



StorageCraft Cloud Services User Guide

StorageCraft Copyright Declaration

StorageCraft ImageManager, StorageCraft ShadowProtect, StorageCraft Cloud, and StorageCraft Cloud Services, together with any associated logos, are trademarks of StorageCraft Technology Corporation in the United States and elsewhere. All other brands and product names are or may be trademarks or registered trademarks of their respective owners.

Table of Content

Table of Content	2
1 StorageCraft Cloud Overview	3
1.1 StorageCraft Cloud Program Models	5
1.2 StorageCraft Cloud Service Levels	5
2 StorageCraft Cloud Getting Started	6
2.1 Setting up StorageCraft Cloud Services	7
2.2 StorageCraft Cloud User Workspace	17
3 StorageCraft Cloud Failover and Recovery	26
3.1 StorageCraft Cloud BMR Process	26
3.2 StorageCraft Cloud File and Folder Restore	28
3.3 StorageCraft Cloud Virtualization	28
3.4 Restarting the Cloud Backup Process	31
4 StorageCraft Cloud Metrics and Reports	31
4.1 StorageCraft Cloud Account Details	32
4.2 Account Space Utilization Trends	33
4.3 Current Account Space Utilized	33
4.4 Current Account Devices/Tools in Use	34
4.5 Device Space Utilization Trends	34
4.6 Current Device Space Utilized	35
5 Tips and Tricks	35
5.1 StorageCraft Cloud Services FAQ	36
5.2 Troubleshooting StorageCraft Cloud Services	39

StorageCraft Cloud Services User Guide

Welcome to the StorageCraft® Cloud Services *User Guide*. The StorageCraft Cloud allows you to create a remote backup of your local backup. In the StorageCraft Cloud your data is protected against a major local disaster. If you are a Cloud+ or Cloud Premium member you can access your data from any location that has an internet connection. Cloud Premium members can quickly failover to a virtualized device in the StorageCraft Cloud to keep business running.

StorageCraft Cloud is based on encrypted ShadowProtect backup images. The backup images are replicated to the cloud by StorageCraft ImageManager. StorageCraft Cloud accounts, devices and backup images can be managed in the MSP portal.

The cloud elements, user workspace and other tools are explained in the following major sections of this user guide:

- [Getting Started](#)
- [StorageCraft Cloud Failover and Recovery](#)
- [Managing StorageCraft Cloud Metrics and Reports](#)
- [Tips and Tricks](#)

Additionally, this guide includes these general information sections:

- [Product Support](#)
- [StorageCraft Glossary](#)

Additional Information

For emerging issues and other resources, see:

- The StorageCraft technical support Web site at www.storagecraft.com/support.html.
- For more information about using ShadowProtect, see the StorageCraft [ShadowProtect User Guide](#).
- For more information about using ImageManager, see the StorageCraft [ImageManager User Guide](#).

Documentation Conventions

 **Note, Important, Warning**

The Note, Important and Warning symbols identify context-sensitive critical information about understanding or using the StorageCraft cloud.

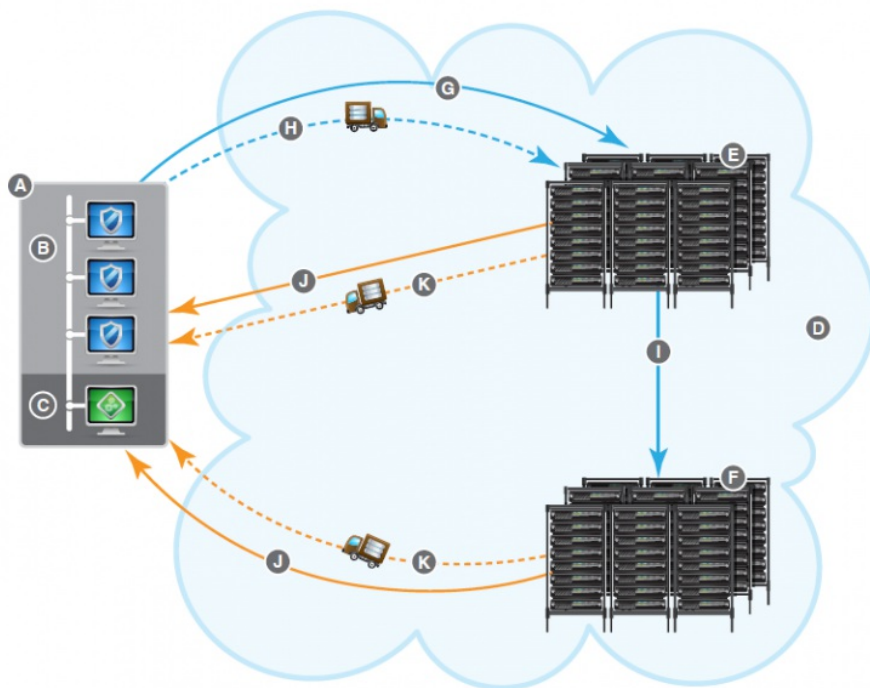
1 StorageCraft Cloud Overview

Welcome to the StorageCraft Cloud services overview.

The StorageCraft Cloud, as defined in this user guide, means all systems, devices, components, data centers, etc. outside your local business network. This overview shows the interaction between your business network and the StorageCraft Cloud.

StorageCraft Cloud Services Overview Image

Each alphabet letter in this image is described by the corresponding information (identified by matching alphabet letter) in the image description section below. The dashed connecting lines in the image represent physical (shipped) transfer of data via USB seed drives (shipped from you to StorageCraft) or USB BMR drives (shipped from StorageCraft to you).



⚠ Note: The solid connecting lines in the image between the local business network and the data centers indicate transfer of data over the internet. Dashed lines represent physical shipping of seed or BMR drives.

Image Description

Each alphabet letter in the image above is described by the corresponding information below (identified by matching alphabet letter).

- A. Local business network (everything inside your normal business network)
- B. ShadowProtect clients (devices which create encrypted StorageCraft backup image files)
- C. ImageManager client (manages and replicates encrypted StorageCraft backup image files to the cloud)
- D. The StorageCraft Cloud, for the purposes of this user guide, is defined as everything outside your local business network.
- E. Primary data center is where VMs, cloud devices and backup images are stored in the cloud.
- F. Secondary data center (mirrored) is identical to the primary data center but is located in another geographical region to protect against a major "localized" disaster. If the primary data center goes down, the secondary data center is there to provide the same services as the primary data center.
- G. Replicate to the cloud (ImageManager sends encrypted backup images over an internet connection to the cloud).
- H. Seed the cloud by populating a USB seed drive. The USB drive is shipped to StorageCraft. See [seeding the cloud](#) for details.
- I. Mirror data from the primary data center to the secondary data center.
- J. Recover files and folders via internet browser from the cloud.

⚠ Note: You can also virtualize (create VMs and a virtual network in the cloud) using one of the cloud backup images but this is not indicated in the image for the sake of clarity. See the [cloud services program models](#) and [StorageCraft Cloud service levels](#) pages to learn more about specific features and limitations.

K. Recover systems and data by requesting a Bare Metal Recovery (BMR) USB drive. The drive will be populated with the selected data from the data center and shipped from StorageCraft to the address specified in the BMR drive request.

1.1 StorageCraft Cloud Program Models

StorageCraft Cloud services is available for all user types:

- Individuals
- Managed Service Providers (MSPs)
- OEMs
- Other resellers

MSPs and OEMs can sell and manage cloud services for themselves or their customers.

- Pay for storage space used (pay per GB).
- Used space is rounded up to the nearest GB.
- Billing is on a monthly basis.
- Each device can have a unique service level.
- Can request a StorageCraft seed drive.
- Analysis tools (metrics) are provided so you can constantly monitor used space.

Prepaid storage space for all other Users

- Account minimum (similar to gift-card model): \$250
- Additional storage can be purchased in \$250 increments.
- The storage block lease is for a 1 year period.
- VARs can [lease additional storage](#).
- All devices for any given account must have the same service level.
- Can request a a StorageCraft seed drive.

How to Lease Additional Storage

All users, other than MSPs, can prepay for storage space. The initial purchase minimum is \$250. You can prepay as much as you want in increments of \$250. You can determine your storage costs using the US pricing calculator and the Canadian pricing calculator pages.

1.2 StorageCraft Cloud Service Levels

Service levels give you flexibility for the functionality you need. If your current service level doesn't provide features you need, you can change as needed within the limits described in [changing service levels - terms and conditions](#).

Cloud service levels:

- Cloud Basic
- Cloud Basic, Mirrored
- Cloud+
- Cloud+, Mirrored
- Cloud Premium
- Cloud Premium, Mirrored

⚠ Note: All features of a mirrored and a non-mirrored service level are identical except for mirroring. Mirroring means that all the data (backup images) stored in the primary data center are also backed up at a secondary data center (in a different geographic region). Mirroring is only available in the U.S.A.

Cloud Basic Features

Cloud Basic features include:

- Image archiving in the cloud
- Recovery: image recovery only available through BMR drive request
- Replicated: customer data stored at a single datacenter
- Bandwidth: unlimited for data transfer to the datacenter
- Snapshotting: customer can take and store an unlimited number of Snapshots

⚠ Note: Using a seed drive is the recommended method for getting large amounts of data into the cloud. Use replication for sending incrementals.

Cloud+ Features

Cloud+ includes all Cloud Basic features and:

- Immediate mount and search via browser from a mounted recovery point (defined per volume associated to a device)
- Immediate file and folder download from a mounted recovery point (defined per volume associated to a device)

Cloud Premium Features

Cloud Premium includes all Cloud+ features and:

- Instant full-data virtualization and failover in the cloud
- Virtualization support for Windows 2000 through Windows 8.
- Virtualized machine accessible via RDP, Public IP, and/or VPN
- VPN support
- Public dedicated IP address reservation for failover (additional fee required for each dedicated IP address)
- Dynamic IP address failover (takes longer to failover than dedicated/static IP)
- Support for Exchange, web and FTP servers

Changing Service Levels - Terms and Conditions

Changing service levels is subject to the following terms and conditions:

During the 7-day grace period

There is a 7-day grace period when you first create a cloud services replication target. During this grace period the service level selection is not locked and can be changed immediately.

After the 7-day grace period

After the grace period ends, the changes won't be immediate. There is a 7-day (minimum) waiting period after a change request. Service level change requests go into effect at the beginning of the next month after the 7-day waiting period but no sooner than 7 days.

2 StorageCraft Cloud Getting Started

This outline of essential steps contains links to detailed startup and configuration instructions.

Getting started - Overview

- Gain a better understanding of cloud services in the [StorageCraft Cloud services overview](#)
- Create StorageCraft Cloud user accounts in the StorageCraft portal for [MSPs](#) or [All other users](#).
- [Create encrypted](#) backup images with ShadowProtect
- [Manage](#) and [replicate](#) backup images to the cloud with ImageManager
- Manage data and devices in the cloud with the StorageCraft Cloud portal

Getting started - Details

- Follow the step-by-step instructions to [set up StorageCraft Cloud services](#)
- Learn more about menus and options in the [StorageCraft Cloud workspace](#)
- Understand how to recover from a system failure with [StorageCraft Cloud failover and recovery](#)
- Look up unfamiliar terms in the [StorageCraft glossary](#).

Get additional help on the [tips and tricks](#) page.

2.1 Setting up StorageCraft Cloud Services

StorageCraft Cloud backups are based on encrypted StorageCraft ShadowProtect backup images. Backup images are managed locally and replicated to the cloud with Imagemanager (version 6 or newer). ImageManager is also used to populate a seed drive (copying backup images to the seed drive). The StorageCraft portal is used to create and manage cloud user accounts. Cloud user accounts are used to manage cloud devices and backup images stored in the cloud.

These steps guide you through the process of setting up the StorageCraft Cloud. You can find additional supporting information in the [StorageCraft Cloud reference documents](#).

StorageCraft Cloud Replication Preliminary Steps

- ⚠ Warning: The image replicated to the StorageCraft Cloud is based on the volume size at the time of the initial backup. Always create a new base image after resizing a volume. ImageManager won't send additional files to the cloud if the local volume is resized after the initial files are pushed to the cloud.**
- ⚠ Note: Incrementals created by ImageReady, or created manually by mounting an image, making changes to it and then taking a new snapshot won't be consolidated or replicated by ImageManager.**

1. [Create a new StorageCraft Cloud Services account](#). Use the applicable link to create an account for your membership type:

- [MSP](#)
- [All other users](#).

The cloud services username and password are used when setting up cloud replication targets in ImageManager.

2. [Create encrypted backup image files](#) or use existing encrypted backup files created by ShadowProtect.

Backup image files need to be stored in a destination folder (local, USB, network or NAS) that is managed by ImageManager. The backup image password is used when virtualizing images, recovering files and folders, or requesting BMR drives.

- ⚠ Important: For security purposes, StorageCraft backup images are encrypted and password protected. As an additional security feature the images are replicated over a secure SSH internet connection. Make sure your password is stored in a secure location. The image passwords are not recoverable from the Cloud. StorageCraft has no method for gaining access to encrypted backup image files. If you enter the wrong password, or forget the password, you won't be able to access the cloud backup images.**

3. Configure ImageManager to manage the ShadowProtect encrypted backup image files.

The ShadowProtect encrypted backup image files must be stored in a destination folder that is managed by ImageManager.

- ⚠ Note: Verification needs to be completed before images can be replicated to the cloud. If consolidated images need to be replicated, the consolidation and verification must be done before they will be replicated.**

Setting up cloud destinations and replication

1. Select [Add new replication target](#) in ImageManager.

2. Create a name for the replication target.

This is done on the General tab under the ImageManager replication target setup page.

3. Select StorageCraft Cloud Services as the Destination Type in ImageManager.

4. Select "<Add new location . . . >" in the ImageManager location drop down to [create a new location](#).

- ⚠ Note: The checkbox for "This location requires authentication" is selected by default and can't be changed.**

5. Enter the username and password for the location and click Save.

This is the same cloud services username and password that was used when the StorageCraft Cloud services account was created.

6. Optional step - check the Override global throttling and adjust settings as desired on the General tab in the ImageManager Replication Target window.

7. Enter the password in the "Backup Image Password" field in the ImageManager Replication Target window..

This is the same password you used when creating the ShadowProtect encrypted backup image files.

8. Select the type of backup files to be replicated to the cloud.

The options are: "Only consolidated images files" or "All image files".

Warning: Select this option carefully because if you want to change it you'll need to delete the device in the cloud and create a new cloud replication target. Deleting a device also deletes all the data associated with the device.

9. Click the Cloud Settings tab in the ImageManager Replication Target window.

This tab appears when you select an existing cloud location with valid credentials or when you create the cloud location.

10. Select the desired Service Level from the drop down.

See [StorageCraft Cloud service levels](#) for more information.

11. Optional step - Check the "Generate warning when file is larger than:" box and specify a file size.

Important: The "Generate warning . . ." option sends an email to the recipient configured in notification settings if a file is larger than the specified size. Replication can continue without user intervention, but the notification allows you to pause replication and seed that large file instead of replicating it.

Notification settings must indicate that you want to receive warnings or this option won't work.

Warning: Don't pause the replication process for long periods of time. If the process is paused longer than the time specified in retention policies, the next file in the chain could be deleted before it can be replicated.

12. Uncheck the "Send initial backup images" box if you are not going to use a seed drive to seed the cloud.

When you click Save, the replication target settings are complete.

Note: If you previously requested a seed drive, but haven't received it, don't make any changes to the drop down. When you click Save, the replication target is disabled. The replication target can be enabled by saving the settings when you receive the seed drive.

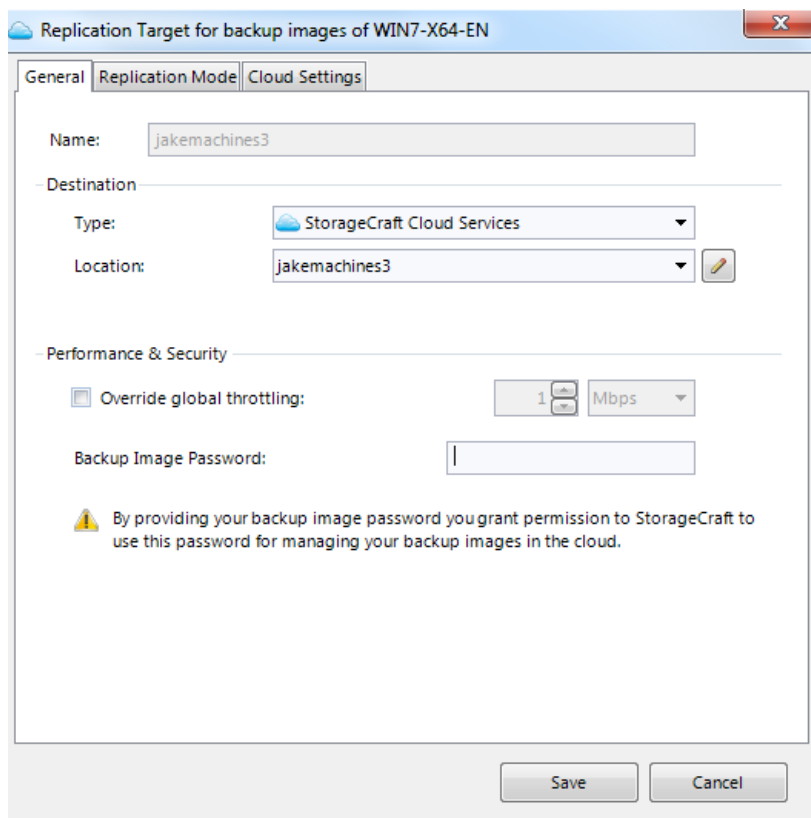
13. Complete the steps for [Setting up cloud destinations](#) and replication when the requested seed drive arrives.

Specifically you need to select the Service level and check the Send initial backup images box once the seed drive is attached.

Creating a Cloud Target

General Tab

The General Tab specifies the destination type (StorageCraft Cloud Services in this example) for this replication job.



Create a replication target

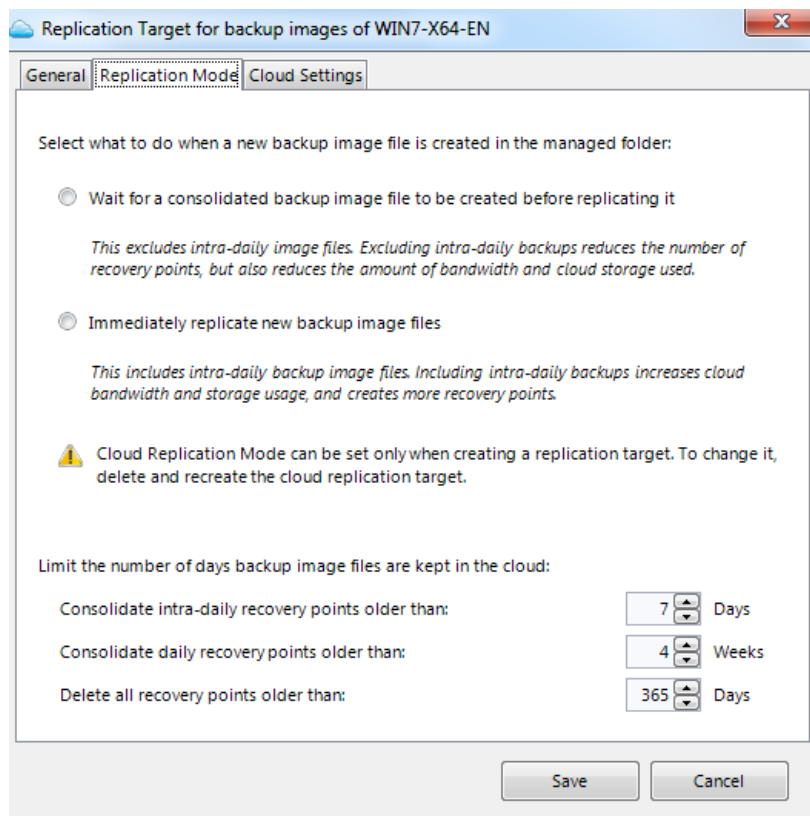
1. Enter a replication target identifier name (any name of your choosing) for this replication target
2. Select StorageCraft Cloud Services [in the Destination Type dropdown box] as the replication type.
3. Select a Cloud Location from the drop down that contains the credentials you want to use. A cloud location is identified only by it's credentials. ImageManager displays the Cloud Settings tab after the cloud location is selected.
4. If you want to choose specific throttling values, check the Override global throttling box and set the values
5. Enter the Backup Image Password to give StorageCraft permission to manage your images in the cloud.

⚠ Note: For security your Backup Image Password is never saved to disk in the cloud.

Replication Mode Tab

The replication mode tab allows you to select which backup image files will be replicated to the cloud. **Plan this selection carefully. See the warning below.**

⚠ Warning: This selection is permanent. It cannot be changed after the target is created. The only workaround is to completely delete your replication target and start over (which also means reseeding).



Select what to do when a new backup image file is created in the managed folder

The options are:

- Wait for a consolidated backup image file to be created before replacing it.
- Immediately replicate new backup image files.

⚠ Note: StorageCraft strongly recommends using the "Wait for a consolidated backup image file to be created before replacing it" option.

Limit the number of days backup image files are kept in the cloud

The Replication Mode tab in ImageManager also lets you specify the initial retention settings (the number of days backup image files are kept in the cloud) for the Cloud Device.

⚠ Note: The "Limit the number of days backup image files are kept in the cloud" settings are initially selected in ImageManager. However, after saving the settings they are no longer visible in ImageManager and must be managed in the StorageCraft Cloud Portal.

fg

The retention settings are:

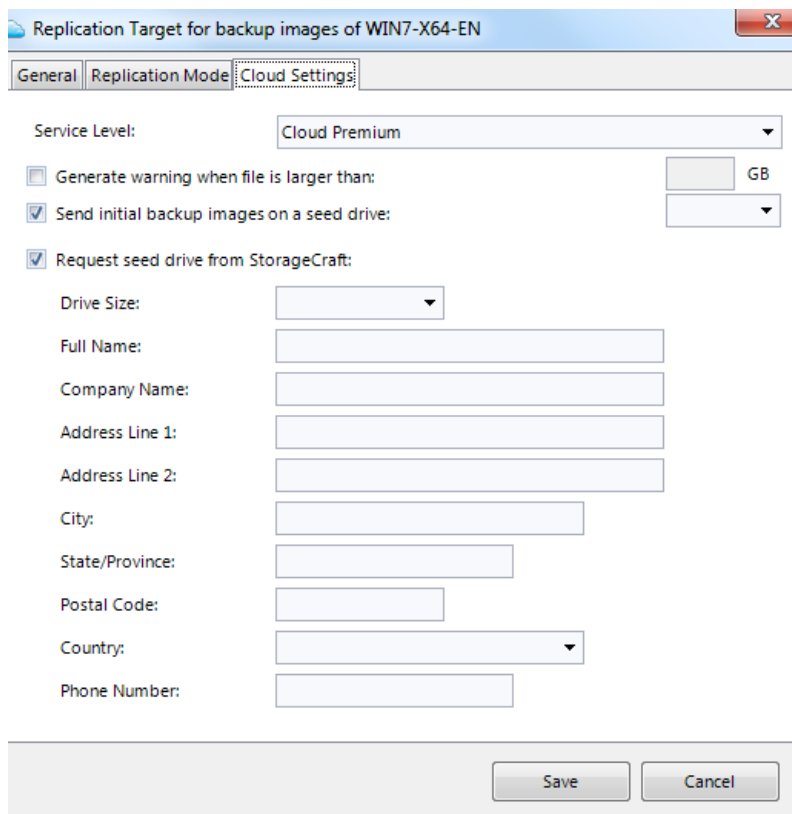
- Consolidate intra-daily recovery points older than: Select the number of days.
- Consolidate daily recovery points older than: Select the number of weeks.
- Delete all recovery points older than: Select the number of days.

⚠ Note: Cloud retention policies can be completely different than locally managed backup image retention policies. As a precaution, the most recent recovery point will never be removed.

Cloud Settings Tab

The cloud settings tab allows you to select a service level, populate a seed drive, or request a seed drive.

⚠ Important: See Important service level restrictions below.



Populating a seed drive

This section describes the steps for populating a seed drive. Additional information on populating seed drives can be found [here](#).

1. Select the Service Level for this target from the dropdown list.
2. Check the "Generate warning when file is larger than" box and set the desired value (if you need to change it).
3. Check the "Send Initial backup images on a seed drive" box (optional).

⚠ Important: Notifications must be turned on and a warning recipient must be configured for this to work.

4. Select the drive letter in the dropdown on the right (if you have a seed drive and are ready to populate it).

⚠ Note: The seed drive needs to be connected and recognized by Windows before you can select the drive letter from the drop down list.

5. Click Save. You have completed the replication target cloud settings.

Requesting a seed drive

1. Check the "Request seed drive from StorageCraft" box.
2. Provide the required information.
3. Click **Save**.
4. When you receive the seed drive return to the Cloud Settings tab and complete steps 3, 4 and 5 in "Populating a seed drive".

⚠ Note: You can choose to use your own USB drive instead of requesting a StorageCraft seed drive.

Important Service Level Restrictions

Plan carefully before choosing a service level. You have 7 days after initial agent creation (setting the service level for a specific end point) to change the service type before it gets locked in. After the initial 7 days, a fee is required to change the service level. There

is also a 7-day waiting period if you change service levels after the initial 7-day period. Service level changes don't go into effect until the following month and is in no case less than 7 days from the time of change.

Restrictions Summary:

- Service level "locked in" 7 days after initial agent creation
- No method to fast track level changes
- Level changes require a minimum of 7 days before becoming active
- Level changes don't become active until the beginning of the month (after the 7-day waiting period)

Retention Settings Details

Retention

The retention system is designed to automatically limit the amount of information that is kept on the cloud accounts. Using retention settings, you can tailor the cloud's storage to mirror security policies, DR scenarios and keep cloud storage costs in line. StorageCraft Cloud Services offers a unique system allowing recovery points to be consolidated, freeing up space while retaining useful backup histories.

There are three settings involved with Retention; Daily, Weekly and Delete.

Daily Retention

Over the course of a day you may instruct ImageManager to upload multiple recovery points to the cloud. After several days, the need to have these multiple backups throughout a day diminishes. The **Daily Retention** setting lets you set the number of days to keep these intra-daily recovery points in the cloud.

Once a day's backups are older than this date recovery points will be consolidated into one single full-day recovery point. This point's timestamp will be the same as the last recovery point taken that day.

Weekly Retention

As time goes by the need for individual daily backups can also diminish. Along the same idea as the Daily Retention system, there is a **Weekly Retention** system. This allows you to set the number of weeks to keep the full-day recovery points around.

When a business week comes to a close, the system will consolidate an entire week's worth of full-day or intra-daily recovery points into a full-week recovery point. This point's timestamp will be the same as the last recovery point of that week.

Delete Retention

Over time the usefulness of a backup decreases. Changes to configurations, data revisions and other operations makes restoring from a very old backup almost as costly as starting from scratch. To remove unnecessary and minimally useful backups the **Delete Retention** system can be used to delete these old recovery points.

See the [Retention Settings Examples](#) page for more details.

Once a backup is older than the number of days set in the **Delete Retention** setting, it will be securely deleted. This means the data is unrecoverable in that snapshot, but the system will maintain the backup chain integrity.

 **Note: The latest recovery point will never be removed, no matter the retention settings.**

Retention Settings Examples

Example settings:

1. A code repository server needs to have several daily backups for a couple of weeks, and then the system can begin consolidation. The settings are as follows:

- Daily: 14 Days
- Weekly: 3 Weeks
- Delete: 30 Days

Today is February 1st, 2012. ImageManager sends a new recovery point to the cloud every hour during normal business hours. Every single hourly recovery point is available backwards into January 18th. The 17th's backups have been consolidated into a full-day backup. At the end of the week, the full-day backups from the 9th through the 13th will be combined into a full-week backup, with a timestamp for 5 PM on Friday the 13th. (Might be a backup that you don't want to use). This situation has a standard progression of intra-daily -> daily -> weekly -> deleted. 2. An exchange server only needs a very recent backup in case of a disaster. You set the retention settings to the following:

- Daily: 1 Day

- Weekly: 1 Week
- Delete: 3 Days

Today is Thursday, and the system has been backing up to the cloud since Monday. Monday and Tuesday's intra-daily recovery points have been consolidated into single full-day recovery points. This evening, Wednesday's backups will be consolidated in similar fashion. Monday's full-day recovery point will be deleted from the system at the same time. Because the Delete Retention setting is less than a week, the Weekly setting is never used. 3. You have a financial system transaction log that is used for auditing purposes, and needs to be retained for precisely 60 days. The settings are as follows:

- Daily: 365 Days
- Weekly: 54 Weeks
- Delete: 60 Days

In this case, every single intra-daily backup will be available until 60 days pass, at which point they will be removed that evening. Because the delete date passes before either the Daily or Weekly retention points, both systems are not used. This is liable to create a very large amount of data in the cloud and is (thus) not recommended.

Creating a Cloud Location

Use the same username and password for creating a cloud location that was used for the cloud user account in the StorageCraft portal. The same credentials are required for the cloud location object.

Enter the following information to create the cloud location:

- The cloud username
- The cloud password
- The location name (used only for display purposes in ImageManager)

The default block size of 66536 bytes can be used or can be changed when creating a cloud location.

 **Note: The location can't be saved if a connection can't be made, or if the credentials are wrong.**

Creating Encrypted Backup Images

Backup image files intended for cloud backups must be encrypted. ImageManager rejects backup image files that are not encrypted.

See the StorageCraft [ShadowProtect user guide](#) and the [ImageManager user guide](#) for details on how to create StorageCraft backup image files.

Adding New Volumes When Only Replicating Collapsed Files (Send Collapses Only)

If the settings indicate that only collapses are to be replicated, a problem occurs when a new volume is added to the backup job. New base images (.spf) will be created when new volumes are added to the backup. However, the changes in the other volumes are contained in incremental files which won't be sent to the cloud until they have been collapsed into a daily incremental at the end of the day. This new base image is immediately sent to the cloud and prompts a new recovery point to be created. This recovery point contains the new volume, but the other volumes will be unchanged until the next recovery point is created. The next recovery point will be created from the daily collapse of all the volumes. This is because the user has indicated that they do not want intra-daily incrementals to be sent to the cloud.

 **Warning: All backups must be encrypted and password protected or ImageManager won't replicate them to the cloud. Multiple backup jobs running on the same computer, must use the same password.**

For security reasons, ShadowProtect image passwords are not recoverable from the Cloud. StorageCraft has no method for accessing encrypted backup image files. Make sure the password is stored in a secure location. StorageCraft Cloud backup images can't be accessed without the password.

Backups with Multiple Volumes

Backups with multiple volumes need to have all of the images go to the same managed folder. Otherwise they will not be associated with the same Cloud Device. Multiple volumes can be backed up as a single job or as multiple jobs.

- The advantage of multiple jobs is the flexibility to place different volumes onto different backup schedules.
- The advantage of a single backup is that all volumes can be synchronized at each point in time. StorageCraft recommends a single backup job if the device will be virtualized.

Creating a Cloud Services Account

Create cloud services accounts in the Cloud Services tab in the MSP portal.

1. Login: [MSPs All other users](#).
2. Click on the Cloud Services tab
3. Create a cloud user account - type a new login name, password and other requested information.

⚠ Note: Keep track of the username and password. They will be needed when setting up your Cloud Locations in ImageManager.

How your physical and IP addresses affect your service

The physical address you enter when creating your account will help determine which data center is used and which service levels are available to you. The combination of your physical address and your IP address (checked automatically by the system) determines whether your backup images are replicated to a data center in the U.S. or Canada. This combination also determines if mirroring is available for you. Mirroring is available only if you have a U.S. address and your IP address checks out to be one from the U.S.

⚠ Note: To ensure security, data from Canadian companies is stored only in Canadian data centers. If you directly upload your base image and incrementals to a StorageCraft datacenter in Canada, your data stays in Canada.

Seeding the StorageCraft Cloud

Seeding the cloud consists of the following:

- [Seeding vs Replication](#)
- [Seed drive requirements and limitations](#)
- [Requesting a Seed Drive](#)
- [Populating the Seed Drive](#)
- [Shipping the drive to StorageCraft](#)
- [Syncing ImageManager with the Cloud](#)

⚠ Note: ImageManager uses the shortest chain possible when seeding the cloud. Only a small percentage of backup image files from the local managed folder become recovery points in the cloud. This reduces the amount of space used in the cloud.

Seeding vs Replication

This overview can help with the decision whether to seed the base images (recommended), or copy (replicate) the files to the cloud using ImageManager replication. Seeding is always followed by replication, but replication is not necessarily preceded by seeding.

Seeding

Seeding is the fastest (and suggested) method for getting your base images backed up to the cloud. You can request a seed drive from StorageCraft or you can use your own seed drive. The seed drive is populated with backup images managed by ImageManager. The seed drive must be a clean (newly formatted) NTFS formatted USB drive. See [Seeding the cloud](#) for more details about the seeding process and how to request a seed drive.

Replicating

Your base image backup files can also be replicated to the cloud by selecting the Cloud Services Replication option in ImageManager. If your base images are large this is not the suggested method. It takes longer and uses more bandwidth. However, if you don't mind taking longer to replicate your base image to the cloud this option may work for you. See [Creating a cloud target](#) for details about setting up replication.

Seed Drive Requirements and Limitations

Seed drives are used when you have a large base file, large backup image chains or small bandwidth capabilities.

Points to remember when preparing to seed the cloud.

Restrictions and Limitations

- Participants must use a StorageCraft Cloud drive to seed the cloud.
- Don't copy personal files or extra information to the seed drive.
- ShadowProtect backup Images must be encrypted and password protected.

Reserving Space on Seed Drives

- ImageManager (version 6 or newer) verifies there is enough space on the drive for every file defined for population by the current target) before it starts populating to the drive. ImageManager then reserves the required space so another target can't use the space needed for the files of the current target. One seed drive can be used to seed base images for multiple devices.

Requesting a Seed Drive

Seed Drive Request and Seeding Times

You can request a StorageCraft seed drive to streamline the seeding process.

1. Request a seed drive through the StorageCraft portal: [MSPs](#) [All other users](#).
 2. When requesting a seed drive, make sure to choose a drive size large enough to meet your needs. One drive can be used for multiple devices.
 3. After the seed drive arrives, connect it to your computer and note the volume letter assigned to the drive.
 4. Edit the replication target so it points to the seed drive. Use the volume letter assigned to the drive.
 5. Start populating the drive (the first part of seeding the cloud).
 6. ImageManager notifies you when it is finished populating the drive.
 7. Return the media to StorageCraft in the StorageCraft postage-paid mailer.
- For customer data of one (1) terabyte (TB) or less, seeding will be completed within seven (7) calendar days of receiving the storage media from customer.
 - For customer data in excess of one (1) TB, one (1) extra day per TB will be required to complete the seeding.
 - All shipments will be delivered to the customer destination via commercial courier with tracking capabilities.

Populating the Seed Drive

When a folder is selected for seeding, ImageManager takes all of the files that were in the folder when the user indicated that they wanted to seed. The snapshot may include the base image and consolidated weekly, daily, and/or intra-daily incremental images.

⚠ Note: You must set the drive path before attempting to enable a job. If the path isn't set, the job is disabled when it is added.

ImageManager won't start populating the drive unless:

- The drive is blank and in NTFS format
- The path (or drive letter) is supplied and the job is enabled

See the Populating a Seed Drive section on the [Creating a cloud target](#) page.

During the seed drive population:

- ImageManager reserves space on the seed drive for all backup images from each target. An error is displayed if you try to save a job when the drive is not big enough to hold the images of all the jobs that are seeding to the drive. This ensures that

a newer target does not prevent the other previously running jobs (that have already started the population process) from finishing.

- ImageManager can simultaneously populate a single seed drive with multiple image files or multiple managed folders from any number of replication targets across multiple accounts.
- The "Percent Complete Progress Indicator" applies to the file currently being populated to the drive.

When the drive population is complete:

- ImageManager displays an onscreen notification and sends an email notification when drive seeding is complete and indicates that the drive is ready to be shipped.
- ImageManager starts replicating new incremental files (incrementals created after the drive is ready to ship) to the cloud.

Shipping Seed Drives

Drive Populated (Ready to Ship)

When all files have been copied to the seed drive (the drive is populated) ImageManager notifies you that the drive is ready to ship to the data center. Follow the process below to get your data seeded to the cloud:

1. Pack the drive in the shipping box provided.
2. Make sure the correct shipping address is included on the label. See StorageCraft seed drive address below.
3. Send the drive.



Warning: Properly package the drive for safe shipping. The drive should be packaged to withstand a 6 foot drop (standard shipping expectations from shipping providers).

StorageCraft seed drive address

StorageCraft
101 Merritt 7
7th Floor Suite 2
Norwalk, CT 06851

Replication without a base image

ImageManger version 6 (and newer) has the ability to replicate to the cloud after populating the seed drive. The replicated files are dormant in the cloud until the base image is seeded. ImageManager immediately starts replicating files to the cloud after the drive population is complete. The replicated files will be synced with the base image after it has been seeded onto the cloud server.

Syncing ImageManager with the Cloud

Once the Seed Drive is populated:

- ImageManager starts replicating new incrementals directly to the cloud.
- When the synchronization is complete, ImageManager knows which files (.spf/.spi/.md5) to send and sends them up to the cloud.
- Cloud services deletes the .seed files when they are no longer needed.
- ImageManager reports to cloud services when all files are transmitted and a snapshot is taken.

Note

The image password is not stored on the seed drive for security reasons. This password is needed before the cloud can do anything with the images from the seed drive. For example if you have 10 image files (from your seed drive) on the cloud, and no new images have been replicated (sent to the cloud from ImageManager over the wire), those 10 files are effectively dormant. Cloud services can't do anything with those files until another image file gets replicated from ImageManager. When the new image is replicated, the password is also sent from ImageManager. When cloud services receives the new image file and the password, that password is used to decrypt all the seeded files. The files are then converted to StorageCraft Cloud backup image file format and merged with the files replicated from ImageManager and then the consolidated files are re-encrypted. This password is never accessible to a person and is never written to disk. It is only temporarily kept in memory for a short time.

StorageCraft Cloud Reference Documents

This page contains information to help you understand the details of creating backup images, selecting backup options and managing backup folders, creating backup locations and targets, and other important subjects that are not contained in the cloud user guide. Each subject is listed under the StorageCraft product used to perform the task.

- The ShadowProtect User Guide
 - [Create a backup image \(overview\)](#)
 - [Creating backup images \(steps\)](#)
 - [Selecting backup options](#) (encryption is required for cloud storage)

⚠ Note: ImageManager 6 is required for creating backup images that can be replicated to the StorageCraft Cloud. ShadowProtect 5 is also required if you want to use rolling consolidation.

- The ImageManager User Guide
 - [Create a managed folder](#)
 - [Creating Locations](#) (see also [creating locations and targets](#) in the StorageCraft Cloud user guide)
 - [Requesting a seed drive](#)
- The StorageCraft MSP portal User Guide.
 - [Creating a StorageCraft Cloud user account](#)
 - [Managing StorageCraft Cloud accounts and devices](#)
 - [Requesting a seed drive](#)

2.2 StorageCraft Cloud User Workspace

The StorageCraft Cloud user workspace is the collection of screens, commands, and reporting links that help you manage devices and navigate through the system.

StorageCraft Portal

Use the portal to manage your accounts and to manage cloud backup images and recovery points, and cloud devices. Do this after completing the prerequisite steps of using StorageCraft ShadowProtect (used to create encrypted backup images) and StorageCraft ImageManager (used to manage the backup images and replicate them to the cloud).



- Add cloud accounts and sub-accounts on the Account management tab
- View cloud account details
- View cloud account alerts
- View cloud account metrics
- Manage Devices

- Request Seed Drive
- View Drive request details

Managing Cloud Accounts and Devices

1. Login to the StorageCraft portal: [MSPs All other users](#).
2. Click on the StorageCraft Cloud Services tab.
3. Click on the Manage Devices button at the bottom of the page.
4. Select the devices and recovery points you want to manage.

- [StorageCraft Cloud Status](#) (default screen)
- [StorageCraft Cloud Sub Accounts](#)
- [StorageCraft Cloud Devices](#)
- [StorageCraft Cloud Virtualization](#)
- Help
- Logout (dropdown also allows context based account switching)

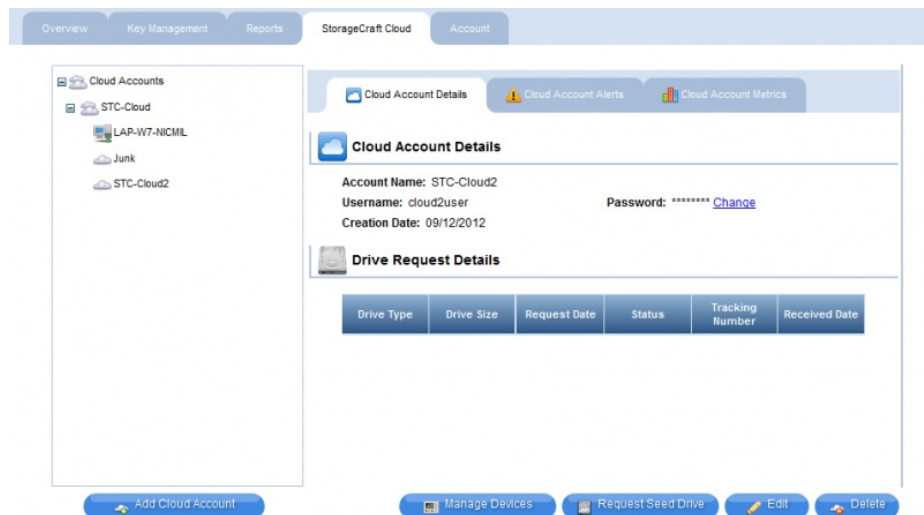
StorageCraft Cloud Account Management

StorageCraft Cloud Account management is done in the StorageCraft portal: [MSPs All other users](#). The account management interface consists of 3 main screens:

- Cloud Account Details
- Cloud Account Alerts
- Cloud Account Metrics

The StorageCraft portal interface for MSPs is similar to the one for all other users. However, there may be some minor differences (based on your account type) between the screens shown below and the ones displayed when you login.

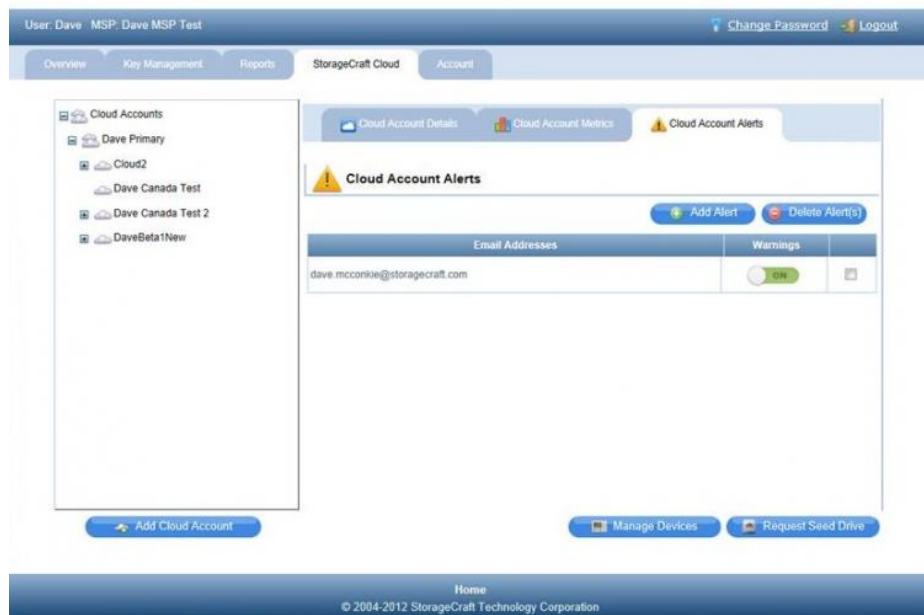
Cloud Account Details



The cloud account details screen allows you to:

- Add Cloud Accounts
- View Account Details
- View seed drive request details
- Change the account password
- Manage Devices
- Request a seed drive
- Edit the cloud account name
- Delete the account (warning: this also deletes all devices and recovery points)

Cloud Account Alerts

STORAGECRAFT.
MSP PORTAL


Note: The initial release will send a warning for devices that haven't replicated a file for more than 3 days. Additional alerts will be added in the future.

The cloud account alerts page allows you to:

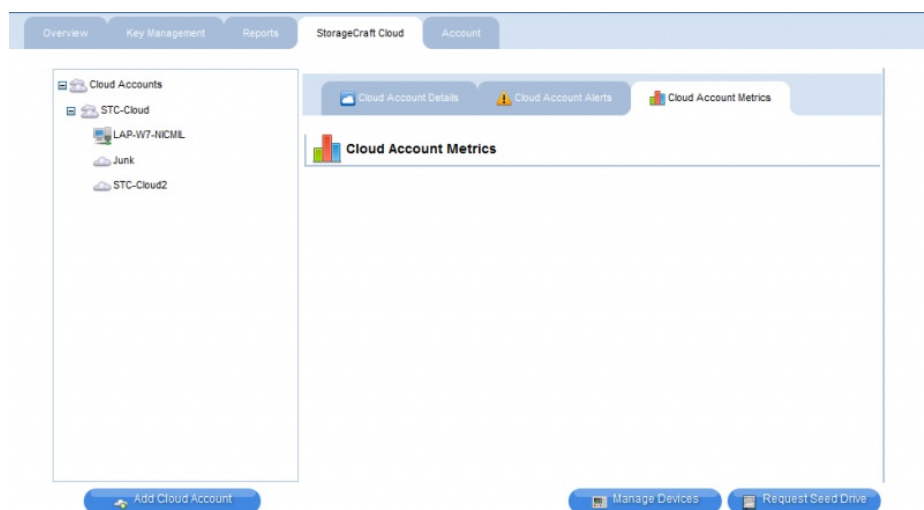
- Add Alerts
- Delete Alerts
- Manage Devices
- Request a Seed Drive

Adding new alerts consists of creating a new email recipient and selecting which alerts you want to receive. The alert types are:

- Errors
- Warnings
- Notices
- Successes

Deleting Alerts

1. Check the box next to the alert to be deleted.
2. Click Delete Alert(s)

Cloud Account Metrics


Details of Cloud Account Metrics will be added when the functionality is fully implemented.

Cloud Account Management - Administrative

Administrative

Administrative options in the left side menu consist of:

- Seed Drive
- Remove Data
- Remove Agent

Seed Drive

When you request a seed drive you must enter the following information:

- Name
- Address
- City
- State
- Zip/Postal code
- Country name
- Phone #)

Click the Request Drive button after filling in the required information.

Remove Data

- This option allows you to remove a snapshot.

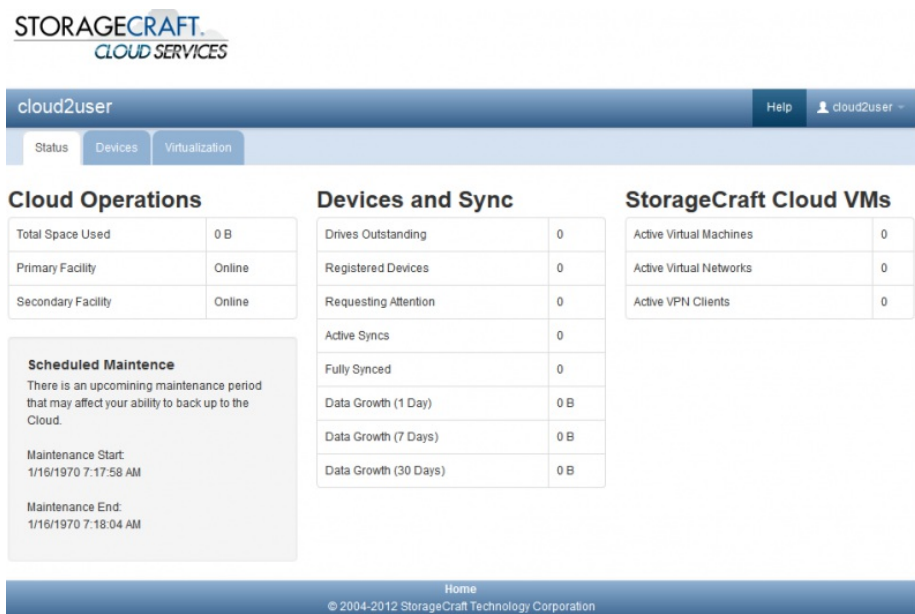
Warning: This is a permanent unrecoverable process. Once a snapshot is removed it can't be recovered.

- Select an agent from the drop down list. This displays the available time stamped snapshot.
- Make sure you want to delete the data before clicking "Remove Point" because the deleted data is unrecoverable.

Remove Device

Devices are managed through the StorageCraft portal: [MSPs All other users.](#)

StorageCraft Cloud Status



The screenshot shows the StorageCraft Cloud Services user interface. At the top, there is a navigation bar with "cloud2user" on the left, "Help" and "cloud2user" on the right, and tabs for "Status", "Devices", and "Virtualization". The main content area is divided into three columns:

- Cloud Operations:**

Total Space Used	0 B
Primary Facility	Online
Secondary Facility	Online

Scheduled Maintenance
There is an upcoming maintenance period that may affect your ability to back up to the Cloud.
Maintenance Start: 1/16/1970 7:17:58 AM
Maintenance End: 1/16/1970 7:18:04 AM
- Devices and Sync:**

Drives Outstanding	0
Registered Devices	0
Requesting Attention	0
Active Syncs	0
Fully Synced	0
Data Growth (1 Day)	0 B
Data Growth (7 Days)	0 B
Data Growth (30 Days)	0 B
- StorageCraft Cloud VMs:**

Active Virtual Machines	0
Active Virtual Networks	0
Active VPN Clients	0

At the bottom of the interface, there is a "Home" button and a copyright notice: "© 2004-2012 StorageCraft Technology Corporation".

The status window includes:

- Cloud Operations

- Devices and Sync
- StorageCraft Cloud VMs
- Scheduled Maintenance

Cloud Operations

The cloud operations section displays:

- Total Space Used
- Whether the primary data center is online or offline
- Whether the secondary data center (if applicable) is online or offline

Devices and Sync

The Agents and Sync section provides important information about agents (end points) and how fast your data space is growing.

This section displays:

- Requesting attention: Shows the number of devices that need manual attention
- Active Syncs: Shows how many devices are in the syncing process
- Devices fully synced: Shows the number of Devices (end points) that are synced with ImageManager
- Data Growth (1 day): Shows how much your data has grown in 1 day.
- Data Growth (7 days): Shows how much your data has grown in 7 days.
- Data Growth (30 days): Shows how much your data has grown in 30 days.

Cloud Virtualizations

The cloud virtualization section displays:

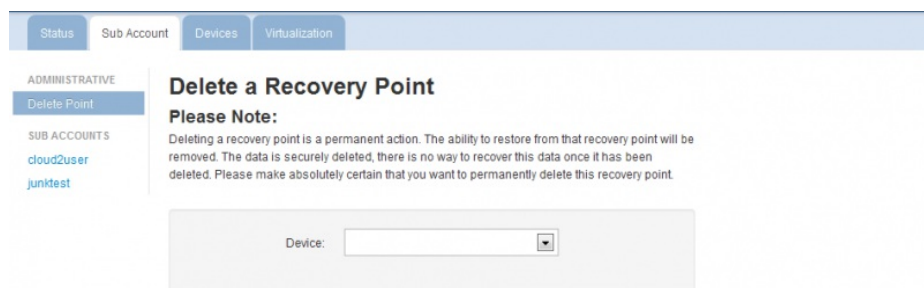
- Active Virtual Machines: shows how many VMs are configured and running.
- Active Virtual Networks: shows how many active virtual Networks are available.
- Active VPN Clients: Shows how many active clients are logged in via VPN clients

Scheduled Maintenance

The scheduled maintenance section includes important notifications such as:

- There are no scheduled maintenance events affecting cloud services coming up in the next 2 weeks.
- There is a maintenance operation on Thursday, July 26, 2012 at 12:00:00 AM. Please be aware your machine may not back up during this time period.

StorageCraft Cloud Sub Accounts



The main use of sub accounts is to help users manage all customer accounts. Sub account customers may need to access and manage their information, but they shouldn't have access or control over the data or devices of other users.

A primary (parent) account user can manage a sub account. If you are logged in as the primary account user, all status data is for the primary account level. When you are logged in as the primary (parent) you are able to do anything that the sub account user can do. However, if you don't have the encryption password for the backup images you can't access the data owned by the sub account.

⚠ Warning Use extra caution when managing accounts as a primary account manager. You can entirely delete the backup images for any subaccount. You won't be able to access the actual data but you can destroy it.

Sub accounts allow you to:

- View devices

- Manage subaccounts
- View date created
- Assume identity (allows you to effectively login as one of the sub accounts so you can manage the account directly.) This changes the name shown in the top right portion of the screen. To return to the "parent" account, click the drop down arrow in the top right menu bar.

StorageCraft Cloud Devices

Left Side Menu

Device status options in the left side menu include:

Devices

When you click any option in the left menu bar, the related information displays in the right side window.

- All devices
- My devices (default screen when you click on the Devices tab)
- New devices (Recent devices)
- Sub devices (Sub Account devices, when a primary account is selected)
- Synced devices (Successful devices)
- Syncing devices (Devices currently syncing)
- Trouble devices (devices needing attention)

Sub Accounts

This lists the name of each sub account. Click on a sub account name to view information about each account.

A sub account can be managed by a parent account. When logged in as the parent you can do anything the sub account user can do. However if the sub account user doesn't give the encryption password to the MSP (parent user), the parent can't access the data in the backup image.

⚠ Warning As an MSP or parent account, even if you don't have the encryption password, you can still delete backup images. All backup images, except the latest can be removed.

The main use of sub accounts is to facilitate MSPs and parent accounts. The parent account allows the administrator to manage the accounts of all their customers. The customers can login and access their information but don't have the ability to view or tamper with the data owned by others.

General Heading Information

When you select any of the options from the Left Menu, information for the selected option is displayed in the larger panel or window on the right side. All left menu options have the same information (details displayed in the right column). This is a list of information for the right panel.

- The device status
- Hostname where the device is running
- Latest Point (snapshot - recovery point)
- Storage space used
- OS of the device
- Account name
- Details (shows an alternate view of status with a few additional details)

All Devices

The all devices option displays a list of all devices being managed by the currently logged in user.

My Devices

Status is identified by circular icons. A black circle with a white i in the middle means that the device needs attention. A white circle with a black checkmark in it means the device is idle.

Hostname is just the "Computer name" found in Windows "Computer name, domain, and workgroup settings".

Latest Point gives the day of the week, month name, date of the month, year, and time of the most recent recovery point.

New Devices

This lists all recently created devices.

Sub Devices

This option lists all the sub account devices. A sub account device only shows if a primary is selected.

Synced (Successful) Devices

Synced devices are also known as successful devices. This means that the information in the cloud is complete and synchronized with data at the local ImageManager location. All files that need to be backed up, have been replicated to the cloud.

Syncing Devices

The devices currently in the syncing process are listed on this screen.

Trouble Devices (Devices needing attention)

If there is a problem during the synchronization process the information for the device is displayed in this screen.

Managing Device Details

Details

The menu options (left column) for each device are:

- Status
- Options
- Recovery Points

Restore

- Files and Folders
- Virtualization
- Physical Restore

Status

Status: Needs attention (synced and idling)

Storage used: typically shown in Gigabytes

Newest recovery point: This will either say "None" or will give a date and time stamp.

Oldest recovery point: This will either say "None" or will give a date and time stamp.

Recovery points: Lists all recovery points

- Virtualization enabled
- File and folder enabled
- Mirroring enabled

Options (Retention Options)

Retention options include the ability to rollup (combine) individual snapshots into consolidated backups.

- Daily Rollup
- Weekly Rollup
- Deletion Date
- Save

Daily Rollup lets you select the number of days to keep intra-daily backups (minimum 3 days). Daily backups can then be rolled up into weekly backups.

Weekly Rollup lets you select the number of days to keep intra-weekly backups (minimum 7 days).

Deletion Date lets you set the number of days to keep backups (minimum 30).

⚠ Warning: Backups will be automatically (and permanently) removed when they are older than the number of days specified in the Deletion Date.

Delete a volume

Retention options will never delete a volume. To manually delete a volume:

1. Select a device.
2. Click "Delete Volume" in the left menu.
3. Select the volume to delete (click radio button next to the volume name).
4. Click delete.
5. Enter the backup image password.
6. Confirm the deletion.

⚠ Warning: This feature allows you to delete volumes no longer backed up by ShadowProtect and replicated to the cloud. This will free up cloud storage space when older recovery points are removed (either manually or by retention settings). Removing old recovery points also prevents volumes from showing up as future File and Folder recovery points.

Do not use this feature if the volume is still being backed up by ShadowProtect and replicated to the Cloud. Be sure that the volume you want to delete is no longer part of the ShadowProtect backup job.

Recovery Points

Recovery points gives you the Time of each recovery point and the size of the backup.

Restore

Files and Folders (if entitled)

You can restore files and folders by selecting one of the recovery points and providing the ShadowProtect backup image encryption password. This allows you to pull the information you need from the cloud directly through your browser to your local drive.

Virtualization (if entitled)

You can select a recovery point and create a VM (virtualize) it using cloud services.

Physical Restore

The Physical Restore option allows you to request that a recovery drive be shipped to you. You need to complete the following information and then click Request Drive.

- Name
- Address
- City
- State
- Zip/Postal Code
- Country
- Phone
- Recovery point
- System architecture (x86 or 64 bit*)
- ShadowProtect image password
- Testing Request: Warning- there is a fee for testing the BMR system.

⚠ Note: *Incrementals are only possible when using 64 bit hardware.

StorageCraft Cloud Virtualization

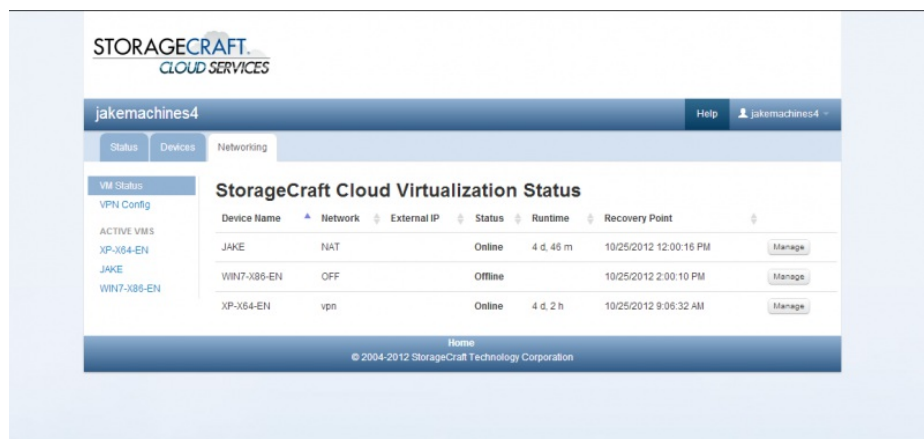
The Virtualization tab gives you the following menu options:

- VM Status
- VM Config
- Active VMs

VM Status

The VM Status menu option displays the Cloud Virtualization Status. This includes the list of all VMs and the following information:

- VM Hostname
- VM Network connection status
- VM Status (is the VM is powered on or off)
- Recovery Point (indicates which snapshot is mounted for the VM)
- Details link



The Manage link gives you additional functionality. It allows you to:

- Start and stop the VM (encryption password required)
- Select different point (Destroys the current VM and allows you to switch to another VM)
- Storage controller type (can't be changed in this window)
- Network type (Network Address Translation, Bridged, Host Only, or None)
- RAM amount (you can select between 1 GB and 16 GB for VM memory)
- Destroy VM (No delete confirmation if VM is not running. Delete verification occurs if the VM is running.)

⚠ Note: You will be prompted to install virtual boot software before being able to access the vm desktop.

You have a variety of control options for a VM that is running. You can:

- Restart
- Stop
- Download the RDP link
- Ctrl-Alt-Del

Downloading the RDP link allows you to remotely manage the associated VM in the same way you can use Windows RDP to manage any remote computer.

VPN Config

The VPN Config menu option displays the Virtual Private Network Configuration window.



This screen allows you to:

- Create a New VPN
- Edit existing VPNs
- View a summary status of each existing VPNs

Create new VPN

⚠ Note: You must add a VM before attempting to start the VPN. If a VM has not been added before starting the VPN (VPN not configured correctly) a warning error is displayed.

New VPNs require the following information when they are created:

- Name (a reference name for the new VPN)
- Gateway (the gateway address for the VPN)
- IP address (network address for the VPN)
- Subnet mask (subnet mask for the VPN)

This screen also lists all existing VPNs and allows you to Start (if not running), Stop (if it is running), and Edit the VPN.

Clicking on the Edit button displays the following:

- VPN values entered when the VPN was created
- A list of all available Cloud VMs
- Remote end point (client) devices (must be manually entered)

Active VMs

Clicking on any active VM link displays the virtualization screen for that VM. This is the same screen shown when you click the Details button in the Virtualization screen.

3 StorageCraft Cloud Failover and Recovery

Failover and recovery are the main reason for replicating your backup images to the cloud. Data stored in the cloud can be recovered by the following methods:

- [Bare Metal Recovery \(BMR\)](#) - Request a physical drive for a selected point in time
- [File and Folder Restore](#) - Download individual files and/or folders
- [StorageCraft Cloud Virtualization](#) - Failover to your cloud VM or create a VPN

Start a New Backup

You need to start a new backup after restoring your system. The original backup configuration is not correlated with or applicable to the restored system. Refer to [Restarting after a successful BMR](#) for more detailed information.

⚠ Note: The BMR drive contains snapshots (recovery points) from only one device.

Requesting a BMR Drive

1. Login to the StorageCraft portal: [MSPs All other users](#).
2. Select the StorageCraft Cloud tab.
3. Select one of the cloud accounts in the left panel.
4. Click Manage Devices. This displays the StorageCraft Cloud control panel.
5. Click the Devices tab.
6. Select the specific recovery point for the device to be restored.
7. Click Physical Restore in the left panel.
8. Complete all the fields for the required information.
9. Click Request Drive.

[Required BMR drive request information:](#)

⚠ Note: StorageCraft overnight ships the BMR drive (if overnight service is available) after the recovery image is copied to the drive. Be aware that it takes two or three days to prepare the drive after receiving a request. Larger images require more time. StorageCraft makes every effort to prepare and send the BMR drive as quickly as possible.

⚠ Important: A fee is associated for a BMR Testing Request.

Restoring the System

The cloud services Bare Metal Restore process is different than the standard StorageCraft Bare Metal Restore. In cloud services a specific point-in-time backup image is requested. StorageCraft copies the requested image to a USB BMR drive and ships it to the address provided in the request.

The drive contains all the tools required to boot the new target hardware and restore the backup image. Connect the USB BMR drive to one of the USB ports on the new bare metal "target" computer and boot it. The target machine boots from the USB BMR drive. The BMR restore process displays step-by-step on-screen instructions to complete the restore process.

When the BMR drive arrives

1. Connect the USB BMR drive to the target hardware.
2. Boot the new target hardware from the USB BMR drive.
3. Follow the on-screen instructions displayed by the BMR recovery software. This software is built into the BMR drive.
4. Click OK when the BMR process finishes.
5. Turn off the restored target computer.
6. Disconnect the USB BMR disk. (This is required so the restored computer will boot instead of the BMR recovery process.)
7. Start the restored target computer and verify that the restore was successful.

The BMR process is now complete.

BMR Request Required Information

Required information for requesting a BMR drive:

⚠ Note: StorageCraft always prompts for the cloud password to provide additional security.

- Device Name (which machine needs to be restored)
- Which Recovery Point to recover

or

- Which running virtual machine to recover
- Whether to restart a VM after a snapshot if a virtual machine is selected (checked by default)

⚠ Note: Virtual Machines are taken offline during a snapshot to ensure a consistent/stable state when the snapshot is taken. If "Restart VM" is selected, the VM is restarted automatically when the snapshot process is complete.

⚠ Note: Indicate whether the target machine is 32 bit or 64 bit (only 64 bit machines are capable of pulling deltas).

3.2 StorageCraft Cloud File and Folder Restore

Recover files or folders from the cloud with the following steps:

1. Login to the StorageCraft portal: [MSPs All other users](#).
2. Click the StorageCraft Cloud Services tab
3. Click the Manage Devices button at the bottom of the cloud services page.
4. Click the Devices tab.
5. Select Files and Folders (from the Restore menu)
6. Select a Recovery Point
7. Provide the backup image password
8. Navigate to the file or folder to be recovered
9. Click the Download button next to the file or folder name
10. StorageCraft software zips the file(s) or folder(s) to streamline the download process
11. The file(s) or folder(s) are saved to the currently-defined default download folder.

The File and Folder recovery is complete. Manage the recovered file(s) or folder(s) like any Windows files or folders..

3.3 StorageCraft Cloud Virtualization

Use these steps to create a cloud VM (virtualize) from a cloud recovery point:




Important: Virtualizing in the cloud is a short term solution. StorageCraft suggests not to virtualize unless it is essential. A single device can be virtualized for no more than 30 days per calendar year. A substantial per-hour fee will be charged per device when the 30-day limit is exceeded. The time-charge for virtualizing even for a few minutes will be rounded up to the nearest day. For example: A device virtualized for 10 minutes a day for 30 days uses the maximum days per year.

StorageCraft has the option and right to turn a VM off if it has been live for more than 30 days.



Note: Additional virtualization information is found in the [virtualization workspace pages](#).

1. Login to the StorageCraft portal: [MSPs All other users](#).
2. Select the StorageCraft Cloud tab.
3. Select the account containing the device to be virtualized.
4. Click Manage devices on the bottom right.
5. Click the devices tab.
6. Select the device to be virtualized.
7. Select Virtualization in the left panel.
8. Select a recovery point
9. Click the Load button
10. Choose the number of CPU cores, amount of RAM (if applicable), network type, etc. in the right panel.
11. Click the Create VM button.
 1.  **Note: Set up the VPN now (if needed) so the virtualized device can be added to the [VPN configuration](#) then go to step 12. Skip to step 12 if a VPN won't be used.**
12. Type the backup image password then click Start VM.
13. Manage the VM by clicking Download RDP Link.
14. Click the Open button at the bottom of the browser.
15. If a dedicated [IP address](#) was not previously defined, define it now. Be sure to use a valid dedicated IP address.

Note: If prompted to install VirtualBox guest additions, follow the onscreen instructions and then restart the vm if prompted. VirtualBox guest additions are vm hardware drivers that prevent mouse ghosting and other problems.

16. Login and restart when prompted.

The Virtualization process is complete.

Understanding StorageCraft Cloud IP/VPN

You only need to configure a cloud IP address when you want a dedicated IP address for your cloud VM, or when you set up a VPN for your site during disaster recovery. Network Address Translation (NAT), if selected, auto-assigns an IP address for your VM. NAT blocks all traffic coming to the VM from the internet but allows the VM to access the internet (one-way communication). Dedicated IPs allow traffic in both directions.

If you need a dedicated IP address, contact StorageCraft support. An additional fee is required for a dedicated IP address. The dedicated IP address will be assigned to the cloud VM of your choice. Each VM requires a separate IP address. The dedicated IP address enables the VM to have full two-way communication. If NAT is used you only have the ability to send traffic from the VM.

Virtual private networks (VPN) are different from IP address. With VPN you can attach your cloud VMs to a virtual network (VPN = virtual private network). Your cloud VM (if you are using VPN) appears to be running in your own on-site network. This prevents exposing your VM directly to the internet as it would happen if you bridged to a dedicated IP address. With VPN, you control the access through your own on-site router/firewall configuration. It basically makes it seem as though the cloud VM is sitting with your other computers, routers and firewalls in your office. The following information helps make this a little clearer.

NAT - Best for testing your cloud VMs or bringing up machines that only need to make connections to other places on the internet, but not accept outside attempts to connect to the VM.

Note: You need to alter your DNS records in a data recovery scenario to point to the dedicated VM IP so communication is not interrupted.

VPN - Best when you are recovering an internal workstation or server that was within your on-site network and not directly exposed to the internet. With a VPN setup the restored machine can seem as though it never went down. It can be accessible the same way the original machine was. VPN is the most flexible solution because after you connect the VM to your site you can control it with your own internal network hardware as you did with the original machine. It is also the most complicated.

Configuring a StorageCraft Cloud VPN

VPN configuration:

1. Login to the cloud portal.
2. Click on the Networking tab
3. Click VPN config in the left menu. This shows the VPN configuration page.



Previously created VPNs are displayed in this menu. These VPNs can be managed.

Note: Turn the virtual machine device off before creating the VPN. Don't start a new vm if it has just been created until after the VPN is created.

4. Click the Create new VPN button. This displays the configuration options.



5. Enter the VPN configuration information. The fields are described below:
 - o Name - type in the name of your VPN
 - o Gateway address - type in the IP address to be used for the default gateway.

- Note: This can be any IP address range, but should be limited to the private ranges 10.x.172.192.x. These are ranged that shouldn't be used by anyone on the internet. Using IP addresses from other ranges could cause communication problems on the internet.
 - Network Address - This is the address of the network based on the mask and range selected. This should normally end in zero. For example if the gateway address is 10.0.0.1 and the subnet mask is 255.255.255.0 then the network address would be 10.0.0.0.
 - StorageCraft Cloud VMs - this drop down list shows the previously created VMs that can be selected for the VPN. At least one vm needs to be selected and added. Multiple VMs can be added if two or more devices need to communicate with each other.
6. Select the VM's to be added to the VPN from the StorageCraft Cloud VM's the drop down menu.

Each VM must be stopped before it will show up in the list.
Click the + icon to add the selected VM.

7. Create the Remote Devices.

Make an entry here for each remote device to be connected to the VPN.

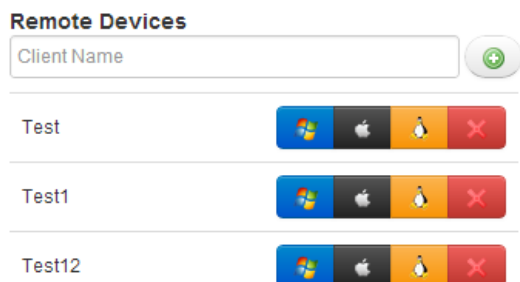
8. Click the Create icon.
9. The VPN will now show in the list of configured VPN's. By default it will be in the Stopped state.
10. Click Start to start the VPN.



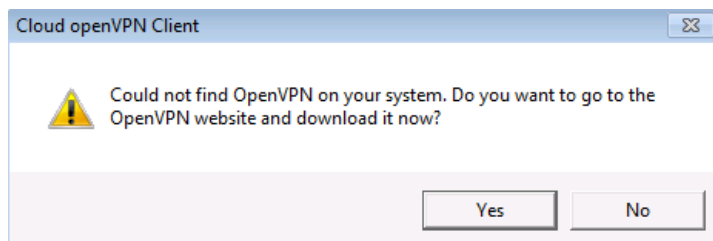
11. Start Each of the Cloud VM's.
12. Download the RDP shortcut and connect to the VM.
13. Send CTRL-ALT-DEL as a pass-through.

⚠ Note: If VB client tools have not been installed, the cursor alignment might be off. Install VB client tools and reboot the VM to fix the problem.

14. Remote Devices

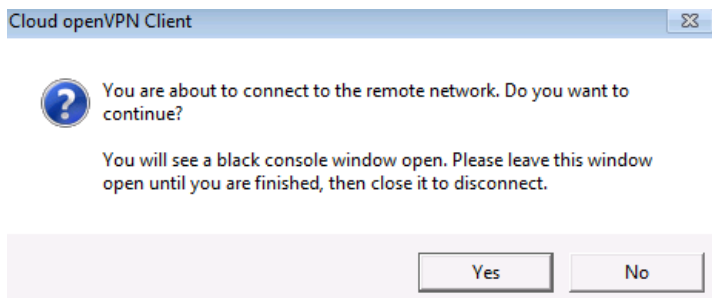


15. Run the current Windows installer from the Open VPN website (if necessary).



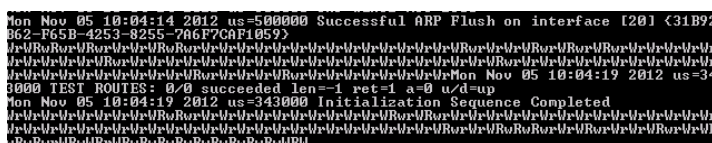
⚠ Note: Download only the 32-bit version of the [Open VPN Installer](#). Select either "Windows Installer openvpn-2.2.2-install.exe" or "Windows Installer (32-bit) openvpn-install-2.3.x.exe". The 64-bit openvpn client is not currently supported.

16. When the download is complete, run the "Open VPN installer" then proceed to the next step.
17. Connect to the remote network.

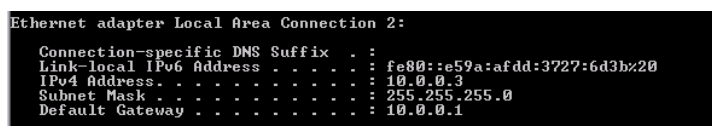


Select Yes. It opens a command prompt window. You should see a series of Wr rW characters scrolling past in the window. See the image below.

Note: The scrolling Wr rW characters means the connection to the VPN is active. This window needs to stay open to keep the VPN connection active.



18. Discover the IP address range.



Open a second command prompt window and type IPCONFIG. Look for the address in the command prompt.

19. When the vm is running in the cloud, use the IP address to access it with RDP.

3.4 Restarting the Cloud Backup Process

After a successful Bare Metal Restore:

StorageCraft Cloud services currently has no fail-back method. The backup image stored in the cloud becomes obsolete after the BMR is complete. The backup process must be restarted each time a BMR is performed.

The process is simple yet important:

1. Delete the old cloud device and all related recovery points.
2. Create a new cloud replication job in ImageManager.

4 StorageCraft Cloud Metrics and Reports

StorageCraft Cloud metrics and reports help you manage space and bandwidth usage by providing data about stored images, devices, drive requests and trends. This page describes how to access the metrics and reports and provides an overview of the data collected.

Accessing Metrics and Reports

You can view your data in the metrics charts in the StorageCraft portal. The images and descriptions below will help you find and understand the data you need. Users that have data or accounts in the cloud can view the information relative to the data or the accounts. Some of these screens may not be available based on your account type.

To access the [StorageCraft Cloud account details](#):

1. Login to the StorageCraft portal: [MSPs All other users](#).
2. Click the StorageCraft Cloud tab
3. Select the account or device you want from the left panel
4. Choose the cloud account metrics or cloud device metrics tab



Important: StorageCraft Cloud images (recovery points) are not compressed as much as locally managed backup image files. This allows almost instantaneous vm virtualization and easier file and folder access in the cloud. Cloud images are also compressed after they are encrypted for additional security. Locally managed StorageCraft backup images (non-cloud) are compressed before they are encrypted.

Account Metrics

If you selected cloud account, your options are:

- [Space utilization trends](#) - show the average space used over the past year
- [Current space utilized](#) - shows the current space used per account type
- [Current devices/tools in use](#) - shows various tools and the number of devices assigned to this account
 - Devices - shows the device count
 - IPs reserved - how many static/dedicated IP addresses are assigned to this account
 - VMs running - how many virtual machines are currently running
 - Seed drives requested - how many seed drive requests have been made by this account
 - BMRs requested - how many recovery drives have been requested by this account

Device Metrics

If you selected cloud devices, your options are:

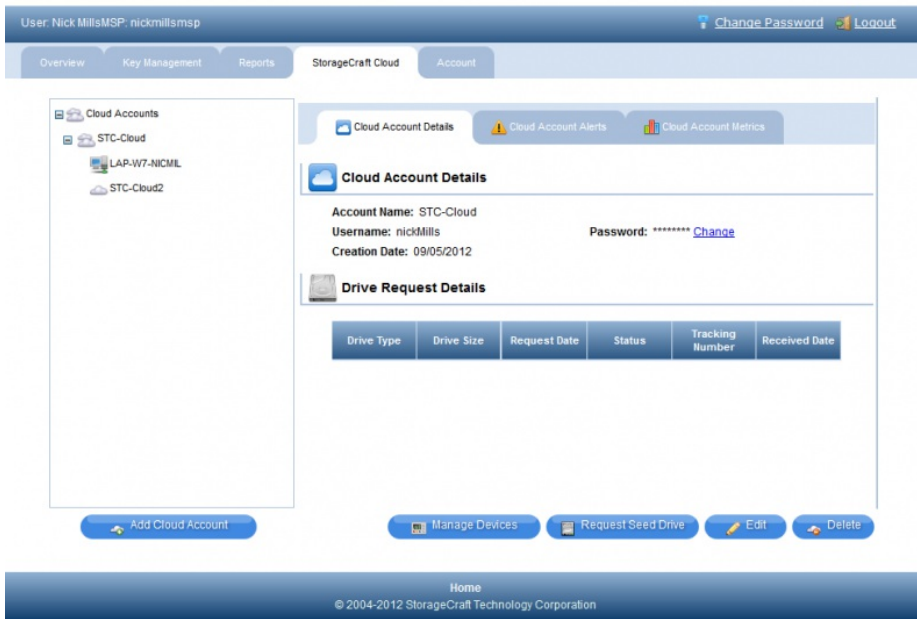
- [Space utilization trends](#) - illustrates the average space used over the past year
- [Current space utilized](#) - illustrates the current amount of space in use

Overview of collected data

- Data is collected every day for each account and device
- The data illustrated does not include the current day because a snapshot has not been taken
- The space utilization trend data is an average value calculated from the snapshots gathered in a one month period
- If no data is available, the charts will either say No Data to Load or consists of nonsense values such as NAN.
- The account metrics consist of data at the account level (includes all devices); the device metrics consist of data at each device's level

4.1 StorageCraft Cloud Account Details

This page shows a sample screen shot of the cloud account details in the StorageCraft Cloud tab. Information details may vary depending on your account type.



4.2 Account Space Utilization Trends

This image shows the cloud account metrics space utilization trends in the StorageCraft Cloud tab in the StorageCraft portal. Information displayed may vary based on your account type.



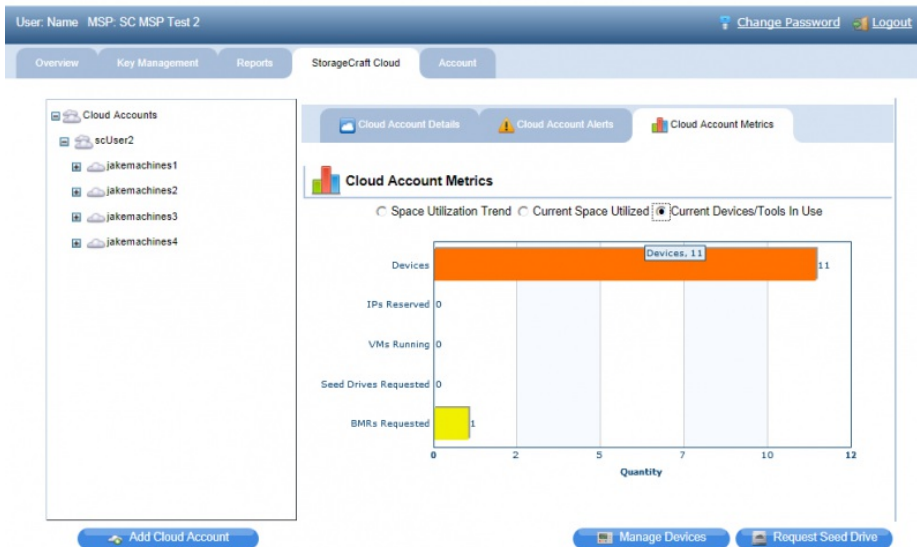
4.3 Current Account Space Utilized

This image shows the cloud account current space utilized in the StorageCraft Cloud tab. Information displayed may be different based on your account type.

STORAGECRAFT.
MSP PORTAL

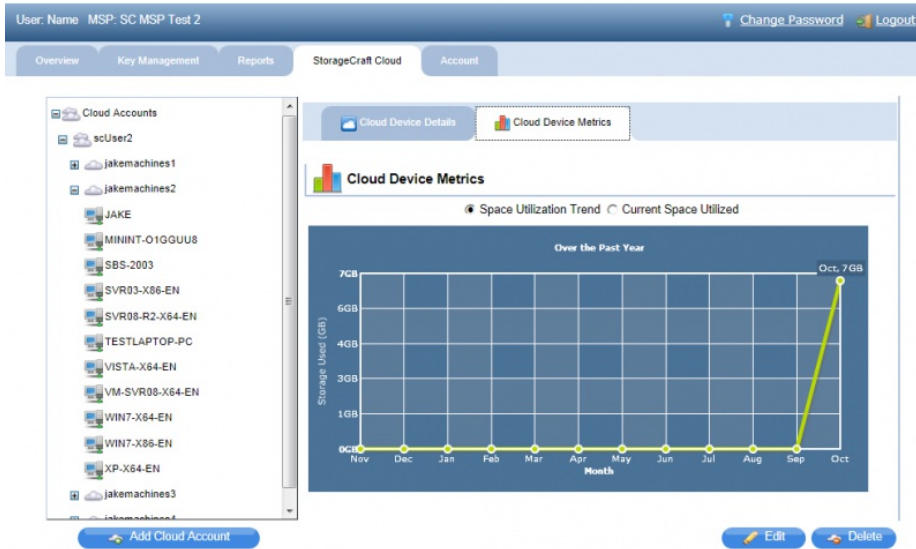

4.4 Current Account Devices/Tools in Use

This page shows a sample screen shot of the cloud account current devices and tools in use from the StorageCraft portal. Information displayed may vary based on your account type.

STORAGECRAFT.
MSP PORTAL


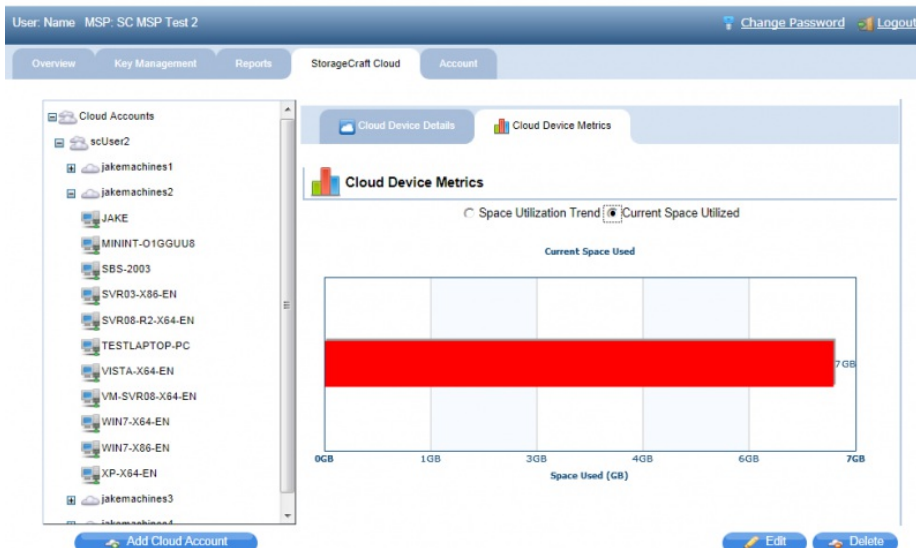
4.5 Device Space Utilization Trends

This image shows the cloud device metrics space utilization trends in the StorageCraft portal. Information displayed may vary based on your account type.

STORAGECRAFT.
MSP PORTAL


4.6 Current Device Space Utilized

This image shows the cloud device current space utilized in the cloud. Information displayed may vary based on your account type.

STORAGECRAFT.
MSP PORTAL


5 Tips and Tricks

The tips and tricks page contains links to help you find answers to your questions. The page includes links to the StorageCraft product glossary, Frequently asked questions (FAQ) and a troubleshooting page.

[Consolidated Glossary](#) - (combined glossary for ShadowProtect, ImageManager and Cloud Services).

[FAQ](#) - StorageCraft Cloud Services Frequently Asked Questions

[Troubleshooting](#) - Troubleshooting StorageCraft Cloud Services

If you can't find the answers you're looking for here, contact StorageCraft support via the [StorageCraft home page](#).

5.1 StorageCraft Cloud Services FAQ

What is the suggested way to Capture multiple volume backups?

You should use a single ShadowProtect backup job. If your virtualized backup in the cloud consists of multiple volumes we recommend that you capture all of these volumes with a single ShadowProtect backup job. This is a better than having multiple backup jobs that take snapshots of the different volumes. Using a single backup job is the only way to ensure that the recovery points in the cloud represent a complete single point in time.

How do I decide what service level to select (Basic, Plus, Premium)?

The StorageCraft Cloud Services service level determines the type of recovery supported by your cloud solution. Your organization's Recovery Time Objective (RTO) should determine the Cloud Services service level you select.

Cloud Basic (Data and System RTO > 1 day) Supports only a Bare Metal Restore (BMR) option for recovering data. This process involves copying your cloud data to a BMR drive and sending it to you via overnight mail. Once you have the drive, you can restore the system data as needed.

Cloud+ (Data RTO < 10 minutes; System RTO > 1 day) Supports both the BMR option provided by Cloud Basic, and file/folder recovery directly (via a browser) from the cloud. File/Folder recovery lets you recover data from the Cloud quickly and easily, but application/services recovery or full system recovery requires the slower BMR option.

Cloud Premium (Data and System RTO < 10 minutes) Supports file-folder recovery option, also provided by Cloud+, and system virtualization directly in the cloud. Cloud virtualization lets you fail over to a fully functional VM in the cloud almost instantly. The (BMR) process is also available for Cloud Premium customers.

Choose wisely when selecting a service level for your StorageCraft Cloud solution. All service level changes require seven days to complete. This means you can't jump up to Cloud Services Premium when disaster strikes if you suddenly need to virtualize in the cloud.

Carefully evaluate your organizational needs, based on RPO and RTO, then select a Cloud Services service level that supports those recovery needs.

How do I figure out how much storage space I need in the cloud?

StorageCraft Cloud Services replicates ShadowProtect backup image files to the cloud. This means you can use existing backup image files to estimate your StorageCraft Cloud storage needs.

The following simple formula can help you do this:

$$\text{Full} + (\Delta * \text{BDW} * \text{ST})$$

You should perform this calculation separately for each system you want to replicate to the cloud because some of the variables are system-specific.

Variable	Defintion
Full	The size of the systems full backup image, in MB or GB.
Δ (Delta)	The incremental change per day in system data. This is effectively the sum of the various incremental backup image files created during a day. However, make sure to use at least a 30-day average for this value to account for atypical spikes in system activity.
BDW	The number of business days per week. This is the number of days per week that ShadowProtect creates system backups.
ST	The amount of time, in weeks, that you want to maintain replicated data in the StorageCraft Cloud.

For example: an organization operates seven days a week, and wants to maintain replicated data in the cloud for 90 days. Its application server has the following characteristics:

SYS Volume: 100GB (Full backup image = 27GB, average daily incremental = .15GB)

APPS Volume: 1024GB (Full backup image = 192GB, average daily incremental = .39GB)

DATA Volume: 2048GB (Full backup image = 498GB, average daily incremental = 1.6GB)

The cloud storage estimate for this server is as follows:

$$(27 + 192 + 498) + ((.15 + .39 + 1.6) * 7 * 90) = 717\text{GB} + 1348\text{GB} = \mathbf{2065\text{GB (about 2.1TB)}}$$

When does rounding occur for storage space billing?

This applies to all MSP accounts. All space used by subaccounts at the same service level is aggregated first and then rounded up to the nearest GB for billing.

Do I have to use a seed drive to seed my cloud storage, or can I just replicate my full backup image across the network?

The question of seeding vs. replicating is really a question of image size vs. network bandwidth. It's possible to replicate a full image to the cloud if it doesn't compromise the performance of your network.

You can use the following formula to estimate the time required to replicate a particular backup image file:

$$((FS * 1024) / AB * 60) = \text{Time to transfer file (minutes)}$$

Variable	Definition
FS	Backup image file size in GB.
AB	The available bandwidth to transfer the file in MB/sec. This is likely less than the total network bandwidth since there is always other network activity that occupies some of the bandwidth.

For example, an organization with 28 Mbps available bandwidth wants to transfer a full backup image file of 410GB:

$$((410 * 1024) / 28 * 60) = \mathbf{249 \text{ minutes}}$$

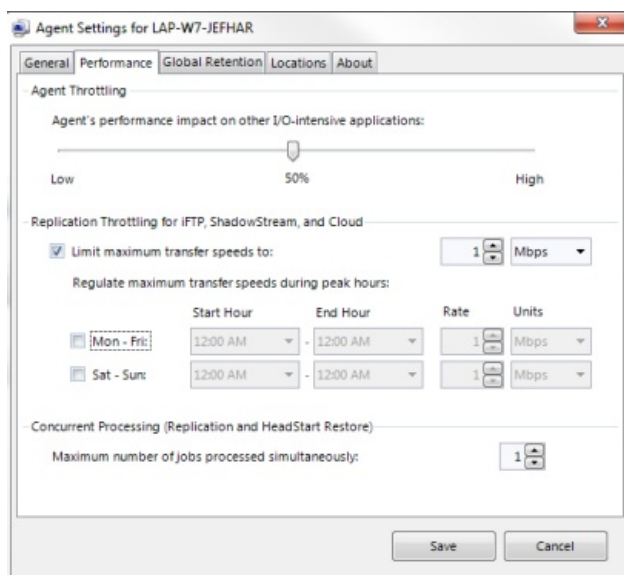
Why would I need to mirror my cloud data to a secondary location?

Mirroring to a secondary data center protects your data in case of a natural disaster that destroys the primary data center. For those who want to guarantee data recovery, regardless of disaster scope, mirroring provides the necessary peace-of-mind.

Can I manage cloud replication to avoid slowing down my network?

I'm concerned that using StorageCraft Cloud Services will adversely affect my network performance, especially during business hours.

StorageCraft ImageManager provides the ability to manage its use of network bandwidth for replication.



ImageManager replication throttling lets you control transfer speeds based on day (weekday vs. weekend) and time. This lets you manage network bandwidth loads during business hours or other critical times to make sure replication doesn't adversely affect other important business activities.

How do I manage IP addresses (including DHCP, DNS, etc.) when virtualizing into the cloud or failing back to my local site?

Manually Configuring an IP Address

The only time you need to worry about manually configuring a dedicated IP address is when you are setting up a VPN between your site and your VM. Typically this needs to be done during a disaster recovery. The IP address is attached to your cloud VM. NAT automatically assigns an IP address to the VM if you don't want to configure it manually.

Dedicated IP Addresses

If you need a dedicated IP address, request it from StorageCraft technical support via the cloud portal. The StorageCraft support engineers will explain everything you need to know and then assign the IP address to a specific cloud VM. The dedicated IP address gives your VM a direct open line (bi-directional) to the internet. This provides more functionality and better communication scenarios than NAT. NAT allows your VM to send outgoing internet traffic but blocks incoming traffic.

VPNs

Cloud VPN allows you to attach your cloud VMs to a virtual network (VPN – Virtual Private Network) in a way that allows your VMs to work as if they were part of the network at your office. With a VPN configuration your VMs don't need to be exposed directly to the network as happens when bridging to a dedicated IP address. You control access to your VM through your own on-site router/firewall configuration. In essence, it is as if your VM is on a machine in your local server room.

Networking Summary

NAT - Best for testing your cloud VMs or bringing up machines that only need to make connections on the internet, but not receive any connections.

Bridged to Dedicated IP - Best for web servers, web accessible database servers, and mail servers that are accessed from the internet. You need to change your DNS records in a disaster recovery scenario to point to the assigned dedicated IP for seamless communication.

VPN - Best when you are dealing with an internal workstation or server which is normally connected to your on-site network, and not directly exposed to the internet. With a VPN setup it can be as if the machine never went down. You can make it accessible the same way the original machine was. VPN is the most flexible option because after you connect your VM to your site, you can control it with your own internal network hardware the same way you controlled the original machine. However, it is also the most complicated.

Where does StorageCraft Cloud Services store backup image files?

StorageCraft Cloud Services utilizes SSAE 16 Type II-compliant datacenters located in Utah and Pennsylvania. StorageCraft Cloud Services are deployed on hardware and a networking infrastructure dedicated solely to StorageCraft Cloud Services.

What options are available to "seed" StorageCraft Cloud Services with base images?

All cloud users can request a seed drive from StorageCraft. Personal drives will not be accepted for seeding the cloud.

If a backup image runs as a virtual machine in the StorageCraft Cloud, how long can this virtual machine be kept in production mode?

A production virtual machine can run in StorageCraft Cloud Services for a maximum of 30 days. This allows for a controlled migration to replacement infrastructure of the partners' choosing.

What if I lose my connection during a sync between ImageManager and Cloud Services?

ImageManager tracks the data sent and knows where to start again when the connection is restored.

What happens if I delete an account in the cloud and want re-add that account?

Deleting an account erases all data and associated devices. You can create an account with the same name as a deleted account, but that is the end of the similarity.

Why can't I backup Windows 8 and Server 2012 images to the cloud with the initial release of the StorageCraft Cloud?

Windows 8 and Server 2012 replication to the StorageCraft Cloud requires an update to the cloud services software. This functionality will be available in cloud services early in 2013. The update will be transparent to users (you won't need to update ShadowProtect or ImageManager).

What is the turn around-time for getting the cloud seeded after the drive is received by StorageCraft?

A one (1) TB (or less) seed drive will be seeded within seven (7) calendar days after StorageCraft receives it. Drives larger than one (1) TB will require one (1) additional day per TB before the seeding is complete.

5.2 Troubleshooting StorageCraft Cloud Services

Adding New Volumes when "Collapses Only" are Being Replicated

When you select Replicate Collapses Only and later add a new drive or new volume, the volumes in the backup will be temporarily out of sync. The new volume causes a base image to be created. The new base image file is immediately replicated to the cloud which causes a new recovery point to be created. The new recovery point reflects the current state of the new volume. However, since incrementals are not being replicated (just collapses at the end of the day) the other (previously existing) volumes won't change until the day's collapse is replicated to the cloud.

Migration Steps:

1. Install ImageManger on the new machine.
2. Manage a folder containing the EXACT SAME image files the old machine was sending.

3. With help from STC support, edit the registry on the new machine so that the ManagedFolder ID is the EXACT SAME as the ManagedFolder ID on the old machine.
4. Restart the ImageManager Service.
5. Create a Cloud Location that uses the EXACT SAME credentials that were used previously.
6. Create a Replication target using the new location.