Actiphy

ActiveImage™ PROTECTOR 2018 Update

Server / Desktop Edition (Update 5)/for Hyper-V Startup Guide

6th Edition Feb., 2020

Table of Contents

1. Overview

ActiveImage Protector is a backup and recovery solution designed with the latest sector-based disk imaging technology to flexibly support Windows machines in a variety of system environments ranging from legacy machines to the latest virtual machines.

ActiveImage Protector provides features essential for a backup solution such as Hot Imaging feature allowing you to back up a running system, Cold Imaging feature enabling you to create a backup image of a clean Windows system before starting it up, fast Incremental Backup that includes only the sectors that have changed since the last full or incremental backup image was written, Command Line Interface allowing backups to be administered by third-party system management tools.

System Requirements

The following are the system requirements for ActiveImage Protector Server Edition / Desktop Edition and for Hyper-V Enterprise.

Before you start using ActiveImage Protector 2018 Update Server Edition / Desktop Edition, please ensure that the following system requirements are met.

CPU	Pentium 4 or above CPU
Main Memory	1024MB or more is required.
Hard Disk	1.5GB or more of available disk space is required.
DVD-ROM Drive	Necessary to install the product, boot or start up ActiveImage Protector boot environment
Supported Operating System (Server Edition Update)	**Windows:** Windows Server 2019, Windows Server 2016, Windows Server 2012 and 2012 R2, Windows Server 2008 (x86/x64) and 2008 R2, Windows Storage Server 2016, Windows Storage Server 2012 and 2012 R2, Windows Storage Server 2008 and 2008 R2 (x86/x64) **Hypervisor:** Windows Server 2016 Hyper-V (Hot ＆ Cold

	Imaging), Windows Server 2012 and 2012 R2 Hyper-V (Hot & Cold Imaging), Windows Server 2008 R2 Hyper-V (Hot & Cold Imaging)
Supported Operating System (for Hyper-V Enterprise)	Windows Server 2008 R2 or later server OS (including Hyper-V Server) on which Hyper-V is configured. *As for Windows Server 2008 R2, please make sure that Microsoft .Net Framework 4.5 or later is already configured.

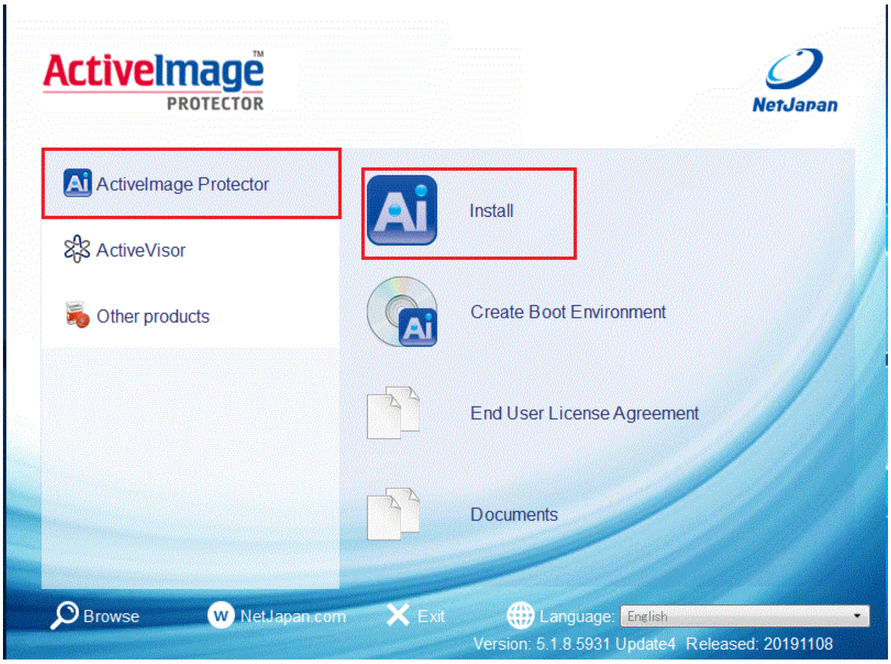
*As to the limitations for using the product, please refer to the release note included in ActiveImage Protector's media.

*This document includes the screen shots captured in Server Edition, the operating procedures are the same for Desktop Edition.

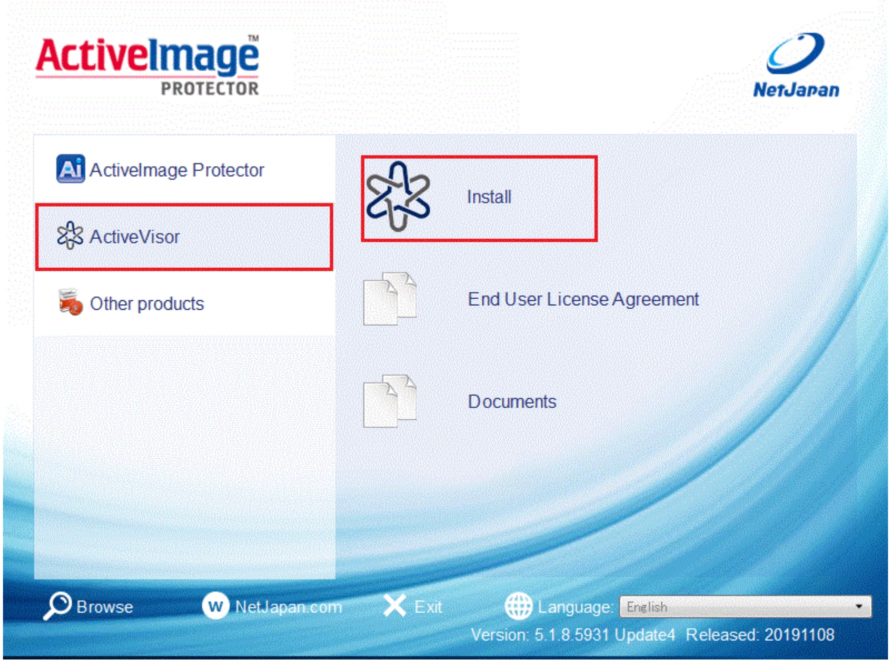
2. Installation

The following are the operating procedures required to install ActiveImage Protector on the machine specified as backup source.

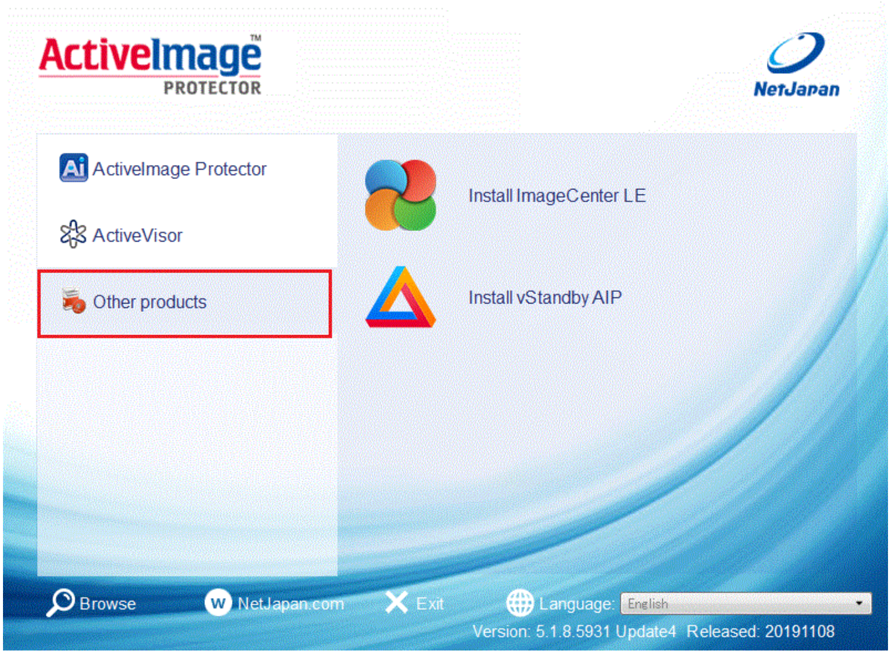
1. Set the product media to the machine to start the installation launcher. Click on **[Install]**. If the launcher does not start, please execute Launch.exe in the product media.



Note) Server/Desktop Edition:
When you click on [ActiveVisor], you can install "ActiveVisor" . When you click on [Other products], you can install "ImageCenter LE" or "vStandby AIP".

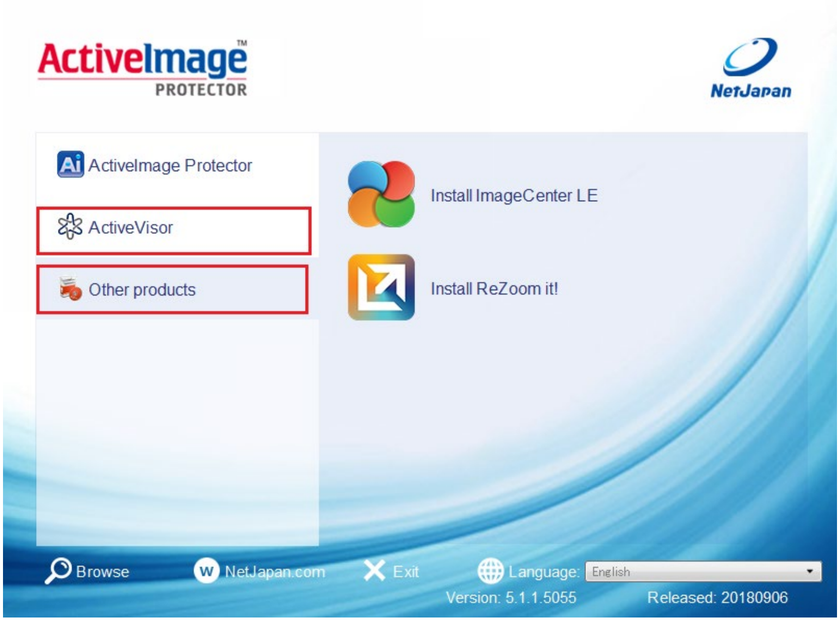


ActiveImage PROTECTOR
NetJapan
ActiveImage Protector
ActiveVisor
Other products
Install
End User License Agreement
Documents
Browse
NetJapan.com
Exit
Language: English
Version: 5.1.8.5931 Update4 Released: 20191108



ActiveImage PROTECTOR
NetJapan
ActiveImage Protector
ActiveVisor
Other products
Install ImageCenter LE
Install vStandby AIP
Browse
NetJapan.com
Exit
Language: English
Version: 5.1.8.5931 Update4 Released: 20191108

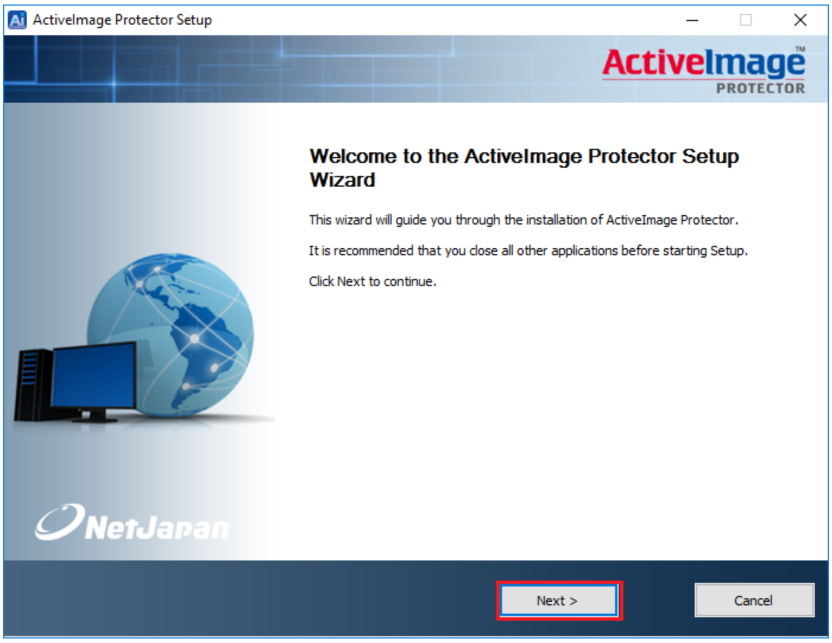
Note) for Hyper-V Enterprise:
When you click on [ActiveVisor], you can install “ActiveVisor” . When you click on [Other products], you can install “ImageCenter LE” or “ReZoom it!”.



Version: 5.1.1.5055

Released: 20180906

2. Click **[Next]**.



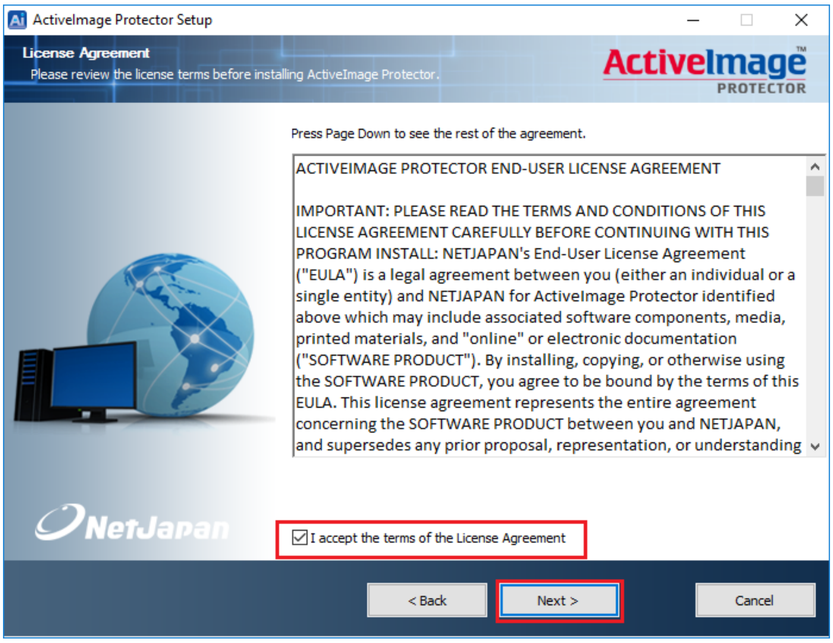
Welcome to the ActiveImage Protector Setup Wizard

This wizard will guide you through the installation of ActiveImage Protector.

It is recommended that you close all other applications before starting Setup.

Click Next to continue.

3. Please review the End User's License Agreement.
   Check the box next to **[I accept the terms of the License Agreement]** to continue the installation. Click **[Next]**.



License Agreement

Please review the license terms before installing ActiveImage Protector.

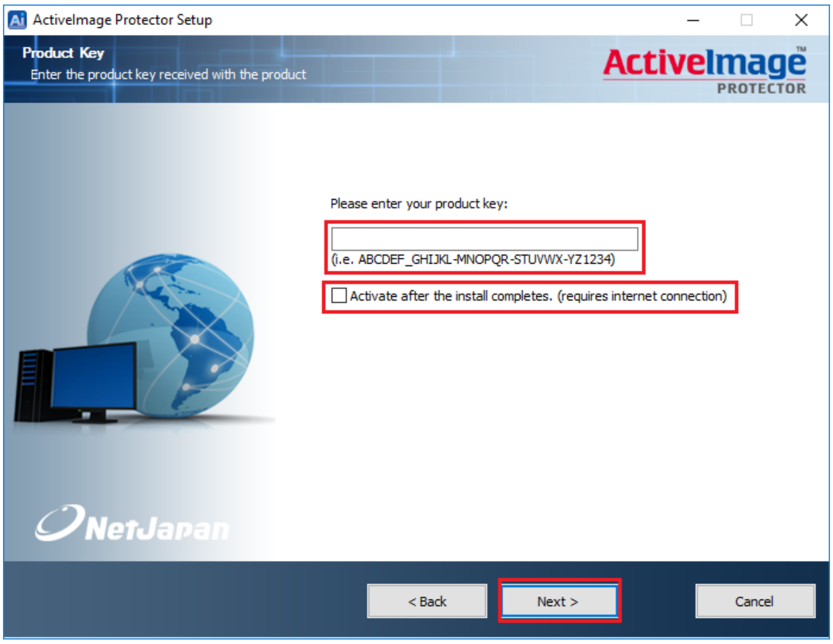
Press Page Down to see the rest of the agreement.

ACTIVEIMAGE PROTECTOR END-USER LICENSE AGREEMENT

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CONTINUING WITH THIS PROGRAM INSTALL: NETJAPAN's End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and NETJAPAN for ActiveImage Protector identified above which may include associated software components, media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. This license agreement represents the entire agreement concerning the SOFTWARE PRODUCT between you and NETJAPAN, and supersedes any prior proposal, representation, or understanding

☑ I accept the terms of the License Agreement

4. Enter the product key. **[Activate after the install completes]** option may be selected to automatically activate the product upon completion of the installation process. Click **[Next]**.



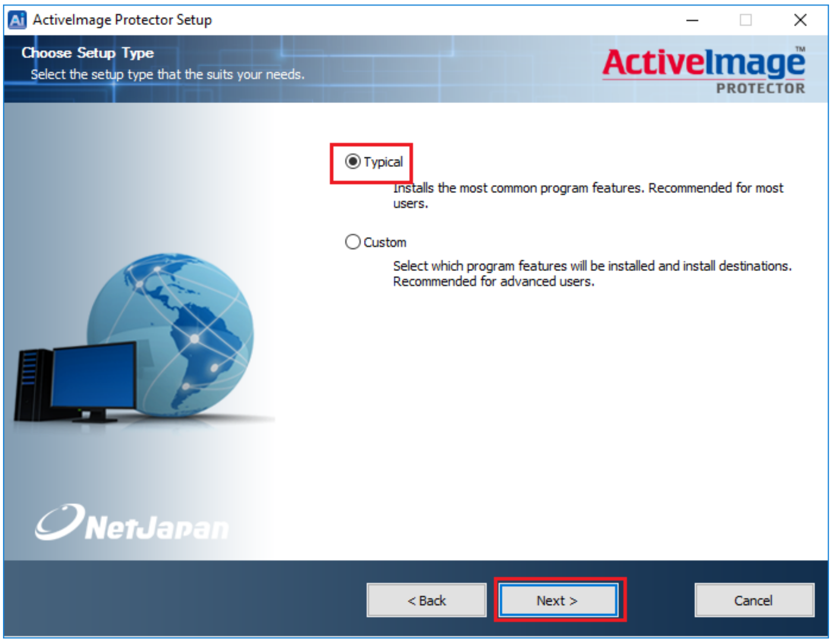
ActiveImage Protector Setup
Product Key
Enter the product key received with the product
ActiveImage PROTECTOR
NetJapan
< Back
Next >
Cancel

Please enter your product key:

(i.e. ABCDEF_GHIJKL-MNOPQR-STUVWX-YZ1234)

□ Activate after the install completes. (requires internet connection)

5. Select **[Typical]** for the setup type and click **[Next]**.



ActiveImage Protector Setup

Choose Setup Type

Select the setup type that the suits your needs.

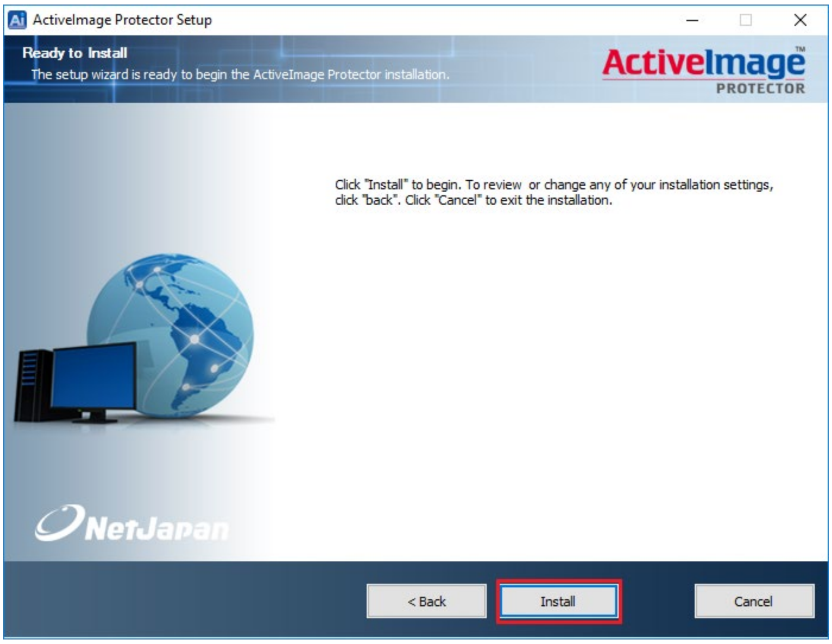
● Typical

Installs the most common program features. Recommended for most users.

○ Custom

Select which program features will be installed and install destinations. Recommended for advanced users.

6. Review the installation settings and click **[Install]** to complete the installation.



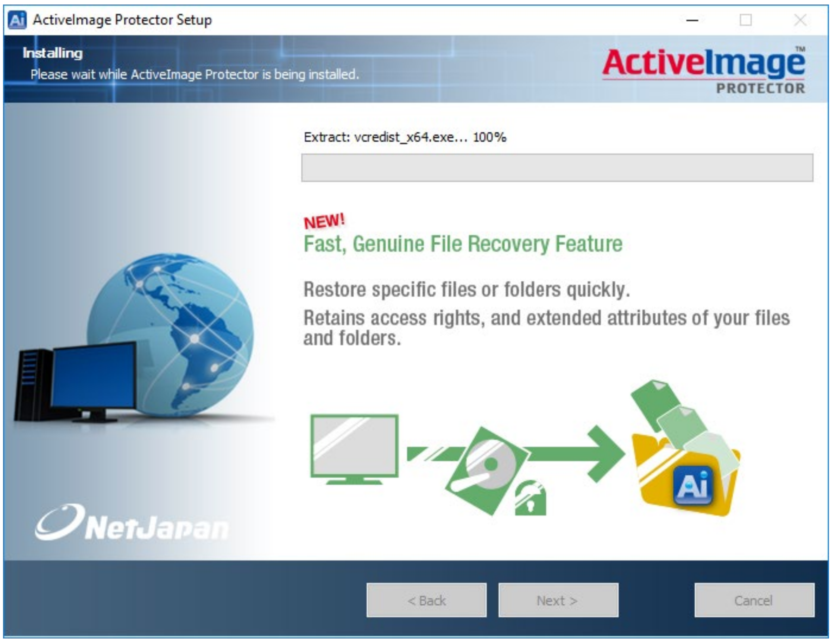
ActiveImage Protector Setup

Ready to Install

The setup wizard is ready to begin the ActiveImage Protector installation.

Click "Install" to begin. To review or change any of your installation settings, click "back". Click "Cancel" to exit the installation.

7. Please wait until installation of ActiveImage Protector completes.



ActiveImage Protector Setup

Installing

Please wait while ActiveImage Protector is being installed.

Extract: vcredist_x64.exe... 100%

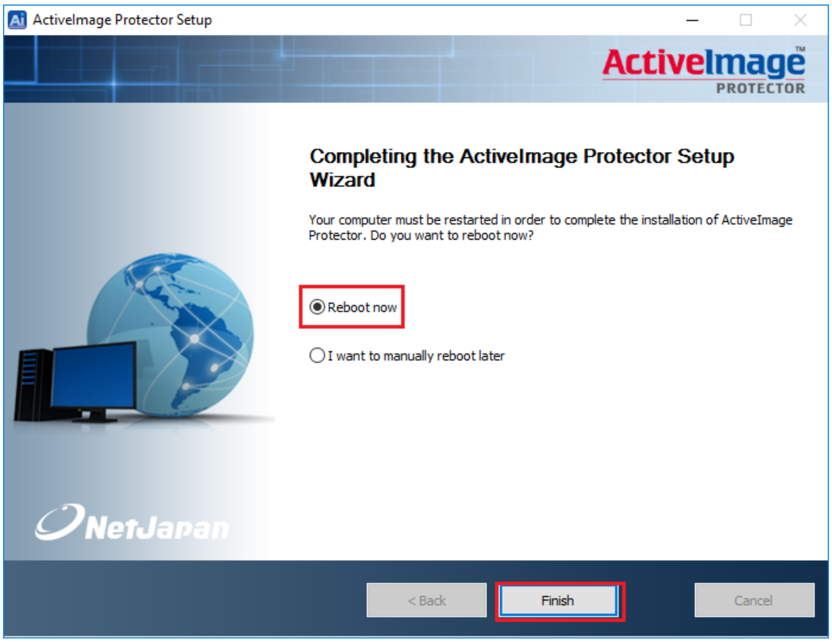
NEW!

Fast, Genuine File Recovery Feature

Restore specific files or folders quickly.

Retains access rights, and extended attributes of your files and folders.

8. Upon completion of the product installation, eject the product media and select **[Reboot now]** to reboot the machine immediately and **[Finish]**.
The machine is automatically rebooted.



ActiveImage Protector Setup

Completing the ActiveImage Protector Setup Wizard

Your computer must be restarted in order to complete the installation of ActiveImage Protector. Do you want to reboot now?

● Reboot now

○ I want to manually reboot later

3. Product Activation

Manual activation of the installed ActiveImage Protector terminates the live trial period. If the **[Activate after the install completes...]** was checked to automatically activate the product upon completion of installation, the following procedures are not required.

Two types of activation practices are supported; one is traditional online activation over the internet and the other is offline activation on standalone machine with no internet connection due to security reason.

Offline activation:
●No auto-update over network
●No E-Mail communication updating you with the latest information about ActiveImage Protector is provided from Actiphy.

The following are the operating procedures for online activation.

1. Start ActiveImage Protector

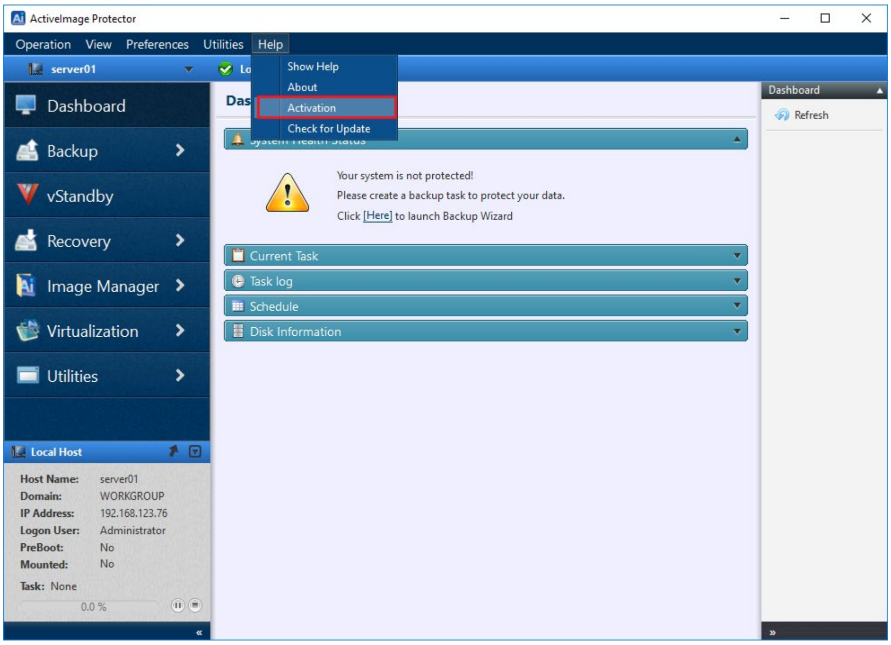
   Windows Server 2008 R2 or earlier server OS:
   Click **[Start]** – **[All Programs]** – **[NetJapan]** – **[ActiveImage Protector]**.

   Windows 7 or earlier Desktop OS:
   Click **[Start]** – **[All Programs]** – **[NetJapan]** – **[ActiveImage Protector]**.

   Windows Server 2012 or later server OS:
   Click **[Start]** – **[Applications]** – **[NetJapan]** – **[ActiveImage Protector]**.

   Windows Server 8 or later Desktop OS :
   Click **[Start]** – **[Applications]** – **[NetJapan]** – **[ActiveImage Protector]**.

2. Click **[Help]** and select **[Activation]** from the drop down menu.

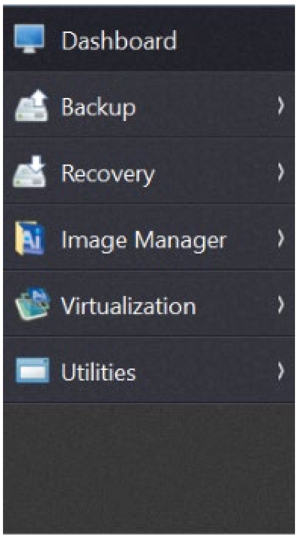


Your system is not protected!
Please create a backup task to protect your data.
Click [Here] to launch Backup Wizard

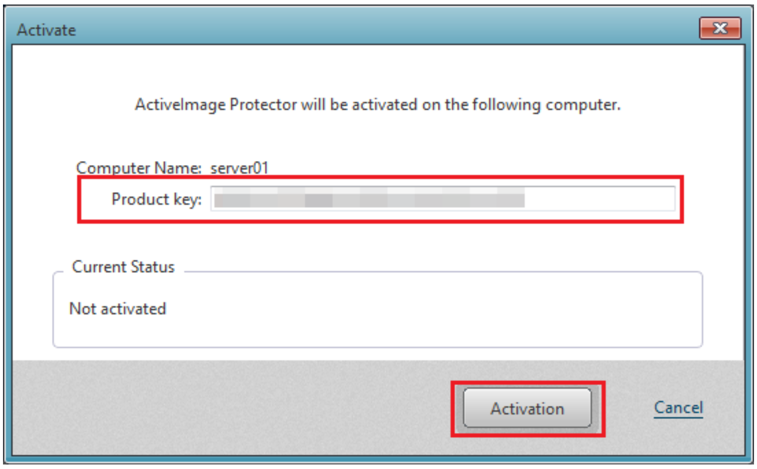
Host Name:	server01
Domain:	WORKGROUP
IP Address:	192.168.123.76
Logon User:	Administrator
PreBoot:	No
Mounted:	No

Task: None

Note) The left pane of ActiveImage Protector for Hyper-V Enterprise screen is different from the one of Server Edition.



3. Enter the product key and click **[Activation]**.



Activate

ActiveImage Protector will be activated on the following computer.

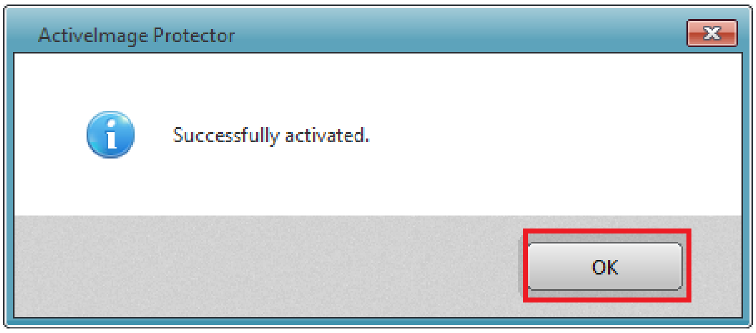
Computer Name: server01

Product key: [redacted]

Current Status

Not activated

4. When you get the following message, activation process completes. Click **[OK]**.



ActiveImage Protector

Successfully activated.

4. Backup

4-1. Backup Now

The following are the operating procedures for Backup Now.

1. Start ActiveImage Protector

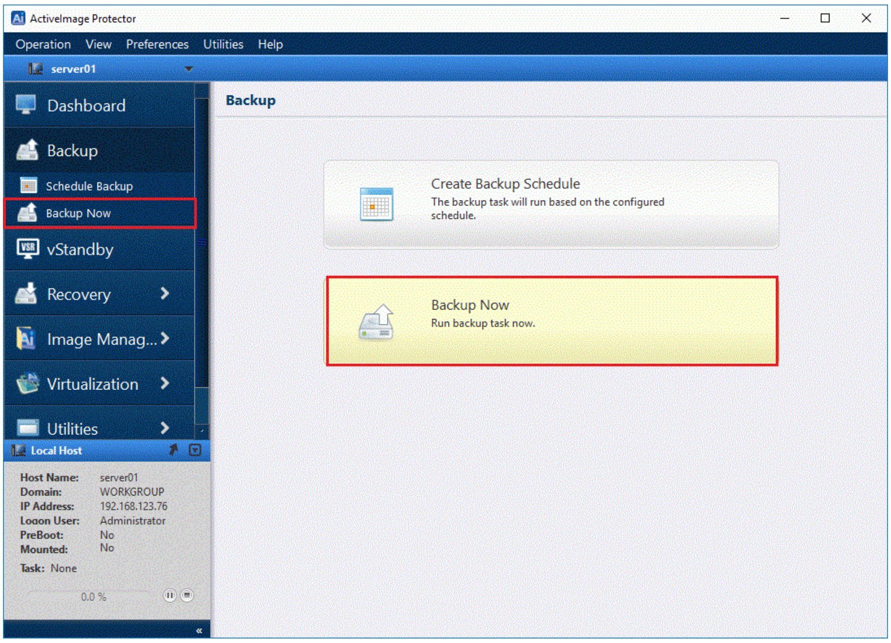
   Windows Server 2008 R2 or earlier server OS:
   Click **[Start]** – **[All Programs]** – **[NetJapan]** – **[ActiveImage Protector]**.

   Windows 7 or earlier Desktop OS:
   Click [Start] – [All Programs] – [NetJapan] – [ActiveImage Protector].

   Windows Server 2012 or later server OS: Click **[Start]** – **[Applications]** – **[NetJapan]** – **[ActiveImage Protector]**.

   Windows Server 8 or later Desktop OS :
   Click **[Start]** – **[Applications]** – **[NetJapan]** – **[ActiveImage Protector]**.

2. Click [Backup] – [Backup Now].

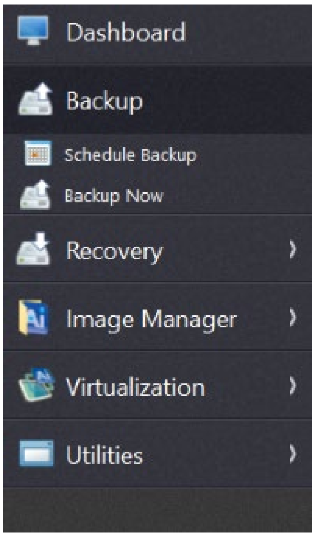


Create Backup Schedule
The backup task will run based on the configured schedule.

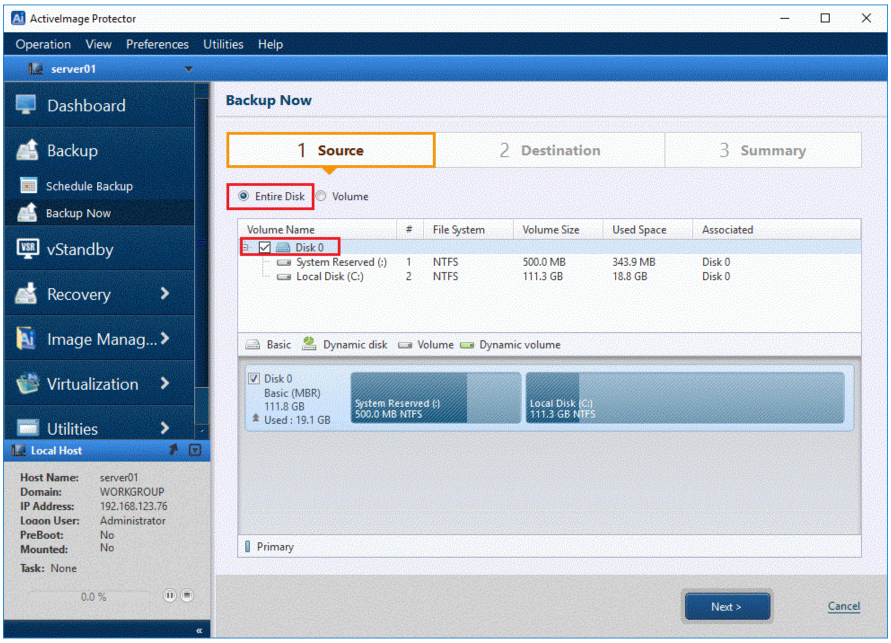
Backup Now
Run backup task now.

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

Note) The left pane of ActiveImage Protector for Hyper-V Enterprise screen is different from the one of Server Edition.



3. Select backup source.
   The following example shows that the entire disk is selected for the backup source.
   Click [Entire Disk] and check the checkbox for [Disk 0].
   When the backup source is selected, click [Next].



● Entire Disk ○ Volume

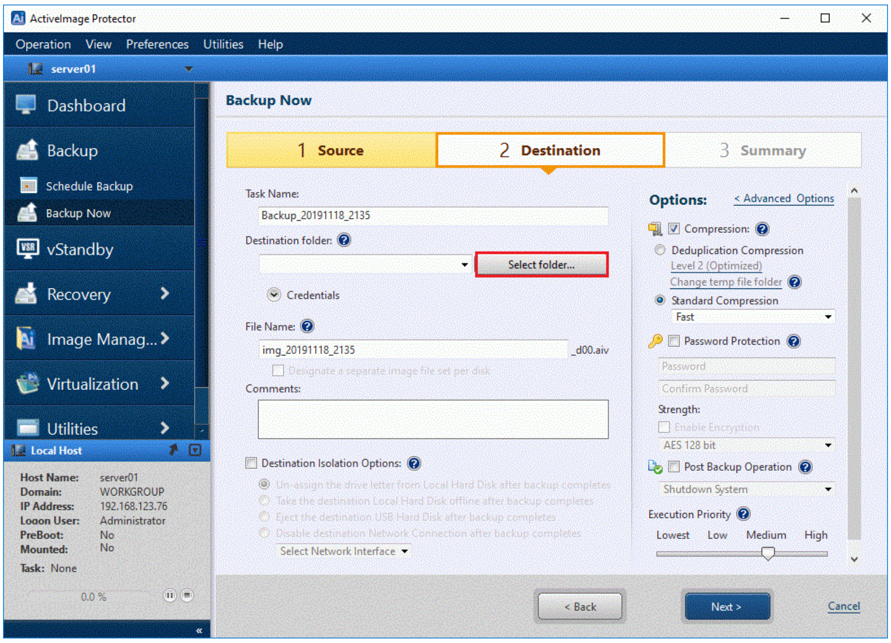
Volume Name	#	File System	Volume Size	Used Space	Associated
☑ Disk 0					
System Reserved (:)	1	NTFS	500.0 MB	343.9 MB	Disk 0
Local Disk (C:)	2	NTFS	111.3 GB	18.8 GB	Disk 0

☑ Disk 0
Basic (MBR)
111.8 GB
Used : 19.1 GB

Host Name:	server01
Domain:	WORKGROUP
IP Address:	192.168.123.76
Loaon User:	Administrator
PreBoot:	No
Mounted:	No

Task: None

4. Select a target destination for the backup image.
The following example show that “ \\192.168.123.77\disk “ in the network shared folder is specified for the target destination.
Click **[Select Folder]**.

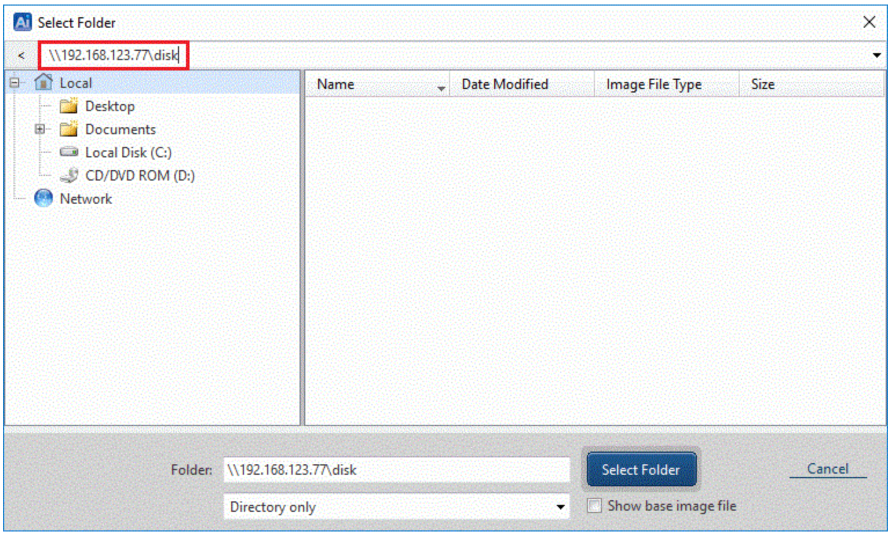


Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

Task Name: Backup_20191118_2135
Destination folder:
File Name: img_20191118_2135 _d00.aiv
□ Designate a separate image file set per disk
Comments:
□ Destination Isolation Options:
● Un-assign the drive letter from Local Hard Disk after backup completes
○ Take the destination Local Hard Disk offline after backup completes
○ Eject the destination USB Hard Disk after backup completes
○ Disable destination Network Connection after backup completes

Options:
☑ Compression:
○ Deduplication Compression
Level 2 (Optimized)
● Standard Compression
Fast
□ Password Protection
Password
Confirm Password
Strength:
□ Enable Encryption
AES 128 bit
□ Post Backup Operation
Shutdown System
Execution Priority
Lowest Low Medium High

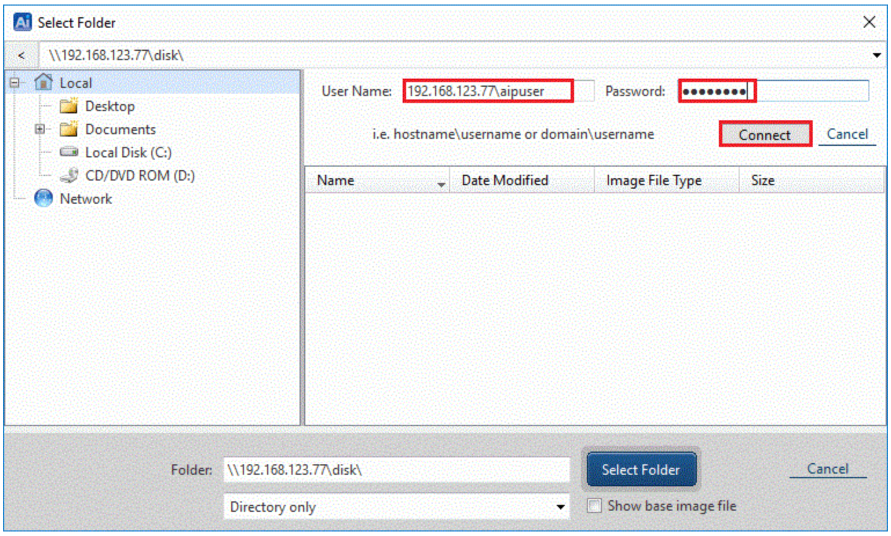
5. Please specify the path for the location of the target destination.
Please enter the following path “ \\192.168.123.77\disk “ for the target destination and press Enter key.



\\192.168.123.77\disk

Folder: \\192.168.123.77\disk
Directory only
□ Show base image file

Please enter the credentials to access the target destination.
User Name must be specified in “Host Name \ User Name” format.
The following example shows that the host name “192.168.123.77” and user name “aipuser” are entered. The credentials are predefined to access the destination folder.
Enter “ \\192.168.123.77\aipuser” for [User Name] and the password for [Password].
Click [Connect].

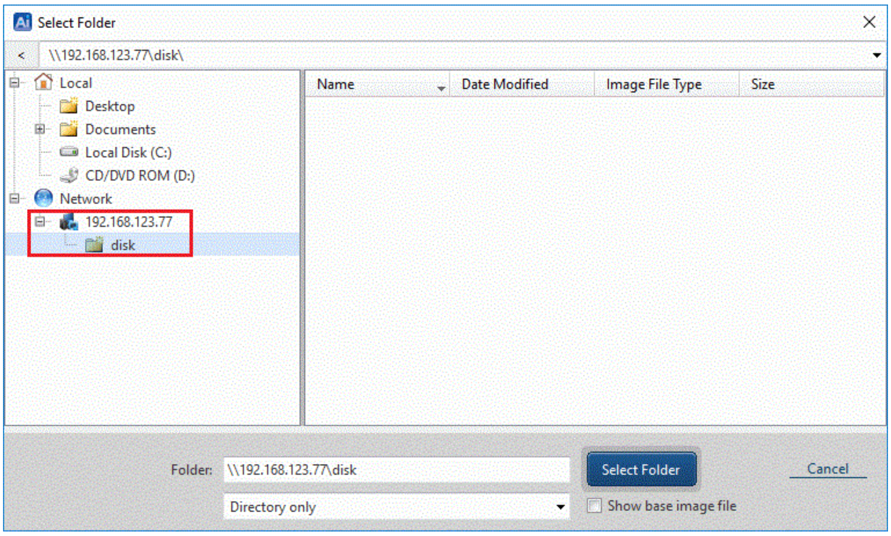


\\192.168.123.77\disk\

User Name: 192.168.123.77\aipuser
Password: ••••••••
i.e. hostname\username or domain\username

Folder: \\192.168.123.77\disk\
Directory only
□ Show base image file

6. Ensure the target destination is correctly specified and click **[Select Folder]**.

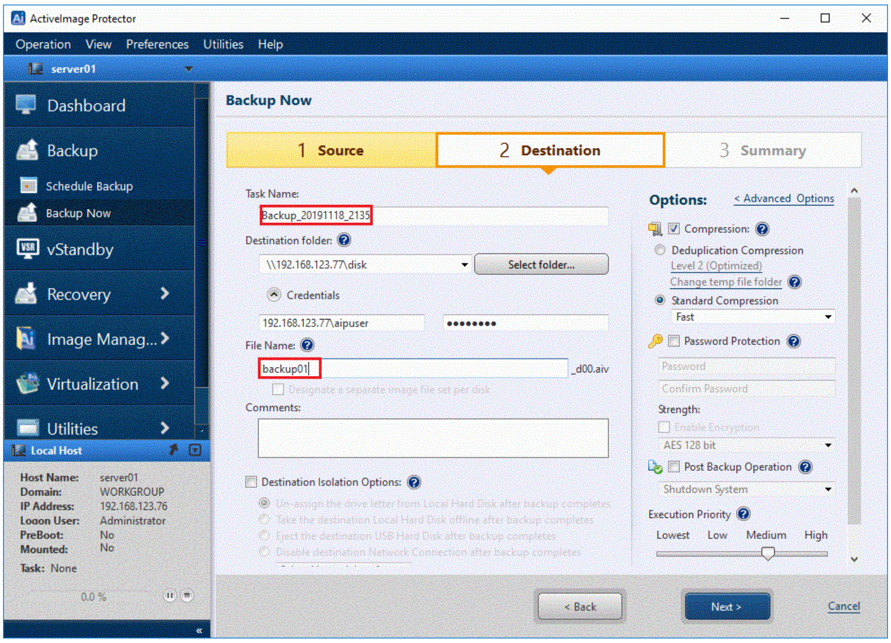


\\192.168.123.77\disk\

Folder: \\192.168.123.77\disk
Directory only
□ Show base image file

7. Specify the backup image file name.
   The following example shows that “backup01” is specified for the image file (the file extension is automatically entered.)
   Destination Isolation feature is available in ActiveImage Protector Update, disconnecting network access to backup image storage drives after backups complete. For more detailed description about **[Destination Isolation Options],** please refer to “Scheduled Backup”.

Enter “backup01” for **[File Name]** and click **[Next]**.



Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None

Backup Now

Task Name: Backup_20191118_2135

Destination folder: \\192.168.123.77\disk

Credentials: 192.168.123.77\aipuser ●●●●●●●●●

File Name: backup01 _d00.aiv

□ Designate a separate image file set per disk

Comments:

□ Destination Isolation Options:

- ● Un-assign the drive letter from Local Hard Disk after backup completes
- ○ Take the destination Local Hard Disk offline after backup completes
- ○ Eject the destination USB Hard Disk after backup completes
- ○ Disable destination Network Connection after backup completes

Options:

☑ Compression:

○ Deduplication Compression

● Standard Compression: Fast

□ Password Protection

Password

Confirm Password

Strength:

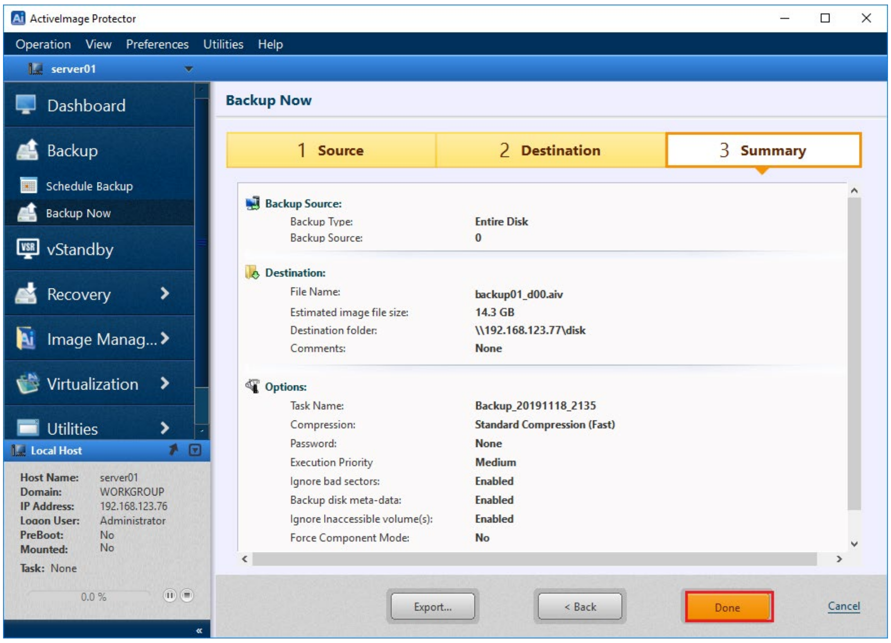
□ Enable Encryption

AES 128 bit

□ Post Backup Operation: Shutdown System

Execution Priority: Lowest Low Medium High

8. The backup configuration and option settings are displayed.
   Review the settings and click **[Done]** to start the backup task.



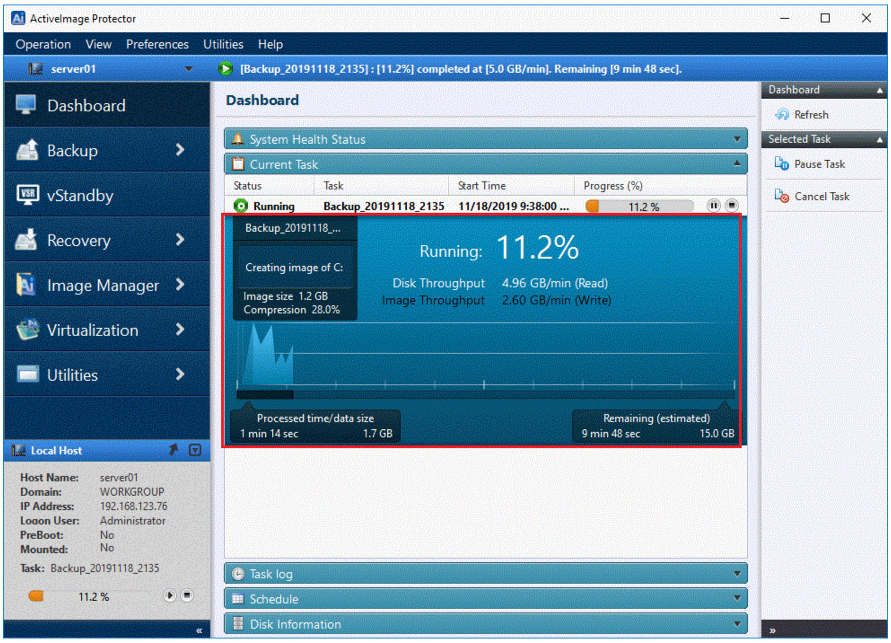
Backup Source:
Backup Type: Entire Disk
Backup Source: 0

Destination:
File Name: backup01_d00.aiv
Estimated image file size: 14.3 GB
Destination folder: \\192.168.123.77\disk
Comments: None

Options:
Task Name: Backup_20191118_2135
Compression: Standard Compression (Fast)
Password: None
Execution Priority Medium
Ignore bad sectors: Enabled
Backup disk meta-data: Enabled
Ignore Inaccessible volume(s): Enabled
Force Component Mode: No

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

9. When the backup task is started, the current task information is displayed in **[Dashboard]**.



[Backup_20191118_2135] : [11.2%] completed at [5.0 GB/min]. Remaining [9 min 48 sec].

Status	Task	Start Time	Progress (%)
Running	Backup_20191118_2135	11/18/2019 9:38:00 ...	11.2 %

Backup_20191118_...
Creating image of C:
Image size 1.2 GB
Compression 28.0%

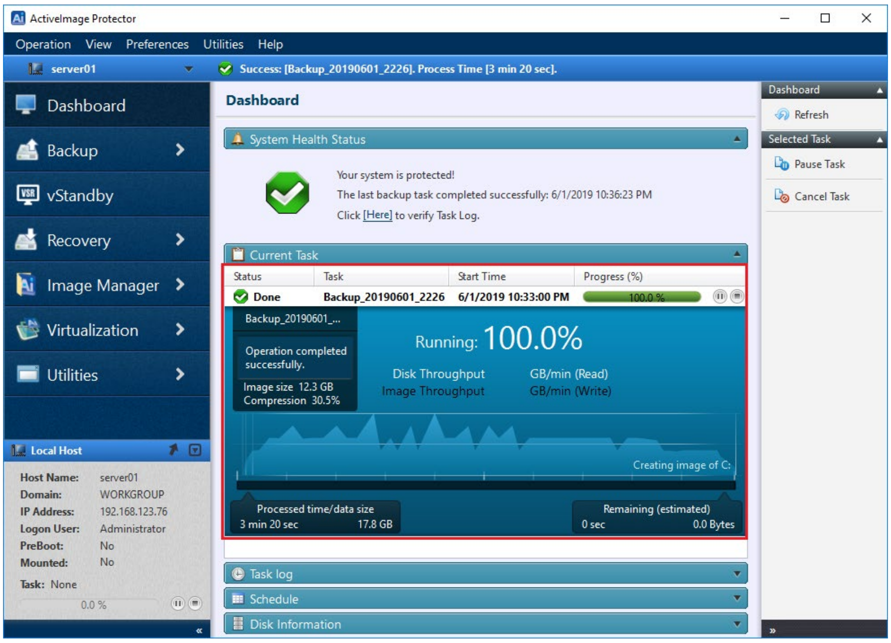
Running: 11.2%
Disk Throughput 4.96 GB/min (Read)
Image Throughput 2.60 GB/min (Write)

Processed time/data size
1 min 14 sec 1.7 GB

Remaining (estimated)
9 min 48 sec 15.0 GB

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: Backup_20191118_2135
11.2 %

10. When the progress of **[Running]** task indicates “100%”, the backup process is completed.



Success: [Backup_20190601_2226]. Process Time [3 min 20 sec].

Your system is protected!
The last backup task completed successfully: 6/1/2019 10:36:23 PM
Click [Here] to verify Task Log.

Status	Task	Start Time	Progress (%)
Done	Backup_20190601_2226	6/1/2019 10:33:00 PM	100.0 %

Backup_20190601_...

Operation completed successfully.

Image size 12.3 GB
Compression 30.5%

Running: 100.0%

Disk Throughput GB/min (Read)
Image Throughput GB/min (Write)

Creating image of C:

Processed time/data size
3 min 20 sec 17.8 GB

Remaining (estimated)
0 sec 0.0 Bytes

Host Name:	server01
Domain:	WORKGROUP
IP Address:	192.168.123.76
Logon User:	Administrator
PreBoot:	No
Mounted:	No

Task: None

0.0 %

4-2. Scheduled Backup

The following are the operating procedures for Scheduled Backup.

1. Start ActiveImage Protector.

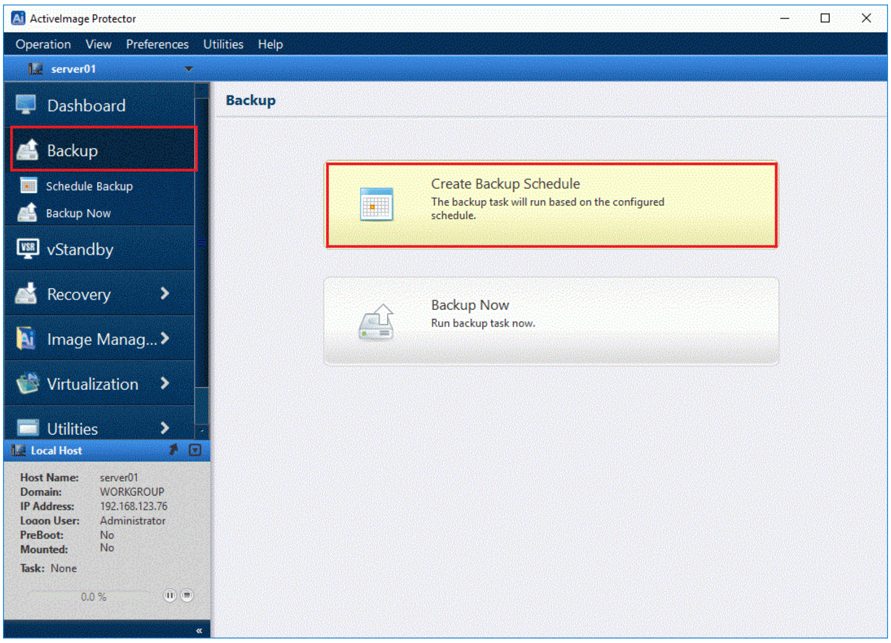
   Windows Server 2008 R2 or earlier server OS:
   Click **[Start]** – **[All Programs]** – **[NetJapan]** – **[ActiveImage Protector]**.

   Windows 7 or earlier Desktop OS:
   Click [Start] – [All Programs] – [NetJapan] – [ActiveImage Protector].

   Windows Server 2012 or later server OS:
   Click **[Start]** – **[Applications]** – **[NetJapan]** – **[ActiveImage Protector]**.

   Windows Server 8 or later Desktop OS :
   Click [Start] – [Applications] – [NetJapan] – [ActiveImage Protector].

2. Click [Backup] – [Create Backup Schedule].

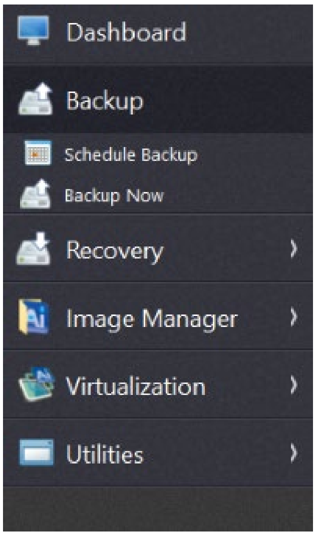


Create Backup Schedule
The backup task will run based on the configured schedule.

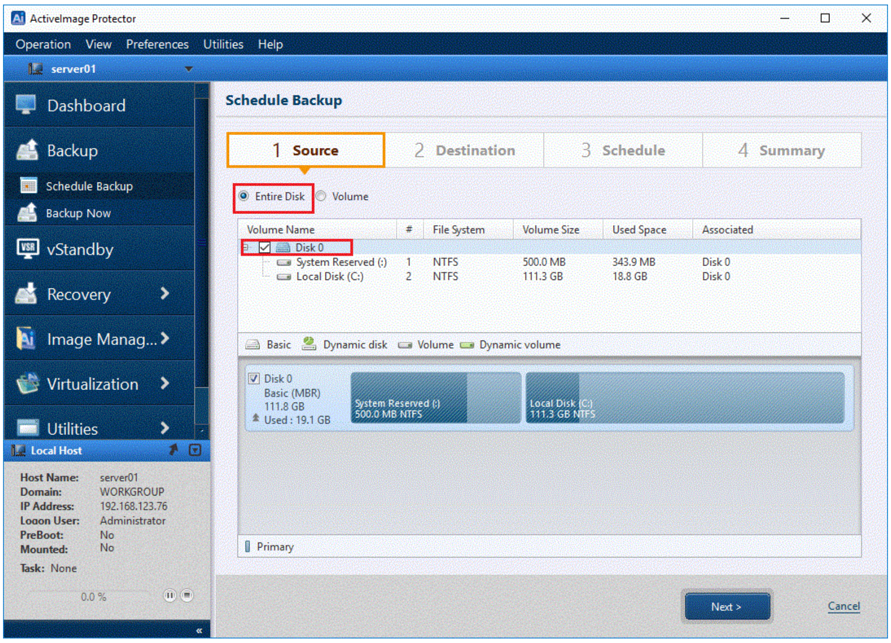
Backup Now
Run backup task now.

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Looon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

Note) The left pane of ActiveImage Protector for Hyper-V Enterprise screen is different from the one of Server Edition.



3. Select backup source.
   The following example shows that the entire disk is selected for the backup source. Click [Entire Disk] and check the checkbox for [Disk 0].
   When the backup source is selected, click [Next].



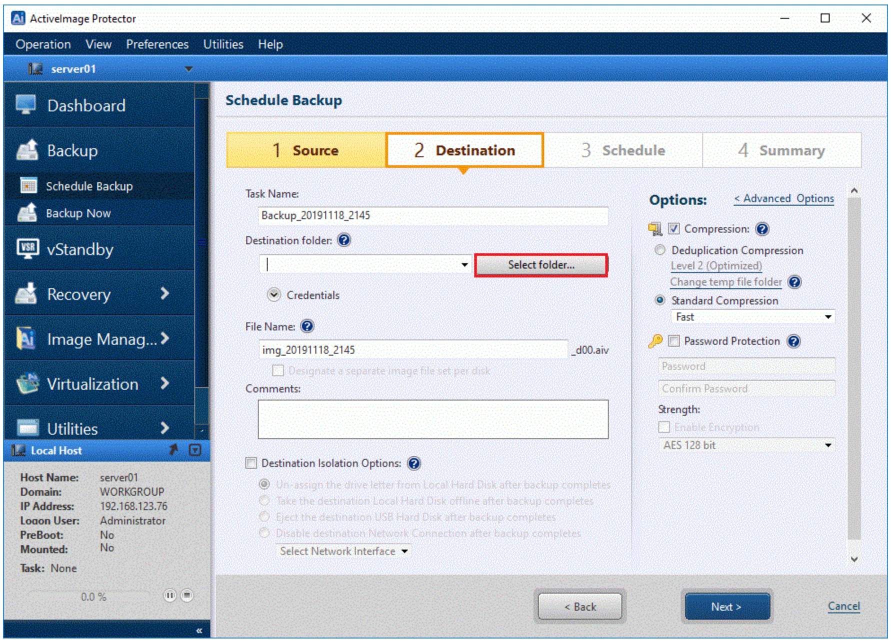
● Entire Disk ○ Volume

Volume Name	#	File System	Volume Size	Used Space	Associated
☑ Disk 0					
System Reserved (:)	1	NTFS	500.0 MB	343.9 MB	Disk 0
Local Disk (C:)	2	NTFS	111.3 GB	18.8 GB	Disk 0

☑ Disk 0
Basic (MBR)
111.8 GB
Used : 19.1 GB
System Reserved (:)
500.0 MB NTFS
Local Disk (C:)
111.3 GB NTFS

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None

4. Select a target destination for the backup image.
   The following example shows that “ \\192.168.123.77\disk “ in the network shared folder is specified for the target destination.
   Click **[Select Folder]**.

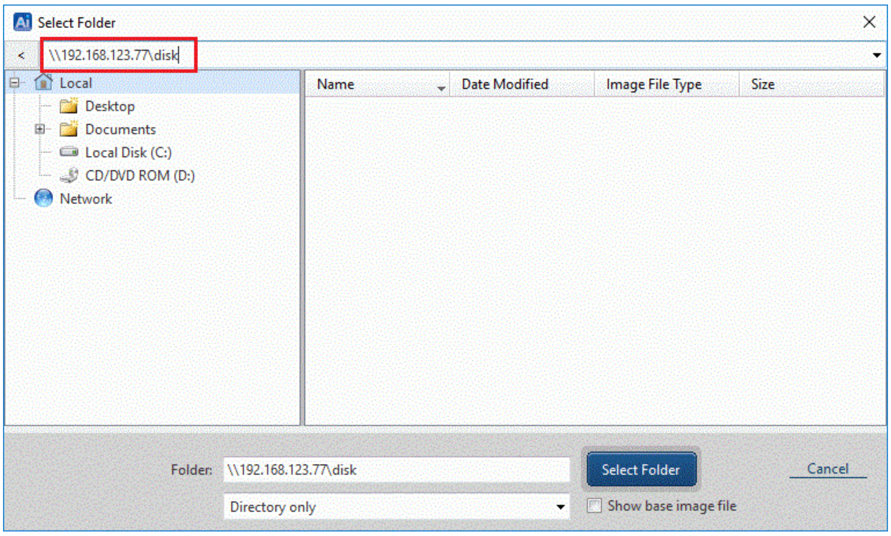


Task Name: Backup_20191118_2145
Destination folder:
File Name: img_20191118_2145 _d00.aiv
□ Designate a separate image file set per disk
Comments:
□ Destination Isolation Options:
● Un-assign the drive letter from Local Hard Disk after backup completes
○ Take the destination Local Hard Disk offline after backup completes
○ Eject the destination USB Hard Disk after backup completes
○ Disable destination Network Connection after backup completes
Select Network Interface

Options:
☑ Compression:
○ Deduplication Compression
Level 2 (Optimized)
Change temp file folder
● Standard Compression
Fast
□ Password Protection
Password
Confirm Password
Strength:
□ Enable Encryption
AES 128 bit

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None

5. Please specify the path for the location of the target destination. Please enter the following path “ \\192.168.123.77\disk “ for the target destination and press Enter key.



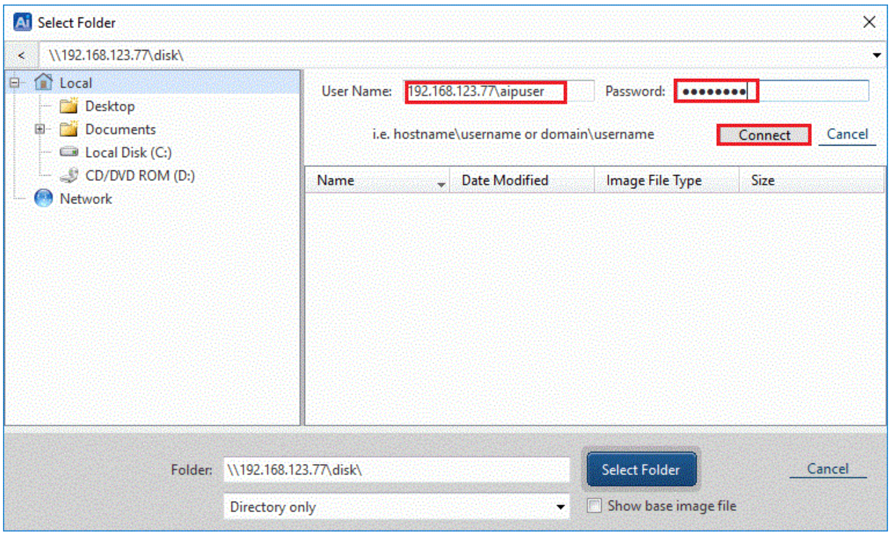
Select Folder

\\192.168.123.77\disk

Folder: \\192.168.123.77\disk

Directory only

6. Please enter the credentials to access the target destination. User Name must be specified in “Host Name \ User Name” format. The following example shows that the host name “192.168.123.77” and user name “aipuser” are entered. The credentials are predefined to access the destination folder. Enter “192.168.123.77\aipuser” for **[User Name]** and the password for **[Password]**. Click **[Connect]**.



Select Folder

\\192.168.123.77\disk\

User Name: 192.168.123.77\aipuser Password: ••••••••

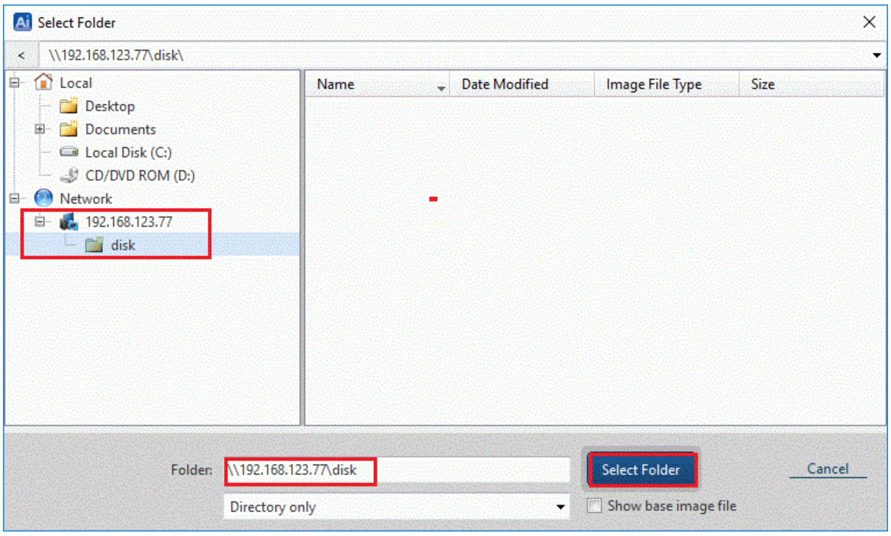
i.e. hostname\username or domain\username

Folder: \\192.168.123.77\disk\

Directory only

If you specify the same target destination that you selected before, since the credentials are saved, the windows for the above step 5 and 6 are skipped.

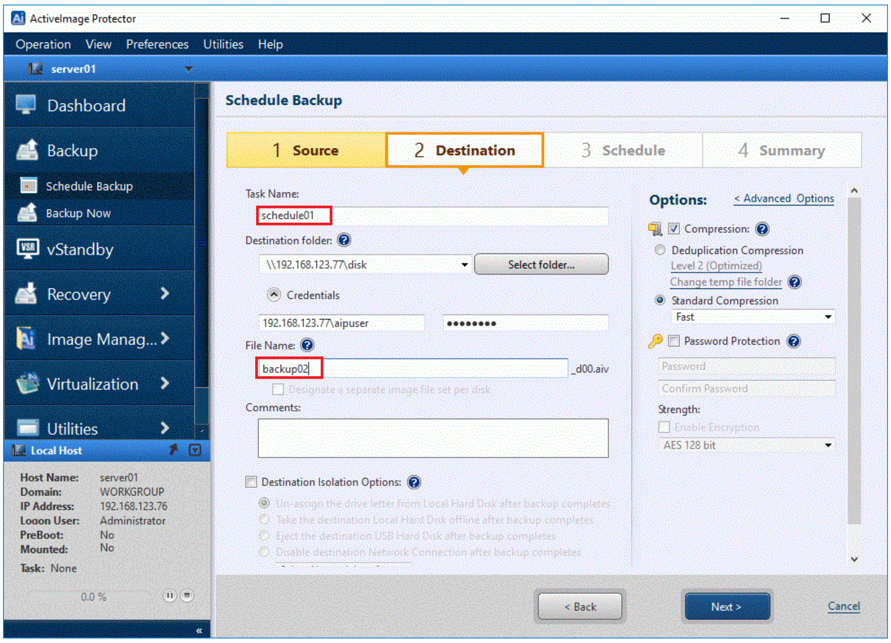
7. Ensure the target destination is correctly specified and click **[Select Folder]**.



Folder: \\192.168.123.77\disk

Directory only

8. Specify the backup image file name.
The following example shows that “schedule 01” is specified for the task name, “backup02” for the image file name (the file extension is automatically entered.)
Enter “schedule 01” for **[Task Name]**, “backup02” for **[File Name]**.



Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

Schedule Backup

Task Name: schedule01

Destination folder: \\192.168.123.77\disk

Credentials: 192.168.123.77\aipuser ••••••••

File Name: backup02 _d00.aiv

□ Designate a separate image file set per disk

Comments:

□ Destination Isolation Options:

- ● Un-assign the drive letter from Local Hard Disk after backup completes
- ○ Take the destination Local Hard Disk offline after backup completes
- ○ Eject the destination USB Hard Disk after backup completes
- ○ Disable destination Network Connection after backup completes

Options: < Advanced Options

☑ Compression:

- ○ Deduplication Compression
  Level 2 (Optimized)
  Change temp file folder
- ● Standard Compression
  Fast

□ Password Protection

Password

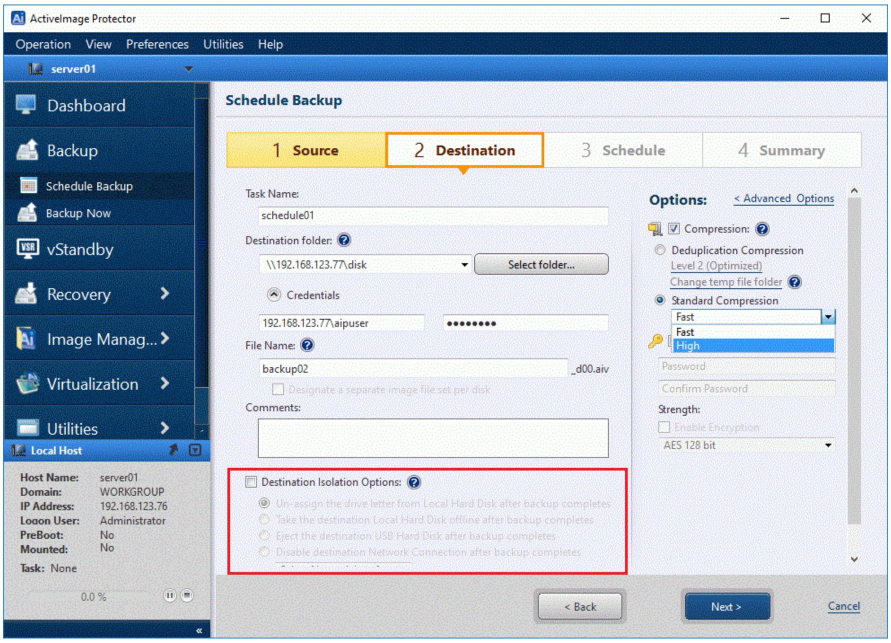
Confirm Password

Strength:

□ Enable Encryption

AES 128 bit

9. Next, configure the setting for **[Destination Isolation Options]**. Destination Isolation feature, available in ActiveImage Protector Update, disconnects network access to backup image storage drives or setting the destination disk to offline upon completion of backup process. ImageIsolate™ technology protects the backup storage and backup files from potential malware or ransomware attacks. **[Destination Isolation]** provides four options. Enabling **[Un-assign drive letter from Local Hard Disk post backup]**, the drive letter assigned to the local hard disk is de-assigned upon completion of backup process. Selection of **[Make destination Local Hard disk offline post backup]** sets the destination disk to offline upon completion of backup process (same behavior as **[Disk Management]** in Disk Management Tool). When **[Eject destination Removable USB Hard disk post backup]** is enabled, a removable hard disk such as USB hard disk become removable upon completion of backup process. If **[Disable destination Network Connection post backup]** is enabled, network connection to backup destination is disconnected upon completion of backup process. You can select the network interface to block in the selection box at the bottom.



Schedule Backup

Task Name: schedule01

Destination folder: \\192.168.123.77\disk

Credentials: 192.168.123.77\aipuser ••••••••

File Name: backup02_d00.aiv

□ Designate a separate image file set per disk

Comments:

□ Destination Isolation Options:

- ● Un-assign the drive letter from Local Hard Disk after backup completes
- ○ Take the destination Local Hard Disk offline after backup completes
- ○ Eject the destination USB Hard Disk after backup completes
- ○ Disable destination Network Connection after backup completes

Options:

☑ Compression:

○ Deduplication Compression

Level 2 (Optimized)

Change temp file folder

● Standard Compression

Fast

Fast

High

Password

Confirm Password

Strength:

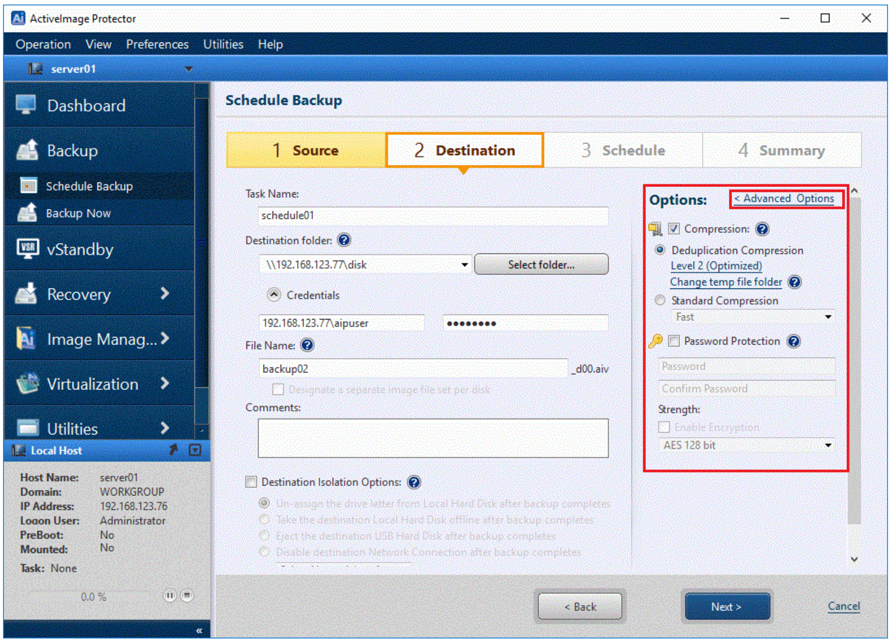
□ Enable Encryption

AES 128 bit

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None

0.0 %

10. Configure Compression settings. ActiveImage Protector provides two compression types.
    One is Standard Compression that offers the common file / folder compression tool same as ZIP. The other is Deduplication Compression designed to create index for every block of backup stream and delete duplicated blocks when identified while creating a backup image file. Deduplication Compression feature efficiently and dramatically reduces backup storage space requirements on a server hosting multiple virtual machines.
    Check the checkbox for **[Compression]** in **[Option]** pane. When **[Deduplication Compression]** option is selected, **[Level 2] (Optimized)** and **[Change temp folder]** are enables.



Task Name: schedule01

Destination folder: \\192.168.123.77\disk

Credentials

192.168.123.77\aipuser ●●●●●●●●●

File Name: backup02 _d00.aiv

□ Designate a separate image file set per disk

Comments:

□ Destination Isolation Options:

● Un-assign the drive letter from Local Hard Disk after backup completes
○ Take the destination Local Hard Disk offline after backup completes
○ Eject the destination USB Hard Disk after backup completes
○ Disable destination Network Connection after backup completes

Options: < Advanced Options

☑ Compression:
● Deduplication Compression
Level 2 (Optimized)
Change temp file folder
○ Standard Compression
Fast

□ Password Protection
Password
Confirm Password
Strength:
□ Enable Encryption
AES 128 bit

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

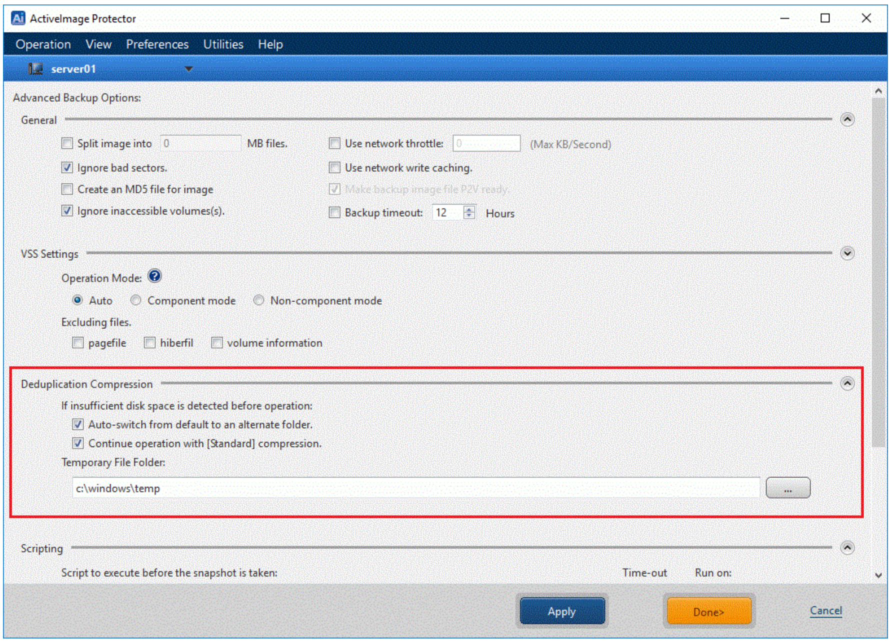
The compression level goes up according to the compression ratio. When a backup task runs in boot environment, the temporary work folder is located on memory by default, therefore, please be aware that the available space in the temporary work folder may be insufficient. If the backup source includes large data volume, please change the temporary work folder to other location such as the target destination.

Click **[Advanced Option]** to configure the advanced option settings.

In **[General]**, please select **[Split image into xx MB files]** to split and save the created backup files.

In **[VSS Setting]**, You can edit the VSS setting for a backup task if you need to forcefully run VSS in component mode or exclude specific files from backup source.

In **[Deduplication Compression]**, you can select an option ensuring that the backup task completes without interruption if insufficient disk space is detected in the temporary file folder before operation. You can also specify the location for deduplication to process temporary files. Since the execution of a backup task in boot environment processes the temporary files in memory space, by default, it may cause insufficient available memory. If the backup source is large in data size, please change the location of temporary file folder.



Advanced Backup Options:

General

☐ Split image into 0 MB files.
☑ Ignore bad sectors.
☐ Create an MD5 file for image
☑ Ignore inaccessible volumes(s).

☐ Use network throttle: 0 (Max KB/Second)
☐ Use network write caching.
☑ Make backup image file P2V ready.
☐ Backup timeout: 12 Hours

VSS Settings

Operation Mode:
● Auto ○ Component mode ○ Non-component mode
Excluding files.
☐ pagefile ☐ hiberfil ☐ volume information

Deduplication Compression

If insufficient disk space is detected before operation:
☑ Auto-switch from default to an alternate folder.
☑ Continue operation with [Standard] compression.
Temporary File Folder:
c:\windows\temp

Scripting

Script to execute before the snapshot is taken: Time-out Run on:

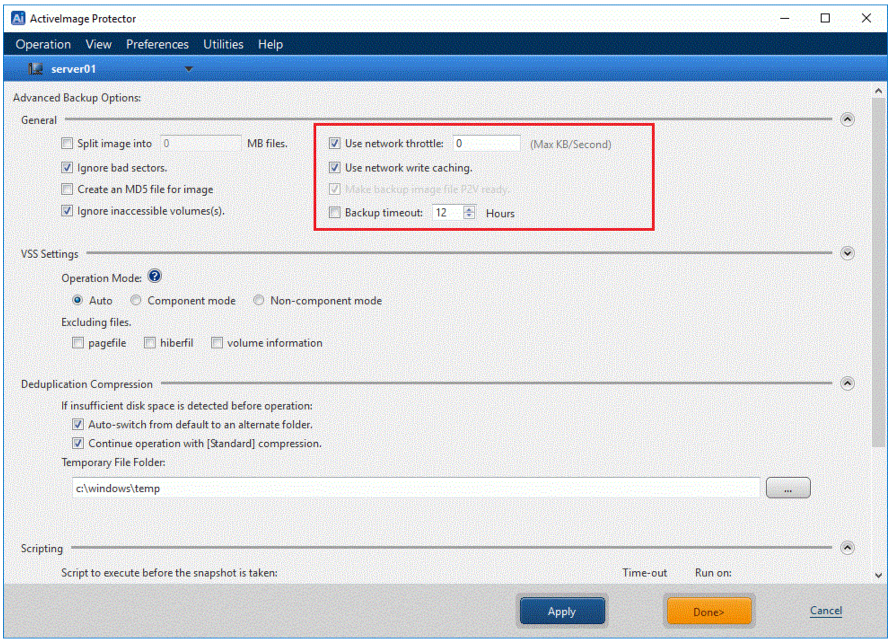
Backing up multiple number of virtual machines at a time increases backup traffic over the network. Network throttle defines the maximum throughput over the network and the use of cached data shortens data access time.

Enable **[Use network throttle]** option to define the maximum throughput in KB/second to reduce traffic over the network while saving backup image files to network shared folder.

Enable **[Use network write caching]** option to use cached data and shorten data access time in saving backup image files to the destination over network.

Enable **[Backup Time-out]** option and specify the maximum time to wait for a backup task to complete the backup process. Time-out occurs to cancel the backup task if the backup process does not complete within the specified time.

.



Advanced Backup Options:

General

□ Split image into 0 MB files.

☑ Ignore bad sectors.

□ Create an MD5 file for image

☑ Ignore inaccessible volumes(s).

☑ Use network throttle: 0 (Max KB/Second)

☑ Use network write caching.

☑ Make backup image file P2V ready.

□ Backup timeout: 12 Hours

VSS Settings

Operation Mode:

● Auto ○ Component mode ○ Non-component mode

Excluding files.

□ pagefile □ hiberfil □ volume information

Deduplication Compression

If insufficient disk space is detected before operation:

☑ Auto-switch from default to an alternate folder.

☑ Continue operation with [Standard] compression.

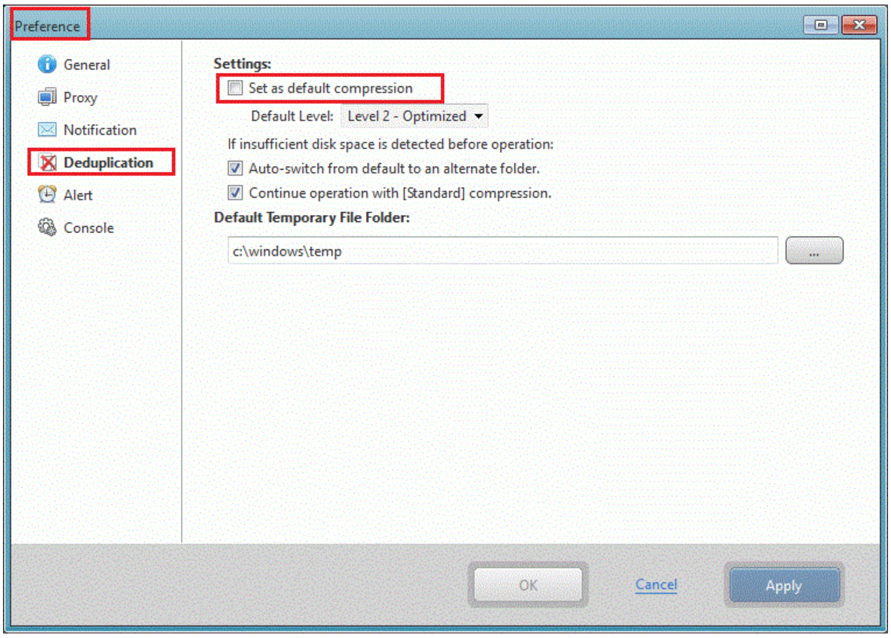
Temporary File Folder:

c:\windows\temp

Scripting

Script to execute before the snapshot is taken: Time-out Run on:

11. To enable Deduplication Compression feature by default, go to [Preference] – [Deduplication] and check the checkbox for **[Set as default compression]** and select **[Deduplication Compression]** for **[Default Level]**. Click **[Apply]**.



Settings:

□ Set as default compression

Default Level: Level 2 - Optimized

If insufficient disk space is detected before operation:

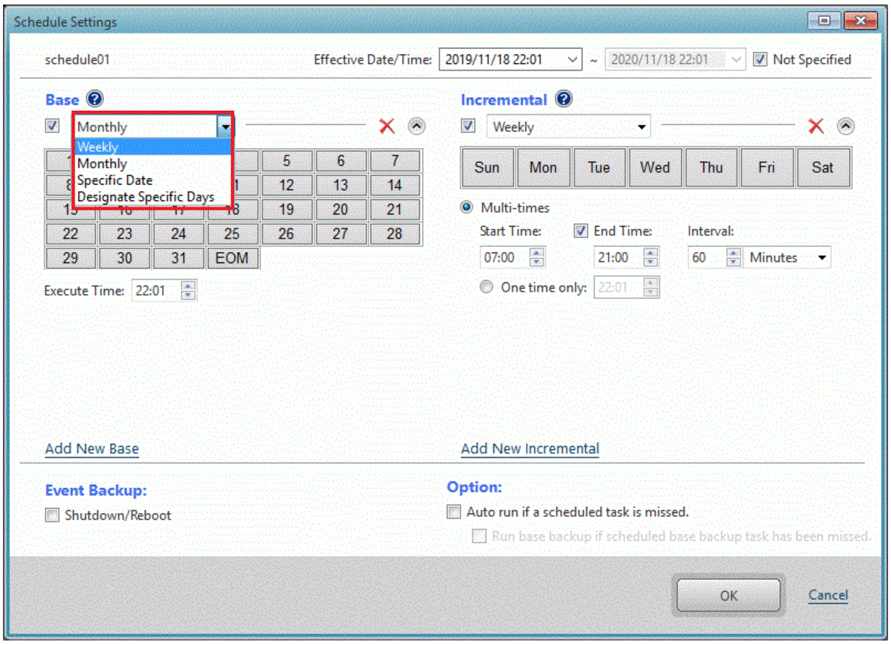
☑ Auto-switch from default to an alternate folder.

☑ Continue operation with [Standard] compression.

Default Temporary File Folder:

c:\windows\temp

12. Schedule type can be selected to configure the backup schedule.
Begin by specifying **[Effective Date/Time]** that the scheduled task becomes live. The [Effective Date/Time] defaults 10 minutes from the time of beginning the configuration in the wizard. **[Not Specified]** option may be selected so that the scheduled task is live for unlimited period. Options include **[Weekly]**, **[Monthly]**, **[Specific Date]**, **[Designate Specific Days]** for full base backup.



schedule01

Effective Date/Time: 2019/11/18 22:01 ~ 2020/11/18 22:01 ☑ Not Specified

Base: ☑ Monthly

Execute Time: 22:01

Incremental: ☑ Weekly

● Multi-times

Start Time: 07:00 ☑ End Time: 21:00 Interval: 60 Minutes

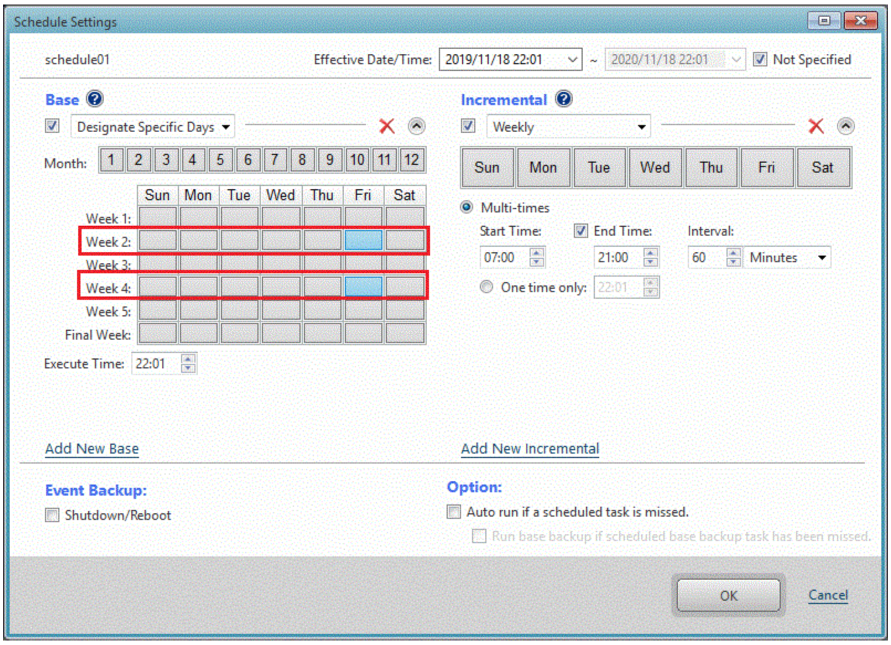
○ One time only: 22:01

□ Shutdown/Reboot

□ Auto run if a scheduled task is missed.

□ Run base backup if scheduled base backup task has been missed.

[Designate Specific Days] is a new schedule type ActiveImage Protector 2018 Update provides. For example, you can specify “Every second Friday from January to December” for the schedule setting. In case you have a routine of business operations such as financial closing or inventory management which requires to make significant changes on a specific day of a specific week every month, you will find this schedule type very convenient.



schedule01

Effective Date/Time: 2019/11/18 22:01 ~ 2020/11/18 22:01 ☑ Not Specified

Base: ☑ Designate Specific Days

Execute Time: 22:01

Incremental: ☑ Weekly

● Multi-times

Start Time: 07:00 ☑ End Time: 21:00 Interval: 60 Minutes

○ One time only: 22:01

□ Shutdown/Reboot

□ Auto run if a scheduled task is missed.

□ Run base backup if scheduled base backup task has been missed.

The following example shows the weekly backup schedule settings.

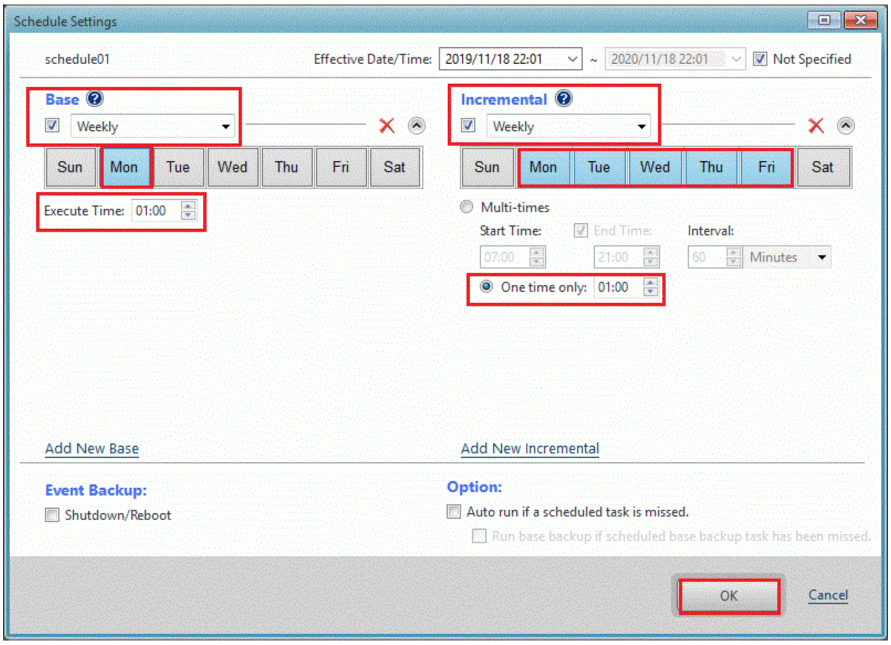
・Base backup: Weekly

・Incremental backup: Weekly

・Base backup: Every Sunday at 1:00 AM

・Incremental backup: From Monday to Friday at 1:00 AM

After configuring the settings, click **[OK]**.



Schedule Settings

schedule01 Effective Date/Time: 2019/11/18 22:01 ~ 2020/11/18 22:01 ☑ Not Specified

Base

☑ Weekly

Execute Time: 01:00

Incremental

☑ Weekly

○ Multi-times

Start Time: 07:00 ☑ End Time: 21:00 Interval: 60 Minutes

● One time only: 01:00

Event Backup:

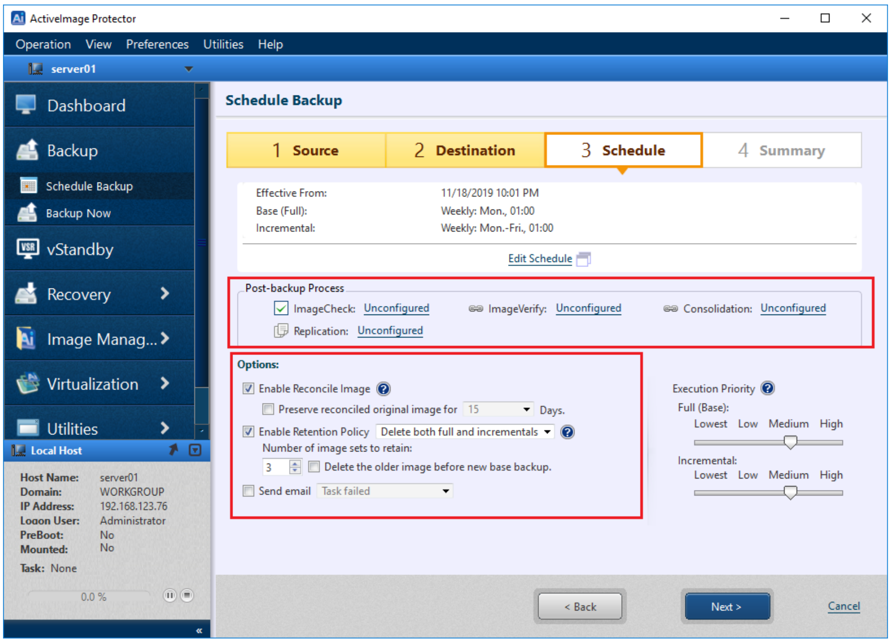
□ Shutdown/Reboot

Option:

□ Auto run if a scheduled task is missed.

□ Run base backup if scheduled base backup task has been missed.

13. Configure the option settings including Retention Policy, BootCheck and Consolidation for post backup processing.
Check the checkbox for **[Enable Retention Policy]** option and enter "3" for [Number of image sets to retain:] (3 sets of incremental backup files are retained in the target destination before deletion).



Schedule Backup

Effective From: 11/18/2019 10:01 PM
Base (Full): Weekly: Mon., 01:00
Incremental: Weekly: Mon.-Fri., 01:00

Post-backup Process
☑ ImageCheck: Unconfigured ImageVerify: Unconfigured Consolidation: Unconfigured
Replication: Unconfigured

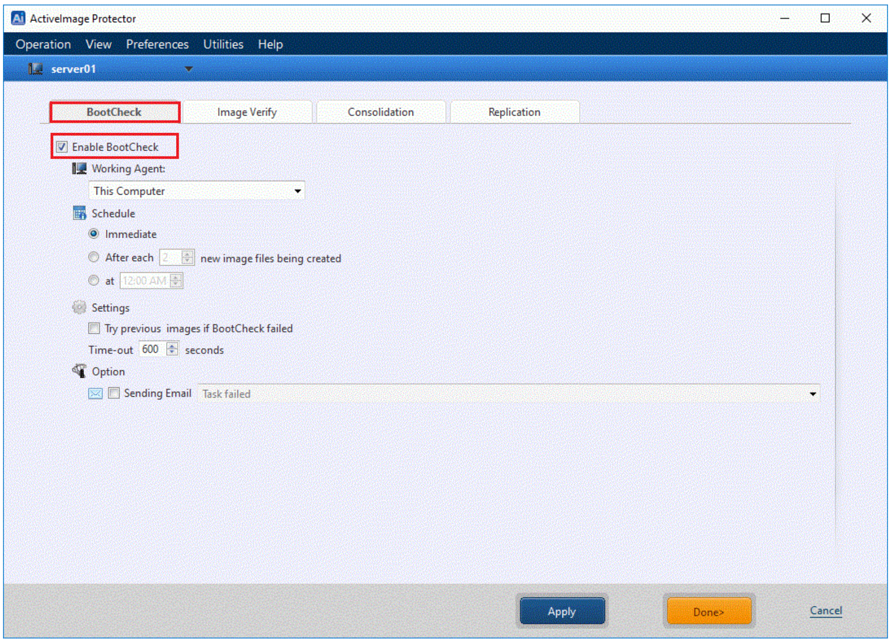
Options:
☑ Enable Reconcile Image
□ Preserve reconciled original image for 15 Days.
☑ Enable Retention Policy Delete both full and incrementals
Number of image sets to retain:
3 □ Delete the older image before new base backup.
□ Send email Task failed

Execution Priority
Full (Base):
Lowest Low Medium High
Incremental:
Lowest Low Medium High

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

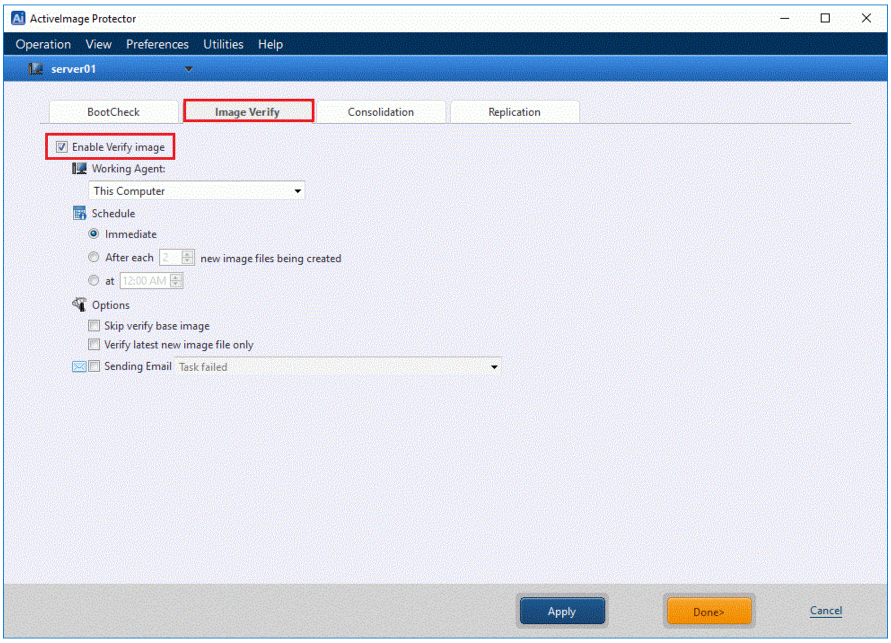
You can select an option for Post-backup Process, i.e., **[BootCheck]**, **[Image Verify]**, **[Consolidation]**, **[Replication]**. **[BootCheck]** tests that backup images can successfully boot up by using virtual machine on the specified host.
Click **[Unconfigured]** to display the setting window. ActiveImage Protector allows users to specify the timing to start BootCheck process (ref. “7-6 Manually run BootCheck” in “7. Image Manager”.

14. In **[BootCheck]** tab, check the checkbox for **[Enable BootCheck]**.



☑ Enable BootCheck
Working Agent:
This Computer
Schedule
● Immediate
○ After each 2 new image files being created
○ at 12:00 AM
Settings
□ Try previous images if BootCheck failed
Time-out 600 seconds
Option
□ Sending Email Task failed

15. Click **[Image Verify]** tab. Check in the check box for **[Enable Verify Image]** to verify the integrity of a created backup image. Please configure the setting for **[Schedule]**.



☑ Enable Verify image

Working Agent: This Computer

Schedule

● Immediate

○ After each 2 new image files being created

○ at 12:00 AM

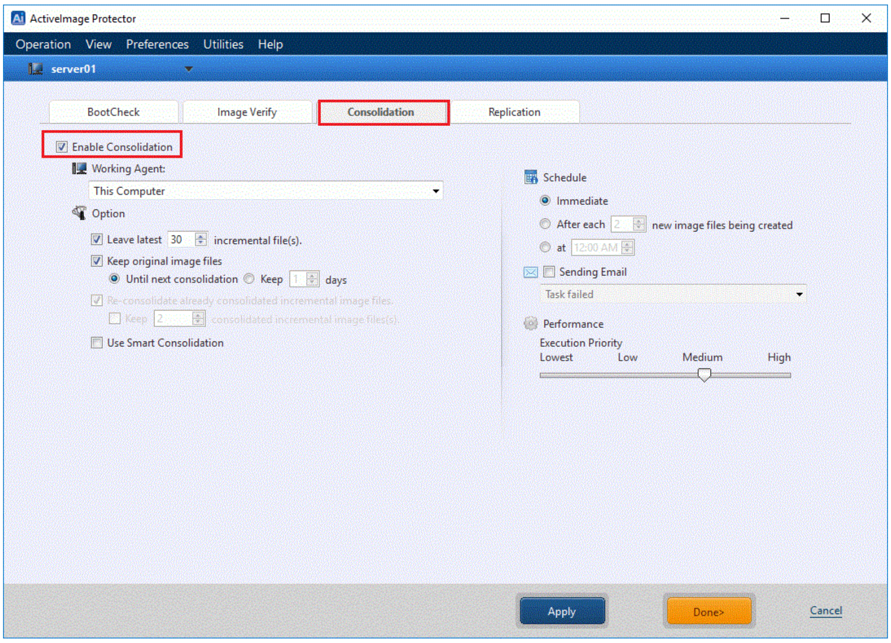
Options

□ Skip verify base image

□ Verify latest new image file only

□ Sending Email Task failed

16. Click **[Consolidation]** tab. Check the checkbox for **[Enable Consolidation]**. Incremental backup saves processing time, however, recurring scheduled backup tasks creates a growing and sometimes unmanageable number of incremental files. Consolidation consolidates an uninterrupted series of backup image files in the same generation set to facilitate file management.
    The following example shows that 15 consolidated files are retained while the latest 30 incremental files are saved. Consolidation task runs whenever a new incremental backup file is created.
    Click **[Done]** to go back to **[Schedule]** window.



☑ Enable Consolidation

Working Agent:
This Computer

Option
☑ Leave latest 30 incremental file(s).
☑ Keep original image files
● Until next consolidation ○ Keep 1 days
☑ Re-consolidate already consolidated incremental image files.
□ Keep 2 consolidated incremental image files(s).
□ Use Smart Consolidation

Schedule
● Immediate
○ After each 2 new image files being created
○ at 12:00 AM
□ Sending Email
Task failed

Performance
Execution Priority
Lowest Low Medium High

17. The use of Replication feature enables you to replicate backup data to an offsite storage share including cloud storages, delivering emergency responses to natural and unexpected disasters. ActiveImage Protector Replication feature supports the following for the replication targets:

- Local Folder
- Network Shared Folder
- SFTP
- FTP
- WebDAV
- Amazon S3

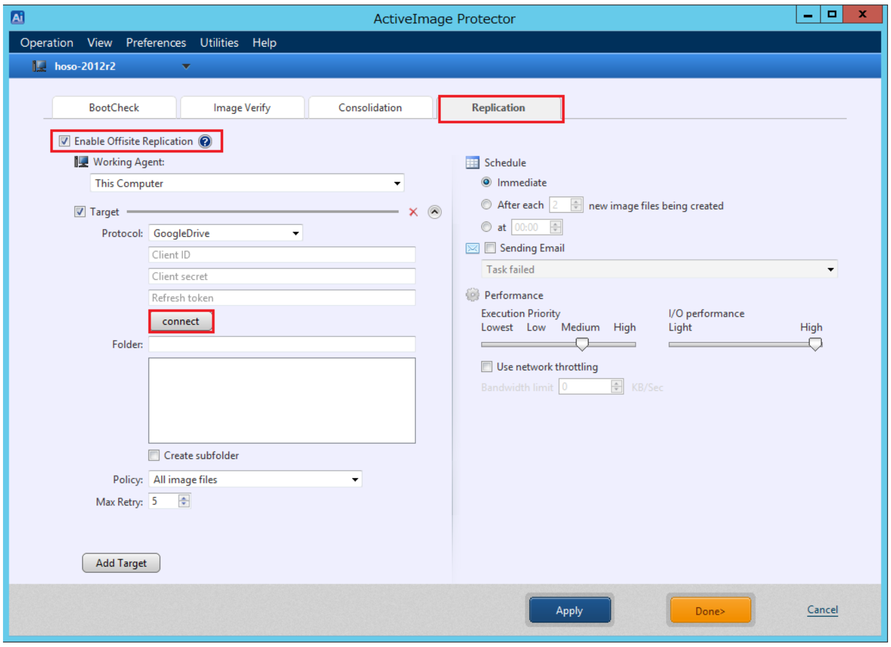
- Azure
- OneDrive
- Dropbox
- Google Drive

Except for local storage, the supported targets are cloud storages that are becoming more widespread in the world. Replication of backup files to the cloud storages helps you prepared for emergency situations.

In this example, Google Drive is selected for the replication target which requires you to enter the following information:

- Client ID
- Client Secret
- Refresh Token

You need to get the above listed information that should be issued by configuring Google Drive settings (Ref. “Appendix A: Replicate backup data to Google Drive”.) Please enter the information in the following dialog.



☑ Enable Offisite Replication

Working Agent: This Computer

☑ Target

Protocol: GoogleDrive

Client ID

Client secret

Refresh token

Folder:

□ Create subfolder

Policy: All image files

Max Retry: 5

Schedule

● Immediate

○ After each 2 new image files being created

○ at 00:00

□ Sending Email

Task failed

Performance

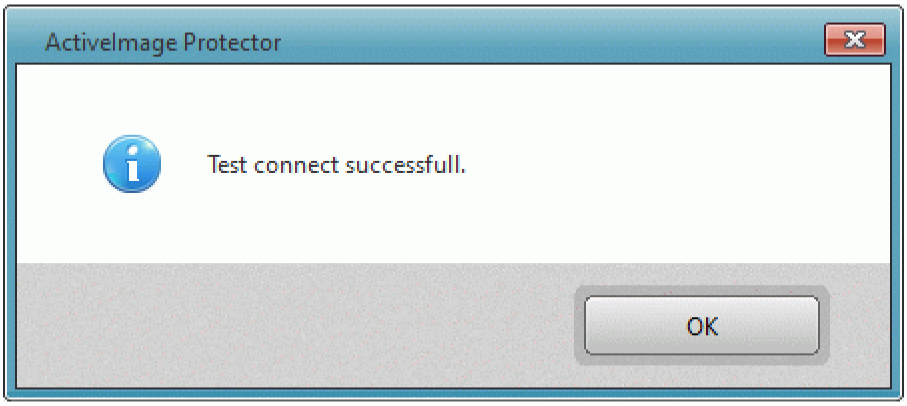
Execution Priority: Lowest Low Medium High

I/O performance: Light High

□ Use network throttling

Bandwidth limit 0 KB/Sec

Click **[Connection]** button. When the following message is displayed, the backup files can be replicated to Google Drive



ActiveImage Protector

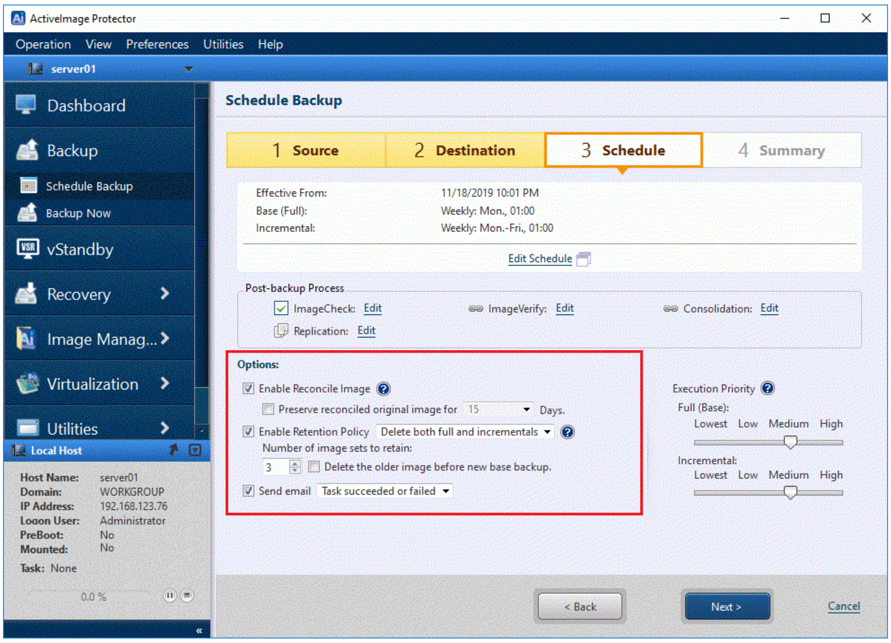
Test connect successfull.

Replication of backup files to a cloud storage provides higher availability, however, consumes network resources. ActiveImage Protector's Replication offers flexible scheduling feature and performance setting, offloading additional resource demand on the machine ActiveImage Protector backup tasks are executed.

18. In **[Option]** section, the following options are provided.

- Enable Retention Policy
- Send email

Retention Policy defines how many sets of backup files to retain before deletion. Enabling Retention Policy, you can configure the setting for the number of image sets to retain as well as which backup image files to delete. Enable [Send email] option to send E-Mail informing you of a task completed with a specified status.



Schedule Backup

Effective From: 11/18/2019 10:01 PM
Base (Full): Weekly: Mon., 01:00
Incremental: Weekly: Mon.-Fri., 01:00

Edit Schedule

Post-backup Process

☑ ImageCheck: Edit ImageVerify: Edit Consolidation: Edit

Replication: Edit

Options:

☑ Enable Reconcile Image

□ Preserve reconciled original image for 15 Days.

☑ Enable Retention Policy Delete both full and incrementals

Number of image sets to retain:

3 □ Delete the older image before new base backup.

☑ Send email Task succeeded or failed

Execution Priority

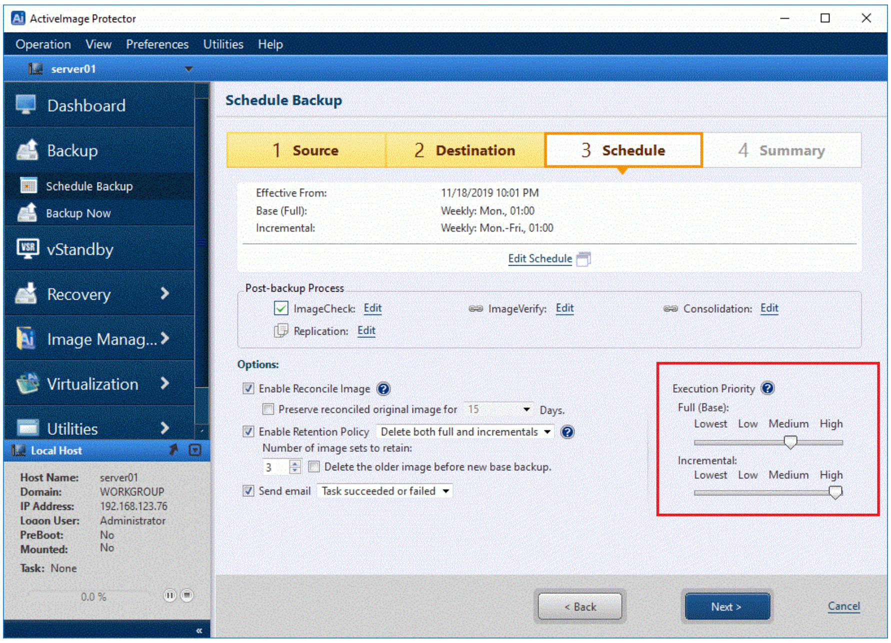
Full (Base): Lowest Low Medium High

Incremental: Lowest Low Medium High

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

Backing up multiple number of virtual machines at a time increases backup traffic over the network. Network throttle defines the maximum throughput over the network and the use of cached data shortens data access time.

You can also select a level of task Execution Priority for CPU usage.



Schedule Backup

Effective From: 11/18/2019 10:01 PM
Base (Full): Weekly: Mon., 01:00
Incremental: Weekly: Mon.-Fri., 01:00

Edit Schedule

Post-backup Process

☑ ImageCheck: Edit ImageVerify: Edit Consolidation: Edit

Replication: Edit

Options:

☑ Enable Reconcile Image

□ Preserve reconciled original image for 15 Days.

☑ Enable Retention Policy Delete both full and incrementals

Number of image sets to retain:

3 □ Delete the older image before new base backup.

☑ Send email Task succeeded or failed

Execution Priority

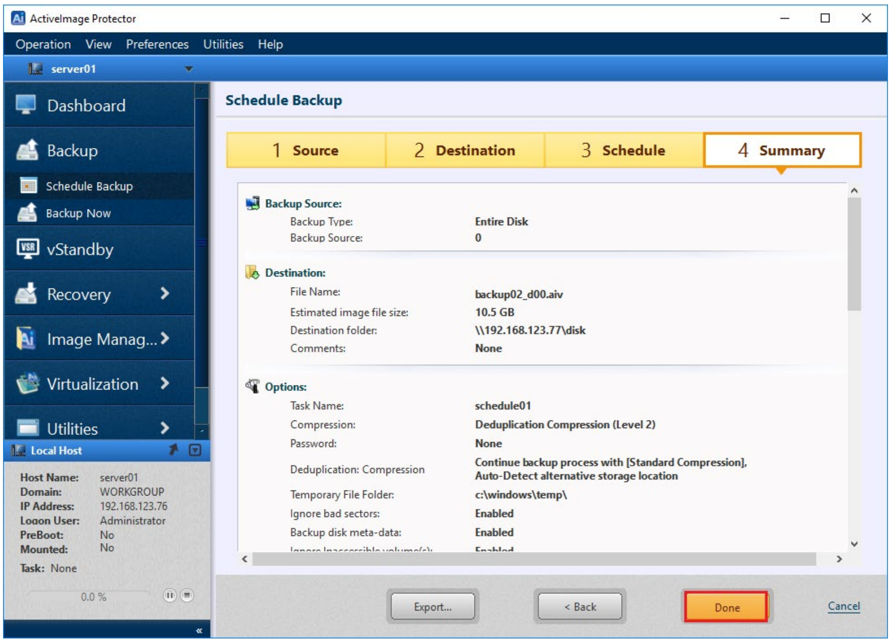
Full (Base): Lowest Low Medium High

Incremental: Lowest Low Medium High

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

When the option settings are configured, click **[Next]**.

19. In **[Summary]** window, review the backup configuration and options. Click **[Done]** to complete backup setting.



Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

Backup Source:

Backup Type:	Entire Disk
Backup Source:	0

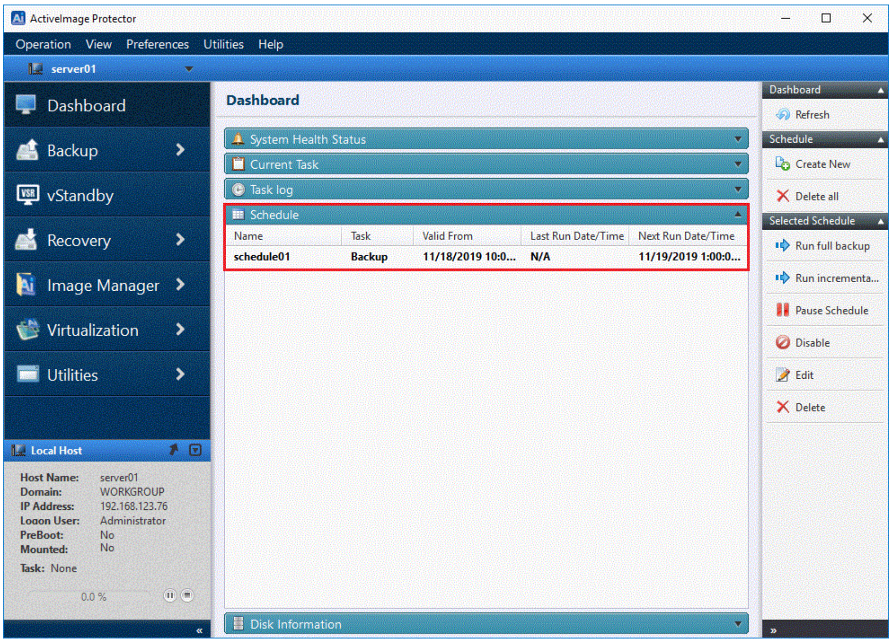
Destination:

File Name:	backup02_d00.aiv
Estimated image file size:	10.5 GB
Destination folder:	\\192.168.123.77\disk
Comments:	None

Options:

Task Name:	schedule01
Compression:	Deduplication Compression (Level 2)
Password:	None
Deduplication: Compression	Continue backup process with [Standard Compression], Auto-Detect alternative storage location
Temporary File Folder:	c:\windows\temp\
Ignore bad sectors:	Enabled
Backup disk meta-data:	Enabled
Ignore Inaccessible volume(s):	Enabled

20. Go to **[Dashboard]** – **[Schedule]** to monitor the created schedule. The scheduled backup task runs according to the schedule you specified.



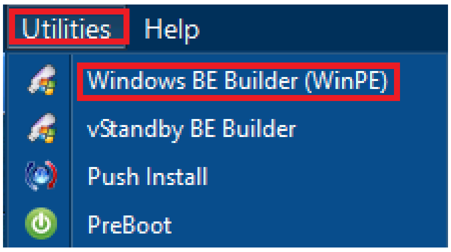
Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

Name	Task	Valid From	Last Run Date/Time	Next Run Date/Time
schedule01	Backup	11/18/2019 10:0...	N/A	11/19/2019 1:00:0...

5. Boot Environment Builder

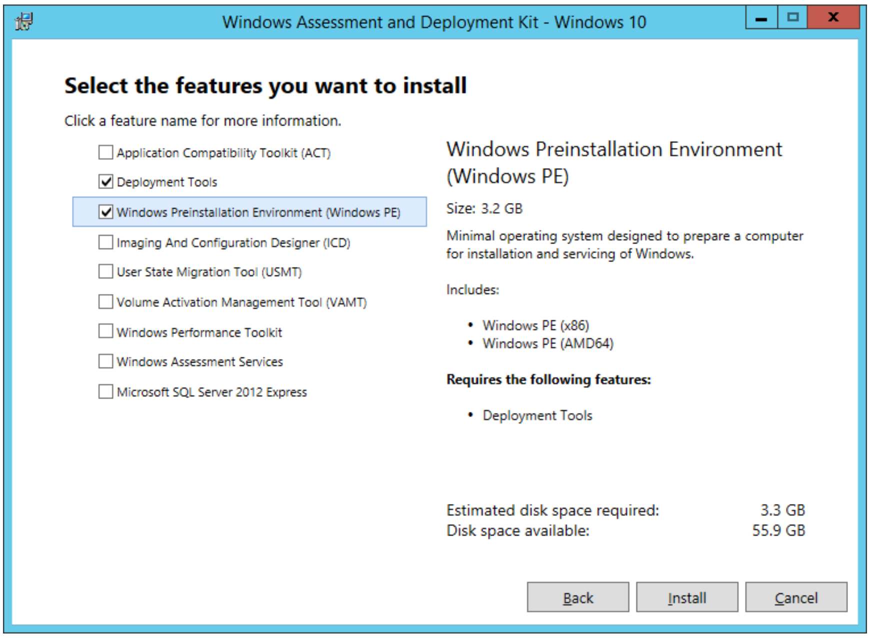
Build Windows-PE based Boot Environment

1. Start by selecting [BE Builder (Windows PE)] from the [Utilities] menu bar.



2. Microsoft Windows ADK or AIK is required to be installed on the host to build the Windows PE based boot environments.
   As for Windows ADK, please select the following components to install:

   - Deployment Tools
   - Windows Preinstallation Environment (Windows PE)


Windows Assessment and Deployment Kit - Windows 10

Select the features you want to install

Click a feature name for more information.

☐ Application Compatibility Toolkit (ACT)
☑ Deployment Tools
☑ Windows Preinstallation Environment (Windows PE)
☐ Imaging And Configuration Designer (ICD)
☐ User State Migration Tool (USMT)
☐ Volume Activation Management Tool (VAMT)
☐ Windows Performance Toolkit
☐ Windows Assessment Services
☐ Microsoft SQL Server 2012 Express

Windows Preinstallation Environment (Windows PE)

Size: 3.2 GB

Minimal operating system designed to prepare a computer for installation and servicing of Windows.

Includes:

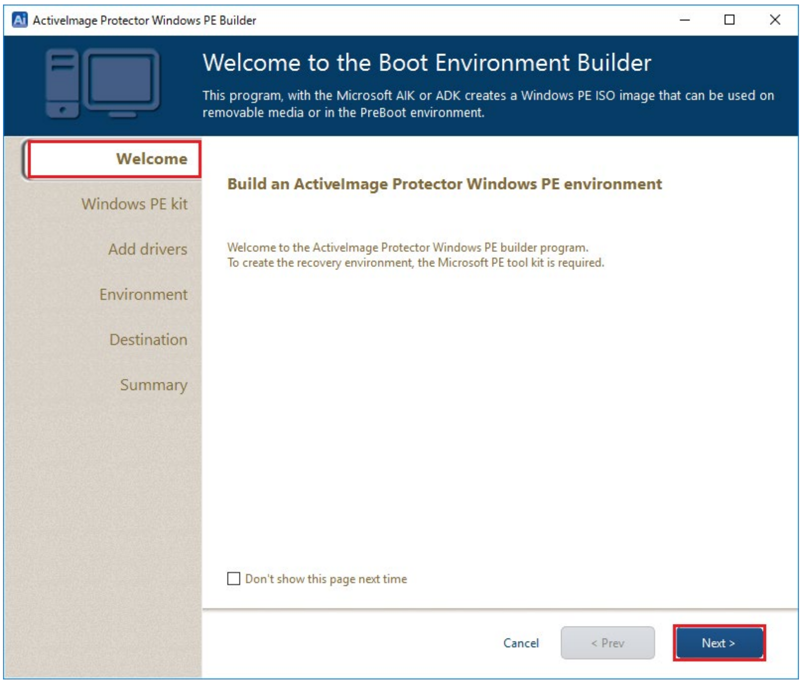
- Windows PE (x86)
- Windows PE (AMD64)

Requires the following features:

- Deployment Tools

Estimated disk space required: 3.3 GB
Disk space available: 55.9 GB

3. **[Welcome to Boot Environment Builder]** window comes up, then click on [Next].



Welcome to the Boot Environment Builder

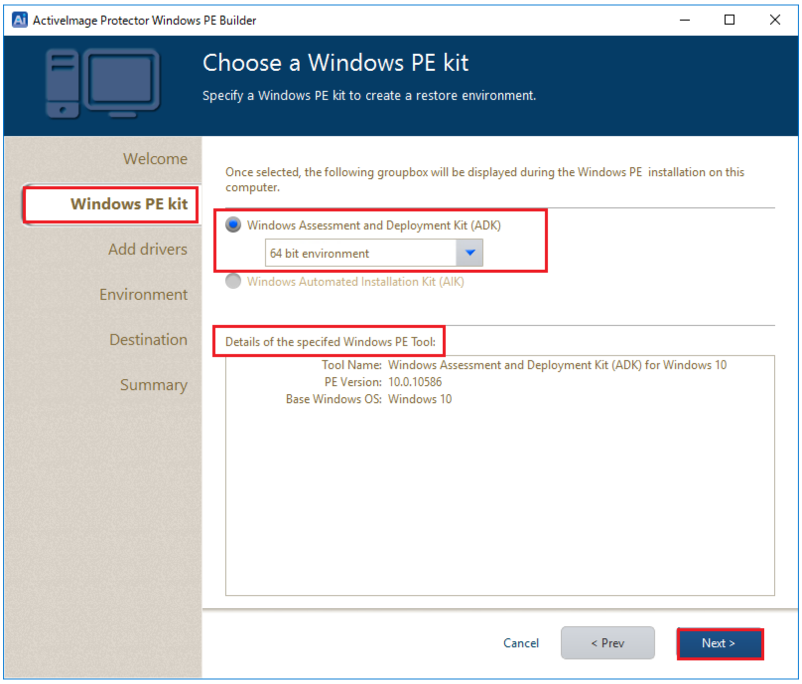
This program, with the Microsoft AIK or ADK creates a Windows PE ISO image that can be used on removable media or in the PreBoot environment.

Build an ActiveImage Protector Windows PE environment

Welcome to the ActiveImage Protector Windows PE builder program.
To create the recovery environment, the Microsoft PE tool kit is required.

□ Don't show this page next time

4. Specify the Windows PE toolkit needed for the installed operating system by clicking the appropriate radio button. The 32-bit version of Windows PE boot environment can be built on 64-bit host. The information of a specific Windows PE toolkit can be displayed. Click **[Next]**.



Choose a Windows PE kit

Specify a Windows PE kit to create a restore environment.

Once selected, the following groupbox will be displayed during the Windows PE installation on this computer.

● Windows Assessment and Deployment Kit (ADK)

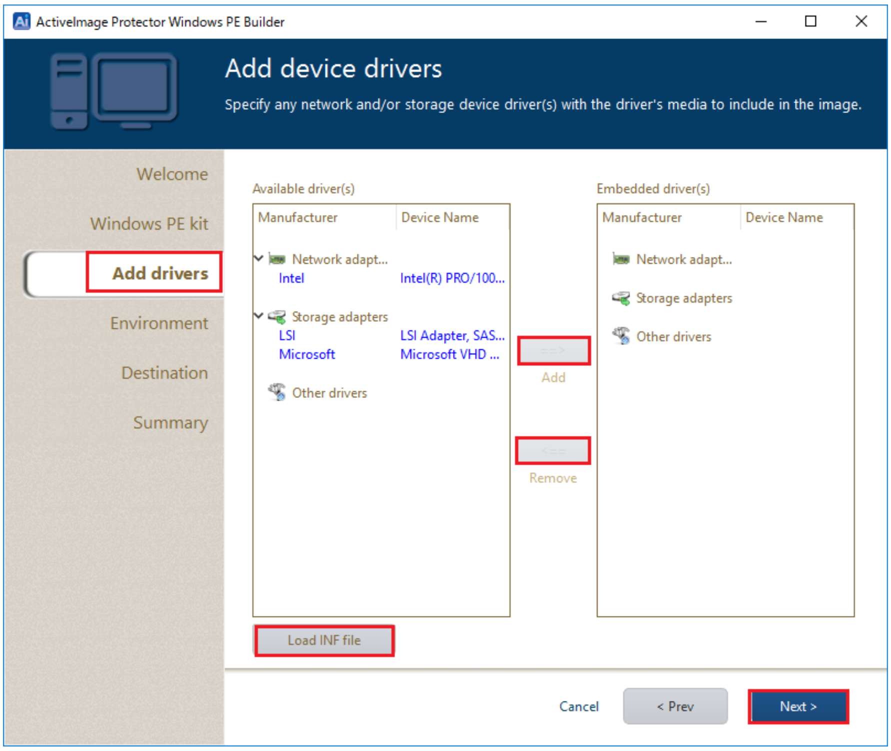
64 bit environment

○ Windows Automated Installation Kit (AIK)

Details of the specifed Windows PE Tool:

Tool Name: Windows Assessment and Deployment Kit (ADK) for Windows 10
PE Version: 10.0.10586
Base Windows OS: Windows 10

5. Specify device driver(s) to include in the boot environment.
   Network and storage device drivers included in the current system are detected and listed on the left pane. Click **[Load INF file]** to add a driver by selecting INF file if the driver is not listed.
   After selecting a driver to add, click on **[==>]** to include the driver in **[Embedded driver(s)]**. To exclude a driver from **[Embedded driver(s)]**, select the driver and click on **[<==]**. Click **[Next]**.
   * Only LAN (Ethernet) driver is supported as network driver.



ActiveImage Protector Windows PE Builder

Add device drivers

Specify any network and/or storage device driver(s) with the driver's media to include in the image.

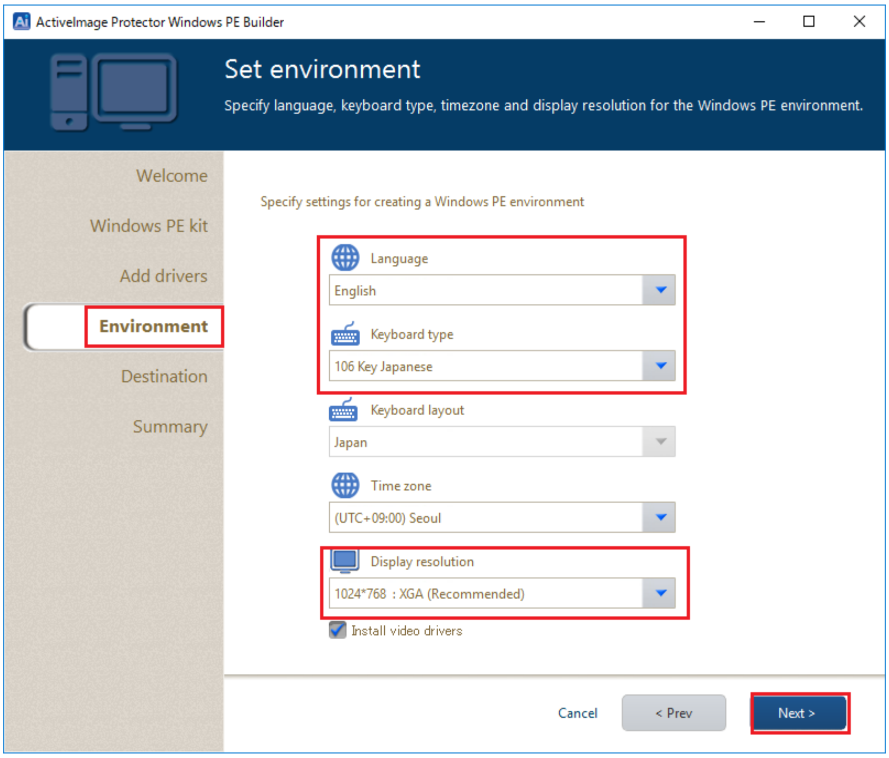
Available driver(s)

Manufacturer	Device Name
Network adapt...	
Intel	Intel(R) PRO/100...
Storage adapters	
LSI	LSI Adapter, SAS...
Microsoft	Microsoft VHD ...
Other drivers	

Embedded driver(s)

Manufacturer	Device Name
Network adapt...	
Storage adapters	
Other drivers	

6. Specify the Language, Keyboard type, Time zone and/or Display resolution for the Windows PE boot environment by selecting the preferred option from the drop-down menu. Click **[Next]**.



ActiveImage Protector Windows PE Builder

Set environment

Specify language, keyboard type, timezone and display resolution for the Windows PE environment.

Specify settings for creating a Windows PE environment

Language: English

Keyboard type: 106 Key Japanese

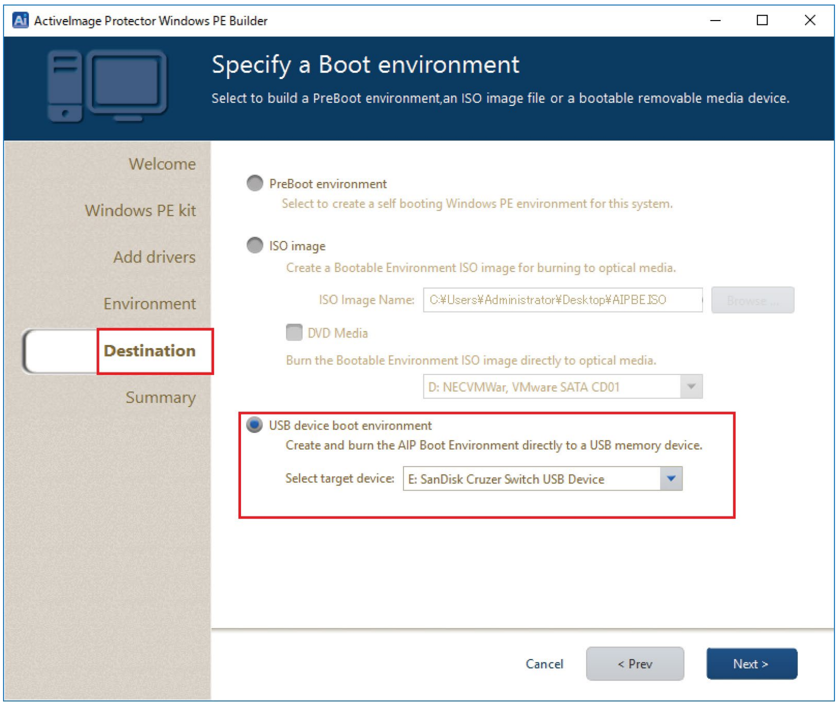
Keyboard layout: Japan

Time zone: (UTC+09:00) Seoul

Display resolution: 1024*768 : XGA (Recommended)

☑ Install video drivers

7. Select the bootable media to build the boot environment.
PreBoot environment - Creates the boot environment in the system volume to boot from the hard disk.
ISO Images - Creates an ISO image file in the specified location. The created ISO file may be burned to DVD media at a later time.
* [DVD media] option is not provided for Windows XP/2003. After creating ISO image, please use a third-party writing software to burn the ISO image to DVD media.
USB device boot environment - Creates boot environment on a USB memory device. The USB media currently connected to the PC may be selected. All data on the selected USB media device will be erased. * [USB device boot environment] option is not provided for Windows XP/2003.
Click **[Next]**.



ActiveImage Protector Windows PE Builder

Specify a Boot environment

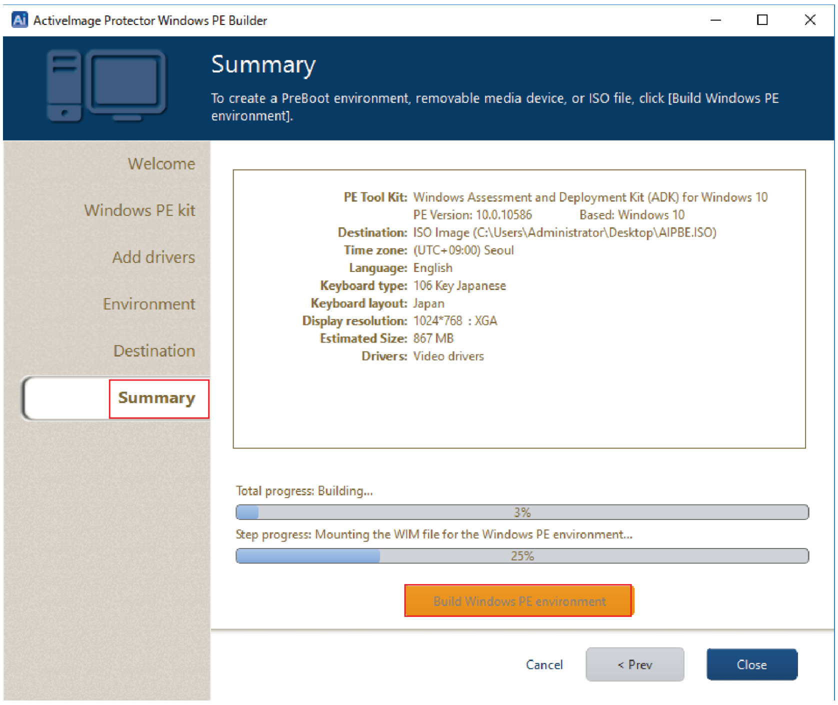
Select to build a PreBoot environment,an ISO image file or a bootable removable media device.

○ PreBoot environment
Select to create a self booting Windows PE environment for this system.

○ ISO image
Create a Bootable Environment ISO image for burning to optical media.
ISO Image Name: C:¥Users¥Administrator¥Desktop¥AIPBE.ISO
□ DVD Media
Burn the Bootable Environment ISO image directly to optical media.
D: NECVMWar, VMware SATA CD01

● USB device boot environment
Create and burn the AIP Boot Environment directly to a USB memory device.
Select target device: E: SanDisk Cruzer Switch USB Device

8. Please review the configured settings.
   Click **[< Prev]** to make changes to previous settings. Click on a node to go back to a specific page. Click on **[Build Windows PE environment]** to display the confirmation message. Click on **[OK]** to start building Windows PE environment. You can monitor the progress in the following window.



ActiveImage Protector Windows PE Builder

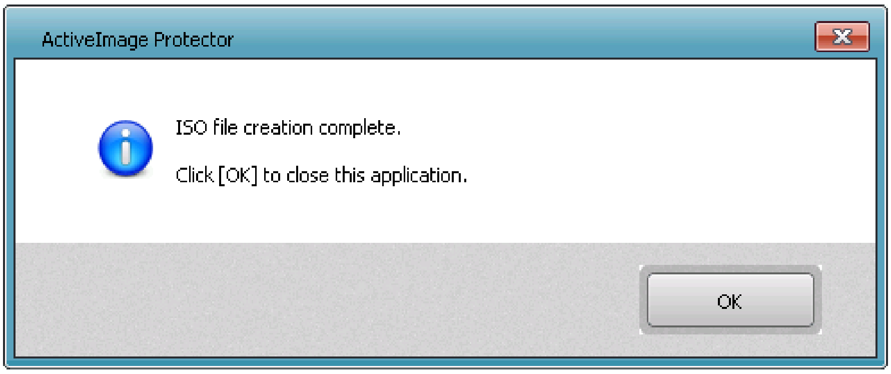
Summary

To create a PreBoot environment, removable media device, or ISO file, click [Build Windows PE environment].

PE Tool Kit: Windows Assessment and Deployment Kit (ADK) for Windows 10
PE Version: 10.0.10586 Based: Windows 10
Destination: ISO Image (C:\Users\Administrator\Desktop\AIPBE.ISO)
Time zone: (UTC+09:00) Seoul
Language: English
Keyboard type: 106 Key Japanese
Keyboard layout: Japan
Display resolution: 1024*768 : XGA
Estimated Size: 867 MB
Drivers: Video drivers

Total progress: Building...
3%
Step progress: Mounting the WIM file for the Windows PE environment...
25%

9. When boot environment creation completes, the following message is displayed. Click on **[OK]** to close the window.



ISO file creation complete.

Click [OK] to close this application.

6. Restore

6-1. File Recovery

A specific file or folder can be restored from a backup image file to a specified location. Please take the following procedures.

1. Start ActiveImage Protector.

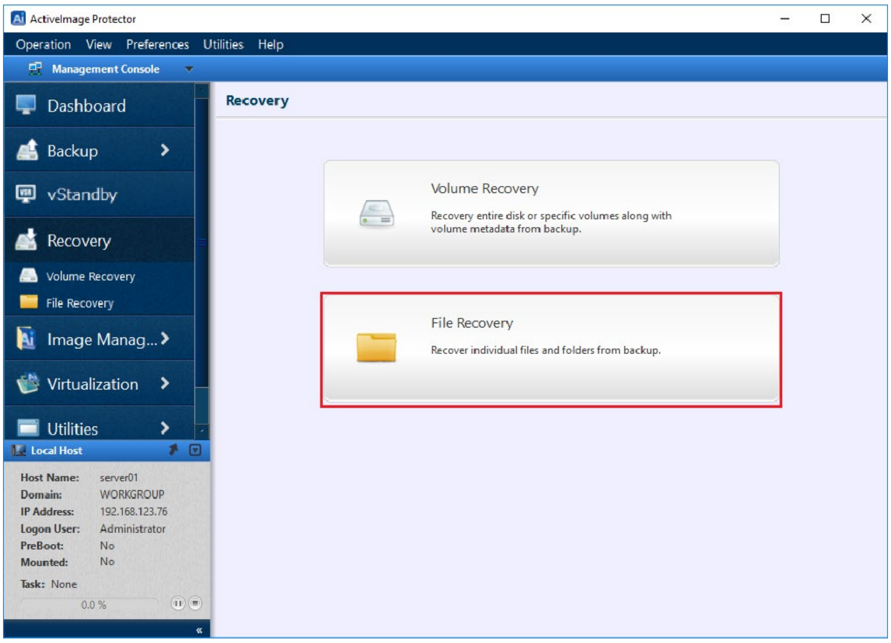
   Windows Server 2008 R2 or earlier server OS:
   Click **[Start]** – **[All Programs]** – **[NetJapan]** – **[ActiveImage Protector]**.

   Windows 7 or earlier Desktop OS:
   Click [Start] – [All Programs] – [NetJapan] – [ActiveImage Protector].

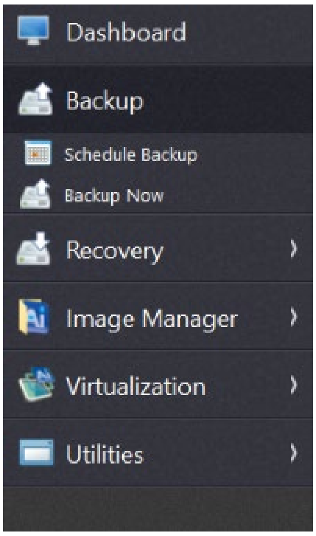
   Windows Server 2012 or later server OS:
   Click [Start] – [Applications] – [NetJapan] – [ActiveImage Protector].

   Windows Server 8 or later Desktop OS :
   Click [Start] – [Applications] – [NetJapan] – [ActiveImage Protector].

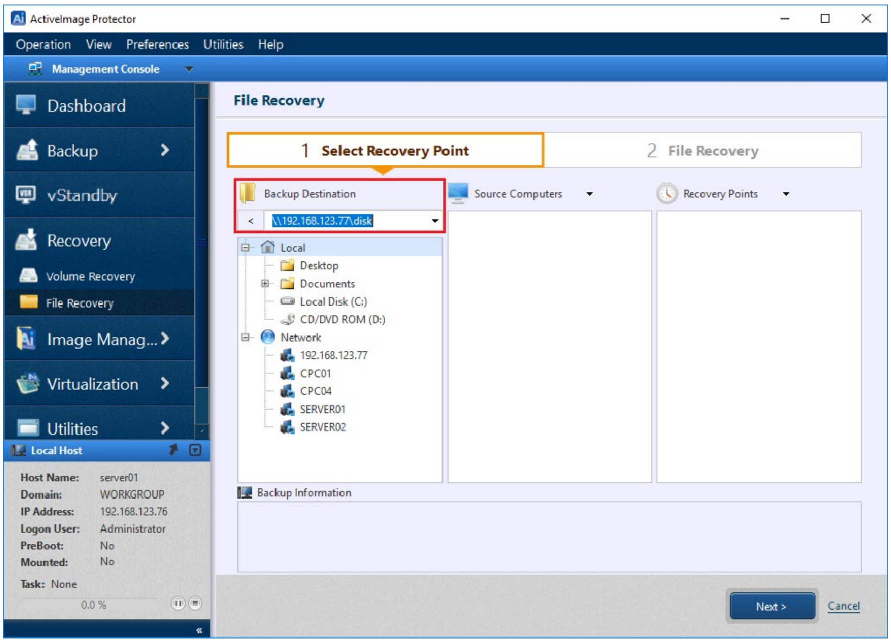
2. Select [Recovery] – [File Recovery].



Note) The left pane of ActiveImage Protector for Hyper-V Enterprise screen is different from the one of Server Edition.



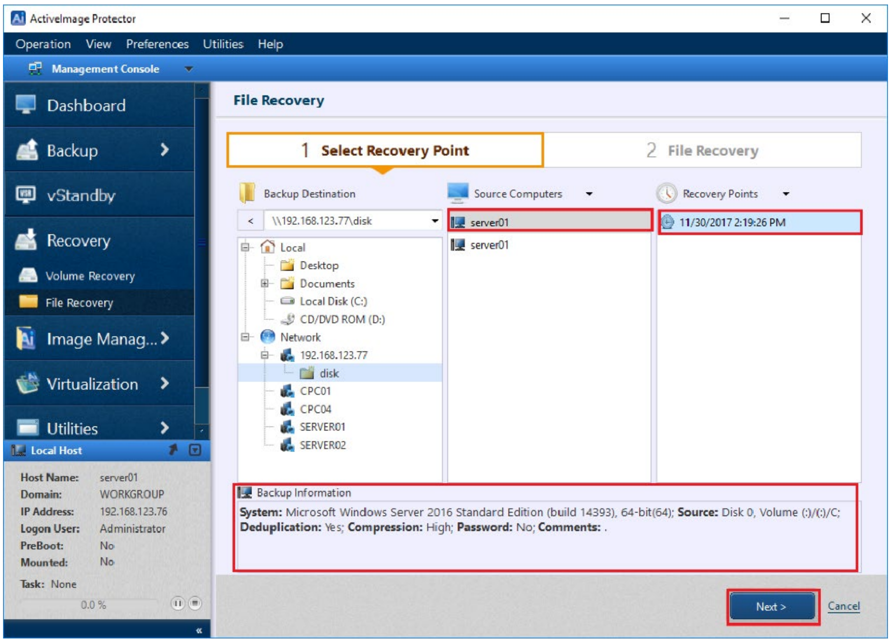
3. Select the backup image file in **[Backup Destination]**. You can specify the path for the destination. This example shows that " \\192.168.123.77\disk " is specified for the destination. Press Enter key.



\\192.168.123.77\disk

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

4. Select the backup source host from the list and recovery point. Click **[Next]**. The information of the selected recovery point (image) is displayed in **[Backup Information]**.



\\192.168.123.77\disk

server01

server01

11/30/2017 2:19:26 PM

System: Microsoft Windows Server 2016 Standard Edition (build 14393), 64-bit(64); **Source:** Disk 0, Volume (:)/(:)/C; **Deduplication:** Yes; **Compression:** High; **Password:** No; **Comments:** .

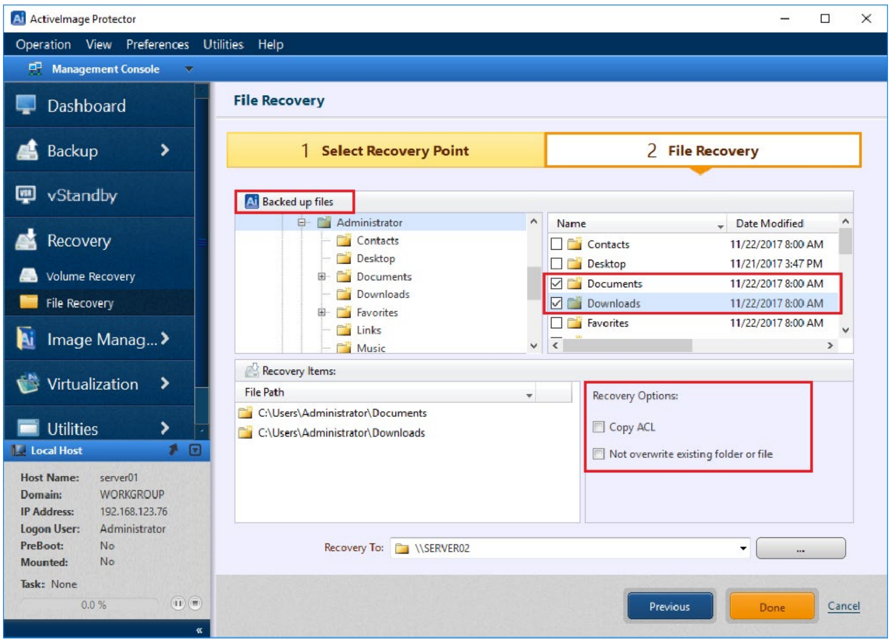
Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

5. Check the checkbox for the items in **[Backed up files]** to restore. The selected items are listed in **[Recovery Items]**.

The following **Recovery Options** may be configured.

・**Copy ACL** - The selected file is restored keeping Access Control List (ACL) configured for restore source file.

・**Not overwrite existing folder or file** – If there already exists a file / folder in the destination, the file / folder is restored under a unique name instead of overwriting the existing file.



Name	Date Modified
□ Contacts	11/22/2017 8:00 AM
□ Desktop	11/21/2017 3:47 PM
☑ Documents	11/22/2017 8:00 AM
☑ Downloads	11/22/2017 8:00 AM
□ Favorites	11/22/2017 8:00 AM

File Path
C:\Users\Administrator\Documents
C:\Users\Administrator\Downloads

Recovery Options:

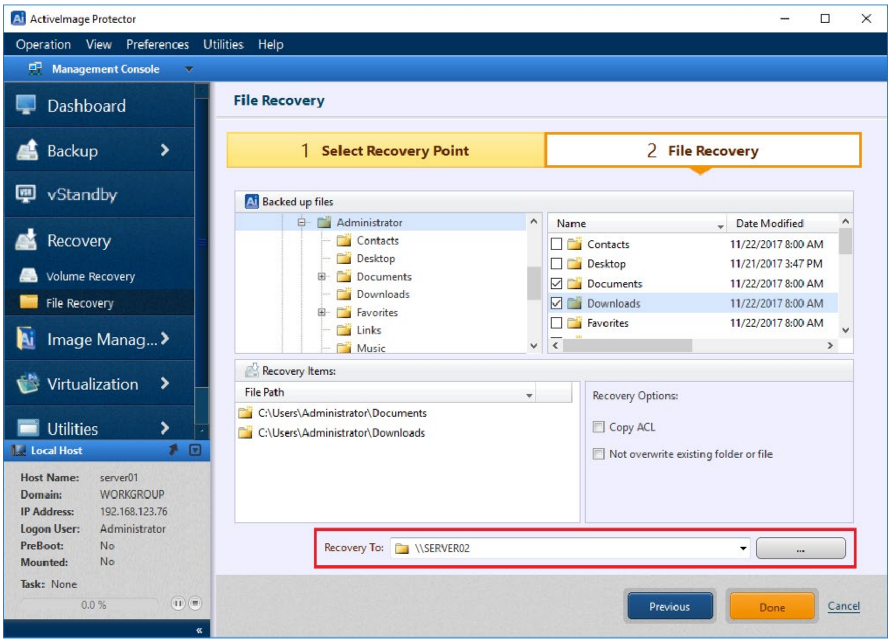
□ Copy ACL

□ Not overwrite existing folder or file

Recovery To: \\SERVER02

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

6. Click [...] (Browse) to select the destination to save the restored item.
   Click [Save].



Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

File Recovery

1 Select Recovery Point | 2 File Recovery

Backed up files

- Administrator
  - Contacts
  - Desktop
  - Documents
  - Downloads
  - Favorites
  - Links
  - Music

Name	Date Modified
□ Contacts	11/22/2017 8:00 AM
□ Desktop	11/21/2017 3:47 PM
☑ Documents	11/22/2017 8:00 AM
☑ Downloads	11/22/2017 8:00 AM
□ Favorites	11/22/2017 8:00 AM

Recovery Items:

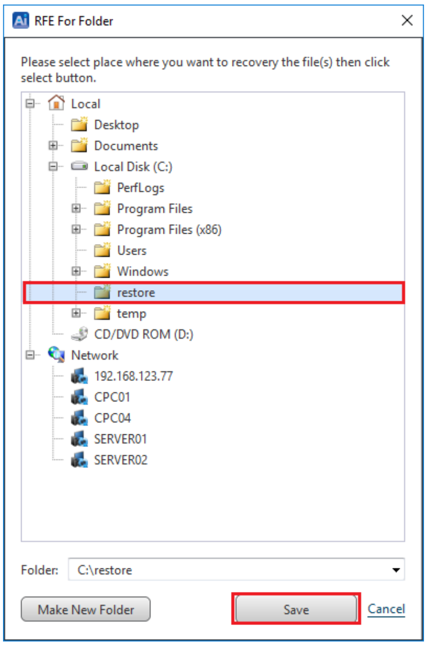
File Path
C:\Users\Administrator\Documents
C:\Users\Administrator\Downloads

Recovery Options:

□ Copy ACL

□ Not overwrite existing folder or file

Recovery To: \\SERVER02 [...]



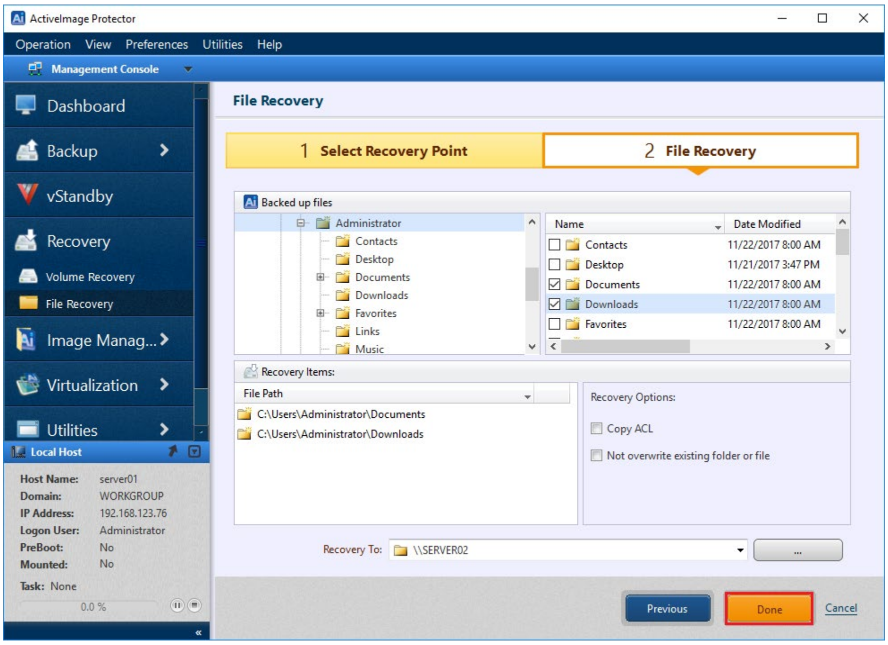
RFE For Folder

Please select place where you want to recovery the file(s) then click select button.

- Local
  - Desktop
  - Documents
  - Local Disk (C:)
    - PerfLogs
    - Program Files
    - Program Files (x86)
    - Users
    - Windows
    - restore
    - temp
  - CD/DVD ROM (D:)
- Network
  - 192.168.123.77
  - CPC01
  - CPC04
  - SERVER01
  - SERVER02

Folder: C:\restore

7. Click [Done] to start the recovery process.



Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

	Name	Date Modified
☐	Contacts	11/22/2017 8:00 AM
☐	Desktop	11/21/2017 3:47 PM
☑	Documents	11/22/2017 8:00 AM
☑	Downloads	11/22/2017 8:00 AM
☐	Favorites	11/22/2017 8:00 AM

File Path:
C:\Users\Administrator\Documents
C:\Users\Administrator\Downloads

☐ Copy ACL
☐ Not overwrite existing folder or file

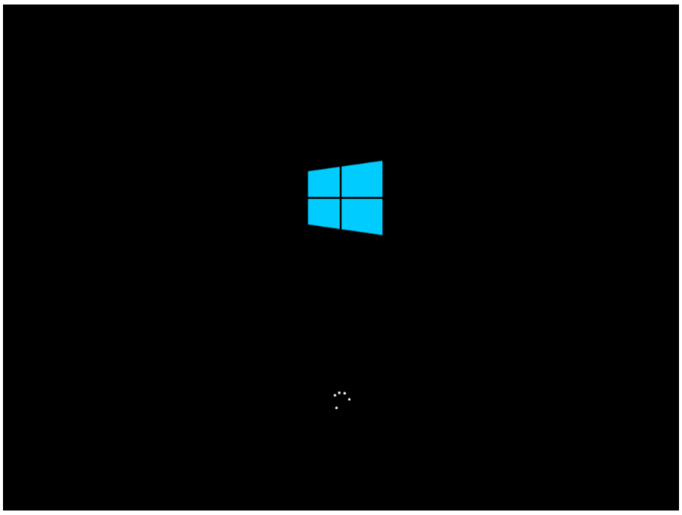
Recovery To: \\SERVER02

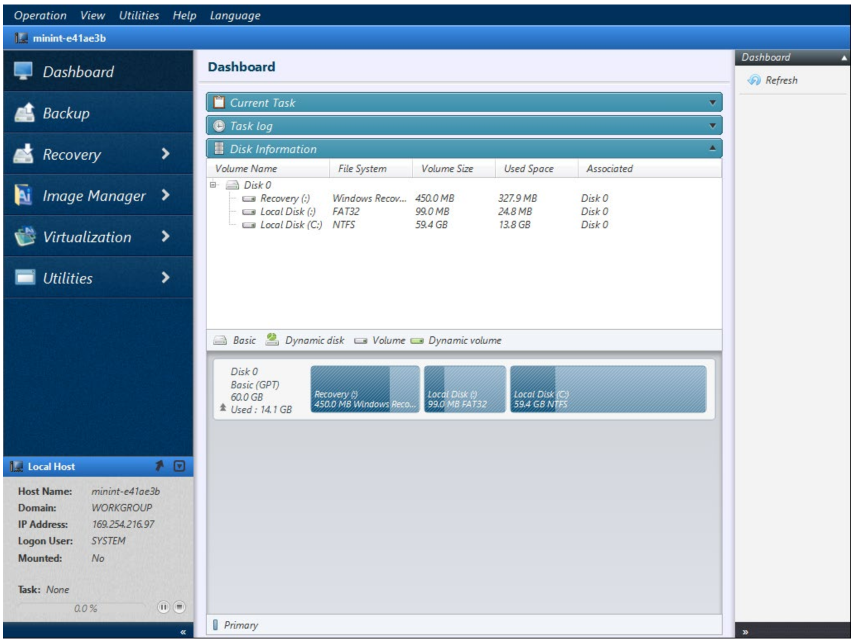
6-2. System Recovery

The following are the operating procedures for system recovery by using boot environment in USB device or optical media built with ActiveImage Protector BE Builder.

Note: Please be aware that, as a result of system recovery, the data stored in local folder are entirely purged.

1. Set the boot media to your machine and boot into the boot environment from the boot media. Please wait until boot environment completely boots up.



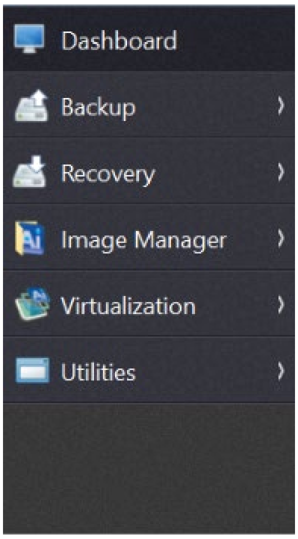


Volume Name	File System	Volume Size	Used Space	Associated
Disk 0				
Recovery (:)	Windows Recov...	450.0 MB	327.9 MB	Disk 0
Local Disk (:)	FAT32	99.0 MB	24.8 MB	Disk 0
Local Disk (C:)	NTFS	59.4 GB	13.8 GB	Disk 0

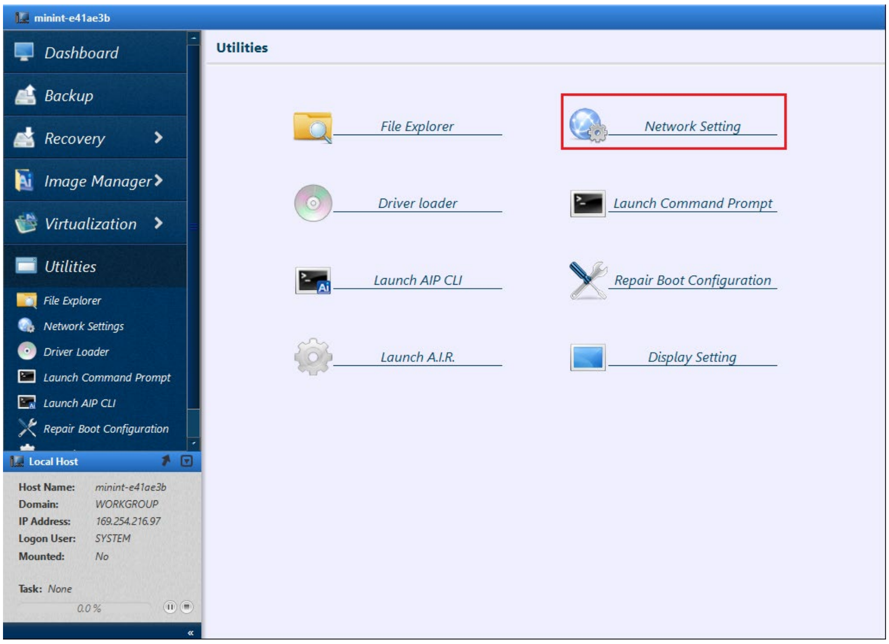
Host Name: minint-e41ae3b
Domain: WORKGROUP
IP Address: 169.254.216.97
Logon User: SYSTEM
Mounted: No

Task: None
0.0 %

Note) The left pane of ActiveImage Protector for Hyper-V Enterprise screen is different from the one of Server Edition.



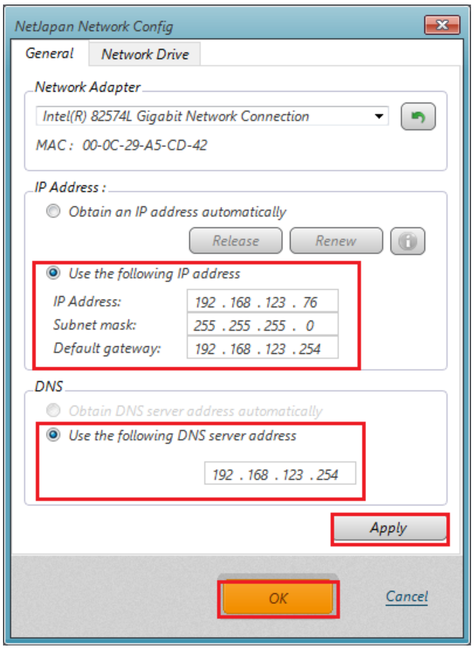
2. Please configure the network settings in order to access the network shared folder specified for the target destination.
   Select **[Utilities] – [Network Setting]**.



Host Name: minint-e41ae3b
Domain: WORKGROUP
IP Address: 169.254.216.97
Logon User: SYSTEM
Mounted: No

Task: None
0.0 %

3. **[NetJapan Network Config]** windows is displayed. This example shows that **[Use the Following IP address]** is selected. Please configure the settings according to your network environment. Specify “192.168.123.76” for **[IP Address:]**, “255.255.255.0” for **[Subnet mask]**, “192.168.123.254” for **[Default gateway]**, Select **[Use the following DNS server address]** and enter “192.168.123.254”. Click **[Apply]** and **[OK]** to complete the settings.

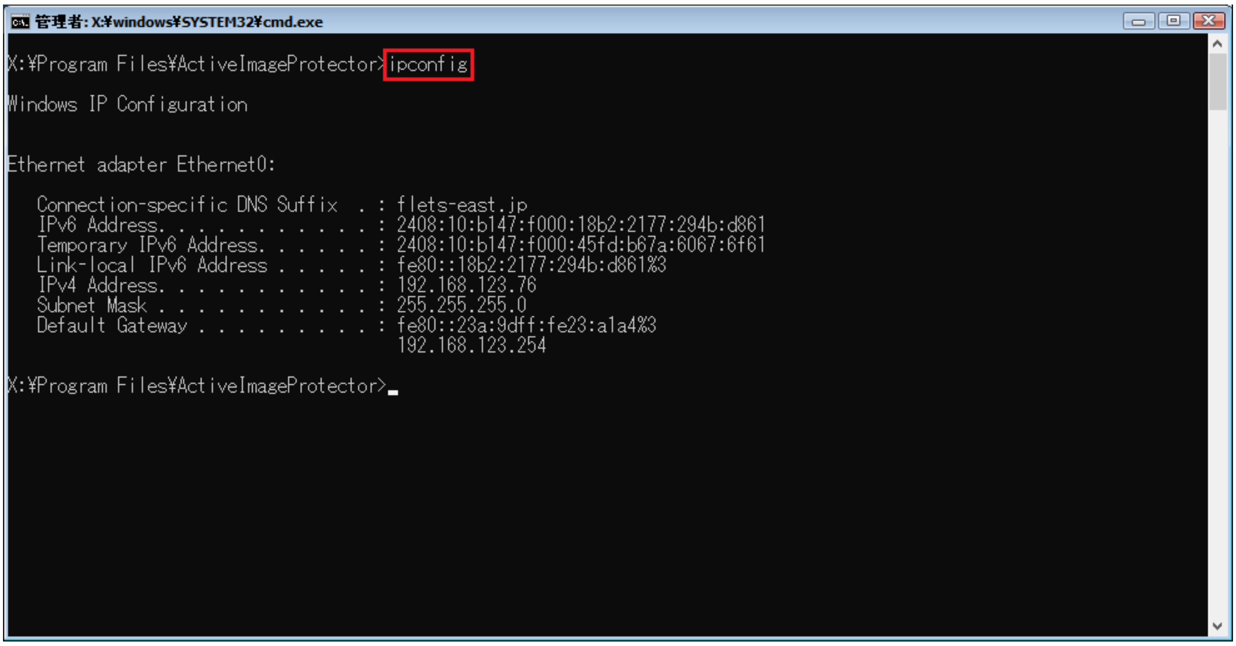


Network Adapter
Intel(R) 82574L Gigabit Network Connection
MAC : 00-0C-29-A5-CD-42

IP Address :
○ Obtain an IP address automatically
● Use the following IP address
IP Address: 192 . 168 . 123 . 76
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 123 . 254

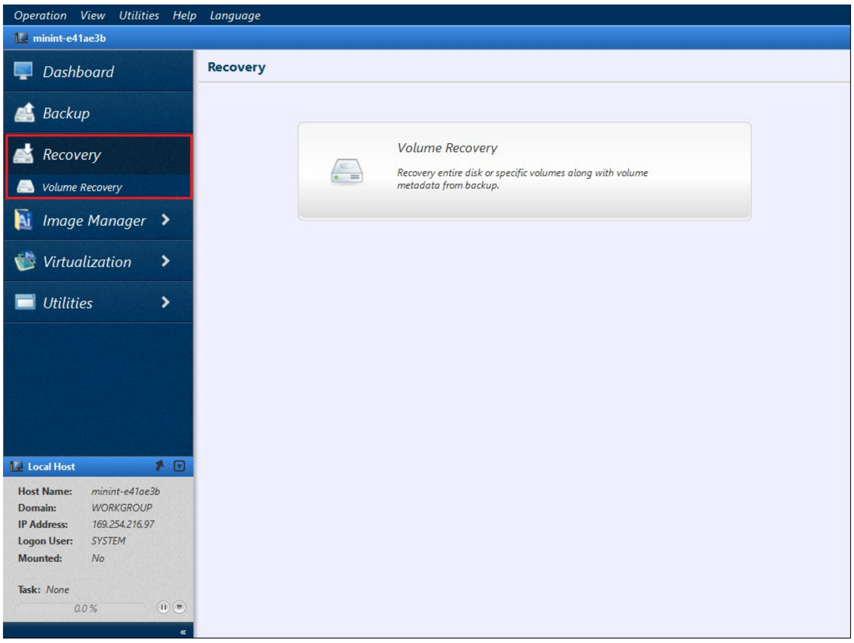
DNS
○ Obtain DNS server address automatically
● Use the following DNS server address
192 . 168 . 123 . 254

4. Go to **[Option]** – **[Launch Command Prompt]** and ensure that the settings such as IP Address are correctly configured. Enter “ipconfig” command and press Enter key. Make sure that the IP address is correctly specified.



```
X:¥Program Files¥ActiveImageProtector>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : flets-east.jp
   IPv6 Address. . . . . . . . . . . : 2408:10:b147:f000:18b2:2177:294b:d861
   Temporary IPv6 Address. . . . . . : 2408:10:b147:f000:45fd:b67a:6067:6f61
   Link-local IPv6 Address . . . . . : fe80::18b2:2177:294b:d861%3
   IPv4 Address. . . . . . . . . . . : 192.168.123.76
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::23a:9dff:fe23:a1a4%3
                                       192.168.123.254

X:¥Program Files¥ActiveImageProtector>_
```

5. Select [Recovery] – [Volume Recovery].

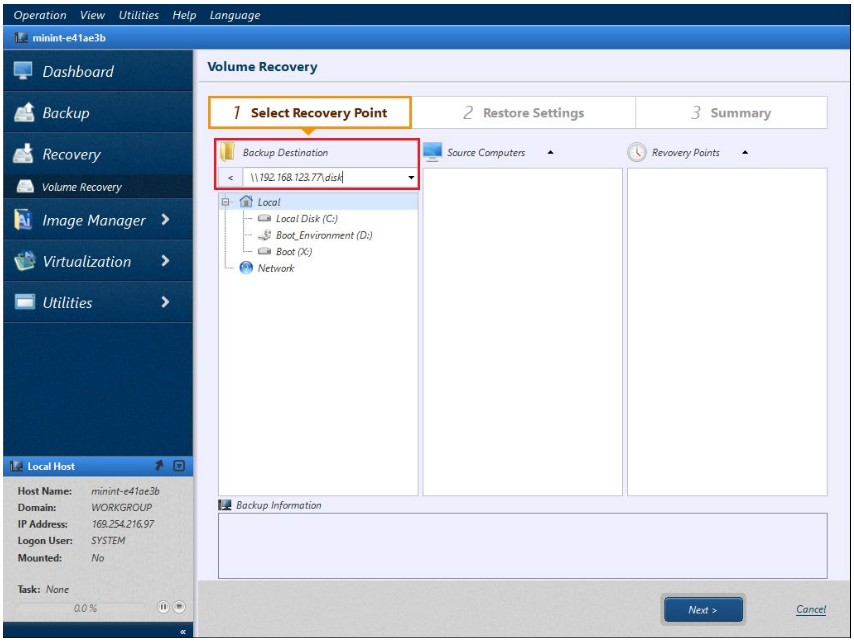


Recovery entire disk or specific volumes along with volume metadata from backup.

Host Name: minint-e41ae3b
Domain: WORKGROUP
IP Address: 169.254.216.97
Logon User: SYSTEM
Mounted: No

Task: None
0.0 %

6. Enter “ \\192.168.123.77\disk ” for **[Backup Destination]** and press Enter key.

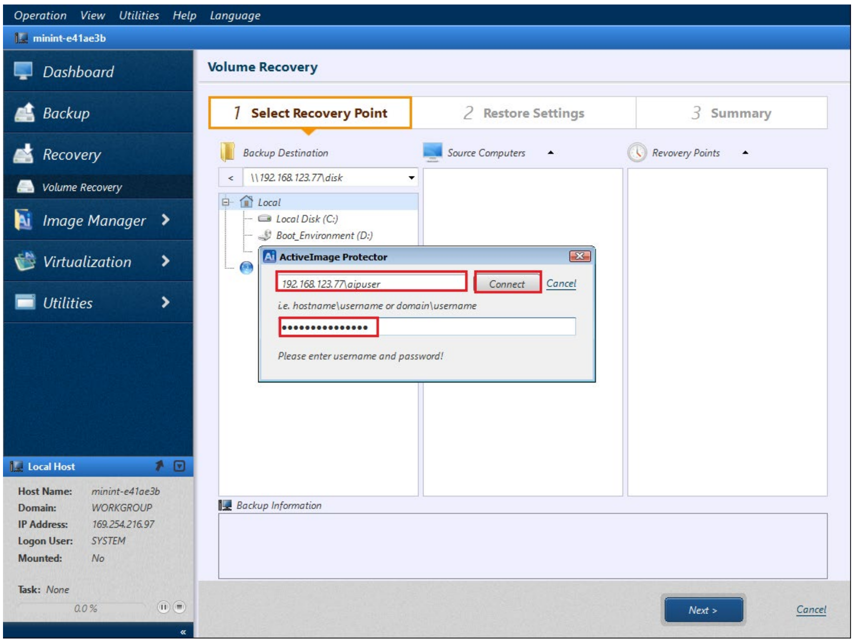


Backup Destination: \\192.168.123.77\disk

Host Name: minint-e41ae3b
Domain: WORKGROUP
IP Address: 169.254.216.97
Logon User: SYSTEM
Mounted: No

Task: None
0.0 %

7. For user authentication, please enter “192.168.123.77\aipuser” for user name and predefined password. Click **[Connect]**.



\\192.168.123.77\disk

192.168.123.77\aipuser

i.e. hostname\username or domain\username

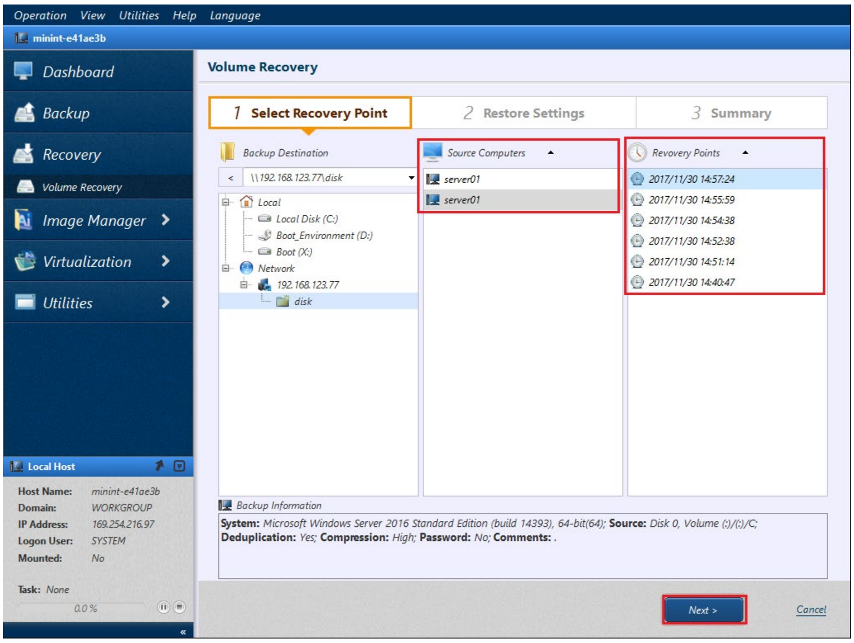
•••••••••••••••

Please enter username and password!

Host Name: minint-e41ae3b
Domain: WORKGROUP
IP Address: 169.254.216.97
Logon User: SYSTEM
Mounted: No

Task: None
0.0 %

8. Select Source Computer and Recovery Point. Click **[Next]**.



\\192.168.123.77\disk

server01
server01

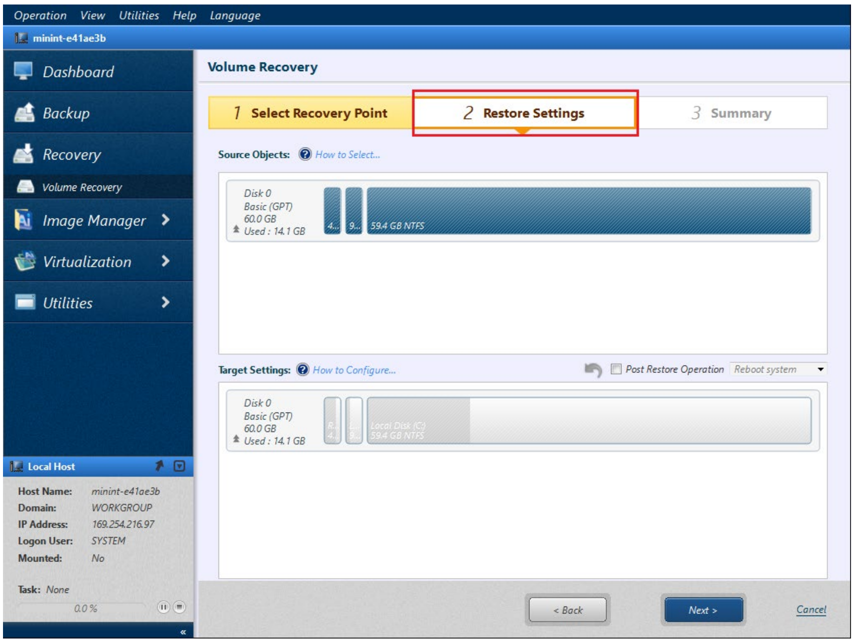
2017/11/30 14:57:24
2017/11/30 14:55:59
2017/11/30 14:54:38
2017/11/30 14:52:38
2017/11/30 14:51:14
2017/11/30 14:40:47

System: Microsoft Windows Server 2016 Standard Edition (build 14393), 64-bit(64); **Source:** Disk 0, Volume (:)/(:)/C; **Deduplication:** Yes; **Compression:** High; **Password:** No; **Comments:** .

Host Name: minint-e41ae3b
Domain: WORKGROUP
IP Address: 169.254.216.97
Logon User: SYSTEM
Mounted: No

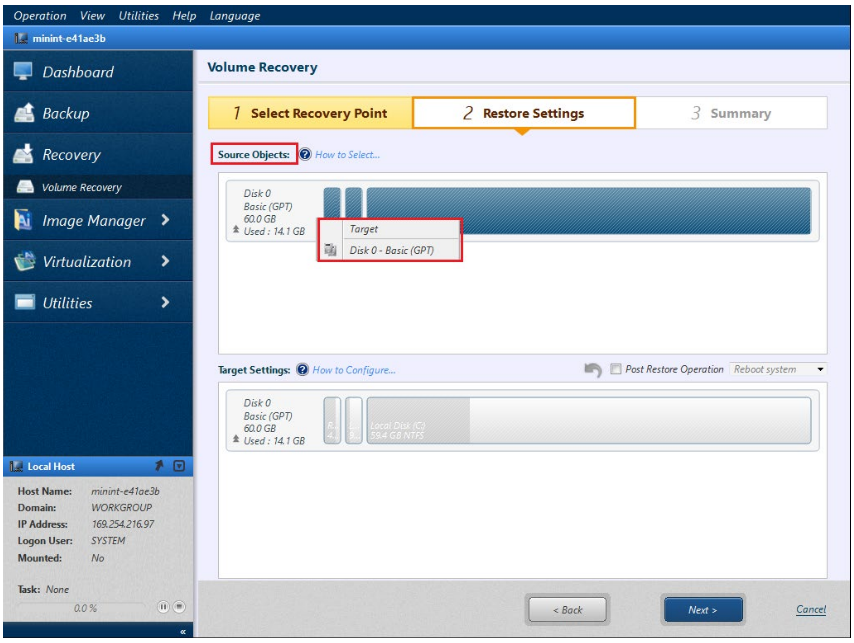
Task: None
0.0 %

9. **[Restore Settings]** window is displayed.



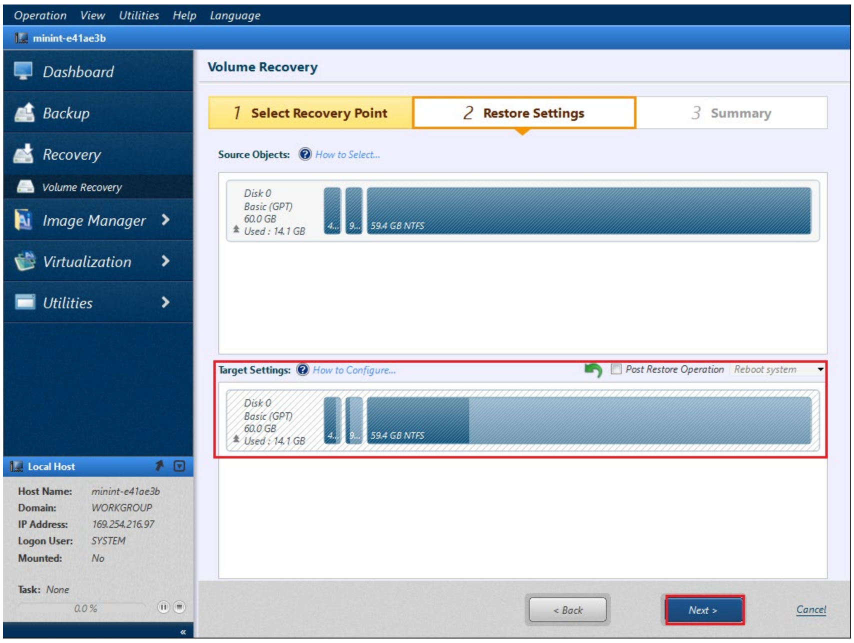
Host Name: minint-e41ae3b
Domain: WORKGROUP
IP Address: 169.254.216.97
Logon User: SYSTEM
Mounted: No
Task: None
0.0 %

10. Right-click on the restore source selected in **[Source Objects]** and select “Disk 0 - Basic (GPT)” for **[Target]**.



Host Name: minint-e41ae3b
Domain: WORKGROUP
IP Address: 169.254.216.97
Logon User: SYSTEM
Mounted: No
Task: None
0.0 %

11. Please review the settings in **[Target Settings]** and click **[Next]**.



Source Objects:

Disk 0
Basic (GPT)
60.0 GB
Used : 14.1 GB
59.4 GB NTFS

Target Settings:

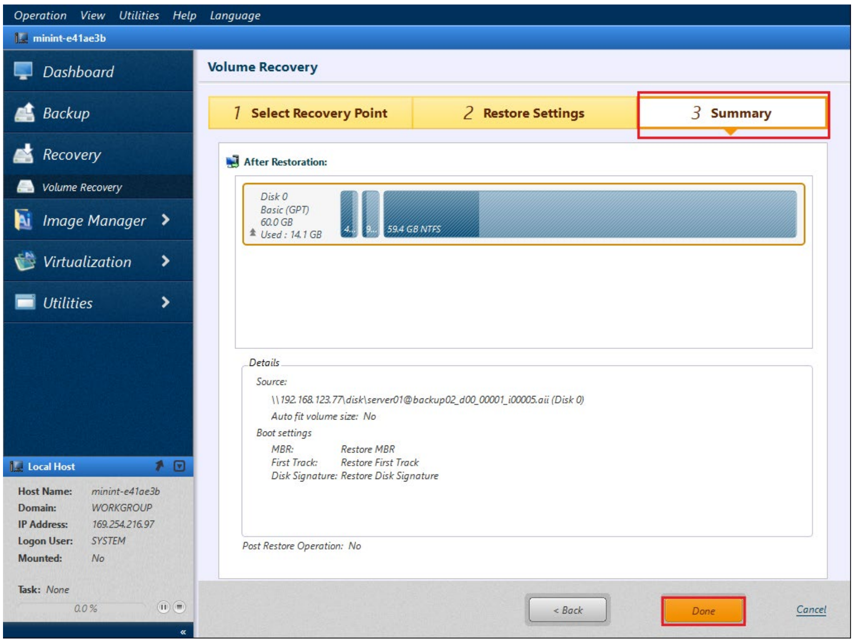
□ Post Restore Operation Reboot system

Disk 0
Basic (GPT)
60.0 GB
Used : 14.1 GB
59.4 GB NTFS

Host Name: minint-e41ae3b
Domain: WORKGROUP
IP Address: 169.254.216.97
Logon User: SYSTEM
Mounted: No

Task: None
0.0 %

12. Review the summary and click **[Done]** to complete.



After Restoration:

Disk 0
Basic (GPT)
60.0 GB
Used : 14.1 GB
59.4 GB NTFS

Details

Source:

\\192.168.123.77\disk\server01@backup02_d00_00001_i00005.aii (Disk 0)

Auto fit volume size: No

Boot settings

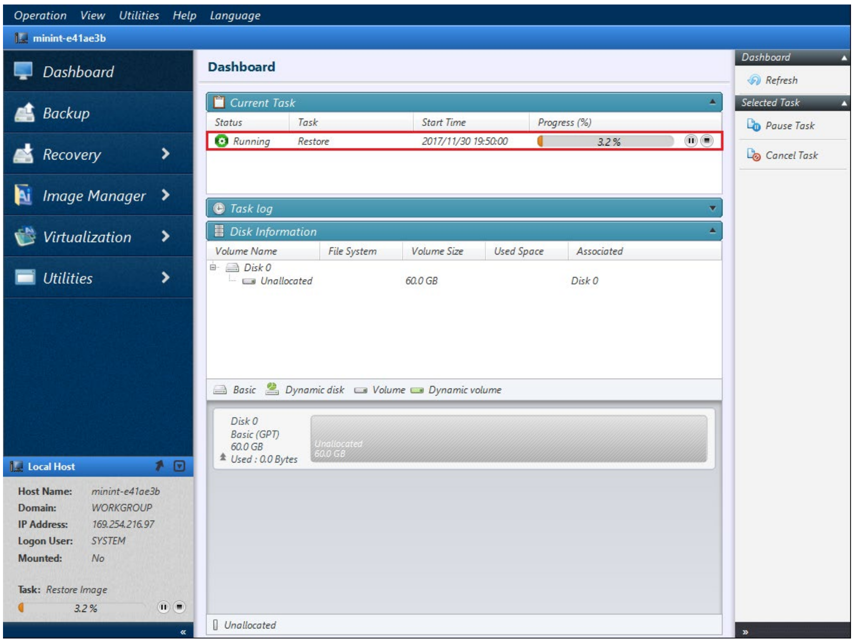
MBR: Restore MBR
First Track: Restore First Track
Disk Signature: Restore Disk Signature

Post Restore Operation: No

Host Name: minint-e41ae3b
Domain: WORKGROUP
IP Address: 169.254.216.97
Logon User: SYSTEM
Mounted: No

Task: None
0.0 %

13. Restore task started.



Status	Task	Start Time	Progress (%)
Running	Restore	2017/11/30 19:50:00	3.2 %

Volume Name	File System	Volume Size	Used Space	Associated
Disk 0				
Unallocated		60.0 GB		Disk 0

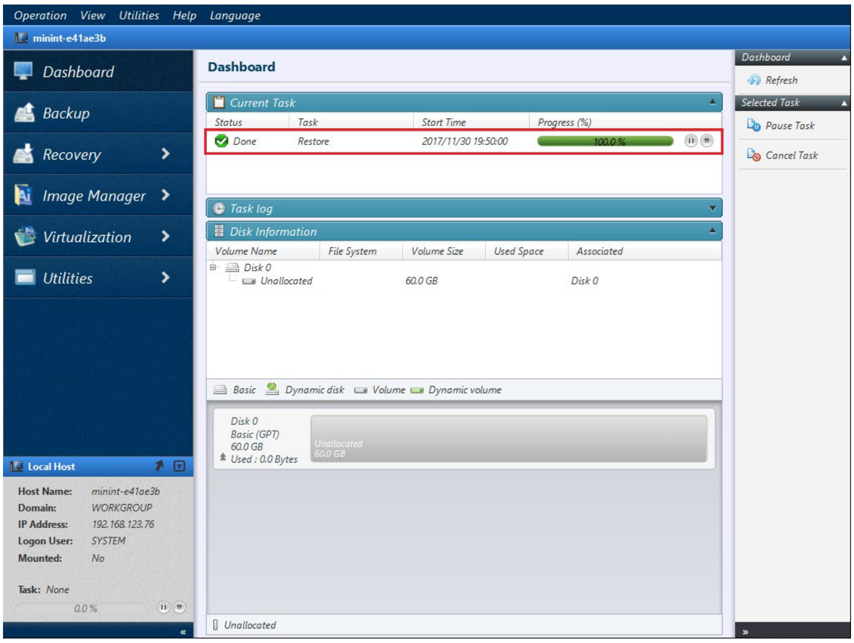
Disk 0
Basic (GPT)
60.0 GB
Used : 0.0 Bytes

Host Name:	minint-e41ae3b
Domain:	WORKGROUP
IP Address:	169.254.216.97
Logon User:	SYSTEM
Mounted:	No

Task: Restore Image
3.2 %

14. When the Progress reaches “100%”, the recovery task completed. Select **[Operation]** – **[End]** to shut down or reboot the machine.

Ensure that the restore task successfully completed.



Status	Task	Start Time	Progress (%)
Done	Restore	2017/11/30 19:50:00	100.0 %

Volume Name	File System	Volume Size	Used Space	Associated
Disk 0				
Unallocated		60.0 GB		Disk 0

Disk 0
Basic (GPT)
60.0 GB
Used : 0.0 Bytes

Host Name:	minint-e41ae3b
Domain:	WORKGROUP
IP Address:	192.168.123.76
Logon User:	SYSTEM
Mounted:	No

Task: None
0.0 %

7. Image Manager

Image Manager tools provide a number of options that provide efficient management of backup image files.

1. Start ActiveImage Protector.

Windows Server 2008 R2 or earlier server OS:
Click **[Start]** – **[All Programs]** – **[NetJapan]** – **[ActiveImage Protector]**.

Windows 7 or earlier Desktop OS:
Click [Start] – [All Programs] – [NetJapan] – [ActiveImage Protector].

Windows Server 2012 or later server OS:
Click [Start] – [Applications] – [NetJapan] – [ActiveImage Protector].

Windows Server 8 or later Desktop OS :
Click [Start] – [Applications] – [NetJapan] – [ActiveImage Protector].

2. Select [Image Manager] - [Image Manager].

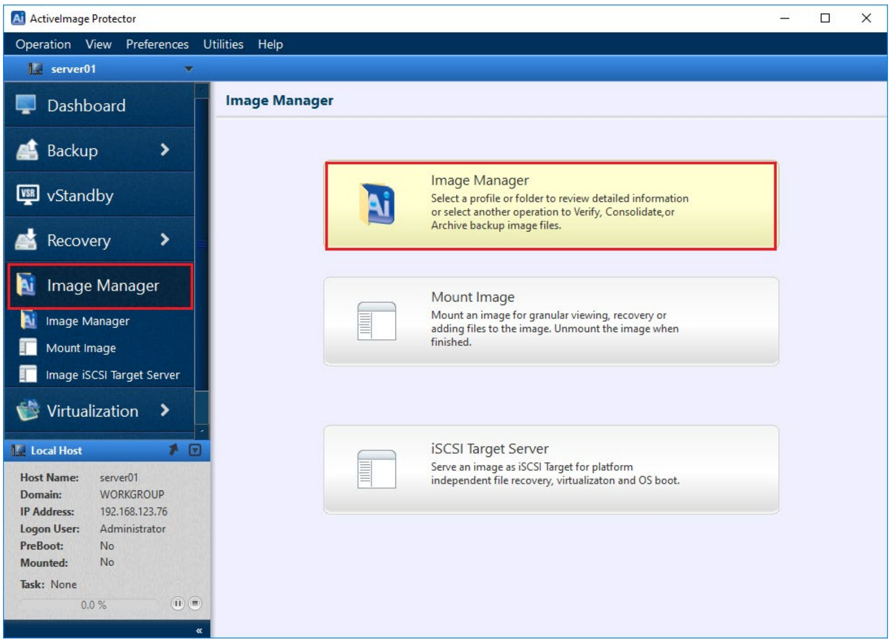
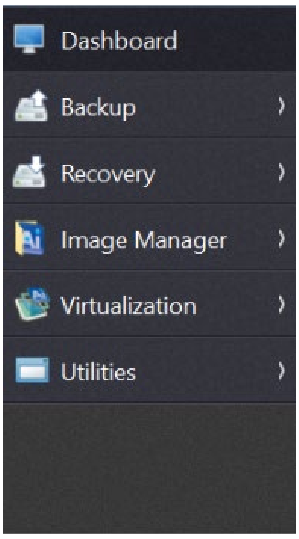


Image Manager
Select a profile or folder to review detailed information or select another operation to Verify, Consolidate,or Archive backup image files.

Mount Image
Mount an image for granular viewing, recovery or adding files to the image. Unmount the image when finished.

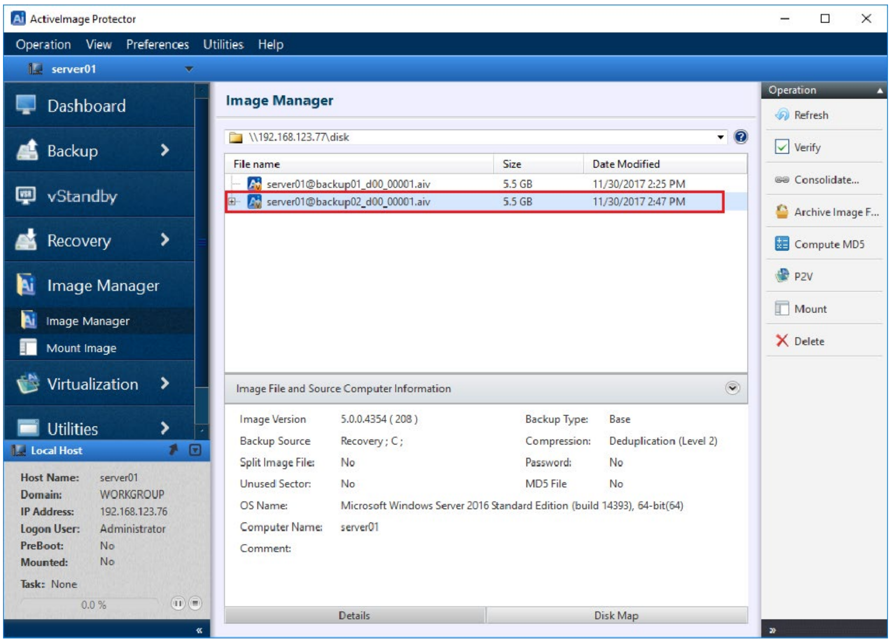
iSCSI Target Server
Serve an image as iSCSI Target for platform independent file recovery, virtualizaton and OS boot.

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %



Note) The left pane of ActiveImage Protector for Hyper-V Enterprise screen is different from the one of Server Edition. There is no “iSCSI Target Server” menu.

3. Select a backup image file.



\\192.168.123.77\disk

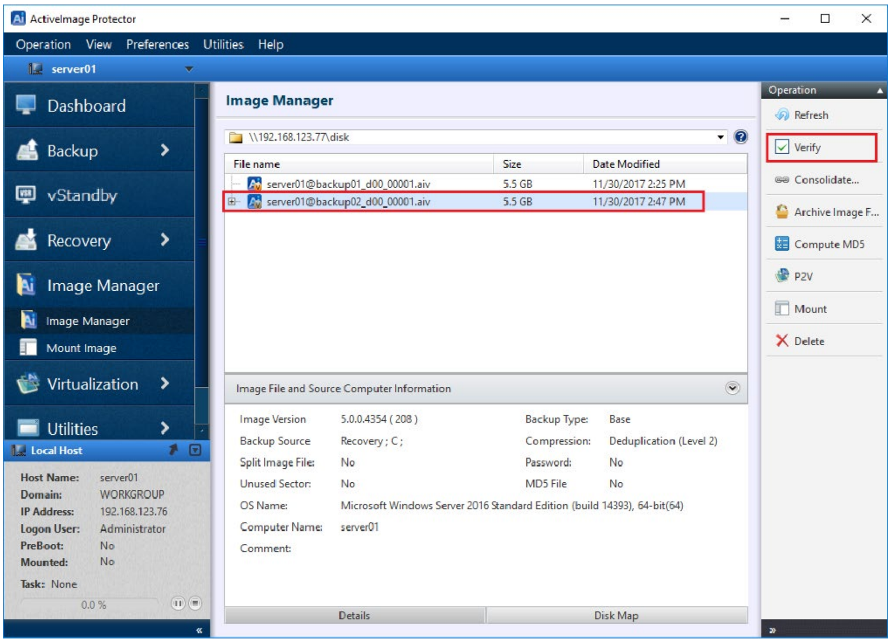
File name	Size	Date Modified
server01@backup01_d00_00001.aiv	5.5 GB	11/30/2017 2:25 PM
server01@backup02_d00_00001.aiv	5.5 GB	11/30/2017 2:47 PM

Image Version	5.0.0.4354 (208)	Backup Type:	Base
Backup Source	Recovery ; C ;	Compression:	Deduplication (Level 2)
Split Image File:	No	Password:	No
Unused Sector:	No	MD5 File	No
OS Name:	Microsoft Windows Server 2016 Standard Edition (build 14393), 64-bit(64)		
Computer Name:	server01		
Comment:			

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

7-1. Verify Image

1. Verify the integrity of a backup image. Select a file then click **[Verify]**.

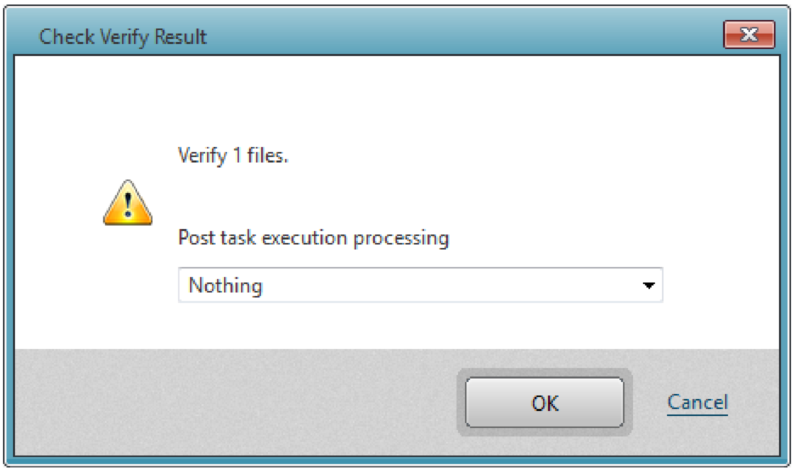


\\192.168.123.77\disk

File name	Size	Date Modified
server01@backup01_d00_00001.aiv	5.5 GB	11/30/2017 2:25 PM
server01@backup02_d00_00001.aiv	5.5 GB	11/30/2017 2:47 PM

Image Version	5.0.0.4354 (208)	Backup Type:	Base
Backup Source	Recovery ; C ;	Compression:	Deduplication (Level 2)
Split Image File:	No	Password:	No
Unused Sector:	No	MD5 File	No
OS Name:	Microsoft Windows Server 2016 Standard Edition (build 14393), 64-bit(64)		
Computer Name:	server01		
Comment:			

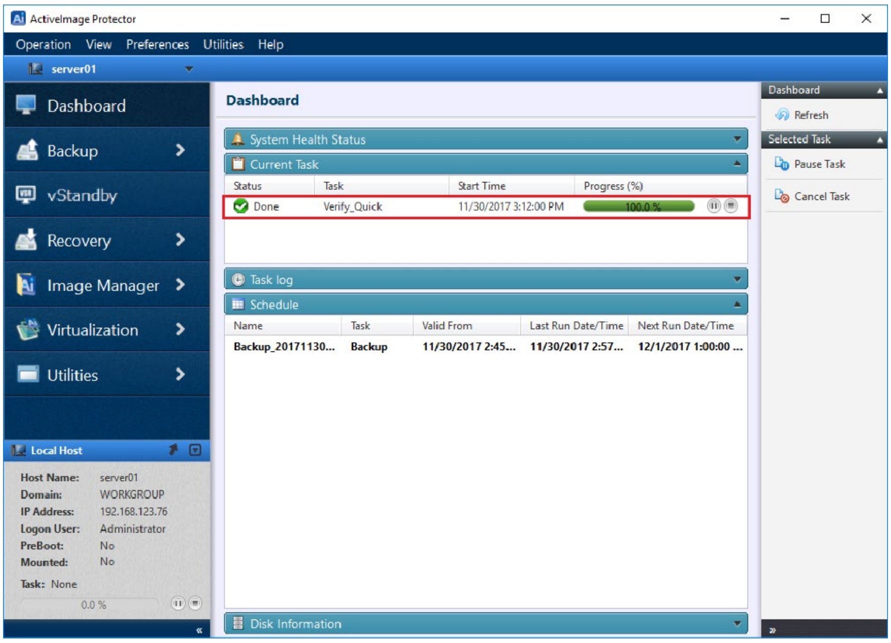
Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %



Verify 1 files.

Post task execution processing: Nothing

2. Upon completion of Verify task, the status and progress are displayed as follows.



Current Task

Status	Task	Start Time	Progress (%)
Done	Verify_Quick	11/30/2017 3:12:00 PM	100.0 %

Schedule

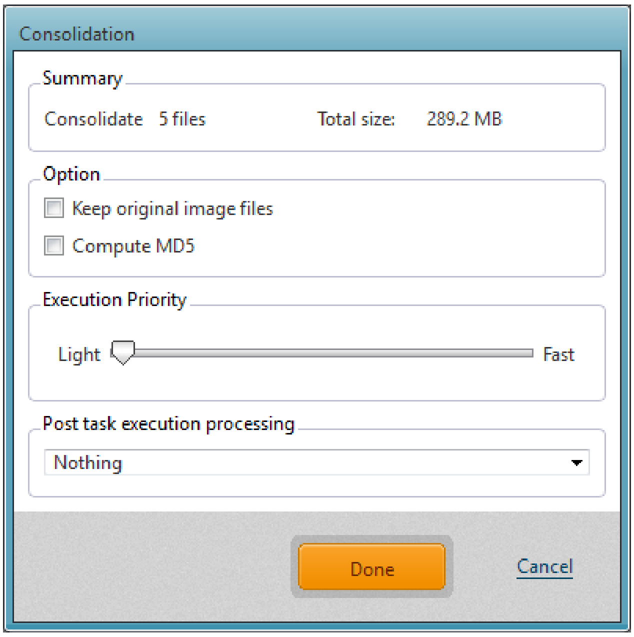
Name	Task	Valid From	Last Run Date/Time	Next Run Date/Time
Backup_20171130...	Backup	11/30/2017 2:45...	11/30/2017 2:57...	12/1/2017 1:00:00 ...

Local Host

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

7-2. Consolidate Image Files

1. Select multiple incremental backup images to consolidate them into a single incremental file. Select the files and click **[Consolidate]** in the right pane.
   You can configure the following option settings.
   Keep original image files - By default, the original image files will be deleted after the consolidated file is created. Check this box to retain the original files.
   Compute MD5 - Check this box to create an MD5 checksum file for the consolidated image file.
   Execution Priority - Depending on the number of processes running on the system, adjust the execution priority for the consolidation process.
   Post task execution processing - Choices included are to **[Reboot]** or **[Shutdown]** once the consolidated file is created.



Consolidation

Summary

Consolidate 5 files Total size: 289.2 MB

Option

□ Keep original image files

□ Compute MD5

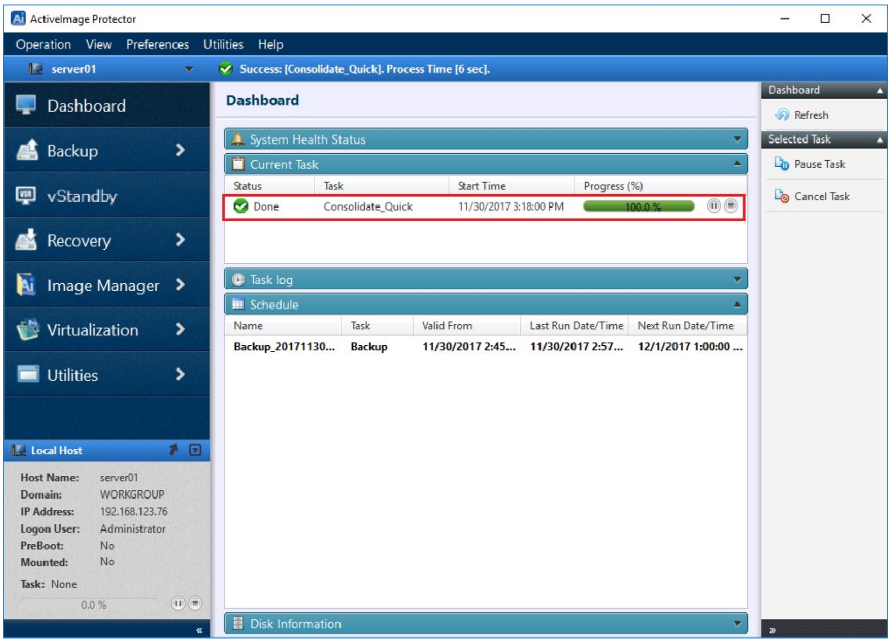
Execution Priority

Light Fast

Post task execution processing

Nothing

2. Upon completion of the consolidation task, the following window is displayed.



ActiveImage Protector

server01

Success: [Consolidate_Quick]. Process Time [6 sec].

Dashboard

Current Task

Status	Task	Start Time	Progress (%)
Done	Consolidate_Quick	11/30/2017 3:18:00 PM	100.0 %

Schedule

Name	Task	Valid From	Last Run Date/Time	Next Run Date/Time
Backup_20171130...	Backup	11/30/2017 2:45...	11/30/2017 2:57...	12/1/2017 1:00:00 ...

Local Host

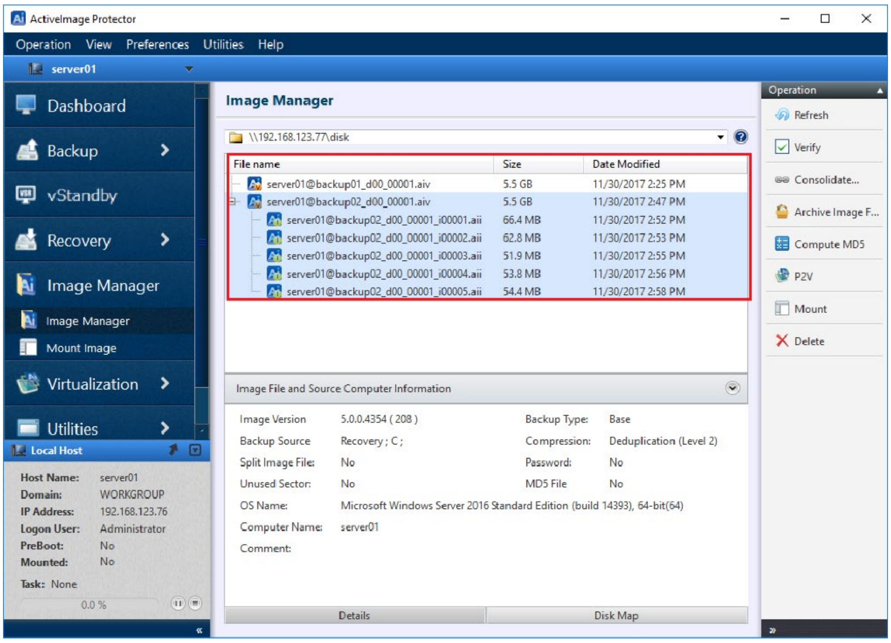
Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No

Task: None

0.0 %

7-3. Archive Backup Image File

1. Archive feature unifies a base image file and an uninterrupted series of incremental files in the same generation set into a full backup file and saves it under a different name. Select a full (base image file) and incremental files from the same generation set.



Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

Image Manager

\\192.168.123.77\disk

File name	Size	Date Modified
server01@backup01_d00_00001.aiv	5.5 GB	11/30/2017 2:25 PM
server01@backup02_d00_00001.aiv	5.5 GB	11/30/2017 2:47 PM
server01@backup02_d00_00001_i00001.aii	66.4 MB	11/30/2017 2:52 PM
server01@backup02_d00_00001_i00002.aii	62.8 MB	11/30/2017 2:53 PM
server01@backup02_d00_00001_i00003.aii	51.9 MB	11/30/2017 2:55 PM
server01@backup02_d00_00001_i00004.aii	53.8 MB	11/30/2017 2:56 PM
server01@backup02_d00_00001_i00005.aii	54.4 MB	11/30/2017 2:58 PM

Image File and Source Computer Information

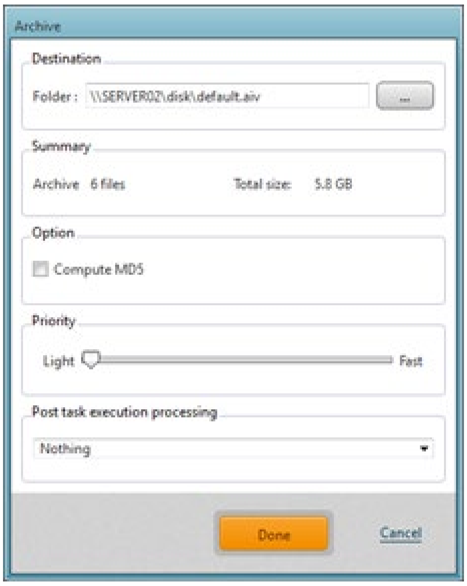
Image Version 5.0.0.4354 (208) Backup Type: Base
Backup Source Recovery ; C ; Compression: Deduplication (Level 2)
Split Image File: No Password: No
Unused Sector: No MD5 File No
OS Name: Microsoft Windows Server 2016 Standard Edition (build 14393), 64-bit(64)
Computer Name: server01
Comment:

2. You can configure the following option settings.

Compute MD5 - Creates an MD5 checksum file for the archived file.

Priority - Depending on the number of processes running on the system, adjust the execution priority for the archiving process.

Post task execution processing - Choices included are to [Reboot] or [Shutdown] once the archived file is created.



Folder : \\SERVER02\disk\default.aiv

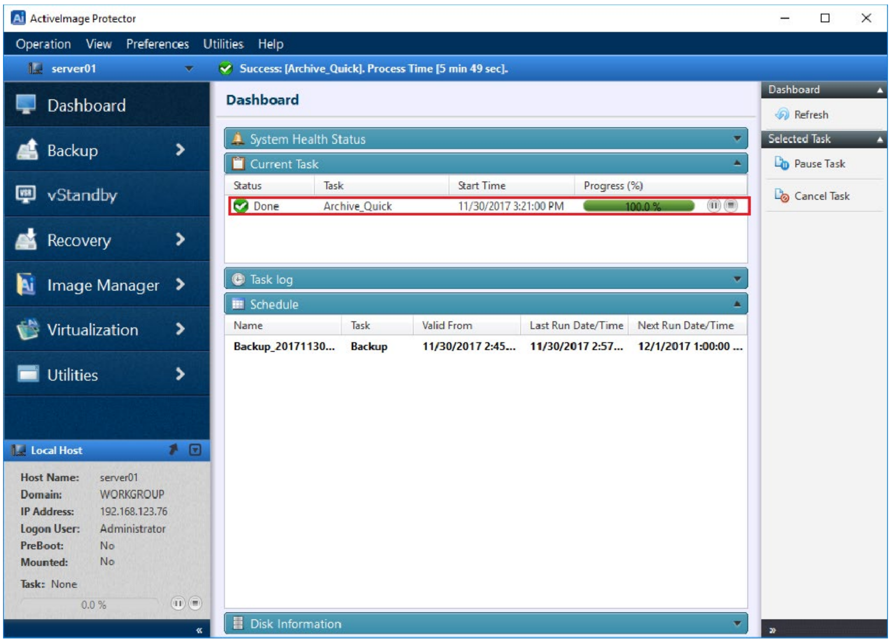
Archive 6 files Total size: 5.8 GB

□ Compute MD5

Light — Fast

Nothing

3. Upon completion of Archive task, the following information is displayed in Dashboard window.



Success: [Archive_Quick]. Process Time [5 min 49 sec].

Status	Task	Start Time	Progress (%)
Done	Archive_Quick	11/30/2017 3:21:00 PM	100.0 %

Name	Task	Valid From	Last Run Date/Time	Next Run Date/Time
Backup_20171130...	Backup	11/30/2017 2:45...	11/30/2017 2:57...	12/1/2017 1:00:00 ...

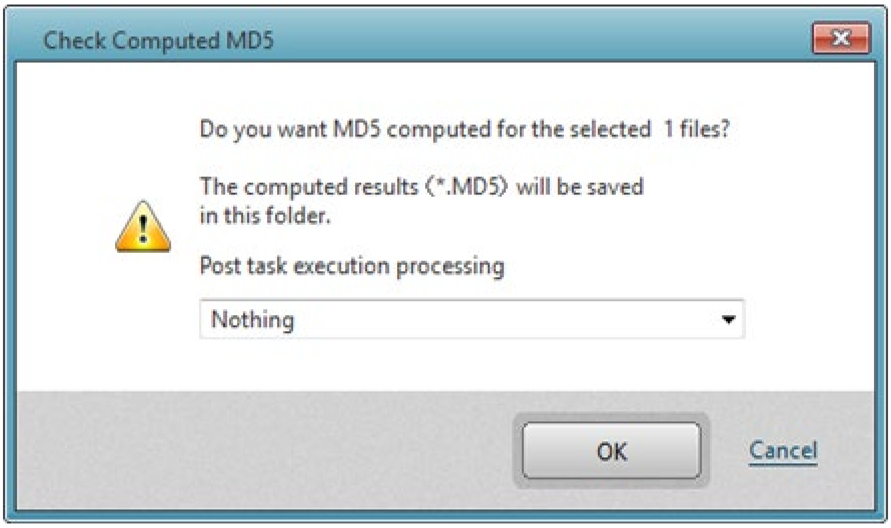
Host Name:	server01
Domain:	WORKGROUP
IP Address:	192.168.123.76
Logon User:	Administrator
PreBoot:	No
Mounted:	No

Task: None

0.0 %

7-4. Compute MD5 hash value

1. Create an MD5 checksum for the selected image file. This can be used as a security measure to check if internal tampering of the image file has occurred in a copy of the image.



Check Computed MD5

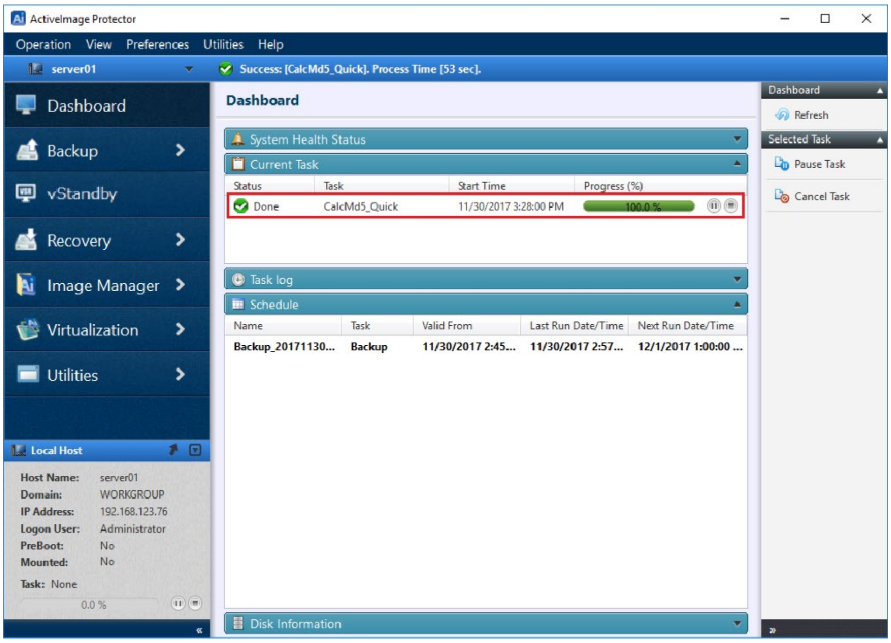
Do you want MD5 computed for the selected 1 files?

The computed results (*.MD5) will be saved in this folder.

Post task execution processing

Nothing

2. Upon completion of computing MD5, the following information is displayed in Dashboard window.



Success: [CalcMd5_Quick]. Process Time [53 sec].

Dashboard

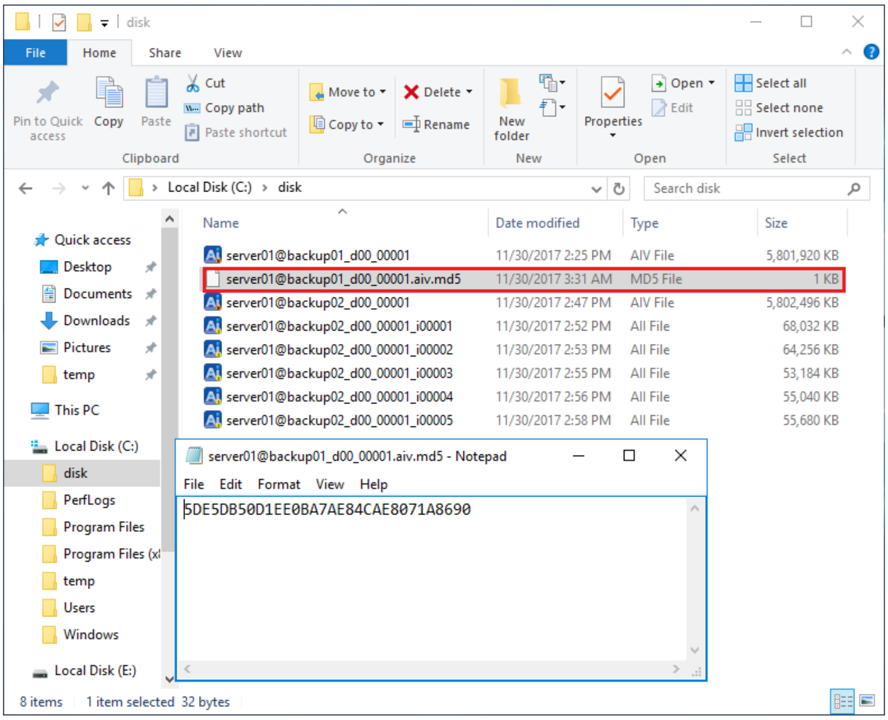
Status	Task	Start Time	Progress (%)
Done	CalcMd5_Quick	11/30/2017 3:28:00 PM	100.0 %

Name	Task	Valid From	Last Run Date/Time	Next Run Date/Time
Backup_20171130...	Backup	11/30/2017 2:45...	11/30/2017 2:57...	12/1/2017 1:00:00 ...

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No

Task: None
0.0 %

3. Please make sure that the MD5 file is created by using Windows Explorer.



Name	Date modified	Type	Size
server01@backup01_d00_00001	11/30/2017 2:25 PM	AIV File	5,801,920 KB
server01@backup01_d00_00001.aiv.md5	11/30/2017 3:31 AM	MD5 File	1 KB
server01@backup02_d00_00001	11/30/2017 2:47 PM	AIV File	5,802,496 KB
server01@backup02_d00_00001_i00001	11/30/2017 2:52 PM	AII File	68,032 KB
server01@backup02_d00_00001_i00002	11/30/2017 2:53 PM	AII File	64,256 KB
server01@backup02_d00_00001_i00003	11/30/2017 2:55 PM	AII File	53,184 KB
server01@backup02_d00_00001_i00004	11/30/2017 2:56 PM	AII File	55,040 KB
server01@backup02_d00_00001_i00005	11/30/2017 2:58 PM	AII File	55,680 KB

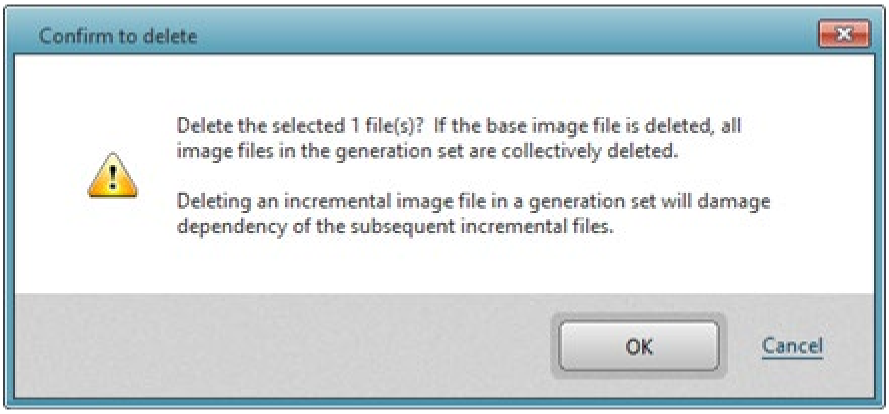
server01@backup01_d00_00001.aiv.md5 - Notepad

```
5DE5DB50D1EE0BA7AE84CAE8071A8690
```

8 items   1 item selected 32 bytes

7-5. Delete

You can select to delete a base or incremental image file(s). Please keep in mind that this type of deletion cannot be undone.



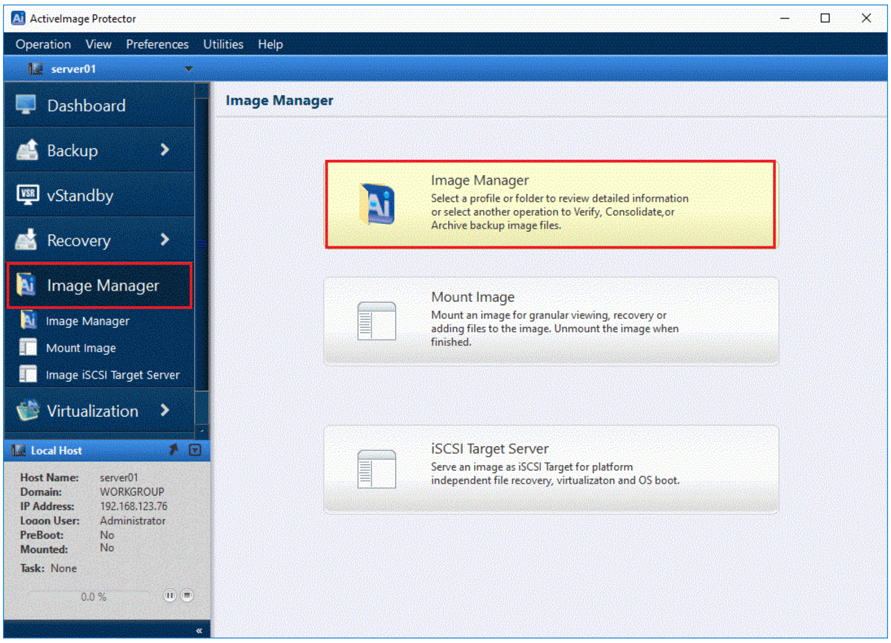
Delete the selected 1 file(s)? If the base image file is deleted, all image files in the generation set are collectively deleted.

Deleting an incremental image file in a generation set will damage dependency of the subsequent incremental files.

7-6. Manually run BootCheck

BootCheck automatically tests to provide confidence that your backup images are bootable. In earlier versions of ActiveImage Protector, BootCheck feature was provided as an option for Post-backup Process (to run the task upon completion of a backup process). ActiveImage Protector Update 4 provides newly enhanced BootCheck enabling you to ensure that backup images are bootable locally or on a remote Hyper-V or ESXi host you specify. Besides, you can now manually configure BootCheck task to run at a specified time.

1. To manually run BootCheck, please select **[Image Manager] - [Image Manager]** in the left menu pane.



Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Loqon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

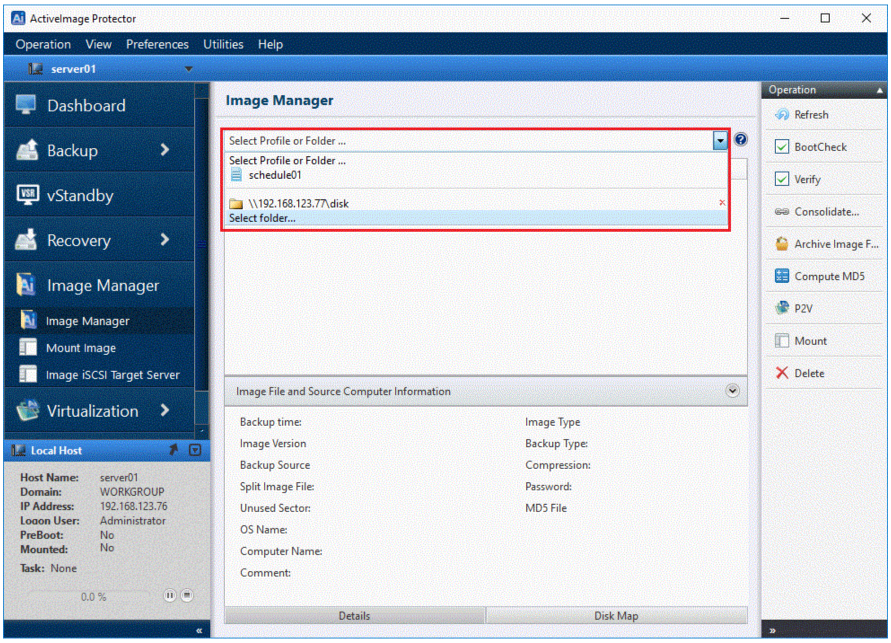
Image Manager

Image Manager
Select a profile or folder to review detailed information or select another operation to Verify, Consolidate,or Archive backup image files.

Mount Image
Mount an image for granular viewing, recovery or adding files to the image. Unmount the image when finished.

iSCSI Target Server
Serve an image as iSCSI Target for platform independent file recovery, virtualizaton and OS boot.

2. **[Image Manager]** window is displayed as follows. Click on [▼] to the right of the the text box at the top of the list.



Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Loqon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

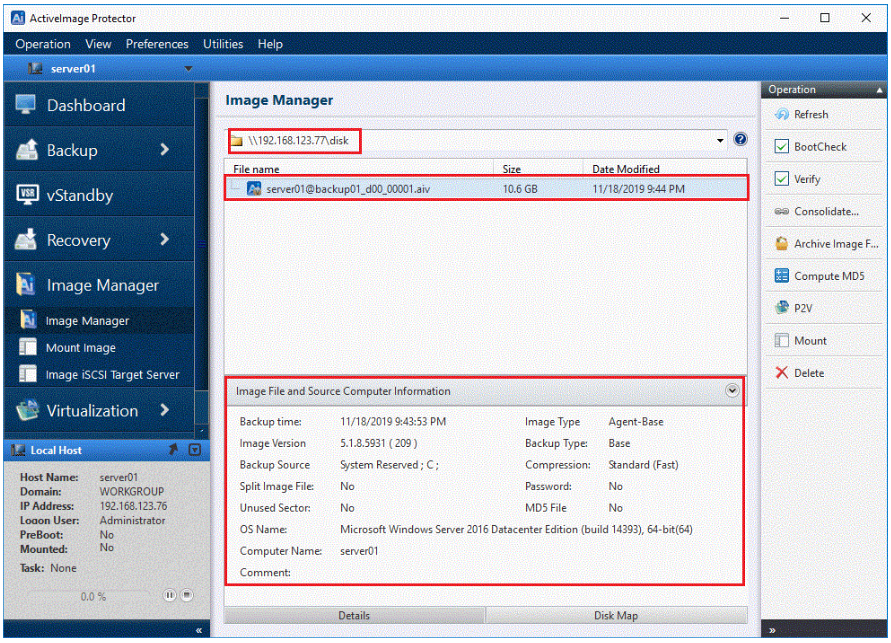
Image Manager

Select Profile or Folder ...
Select Profile or Folder ...
schedule01
\\192.168.123.77\disk
Select folder...

Image File and Source Computer Information

Backup time:
Image Version
Backup Source
Split Image File:
Unused Sector:
OS Name:
Computer Name:
Comment:
Image Type
Backup Type:
Compression:
Password:
MD5 File

3. Select a folder and the backup image files included in the folder are listed. The detailed information of the selected backup image file is shown in the lower pane.



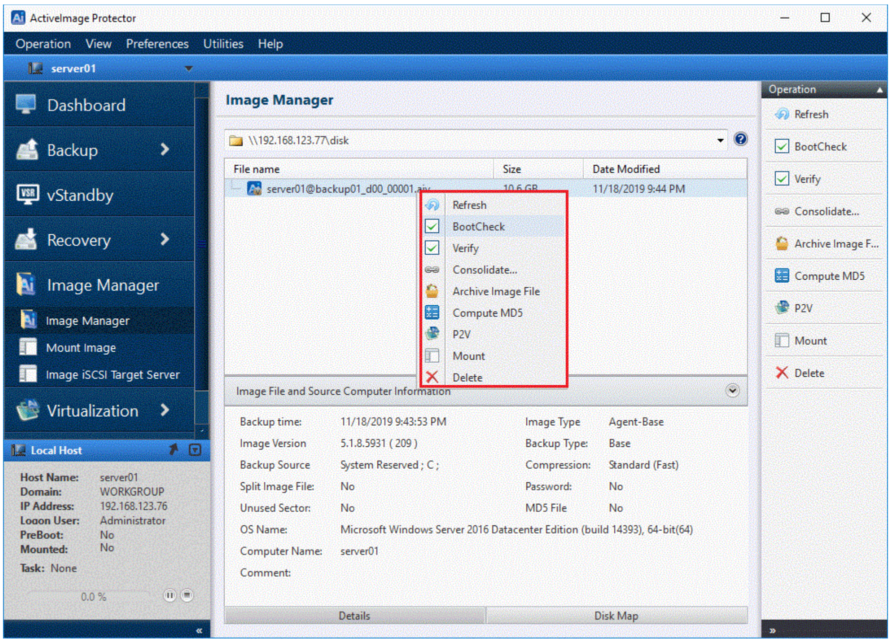
\\192.168.123.77\disk

File name	Size	Date Modified
server01@backup01_d00_00001.aiv	10.6 GB	11/18/2019 9:44 PM

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

Backup time:	11/18/2019 9:43:53 PM	Image Type	Agent-Base
Image Version	5.1.8.5931 (209)	Backup Type:	Base
Backup Source	System Reserved ; C ;	Compression:	Standard (Fast)
Split Image File:	No	Password:	No
Unused Sector:	No	MD5 File	No
OS Name:	Microsoft Windows Server 2016 Datacenter Edition (build 14393), 64-bit(64)		
Computer Name:	server01		
Comment:			

4. Summary of the backup task is displayed. Right-click on a backup image file in the upper pane to display the right-click menu.



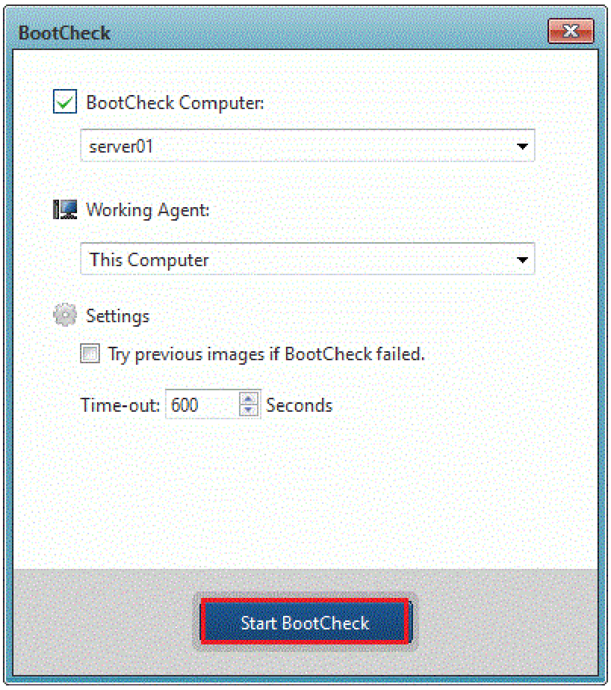
\\192.168.123.77\disk

File name	Size	Date Modified
server01@backup01_d00_00001.aiv	10.6 GB	11/18/2019 9:44 PM

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

Backup time:	11/18/2019 9:43:53 PM	Image Type	Agent-Base
Image Version	5.1.8.5931 (209)	Backup Type:	Base
Backup Source	System Reserved ; C ;	Compression:	Standard (Fast)
Split Image File:	No	Password:	No
Unused Sector:	No	MD5 File	No
OS Name:	Microsoft Windows Server 2016 Datacenter Edition (build 14393), 64-bit(64)		
Computer Name:	server01		
Comment:			

5. Select [BootCheck] in the right-click menu. Review the configured settings and if you do not need to change the setting, click [Start BootCheck] button in the following dialog.



BootCheck

☑ BootCheck Computer:

server01

Working Agent:

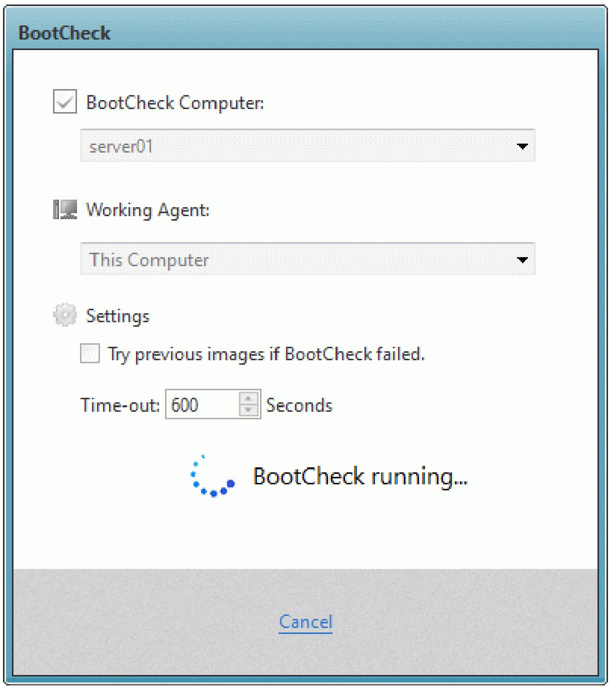
This Computer

Settings

□ Try previous images if BootCheck failed.

Time-out: 600 Seconds

6. BootCheck process starts to ensure that the selected backup image is bootable.



BootCheck

☑ BootCheck Computer:

server01

Working Agent:

This Computer

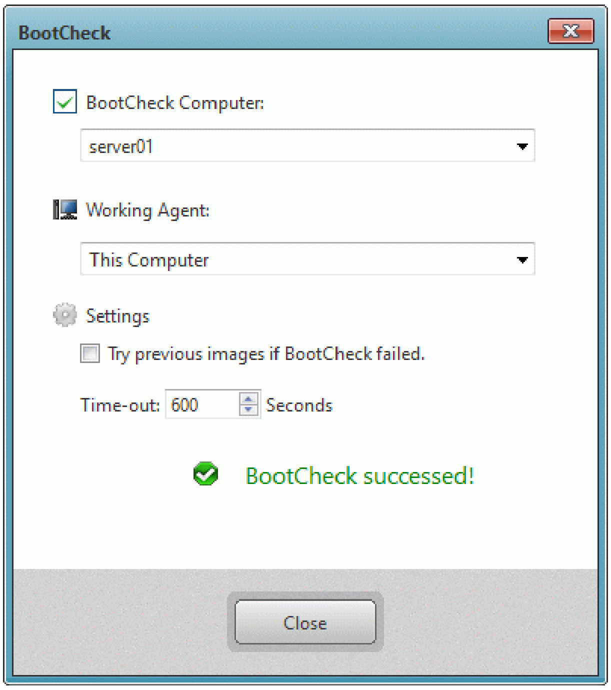
Settings

□ Try previous images if BootCheck failed.

Time-out: 600 Seconds

BootCheck running...

7. Upon successful completion of BootCheck process, you will get the following message.



☑ BootCheck Computer: server01

Working Agent: This Computer

Settings

□ Try previous images if BootCheck failed.

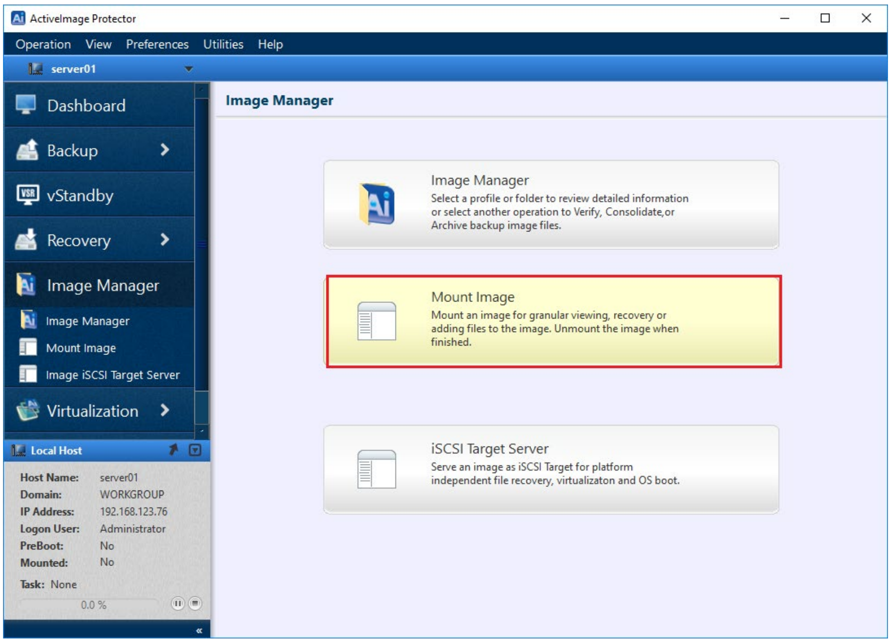
Time-out: 600 Seconds

BootCheck successed!

Manual BootCheck added to Image Manager enables you to check bootability of a backup image file of which bootability is yet to be tested at a specific timing for example right before restoring the backup image.

8. Mount Backup Image

1. Go to [Image Manager] and select [Mount Image].



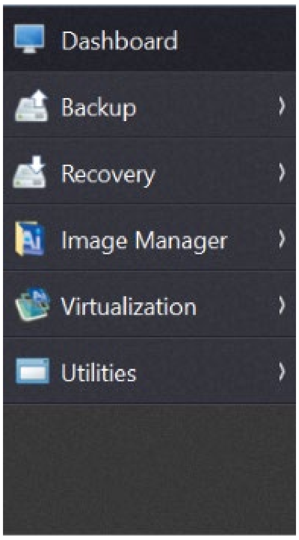
Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

Image Manager
Select a profile or folder to review detailed information or select another operation to Verify, Consolidate,or Archive backup image files.

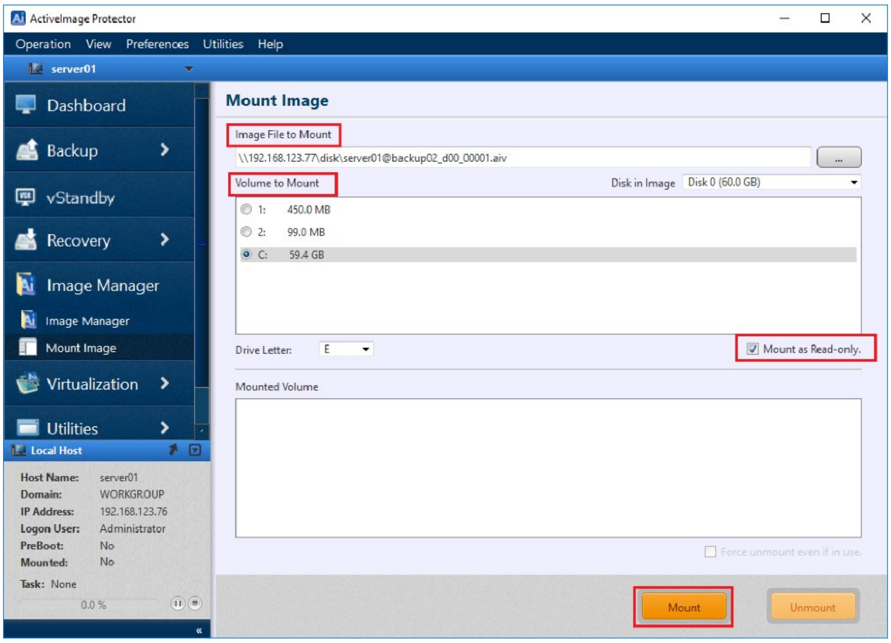
Mount Image
Mount an image for granular viewing, recovery or adding files to the image. Unmount the image when finished.

iSCSI Target Server
Serve an image as iSCSI Target for platform independent file recovery, virtualizaton and OS boot.

Note) The left pane of ActiveImage Protector for Hyper-V Enterprise screen is different from the one of Server Edition. There is no “iSCSI Target Server” menu.



2. Select the backup image to mount. If the selected image includes multiple disks, select a disk.
   Select a volume to mount from the image.
   Specify the drive letter and click **[Mount]**. The image file can be mounted as read-only (default) by selecting the **[Mount as Read-only]** option.



Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

Mount Image

Image File to Mount
\\192.168.123.77\disk\server01@backup02_d00_00001.aiv

Volume to Mount
Disk in Image: Disk 0 (60.0 GB)

○ 1: 450.0 MB
○ 2: 99.0 MB
● C: 59.4 GB

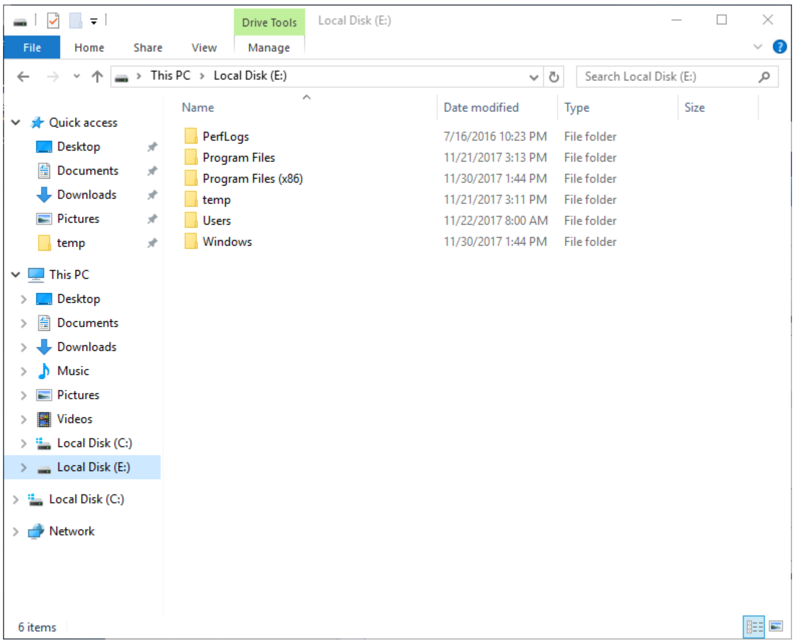
Drive Letter: E

☑ Mount as Read-only.

Mounted Volume

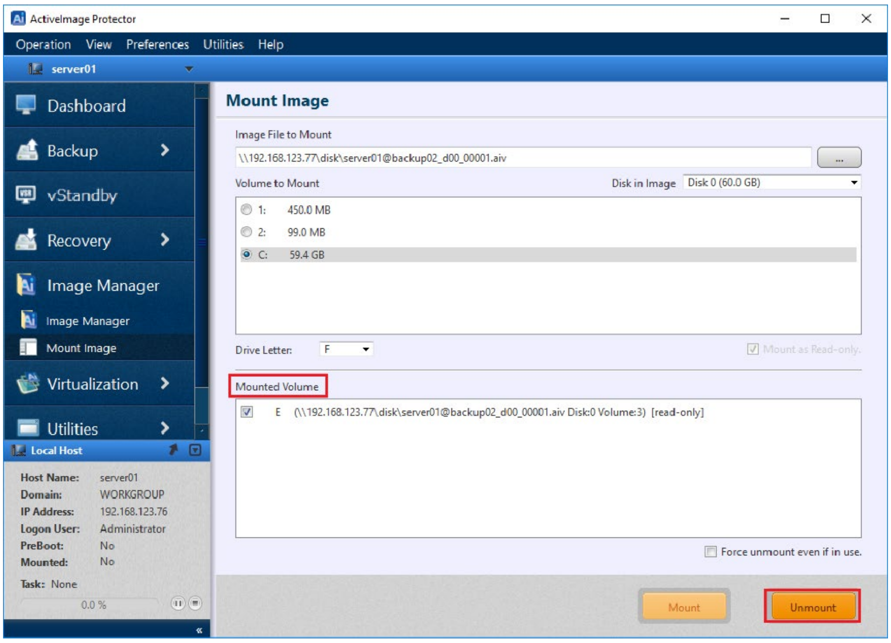
□ Force unmount even if in use.

3. In the mounted image file, you can select and open or copy a file / folder in the same manner as you operate read-only drive in Windows Explorer.



Name	Date modified	Type	Size
PerfLogs	7/16/2016 10:23 PM	File folder	
Program Files	11/21/2017 3:13 PM	File folder	
Program Files (x86)	11/30/2017 1:44 PM	File folder	
temp	11/21/2017 3:11 PM	File folder	
Users	11/22/2017 8:00 AM	File folder	
Windows	11/30/2017 1:44 PM	File folder	

4. To unmount the image file, Select a mount point from the **[Mounted Volume]**. Click **[Unmount]**.



Mount Image

Image File to Mount: \\192.168.123.77\disk\server01@backup02_d00_00001.aiv

Volume to Mount — Disk in Image: Disk 0 (60.0 GB)

○ 1: 450.0 MB
○ 2: 99.0 MB
● C: 59.4 GB

Drive Letter: F

☑ Mount as Read-only

Mounted Volume

☑ E (\\192.168.123.77\disk\server01@backup02_d00_00001.aiv Disk:0 Volume:3) [read-only]

□ Force unmount even if in use.

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

*Uncheck **[Mount as Read-only]** option to mount the image file as writable. The changes made to the image file are saved in a differential image file (.aix) after the volume is unmounted.

9. Image Management –iSCSI Target Server

Networked data storage (Network Attached Storage) includes SAN (Storage Area Network), NAS (Network Attached Storage), etc. FC-SAN (Fibre Channel Storage Area Network) provides high-speed data communication. However, they are expensive in cost and complex to configure and manage.

In the meantime, iSCSI contributes to solve those problems. iSCSI provides direct access to storage devices over network and TCP/IP packet transmission carrying SCSI commands and data. The use of your IP connectivity enables to freely configure iSCSI targets. iSCSI targets may be recognized and utilized to serve as a local drive. It may consume extra CPU resources and increase the load on the network. However, the advantages are that iSCSI targets can be freely deployed in your system environment and the existing network devices can be used without modification.

ActiveImage Protector Update 4 provides a new feature to utilize any backup image file serving as an iSCSI target.

9-1. Mount Backup Files to Local Disk

1. Select **[Image manager]** – **[Image iSCSI Target Server]** in the left menu in ActiveImage Protector.

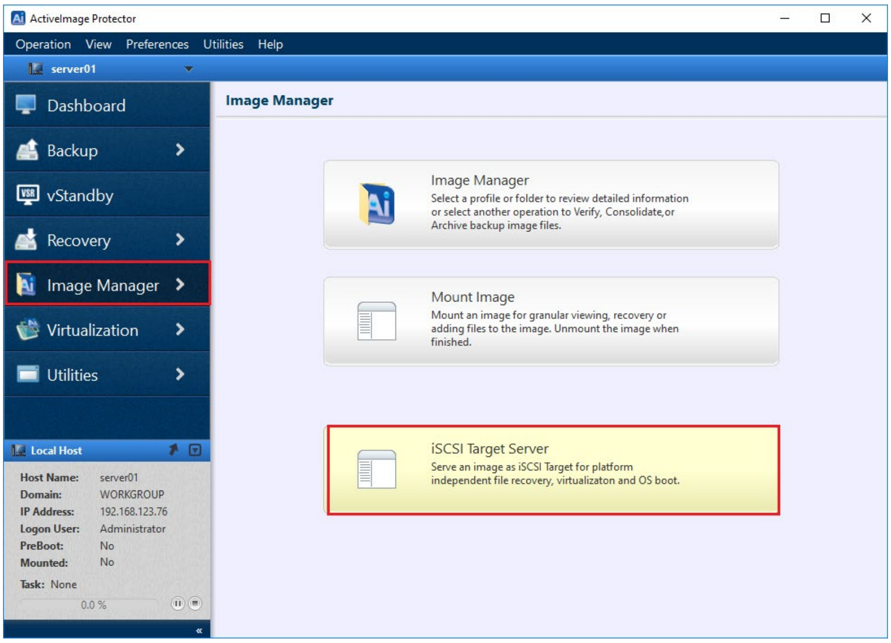


Image Manager
Select a profile or folder to review detailed information or select another operation to Verify, Consolidate,or Archive backup image files.

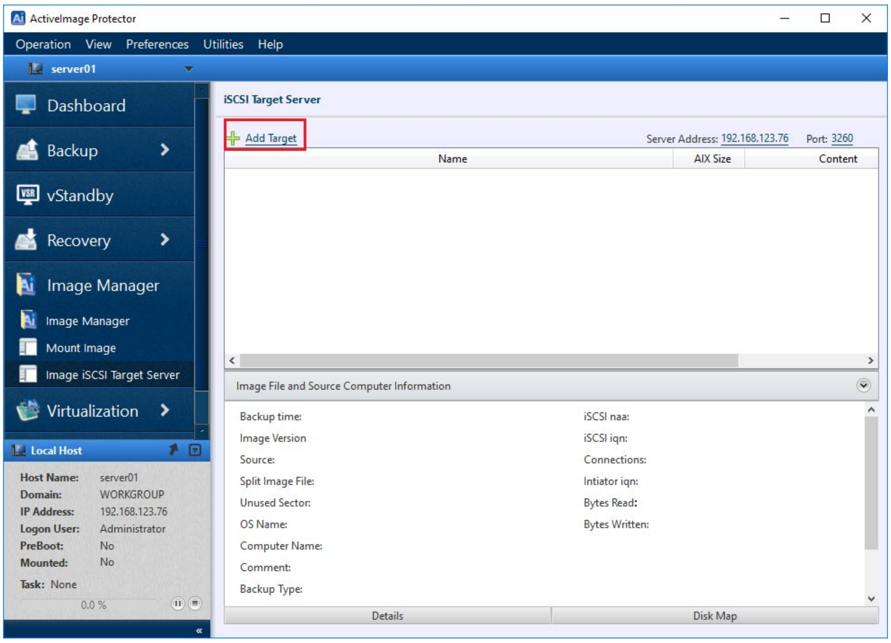
Mount Image
Mount an image for granular viewing, recovery or adding files to the image. Unmount the image when finished.

iSCSI Target Server
Serve an image as iSCSI Target for platform independent file recovery, virtualizaton and OS boot.

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

Note) The left pane of ActiveImage Protector for Hyper-V Enterprise screen is different from the one of Server Edition. There is no “iSCSI Target Server” menu.

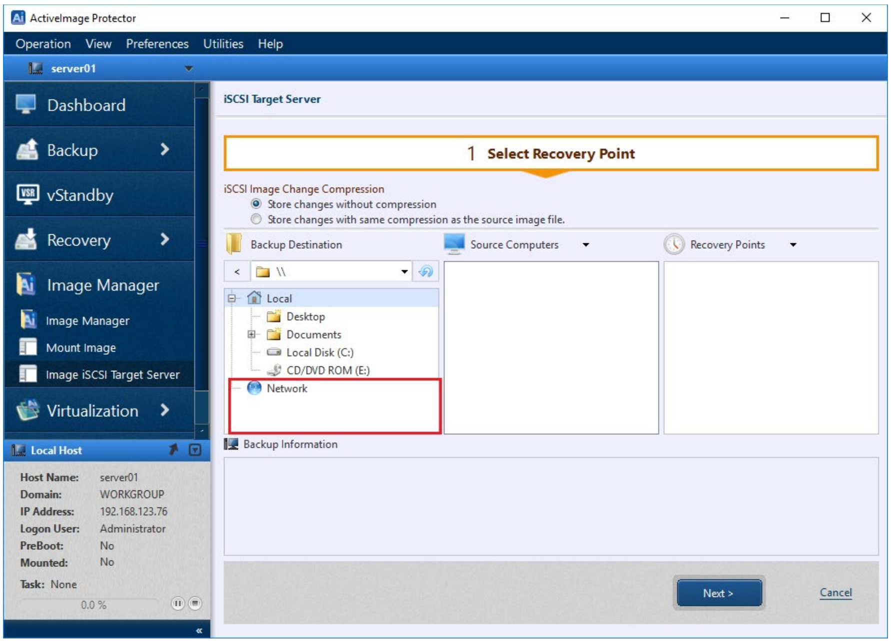
2. **[iSCSI Target Server]** window is shown as below. iSCSI targets will be listed in the window. To add a target, click **[Add Target]** at the upper left corner of the list.



Server Address: 192.168.123.76 Port: 3260

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

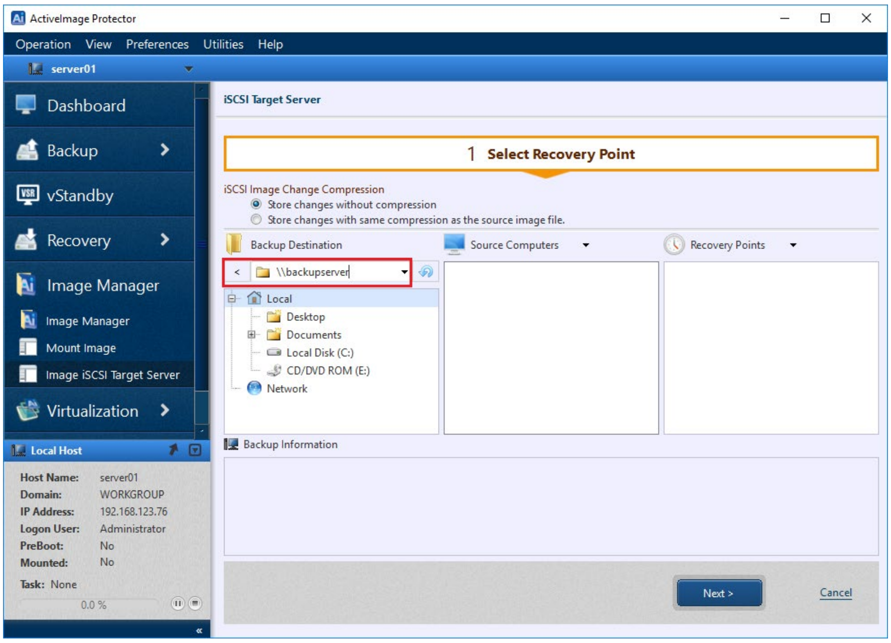
3. Select a backup image file and recovery point.



iSCSI Image Change Compression
● Store changes without compression
○ Store changes with same compression as the source image file.

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

If no network shared folder is displayed under “Network” in [Backup Destination] column, enter a server name following “\\” in the text box.



iSCSI Image Change Compression

● Store changes without compression

○ Store changes with same compression as the source image file.

\\backupserver

Host Name: server01

Domain: WORKGROUP

IP Address: 192.168.123.76

Logon User: Administrator

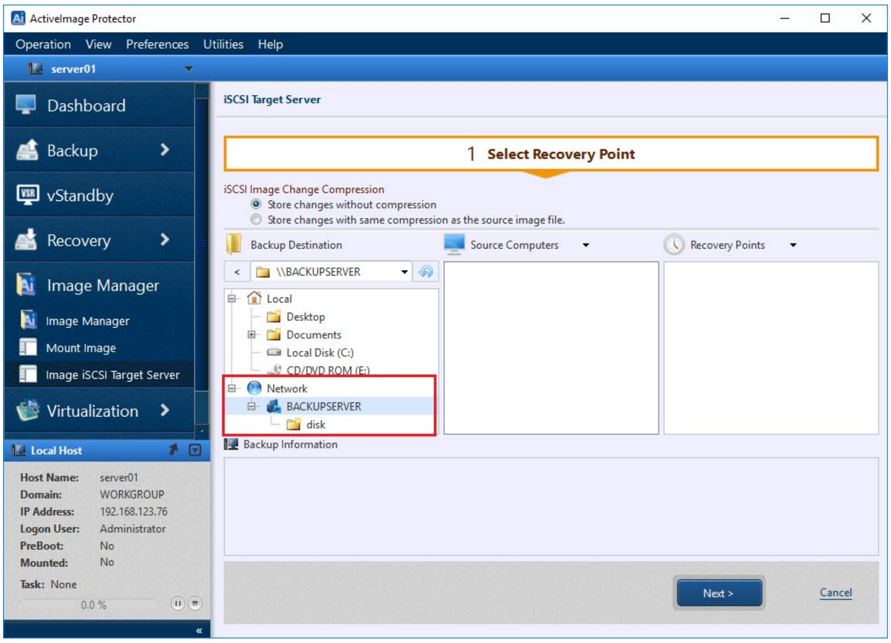
PreBoot: No

Mounted: No

Task: None

0.0 %

4. Upon completion of a search, shared folders are found under “Network”.



iSCSI Image Change Compression

● Store changes without compression

○ Store changes with same compression as the source image file.

\\BACKUPSERVER

Host Name: server01

Domain: WORKGROUP

IP Address: 192.168.123.76

Logon User: Administrator

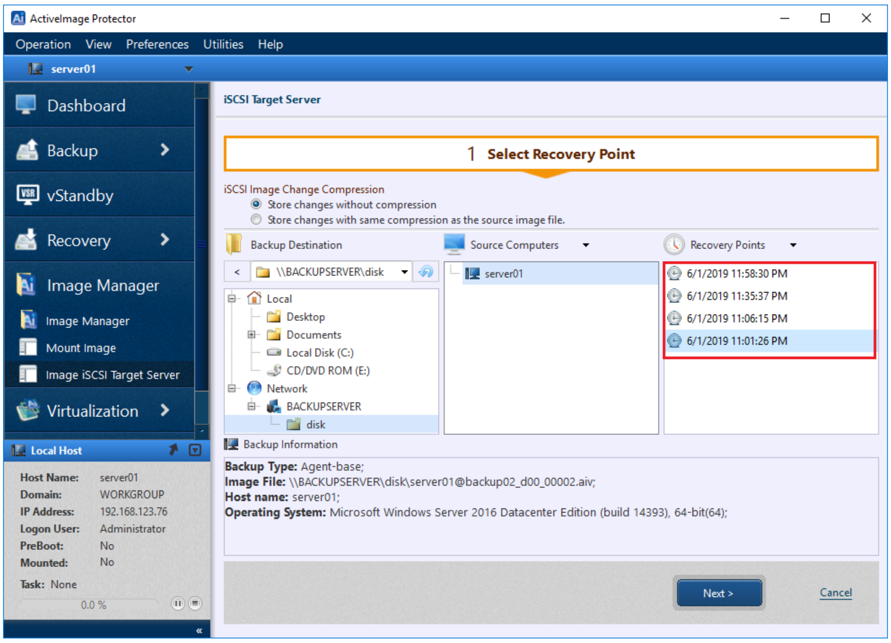
PreBoot: No

Mounted: No

Task: None

0.0 %

5. Select a backup file and a recovery point.



iSCSI Image Change Compression

● Store changes without compression

○ Store changes with same compression as the source image file.

\\BACKUPSERVER\disk

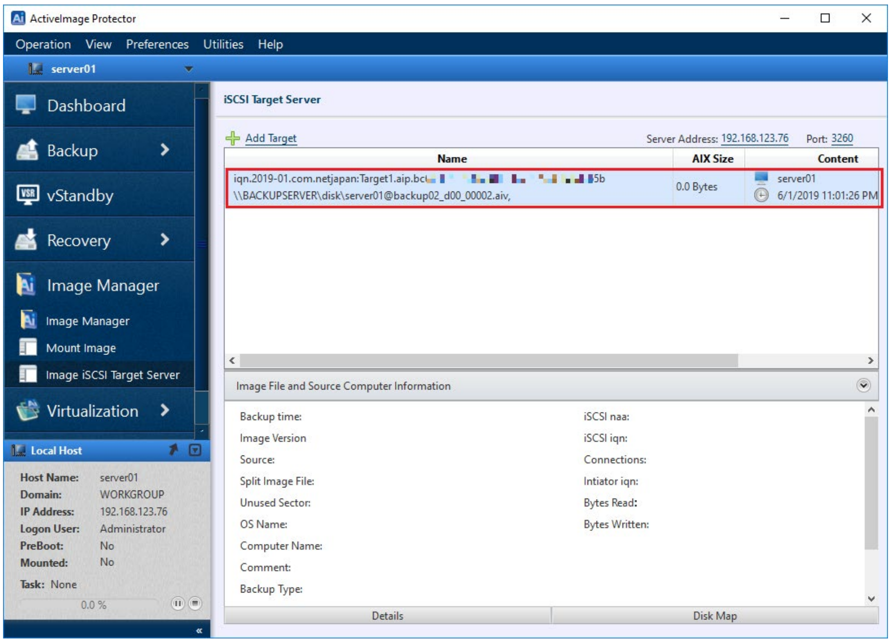
6/1/2019 11:58:30 PM
6/1/2019 11:35:37 PM
6/1/2019 11:06:15 PM
6/1/2019 11:01:26 PM

Backup Type: Agent-base;
Image File: \\BACKUPSERVER\disk\server01@backup02_d00_00002.aiv;
Host name: server01;
Operating System: Microsoft Windows Server 2016 Datacenter Edition (build 14393), 64-bit(64);

Host Name:	server01
Domain:	WORKGROUP
IP Address:	192.168.123.76
Logon User:	Administrator
PreBoot:	No
Mounted:	No
Task:	None

0.0 %

6. The backup file serving as iSCSI target is listed.



Server Address: 192.168.123.76 Port: 3260

Name	AIX Size	Content
iqn.2019-01.com.netjapan:Target1.aip.bc[redacted]5b \\BACKUPSERVER\disk\server01@backup02_d00_00002.aiv,	0.0 Bytes	server01 6/1/2019 11:01:26 PM

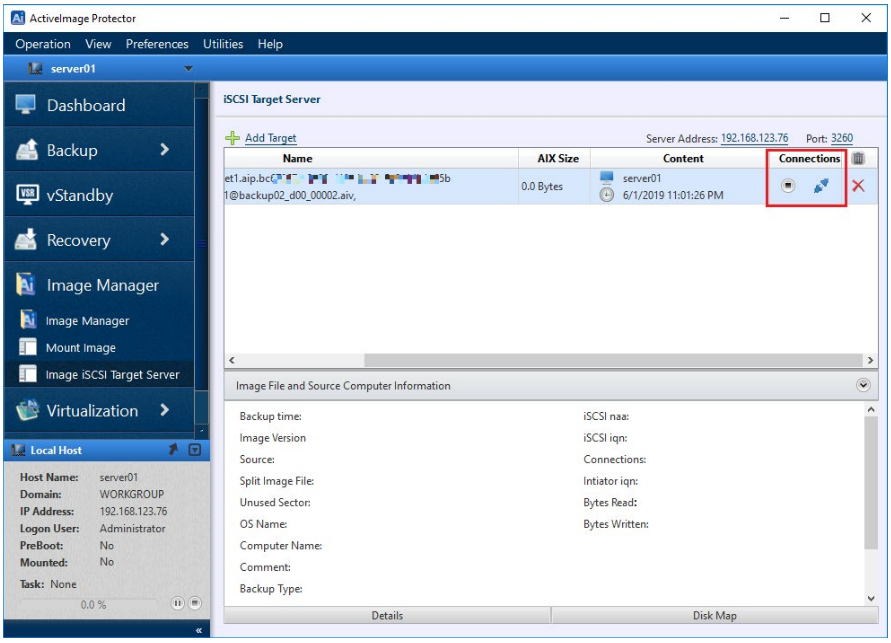
Backup time:
Image Version
Source:
Split Image File:
Unused Sector:
OS Name:
Computer Name:
Comment:
Backup Type:

iSCSI naa:
iSCSI iqn:
Connections:
Intiator iqn:
Bytes Read:
Bytes Written:

Host Name:	server01
Domain:	WORKGROUP
IP Address:	192.168.123.76
Logon User:	Administrator
PreBoot:	No
Mounted:	No
Task:	None

0.0 %

7. Move the slide bar to the right and display the **[Connection]** column.



Server Address: 192.168.123.76 Port: 3260

Name	AIX Size	Content	Connections
et1.aip.bc[redacted]5b 1@backup02_d00_00002.aiv,	0.0 Bytes	server01 6/1/2019 11:01:26 PM	

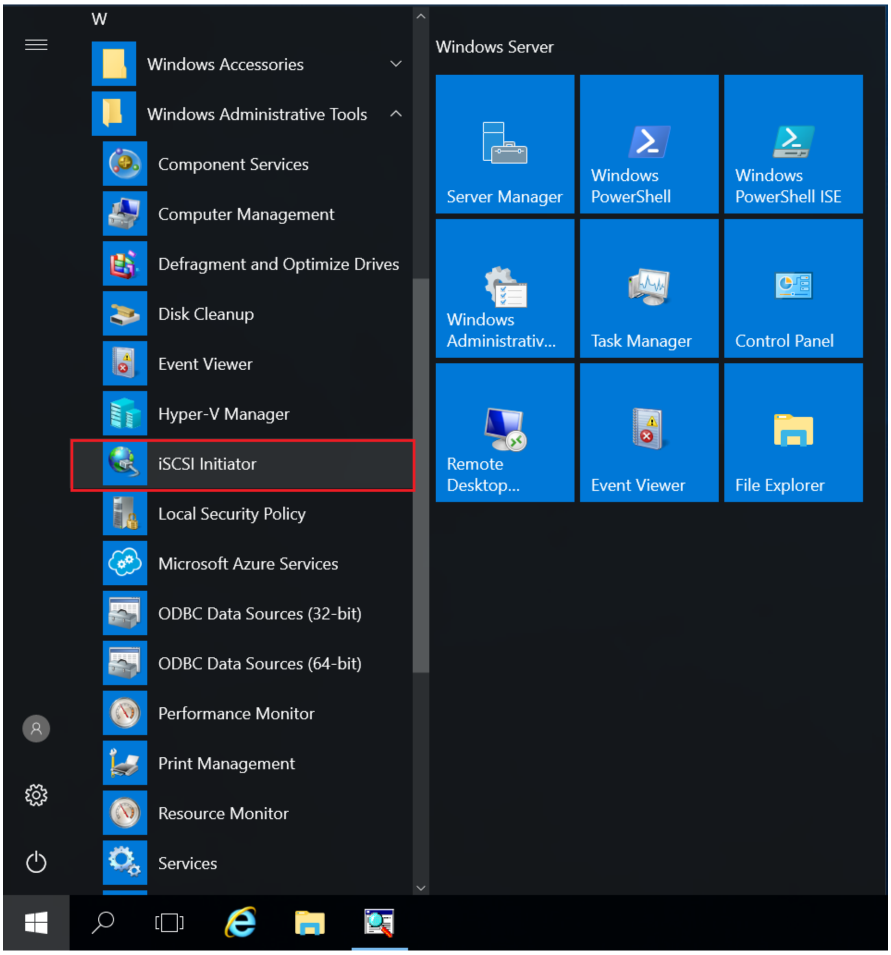
Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

Backup time:
Image Version
Source:
Split Image File:
Unused Sector:
OS Name:
Computer Name:
Comment:
Backup Type:

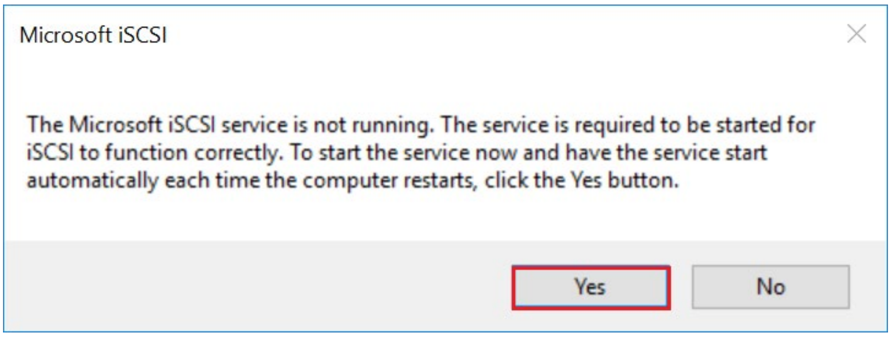
iSCSI naa:
iSCSI iqn:
Connections:
Intiator iqn:
Bytes Read:
Bytes Written:

Please be aware of the detached connector icon indicating that the iSCSI target is not network connected.

8. Next, select **[iSCSI Initiator]** in Start menu to discover iSCSI target.



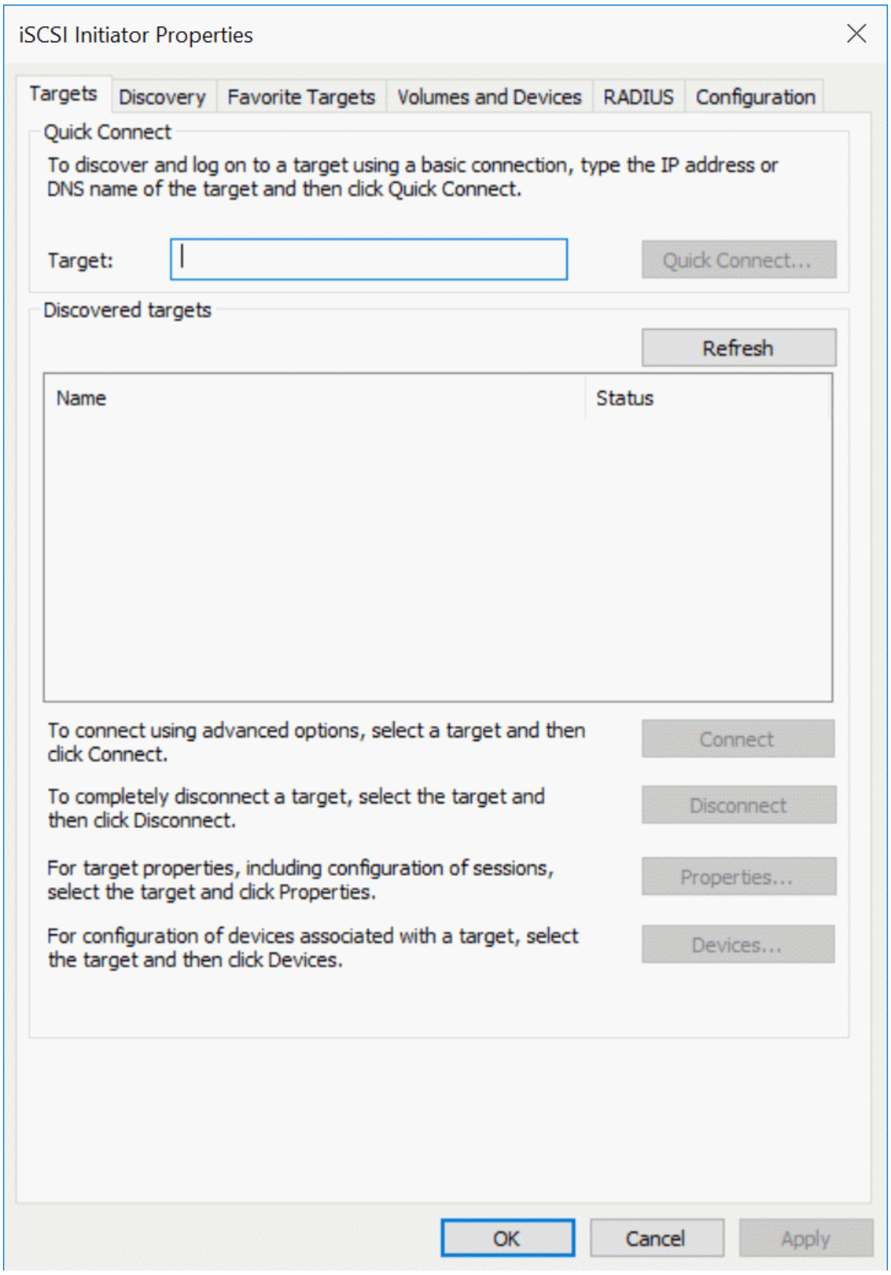
9. When you try to start Microsoft iSCSI Service for the first time, you will get the following confirmation message as shown below. Click **[Yes]**.



Microsoft iSCSI

The Microsoft iSCSI service is not running. The service is required to be started for iSCSI to function correctly. To start the service now and have the service start automatically each time the computer restarts, click the Yes button.

10. iSCSI Initiator is started and iSCSI Initiator Properties window is displayed as shown below.



iSCSI Initiator Properties

Quick Connect

To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target:

Discovered targets

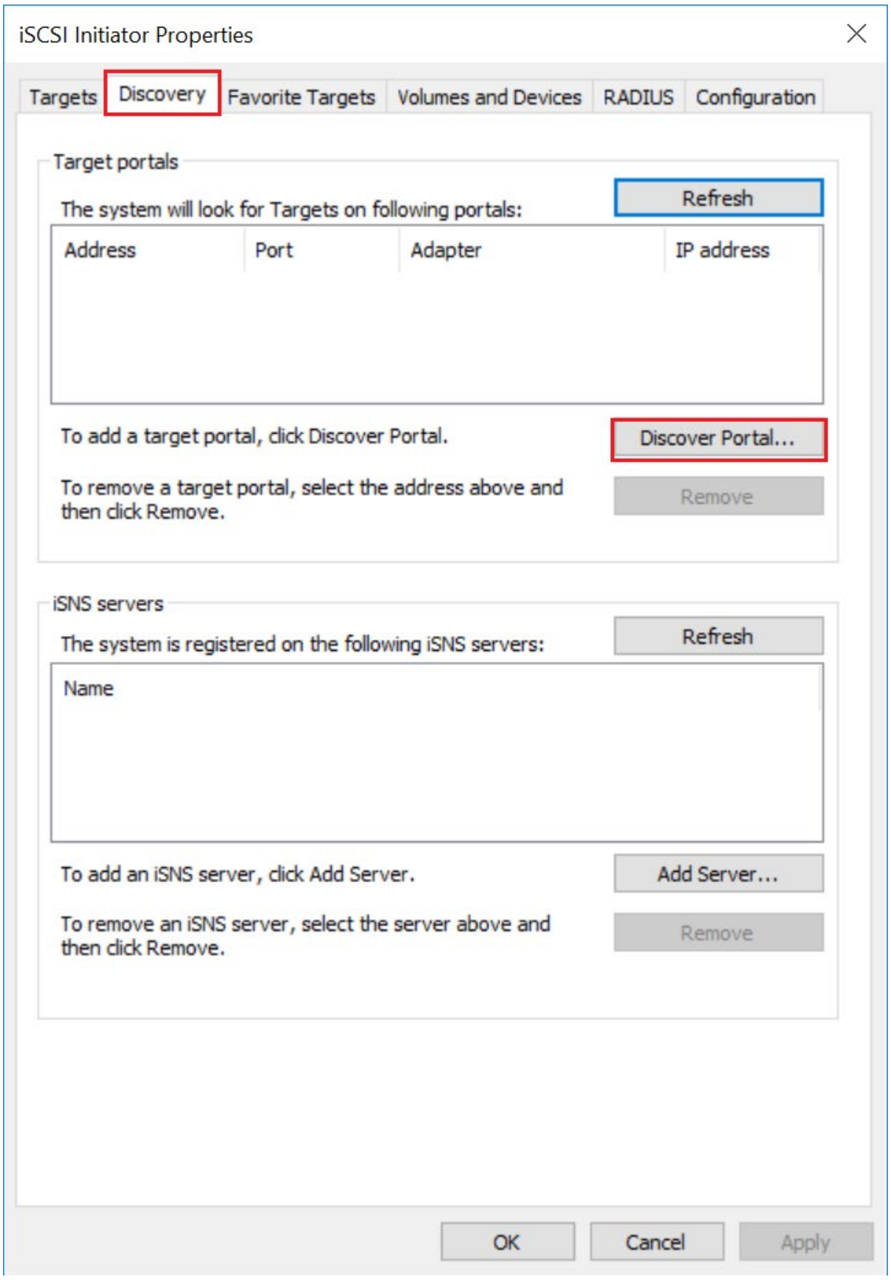
To connect using advanced options, select a target and then click Connect.

To completely disconnect a target, select the target and then click Disconnect.

For target properties, including configuration of sessions, select the target and click Properties.

For configuration of devices associated with a target, select the target and then click Devices.

11. At present, no iSCSI target is added to the list. Select **[Discovery]** tab.



iSCSI Initiator Properties

Target portals

The system will look for Targets on following portals:

Address	Port	Adapter	IP address

To add a target portal, click Discover Portal.

To remove a target portal, select the address above and then click Remove.

iSNS servers

The system is registered on the following iSNS servers:

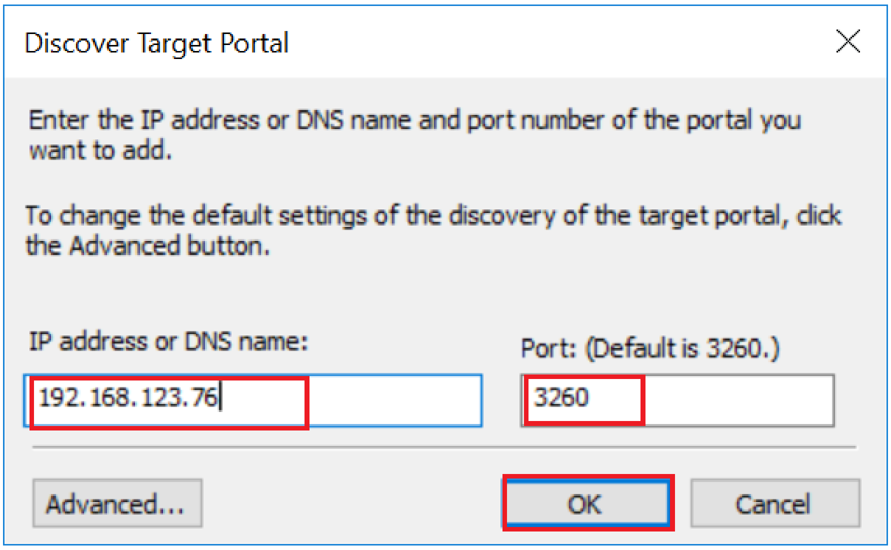
Name

To add an iSNS server, click Add Server.

To remove an iSNS server, select the server above and then click Remove.

12. iSCSI target created by using ActiveImage Protector is searched for and added to the list. Click **[Discover Target Portal].**

13. Target portal is searched for.



Discover Target Portal

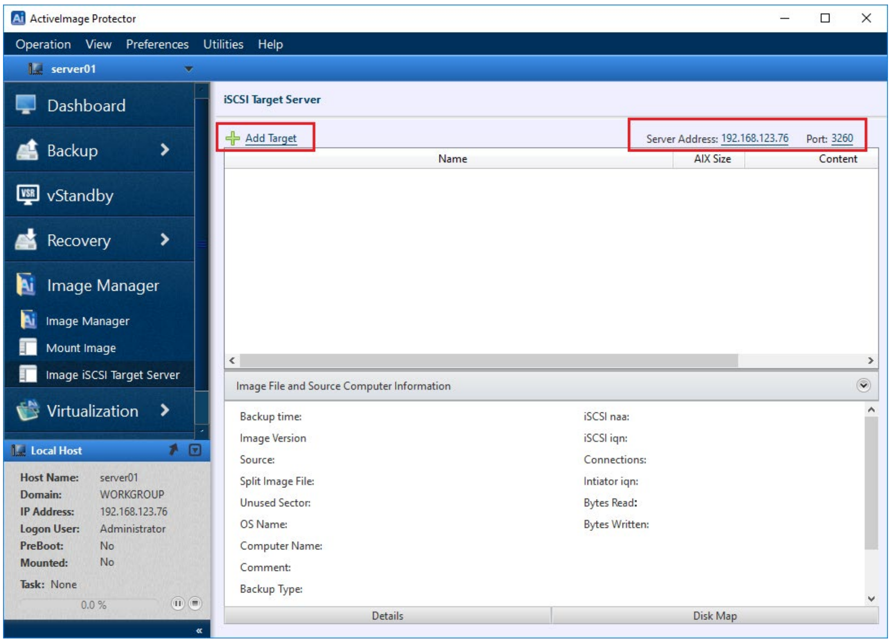
Enter the IP address or DNS name and port number of the portal you want to add.

To change the default settings of the discovery of the target portal, click the Advanced button.

IP address or DNS name: 192.168.123.76

Port: (Default is 3260.) 3260

Enter “192.168.123.11” in the blank field for **[IP address or DNS name]**. This IP address was indicated for **[Server Address]** at the upper right in **[iSCSI Target Server]** window of ActiveImage Protector. “3260” was indicated, by default, for **[Port]**. Please make sure these numbers are identical.



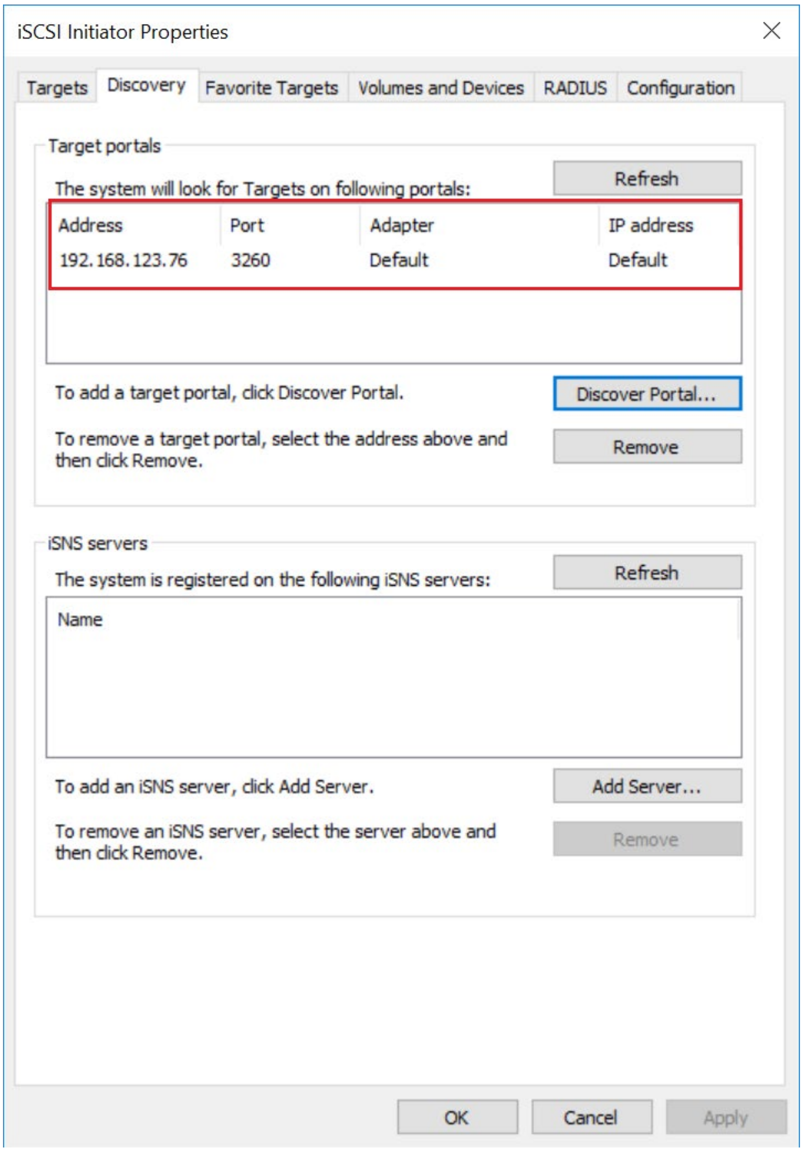
Server Address: 192.168.123.76 Port: 3260

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

Backup time:
Image Version
Source:
Split Image File:
Unused Sector:
OS Name:
Computer Name:
Comment:
Backup Type:

iSCSI naa:
iSCSI iqn:
Connections:
Intiator iqn:
Bytes Read:
Bytes Written:

14. Click [OK] and the entered IP address is indicated under [The system will look for Targets on following portals:].



The system will look for Targets on following portals:

Address	Port	Adapter	IP address
192.168.123.76	3260	Default	Default

To add a target portal, click Discover Portal.

To remove a target portal, select the address above and then click Remove.

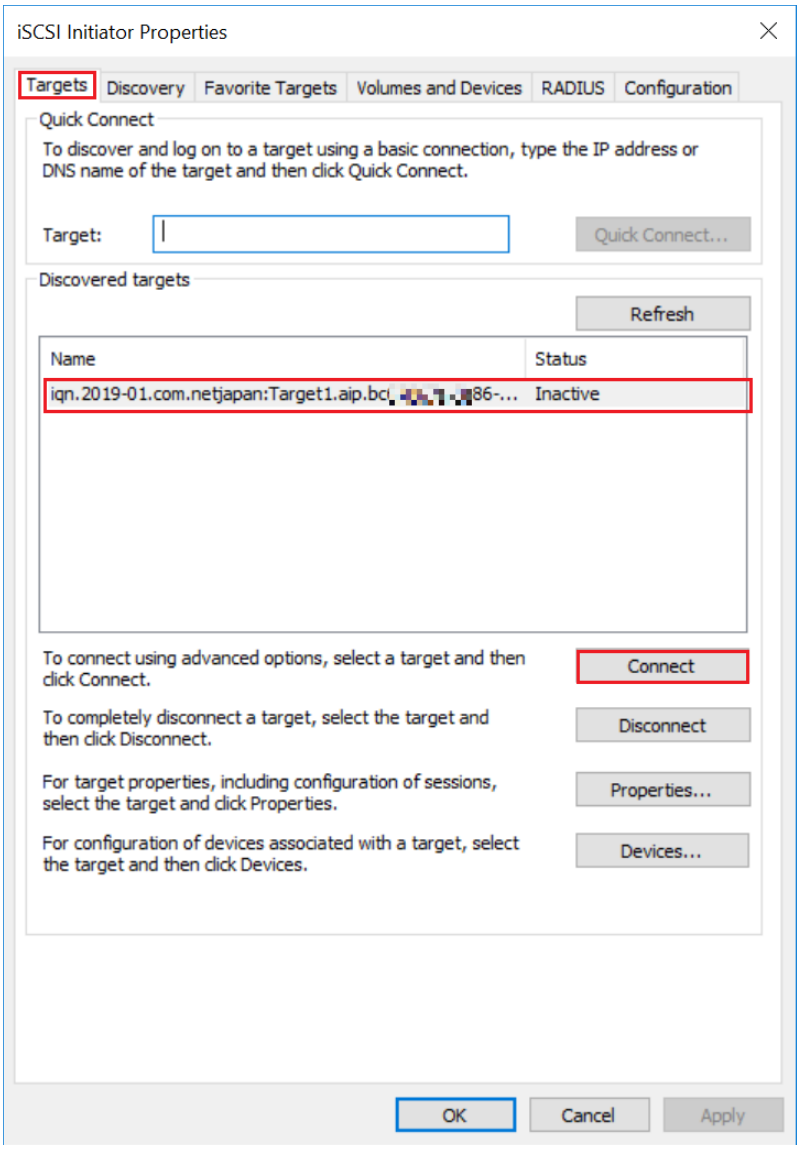
The system is registered on the following iSNS servers:

Name

To add an iSNS server, click Add Server.

To remove an iSNS server, select the server above and then click Remove.

15. Go back to **[Target]** tab. iSCSI target indicated in the following screen is listed in **[Discovered targets]**.



iSCSI Initiator Properties

Quick Connect

To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target:

Discovered targets

Name	Status
iqn.2019-01.com.netjapan:Target1.aip.bc[redacted]86-...	Inactive

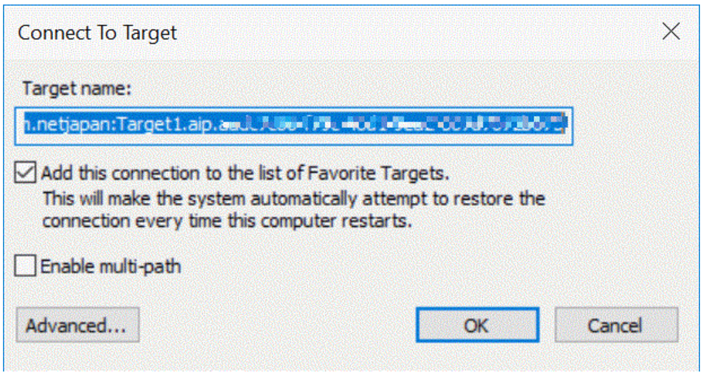
To connect using advanced options, select a target and then click Connect.

To completely disconnect a target, select the target and then click Disconnect.

For target properties, including configuration of sessions, select the target and click Properties.

For configuration of devices associated with a target, select the target and then click Devices.

16. The name of the discovered target is the same as the backup file name added to iSCSI target list shown blow. click **[Connect]** to connect to the target.



Connect To Target

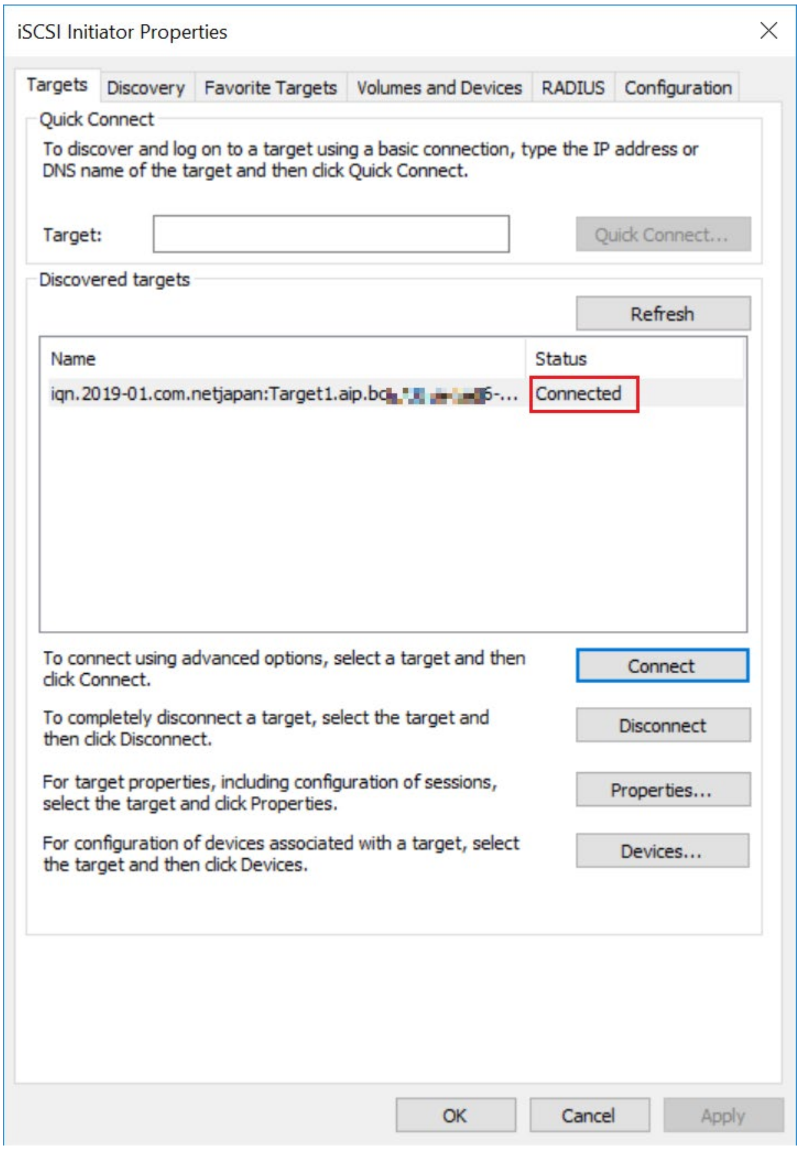
Target name:

n.netjapan:Target1.aip.[redacted]

☑ Add this connection to the list of Favorite Targets.
This will make the system automatically attempt to restore the connection every time this computer restarts.

☐ Enable multi-path

17. By default, **[Add this connection to the list of Favorite Targets]** option is enabled. As explained under the option, the system automatically attempts to restore the connection every time the computer restarts. Click **[OK]** to connect to the target.
The **[Status]** of the **[Discovered target]** is **[Connected]** in **[Target]** tab.



To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target:

Name	Status
iqn.2019-01.com.netjapan:Target1.aip.bc[redacted]6-...	Connected

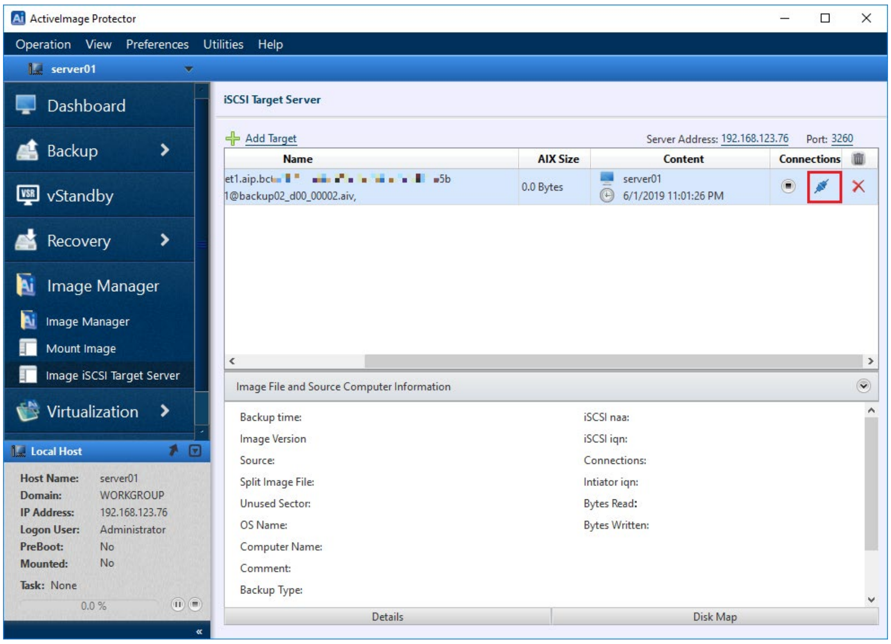
To connect using advanced options, select a target and then click Connect.

To completely disconnect a target, select the target and then click Disconnect.

For target properties, including configuration of sessions, select the target and click Properties.

For configuration of devices associated with a target, select the target and then click Devices.

Now, go back to ActiveImage Protector. The detached connector icon is attached now as you see in the following screen.



Server Address: 192.168.123.76 Port: 3260

Name	AIX Size	Content	Connections
et1.aip.bc[redacted]5b 1@backup02_d00_00002.aiv,	0.0 Bytes	server01 6/1/2019 11:01:26 PM	

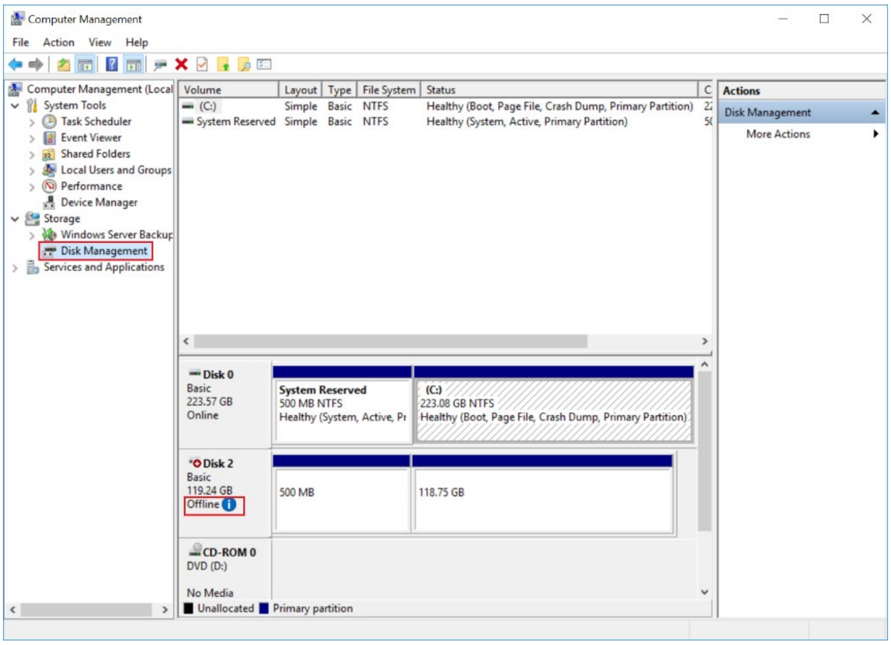
Host Name:	server01
Domain:	WORKGROUP
IP Address:	192.168.123.76
Logon User:	Administrator
PreBoot:	No
Mounted:	No

Task: None
0.0 %

Backup time:
Image Version
Source:
Split Image File:
Unused Sector:
OS Name:
Computer Name:
Comment:
Backup Type:

iSCSI naa:
iSCSI iqn:
Connections:
Intiator iqn:
Bytes Read:
Bytes Written:

18. Go to **[Management Tool]** and launch **[Computer Management]** to select [Disk Management] in the left menu.



Volume	Layout	Type	File System	Status
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)

Disk 0
Basic
223.57 GB
Online

System Reserved
500 MB NTFS
Healthy (System, Active, Pr

(C:)
223.08 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Disk 2
Basic
119.24 GB
Offline

500 MB

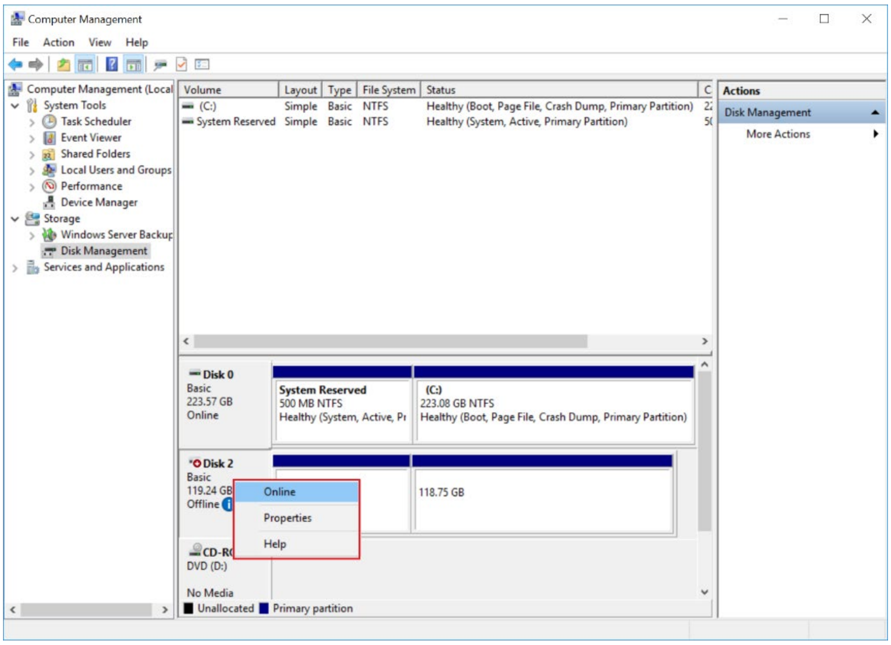
118.75 GB

CD-ROM 0
DVD (D:)

No Media

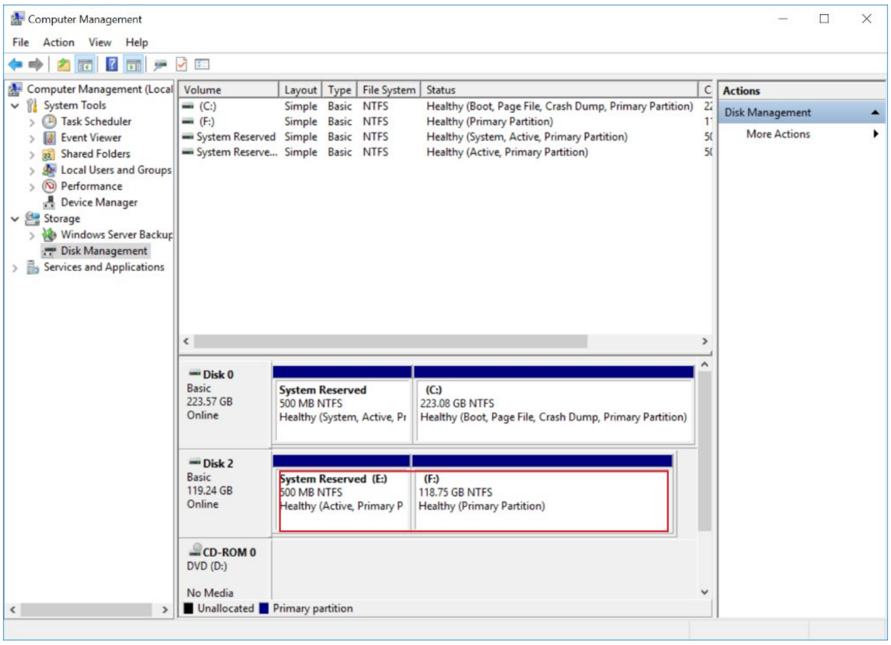
Disk 1 is added under offline condition.

19. Right-click on Disk 1 to display the context-menu as shown below.



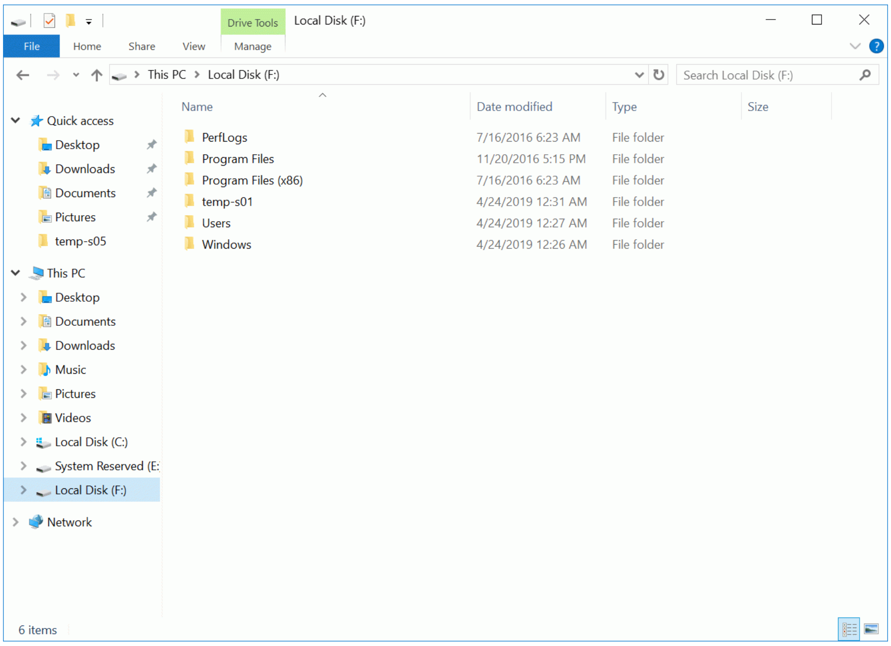
Volume	Layout	Type	File System	Status	C
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	22
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	50

20. Select **[Online]** in the context menu and Disk 1 will be recognized as a local disk. The drive letter is assigned to the partition.



Volume	Layout	Type	File System	Status	C
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	22
(F:)	Simple	Basic	NTFS	Healthy (Primary Partition)	1
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	50
System Reserve...	Simple	Basic	NTFS	Healthy (Active, Primary Partition)	50

21. You can browse the disk in File Explorer as shown below:



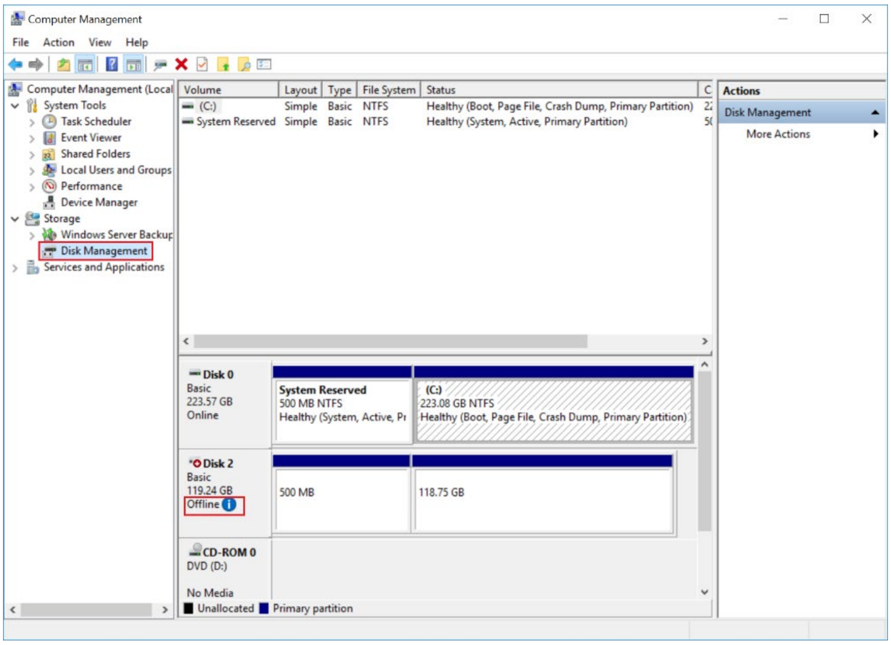
Name	Date modified	Type	Size
PerfLogs	7/16/2016 6:23 AM	File folder	
Program Files	11/20/2016 5:15 PM	File folder	
Program Files (x86)	7/16/2016 6:23 AM	File folder	
temp-s01	4/24/2019 12:31 AM	File folder	
Users	4/24/2019 12:27 AM	File folder	
Windows	4/24/2019 12:26 AM	File folder	

ActiveImage Protector provides Mount Image feature, which, however, enables you to mount a backup image via ActiveImage Protector. A local disk serving as iSCSI target offers a local file system in data area, which provides disaster recovery solution in the event of a system failure.

9.2 Attach virtual disk to virtual machine

Another possible use for iSCSI target is to attach a virtual disk to virtual machine. Before starting, please make sure that iSCSI target is offline in [Disk Management] window.

1. Go to [Management Tool] in Start menu and launch [Hyper-V Manager].



Volume	Layout	Type	File System	Status	C
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	22
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	5(

Disk 0
Basic
223.57 GB
Online

System Reserved
500 MB NTFS
Healthy (System, Active, Pr

(C:)
223.08 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Disk 2
Basic
119.24 GB
Offline

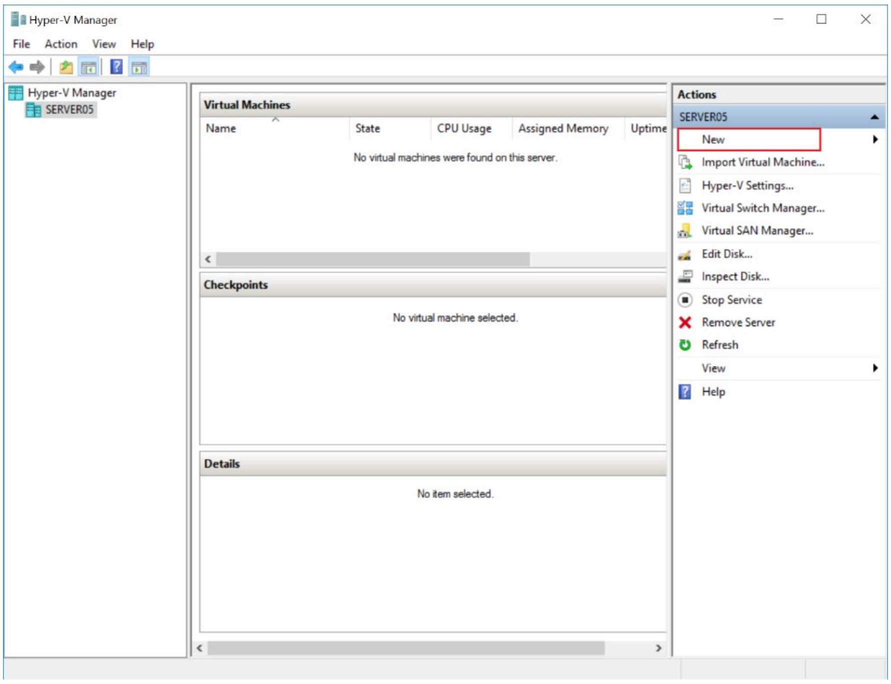
500 MB

118.75 GB

CD-ROM 0
DVD (D:)

No Media

2. At present, there exists no virtual machine. Select **[New]** in the right menu to create a new virtual machine.

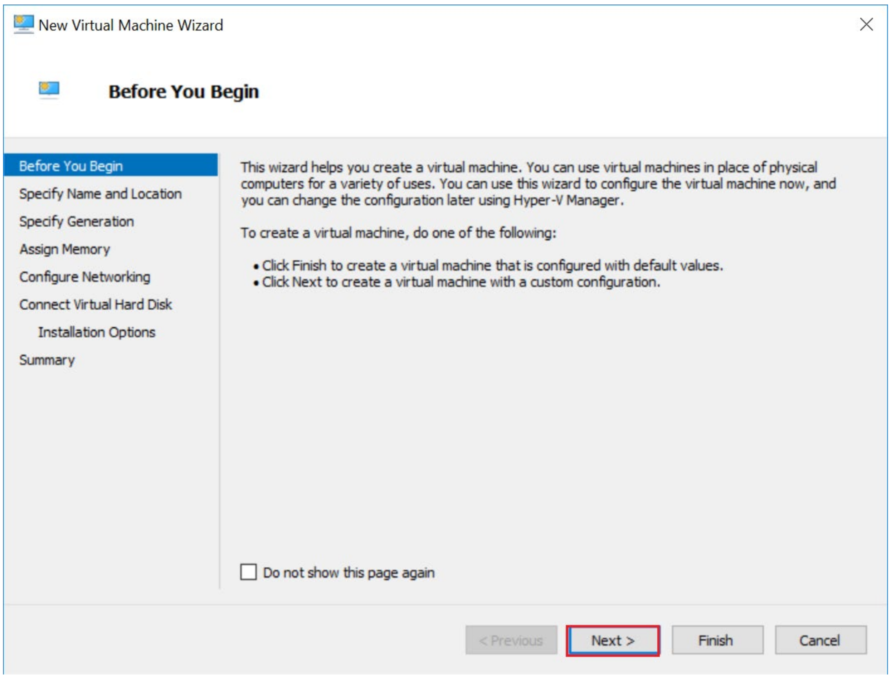


No virtual machines were found on this server.

No virtual machine selected.

No item selected.

3. New Virtual Machine Wizard is launched as follows.



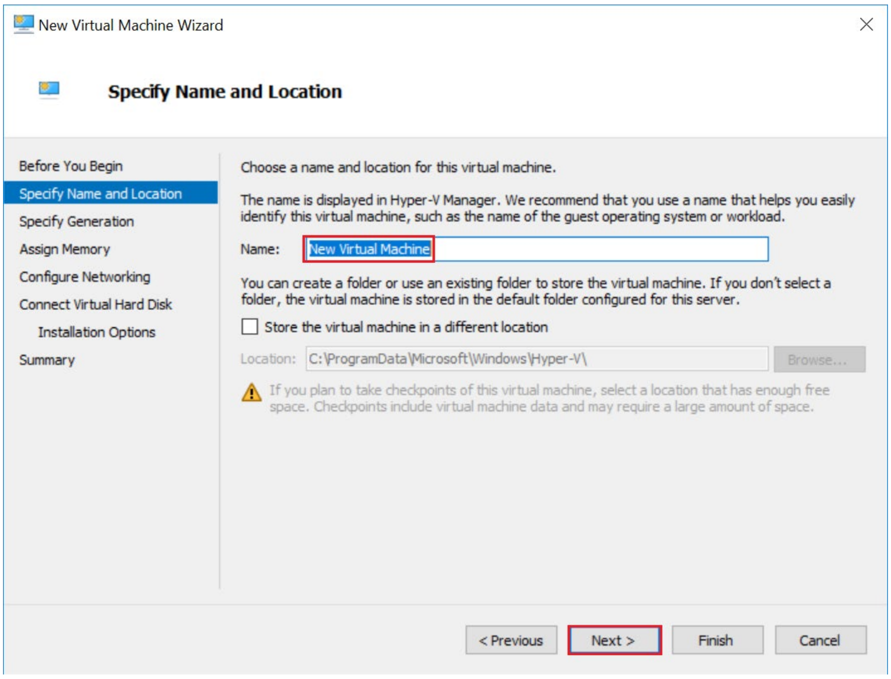
This wizard helps you create a virtual machine. You can use virtual machines in place of physical computers for a variety of uses. You can use this wizard to configure the virtual machine now, and you can change the configuration later using Hyper-V Manager.

To create a virtual machine, do one of the following:

- Click Finish to create a virtual machine that is configured with default values.
- Click Next to create a virtual machine with a custom configuration.

☐ Do not show this page again

4. Click [Next] to display [Specify Name and Location].



Specify Name and Location

Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name: New Virtual Machine

You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

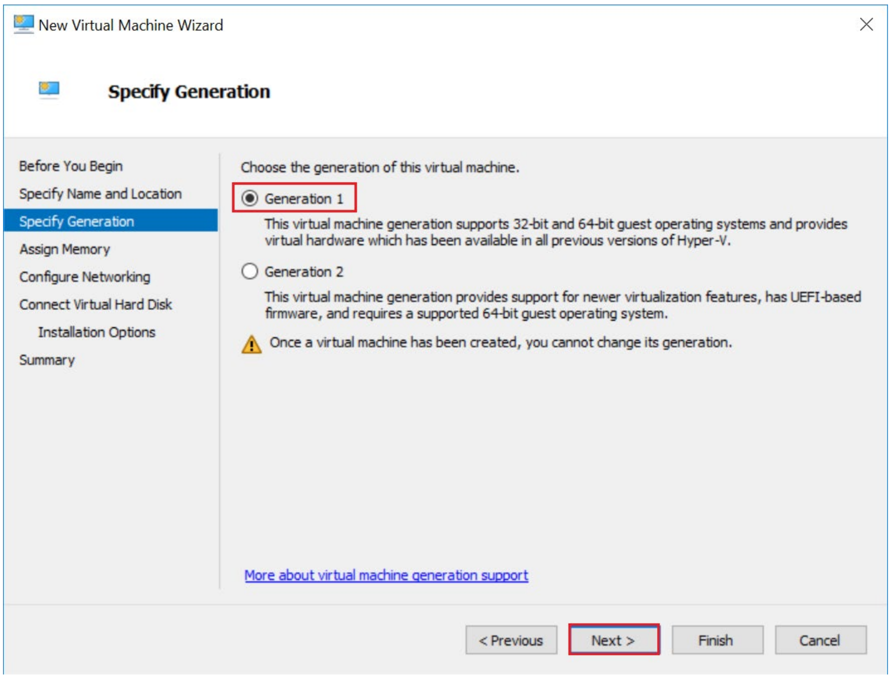
□ Store the virtual machine in a different location

Location: C:\ProgramData\Microsoft\Windows\Hyper-V\

If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

In this example, the default name “New Virtual Machine” is used for **[Name]** and the default destination location is used.

5. Click **[Next]** to display **[Specify Generation]** window.



New Virtual Machine Wizard

Specify Generation

Choose the generation of this virtual machine.

● Generation 1

This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V.

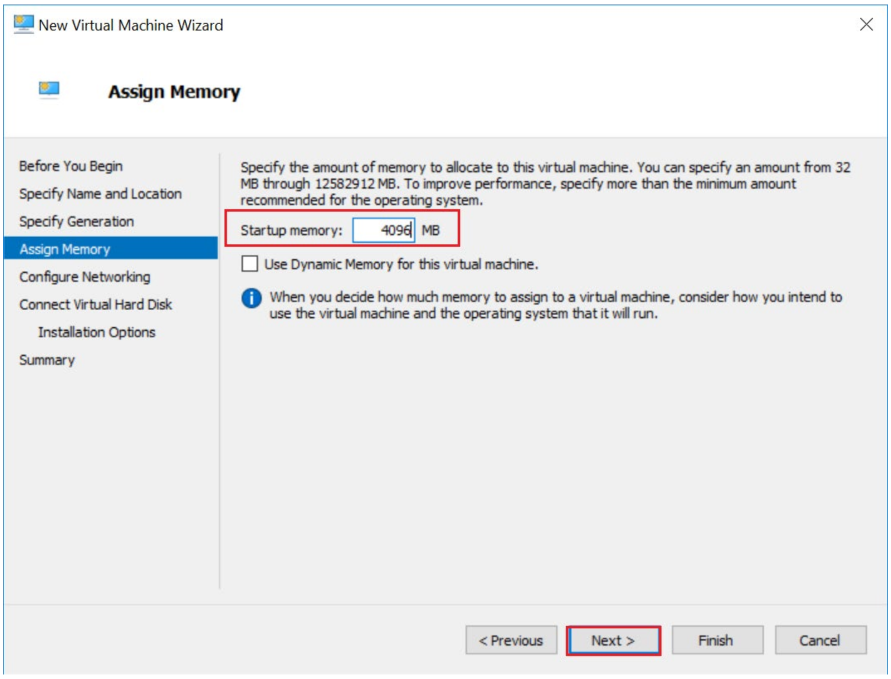
○ Generation 2

This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.

⚠ Once a virtual machine has been created, you cannot change its generation.

By default, **[Generation 1]** is selected.

6. Click **[Next]** to display **[Assign Memory]** window.



New Virtual Machine Wizard

Assign Memory

Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

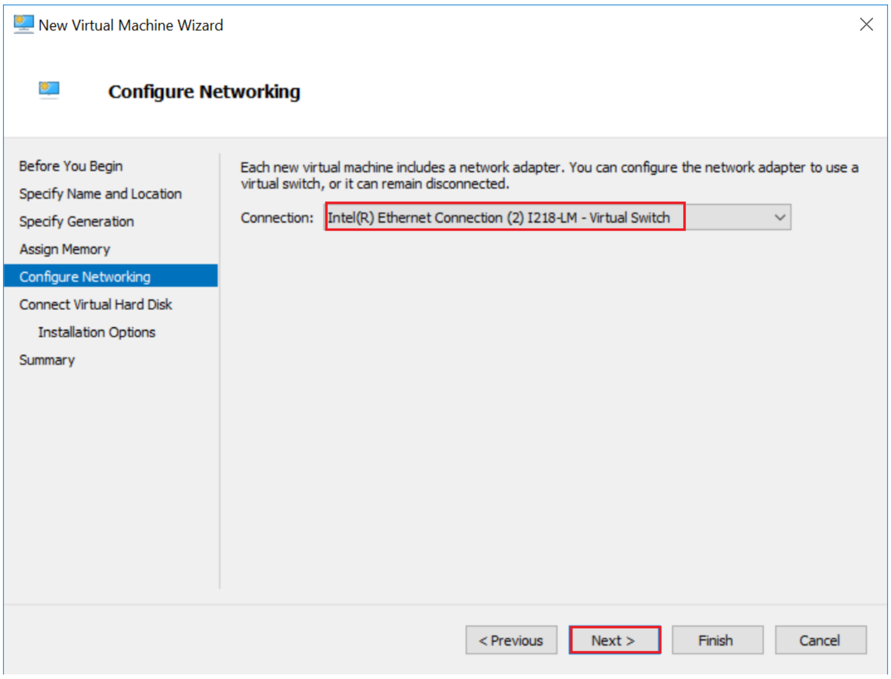
Startup memory: 4096 MB

□ Use Dynamic Memory for this virtual machine.

When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

Here, “4096MB”, the same memory size as the backup source virtual machine, is assigned in **[Startup memory]**.

7. Click [Next] to display **[Configure Networking]** window.



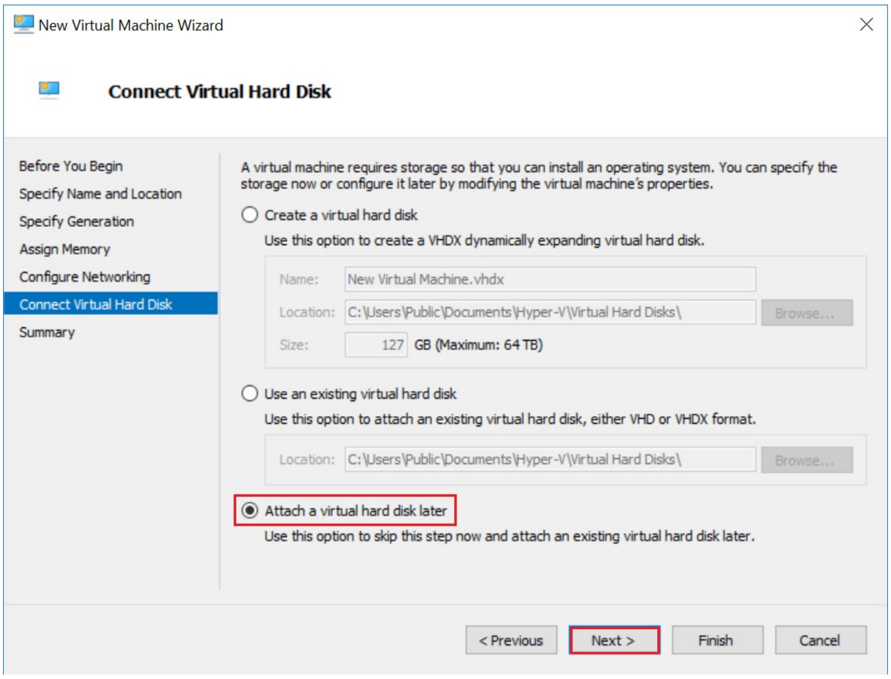
New Virtual Machine Wizard

Configure Networking

Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.

Connection: Intel(R) Ethernet Connection (2) I218-LM - Virtual Switch

8. Here, “Intel(R) Ethernet Connection (2) I218-LM - Virtual Switch”, the same virtual switch as for the backup source virtual machine, is selected. Click **[Next]** to display **[Connect Virtual Hard Disk]**.



New Virtual Machine Wizard

Connect Virtual Hard Disk

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

○ Create a virtual hard disk

Use this option to create a VHDX dynamically expanding virtual hard disk.

Name: New Virtual Machine.vhdx

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

Size: 127 GB (Maximum: 64 TB)

○ Use an existing virtual hard disk

Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

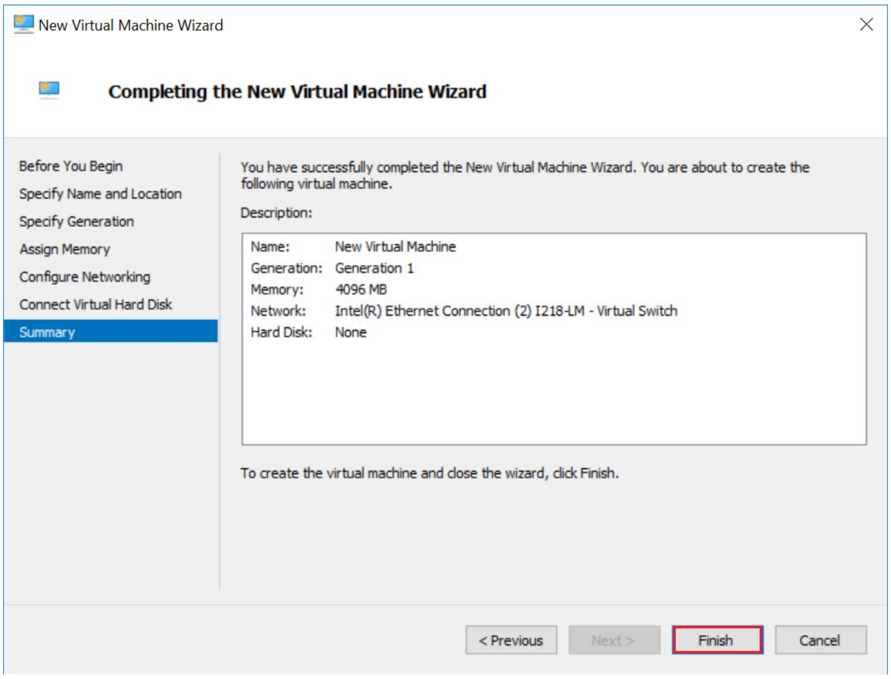
Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

● Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.

In this example, [Attach a virtual hard disk later] is selected to skip selection of a virtual disk. Please be aware you are taking different operating procedures from the regular routine.

9. Click [Next] to display [Completing the New Virtual Machine Wizard].



Completing the New Virtual Machine Wizard

You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine.

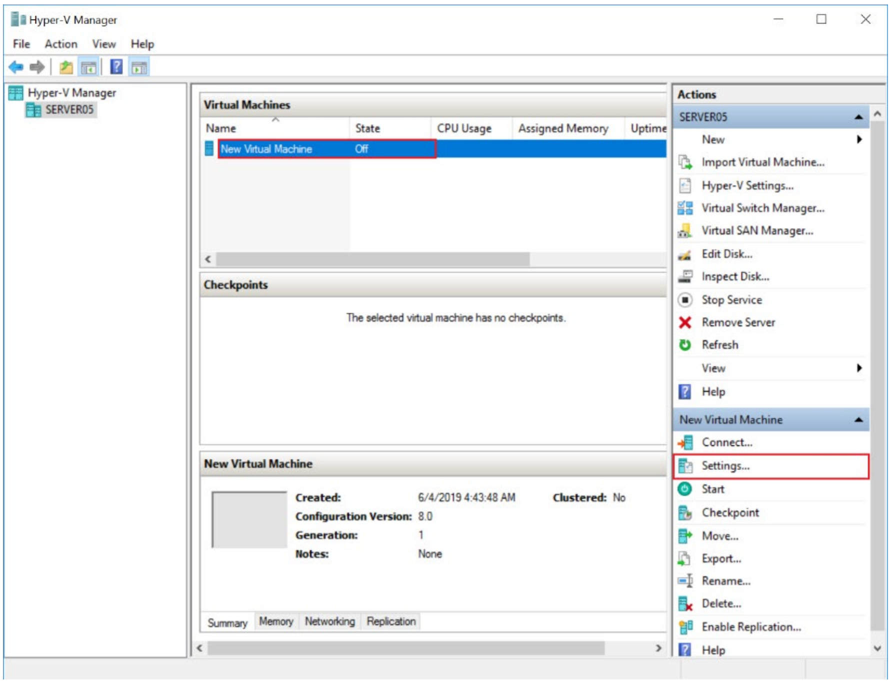
Description:

Name:	New Virtual Machine
Generation:	Generation 1
Memory:	4096 MB
Network:	Intel(R) Ethernet Connection (2) I218-LM - Virtual Switch
Hard Disk:	None

To create the virtual machine and close the wizard, click Finish.

Please review the configured settings and click **[Finish]** to create a new virtual machine.

10. Configure the settings for the new virtual machine.



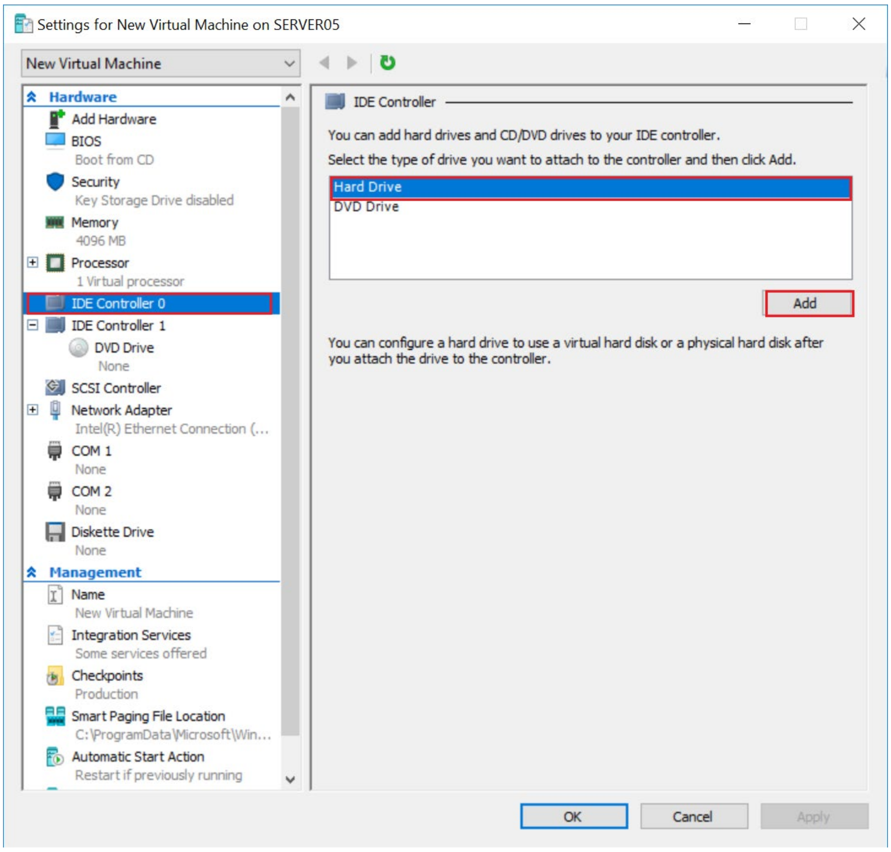
Name	State	CPU Usage	Assigned Memory	Uptime
New Virtual Machine	Off			

The selected virtual machine has no checkpoints.

Created: 6/4/2019 4:43:48 AM Clustered: No
Configuration Version: 8.0
Generation: 1
Notes: None

11. Select **[IDE Controller 0]** in [Hardware].

Select **[Hard Drive]** for [IDE Controller] and click **[Add]**.



Settings for New Virtual Machine on SERVER05

IDE Controller

You can add hard drives and CD/DVD drives to your IDE controller.

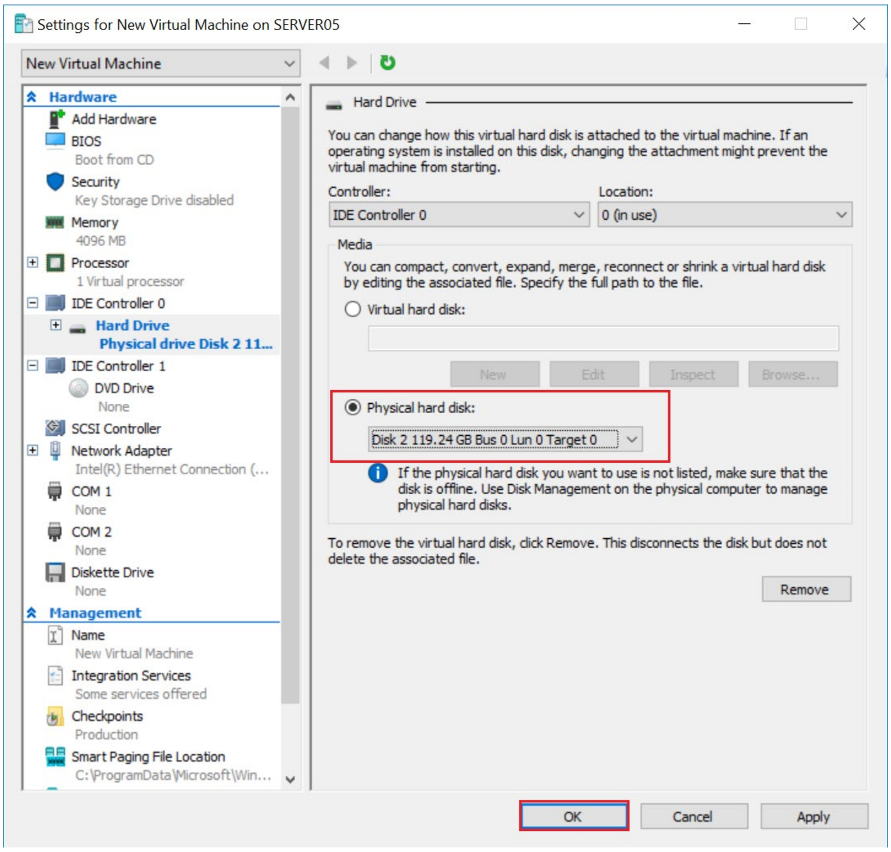
Select the type of drive you want to attach to the controller and then click Add.

Hard Drive

DVD Drive

You can configure a hard drive to use a virtual hard disk or a physical hard disk after you attach the drive to the controller.

12. In **[Hard Drive]** section, select **[Physical hard disk]** and “Disk 1 20.00GB Bus 0 Lun 0 Target 0” by default. If no other iSCSI target is listed, this is the only option you are allowed to select. Click **[OK]**.



Settings for New Virtual Machine on SERVER05

Hard Drive

You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.

Controller: IDE Controller 0

Location: 0 (in use)

Media

You can compact, convert, expand, merge, reconnect or shrink a virtual hard disk by editing the associated file. Specify the full path to the file.

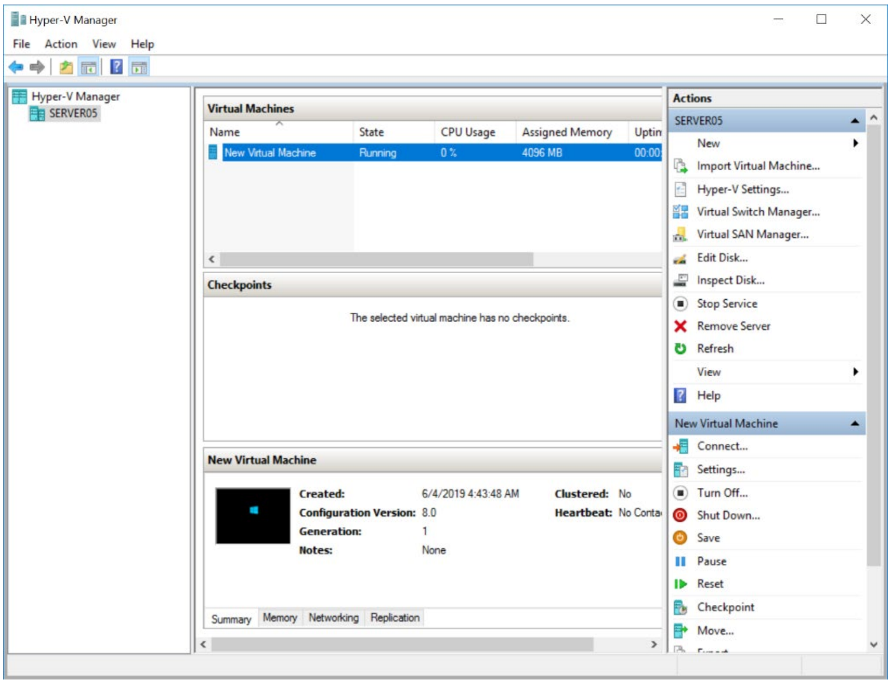
○ Virtual hard disk:

● Physical hard disk: Disk 2 119.24 GB Bus 0 Lun 0 Target 0

If the physical hard disk you want to use is not listed, make sure that the disk is offline. Use Disk Management on the physical computer to manage physical hard disks.

To remove the virtual hard disk, click Remove. This disconnects the disk but does not delete the associated file.

13. Run the new virtual machine in the following window.

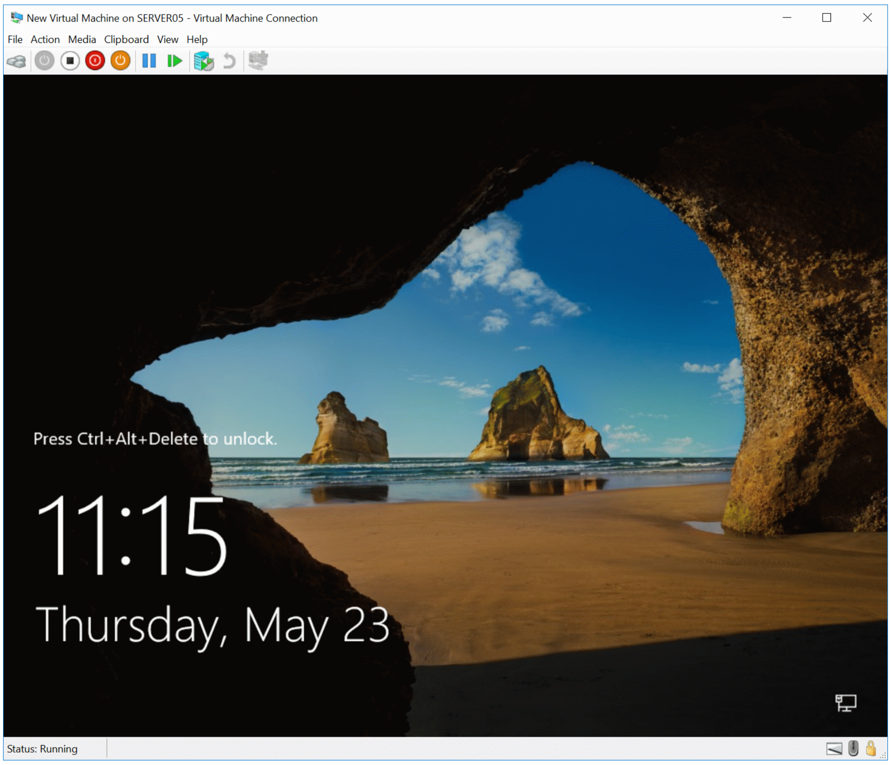


Name	State	CPU Usage	Assigned Memory	Uptin
New Virtual Machine	Running	0 %	4096 MB	00:00

The selected virtual machine has no checkpoints.

Created:	6/4/2019 4:43:48 AM	Clustered:	No
Configuration Version:	8.0	Heartbeat:	No Conta
Generation:	1		
Notes:	None		

14. When the virtual machine is connected to the server system, the following window is displayed.


New Virtual Machine on SERVER05 - Virtual Machine Connection
File Action Media Clipboard View Help

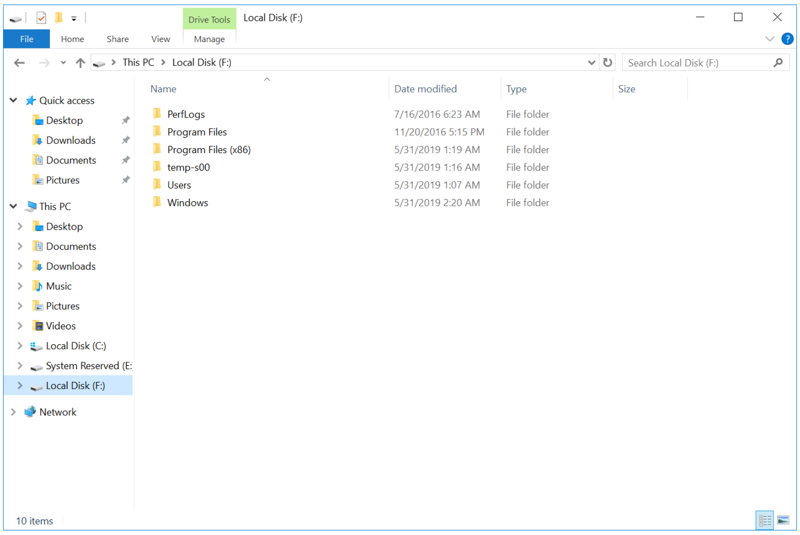
Press Ctrl+Alt+Delete to unlock.

11:15

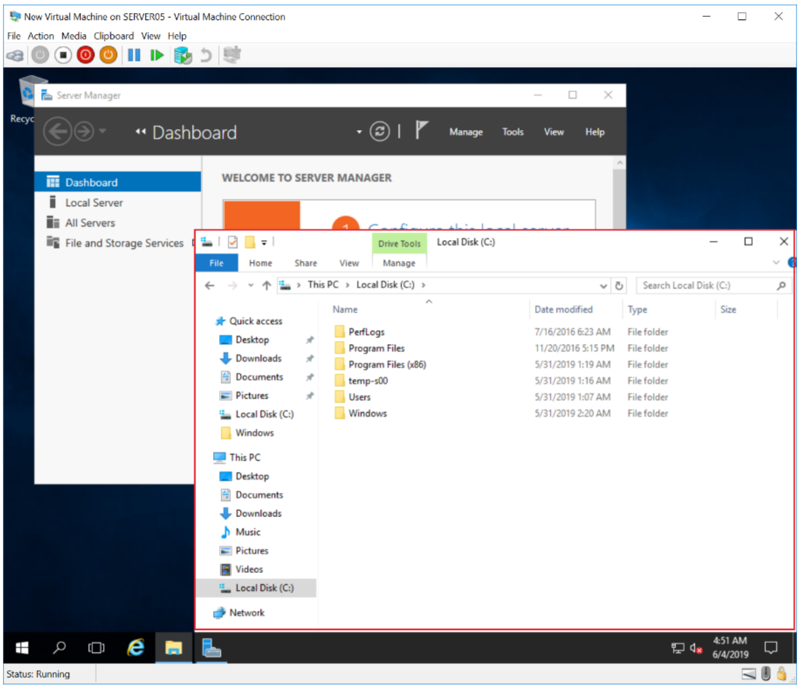
Thursday, May 23

Status: Running

15. Please make sure that the folder structure is configured the same as previous Explorer screen.



Name	Date modified	Type	Size
PerfLogs	7/16/2016 6:23 AM	File folder	
Program Files	11/20/2016 5:15 PM	File folder	
Program Files (x86)	5/31/2019 1:19 AM	File folder	
temp-s00	5/31/2019 1:16 AM	File folder	
Users	5/31/2019 1:07 AM	File folder	
Windows	5/31/2019 2:20 AM	File folder	

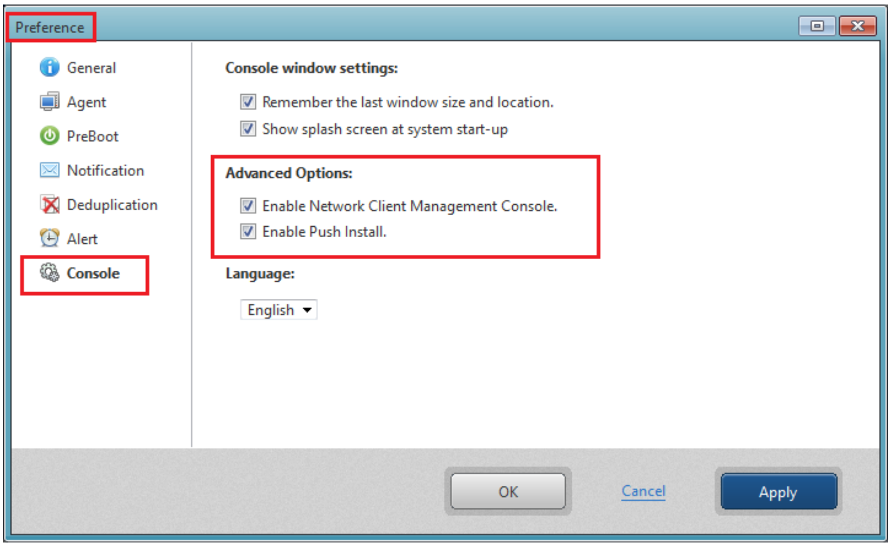


Name	Date modified	Type	Size
PerfLogs	7/16/2016 6:23 AM	File folder	
Program Files	11/20/2016 5:15 PM	File folder	
Program Files (x86)	5/31/2019 1:19 AM	File folder	
temp-s00	5/31/2019 1:16 AM	File folder	
Users	5/31/2019 1:07 AM	File folder	
Windows	5/31/2019 2:20 AM	File folder	

16. The use of this feature enables you to attach a backup image of the failed virtual machine to another virtual machine as a virtual disk and immediately recover the failed virtual machine. Though this document has not provided a detailed description, the use of VMware vMotion streamlines the backup / recovery process by seamlessly migrating live virtual machines booted from the iSCSI target to a hypervisor in a production environment.

10. Manage Remote Host

This topic describes Push Install and Network Client Management Console. These features are enabled by selecting [Console] in [Preferences] menu.



Console window settings:

☑ Remember the last window size and location.

☑ Show splash screen at system start-up

Advanced Options:

☑ Enable Network Client Management Console.

☑ Enable Push Install.

Language:

English ▾

10-1. Push Install

Note) The Push Install function is invalid on ActiveImage Protector for Hyper-V Enterprise

Please select **[Enable Push Install]** option in **[Advanced Options]** in the above **[Preference]** Window.

1. Start ActiveImage Protector.

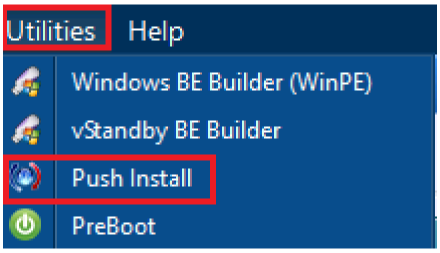
   Windows Server 2008 R2 or earlier server OS:
   Click **[Start]** – **[All Programs]** – **[NetJapan]** – **[ActiveImage Protector]**.

   Windows 7 or earlier Desktop OS:
   Click [Start] – [All Programs] – [NetJapan] – [ActiveImage Protector].

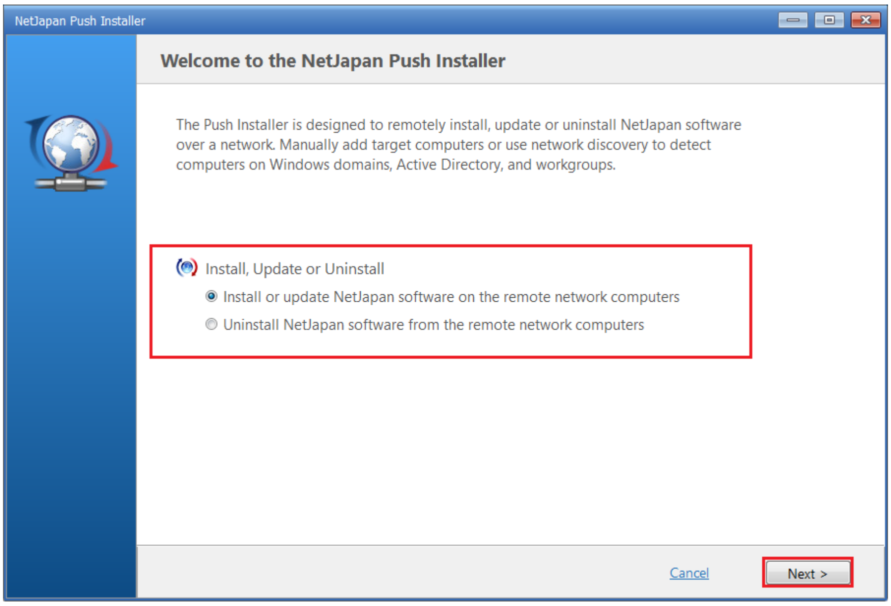
   Windows Server 2012 or later server OS:
   Click [Start] – [Applications] – [NetJapan] – [ActiveImage Protector].

   Windows Server 8 or later Desktop OS :
   Click [Start] – [Applications] – [NetJapan] – [ActiveImage Protector].

2. Select [Push Install] in [Utilities] menu.



3. To install ActiveImage Protector, select [Install or upgrade Actiphy software on the remote network computers] and click [Next].



Welcome to the NetJapan Push Installer

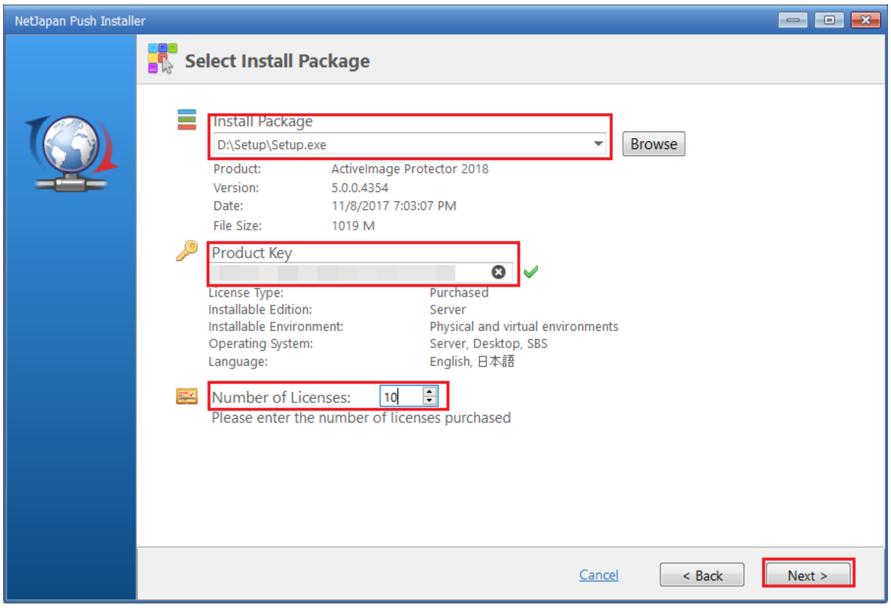
The Push Installer is designed to remotely install, update or uninstall NetJapan software over a network. Manually add target computers or use network discovery to detect computers on Windows domains, Active Directory, and workgroups.

Install, Update or Uninstall

● Install or update NetJapan software on the remote network computers

○ Uninstall NetJapan software from the remote network computers

4. Select [Install Package]. Enter [Product Key] and [Number of Licenses] and click [Next].



Select Install Package

Install Package
D:\Setup\Setup.exe

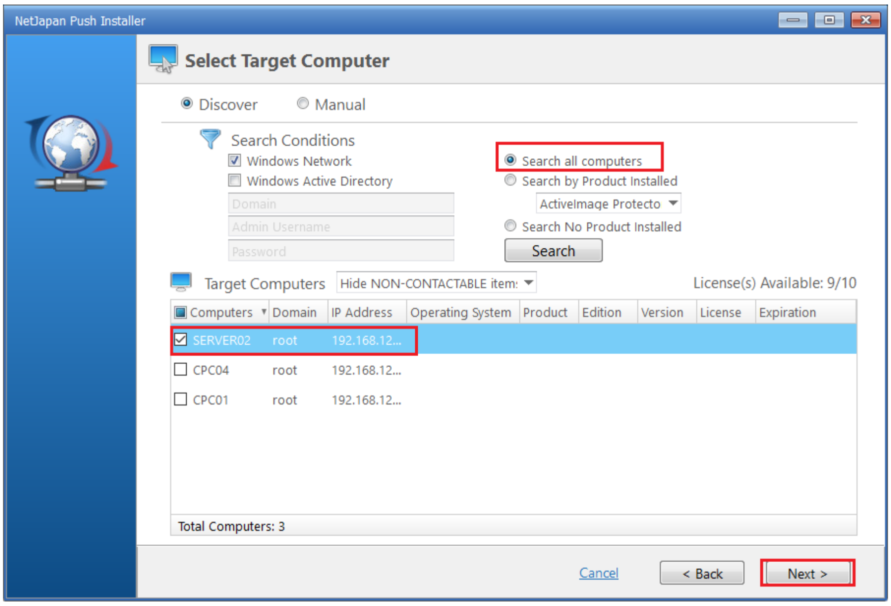
Product: ActiveImage Protector 2018
Version: 5.0.0.4354
Date: 11/8/2017 7:03:07 PM
File Size: 1019 M

Product Key
[redacted]

License Type: Purchased
Installable Edition: Server
Installable Environment: Physical and virtual environments
Operating System: Server, Desktop, SBS
Language: English, 日本語

Number of Licenses: 10
Please enter the number of licenses purchased

5. Please specify the host to install the product.
You can search for the host name from the networked hosts or directly enter the host name.
You can specify the criteria and filtering conditions to search for a specific networked host.
・**Windows network** : A search for host computers on the same network is performed.
・**Windows Active Directory** : A list of host computers in the specified Active Directory is obtained.
・**Search all computers** ： All hosts are searched.
・**Search by Product Installed** : The hosts on which ActiveImage Protector is installed are listed.
・**Search No Product Installed** : The hosts on which ActiveImage Protector is not installed are listed
This example shows that [Search all computers] option is selected. Check the checkbox for “SERVER02” in the host list on which ActiveImage Protector is not installed, and click [Next].



NetJapan Push Installer

Select Target Computer

● Discover ○ Manual

Search Conditions

☑ Windows Network

□ Windows Active Directory

Domain

Admin Username

Password

● Search all computers

○ Search by Product Installed

ActiveImage Protecto

○ Search No Product Installed

Target Computers Hide NON-CONTACTABLE item:

License(s) Available: 9/10

Computers	Domain	IP Address	Operating System	Product	Edition	Version	License	Expiration
☑ SERVER02	root	192.168.12...						
□ CPC04	root	192.168.12...						
□ CPC01	root	192.168.12...						

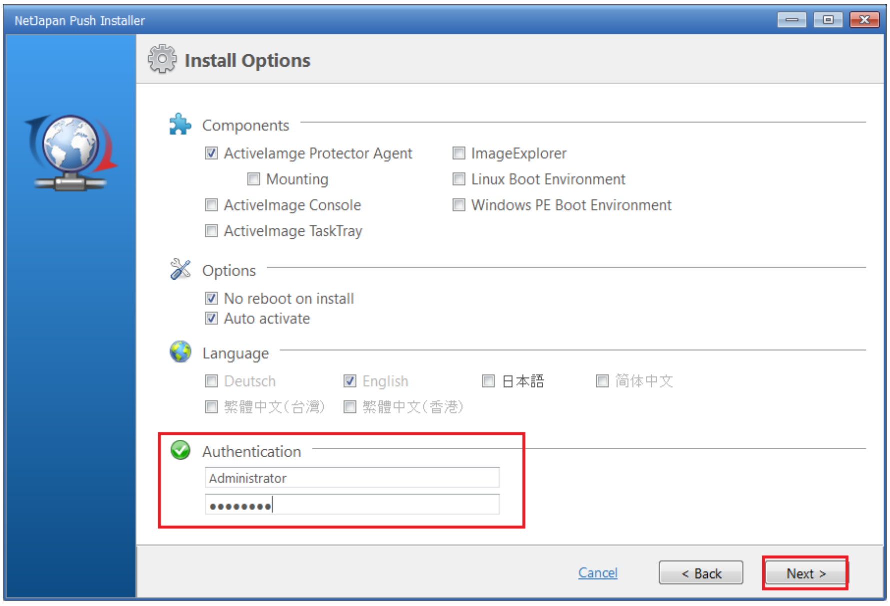
Total Computers: 3

6. You can configure the installation option settings. Please select the components to install in **[Component]** option. **[Options]** provides the options for post-installation behavior (reboot / activate).

・**Do not reboot the system** : Select this option not to reboot the system upon completion of the product installation. Your computer must be restarted to complete the installation and start operation of the ActiveImage Protector agent even when this option is enabled.

・**Automatically activate** : Upon completion of the product installation you can predefine whether the product is automatically activated.

Enter credentials and click **[Next]**.



Install Options

Components

☑ Activelamge Protector Agent

□ Mounting

□ ActiveImage Console

□ ActiveImage TaskTray

□ ImageExplorer

□ Linux Boot Environment

□ Windows PE Boot Environment

Options

☑ No reboot on install

☑ Auto activate

Language

□ Deutsch ☑ English □ 日本語 □ 简体中文

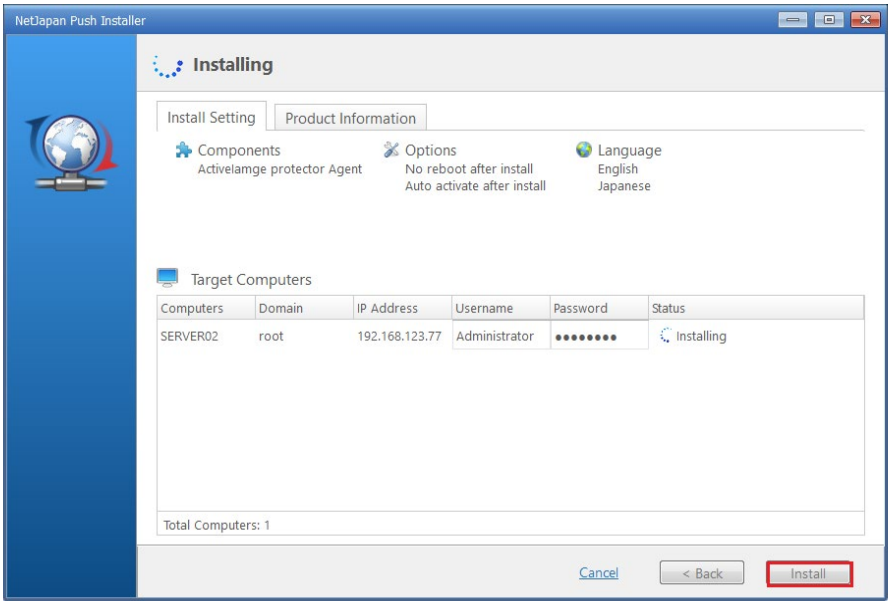
□ 繁體中文(台灣) □ 繁體中文(香港)

Authentication

Administrator

••••••••

7. Review the settings and click **[Install]**. Installation of ActiveImage Protector starts.



Installing

Components
Activelamge protector Agent

Options
No reboot after install
Auto activate after install

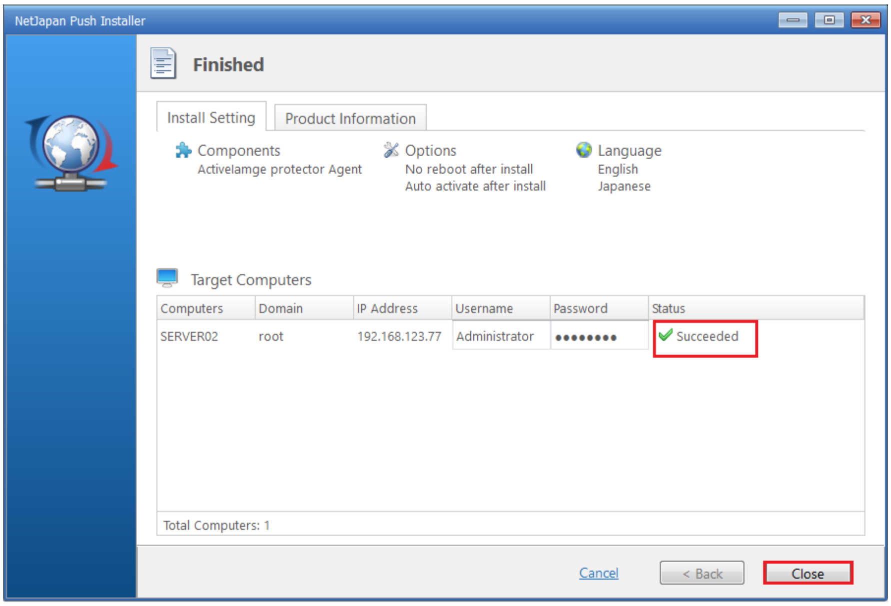
Language
English
Japanese

Target Computers

Computers	Domain	IP Address	Username	Password	Status
SERVER02	root	192.168.123.77	Administrator	••••••••	Installing

Total Computers: 1

8. Upon completion of installation, **[Succeeded]** is indicated for **[Status]** in the following window. Click **[Close]** to end Push Install.



Finished

Components
Activelamge protector Agent

Options
No reboot after install
Auto activate after install

Language
English
Japanese

Target Computers

Computers	Domain	IP Address	Username	Password	Status
SERVER02	root	192.168.123.77	Administrator	••••••••	✓ Succeeded

Total Computers: 1

10-2. Network client management console

You can monitor the status and manage ActiveImage Protector installed on a networked remote host.

1. Start ActiveImage Protector.

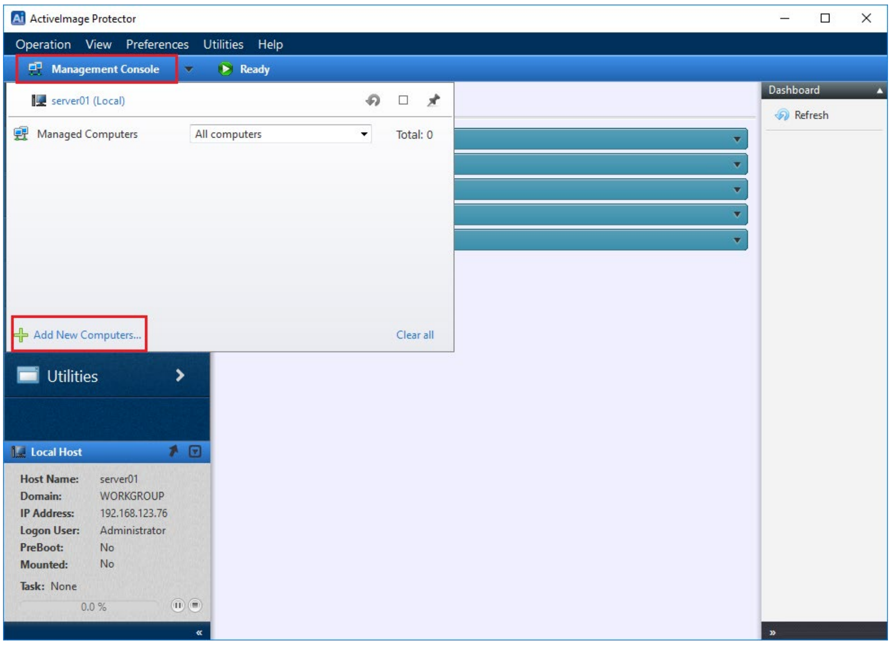
   Windows Server 2008 R2 or earlier server OS:
   Click **[Start]** – **[All Programs]** – **[NetJapan]** – **[ActiveImage Protector]**.

   Windows 7 or earlier Desktop OS:
   Click [Start] – [All Programs] – [NetJapan] – [ActiveImage Protector].

   Windows Server 2012 or later server OS:
   Click [Start] – [Applications] – [NetJapan] – [ActiveImage Protector].

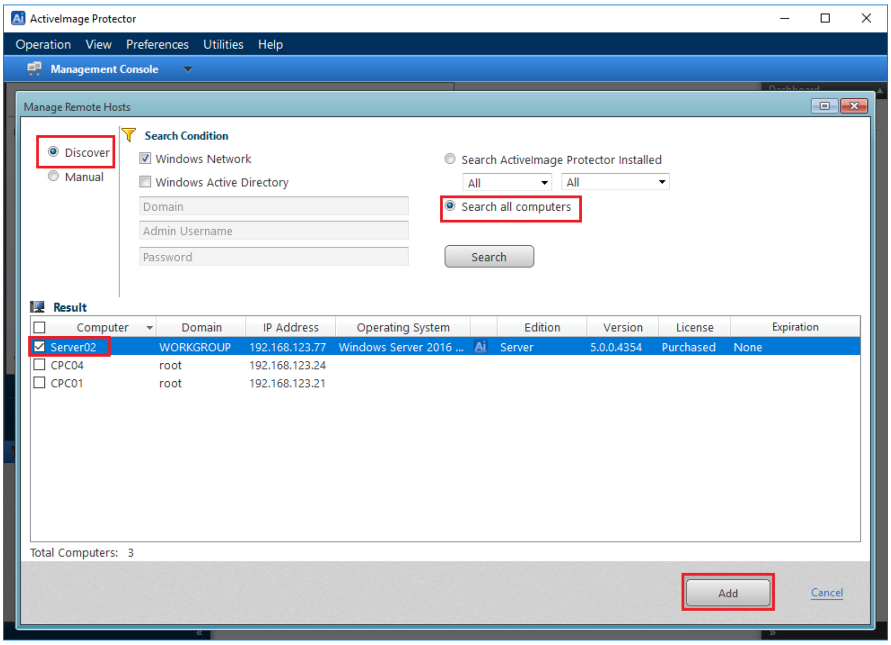
   Windows Server 8 or later Desktop OS :
   Click [Start] – [Applications] – [NetJapan] – [ActiveImage Protector].

2. Before you start using Remote Control feature, you need to display a list of remote hosts in **[Management Console]** window. Click **[Add New Computers]**.



Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

3. Specify the host to add to the list. You can add a new computer by selecting **[Discover]** or [**Manual**]. This example show that [Discover] and [Search all computers] option are selected. Check the checkbox for “Server02” in the host list and click **[Add]**.



● Discover
○ Manual

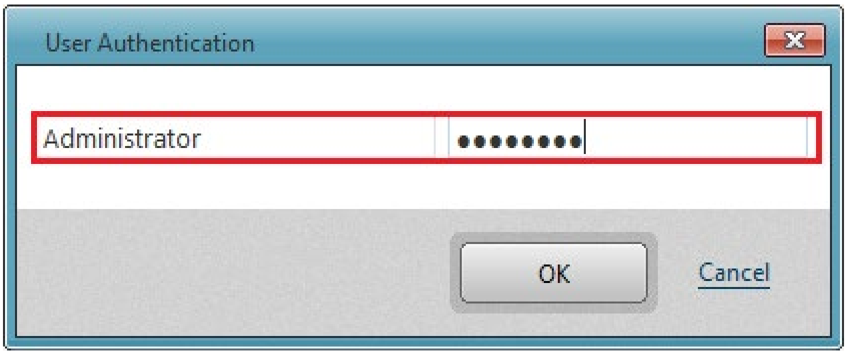
☑ Windows Network
☐ Windows Active Directory

○ Search ActiveImage Protector Installed
All All
● Search all computers

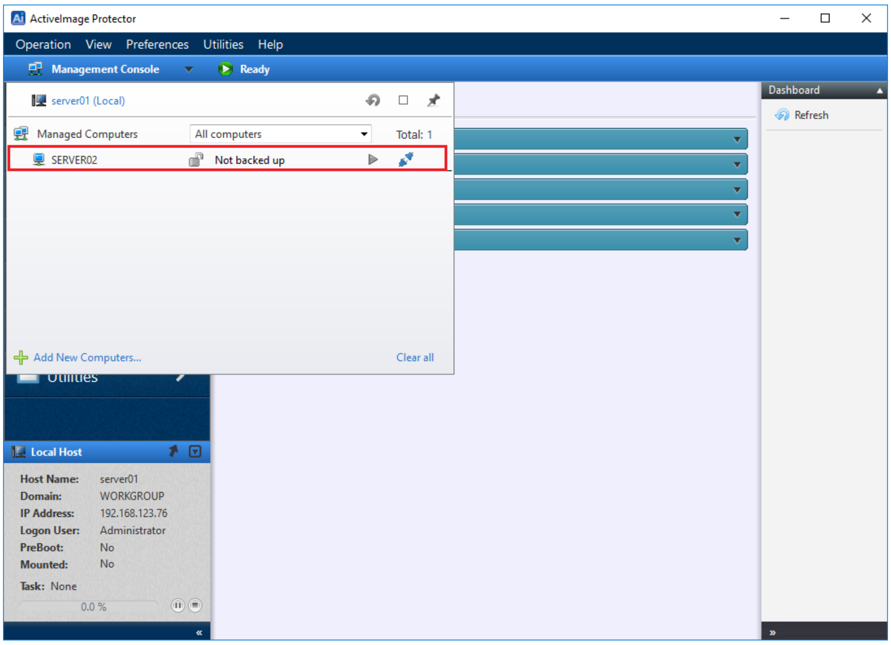
☐ Computer	Domain	IP Address	Operating System	Edition	Version	License	Expiration
☑ Server02	WORKGROUP	192.168.123.77	Windows Server 2016 ...	Server	5.0.0.4354	Purchased	None
☐ CPC04	root	192.168.123.24					
☐ CPC01	root	192.168.123.21					

Total Computers: 3

4. Enter the credentials to access the host.

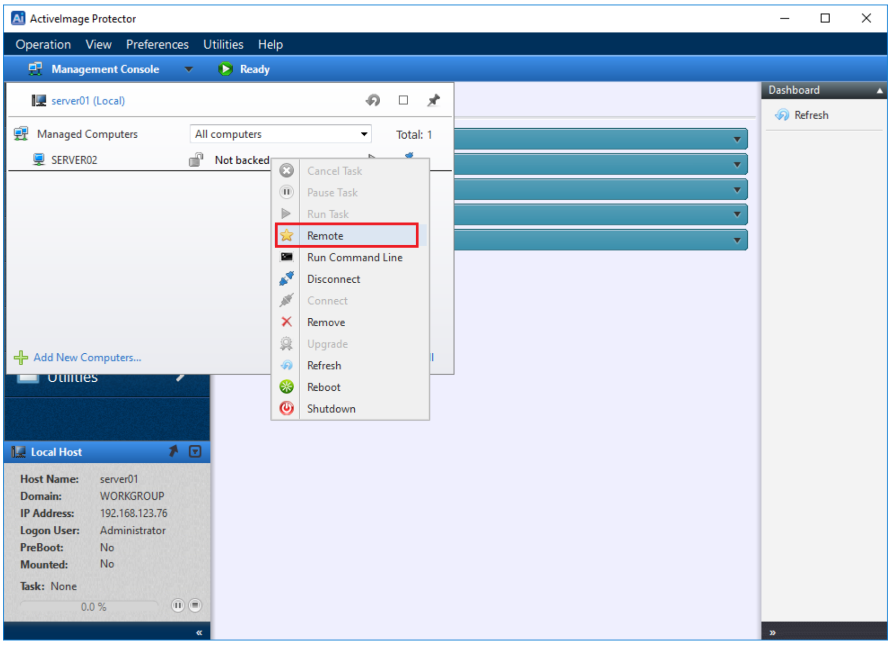


5. “Server02” is added to the Managed Computers list.



Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

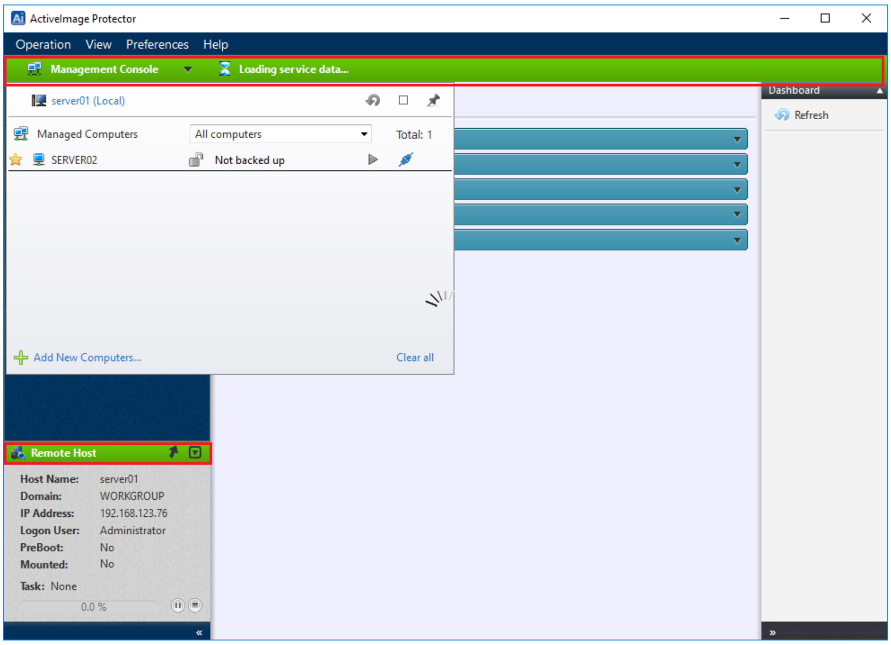
6. Select a host from the list and double-click or right-click on the host. Select [Remote] from the context menu to directly connect to agent installed on remote host from the console.



SERVER02 Not backed

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None

7. When connection is successfully established, the status bar is green-colored. Now one-click offers execution of scheduling backup tasks on remote network hosts and monitoring log information.



SERVER02 Not backed up

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None

8. Double-click on the local host name to disconnect from the remote host.

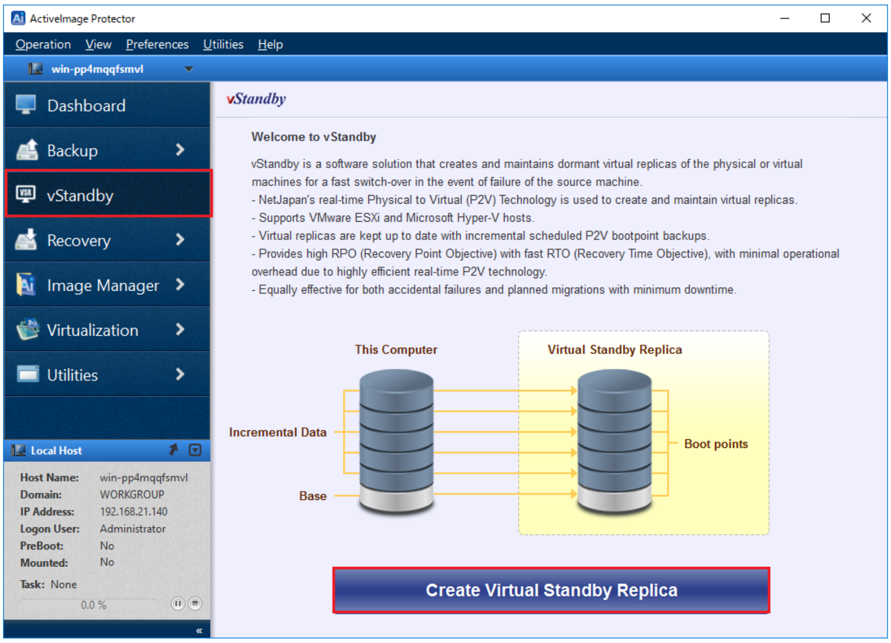
11. vStandby

vStandby is a software solution that creates and maintains dormant virtual replicas of physical or virtual machines to provide a switch-over option in the event of failure of the source machine. This virtual standby virtual replica is kept current by taking scheduled incremental P2V boot points of the source machine. This ensures a successful start-up of the standby virtual machine created at the point in time before the system failure. vStandby is equally valuable as a tool for migrating legacy physical machines to an ESXi or Hyper-V host in real-time. Minimal downtime is expected as Actiphy's P2V technology is utilized for the migration of the legacy machines.

Note) The vStandby function is invalid on ActiveImage Protector for Hyper-V Enterprise.

For detailed system requirements, please refer to Actiphy web site.

1. To start creating a virtual standby replica, click **[vStandby]** from the left menu. **[Welcome to vStandby]** window is displayed. Click **[Create Virtual Standby Replica]**.

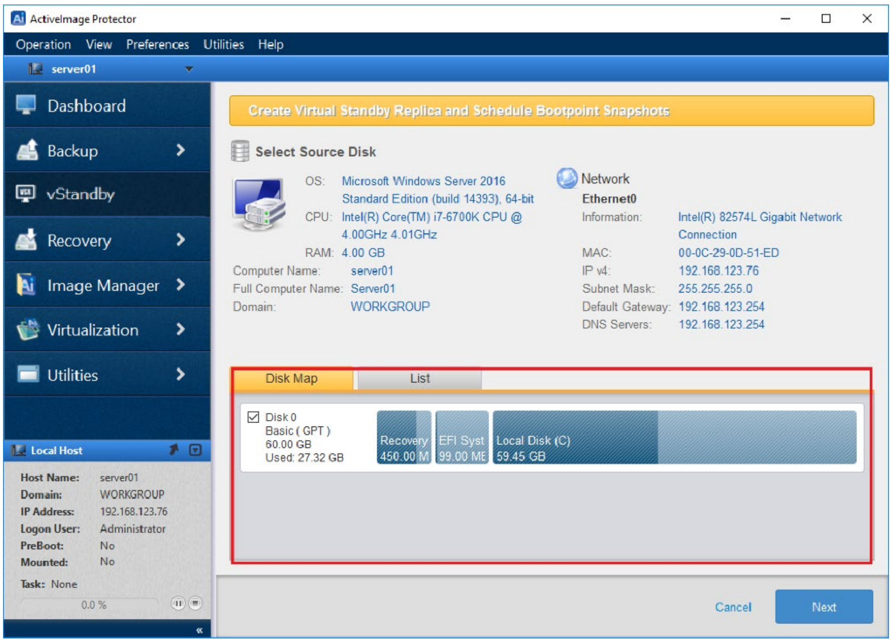


Welcome to vStandby

vStandby is a software solution that creates and maintains dormant virtual replicas of the physical or virtual machines for a fast switch-over in the event of failure of the source machine.
- NetJapan's real-time Physical to Virtual (P2V) Technology is used to create and maintain virtual replicas.
- Supports VMware ESXi and Microsoft Hyper-V hosts.
- Virtual replicas are kept up to date with incremental scheduled P2V bootpoint backups.
- Provides high RPO (Recovery Point Objective) with fast RTO (Recovery Time Objective), with minimal operational overhead due to highly efficient real-time P2V technology.
- Equally effective for both accidental failures and planned migrations with minimum downtime.

Host Name: win-pp4mqqfsmvl
Domain: WORKGROUP
IP Address: 192.168.21.140
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

2. Select the source disk to create the standby virtual machine by checking the checkbox for the source disk in the disk map or the list. Click **[Next]**.



Create Virtual Standby Replica and Schedule Bootpoint Snapshots

Select Source Disk

OS: Microsoft Windows Server 2016 Standard Edition (build 14393), 64-bit
CPU: Intel(R) Core(TM) i7-6700K CPU @ 4.00GHz 4.01GHz
RAM: 4.00 GB
Computer Name: server01
Full Computer Name: Server01
Domain: WORKGROUP

Network
Ethernet0
Information: Intel(R) 82574L Gigabit Network Connection
MAC: 00-0C-29-0D-51-ED
IP v4: 192.168.123.76
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.123.254
DNS Servers: 192.168.123.254

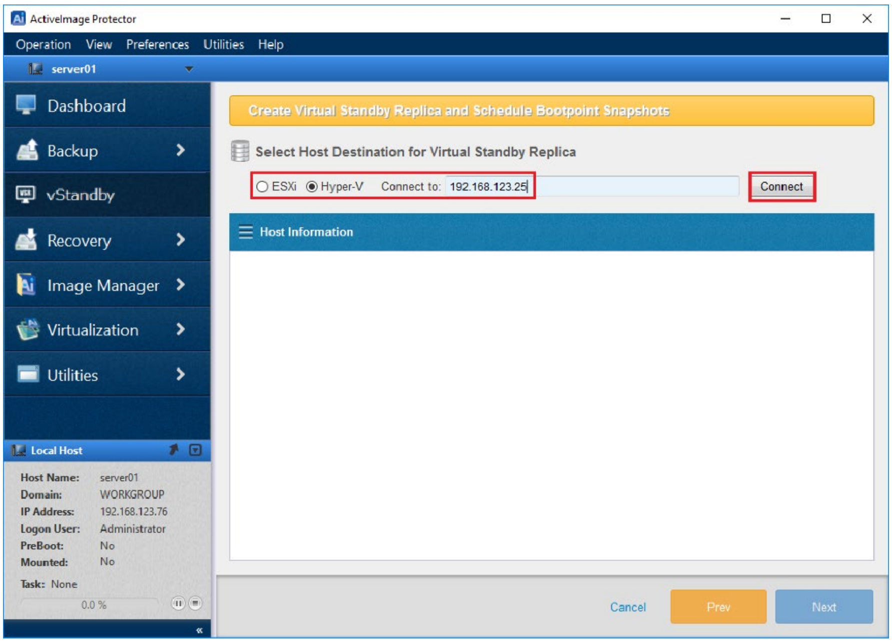
Disk Map | List

☑ Disk 0
Basic (GPT)
60.00 GB
Used: 27.32 GB

Recovery 450.00 M | EFI Syst 99.00 ME | Local Disk (C) 59.45 GB

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

3. Select ESXi or Hyper-V for the target host to create virtual standby replica. This example shows that [Hyper-V] is selected. Enter “192.168.123.25 “ and click [Connect].



Create Virtual Standby Replica and Schedule Bootpoint Snapshots

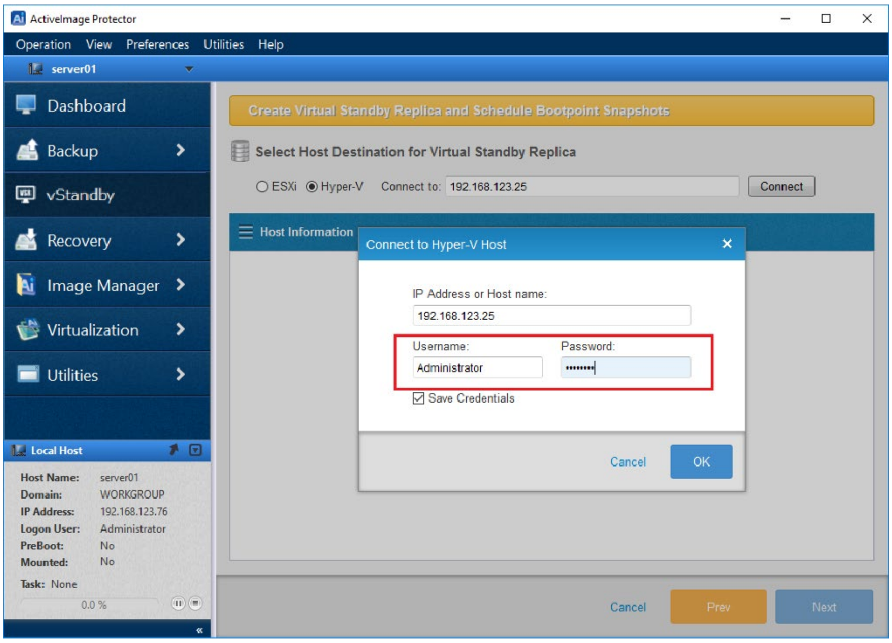
Select Host Destination for Virtual Standby Replica

○ ESXi ● Hyper-V Connect to: 192.168.123.25

Host Information

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

4. Enter credentials to log in Hyper-V host. Enter “Administrator” for [User Name] and the predefined password for [Password].



Select Host Destination for Virtual Standby Replica

○ ESXi ● Hyper-V Connect to: 192.168.123.25

Connect to Hyper-V Host

IP Address or Host name: 192.168.123.25

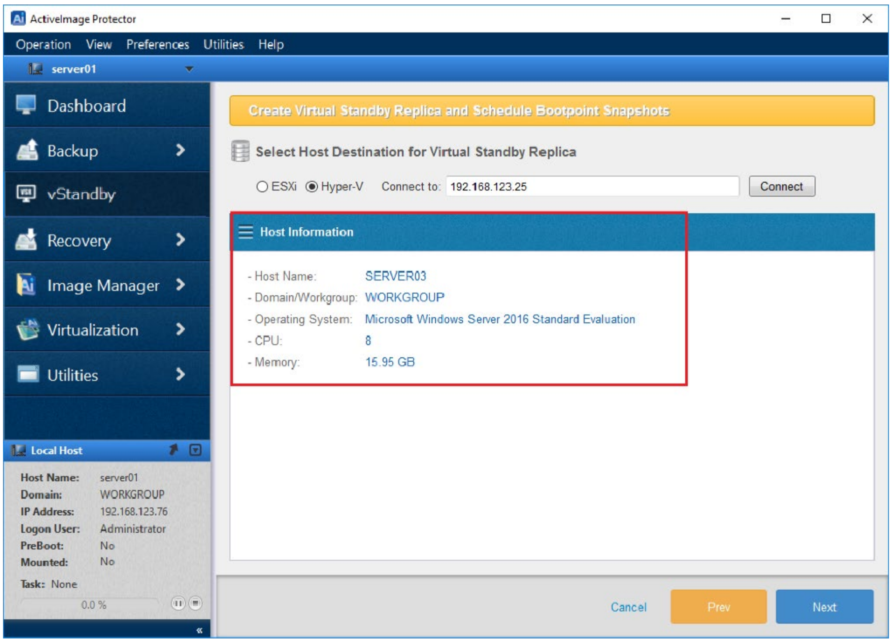
Username: Administrator

Password: ••••••••

☑ Save Credentials

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

5. Hyper-V Host Information is displayed. Click **[Next]**.



Select Host Destination for Virtual Standby Replica

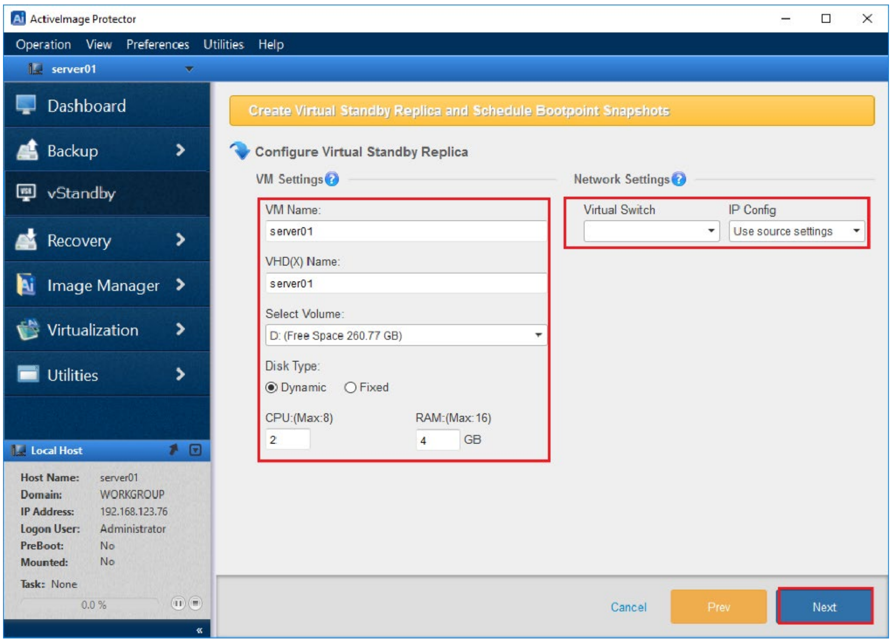
○ ESXi ● Hyper-V Connect to: 192.168.123.25

Host Information

- Host Name: SERVER03
- Domain/Workgroup: WORKGROUP
- Operating System: Microsoft Windows Server 2016 Standard Evaluation
- CPU: 8
- Memory: 15.95 GB

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

6. **[Configure Virtual Standby Replica]** window is displayed. Please configure the virtual standby replica settings. In **[VM Settings]** please enter **[VM Name]**, **[VHD(X) Name]**, **[Select Volume]**, **[Disk Type]**. In Network Settings please enter **[Virtual Switch]**, **[IP Config]**. Click **[Next]**. **[Virtual Switch]** is configured on host machine and **[IP Address]** configured on source machine.



Configure Virtual Standby Replica

VM Settings

VM Name: server01

VHD(X) Name: server01

Select Volume: D: (Free Space 260.77 GB)

Disk Type: ● Dynamic ○ Fixed

CPU:(Max:8) 2

RAM:(Max:16) 4 GB

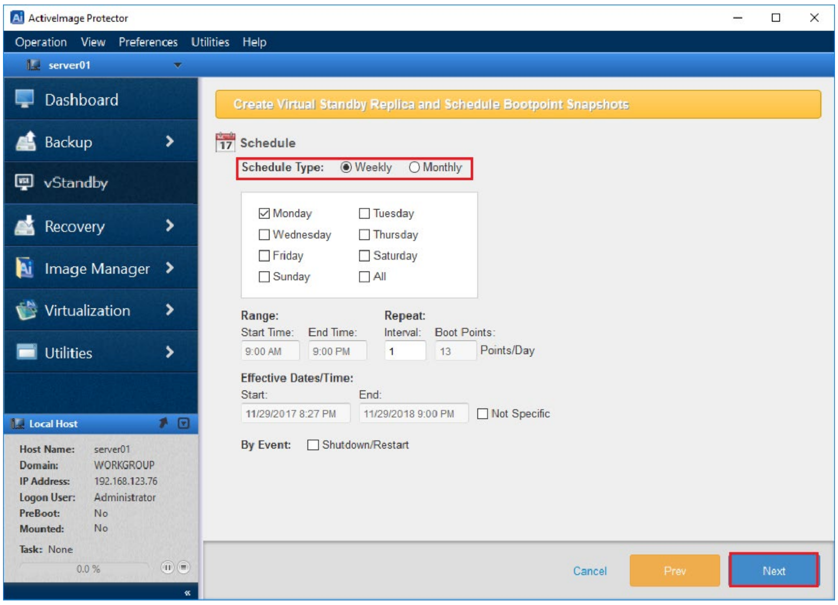
Network Settings

Virtual Switch:

IP Config: Use source settings

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

7. You can configure weekly or monthly intervals for creating incremental boot points of the standby virtual machine. The following example shows Weekly schedule setting window. Click **[Next]**.



Schedule

Schedule Type: ● Weekly ○ Monthly

☑ Monday ☐ Tuesday
☐ Wednesday ☐ Thursday
☐ Friday ☐ Saturday
☐ Sunday ☐ All

Range:
Start Time: 9:00 AM
End Time: 9:00 PM

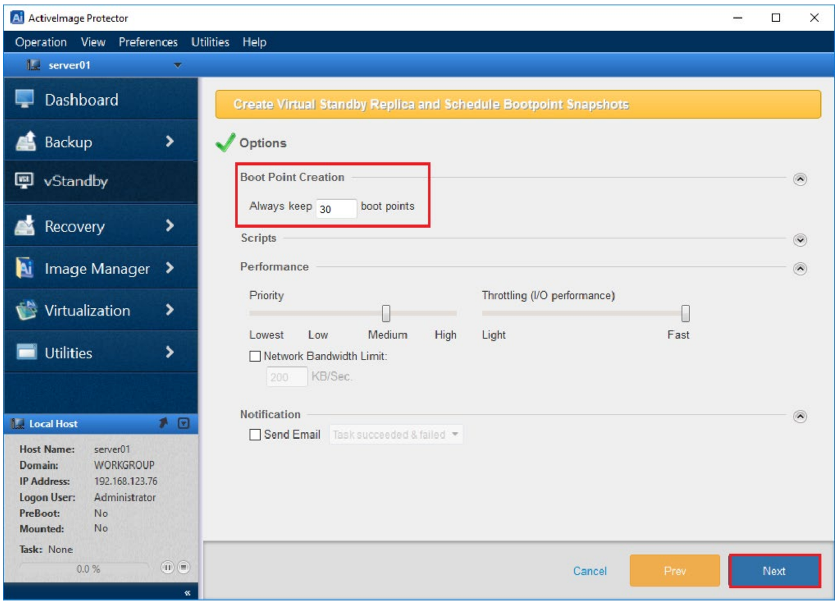
Repeat:
Interval: 1
Boot Points: 13 Points/Day

Effective Dates/Time:
Start: 11/29/2017 8:27 PM
End: 11/29/2018 9:00 PM
☐ Not Specific

By Event: ☐ Shutdown/Restart

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

8. Please configure the option settings. You can configure the maximum limit (up to 30) for the number of boot points to create for a virtual standby replica. When the number of the boot points reaches the predefined limit, the most and the second obsolete boot points are merged.
Set the priority for the vStandby Windows process. Adjusting the priority setting can allocate more or less CPU time for the vStandby processes. This is all dependent on the number of other mission critical applications running on the protected machine. Click **[Next]**.



Options

Boot Point Creation
Always keep 30 boot points

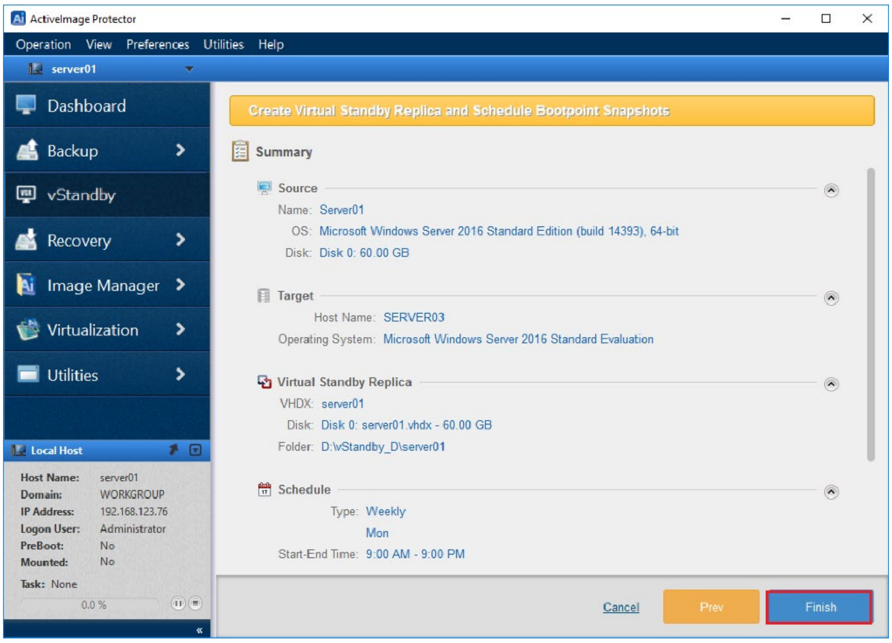
Scripts

Performance
Priority
Throttling (I/O performance)
☐ Network Bandwidth Limit:
200 KB/Sec.

Notification
☐ Send Email Task succeeded & failed

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

9. **[Summary]** window is displayed. Review the settings and click **[Finish]**.



Create Virtual Standby Replica and Schedule Bootpoint Snapshots

Summary

Source
Name: Server01
OS: Microsoft Windows Server 2016 Standard Edition (build 14393), 64-bit
Disk: Disk 0: 60.00 GB

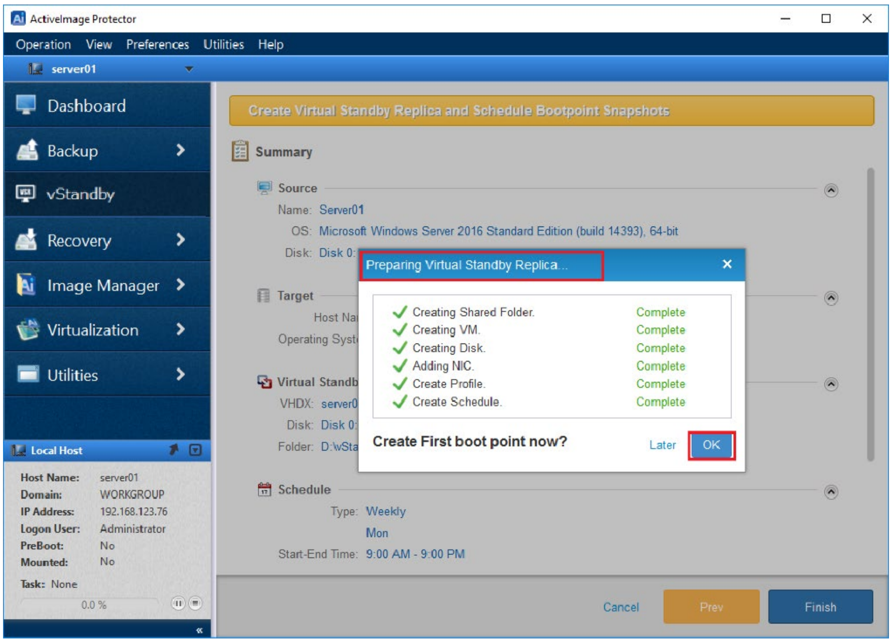
Target
Host Name: SERVER03
Operating System: Microsoft Windows Server 2016 Standard Evaluation

Virtual Standby Replica
VHDX: server01
Disk: Disk 0: server01.vhdx - 60.00 GB
Folder: D:\vStandby_D\server01

Schedule
Type: Weekly
Mon
Start-End Time: 9:00 AM - 9:00 PM

Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None

10. vStandby task is created. If you want to run the task immediately, click **[OK]**.

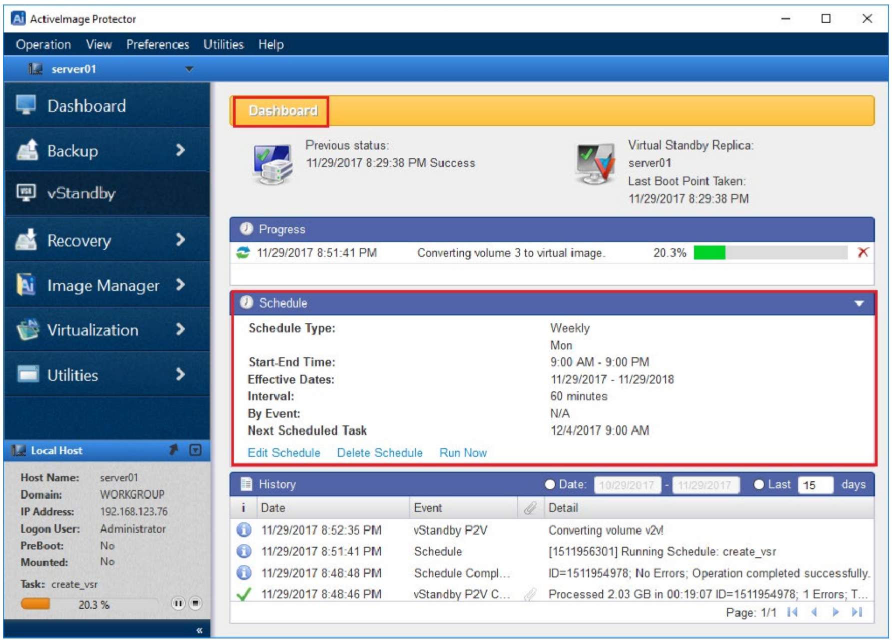


Preparing Virtual Standby Replica...

✓ Creating Shared Folder. Complete
✓ Creating VM. Complete
✓ Creating Disk. Complete
✓ Adding NIC. Complete
✓ Create Profile. Complete
✓ Create Schedule. Complete

Create First boot point now?

11. Dashboard monitors scheduled recurring tasks.



Previous status:
11/29/2017 8:29:38 PM Success

Virtual Standby Replica:
server01
Last Boot Point Taken:
11/29/2017 8:29:38 PM

Progress: 11/29/2017 8:51:41 PM Converting volume 3 to virtual image. 20.3%

Schedule Type:	Weekly Mon
Start-End Time:	9:00 AM - 9:00 PM
Effective Dates:	11/29/2017 - 11/29/2018
Interval:	60 minutes
By Event:	N/A
Next Scheduled Task	12/4/2017 9:00 AM

History: ○ Date: 10/29/2017 - 11/29/2017 ○ Last 15 days

i	Date	Event		Detail
ⓘ	11/29/2017 8:52:35 PM	vStandby P2V		Converting volume v2v!
ⓘ	11/29/2017 8:51:41 PM	Schedule		[1511956301] Running Schedule: create_vsr
ⓘ	11/29/2017 8:48:48 PM	Schedule Compl...		ID=1511954978; No Errors; Operation completed successfully.
✓	11/29/2017 8:48:46 PM	vStandby P2V C...		Processed 2.03 GB in 00:19:07 ID=1511954978; 1 Errors; T...

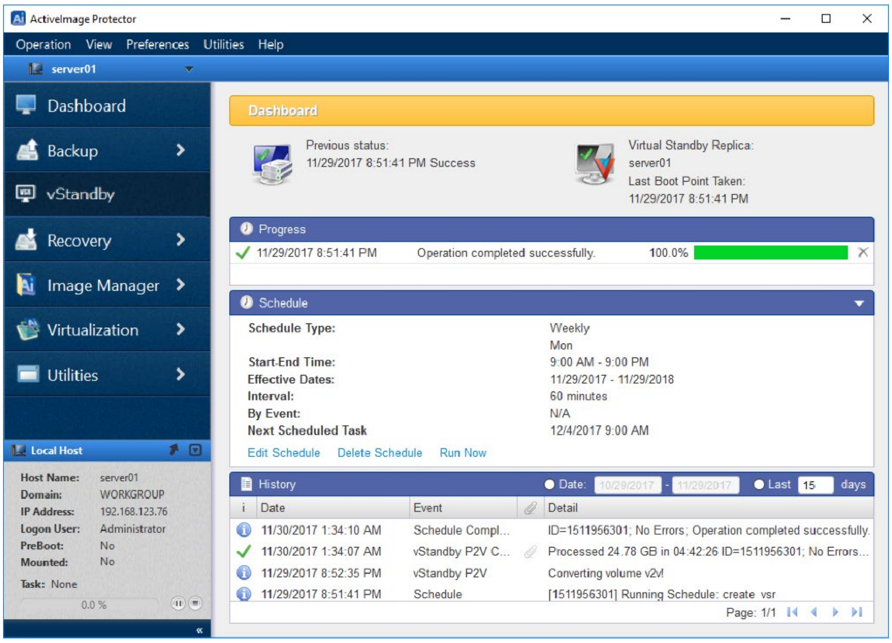
Page: 1/1

Host Name:	server01
Domain:	WORKGROUP
IP Address:	192.168.123.76
Logon User:	Administrator
PreBoot:	No
Mounted:	No

Task: create_vsr

20.3 %

12. When a virtual standby replica is created, the following window is displayed.



Host Name: server01
Domain: WORKGROUP
IP Address: 192.168.123.76
Logon User: Administrator
PreBoot: No
Mounted: No
Task: None
0.0 %

Dashboard

Previous status:
11/29/2017 8:51:41 PM Success

Virtual Standby Replica:
server01
Last Boot Point Taken:
11/29/2017 8:51:41 PM

Progress

✓ 11/29/2017 8:51:41 PM Operation completed successfully. 100.0%

Schedule

Schedule Type:	Weekly Mon
Start-End Time:	9:00 AM - 9:00 PM
Effective Dates:	11/29/2017 - 11/29/2018
Interval:	60 minutes
By Event:	N/A
Next Scheduled Task	12/4/2017 9:00 AM

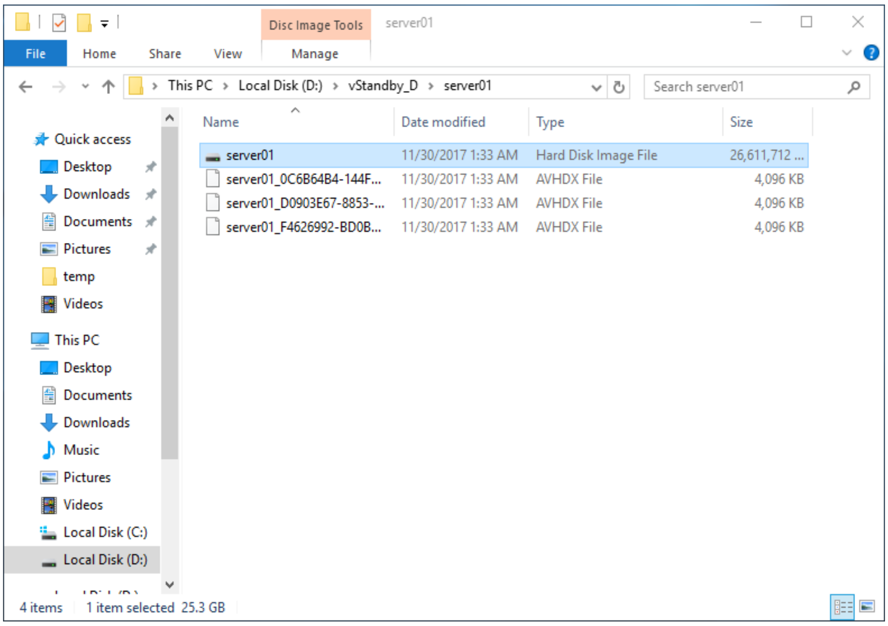
Edit Schedule Delete Schedule Run Now

History ○ Date: 10/29/2017 - 11/29/2017 ○ Last 15 days

i	Date	Event		Detail
ⓘ	11/30/2017 1:34:10 AM	Schedule Compl...		ID=1511956301; No Errors; Operation completed successfully.
✓	11/30/2017 1:34:07 AM	vStandby P2V C...		Processed 24.78 GB in 04:42:26 ID=1511956301; No Errors...
ⓘ	11/29/2017 8:52:35 PM	vStandby P2V		Converting volume v2v!
ⓘ	11/29/2017 8:51:41 PM	Schedule		[1511956301] Running Schedule: create vsr

Page: 1/1

13. On Hyper-V host, you can monitor the virtual standby replica as follows.



Name	Date modified	Type	Size
server01	11/30/2017 1:33 AM	Hard Disk Image File	26,611,712 ...
server01_0C6B64B4-144F...	11/30/2017 1:33 AM	AVHDX File	4,096 KB
server01_D0903E67-8853-...	11/30/2017 1:33 AM	AVHDX File	4,096 KB
server01_F4626992-BD0B...	11/30/2017 1:33 AM	AVHDX File	4,096 KB

4 items 1 item selected 25.3 GB

12. HyperBoot

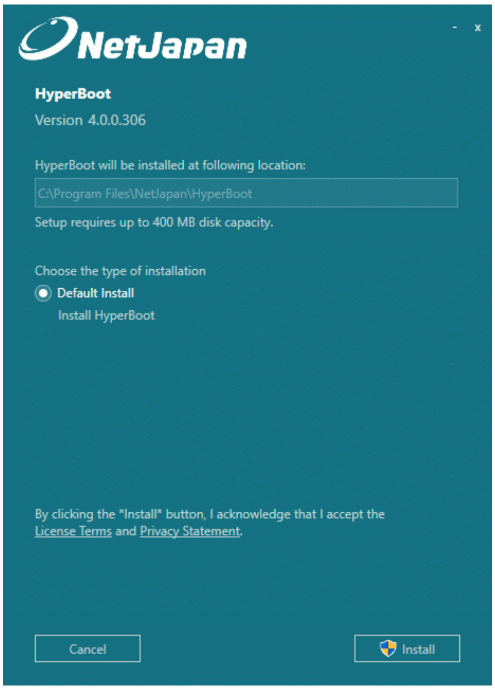
HyperBoot, developed based on Actiphy's virtual conversion technology, immediately starts a virtual machine from any ActiveImage Protector backup image file, bypassing lengthy physical to virtual conversion and recovery process. As is often the case, it takes about a couple of hours to restore a 1TB backup image file. The use of HyperBoot enables you to boot a backup image file as a virtual machine in as little as two minutes. The supported hypervisors are Microsoft Hyper-V, VMware Workstation/Player, ESXi and Hyper-V on remote host.

Note) When you wish to use HyperBoot, please visit our website and download it at free of charge.

The following are the examples for practical use of HyperBoot:

- Common disaster recovery approaches include backup image boot test to provide confidence that your backup images are bootable. However, it's time consuming and cumbersome process to test every backup images. The use of HyperBoot lets you bypass the lengthy test process.
- The use of incremental backup images enables to locate the point of a server system failure. However, you need to check the entire incremental backup files to identify the cause of the problem. Combined with the recovery process, it takes quite long. The use of HyperBoot help you identify the point of failure bypassing recovery process.
- Verification of P2V migration on a variety of system environments takes long. HyperBoot provides confidence in P2V migration by using backup image files.
- vStandby, as stated above, also provides immediate start-up of standby virtual machines. The difference between the two products is that HyperBoot immediately starts from a ActiveImage Protector backup image file. HyperBoot, as well as HyperStandby, performs P2V process virtualizing an image of physical environment to virtual environment and configuring required boot settings. Without the need for making changes to the backup image files or boot environment, a backup image file of the source machine OS environment can be booted as a virtual machine. HyperBoot lets you perform testing upgraded version of an application or updated services.

1. Please download the HyperBoot setup file from Actiphy's Web site and double-click on Setup.exe to run the installer.
   The following set-up wizard will be launched.



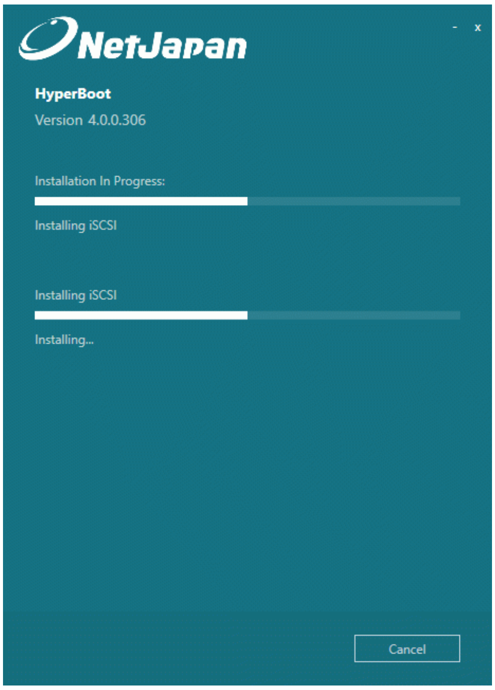
HyperBoot
Version 4.0.0.306

HyperBoot will be installed at following location:
C:\Program Files\NetJapan\HyperBoot
Setup requires up to 400 MB disk capacity.

Choose the type of installation
● Default Install
Install HyperBoot

By clicking the "Install" button, I acknowledge that I accept the License Terms and Privacy Statement.

2. You do not have to make any changes for setup.
   Click **[Install]** and the installation process starts.

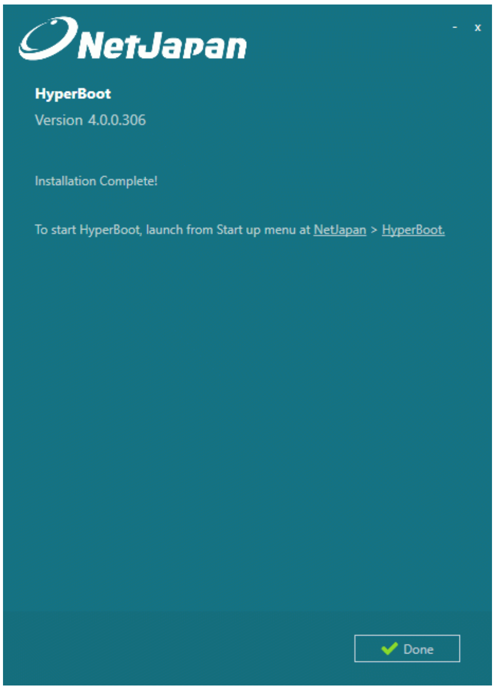


HyperBoot
Version 4.0.0.306

Installation In Progress:
Installing iSCSI

Installing iSCSI
Installing...

3. Upon completion of the installation process, the following window will be displayed.
   Click **[Done]** to end the setup wizard.



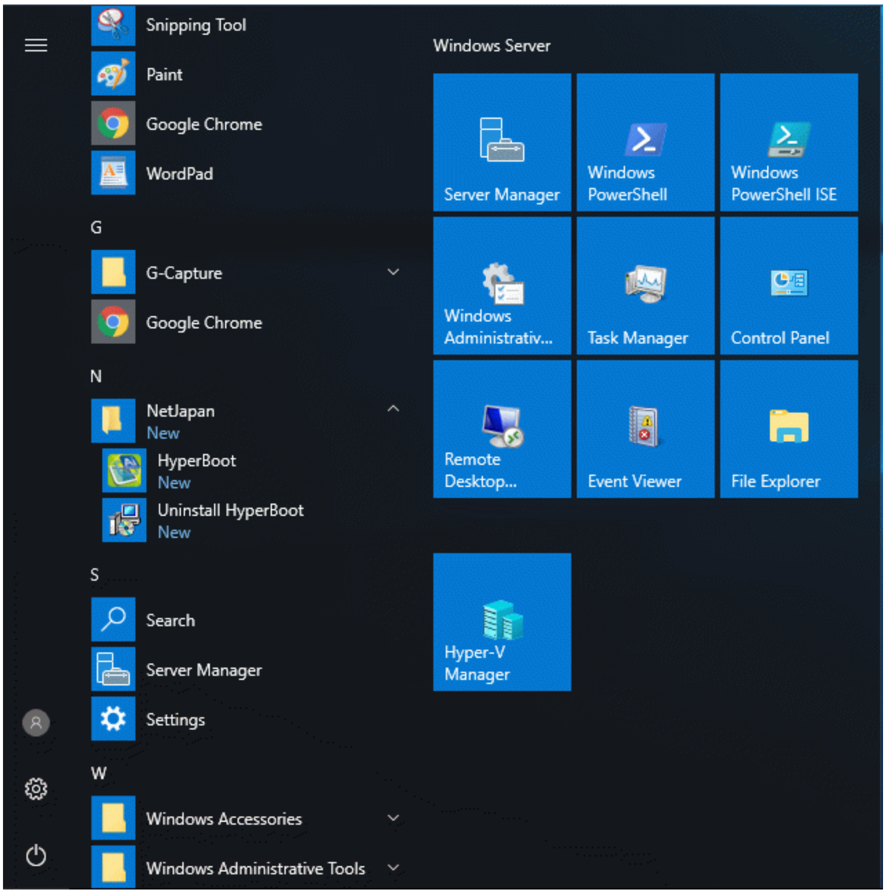
HyperBoot

Version 4.0.0.306

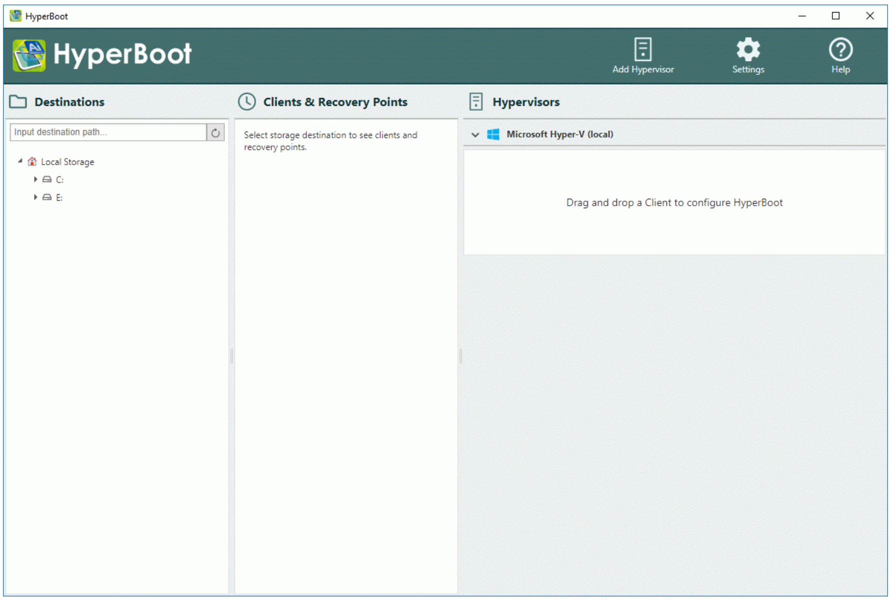
Installation Complete!

To start HyperBoot, launch from Start up menu at NetJapan > HyperBoot.

4. By default, HyperBoot shortcut icon is created on your desktop.
   Click on the shortcut icon or go to **[NetJapan]** in Start menu and select **[HyperBoot]**.



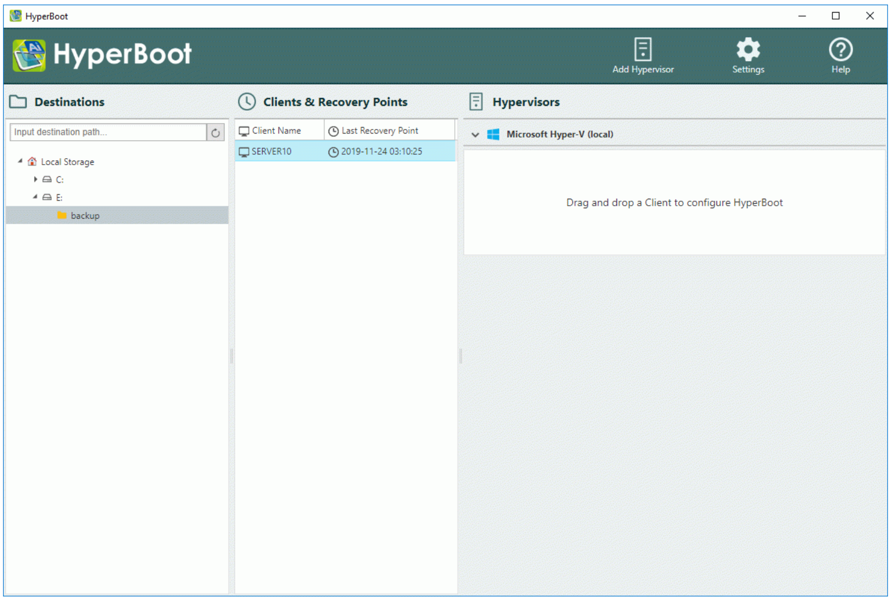
5. HyperBoot is started.



Select storage destination to see clients and recovery points.

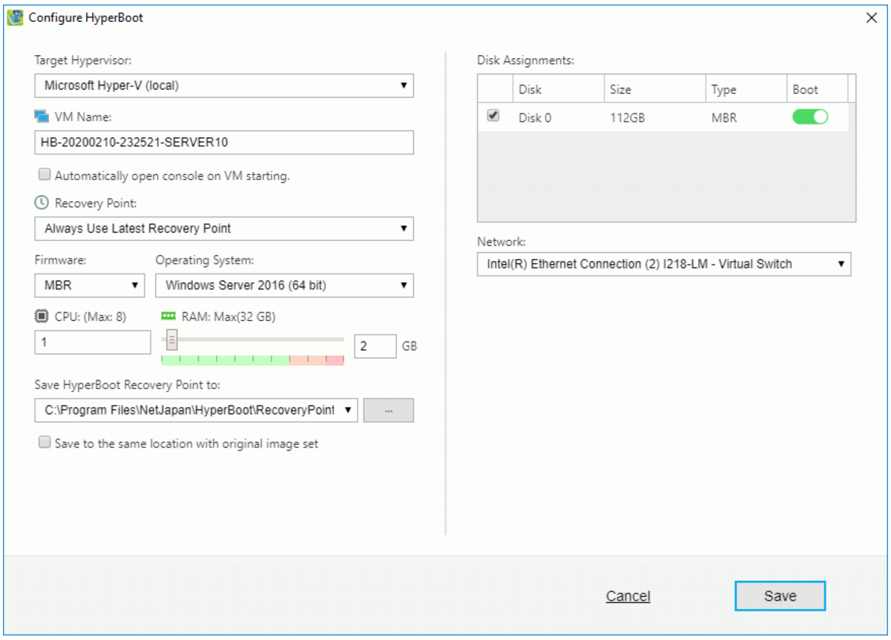
Drag and drop a Client to configure HyperBoot

6. Select an ActiveImage Protector backup image file in **[Destination]** and the latest recovery point.


HyperBoot
HyperBoot
Add Hypervisor
Settings
Help
Destinations
Clients & Recovery Points
Hypervisors
Input destination path...
Local Storage
C:
E:
backup
Microsoft Hyper-V (local)
Drag and drop a Client to configure HyperBoot

Client Name	Last Recovery Point
SERVER10	2019-11-24 03:10:25

7. Drag and drop the recovery point to the white space in the right pane. The following **[Configure HyperBoot]** window is displayed.



Target Hypervisor: Microsoft Hyper-V (local)

VM Name: HB-20200210-232521-SERVER10

□ Automatically open console on VM starting.

Recovery Point: Always Use Latest Recovery Point

Firmware: MBR

Operating System: Windows Server 2016 (64 bit)

CPU: (Max: 8) 1

RAM: Max(32 GB) 2 GB

Save HyperBoot Recovery Point to: C:\Program Files\NetJapan\HyperBoot\RecoveryPoint

□ Save to the same location with original image set

Disk Assignments:

	Disk	Size	Type	Boot
☑	Disk 0	112GB	MBR	●

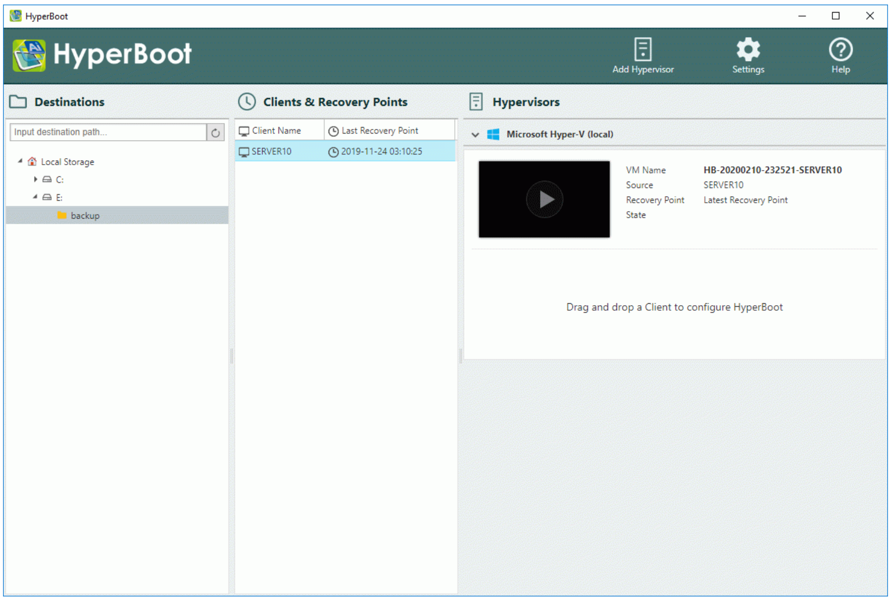
Network: Intel(R) Ethernet Connection (2) I218-LM - Virtual Switch

Select a hypervisor. In this example, “Microsoft Hyper-V” is selected. Please also configure the settings for CPU, RAM, Network, etc. You may change the VM name, if necessary.

Specify a location for **[Save HyperBoot Recovery Point to]**. If you do not change the location, the default location is selected. Or, check in the checkbox for **[Save to the same location with original image set]** to select the same location as original image set. HyperBoot enables you to boot a backup image on a hypervisor on remote host.

Upon completion of configuring the settings, click **[Save]**.

8. The virtual machine to boot is listed in **[Hypervisor]**.

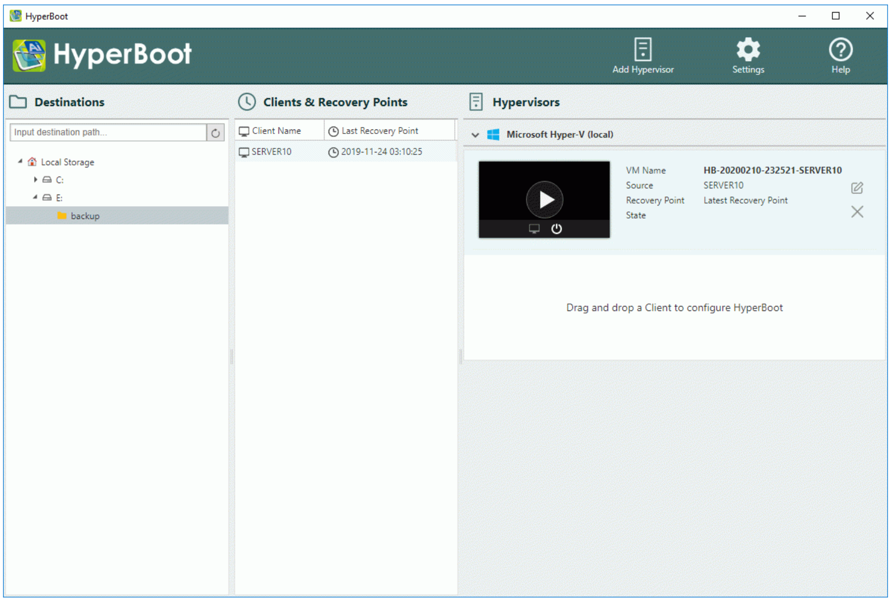


Client Name	Last Recovery Point
SERVER10	2019-11-24 03:10:25

VM Name HB-20200210-232521-SERVER10
Source SERVER10
Recovery Point Latest Recovery Point
State

Drag and drop a Client to configure HyperBoot

9. Mouse-over the thumbnail and two buttons are shown.



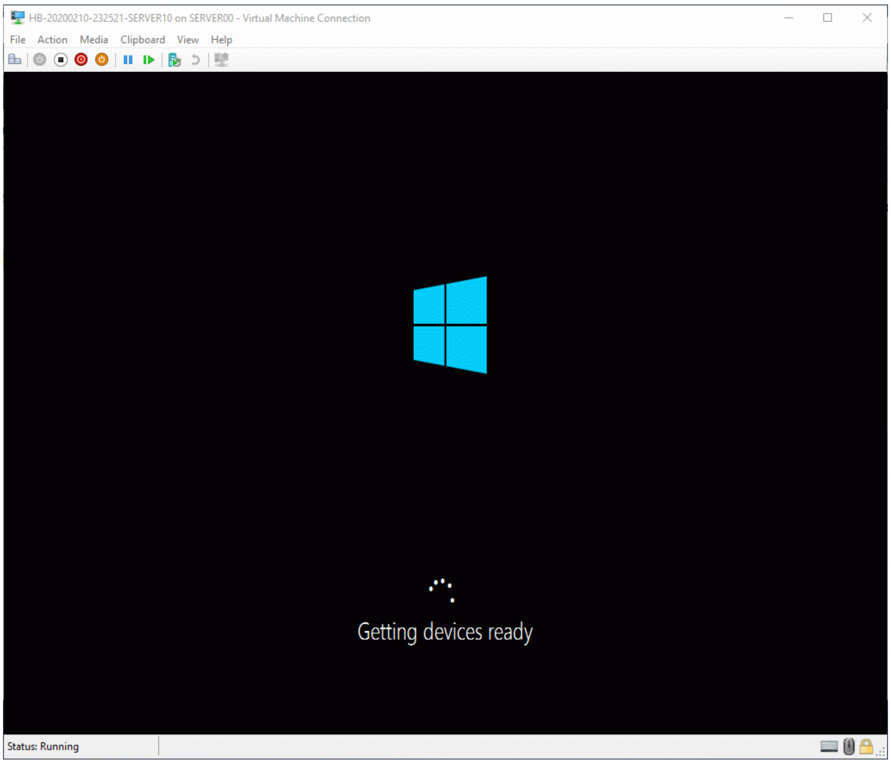
Client Name	Last Recovery Point
SERVER10	2019-11-24 03:10:25

VM Name	HB-20200210-232521-SERVER10
Source	SERVER10
Recovery Point	Latest Recovery Point
State	

Drag and drop a Client to configure HyperBoot

Click on the left button to display the connection console. Click on the right button to switch on/off the virtual machine. When the virtual machine boots up, click the button to connect to the connection console.

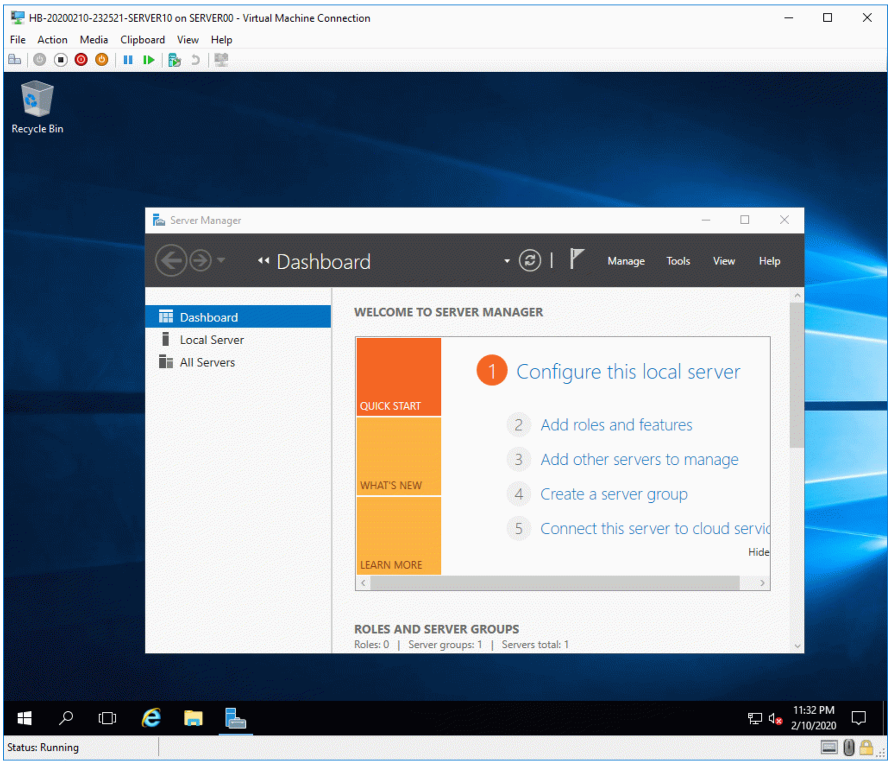
10. Click on the triangle button and switch-on/off button in the thumbnail to boot up the virtual machine. When booting up, the devices are getting ready.


HB-20200210-232521-SERVER10 on SERVER00 - Virtual Machine Connection
File
Action
Media
Clipboard
View
Help

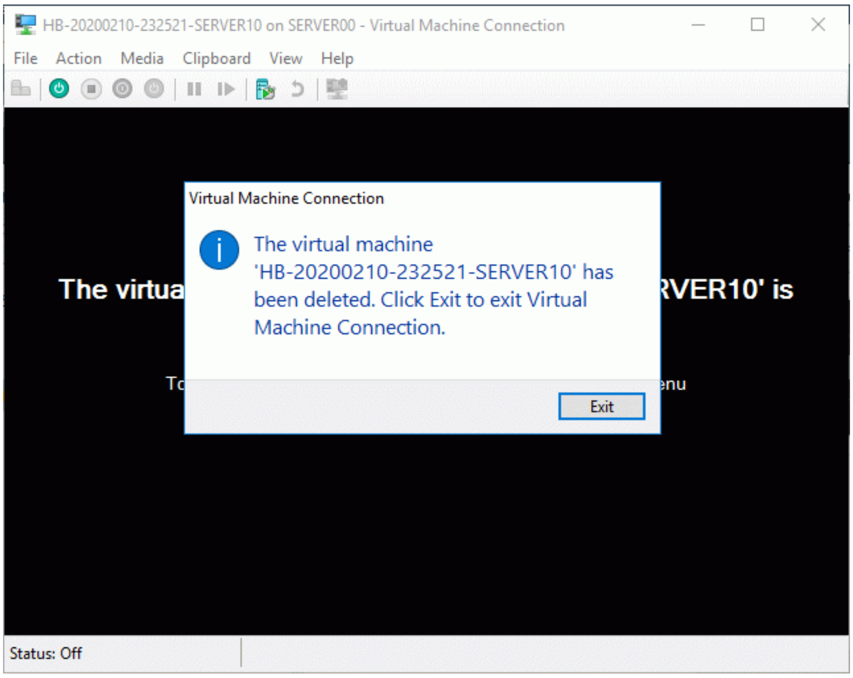
Getting devices ready

Status: Running

11. In this example, the virtual machine is booted from a backup image file of Windows Server 2016.


HB-20200210-232521-SERVER10 on SERVER00 - Virtual Machine Connection
File Action Media Clipboard View Help
Recycle Bin
Server Manager
Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud servic
Hide
ROLES AND SERVER GROUPS
Roles: 0 | Server groups: 1 | Servers total: 1
11:32 PM
2/10/2020
Status: Running

12. When the virtual machine shuts down, the following window is displayed. Click **[Exit]** to terminate the connection with the virtual machine.
When the virtual machine shuts down, the created virtual machine will be automatically deleted.


HB-20200210-232521-SERVER10 on SERVER00 - Virtual Machine Connection
File Action Media Clipboard View Help
The virtua
RVER10' is
To
enu
Virtual Machine Connection

The virtual machine 'HB-20200210-232521-SERVER10' has been deleted. Click Exit to exit Virtual Machine Connection.

APPENDIX A: Replicate backup data to Google Drive

This chapter provides you the description about the operating procedures how to obtain the following information required to configure Google Drive as the replication target.

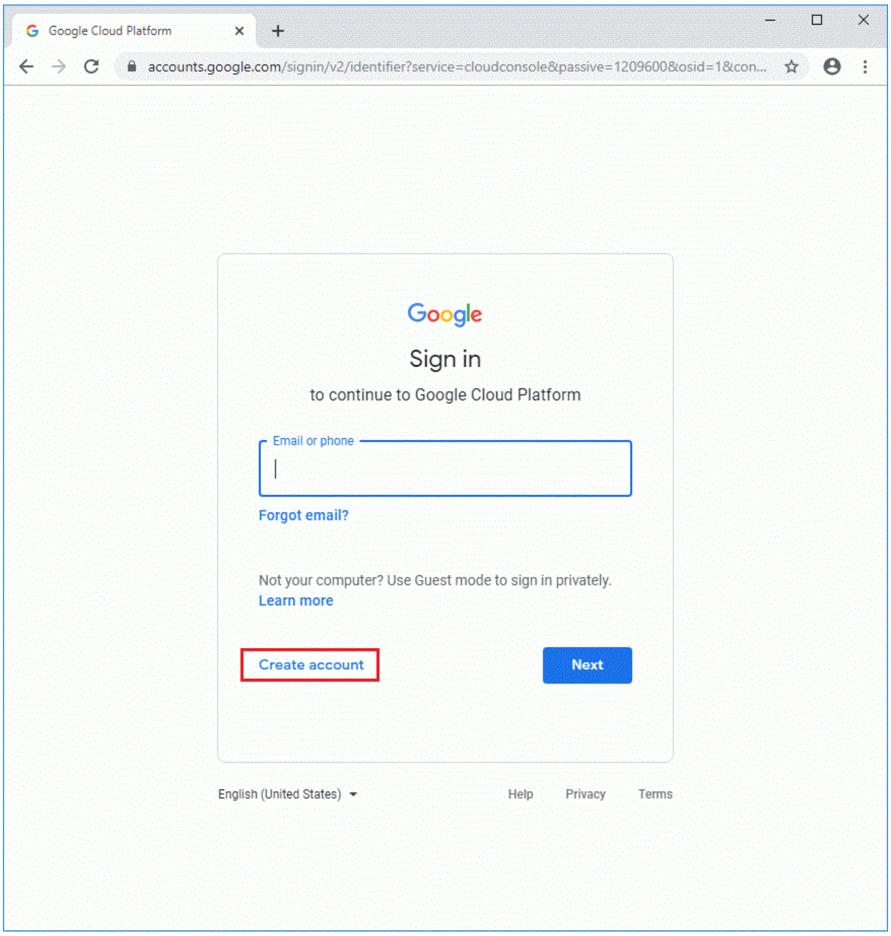
●Client ID

●Client Secret

●Refresh Token

To obtain the above information, please take the following operating procedures (effective as of November, but subject to change without notice.)

1. Log in Google by using your Google account.
   If you do not have Google account yet, click **[Create account]** button.



accounts.google.com/signin/v2/identifier?service=cloudconsole&passive=1209600&osid=1&con...

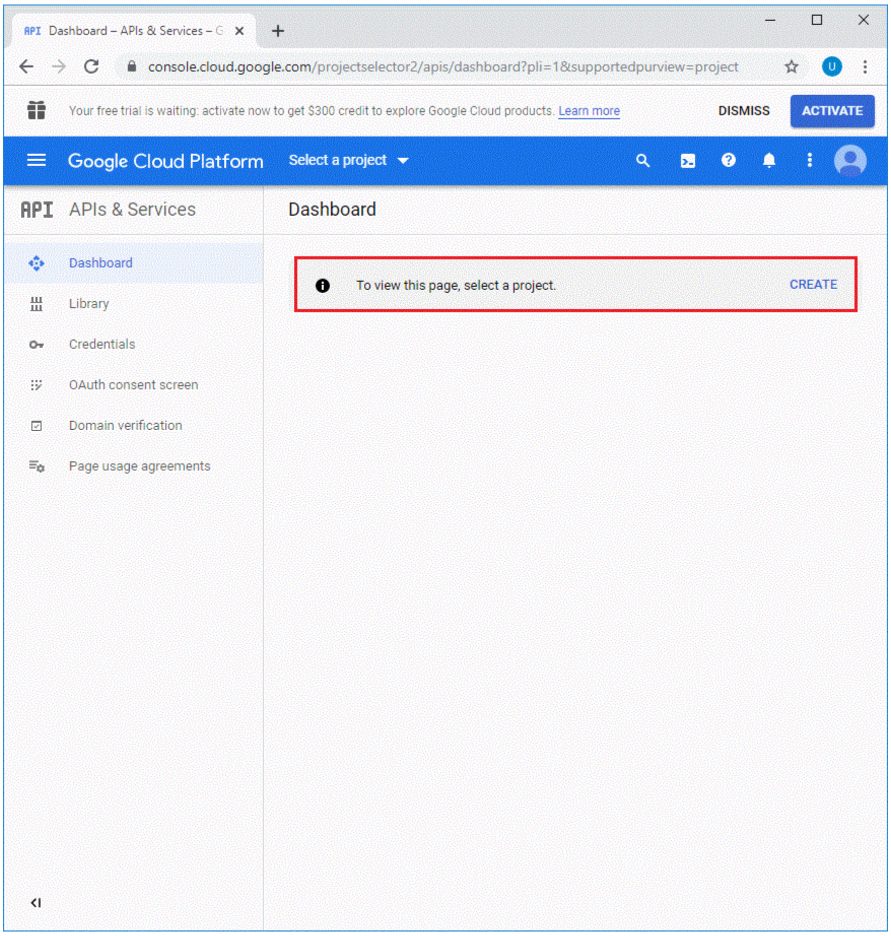
Google

Sign in

to continue to Google Cloud Platform

Not your computer? Use Guest mode to sign in privately.

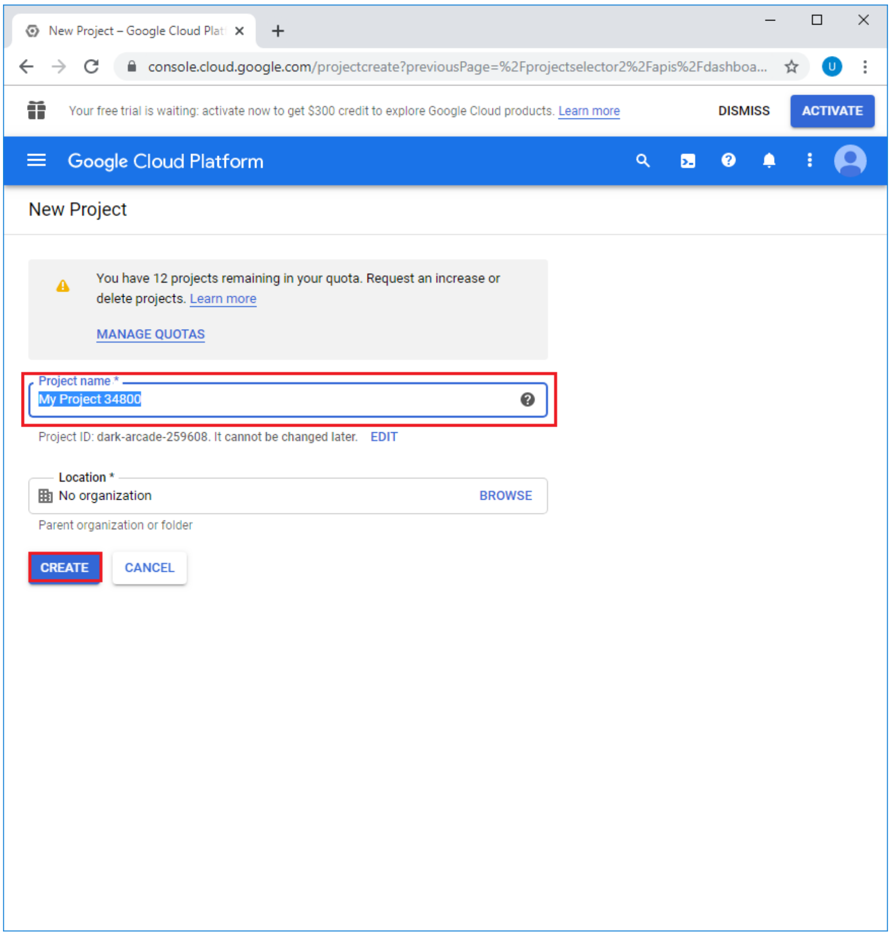
2. Access Google API Console (Google Cloud Platform API and Services) by using your Google account or the newly created account.
First, you need to create a project.



Dashboard – APIs & Services – G
console.cloud.google.com/projectselector2/apis/dashboard?pli=1&supportedpurview=project
Your free trial is waiting: activate now to get $300 credit to explore Google Cloud products. Learn more
DISMISS
ACTIVATE
Google Cloud Platform
Select a project
API APIs & Services
Dashboard
Dashboard
Library
Credentials
OAuth consent screen
Domain verification
Page usage agreements

To view this page, select a project. CREATE

In this example, the project is created in the default name.



New Project – Google Cloud Plat
console.cloud.google.com/projectcreate?previousPage=%2Fprojectselector2%2Fapis%2Fdashboa...
Your free trial is waiting: activate now to get $300 credit to explore Google Cloud products. Learn more
DISMISS
ACTIVATE
Google Cloud Platform

New Project

You have 12 projects remaining in your quota. Request an increase or delete projects. Learn more

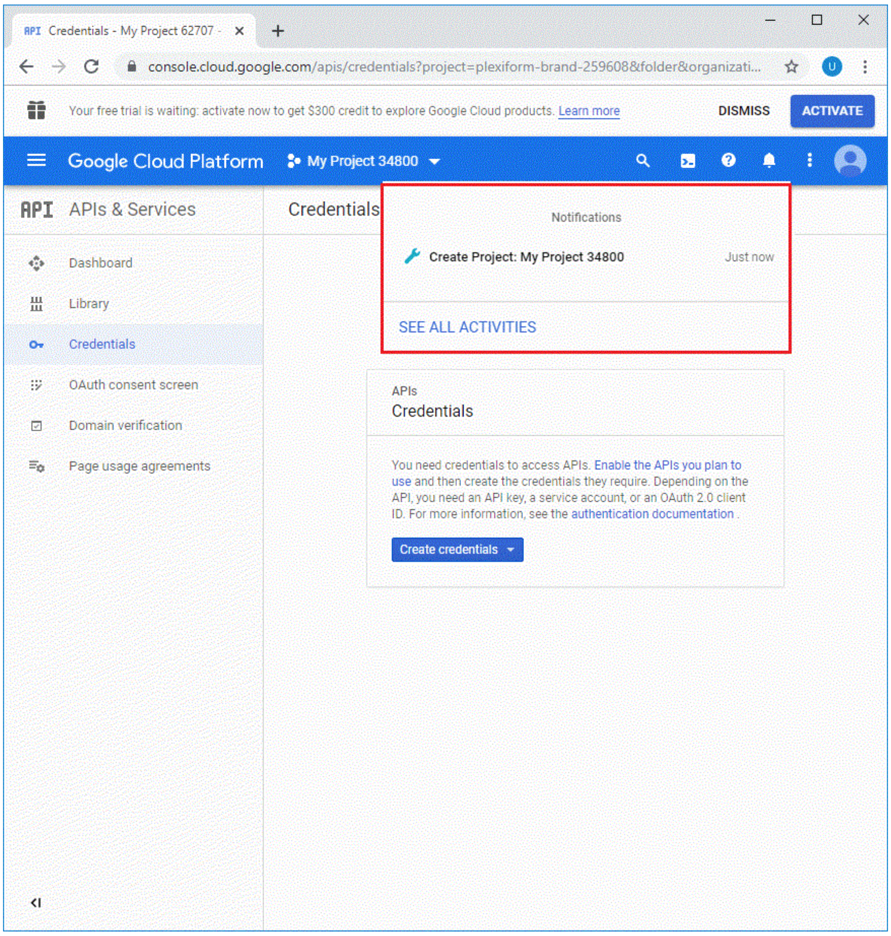
MANAGE QUOTAS

Project name *
My Project 34800

Project ID: dark-arcade-259608. It cannot be changed later. EDIT

Location *
No organization BROWSE

Parent organization or folder

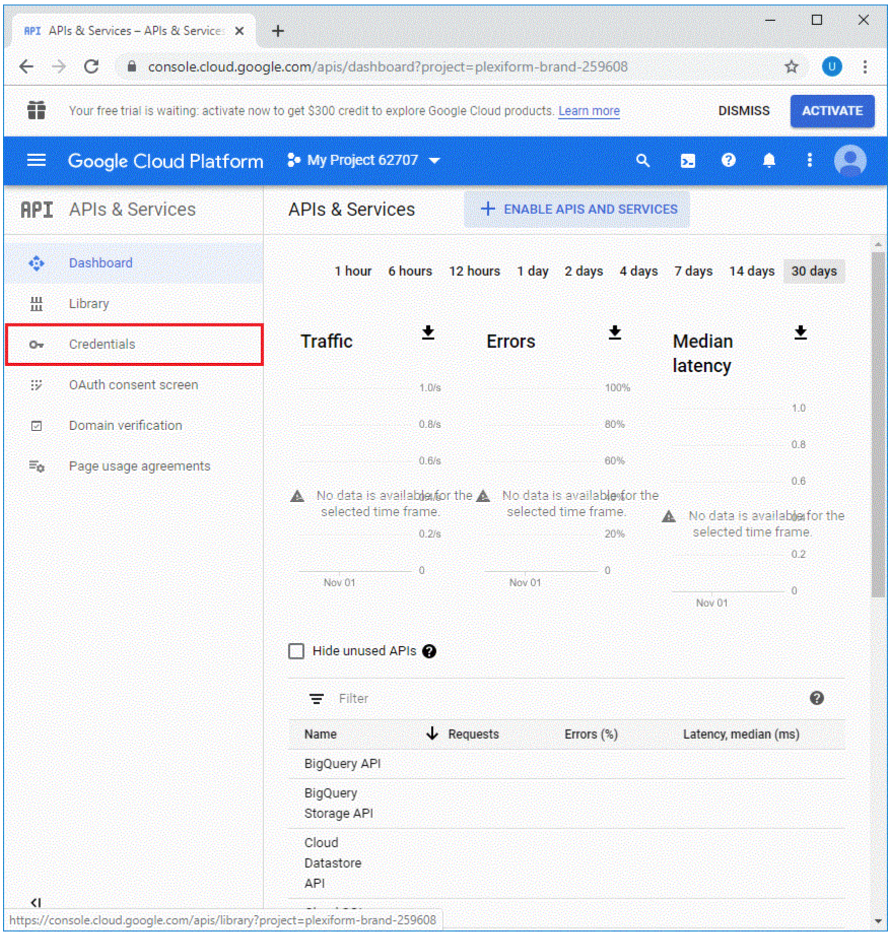


Credentials - My Project 62707 -
console.cloud.google.com/apis/credentials?project=plexiform-brand-259608&folder&organizati...
Your free trial is waiting: activate now to get $300 credit to explore Google Cloud products. Learn more
DISMISS
ACTIVATE
Google Cloud Platform
My Project 34800
API APIs & Services
Credentials
Dashboard
Library
Credentials
OAuth consent screen
Domain verification
Page usage agreements
Notifications
Create Project: My Project 34800
Just now
SEE ALL ACTIVITIES
APIs
Credentials
Create credentials

You need credentials to access APIs. Enable the APIs you plan to use and then create the credentials they require. Depending on the API, you need an API key, a service account, or an OAuth 2.0 client ID. For more information, see the authentication documentation .

The information including available API is displayed in Dashboard.

3. Select [Credentials].



Your free trial is waiting: activate now to get $300 credit to explore Google Cloud products. Learn more

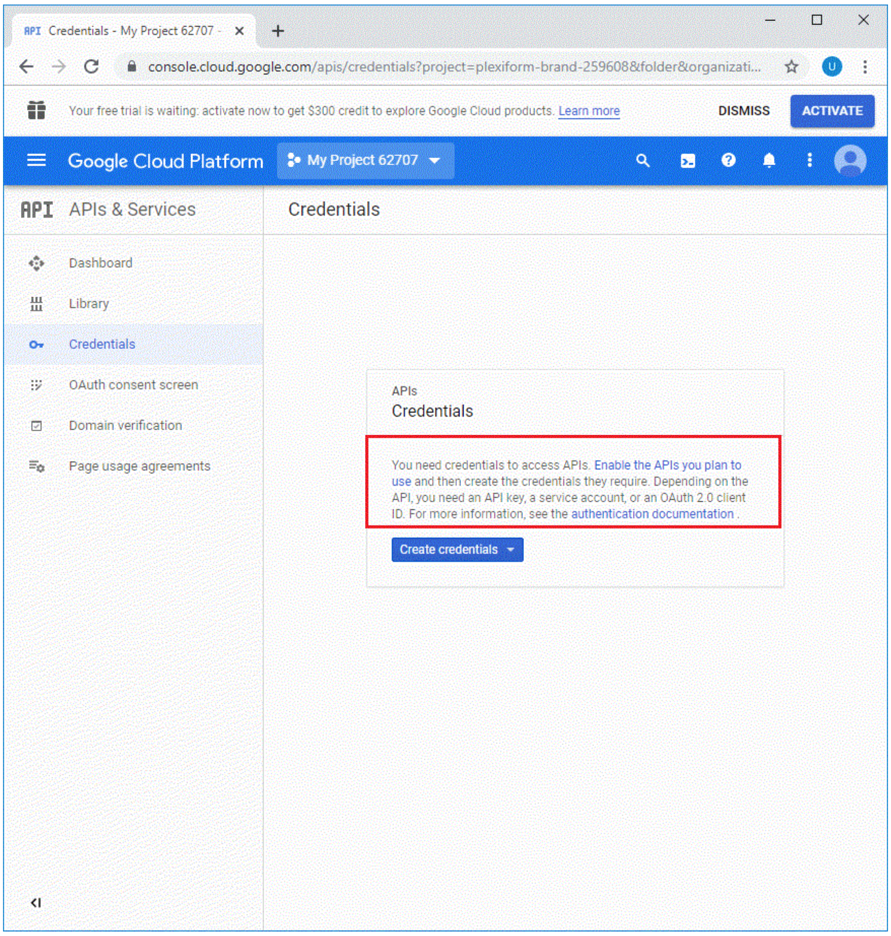
No data is available for the selected time frame.

No data is available for the selected time frame.

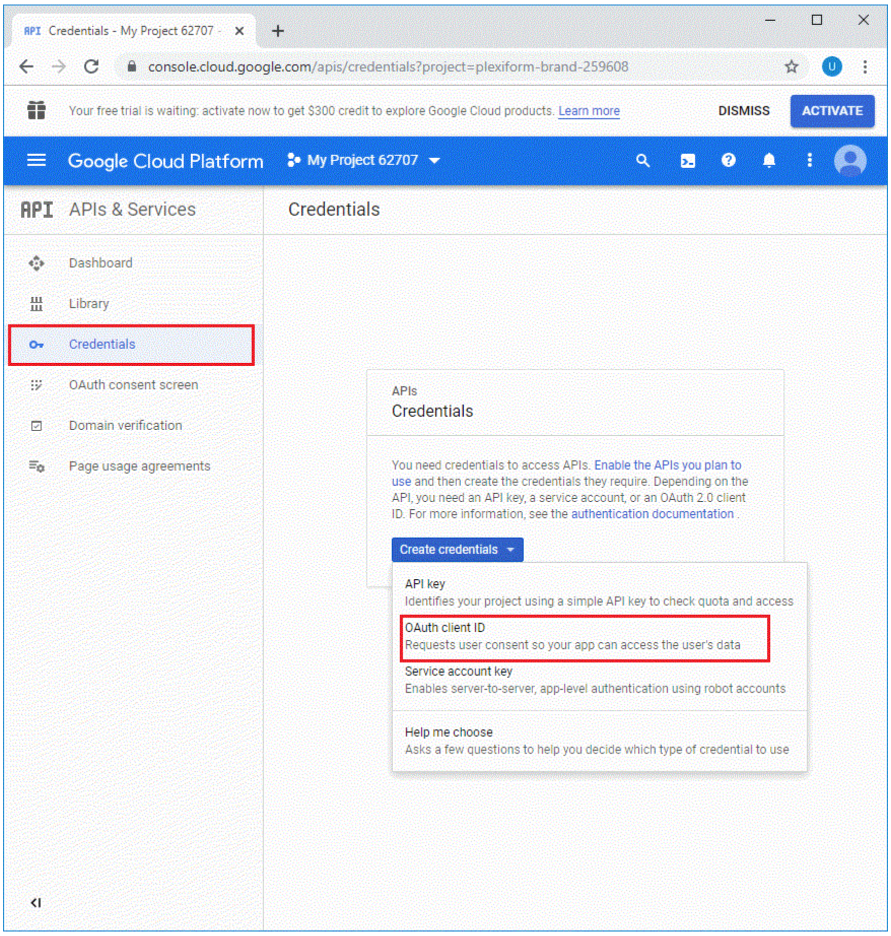
No data is available for the selected time frame.

□ Hide unused APIs

Name	Requests	Errors (%)	Latency, median (ms)
BigQuery API			
BigQuery Storage API			
Cloud Datastore API			


Credentials - My Project 62707 -
console.cloud.google.com/apis/credentials?project=plexiform-brand-259608&folder&organizati...
Your free trial is waiting: activate now to get $300 credit to explore Google Cloud products. Learn more
DISMISS
ACTIVATE
Google Cloud Platform
My Project 62707
APIs & Services
Credentials
Dashboard
Library
Credentials
OAuth consent screen
Domain verification
Page usage agreements
APIs
Credentials

You need credentials to access APIs. Enable the APIs you plan to use and then create the credentials they require. Depending on the API, you need an API key, a service account, or an OAuth 2.0 client ID. For more information, see the authentication documentation .



Credentials - My Project 62707 -
console.cloud.google.com/apis/credentials?project=plexiform-brand-259608
Your free trial is waiting: activate now to get $300 credit to explore Google Cloud products. Learn more
DISMISS
ACTIVATE
Google Cloud Platform
My Project 62707
API APIs & Services
Credentials
Dashboard
Library
Credentials
OAuth consent screen
Domain verification
Page usage agreements

APIs
Credentials

You need credentials to access APIs. Enable the APIs you plan to use and then create the credentials they require. Depending on the API, you need an API key, a service account, or an OAuth 2.0 client ID. For more information, see the authentication documentation .

Create credentials

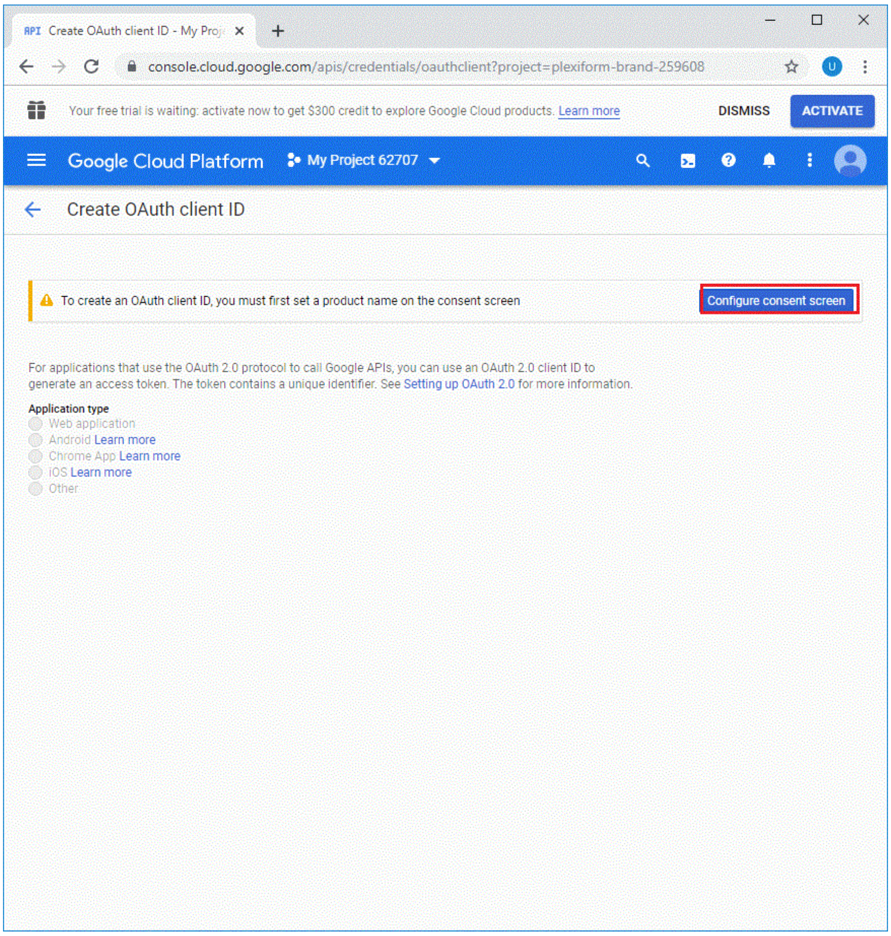
API key
Identifies your project using a simple API key to check quota and access

OAuth client ID
Requests user consent so your app can access the user's data

Service account key
Enables server-to-server, app-level authentication using robot accounts

Help me choose
Asks a few questions to help you decide which type of credential to use

4. To create OAuth Client ID, you will get a mesasge saying that you need to specify the service name in OAuth Consent screen.



API Create OAuth client ID - My Proj
console.cloud.google.com/apis/credentials/oauthclient?project=plexiform-brand-259608
DISMISS
ACTIVATE
Google Cloud Platform
My Project 62707
Configure consent screen

Your free trial is waiting: activate now to get $300 credit to explore Google Cloud products. Learn more

Create OAuth client ID

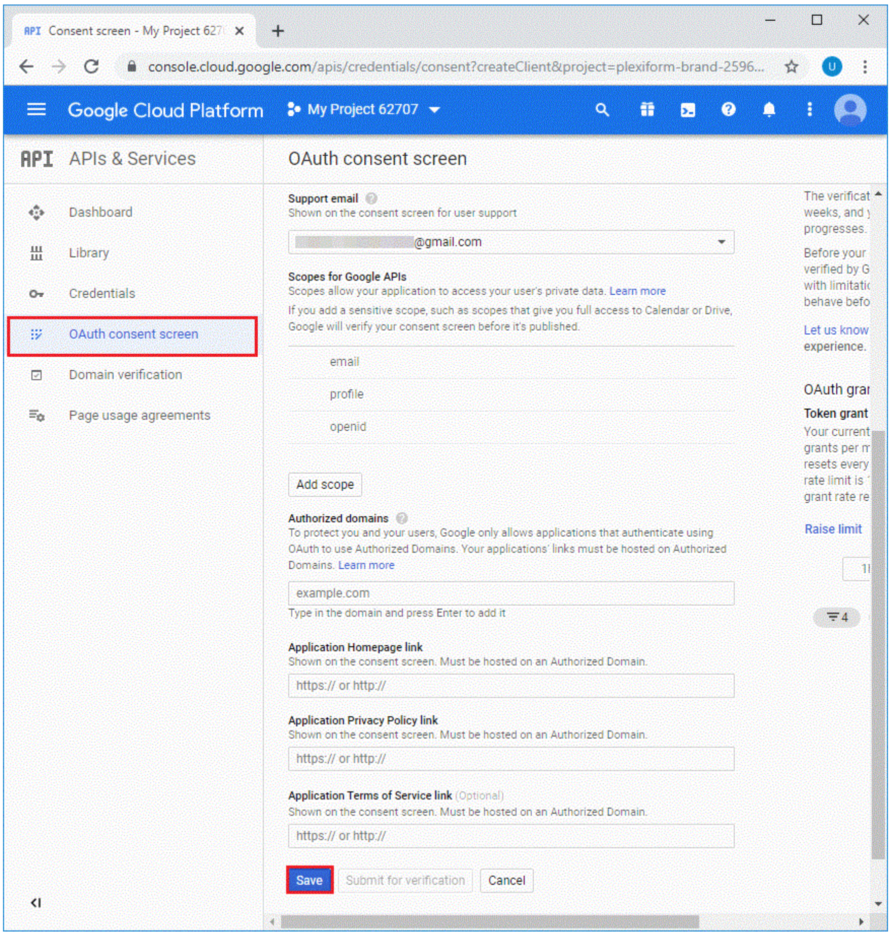
To create an OAuth client ID, you must first set a product name on the consent screen

For applications that use the OAuth 2.0 protocol to call Google APIs, you can use an OAuth 2.0 client ID to generate an access token. The token contains a unique identifier. See Setting up OAuth 2.0 for more information.

Application type

○ Web application
○ Android Learn more
○ Chrome App Learn more
○ iOS Learn more
○ Other

5. Click **[Configure consent screen]** and enter the application name (ex. ActiveImage Replication) and click **[Save]**.



Support email
Shown on the consent screen for user support

[redacted]@gmail.com

Scopes for Google APIs
Scopes allow your application to access your user's private data. Learn more

If you add a sensitive scope, such as scopes that give you full access to Calendar or Drive, Google will verify your consent screen before it's published.

email
profile
openid

Authorized domains
To protect you and your users, Google only allows applications that authenticate using OAuth to use Authorized Domains. Your applications' links must be hosted on Authorized Domains. Learn more

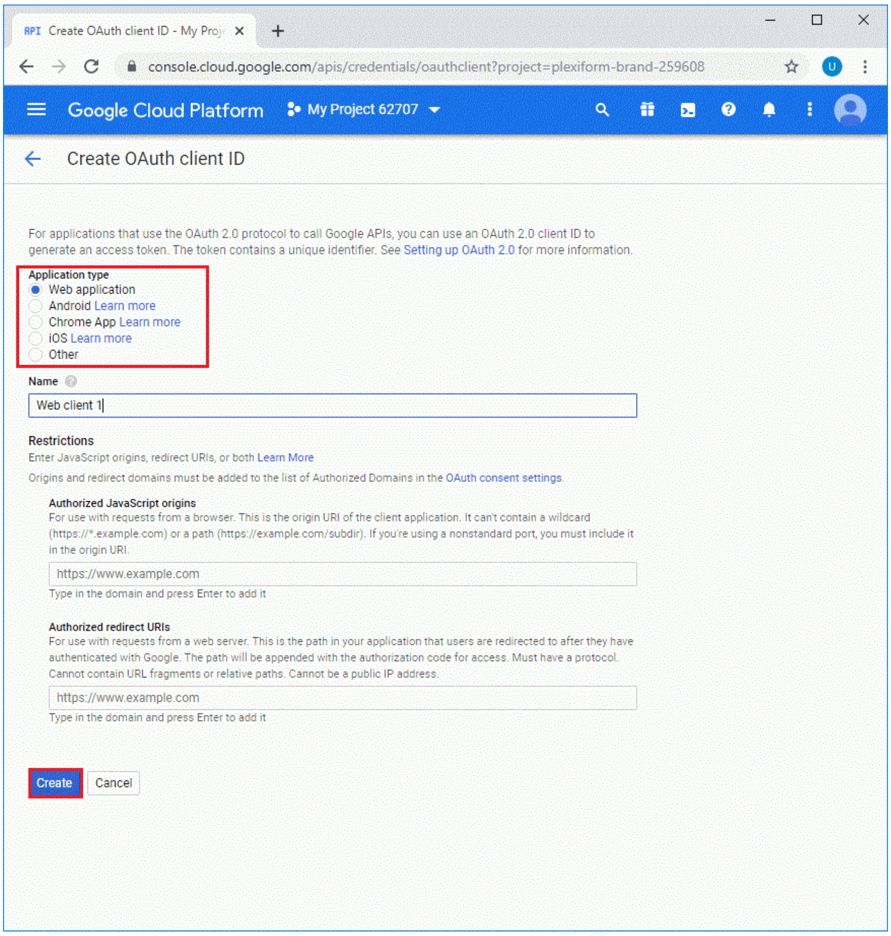
example.com
Type in the domain and press Enter to add it

Application Homepage link
Shown on the consent screen. Must be hosted on an Authorized Domain.
https:// or http://

Application Privacy Policy link
Shown on the consent screen. Must be hosted on an Authorized Domain.
https:// or http://

Application Terms of Service link (Optional)
Shown on the consent screen. Must be hosted on an Authorized Domain.
https:// or http://

6. Select [Web Application] for [Application Type].



Create OAuth client ID - My Proj
console.cloud.google.com/apis/credentials/oauthclient?project=plexiform-brand-259608
Google Cloud Platform
My Project 62707

Create OAuth client ID

For applications that use the OAuth 2.0 protocol to call Google APIs, you can use an OAuth 2.0 client ID to generate an access token. The token contains a unique identifier. See Setting up OAuth 2.0 for more information.

Application type
- ● Web application
- ○ Android Learn more
- ○ Chrome App Learn more
- ○ iOS Learn more
- ○ Other

Name

Web client 1

Restrictions

Enter JavaScript origins, redirect URIs, or both Learn More

Origins and redirect domains must be added to the list of Authorized Domains in the OAuth consent settings.

Authorized JavaScript origins

For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard (https://*.example.com) or a path (https://example.com/subdir). If you're using a nonstandard port, you must include it in the origin URI.

https://www.example.com

Type in the domain and press Enter to add it

Authorized redirect URIs

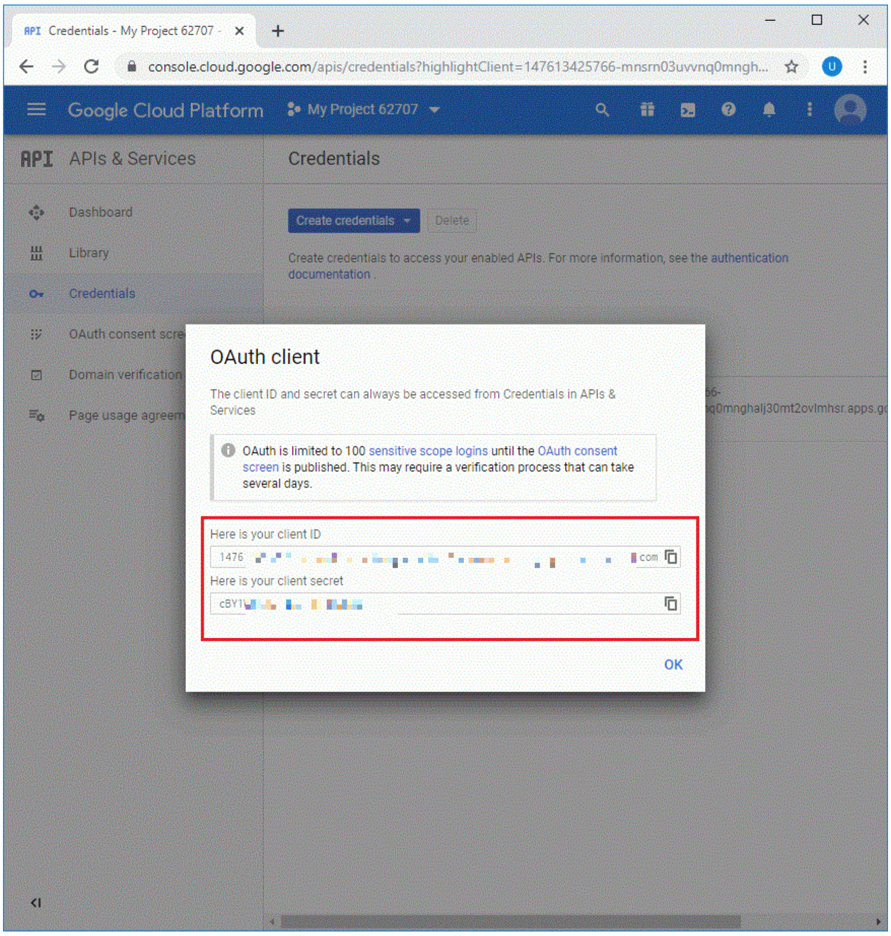
For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

https://www.example.com

Type in the domain and press Enter to add it

7. Please review the settings and click **[Create]**.

8. Client ID and Client Secret are indicated. Click on the square button to the right of [Client ID] and [Client Secret] to copy. You are recommended to save the [Client ID] and [Client Secret] in a text file.



Create credentials to access your enabled APIs. For more information, see the authentication documentation .

OAuth client

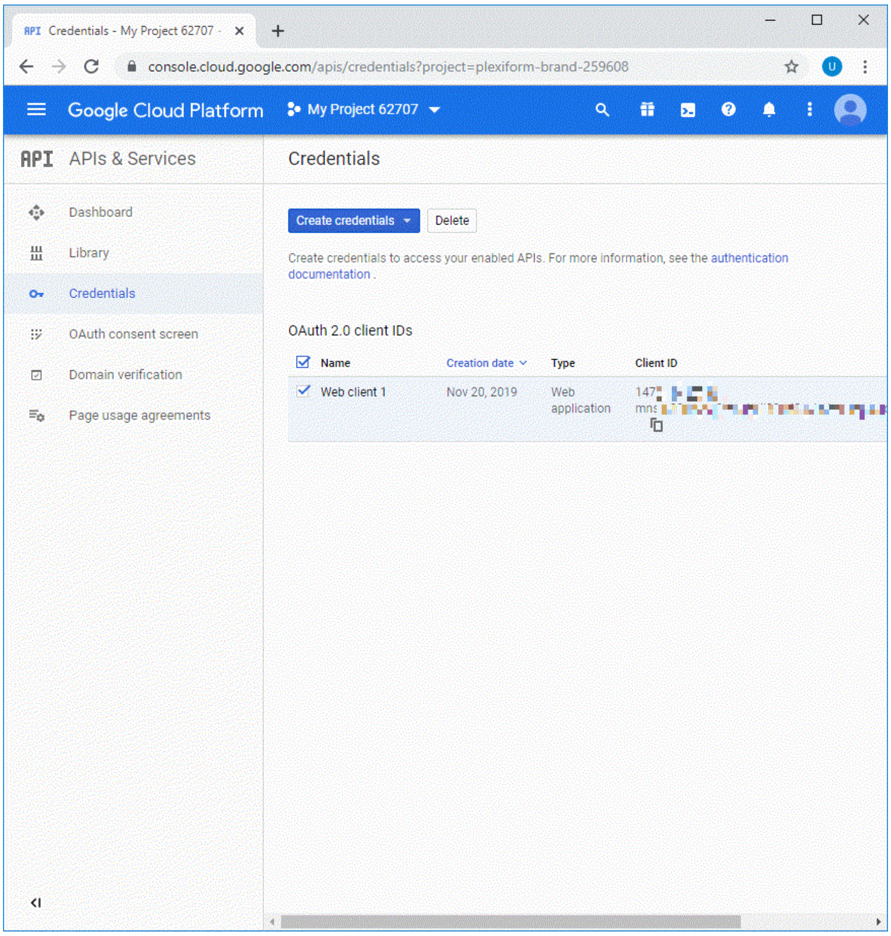
The client ID and secret can always be accessed from Credentials in APIs & Services

OAuth is limited to 100 sensitive scope logins until the OAuth consent screen is published. This may require a verification process that can take several days.

Here is your client ID: 1476 [redacted] com

Here is your client secret: cBY1 [redacted]

9. You can check the Client ID on your Web browser.



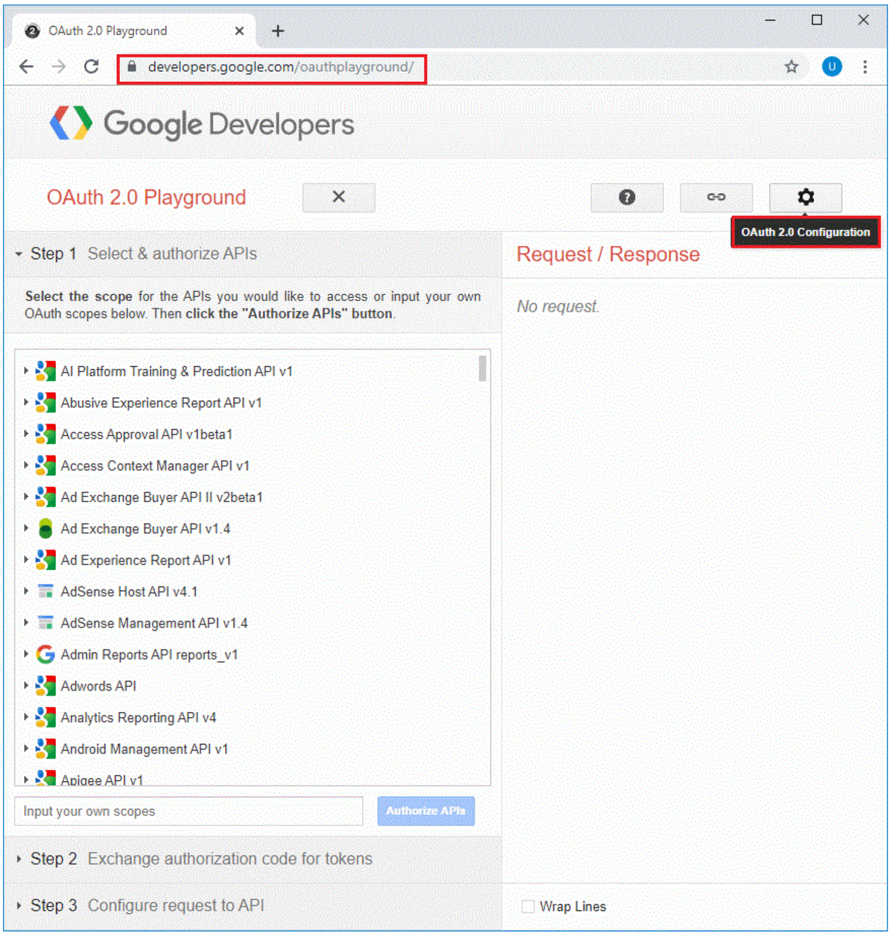
Credentials

Create credentials to access your enabled APIs. For more information, see the authentication documentation .

OAuth 2.0 client IDs

☑	Name	Creation date	Type	Client ID
✓	Web client 1	Nov 20, 2019	Web application	147[redacted] mn[redacted]

10. Next, let’s get Refresh Token.
    Access https://developers.google.com/oauthplayground on your Web browser.



OAuth 2.0 Playground

developers.google.com/oauthplayground/

Google Developers

OAuth 2.0 Playground

OAuth 2.0 Configuration

Step 1 Select & authorize APIs

Select the scope for the APIs you would like to access or input your own OAuth scopes below. Then click the "Authorize APIs" button.

- AI Platform Training & Prediction API v1
- Abusive Experience Report API v1
- Access Approval API v1beta1
- Access Context Manager API v1
- Ad Exchange Buyer API II v2beta1
- Ad Exchange Buyer API v1.4
- Ad Experience Report API v1
- AdSense Host API v4.1
- AdSense Management API v1.4
- Admin Reports API reports_v1
- Adwords API
- Analytics Reporting API v4
- Android Management API v1
- Apigee API v1

Input your own scopes

Authorize APIs

Step 2 Exchange authorization code for tokens

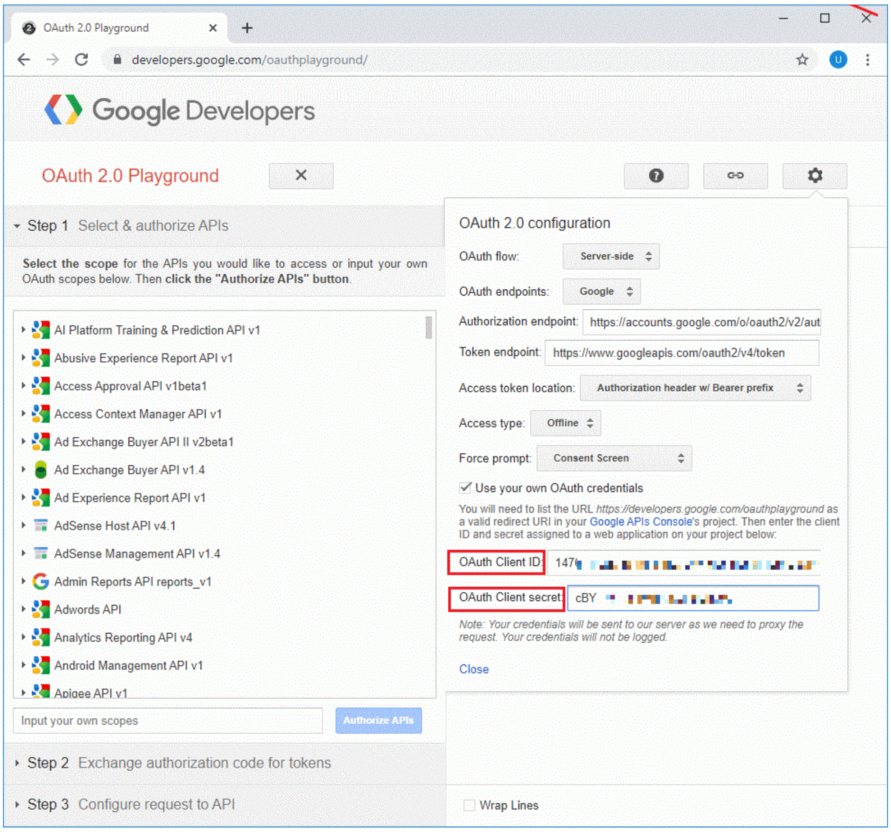
Step 3 Configure request to API

Request / Response

No request.

□ Wrap Lines

11. Click **[OAuth 2.0 Configuration]** button in the upper right of the window and enable **[Use your own OAuth credentials]**. Enter Client ID and Client Secrete created in the above step. Click **[Close]**.



Step 1 Select & authorize APIs

Select the scope for the APIs you would like to access or input your own OAuth scopes below. Then **click the "Authorize APIs" button**.

- AI Platform Training & Prediction API v1
- Abusive Experience Report API v1
- Access Approval API v1beta1
- Access Context Manager API v1
- Ad Exchange Buyer API II v2beta1
- Ad Exchange Buyer API v1.4
- Ad Experience Report API v1
- AdSense Host API v4.1
- AdSense Management API v1.4
- Admin Reports API reports_v1
- Adwords API
- Analytics Reporting API v4
- Android Management API v1
- Apigee API v1

Step 2 Exchange authorization code for tokens

Step 3 Configure request to API

OAuth 2.0 configuration

OAuth flow: Server-side

OAuth endpoints: Google

Authorization endpoint: https://accounts.google.com/o/oauth2/v2/aut

Token endpoint: https://www.googleapis.com/oauth2/v4/token

Access token location: Authorization header w/ Bearer prefix

Access type: Offline

Force prompt: Consent Screen

☑ Use your own OAuth credentials

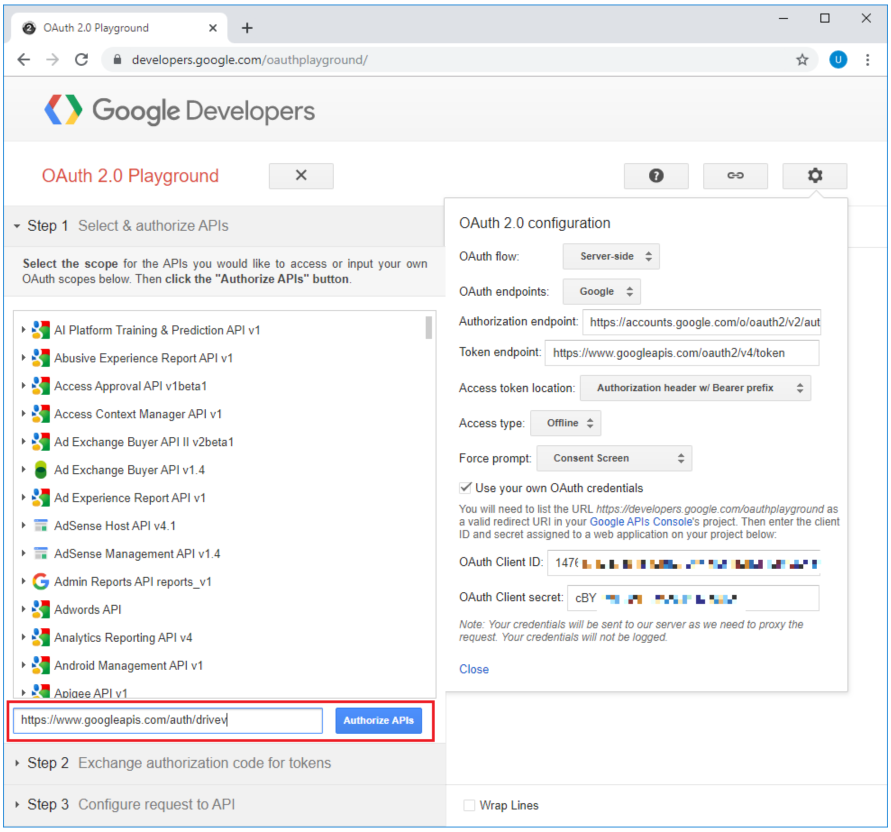
You will need to list the URL *https://developers.google.com/oauthplayground* as a valid redirect URI in your Google APIs Console's project. Then enter the client ID and secret assigned to a web application on your project below:

OAuth Client ID: 147[redacted]

OAuth Client secret: cBY [redacted]

Note: Your credentials will be sent to our server as we need to proxy the request. Your credentials will not be logged.

12. Go back to previous screen and enter https://www.googleapis.com/auth/drive in **[Input your own scop]**.



OAuth 2.0 Playground

developers.google.com/oauthplayground/

Google Developers

OAuth 2.0 Playground

Step 1 Select & authorize APIs

Select the scope for the APIs you would like to access or input your own OAuth scopes below. Then **click the "Authorize APIs" button**.

- AI Platform Training & Prediction API v1
- Abusive Experience Report API v1
- Access Approval API v1beta1
- Access Context Manager API v1
- Ad Exchange Buyer API II v2beta1
- Ad Exchange Buyer API v1.4
- Ad Experience Report API v1
- AdSense Host API v4.1
- AdSense Management API v1.4
- Admin Reports API reports_v1
- Adwords API
- Analytics Reporting API v4
- Android Management API v1
- Apigee API v1

https://www.googleapis.com/auth/drive

Step 2 Exchange authorization code for tokens

Step 3 Configure request to API

OAuth 2.0 configuration

OAuth flow: Server-side

OAuth endpoints: Google

Authorization endpoint: https://accounts.google.com/o/oauth2/v2/aut

Token endpoint: https://www.googleapis.com/oauth2/v4/token

Access token location: Authorization header w/ Bearer prefix

Access type: Offline

Force prompt: Consent Screen

☑ Use your own OAuth credentials

You will need to list the URL *https://developers.google.com/oauthplayground* as a valid redirect URI in your Google APIs Console's project. Then enter the client ID and secret assigned to a web application on your project below:

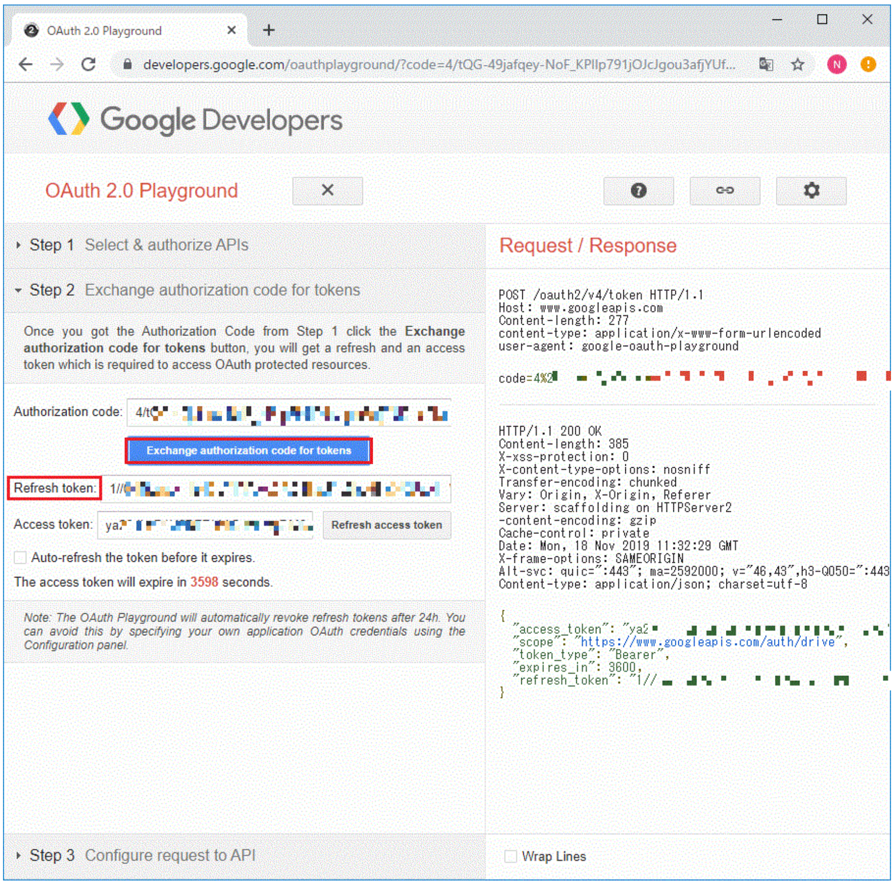
OAuth Client ID: 1476 [redacted]

OAuth Client secret: cBY [redacted]

Note: Your credentials will be sent to our server as we need to proxy the request. Your credentials will not be logged.

☐ Wrap Lines

13. When entered, as **[Authorize APIs]** become active, click the button. Go to Step 2. Click **[Exchange authorization code for token]** to check Refresh Token.


OAuth 2.0 Playground
developers.google.com/oauthplayground/?code=4/tQG-49jafqey-NoF_KPIlp791jOJcJgou3afjYUf...
Google Developers
OAuth 2.0 Playground

Step 1 Select & authorize APIs

Step 2 Exchange authorization code for tokens

Once you got the Authorization Code from Step 1 click the **Exchange authorization code for tokens** button, you will get a refresh and an access token which is required to access OAuth protected resources.

Authorization code: 4/t[redacted]

Exchange authorization code for tokens

Refresh token: 1//[redacted]

Access token: ya[redacted] Refresh access token

□ Auto-refresh the token before it expires.

The access token will expire in 3598 seconds.

Note: The OAuth Playground will automatically revoke refresh tokens after 24h. You can avoid this by specifying your own application OAuth credentials using the Configuration panel.

Step 3 Configure request to API

Request / Response

```
POST /oauth2/v4/token HTTP/1.1
Host: www.googleapis.com
Content-length: 277
content-type: application/x-www-form-urlencoded
user-agent: google-oauth-playground

code=4%2[redacted]
```

```
HTTP/1.1 200 OK
Content-length: 385
X-xss-protection: 0
X-content-type-options: nosniff
Transfer-encoding: chunked
Vary: Origin, X-Origin, Referer
Server: scaffolding on HTTPServer2
-content-encoding: gzip
Cache-control: private
Date: Mon, 18 Nov 2019 11:32:29 GMT
X-frame-options: SAMEORIGIN
Alt-svc: quic=":443"; ma=2592000; v="46,43",h3-Q050=":443
Content-type: application/json; charset=utf-8

{
  "access_token": "ya2[redacted]
  "scope": "https://www.googleapis.com/auth/drive",
  "token_type": "Bearer",
  "expires_in": 3600,
  "refresh_token": "1//[redacted]
}
```

□ Wrap Lines

14. The step automatically transitions to [Step 3]. Clicking [Step 2] goes back to Step 2. Use the ID for authentication to access Google Drive as the replication target.

15. You will have to obtain ID and Token to use OneDrive for Office 365 Business or Dropbox. For more detailed operating procedures, please refer to the respective online manuals for the cloud storages.

APPENDIX B

ActiveImage Protector & Support Information

●Actiphy's Web Site
You will find the product information as well as direct links to download documentation, our full installers or update installers, etc:
https://www.actiphy.com

●ActiveImage Protector FAQ
You can access the support FAQ.
https://kb.actiphy.com/

●For inquiries about ActiveImage Protector, please contact:

Global Sales Dept., Actiphy Inc.

(TEL) +81-3-5256-0877　(FAX) +81-3-5256-0878

E-mail: global-sales@actiphy.com