

KASPERSKY SECURITY CENTER 10 & KASPERSKY SECURITY FOR SERVER

Testing of Installation base on the AWS server

Abstract

This document create to present the result of testing installation of KSC 10 and the Kaspersky Security for Server (ks4w). The result show the component that contain in the KES console if the KES install into the server. This document also show the Network Polling to push Network Agent remotely on the AWS server. Perform Backup & Restore the KSC.

Table of Contain

Table of Contain.....	i
List of Figure	ii
Introduction	1
Installation Kaspersky Security Center on Windows Server 2012 (KSC Server)	1
Remote Installation of Network Agent and KES 10 (KES Server)	6
1. Network Polling	6
2. Push installation of Network Agent and KES	7
Kaspersky Security for Windows Server (ks4ws).....	8
1. Download the ks4ws into the KES Server	8
2. Install the ks4ws into KES Server.	8
3. Install Kaspersky Security Plug-in into KSC Server	12
4. Create Windows Server Policies	13
Backup and Restore the KSC	15
1. Apply Backup on KSC Server	15
2. Apply Restore on new KSC Server	16
3. Klmover - a utility for changing Network Agent settings.....	18

List of Figure

Figure 1: List of Policies	1
Figure 2: Properties: KES 10	1
Figure 3: Firewall setting Window.....	2
Figure 4: Network rule	2
Figure 5: KSC 10 Console	3
Figure 6: KES 10 for Windows on Server	4
Figure 7: KES 10 for Windows on Endpoint Workstation (Endpoint Control).....	4
Figure 8: KES 10 for Windows on Endpoint Workstation (Protection)	5
Figure 9: Setup the IP address range	6
Figure 10: List of the IP Address	6
Figure 11: Status of the installation server.....	7
Figure 12: ks4ws.exe Installer.....	8
Figure 13: KS4WS installation console	8
Figure 14: Welcome page setup wizard	9
Figure 15: End User License Agreement	9
Figure 16: Quick Scan page	10
Figure 17: Activation of the application.....	10
Figure 18: KS4WS installation console	11
Figure 19: Kaspersky Security Console	11
Figure 20: KS4WS installation console	12
Figure 21: Plug-in setup Wizard	12
Figure 22: Policies tab.....	13
Figure 23: New Policy wizard.....	13
Figure 24: Application to create a group Policy.....	14
Figure 25: Window Server policy created.....	14

Figure 26: klbackup.exe directory	15
Figure 27: Choose action.....	15
Figure 28: Backup destination folder & password	16
Figure 29: klbackup.exe directory.....	16
Figure 30: Choose action.....	17
Figure 31: Folder for storage of backup copies.....	17
Figure 32: CMD	18

Introduction

For this testing environment, have create two (2) AWS Server that name as KSC Server and KES Server.

Before install the KSC, make sure all the port are open and close the Windows Firewall for both server. Install the telnet client and server on the both server.

Installation Kaspersky Security Center on Windows Server 2012 (KSC Server)

After installation and active the license of KSC into the server, click **Policies (Managed computers > Policies)**, double click on Kaspersky Endpoint Security 10. Refer Figure 1.

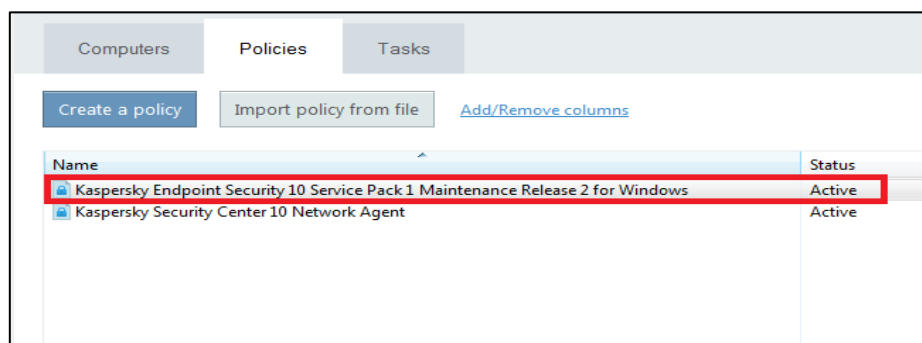


Figure 1: List of Policies

Then, select **Firewall > Setting (Configure rules for Application Privilege Control in the operating system)**. Refer to Figure 2.

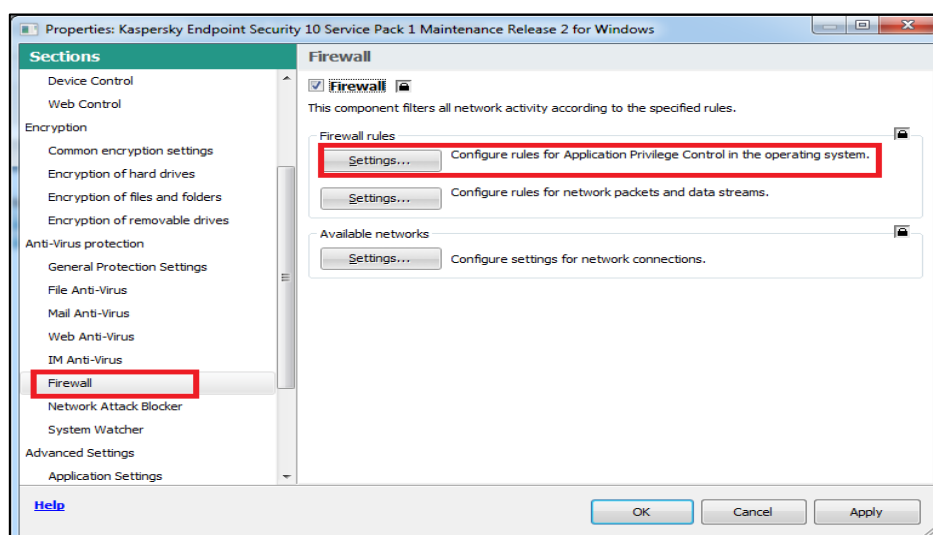


Figure 2: Properties: KES 10

Select **Network packet rules** > **Remote Desktop network activity** > **Edit**. Refer Figure 3.

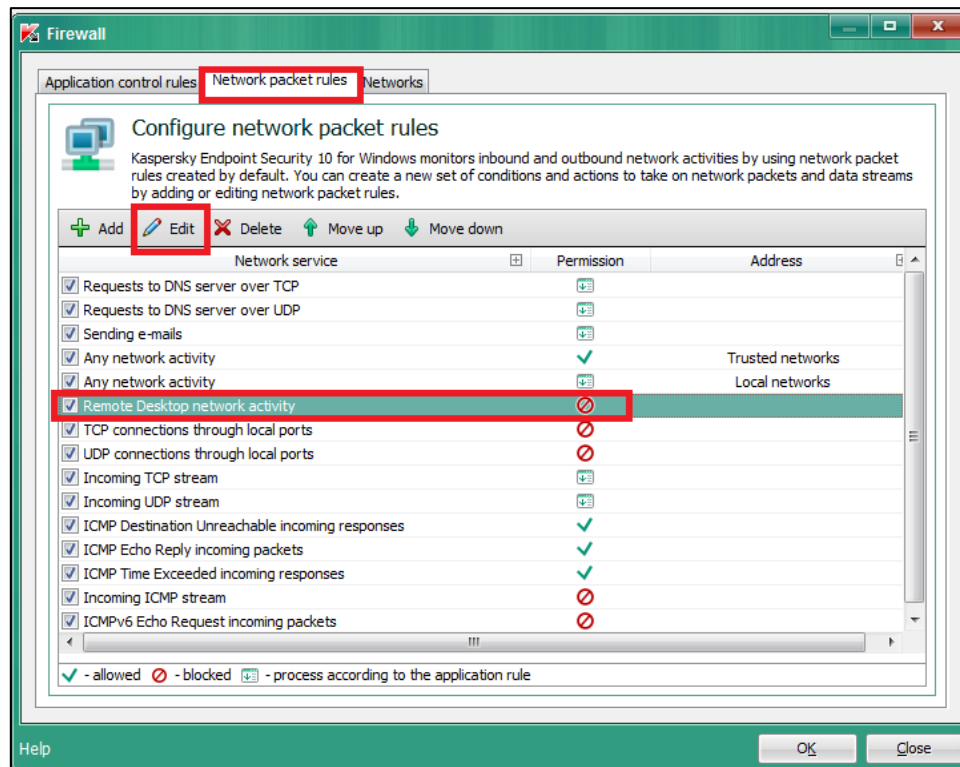


Figure 3: Firewall setting Window

Change the **Action** status from Block to Allow. (This setting to allow the RDP activity to AWS server). Then click OK. Refer Figure 4.

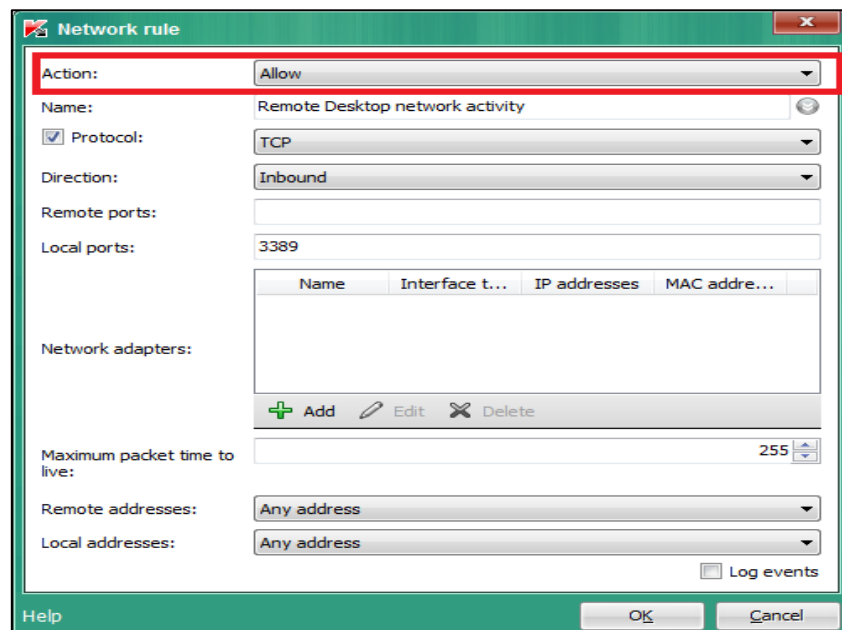


Figure 4: Network rule

Then install the KES and make sure all the status on **Managed computers > Computer** are green. Refer to the image below.

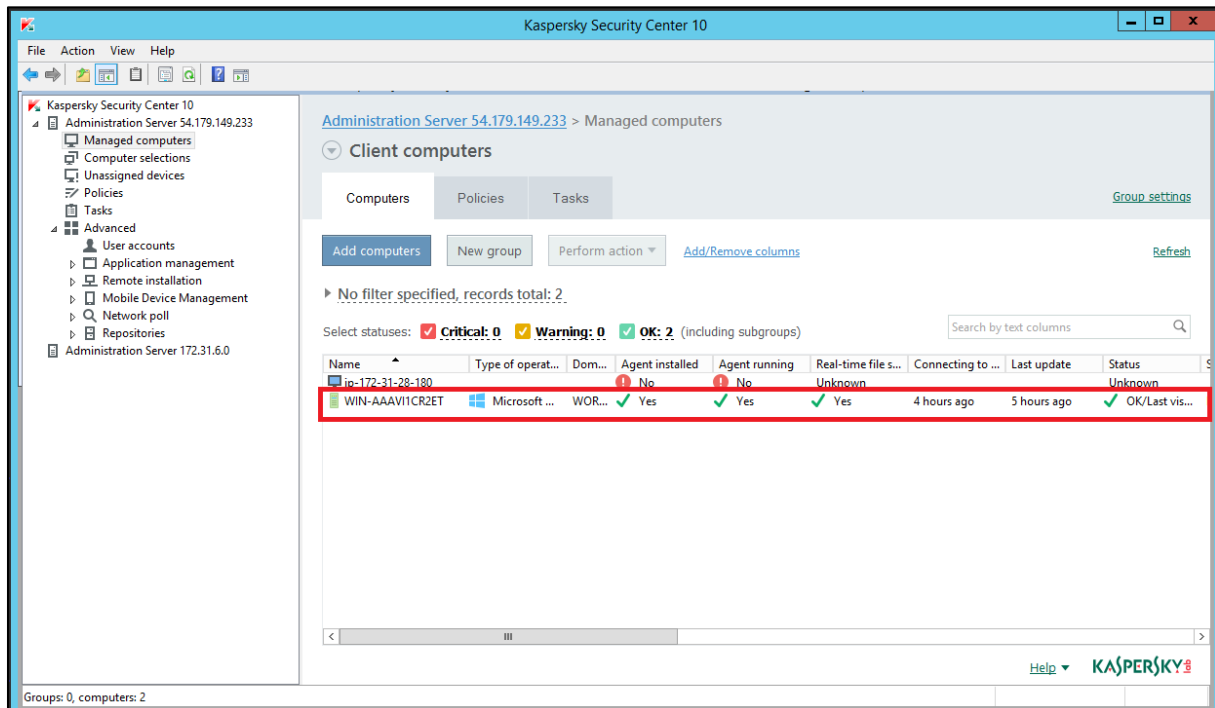


Figure 5: KSC 10 Console

For the Windows Server, there are only three (3) component of the KES 10 for Windows running to protect the server and no Endpoint Control running for server. KES 10 for Windows run full protection only for the Endpoint Workstation.

There are three (3) component that run on the server.

- File Anti-Virus Protection
- Firewall Protection (if the server running by RDP, must allow the RDP session on Firewall setting under Policies)
- Network Attack Blocker protection

Image below show the different of the KES 10 for Windows on Server and Endpoint Workstation.

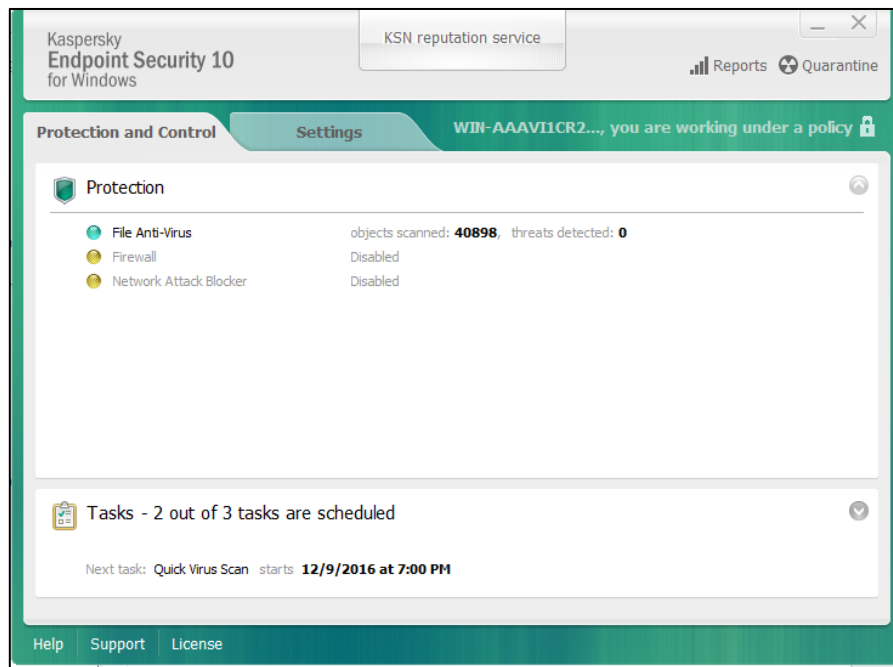


Figure 6: KES 10 for Windows on Server

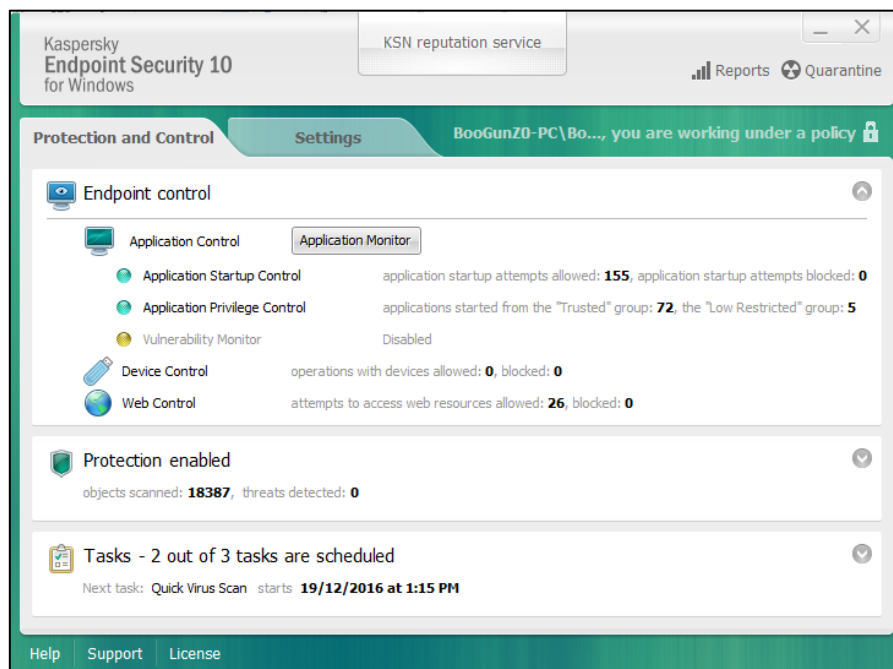


Figure 7: KES 10 for Windows on Endpoint Workstation (Endpoint Control)

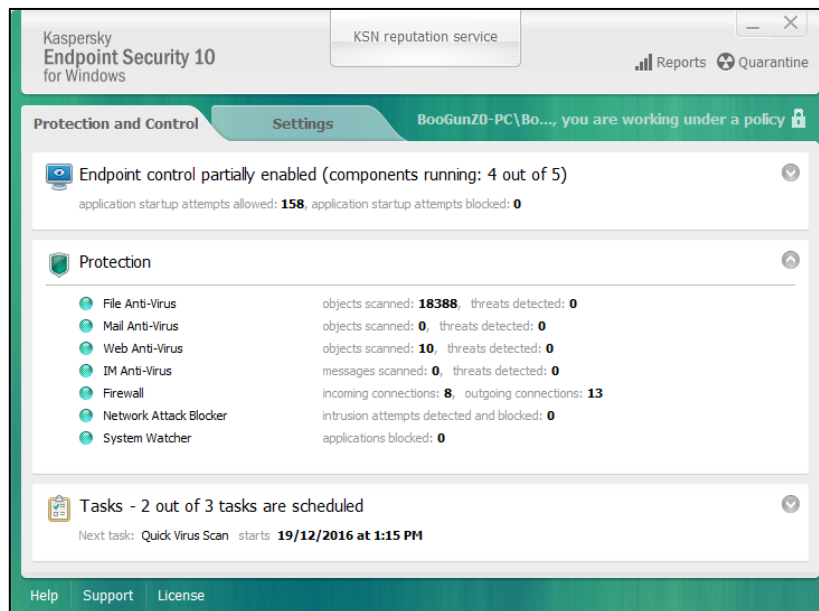


Figure 8: KES 10 for Windows on Endpoint Workstation (Protection)

Remote Installation of Network Agent and KES 10 (KES Server)

1. Network Polling

For the computers in same network or domain, it will detect on under the **Unassigned device**. For AWS server, we need to perform the Network poll to push the Network agent into the targeted device. To perform the Network poll as follow.

Advanced > Network poll > Add subnet

Select **Specify IP subnet using IP address range** by put the private IP address of the Server. For example, the KES Server private IP address are 172.31.25.31 and put the range of the IP address between 172.31.25.29 – 172.31.25.34 then click OK. Then click Poll now to poll the IP address. Refer to Figure 5. Wait until the process of the network polling finish. After finish, click the Private under IP subnet to find the IP address for the KES Server.

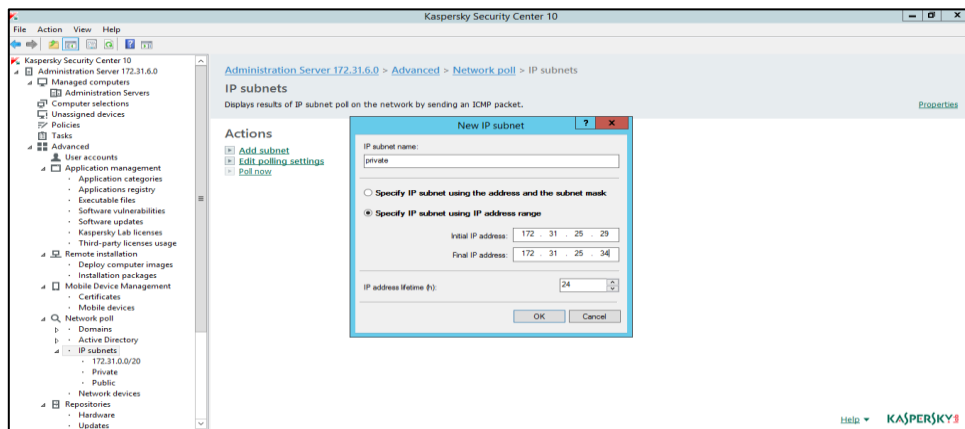


Figure 9: Setup the IP address range

Find the IP address, then move the IP address into Managed Computer by Right-click and select move.

Name	Description	Type	Subtype	Last vi
WIN-U1F2FNGCVDG		Computer		12/8/2
WIN-J3R1PQHEJH5		Computer		12/7/2
WIN-AAAVI1CR2ET		Computer		12/8/2
WIN-6J0C1KGN65D		Computer		12/8/2
ip-172-31-31-199		Computer		12/7/2
ip-172-31-28-36		Computer		12/8/2
ip-172-31-28-180		Computer		12/7/2
ip-172-31-25-31		Computer		12/8/2
ip-172-31-12-151		Computer		12/8/2
ip-172-31-0-1		Computer		12/8/2
ec2-52-221-253-77		Computer		12/8/2
ec2-52-221-253-69		Computer		12/8/2
ec2-52-221-253-68		Computer		12/8/2

Figure 10: List of the IP Address

2. Push installation of Network Agent and KES

After move the IP address into Managed computer, run push installation of Network Agents to the server. After finish, the name of the server will appear into the Managed computer with status of the Agent installed green and the IP still with red status. The KES Server have register by the name of server into Managed computer.

Click the server name and run the installation of the KES 10 for Windows. After installation, make sure all the status are green and protected.

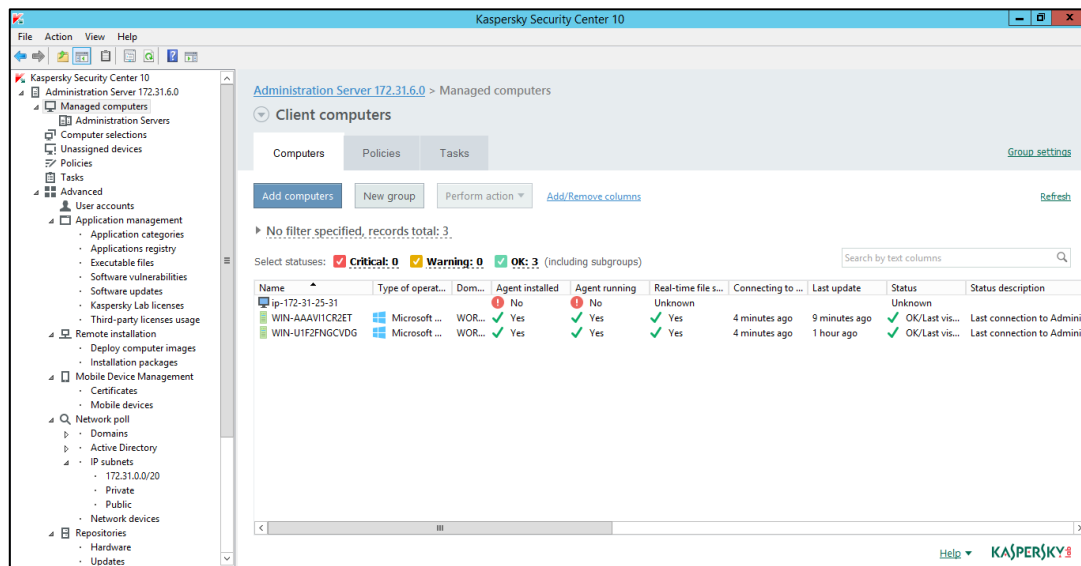


Figure 11: Status of the installation server

Kaspersky Security for Windows Server (ks4ws)

For windows server, we need to install the security protection to prevent the malicious attack to the server. For server, there are using the Anti-Cryptor technology to prevent the Ransomware attack to the server.

1. Download the ks4ws into the KES Server

Download the ks4ws installer from link → <http://support.kaspersky.com/ksws10#downloads>

2. Install the ks4ws into KES Server.

Before run the installation, we need to uninstall the KES 10 from the server. KES 10 and ks4ws can't in same workstation.

Double click the .exe file to run the installation.

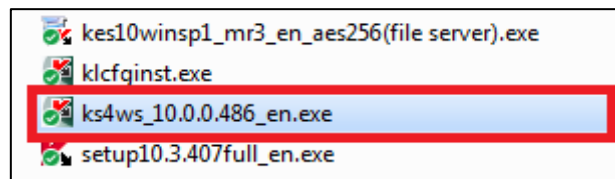


Figure 12: ks4ws.exe Installer

Click **Next** Button twice to unpack the installation. Wait until the installation window appear. Refer Figure 13.



Figure 13: KS4WS installation console

On KES Server, we need to install the **Kaspersky Security** and **Kaspersky Security Console**.

First click on **Install Kaspersky Security**. Click **Next** on welcome wizard.

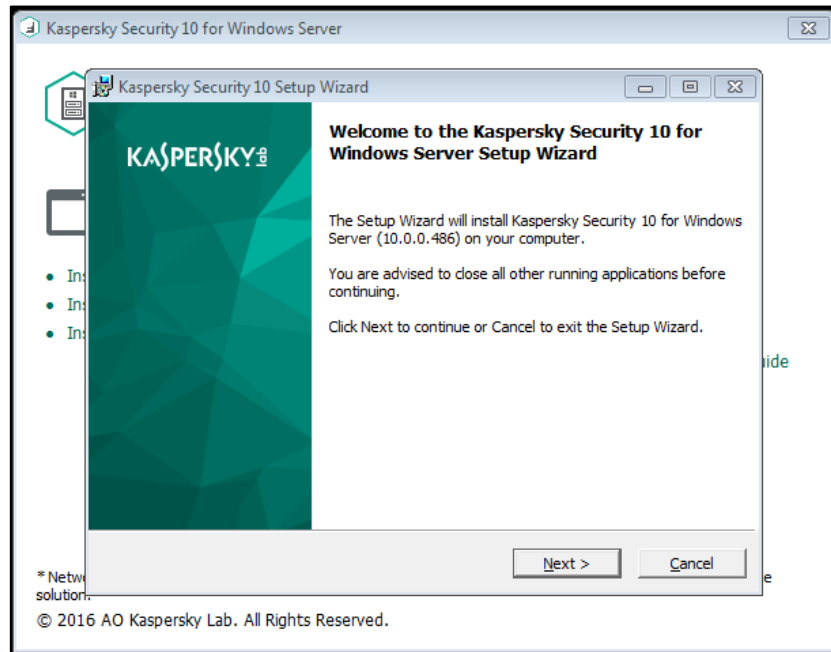


Figure 14: Welcome page setup wizard

Accept the term and click **Next**.

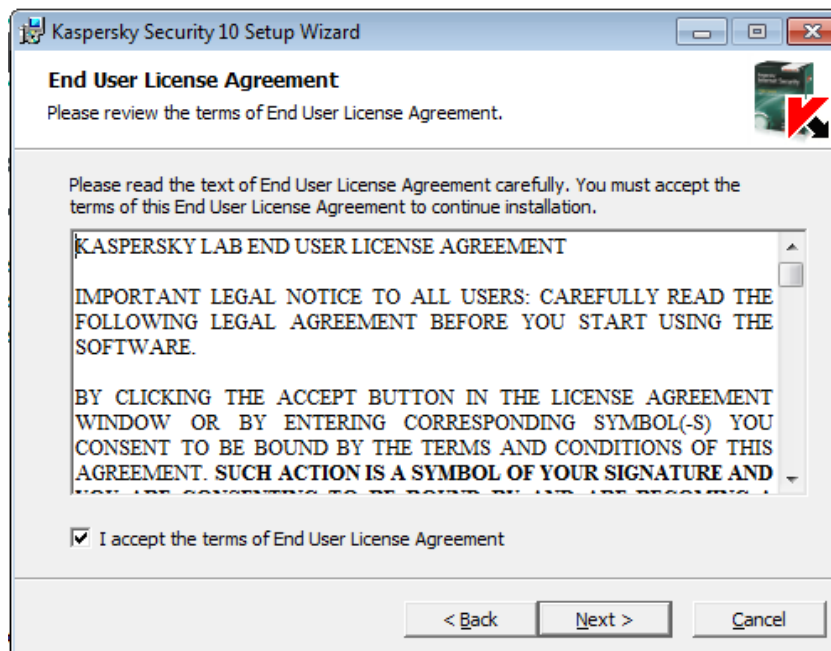


Figure 15: End User License Agreement

Tick **Scan computer for viruses** and click **Next**. After finish virus scan, click **Next** button.

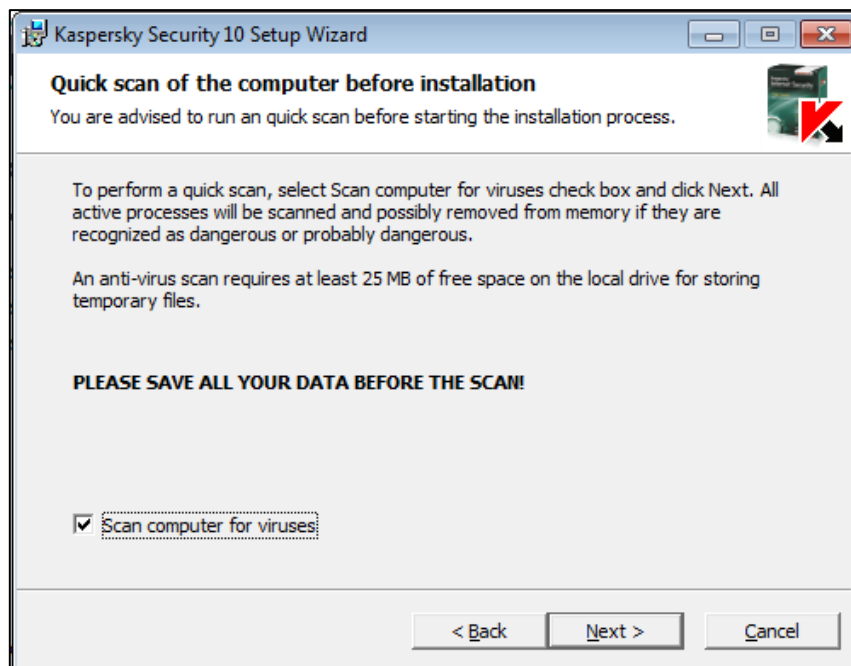


Figure 16: Quick Scan page

Click **Next** button until the Activation of the application. Enter the activation key license. Then click **Next**.

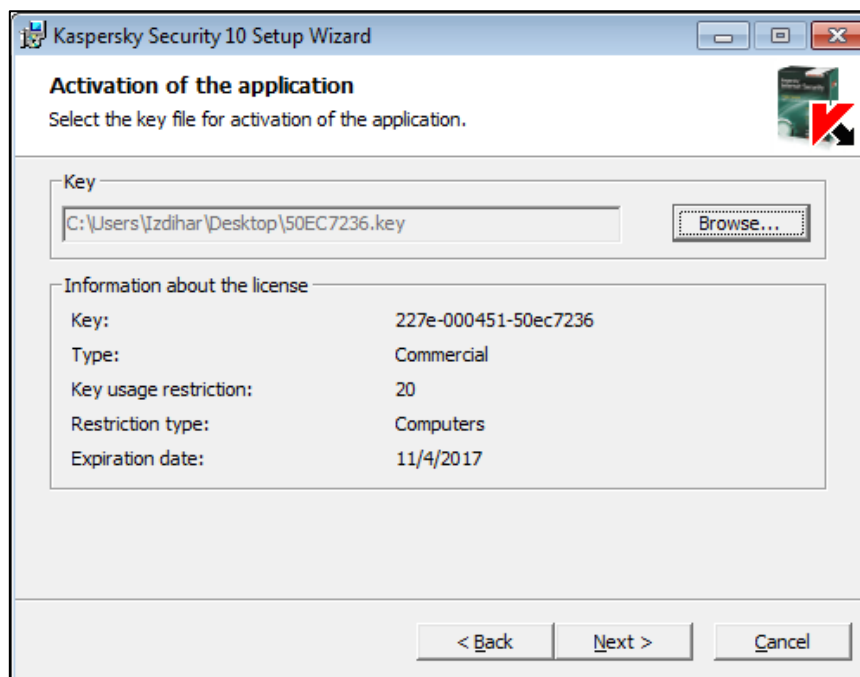


Figure 17: Activation of the application

Click **Install** button to install the Kaspersky Security.

Second, install Kaspersky Security Console. Click the installation



Figure 18: KS4WS installation console

On welcome windows click **Next**.

Accept the terms of end user license then click **Next**.

Click Next button for following page. On advanced installation settings, tick allow remote access. Then click **Next**.

On installation page, click **Install**. Wait until finish the installation. Figure 19 show the Kaspersky security console.

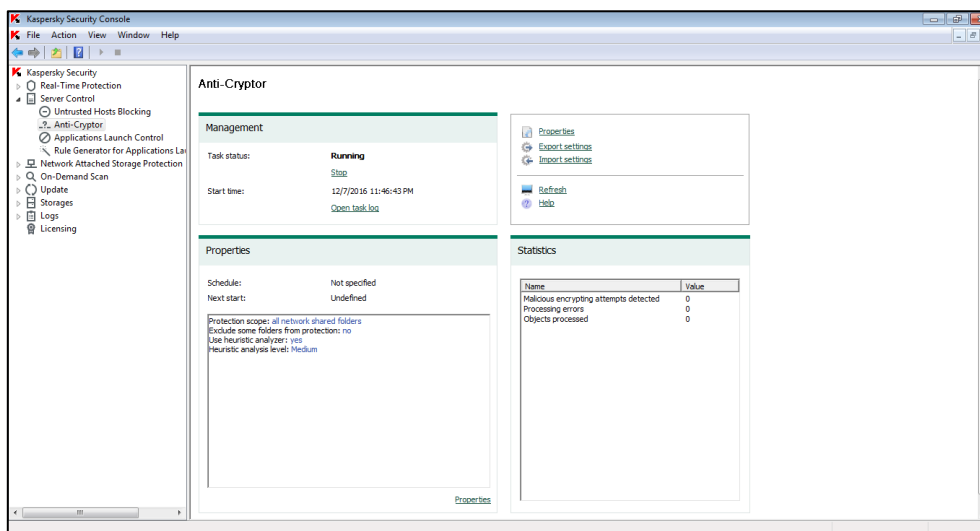


Figure 19: Kaspersky Security Console

3. Install Kaspersky Security Plug-in into KSC Server

The Plug-in ensures the application integration with Kaspersky Security Center for centralized application management on a group of protected servers.

Click Install Kaspersky Security Plug-in to install plug-in into KSC Server.



Figure 20: KS4WS installation console

Click Next to start install the plug-in. After done install, click OK to finish the installation.

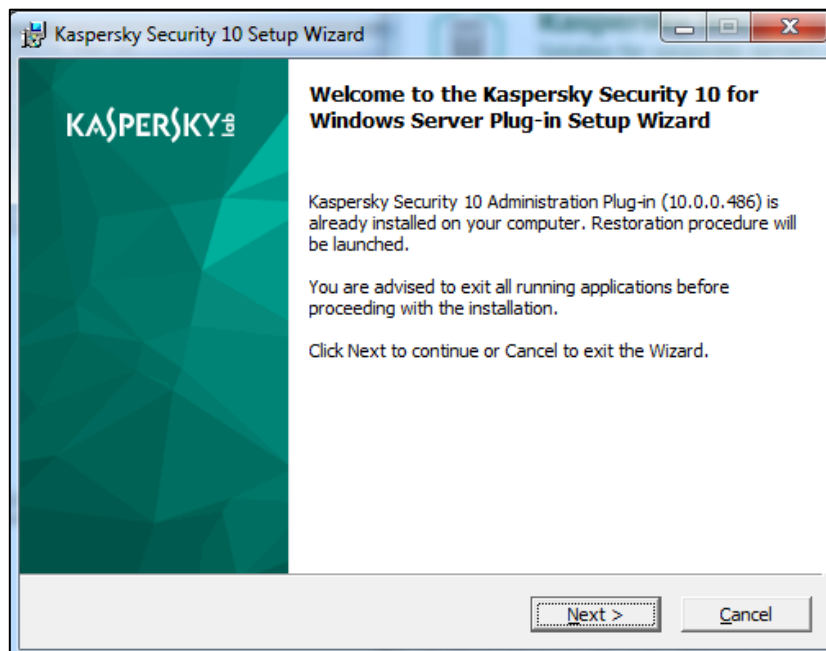


Figure 21: Plug-in setup Wizard

4. Create Windows Server Policies

Click **Create a policy** to add Windows Server policy.

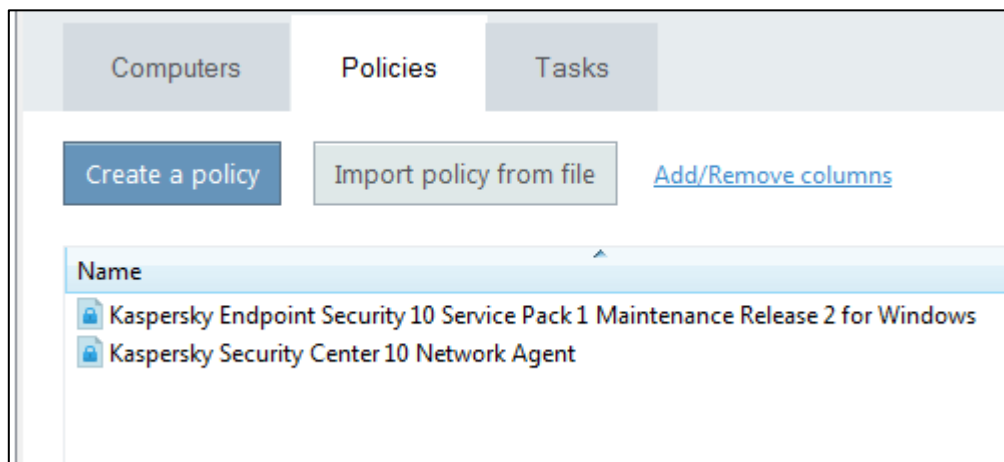


Figure 22: Policies tab

Enter the Policy Name. Then click Next button.

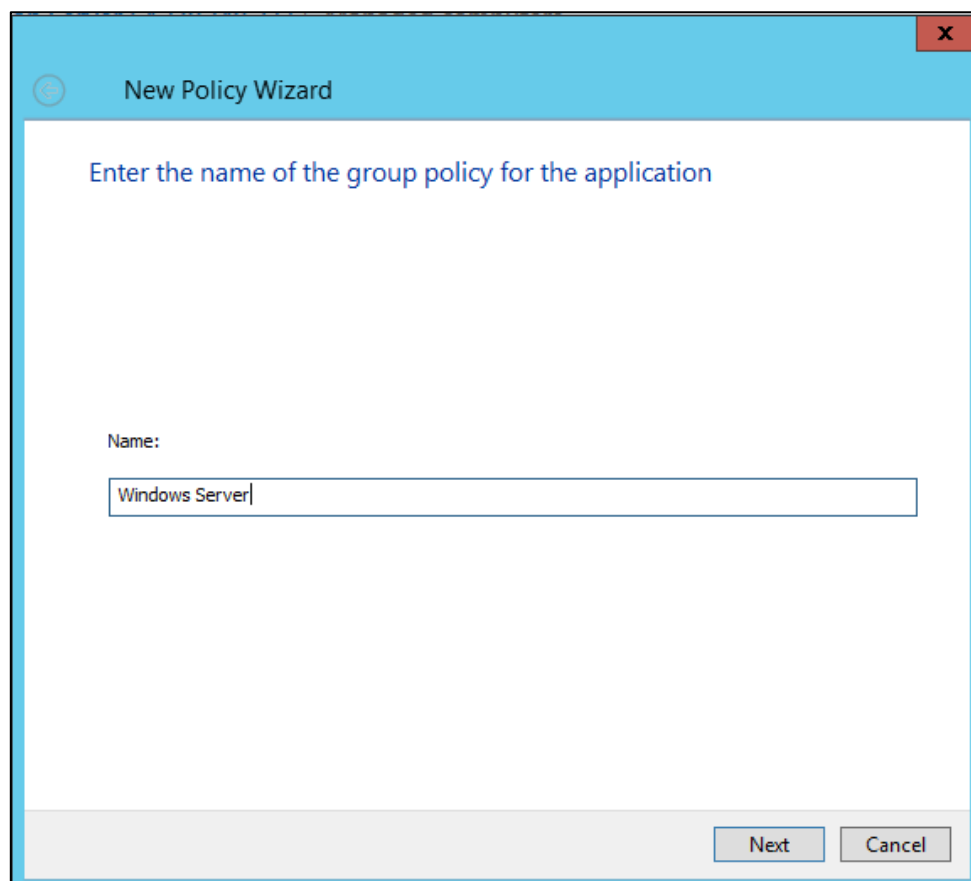


Figure 23: New Policy wizard

Select the application that want to create group policy, then click Next.

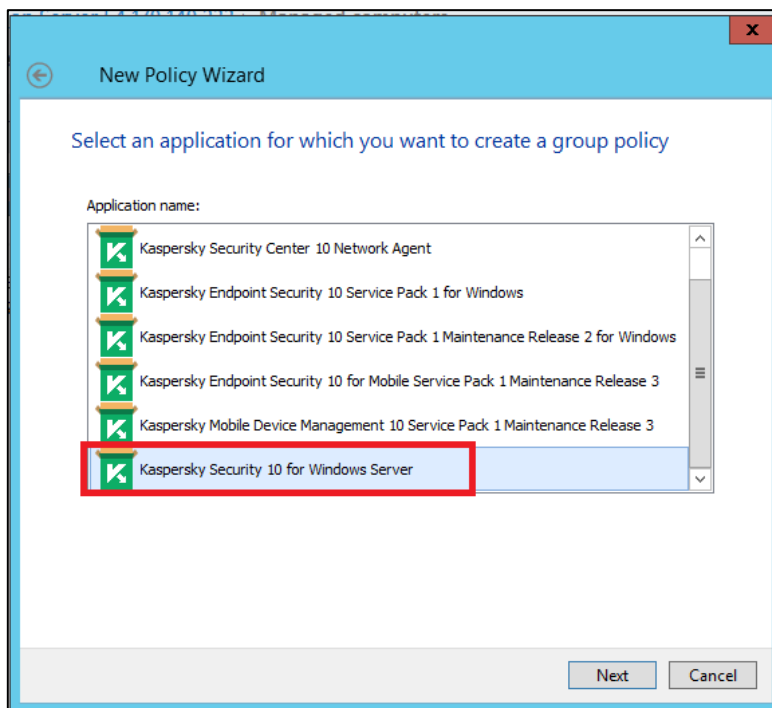


Figure 24: Application to create a group Policy

On the following page, select New for policy creation method, then click Next.

On Real-Time Protection page, the setting for the Real-Time File Protection, Script Monitoring and KSN Usage. We can do a setting to this policy to apply.

On following page, select the Active policy then click Finish.

Wait the policy apply to the server on KES Server. Using this policy, we can control by remote to apply the protection on Console.

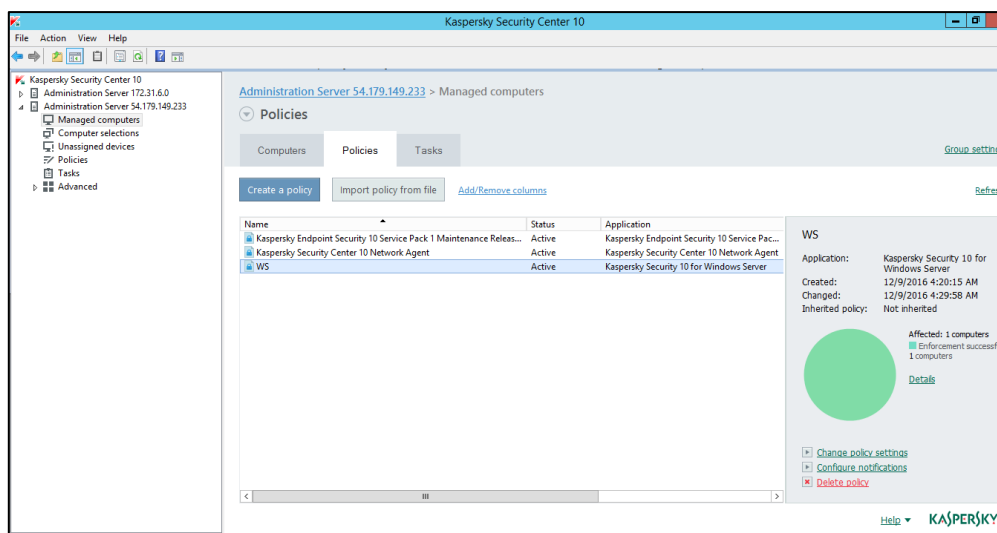


Figure 25: Window Server policy created

Backup and Restore the KSC

Do a backup on the KSC Server and KSC Server will terminate. Create new KSC Server then install the KSC into the new server. Then restore back the backup into new server.

1. Apply Backup on KSC Server

C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center

Double click klbackup.exe. On welcome page, click **Next**.

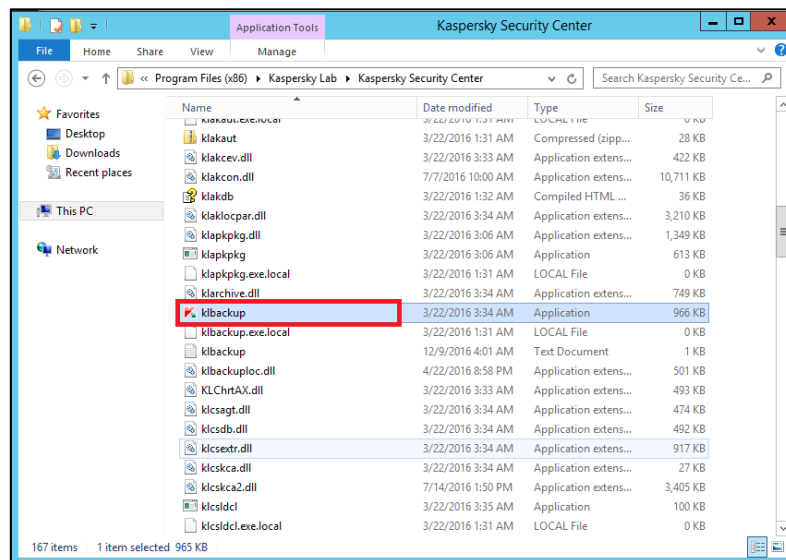


Figure 26: klbackup.exe directory

Choose **Perform backup of Administrator Server data**, then click **Next**.

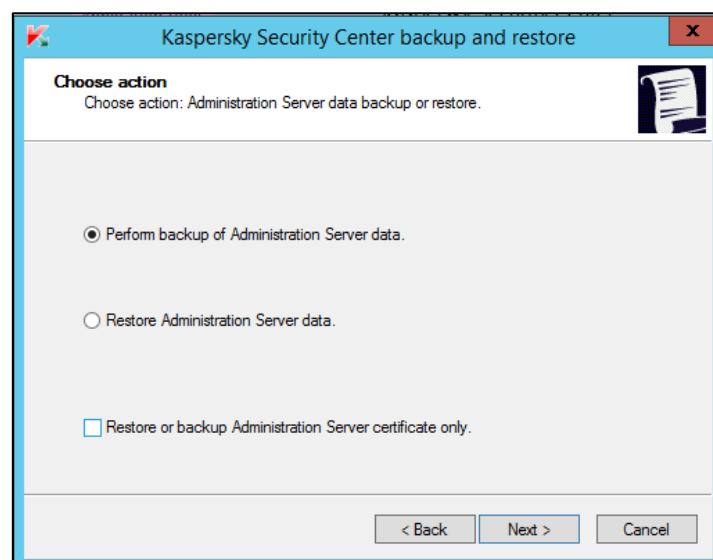


Figure 27: Choose action

On backup settings, select the destination folder and put the password. Then click **Next**. The backup of Administrator server done, click **Finish**. Copy the backup folder into the new KSC Server.

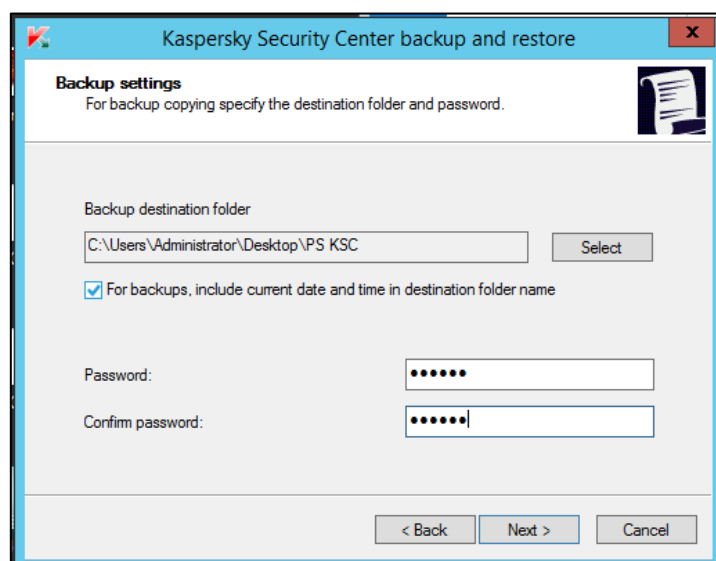


Figure 28: Backup destination folder & password

2. Apply Restore on new KSC Server

Double click klbackup.exe. On welcome page, click **Next**.

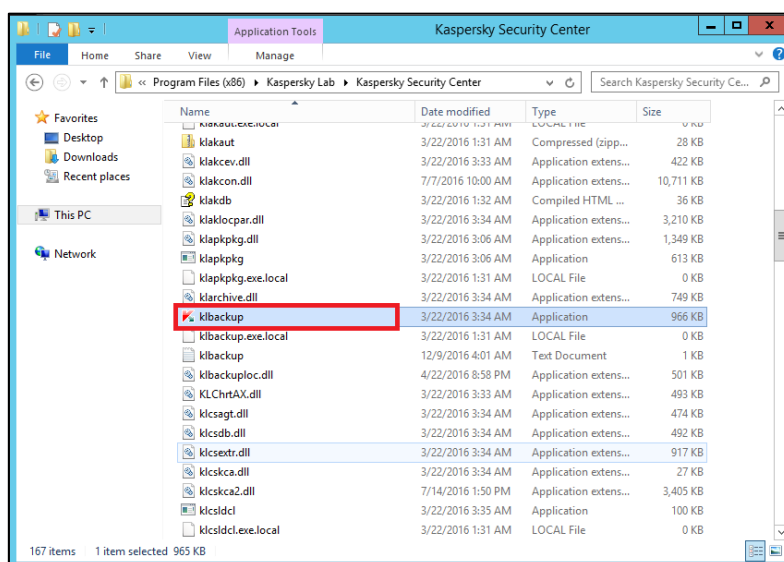


Figure 29: klbackup.exe directory

Choose **Restore Administrator Server data**, then click **Next**.

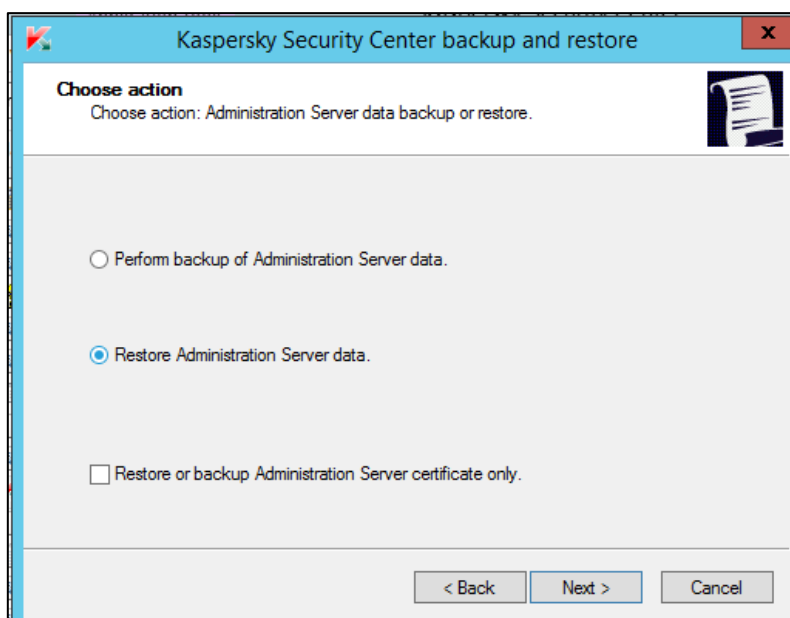


Figure 30: Choose action

On Restore setting page, select the backup folder directory and put the password that we create when perform the backup. Then click **Next** button. Wait until the restore finish.

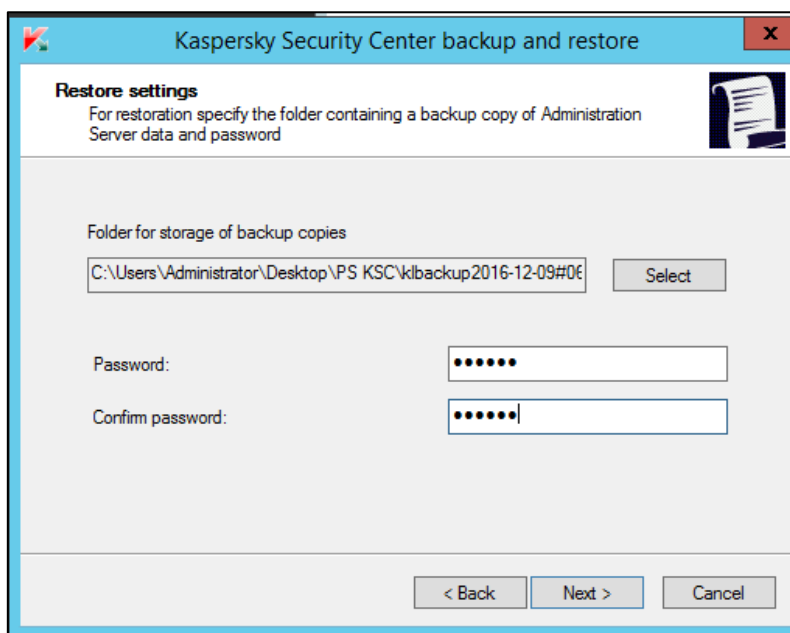


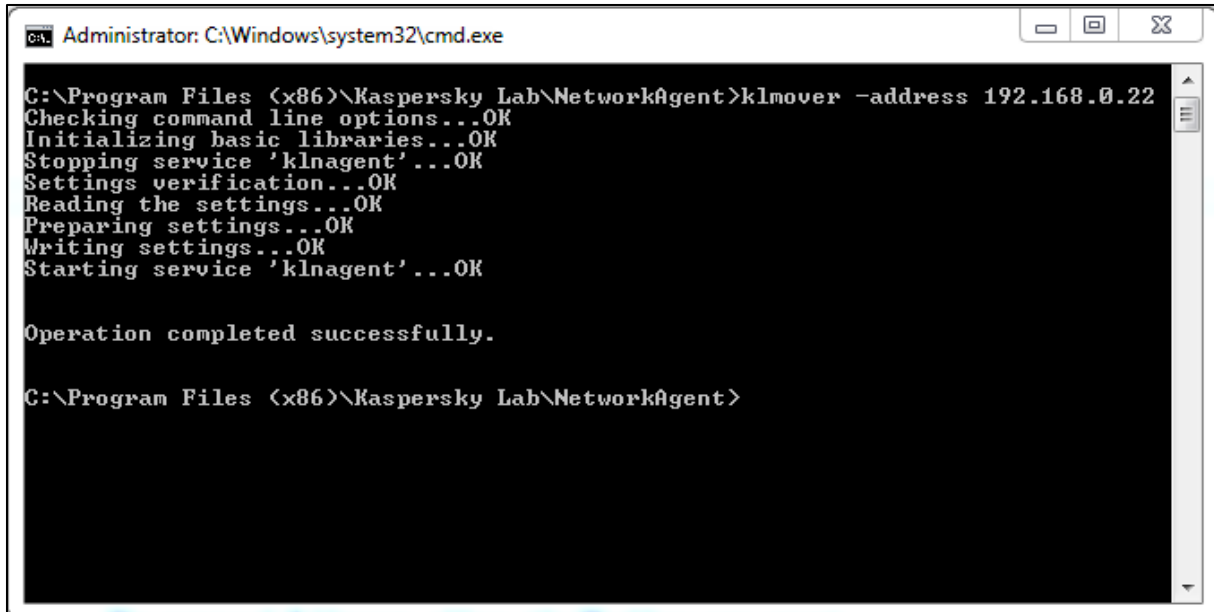
Figure 31: Folder for storage of backup copies

After done restore, we need to assign the new IP address of the new KSC Server to make the Network Agent communicate with the server.

3. Klmover - a utility for changing Network Agent settings

Klmover.exe utility is designed for changing Administration server parameters in Network agent settings on a client PC. The utility is located on a client PC in the Network agent installation folder - C:\Program Files\Kaspersky Lab\NetworkAgent.

The command → klmover -address <the IP address new server>



```
Administrator: C:\Windows\system32\cmd.exe
C:\Program Files (x86)\Kaspersky Lab\NetworkAgent>klmover -address 192.168.0.22
Checking command line options...OK
Initializing basic libraries...OK
Stopping service 'klnagent'...OK
Settings verification...OK
Reading the settings...OK
Preparing settings...OK
Writing settings...OK
Starting service 'klnagent'...OK

Operation completed successfully.

C:\Program Files (x86)\Kaspersky Lab\NetworkAgent>
```

Figure 32: CMD

Now the Network Agent on KES Server are connected with KSC on KSC Server. This command need run on each client PCs that will connect to the server. If the Network Agent fail to communicate with server, it will not get the update and the protection from the server.