

Online Backup Manager v7

Cloud File Backup & Restore Guide for Windows

Copyright Notice

The use and copying of this product is subject to a license agreement. Any other use is prohibited. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system or translated into any language in any form by any means without prior written consent of THE SUPPLIER. Information in this manual is subject to change without notice and does not represent a commitment on the part of the vendor, THE SUPPLIER does not warrant that this document is error free. If you find any errors in this document, please report to THE SUPPLIER in writing.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

Trademarks

All product names are registered trademarks of their respective owners.

Disclaimer

THE SUPPLIER will not have or accept any liability, obligation or responsibility whatsoever for any loss, destruction or damage (including without limitation consequential loss, destruction or damage) however arising from or in respect of any use or misuse of reliance on this document. By reading and following the instructions in this document, you agree to accept unconditionally the terms of this Disclaimer and as they may be revised and/or amended from time to time by THE SUPPLIER without prior notice to you.

Table of Contents

1	Overview.....	1
1.1	About This Document.....	3
2	Preparing for Backup and Restore	4
2.1	Requirements and Recommendations.....	4
2.2	Best Practices and Recommendations	4
3	Login to OBM / CBS User Web Console.....	6
3.1	Login to OBM	6
3.2	Login to the CBS User Web Console.....	7
4	Creating a Cloud File Backup Set	8
4.1	Create a Cloud File Backup Set in OBM.....	8
4.2	Create a Cloud File Backup Set on the Web Console	17
5	Overview of Cloud File Backup	22
6	Running a Backup	24
6.1	Start a Manual Backup in OBM.....	24
6.2	Start a Manual Backup on the User Web Console	25
6.3	Configure Backup Schedule for Automated Backup in OBM.....	26
6.4	Configure Backup Schedule for Automated Backup on the Web Console	28
7	Restoring with a Cloud File Backup Set.....	30
7.1	Restore with OBM	30
7.2	Restore with the CBS Web Console	35

1 Overview



Selectable Backup Run Type

You can choose to either run the backup set you created on **Server** (CBS) or **Client** (OBM).

The run type of a cloud file backup set can only be set if you create a backup set via the CBS Web Console. For backup set created via the backup client application (i.e. OBM), the run type is set to Run on Client by default.

Run on Server

A Run on Server cloud file backup set provides you with an agentless backup solution. Manual or scheduled backup job is performed on the backup server (i.e. CBS); you do not need to install a backup agent on your personal computer in order to backup your data on cloud storages.

What are the benefits?

- ▶ **Physical Machine not Required**

Since the whole backup and restore process is done over the CBS server and therefore you do not need a physical machine at all.

- ▶ **Simplified Installation**

Unlike agent-based backup, you do not need to install the client backup agent on your computer or upgrade it when a newer version becomes available.

- ▶ **Simplified Administration**

With one software to manage (CBS, the backup server application), this allows administrator / user to manage backup and restore operations from a centralized console with lower time investment.

- ▶ **Compliance**

Some organizations cannot install client agents due to regulatory requirements. An agentless solution allows for compliance during backup or restore.

- ▶ **Consistency and Recoverability**

Backup client agent could interfere with the processing power of core applications of the machines that it is installed on. Run on Server cloud file backup job is performed on the backup server, which does not consume resources on client computer during a backup job.

The advantages of agentless backup technology make it a good option for administrators / users who want to simplify the backup and restore management.

Run on Client

A Run on Client cloud file backup set provides you with an agent-based backup solution. Manual or scheduled backup job is performed on the client computer (i.e. OBM); you need to install a backup agent on your personal computer in order to back up your data on cloud storages.

What are the benefits?

Robustness

In the event of a failure to a single backup agent, it fails in isolation to other users' environment.

Industry standard requires minimal learning curve

Agent-based backup is the traditional backup approach that is well understood by most administrators and end users whom would only need minimal effort and time to understand the backup and restore process and operations.

Performance

Unlike an agentless backup, where backup / restore operations of all users are performed on the backup server which may have multiple jobs to run at the same time, resulting in slower performance. Agent-based backup is performed on your computer with resources that is dedicated for your own backup and restores.

The advantages of agent-based backup technology make it a good option for users who want to have more control on individual backup / restore and resources management.

With both **Run on Server** (agentless) and **Run on Client** (agent-based) backup options available and the freedom to use different setting on different backup sets according to your needs, our backup solution offers you with high level of flexibility and efficiency for cloud file backup and restore.

1.1 About This Document

What is the purpose of this document?

This document aims at providing all necessary information for you to get started with setting up your system for Cloud File backup and restore, followed by step-by-step instructions on creating backup set, running backup job and restoring backed up data, using both the OBM and CBS Web User Console.

The document can be divided into 3 main parts.

Part 1: Preparing for Cloud File Backup & Restore

Requirements

Requirements on hardware & software for installation

Best Practices and Recommendations

Items recommended to pay attention to before backup and restore

Part 2: Performing Cloud File Backup

Logging in to Client Agent or User Web Console

Log in to OBM or User Web Console

Creating a Backup Set

Create a backup set using OBM and User Web Console

Running a Backup Set

Run a backup set using the OBM and User Web Console

Configuring an Automated Backup

Configure backup schedule for automated backup

Part 3: Restoring Cloud File Backup

Restoring a Backup Set using OBM & User Web Console

Restore a backup using the OBM and User Web Console

2 Preparing for Backup and Restore

2.1 Requirements and Recommendations

Ensure that the following requirements are met:

🔹 OBM Installation

Make sure that OBM is installed on a computer with Internet access for connection to the cloud storage.

🔹 Access for CBS User Web Console

It is now possible to perform agentless backup and restore, which can be done via the CBS User Web Console without using the OBM client agent. In order to access the User Web Console, make sure you have Internet connection and a web browser installed on your computer or mobile device.

🔹 Backup Quota Requirement

Make sure that your OBM user account has sufficient quota assigned to accommodate the storage for the Cloud File backup. Contact your backup service provider for details.

2.2 Best Practices and Recommendations

The following are some best practices or recommendations we strongly recommend you to follow before you start any Cloud File backup and restore.

🔹 Temporary Directory Folder Location (For backup and restore running on OBM only)

Temporary directory folder is used by OBM for storing backup set index files and any incremental or differential backup files generated during a backup job. To ensure optimal backup/restoration performance, it is recommended that the temporary directory folder is set to a local drive.

🔹 Performance Recommendations

Consider the following best practices for optimized performance of the backup operations:

- Schedule backup jobs when system activity is low to achieve the best possible performance.
- Perform test restores periodically to ensure your backup is set up and performed properly. Performing recovery test can also help identify potential issues or gaps in your recovery plan. It's important that you do not try to make the test easier, as the objective of a successful test is not

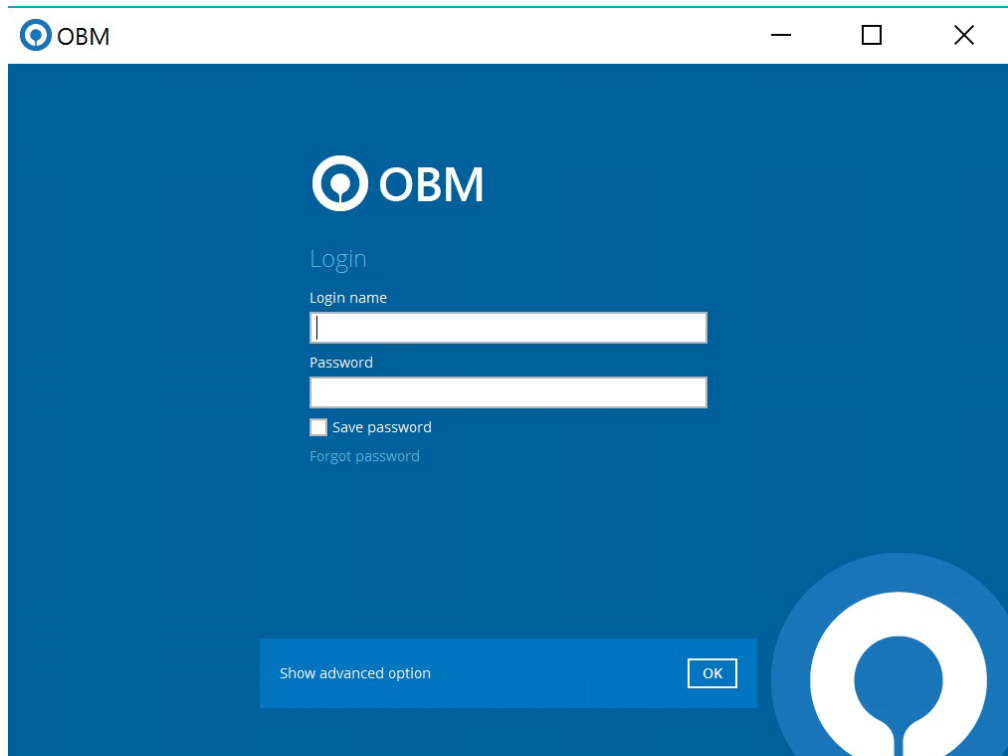
to demonstrate that everything is flawless. There might be flaws identified in the plan throughout the test and it is important to identify those flaws.

3 Login to OBM / CBS User Web Console

3.1 Login to OBM

1. Login to the OBM application user interface.

For client installation on Windows, double click the OBM desktop icon to launch the application.

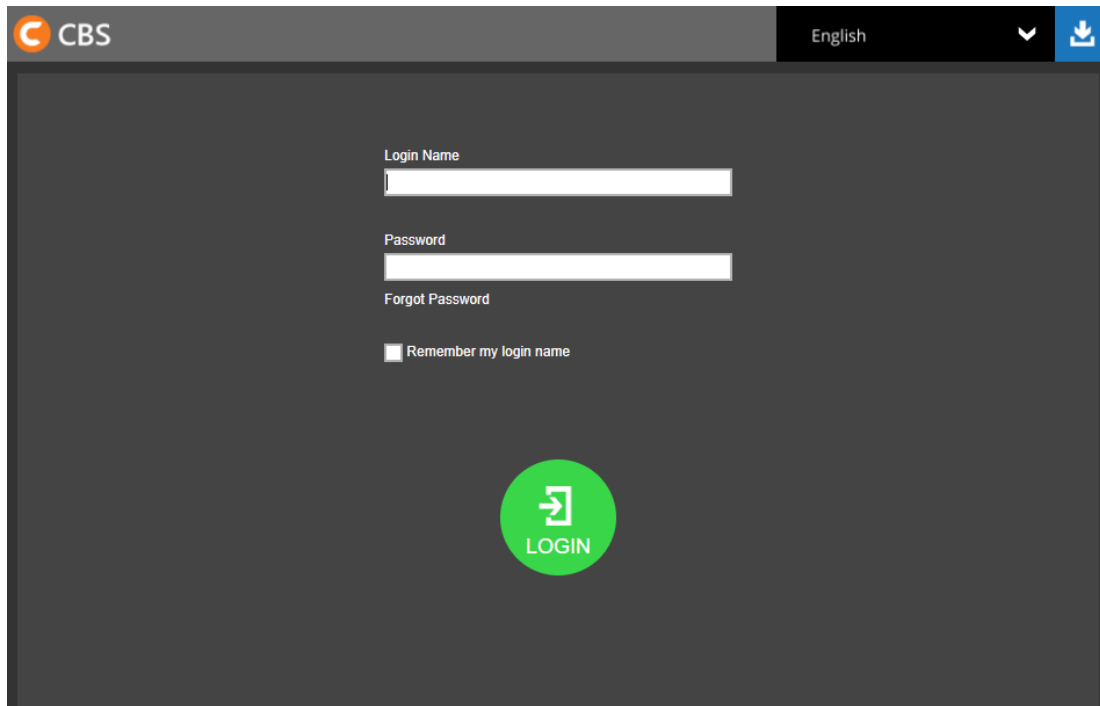


2. Enter the **Login name** and **Password** of your OBM account.
3. Click **Show advanced option** to configure the **Backup Server** and **Proxy** details if necessary.
4. Click **OK** afterward to login to OBM.

3.2 Login to the CBS User Web Console

1. Login to the CBS web console at

<https://cluster.backupserver.cloud>



The screenshot shows the CBS User Web Console login interface. At the top left is the CBS logo (an orange 'C' followed by 'CBS'). To the right of the logo is a dark grey bar containing the text 'English' and a downward arrow. Further right is a blue button with a white download icon. The main content area is dark grey and contains the following elements: a 'Login Name' label above a white text input field; a 'Password' label above a white text input field; a 'Forgot Password' link; a checkbox labeled 'Remember my login name'; and a large green circular button with a white right-pointing arrow icon and the word 'LOGIN' in white capital letters.

2. Enter the **Login Name** and **Password** of your OBM account.
3. Click **Login** afterward to login to the web console.

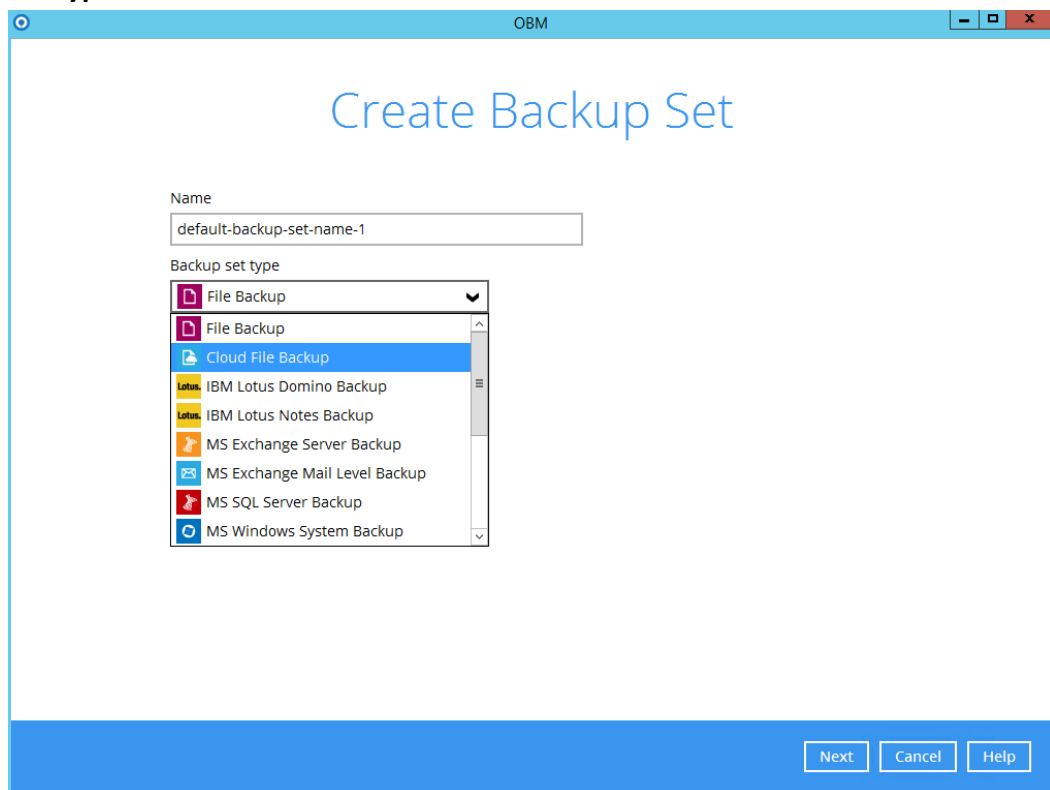
4 Creating a Cloud File Backup Set

4.1 Create a Cloud File Backup Set in OBM

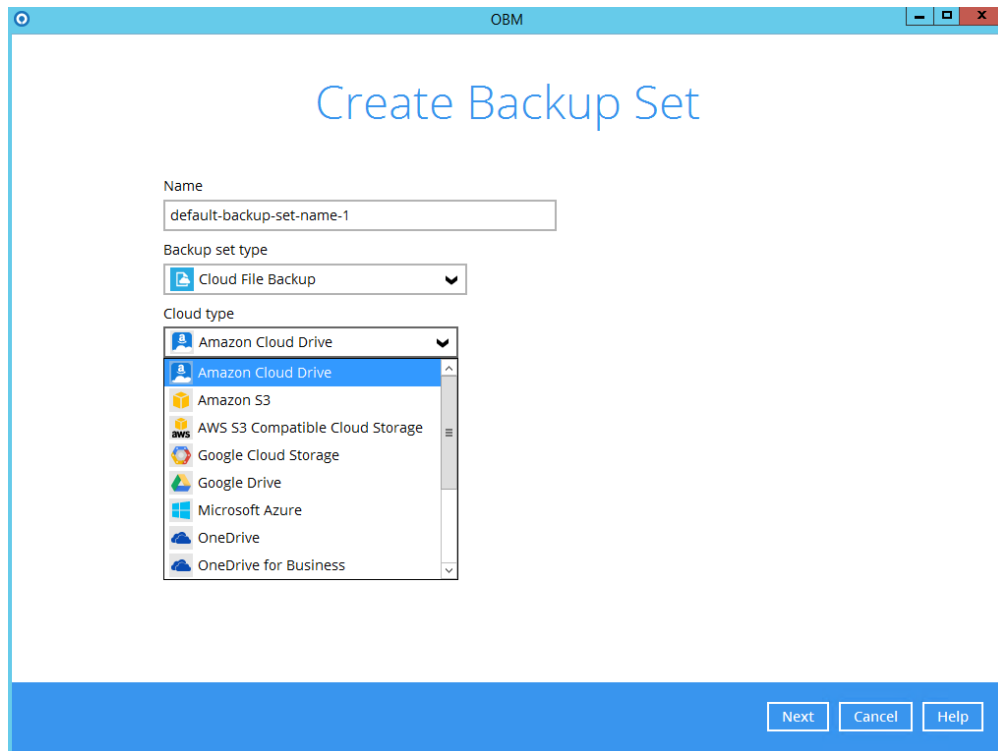
1. In the OBM main interface, click **Backup Sets**.



2. Create a Cloud File backup set by clicking the “+” icon next to **Add new backup set**.
3. Enter a **Name** for your backup set and select **Cloud File Backup** as the **Backup set type**.



4. Select the **Cloud type** of the cloud storage that contain the data that you want to backup.

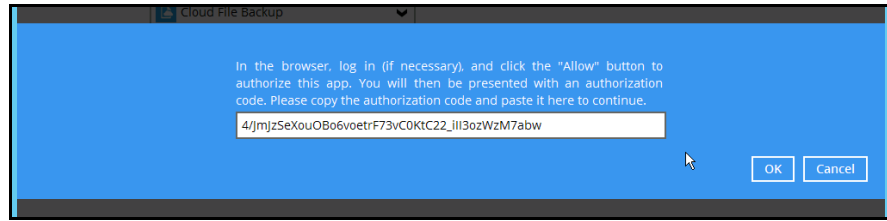


5. Depending on the cloud type you have selected, you will be prompted to enter the cloud service login details in either way below.

- Enter the login details on the current page in OBM, then click **Test** to validate your account information. A confirmation text **Test completed successfully** shows when OBM is connected to the cloud service successfully. If you need to route through proxy server to access the Internet, enable the **Access the Internet through proxy** checkbox to configure the settings.

-OR-

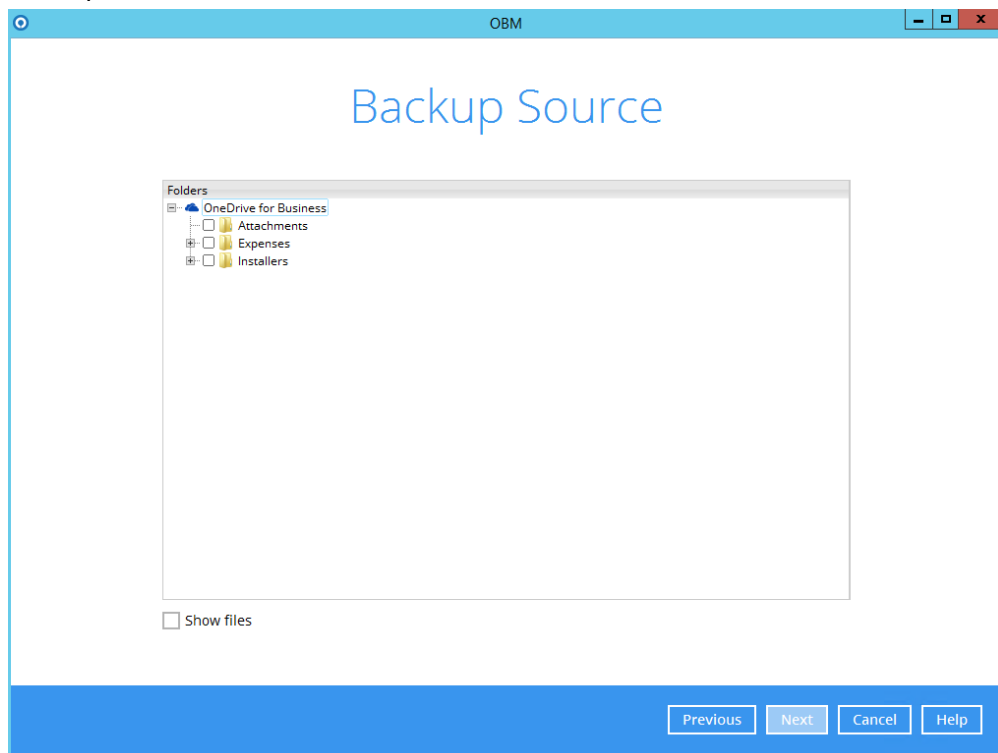
- Click **Test** to get redirected to the login page of the cloud service provider on your default browser, then enter the login details there. Click **Allow** to permit OBM to access the cloud storage. Copy and paste the code generated by the cloud service provider to OBM where you will be prompted to enter, then click **OK** to confirm.



IMPORTANT

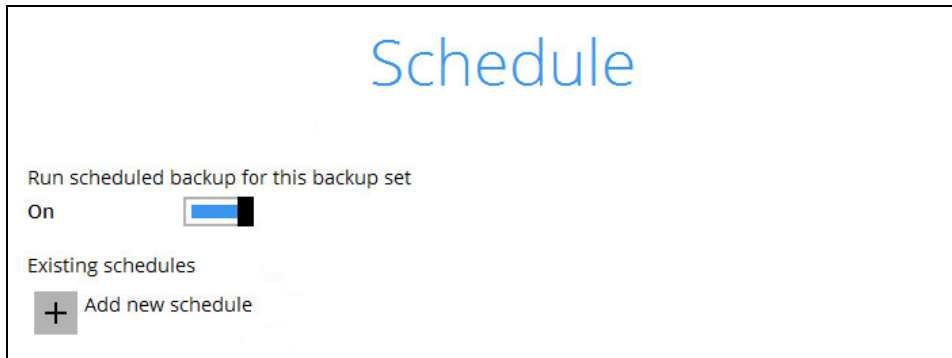
The authentication request will be opened in a new tab / window on the browser, ensure that the pop-up tab / window is not blocked (e.g. pop-up blocker in your browser).

6. In the **Backup Source** menu, select the folder / files that you would like to backup.



Enable the **Show files** checkbox at the bottom left corner if you would like to choose individual file for backup. Click **Next** to proceed when you are done with the selection.

7. In the **Schedule** menu, configure a backup schedule for backup job to run automatically at your specified time interval. Click **Add new schedule** to add a new schedule, then click **Next** to proceed afterward.



Schedule

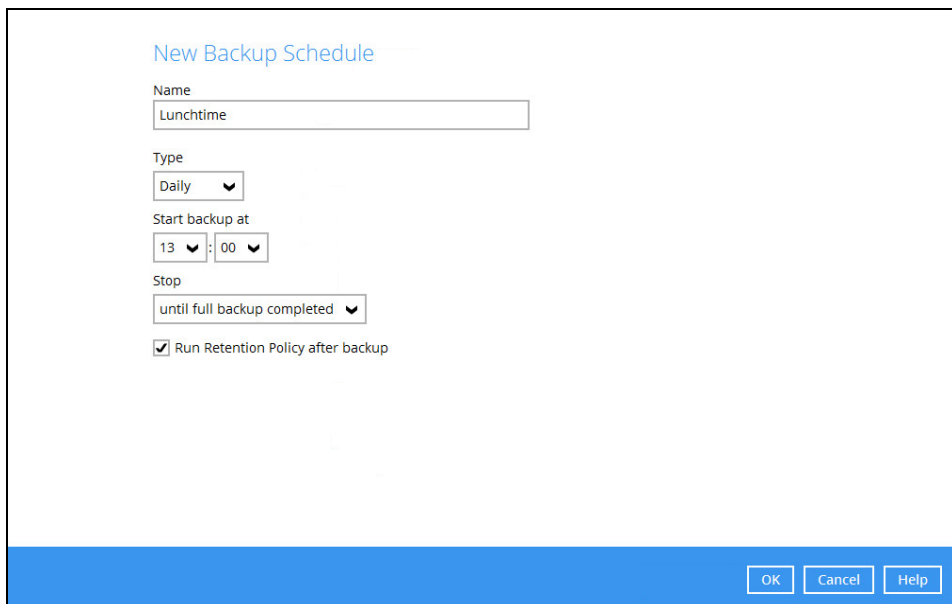
Run scheduled backup for this backup set

On ☐

Existing schedules

+ Add new schedule

Configure the backup schedule settings on this page, then click **OK** when you are done with the settings, then click **Next** to proceed.



New Backup Schedule

Name
Lunchtime

Type
Daily

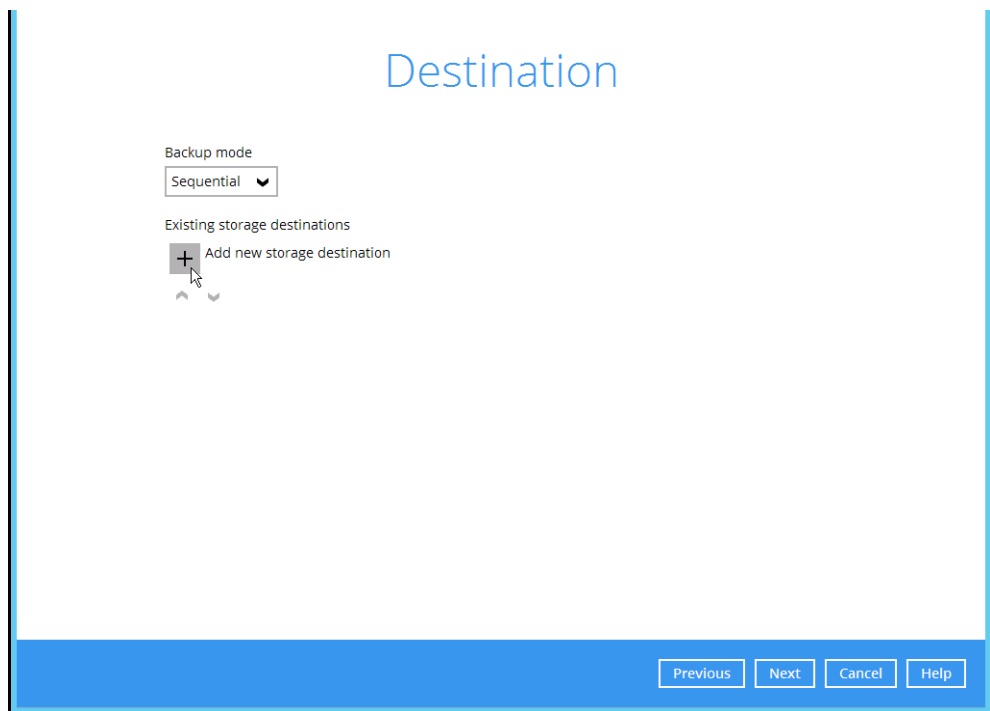
Start backup at
13 : 00

Stop
until full backup completed

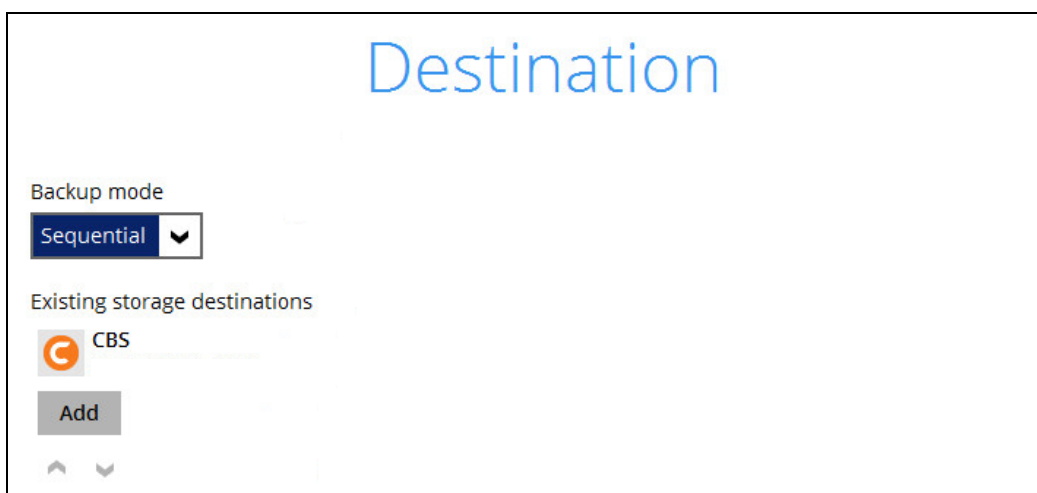
☒ Run Retention Policy after backup

OK Cancel Help

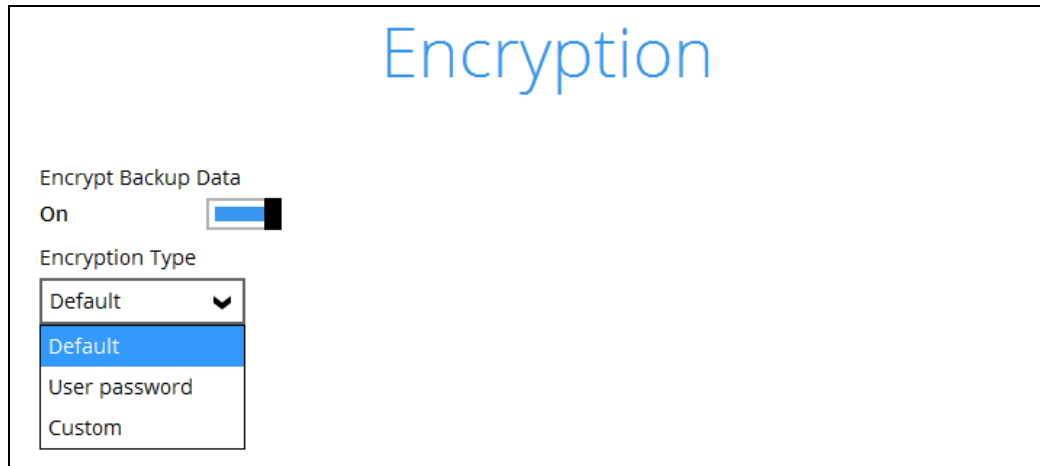
8. The Destination Window will appear:



9. In the Destination menu select CBS or CBS & Local / Mapped Drive / Removable Drive.
10. You can add multiple storage destinations (e.g. CBS and Local USB Drive). The backup data will be uploaded to all the destinations you have selected in the order you added them. Press the   icon to alter the order. Click **Next** to proceed when you are done with the selection.
11. In the Destination window, your selected storage destination will be shown.



12. In the Encryption window, the default **Encrypt Backup Data** option is enabled with an encryption key preset by the system which provides the most secure protection.



You can choose from one of the following three Encryption Type options:

- **Default** – an encryption key with 44 alpha numeric characters will be randomly generated by the system
- **User password** – the encryption key will be the same as the login password of your OBM at the time when this backup set is created. Please be reminded that if you change the OBM login password later, the encryption keys of the backup sets previously created with this encryption type will remain unchanged.
- **Custom** – you can customize your encryption key, where you can set your own algorithm, encryption key, method and key length.

Encryption

Encrypt Backup Data
On ☒

Encryption Type
Custom ▼

Algorithm
AES ▼

Encryption key

Re-enter encryption key

Method
☐ ECB ☒ CBC

Key length
☐ 128-bit ☒ 256-bit

Click **Next** when you are done setting.

13. If you have enabled the Encryption Key feature in the previous step, the following pop-up window shows, no matter which encryption type you have selected.

Encryption

Encrypt Backup Data
On ☒

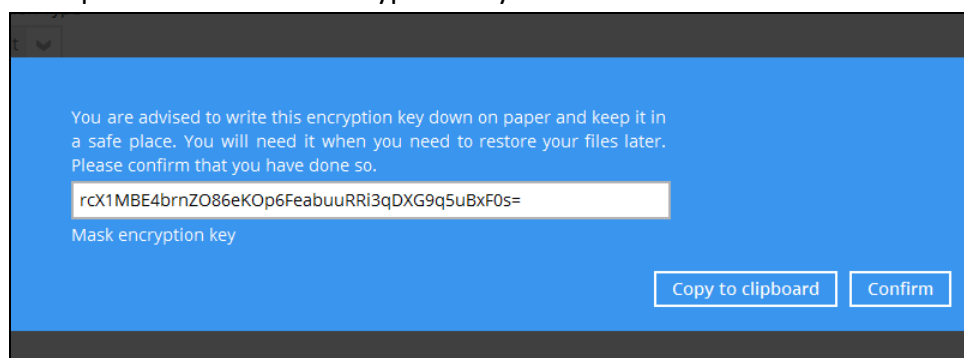
Encryption Type
Default ▼

You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later. Please confirm that you have done so.

Unmask encryption key

The pop-up window has the following three options to choose from:

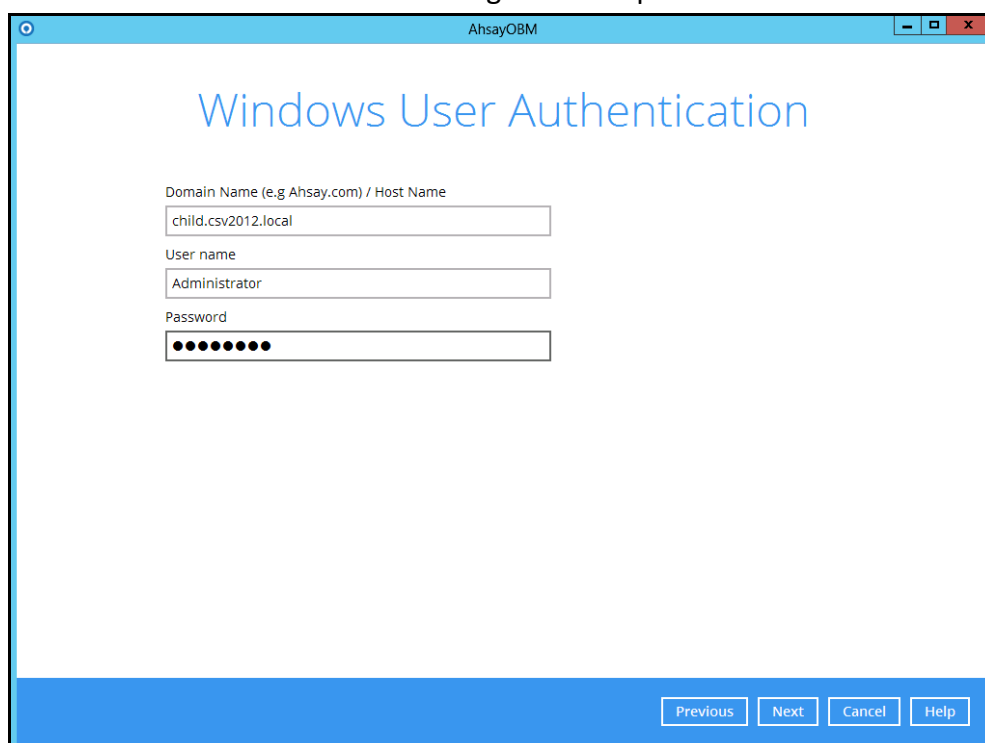
- **Unmask encryption key** – The encryption key is masked by default. Click this option to show the encryption key.



- **Copy to clipboard** – Click to copy the encryption key, then you can paste it in another location of your choice.
- **Confirm** – Click to exit this pop-up window and proceed to the next step

WARNING: If a note of the encryption key is NOT taken and the machine the key(s) are on has a major failure VSL will NOT be able to provide the key, and the data will not be restorable.

14. Enter the **Domain Name / Host Name**, **User Name** and **Password** of the Windows account that will be running the backup.

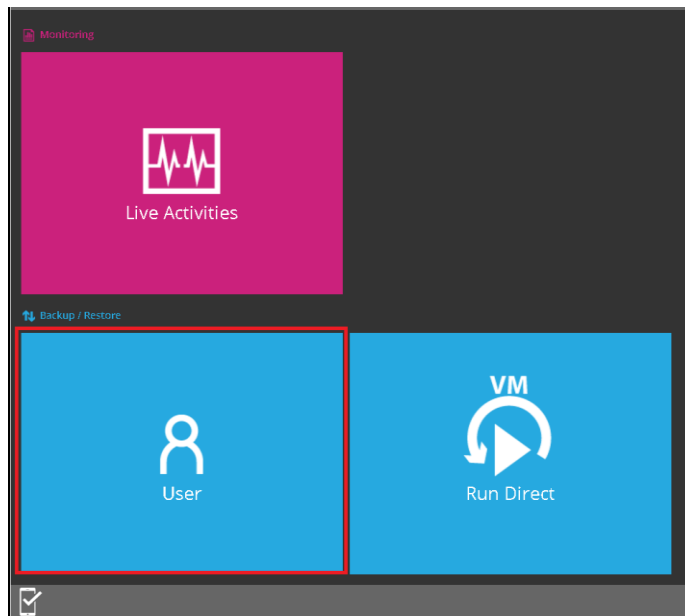


Note: *This menu will only be displayed for backup set with backup schedule configured (for installation on Windows).*

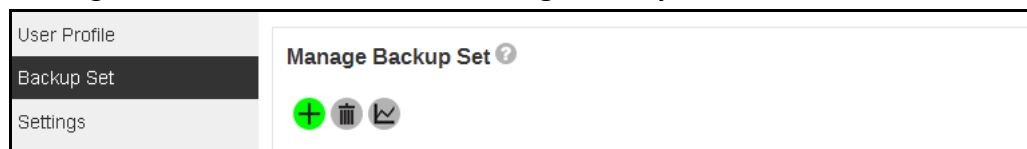
15. Click **Next** to create the backup set.

4.2 Create a Cloud File Backup Set on the Web Console

1. Log in to the User Web Console according to the instructions in [Login to the CBS User Web Console](#).
2. Click the **User** icon on the User Web Console landing page.



3. Select **Backup Set** from the left panel, then create a Cloud File backup set by clicking the circular “+” icon under **Manage Backup Set**.



4. Select **Cloud File Backup** as the **Type**, and enter a **Name** for the backup set.

Add New Backup Set

General

Name

Server Run Cloud File Backup

Owner

Type

Cloud File Backup

5. On the same menu under **Run on**, select **Server** to create a run on server (agentless backup) backup set or **Client** to create a run on client (agent-based backup) backup set.

- **Server** - If you choose to run the backup set on the CBS server, you won't be able to back up, restore or manage your backups on the OBM once the backup set is created.
- **Client** - If you choose to run the backup set on the OBM, you won't be able to back up, restore or manage your backups on the CBS Web Management Console once the backup is created.

Run on

☒ Server ☐ Client

Notes

1. This setting **CANNOT** be altered once the backup set is created. If you wish to change the backup method later, you will have to create a new backup set and start over the configurations again.

6. Select the cloud storage that contains the data that you want to backup under **Backup From**. Click **Test** afterward to authenticate CBS / OBM to access the cloud storage.

Backup From

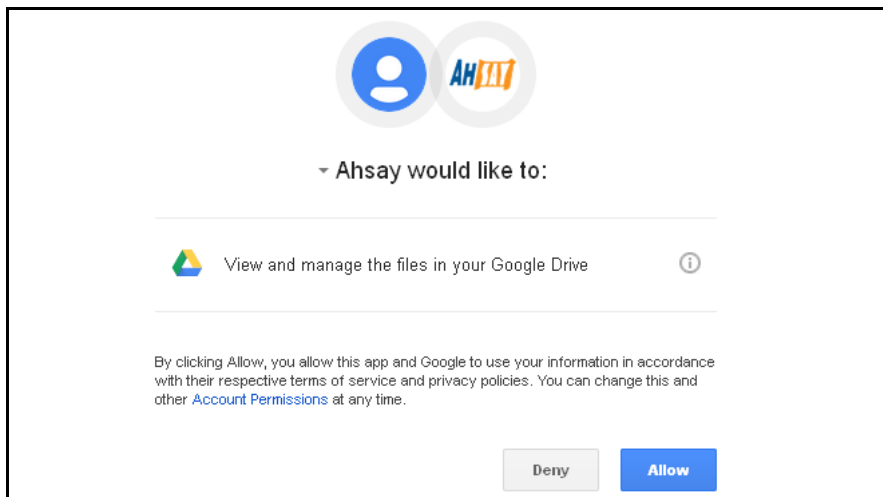
Google Drive 

Test

IMPORTANT

The authentication request will be opened in a new tab / window on the browser, ensure that the pop-up tab / window is not blocked (e.g. pop-up blocker in your browser).

7. Click **Allow** to permit access the cloud storage.



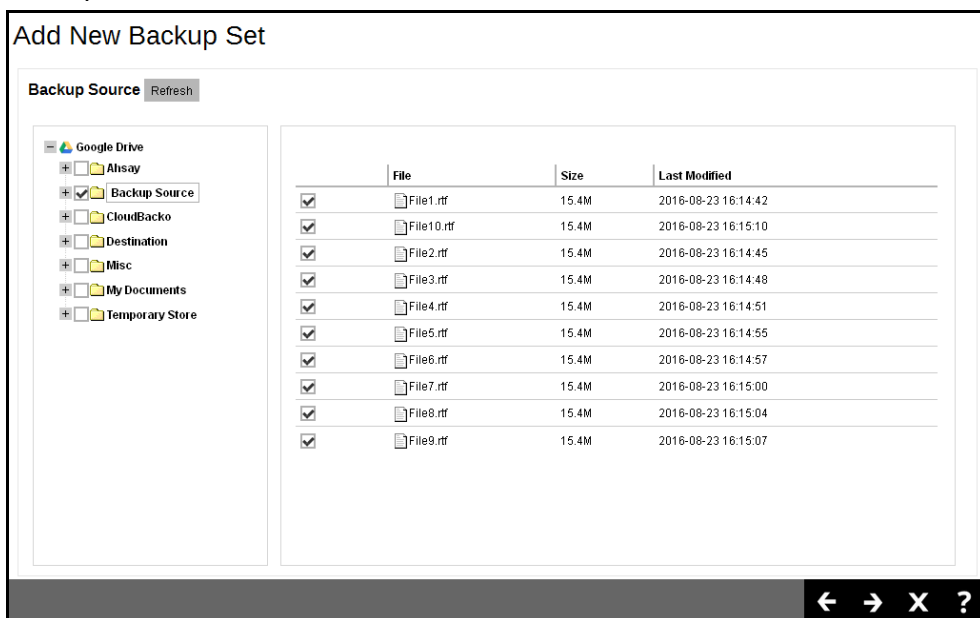
Enter the **Authentication code** returned on the web console to complete the authentication setup.

Authorization code

Ht3CXN3N0HCQjmgivi291ha_94PgZxC6HnNm6DA

Test

8. In the **Backup Source** menu, select the folder / files that you would like to backup.



9. In the **Schedule** menu, configure a backup schedule for backup job to run automatically at your specified time interval. Slide the on/off button to turn on this feature. Click the + icon under **Manage Schedule** to add a new schedule, then click **Next** to proceed afterward.

10. For **Run on Client** Cloud File backup set, select a predefined backup destination where the backup data will be stored. Click the “+” icon under **Predefined Destination**.

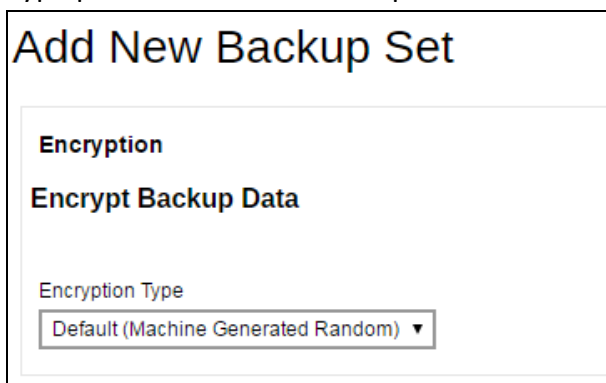
IMPORTANT

The **Destination** menu will only be displayed for **Run on Client** Cloud File backup set. For **Run on Server** Cloud File backup set, the destination will automatically be set to the backup server (CBS), the destination is not configurable.

If you would like to create a **Run on Client** Cloud File backup set with a standard backup destination, please create the backup set via the OBM user interface instead.

Select the corresponding predefined destination, and then click **Add**. Click **Next** to proceed afterward.

11. By default, the **Encrypt Backup Data** option is enabled with the Encryption Type preset as **Default** which provides the most secure protection.



The screenshot shows a web form titled "Add New Backup Set". Under the "Encryption" section, the "Encrypt Backup Data" checkbox is checked. Below it, the "Encryption Type" is set to "Default (Machine Generated Random)" in a dropdown menu.

You can choose from one of the following three Encryption Type options:

- **Default (Machine Generated Random)** – an encryption key with 44 alpha numeric characters will be randomly generated by the system
- **User password** – the encryption key will be the same as the login password of your ACB at the time when this backup set is created. Please be reminded that if you change the ACB login password later, the encryption keys of the backup sets previously created with this encryption type will remain unchanged.

- **Custom** – you can customize your encryption key, where you can set your own algorithm, encryption key, method and key length.

Add New Backup Set

Encryption

Encrypt Backup Data

Encryption Type

Custom

Algorithm

AES

Encrypting key

Re-type encrypting key

Method

☐ ECB ☒ CBC

Key length

☐ 128-bit ☒ 256-bit

Click the green  icon at the bottom right corner to confirm the backup schedule once you finish setting.

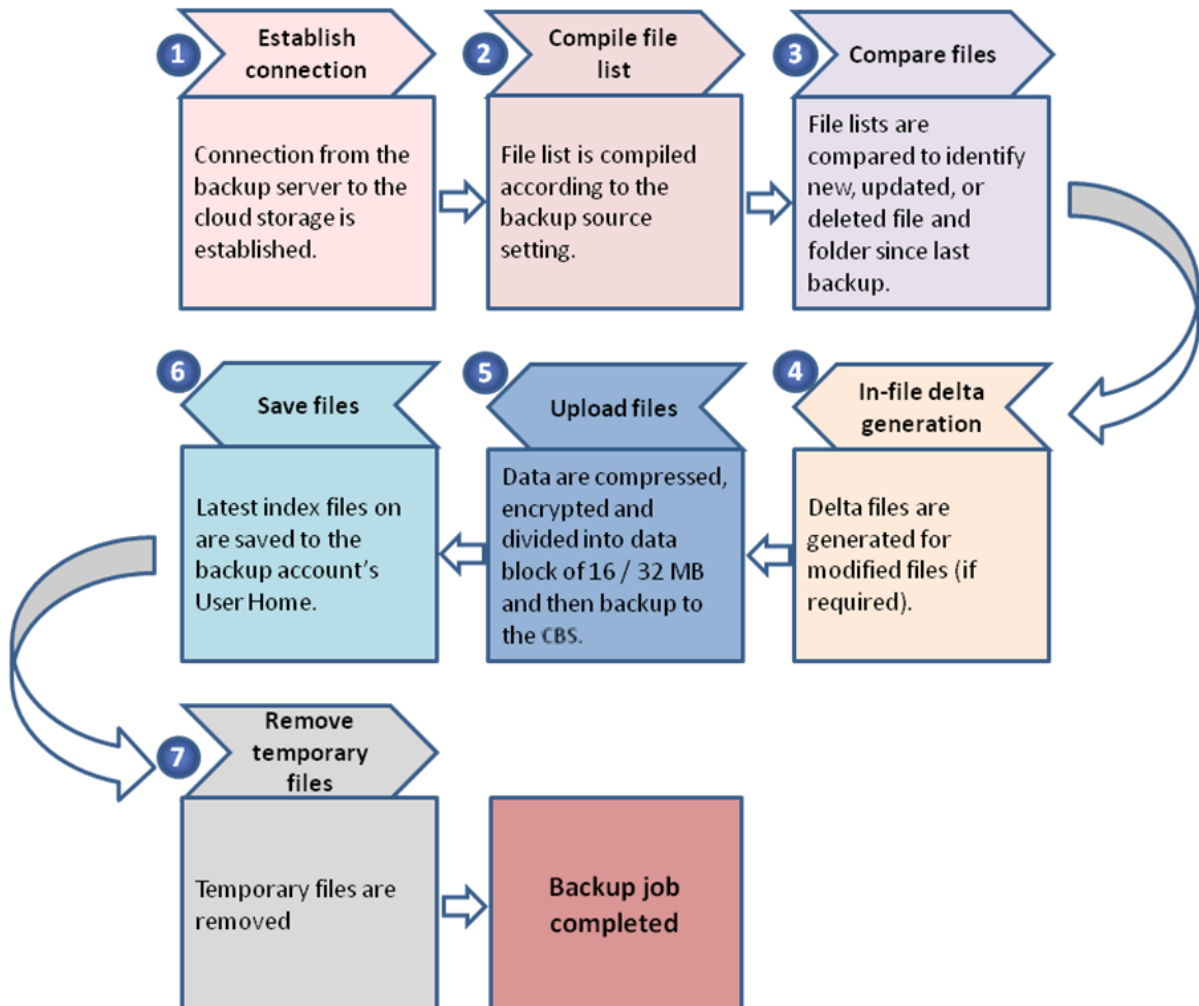
WARNING: If a note of the encryption key is NOT taken and the machine the key(s) are on has a major failure VSL will NOT be able to provide the key, and the data will not be restorable.

12. Click the  icon at the bottom right corner to confirm creating this backup set.

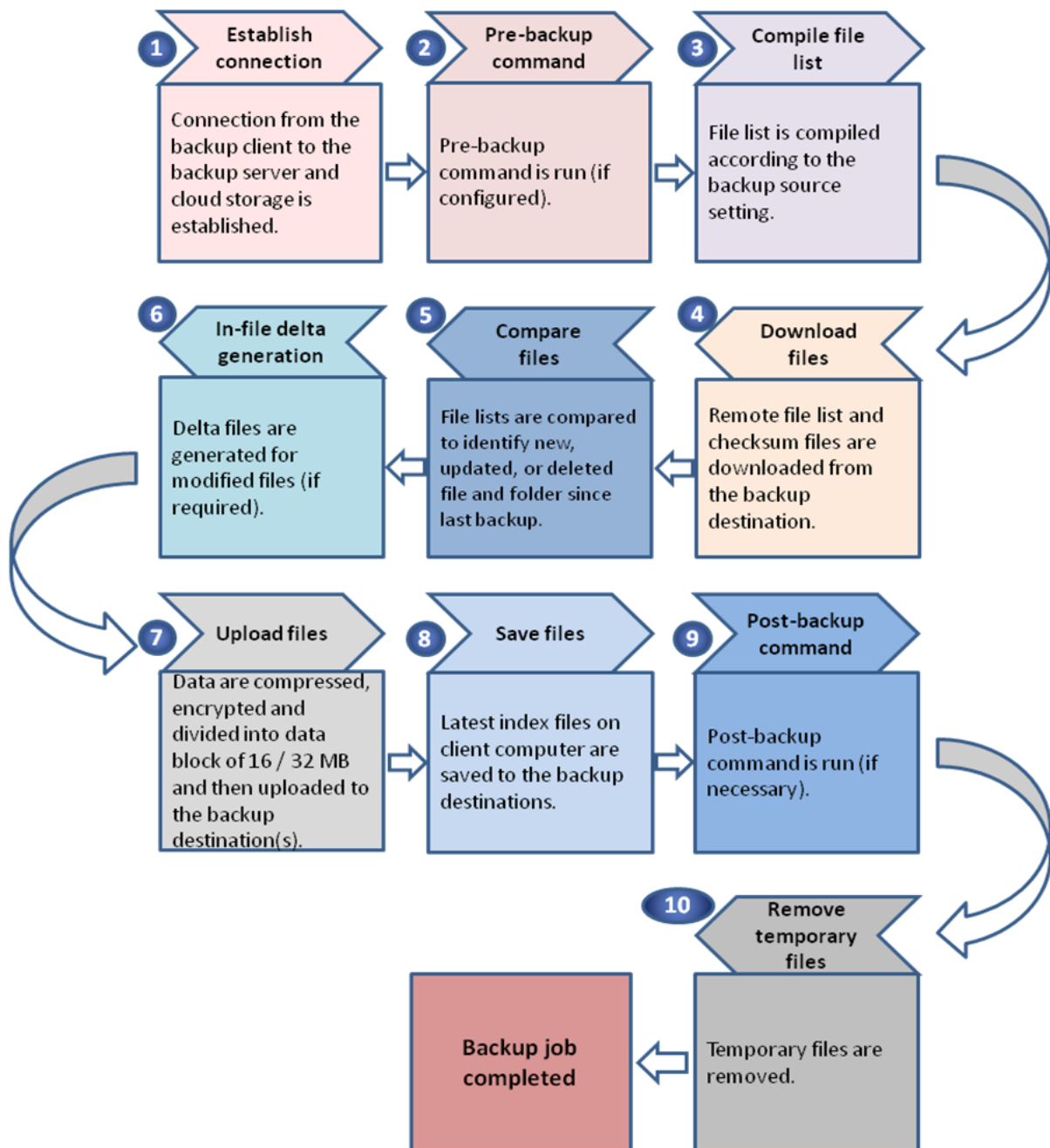
5 Overview of Cloud File Backup

The following steps are performed during a cloud file backup job:

Run on Server Cloud File Backup



Run on Client Cloud File Backup



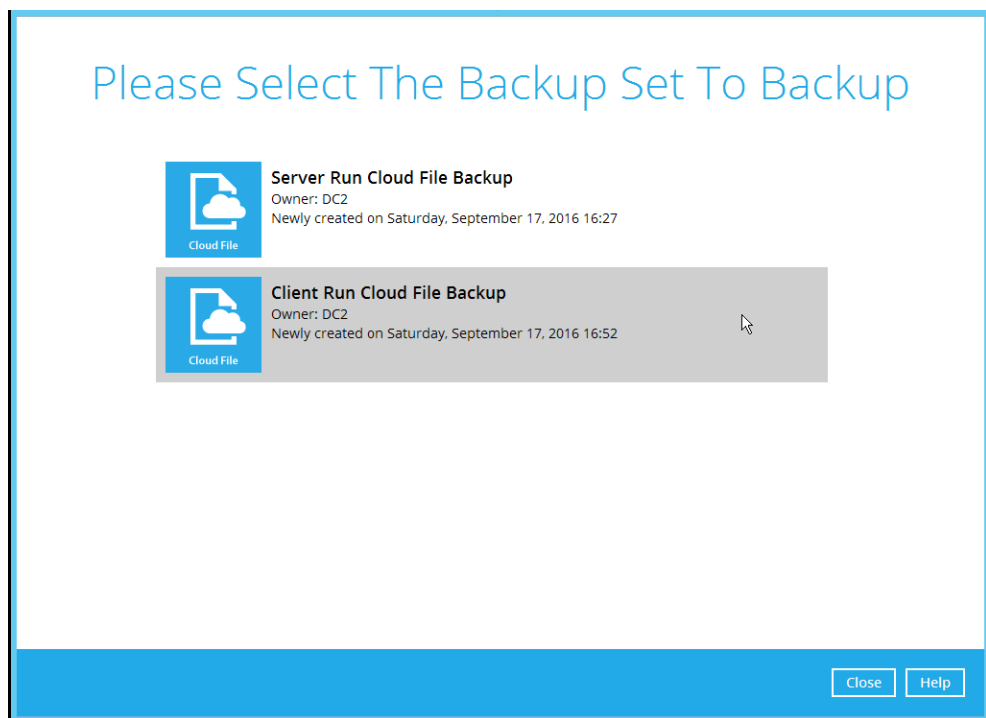
6 Running a Backup

6.1 Start a Manual Backup in OBM

1. Click the **Backup** icon on the main interface of OBM.



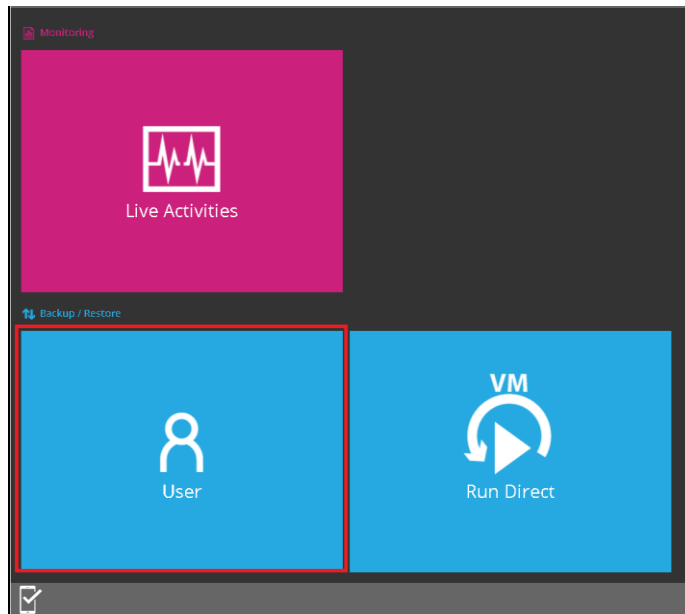
2. Select the backup set which you would like to start a backup for.



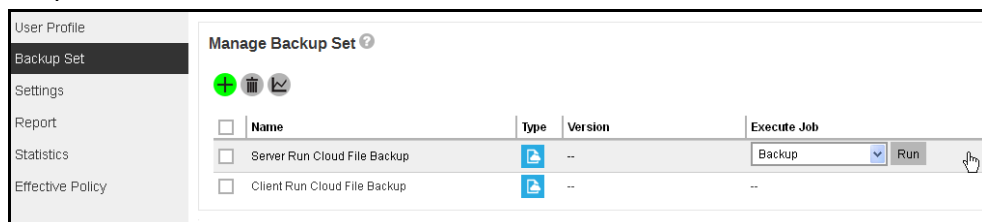
3. If you would like to modify the In-File Delta type, Destinations and Retention Policy Settings, click **Show advanced option**.
4. Click **Backup** to start the backup.

6.2 Start a Manual Backup on the User Web Console

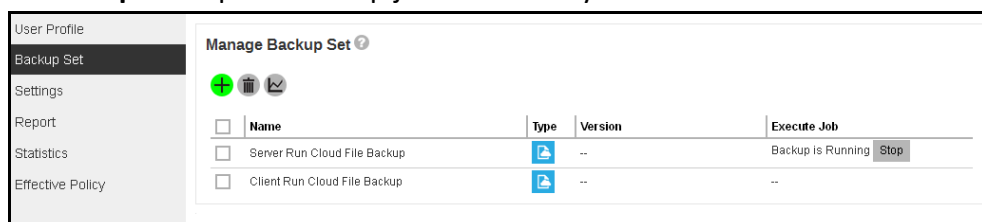
1. Log in to the User Web Console according to the instructions in [Login to the CBS User Web Console](#).
2. Click on the **User** icon.



3. Select **Backup Set** from the left panel, then select **Backup** under **Execute Job** drop down menu, then click **Run**.



4. Modify the **In-File Delta type** and **Retention Policy** setting if necessary.
5. Click **Run Backup** to start the backup job.
6. When a backup job is running, the status **Backup is Running** will be displayed. Click **Stop** to stop the backup job if necessary.

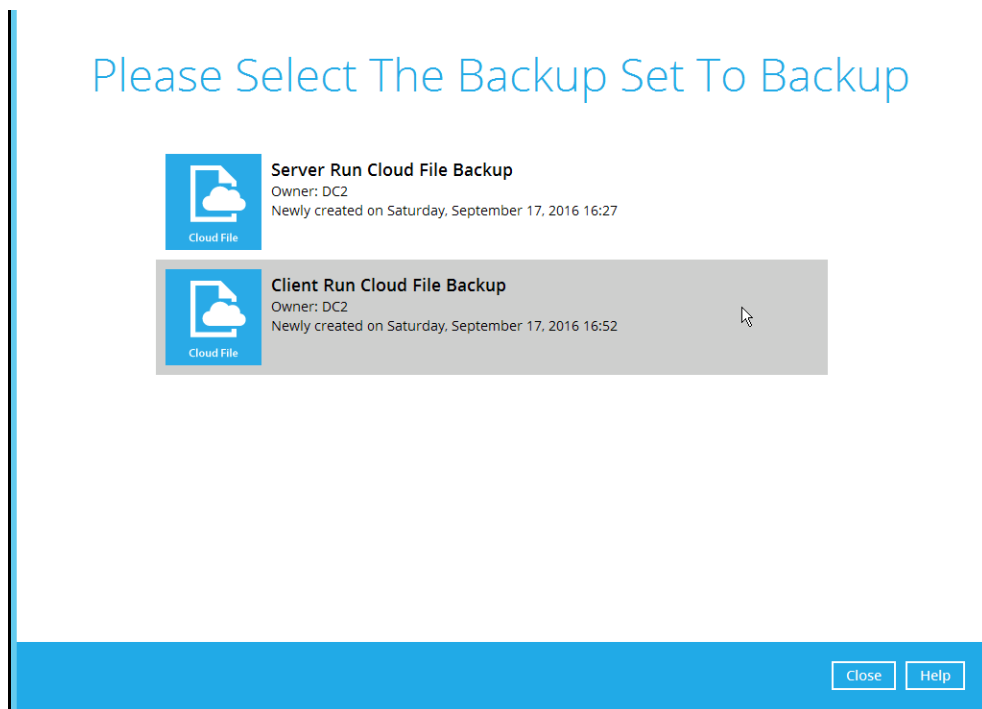


6.3 Configure Backup Schedule for Automated Backup in OBM

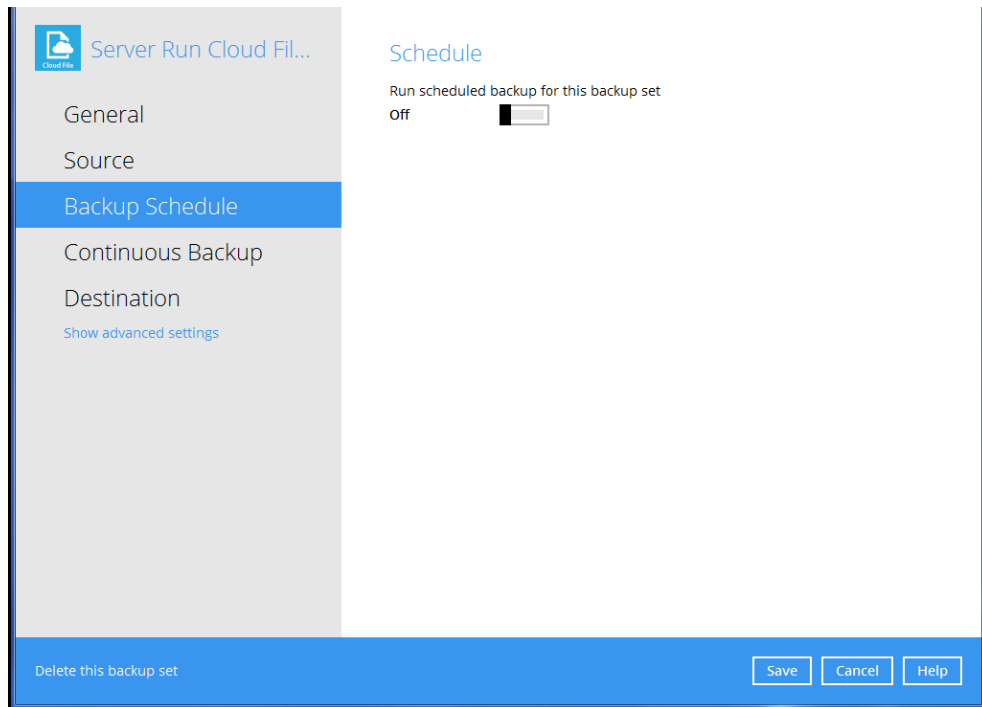
1. Click the **Backup Sets** icon on the OBM main interface.



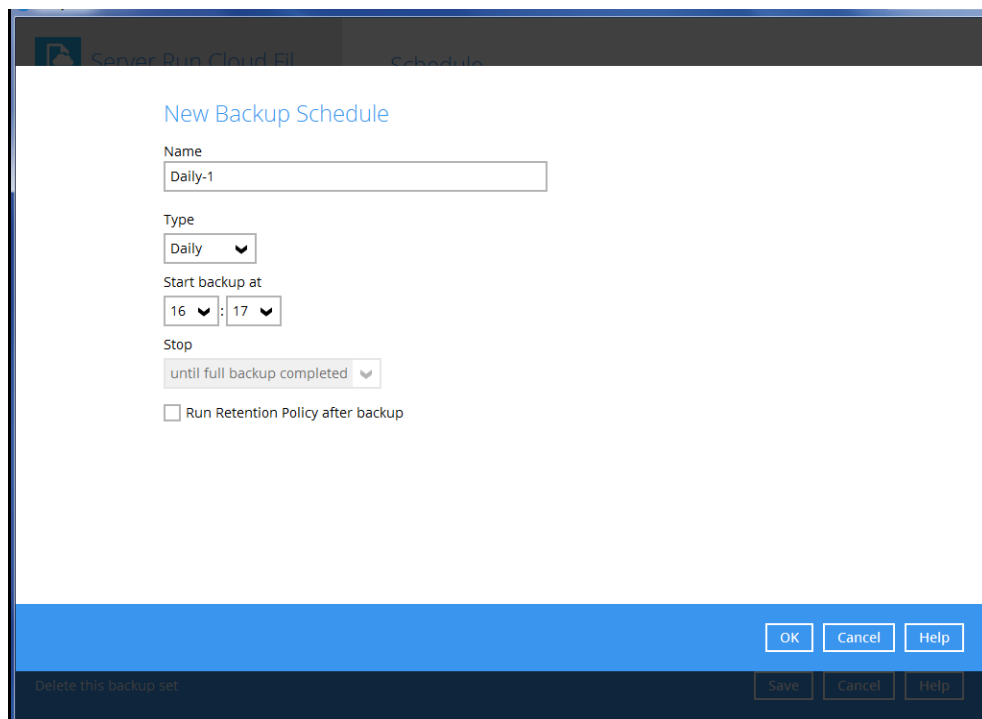
2. Select the backup set that you want to create a backup schedule for.



3. Click **Backup Schedule**, switch on the **Run scheduled backup for this backup set** button and click **Add new schedule**.



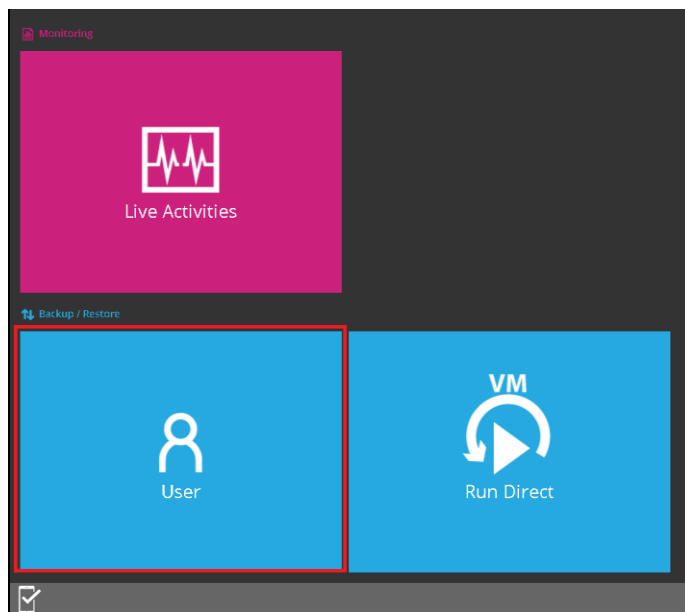
4. Configure the backup schedule settings, then click **OK** to proceed.



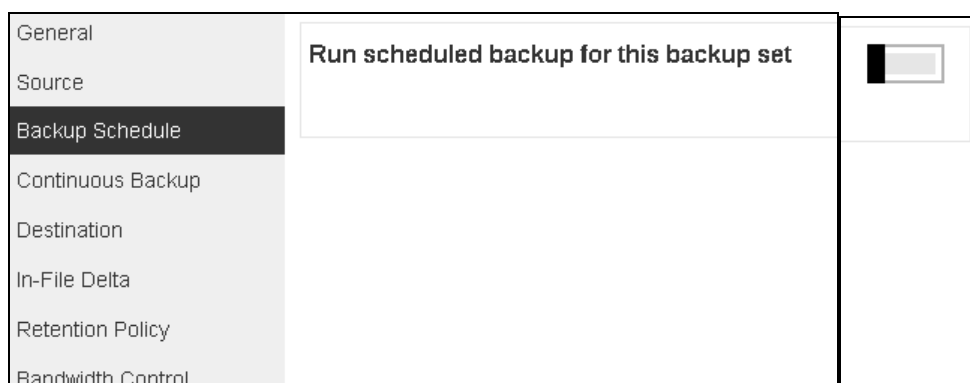
5. Click **Save** to confirm your settings.

6.4 Configure Backup Schedule for Automated Backup on the Web Console

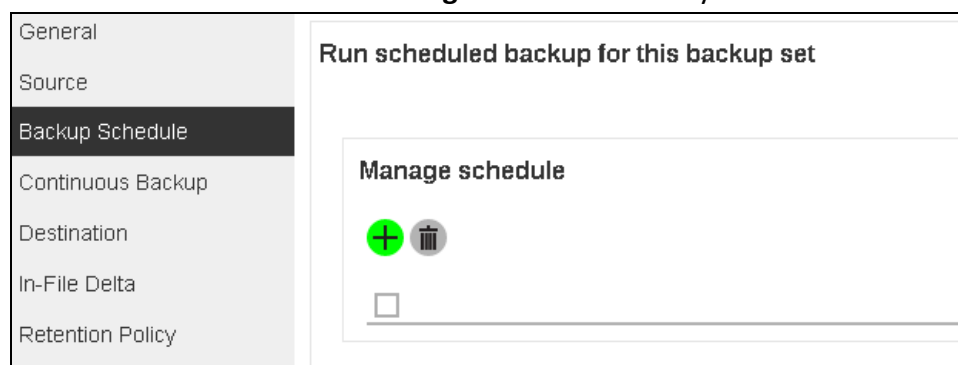
1. Click on the **User** icon on the main page of the User Web Console.



2. Select **Backup Set** from the left panel, then click on the corresponding backup set.
3. Go to the **Backup Schedule** menu, slide the on/off switch at the right to turn this feature on.



4. Click the  icon under the **Manage schedule** to add your desired schedule.



5. You may configure the following items for the schedule.

- Name of the scheduled backup
- Backup schedule type
- Backup start time
- Run Retention Policy after backup

Backup Schedule

Details

Name

Type

Daily ▾

Start backup at

00 ▾

 :

00 ▾

Stop

until full backup completed ▾

☐ Run Retention Policy after backup

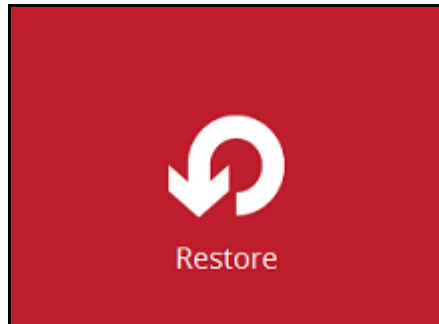
6. Click the  icon and then the  icon to confirm the setting.

7 Restoring with a Cloud File Backup Set

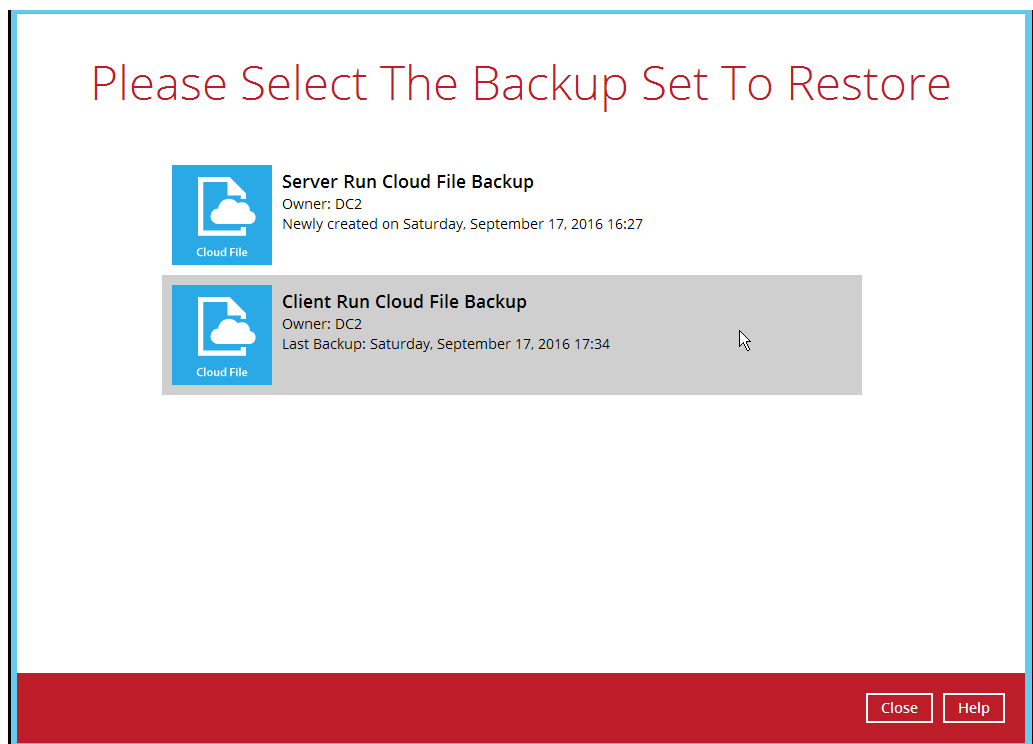
7.1 Restore with OBM

Login to the OBM application according to the instruction provided in the chapter on [Login to OBM](#).

1. Click the **Restore** icon on the main interface of OBM.



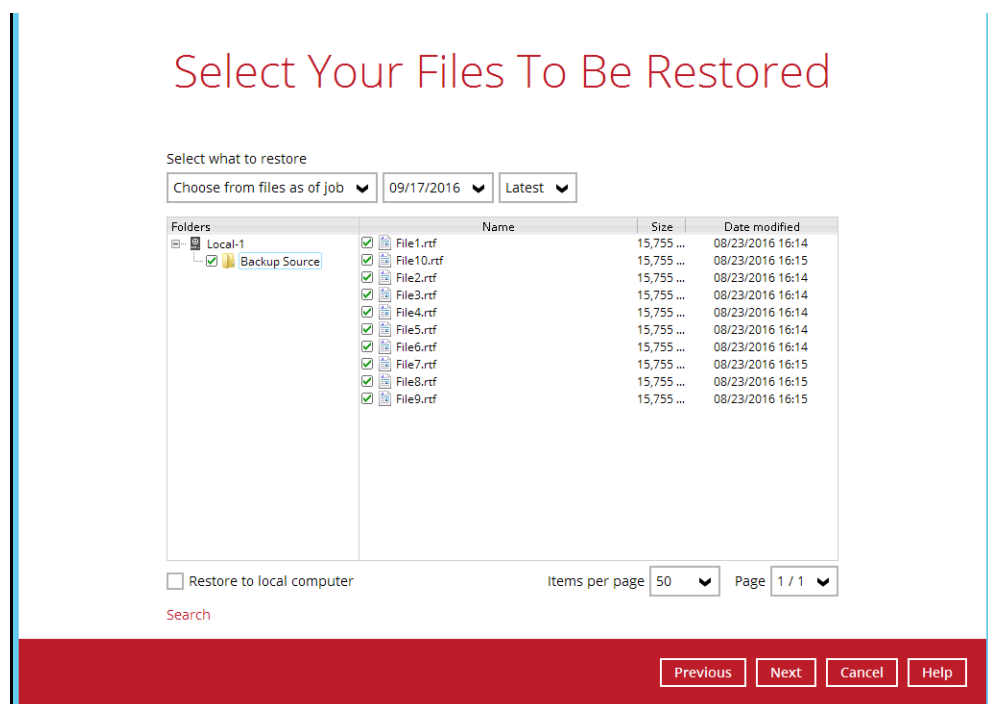
2. Select the backup set that you would like to restore from.



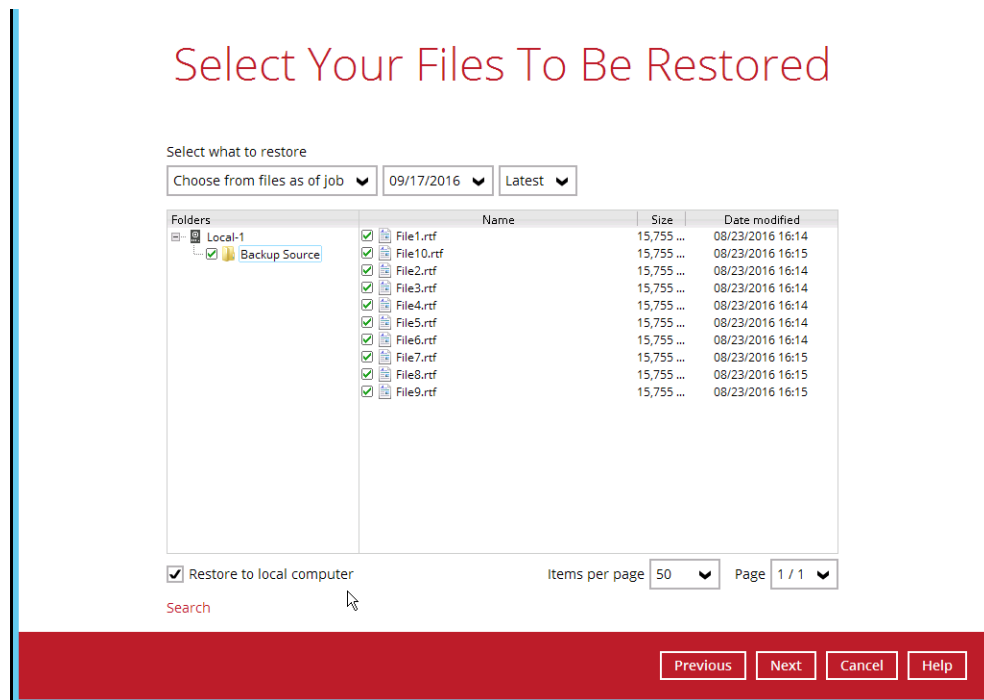
3. Select the backup destination that contains the data that you would like to restore.



4. Select to restore from a specific backup job, or the latest job available from the **Select what to restore** drop down menu.

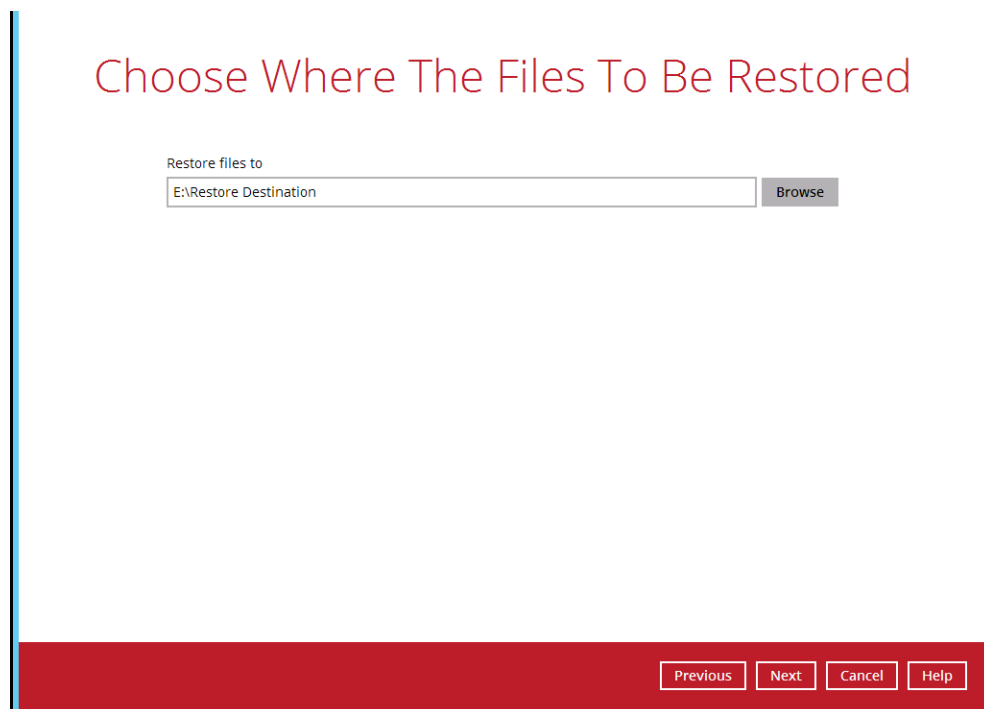


5. Select **Restore to local computer** if you want to restore the backed up data to the local computer.



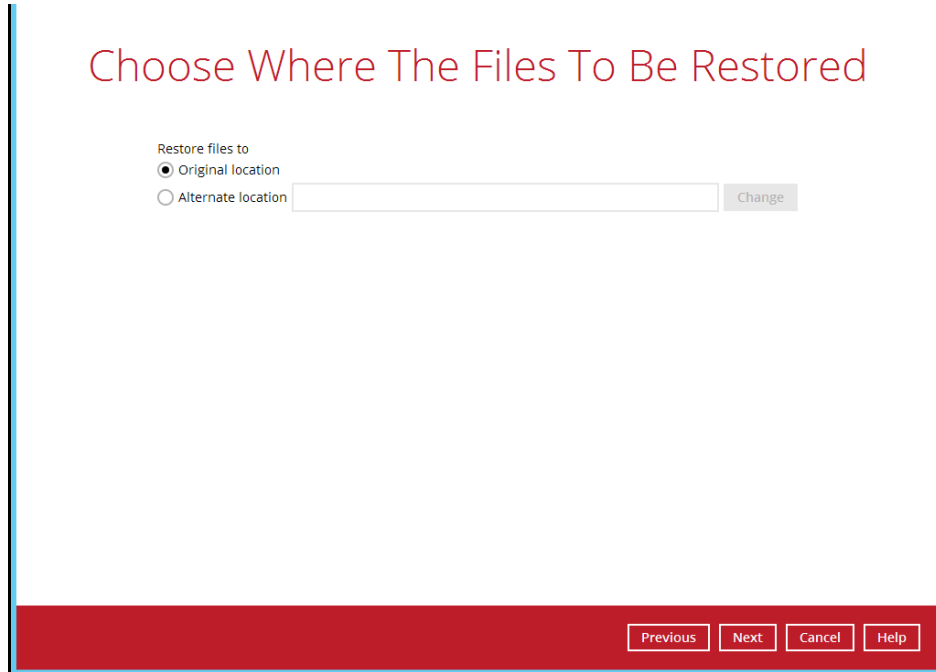
Click **Next** to continue.

6. If **Restore to local computer** is enabled, browse to the corresponding directory path on the local computer that you want the data to be restored to.



-OR-

If **Restore to local computer** is disabled, select **Original location** to restore the data to the original directory path on the cloud storage, or **Alternate location** to restore to the data to an alternate path on the cloud storage.

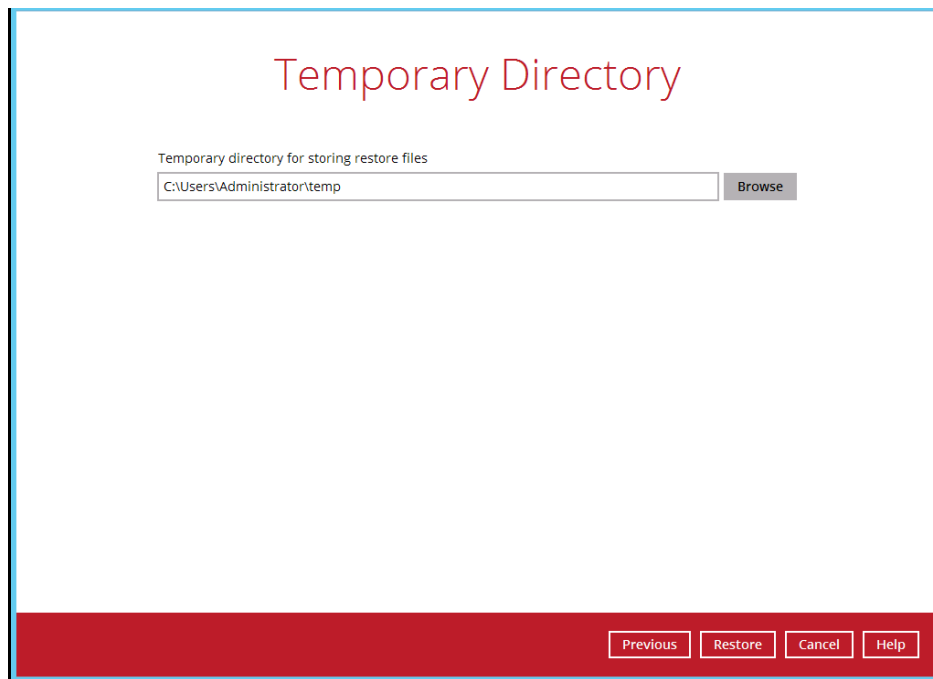


The screenshot shows a dialog box titled "Choose Where The Files To Be Restored" in red text. Below the title, there is a section labeled "Restore files to" with two radio button options: "Original location" (which is selected) and "Alternate location". To the right of the "Alternate location" option is a text input field and a "Change" button. At the bottom of the dialog, there is a red bar containing four buttons: "Previous", "Next", "Cancel", and "Help".

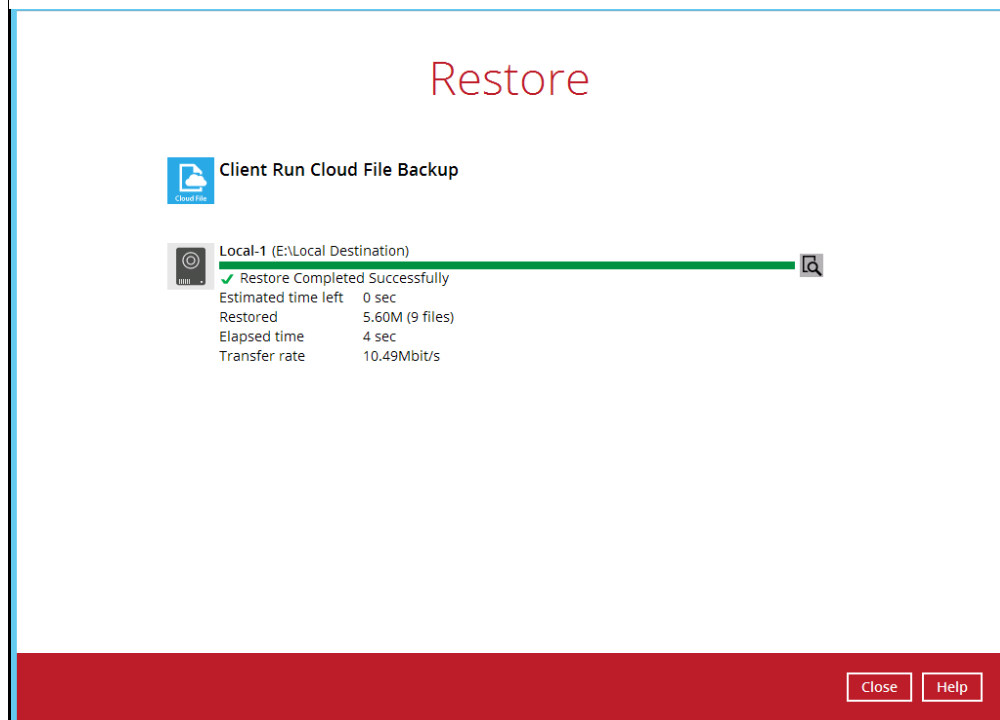
Click **Change** to browse to the alternate path on the cloud storage.

Important: Data can only be restored to a local computer, or to the original cloud storage that the data was backed up from (e.g. same cloud storage provider and same account). You cannot restore the data to a different cloud storage (e.g. a different cloud storage provider or different account)

7. Select the temporary directory for storing temporary files.

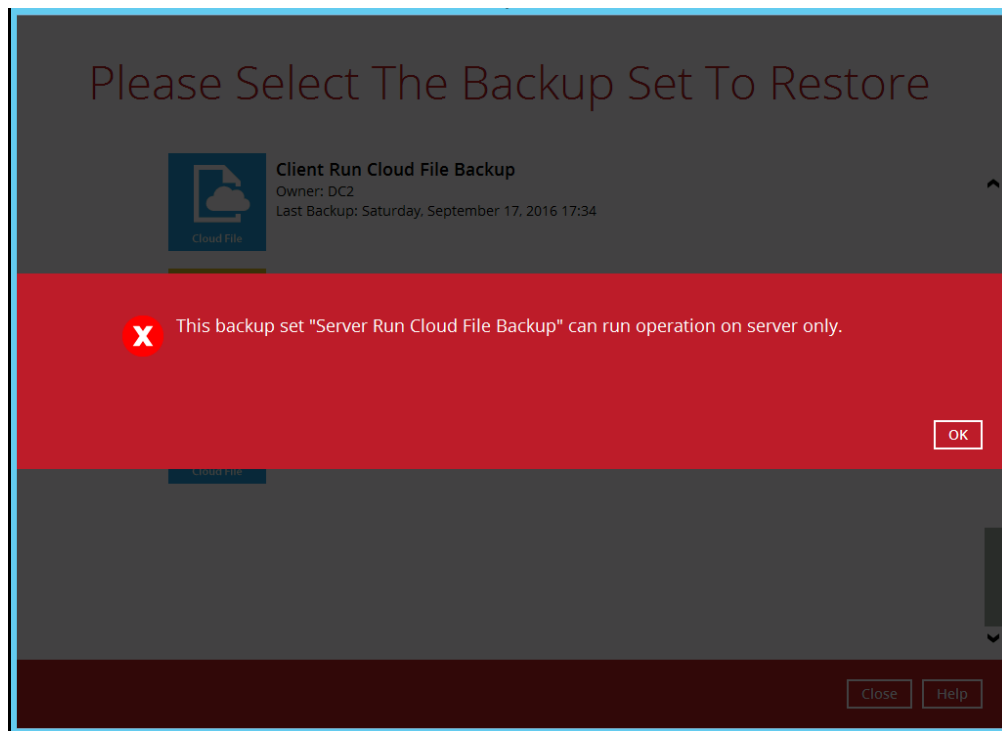


8. Click **Restore** to start the restoration.
9. The following screen is displayed when the files are restored successfully.



Important: Data of a **Run on Server** Cloud File backup set can only be restored via the CBS web console. The following error message will be displayed if you try to restore data of a **Run on Server** Cloud File backup set via the OBM user

interface.



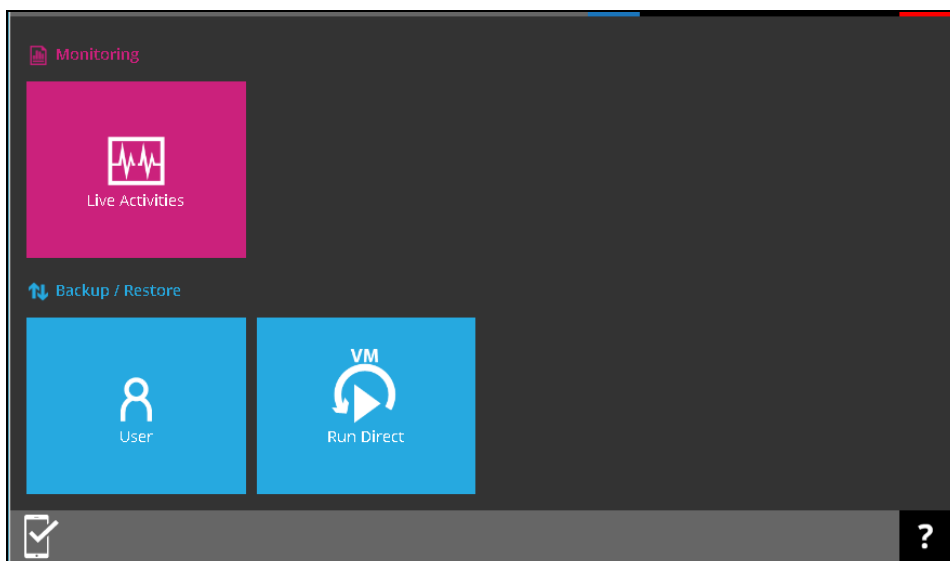
Refer to the chapter on [Restore with the CBS Web Console](#) for instruction on how to restore data for a **Run on Server** Cloud File backup set.

7.2 Restore with the CBS Web Console

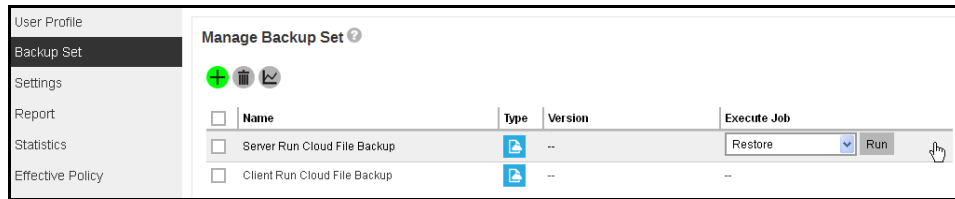
Login to the web console according to the instruction provided in the chapter on [Login to the CBS Web Console](#).

*Note: Data of a **Run on Server** Cloud File backup set can only be restored via the CBS web console.*

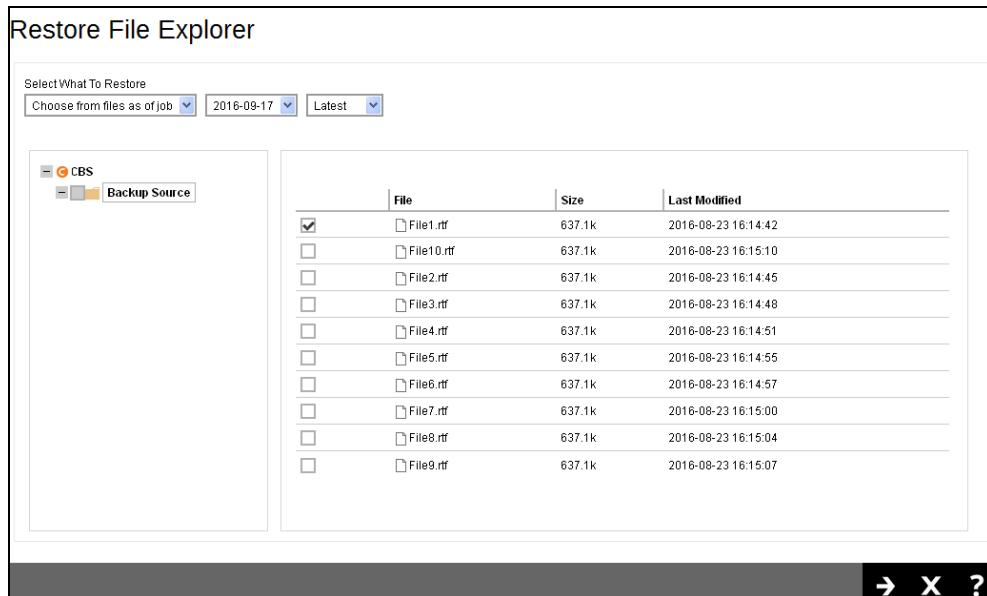
1. Click on the **User** icon.



2. Select **Backup Set** from the left panel, then select **Restore** under **Execute Job** drop down menu, then click **Run**.



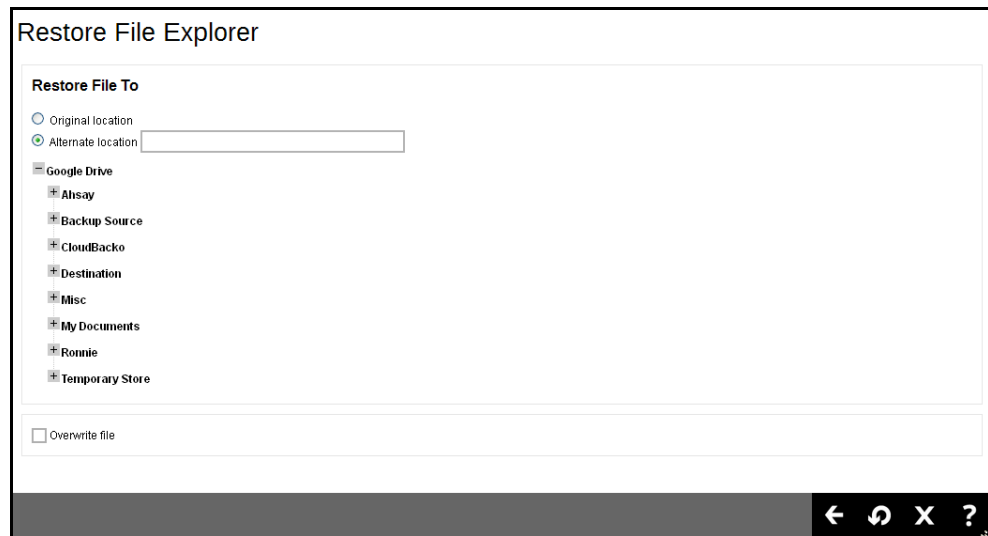
3. Select to restore from a specific backup job, or the latest job available from the **Select What To Restore** drop down menu. Click **Next** to proceed.



4. Select **Original location** to restore the data to the original directory path on the cloud storage, or **Alternate location** to restore to the data to an alternate path on the cloud storage



Expand the directory path to browse to the alternate location on the cloud storage.



Important: Data can only be restored to the original cloud storage that the data was backed up from (e.g. same cloud storage provider and same account).

5. Click the  icon to start the restoration.
6. You will see the status showing **Restore is Running** when the restore is in progress.