Kaseya 2

Data Backup

User Guide

Version 6.5 and 2.0

January 23, 2014

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULA as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

Contents

Data Backup Overview

Data Backup (KDB) is an add-on module that backs up selected files and folders either to the Amazon S3 cloud or to your own private storage. Private storage can be configured locally or as private *cloud* storage. The Amazon S3 cloud-based backup service eliminates the cost and maintenance of self-owned backup solutions that provide either too little or too much storage capacity. The private storage option gives you the flexibility to leverage existing investments in storage.

Fee-Based or Private Storage Locations

You can use the storage provider Amazon S3 for an additional billing charge or you can designate agent managed machines as private storage locations for your backups. There is no file size limit to use either type of storage. The private storage server does not have to be on the same local network as the machine being backed up. A private storage server can specify a local drive or a UNC path to external storage such as a NAS device. You only need to specify a DNS name or IP address, port number, and local drive and folder path to access a private storage server. Private storage servers have no associated licensing fees.

- A private storage server is configured using the **Private Storage** *(page 16)* page.
- The Amazon S3 server is enabled using the **Kaseya Cloud Storage** *(page 17)* page.

Cloud Billing Service

The **Data Backup** service is initiated and billed using the Kaseya cloud billing service. Billing information is available on the **Kaseya Portal** *(http://portal.kaseya.net)*. The service includes scheduling and bandwidth options that reduce or prevent backups during peak working hours.

Retention Policy

- 30 days of backup data are retained in the online storage space.
- Incremental backups are only stored if the file has changed.
- If more than 30 incremental backups have been stored, the next backup after the last 30th incremental is a mirror backup (full).
- If an incremental is 80% or more of the size of the file being backed up, a mirror backup (full) is created.
- If a file has not changed for more than 30 days, only the latest version is retained.
- If a file is deleted from the agent, the latest version will be kept offsite indefinitely unless deleted using the **Manage** *(page 8)* function.
- For both cloud and private storage, if **Data Backup** is uninstalled from an endpoint, then all backup data for that endpoint will be removed from the storage server.
- For cloud storage, if the Kaseya agent is uninstalled before uninstalling **Data Backup** on an endpoint, the data will remain on the Amazon S3 server *and you will continue to get billed.*

Install/Remove

The **Install/Remove** page does not install anything on the agent machine being backed up. Rather it enables management of that machine by **Data Backup**. Installation is required to display the machine ID on other **Data Backup** pages.

Backup Profiles

The **Backup Profiles** page defines backup configuration profiles. Each backup profile represents a different set of enabled or disabled backup options, including file types and file locations to be backed up. Include and exclude rules can be defined by file type. **Files and directories are included/excluded using a fixed order of precedence** *(page 14)*.

Changes to a profile affect all machine IDs assigned that profile. Typically different types of machines

require different backup profiles. A sample profile is provided for you. You can't change a sample profile, but you can save it under a new name and make changes to the copy. Backup profile options include bandwidth throttling and CPU throttling performance options.

Backup profiles are optional but highly recommended. The other only method of scheduling an backup requires you to select individual files on a machine. Backup profiles are assigned to a machine ID account using the profile selector in the upper right hand corner of the **Schedule** *(page 4)* page.

Profile Variables

When specifying objects to include or exclude in a profile, enter a % character as the first character to display a list of *profile variables*. Not all profile variables apply to OSX operating systems.

Creating Backups

Use the **Schedule** page to create backups.

1. Select one or more machines IDs.
2. Select a storage server. An Amazon S3 storage server is available if enabled using the **Kaseya Cloud Storage** *(page 17)* page. A *private storage server* only displays if you have designated it using the **Private Storage** *(page 16)* page.
3. Select either **Backup Profile** or **File Selection** or both. You must select at least one of these options.
4. Click **Schedule** or **Backup Now** to schedule the creation of backups for selected machine IDs.

Restoring Backups

The **Restore** page restores selected folders and files from a backup to either the same machine it was backed up from, or a different OS compatible machine. You can choose to overwrite files or create copies of files with the same name. You can choose to restore the files and folders to their original location or to a new location.

Alerts

The **Alerts** page creates alerts in response to the success or failure of **Data Backup** events.

Storage Status

The following pages and reports help you track the status of storage servers and backups.

- **Status** *(page 3)*
- **Logs** *(page 6)*
- **Summary** *(page 8)*
- **Overview** *(page 9)*
- **Data Backup Summary** *(page 17)*
- **Data Backup Usage Over Time** *(page 18)*

> Note: See **Data Backup System Requirements** *(page 3)*.

Functions	Description
Status *(page 3)*	Provides a dashboard view of the status of machine IDs using Data Backup.
Schedule *(page 4)*	Schedules backups for selected machine IDs.
Logs *(page 6)*	Displays logs of all backups and restores you have performed for the last 90 days.
Restore *(page 6)*	Restores selected folders and files from a backup to a selected machine ID.

Manage *(page 8)*	Enables deletion of folders and files from an backup for a selected machine ID.
Summary *(page 8)*	Displays storage statistics for each machine ID being backed up.
Overview *(page 9)*	Displays storage statistics, grouped by private storage server first, then by machine ID.
Install/Remove *(page 9)*	Enables or removes Data Backup for selected machines IDs.
Backup Profiles *(page 10)*	Defines backup configuration profiles.
Alerts *(page 14)*	Defines alerts for backup events.
Private Storage *(page 16)*	Specifies managed machines as private storage servers.
Kaseya Cloud Storage *(page 17)*	Enables Amazon S3 cloud storage.

Data Backup System Requirements

Kaseya Server
- The Data Backup 6.5 module requires VSA 6.5.

Requirements for Each Managed Machine
- Microsoft Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2
- Microsoft Windows XP, Vista, 7, 8, 8.1
- Apple OS X 10.5 through 10.9 - Intel only

Requirements for Each Private Storage Server
- Microsoft Windows XP, Vista, 7, 8
- Microsoft Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012
- An agent is required on a private storage server.
- Ensure sufficient disk capacity exists on a private storage server to meet your endpoint storage requirements.

Note: See general **System Requirements** *(http://help.kaseya.com/WebHelp/EN/System-Requirements.asp)*.

Status

Data Backup > Backup > Status

The **Status** page provides a dashboard view of the status of machine IDs using backup.

The **Backup Status** pane displays a pie chart showing complete, completed with exceptions, skipped, failed, partial failure, in progress, and unscheduled backups. Partial failures indicate some files may not be backed up. Click any slice of the pie chart or any label of the pie chart to display a list of individual machines belonging to that slice.

> Note: Backups may be `Skipped` if the connection was down temporarily. `Complete with Exceptions` can indicate a critical problem with the backup. In both cases, a description of the issue is displayed on the **Status** page and the **Logs** *(page 6)* page.

Statistics are filtered in two ways:

- **Backup Status for the last <N> <periods>** - Limits statistics to the range of time selected.
- **Machine ID/group ID filter** - Limits statistics to the backup machines specified by the machine ID/group ID filter.

> Note: Machines IDs only display on this page if **Data Backup** has been **installed** *(page 9)*. The list of machine IDs you can select depends on the machine ID / group ID filter.

Select hyperlinked non-zero numbers in the **Skipped** column to display entries in the **Logs** *(page 6)* page for each machine.

Schedule

Data Backup > Backup > Schedule

The **Schedule** page schedules backups for selected machine IDs.

1. Select one or more machines IDs.
2. Select a storage server. An Amazon S3 storage server is available if enabled using the **Kaseya Cloud Storage** *(page 17)* page. A *private storage server* only displays if you have designated it using the **Private Storage** *(page 16)* page.
3. Select either **Backup Profile** or **File Selection** or both. You must select at least one of these options.
4. Click **Schedule** or **Backup Now** to schedule the creation of backups for selected machine IDs.

> Note: Machines IDs only display on this page if **Data Backup** has been **installed** *(page 9)*. The list of machine IDs you can select depends on the machine ID / group ID filter.

Retention Policy

- 30 days of backup data are retained in the online storage space.
- Incremental backups are only stored if the file has changed.
- If more than 30 incremental backups have been stored, the next backup after the last 30th incremental is a mirror backup (full).
- If an incremental is 80% or more of the size of the file being backed up, a mirror backup (full) is created.
- If a file has not changed for more than 30 days, only the latest version is retained.
- If a file is deleted from the agent, the latest version will be kept offsite indefinitely unless deleted using the **Manage** *(page 8)* function.
- For both cloud and private storage, if **Data Backup** is uninstalled from an endpoint, then all backup data for that endpoint will be removed from the storage server.
- For cloud storage, if the Kaseya agent is uninstalled before uninstalling **Data Backup** on an endpoint, the data will remain on the Amazon S3 server *and you will continue to get billed.*

Actions

- **Schedule** - Click **Schedule** to display the **Scheduler** window, which is used throughout the VSA to schedule a task. Schedule a task once or periodically. Each type of recurrence—Continuous, Once, Minutes, Hourly, Daily, Weekly, Monthly—displays additional options appropriate for that

type of recurrence. Periodic scheduling includes setting start and end dates for the recurrence. Not all options are available for each task scheduled. Options can include:

- ➢ **Continuous** - File changes are backed up within 10 minutes. New files are backed up within 24 hours.
- ➢ **Distribution Window** - Reschedules the task to a randomly selected time no later than the number of periods specified, to spread network traffic and server loading. For example, if the scheduled time for a task is 3:00 AM, and the distribution window is 1 hour, then the task schedule will be changed to run at a random time between 3:00 AM and 4:00 AM.
- ➢ **Skip if offline** - If checked and the machine is offline, skip and run the next scheduled period and time. If blank and the machine is offline, run the task as soon as the machine is online again.
- ➢ **Power up if offline** - Windows only. If checked, powers up the machine if offline. Requires Wake-On-LAN or vPro and another managed system on the same LAN.
- ➢ **Exclude the following time range** - **Applies only to the distribution window.** If checked, specifies a time range to exclude the scheduling of a task within the distribution window. Specifying a time range outside of the distribution window is ignored by the scheduler.

- ▪ **Backup Now** - Schedules an backup immediately.
- ▪ **Cancel** - Clears pending backups for selected machine IDs. Does not clear backups that have already started.
- ▪ **Apply Storage Server** - Select a storage server to apply to selected machine IDs.
  - ➢ A private storage server only displays if you have designated it using the **Private Storage** *(page 16)* page.
  - ➢ Amazon S3 server displays if you have enabled it using the **Kaseya Cloud Storage** *(page 17)* page.
- ▪ **Apply Profile** - Select a profile to apply to selected machine IDs.

> Note: You must apply a backup profile or use file selection or both to specify the folders and files to backup.

- ▪ **Remove** - Remove a profile, remove a file selection or remove both from selected machine IDs.

Machine ID

The list of Machine IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to see using System > User Security > Scopes. Also, machines IDs only display on this page if backup has been **installed** *(page 9)*.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent Quick View window.

- 🟢 Online but waiting for first audit to complete
- 🟢 Agent online
- 🔵 Agent online and user currently logged on.
- 🔵 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

Backup Profile

The **backup profile** *(page 10)* assigned this machine ID.

Storage Server

The storage server assigned to this machine ID.

File Selection

Optionally click the File Selection icon for a machine ID to select folders and files not specified by the backup profile. **Files and directories are included/excluded using a fixed order of precedence** *(page 14)*.

Recurrence

Indicates if a backup is scheduled and whether it's recurring or not. If recurring, indicates the pattern of the recurrence.

Next Backup

Displays the scheduled date and time for the next backup. Overdue date/time stamps display as <mark>red text with yellow highlight</mark>.

Logs

Data Backup > Backup > Logs

The **Logs** page displays a list of all backups you have performed for the last 90 days. Click a machine ID to display a log containing the time, date, duration, result, and exception count.

One of several kinds of results, displays in the **Results** column.

- `Skipped` - Backups may be skipped if the connection was down temporarily.
- `Canceled` - The backup was canceled.

For the following results, clicking the link provides additional information.

- `Complete with Exceptions` - Indicates a critical problem with the backup.
- `Complete` - Lists the files that have been backed up and the unchanged files that did not require a backup.
- `Partial Failure` - Lists the files that may not have been backed up successfully.

> Note: Machines IDs only display on this page if **Data Backup** has been **installed** *(page 9)*. The list of machine IDs you can select depends on the machine ID / group ID filter.

Restore

Data Backup > Recovery > Restore

The **Restore** page restores selected folders and files from a backup to either the same machine it was backed up from, or a different OS compatible machine. You can choose to overwrite files or create copies of files with the same name. You can choose to restore the files and folders to their original location or to a new location.

> Note: Restores may be **Skipped** if the connection was down temporarily. **Complete with Exceptions** can indicate a critical problem with the restore. In both cases, a description of the issue is displayed on the **Logs** *(page 6)* page.

> Note: Machines IDs only display on this page if **Data Backup** has been **installed** *(page 9)*. The list of machine IDs you can select depends on the machine ID / group ID filter.

Retention Policy

- 30 days of backup data are retained in the online storage space.
- Incremental backups are only stored if the file has changed.
- If more than 30 incremental backups have been stored, the next backup after the last 30th incremental is a mirror backup (full).
- If an incremental is 80% or more of the size of the file being backed up, a mirror backup (full) is created.
- If a file has not changed for more than 30 days, only the latest version is retained.
- If a file is deleted from the agent, the latest version will be kept offsite indefinitely unless deleted using the **Manage** *(page 8)* function.
- For both cloud and private storage, if **Data Backup** is uninstalled from an endpoint, then all backup data for that endpoint will be removed from the storage server.
- For cloud storage, if the Kaseya agent is uninstalled before uninstalling **Data Backup** on an endpoint, the data will remain on the Amazon S3 server *and you will continue to get billed.*

Restore Status

The restore status of a machine ID is indicated by icons and whether text is enabled or disabled.

- No backup files exist for this machine ID. The name of the machine ID displays in *gray italics*.

- Backup files exist and can be restored on this machine ID or to a different OS-compatible machine. The name of the machine ID displays in *enabled text*.

- Backup files exist but the machine is offline. Backup files can only be restored to a *different* machine.

Restore a Backup from an *Online* Machine

1. Select a machine ID showing a ☁ icon and *enabled text* in the middle pane of the Data Backup > **Restore** page.
2. Use the **Select Backup Instance** drop-down list to select the date and time of an existing backup.
3. Click **My Computer** to expand the folder tree. The folder tree displays the folders and files that were included in the backup instance you selected.
4. Select the folders and files you want to restore.
5. Optionally check **Overwrite existing files**.
6. Choose the **Restore To** location on the *original* machine to restore the backup to. Leaving this field blank restores the files to their original location. You can enter in a different path location on the original machine if you like. UNC paths are not supported. Whatever location is specified, you can choose to:
   - **Replace file if it exists** in the specified location.
   - **Rename file if it exists** in the specified location.
7. Perform *either one* of the following to schedule the restore.
   - Click the **Restore** button to restore the file to the original machine, or
   - Click the **Select Target** button to restore to a different OS compatible machine.
     - ✓ A list of OS-compatible alternate machines displays in a popup window.
     - ✓ You can filter this list by specifying a machine ID or machine group, then clicking the **Update** button.
     - ✓ Select a machine.

Restore a Backup from an *Offline* Machine

You can still restore a backup to another machine if the original machine is *offline*.

1. Select an *offline* machine ID showing ⬤ 🖳 icons and *enabled text* in the middle pane of the Online Backup > **Restore** page.
   - ➢ A list of OS-compatible alternate machines displays in a popup window.
   - ➢ You can filter this list by specifying a machine ID or machine group, then clicking the **Update** button.
   - ➢ Select a machine.
2. Select an alternate machine.
3. Use the **Select Backup Instance** drop-down list to select the date and time of an existing backup.
4. Click **My Computer** to expand the folder tree. The folder tree displays the folders and files that were included in the backup instance you selected.
5. Select the folders and files you want to restore.
6. Optionally check **Overwrite existing files**.
7. Choose the **Restore To** location on the *alternate* machine to restore the backup to. Leaving this field blank restores the files to the original backup path location on the alternate machine. You can enter in a different path location on the alternate machine if you like. UNC paths are not supported. Whatever location is specified, you can choose to:
   - ➢ **Replace file if it exists** in the specified location.
   - ➢ **Rename file if it exists** in the specified location.
8. Click **Restore to <machine ID>** to schedule the restore to the alternate machine.

Manage

Data Backup > Recovery > Manage

The **Manage** page delete files and folders from the cloud storage space, for the selected machine ID. Select one or more files or folders director in the right hand pane. Then click the **Delete** button at the bottom of the page.

The backup instance selector allows you to see which files were stored at the time of the specified backup. **All instances of selected files are deleted from storage, regardless of which backup instance is selected.**

> Note: Machines IDs only display on this page if **Data Backup** has been **installed** *(page 9)*. The list of machine IDs you can select depends on the machine ID / group ID filter.

Summary

Data Backup > Storage > Summary

The **Summary** page displays storage statistics for each machine ID being backed up. These statistics include the date and time of the last backup, the *compressed* size of the last backup and the total *compressed* size of all files being stored.

> Note: Machines IDs only display on this page if **Data Backup** has been **installed** *(page 9)*. The list of machine IDs you can select depends on the machine ID / group ID filter.

Columns

- ▪ **Machine ID -** The machine ID of the managed machine being backed up.
- ▪ **Storage Server** - The storage server used by this machine ID.
- ▪ **Last Backup** - The date/time of the last backup for this machine ID.
- ▪ **Last Backup Size** - The compressed size of the last backup for this machine.
- ▪ **Storage Summary** - The compressed size of all backups for this machine.
- ▪ **Efficiency Factor** - The ratio of the original backup size to the compressed backup size, expressed as a multiple, for this machine ID.
- ▪ **Restore Rate** - The average rate backups were restored to this machine ID.

Overview

`Data Backup > Storage > Overview`

The **Overview** page displays storage statistics, grouped by private storage server first, then by machine ID. These statistics include the number of files stored and the *original* and *compressed* size of files being stored.

> Note: Only machines defined as **Data Backup** storage machines display on this page. The list of machines displayed depends on the machine ID / group ID filter and machine groups the user is authorized to see using System > Scope.

Columns Displayed for Each Storage Server

- ▪ **Storage Server** - The machine ID for the storage server.
- ▪ **Restore Time** - The time required for this storage server to restore backups.
- ▪ **Restore Rate (MB/Sec)** - The average rate backups were restored using this storage server.
- ▪ **Number of Files** - The number of files backed up by this storage server.
- ▪ **Raw Backup Size** - The original size of all files and folders backed up by this storage server.
- ▪ **Actual Backup Size** - The compressed size of all files an folders backed up by this storage server.
- ▪ **Efficiency Factor** - The ratio of the original backup size to the compressed backup size, expressed as a multiple.

Columns Displayed for Each Machine

- ▪ **Agent** - The machine ID of the agent machine.
- ▪ **Restore Time** - The time required restore backups to this agent machine.
- ▪ **Restore Rate (MB/Sec)** - The average rate backups were restored to this agent machine.
- ▪ **Number of Files** - The number of files backed up for this agent machine.
- ▪ **Raw Backup Size** - The original size of all files and folders backed up for this agent machine.
- ▪ **Actual Backup Size** - The compressed size of all files an folders backed up for this agent machine.
- ▪ **Efficiency Factor** - The ratio of the original backup size to the compressed backup size, expressed as a multiple.

Install/Remove

`Data Backup > Configure > Install/Remove`

The **Install/Remove** page does not install anything on the agent machine being backed up. Rather it

enables management of that machine by **Data Backup**. Installation is required to display the machine ID on other **Data Backup** pages.

Operating systems supported:

Kaseya Server

- The Data Backup 6.5 module requires VSA 6.5.

Requirements for Each Managed Machine

- Microsoft Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2
- Microsoft Windows XP, Vista, 7, 8, 8.1
- Apple OS X 10.5 through 10.9 - Intel only

Backups are created using the **Schedule** *(page 4)* page.

Actions

- **Install** - Enables the **Data Backup** functionality for selected machines IDs.
- **Remove** - Removes **Data Backup** functionality from selected machines.

> Warning: Removal also deletes all backup data stored in the cloud.

- **Auto Refresh** - Selecting this checkbox automatically updates the paging area every five seconds.

Machine ID

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

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent Quick View window.

- ◉ Online but waiting for first audit to complete
- ◯ Agent online
- ◉ Agent online and user currently logged on.
- ◉ 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

Installed

The **Data Backup** install status of each machine ID.

Backup Profiles

Data Backup > Configure > Backup Profiles

The Backup Profiles page defines backup configuration profiles. Each backup profile represents a different set of enabled or disabled backup options, including file types and file locations to be backed up. Include and exclude rules can be defined by file type. **Files and directories are included/excluded using a fixed order of precedence** *(page 14)*.

Changes to a profile affect all machine IDs assigned that profile. Typically different types of machines require different backup profiles. A sample profile is provided for you. You can't change a sample profile, but you can save it under a new name and make changes to the copy. Backup profile options

include bandwidth throttling and CPU throttling performance options.

Backup profiles are optional but highly recommended. The other only method of scheduling an backup requires you to select individual files on a machine. Backup profiles are assigned to a machine ID account using the profile selector in the upper right hand corner of the **Schedule** *(page 4)* page.

Retention Policy

- 30 days of backup data are retained in the online storage space.
- Incremental backups are only stored if the file has changed.
- If more than 30 incremental backups have been stored, the next backup after the last 30th incremental is a mirror backup (full).
- If an incremental is 80% or more of the size of the file being backed up, a mirror backup (full) is created.
- If a file has not changed for more than 30 days, only the latest version is retained.
- If a file is deleted from the agent, the latest version will be kept offsite indefinitely unless deleted using the **Manage** *(page 8)* function.
- For both cloud and private storage, if **Data Backup** is uninstalled from an endpoint, then all backup data for that endpoint will be removed from the storage server.
- For cloud storage, if the Kaseya agent is uninstalled before uninstalling **Data Backup** on an endpoint, the data will remain on the Amazon S3 server *and you will continue to get billed.*

Actions

- **New** - Create a new profile.
- **Save** - Save changes to selected profile.
- **Save As** - Save a selected profile under a new name.
- **Rename** - Rename a selected profile.
- **Delete** - Delete a selected profile.

File Rules

> Note: When specifying objects to include or exclude in a profile, enter a % character as the first character to display a list of **profile variables** *(page 12)*. Not all profile variables apply to OSX operating systems.

Include   Files and Folders

Specify the types of files to include.

- **Include File Type** - Enter file type extensions separated by a space. Example. `DOC TXT PDF HTML`
- **Include Folder** - Enter the path of a folder to include.
- **Include File** - Enter the full path of a file to include.
- **Exclude files greater than <N> megabytes** - Enter the number of megabytes.

Exclude Files and Folders

Files and directories are included/excluded using a fixed order of precedence *(page 14)*.

- **Exclude File Type** -   Enter file type extensions separated by a space. Example. `DOC TXT PDF HTML`
- **Exclude Folder** - Enter the full path of the folder to exclude.
- **Exclude File** - Enter the full path of the file to exclude.

Performance

- ■ **Enable Bandwidth Throttling** - If checked, bandwidth throttling is enabled, using the options you specify below.
  - ➤ **Limit the transfer to a percentage of the total network connection** - Select or enter the percentage of network connection bandwidth allocated to backups.
  - ➤ **Throttle all day long / Throttle between the following hours** - Select when bandwidth throttling occurs during the day or night.
- ■ **Enable CPU Throttling** - If checked, CPU throttling is enabled using the options below.
  - ➤ **Limit the amount of CPU as a percentage utilized by backup** - Limit the percentage of CPU allocated to **Data Backup**.
  - ➤ **Throttle all day long / Throttle between the following hours** - Select when CPU throttling occurs during the day or night.

Share Profile

Choose to make the profile public or assigned only to your user role.

- ■ **Public** - All users can view, edit or share this profile.
- ■ **Private** - Access to this profile is limited to master role users and users belonging to your role.

Lifespan Policies

When **Selective Lifespan** is enabled, files older than a specified time period are deleted from *storage* during the next backup if they have been excluded from being backed up or deleted from the disk. This ensures a "grace period" is maintained for deleted files, while still reducing storage requirements overall. This applies to the backups of all agent machines managed by this profile.

> Warning: *Enabling this feature can result in the automatic deletion of backups in storage!* If enabled, ensure recurring backup schedules run more frequently than the **Storage Expiration** time period specified.

- ■ **Enable Selective lifespan policy** - If checked, files older than the days specified by the **Storage Expiration** field are deleted from *storage* during the next backup if they have been excluded from being backed up or deleted from the disk.
- ■ **Storage Expiration (5-60 days)** - Defaults to 30 days.

Restore Horizon

This option is always enabled. Full and incremental backups older than the Restore Horizon are consolidated to create a single backup instance nearest the restore horizon. Multiple backup instances prior to the restore horizon are removed. Valid values for the restore horizon are between 15 and 120 days.

- ■ **Restore Horizon (15-120 days)** - Defaults to 30 days.

Incremental Backup Count

This option is always enabled. The Incremental Backup Count controls how many incremental backups are allowed between full backups of a file. This value is applied per file. Once a file has the maximum number of incremental backups, a full backup is performed.

- ■ **Incremental Backup Count (0-30)** - Defaults to 30 days. If 0, every backup results in a full file backup.

Profile Variables

When specifying objects to include or exclude in a profile, enter a % character as the first character to display a list of *profile variables*. Not all profile variables apply to OSX operating systems. **Files and directories are included/excluded using a fixed order of precedence** *(page 14)*.

Windows OS

User Environment Vars.

- `%AppData%` - The user-specific AppData directory
- `%Desktop%` - The user-specific Desktop directory
- `%Favorites%` - The user's favorites are stored in this directory
- `%LocalApplicationData%` - The user-specific Local AppData directory.
- `%MyMusic%` - The user's "My Music" directory
- `%MyPictures%` - The user's "My Pictures" directory
- `%Personal%` - The user's "My Documents" directory
- `%MyDocuments%` - The user's "My Documents" directory
- `%UserProfile%` - The user's "Profile" or "Home" directory.
- `%Programs%` - The user's Start Menu programs
- `%UserName%` - The user's login name (not the user's full name)

System Env Vars.

- `%CommonApplicationData%` - The All User's AppData directory
- `%CommonDesktop%` - The All User's Desktop directory
- `%CommonDocuments%` - The All User's Documents directory
- `%CommonProgramFiles%` - The All User's Common Files directory
- `%CommonStartMenu%` - The All User's Start Menu items directory
- `%WinDir%` - Where Windows is installed
- `%ComputerName%` - The name of the computer. On a domain, the qualified name
- `%System%` - Where the system files are installed
- `%Profiles%` - Where the system keeps user directories.
- `%ProgramFiles%` - Where the system keeps its programs

OSX

User Env Vars

- `%Desktop%` - The user's `\Desktop` directory
- `%MyMusic%` - The user's `\Music` directory.
- `%MyPictures%` - The user's `\Pictures` directory.
- `%MyDocuments%` - The user's `\Documents` directory.
- `%Programs%` - The users's `\Library` directory.
- `%UserName%` - The user's login name (not the user's full name)

System Env Vars

- `%CommonProgramFiles%` - The `\Library` directory
- `%WinDir%` - The `\Bin` directory.
- `%ComputerName%` - The name of the computer. On a domain, the qualified name
- `%System%` - The `\System` directory.
- `%ProgramFiles%` - The `\Applications` directory.

Including/Excluding Files and Directories

Data Backup uses the following order of precedence for including and excluding files and directories. The lower the number, the higher the priority. These include/exclude priorities apply to any combination of the two methods of including/excluding files and directories:

- Directory and file selection using the explorer tree on the **Schedules** *(page 4)* page.
- Selections made to user profiles in the **Backup Profiles** *(page 10)* page.

Type of Profile Entry	Precedence priority
Include File	1
Exclude size > X	2
Exclude File Type*	3
Exclude File	4
Include Folder	5
Exclude Folder	6
Include File Type*	7

* Environment variables work like include/exclude file types as well.

> Note: See examples in the **knowledge base**
> *(http://community.kaseya.com/kb/w/wiki/including-excluding-files-and-directories-in-kob-and-kdb.aspx)*.

Alerts

Data Backup > Configure > Alerts

The **Alerts** page creates alerts in response to the success or failure of **Data Backup** events.

> Note: Machines IDs only display on this page if **Data Backup** has been **installed** *(page 9)*. The list of machine IDs you can select depends on the machine ID / group ID filter.

To Create an Alert

1. Check any of these checkboxes to perform their corresponding actions when an alert condition is encountered:
   - Create **A**larm
   - Create **T**icket
   - Run **S**cript
   - **E**mail Recipients
2. Set additional email parameters.
3. Select one of the following:
   - Alert on Data Backup Complete
   - Alert on Data Backup Completed with Exceptions
   - Alert on Data Backup Skipped

> ➢ Alert on Data Backup Storage Used X GB
> ➢ OnlineBackupMonitorService Failure

4. Check the machine IDs to apply the alert settings to.
5. Click **Apply** to assign the alert settings to selected machine IDs.

To Copy Alert Settings

1. Select copy all settings from.
2. Click **(click to select)** to select the **Data Backup** managed machine to copy alert settings from.
3. Check the machine IDs to apply the alert settings to.
4. Click **Apply** to assign the alert settings to selected machine IDs.

Create Alarm

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

Create Ticket

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

Run Agent Procedure

If checked and an alert condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an agent procedure to run. You can optionally direct the agent 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 encountered the alert condition.

Send email to

If checked and an alert condition is encountered, emails are sent to the specified email addresses.

- 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 **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > Outbound Email.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent Quick View window.

- ◑ Online but waiting for first audit to complete
- ◯ Agent online
- ◉ Agent online and user currently logged on.
- ◉ 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

Machine.Group ID

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

Alert Name

Lists the alerts possible for each machine ID.

Responses

The ATSE response code assigned to each alert for each machine IDs:

- A = Create **A**larm
- T = Create **T**icket
- S = Run **S**cript
- E = **E**mail Recipients

Agent Procedure to Run

The agent procedure to run, if this alert condition occurs.

Agent Procedure to On

The machine ID the agent procedure is run on, if this alert condition occurs.

Email To

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

Private Storage

`Data Backup > Configure > Private Storage`

The **Private Storage** page specifies agent machines as private storage servers. The private storage server does not have to be on the same local network as the machine being backed up. A private storage server can specify a local drive or a UNC path to external storage such as a NAS device. You only need to specify a DNS name or IP address, port number, and local drive and folder path. There is no file size limit for storage. Private storage servers have no associated licensing fees. You do not have to install **Data Backup** on the machine designated as the private storage server.

> Note: The list of machine IDs you can select depends on the machine ID / group ID filter.

To Create Private Storage

1. Select a machine in the middle pane.
2. Enter the following storage credentials:
   - ➢ **IP Address** - The IP address used to contact the storage server.
   - ➢ **Port** - The inbound port used to contact the storage server. Use any port number not used by another process.
   - ➢ **Backup Location** - The drive and folder path on a storage server to store backups. The folder path must exist on the storage server. It will not be automatically created for you. Example: `c:\databackups`

Columns

- **Machine ID** - The name for this machine's agent in the VSA.
- **Storage** - If a server icon 🖥 displays, this machine is being used as a private storage server.
- **Available Capacity** - The total amount of free space on the machine ID.
- **Uptime** - The percentage of time a managed machine has been up.

Kaseya Cloud Storage

`Data Backup > Configure > Kaseya Cloud Storage`

Kaseya leverages the power of Amazon S3 based storage to make storing your data in the Cloud both simple and secure. Amazon's storage provides a highly reliable and robust repository for your data, ensuring peace of mind for data availability and also compliance to important industry standards.

You have two options:

- **Trial Storage**
- **Start Using Paid Storage**

Trial Storage

You can start trialing **Kaseya Cloud Storage** straight away—the trial begins when you start backing up. By clicking the **Trial Storage** button you will add the Amazon S3 storage option to your **Apply Storage Server** options on the **Schedule** *(page 4)* page.

You can store as much data as you like during the trial. At the end of the trial your data will be securely erased unless you choose to activate your storage and turn it into a paid account. If you choose to activate you can continue to use the data you have already stored.

Start Using Paid Storage

To go live with **Kaseya Cloud Storage** and start using it today all you need to do is activate it with a credit card. You won't be charged until you start storing data.

You will need to log on to your **Kaseya Help Desk** *(https://helpdesk.kaseya.com/home)* account and register a credit card to activate. If you don't already have a Kaseya account you will need your Client ID and call Customer Service to create a logon.

> **Note:** To avoid being charged for **Kaseya Cloud Storage** that you no longer require, you must make sure you first uninstall any components from machines that are using Kaseya Cloud Storage before you uninstall Kaseya agents (e.g. Kaseya Data Backup agents). This will trigger a deletion of the data stored in the Cloud at the end of the billing cycle and any associated charges for that data will cease. If you uninstall the Kaseya agent first, the data will not be removed and you will continue to be charged for any previously stored data, as the storage system will assume you want to keep it.

Data Backup Summary

`Info Center > Reporting > Reports > KOB - Data Backup Summary`
- Displays only if the Data Backup add-on module is installed.

The **Data Backup Summary** report definition generates a summary report of **Data Backup** activities by machine ID.

Configure your report definition using the following parameters:

Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Number Of Days** - Applies only if `Last N Days` is selected time range type.
- **Custom Start DateTime** - Applies only if `Fixed Range` is select time range type.

- **Custom End DateTime** - Applies only if `Fixed Range` is select time range type.

Parameters

- **Include Machines with No Data** - If checked, includes machines that have no backups.
- **Show Detail** - If checked, displays all backup activities for a machine. If blank, only the last backup activity is displayed.

Data Backup Usage Over Time

`Info Center > Reporting > Reports > KOB - Data Backup Usage Over Time`
- `Displays only if the` Data Backup `add-on module is installed.`

The **Data Backup Usage Over Time** report definition generates a report of **Data Backup** usage by time period.

Configure your report definition using the following parameters:

Time Selection

- **Select the Time Range Type** - Filters by a fixed type of date range.
- **Number Of Days** - Applies only if `Last N Days` is selected time range type.
- **Custom Start DateTime** - Applies only if `Fixed Range` is select time range type.
- **Custom End DateTime** - Applies only if `Fixed Range` is select time range type.

Parameters

- **Include Machines with No Data** - If checked, includes machines that have no backups.
- **Select the Time Period** - `Daily`, `Weekly`, `Monthly`, `Quarterly`, `Yearly`.
- **Select the Usage Type** - `Show Peak Usage`, `Show Average Usage`.

Index