Kaseya Backup and Disaster Recovery

User Guide

Version 3.0

October 12, 2009

About Kaseya

Kaseya is a global provider of IT automation software for IT Solution Providers and Public and Private Sector IT organizations. Kaseya's IT Automation Framework allows IT Professionals to proactively monitor, manage and maintain distributed IT infrastructure remotely, easily and efficiently with one integrated Web based platform. Kaseya's technology is licensed on over three million machines worldwide.

Copyright © 2000-2009 Kaseya International Limited. All Rights Reserved.

Contents

Backup 3

Backup Tab ... 4
Backup Status ... 6
Schedule Volumes ... 6
Pre/Post Procedure: Backup ... 12
Schedule Folders ... 13
Backup Sets ... 17
Backup Logs ... 17
Explore Volumes ... 18
Explore Folders ... 18
Verify Images ... 19
Image to VM ... 20
Auto Recovery ... 21
CD Recovery ... 23
Universal Restore ... 25
Offsite Servers ... 26
Local Servers ... 29
Offsite Alert ... 32
Schedule Transfer ... 34
Install/Remove: Backup ... 35
Image Location ... 39
Image Password ... 41
Folder Backup ... 43
Backup Alert ... 44
Compression ... 47
Max File Size ... 48
Max Log Age ... 50
Secure Zone ... 51

Index 53

Chapter 1

Backup

In This Chapter

Backup Tab	4
Backup Status	6
Schedule Volumes	6
Pre/Post Procedure: Backup	12
Schedule Folders	13
Backup Sets	17
Backup Logs	17
Explore Volumes	18
Explore Folders	18
Verify Images	19
Image to VM	20
Auto Recovery	21
CD Recovery	23
Universal Restore	25
Offsite Servers	26
Local Servers	29
Offsite Alert	32
Schedule Transfer	34
Install/Remove: Backup	35
Image Location	39
Image Password	41
Folder Backup	43
Backup Alert	44
Compression	47
Max File Size	48
Max Log Age	50
Secure Zone	51

Backup Tab

Backup

Kaseya Backup and Disaster Recovery (BU/DR) provides real-time automated disk backup, disk imaging, file level backup and bare-metal restore for Windows servers and workstations.

Automation, superior performance, ease of use and security are the cornerstone features of Kaseya Backup and Disaster Recovery. Unlike conventional file-based back-up products, Kaseya BU/DR creates an image of the entire system state, including operating system, user settings, applications and data. Applications and servers are always available since the backup process does not require system downtime.

Once a backup is created, Offsite Replication ensures that image and folder backups are immediately and automatically transferred and stored safely away from the business location. This process is completely automated and eliminates the need for a person to remember to take backup media, such as tapes, home or drop them off at a location for storage.

Data can be recovered quickly and easily with Kaseya Backup and Disaster Recovery. Whether it is a simple need to recover a few files, restore a system from a crash or recover systems from bare-metal in the event of a disaster, Kaseya BU/DR provides IT Managed Service Providers and IT users with the most comprehensive, reliable, and cost effective server and workstation protection.

Fully Automated Real-Time Backup

- No user intervention required
- No system downtime required
- Schedule full and incremental imaging
- Schedule folder and file backups
- All processes are automated and occur when scheduled

Complete Disk Imaging

- Sector level backup
- Multiple partitions
- Full and incremental images provides for granular restoration points and reduced file size transfer for offsite replication
- Complete data protection of all programs, settings, configuration, system and user data

Fully Automated Offsite Replication

- Scheduled time periods
- Occurs automatically without user intervention
- No downtime required
- No tapes or other media to transport
- Supports synthetic full backups on offsite servers

Fast and Easy Recovery

- Granular date selection for recovery
- Remotely mount drive volumes
- Complete system image restoration
- Drag and drop restoration of folder and files
- Bare-metal image restoration
- Minimizes downtime

Flexible Configuration and Control

- Configure globally, by group, OS type, etc.
- Granular by server or workstation
- Scheduled and unattended backup and file restoration
- Remote and automated deployment
- No need to physically visit the server or workstation or customer site
- No additional hardware or software is required

Note: You can view Backup and Disaster Recovery demos at http://www.kaseya.com/get-started/demo.aspx.

Note: You can view a Backup and Disaster Recovery training video at https://training.kaseya.com

Functions	Description
Backup Status *(page 6)*	Review the status of scheduled backups for any machine.
Schedule Volumes *(page 6)*	Schedules backups for selected hard disk volumes on any managed machine.
Pre/Post *(page 12)*Procedure	Specify a procedure to run before and/or after Volume Backup
Schedule Folders *(page 13)*	Can independently schedule backups for individual folders.
Backup Sets *(page 17)*	Displays a list of the current backup sets you have stored, for both volumes and folders.
Backup Logs *(page 17)*	Review the logs generated by every backup action.
Explore Volumes *(page 18)*	Mounts a backup as a new drive letter on the managed machine.
Explore Folders *(page 18)*	Copies the .zip archive back to the managed machine.
Verify Images *(page 19)*	Verify any volume or folder backup image
Image to VM *(page 20)*	Converts an existing backup file to one of three types of virtual machine file formats: Virtual PC, VMware and ESX
Auto Recovery *(page 21)*	Select a volume backup image to automatically restore to a selected machine. Requires the machine can still boot and the agent can communicate with the server.
CD Recovery *(page 23)*	Boot the managed machine from a CD and then automatically restore a selected volume backup image.
Universal Restore *(page 25)*	Provides instructions for creating a boot CD and restoring a backup image manually by walking through a wizard.
Offsite Servers *(page 26)*	Specify a machine to act as an offsite server and receive files from a local server.
Local Servers *(page 29)*	Specify a machine to act as a local server and send files to an offsite server.
Offsite Alert *(page 32)*	Generate alerts when a local server fails to connect to an offsite server.
Schedule Transfer *(page 34)*	Set up a day by day schedule for each local server to push files to an offsite server.
Install/Remove *(page 35)*	Install and uninstall the backup driver and software on

	any managed machine.
Image Location *(page 39)*	Set the path to the backup storage location.
Image Password *(page 41)*	Look up the password used to protect backup images.
Folder Backup *(page 43)*	Specify a list of folders to backup during Schedule Folders
Backup Alert *(page 44)*	Activate/deactivate alerts associated with backup events.
Compression *(page 47)*	Set compression level used by both volume and folder backups
Max File Size *(page 48)*	Set a maximum file size used for backup images. Images larger than this maximum are broken into multiple files.
Max Log Age *(page 50)*	Set the maximum number of days to save backup log data.
Secure Zone *(page 51)*	Install a secure zone to support Auto Recovery

Backup Status

Backup > Backup Status

- Similar information is provided using Reports > Backup.

The Backup Status page provides a dashboard view of the backup status of machine IDs that have the backup client installed. The dashboard is organized into the following panes:

- In Process Backups - Lists backups in process and the percentage complete.
- Backup Status at a Glance - Displays pie charts showing scheduled, succeeded, skipped, failed and cancelled backups. Click on any slice of the pie chart or any label of the pie chart to display a list of individual machines belonging to that slice.
- Backup Status by Machine - Shows the status of backups scheduled, succeeded, skipped, failed or cancelled for each machine.
- Offsite Server Status - Displays the total files, files remaining to upload, and data remaining to upload on offsite servers.
- Local Server Status - Displays the total files, files remaining to upload, data remaining to upload on local servers.

Show Status for Last <N> <Periods> and Refresh

Specify the number of periods to collect the results shown on this page, then click the Refresh button.

Schedule Volumes

Backup > Schedule Volumes

The Schedule Volumes page schedules the backup of volumes for selected machine IDs. The list of machine IDs you can select depends on the Machine ID / Group ID / Organization ID filter. To display on this page, machine IDs must have backup software installed on the managed machine using the Backup > Install/Remove *(page 35)* page.

Note: If a network connection is dropped, the system retries for up to 10 seconds before giving up.

Volume Backups vs Folder Backups

When you perform a backup using Schedule Folders *(page 13)*, only the data, along with the folder tree,

is compressed and stored.

Backing up disks and partitions is performed in a different way: Schedule Volumes stores a sector-by-sector snapshot of the disk, which includes the operating system, registry, drivers, software applications and data files, as well as system areas hidden from the user. This procedure is called creating a disk image, and the resulting backup archive is often called a disk/partition image.

Only those hard disk parts that contain data are stored. Further, it does not back up swap file information. This reduces image size and speeds up image creation and restoration.

You can backup individual drive letters (partitions) or entire disk drives.

A partition image includes all files and folders independent of their attributes (including hidden and system files), boot record, FAT (file allocation table), root and the zero track of the hard disk with master boot record (MBR).

A disk image includes images of all disk partitions as well as the zero track with master boot record (MBR). To ensure recovery from complete disk failure, you should backup entire disk drives. Only by backing up entire disks will you capture hidden recovery partitions that may have been installed by your PC system vendor.

Full Backups, Incremental and Differential Backups

Full backups take significant time to complete compared with incremental or differential backups. To save time and disk space, schedule full backups to run less frequently than incremental or differential backups. Typically full backups are scheduled once per week or once per month, while incremental or differential backups run daily. All files required for a full backup, including all incremental or differential backups, are saved together in a backup set. You may save any number of full backup sets you wish.

Synthetic Backups

A synthetic full backup is created by consolidating existing incremental or differential backups with the previous full backup image. This is sometimes called an 'Incremental Forever Backup'. Unlike traditional full backups, synthetic full backups are not transferred from the local server to the offsite server. Instead, after the *first* full backup is transferred, only the incremental or differential files are transferred to the offsite server. A synthetic backup component on the offsite server recreates the next full synthetic backup in parallel with the local server. This eliminates the need to transfer full backups between the local server and offsite server. With synthetic backups, bandwidth requirements for transferring full backups are eliminated, but the offsite server's access to its own file server may need to be enhanced to handle the processing of its synthetic backups.

Configuring synthetic backups involves the following steps:

> Note: The first three steps are required even if synthetic backups are not enabled on the offsite server.

1. Install an agent on a local server. Typically the backup image locations of machine IDs being backed up point to the local server.
2. Install an agent on the offsite server.
3. Define a machine ID as an offsite server using Backup > Offsite Servers *(page 26)*.

   > Note: You do not have to install the backup client to a local server or an offsite server.

4. Click the Schedule Install hyperlink on the Backup > Offsite Servers page for the machine ID you want to schedule synthetic support on. A dialog box displays. Schedule the installation of synthetic support components to the offsite server.
5. Schedule volume backups for machine IDs, ensure the Synthetic Full checkbox is checked. These are machine IDs that store backups on local servers that transfer backups to the offsite server you defined above.

Dynamic Disk Backups

Dynamic storage involves dividing a physical disk into multiple volumes or combining a physical disk with other physical disks to form volumes that are greater in size than any one physical disk. A traditional disk volume is called a "basic" disk volume. BUDR supports the following basic and dynamic backup and restore combinations:

- backup basic disks
- backup dynamic disks
- restore basic volumes to basic disks
- restore basic volumes to dynamic disks
- restore dynamic volumes to basic disks
- restore dynamic volumes to dynamic disks

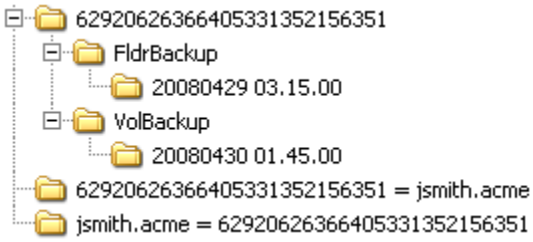
Note: While Universal Restore supports restoration of dynamic disks to similar hardware, it does not support restoration of dynamics disks to different hardware platforms that require new drivers. To restore to different hardware platforms, you must restore the dynamic disk backup to a basic disk.

Backup Folder Structure

Separate Image Location *(page 39)* paths may be specified for volume and folder backups. Volume backups and folder backups are saved as full backup sets. Each backup set gets its own folder. Backup files have a '*.tib extension.

Backup folders are organized by the GUID used to uniquely identify each machine ID. By using the GUID instead of the machine ID, renaming the machine ID or assigning the machine ID to a different group does not prevent the backup files from becoming unavailable.

Two extra, empty, folders in the same backup image location folder identify the machine ID associated with each GUID. For instance, if you have a machine ID named `jsmith.acme` and its GUID is `629206263664053313521563 51` then folders might be organized as follows in the image location folder:



The first folder contains the backups. The second empty folder identifies the machine ID for a GUID. The third empty folder identifies the GUID for a machine ID. If you have backups for many machine IDs all stored in the same image location folder, you can use either of the two empty cross-reference folders to identify the appropriate GUID backup folder, either by machine ID or by GUID.

Backing Up the KServer

Do not attempt to backup the KServer using BUDR while the KServer is running, even if VSS is enabled. Doing so can cause problems when the VSA attempts to write information about the backup to a database that is being backed up. KServer data is backed up automatically each time a database maintenance cycle is run. Database maintenance cycle frequency is set using the Run database backup / maintenance every <N> Days @ <Time> option in System > Server Management > Configure. You can use Schedule Folders *(page 13)* to backup the folder containing the Kaseya database backup files.

For maximum flexibility and resiliency when using BUDR backups of Kaseya-related files, Kaseya recommends that you configure a Folder Backup to back up the following folders on your Kaseya server in addition to any other backups that you run on the server:

```
C:\Kaseya\UserProfiles
C:\Kaseya\WebPages\ManagedFiles
C:\Kaseya\WebPages\banner\default\images\new
```

```
C:\Kaseya\WebPages\compact\default\images\new
C:\Kaseya\WebPages\themes\default\images\new
C:\Kaseya\WebPages\Access
```

> Note: Change `C:\Kaseya` above to the appropriate install directory, if you did not install the KServer to the default install directory.

See the knowledge base article http://kb.kaseya.com/article.asp?p=11855&article=270436 for details.

Confirm that the Schedule Folders schedule does not coincide with the Kaseya database backup configured on the System > Server Management > Configure page, and that the folder you have configured as the Backup folder on KServer is included in folders in the Folder Backup.

You should not attempt to stop the SQL services or Kaseya Server services while running any BUDR backup of your Kaseya server, as Kaseya requires write access to the SQL database in order to update the backup results.

Schedule Full

Click Schedule Full to schedule a new full backup of selected machine IDs using the backup options previously selected. Backup options set using the four Apply buttons are applied to selected machine IDs when Schedule Full is clicked.

> Note: Backups can consume significant network bandwidth. To prevent congesting the network during normal business hours, schedule backups to run at off hours.

Date/Time

Enter the year, month, day, hour, and minute to schedule this task.

Cancel

Click Cancel to clear pending backups for selected machine IDs, including backup options set using the four Apply buttons.

Backup Now

Click Backup Now button to start a full backup if no backups exist. Otherwise, clicking Backup Now creates an incremental or differential backup.

Stagger by

You can distribute the load on your network by staggering this task. If you set this parameter to 5 minutes, then the task on each machine ID is staggered by 5 minutes. For example, machine 1 runs at 10:00, machine 2 runs at 10:05, machine 3 runs at 10:10, ...

Skip if Machine Offline

Check to perform this task only at the scheduled time, within a 15 minute window. If the machine is offline, skip and run the next scheduled period and time. Uncheck to perform this task as soon as the machine connects after the scheduled time.

Backup Set Type

Select the type of backup set to schedule:

- Incremental - Captures only the files that have changed *since the previous full or incremental backup.* Restoring from an incremental backup requires all previous incremental image file plus the original full backup. Do not remove files from the full backup set directory.

  > Warning: Incremental backups detect changes at the sector level. If you defragment your hard disk, a large number of disk sectors will move and appear to change. This results in a large

incremental backup file. This is perfectly normal for a sector level backup system.

- Last Differential - Captures all changes to the target system *since the last full backup.* To save disk space, only the latest differential backup is saved with each full backup set. Select Last Differential to minimize backup storage requirements.
- All Differentials - Captures all changes to the target system *since the last full backup.* Saves all differential backups in addition to the last differential backup.

Click Apply to apply these settings to selected machine IDs without changing the backup schedule.

Every <N> Periods

Incremental and differential backups are always performed as a recurring task. Enter the number of times to run this task each time period. Click Apply to apply these settings to selected machine IDs. Enter 0 to disable the scheduling of incremental or differential backups.

Apply Full Every <N> Periods

Full backups are always performed as a recurring task. Enter the number of times to run this task each time period. Click Apply to apply these settings to selected machine IDs.

Save last <N> backup sets

Specify the number of full backup sets to keep. A backup set is a full backup plus all incremental backups or differential backups referencing that full backup. Starting a new full backup creates a new full backup set. So, entering 3 here maintains the current full backup, plus that last two full backup sets. Click Apply to apply these settings to selected machine IDs without changing the backup schedule.

Synthetic Full

If checked, creates a new full backup by consolidating existing incremental or differential backups with the previous base full backup image.

Delete before running backup

If checked, the system deletes any backups sets not being saved using Save last <N> backup sets before creating a new backup set. If blank, backup sets scheduled for deletion are deleted only after the new backup set is successfully created.

Verify Backup

If checked, verifies each backup image immediately after each full, incremental, or differential backup completes. Verify takes the same amount of time as the original backup to complete. Only verify in situations where you question the integrity of the network connection to the backup file location. You do not generally need to use this option. Use the Verify Images *(page 19)* function to spot check backup files at any time. Click Apply to apply these settings to selected machine IDs without changing the backup schedule.

Enable VSS Support

Enables Volume Shadow Service (VSS) on 2003 servers. VSS ensures completion of all transactions before the backup process starts. Click Apply to apply these settings to selected machine IDs without changing the backup schedule.

Select All/Unselect All

Click the Select All link to check all rows on the page. Click the Unselect All link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine:

- Online but waiting for first audit to complete
- Agent online
- Agent online and user currently logged on. Icon displays a tool tip showing the logon name.
- Agent online and user currently logged on, but user not active for 10 minutes
- Agent is currently offline
- Agent has never checked in
- Agent is online but remote control has been disabled
- The agent has been suspended

Note: Different icon images display when this addon module is installed in a 5.x VSA. The Remote Control > Control Machine page displays a legend of the specific icons your VSA system is using.

Machine.Group ID

The list of Machine ID.Group IDs.Organization IDs displayed is based on the Machine ID / Group ID / Organization ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.

Disks

The list of local hard drive disks available on a machine. Check a disk number to include it in a volume backup. Backup an entire disk to insure any hidden partitions that may have been installed by your PC vendor are also backed up. These hidden partitions may be required to boot your system in the event of a restore.

Sets

The number of backup sets maintained at any one time.

Inc / Diff

The type of backup set maintained:

- - Incremental
- - Differential
- - All differential
- - Synthetic full

Last Backup

The last time a backup was performed.

Partitions

The list of available drive letter partitions available on a machine. Check a driver letter to include it in a volume backup.

Next Backup

The next scheduled backup. Pending timestamps display as red text with yellow highlight.

Period (full)

The scheduled interval between full backups.

Period (inc)

The scheduled interval between incremental or differential backups.

Verify VSS

If checked, Volume Shadow Service (VSS) is enabled when performing a backup.

Pre/Post Procedure: Backup

Backup > Pre/Post Procedure

Use the Pre/Post Procedure page to run procedures either before a Schedule Volumes *(page 6)* backup starts or after it completes. Does not apply to Schedule Folders *(page 13)* backups.

Use this page to suspend services that may lock files and prevent volume backup from completing. You may also wish to force a system service, such as Exchange or a database, to write all its data to disk prior to system backup. Typically this can be done without requiring the service in question to be down during backup. All critical services can be left fully operational at all times. For example, to backup an Exchange Server, a snap shot of the database is needed prior to the backup start. A procedure will quickly start and stop Exchange to take the snapshot of the database prior to the start of the backup.

To Run a Pre/Post Procedure

1. Select machine IDs.
2. Click the select procedure link to select a procedure to run before a Schedule Volumes backup starts or after it completes.
3. For procedures run after completion, specify whether the procedures should run `with any status`, `with success` or `with failure`.
4. Click Set.

Schedule

Click Set to run the selected procedures run before a Schedule Volumes backup starts or after it completes.

Run Select Procedure Before Initial Update Starts

If checked, runs the selected procedure *before* a Schedule Volumes backup starts.

Run Select Procedure After Initial Update Completes

If checked, runs the selected procedure *after* a Schedule Volumes backup completes. For procedures run after completion, specify whether the procedures should run `with any status`, `with success` or `with failure`.

Select All/Unselect All

Click the Select All link to check all rows on the page. Click the Unselect All link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine:

- Online but waiting for first audit to complete
- Agent online
- Agent online and user currently logged on. Icon displays a tool tip showing the logon name.

- Agent online and user currently logged on, but user not active for 10 minutes
- Agent is currently offline
- Agent has never checked in
- Agent is online but remote control has been disabled
- The agent has been suspended

Note: Different icon images display when this addon module is installed in a 5.x VSA. The Remote Control > Control Machine page displays a legend of the specific icons your VSA system is using.

Machine.Group ID

The list of Machine ID.Group IDs.Organization IDs displayed is based on the Machine ID / Group ID / Organization ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.

Pre Procedure / Post Procedure

This column lists the procedures set to run before a Schedule Volumes backup starts or after it completes.

Schedule Folders

Backup > Schedule Folders

The Schedule Folders page schedules the backup of folders for selected machine IDs. The folders backed up are specified using Backup > Folder Backup *(page 43)*. The list of machine IDs you can select depends on the Machine ID / Group ID / Organization ID filter. To display on this page, machine IDs must have backup software installed on the managed machine using the Backup > Install/Remove *(page 35)* page.

Note: If a network connection is dropped, the system retries for up to 10 seconds before giving up.

Sector Level Backups

Folder backups perform sector level backups of selected folders. Sector level copying allows the system to backup locked and in-use files so you can safely backup at any time of the day.

Full Backups, Incremental and Differential Backups

Full backups take significant time to complete compared with incremental or differential backups. To save time and disk space, schedule full backups to run less frequently than incremental or differential backups. Typically full backups are scheduled once per week or once per month, while incremental or differential backups run daily. All files required for a full backup, including all incremental or differential backups, are saved together in a backup set. You may save any number of full backup sets you wish.

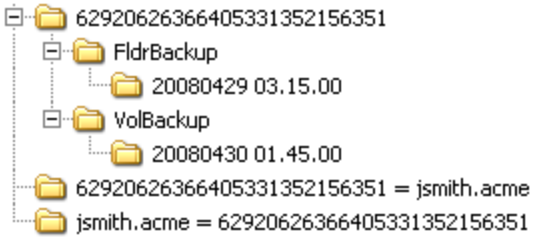
Backup Folder Structure

Separate Image Location *(page 39)* paths may be specified for volume and folder backups. Volume backups and folder backups are saved as full backup sets. Each backup set gets its own folder. Backup files have a '*.tib extension.

Backup folders are organized by the GUID used to uniquely identify each machine ID. By using the GUID instead of the machine ID, renaming the machine ID or assigning the machine ID to a different group does not prevent the backup files from becoming unavailable.

Two extra, empty, folders in the same backup image location folder identify the machine ID associated with each GUID. For instance, if you have a machine ID named `jsmith.acme` and its

GUID is 629206263664053313521563 51 then folders might be organized as follows in the image location folder:



The first folder contains the backups. The second empty folder identifies the machine ID for a GUID. The third empty folder identifies the GUID for a machine ID. If you have backups for many machine IDs all stored in the same image location folder, you can use either of the two empty cross-reference folders to identify the appropriate GUID backup folder, either by machine ID or by GUID.

Schedule Full

Click Schedule Full to schedule a new full backup of selected machine IDs using the backup options previously selected. Backup options set using the four Apply buttons are applied to selected machine IDs when Schedule Full is clicked.

> Note: Backups can consume significant network bandwidth. To prevent congesting the network during normal business hours, schedule backups to run at off hours.

Date/Time

Enter the year, month, day, hour, and minute to schedule this task.

Cancel

Click Cancel to clear pending backups for selected machine IDs, including backup options set using the four Apply buttons.

Backup Now

Click Backup Now button to start a full backup if no backups exist. Otherwise, clicking Backup Now creates an incremental or differential backup.

Stagger by

You can distribute the load on your network by staggering this task. If you set this parameter to 5 minutes, then the task on each machine ID is staggered by 5 minutes. For example, machine 1 runs at 10:00, machine 2 runs at 10:05, machine 3 runs at 10:10, ...

Skip if Machine Offline

Check to perform this task only at the scheduled time, within a 15 minute window. If the machine is offline, skip and run the next scheduled period and time. Uncheck to perform this task as soon as the machine connects after the scheduled time.

Backup Set Type

Select the type of backup set to schedule:

- Incremental - Captures only the files that have changed *since the previous full or incremental backup.* Restoring from an incremental backup requires all previous incremental image file plus the original full backup. Do not remove files from the full backup set directory.

  > Warning: Incremental backups detect changes at the sector level. If you defragment your hard disk, a large number of disk sectors will move and appear to change. This results in a large

incremental backup file. This is perfectly normal for a sector level backup system.

- Last Differential - Captures all changes to the target system *since the last full backup.* To save disk space, only the latest differential backup is saved with each full backup set. Select Last Differential to minimize backup storage requirements.
- All Differentials - Captures all changes to the target system *since the last full backup.* Saves all differential backups in addition to the last differential backup.

Click Apply to apply these settings to selected machine IDs without changing the backup schedule.

Every <N> Periods

Incremental and differential backups are always performed as a recurring task. Enter the number of times to run this task each time period. Click Apply to apply these settings to selected machine IDs. Enter 0 to disable the scheduling of incremental or differential backups.

Apply Full Every <N> Periods

Full backups are always performed as a recurring task. Enter the number of times to run this task each time period. Click Apply to apply these settings to selected machine IDs.

Save last <N> backup sets

Specify the number of full backup sets to keep. A backup set is a full backup plus all incremental backups or differential backups referencing that full backup. Starting a new full backup creates a new full backup set. So, entering 3 here maintains the current full backup, plus that last two full backup sets. Click Apply to apply these settings to selected machine IDs without changing the backup schedule.

Synthetic Full

If checked, creates a new full backup by consolidating existing incremental or differential backups with the previous base full backup image.

Delete before running backup

If checked, the system deletes any backups sets not being saved using Save last <N> backup sets before creating a new backup set. If blank, backup sets scheduled for deletion are deleted only after the new backup set is successfully created.

Verify Backup

If checked, verifies each backup image immediately after each full, incremental, or differential backup completes. Verify takes the same amount of time as the original backup to complete. Only verify in situations where you question the integrity of the network connection to the backup file location. You do not generally need to use this option. Use the Verify Images *(page 19)* function to spot check backup files at any time. Click Apply to apply these settings to selected machine IDs without changing the backup schedule.

Enable VSS Support

Enables Volume Shadow Service (VSS) on 2003 servers. VSS ensures completion of all transactions before the backup process starts. Click Apply to apply these settings to selected machine IDs without changing the backup schedule.

Select All/Unselect All

Click the Select All link to check all rows on the page. Click the Unselect All link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine:

- Online but waiting for first audit to complete
- Agent online
- Agent online and user currently logged on. Icon displays a tool tip showing the logon name.
- Agent online and user currently logged on, but user not active for 10 minutes
- Agent is currently offline
- Agent has never checked in
- Agent is online but remote control has been disabled
- The agent has been suspended

Note: Different icon images display when this addon module is installed in a 5.x VSA. The Remote Control > Control Machine page displays a legend of the specific icons your VSA system is using.

Machine.Group ID

The list of Machine ID.Group IDs.Organization IDs displayed is based on the Machine ID / Group ID / Organization ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.

Sets

The number of backup sets maintained at any one time.

Inc / Diff

The type of backup set maintained:

- - Incremental
- - Differential
- - All differential

Last Backup

The last time a backup was performed.

Next Backup

The next scheduled backup. Pending timestamps display as red text with yellow highlight.

Period (full)

The scheduled interval between full backups.

Period (inc)

The scheduled interval between incremental or differential backups.

Verify VSS

If checked, Volume Shadow Service (VSS) is enabled when performing a backup.

Backup Sets

Backup > Backup Sets

The Backup Sets page displays a list of the *current* backup sets you have stored, for both volumes and folders. If you specified 5 backup sets using either Schedule Volumes *(page 6)* or Schedule Folders *(page 13)* this page displays 5 backups sets. This page also displays all backups that have failed while trying to store up to the specified number of backup sets. You can can also:

- Clear all backups sets for a volume or folder.

  Note: The backup sets are not actually cleared from the image location until the next full backup runs.

- Cancel a backup in progress.
- Click the backup link to display the log details of a backup in XML format.

  You should never need to look at this log file unless backup reports strange or unexplained failures. In those cases, the log may provide more insight into the cause of the backup failure such as identifying corrupt files or disk sectors.

  Note: Bad disks may cause backup failures. Running CHKDSK.EXE on the drive in question may resolve failures.

The backup set table lists:

- The End Time the backup set was completed.
- The Type of backup: full, differential, or incremental.
- The Duration required to perform the backup.
- The Size of the backup.
- Whether the backup succeeded or failed. If failed, an error message also displays.

The list of machine IDs you can select depends on the Machine ID / Group ID / Organization ID filter. To display on this page, machine IDs must have backup software installed on the managed machine using the Backup > Install/Remove *(page 35)* page.

Note: See Backup Logs *(page 17)* for a list of *all* backups.

Clear

Click the Clear button to manually remove all volume backup sets or folder backup sets. This might be necessary to remove a "stuck" backup set or to free up disk space.

Warning: Clears *all* volume backups sets or folder backup sets for a machine ID.

Cancel

Click Cancel to cancel an in process backup.

Backup Logs

Backup > Backup Logs

The Backup Logs page displays a list of the *all* backups you have performed, for both volumes and folders, up to the number of days specified for backup logs using Backup > Max Log Age *(page 50)*. Click a machine ID to display a log containing the date, type, duration, result and description of each backup operation performed.

> Note: Backup Logs provides more detailed information about why a backup failed than provided by Backup Sets *(page 17)*. Backups Sets displays a list of all *current* backups.

The list of machine IDs you can select depends on the Machine ID / Group ID / Organization ID filter. To display on this page, machine IDs must have backup software installed on the managed machine using the Backup > Install/Remove *(page 35)* page.

> Note: Bad disks may cause backup failures. Running CHKDSK.EXE on the drive in question may resolve failures.

Explore Volumes

Backup > Explore Volumes

The Explore Volumes page mounts a volume backup as a new read only drive letter on the same machine or on a different machine. The backup volume can be browsed, just like any other drive, with Windows Explorer. Individual files or folders can be copied from mounted backup volumes to any other folder on your local machine you have write access to. Mounted volume backups remain available for browsing unless the computer is rebooted or the drive is unmounted by clicking the Unplug All button.

> Note: A user with access rights to the Image Location *(page 39)* must be logged in at the time the backup is mounted.

Click a machine ID to select a volume backup to mount. The list of machine IDs you can select depends on the Machine ID / Group ID / Organization ID filter. To display on this page, machine IDs must have backup software installed on the managed machine using the Backup > Install/Remove *(page 35)* page.

Mount to machine ID

Select Mount to machine ID to mount the backup image to the same machine ID that the backup image was made on.

Mount to select machine ID

Select Mount to select machine ID to mount the backup image to a different machine ID than the backup image was made on.

Mount

To explore a full or incremental/differential backup, click the radio button next to the date listed. The complete image, as of that date, gets mounted on the managed machine as a new drive letter. Click the Mount button to generate a procedure to mount the backup image. The screen automatically refreshes every 5 seconds and reports status of the mount until the mount procedure completes execution.

Unplug All

Click Unplug All to remove any mounted volume backups.

Explore Folders

Backup > Explore Folders

The Explore Folders page restores folder backups to a specified directory on a target machine, maintaining the same structure they had in the backup. Unlike Explore Volumes *(page 18)*, this page can

not mount the data as a new drive letter. Manually delete restored backup folders to remove them.

> Note: A user with access rights to the Image Location *(page 39)* must be logged in at the time the backup is mounted.

Restore to machine ID

If selected, the folder backup is restored to the same machine ID the folder backup was made on.

Restore to select machine ID

If selected, the folder backup is restored to a different machine ID the folder backup was made on..

Restore

Click Restore to restore a selected folder backup to a selected machine ID.

Create new folder in

Enter the path on the target machine where the folder backup will be restored.

Folder Backup

Click the radio button next to the date of a folder backup to select it.

Verify Images

Backup > Verify Images

The Verify Images page performs a one time verification of any selected volume or folder backup. Use this function to spot check that backups are completed and can be used to restore from successfully. Verification does *not* involve comparing the backup to the original source files, so any other machine with an agent can be used to perform the verification of the backup file so long as the machine has read/access to the image location.

Successful backups may fail to verify if the backup image file was not copied successfully to the Image Location *(page 39)* path. This problem typically only occurs in slow or unreliable networks. On slow networks, consider selecting the Verify Backup option in Schedule Volumes *(page 6)* and Schedule Folders *(page 13)* to verify the backup every time.

Click a machine ID to select a volume backup to mount. The list of machine IDs you can select depends on the Machine ID / Group ID / Organization ID filter. To display on this page, machine IDs must have backup software installed on the managed machine using the Backup > Install/Remove *(page 35)* page.

Verifying Manual Backups

The Verify Images page can verify images created by Acronis directly, so long as the version of Acronis is a version supplied by Kaseya.

Verify from machine ID

Select Verify from machine ID to verify the backup on the same machine ID that the backup image was made on.

Verify from select machine ID

Select Verify from select machine ID to verify the backup on a different machine ID than the backup image was made on.

Verify Volume

To verify a full or incremental/differential volume backup, select the radio button next to the date listed and click the Verify Volumes button.

Verify Folder

To verify a full or incremental/differential folder backup, click the radio button next to the date listed and click the Verify Folders button.

Image to VM

Backup > Image to VM

The Image to VM page converts an existing backup file to one of three types of virtual machine file formats: Virtual PC, VMware and ESX. This enables you to install a backup to a virtual machine environment.

Any other machine with an agent can be used to perform the conversion of the backup file so long as the machine has read/access to the image location.

Successful and failed Image to VM conversion log entries are listed in Backup Logs *(page 17)*.

Click a machine ID to select a volume backup to convert. The list of machine IDs you can select depends on the Machine ID / Group ID / Organization ID filter. To display on this page, machine IDs must have backup software installed on the managed machine using the Backup > Install/Remove *(page 35)* page.

Convert from machine ID

Select Convert from machine ID to convert the backup using the same machine ID that the backup image was made on.

Convert from select machine ID

Select Convert from select machine ID to convert the backup using a different machine ID.

Destination Virtual Harddrive Image Type

Select one of the following virtual harddrive image types:

- Virtual PC - Microsoft's brand of virtual machine manager. Virtual PC is installed on top of a Windows OS.
- VMware - Creates a VMware image type file compatible with a Windows-based VMware product such as VMware Server or VMware Workstation. VMware Server in installed on top of a Windows OS and depends on Windows to manage hardware partitioning and access.
- ESX - ESX is VMware's version of a virtual machine hypervisor. A hypervisor is a thin OS that is installed on the hardware directly, bypassing the use of a general purpose server OS, such as Microsoft Server.

Converted image will be written to Volume Path

Identifies the path where the converted VM image will be written.

Destination File Name

Enter a unique filename for VM image file you are about to create.

Convert Image

Select one of the existing volume backups to convert, then click Convert Image to begin the conversion.

Auto Recovery

Backup > Auto Recovery

The Auto Recovery page restores any volume backup image to the same machine the backup was created on. Auto Recovery requires:

- The target machine's agent can still communicate with the KServer.
- Secure Zone *(page 51)* be installed on the target machine ID.

Note: Folder backups are restored using Explore Folders *(page 18)*. To restore a target machine that cannot communicate with the KServer see CD Recovery *(page 23)* or Universal Restore *(page 25)*.

Auto Recovery lets you select any volume backup image (full, incremental, or differential) for the selected machine ID to restore without any user interaction at all. The restore may be scheduled to run at any time of day or on a recurring schedule. Set a recurring schedule to auto restore a machine in a public area subject to abuse by random users.

The server and agent configure the hidden Secure Zone partition to automatically restore the selected backup image from the Image Location *(page 39)* path. Once configuration completes, the agent reboots the machine without warning. The machine boots into the secure zone partition and automatically restores the selected backup image.

Dynamic Disk Restores

Dynamic storage involves dividing a physical disk into multiple volumes or combining a physical disk with other physical disks to form volumes that are greater in size than any one physical disk. A traditional disk volume is called a "basic" disk volume. BUDR supports the following basic and dynamic backup and restore combinations:

- backup basic disks
- backup dynamic disks
- restore basic volumes to basic disks
- restore basic volumes to dynamic disks
- restore dynamic volumes to basic disks
- restore dynamic volumes to dynamic disks

Note: While Universal Restore supports restoration of dynamic disks to similar hardware, it does not support restoration of dynamics disks to different hardware platforms that require new drivers. To restore to different hardware platforms, you must restore the dynamic disk backup to a basic disk.

Restore Failure

Restores can fail for the following reasons:

- The Image Location points to a local driver letter - When Windows boots, drive letters are automatically assigned to hard drives starting with `C:`. With the disk manager, you can reassign these to any other unused drive letter. For example, you may decide to turn your `D:` drive into `G:` and set the Image Location path to `G:\backups`. The recovery boot process will not know about the driver letter mapping and will assign `D:` to the hard disk. The restore will then fail trying to access `G:\backups`. You can resolve this problem by setting your image location to `D:\backups` prior to selecting the restore options. Restore will then successfully access `D:\backups`.
- Image stored on a USB drive - Similar to the issue above, when the recovery boot process assigns drive letters, it may assign the USB drive a different drive letter than Windows assigned it. You can resolve this problem by setting your Image Location to the new drive letter prior to selecting the restore options. Restore will then successfully access the USB drive.

- Image stored on a network drive - If the remote drive, or the machine hosting the drive, is not turned on, or if the username and password have changed, then the recovery boot process will not be able to access the network drive.

Schedule

Click Schedule to schedule restore of volume backup images to selected machine IDs using the restore parameters previously selected. Remember, the restore reboots the machine and restores an image without warning the user first.

Date/Time

Enter the year, month, day, hour, and minute to schedule this task.

Cancel

Click Cancel to clear a scheduled restore of selected machine IDs.

Restore Now

Click Restore Now to restore volume backup images to selected machine IDs immediately.

Run recurring every <N> periods

Check this box to make this task a recurring task. Enter the number of times to run this task each time period.

Stagger by

You can distribute the load on your network by staggering this task. If you set this parameter to 5 minutes, then the task on each machine ID is staggered by 5 minutes. For example, machine 1 runs at 10:00, machine 2 runs at 10:05, machine 3 runs at 10:10, ...

Skip if Machine Offline

Check to perform this task only at the scheduled time, within a 15 minute window. If the machine is offline, skip and run the next scheduled period and time. Uncheck to perform this task as soon as the machine connects after the scheduled time.

Select All/Unselect All

Click the Select All link to check all rows on the page. Click the Unselect All link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine:

- Online but waiting for first audit to complete
- Agent online
- Agent online and user currently logged on. Icon displays a tool tip showing the logon name.
- Agent online and user currently logged on, but user not active for 10 minutes
- Agent is currently offline
- Agent has never checked in
- Agent is online but remote control has been disabled
- The agent has been suspended

> Note: Different icon images display when this addon module is installed in a 5.x VSA. The Remote Control > Control Machine page displays a legend of the specific icons your VSA system is using.

Machine.Group ID

The list of Machine ID.Group IDs.Organization IDs displayed is based on the Machine ID / Group ID / Organization ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.

Select backup to restore

Select a backup image to restore from the drop down control listing all available backups for the selected machine ID.

Last Restore

The last time an image was restored to this machine ID.

Next Restore

The next time an image is scheduled to be restored.

Interval

The interval for the scheduled task to recur.

CD Recovery

Backup > CD Recovery

The CD Recovery page restores volume backup images to the same machine or same type of machine that the backup was created on. CD Recovery requires the target machine be booted from a CD.

Use CD Recovery to restore backup images if the target machine's agent can not currently communicate with the KServer. The target machine must be physically connected to a network that provides access to the KServer. Once the target machine boots up from the CD, no further user interaction is required. The network card is configured automatically. The KServer automatically downloads and restores a backup image to the target machine.

Procedure

1. Create an ISO file - If an ISO image file record doesn't already exist in the paging area, create a new ISO image file by clicking the Create New ISO button. The same ISO file is created each time this button is clicked, but with a different *filename*. It is the ISO *filename* on the recovery CD that tells the KServer which machine ID and backup image to restore from.

   > Note: You can leave the machine ID and backup image unassigned or change the machine ID and backup image associated with an ISO image file at any time. This lets you create and distribute the recovery CD in advance to all the locations you manage. Then use this page to select the backup image you want to restore from just before the target machine is booted up from the CD. However, you must assign a machine ID and backup image *before* you start the restore or an error will result.

2. Select a Machine ID - Associate a machine ID with the ISO file. The machine ID must specify an Image Location *(page 39)* that contains the backup image you want to restore.
3. Select a Backup Image - Associate a backup image timestamp with the ISO filename and machine ID.
4. Download the ISO image - Download the created ISO file to a workstation that can write the ISO file to a CD.

5. Create the Recovery CD - Use a CD recording application to write the ISO file *as an image* to a CD. Do not simply copy the ISO file to the CD as a data file.
6. Boot the target machine using the recovery CD - The target machine must be physically connected to a network that provides access to the KServer. No further user interaction is required.

Dynamic Disk Restores

Dynamic storage involves dividing a physical disk into multiple volumes or combining a physical disk with other physical disks to form volumes that are greater in size than any one physical disk. A traditional disk volume is called a "basic" disk volume. BUDR supports the following basic and dynamic backup and restore combinations:

- backup basic disks
- backup dynamic disks
- restore basic volumes to basic disks
- restore basic volumes to dynamic disks
- restore dynamic volumes to basic disks
- restore dynamic volumes to dynamic disks

Note: While Universal Restore supports restoration of dynamic disks to similar hardware, it does not support restoration of dynamics disks to different hardware platforms that require new drivers. To restore to different hardware platforms, you must restore the dynamic disk backup to a basic disk.

Restore Failure

Restores can fail for the following reasons:

- The Image Location points to a local driver letter - When Windows boots, drive letters are automatically assigned to hard drives starting with `C:`. With the disk manager, you can reassign these to any other unused drive letter. For example, you may decide to turn your `D:` drive into `G:` and set the Image Location path to `G:\backups`. The recovery boot process will not know about the driver letter mapping and will assign `D:` to the hard disk. The restore will then fail trying to access `G:\backups`. You can resolve this problem by setting your image location to `D:\backups` prior to selecting the restore options. Restore will then successfully access `D:\backups`.
- Image stored on a USB drive - Similar to the issue above, when the recovery boot process assigns drive letters, it may assign the USB drive a different drive letter than Windows assigned it. You can resolve this problem by setting your Image Location to the new drive letter prior to selecting the restore options. Restore will then successfully access the USB drive.
- Image stored on a network drive - If the remote drive, or the machine hosting the drive, is not turned on, or if the username and password have changed, then the recovery boot process will not be able to access the network drive.
- Unable to establish a network connection - CD Recovery allows the recovery of an image without the need for the user to enter details such as the image to be restored, its location, the password, etc. Instead the machine connects to the KServer to retrieve this information. However, if there is a proxy between the managed machine and the KServer, or DHCP is not enabled, that machine may not be able to establish a network connection to get out to the internet and retrieve the settings. In cases where a DHCP server is not enabled or there is a proxy in place, use Universal Restore *(page 25)*, as there is no way to configure network connection information for CD Recovery.

Create New ISO

Click Create New ISO to create a new ISO image file, if one does not already exist that you can use. Creating a new ISO image file creates a new record in the paging area.

Delete

Click the delete icon to delete an ISO image file record.

Edit

Click the edit icon to change the Title of an ISO image file record.

Share

By default, ISO images are private to the user that created it. You can share an ISO image with other users, user roles, or make the ISO image file public.

Title

A descriptive title of the backup image being restored.

Machine ID

Select a machine ID. The machine ID must specify an Image Location *(page 39)* that contains the backup image you want to restore.

Backup Date

Select the backup image, by date, to restore from.

Universal Restore

Backup > Universal Restore

Universal Restore enables you to restore the backup image of a system. The restore can be to a different hardware platform or to a virtual machine. Universal Restore requires someone at the machine to boot from the CD and navigate through the recovery wizard to restore the backup image. Manual recovery requires a user with knowledge of the Image Location *(page 39)* path and the Image Password *(page 41)* to restore a backup image.

A damaged boot volume may prevent a system from even booting. To restore images to the system partition, requires that the system boot from a separate partition. This recovery CD provides that image. Follow the on screen instructions to create the recovery CD and restore a volume.

ISO Image File Builds

A recovery boot CD is created using an ISO image file that you download and burn to a CD. If you discover the recovery boot CD you are using fails to restore a particular backup image file, try creating a new recovery boot CD using a different build version of the ISO image file. You can display the list of ISO image file versions supported by Kaseya by clicking the hyperlink under `here` in `If there are any problems with the Recovery Boot CD, you may download additional builds here.`

Dynamic Disk Restores

Dynamic storage involves dividing a physical disk into multiple volumes or combining a physical disk with other physical disks to form volumes that are greater in size than any one physical disk. A traditional disk volume is called a "basic" disk volume. BUDR supports the following basic and dynamic backup and restore combinations:

- backup basic disks
- backup dynamic disks
- restore basic volumes to basic disks
- restore basic volumes to dynamic disks
- restore dynamic volumes to basic disks

- restore dynamic volumes to dynamic disks

Note: While Universal Restore supports restoration of dynamic disks to similar hardware, it does not support restoration of dynamics disks to different hardware platforms that require new drivers. To restore to different hardware platforms, you must restore the dynamic disk backup to a basic disk.

Offsite Servers

Backup > Offsite Servers

The Offsite Servers page safely and securely transfers backup images from a LAN to a remote location. Offsite replication transfers all *changes* to files and sub-directories in the Local Server directory to a specified offsite server directory. File transfers are scheduled using Schedule Transfer *(page 34)*. Image Location *(page 39)* directories should be defined as subdirectories of a Local Server directory to be included in these transfers.

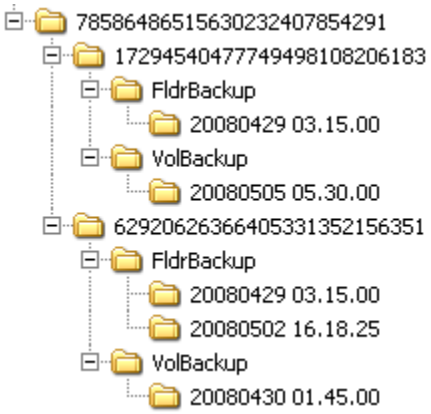
Offsite Server Configuration

Any machine ID may act as an offsite server. You may also have as many offsite servers as you like. Example Offsite Replication configurations include:

- One global offsite server - A local server at each managed LAN pushes data to the global offsite server.
- Multiple offsite servers - Several local servers are assigned to each offsite server. Multiple offsite servers are used to balance the load.
- Cross offsite servers - Supports offsite replication for companies with multiple locations. For example, two company sites each act as the offsite server location for the other company site.

Offsite Folder Structure

The offsite server stores data received from local servers in the directory specified. The top level GUID folder is the GUID of the local server the data is coming from. Second level GUID folders are the GUIDs of the machine IDs being backed up. The following diagram illustrates a typical offsite server directory structure.



File Transfers

Only file changes are pushed to the offsite server. Broken file transfers are automatically restarted at the point left off. Restarting the file transfer from the beginning is not required. Offsite replication uses the same communications technology used in the agent/server communications. All traffic is 256-bit encrypted.

Using the Same Machine for the Local Server and Offsite Server

You may assign the offsite server to be the same machine as the local server, but note the following:

- You'll need to open a port just to replicate across drives, whereas other replication tools can do so locally.
- The files aren't copied offsite. You'll lose the disaster recovery benefit of an offsite backup.

Setting the Name/IP Address and Port

Select a target machine with an agent that will act as the offsite server. The offsite server is always running and listens for connections from local servers using any TCP port you specify. The port cannot be used by any other application. Try using 5722 as it is similar to the agent checkin port. Offsite server ports are restricted to between 1024 and 49151.

You must specify a DNS name or IP address that can be resolved from the local server. Typically, this is the *external* name/IP address of the gateway/firewall/router used by the target machine. Configure port range forwarding on your gateway/firewall/router to direct requests for port 5722—or whatever port number you've chosen—to the internal IP address of the machine ID acting as the offsite server.

> Note: The offsite server must have a credential set to access the network directory receiving data transfers.

Testing the Offsite Configuration

Once you have configured the offsite server, check pending procedures on the offsite server machine:

1. Click the or or icon.
2. Click the Pending Procedures tab on the Machine Summary page.
3. Ensure the `Start Offsite Server` procedure ran successfully.

Try to connect to the offsite server component using Telnet. In the command below replace the string `your.offsiteServer.com` with your Name/IP address. Replace `5722` with the port number you are using.

```
telnet your.offsiteServer.com 5722
```

If the connection is successful you should see only see a blinking cursor. Once you can verify the offsite server is ready, You can configure the Local Servers.

Synthetic Backups

A synthetic full backup is created by consolidating existing incremental or differential backups with the previous full backup image. This is sometimes called an 'Incremental Forever Backup'. Unlike traditional full backups, synthetic full backups are not transferred from the local server to the offsite server. Instead, after the *first* full backup is transferred, only the incremental or differential files are transferred to the offsite server. A synthetic backup component on the offsite server recreates the next full synthetic backup in parallel with the local server. This eliminates the need to transfer full backups between the local server and offsite server. With synthetic backups, bandwidth requirements for transferring full backups are eliminated, but the offsite server's access to its own file server may need to be enhanced to handle the processing of its synthetic backups.

Configuring synthetic backups involves the following steps:

> Note: The first three steps are required even if synthetic backups are not enabled on the offsite server.

1. Install an agent on a local server. Typically the backup image locations of machine IDs being backed up point to the local server.
2. Install an agent on the offsite server.
3. Define a machine ID as an offsite server using Backup > Offsite Servers *(page 26)*.

   > Note: You do not have to install the backup client to a local server or an offsite server.

4. Click the Schedule Install hyperlink on the Backup > Offsite Servers page for the machine ID you want to schedule synthetic support on. A dialog box displays. Schedule the installation of synthetic support components to the offsite server.
5. Schedule volume backups for machine IDs, ensure the Synthetic Full checkbox is checked. These are machine IDs that store backups on local servers that transfer backups to the offsite server you defined above.

Create

Click Create to create an offsite server using the options previously selected.

Select Machine ID

Select the machine ID you want to act as the offsite server.

Name/IP

Enter the IP DNS name or IP address of the offsite server.

Port

Enter an unused port number.

Full path to directory (UNC or local) which receives all data transfers

Enter the full path to the directory, either UNC or local, which receives all data transfers. Do not specify an offsite server directory using a mapped drive.

Check-in status

These icons indicate the agent check-in status of each managed machine:

- Online but waiting for first audit to complete
- Agent online
- Agent online and user currently logged on. Icon displays a tool tip showing the logon name.
- Agent online and user currently logged on, but user not active for 10 minutes
- Agent is currently offline
- Agent has never checked in
- Agent is online but remote control has been disabled
- The agent has been suspended

Note: Different icon images display when this addon module is installed in a 5.x VSA. The Remote Control > Control Machine page displays a legend of the specific icons your VSA system is using.

Delete Icon

Click the delete icon to delete an offsite server record.

Edit Icon

Click a row's edit icon to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

Restart Icon

Click the restart icon to restart a service on a local server or offsite server. You can determine whether this is necessary by displaying the Remote Control > Task Manager process list for a local server or offsite server. You should see `KORepCln.exe` running on the local server and

KORepSrv.exe running on an offsite server. If not, click the restart icon for the respective local server or offsite server. Other symptoms include:

- One local server is inactive and the others are fine: restart local server.
- All local servers are inactive: restart offsite server.

Machine.Group ID

The list of Machine ID.Group IDs.Organization IDs displayed is based on the Machine ID / Group ID / Organization ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.

Name/IP

The DNS name or IP address used by the offsite server.

Port

The port used by the offsite server.

Directory Path

The directory path used by the offsite server.

> Note: Do not specify an offsite server directory using a mapped drive.

Local Servers

Backup > Local Servers

The Local Server page defines the machine ID and directory on the local LAN used to transfer all new files to an Offsite Server *(page 26)*. Offsite replication transfers all *changes* to files and sub-directories in the Local Server directory to a specified offsite server directory. Files transfers are scheduled using Schedule Transfer *(page 34)*. Image Location *(page 39)* directories should be defined as subdirectories of a Local Server directory to be included in these transfers.

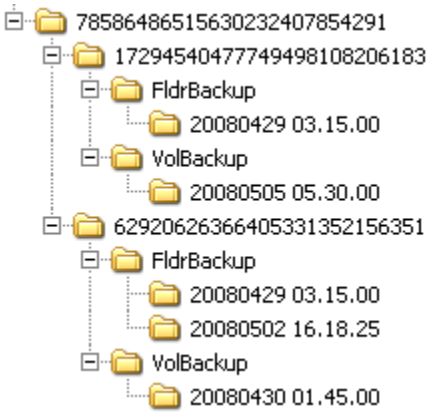
For each local server specify:

- The offsite server to push files to.
- The local directory path to push to the offsite server.
- Optional bandwidth limit.

The local server directory can be a UNC path pointing to a directory on a network file share. Do not specify a local server directory using a mapped drive. The local server must have a credential set in order to access the network.

Offsite Folder Structure

The offsite server stores data received from local servers in the directory specified. The top level GUID folder is the GUID of the local server the data is coming from. Second level GUID folders are the GUIDs of the machine IDs being backed up. The following diagram illustrates a typical offsite server directory structure.



File Transfers

Only file changes are pushed to the offsite server. Broken file transfers are automatically restarted at the point left off. Restarting the file transfer from the beginning is not required. Offsite replication uses the same communications technology used in the agent/server communications. All traffic is 256-bit encrypted.

Using the Same Machine for the Local Server and Offsite Server

You may assign the offsite server to be the same machine as the local server, but note the following:

- You'll need to open a port just to replicate across drives, whereas other replication tools can do so locally.
- The files aren't copied offsite. You'll lose the disaster recovery benefit of an offsite backup.

Create

Click Create to create an local server using the options previously selected.

Select Machine ID

Select the machine ID you want to act as the local server.

Offsite Server

Select the offsite server to transfer backup files to.

Bandwidth Limit

- No Limit - The local server transfers data to the offsite server as fast as possible.
- kBytes/Sec - The local server limits data transfer to the rate specified.

Full path to directory (UNC or local) to push to offsite replication server

Enter the full path to the directory, either UNC or local, which sends data transfers. The local server sends the total contents of this directory to the offsite server. Do not specify a local server directory using a mapped drive.

Check Status

Click Check Status to check the amount of data left to be written to the offsite server immediately. Normally this check is performed only at the end of an active transfer cycle.

Check-in status

These icons indicate the agent check-in status of each managed machine:

- Online but waiting for first audit to complete
- Agent online
- Agent online and user currently logged on. Icon displays a tool tip showing the logon name.
- Agent online and user currently logged on, but user not active for 10 minutes
- Agent is currently offline
- Agent has never checked in
- Agent is online but remote control has been disabled
- The agent has been suspended

Note: Different icon images display when this addon module is installed in a 5.x VSA. The Remote Control > Control Machine page displays a legend of the specific icons your VSA system is using.

Delete Icon

Click the delete icon to delete a local server record.

Edit Icon

Click a row's edit icon to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

Restart Icon

Click the restart icon to restart a service on a local server or offsite server. You can determine whether this is necessary by displaying the Remote Control > Task Manager process list for a local server or offsite server. You should see `KORepCln.exe` running on the local server and `KORepSrv.exe` running on an offsite server. If not, click the restart icon for the respective local server or offsite server. Other symptoms include:

- One local server is inactive and the others are fine: restart local server.
- All local servers are inactive: restart offsite server.

Status

- Active - Indicates files are actively being sent to the offsite server.
- Suspended - The local server is suspended per the schedule set out in Schedule Transfer *(page 34)*.
- At the end of each active cycle, the system checks the local server and reports back the amount of data left to be written.

Offsite Server

The name of the offsite server being sent backup files from this local server.

BW Limit

The bandwidth limit assigned to this local server.

Directory Path

The directory on the local server sending data to the offsite server.

Note: Do not specify a local server directory using a mapped drive.

Offsite Alert

Backup > Offsite Alert

The Offsite Alerts page creates an alert when the specified local server can not connect to its offsite server. Alarms are only generated during the times allowed by Schedule Transfer *(page 34)* for each local server. Once defined, you can apply this alert immediately to any machine ID displayed on this page.

The list of machine IDs you can select depends on the Machine ID / Group ID / Organization ID filter. To display on this page, machine IDs must be defined as a local server using Backup > Local Servers *(page 29)*.

To Create an Offsite Alert

1. Check any of the last three checkboxes to perform their corresponding actions when a offsite alarm is triggered for a machine ID.
   - Create Alarm - This is always checked. Offsite alarms are enabled when an offsite alert is defined on this page.
   - Create Ticket
   - Run Procedure after alarm.
   - Email Recipients
2. Set additional email parameters.
3. Set additional offsite alert specific parameters.
4. Check the machine IDs to apply the alert to.
5. Click the Apply button.

To Cancel a Offsite Alert

1. Select the machine ID checkbox.
2. Click the Clear button.

   The alert information listed next to the machine ID is removed.

Passing Alert Information to Emails and Procedures

The following types of offsite alert emails can be sent and formatted:

- Offsite failed

Note: Changing the email alarm format changes the format for *all* offsite alert emails.

The following variables can be included in your formatted email alerts and in procedures.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<db-view.column>	not available	Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<gr>	#gr#	group ID
<id>	#id#	machine ID
<op>	#op#	offsite replication server ip:port

Create Alarm

If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > Dashboard List, Monitor > Alarm Summary and Reports > Logs > Alarm Log.

Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

Run procedure after alert

If checked and an alarm condition is encountered, a procedure is run. You must click the select script link to choose a procedure to run. You can optionally direct the procedure to run on a specified range of machine IDs by clicking this machine ID link. These specified machine IDs do not have to match the machine ID that triggered the alarm condition.

Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged in user displays in the Email Recipients field. It defaults from System > Preferences.
- Click Format Email to display the Format Alert Email popup window. This window enables you to format the display of emails generated by the system when an alarm condition is encountered. This option only displays for master users.
- If the Add to current list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the Replace list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If Removed is clicked, all email addresses are removed without modifying any alert parameters.
- Email is sent directly from the KServer to the email address specified in the alert. The SMTP service in IIS sends the email directly to the address specified. Set the From Address using System > Configure.

Apply

Click Apply to apply alert parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click Clear to remove all parameter settings from selected machine IDs.

Offsite Alert Parameters

- Check every <N> periods - Specifies how often to check the connection between the local server and the offsite server.
- Alarms if connection fails for <N> periods - Triggers an alarm if the connection fails for greater than the number of periods specified.

Three additional parameters can be set:

- Add - Adds alert parameters to selected machine IDs when Apply is selected without clearing existing parameters.
- Replace - Replaces alert parameters on selected machine IDs when Apply is selected.
- Remove - Clear alert parameters from selected machine IDs. Click the edit icon next to a machine ID group *first* to select the alert parameters you want to clear.

Select All/Unselect All

Click the Select All link to check all rows on the page. Click the Unselect All link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine:

- Online but waiting for first audit to complete
- Agent online
- Agent online and user currently logged on. Icon displays a tool tip showing the logon name.
- Agent online and user currently logged on, but user not active for 10 minutes
- Agent is currently offline
- Agent has never checked in
- Agent is online but remote control has been disabled
- The agent has been suspended

Note: Different icon images display when this addon module is installed in a 5.x VSA. The Remote Control > Control Machine page displays a legend of the specific icons your VSA system is using.

Machine.Group ID

The list of Machine ID.Group IDs.Organization IDs displayed is based on the Machine ID / Group ID / Organization ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.

ATSE

The ATSE response code assigned to machine IDs or SNMP devices:

- A = Create Alarm
- T = Create Ticket
- S = Run Procedure
- E = Email Recipients

Email Address

A comma separated list of email addresses where notifications are sent.

Interval

The number of periods to wait before checking the connection between the local server and the offsite server.

Duration

The number of periods to wait before triggering an alert.

Schedule Transfer

Backup > Schedule Transfer

The Schedule Transfer page specifies the time of day each local server sends files to the offsite server, based on the time zone used by the KServer. You may set different start and end times for each day of the week.

For example, to schedule transfers for all night Tuesday, set the Start Time for Tuesday at 6:00 pm and the End Time for Wednesday at 6:00 am.

The list of machine IDs you can select depends on the Machine ID / Group ID / Organization ID filter. To display on this page, machine IDs must be defined as a local server using Backup > Local Servers *(page 29)*.

Apply

Click Apply to apply weekly schedule settings selected local servers.

Select All/Unselect All

Click the Select All link to check all rows on the page. Click the Unselect All link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine:

- Online but waiting for first audit to complete
- Agent online
- Agent online and user currently logged on. Icon displays a tool tip showing the logon name.
- Agent online and user currently logged on, but user not active for 10 minutes
- Agent is currently offline
- Agent has never checked in
- Agent is online but remote control has been disabled
- The agent has been suspended

Note: Different icon images display when this addon module is installed in a 5.x VSA. The Remote Control > Control Machine page displays a legend of the specific icons your VSA system is using.

Edit Icon

Click a row's edit icon to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

Machine.Group ID

The list of Machine ID.Group IDs.Organization IDs displayed is based on the Machine ID / Group ID / Organization ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.

Weekday Start-End

Displays the start and end times for each day of the week that backup files are transferred from each local server to its offsite server.

Install/Remove: Backup

Backup > Install/Remove

The Install/Remove page installs or uninstalls Acronis backup and disaster recovery (BUDR) software on selected machine IDs. Each BUDR installation on a managed machine uses up one BUDR license. The number of licenses available depends on the total number of licenses purchased and allocated to each group ID using System > License Manager. BUDR licenses are purchased and allocated separately for workstations and servers.

- Backups require additional agent capability so you may be prompted to update the agent prior to installing backup.
- Backup installation requires Windows Installer v3 and up. Your system checks the results from the last audit for v3. Your system will not recognize you have installed the latest Windows Installer until after the next audit runs on that machine.

> Note: BUDR does not support new installs of 9x and NT.

Installing BU-DR Client 9.5

Customers are not required to install the new BU-DR client to keep using backup. BU-DR will work with a mix of BU-DR client versions 9.1 and 9.5 (the new client version). However, in order for the endpoint to take advantage of the new features including encryption, synthetic backup and image conversion, the endpoint must be updated to the new version of the BU-DR client software.

Customers need to update the Kaseya agent to 5.1.0.1 to cancel a backup with the new 9.5 client. Kaseya recommends deploying the new agent to all systems that have the new backup client software. Use the "Force update even if agent is at…" option to force the agent to update to 5.1.0.1.

Installation Requires a Reboot

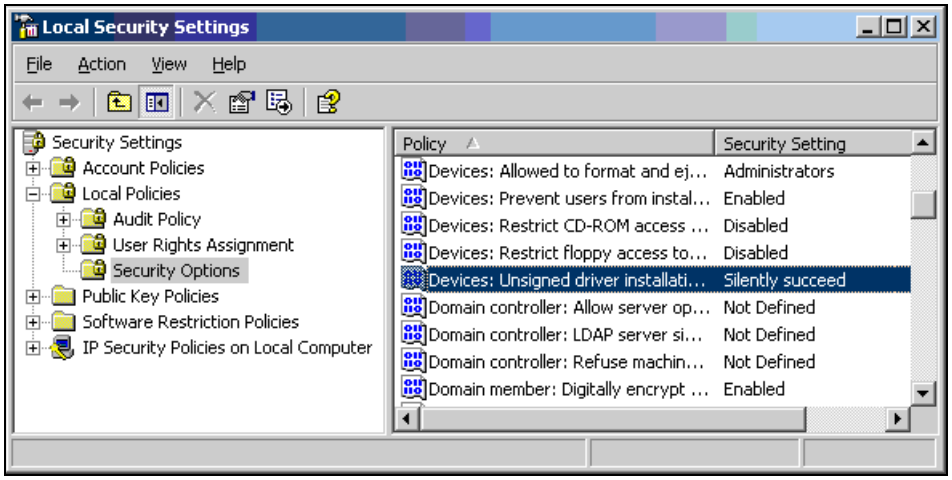
Backup can backup all volumes, including the boot volume, while in use. Backup accomplishes this through the use of a low level driver. As such, backup require a reboot to complete its installation.

- After installation completes, if a user is logged in, the systems asks the user to Reboot Now or Continue Working. If the dialog is not answered within 5 minutes, Continue Working is assumed. If no one is logged in, the system reboots immediately.
- You can avoid displaying this dialog box by clicking the Do not reboot after install checkbox.
- A Reboot Now button displays in the Install column next to a machine ID if Do not reboot after install was checked or the Reboot Now/Continue Working dialog box on the target machine timed out.
- Installing backup on a server when no one is logged in reboots the server when backup installation completes.

If Installation Fails on Windows 2003 Server

By default, Windows 2003 Server warns before installing any low level drivers. To date, Microsoft only signs their own low level drivers. Acronis can only deliver an unsigned driver as part of their backup system. To successfully install on a 2003 server, you must do one of the following:

- Click Yes when asked if it is OK to install the unsigned driver. If this dialog box gets no response in two minutes, then Windows assumes No and blocks the installation.
- Prior to installation, set the Local Group Policy to Silently Succeed for Devices: Unsigned driver installation (see below).



Install/Reinstall

Click Install/Reinstall to install or reinstall backup software on selected machine IDs using the options previously selected.

Date/Time

Enter the year, month, day, hour, and minute to schedule this task.

Cancel

Click Cancel to cancel execution of this task on selected managed machines.

Verify Install

Click Verify Install to confirm the backup software is installed on selected machine IDs. Use this if you suspect someone removed the backup software on managed machines.

Copy backup settings from select machine ID

Click this link to copy the backup configuration and schedules from an existing machine to all selected machines.

Warn if installer pushes from server

If checked, a warning message displays if the backup file is installed from the KServer. The backup install file is over 100MB. Avoid file transfer from the KServer to each machine in a LAN using Patch Management > File Source. Select the File share located on option. Once set, the KServer writes a single copy to the LAN file share. The backup installation runs from that location for all managed machines on that LAN.

Remove

Click Remove to uninstall the backup software from selected machine IDs. A reboot on the machine is required to remove the low level driver and complete the uninstall.

Stagger by

You can distribute the load on your network by staggering this task. If you set this parameter to 5 minutes, then the task on each machine ID is staggered by 5 minutes. For example, machine 1 runs at 10:00, machine 2 runs at 10:05, machine 3 runs at 10:10, ...

Skip if Machine Offline

Check to perform this task only at the scheduled time, within a 15 minute window. If the machine is offline, skip and run the next scheduled period and time. Uncheck to perform this task as soon as the machine connects after the scheduled time.

Do not reboot after install

If checked, selected machine IDs are *not* rebooted after the backup software is installed.

Select All/Unselect All

Click the Select All link to check all rows on the page. Click the Unselect All link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine:

- Online but waiting for first audit to complete
- Agent online

Agent online and user currently logged on. Icon displays a tool tip showing the logon name.

Agent online and user currently logged on, but user not active for 10 minutes

Agent is currently offline

Agent has never checked in

Agent is online but remote control has been disabled

The agent has been suspended

Note: Different icon images display when this addon module is installed in a 5.x VSA. The Remote Control > Control Machine page displays a legend of the specific icons your VSA system is using.

Machine.Group ID

The list of Machine ID.Group IDs.Organization IDs displayed is based on the Machine ID / Group ID / Organization ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.

Installed

This column displays the status of installed software on selected machines:

- Awaiting reboot. A Reboot Now button displays in the Install column next to a machine ID if Do not reboot after install was checked or the Reboot Now/Continue Working dialog box on the target machine timed out.
- Backup does not support Vista at this time.
- Failed to install – unsigned driver installation policy may have blocked install
- Failed to install
- Install pending
- Remove pending
- Remove pending
- Reset Policy pending
- The date and time the backup software successfully installed
- Unsigned driver policy reset
- Update Agent required to support backup
- Verify failed
- Window v3 installer and up required

Version

Displays the version of Acronis backup software installed on the managed machine. If a new version is available, also displays `Update Available`. Latest at the top of the column displays the latest version of backup software available.

Verify

Displays one of the following:

- The date and time the backup software was verified as installed on the machine ID.
- `Verify pending` - Displays with a Cancel button.
- `Not Verified` - Displays with a Verify button.

Type

The type of machine the backup software is installed on:

- Workstation
- Server

Image Location

Backup > Image Location

The Image Location page specifies the folder on a local network or local drive where volume backups and folder backups are stored. Typically this is a path to a LAN based file server such as `\\LAN_Server\Backups\`. But it can also be as simple as another physical drive on the machine, such as a USB drive, or a shared network drive. Writing data to a tape drive is supported. The tape drive must be recognized by the Windows OS as a removable storage device.

- Separate paths may be specified for volume and folder backup paths.
- You can not save the backup image to the same drive you are backing up.
- Mapped drive letters are not supported. The path must be a full UNC path or a local physical drive.
- If a UNC path is specified, a credential must be defined using Agent > Set Credentials that provides access to this UNC path. Without the credential, the machine will *not* have access to the image location and the backup will fail.

> Note: Windows 98 and Windows ME do not support user credentials. You may only use local drive paths for 98 and ME.

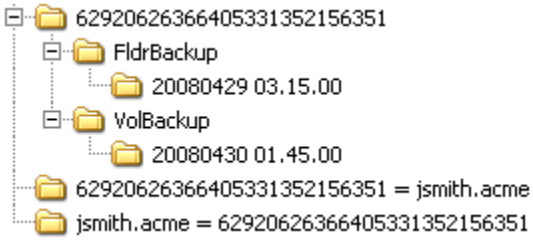
The list of machine IDs you can select depends on the Machine ID / Group ID / Organization ID filter. To display on this page, machine IDs must have backup software installed on the managed machine using the Backup > Install/Remove *(page 35)* page.

Backup Folder Structure

Separate Image Location *(page 39)* paths may be specified for volume and folder backups. Volume backups and folder backups are saved as full backup sets. Each backup set gets its own folder. Backup files have a '*.tib extension.

Backup folders are organized by the GUID used to uniquely identify each machine ID. By using the GUID instead of the machine ID, renaming the machine ID or assigning the machine ID to a different group does not prevent the backup files from becoming unavailable.

Two extra, empty, folders in the same backup image location folder identify the machine ID associated with each GUID. For instance, if you have a machine ID named `jsmith.acme` and its GUID is `629206263664053313521563 51` then folders might be organized as follows in the image location folder:



The first folder contains the backups. The second empty folder identifies the machine ID for a GUID. The third empty folder identifies the GUID for a machine ID. If you have backups for many machine IDs all stored in the same image location folder, you can use either of the two empty cross-reference folders to identify the appropriate GUID backup folder, either by machine ID or by GUID.

Local Servers and Image Locations

If you are going to configure replication using Offsite Servers *(page 26)*, then Image Location *(page 39)*

directories should be defined as subdirectories of a Local Server *(page 26)* directory.

Set

Click Set to set the image locations used for backups for selected machine IDs.

> Warning: Do not change the image location unless you're certain you want to make this change. *Changing* the image location for existing backups forces the scheduling of a new, full, non-synthetic backup. If an offsite server is defined, than the new full non-synthetic backup must be transferred to the offsite server again, even if synthetic backups are enabled. If the previous full and incremental backup files are moved to the new image location, then a new full backup is created the next time a full backup is scheduled. If the previous full and incremental backup files are not found at the new image location, then the new full backup is created the next time an incremental backup is scheduled.

Clear

Click Clear to remove the image location settings from selected machine IDs.

> Note: Clearing an image location for a machine removes any scheduled backups for that machine.

Volume Path / Folder Path

Enter folder paths to store backups.

Auto Refresh

Selecting this checkbox automatically updates the paging area every five seconds.

Check free space

You can check the amount of free space available on any machine's image location directory by checking the desired machine IDs and clicking the Check button. Also use this check to verify the credential is set correctly for the client to access the image location.

> Note: Available free space changes all the time. To prevent showing stale data, reported free space only remains available for 10 minutes after the free space check completes.

Select All/Unselect All

Click the Select All link to check all rows on the page. Click the Unselect All link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine:

- Online but waiting for first audit to complete
- Agent online
- Agent online and user currently logged on. Icon displays a tool tip showing the logon name.
- Agent online and user currently logged on, but user not active for 10 minutes
- Agent is currently offline
- Agent has never checked in
- Agent is online but remote control has been disabled
- The agent has been suspended

Note: Different icon images display when this addon module is installed in a 5.x VSA. The Remote Control > Control Machine page displays a legend of the specific icons your VSA system is using.

Machine.Group ID

The list of Machine ID.Group IDs.Organization IDs displayed is based on the Machine ID / Group ID / Organization ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.

Volume Path / Folder Path

The folder paths specified for each machine ID.

Free Space

The free space available for each machine ID's image location.

Image Password

Backup > Image Password

The Image Password page sets the passwords to access backup files. Folder backup and volume backup .tib files are all password protected using a unique password for each machine ID. This password remains constant for each machine ID. You may set the password to anything you like. The same password may be set on multiple machines.

Warning: If you decide to keep backup files outside of this system, print out the password for each machine ID or you will not be able to recover the backup later. Kaseya can not recover a backup file for you if you lose this password.

The list of machine IDs you can select depends on the Machine ID / Group ID / Organization ID filter. To display on this page, machine IDs must have backup software installed on the managed machine using the Backup > Install/Remove *(page 35)* page.

View Password Log

Displays a history of the backup image passwords assigned to machine IDs.

Change

Click Change to change the backup image password of selected machine IDs to the password entered in Create Password and Confirm Password.

Warning: Do not change the password unless you're certain you want to make this change. *Changing* the password for existing backups forces the scheduling of a new, full, non-synthetic backup. If an offsite server is defined, than the new full non-synthetic backup must be transferred to the offsite server again, even if synthetic backups are enabled. The new password begins to be used the next time a full backup is scheduled.

Enable Password

If checked, backup images are password protected. If blank, backup images are not password protected.

Create Password / Confirm Password

Enter a backup image password.

Suggest Password

Click Suggest Password to populate the Create Password and Confirm Password with a randomly generated alphanumeric string.

Apply

Click Apply to apply encryption options.

Enable Image Encryption

If checked, image encryption provides additional security by encrypting the contents of the `.tib` file. The encryption is enabled in conjunction with the password. Three Advanced Encryption Standard (AES) options are available using cryptographic keys of 128, 192, and 256 bits.

- aes 128
- aes 192
- aes 256

Select All/Unselect All

Click the Select All link to check all rows on the page. Click the Unselect All link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine:

Online but waiting for first audit to complete

Agent online

Agent online and user currently logged on. Icon displays a tool tip showing the logon name.

Agent online and user currently logged on, but user not active for 10 minutes

Agent is currently offline

Agent has never checked in

Agent is online but remote control has been disabled

The agent has been suspended

Note: Different icon images display when this addon module is installed in a 5.x VSA. The Remote Control > Control Machine page displays a legend of the specific icons your VSA system is using.

Machine.Group ID

The list of Machine ID.Group IDs.Organization IDs displayed is based on the Machine ID / Group ID / Organization ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.

Password

The backup image password currently assigned to each machine ID.

Encryption

The encryption standard used to create .tib files.

Folder Backup

Backup > Folder Backup

The Folder Backup page specifies files and folders backed up by Schedule Folders *(page 13)* for each machine ID. You may backup any number of files and folders. You can only specify one file or folder at a time.

You can also exclude specific files from being backed up within these folders. For example, you can exclude `*.avi`, `*.mp3`, and `*.bmp` files when backing up someone's `My Documents` folder.

Folder Backup performs sector level backups. Sector level copying allows the system to backup locked and in-use files so you can safely backup at any time of the day.

The list of machine IDs you can select depends on the Machine ID / Group ID / Organization ID filter. To display on this page, machine IDs must have backup software installed on the managed machine using the Backup > Install/Remove *(page 35)* page.

Include Directories

Click Include Directories to apply Include File or Folder settings to selected machine IDs.

> Note: You cannot include the root directory of a drive, such as `c:` or `c:\`. An error will result during the backup.

Include File or Folder

Specify the full path to the file or folder you wish to back up on selected machine IDs. Paths must point to local drives, not mapped drives or network paths. You can only specify one file or folder at a time. Paths can include commas. For example, you can enter the path `C:\Program Files\Company, Inc\`.

Exclude Files

Specify files or classes of files to exclude from being backed up. Paths are not allowed. Only file names, with or without wild cards, are allowed. For example: `*.jpg`, `outlook.pst`. Click Exclude Files to apply these exclusions to selected machine IDs. You can only specify one file or class of files at a time.

Remove...

Click Remove... to display a dialog box that allows you to select the folders and files to remove from selected machine IDs.

Select All/Unselect All

Click the Select All link to check all rows on the page. Click the Unselect All link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine:

- Online but waiting for first audit to complete
- Agent online
- Agent online and user currently logged on. Icon displays a tool tip showing the logon name.
- Agent online and user currently logged on, but user not active for 10 minutes
- Agent is currently offline
- Agent has never checked in

- Agent is online but remote control has been disabled
- The agent has been suspended

Note: Different icon images display when this addon module is installed in a 5.x VSA. The Remote Control > Control Machine page displays a legend of the specific icons your VSA system is using.

Machine.Group ID

The list of Machine ID.Group IDs.Organization IDs displayed is based on the Machine ID / Group ID / Organization ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.

Path

Lists the paths of files or folders being backed up for each machine ID. Files or classes of files being excluded from backups display in red text.

Backup Alert

Backup > Backup Alert
Monitor > Alerts

Select Backup Alert from the Select Alert Function drop-down list The Backup Alert page creates alerts for backup events on managed machines. The list of machine IDs you can select depends on the Machine ID / Group ID / Organization ID filter. To display on this page, machine IDs must have backup software installed on the managed machine using the Backup > Install/Remove *(page 35)* page.

To Create a Backup Alert

1. Check any of these checkboxes to perform their corresponding actions when a an alarm condition is encountered:
   - Create Alarm
   - Create Ticket
   - Run Agent Procedure
   - Email Recipients
2. Set additional email parameters.
3. Set additional backup alert specific parameters.
4. Check the machine IDs to apply the alert to.
5. Click the Apply button.

To Cancel a Patch Alert

1. Select the machine ID checkbox.
2. Click the Clear button.

   The alert information listed next to the machine ID is removed.

Passing Alert Information to Emails and Procedures

The following types of backup alert emails can be sent and formatted:

- Backup failed
- Verify backup failed
- Recurring backup skipped if machine offline
- Backup Completed Successfully
- Full Backup Completed Successfully

- Image Location free space below

Note: Changing the email alarm format changes the format for all Backup Alert emails.

The following variables can be included in your formatted email alerts and in procedures.

Within an Email	Within a Procedure	Description
<at>	#at#	alert time
<be>	#be#	backup failed error message
<bt>	#bt#	backup type
<db-view.column>	not available	Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<gr>	#gr#	group ID
<id>	#id#	machine ID
<im>	#im#	backup image location
<mf>	#mf#	megabytes free space remaining
<sk>	#sk#	backup skip count

Create Alarm

If checked and an alarm condition is encountered, an alarm is created. Alarms are displayed in Monitor > Dashboard List, Monitor > Alarm Summary and Reports > Logs > Alarm Log.

Create Ticket

If checked and an alarm condition is encountered, a ticket is created.

Run Procedure

If checked and an alarm condition is encountered, a procedure is run. You must click the select script link to choose a procedure to run. You can optionally direct the procedure to run on a specified range of machine IDs by clicking this machine ID link. These specified machine IDs do not have to match the machine ID that triggered the alarm condition.

Email Recipients

If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

- The email address of the currently logged in user displays in the Email Recipients field. It defaults from System > Preferences.
- Click Format Email to display the Format Alert Email popup window. This window enables you to format the display of emails generated by the system when an alarm condition is encountered. This option only displays for master users.
- If the Add to current list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the Replace list radio option is selected, when Apply is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If Removed is clicked, all email addresses are removed without modifying any alert parameters.

- Email is sent directly from the KServer to the email address specified in the alert. The SMTP service in IIS sends the email directly to the address specified. Set the From Address using System > Configure.

Apply

Click Apply to apply alert parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

Clear

Click Clear to remove all parameter settings from selected machine IDs.

Backup Alert Parameters

The system triggers an alarm whenever the system discovers one of four different backup alert conditions for a selected machine ID:

- Any Backup Completed - Alerts when any volume or folder backup completes successfully.
- Full Backup Completed - Alerts when a full volume or folder backup completes successfully.
- Backup Fails - Alerts when a volume or folder backup stops prior to completion for any reason. Typically, backup fails because the machine is turned off mid-backup or because the network connection to the file server referenced by Image Location *(page 39)* is lost.
- Recurring backup skipped if machine offline <N> times - Alerts when Skip if machine offline is set in Schedule Volumes *(page 6)* and the backup is rescheduled the specified number of times because the machine is offline. Use this alert to notify you that backups are not even starting because the machine is turned off at the scheduled volume backup time.
- Image location free space below <N> MB - Alerts when the hard disk being used to store the backups is less than a specified number of megabytes.

Three additional parameters can be set:

- Add - Adds alert parameters to selected machine IDs when Apply is selected without clearing existing parameters.
- Replace - Replaces alert parameters on selected machine IDs when Apply is selected.
- Remove - Clear alert parameters from selected machine IDs. Click the edit icon next to a machine ID group *first* to select the alert parameters you want to clear.

> Note: You may specify different alert email addresses for each backup alert type. This lets you send backup complete alerts to the user and only send failures to the user.

Select All/Unselect All

Click the Select All link to check all rows on the page. Click the Unselect All link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine:

- Online but waiting for first audit to complete
- Agent online
- Agent online and user currently logged on. Icon displays a tool tip showing the logon name.
- Agent online and user currently logged on, but user not active for 10 minutes
- Agent is currently offline
- Agent has never checked in
- Agent is online but remote control has been disabled

- The agent has been suspended

Note: Different icon images display when this addon module is installed in a 5.x VSA. The Remote Control > Control Machine page displays a legend of the specific icons your VSA system is using.

Machine.Group ID

The list of Machine ID.Group IDs.Organization IDs displayed is based on the Machine ID / Group ID / Organization ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.

ATSE

The ATSE response code assigned to machine IDs or SNMP devices:

- A = Create Alarm
- T = Create Ticket
- S = Run Procedure
- E = Email Recipients

Email Address

A comma separated list of email addresses where notifications are sent.

Any Complete

If checked, an alarm is triggered when any backup is completed for this machine ID.

Full Complete

If checked, an alarm is triggered when a full backup is is completed for this machine ID.

Backup Fails

If checked, an alarm is triggered when any backup fails for this machine ID.

Backup Skipped

If checked, an alarm is triggered when any backup is skipped for this machine ID.

Compression

Backup > Compression

The Compression page specifies the compression level used to backup. Higher compression takes longer to complete a backup. Lower compression produces larger backup file sizes. The compression setting effects both folder and volume backup.

The list of machine IDs you can select depends on the Machine ID / Group ID / Organization ID filter. To display on this page, machine IDs must have backup software installed on the managed machine using the Backup > Install/Remove *(page 35)* page.

Sample Compression Ratios

The table below shows the times, reduction and size of a typical Windows XP system drive (C:), with office and other expected applications. These numbers are only a guide and will differ greatly for different types of data. MP3 or other highly compressed files will not compress much, but text or other uncompressed data will compress more.

Backup Type	original	none	normal	high	maximum

Size (GB)	8.78	8.78	6.29	5.74	5.64
% reduction (%)	0	0	28.36	34.62	35.76
Time (mm:ss)	00:00	19:55	16:21	28:41	43:55

Set

Click Set to assign a compression option to selected machine IDs.

Compression Option

- None
- Normal - the default
- High
- Maximum

Select All/Unselect All

Click the Select All link to check all rows on the page. Click the Unselect All link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine:

- Online but waiting for first audit to complete
- Agent online
- Agent online and user currently logged on. Icon displays a tool tip showing the logon name.
- Agent online and user currently logged on, but user not active for 10 minutes
- Agent is currently offline
- Agent has never checked in
- Agent is online but remote control has been disabled
- The agent has been suspended

Note: Different icon images display when this addon module is installed in a 5.x VSA. The Remote Control > Control Machine page displays a legend of the specific icons your VSA system is using.

Machine.Group ID

The list of Machine ID.Group IDs.Organization IDs displayed is based on the Machine ID / Group ID / Organization ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.

Compression

The compression option assigned to each machine ID.

Max File Size

Backup > Max File Size

The Max File Size page applies to volume backups *(page 6)* only. When a volume backup runs, image files of the volume get created. The file size specified in this option is the maximum size of each image file. For example, a volume containing 10 GB of data has been set to run. The image that gets

created for a full backup may be 5 GB. If the max file size is set to 600 MB, the system will create 9 files, 8 that are 600 MB and 1 file with the balance of the data.

If you are going to write the image files to a CD or DVD, select the file size that is appropriate for the media.

Unrestricted file sizes are only supported on NTFS formatted disks. If you select a max file size and modify the default unrestricted value, the largest value supported by the configuration is 2000 MB. This is to support FAT32 formatting on storage devices. If a larger size is desired the only other option is unrestricted.

The list of machine IDs you can select depends on the Machine ID / Group ID / Organization ID filter. To display on this page, machine IDs must have backup software installed on the managed machine using the Backup > Install/Remove *(page 35)* page.

Set

Click Set to assign a Max File Size to selected machine IDs.

Max File Size

Enter the maximum file size allowed for a volume image file. Cannot be larger than 2000 MB.

Select All/Unselect All

Click the Select All link to check all rows on the page. Click the Unselect All link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine:

- Online but waiting for first audit to complete
- Agent online
- Agent online and user currently logged on. Icon displays a tool tip showing the logon name.
- Agent online and user currently logged on, but user not active for 10 minutes
- Agent is currently offline
- Agent has never checked in
- Agent is online but remote control has been disabled
- The agent has been suspended

Note: Different icon images display when this addon module is installed in a 5.x VSA. The Remote Control > Control Machine page displays a legend of the specific icons your VSA system is using.

Machine.Group ID

The list of Machine ID.Group IDs.Organization IDs displayed is based on the Machine ID / Group ID / Organization ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.

Max Size

The maximum file size assigned to each machine ID.

Max Log Age

Backup > Max Log Age

The Max Log Age page specifies the number of days to retain log data for backups. Entries older than the specified maximum are automatically deleted.

A log is created for each machine every time a backup operation runs. The log contains the date, type, duration, result, and description of the backup operation performed.

The list of machine IDs you can select depends on the Machine ID / Group ID / Organization ID filter. To display on this page, machine IDs must have backup software installed on the managed machine using the Backup > Install/Remove *(page 35)* page.

Set

Click Set to assign a maximum number of log days to selected machine IDs.

<N> Days

Enter the maximum number of log days for backups.

Select All/Unselect All

Click the Select All link to check all rows on the page. Click the Unselect All link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine:

- Online but waiting for first audit to complete
- Agent online
- Agent online and user currently logged on. Icon displays a tool tip showing the logon name.
- Agent online and user currently logged on, but user not active for 10 minutes
- Agent is currently offline
- Agent has never checked in
- Agent is online but remote control has been disabled
- The agent has been suspended

Note: Different icon images display when this addon module is installed in a 5.x VSA. The Remote Control > Control Machine page displays a legend of the specific icons your VSA system is using.

Machine.Group ID

The list of Machine ID.Group IDs.Organization IDs displayed is based on the Machine ID / Group ID / Organization ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.

Max Age

The maximum number of log days assigned to each machine ID.

Secure Zone

Backup > Secure Zone

The Secure Zone page installs a 56 MByte hidden boot partition on managed machines. Secure zones are used by Auto Recovery *(page 21)* to boot the managed machine and restore backup volume images without any user interaction. Installing or removing a secure zone requires a reboot of the machine.

Install

Click Install to create a secure zone partition on the selected machines. Installing the secure zone reboots the selected machine.

Remove

Click Remove to uninstall the secure zone from the selected machines. Removing the secure zone reboots the selected machine.

Cancel

Click Cancel to clear a pending task.

Verify

Click Verify to verify an install if you suspect someone removed the backup installation at the managed machine.

Show Partitions

If checked, lists the disk drives and partitions on managed machines.

Select All/Unselect All

Click the Select All link to check all rows on the page. Click the Unselect All link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine:

- Online but waiting for first audit to complete
- Agent online
- Agent online and user currently logged on. Icon displays a tool tip showing the logon name.
- Agent online and user currently logged on, but user not active for 10 minutes
- Agent is currently offline
- Agent has never checked in
- Agent is online but remote control has been disabled
- The agent has been suspended

Note: Different icon images display when this addon module is installed in a 5.x VSA. The Remote Control > Control Machine page displays a legend of the specific icons your VSA system is using.

Machine.Group ID

The list of Machine ID.Group IDs.Organization IDs displayed is based on the Machine ID / Group ID / Organization ID filter and the machine groups the user is authorized to see using System > User Security > Scopes.

Secure Zone

If checked, a secure zone is installed on a managed machine.

Index

A

Auto Recovery • 21

B

Backup • 3
Backup Alert • 44
Backup Logs • 17
Backup Sets • 17
Backup Status • 6
Backup Tab • 4

C

CD Recovery • 23
Compression • 47

E

Explore Folders • 18
Explore Volumes • 18

F

Folder Backup • 43

I

Image Location • 39
Image Password • 41
Image to VM • 20
Install/Remove
    Backup • 35

L

Local Servers • 29

M

Max File Size • 48
Max Log Age • 50

O

Offsite Alert • 32
Offsite Servers • 26

P

Pre/Post Procedure
    Backup • 12

S

Schedule Folders • 13
Schedule Transfer • 34
Schedule Volumes • 6
Secure Zone • 51

U

Universal Restore • 25

V

Verify Images • 19