DATASHEET

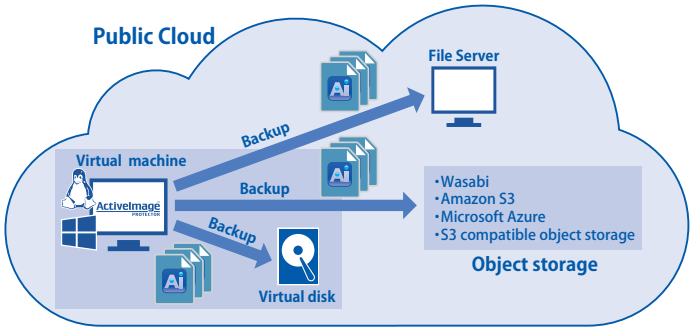
ActiveImage™ 2022 PROTECTOR Cloud

A System / Data Protection Solution optimized for virtual machines in Cloud Environment

ActiveImage Protector™ Cloud is system / data protection solution optimized for Cloud environment. ActiveImage Protector™ entirely backs up the entire hard disk of virtual machine on Cloud, including the operating system along with all your applications and data in a backup image file, using mostly the same operating procedures as on-premise physical / virtual machines. The major cloud services including Amazon Web Services (AWS), Microsoft Azure (Azure), Google Cloud Platform (GCP), Oracle Cloud Infrastructure (OCI) are supported.

In the event of emergency, ActiveImage Protector™ restores the entire system from a backup file via an intuitive software operation. Save your backups to any available storage location depending on the system configuration or intended use of the backup files, including file server in VLAN on cloud or cloud storage in the same / outside the cloud environment.

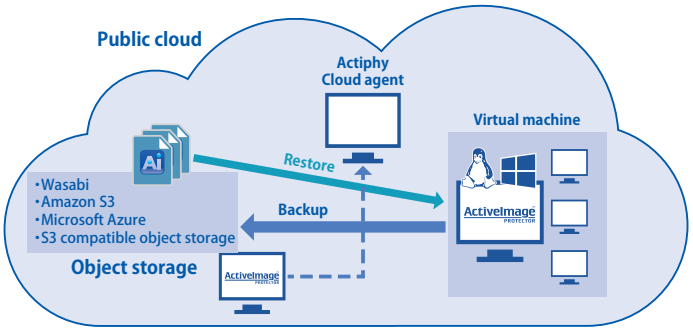
ActiveImage Protector™ Cloud license is cost-effective and can be applied to one cloud environment, enabling to back up a maximum of five virtual machines configured in the cloud environment.



In-Cloud Recovery™ offers an immediate system recovery on cloud

In-Cloud Recovery™ restores the entire system to a virtual machine on cloud environment from backup files in cloud storage without the need for management console for cloud environment or command line operation. A volume or file / folder can be flexibly selected to restore from a backup image.

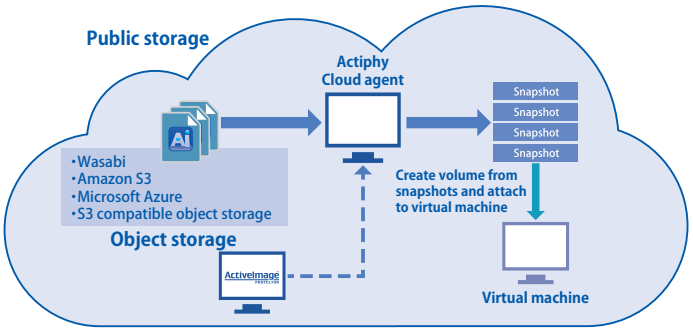
Users can safely implement backup operation of the system in cloud environment based on even little experience as a cloud system administrator.



Immediately boot up virtual machine on cloud

ActiveImage Protector™ creates scheduled incremental snapshots from backup files saved in cloud storage.

In the event of emergency, a volume created from the snapshot is attached to the virtual machine for immediate startup of the system restored to the point the snapshot was taken, bypassing the time-consuming recovery process.



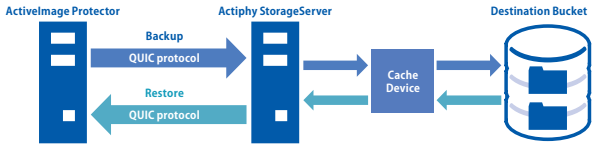
Backup Features

Multiple cloud storages are supported NEW !

Built-in wizards guide you through every step to perform simple and unified backup operation for virtual machines on Google Cloud Platform, Oracle Cloud Infrastructure as well as Amazon Web Services, Microsoft Azure.

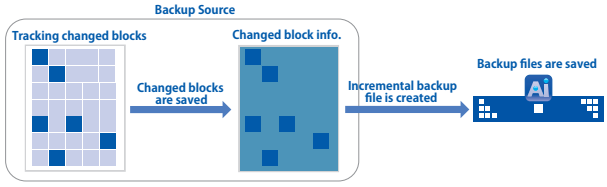
Actiphy StorageServer™ NEW !

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 !

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.



Quickly back up the entire system

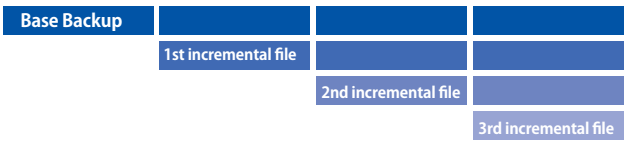
ActiveImage Protector™ backs up the entire virtual machine on Amazon Web Services, Microsoft Azure, Google Cloud Platform or Oracle Cloud Infrastructure to include the OS, applications, and data files to a disk image. When disaster strikes, select a backup image to quickly restore for a complete recovery. Use the File or Folder Recovery option to restore a specific file or a folder from a backup image file.

File Backup

ActiveImage Protector™ includes File / Folder Backup to back up granularly selected files and folders and provides File or Folder Exclusion configuration options and back up from a network shared folder.

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.

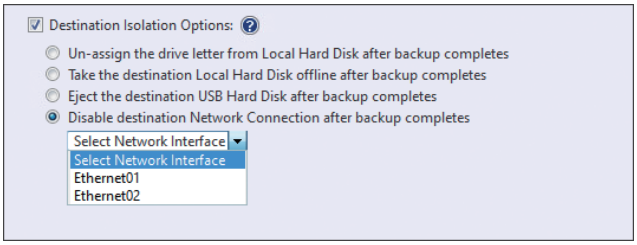


Upon completion of backup task, protect the destination (Destination Isolation Option)

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.

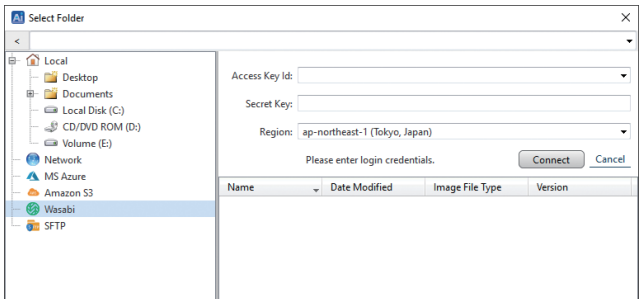


A variety of Storage Media are supported

Backup images in locally attached virtual disk, file server in VLAN on cloud or cloud storage in / outside the cloud environment (Wasabi, Amazon S3, Azure Storage, S3-compatible object storage) are supported. You can use 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 and NAS are supported for restore. Save your large volume backup data in cost-effective Wasabi Hot cloud storage to further secure your data by isolating the backups from a cyber attack.

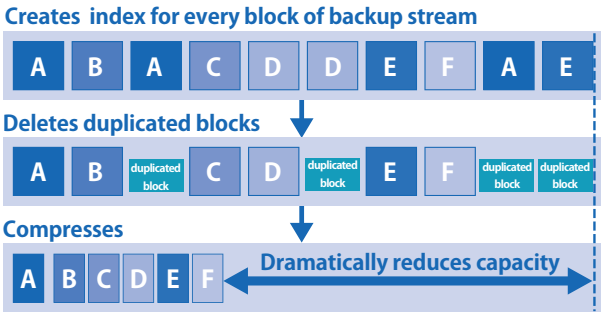


Encryption of Backup Images

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.

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.



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. Create consistent backup of Windows VSS (Volume Shadow Service) aware server applications such as SQL Server, Exchange Server and Oracle.

Flexible schedule backup

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.

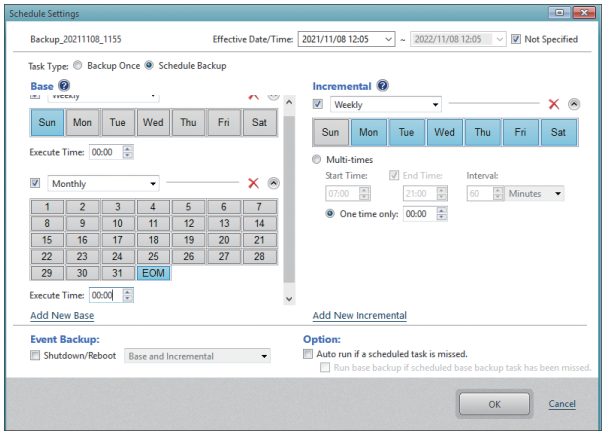
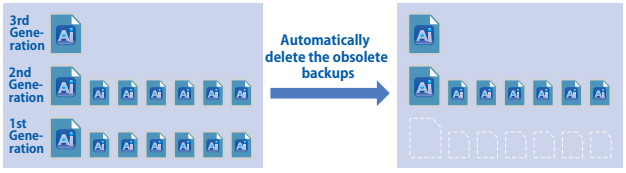


Image Retention Policy

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

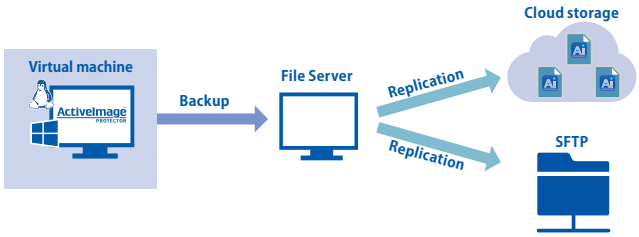
Scripts can be implemented to run before, after, or during the moment snapshots are taken or after the backup image has been created. An example would be to execute a user-specified script to purge database cache before taking a snapshot and then resume the database after taking a snapshot (before starting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

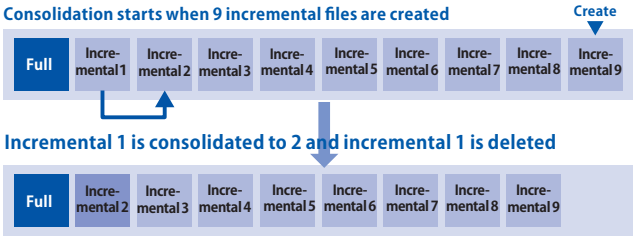
Distributed Backup Storage (Offsite Replication)

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.



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.



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).

Command line execution support

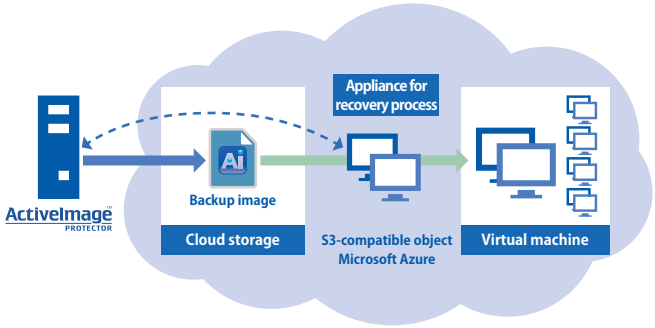
Most of ActiveImage Protector™'s features can be used by specifying parameters for command line tool or with command file. ActiveImage Protector™'s CLI allows backups to be seamlessly administered by system management tools, if any, by using prepared script file.

Restore Features

In-Cloud Recovery™

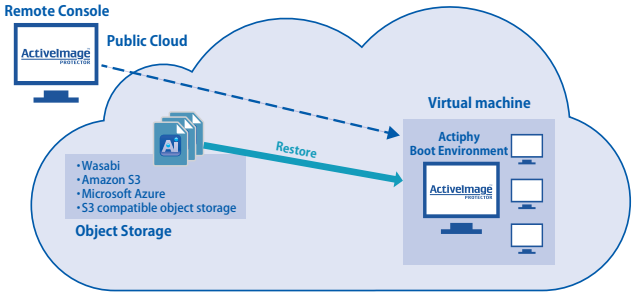
Restore a backup in cloud storage (Amazon S3, Azure Storage, S3-compatible object storage) can be restored to a virtual machine on the cloud (AWS, Azure). The data transfer within the same region when restoring a backup image to a virtual machine on the same cloud does not incur additional costs.

* In-Cloud Recovery™ does not support Google Cloud Platform, Oracle Cloud Infrastructure. When restoring a virtual machine, boot environment booted from RescueBoot is used.



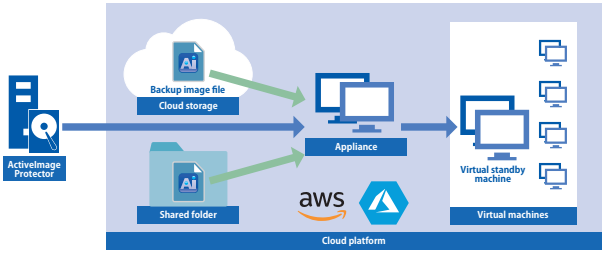
Remotely operate the RescueBoot boot environment

Start up the Actiphy Boot Environment created and booted directly from the internal disk, so that system administrator can remotely restore the failed system of virtual machine from a backup in cloud environment without the use of external device.



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.



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.

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.

Restores to a virtual machine on a different hypervisor

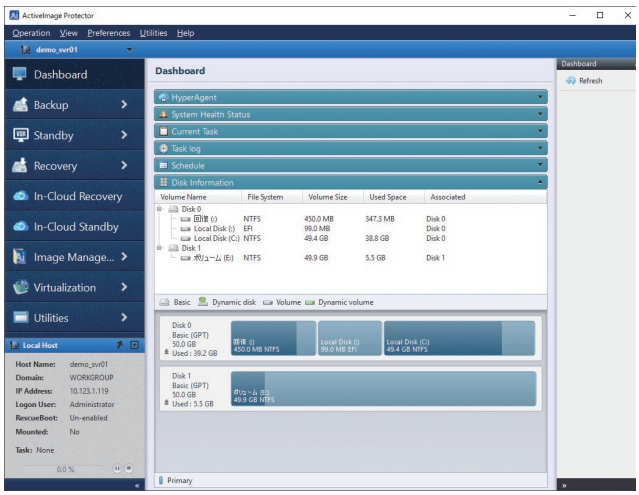
ActiveImage Protector™ provides flexible restore feature enabling to restore a backup image to a virtual machine on different cloud environment (AWS, Azure) or a virtual machine configured on VMware vSphere or Hyper-V in on-premise environment, reducing the system administrators workload.

* Please keep in mind that [Make backup image file P2V ready] option is enabled for backup setting.

Management Console

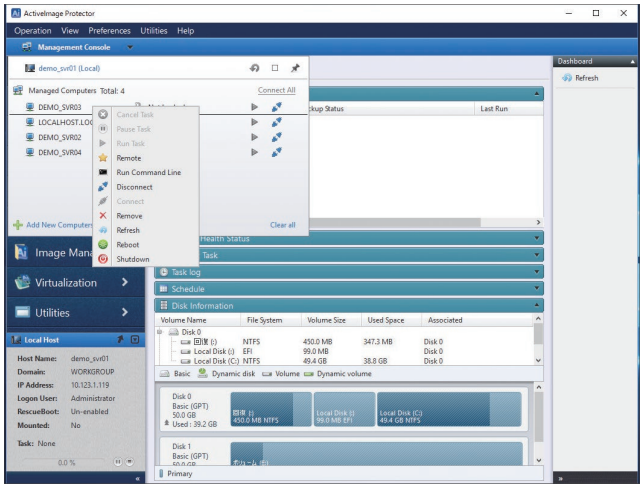
GUI provides tools for efficient operations

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.



Management of Backup Files

Image Explorer

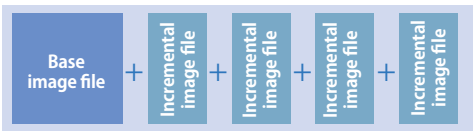
Windows Explorer opens a backup file providing direct access to restore individual files or folders from a backup file.

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.

Archive Backup Files

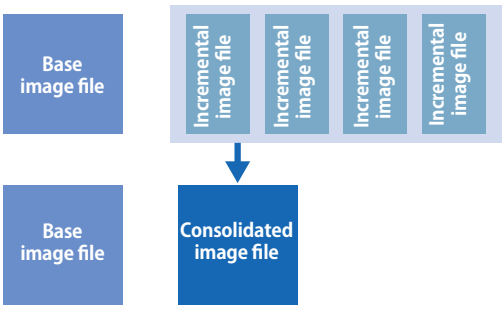
Use the archive feature to unify a full base image file and all associated incremental files into a single backup file.



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.

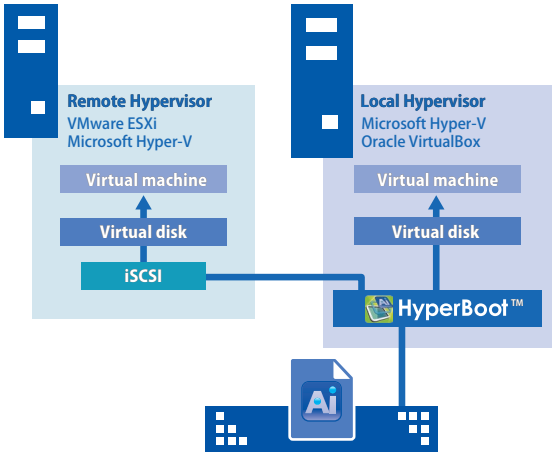


Free Add-on Tool

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.



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.

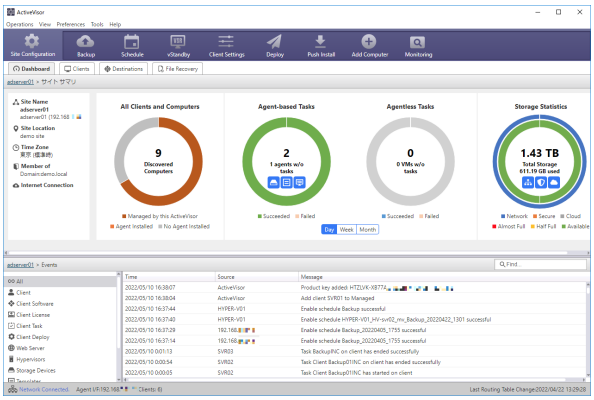
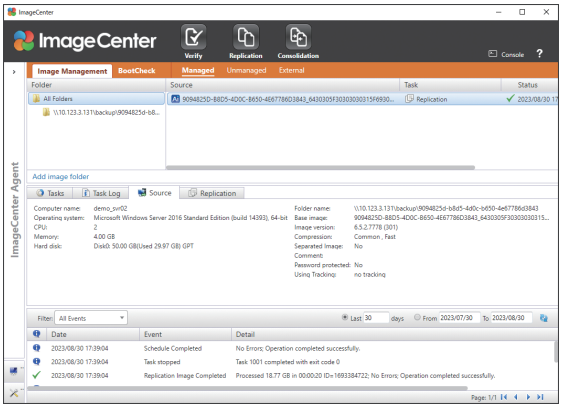


Image Management tool for backup files(ImageCenter™)

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.



refers to the features supporting Windows 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