ActiveVisor™

Setup Guide

1st Edition August 2022

Actiphy

Contents

1. Overview

ActiveVisor offers a centralized management console to monitor the overall system protection of your backup source computers running ActiveImage Protector agents. In addition, ActiveVisor:

- Collects information about your ActiveImage Protector clients over the network.
- Provides a visual representation of statistical data.
- Real-time monitoring of the backup status of client computers.
- Monitors the storage space available on your backup image servers.
- Administers the deployment of backup tasks and their schedules.

This Set-up Guide provides a description of the installation process as well as basic configuration. For further information on configuring ActiveVisor and its limitations, please refer to our online help (https://webhelp.actiphy.com/AIP/2022/).

1.1. System Requirements

Before installing ActiveVisor, please ensure that your computers meet the following system requirements. (Note: Please refer to our online ActiveVisor requirements page for the latest updates.
https://www.actiphy.com/en-us/product/activevisor/#system-requirements

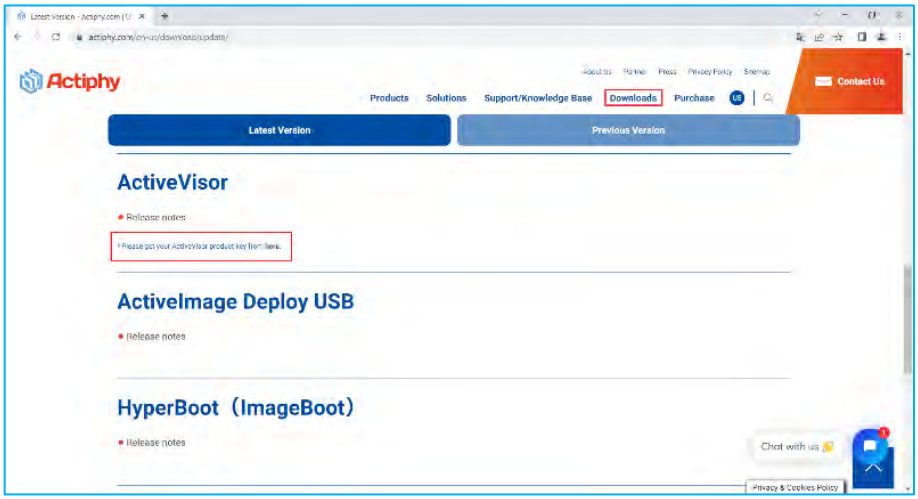
CPU	Pentium 4 or above
Main Memory (RAM)	2048MB or more is required. * 4096MB or more is recommended.
Hard Disk Space	800MB or more available space is required.
Screen Resolution	1280x1024 or above is recommended.
Supported OS	Windows 10（x64）、Windows Server 2012R2 or later OS

- Managed Agent Version:
  - ActiveImage Protector 2022 version 6.0.0.7292 or later.
  - ActiveImage Protector 2018 Update Version 5.1.11.6454 or later.
- We support the following Web browsers for Web access:
  - Google Chrome version 59 or later.
  - Microsoft Edge version 42 or later.
  - Apple Safari version 12 or later.
- Please configure your firewall's security settings as follows before using ActiveVisor:
  - Enable Windows Management Interface (WMI).
  - Enable Group Policy.
  - Allow Inbound Remote Administration in the **[Network]**--**[Network Connection]**--**[Windows Firewall]**.
  - Enable **[File and Printer Sharing]** to push-install, uninstall, or update ActiveImage Protector remotely.
  - Enable **[Allow inbound file and printer sharing exception]** through the **[Network]**--**[Network Connection]**--**[Windows Firewall]** Group Policy menu.

2. Initial Setting and Installation of ActiveVisor

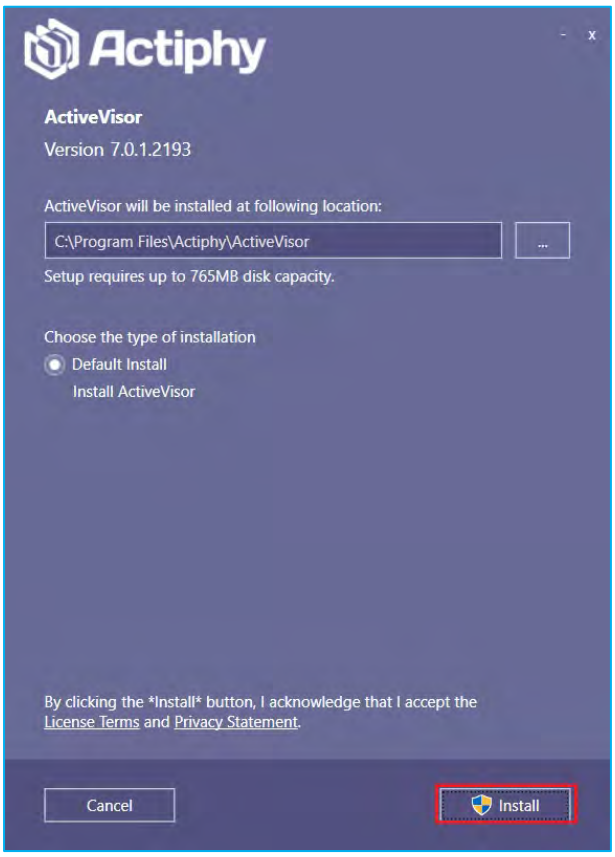
2.1. Download ActiveVisor

You can download the latest version of ActiveVisor from Actiphy's download site: https://www.actiphy.com/en-us/download/update/.



2.2. Install ActiveVisor

1. Double-click on the Setup.exe file to start the installer. Click the **[Install]** button to begin the installation process.

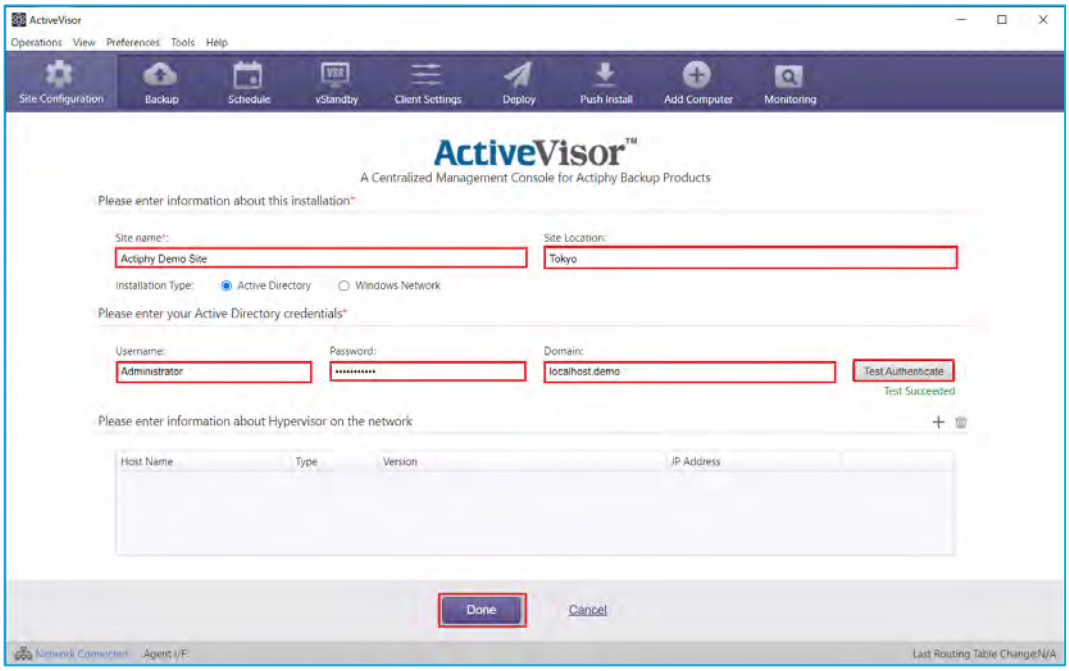


2. Click the **[Done]** button to complete the uninstall process.

   Note: A system restart is not required.

2.3. Initial Settings of ActiveVisor

1. Start ActiveVisor by clicking on the Windows Start menu and selecting the **[Actiphy]**--**[ActiveVisor]** menu item. You will see the following screen the first time you start ActiveVisor. You will need to configure your installation before you can proceed. First, fill out your Site Name, Site Location, and Installation Type. In this example, we're selecting Active Directory as our installation type, so we'll need to fill in our Username, Password, and Domain to complete the Active Directory configuration.
   Once you have filled out all the necessary fields, you can click on the **[Test Authenticate]** button to ensure your credentials are working. When you have finished, click the **[Done]** button.



Site Name: This field is the name of the site you will manage with this ActiveVisor installation. The value can be anything you wish, such as "Main Office" or "Accounting."

Site Location: This field is the location of this ActiveVisor. The value can be anything you wish, such as "Tokyo" or "Headquarters."

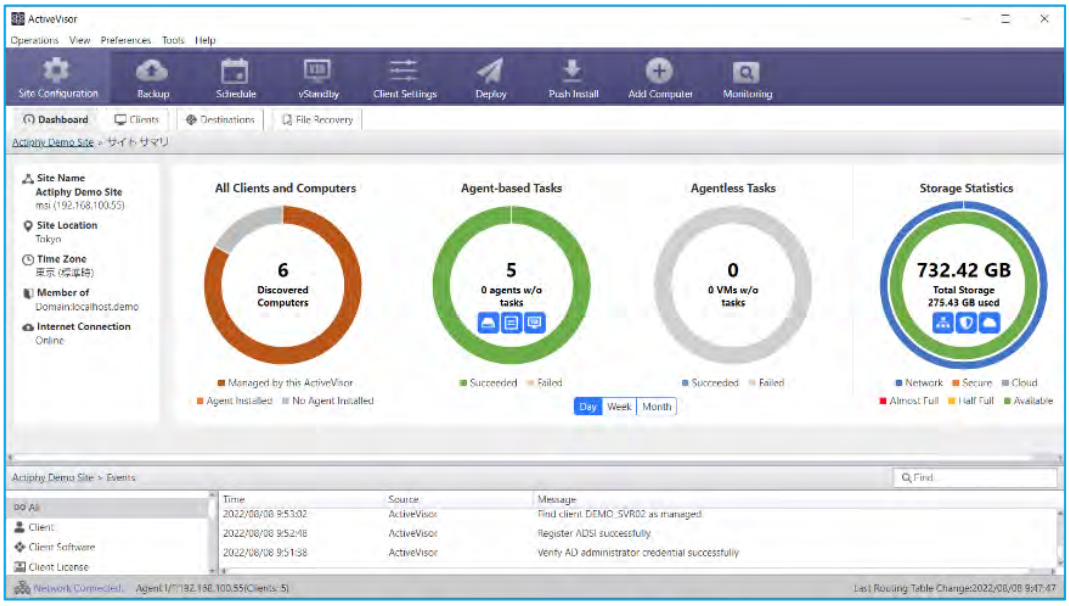
Installation Type: This tells ActiveVisor how to obtain information about your managed computers.

The options are **Active Directory** or **Windows Network**.

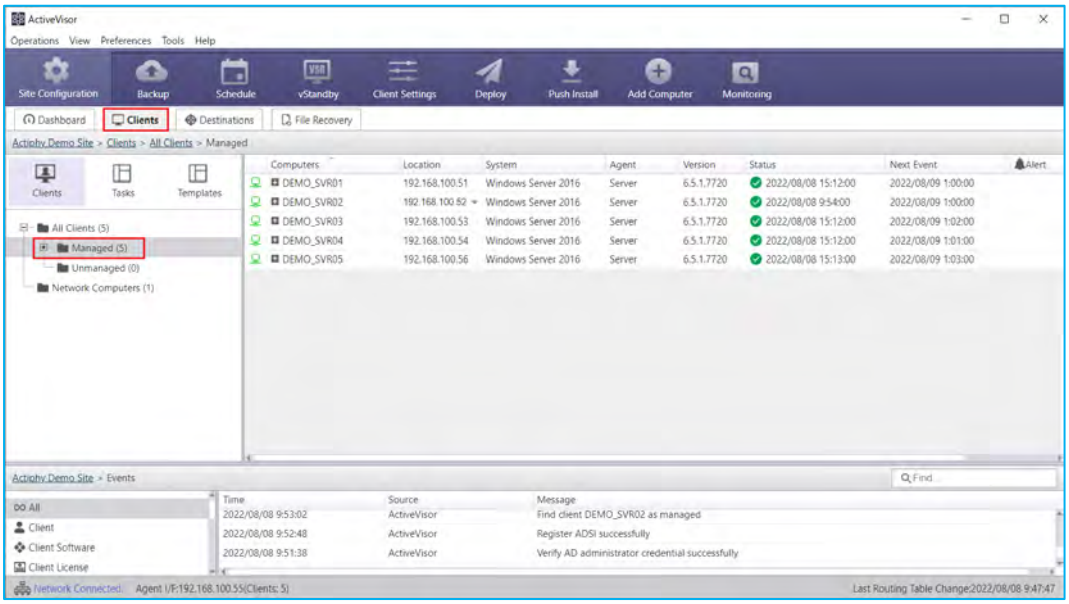
- **Active Directory**: If you choose to use Active Directory, ActiveVisor will ask you for your **Username**, **Password**, and the full path for your **Domain**. Once complete, any computers running ActiveImage Protector will automatically add them to the ActiveVisor database. This method is much faster than using **Windows Network**.
- **Windows Network**: Enter the built-in administrator account credential information to manage the computers. You must add the computers manually when using the Windows Network option.

2. The **[Dashboard]** provides real-time monitoring of the number of discovered computers, etc.

- **All Clients and computers**: The number of computers found in the same domain.
- **Agent-based backup task**: The number of computers that have the ActiveImage Protector agent installed.
- **Agentless backup tasks**: The number of computers installed with the backup management server "HyperAgent."
- **Storage Statistics**: The storage space used by the managed computers.

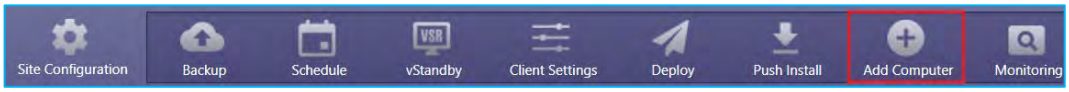


3. The **[Client]** tab lists the managed computers with the ActiveImage Protector agent installed under **[Managed by ActiveVisor].** Computers without the ActiveImage Protector agent are in the **[Network Computer]** section.



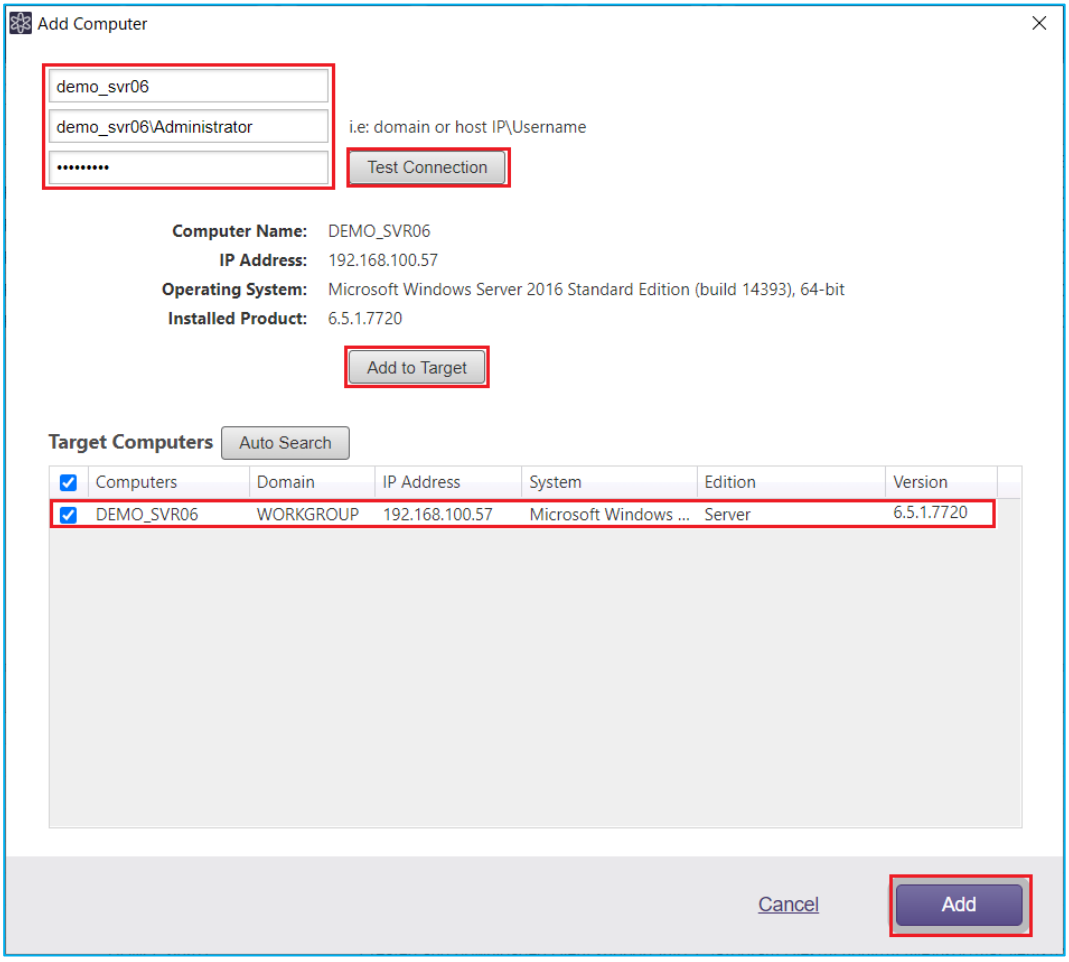
2.4. Add Undiscovered Computers

1. You can add undiscovered computers and computers in the "WORKGROUP" group to the managed group. Click [Add Computer] in the top menu bar to do so.

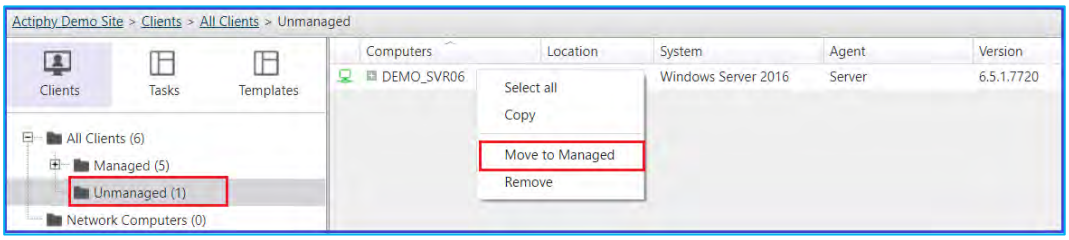


2. This example shows you the steps for adding the computer "demo_svr06," which has ActiveImage Protector installed and is in the "WORKGROUP" group, to the managed group.

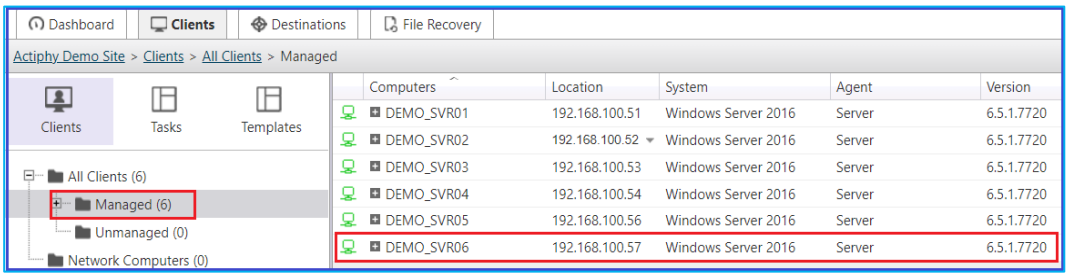
- Enter the computer name "demo_svr06" in **[Hostname or IP Address].**
- Enter the "demo_svr06¥Administrator" credentials in **[Administrator user name]** and **[Password].**
- Click **[Test Connection].**
- Then, click **[Add to Target]**. ActiveVisor will add the computer to **[Target Computers].**
- Check the checkbox for the computer to add it to the managed group.



3. ActiveVisor lists one computer in the **[Unmanaged]** section in this screenshot. To start managing this computer, right-click on the computer's name and select **[Move to Managed]** in the context menu. ActiveVisor will add the computer to the managed list. ActiveVisor lists all computers that don't have the ActiveImage Protector agent installed in **[Network Computers].**



4. Once you complete the previous step, ActiveVisor moves the unmanaged computer "demo_svr06" in the "WORKGROUP" group to the **[Managed]** folder.



3. Push-install ActiveImage Protector on managed computers

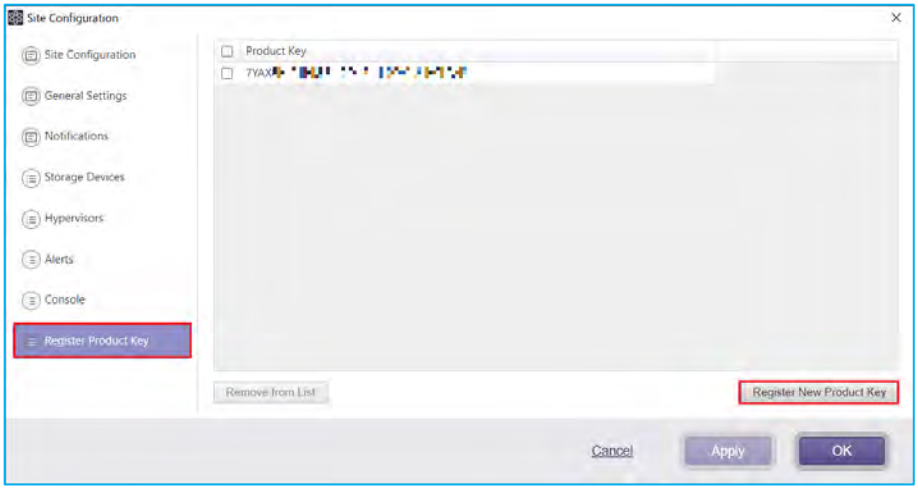
Use the Push-install feature in ActiveVisor to push-install, push-upgrade, or uninstall ActiveImage Protector in a selected group of computers. This example provides steps for push-installing ActiveImage Protector on the target computers using ActiveVisor.

Note: When you uninstall ActiveImage Protector from a local computer that ActiveVisor previously push-installed to, ActiveVisor will run the uninstaller in silent mode. For example, run:

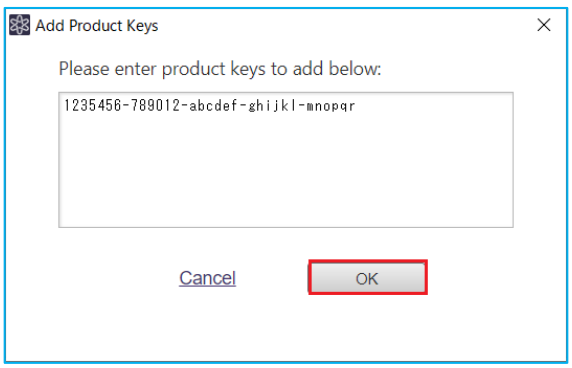
"C:¥Program Files¥Actiphy¥ActiveImage Protector¥uninstaller" /qn from the command prompt.

3.1. Preparatory Steps

1. Copy ActiveImage Protector's installer program (Setup.exe) to a folder such as "D:¥work," which is accessible from the computer running ActiveVisor.
2. Register ActiveImage Protector's product key to ActiveVisor (when push-installing, the system automatically adds the product key to activate the product.). When registering the product key, please select [Site Configuration]--[Register Product Key]. When you add a computer running ActiveImage Protector to the managed list, ActiveVisor will display the license information. To register a new product key, click [Register New Product Key], located in the lower right corner of the screen.

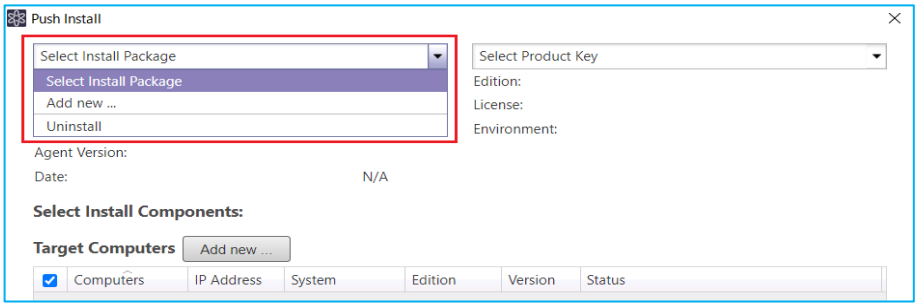


3. ActiveVisor will display the following dialog box to add a product key. Enter the product key and click the **[OK]** button.

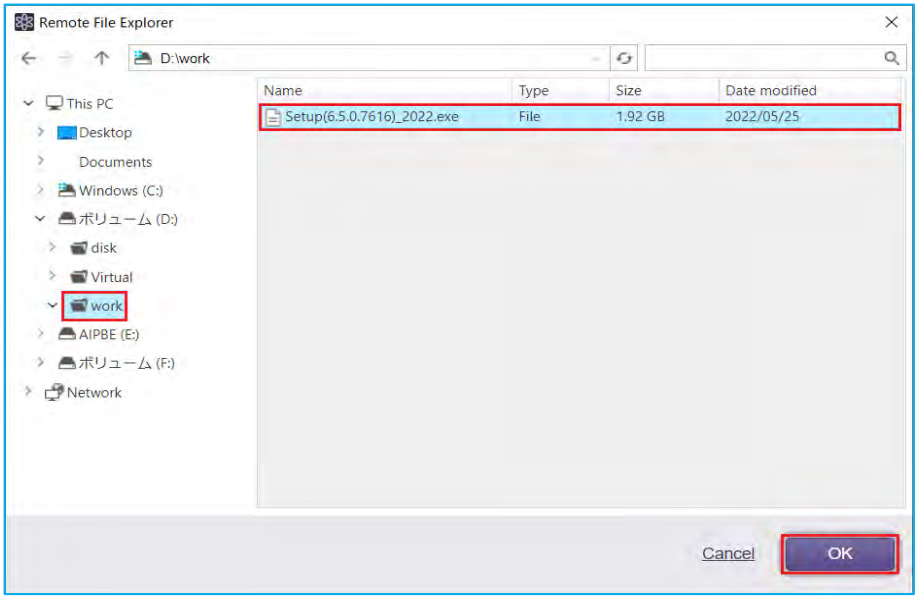


3.2. Run Push Install task

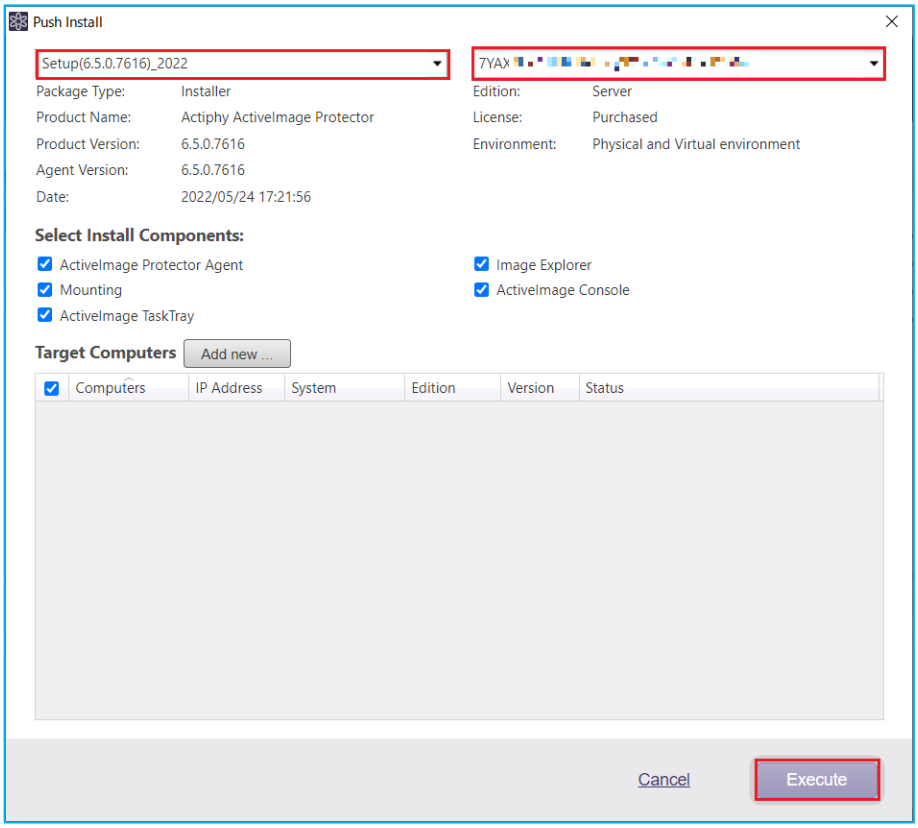
1. Select [Push Install] in the top menu. To select a package to install, click on the "▼" button on the right side of the text box, choose [Select Install Package], and click the [Add new] button.



2. Select the installer program for ActiveImage Protector, which you copied into a folder (D:¥work in this example) a moment ago, then click on the [OK] button.

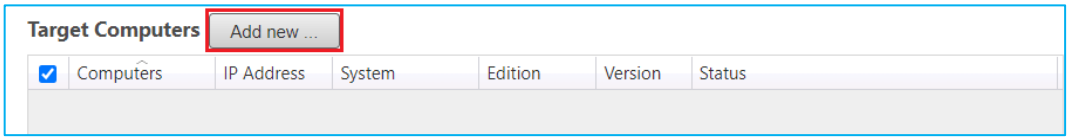


3. Please configure the settings for a push-installation. Select "Setup.exe" as the installer in the pull-down menu and enter the product key for your installer.

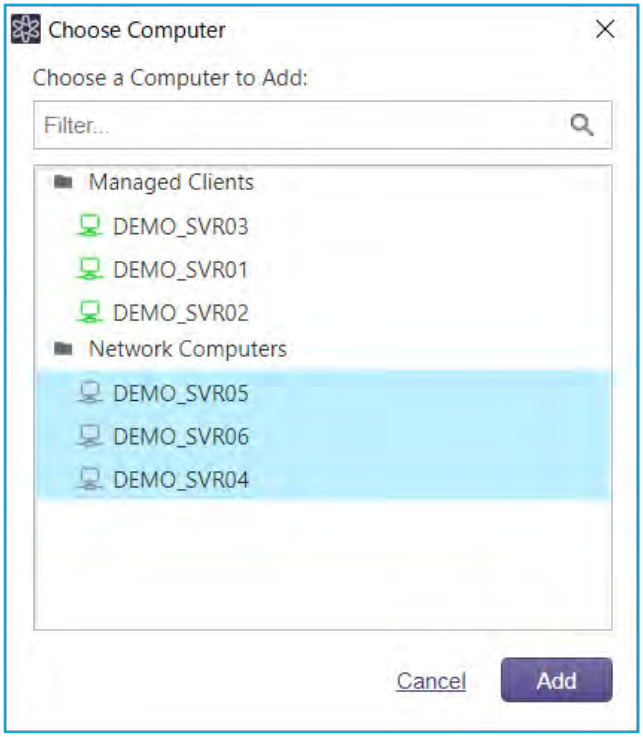


4. Select the components to push-install in **[Select Install Components]**. By default, you can only select **[ActiveImage Protector agent]**. When you only push-install the ActiveImage Protector agent, you cannot launch the ActiveImage Protector console on the computer. In this example, we have selected every component, including **[Mounting]**, **[ActiveImage Task Tray]**, **[Image Explorer]**, and **[ActiveImage Console].**

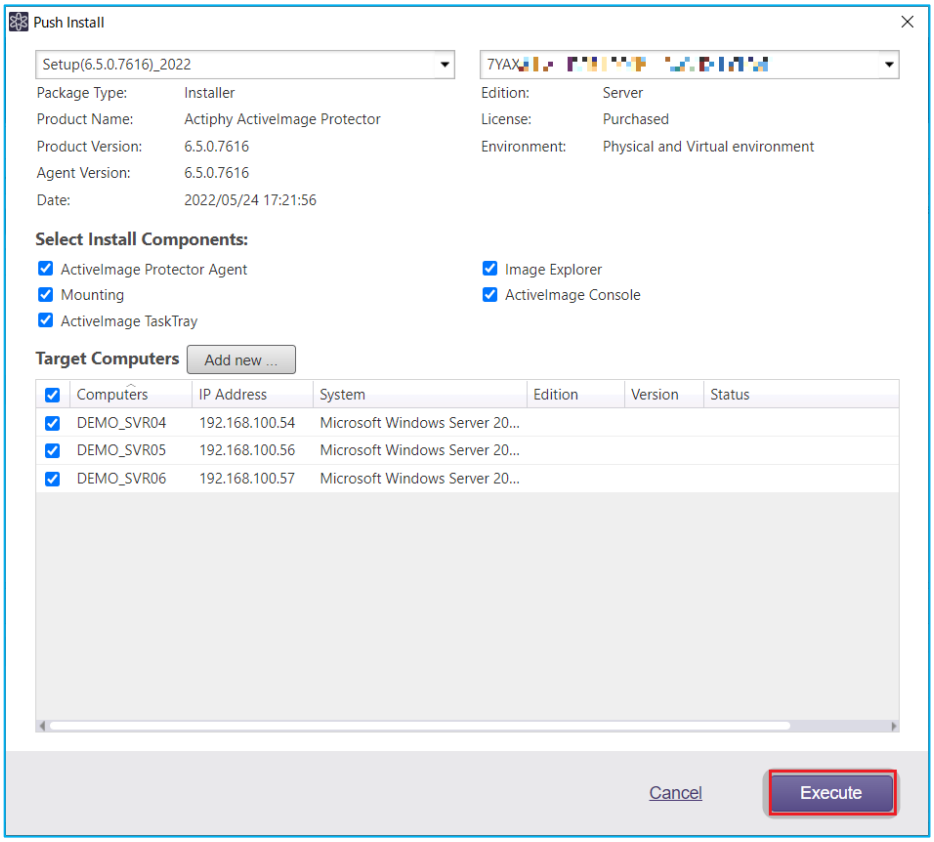
5. Configure the settings for the target computer to push-install the components. Then, click the **[Add New]** button in the **[Target Computers]** dialog.



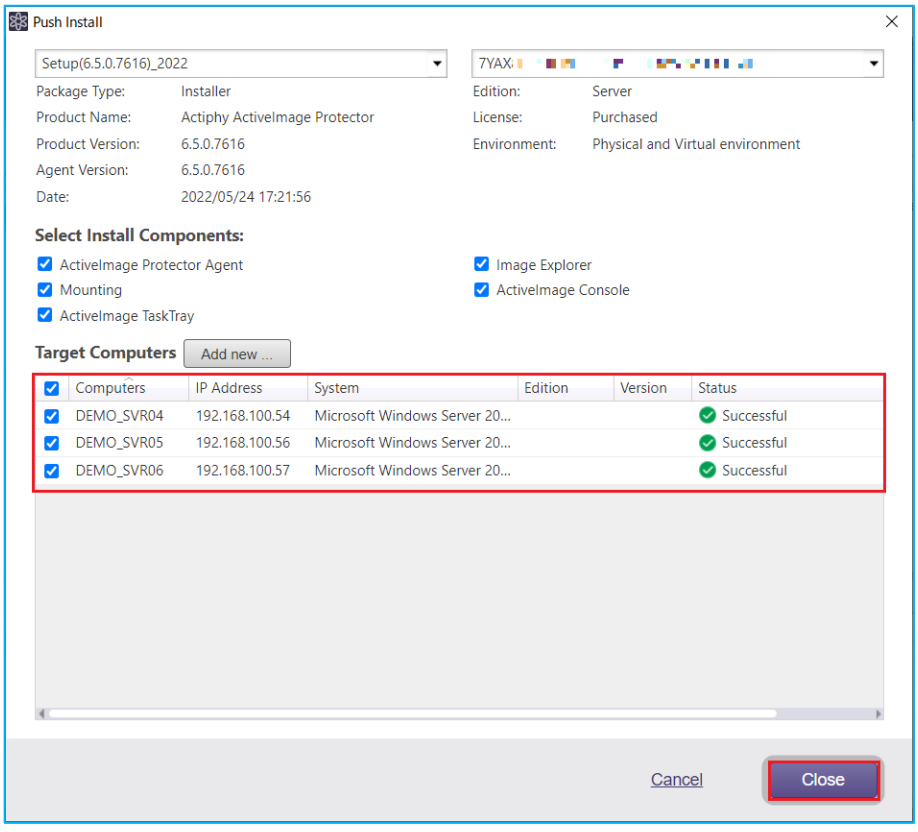
6. ActiveVisor lists the managed computers. If you have installed the ActiveImage Protector agent, the computers will have a green icon and show up in the **[Managed Clients]** section. If the agent is missing, the computers will have a gray icon and show up in the **[Network Computer]** section. To move a computer from the **[Network Computers]** section to the **[Managed Clients]** section, select a computer without the ActiveImage Protector agent and click the **[Add]** button. You can also add multiple computers by holding down the CTRL or Shift keys and clicking on the computers you wish to add.



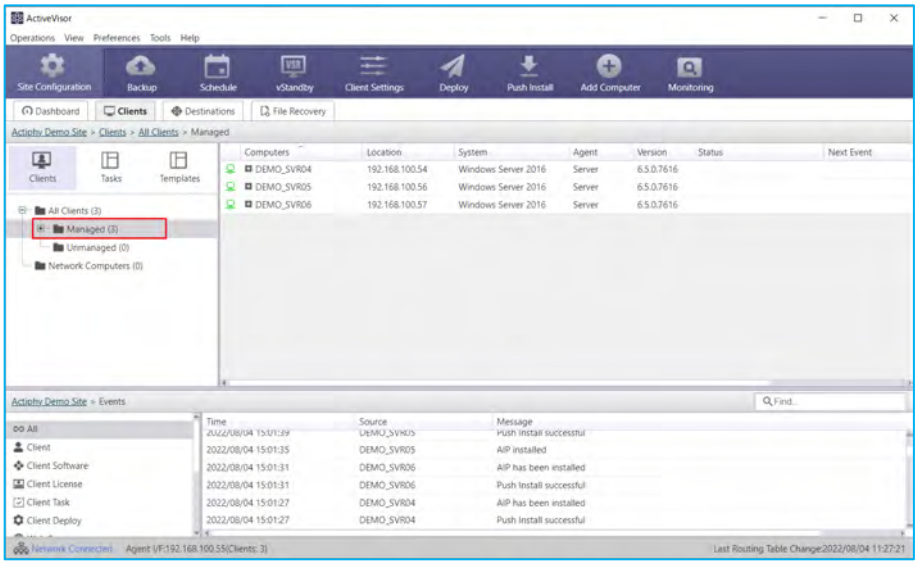
7. The computers targeted for push-install are added to the **[Target Computers]** list. Click **[Execute]** to start push-installation.



8. Upon completion of push-install process, the following dialog is displayed. Click **[Close]** to close the window.



9. In **[Client]** tab, the computers which ActiveImage Protector agents were successfully pushed to are listed in **[Managed]** list and the icons are indicated in green. ActiveImage Protector agents version and type information are also displayed in the list.



4. Create and deploy templates for backup tasks

The following is an explanation of how to create and deploy templates for backup tasks and schedule settings.

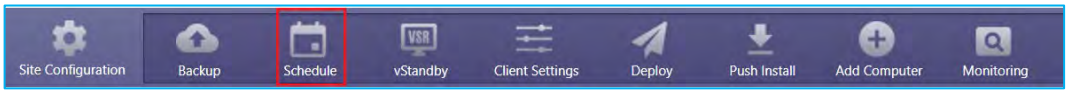
· Create schedule templates

· Create backup templates

· Deploy schedule and backup templates

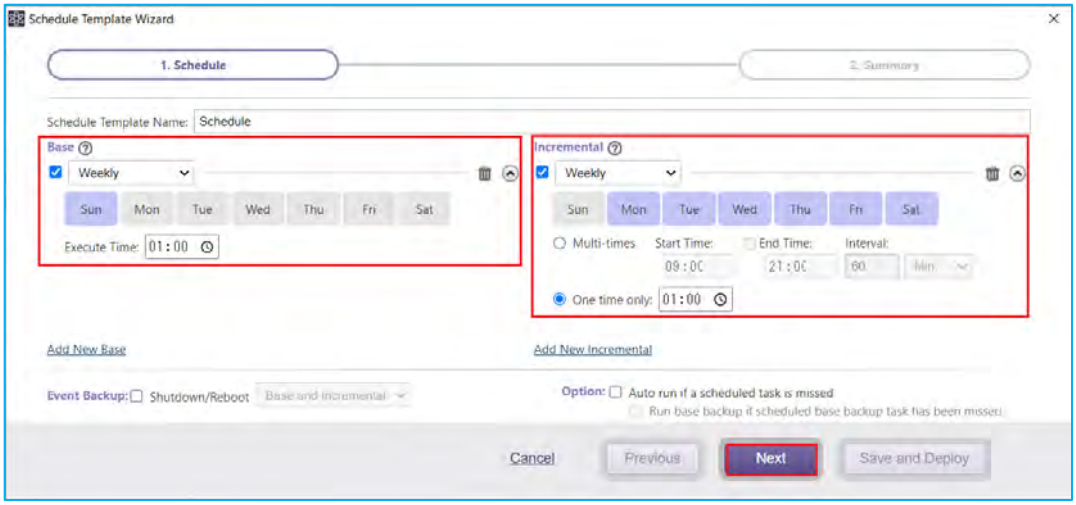
4.1. Create schedule templates

1. Select [Schedule] in the top menu bar and the Schedule Template Wizard will start.

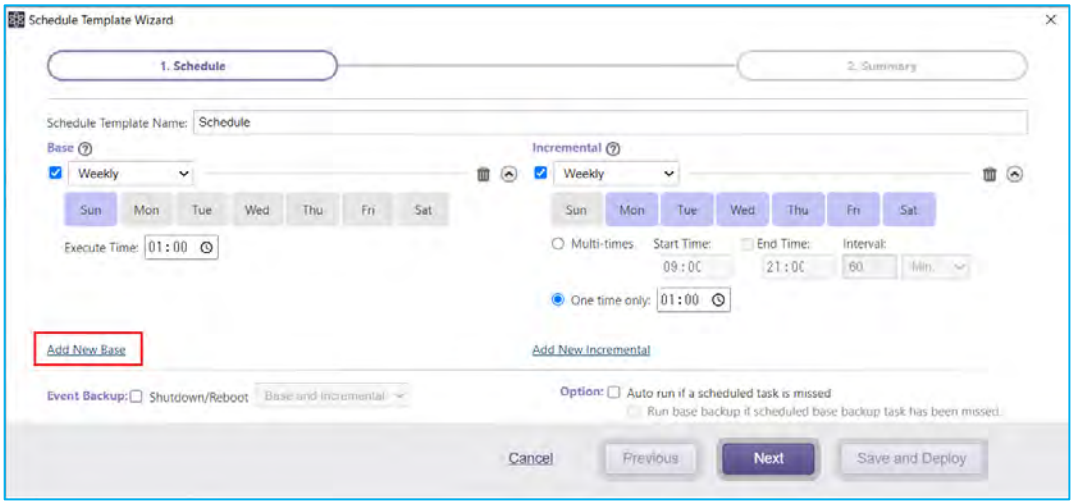


2. ActiveImage Protector has flexible backup schedule options [Weekly], [Monthly], [Specified Date] and [Designate **Specific Days].** In this example**, [Weekly]** is selected. Configure the Weekly backup schedule settings.
   - Base (Full) Backup : Weekly on Sundays at 1:00 a.m.
   - Incremental Backup : Monday to Saturday at 1:00 a.m.

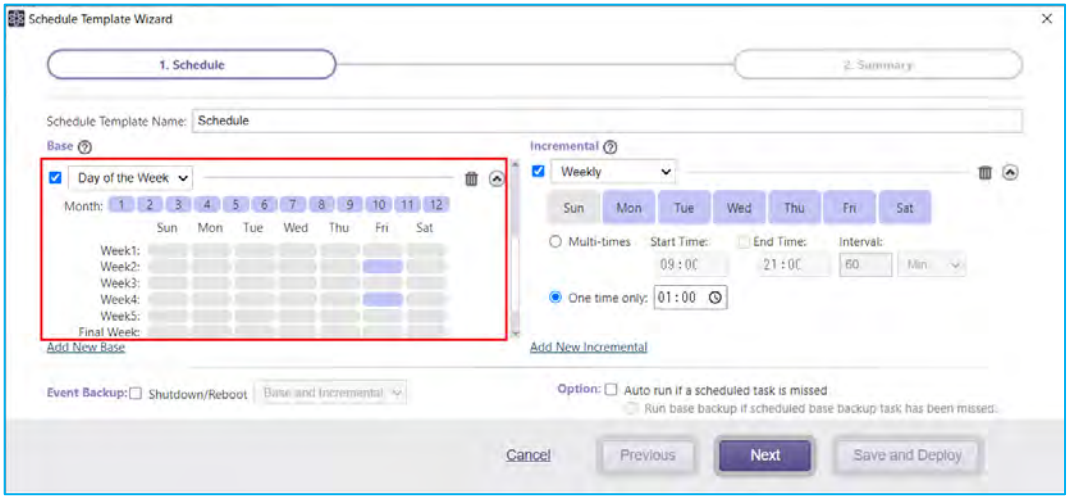
   When the schedule settings are configured, enter the template name and click **[Next].**



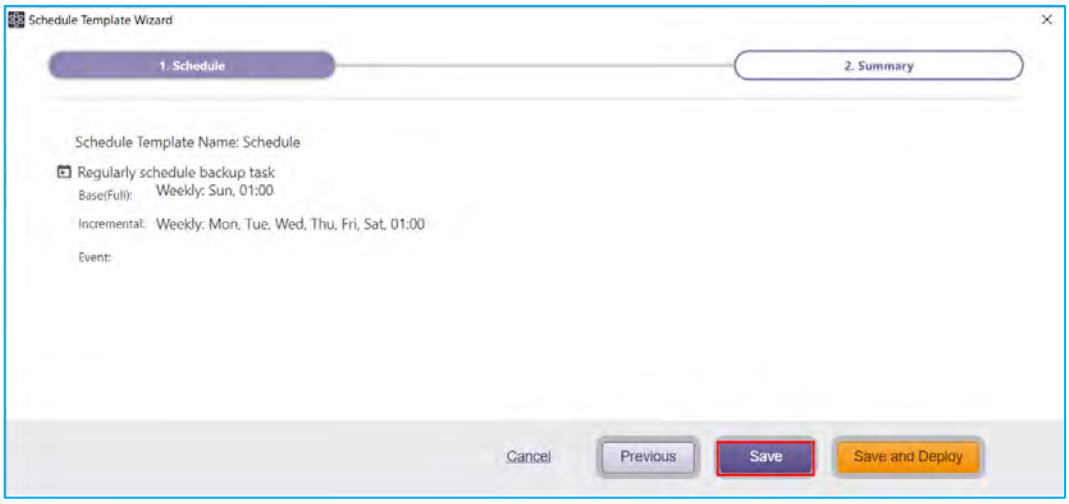
3. Click **[Add New Base]** / **[Add New Incremental]** to configure the additional schedule settings.



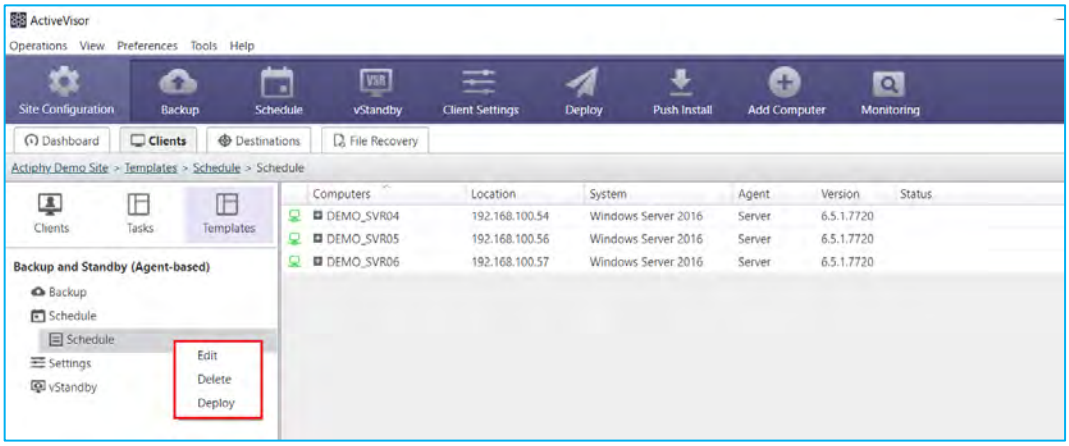
In addition to Weekly schedules, you can select **[Day of the Week]** to schedule backup tasks from January to December, for example on the "second Friday" or "4th Friday".



4. Review the configured schedule settings and click **[Save]**.

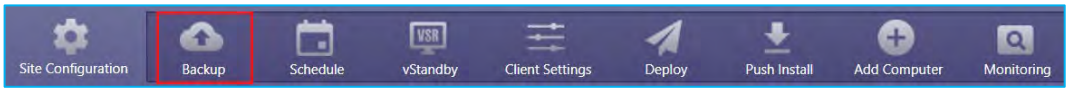


5. To edit, delete or deploy the template, right-click on the template name under schedule.

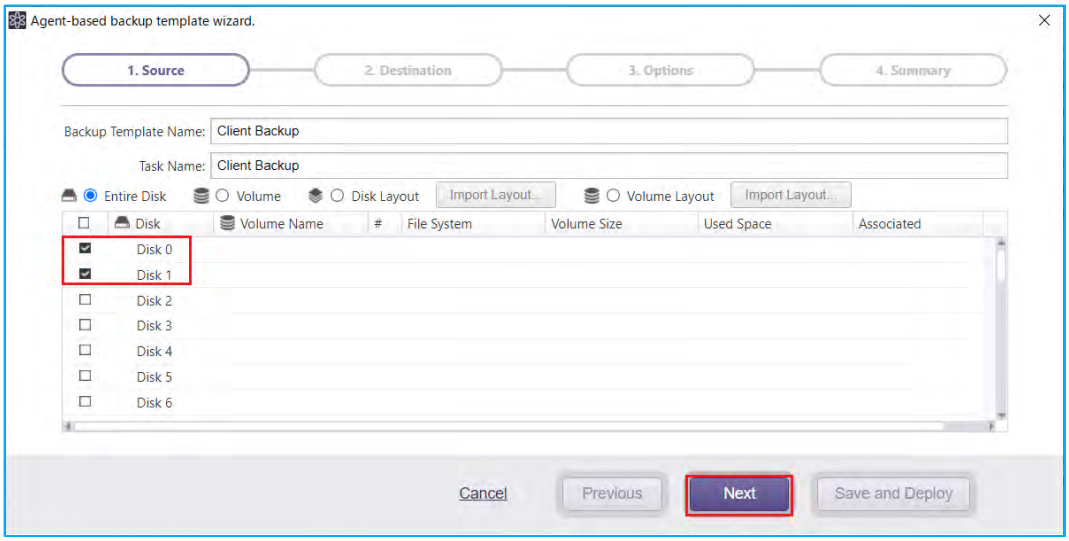


4.2. Create backup template

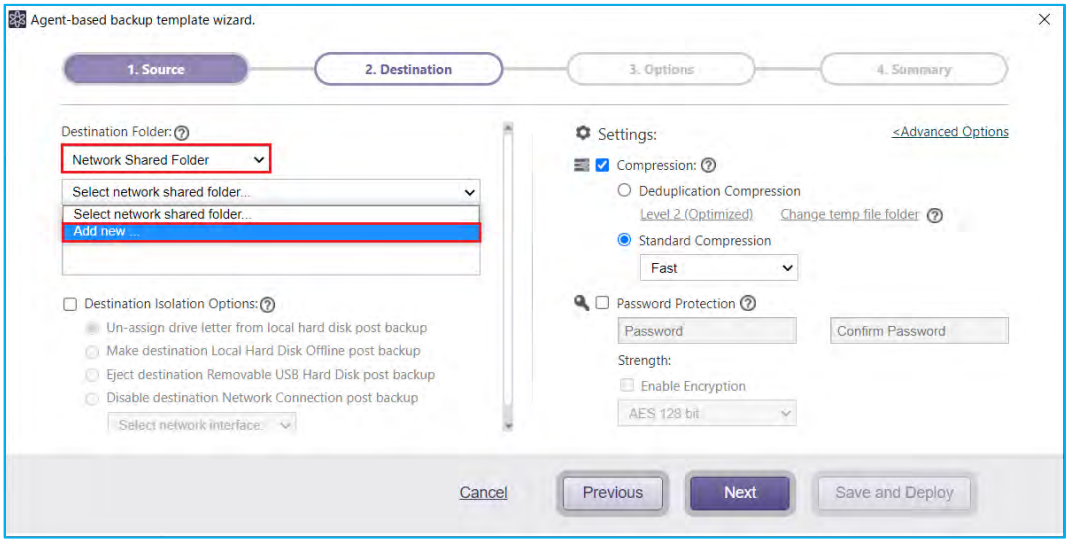
1. The following describes how to create backup templates and select backup source disks and backup destination folders in the template. Click [Backup] on the top menu and select [Agent-based backup template wizard].



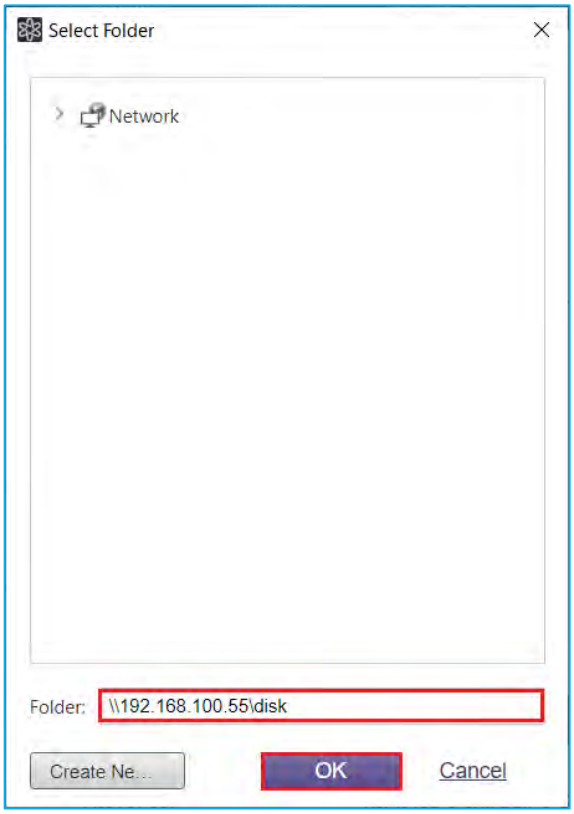
2. Note, ActiveVisor supports backing up a maximum of 31 volumes. In this example, “Disk 0” and “Disk 1” are selected as disks to match in the template. Click [Next]. The physical disks located the backup source computer are set as a backup source if they are selected in the template. For example, if “Disk 1” does not exist on the backup source computer, only “Disk 0” is set as the backup source.



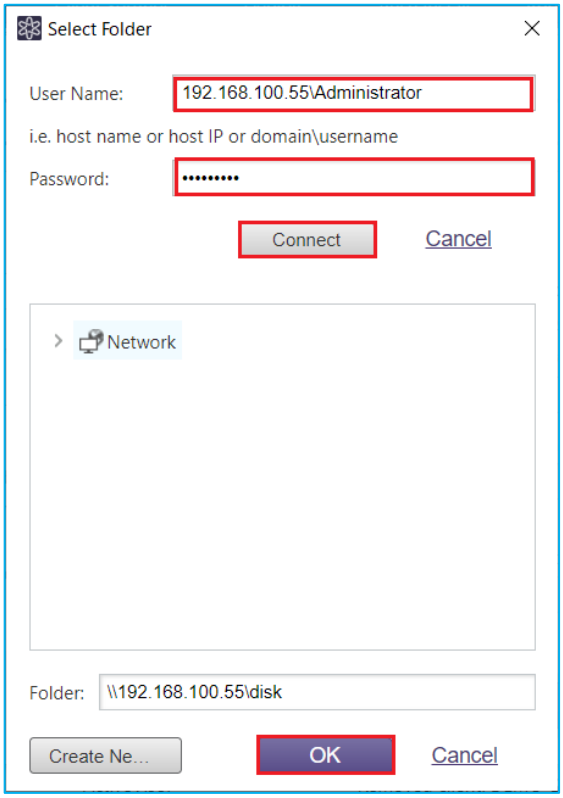
3. Specify a destination location for saving backups. Click “▼” to the right of [Destination Folder] and select [Network Shared Folder]. ActiveVisor maintains a list of all managed computers backup destinations, you can select one of these destination or you can also add a new destination folder, click “▼” to the right of [Select network shared folder] and select [Add new].



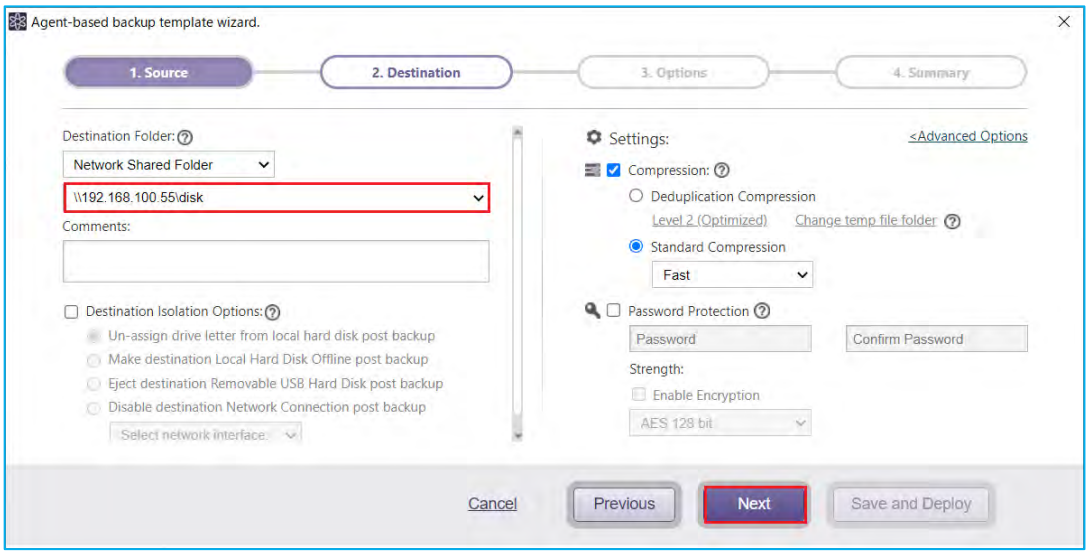
4. Please select a destination folder. In this example, network shared folder "¥¥192.168.100.55¥disk" is specified for [Folder:]. Click [OK].



5. Enter the credential information to access the shared folder and click **[Connect]**. After authentication, click **[OK].**



6. Please configure the settings for **[Destination Isolation Options:]**, **[Settings:]**, and **[Advanced Options],** as required. In this example, we will use the default settings.
   Click **[Next].** Please configure the settings for **[Compression:]**, **[Password Protection]** as needed.



- **Compression:**

  ActiveImage Protector has two compression types; One is Standard Compression and the other is Deduplication Compression. The compression ratio differs depending on the data type. Standard Compression compresses data up to 30% and deduplication compression reduces the file size up to 50% of the backup source. To enable compression, tick the checkbox for **[Compression]** in the **[Option]** pane. When selecting Deduplication Compression, you can set the level of compression and **[Change temp file folder]** specifying the location for deduplication to process temporary files. Deduplication compression consumes more CPU and memory than standard, so on machines with heavy IO loads, **[Standard Compression]** is recommended

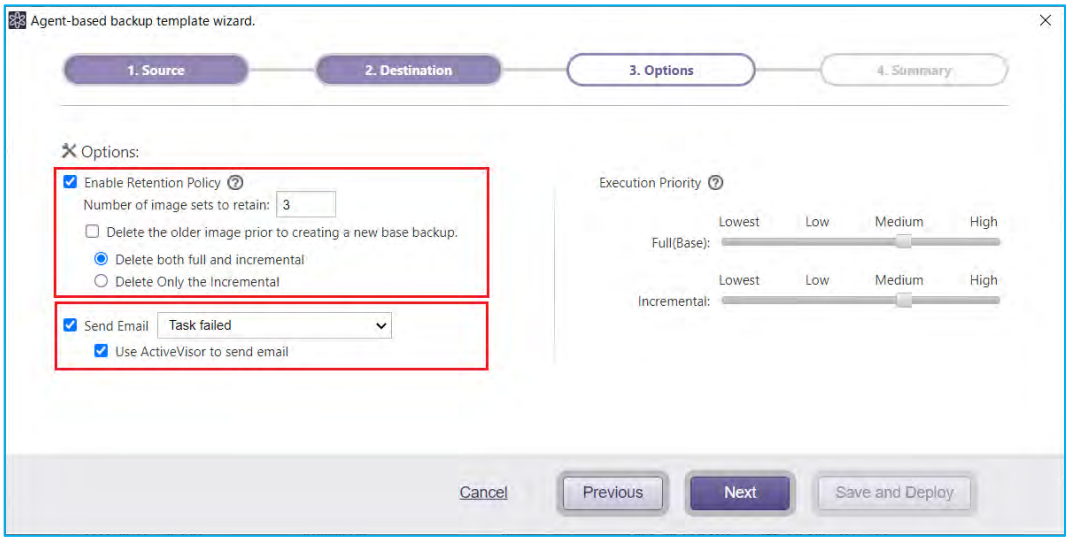
- **Password Protection:**

  Password protect the backup image file by assigning a unique password. This ensures that password input is required for mounting, exploring, or restoring any of the contents of the image file.

- **Enable Encryption:**

  There are three levels of encryption to choose from “RCS”, “AES128 bit”, “AES256 bit”.

7. In **[Options:]**, **[Enable Retention Policy]** and **[Send Email]** options are selected in this example. Click **[Next].**



- **Enable Retention Policy**

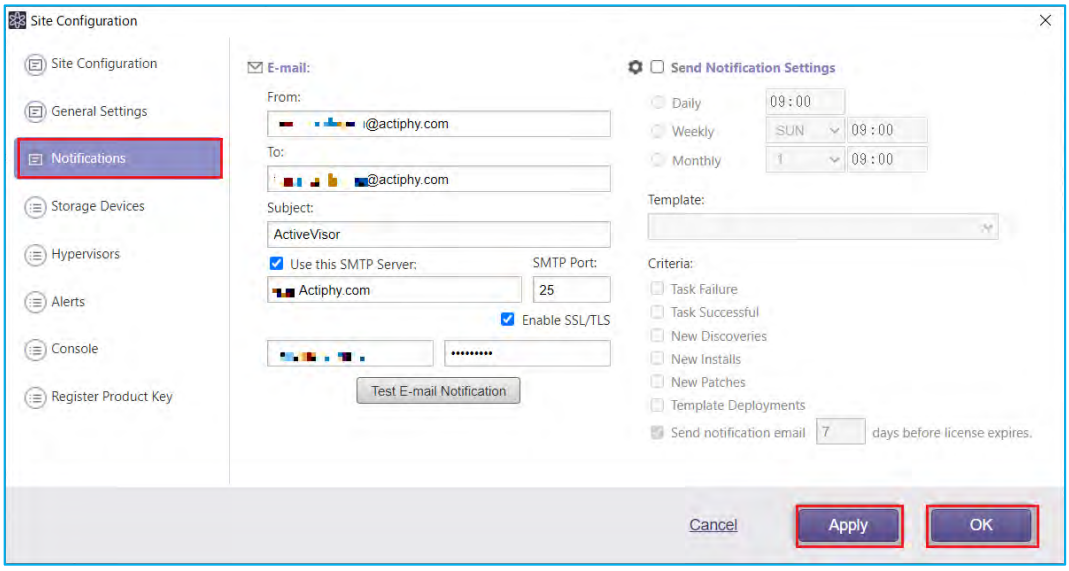
  Retention Policy defines how many sets of backup files to retain before deletion. In this example, **[Enabling Retention Policy]** is selected and the default setting "3" is entered for **[Number of image sets to retain],** so that three generations of backup files are retained in the destination folder.

  *One generation of ActiveImage Protector backup image files represents one base backup image file and the associated incremental backup files.

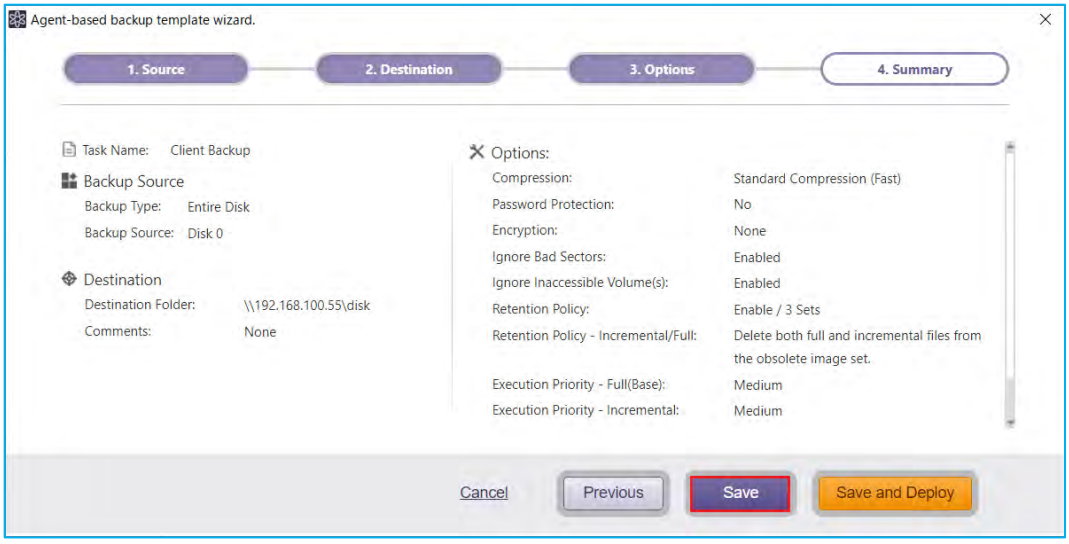
- **Send email**

  Enable this option to send E-Mail informing you of a task completion. **[Task failure]**, you will be notified of a backup task failure. Tick the checkbox for **[Send Email]** – **[Task failure / successful / completed]**, and **[Use ActiveVisor to send email]**. Before enabling **[Send email]** option, go to **[Site Configuration]** – **[Notification]** and configure the email settings.

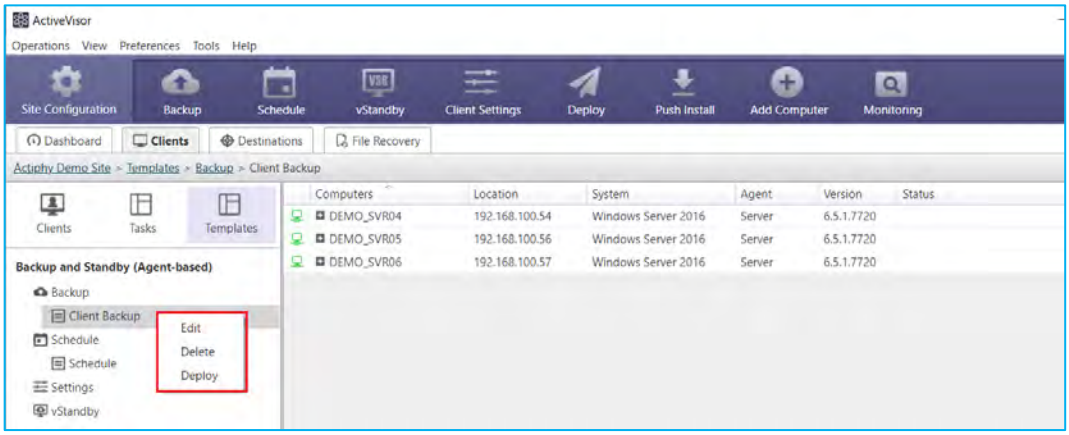
8. Go to **[Site Configuration]** -- **[Notification]** and configure the settings for email notification in ActiveVisor. When you complete the settings, click **[Test E-mail Notification]**. When you confirm that the email is working, click **[OK]**.



9. Use the Summary window to review the configured settings.
   Click **[Save]** to save the created backup template.

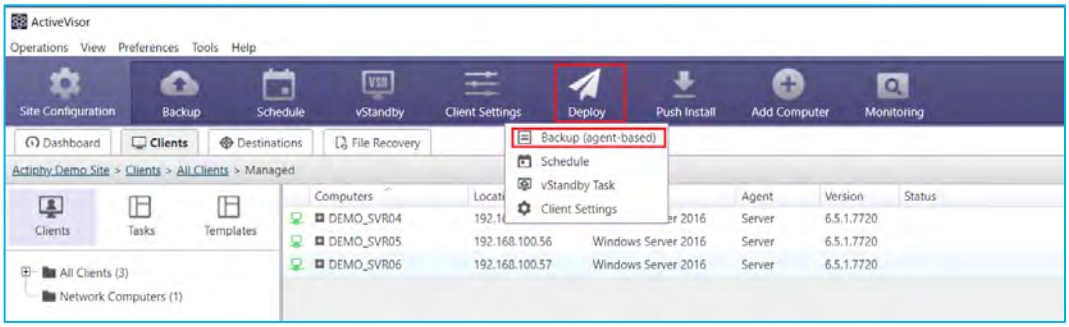


10. Once saved, the backup template can be found under **[Templates]** in the **[Client]** tab and can be edited, deleted or deployed.

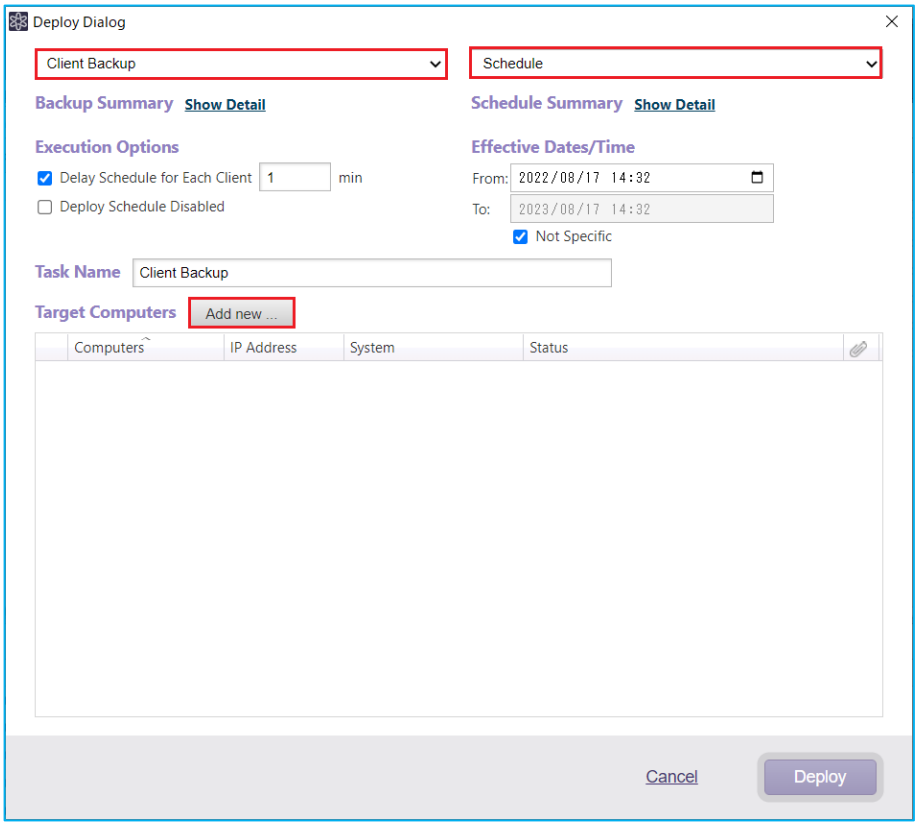


4.3. Deploy templates to managed computers

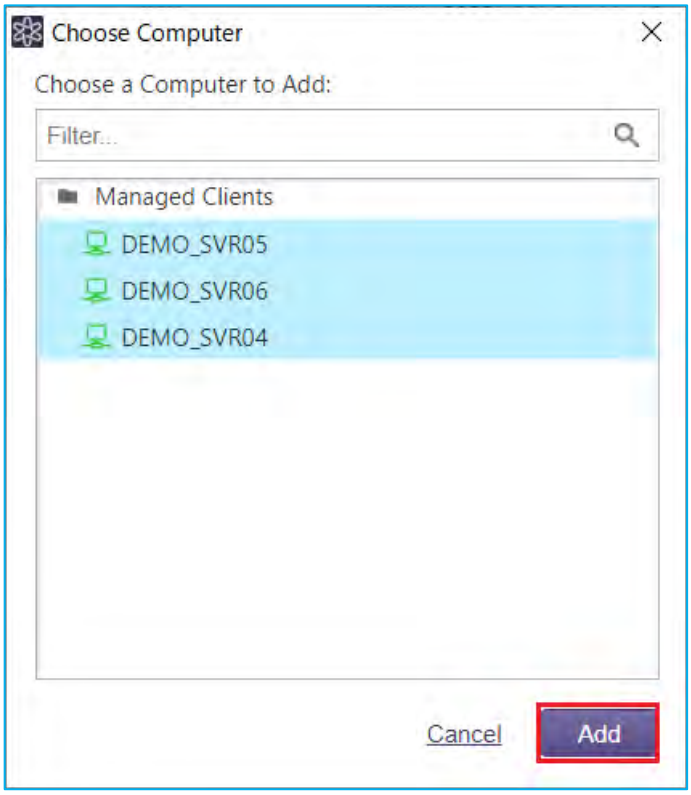
1. To deploy backup templates to clients click **[Deploy]** on the top menu and select **[Backup (agent-based)]** from the drop-down menu.



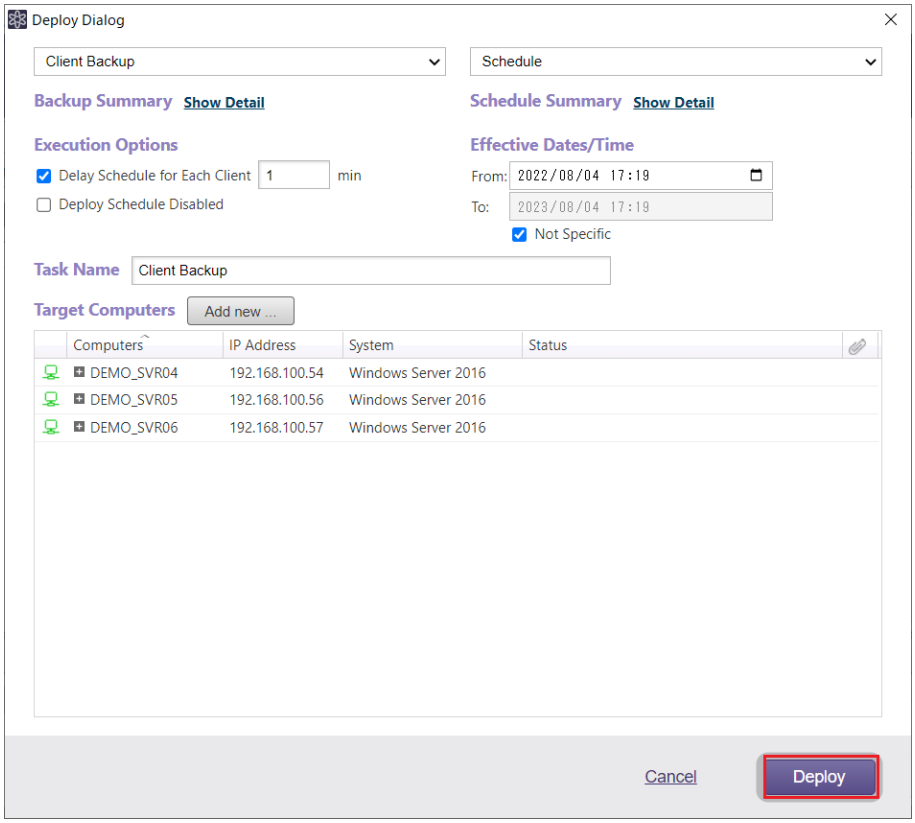
2. Select template items “Client Backup” and “Schedule” from templates created in Step 4.1 and 4.2. Next, click the **[Add new]** button and select the target computers to deploy the templates to.



3. After selecting the deploy target computers, click **[Add]**. When selecting multiple computers, press Ctrl or Shift key and select the computers.



4. The selected computers are added to **[Target Computers]** list. Please configure the following settings for **[Execution Options].**

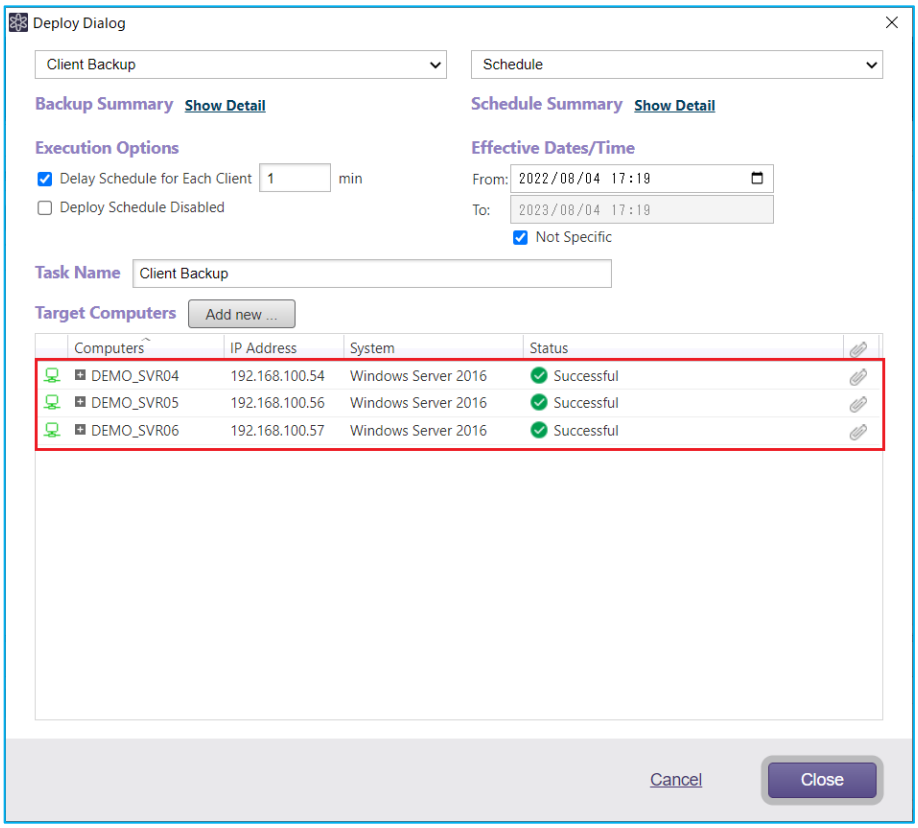


Execution Options:

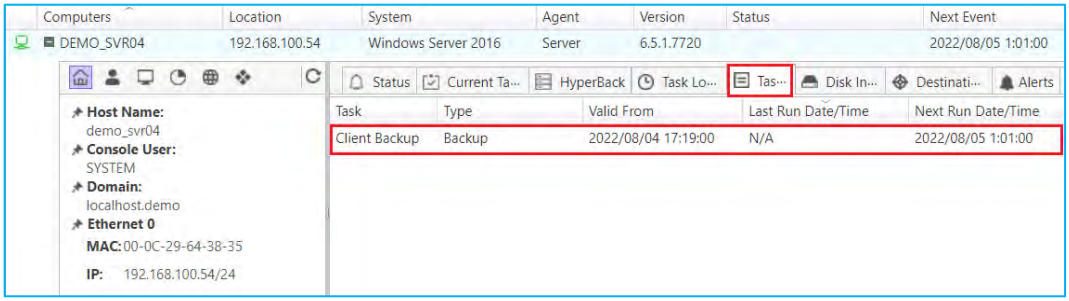
- **Delay Schedule for Each Client xx min:**
  Delay deploy tasks when deploying to multiple client computers by shifting the start time by the amount specified. Setting this may help with network congestion problems.
- **Deploy Schedule Disabled**
  Deploy the schedules to client computers in a disabled state.
- **Effective Dates/Time**
  Specify the period that the template is enabled. If you select **[Not specific]**, the schedule will be enabled for an unlimited period.

Review the configured settings, and click **[Deploy]**. The backup and the schedule templates will then be deployed to the target computers.

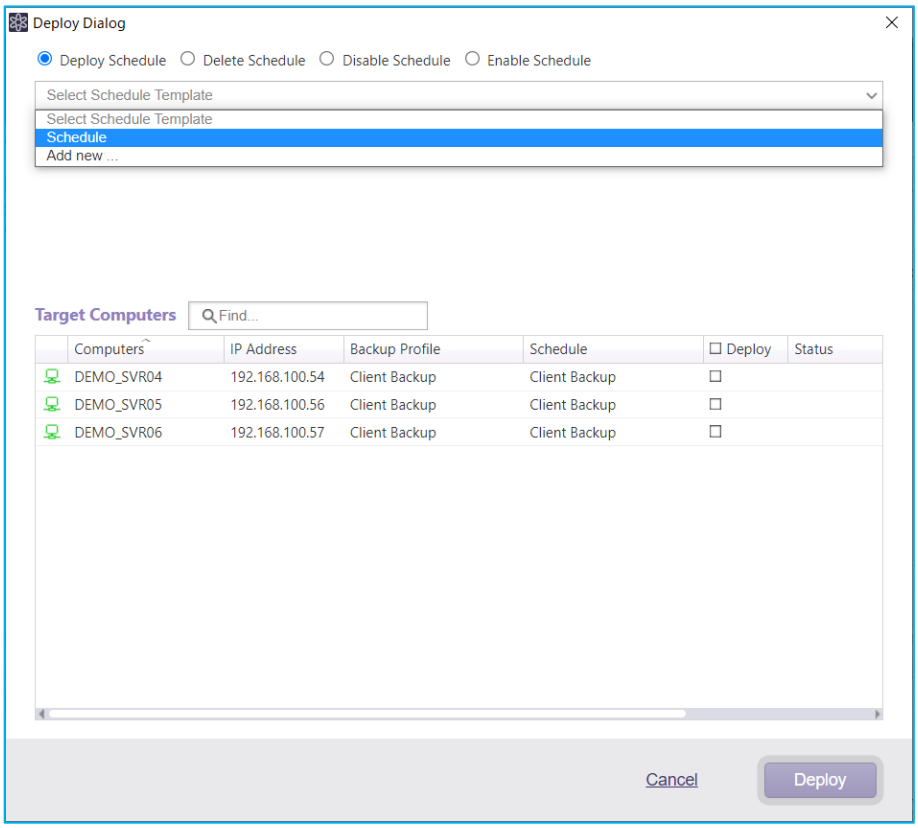
5. When the deployment task successfully completes, “Successful” is indicated for the **[Status].**



6. In the **[Task]** tab of the computer, you can see the deployed task is listed.



7. There are additional operations that can be deployed when select a schedule to deploy. Clicking on the **[Deploy]** icon on the top bar and selecting schedule will display the dialog below.
   In addition, to Deploy you can also select Delete, Disable or Enable Schedule.

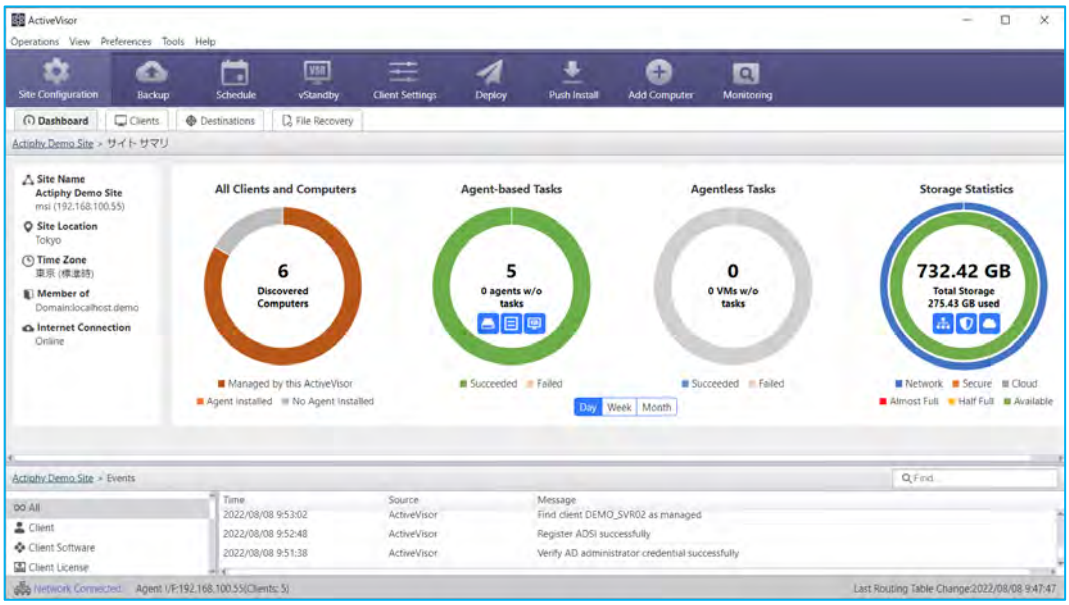


5. ActiveVisor's Monitor feature

ActiveVisor collects a displays a variety of information, such as task logs, status of backups, etc., from managed computer clients that can be useful in your daily backup operations and management.

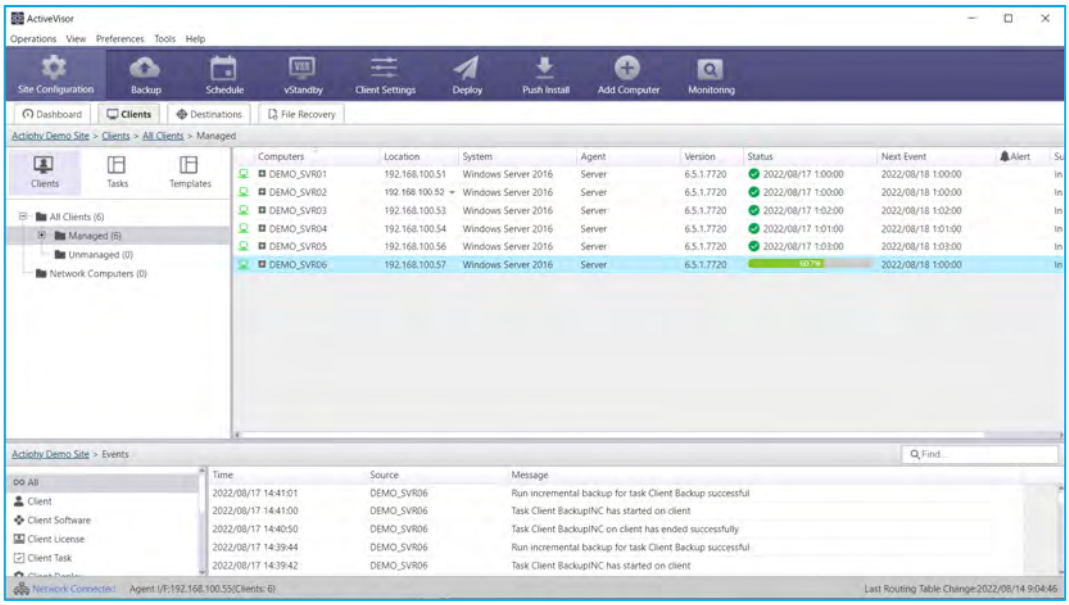
5.1. [Dashboard] tab

1. The **[Dashboard]** tab provides pie chart representations of the number of discovered computers, agent-based backup tasks, agentless backup tasks, successful / failed tasks, storage statistics, etc.

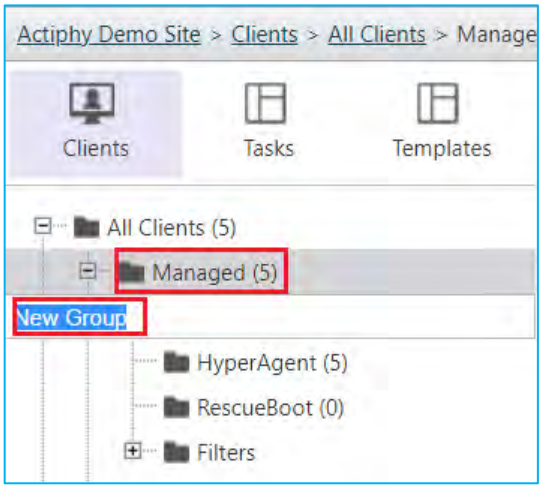


5.2. [Client] tab

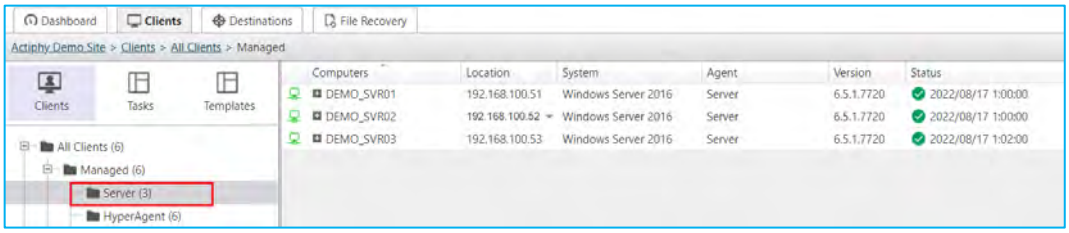
1. The **[Client]** tab is a list of the backup tasks configured on managed computers and provides real-time monitoring of the status of the backup tasks. The information of multiple managed computers is displayed in a list, so you can get an overall picture view of the status of all the computers from one location.



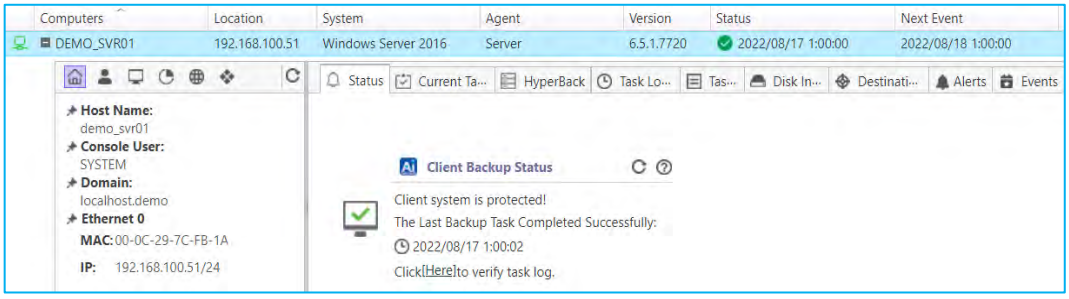
2. In the computer list, the managed computers can be divided into sub-groups. Right-click on **[Managed]** and click on **[Create New Group]** in the context menu.
   The **[New Group]** is created as a sub-group under [Managed].



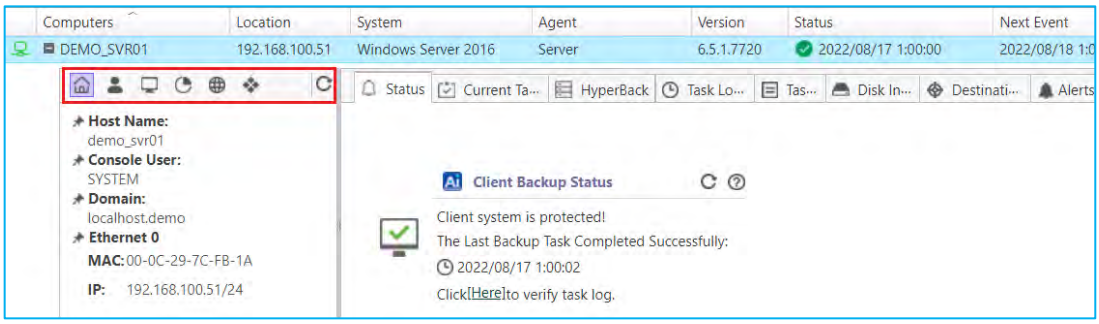
3. Drag and drop the any computer to the created sub-group. In this example, the sub-group "Server" is created and three computers "DEMO_SVR01～DEMO_SVR003" are moved to the sub-group.



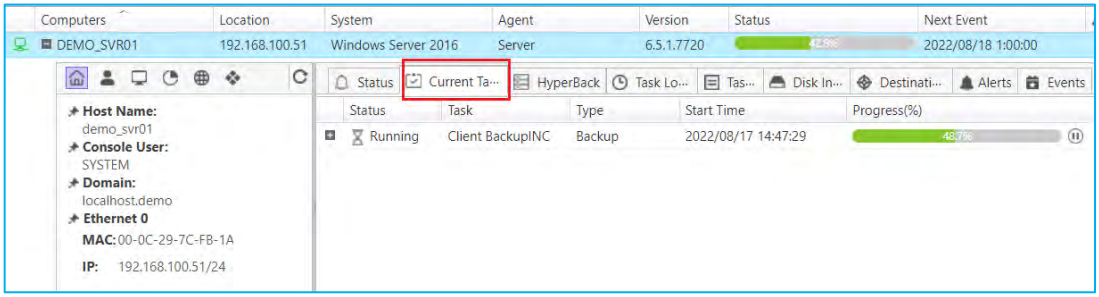
4. Click on "+" in front of the managed computer and more detailed information for the computer is displayed.



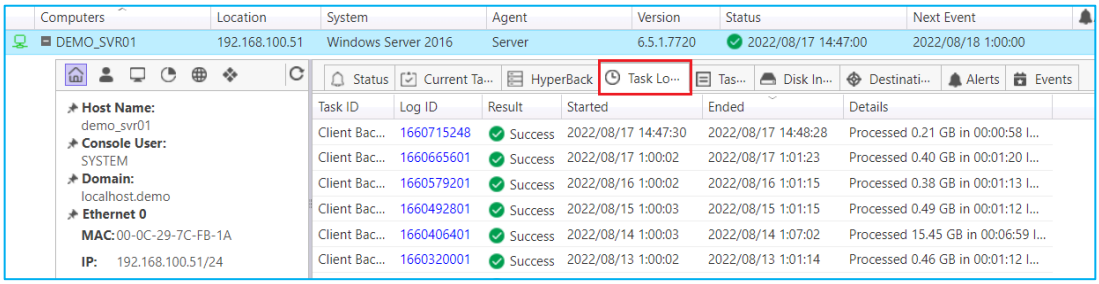
5. A panel of information icon buttons is located at the top of the left pane. You can review inventory information of managed computers including OS, network, etc. by clicking on the icons.



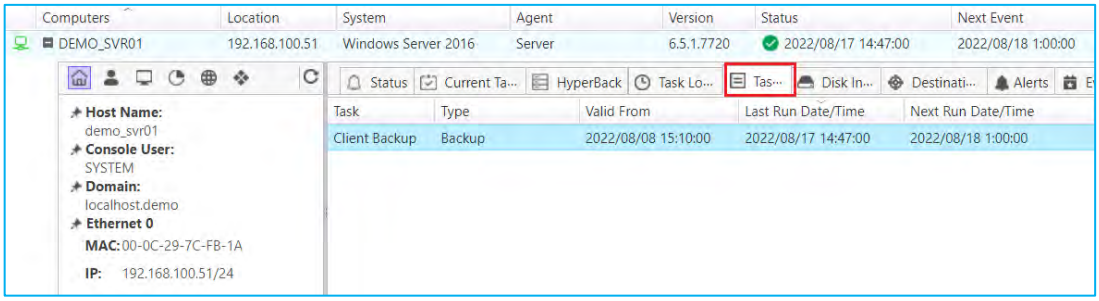
6. In the right pane on the top is a row of tabs for different information and operations. In the **[Current Task]** tab, you can monitor the status of running tasks. Running tasks will have a progress bar and process completion percentage displayed.



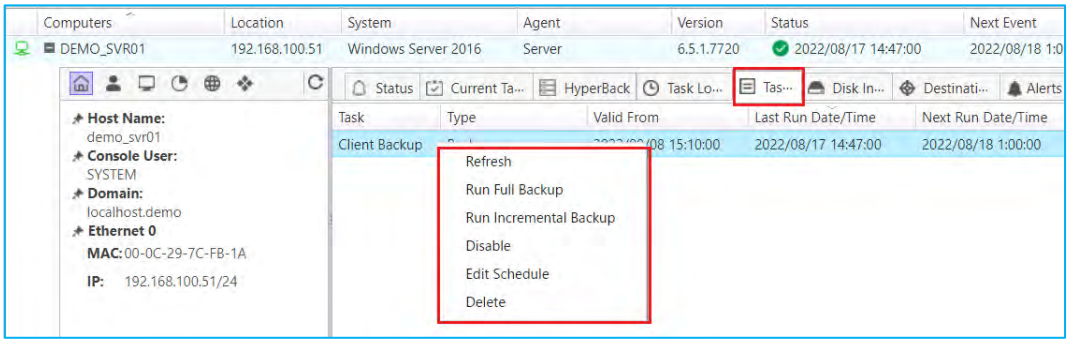
7. In the **[Task Log]** tab, you can view the task log information for the computer.
   Click on the "Log ID" to view detailed information of task log.



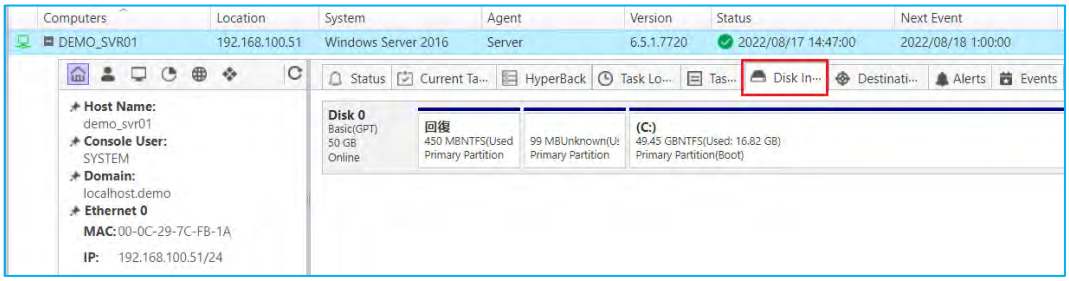
8. In **[Task]** tab, you can check tasks configured for the computer.



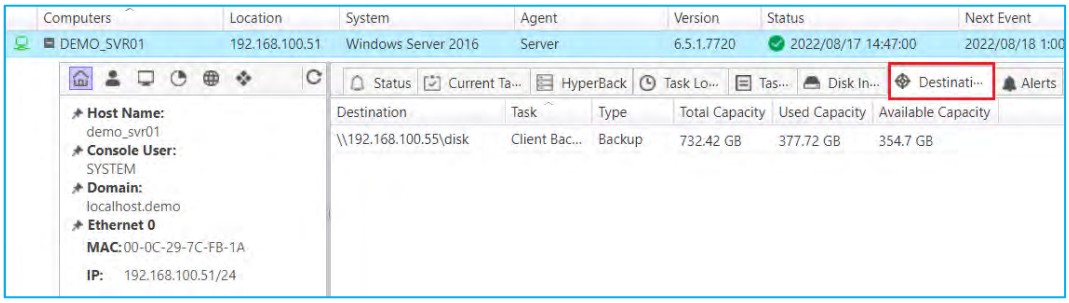
9. Right click on the **[Task Name]** to run tasks, **[Run Full Backup]**, **[Run Incremental Backup]**, **[Disable]**, **[Edit Schedule]**, **[Delete].**



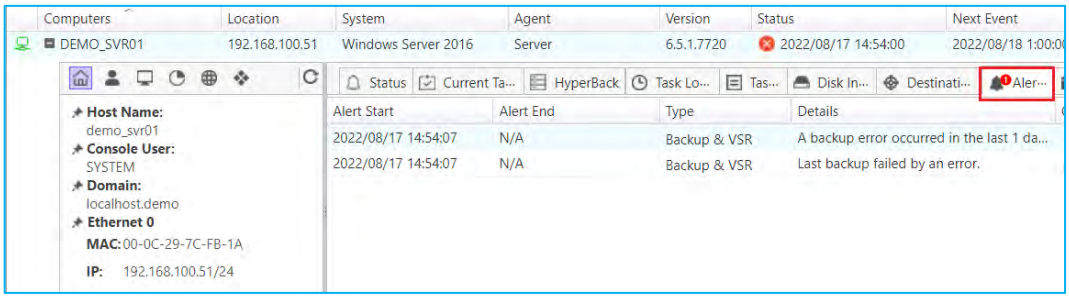
10. In the **[Disk Information]** tab, you can monitor the disk information.



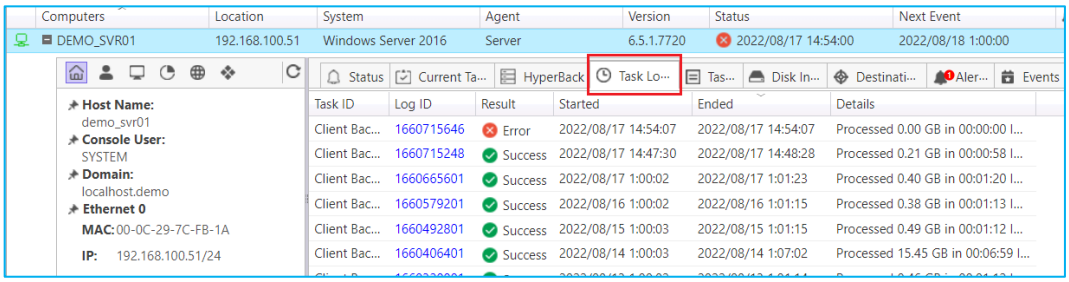
11. In the **[Destination**] tab, you can check the storage information including available space in the destination folder.



12. In the **[Alert]** tab, you can monitor the status of the alerts issued on the computer.

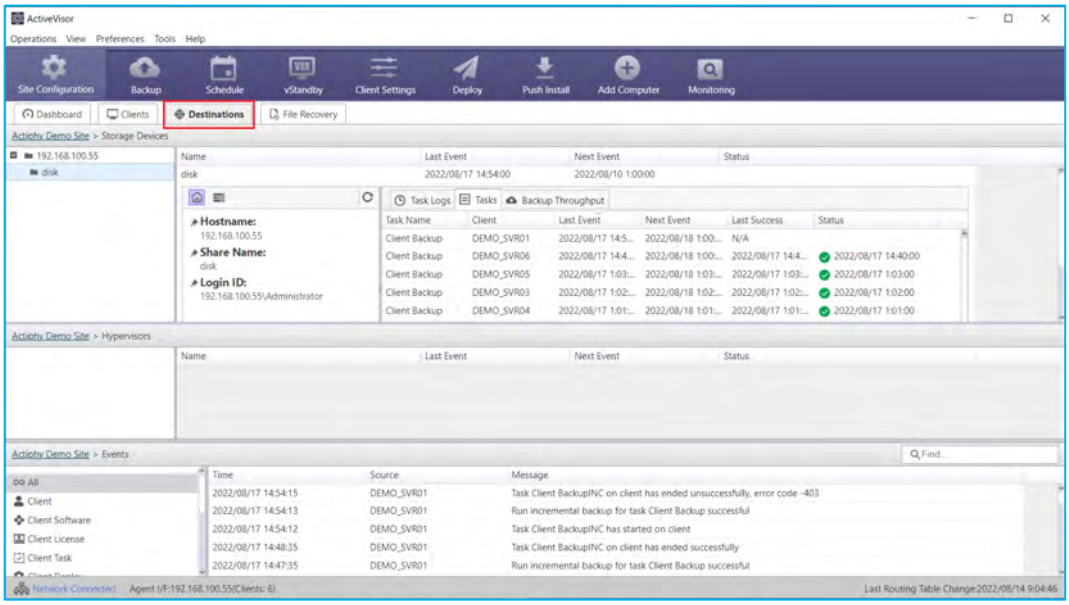


13. Click on the "Log ID" marked with a red icon and you can view more detailed information about an error.



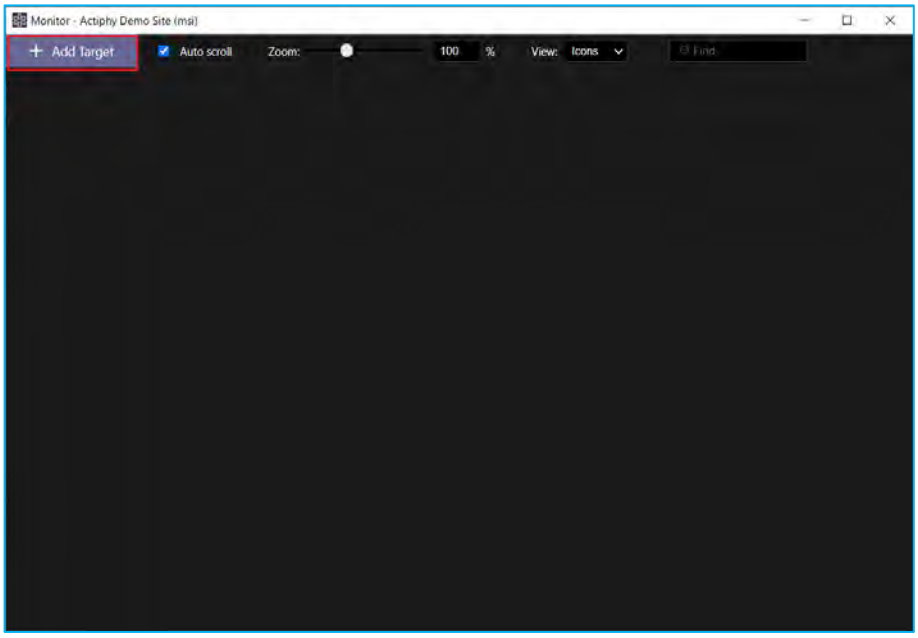
5.3. [Destination] tab

1. In the **[Destinations]** tab, you can check the information backup tasks, task logs, backup throughput that are related to the back destination. This view gives an overall picture of what is taking place on a backup destination.

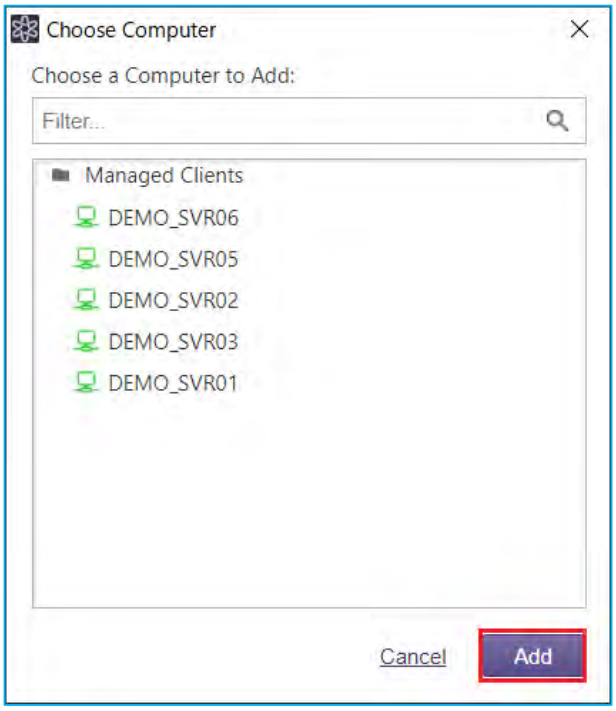


5.4. Monitoring

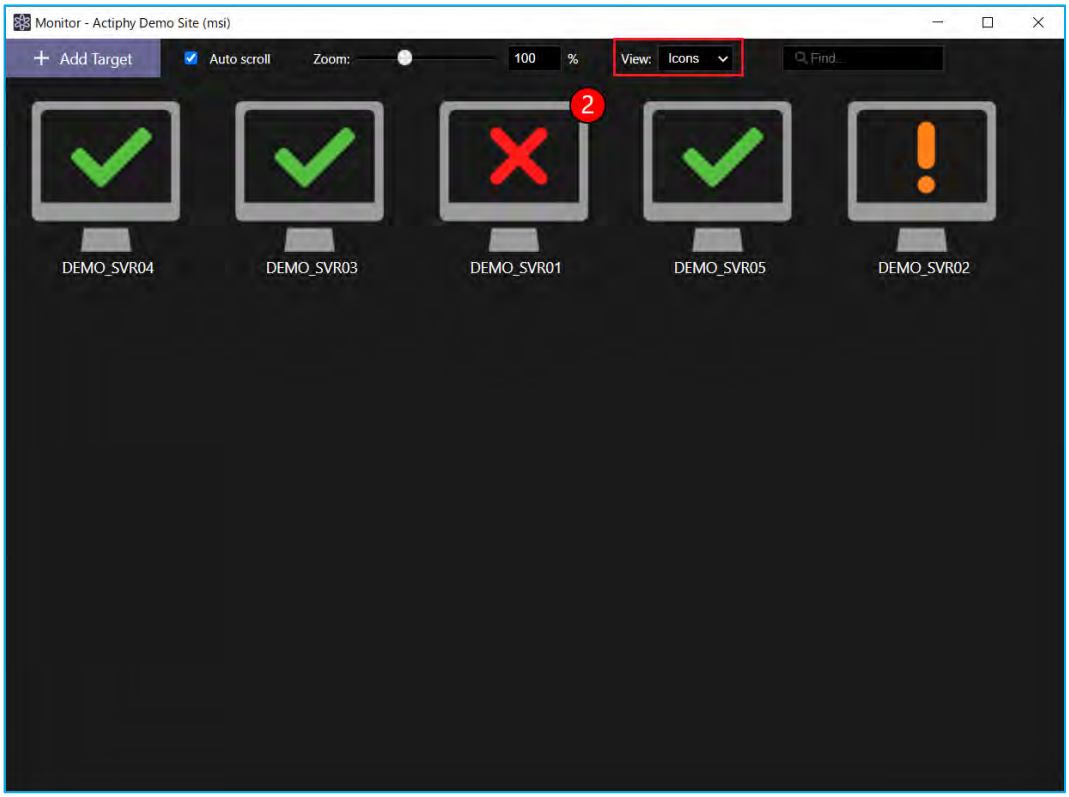
1. The **[Monitor]** window provides a visual indication of task execution status and alerts for managed computers. To start the ActiveVisor Monitor, select **[Monitoring]** in the top menu. To add client computers you want to monitor, Click **[Add Target]** at the left corner of the window.



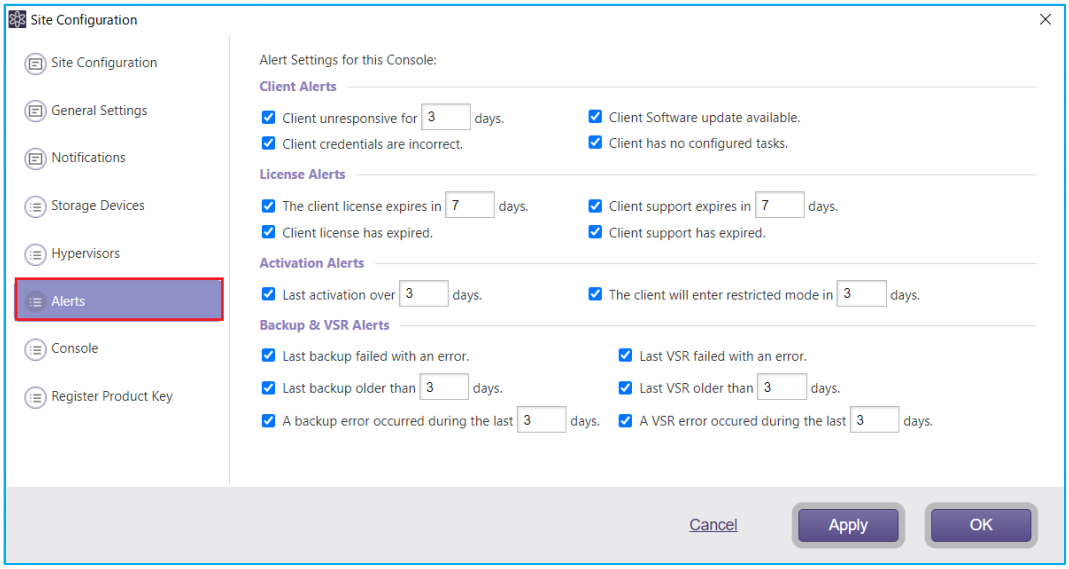
2. The **[Choose Computer]** window is displayed as depicted below. Select managed computers and click **[Add]**. When selecting multiple computers, press Ctrl or Shift key to multiple select items.



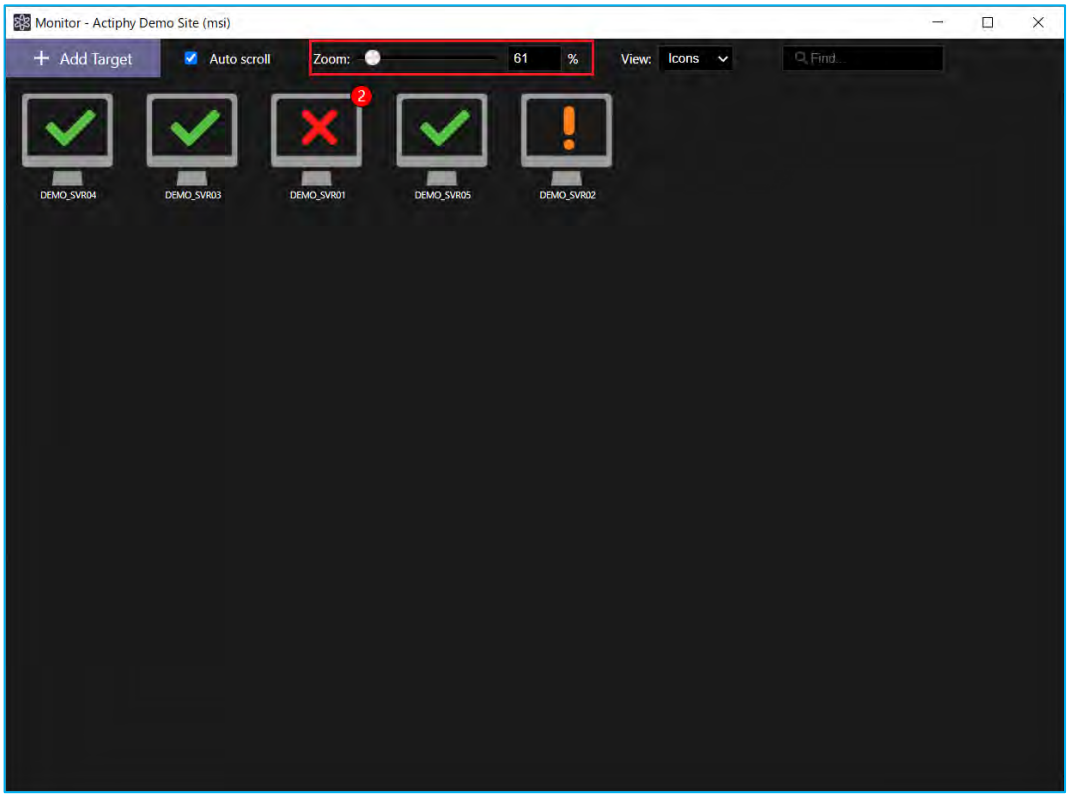
3. **[View Icons]**. The GUI displays a table view illustrating client task status for each of the select computers. A green "✓" indicates tasks were successful and a red "X" indicates task has failed. A "!" indicates no backup task has completed in a predefined period in ActiveVisor Alert settings, or that there is a network communication problem with the client and ActiveVisor, or some other problem. When managing many clients, the Icon view provides a visual indication of alerts (red and orange) on your managed computers.



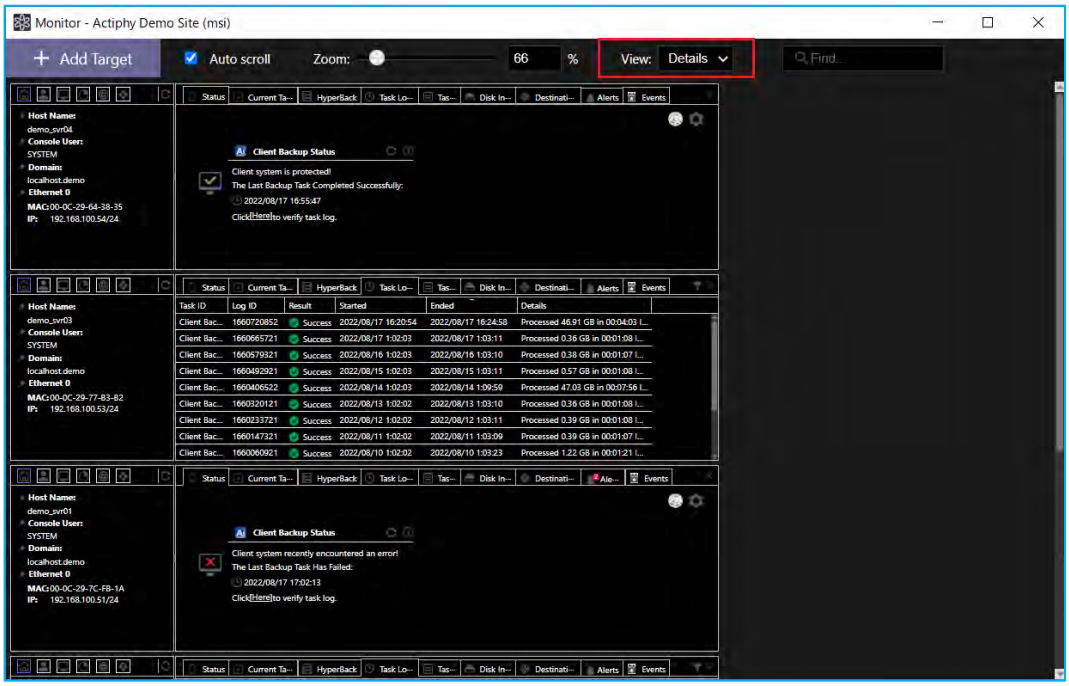
ActiveVisor Alert setting screen.



4. A zoom option is provided to zoom in / out the icon view.



5. **[View: Details]** provides detailed information that is mostly the same as the **[Agent-based]** tab in ActiveVisor's main window. ActiveVisor's monitoring feature provides an easy to understand visual indication of multiple managed computers status.



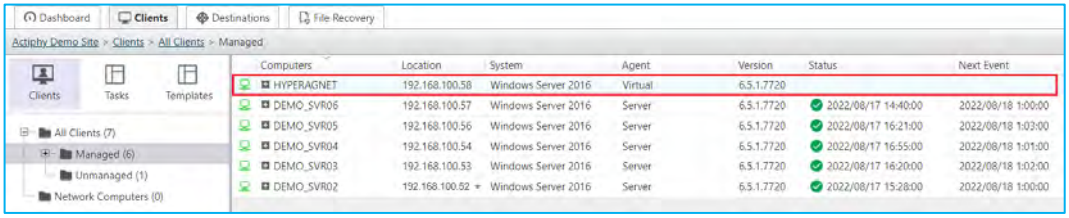
6. Centralized management using ActiveVisor

6.1. Agentless Backup

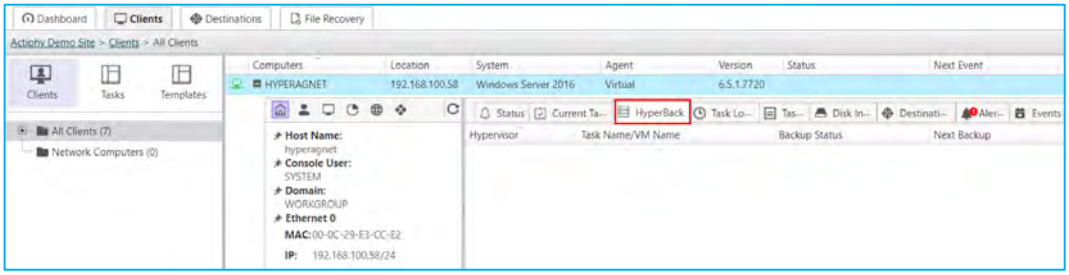
ActiveImage Protector' "HyperAgent", agentless backup feature, enables you to back up virtual machines on a hypervisor (Hyper-V or VMware vSphere) without the need for installing agents on the virtual machines. The following steps explain how to perform agentless vm backups using ActiveVisor.

* Before using agentless backup, "HyperAgent" needs to deployed to a computer on the same network as the hypervisor (for hyper-v the agent can be deployed on the hyper-v host) that hosts the vms to be backed up. After deployment HyperAgent can then be registered with ActiveVisor.

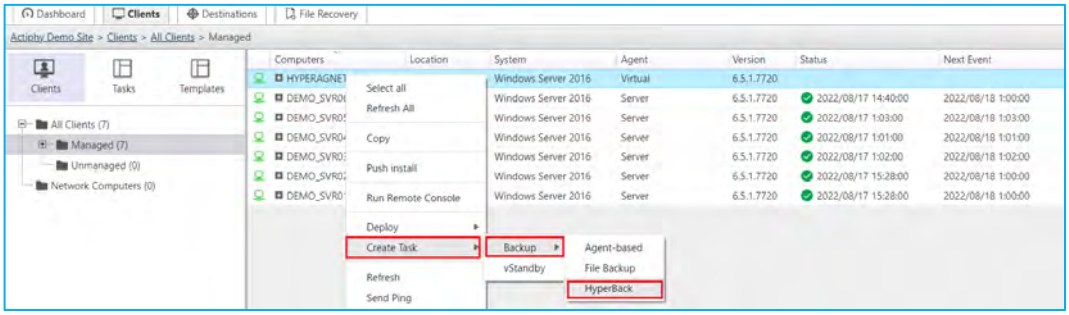
1. In this example, HyperAgent is deployed on the computer with the host name "HYPERAGENT". The steps below explain how to configuring the settings for HyperAgent.



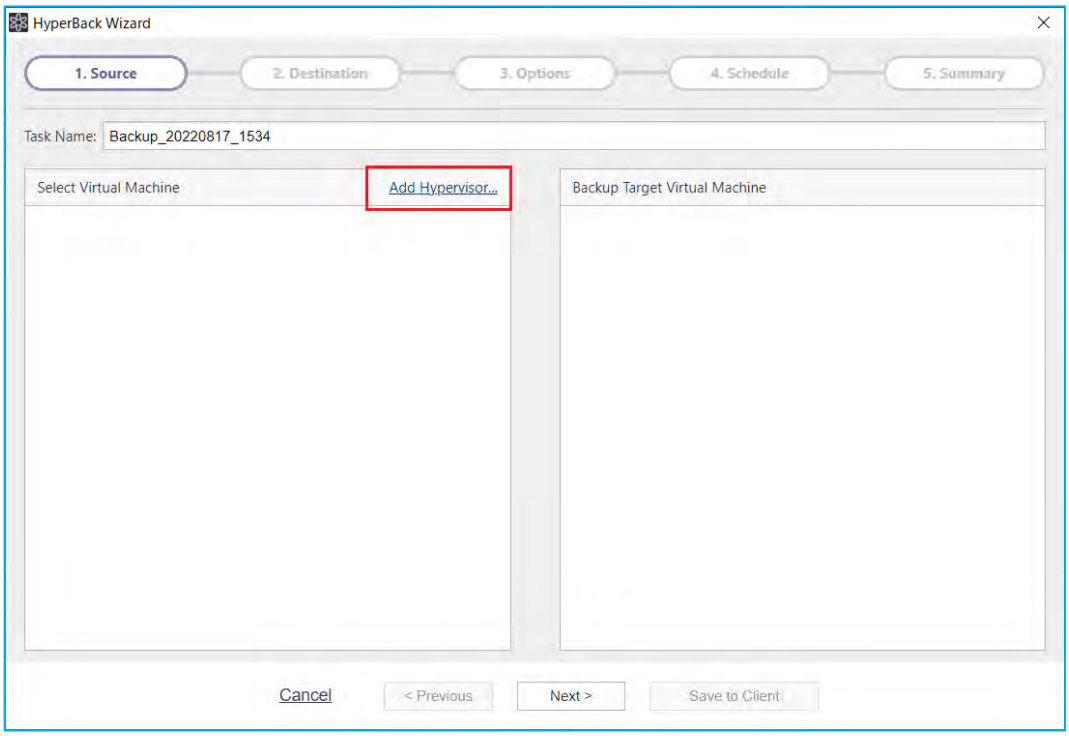
2. Actiphy's agentless backup feature is called "HyperBack". The **[HyperBack]** tab is located on the top of right pane of a selected managed computer on which HyperAgent is installed.



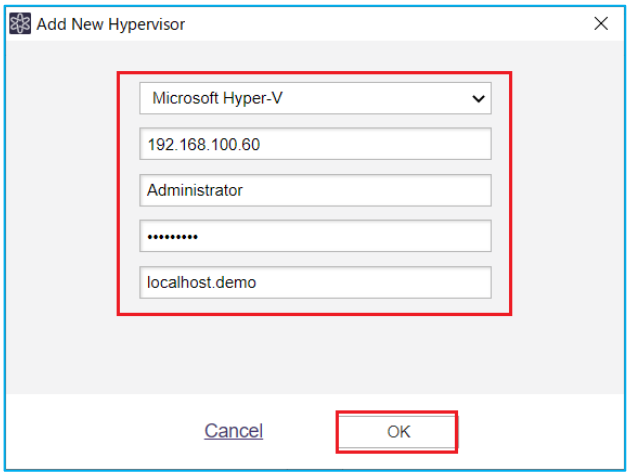
3. To create a backup task for a HyperAgent, right-click on a HyperAgent computer in the computer list, right click to select **[Create Task]** -- **[Backup]** -- **[HyperBack]** from the context menu and configure the backup settings.



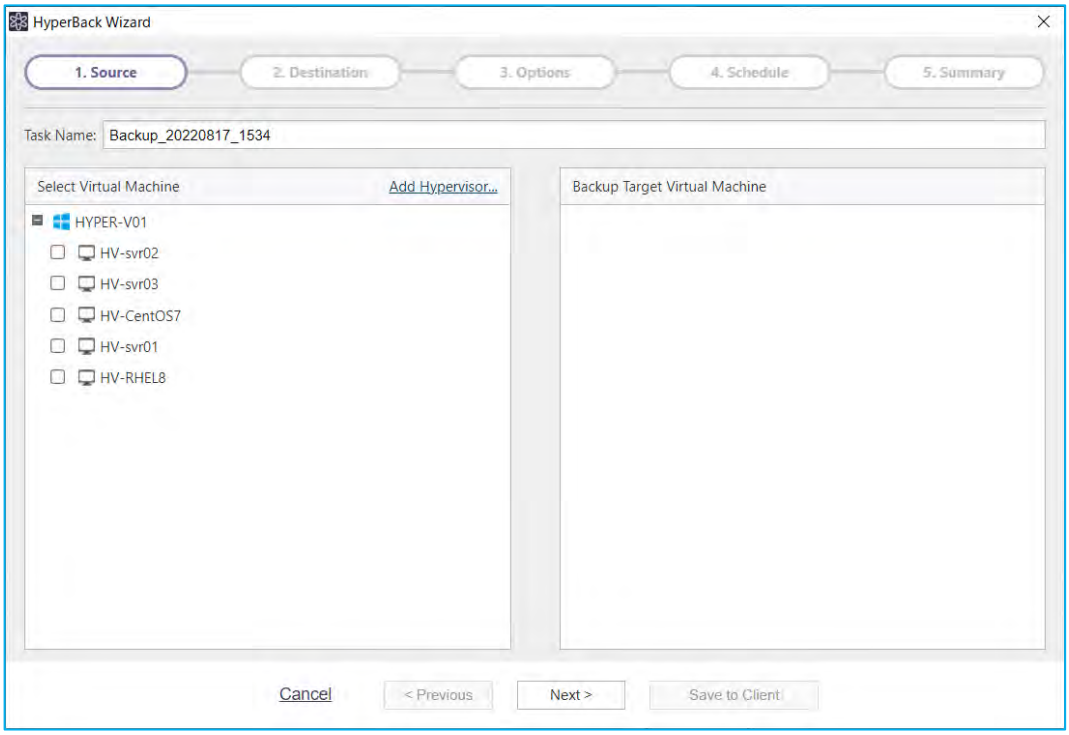
4. Register a hypervisor as a backup source to target virtual machines.
   Click **[Add Hypervisor]**.



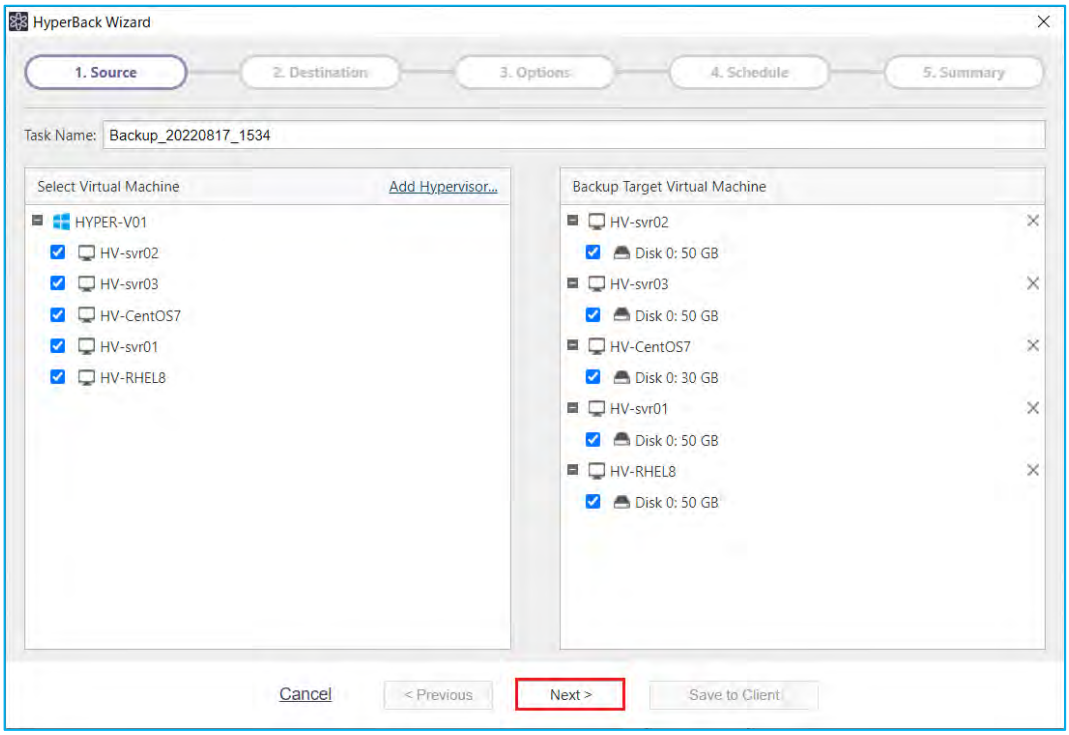
5. Select the type of hypervisor and the enter credential information. In this example, “Microsoft Hyper-V” is selected for **[Hypervisor Type]**, the IP address of Hyper-V host “192.168.100.60” is specified for **[Host Name or IP address:]**. Enter the user credentials and click **[OK]**.



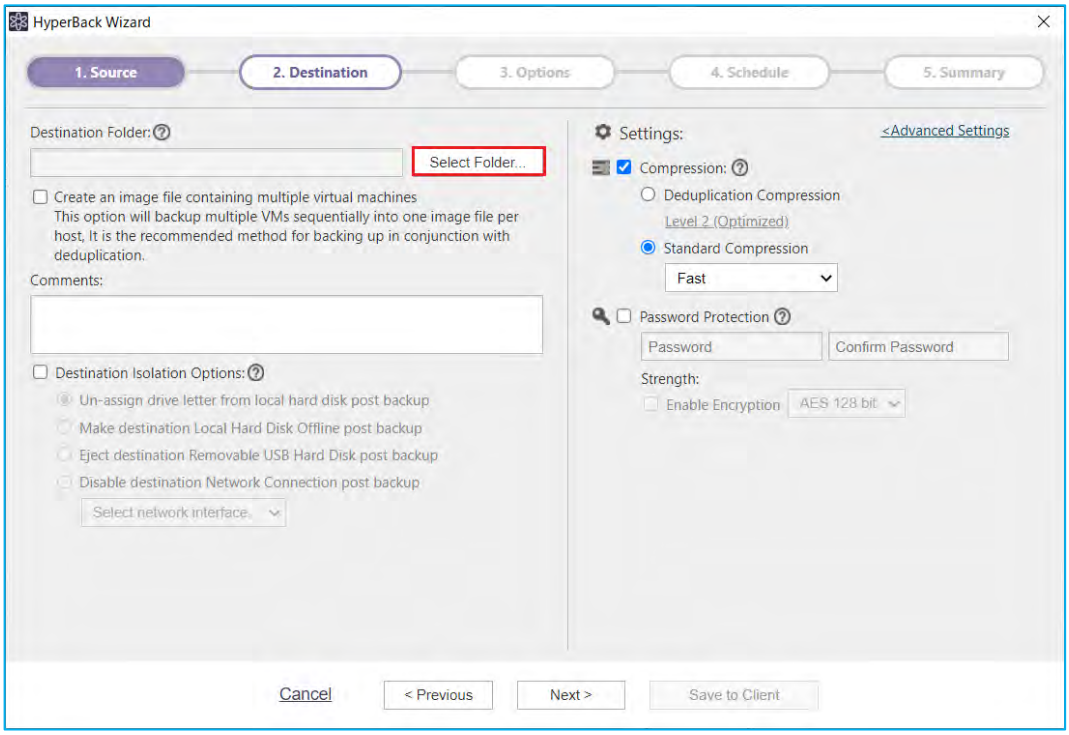
6. The following HyperBack Wizard window is displayed Click on the hypervisor to view a list of virtual machines, select the virtual machines you want to backup.



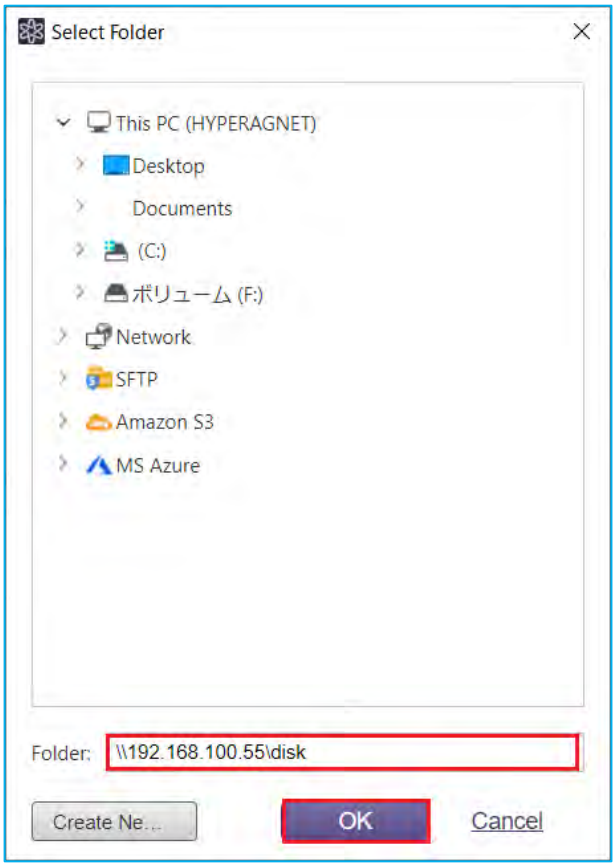
7. You can select virtual machines by ticking the check boxes on the left of vm name, virtual disks can also be selected or deselected on the pane on the right.
   Click **[Next].**



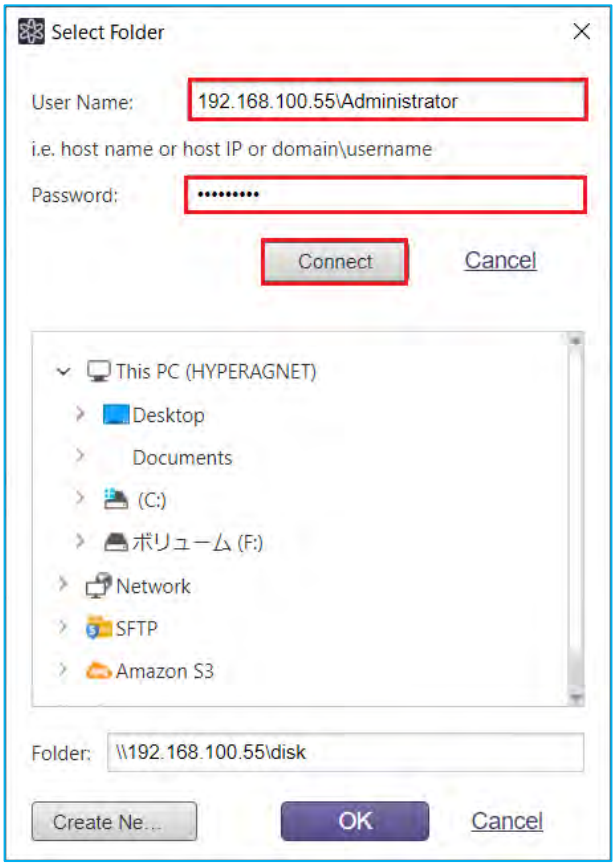
8. Specify the destination folder. Click **[Select Folder…].**



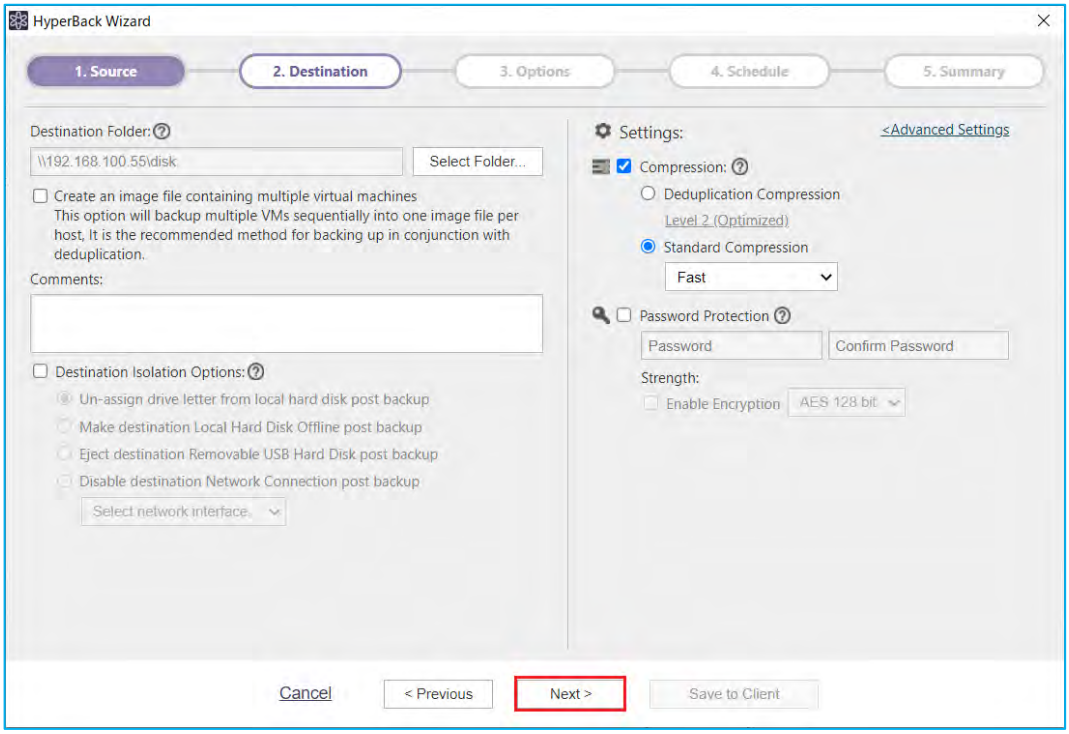
9. The **[Select Folder]** dialog is displayed. Browse to a folder or directly enter one in the text box. In this example, we have entered a shared network folder, "¥¥192.168.100.55¥disk" in **[Folder:]** field. Click **[OK]**.



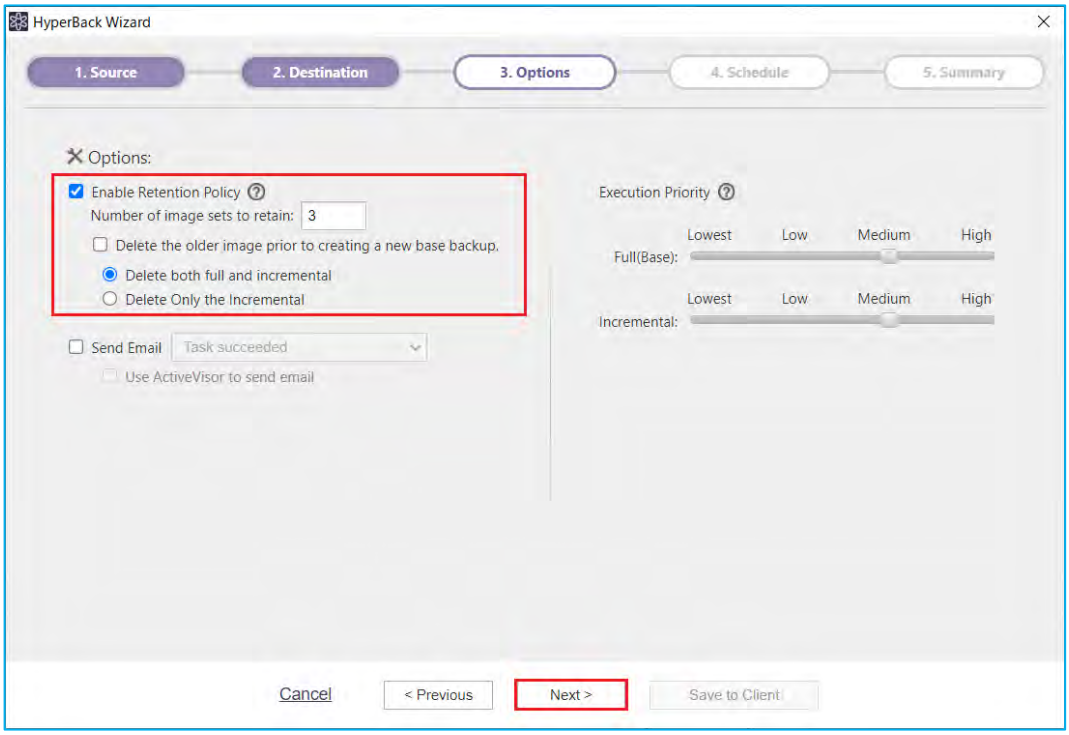
10. To access the contents of the folder enter the credential information (User Name, Password) and click **[Connect].**



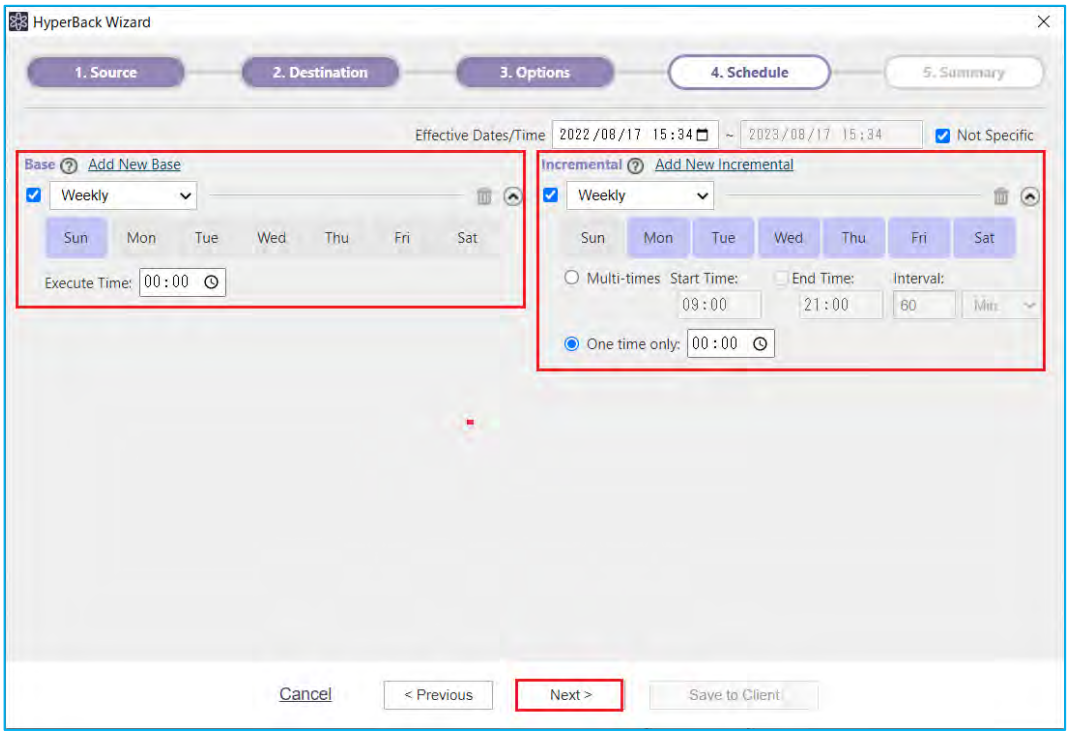
11. After selecting a destination folder click [Next]. Configure any needed settings for **[Destination Isolation Options:]**, **[Settings:]**, **[Advanced Settings].**



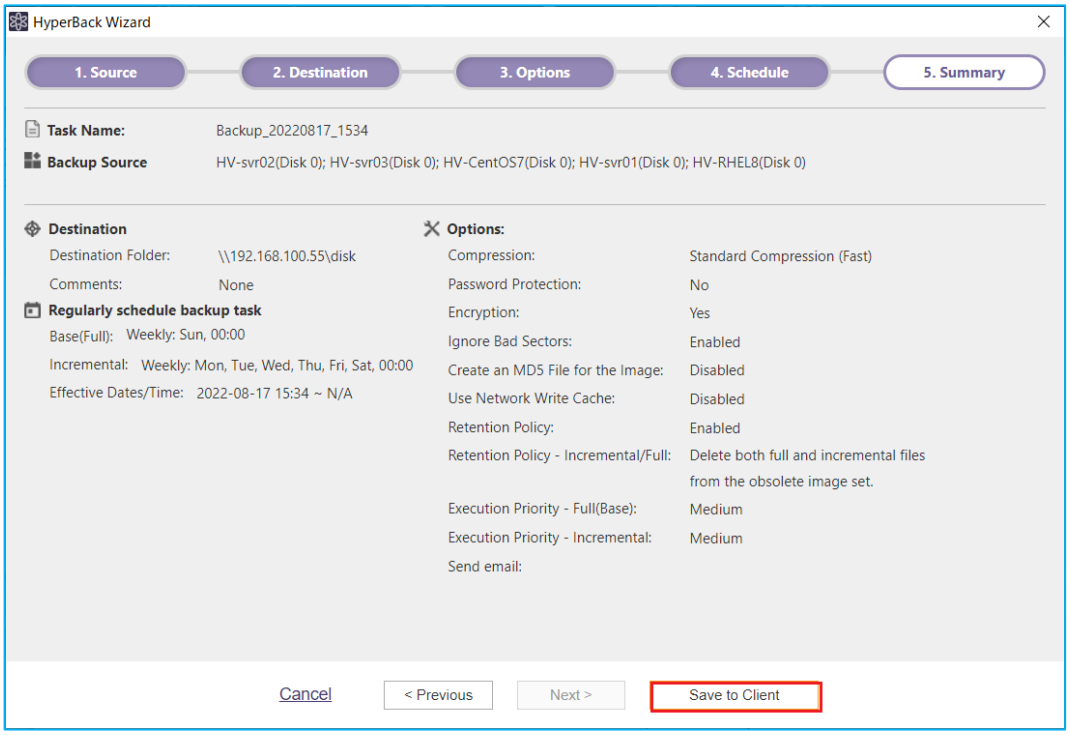
12. On the **[Options:]** screen, you can configure settings for retention policy and notifications. In this example, **[Enabling Retention Policy]** is selected and the default value of"3" is entered for **[Number of image sets to retain]**. **[Delete both full and incremental]** option is selected. You can adjust the desired level of task **[Execution Priority]** by using the slider.
    After configuring the settings, click **[Next].**



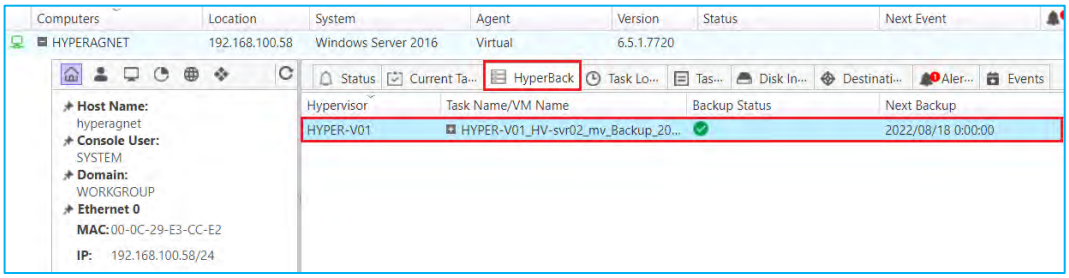
13. You can configure the schedule settings for base/incremental backups in the same manner as agent-based backup. In this example, a base (full) backup is scheduled on every Sunday at 0:00 a.m. and an incremental backup from Monday to Saturday at 0:00 a.m. After configuring the settings, click **[Next].**



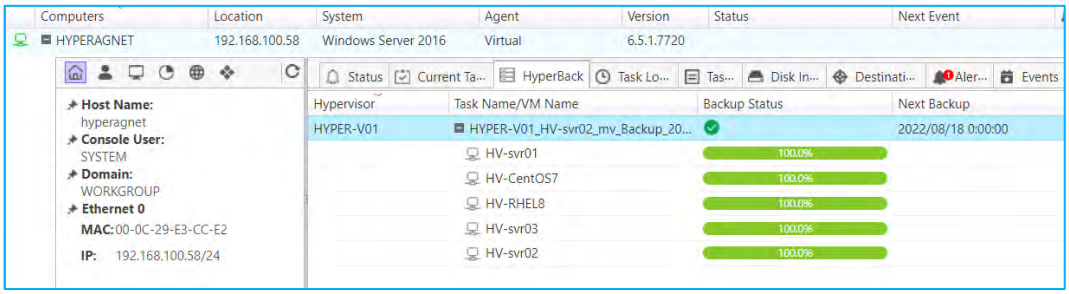
14. Review the settings on the **[Summary]** window. Click **[Save to Client]** to save the agentless backup settings to the managed computer. Close the dialog.



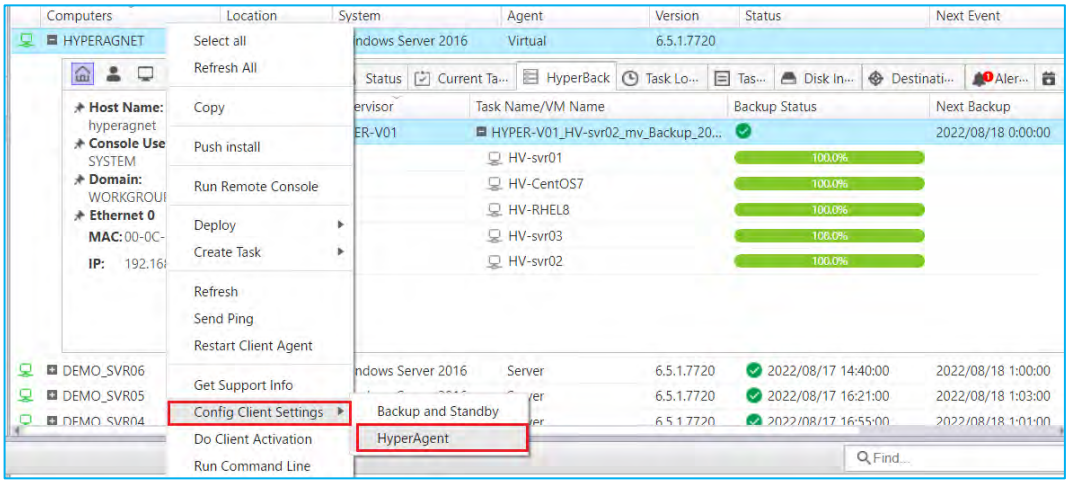
15. The newly created task is visible in **[HyperBack]** tab in the computer list.



16. You can monitor the status of the agentless backup task.

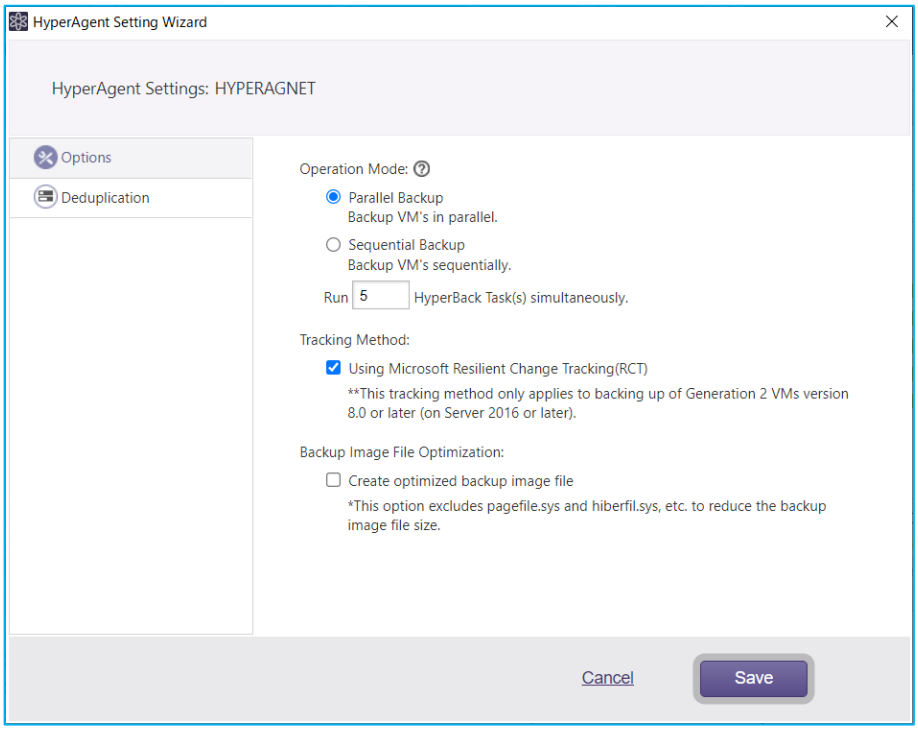


17. To configure additional HyperAgent settings, right-click on a client computer and select **[Config Client Settings]** -- **[HyperAgent]** in the context menu.



18. You can select one of two operating modes, **[Parallel Backup]** or **[Sequential Backup]**. When **[Parallel Backup]** is selected, you can specify the number of HyperBack tasks **[Run xx HyperBack Task(s) simultaneously]** to run simultaneously. When you have limited machine or network resources on the HyperAgent computer, it is recommend to limit the number of Hyperback task to one at a time using **[Sequential Backup]**.

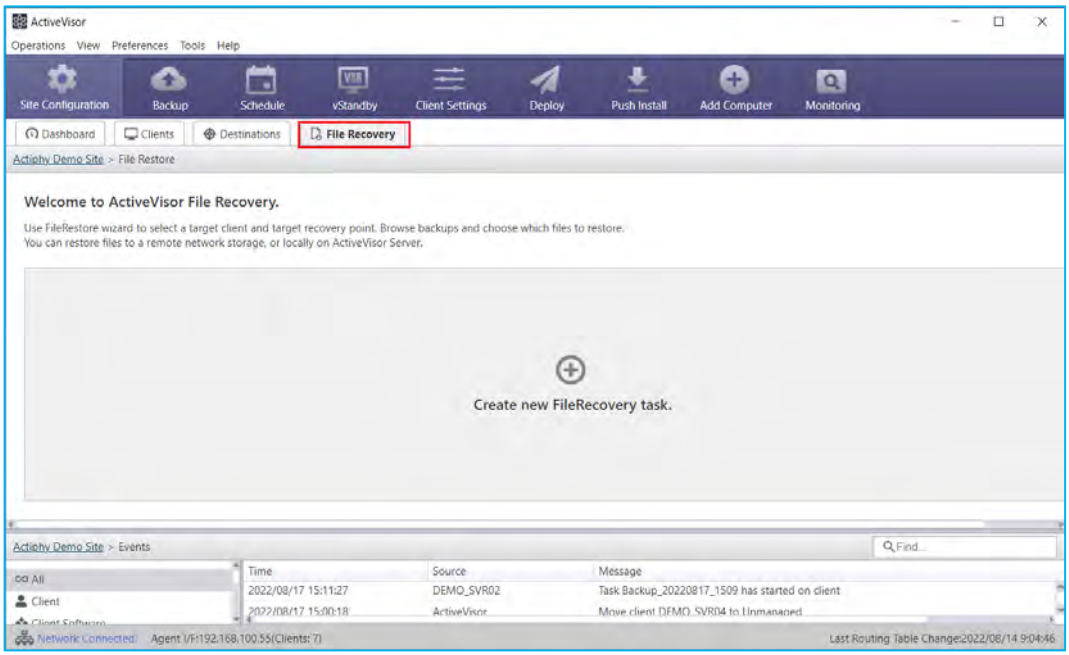
    [Tracking Method] specifies the method of creating incremental backups for virtual machines. When backing up Windows Server 2016 or later second generation virtual machines, HyperBack uses Windows standard RCT (Resilient Change Tracking). For all other systems, HyperBack uses Actiphy's proprietary VM tracking technology.



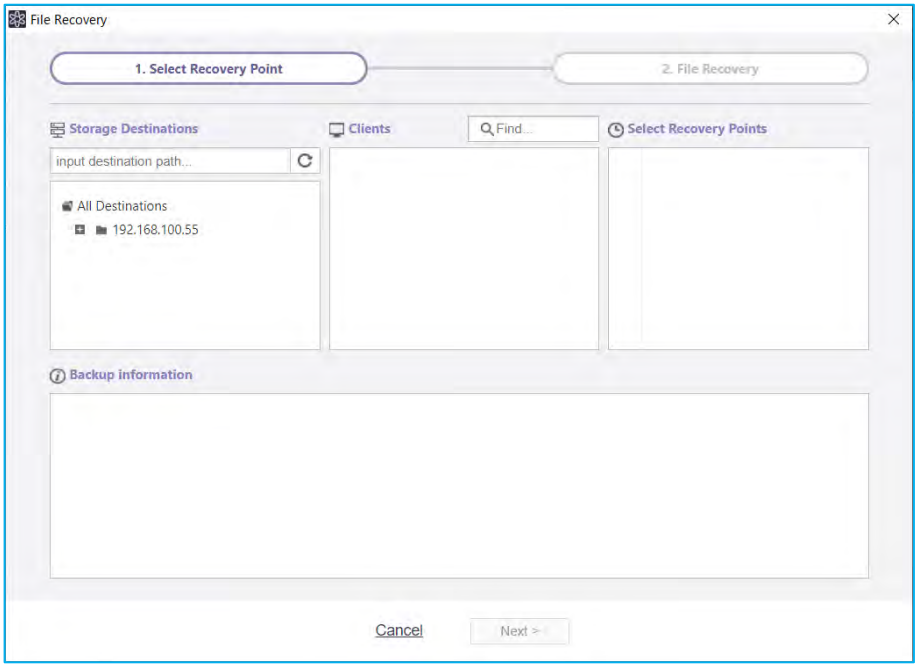
6.2. ActiveVisor's File Recovery Feature

Using file recovery you can restore files or folders from recovery points in client backup files. Restored items can be saved to a local file system or network shared folder.

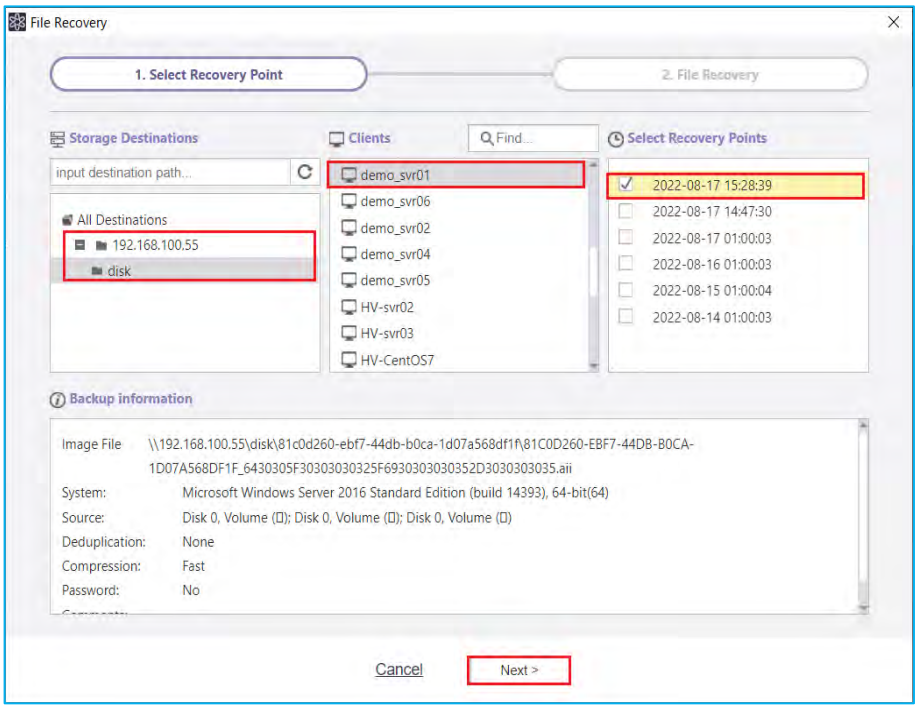
1. The **[File Recovery]** tab is displayed as follows.



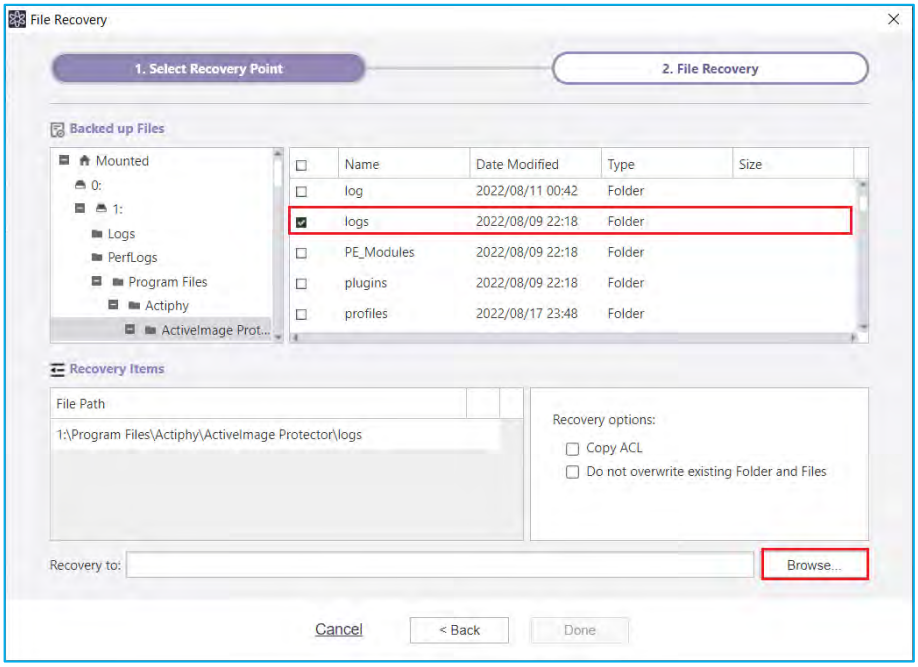
2. To begin click "+ Create new FileRecovery task" button in the center of the screen the will display the "File Recovery" wizard.



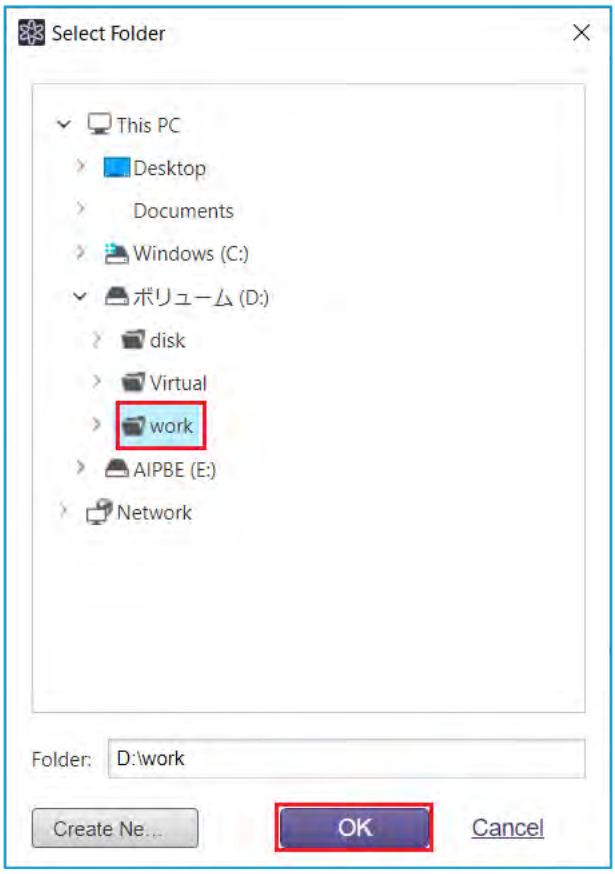
3. Storage destinations previously used in ActiveVisor are automatically discovered and displayed on the screen. After selecting a storage destination, specify a client backup to restore from and select a recovery point. Information for the recovery point is displayed in the “Backup Information” area on the screen.
   Click **[Next]** to mount the recover point.



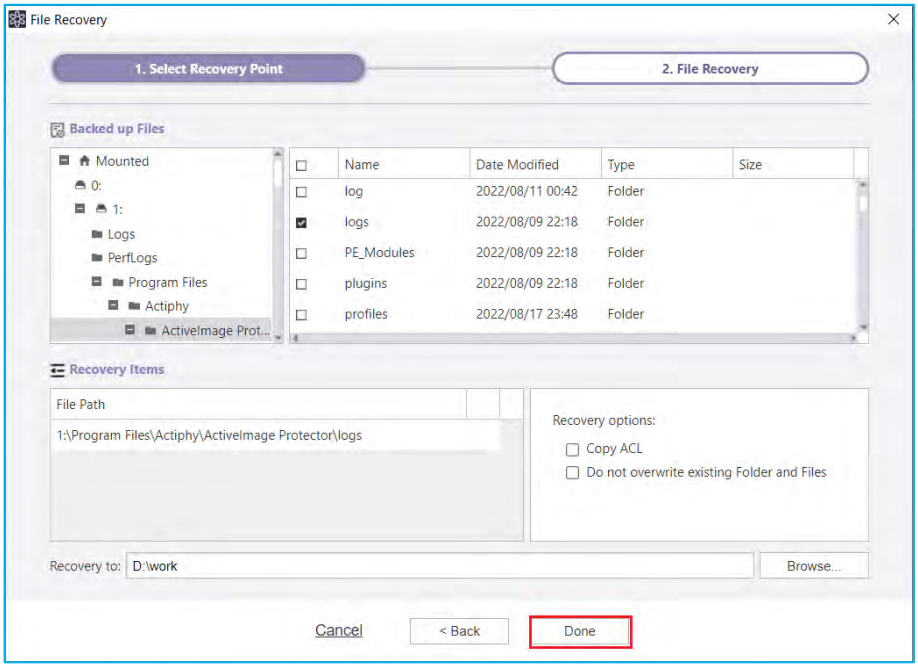
4. The backup is mounted on the local files system (the process is similar to ActiveImage Protector ‘s file recovery feature). Select files folder to restore and specify a recovery target for **[Recovery to:]**.
   Clicking **[Browse…]** will open a file browser or you can enter a path directly. You can also configure any needed items in **[Option].**



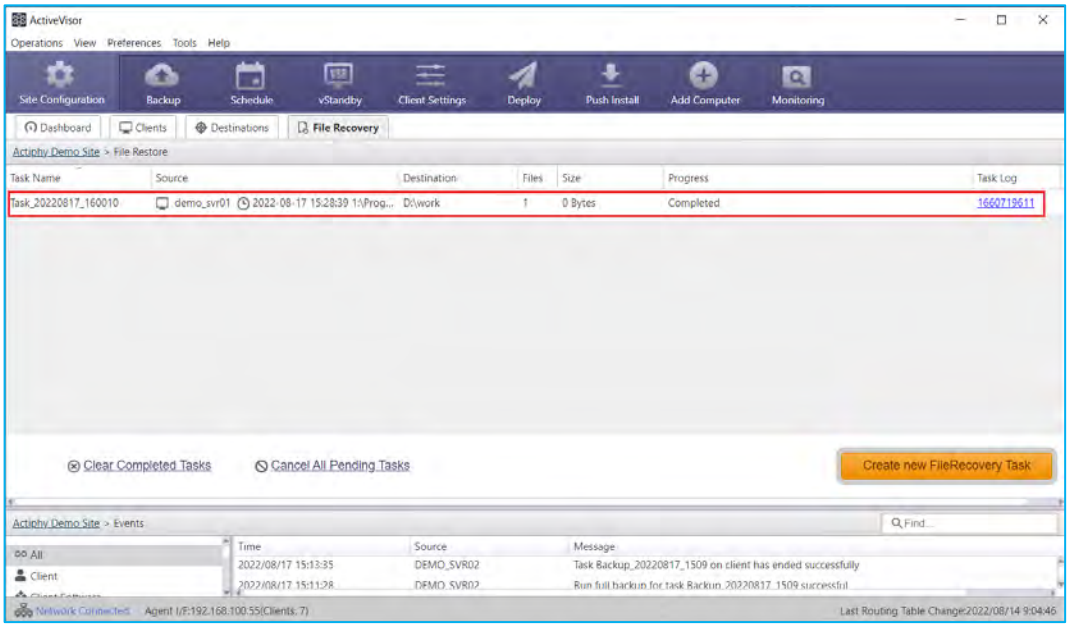
5. In this example, ActiveVisor ‘s local volume “D:¥work” is selected. Click **[OK].**



6. Click **[Done]** to start the recovery task. The restore task execution runs on ActiveVisor server, the remote ActiveImage Protector agent is not used in the process.



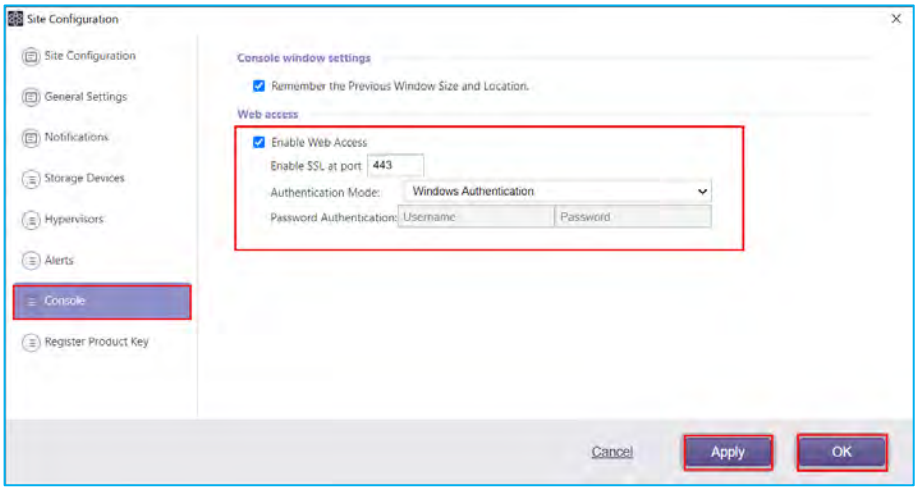
7. When recovery process completes, the following window is displayed.



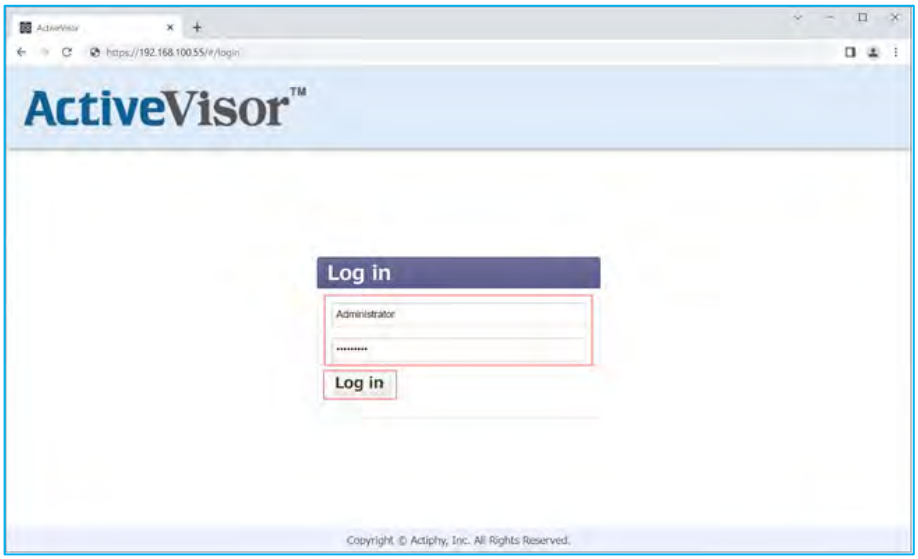
6.3. ActiveVisor's Web Console

Administrators can access ActiveVisor from any location using a browser-based console. With the browser console you can monitor managed computers, edit backup agents and change schedule settings, etc., Google Chrome, Microsoft Edge, Apple Safari are supported.

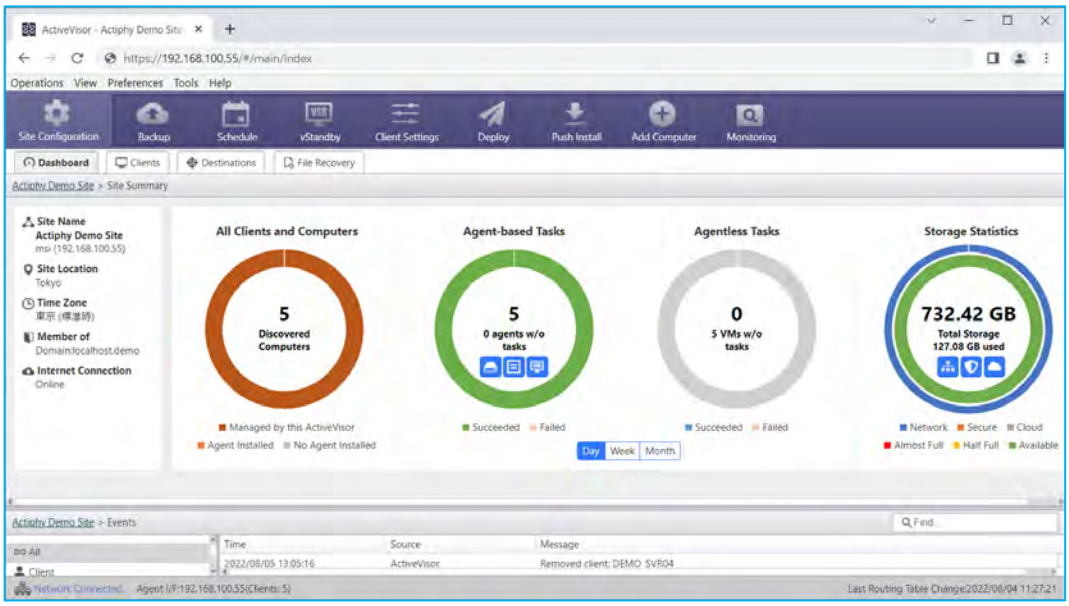
1. To start using the browser-based console, go to **[Site Configuration]** -- **[Console]** -- **[Web Access]** and enable **[Enable Web Access]** option. By default "443" is set for **[Enable SSL at port]**, "Windows Authentication" for **[Authentication Mode].** After configuring the "Web Access" options, click **[OK].**



2. In the example below, in Edge we have enter the IP address of the running ActiveVisor agent, "192.168.100.55". The following **[Log In]** screen is displayed.
   ActiveVisor's "Authentication Mode" is set to "Windows Authentication", enter the Windows authentication for this ActiveVisor agent, for example, "Administrator" and the password. Click **[Login].**



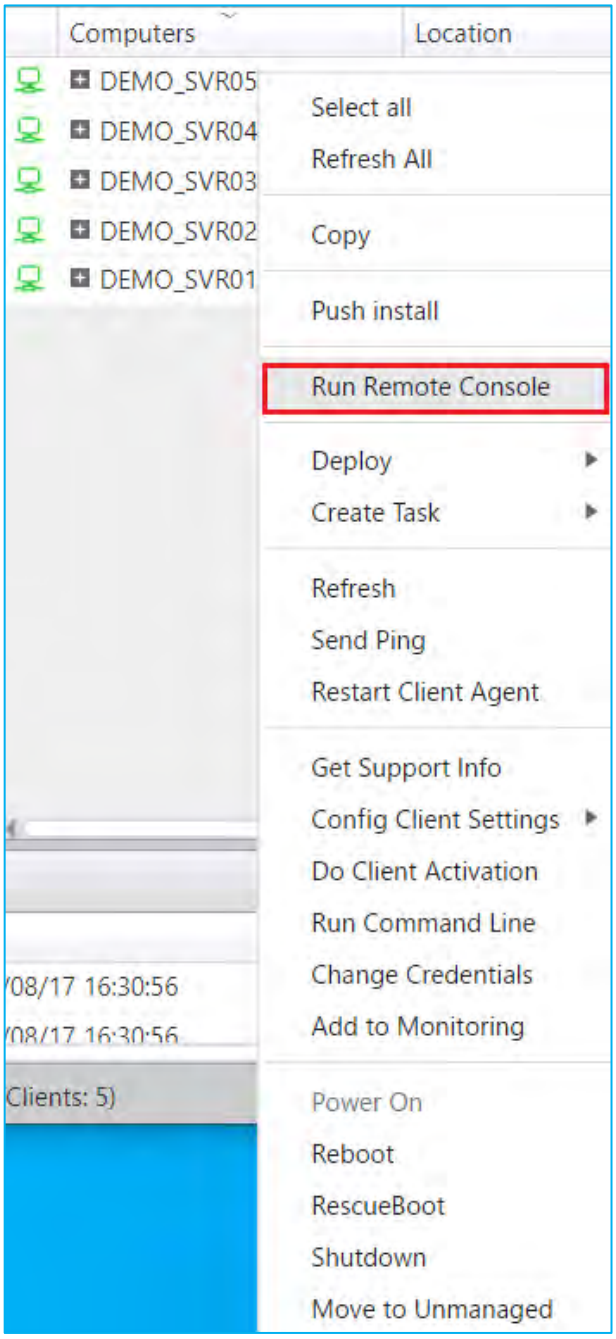
3. After successfully authenticating ActiveVisor's console window is displayed as depicted below. The web-based console offers more flexibility with system management, monitoring and administrating managed computers.



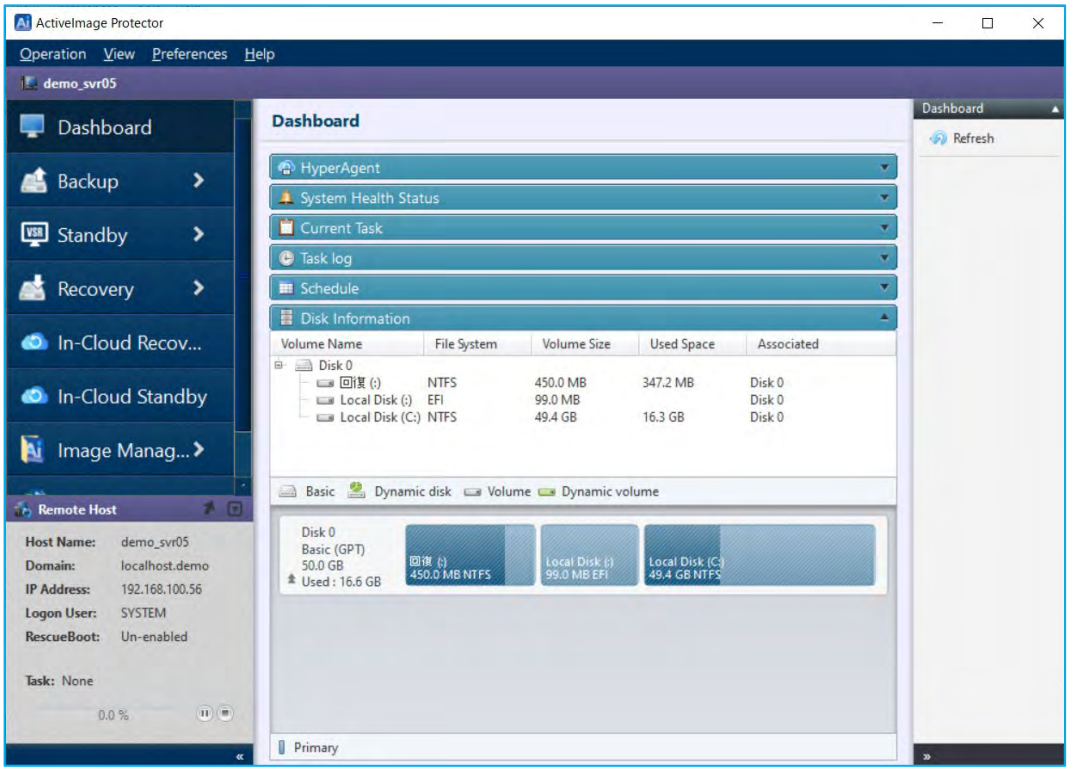
6.4. Access ActiveImage Protector agents from ActiveVisor's Remote Management Console

ActiveVisor can access ActiveImage Protector agents and perform a variety of operations. The following is a description about how to access ActiveImage Protector agents from ActiveVisor's remote management console.

1. From ActiveVisor's computer list, right-click on a managed computer and select **[Run Remote Console]** in the context menu.



2. The remote management console is launched, enabling you to perform most of the same operations as the local management console.

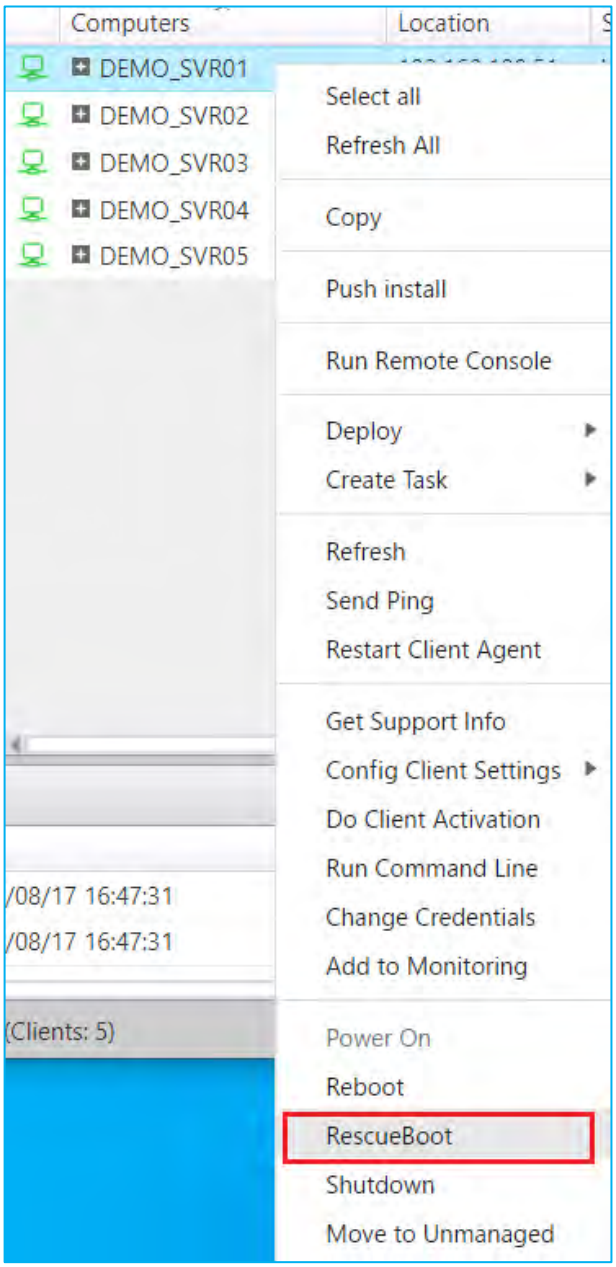


6.5. Remotely operate managed computers booted from RescueBoot in ActiveVisor

ActiveVisor enables to boot up managed computers system via RescueBoot for system recovery without booting from system recovery media. The following is a description about how to access and remotely operate managed computers in the RescueBoot boot environment from within ActiveVisor.

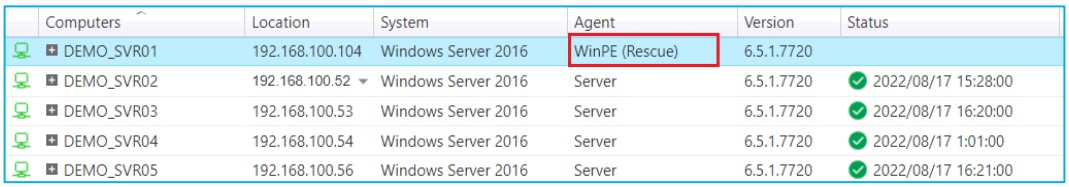
***Before remotely operating a managed computer in RescueBoot boot, please make sure the managed computer's operating system is up and running.**

1. Right-click on a managed computer in ActiveVisor's computer list, and select **[RescureBoot]** in the context menu.



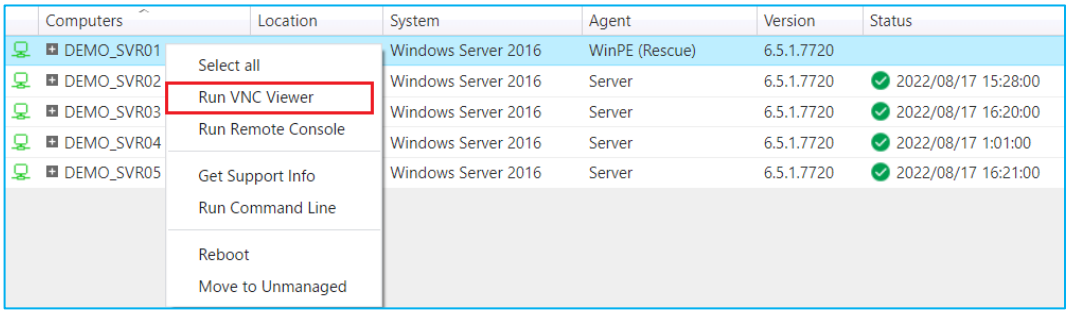
2. Wait for RescueBoot to boot . . .

   After the environment boots, “WinPE (Rescue)” is indicated on the **[Agent]** column.

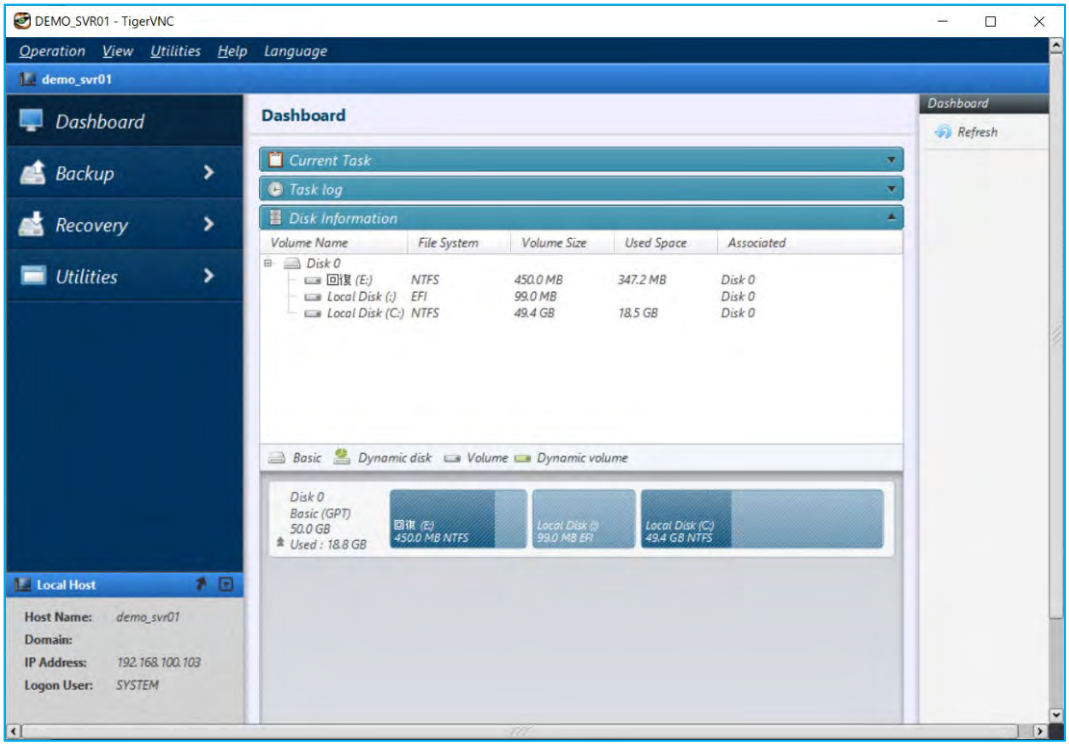


Computers	Location	System	Agent	Version	Status
DEMO_SVR01	192.168.100.104	Windows Server 2016	WinPE (Rescue)	6.5.1.7720	
DEMO_SVR02	192.168.100.52	Windows Server 2016	Server	6.5.1.7720	2022/08/17 15:28:00
DEMO_SVR03	192.168.100.53	Windows Server 2016	Server	6.5.1.7720	2022/08/17 16:20:00
DEMO_SVR04	192.168.100.54	Windows Server 2016	Server	6.5.1.7720	2022/08/17 1:01:00
DEMO_SVR05	192.168.100.56	Windows Server 2016	Server	6.5.1.7720	2022/08/17 16:21:00

3. Right-click on the managed computer and select **[Run VNC Viewer]** in the context menu.



4. A connection to the boot environment on managed computer is established. You can remotely access and operate the AIP agent in boot environment.

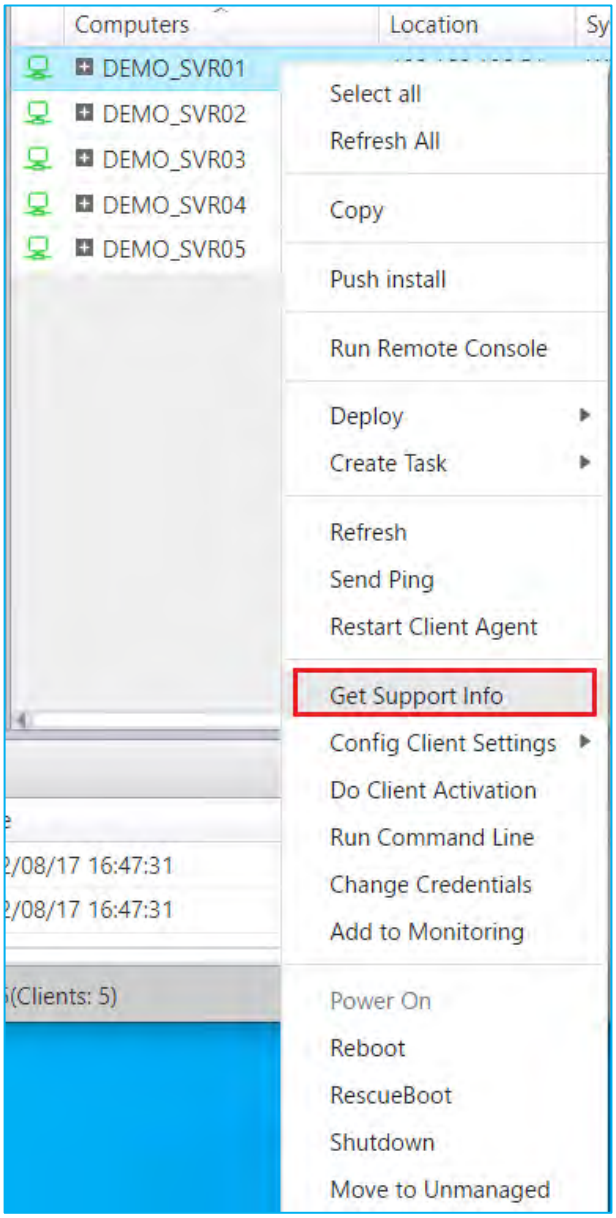


7. APPENDIX

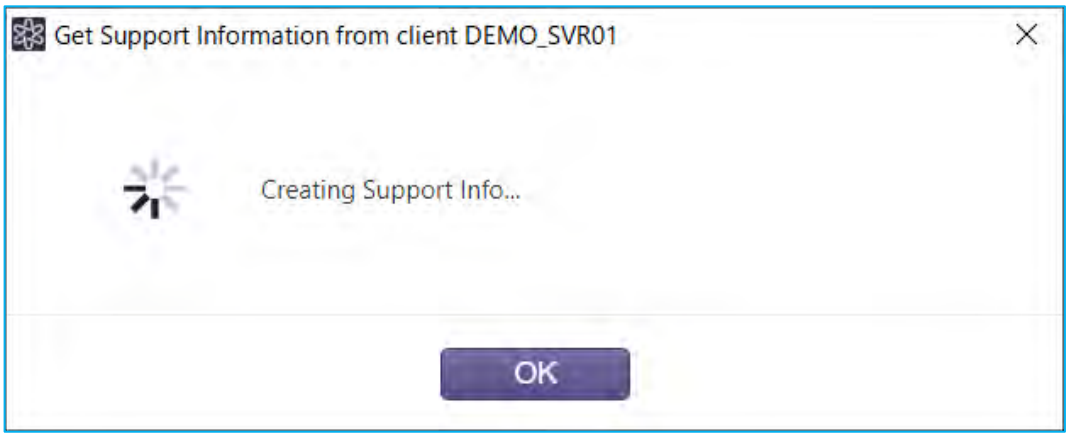
Generating Support Information File

When contacting technical support you may be asked to provide support information for certain clients. From the Activevisor console you can create support information for managed clients, even for clients that have an agent only install. The support information file is generated as ZIP file in ActiveVisor's local folder.

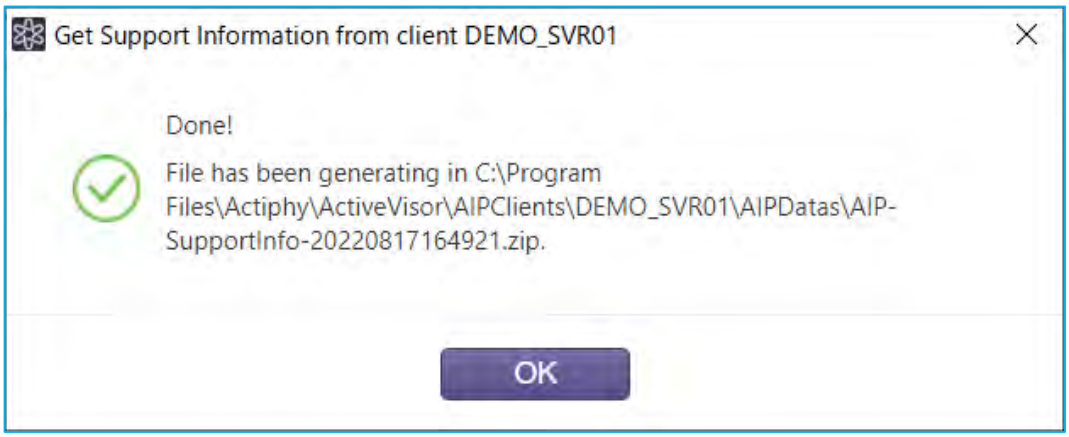
1. Right-click on the managed computer in ActiveVisor's client list and select **[Get Support Info]** in the context menu.



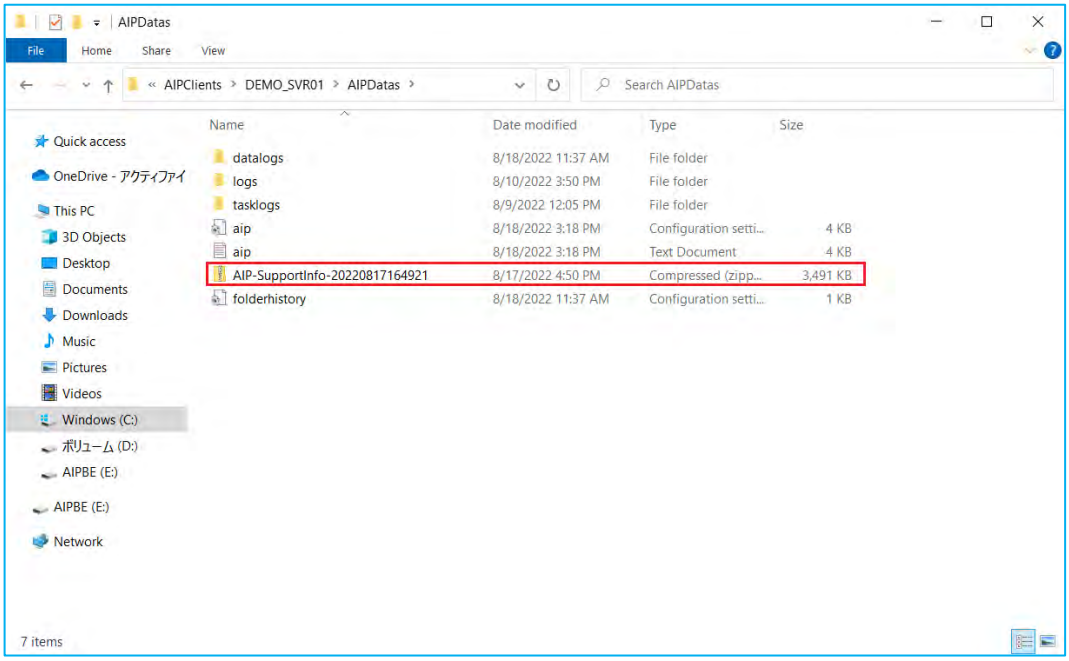
2. The dialog **[Get Support Information from client …]** is displayed as follows.



3. When the support information generation has completed, the path the support ZIP file is indicated as below.



4. When contacting support please provide the support file if requested.



8. Reference

- Actiphy's Web site:

  Actiphy's Web site provides access to comprehensive information including the product information, related documents, technical support, updates, etc.

  https://www.actiphy.com

- ActiveImage Protector FAQ

  Support information is accessible at the following FAQ web site.

  https://enkb.actiphy.com/

- For your inquiries about ActiveVisor, please contact:
  Global Sales Dept., Actiphy Inc.
  E-mail: global-sales@actiphy.co.jp
  (TEL) +81-3-5256-0877 (FAX) +81-3-5256-0878