DATASHEET

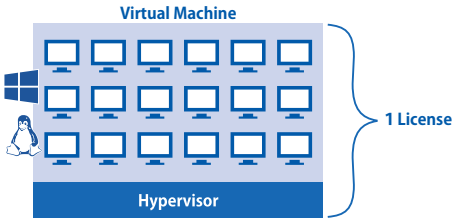
ActiveImage™ 2022 PROTECTOR Virtual

A Data and System Protection Solution supporting agentless backups of Virtual Environments

ActiveImage Protector™ Virtual is an image based backup and recovery solution optimized for virtual environments. ActiveImage Protector™ backs up entire virtual machines hosted on Windows and Linux servers' hypervisors. The backup image includes the system OS with all your applications and data and is performed by an agent-based or agentless backup. When an emergency arises, a wizard-driven interface guides you through the full system recovery. Any backup image can be directly booted as a virtual machine. ActiveImage Protector™ integrates a virtual standby availability solution to replicate your physical or virtual machines directly to a VMware ESX / ESXi or Hyper-V host and keeps the standby machine updated with scheduled incremental snapshots.

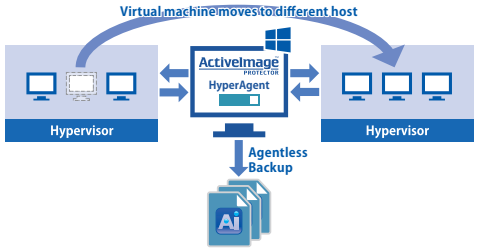
Cost-effective Virtual Environment License

- One license is applied to one virtual environment host
- No restrictions on the number of CPU sockets or cores
- Agentless backup feature is supported



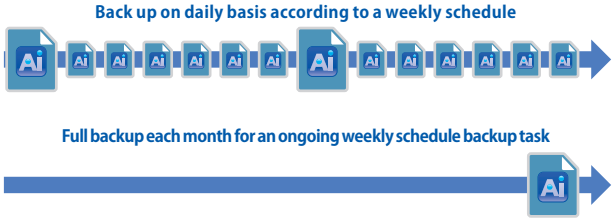
HA or HCI configured virtual environment is supported

- Backup operation continues even when VM moves to a different host
- No installation of agent reduces man-hours required for the product deployment
- No additional load from agents required on virtual machines



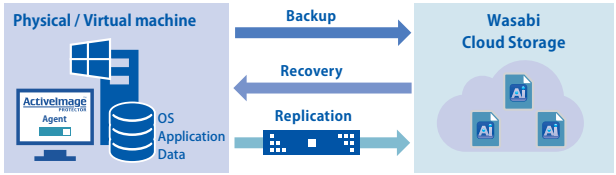
Flexible Scheduled Backup

- Backup tasks can be automatically executed according to the one-time, weekly, monthly or on a specific day of a week
- Multiple schedules can be defined for individual backup tasks (Multi-Scheduling Feature)
- Automatic backup when a machine is shutting down



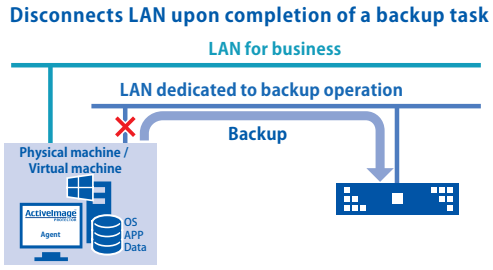
Cloud Storage Wasabi with object lock is supported

- A bucket enabled with object lock is supported as a storage destination
- The same functions are provided for local NAS
- Supported as offsite replication target



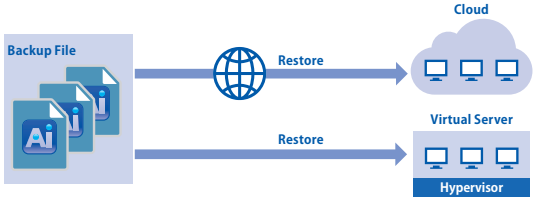
Safely protect backup files

- Disconnect access to a backup storage drives after backups complete (Destination Isolation Option)
- Replicate backup files to remote site (Offsite Replication)
- Encryption of Backup Images



Flexible restore feature

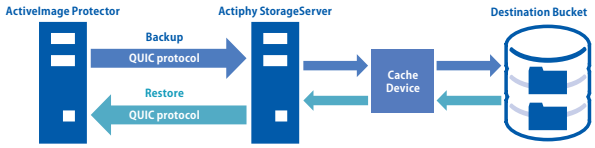
- Restore a disk, a volume, or a single file or folder.
- Restore to a virtual machine on a different hypervisor
- Restore a backup image to a virtual machine and immediately boot up the virtual machine (HyperRecovery)



New Features from Update (released on Sept. 7, 2023)

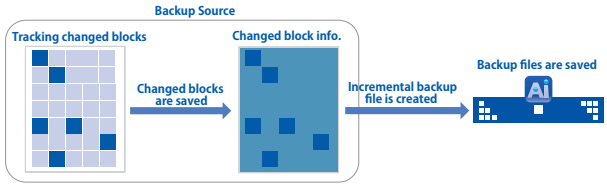
Actiphy StorageServer™

Actiphy StorageServer™ option enables to build secured backup storage for exclusive use with ActiveImage Protector™. Actiphy StorageServer™, as an independent destination storage for backup, protects the backup image files from the attack of a ransomware. The use of new QUIC protocol for data transmission enables to transfer data more safely with high reliability and ensures the security for the communication path. Actiphy StorageServer™ is engineered to take advantage of cache device in storage server, delivering faster data transfer speed than the destination storage device, that secures stable backup process and speed.



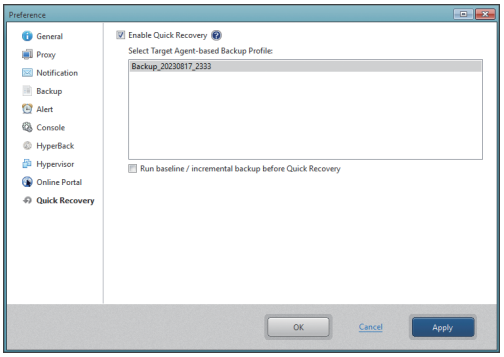
New Tracking Driver

New Tracking Driver is provided to monitor disk I/O and tracking the changes made from the last backup. The changes are saved in an incremental backup file, saving backup process time. The use of the new Tracking Driver suppresses a slowdown of backup processing speed caused by the increasing number of incremental backup files. You can select change tracking mode not to use a tracking driver.

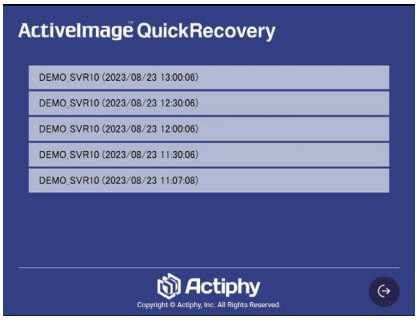


QuickRecovery

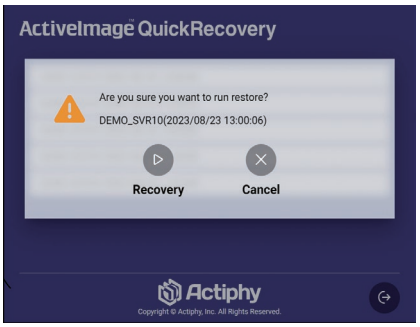
When booting up the system, QuickRecovery automatically starts recovery environment without the need for boot environment media. Boot up the recovery environment and select a specific restore point from the backup for immediately recovery. When restoring the system failed due to a software problem, recovery procedures complete on the restore target machine.



QuickRecovery Boot Settings



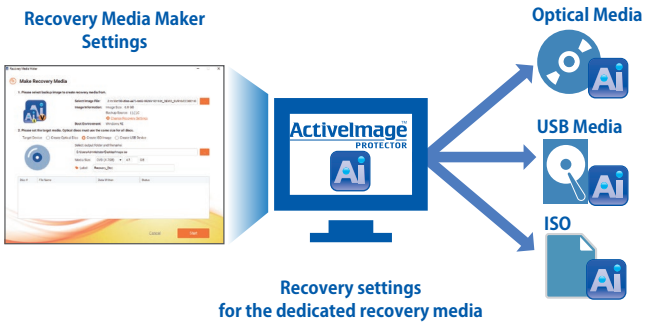
Select Recovery Point



Start Restore

Recovery Media Maker

Recovery Media Maker feature enables to create bootable recovery media with the backup source machine's image embedded for an ideal disaster recovery (DR) solution. Recovery can be performed on dedicated recovery media alone, allowing recovery work to be performed even when the network is not available or when USB media cannot be brought to the site.



Recovery settings for the dedicated recovery media

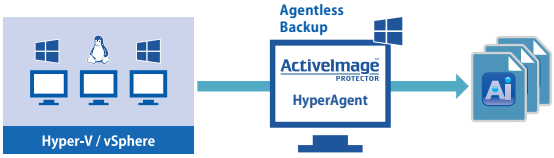
Support for VMware First Class Disk (FCD)

Direct backup and recovery of VMware's FCD formatted disks is supported.

Backup Features

Agentless backup feature (HyperAgent™)

Traditional agent-based backup of virtual machines required installation of ActiveImage Protector™. ActiveImage Protector™ Virtual now provides HyperAgent™ (HyperBack™), agentless backup feature, enabling to select and back up a virtual machine configured on VMware vSphere or Microsoft Hyper-V. HyperAgent™ can be installed on backup source host or destination storage, supporting a variety of system configuration.



In HCI infrastructure, virtual server is automatically discovered

HyperAgent™, agentless backup feature, detects virtual servers on migration target host registered under vCenter, in HCI infrastructure, as backup source for regularly scheduled backup operation, which reduces IT engineers' workload.

Traditional agent-based backup

Agent-based backup feature supports consolidated backup operation in the same manner as on physical server. Agent-based backup feature supports backup of virtual machines configured on a variety of hypervisors (VMware vSphere, Microsoft Hyper-V, Citrix Hyper-V, Proxmox VE, Nutanix Acropolis, etc.)

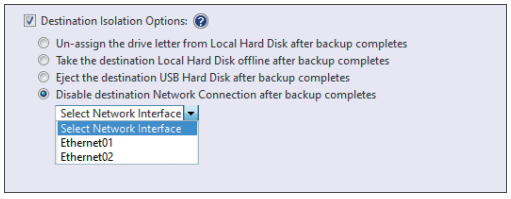
* For further details about the supported hypervisors, please contact us.

Upon completion of backup task, protect the destination (Destination Isolation Option)

Our ImageIsolate™ technology reduces potential malware or ransomware attacks to backup files by disconnecting access to backup storage drives over a network after backups complete. Four options are provided.

- Un-assign the drive letter from the local hard disk after completing the backup
- Take the destination local hard disk offline after completing the backup
- Eject the destination USB hard disk after completing the backup
- Disable the destination network connection after completing the backup

* After the destination USB HDD / SSD drive is ejected, it's necessary to manually plug in the drive and set online before starting the next task.

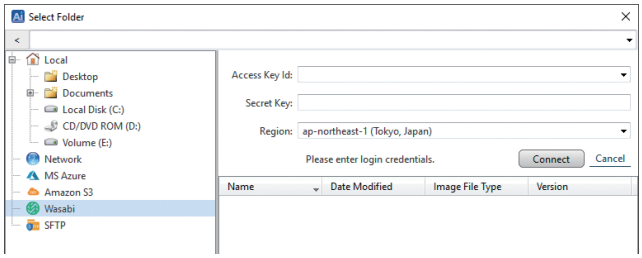


A variety of Storage Media are supported

Save your backups to any available storage location, including local HDD, USB-connected storage, NAS, SAN (fibre channel), SFTP server, LTO or RDX tape, and cloud storage services (Wasabi, Amazon S3, Azure Storage, S3-compatible object storage), etc., using a variety of system configuration and backup policies

Wasabi with object lock is supported

A bucket enabled with object lock in Wasabi Hot Cloud Storage is supported as a storage destination. Source backup images in Wasabi Hot Cloud Storage are supported for restore in the same manner as the backup images in NAS. Saving your large volume backup data in cost-effective Wasabi Hot cloud storage secures your backups as they are isolated from a potential cyber attack. A backup from Wasabi Hot cloud storage can be directly restored to a virtual machine on a different site allowing uninterrupted VM operation.



LTO Tape Support suited for offline storage

The Tape Manager feature in this update provides enhanced operation of the tape pool and library. Allows movement of tapes within LTO tape library. Rescans tapes in the library, etc. When backups are directed to LTO tape with insufficient available space, the LTO tape is replaced with another to continue backup operation. Should a disaster occur, a backup from the LTO tape is used to restore the system.

Back up VMware vSphere ESXi host(Cold Imaging)

Start up your computer from ActiveImage Protector™'s Linux-based bootable media to create a backup image of a clean static system volume of VMware vSphere ESXi host in shut-down state, which is convenient to use for bare-metal recovery.

Back up multiple virtual machines in one image file

ActiveImage Protector™ backs up multiple virtual machines in one image file. Inline Data Deduplication Compression (IDDC) feature eliminates duplicate data, resulting in a significant reduction in backup storage requirements.

Flexible Multi-Scheduling

Backup tasks can be automatically executed according to the onetime, weekly or monthly schedule, or a specific day of a week in a specific month. Schedule baseline and recurring incremental backup tasks to run subsequently.

Multi-Scheduling Feature

Multiple schedules can be defined for individual backup tasks. For example, you can create a new full backup each month for an ongoing Weekly Schedule backup task.

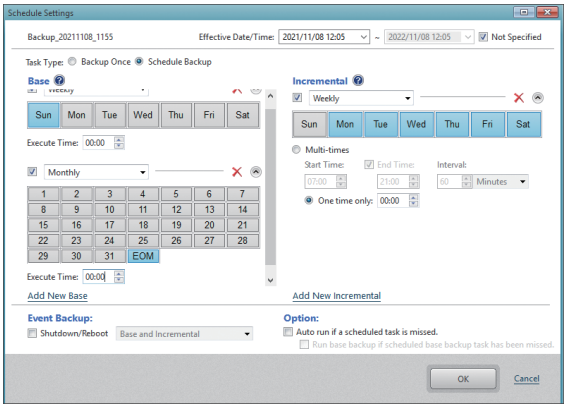
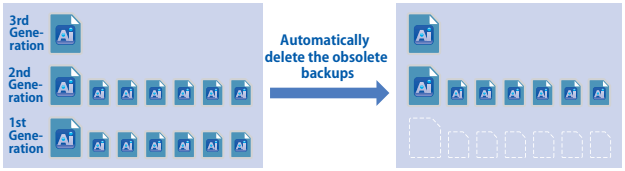


Image Retention Policy

The Image Retention Policy feature can be configured to automatically delete the obsolete backup image set when the number of backup image sets reaches the preset limitation and reduces the storage requirements.



Automatic backup at shutdown

ActiveImage Protector™ automatic backup when a machine is shut down or rebooted. When rebooting the system after a regularly scheduled system maintenance or in the event of an unexpected system shut down, a full baseline backup image is created before or after startup.

Run scripts after scheduled backup

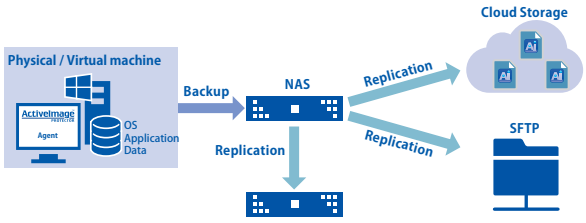
Scripts can be implemented to run before, after, or during the moment snapshots are taken or after the backup image has been created. An example would be to execute a user-specified script to purge database cache before taking a snapshot and then resume the database after taking a snapshot (before starting a backup task), etc. Scripts can be implemented for base and incremental backup tasks.

Post-backup Process

Run BootCheck™, Replication and Consolidation tasks upon completion of a backup or at a specified time.

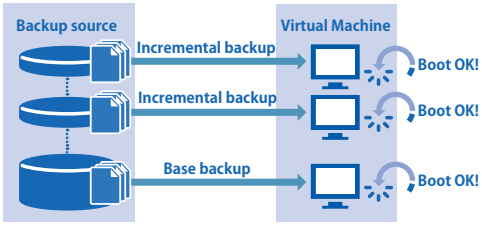
Distributed Backup Storage (Offsite Replication)

Perform a post backup Replication of your backup image files to an offsite storage share that includes local disk, network shared folder, FTP, FTPS, SFTP, WebDAV, Amazon S3, Azure Storage, Wasabi, OneDrive, Google Drive, Dropbox. Distribution of backup files increase the security level.



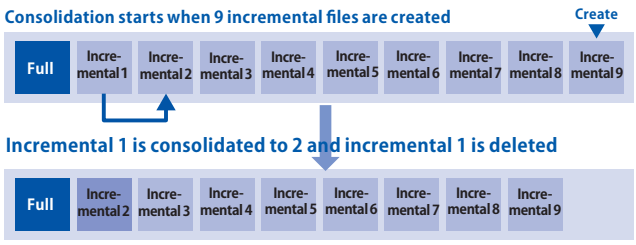
Automated backup "bootability" testing (BootCheck™)

BootCheck™ provides confidence that your backup images are bootable on a local or remote Hyper-V host. BootCheck™ boots up a virtual machine directly from a backup image file to confirm bootability. BootCheck™ can be run manually from the console at any time.



Consolidation of Incremental Backup Files

Regularly scheduled recurring incremental backup tasks may result in an increase in the number of backup files and a decrease in the performance of backup and restore processes. The Consolidation feature consolidates an uninterrupted series of incremental backup image files to one file according to a predefined schedule. For example, if the consolidation settings are configured to retain 7 incremental backup files and when 9 incremental backup tasks complete, the 1st and the 2nd most obsolete incremental files are consolidated to one file. As a result, 7 incremental files remain.



Restore Features

Fast and full-state recovery from a backup file

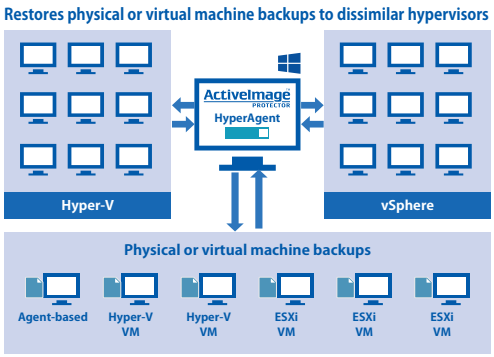
In the event of a hard disk failure, ActiveImage Protector™ can quickly restore a backup to the original machine, a different on-premise physical server or a virtual machine, bypassing the time-consuming process of reinstalling the OS, applications, configuration settings, reapplication of drivers, and data recovery. The built-in wizards guide you through every step to ensure recovery from the backup image file reducing the IT engineers' workload.

File Recovery feature

In the event of a system failure, you may only need specific files to restore in order to maintain continuity. The File Recovery feature optionally provides recovery of single files or folders from a backup image. All stream information and access rights of the individual files are inclusively restored.

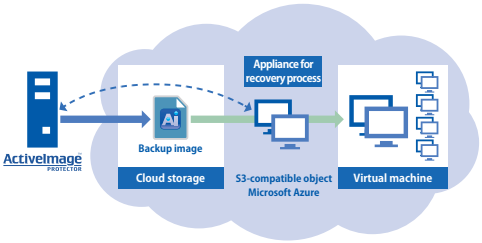
Restore to virtual environment (HyperRecovery™)

HyperRecovery™ restores a backup image to a virtual machine configured on VMware vSphere or Microsoft Hyper-V. Otherwise, you can only create a virtual disk.



In-Cloud Recovery™

Restore a backup in cloud storage （Amazon S3, Azure Storage, S3-compatible object storage) can be restored to a virtual machine on the cloud (AWS, Azure). The data transfer within the same region when restoring a backup image to a virtual machine on the same cloud does not incur additional costs.



RescueBoot

ActiveImage Protector™ includes RescueBoot. A feature when enabled, starts up the Actiphy Boot Environment in the event of emergency. The boot environment is booted directly from the internal disk, so that system administrator can restore the failed system without the use of external device.

VNC on RescueBoot

A VNC viewer is now provided to remotely operate the RescueBoot boot environment. System administrators can now restore the failed system in RescueBoot via VNC instead of the local machine.

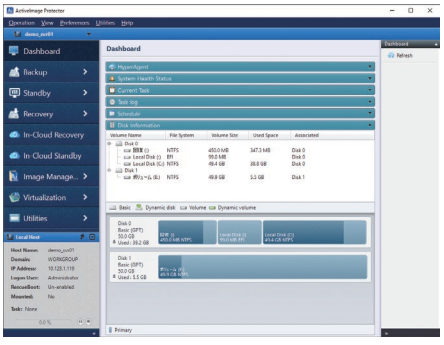
Restore to physical machines with different hardware configuration (A.I.R.)

A.I.R (Architecture Intelligent Restore) included in Actiphy boot environment (Windows PE-based boot environment) is designed to install compatible RAID storage controller drivers after the recovery process and ensure the start up of the restored OS .

Management Console

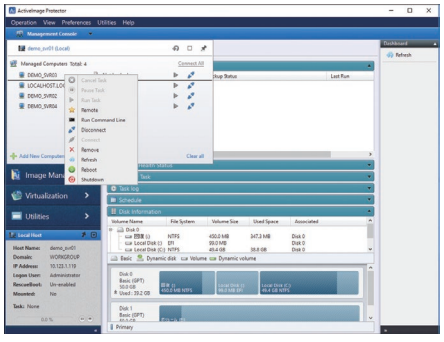
GUI provides tools for efficient operations

ActiveImage Protector™'s GUI provides dashboard window, displays real time monitoring of the status of tasks, logs, schedules, and disk information. Backup and Restore wizards windows make the software operation more intuitive.



Client management console

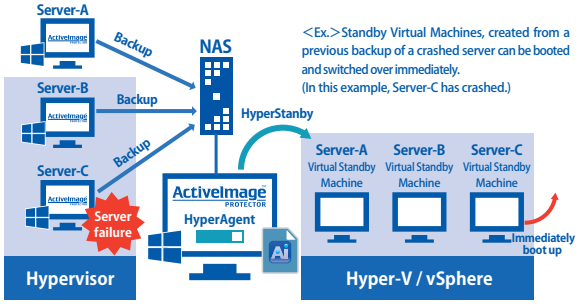
You can monitor the status of remote ActiveImage Protector™ agents over the network. Use the Client management console to monitor the status of backup tasks on multiple agents over network and schedule backup tasks.



Instant boot (System Redundancy)

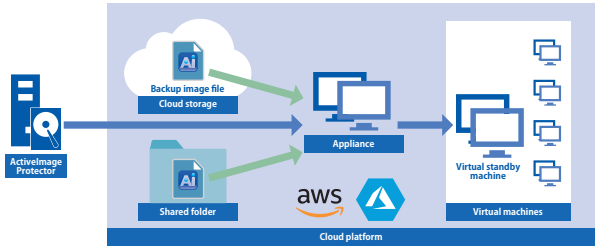
Create standby virtual machine from a backup image (HyperStandby™)

Uses HyperStandby™to create and maintain a standby virtual machine from backup images to Microsoft Hyper-V or VMware vSphere host, up-dating boot points synchronized with scheduled incremental snapshots. When a disaster strikes, the standby virtual machine (SVM) can be started up in as little as two minutes.



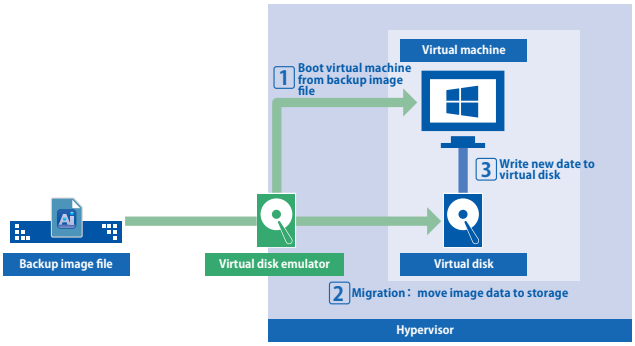
Replicate virtual standby machine from backup on cloud (In-Cloud Standby™)

In-Cloud Standby™ creates snapshots in cloud storage from backup images saved in a storage accessible from the cloud based on a predefined schedule. In the event of emergency, a volume created from the snapshot is attached to the virtual machine which is instantly started to resume the operation on cloud.



HyperRecovery LIVE!

HyperRecovery LIVE! boots up the virtual machine directly from a backup image file, migrates the live virtual machine to the restore target virtual disk in background bypassing the restore process providing uninterrupted VM operation.



Migration to virtual environment

Virtual conversion utility

A virtual conversion utility is provided to convert a backup image file or physical disk to virtual disk bootable as virtual machine. Conversion to the latest virtual disk format, VMware vSphere VMDK, Microsoft Hyper-V VHD / VHDX is supported.

Conversion from a backup image file to virtual disk and attach to virtual machine

The P2V conversion supports Microsoft Hyper-V, VMware vSphere as the target host to create the virtual machine attached with a virtual disk converted from a backup image file providing an immediate boot up of the virtual machine.

Conversion from a hard isk to virtual machine

The P2V conversion feature supports direct conversion from a hard disk to a Microsoft Hyper-V, VMware vSphere virtual disk format to create a virtual machine attached with the converted virtual disk. This bypasses P2V conversion from an image file reducing process time.

Virtualization Adapter

The driver for virtual machine can be injected into the current image file, which is saved as the ActiveImage Protector™differential file (.aix). The differential file may be restored as a virtual machine.

P2V (physical to virtual) disk in local environment is supported on Windows PE

Conversion from physical to virtual disk (virtual disk only) is supported in Windows PE-based boot environment.

Management of Backup Files

Image Explorer

Windows Explorer opens a backup file providing direct access to restore individual files or folders from a backup file.

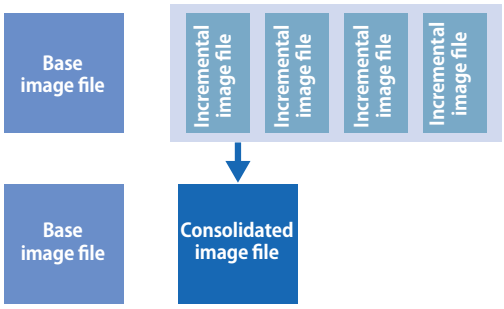
Image Mount

ActiveImage Protector™ can quickly mount an image file as a drive, allowing the restore of any files or folders from the image file. When image file is mounted as a writable drive, the changes made on the drive will be saved as a differential file.

Consolidate backup files

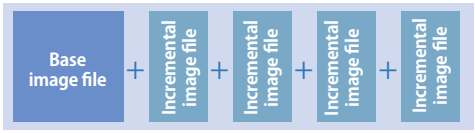
Regularly scheduled recurring incremental backup tasks create a growing and sometimes unmanageable number of incremental files. The Consolidation feature consolidates an uninterrupted series of incremental backup image files to a single file.

* When running scheduled consolidation tasks, please configure the settings for Post-backup Consolidation.



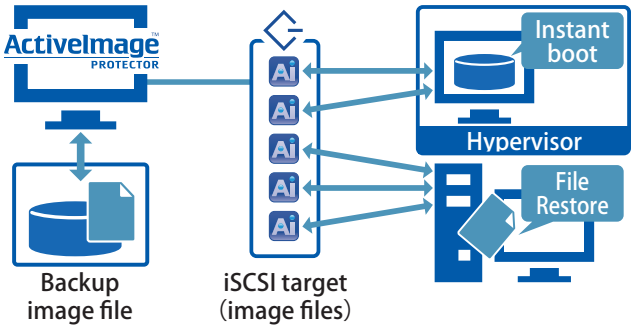
Archive Backup Files

Use the archive feature to unify a full base image file and all associated incremental files into a single backup file.



iSCSI Serves Backup Image Files as iSCSI Targets, Network File System server (Image Target Server)

ActiveImage Protector™ now utilizes iSCSI or NFS server to serve backup images as iSCSI targets to any local or remote iSCSI initiator for mounting backup images as local disks, or as NFS server to access backup images as VMDK file from NFS client; not only providing a method to recover files and folders from a backup, but provides immediate booting of a backup image attached to a virtual machine on a VMware vSphere hypervisor.



License Management Feature

Offline License File

Use of the offline license file provides license activation on a standalone PC without internet connection. Actiphy Authentication Service (AAS) acts as a Standalone Licensing server for computers grouped over intranet without requiring a persistent internet connection.

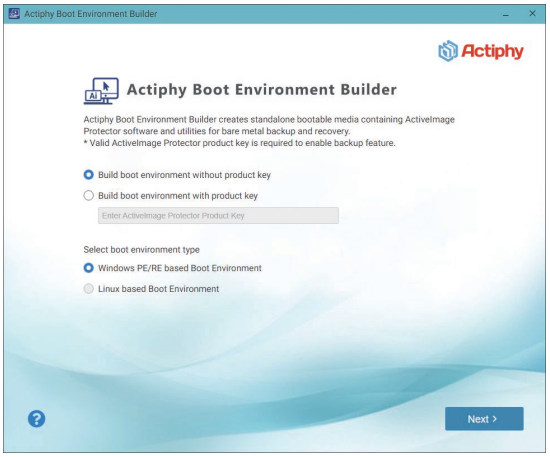
Subscription License

One-month and annual subscription licenses are now available as well as perpetual licenses. Options are provided to purchase one month, one year or a combination of both for the new or extended subscription license.

Free Add-on Tool

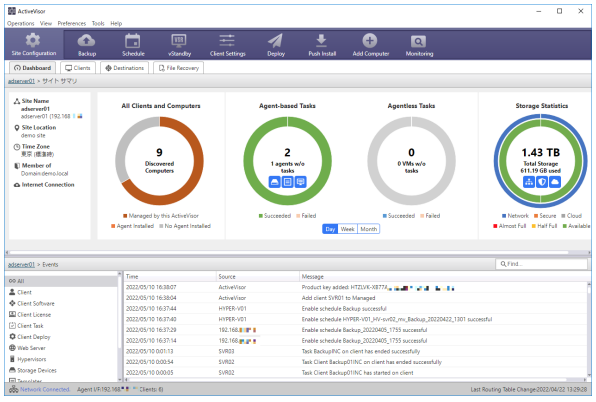
Actiphy BE Builder (boot environment builder)

ActiveImage Protector™ comes with boot environment builder for building a Windows-based boot environment when restoring the system or performing cold backup. You can create a standard Windows RE (Recovery Environment) based boot environment without installing Windows ADK or Windows PE. The Boot Environment Builder automatically detects required drivers, so that you can select the required drivers to install in the media which reduces IT engineers' workload. USB memory / HDD / SSD hard disk, ISO image file and optical media are supported to build the boot environment. If your notebook PC does not come with an optical media drive, the use of bootable USB flash memory / HDD / SSD offers a system recovery option.



ActiveVisor, add-on Centralized Management Console for ActiveImage Protector™

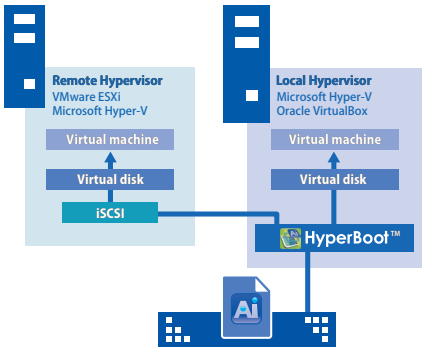
ActiveVisor™ provides a centralized management tool for ActiveImage Protector™ by monitoring networked client computers on which ActiveImage Protector™ agents are installed. Centralized management operation includes auto-discovery of managed computers, push-installing ActiveImage Protector™ agents, creating and deploying templates of backup tasks and configuration files, real-time monitoring of backup status, obtaining license information of ActiveImage Protector™ agents on managed computers, and remote operation of ActiveImage Protector™ agents.



HyperBoot™ add-on to immediately boot backup images as virtual machines

Use our free HyperBoot™ add-on to boot ActiveImage Protector™ backup image files as a fully functional virtual machine in only a few minutes on local and remote Microsoft Hyper-V, VMware ESXi, Oracle VirtualBox. HyperBoot™ serves as an interim replacement server to bridge the gap between disaster and recovery. Before a full-state recovery from the disruption caused by ransomware attack, use HyperBoot™ to check for bootability and verify integrity of the backup. Using VMware vMotion streamlines the recovery process by seamlessly migrating live virtual machines booted in vCenter to a hypervisor in a production environment.

* Backup of Linux machine with LVM configuration is not supported.

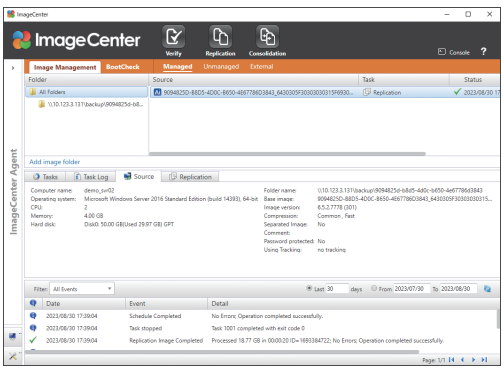


ReZoom™ it! for granular virtual machine recovery

Use ActiveImage Protector™'s ReZoom™ it! to restore specific virtual machines that are included in a backup image of a Hyper-V host. ReZoom™ it! can migrate a virtual machine to the same, different, or a remote Hyper-V host. ReZoom™ it! can be installed as a stand-alone application if needed.

Image Management tool for backup files(ImageCenter™)

ImageCenter™ is a stand-alone image management tool for ActiveImage Protector™. With ImageCenter™, replication of backup image files to local or off-site high-capacity data stores can be scheduled, and automatically run the scheduled Replication task as well as Consolidation of incremental files, BootCheck™, Verify tasks. All of these can be offloaded to a dedicated system, greatly reducing resource demands on the source machine.



Others

Disk-To-Disk Copy

Disk-to-Disk copy is used when migrating data from a hard disk to a large-capacity disk or to an SSD. The Disk-to-disk Copy feature can select the entire disk or a specific volume to copy, or copy to a higher capacity disk or volume. Data volumes from different disks can be combined using Disk-to-Disk copy for a new single disk.

Eject RDX data cartridge

When enabling the [RDX data cartridge eject setting] option, you can configure the settings to eject RDX data cartridges after full or incremental backup on the specified day(s) of a week, at a specified time after full or incremental backup, or when the backup task completes.

Command line execution support

Most of ActiveImage Protector™'s features can be used by specifying parameters for command line tool or with command file. ActiveImage Protector™'s CLI allows backups to be seamlessly administered by system management tools, if any, by using prepared script file.

Monitor task log entries in Windows Event Log Viewer

Every task event is now recorded in the Windows event log to provide better integration into the Windows Management Interface for a more unified experience.

Encryption of Backup Images

ActiveImage Protector™ can create password-protected and encrypted backup images and supports up to AES 256-bit encryption. Enabling the encryption for the backup image file ensures that the backup file cannot be compromised.

Incremental backup saves process time and storage demand

Incremental backups use an in-house developed Change Block Comparison (CBC) technology to include only the sectors that have changed since the previous backup. Using CBC technology instead of a driver reduces the impact on system resources.

Support for LVM Backup

Support for collective backup / restore of disks configured with Logical Volume Manager (LVM). This eliminates the process of configuring boot setting when restoring the system disk. LVM created by XFS is also supported.

Email Notification

Email notification can be sent (using SSL / TSL) to an email address of your choice. Notifications include successfully completed backups or backup failure. Email notification may be set to inform you of the summary of task execution and license status (expiration of the license period).

Cold-Imaging backup for static Windows machines

Start up your computer from ActiveImage Protector™'s bootable media to create a backup image of a clean static system volume (immediately after installation of Windows OS). Cold-imaging backup saving the point-in-time state of the failed system is convenient to examine the cause of the system failure.

Online backup ensuring consistency(Hot Imaging)

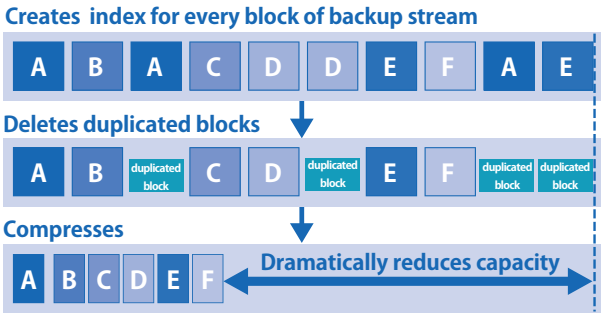
The hot-imaging backup is useful especially when backing up the system and the data frequently updated throughout the day and night on non-stop server. Creates consistent backup of Windows VSS (Volume Shadow Service) aware server applications such as SQL Server, Exchange Server and Oracle.

Fast Bare Metal Recovery

ActiveImage Protector™'s lightning-fast restore engine dramatically speeds up recovery time. Bare Metal Recovery provides capabilities for initializing and creating partitions on the bare metal disk.

Save storage space with IDDC

Our Inline Data Deduplication Compression (IDDC) feature eliminates duplicate data while simultaneously compressing it, resulting in a significant reduction in backup storage requirements. Since backup using IDDC increases the CPU and memory usage, it is recommended to select Level 2 (Optimized) as this is the default level for IDDC.



Enlarge or reduce target volumes or partitions during recovery

NTFS volume may be restored to a volume in specified size larger or smaller than the source volume (NTFS volume only). For example, when restoring to a disk smaller than backup source, the volumes can be restored to reduced size and layout change is supported.

Repair Boot Configuration

Recovery of the BCD in the MBR is supported in the boot environment. In the event that the boot partition in the partition table was not backed up or the restored "C:" drive failed to boot up the system, use the "Repair Boot Configuration" tool to restore the BCD for the restored system.

refers to the features supporting Windows OS only.

refers to the features supporting Linux OS only.

Actiphy, Inc. NCO Kanda-kon'yacho Building, 8 Kanda-kon'yacho, Chiyoda-ku, Tokyo 101-0035, Japan
https://www.actiphy.com global-sales@actiphy.com