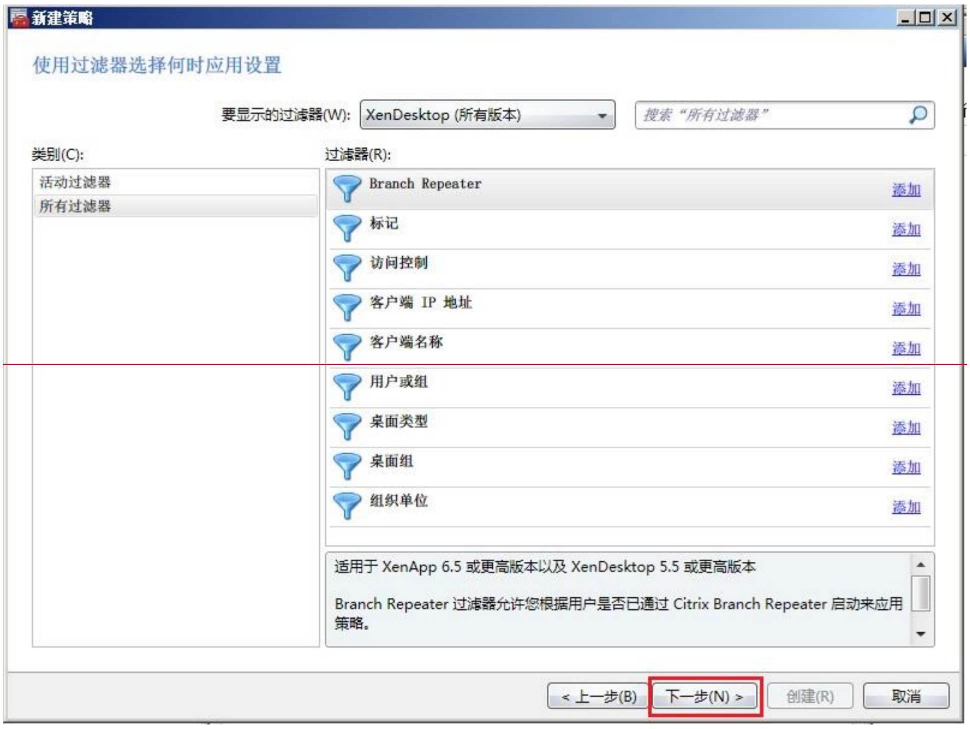
○ 允许(A)
如另有指定，可以映射客户端 USB 设备

● 禁止(P)
将不映射任何客户端 USB 设备

适用于 XenApp 6.0 或更高版本(VM 托管应用程序)以及 XenDesktop 5.0 或更高版本

启用或禁用与客户端之间的双向 USB 设备重定向(仅限工作站主机)。

~~4. Add this policy to the target user or group and click "Next";~~



新建策略

使用过滤器选择何时应用设置

要显示的过滤器(W): XenDesktop (所有版本)

搜索"所有过滤器"

类别(C):
- 活动过滤器
- 所有过滤器

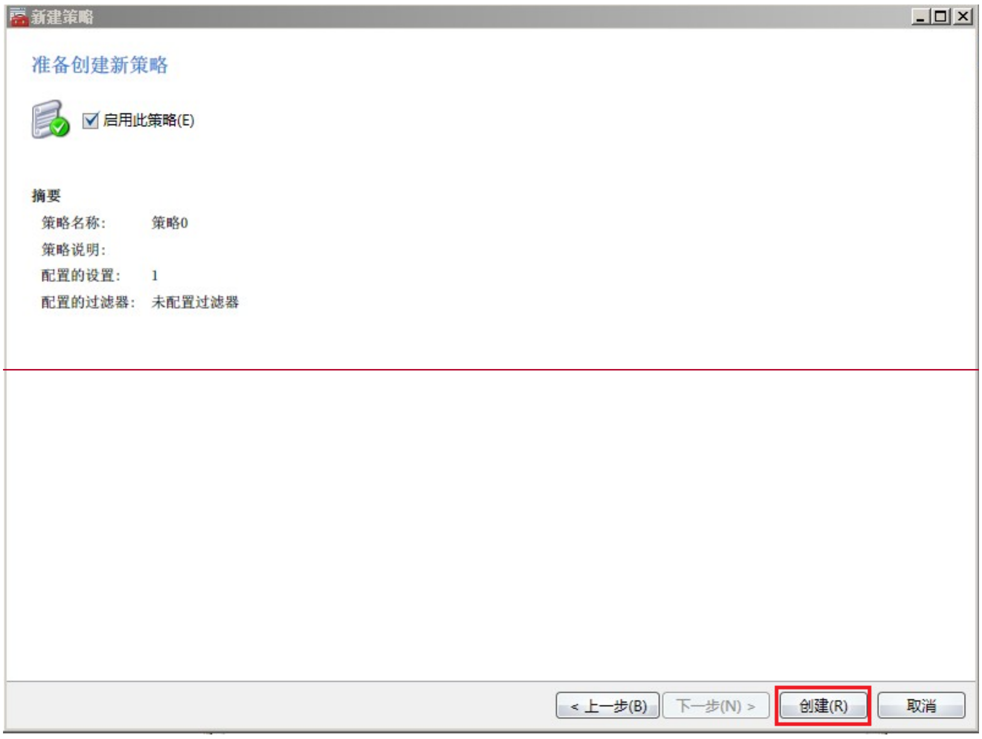
过滤器(R):

Branch Repeater	添加
标记	添加
访问控制	添加
客户端 IP 地址	添加
客户端名称	添加
用户或组	添加
桌面类型	添加
桌面组	添加
组织单位	添加

适用于 XenApp 6.5 或更高版本以及 XenDesktop 5.5 或更高版本

Branch Repeater 过滤器允许您根据用户是否已通过 Citrix Branch Repeater 启动来应用策略。

~~5. Click "Create".~~



新建策略

准备创建新策略

☑ 启用此策略(E)

摘要

策略名称: 策略0

策略说明:

配置的设置: 1

配置的过滤器: 未配置过滤器

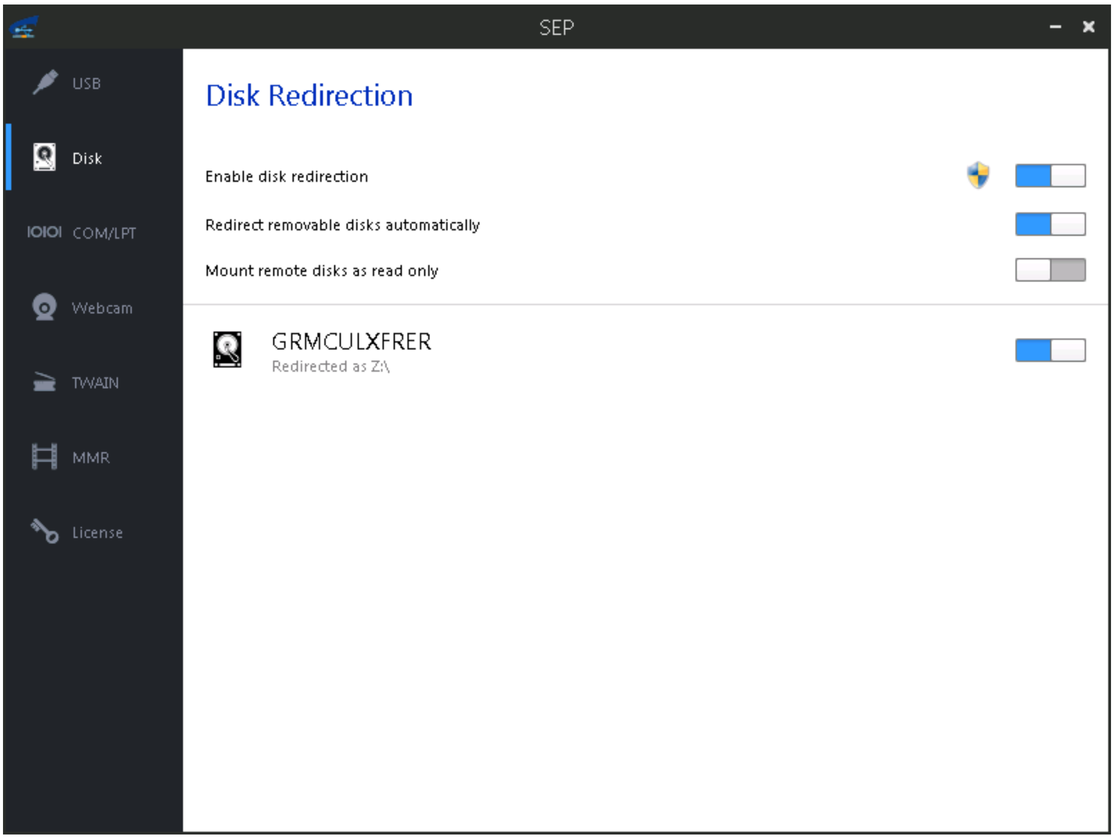
~~After completing the above steps, you can then disable the USB mapping feature of Citrix server.~~

3.4 Disk Mapping

Disk mapping allows you to map the flash disk and mobile HDD on the client side to the virtual desktop. Multi-user isolation is also supported in disk mapping.

3.4.1 Disk mapping configuration

The disk mapping configuration interface is shown below:



Disk Redirection

Enable disk redirection

Redirect removable disks automatically

Mount remote disks as read only

GRMCULXFRER
Redirected as Z:\

3.5 Serial/parallel port mapping

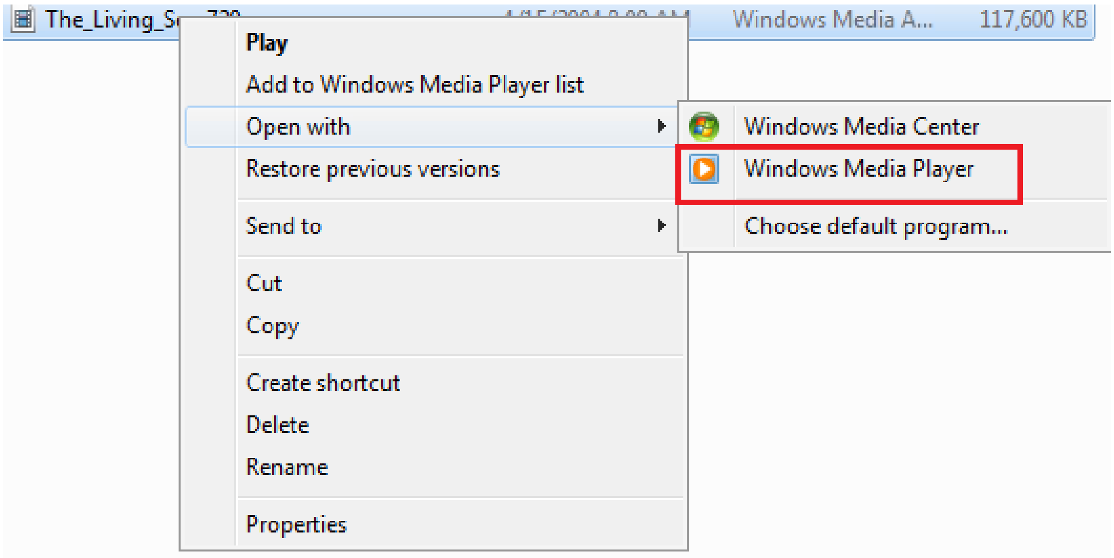
Serial/parallel port mapping allows you to map the serial/parallel port on the client side to the virtual desktop. Multi-user isolation is also supported in serial/parallel port mapping. It's similar to the serial/parallel port mapping feature provided by Microsoft in remote desktop connection.

3.6 MMR

MMR helps optimize the video playback on virtual desktop and resolve the interruptions while the user plays the video on the virtual desktop, so that the playback effect is basically consistent with local playback.

3.6.1 Using MMR to play video

Right-click the video and select "Windows Media Player" to automatically enable MMR to optimize the playback effect.



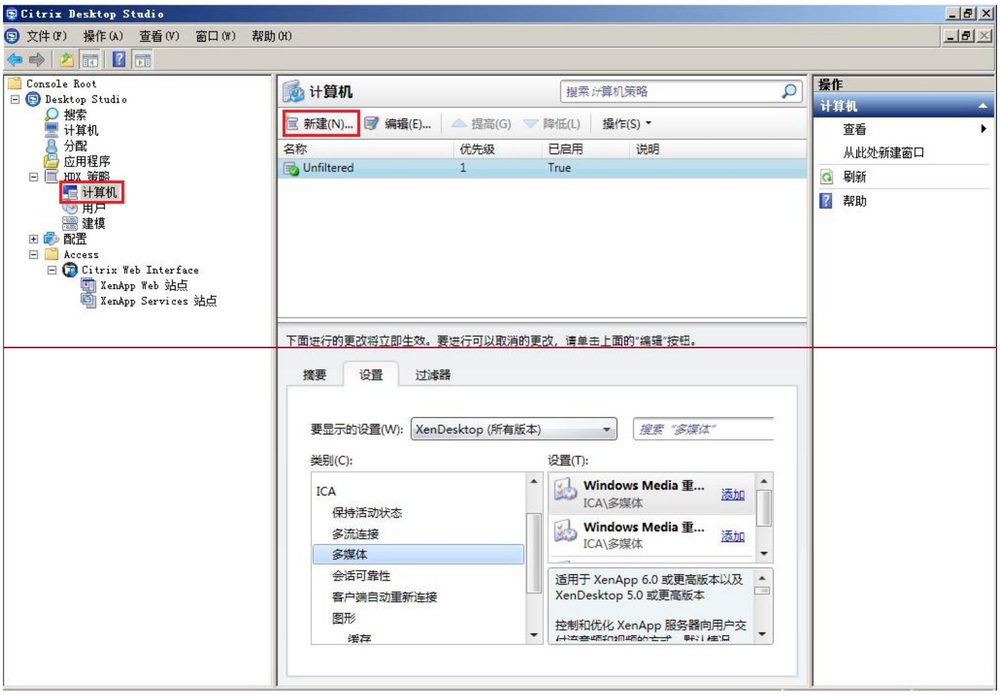
3.6.2 Notes

※ MMR only supports Windows Media Player. MMR cannot optimize the playback effect if you use other types of players.

~~※ Before using the MMR feature of SEP on Citrix virtual desktop, the system administrator must disable the multimedia redirection policy of Citrix server through the following steps:~~

~~1. Log in Citrix server as system administrator;~~

~~2. Go to "Desktop Studio -> HDX Policy -> Computer" and click "New";~~



名称	优先级	已启用	说明
Unfiltered	1	True	

下面进行的更改将立即生效。要进行可以取消的更改，请单击上面的"编辑"按钮。

要显示的设置(W): XenDesktop (所有版本)

搜索 "多媒体"

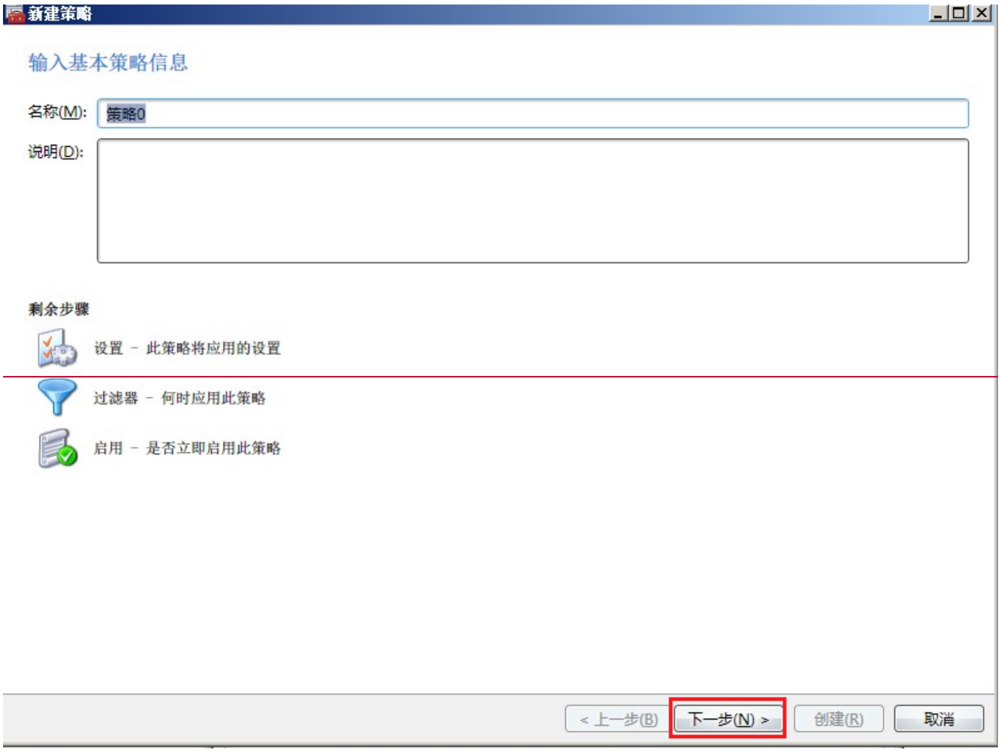
类别(C):

设置(T):

适用于 XenApp 6.0 或更高版本以及 XenDesktop 5.0 或更高版本

控制和优化 XenApp 服务器向用户交

~~2. Click "Next";~~

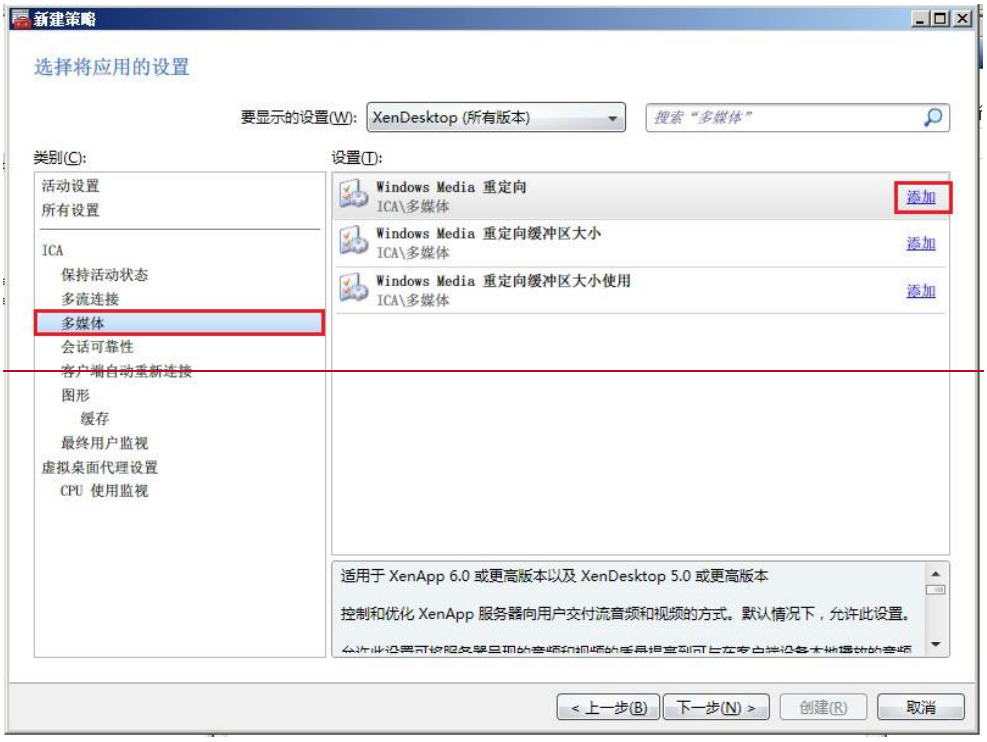


输入基本策略信息

名称(M): 策略0

说明(D):

~~Select "Multimedia" tab and click "Add";~~



新建策略

选择将应用的设置

要显示的设置(W): XenDesktop (所有版本)

搜索"多媒体"

类别(C):
- 活动设置
- 所有设置
- ICA
  - 保持活动状态
  - 多流连接
  - 多媒体
  - 会话可靠性
  - 客户端自动重新连接
  - 图形
    - 缓存
  - 最终用户监视
- 虚拟桌面代理设置
  - CPU 使用监视

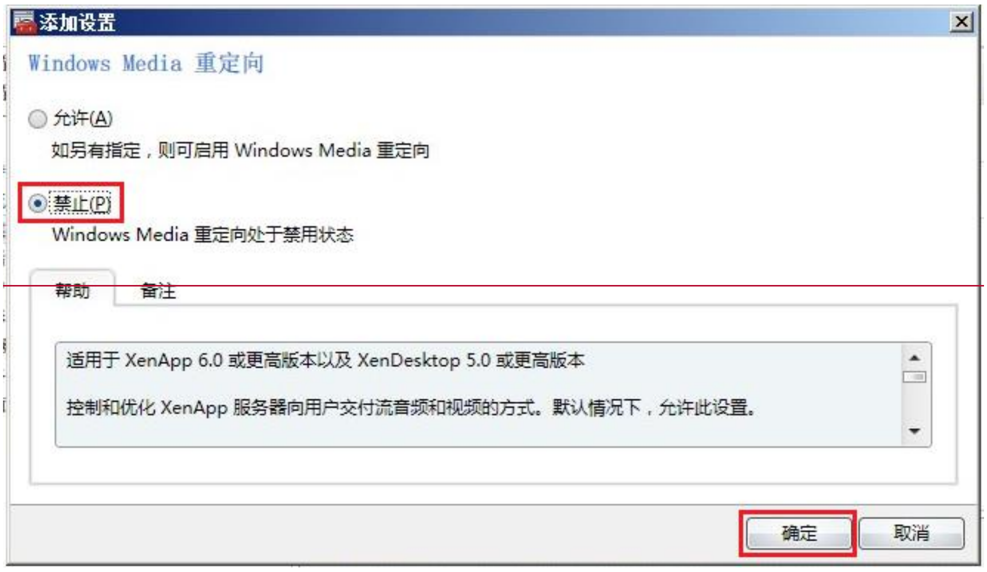
设置(T):
- Windows Media 重定向 ICA\多媒体 添加
- Windows Media 重定向缓冲区大小 ICA\多媒体 添加
- Windows Media 重定向缓冲区大小使用 ICA\多媒体 添加

适用于 XenApp 6.0 或更高版本以及 XenDesktop 5.0 或更高版本

控制和优化 XenApp 服务器向用户交付流音频和视频的方式。默认情况下，允许此设置。

允许此设置可将服务器呈现的音频和视频的质量提高到可与在客户端设备本地播放的音频

~~3. Select "Disable" and click "OK";~~



添加设置

Windows Media 重定向

○ 允许(A)

如另有指定，则可启用 Windows Media 重定向

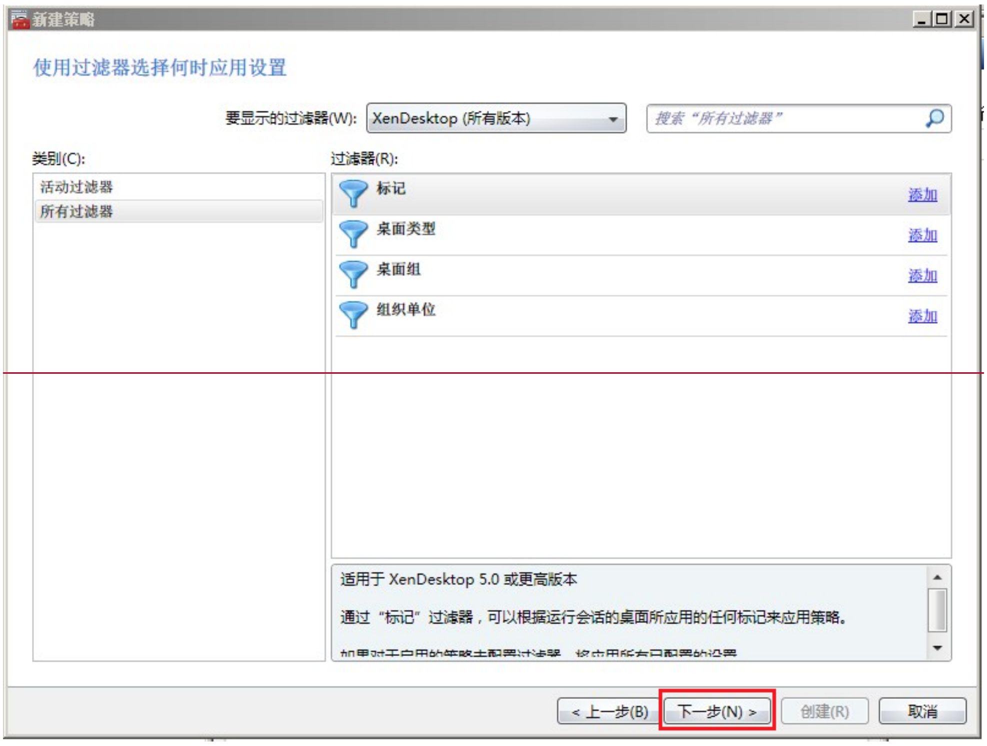
● 禁止(P)

Windows Media 重定向处于禁用状态

适用于 XenApp 6.0 或更高版本以及 XenDesktop 5.0 或更高版本

控制和优化 XenApp 服务器向用户交付流音频和视频的方式。默认情况下，允许此设置。

~~4. Add this policy to the target user or group and click "Next";~~



新建策略

使用过滤器选择何时应用设置

要显示的过滤器(W): XenDesktop (所有版本)

类别(C):
- 活动过滤器
- 所有过滤器

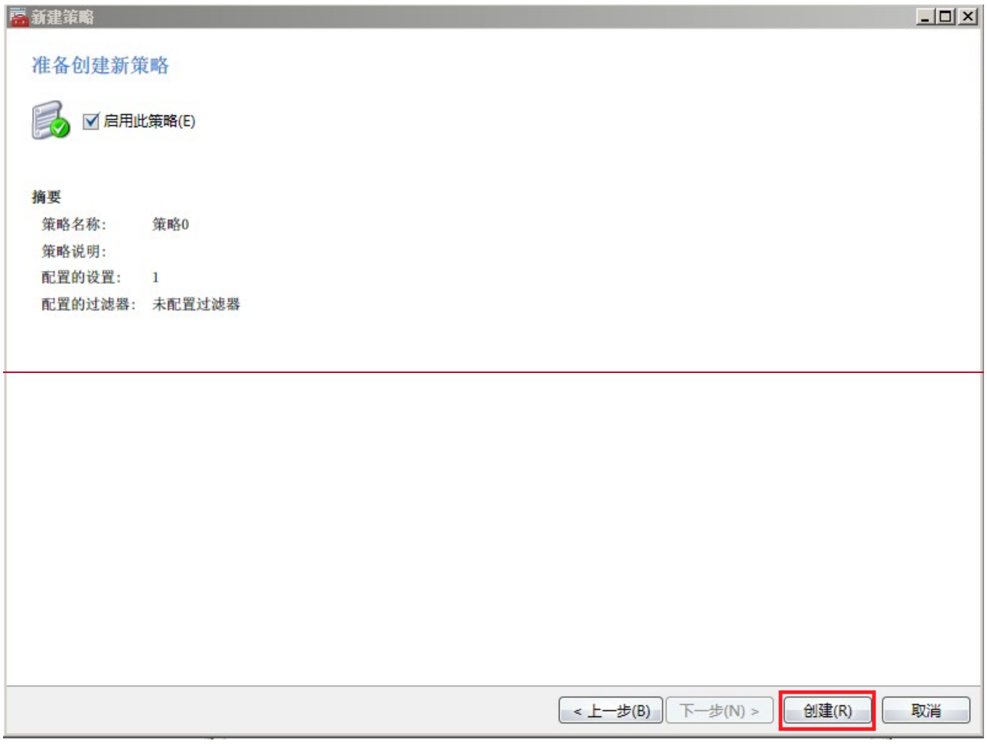
过滤器(R):
- 标记 添加
- 桌面类型 添加
- 桌面组 添加
- 组织单位 添加

适用于 XenDesktop 5.0 或更高版本

通过“标记”过滤器，可以根据运行会话的桌面所应用的任何标记来应用策略。

如果对于启用的策略未配置过滤器，将应用所有已配置的设置

~~5. Click "Create".~~



新建策略

准备创建新策略

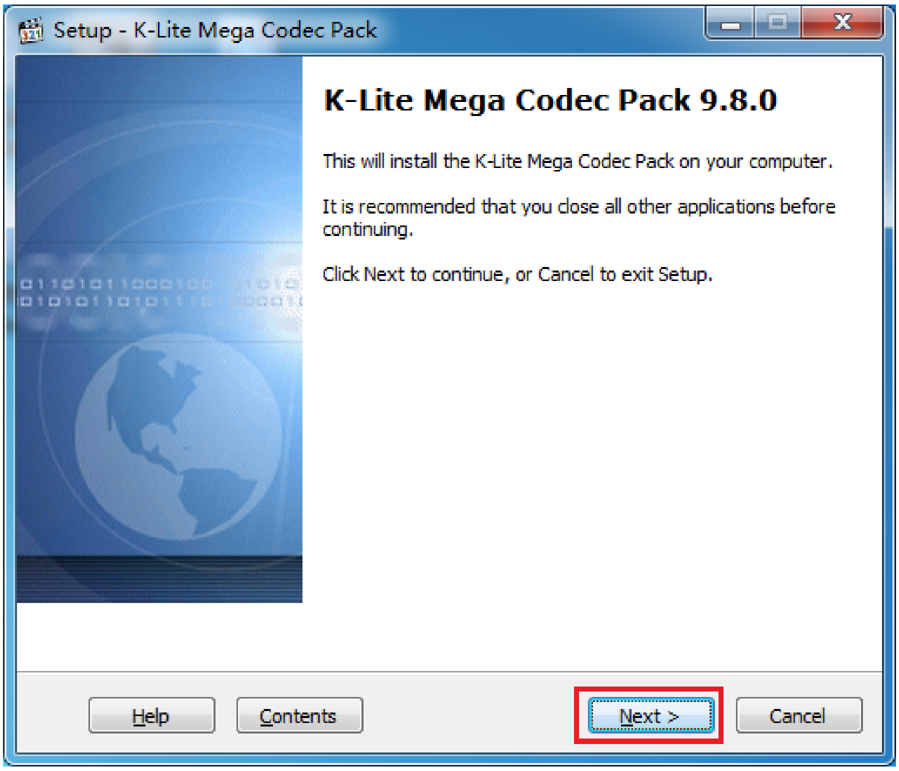
☑ 启用此策略(E)

摘要

策略名称: 策略0
策略说明:
配置的设置: 1
配置的过滤器: 未配置过滤器

~~After completing the above steps, you can then disable the multimedia mapping feature of Citrix server.~~

※ Before using MMR, please install K-Lite first on the server and client. V9.8.0 is highly recommended. The installation steps are shown below:



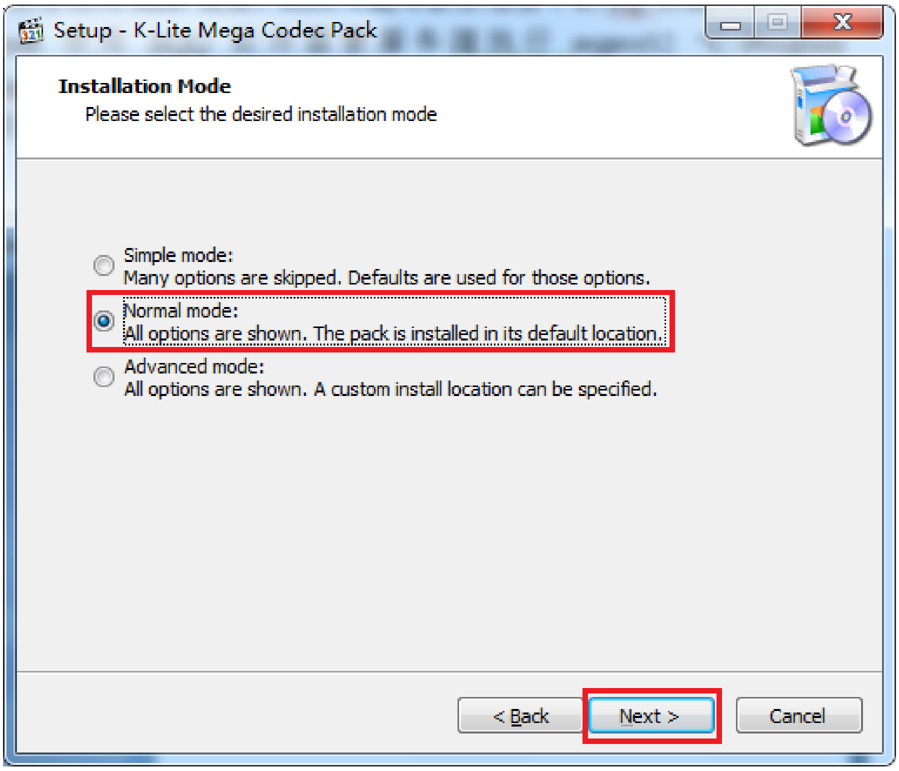
Setup - K-Lite Mega Codec Pack

K-Lite Mega Codec Pack 9.8.0

This will install the K-Lite Mega Codec Pack on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.



Setup - K-Lite Mega Codec Pack

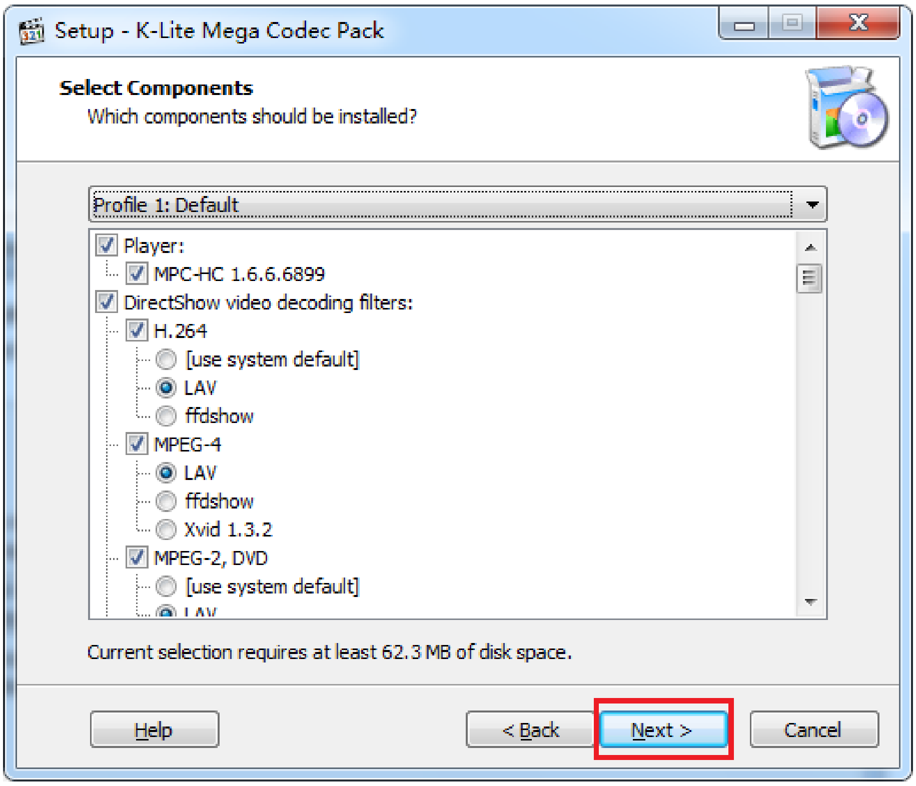
Installation Mode

Please select the desired installation mode

○ Simple mode:
Many options are skipped. Defaults are used for those options.

● Normal mode:
All options are shown. The pack is installed in its default location.

○ Advanced mode:
All options are shown. A custom install location can be specified.



Setup - K-Lite Mega Codec Pack

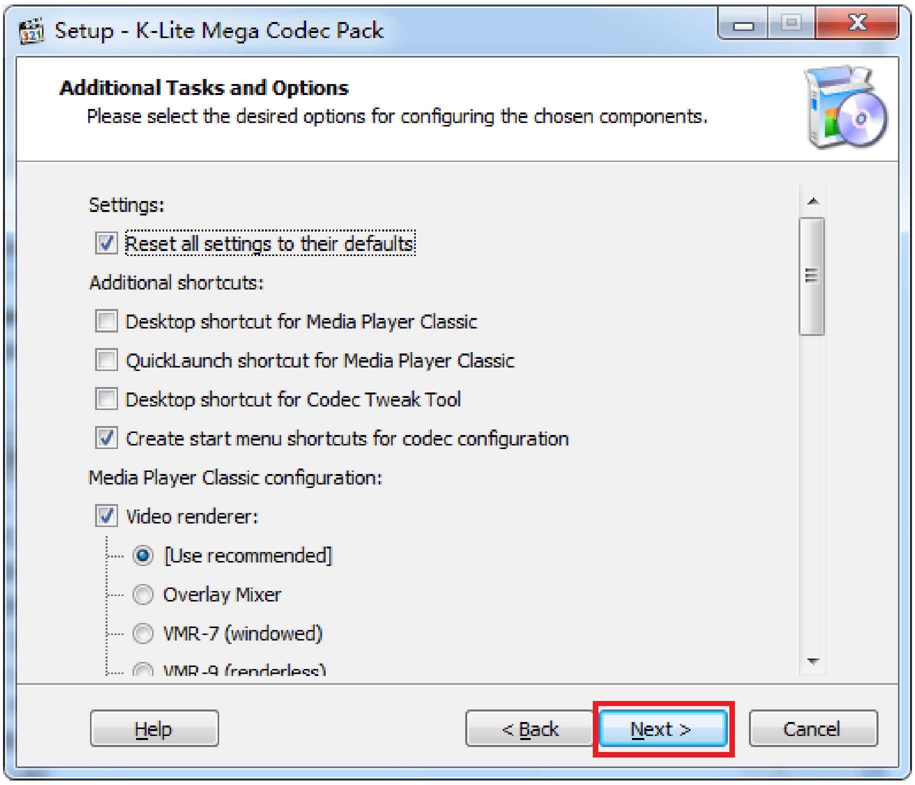
Select Components

Which components should be installed?

Profile 1: Default

- ☑ Player:
  - ☑ MPC-HC 1.6.6.6899
- ☑ DirectShow video decoding filters:
  - ☑ H.264
    - ○ [use system default]
    - ● LAV
    - ○ ffdshow
  - ☑ MPEG-4
    - ● LAV
    - ○ ffdshow
    - ○ Xvid 1.3.2
  - ☑ MPEG-2, DVD
    - ○ [use system default]
    - ● LAV

Current selection requires at least 62.3 MB of disk space.



Setup - K-Lite Mega Codec Pack

Additional Tasks and Options

Please select the desired options for configuring the chosen components.

Settings:

☑ Reset all settings to their defaults

Additional shortcuts:

☐ Desktop shortcut for Media Player Classic

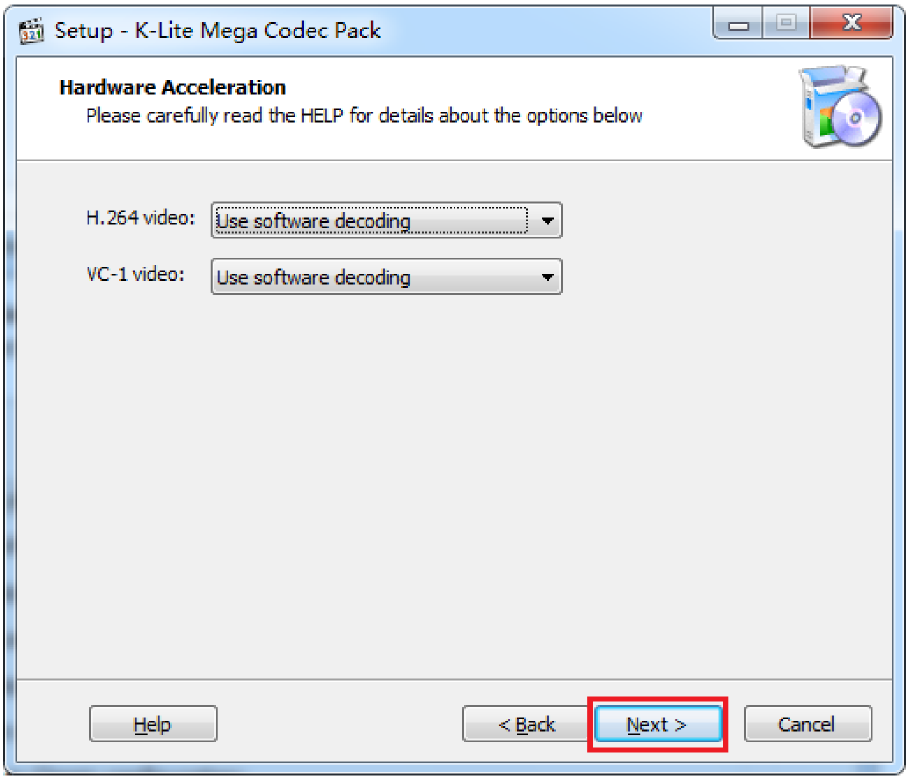
☐ QuickLaunch shortcut for Media Player Classic

☐ Desktop shortcut for Codec Tweak Tool

☑ Create start menu shortcuts for codec configuration

Media Player Classic configuration:

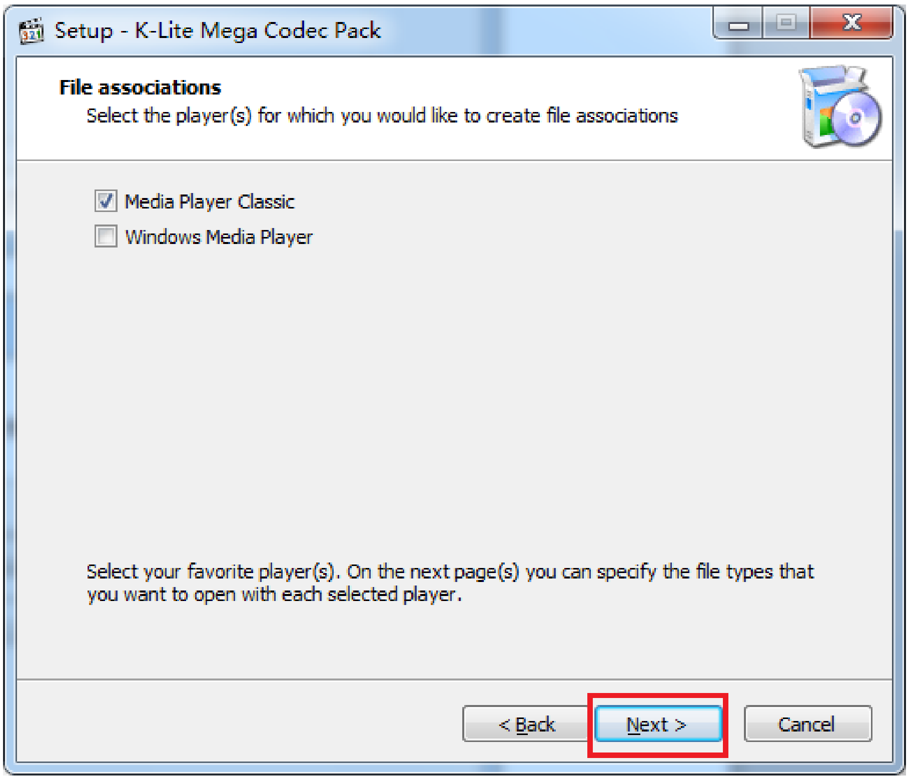
☑ Video renderer:
- ● [Use recommended]
- ○ Overlay Mixer
- ○ VMR-7 (windowed)
- ○ VMR-9 (renderless)



Setup - K-Lite Mega Codec Pack

Hardware Acceleration
Please carefully read the HELP for details about the options below

H.264 video: Use software decoding
VC-1 video: Use software decoding

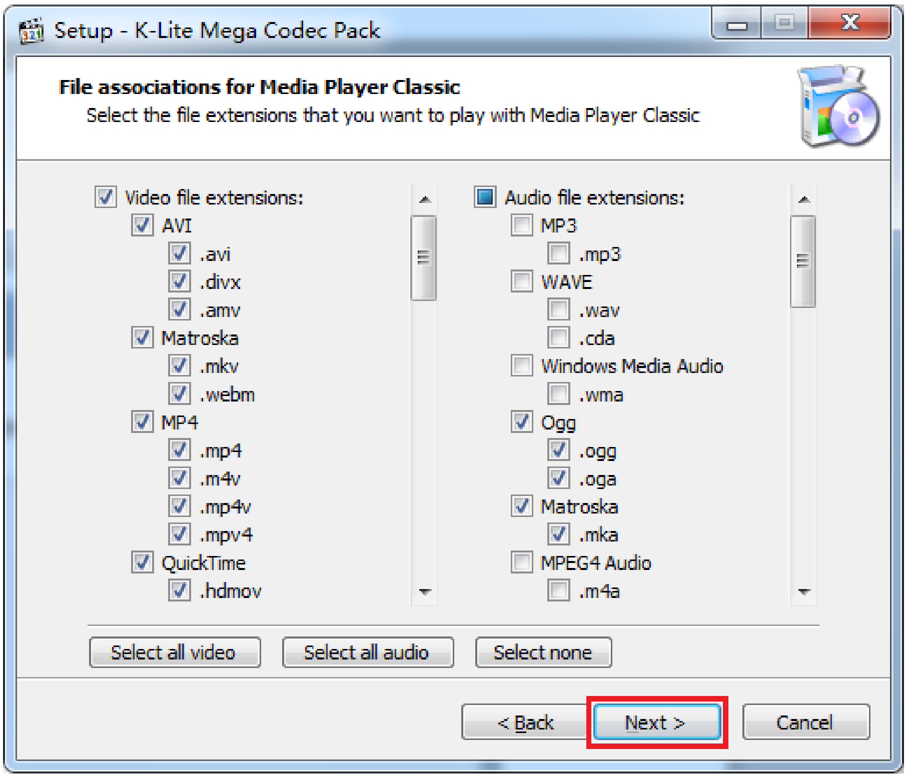


Setup - K-Lite Mega Codec Pack

File associations
Select the player(s) for which you would like to create file associations

☑ Media Player Classic
□ Windows Media Player

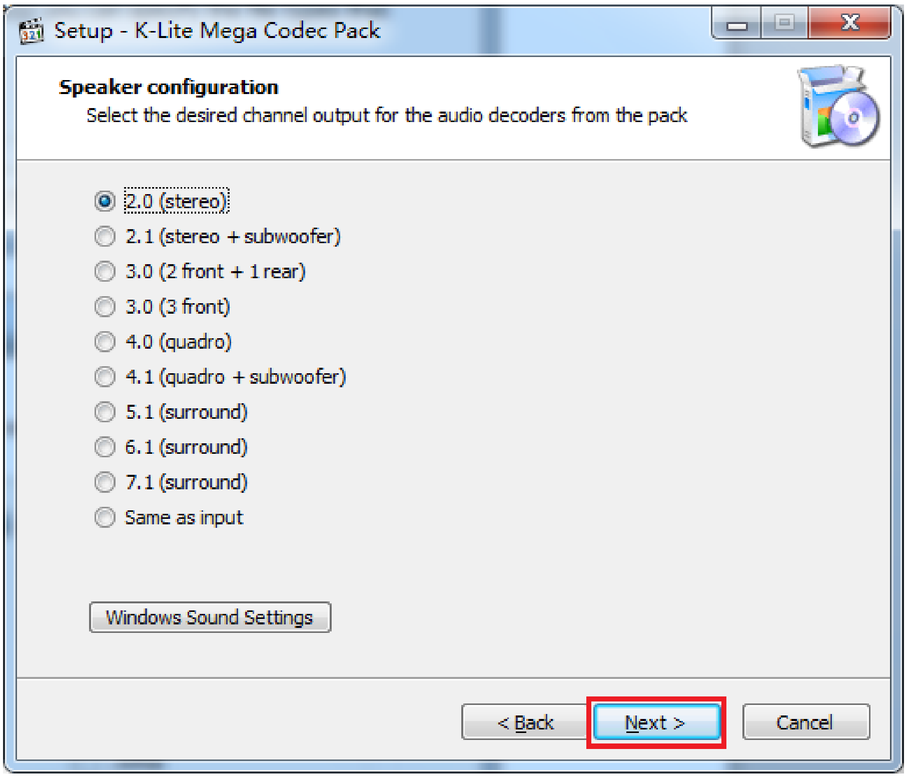
Select your favorite player(s). On the next page(s) you can specify the file types that you want to open with each selected player.


Setup - K-Lite Mega Codec Pack

File associations for Media Player Classic
Select the file extensions that you want to play with Media Player Classic

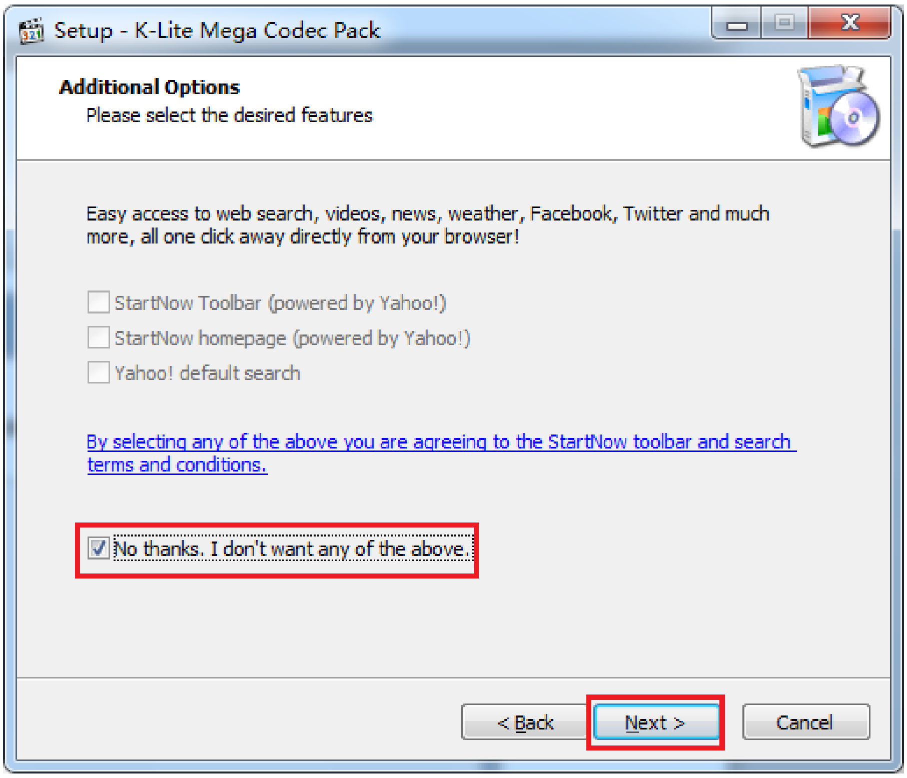
☑ Video file extensions:
- ☑ AVI
  - ☑ .avi
  - ☑ .divx
  - ☑ .amv
- ☑ Matroska
  - ☑ .mkv
  - ☑ .webm
- ☑ MP4
  - ☑ .mp4
  - ☑ .m4v
  - ☑ .mp4v
  - ☑ .mpv4
- ☑ QuickTime
  - ☑ .hdmov

▣ Audio file extensions:
- ☐ MP3
  - ☐ .mp3
- ☐ WAVE
  - ☐ .wav
  - ☐ .cda
- ☐ Windows Media Audio
  - ☐ .wma
- ☑ Ogg
  - ☑ .ogg
  - ☑ .oga
- ☑ Matroska
  - ☑ .mka
- ☐ MPEG4 Audio
  - ☐ .m4a


Setup - K-Lite Mega Codec Pack

Speaker configuration
Select the desired channel output for the audio decoders from the pack

● 2.0 (stereo)
○ 2.1 (stereo + subwoofer)
○ 3.0 (2 front + 1 rear)
○ 3.0 (3 front)
○ 4.0 (quadro)
○ 4.1 (quadro + subwoofer)
○ 5.1 (surround)
○ 6.1 (surround)
○ 7.1 (surround)
○ Same as input



Setup - K-Lite Mega Codec Pack

Additional Options

Please select the desired features

Easy access to web search, videos, news, weather, Facebook, Twitter and much more, all one click away directly from your browser!

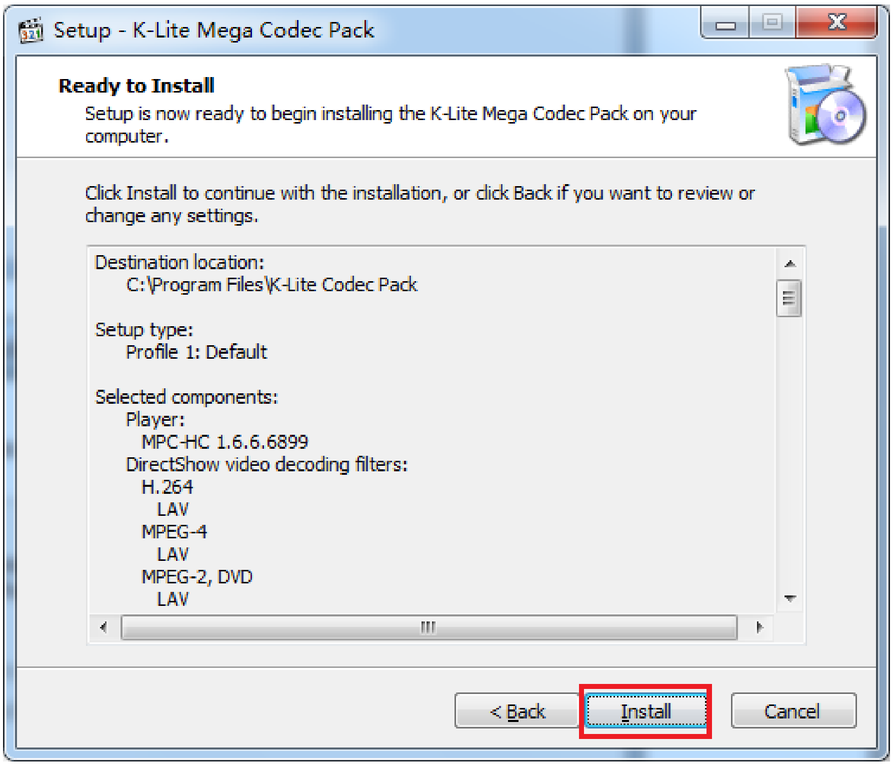
□ StartNow Toolbar (powered by Yahoo!)

□ StartNow homepage (powered by Yahoo!)

□ Yahoo! default search

By selecting any of the above you are agreeing to the StartNow toolbar and search terms and conditions.

☑ No thanks. I don't want any of the above.



Setup - K-Lite Mega Codec Pack

Ready to Install

Setup is now ready to begin installing the K-Lite Mega Codec Pack on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

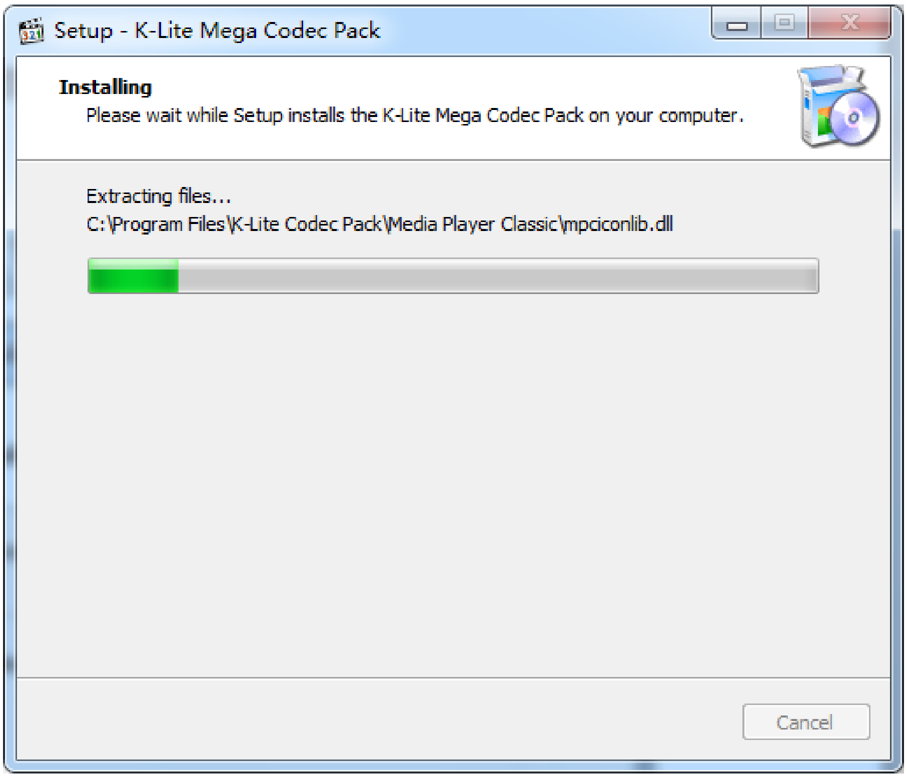
```
Destination location:
    C:\Program Files\K-Lite Codec Pack

Setup type:
    Profile 1: Default

Selected components:
    Player:
      MPC-HC 1.6.6.6899
    DirectShow video decoding filters:
      H.264
        LAV
      MPEG-4
        LAV
      MPEG-2, DVD
        LAV
```

Approved by: Checked by: Prepared by:

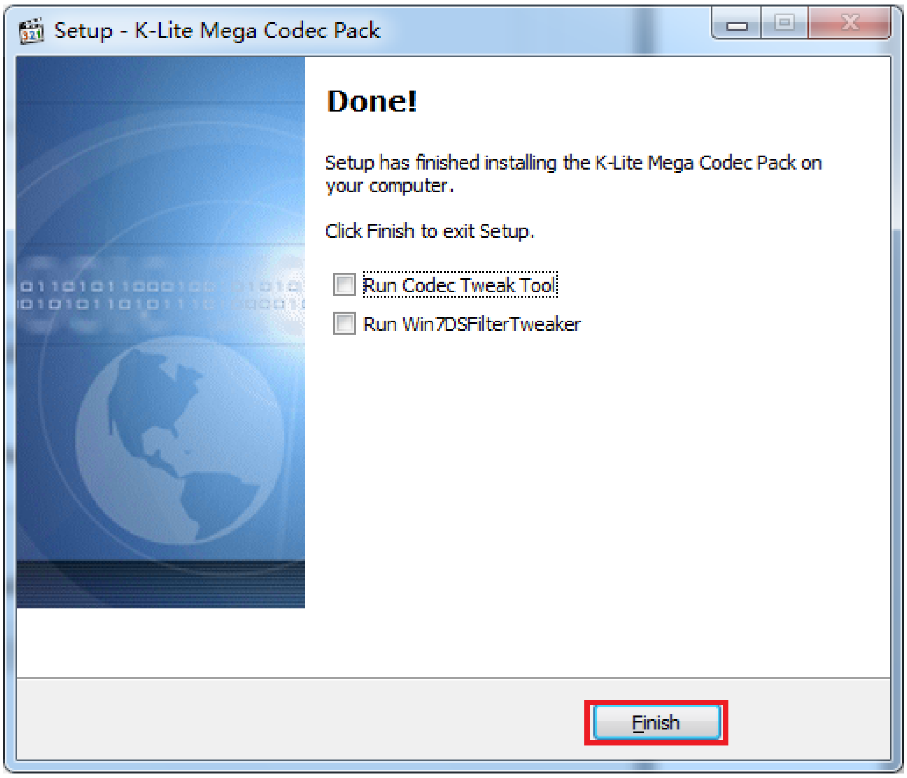
Date: Date: Date:



Setup - K-Lite Mega Codec Pack

Installing
Please wait while Setup installs the K-Lite Mega Codec Pack on your computer.

Extracting files...
C:\Program Files\K-Lite Codec Pack\Media Player Classic\mpciconlib.dll



Setup - K-Lite Mega Codec Pack

Done!

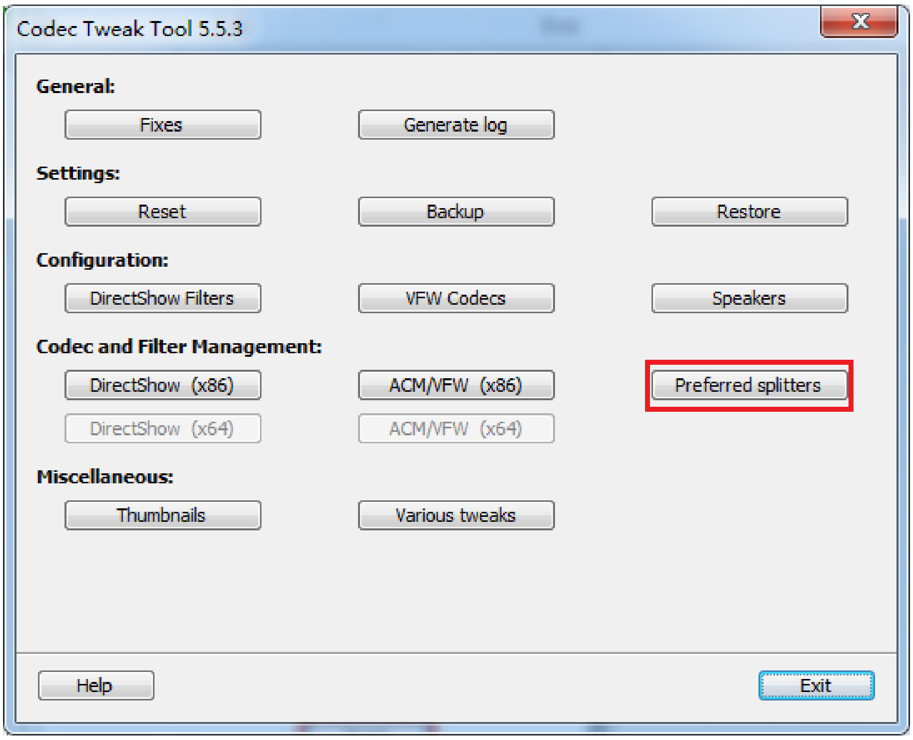
Setup has finished installing the K-Lite Mega Codec Pack on your computer.

Click Finish to exit Setup.

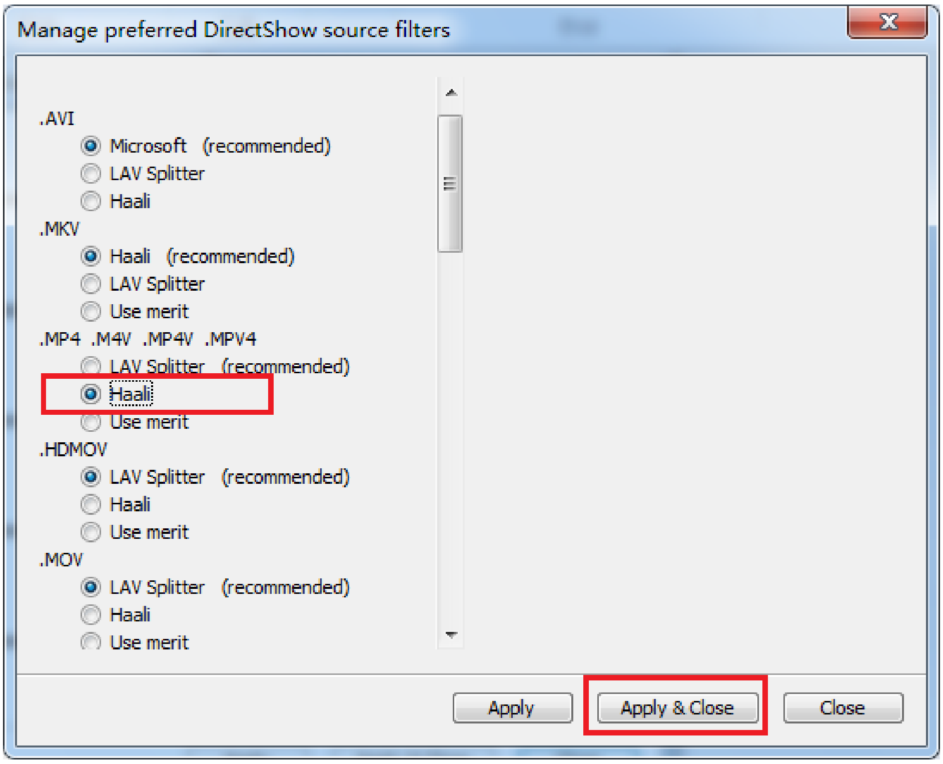
□ Run Codec Tweak Tool
□ Run Win7DSFilterTweaker

※ In case mpeg4 video playback encounters interruptions, you may set MP4 video splitter to "Haali", as shown below:

Go to "Start -> K-Lite Codec Pack -> Codec Tweak Tool" and click "Preferred splitters".



Find ".MP4", ".M4V", ".MP4V" and ".MPV4", select "Haali" and then click "Apply & Close".



.AVI
- ● Microsoft (recommended)
- ○ LAV Splitter
- ○ Haali

.MKV
- ● Haali (recommended)
- ○ LAV Splitter
- ○ Use merit

.MP4 .M4V .MP4V .MPV4
- ○ LAV Splitter (recommended)
- ● Haali
- ○ Use merit

.HDMOV
- ● LAV Splitter (recommended)
- ○ Haali
- ○ Use merit

.MOV
- ● LAV Splitter (recommended)
- ○ Haali
- ○ Use merit

3.7 Other Notes

※ When an RDP connection already exists, exit RDP connection and then use ICA to reestablish the connection. Do not use ICA connection to occupy RDP connection, in which case SEP may not function under this connection.

※ Due to insufficient permissions, the user is unable to read the USB configurations of the administrator on Windows terminals, and the USB client configurations may display the default settings. It's totally normal.