Asigra Cloud Backup v14.1

Management Console User Guide

January 2019

Asigra

Recovery is Everything™

Disclaimer
Information in this document is subject to change without notice and does not represent a commitment on the part of Asigra Inc.

Asigra Inc. makes no representation or warranty, express, implied, or statutory, with respect to, and assumes no responsibility for the accuracy, completeness, sufficiency or usefulness of the information contained herein.

This document may contain sample screen shots, used to demonstrate Asigra Cloud Backup™ procedures. All information appearing in this document is used for illustration purposes only, and should be considered fictitious

The software described in this document is furnished under a license agreement. It is against the law to copy the software on any medium except as specifically allowed in the license agreement.

79 Brisbane Road, Toronto, Ontario, Canada M3J 2K3

Release Date: January 2019

Contents

1 About this guide

This guide describes how to use the Management Console software.

NOTE: For instructions on how to install the Management Console, see the *Client Software Installation Guide.*

1.1 Intended audience

This guide is intended for Management Console users who want to perform remote management and monitoring of their Asigra Cloud Backup software components.

1.2 Formatting conventions

The following formatting conventions are used in this guide:

Bold

Bold font identifies components, window and dialog box titles, and item names.

Italic

Italic font identifies references to related documentation.

`Monospace Font`

Monospace font identifies text that you should type or that the computer displays.

NOTE: Notes emphasize information that is useful but not essential, such as tips or alternative methods for performing a task.

IMPORTANT: Important notes emphasize information that is essential to the completion of a task and draw special attention to actions that could adversely affect the operation of the application or result in a loss of data.

2 Getting started

This section provides an overview of the Management Console and describes how to sign in and start using the application.

2.1 About the Management Console

The Management Console is a web-based application that simplifies the backup and recovery process by providing a centralized environment to manage DS-Systems, DS-Clients, backup sets, schedules, retention rules, and more.

The Management Console Application Programming Interface (API), which is based on the RESTful (Representational State Transfer) framework, allows developers to use their preferred programming languages and tools to integrate with the Management Console. To access the API documentation, add */docs* to the end of your Management Console URL.

NOTE: Before you begin using the Management Console, ensure that all the required DS-Systems and DS-Clients have been installed. You must have the latest version of Java which is required to use the Management Console launcher.

2.2 Signing in to the Management Console

This section describes how to sign in to the Management Console.

NOTE: The default IP address used by the Management Console is **127.0.0.1** and the default port is **9595**. The default user name and password is **admin**. You will be prompted to change your user name and password the first time you sign in.

To sign in to the Management Console:

1. On the **Welcome** page, click **Sign In**.
2. In the **User name** box, type the default user name.
3. In the **Password** box, type the default password.
4. Click **Sign In**.

NOTE: If you forget your password, click **Forgot User Name or Password?** You will be prompted to enter your email address.

2.3 Performing the initial configuration

The first time you sign in to the Management Console you are prompted to perform the initial configuration of the system, including changing your password, configuring a DS-System and DS-Client connection, configuring users and permissions, configuring cloud credentials, and configuring notifications.

To perform the initial configuration:

1. On the **Change Password** page, type your current and new password, and then click **Next**.

   NOTE: You can change your password again later at any time. For detailed instructions, see Section 2.5, “Changing your password”.

2. On the **Components** page, click [**+**] to optionally add a DS-System or a DS-Client connection, and then click **Next**.

   NOTE: For detailed instructions, see Section 3.1.2, “Configuring a DS-System connection” and Section 4.1.2, “Configuring a DS-Client connection”.

3. On the **Users & permissions** page, click [**+**] to optionally configure a user and assign them permissions, and then click **Next**.

   NOTE: For detailed instructions, see Section 4.2.2, “Configuring a user”.

4. On the Two-factor authentication page, click [**+**] to optionally configure 2FA server credentials.

   NOTE: For detailed instructions, see Section 4.3, “Configuring two-factor authentication”.

5. On the **Cloud Credentials** page, click [**+**] to optionally configure cloud credentials, and then click **Next**.

   NOTE: For detailed instructions, see Section 4.4.2, “Configuring cloud credentials”.

6. On the **General** page, optionally configure the settings for email notification settings, and then click **Finish**.

NOTE: For detailed instructions, see Section 4.5.1, “Configuring the email notification settings”.

2.4 Viewing the Management Console dashboard

The dashboard is a user interface that organizes and presents information in a way that is easy to read and is interactive.This section describes how to view the dashboard and various components of the dashboard.

To view the dashboard:

Sign in to the Management Console, to view the dashboard with the following information.

- **Component Summary**: This displays the total number of DS-Systems, DS-Clients and Customer Accounts. If a DS-System or DS-Client has stopped working, it is represented by a different color.
- **Activity Summary**: This displays the total number of backup sets for a customer across all accounts on a daily basis. Different colors represent a successful backup activity, a backup activity with a warning and a backup activity with errors. To view the number of backup sets in each category, hover the mouse on the corresponding color.
- **Error Summary**: This displays a summary of errors that have occurred in various areas of the application.
- **Successful**: This list displays all the activities that were successfully completed. Click the tab **See All** to view the details of the successful activities.
- **Warnings**: This list displays all the warnings that were issued. Click the tab **See All** to view the details of these warnings under activity logs.
- **Errors**: This list displays all the errors that have occurred in the system. Click the tab **See All** to view the details under activity logs or event logs.

2.5 Changing your password

An administrator will provide you with a user name and password for signing in to the Management Console.

NOTE: Your password must contain 8-16 characters, at least one uppercase character (A-Z), at least one lowercase character (a-z), and at least one numeric character (0-9).

To change your password:

1. On the toolbar, click **More Options**, and then click **Change Password**.
2. In the **Current Password** box, type your current password.
3. In the **New Password** box, type your new password.
4. In the **Confirm Password** box, retype your new password.
5. Click **Change**.

2.6 Installing Management Console updates

When an update is available, the **Notifications** icon will flash.

To install the update:

1. On the toolbar, click **Notifications**.
2. In the **Notifications** window, do the following:
   a) To inform the users regarding the updates, click **Notify Users**.
      - On the **Notifications** page enter all the required details and click **Send**. For details, refer Section 4.5.1, “Configuring the email notification settings”
   b) To install the updates, click **Updates**.
      - In the **Management Console Updates** window, under **Package Name**, select the package(s) that you want to install, and then click **Install**.

2.7 Branding the Management Console

This section describes how to apply your own company branding to the Management Console.

To apply branding to the Management Console:

1. On the installation DVD, navigate to the **Management Console Branding** folder which contains the *amc_logo.svg* and *favicon.ico* files.
2. Replace the *amc_logo.svg file* with your company logo that has the same file name and file format.
3. Replace the *favicon.ico* file with your company icon that has the same file name and file format.

NOTE: The icon file must have the dimensions 16 pixels x 16 pixels.

To apply branding to the GDPR certificate:

1. On the installation DVD, navigate to the **Management Console Branding** folder which has the *report_logo.jpg* and the *company_info.properties* files.
2. Replace the *report_logo.jpg* with your company logo that has the same file name and file format.
3. Using a text editor, open the file *company_info.properties*, modify the details as required, and then save the file.

2.8 Translating the Management Console

This section describes how to use the Management Console Translation Utility to translate the Management Console interface.

NOTE: For detailed instructions on how to create a *Google Cloud Platform* account, create a project, enable the translation API, and create a service account, refer *Google* documentation.

To translate the Management Console:

1. Go to https://cloud.google.com and follow the instructions to create a Google Cloud Platform account.
2. Sign in to your Google Cloud Platform account, and create a project.
3. Enable the Google Cloud Translate API, *a*nd then create credentials for the project.

   NOTE: You might need to create a new service account and obtain the credentials which are in the form of service account keys.

   ---

4. Type a name for the service account, select the **App Engine Admin** role, and then click **Create**.

   IMPORTANT: The system generates a file (*.json*) containing all the credentials. This file is used by the system to run the translation utility.

   ---

5. Double click the **Management Console Translation Utility** located in the following folder:

   `\Program Files\CloudBackup\Management Console`

6. In the **Google credentials file** box, click **Browse**, and then select the **.json** file that you created.
7. In the **Management Console WAR file** box, click **Browse**, and then select the **mc-exec.war** file located in the following folder:

   `\Program Files\CloudBackup\Management Console`

8. In the **Proxy server address** box, type the IP address of the proxy server.

> ***NOTE:*** The IP address of the proxy server is required if you are running this tool from behind a firewall.

9. In the **Language** box, select the language for the interface.
10. To start the translation process, click **Generate**.

When the translation is complete, a message is displayed indicating a successful translation.

2.9 Signing out of the Management Console

You can sign out of the Management Console at any time.

To sign out of the Management Console:

On the toolbar, click  **More Options**, and then click **Sign Out**.

3 Configuring the system

This section describes how to configure DS-Systems, customer accounts, and DS-Client accounts.

3.1 Configuring DS-Systems

This section describes how to configure DS-System connections, customer accounts, and DS-Client accounts.

3.1.1 About DS-Systems

The DS-System is a licensed component that receives and processes requests from DS-Clients and serves as the main repository for backed up data.

3.1.2 Configuring a DS-System connection

Before you can configure customer accounts and DS-Client accounts, you must connect to a DS-System. Each DS-System must be able to connect to the DS-License server at all times, since it validates and receives its capacity license allocation from the DS-License Server. To avoid single-point-failures, you can also configure an Emergency License Server.

To configure a DS-System connection:

1. On the toolbar, click **Settings**.
2. Click the **Components** tab.
3. Under **DS-Systems Connections**, do one of the following:
   - To add a new DS-system connection, click [**+**] **Add Connection**.
   - To edit an existing DS-System connection, select the DS-system, and then click **Edit Connection**.
4. In the **Name** box, type the name of the DS-System.
5. In the **User name**, type the name of the user who will log on to the DS-System.
6. In the **Password** box, type the password of the user who will log on to the DS-System.
7. In the **Domain/computer name** box, type the domain or computer name to which this DS-System belongs.
8. In the **Server address** box, type the IP address of the server where the DS-System is installed.

NOTE: To add or delete a server address, click the associated icon.

9. In the **Port** box, enter the port number that will be used by the DS-System.
10. Click **Next**.
11. On the **License Server information** page, do the following:
    - To add a production license server, under **Production License Server**, do the following:
        a) In the **DS-License Server (IP/DNS)** box, type the IP address or the DNS name of the production DS-License Server.
        b) In the **TCP port** box, type the communication port number of the production DS-License Server.

        NOTE: Do not change the port unless you have a specific requirement.

        c) In the **Verification interval** box, type the time interval in minutes at which the license server will verify the validity of the license.
    - To add an emergency license server, under **Emergency License Server**, do the following:
        a) In the **DS-License Server (IP/DNS)** box, type the IP address or the DNS name of the emergency DS-License Server.
        b) In the **TCP port** box, type the communication port number of the emergency DS-License Server.

        NOTE: Do not change the port unless you have a specific requirement.

        c) In the **Failover interval** box, enter the time interval in minutes after which the emergency DS-License Server should take over the function of the production DS-License Server in case of a failover.
12. Click **Add** or **Update**.

3.1.3 Deleting a DS-System connection

This procedure describes how to delete a DS-System connection.

To delete a DS-System connection:

1. On the toolbar, click **Settings**.
2. Under **DS-Systems**, select the DS-System that you want to delete, and then click **Delete Connection**.
3. When the system prompts you to confirm that you want to delete the DS-System connection, click **Yes**.

3.2 Configuring customer accounts

This section describes how to configure customer accounts.

3.2.1 About customer accounts

A customer account is a record of basic information about a customer that is used for billing, data identification, and security purposes. Each customer has a single customer account, but can have multiple DS-Client accounts.

3.2.2 Configuring a customer account

You must configure a customer account for each customer who is associated with a DS-System.

To configure a customer account:

1. On the toolbar, click **Account Management.**
2. Under **DS-Systems**, do one of the following:
   - To add a new customer account, click [**+**] **Add Customer Account**.
   - To edit an existing customer account, select the customer account, and then click **Edit Customer Account**.
3. In the **DS-System** box, select the name of the DS-System you want to associate the account with.
4. In the **Account number** box, type a unique number specific for the customer account.
5. In the **Account name** box, type a unique a name for the customer account.
6. In the **Contact** box, type the name of the contact person for the customer account.

7. In the **Email address** box, enter the email address of the contact person for the customer account.
8. To define a storage limit for the customer account, select the **Enable quota management** check box, and then specify the quota in GB or MB.
9. Click **Add** or **Save**.

3.2.3 Deleting a customer account

This procedure describes how to delete a customer account.

IMPORTANT: Before deleting a customer account, you must first delete all the DS-Clients associated with the customer account.

To delete a customer account:

1. On the toolbar, click **Account Management**.
2. Under **DS-Systems**, expand the required DS-System to display a list of customer accounts.
3. Select the customer account(s) that you want to delete, and then click **Delete Customer Account**.
4. When the system prompts you to confirm that you want to delete the customer account, click **Yes**.

3.3 Configuring DS-Client accounts

This section describes how to configure customer accounts.

3.3.1 About DS-Client accounts

You must create a DS-Client account on the DS-System before customers can use the DS-Client software to back up their data. After you create a DS-Client account, send the DS-Client account number to the customer so that they can register their DS-Client.

The initial default group of 99,999 DS-Client accounts can be identified by the prefix “DSC” and unique system ID, which contains 4 alphanumeric characters followed by a sequentially generated DS-Client number (for example, from DSCxxxx00001 to DSCxxxx99999).

In addition to the default group of 99,999 DS-Client accounts, the DS-System can support another 100 groups of 99,999 DS-Client accounts. Additional groups of 99,999 DS-Client accounts can be identified by the prefix “D00”, “D01”, and so on (for example: D00xxxx00001, D01xxxx00001, etc.).

3.3.2 Configuring a DS-Client account

You must configure a DS-Client account for each customer account that is associated with a DS-System. Each customer account can have multiple DS-Client accounts.

To configure a DS-Client account:

1. On the toolbar, click **Account Management**.
2. Under **DS-Systems**, expand the required DS-System and customer account, and then do one of the following:
   - To add a new DS-Client account, click [**+**] **Add DS-Client Account**.
   - To edit an existing DS-Client account, select the DS-Client account, and then click **Edit DS-Client Account**.
3. In the **Description** box, type a name that describes the DS-Client.
4. To define a storage limit for the DS-Client account, select the **Enable quota management** check box, and then specify the quota in GB or MB.
5. To enable cybersecurity for the DS-Client so that you can perform real-time scans of your files for malware during the backup and restore process, select the **Enable cybersecurity scan** check box.

   NOTE: The cybersecurity feature is currently supported only for File system backup sets on Windows DS-Clients. The trial version includes five (5) free malware detections per DS-Client.

6. To register the DS- Client as a template for mass deployment, select the **Enable auto-registration counter** check box, and then specify the number of DS-Client accounts that can be created from this DS-Client.
7. Click **Add** or **Save**.

3.3.3 Deleting a DS-Client account

This procedure describes how to delete a DS-Client account.

IMPORTANT: Deleting a DS-Client will remove all associated data from the DS-System online storage.

To delete a DS-Client account:

1. On the toolbar, click **Account Management**.
2. Under **DS-Systems**, expand the required DS-System and customer account to display a list of DS-Client accounts.
3. Select the DS-Client account you want to delete, and then click **Delete DS-Client Account**.
4. When the system prompts you to confirm that you want to delete the DS-Client account, type the DS-Client number, and then click **Continue.**

4 Configuring the system settings

This section describes how to configure DS-Client connections, users and permissions, cloud credentials, and the email notification settings.

4.1 Configuring DS-Clients

This section describes how to configure DS-Client connections.

4.1.1 About DS-Clients

DS-Client is responsible for defining the backup sets that determine what data is to be backed up from the source computers and for sending the backed up data through an IP WAN to DS-System for storage.

During the backup process, DS-Client extracts, compresses, and encrypts the data for backup. The backup data is sent to the secure, off-site data center that hosts the DS-System vault. Restore is performed on demand via the same DS-Client.

4.1.2 Configuring a DS-Client connection

You must configure a DS-Client connection to establish communication between the DS-Client and the associated DS-System.

To configure a DS-Client connection:

1. On the **Toolbar**, click **Settings**.
2. Click the **Components** tab.
3. Under **DS-Client Connections**, do one of the following:
   - To add a new DS-Client connection click [**+**] **Add Connection**.
   - To edit an existing DS-Client connection, select the DS-Client connection, and then click **Edit Connection**.

   NOTE: When editing a DS-Client connection, you cannot select the option to add a single DS-Client or multiple DS-Clients.

4. On the **Add/Edit DS-Client Connection** page, do one of the following:
   - To add a single DS-Client, select the **Add single DS-Client** option.
     a) In the **Name** box, type a name for the DS-Client connection.
     b) In the **User name** box, type the user name that will be used to log onto the system where the DS-Client is running.

c) In the **Password** box, type the password that will be used to log onto the system where the DS-Client is running.

d) In the **Domain/computer name** box, type the domain or computer name of the system where the DS-Client is running.

e) In the **Server address** box, type the IP address of the server where the DS-Client is running, and then click [**+**].

f) In the **Port** box, type the port that will be used by the DS-Client to communicated with the DS-System.

- To add multiple DS-Clients, select the **Add multiple DS-Clients** option, and then do the following:

  a) Click **Browse** to select the *.csv* file containing the list of DS-Clients (with their login credentials, domain names, and server addresses).

  b) Click **Submit**.The **Multiple Connection Add Summary** dialog box displays the list of new DS-Clients. If you have an issue adding a DS-Client, resolve the issue and repeat the process.

5. Click **Next**.
6. On the **DS-Client Registration** page, do the following:

   a) In the **Customer name** box, type the customer name associated with the DS-Client account.

   b) In the **Customer account** box, type the account number associated with DS-Client account.

   c) In the **DS-Client number** box, type the DS-Client number that was generated for the associated DS-Client account (this number is provided by the service provider).

   d) In the **Server address** box, type the IP address of the DS-System associated with this DS-Client connection, and then click [**+**].

   e) Click **Next**.
7. On the **Encryption Keys** page, do the following:

   a) Under **Private key**, select a type of encryption algorithm, and then type the key number and confirm it.

NOTE: Encryption keys are case sensitive and the character length depends on the type and level of encryption selected. DES requires 8 characters, AES-128 requires 16 characters, AES-192 requires 24 characters, and AES-256 requires 32 characters. If you type a shorter string, an auto-complete feature repeats the string until all the required characters are filled. For example, “123” becomes “1231231231231231”.

---

b) Under **Account key**, select a type of encryption algorithm, and then type the key number and confirm it.

NOTE: If the customer account has more than one DS-Client installation, each DS-Client for this customer account must be configured with the same account key.

c) To register this DS-Client with the DS-System specified in the *DS-System information* section, select the **Register with DS-System** check box.

d) To allow this DS-Client to send the encryption keys to the DS-System, select the **Allow encryption key forwarding to DS-System** check box.

e) Click **Next**.

8. On the **User information** page, do the following:

a) In the **Country** box, enter the name of the country where the user is located.

b) In the **Number of employees** box, enter the number of employees in the organization.

c) In the **Industry** box, enter the industry vertical to which the organization belongs.

9. Click **Finish**.

4.1.3 Configuring the DS-Client cybersecurity settings

This section describes how to configure the cybersecurity settings for a DS-Client.

If the DS-Client is licensed for cybersecurity, we recommend that you configure a quarantine folder where a copy of any files detected with malware will be saved in a password protected zip file.

NOTE: The cybersecurity feature is available only when connected to a Windows DS-Client.

To configure the DS-Client cybersecurity settings:

1. On the toolbar, click **Settings**.
2. Click the **Components** tab.
3. Under **DS-Client Connections**, select the DS-Client for which you want to configure the cybersecurity settings, and then click **Advanced Configuration**. The **Advanced Configuration** dialog box appears.
4. In the **Configuration settings** box, select **Cybersecurity settings**.
5. Select the **Enable quarantine** check box.

6. In the **Server address** box, type the IP address of the server where you want to create the quarantine folder.

   NOTE: We recommend that you create the quarantine folder on a machine other than the machine running the DS-Client.

7. In the **User name** box, type the user name that will be used to log onto the computer where you are creating the quarantine folder.
8. In the **Password** box, type the password that will be used to log onto the computer where you are creating the quarantine folder.
9. In the **Domain** box, type the domain name of the computer where you are creating the quarantine folder.
10. Click **Select Quarantine Folder**.
11. In the **Select Quarantine Folder** window, select the folder where you want to create the quarantine folder, and then click **Select**.
12. Click **Save**.

    The path of the quarantine folder that you have created is displayed in the **Quarantine folder** box.

4.1.4 Configuring the DS-Client proxy server settings

This section describes how to configure the DS-Client proxy settings.

1. On the toolbar, click **Settings**.
2. Click the **Components** tab.
3. Under **DS-Client Connections**, select the DS-Client for which you want configure the proxy settings, and then click **Advanced Configuration**.

   NOTE: You can select multiple DS-Clients and then configure the proxy server settings for each DS-Client separately.

4. Under **Configuration settings**, select **Proxy server settings** and then do the following:

   a) Select a DS-Client if you have selected multiple DS-Clients.

   b) Select an option for the proxy settings from the following:

   - **No proxy**
   - **Configure automatically**
   - **Configure manually**

5. If you have selected **Configure manually**, type the details for HTTP, HTTPS, and IMAP proxy servers.

6. To use these proxy server settings for all protocols, select the **Use the same proxy server for all protocols** check box.
7. Click **Save**.

4.1.5 Deleting a DS-Client connection

This section describes how to delete a DS-Client connection.

1. On the toolbar, click **Settings**.
2. Click the **Components** tab.
3. Under **DS-Client Connections**, select the DS-Client that you want to edit, and then click **Delete Connection**.
4. When the system prompts you to confirm that you want to delete the DS-Client connection, click **Yes**.

4.2 Configuring users and permissions

This section describes how to configure a user and assign them permissions.

4.2.1 About users and permissions

Each user of the Management Console is assigned a particular role, which defines their level of permissions when using the application.

NOTE: A Super Global Administrator is the administrator who logs in to the Management Console for the very first time and creates the Global Administrator.

There are four types of user roles:

- Global Administrator (see Section 4.2.1.1, “Global Administrator”)
- Customized Administrator (see Section 4.2.1.2, “Customized Administrator”)
- Regular User (DS-System) is created and assigned permissions by the Customized Administrator-Service Provider (see Section 4.2.1.3, “Regular User (DS-System)”).
- Regular User (DS-Client) is created and assigned permissions by the Customized Administrator-End User (see Section 4.2.1.4, “Regular User (DS-Client)”).

After creating the user, you must navigate to the user profile and assign the permissions. For details, see Section 4.2.3, “Assigning permissions”.

4.2.1.1 Global Administrator

A Global Administrator can create, edit, view, or delete any other type of user (Global Administrator, Customized Administrator, Regular User) on both the DS-System and the DS-Client and share the cloud credentials of any user.

Permissions	Global Administrator	
	DS-System	DS-Client
Data Management		
Backup Sets	Full	Full
Schedules	Full	Full
Retention Rules	Full	Full
Account Management		
Customer Accounts	Full	Full
Monitoring		
Backup Sets Report	Full	Full
Cybersecurity Scan Report	Full	Full
Cloud Details Report	Full	Full
GDPR Compliance Report	Full	Full
Logs	Full	Full
Settings		
Components	Full	Full
Users & Permissions	Full	Full
Cloud Credentials	Full*	Full*
Email Notifications	Full	Full
Notifications		
Notify Users	Full	Full
Updates	Full	Full

Legend:

Full - Permission to create, edit, view, and delete.

* A Global Administrator can edit/delete only their own cloud credentials.

4.2.1.2 Customized Administrator

A Customized Administrator can only share the cloud credentials that they configured or that were configured by a regular user that they created.

A Customized Administrator (Service Provider) can only access DS-System components and a Customized Administrator (End User) can only access DS-Client components.

Permissions	Customized Administrator	
	Service Provider	End User
Data Management		
Backup Sets		Full*
Schedules		Full*
Retention Rules		Full*
Account Management		
Customer Accounts	Full*	
Monitoring		
Backup Sets Report	Full	
Cybersecurity Scan Report		Full
Cloud Details Report		Full
GDPR Compliance Report	Full	
Logs	Full	Full
Settings		
Components		Full
Users & Permissions	Full*	Full*
Cloud Credentials	Full**	Full**
Email Notifications		
Notifications		
Notify Users	View	View
Updates	View	View

Legend:

Full - Permission to create, edit, view, and delete.

View - Permission only to view.

Blank column - Feature not available.(Tab is inactive)

* As per permissions assigned by the Global Administrator.

** A Customized Administrator can edit/delete only their own cloud credentials.

4.2.1.3 Regular User (DS-System)

A Regular User (DS-System) created by the Customized Administrator (Service Provider) has two levels of permissions: Administrator or Viewer. A Regular User (DS-System) cannot share their cloud credentials with other users.

Permissions	Regular User (DS-System)		
	Administrator	Viewer	None
Data Management			
Backup Sets			
Schedules			
Retention Rules			
Account Management			
Customer Accounts	Full	View	
Monitoring			
Backup Sets Report	Full	Full	
Cybersecurity Scan Report			
Cloud Details Report			
GDPR Compliance Report	Full	Full	
Logs	Full	Full	
Settings			
Components			
Users & Permissions			
Cloud Credentials	Full*	Full*	
Email Notifications			
Notifications			
Notify Users	View	View	
Updates	View	View	

Legend:

Full - Permission to create, edit, view, and delete.

View - Permission only to view.

Blank columns - Feature not available.(Tab is inactive)

* A Regular User (DS-System) can edit/delete only their own cloud credentials.

4.2.1.4 Regular User (DS-Client)

A Regular User (DS-Client) created by the Customized Administrator (End User) has three levels of permissions: Administrator, Operator, or Viewer. A Regular User (DS-Client) cannot share their cloud credentials with other users.

NOTE: A Regular User (DS-Client) with Operator permission can only backup, restore, and synchronize backup sets.

Permissions	Regular User (DS-Client)		
	Administrator	**Operator**	**Viewer**
Data Management			
Backup Sets	Full*	Full**	View
Schedules	Full	View	View
Retention Rules	Full	View	View
Account Management			
Customer Accounts			
Monitoring			
Backup Sets Report			
Cybersecurity Scan Report	Full	Full	Full
Cloud Details Report	Full	Full	Full
GDPR Compliance Report			
Logs	Full	Full	Full
Settings			
Components			
Users & Permissions			
Cloud Credentials	Full***	Full***	Full***
Email Notifications			
Notifications			
Notify Users	View	View	
Updates	View	View	

Legend:

Full - Permission to create, edit, view, and delete.

View - Permission only to view.

Blank columns - Feature not available.(Tab is inactive)

* As per permissions assigned by the Global or Customized Administrator.

** Permission only to backup, restore, or synchronize.

*** A Regular User (DS-Client) can edit/delete only their own cloud credentials.

4.2.2 Configuring a user

This section describes how to configure a user and assign them permissions. For more information on user roles and permissions, see Section 4.2.1, “About users and permissions”.

NOTE: If a regular user is created by a global administrator, the user can access only DS-System components. If a regular user is created by a customized administrator, the user can access only DS-Client components.

To configure a user:

1. On the toolbar, click **Settings**.
2. Click the **Users & Permissions** tab.
3. Under **Users & Permissions**, do one of the following:
   - To create a user, click **[+] Create User**.
   - To edit a user, select the user, and then click **Edit User**.

   NOTE: You can only edit the email address of the user.
4. On the **Create User** page, do the following:
   a) In the **User name** box, type a name for the user.
   b) In the **Email address** box, type the email address of the user.
   c) In the **Password** box, type the password that the user will require to sign in to the Management Console.
   d) In the **Confirm password** box, retype the password.
   e) Under **Role**, select the role of the user. For more information on user roles and permissions, see Section 4.2.1, “About users and permissions”.
   f) To configure the user so that they must verify their identity when signing in to the Management Console, enable **Two-factor authentication**. For more information, see Section 4.3.1, “About two-factor authentication”.
   g) Click **Create**.

4.2.3 Assigning permissions

You must assign permissions to the user to enable them to access DS-Systems and DS-Clients. For more information on user roles and permissions, see Section 4.2.1, “About users and permissions”

NOTE: A user can access only the DS-System or DS-Client for which they have permissions.

To assign permissions to a user:

1. On the toolbar, click **Settings**.
2. Click the **Users & Permissions** tab.
3. Under **Users & Permissions**, select the DS-System or DS-Client for which you want to assign permissions.
4. Select the permission, and then click  to save the permission.

4.2.4 Deleting a user

This procedure describes how to delete a user.

To delete a user:

1. On the toolbar, click **Settings**.
2. Click the **Users & Permissions** tab.
3. Under **Users & Permissions**, select the user that you want to delete, and then click  **Delete User**.

When the system prompts you to confirm that you want to delete the user, click **Yes**.

4.3 Configuring two-factor authentication

This section describes how to configure two-factor authentication so users must verify their identity when signing in to the Management Console.

4.3.1 About two-factor authentication

Two-factor authentication provides an additional layer of protection that can significantly decrease the risk of a hacker accessing the Management Console. Management Console users who are configured with two-factor authentication must download the Octopus Authenticator application to their mobile device so they can verify their identity when signing in to the Management Console.

4.3.2 Configuring two-factor authentication credential

Before you can a configure two-factor authentication credential, you must contact Secret Double Octopus to obtain the required information.

To configure a two-factor authentication credential:

1. On the toolbar, click **Settings**.
2. Click the **Two-factor Authentication** tab.
3. Under **Two-factor Authentication**, do one of the following:
   - To add a two-factor authentication credential, click [**+**] **Add 2FA Credentials**.
   - To edit a two-factor authentication credential, select the two-factor authentication credential, and then click **Edit 2FA Credentials**.
4. In the **Add 2FA Server Credentials** dialog box, do the following:
   a) In the **Instance name** field, type the name you want to use to identify the 2FA instance.
   b) In the **Instance URL** field, type the URL of the 2FA instance that you received from *Secret Double Octopus.*
   c) In the **User name** field, type the user name that you received from *Secret Double Octopus*.
   d) In the **Password** field, type the password that you received from *Secret Double Octopus*.
   e) Click **Add**/**Save**.

4.3.3 Deleting a two-factor authentication credential

You can delete a two-factor authentication credential if required.

To delete a two-factor authentication credential:

1. On the toolbar, click **Settings**.
2. Click the **Two-factor authentication** tab.
3. Select the two-factor authentication credential that you want too delete, and then click **Delete 2FA Credentials**.
4. When the system prompts you to confirm that you want to delete the two-factor authentication credential, click **Delete**.

4.4 Configuring cloud credentials

This section describes how you can configure users and assign them credentials to use cloud applications, such as Microsoft Office 365.

4.4.1 About cloud credentials

Cloud credentials allow a user to access and use applications hosted in the cloud through a specific domain. The credentials are added separately for each cloud application.

4.4.2 Configuring cloud credentials

This section describes how to configure a cloud credential.

IMPORTANT: A user can edit only their own cloud credentials.

To configure a cloud credential:

1. On the toolbar, click **Settings**.
2. Click the **Cloud Credentials** tab.
3. Under **Cloud Credentials**, do one of the following:
   - To add a cloud credential, click [**+**] **Add Cloud Credentials**.
   - To edit a cloud credential, select the cloud credential, and then click **Edit Cloud Credential**.

     NOTE: When editing a cloud credential, you can only change the password.
4. In the **User name** box, type the name of the user you want to configure.
5. In the **Password** box, type the password this user will require to access the cloud service.
6. In the **Domain** box, type the name of the domain that the user is registered with.
7. Click **Add** or **Save**.
8. To automatically back up all backup sets including newly created backup sets, select the **Autodiscover new items for backup** check box.

   NOTE: To use the **Autodiscover new items for backup** option, a cloud backup set must already exist.

4.4.3 Sharing cloud credentials

Global and customized administrators can share cloud credentials with other regular users so that they can create Microsoft Office 365 backup sets.

- A Global Administrator can share the cloud credentials of any user with any other user.
- A Customized Administrator can share only the cloud credentials of a Regular User who is owned or was configured by the Customized Administrator.
- A Regular User cannot share their cloud credentials with any other user.

To share a cloud credential:

1. On the toolbar, click **Settings**.
2. Click the **Cloud Credentials** tab.
3. Under **Cloud Credentials**, select the user whose cloud credentials you want to share with other users, and then click **Share Cloud Credentials**.
4. On the **Share Cloud Credentials** page, select the users with whom you want to share the cloud credential, and then click **Save**.

4.4.4 Deleting cloud credentials

You can delete a cloud credential if required.

- A Global Administrator can delete any user. The ownership of the cloud credentials of the deleted user are transferred to the Global Administrator who can now edit them.
- A Customized Administrator can delete only a user who is owned or was configured by the Customized User. The ownership of the cloud credentials of the deleted user is transferred to the Customized Administrator who can now edit them.
- A Regular User can delete only their own cloud credentials.

To delete a cloud credential:

1. On the toolbar, click **Settings**.
2. Click the **Cloud Credentials** tab.
3. Under **Cloud Credentials**, select the user whose cloud credentials you want to delete, and then click **Delete Cloud Credential(s)**.
4. When the system prompts you to confirm that you want to delete the cloud credential, click **Yes**.

4.5 Configuring the Management Console settings

This section describes how to configure the email, broadcast, report, and proxy settings for the Management Console.

4.5.1 Configuring the email notification settings

You can configure the SMTP server settings that are used for sending email notifications to other users.

To configure the email notification settings:

1. On the toolbar, click **Settings**, and then click the **General** tab.
2. On the **General page,** click the **Email** tab, and then do the following:
   a) In the **SMTP host** box, type the name or IP address of the email server that will be used for the sending email notifications.
   b) In the **SMTP port** box, enter the port number that will be used by the mail server for sending email notifications.
   c) Select the type of security (**SSL**, **TLS** or **None**) you want to use for establishing an encrypted link between the email server and email client.
   d) To enable a SMTP client to log in using an authentication mechanism from those supported by the SMTP server, select the **Enable SMTP authentication** check box, and then type the user name and password.
   e) In the **Sender's email address** box, type the email address from which the notification will be sent.
   f) To send a test email notification, click **Test**.
   g) Click **Save**.

4.5.2 Configuring the broadcast notification settings

You can configure the broadcast settings to send a notification to all Management Console users. This is useful when you need to update the system and want to notify all users.

To configure the broadcast settings:

1. On the toolbar, click **Settings**, and then click the **General** tab.
2. On the **General page,** click the **Broadcast** tab, and then do the following:
   a) In the **Message** box, type the notification message you want to send.
   b) To email the same notification message to all users, select the **Include email notification** check box.
3. Click **Send**.

4.5.3 Configuring the email report schedule settings

This section describes how to configure a schedule to email a generated report to users.

To configure a scheduled report:

1. On the toolbar, click **Settings**, and then click the **General** tab.
2. On the **General page,** click the **Report** tab, and then do one of the following:
   - To create a new scheduled report, click [**+**].
   - To edit a report, select the required report and then click .
3. In the **Schedule name** box, type a name for the schedule.
4. Under **Report Type**, select the report(s) you want to email.
5. Under **Users**, do the following:
   – To email the reports to a Global Administrator, select the **Global Administrator** check box.
   – To email the report(s) to specific users, type the email addresses.

   NOTE: Separate multiple email address with a comma (,).

   c) Under **Schedule details**, select the frequency at which the reports should be emailed.
6. Click **Create**/**Save**.

4.5.4 Configuring the proxy server settings

This section describes how to configure the proxy server settings for the Management Console.

To configure the proxy server settings:

1. On the toolbar, click **Settings**, and then click the **General** tab.
2. On the **General** page, click the **Proxy** tab, and then do the following:
   a) In the **HTTP proxy address** box, type the IP address of the HTTP proxy server.
   b) In the **HTTP proxy port** box, type the port number required to communicate with the HTTP proxy server.
   c) In the **HTTPS proxy address** box, type the IP address of the HTTPS proxy server.

d) In the **HTTPS proxy port** box, type the port number required to communicate with the HTTPS proxy server.

e) To use the same settings for both HTTP and HTTPS, select the **Use same proxy server settings for http and https** check box.

3. Click **Save**.

5 Working with schedules

This section describes how to configure and work with schedules for unattended activities.

5.1 About schedules

You can perform automatic, unattended activities on specific backup sets when you create a schedule and assign backup sets to that schedule. A Schedule is composed of details that define when unattended backups will be performed.

5.2 Configuring a schedule

In a schedule, each detail determines when and how often a backup or other task is performed. You can add as many details as required to a schedule.

NOTE: A default schedule is provided, which you can edit if required.

To configure a schedule:

1. On the toolbar, click **Data Management**.
2. Click the **Schedules** tab.
3. Under **Schedules**, do one of the following:
   - To add a schedule, select the required DS-Client, and then click **[+] Create Schedule**.
   - To edit a schedule, select the schedule that you want to edit, and then click **Edit Schedule**.
4. In the **Name** box, type a name for the schedule.
5. In the **Occurs** box, select the frequency at which the schedule should be run. Your choices are as follows:
   - **One time** – Select this option if you want the schedule to run only once. Specify the date on which you want the schedule to run.
   - **Daily** – Select this option if you want the schedule to run daily. Specify the interval at which you want the schedule to run.
   - **Weekly** – Select this option if you want the schedule to run weekly. Specify the interval at which you want the schedule to run, and then select the days.
   - **Monthly** - Select this option if you want the schedule to run monthly. Specify the day of the month and the interval at which you want the schedule to run.

   The details will vary depending on the option you select.

6. Under **Frequency**, select one of the following:
   a) **Occurs once** - Select this option if you want the schedule to run just once.
   b) **Occurs every** - Select this option to specify the interval at which the schedule should run in minutes or hours.
7. Under **Time selection**, do the following:
   a) In the **Start date** box, specify the date when the schedule should start.
   b) In the **End date** box, specify the date when the schedule should end.
   c) In the **Starting at** box, specify the time at which the schedule should start.
   d) In the **Ending at** box, specify the time at which the task should end.
   e) In the **Day** box, specify the number of days for which the task should continue.

NOTE: If you have selected the **One time** option, you only need to enter the start time and number of days the schedule should run.

---

8. Under **Tasks**, do the following:
   - To perform a backup, select the **Perform backup** check box.
   - To apply a retention rule, select the **Enforce retention** check box.
9. Click **Create** or **Save**.

5.3 Reassigning a schedule

You can reassign a different schedule to a backup set or to multiple backup sets as required.

To reassign a schedule:

1. On the toolbar, click **Data Management**.
2. Click the **Schedules** tab.
3. Select a schedule, and then click **Reassign Schedule.**
4. On the **Schedule** page, select the backup set(s) to which you want to reassign a schedule, and then click **Reassign**.
5. On the **Reassign to Schedule** page, select a schedule, and then click **Save**.

5.4 Deleting a schedule

You can delete a schedule if required.

To delete a schedule:

1. On the toolbar, click **Data Management**.
2. Click the **Schedules** tab.
3. Under **Schedules**, select the schedule that you want to delete, and then click **Delete Schedule**.
4. When the system prompts you to confirm that you want to delete the schedule, click **Yes**.

6 Working with retention rules

This section describes how to configure and work with retention rules.

6.1 About retention rules

Retention rules allow you to implement granularity (specific pattern retention) in your backed up generations. If you do not use the retention feature, your backup data will remain online according to the settings for backup set generation.

After assigning a retention rule to an individual backup set, you need to enforce the rule either on demand or on a schedule. When a retention rule is enforced, the online data that does not qualify for retention is deleted. If options within a retention rule overlap, the DS-Client software will only apply options that retain more data.

6.2 Configuring a retention rule

This section describes how to configure a retention rule.

NOTE: A default retention rule is provided, which you can edit if required.

To configure a retention rule:

1. On the toolbar, click **Data Management**.
2. Click the **Retention Rules** tab.
3. Under **Retention Rules**, do one of the following:
   - To create a retention rule, select the DS-Client, and then click [**+**] **Create Retention Rule**.
   - To edit an existing retention rule, select the retention rule, and then click **Edit Retention Rule**.
4. In the **Name** box, type a name for the retention rule.
5. Under **Retention settings**, do the following:
   a) In the **Keep most recent generations** box, specify the number of generations of the file that should be retained online.
   b) To specify the time period for which all generations should be retained online, select the **Keep all generations for the last** check box, and then specify the time period in minutes, hours, or days.

6. Under **Time retention rules**, do one of the following:
   - To create a time-based retention rule, click [**+**] **Create Time Retention Rule**.
   - To edit an existing time-based retention rule, select the rule, and then click **Edit Time Retention Rule**.
7. In the **Create**/**Edit Time Retention Rule** dialog box, do the following:
   a) To keep a generation for a specific interval, specify a value in minutes, hours, days, weeks, months, or years. This is applied for all intervals that are applicable within the length of the retention rule.
   b) To keep a generation for a week, month, or a year, specify the value at which or before the generation available should be retained.

NOTE: A time retention rule keeps one generation from each time interval that fits into the retention range. When this rule is enforced, the most recent generation from each interval is retained.

---

   c) In the **Valid for the last** box, type the value and select a parameter from hours, days, weeks, months or years.This defines the time span the retention rule covers. By default, this period is 1 week. If you select a time retention option that spans a longer period, you should extend this value to at least match that period.
   d) Click **Create** or **Save.**

6.3 Reassigning a retention rule

You can reassign a different retention rule to a backup set or to multiple backup sets as required.

To reassign a retention rule:

1. On the toolbar, click **Data Management**.
2. Click the **Retention Rules** tab.
3. Under **Retention Rules**, select the DS-Client for which you want to reassign a retention rule.
4. Select a retention rule, and then click **Reassign Retention Rule**.
5. On the **Retention Rule** page, select the backup set(s) to which you want to reassign a schedule, and then click **Reassign**.
6. On the **Reassign to Retention Rule** page, select a retention rule, and then click **Save**.

6.4 Deleting a retention rule

You can delete a retention rule if required.

NOTE: When you delete a retention rule, any associated time-based retention rules are also deleted.

To delete a retention rule:

1. On the toolbar, click **Data management**,
2. Click the **Retention Rules** tab.
3. Under **Retention Rules**, select the retention rule that you want to delete, and then click **Delete retention rule.**
4. When the system prompts you to confirm that you want to delete the retention rule, click **Yes**.

7 Working with backup sets

This section provides describes how to configure and restore backup sets.

7.1 About backup sets

A backup set consists of a list of the items, that need to be backed up and the settings that define how to perform the backup.The following backup sets are supported by DS-Clients running on different operating systems.

Backup Set	Windows	Linux	Mac
File system Backup Sets			
File system	✓	✓	
Permissions	✓		
Cloud Backup Sets			
Microsoft Office 365	✓		
Database Backup Sets			
Microsoft SQL Server (Classic)	✓		
Microsoft SQL Server (VSS aware)	✓		
Server Backup Sets			
Microsoft Exchange Server (VSS aware)	✓		
Microsoft SharePoint Server (VSS aware)	✓		
Virtual Machine Backup Sets			
Microsoft Hyper-V (Standalone)	✓		
Microsoft Hyper-V (Cluster)	✓		
VMware vSphere Server	✓		

Table 1 Supported backup sets

7.2 File system backup sets

This section describes how to configure a file system backup set.

7.2.1 About File system backup sets

File system backup sets allow you to back up data at various levels of the tree structure in a file system. You can select individual files, folders, or drives to back up from a machine that you can access.

7.2.2 Configuring a File system backup set

This procedure describes how to configure a File system backup set.

To configure a File system backup set:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
   - To create a backup set, click **Create Backup Set**.
   - To edit a backup set, select the DS-System, customer account, and DS-Client number, and then click **Edit Backup Set**.

NOTE: When editing a file system backup set, you can modify only the user name, password, domain, backup set name, schedule, retention rule, and advanced options.

---

3. In the **Backup set type** box, select **File System**.
4. In the **DS-System** box, select the DS-System.
5. In the **Customer account** box, select the customer account.
6. In the **DS-Client number** box, select the DS-Client.
7. In the **Source IP address** box, type the IP address of the DS-Client computer from which the file system will be backed up.
   - To use the DS-Client credentials to connect to the local DS-Client computer, select **Use DS-Client Credentials**.
   - To use other credentials, select **Use network credentials** and then type the user name, password, and domain name in their corresponding boxes.
8. To select the items that you want to back up, click **Select Backup Set Items**.
9. In the **Select Backup Set Items** dialog box, select the individual folders or items that you want to back, and then click **Select**.

NOTE: Subdirectories are included by default. To exclude subdirectories, clear the **Include subdirectories** check box.

---

10. In the **Backup set name** box, type a name for the backup set.
11. In the **Schedule** box, select a schedule for the backup set.
12. In the **Retention rule** box, select a retention rule for the backup set.
13. To configure advanced options for the backup set, click **Advanced Options.**

a) Under **Backup set options**, do the following:

- In the **Compression algorithm** box, select the type of compression algorithm to be used when performing a backup.
- In the **Stop on errors** box, specify the number of errors that must occur during the backup process before the process is stopped.
- To record all the files that were backed up in the Activity Log, select the **Enable detailed log** check box.

b) Under **Cybersecurity options**, do the following:

- To scan your files for malware during the backup process, select the **Enable cybersecurity scan** check box.

NOTE: The cybersecurity option is available only when connected to a Windows DS-Client. If you enable cybersecurity, you must configure the quarantine folder. For more information, see Section 4.1.3, "Configuring the DS-Client cybersecurity settings".

---

c) Under **More options**, do the following:

- To copy the backed up data to the DS-Client buffer, select the **Use buffer** check box. This frees up the backup source as fast as possible. The DS-Client will then send the files from the DS-Client buffer to the DS-System.
- To save the backed up data to a local storage location, select the **Save on a local storage** check box, and then in the **Local storage path** box, type the path for the local storage location.

d) Click **Save**.

14. Click **Create** or **Save**.

7.3 Microsoft Exchange Server backup sets

This section describes how to configure a Microsoft Exchange Server backup set in a standalone configuration.

7.3.1 About Microsoft Exchange Server backup sets

The DS-Client connects to the source machine and instructs the VSS service to take a snapshot of that machine. After the snapshot is generated, DS-Client continues to backup using the VSS snapshot (sufficient storage must be available on the source machine in order to hold the snapshot).

Only one VSS snapshot of a volume can be taken at a time. This means that simultaneous snapshots of the same volume from different VSS-aware backup sets is not possible. Once backup is complete, the space used by the snapshot is freed up.

7.3.2 Configuring a Microsoft Exchange Server backup set

This procedure describes how to configure a Microsoft Exchange Server (VSS-aware) backup set.

To configure a Microsoft Exchange Server backup set:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
   - To create a backup set, click **Create Backup Set**.
   - To edit a backup set, select the DS-System, customer account, and DS-Client number, and then click **Edit Backup Set**.

NOTE: When editing a Microsoft Exchange Server backup set, you can modify only the user name, password, domain backup set name, schedule, retention rule, and advanced options.

---

3. In the **Backup set type** box, select **Microsoft Exchange Server (VSS aware)**.
4. In the **DS-System** box, select the DS-System.
5. In the **Customer account** box, select the customer account.
6. In the **DS-Client number** box, select the DS-Client number.
7. In the **Source IP address** box, type the IP address of the server where the Microsoft Exchange server VSS components are located.
8. Under **Use network credentials**, type the user name, password, and the domain name in their corresponding boxes.
9. To select the items that you want to back up, click **Select Backup Set Items**.
10. On the **Select Backup Set Items** page, select the individual folders or items that you want to backup, and then click **Select**.

NOTE: Subdirectories are included by default. To exclude subdirectories, clear the **Include subdirectories** check box.

---

11. In the **Backup set name** box, type a name for the backup set.

12. In the **Schedule** box, select a schedule for the backup set.
13. In the **Retention rule** box, select the retention rule for the backup set.
14. To configure advanced options for the backup set, click **Advanced Options**.
    a) Under **Backup set options**, do the following:
        - In the **Compression algorithm** box, select the type of compression algorithm to be used when performing a backup.
        - In the **Stop on errors** box, specify the number of errors that must occur during the backup process before the process is stopped.
        - To record all the files that were backed up in the Activity Log, select the **Enable detailed log** check box.
    b) Under **Database backup policy**, in the **Full dump** box, select the method for the database dump. Your choices are as follows:
        - **Always** - Select this option if you want each backup of the target server to perform a full dump of each database. This is the default option.
        - **Plus Differential** - Select this option to perform a full dump of the database on the first backup, followed by differential backups until another full backup is required. Specify the time interval between the database dumps.
        - **Plus Incremental** - Select this option to perform a full dump of the database on the first backup, followed by incremental backups until another full dump is required.
    c) Under **More options**, do the following:
        - To save the backed up data to a local storage location, select the **Save on a local storage** check box, and then in the **Local storage path** box, type the path for the local storage location.
    d) Click **Save**.
15. Click **Create** or **Save**.

7.4 Microsoft Hyper-V Server backup sets

This section describes how to configure a Microsoft Hyper-V Server backup set.

7.4.1 About Microsoft Hyper-V Server backup sets

The backup and restore of Microsoft Hyper-V Server backup sets is based on the Microsoft Hyper-V VSS Writer. The backup unit is the Hyper-V virtual machine and not individual files within the virtual machine. The backup mechanism is called the *Saved State* method, where the virtual machine is put into a saved state during the snapshot process. Snapshots are taken of the appropriate volumes, and the virtual machine is returned to the previous state after the snapshot process is done.

VSS provides a consistent interface that allows online backup of a Hyper-V virtual machine. VSS-related meta-data is saved with the backup data to provide the rules for data integration in each backed up virtual machine.

NOTE: Microsoft Hyper -V Server backup sets are supported only on Windows DS-Clients.

7.4.2 Before you begin

- To perform backup/restore with Microsoft Hyper-V VSS Writer, the “Hyper-V Virtual Machine Management” service must be running on the target server.
- Each target virtual machine must have “Integration Services” installed to be backed up using Microsoft VSS Writers (volume snapshot).

7.4.3 Configuring a Microsoft Hyper-V Server backup set

This procedure describes how to configure a Microsoft Hyper-V backup set.

To configure a Microsoft Hyper-V Server backup set:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
   - To create a backup set, click **Create Backup Set**.
   - To edit a backup set, select the DS-System, customer account, and DS-Client number, and then click **Edit Backup Set**.

3. In the **Backup set type** box, select one of the following:
   - Microsoft Hyper-V Server (Standalone)
   - Microsoft Hyper-V Server (Cluster)

NOTE: When editing a Microsoft Hyper-V Server backup set, you can modify only the user name, password, domain, backup set name, schedule, retention rule, and advanced options.

---

4. In the **DS-System** box, select the DS-System.
5. In the **Customer account** box, select the customer account.
6. In the **DS-Client number** box, select the DS-Client where this backup set will be created.
7. In the **Source IP address** box, type the IP address of the server where the Microsoft Hyper-V Server components are located.
8. Under **Use network credentials**, type the user name, password, and domain name in their corresponding boxes.
9. To select the items that you want to back up, click **Select Backup Set Items**.
10. In the **Select Backup Set Items** dialog box, select the individual folders or items that you want to backup and click **Select**.

NOTE: Subdirectories are included by default. To exclude subdirectories, clear the **Include subdirectories** check box.

---

11. In the **Backup set name** box, type a name for the backup set.
12. In the **Schedule** box, select a schedule for the backup set.
13. In the **Retention rule** box, select the retention rule for the backup set.
14. To configure advanced options for the backup set, click **Advanced Options**.
    a) Under **Backup Set options**, do the following:
       - In the **Compression algorithm** box, select the type of compression algorithm to be used when performing a backup.
       - In the **Stop on errors** box, type the number of errors that must occur before the backup process is stopped.
       - To record all the files that were backed up in the Activity Log, select the **Enable detailed log** check box.

    b) Under **Database backup policy**, in the **Full dump** box, select the method for the database dump. Your choices are as follows:

- **Always** - Select this option if you want each backup of the target server to perform a full dump of each database. This is the default option.
- **Plus Incremental** - Select this option to perform a full dump of the database on the first backup, followed by incremental backups until another full dump is required. Select the time interval in days, weeks, or months when this policy should be applied.
- **Enable File Level Restore** - Select this option to restore individual files.

c) Under **More options**, do the following:

- To save the backed up data to a local storage location, select the **Save on a local storage** check box, and then in the **Local storage path** box, type the path for the local storage location.

d) Click **Save.**

15. Click **Create/Save**.

7.5 Microsoft Office 365 backup sets

This section describes how to configure a Microsoft Office 365 backup set.

7.5.1 About Microsoft Office 365 backup sets

The Microsoft Office 365 data that can be backed up and restored using DS-Client includes Exchange Online data, SharePoint Online data, and OneDrive data (as SharePoint Online data).

NOTE: In Microsoft Office 365 Small Business domains, only the backup and restore of Exchange Online data is supported by DS-Client; the backup and restore of SharePoint Online data is not supported.

Requirements

- A Microsoft Office 365 license is required for every user whose Microsoft Office 365 mailbox or SharePoint site you plan to back up and restore, for every user who will administer the backup and restore process in the Office 365 portal/ admin center, and for every user whose credentials will be used by DS-Client to access the backup source.
- You must install the Microsoft Office 365 DS-Client plug-in on each DS-Client computer on which you want to perform the backup and restore of Microsoft Office 365 backup sets.

Exchange Online

DS-Client can back up Exchange data from Exchange Online, or from an on-premises Exchange Server using Exchange Web Services (EWS) and restore the same. Exchange data that you can back up and restored are the following:

- Calendars and appointments
- Contacts (including Contact Lists, but not Contact Groups)
- Email messages
- Public Folders
- Tasks

Exchange data has to be in a user mailbox, shared mailbox, or resource mailbox to be supported. It can be restored to the same mailbox or a different mailbox of the original domain or of a different domain using DS-Client. Backing up Exchange distribution groups is not supported.

SharePoint Online

DS-Client can back up SharePoint data from SharePoint Online and restore it to SharePoint Online. SharePoint data that can be backed up and restored includes the following:

- Individual list items
- Lists
- Sites
- Site collections
- Web parts

You can select data for backup at the site collection, site, and list levels. You cannot select list items individually as backup set items. However, the individual list items that are within selected lists will be backed up. You can select individual list items for restore. SharePoint data can only be restored to the same site collection at the original domain. Backing up Lookup columns in not supported.

OneDrive

OneDrive data is processed as SharePoint Online data by DS-Client. OneDrive data under personal sites can be backed up and restored using DS-Client. OneDrive data for each user is backed up as the Documents List of each user's personal site.

7.5.2 Configuring a Microsoft Office 365 backup set

This section describes how to configure a Microsoft Office 365 backup set.

To configure a Microsoft Office 365 backup set:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
   - To create a backup set, click **Create Backup Set**.
   - To edit a backup set, select the DS-System, customer account, and DS-Client number, and then click **Edit Backup Set**.

   NOTE: When editing a Microsoft Office 365 backup set, you can modify only the backup set name, schedule, retention rule, and advanced options.

3. In the **Backup set type** box, select **Microsoft Office 365**.
4. In the **DS-System** box, select the DS-System.
5. In the **Customer account** box, select the customer account.
6. In the **Domain** box, select the domain name of the backup source.

   IMPORTANT: The **Backup set name** box is not displayed, because the default setting is to create multiple backup sets of Microsoft Office 365 file types. By default all the file types are also selected.

7. To select the items that you want to back up, click **Select Backup Set Items**.
8. In the **Select Backup Set Items** dialog box, do the following:
   a) Under **Cloud Credentials**, type the user name.
   b) Select the service with the items that you want to back up.

      You can select an entire domain and then select individual items (Inbox, Sent items, Calendar, Contacts, Tasks, Notes) or select mailboxes, and then for each mailbox, select the required item.

      NOTE: For Exchange Online and Public Folders, you can select folders or items. For SharePoint Online and OneDrive, you can only select folders.

   c) Click **Save**.
9. In the **Backup set name** box, type a name for the backup set.

NOTE: This box is displayed if you have selected the option **Single** backup set creation in **Advanced Options**.

10. In the **Schedule** box, select a schedule for the backup set.
11. In the **Retention rule** box, select a retention rule for the backup set.
12. To configure advanced options for the backup set, click **Advanced Options**.
    a) Under **Backup set options**, do the following:
       - In the **Compression algorithm** box, select the type of compression algorithm to be used when performing a backup.
       - In the **Stop on errors** box, specify the number of errors that should occur during the backup process before the backup process is stopped.
       - To record all the files that were backed up in the Activity Log, select the **Enable detailed log** check box.

    b) Under **Microsoft Office 365 options**, do the following:
       - For **Backup sets creation**, use the toggle key to create **Single** or **Multiple** backup sets.
       - For **Service**, select a service or services to backup.

       IMPORTANT: The Single option is recommended only if you are backing up a small number of items. Backing up a large number of items in a single backup set can adversely impact performance.

    c) Under **More options**, do the following:
       - To copy the backed up data to the DS-Client buffer, select the **Use buffer** check box. This frees up the backup source as fast as possible. The DS-Client will then send the files from the DS-Client buffer to the DS-System.
       - To save the backed up data to a local storage location, select the **Save on a local storage** check box, and then in the **Local storage path** box, type the path for the local storage location.

    d) Click **Save**.
13. Click **Create**/**Save**.

7.6 Microsoft SharePoint Server backup sets

This sections describes how to configure a Microsoft SharePoint Server backup set.

7.6.1 About Microsoft SharePoint Server backup sets

This backup set permits the online backup and restore of Microsoft SharePoint Server using the target computer's Microsoft VSS components.

VSS only works with Windows DS-Clients, and the target Windows computer must have the Microsoft Volume Shadow Copy Service (VSS) components necessary to perform this type of backup.

7.6.2 Configuring a Microsoft SharePoint Server backup set

This procedure describes how to configure a Microsoft SharePoint Server backup set.

To configure a Microsoft SharePoint Server backup set:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
   - To create a backup set, click **Create Backup Set**.
   - To edit a backup set, select the DS-System, customer account, and DS-Client number, and then click **Edit Backup Set**.

   NOTE: When editing a Microsoft SharePoint Server backup set, you can modify only the user name, password, domain, backup set name, schedule, and retention rule.

3. In the **Backup set type** box, select **Microsoft SharePoint Server (VSS aware)**.
4. In the **DS-System** box, select the DS-System.
5. In the **Customer account** box, select the customer account.
6. In the **DS-Client number** box, select the DS-Client where this backup set will be created.
7. In the **Source IP address** box, type the IP address of the server where the Microsoft SharePoint Server components are located.

8. Under **Use network credentials**, type the user name, password, and domain name in their corresponding boxes.
9. To select the items that you want to back up, click **Select Backup Set Items**.
10. In the **Select Backup Set Items** dialog box, select the individual folders or items that you want to backup, and then click **Select**.

NOTE: Subdirectories a re included by default. To exclude subdirectories, clear the **Include subdirectories** check box.

---

11. In the **Backup set name** box, type a name for the backup set.
12. In the **Schedule** box, select a schedule for the backup set.
13. In the **Retention rule** box, select the retention rule for the backup set.
14. To configure advanced options for the backup set, click **Advanced Options**.
    a) Under **Backup Set** options, do the following:
       - In the **Compression algorithmCompression algorithm** box, select the type of compression algorithm to be used when performing a backup.
       - In the **Stop on errors** box, type the number of errors that should occur during the backup process before the backup process is stopped.
       - To record all the files that were backed up in the Activity Log, select the **Enable detailed log** check box.

    b) Under **Database backup policy**, in the **Full dump** box, the default method for database dump is **Always**.

    c) Under **More options**, do the following:
       - To save the backed up data to a local storage location, select the **Save on a local storage** check box, and then in the **Local storage path** box, type the path for the local storage location.

    d) Click **Save**.
15. Click **Create**/**Save**.

7.7 Microsoft SQL Server backup sets

This section describes how to configure a Microsoft SQL Server backup set.

7.7.1 About Microsoft SQL Server backup sets

A Microsoft SQL Server backup set contains the backup from a single, successful backup operation. Restore statements operate on a single backup set within the media set on the specified backup device or devices.

7.7.2 Configuring a Microsoft SQL Server backup set

This procedure describes how to configure a Microsoft SQL server backup set.

To configure a Microsoft SQL server backup set:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
   - To create a backup set, click **Create Backup Set**.
   - To edit a backup set, select the DS-System, customer account, and DS-Client number, and then click **Edit Backup Set**.
3. In the **Backup set type** box, select a database from the following:
   - Microsoft SQL Server (Classic)
   - Microsoft SQL Server (VSS aware)

NOTE: When editing a Microsoft SQL Server (VSS-aware) backup set, you can modify only the user name, password, domain, backup set name, schedule, retention rule, and advanced options. For a Microsoft SQL Server (Classic) backup set, you can additionally modify the database user name and database password.

---

4. In the **DS-System** box, select the DS-System.
5. In the **Customer account** box, select the customer account.
6. In the **DS-Client number** box, select the DS-Client where this backup set will be created.
7. In the **Source IP address** box type the IP address of the DS-Client computer where the source database is located.

a) If the source is the DS-Client computer where the Microsoft SQL Server is running, do one of the following:

- To login with DS-Client credentials and connect to the database, select **Use DS-Client Credentials**, and then type the database user name and database password.
- To login with network credentials, select **Use network credentials**, and then type the user name, password, domain name, database user name, and database password in their corresponding boxes.

b) If the source is a remote computer, type the required details for **Use network credentials**.

8. In the **Database Dump Path**, select a location for the database dump. Your choices are as follows:

a) **DS-Client Buffer** - Select this option to save the dump file on the local storage of the DS-Client computer.

b) **DS-Client Pipe** - Select this option if your database is too large to be dumped to a file. During a backup, the DS-Client reads from the pipe on the source database.

c) **Database Server** - Select this option to dump the database in a directory on the remote database server computer, and then click to select the destination folder. This option is available only if you specify a remote DS-Client in the **Source IP address** box.

9. To select the items that you want to back up, click **Select Backup Set Items**.
10. In the **Select Backup Set Items** dialog box, select the individual folders or items that you want to back up, and then click **Select**.

NOTE: Subdirectories are included by default. To exclude subdirectories, clear the **Include subdirectories** check box.

11. In the **Backup set name** box, type a name for the backup set.
12. In the **Schedule** box, select a schedule for the backup set.
13. In the **Retention rule** box, select a retention rule for the backup set.
14. To configure advanced options for the backup set, click **Advanced Options**.

a) Under **Backup set options**, do the following:

- In the **Compression algorithm** box, select the type of compression algorithm to be used when performing a backup.
- In the **Stop on errors** box, specify the number of errors that must occur before the backup process is stopped.

- To record all the files that were backed up in the Activity Log, select the **Enable detailed log** check box.

b) Under **Database backup policy**, in the **Full dump** box, select the method for the database dump. Your choices are as follows:

- **Always** - Select this option if you want each backup of the target server to perform a full dump of each database. This is the default option.
- **Plus Differential** - Select this option to perform a full dump of the database on the first backup, followed by differential backups until another full backup is required. Specify the time interval between the database dumps.

c) Under **More options**, do the following:

- To copy the backed up data to the DS-Client buffer, select the **Use buffer** check box. This frees up the backup source as fast as possible. The DS-Client will then send the files from the DS-Client buffer to the DS-System.
- To save the backed up data to a local storage location, select the **Save on a local storage** check box, and then in the **Local storage path** box, type the path for the local storage location.

NOTE: The option **Save on a local storage** is not available for Microsoft SQL Server (VSS-aware) backup sets.

d) Click **Save**.

15. Click **Create**/**Save**.

7.8 Permissions backup sets

This section describes how to configure and restore a permissions backup set.

7.8.1 About permissions backup sets

You can use the Permissions backup set to back up only the permissions of one or more selected backup items, which reduces the backup time. A separate dump file is saved for each backup item.

When an online File system backup set is performed, the files are saved with the current permissions and attributes. If the permissions or attributes are changed but the content of the files remains the same, DS-Client will not backup the changes to DS-System. With a Permission backup set, modifications to attributes like Compress, Read-Only, Hidden, Archive, and Index can be detected and backed up.

NOTE: Modifications to the Encrypt attribute can be detected only by using an Online File system backup set.

7.8.2 Configuring a permissions backup set

This procedure describes how to configure a permissions backup set that will save the last permissions and attributes of your files.

To configure a permissions backup set:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
   - To create a backup set, click **Create Backup Set**.
   - To edit a backup set, select the DS-System, customer account, and DS-Client number, and then click **Edit Backup Set**.

   NOTE: When editing a permissions backup set, you can modify only the user name, password, domain, backup set name, schedule, retention rule, and advanced options.

3. In the **Backup set type** box, select **Permissions**.
4. In the **DS-System** box, select the DS-System.
5. In the **Customer account** box, select the customer account.
6. In the **DS-Client number** box, select the DS-Client.
7. In the **Source IP address** box, type the IP address of the DS-Client computer from which the permissions will be backed up.
   - To use the DS-Client credentials to connect to the local DS-Client computer, select **Use DS-Client Credentials**.
   - To use other credentials, select **Use network credentials** and then type the user name, password, and domain name in their corresponding boxes.
8. To select the items that you want to back up, click **Select Backup Set Items**.
9. In the **Select Backup Set Items** dialog box, select the individual folders or items that you want to back up, and then click **Select**.
10. In the **Backup set name** box, type a name for the backup set.
11. In the **Schedule** box, select a schedule for the backup set.
12. In the **Retention rule** box, select a retention rule for the backup set.

13. To configure advanced options for the backup set, click **Advanced Options.**

    a) Under **Backup set options**, do the following:

    - In the **Compression algorithm** box, select the type of compression algorithm to be used when performing a backup.
    - In the **Stop on errors** box, specify the number of errors that must occur during the backup process before the process is stopped.
    - To record all the files that were backed up in the Activity Log, select the **Enable detailed log** check box.

    b) Under **More options**, do the following:

    - To copy the backed up data to the DS-Client buffer, select the **Use buffer** check box. This frees up the backup source as fast as possible. The DS-Client will then send the files from the DS-Client buffer to the DS-System.
    - To save the backed up data to a local storage location, select the **Save on a local storage** check box, and then in the **Local storage path** box, type the path for the local storage location.

    c) Click **Save**.

14. Click **Create** or **Save**.

7.9 VMware VSphere Server backup sets

This section describes how to configure and restore a VMware vSphere Server backup set.

7.9.1 About VSphere vSphere backup sets

A VMware vSphere Server backup set uses the native VMware vSphere Storage APIs - Data Protection (VADP) when DS-Client performs backup and restore of the target virtual machines.

7.9.2 Before you begin

Before creating a VMware vSphere Server backup set, ensure that the following requirements are met:

- For application consistent backups, ensure that VMware Tools is installed on the guest operating system of the virtual machine.
- If an ESXi host is added with its DNS name to the vCenter Server, the DS-Client machine must be able to execute a name resolution for that ESXi host to back up or restore the virtual machines.

7.9.3 Limitations for VMware vSphere Server backup sets

VMware vSphere Server backup sets have the following limitations:

- You cannot back up virtual machines that have Fault Tolerance turned on. For more information, see *Backup of fault tolerant virtual machines* in the *DS-Client User Guide*.
- You cannot back up virtual machines with physical or virtual raw disk mapping (RDM) devices.
- Avoid running multiple clones with Local DS-VDR activities on the same virtual machine from the same or different Local DS-VDR Tools.
- Avoid scheduling or performing VMware vSphere Server backup and VMware vSphere snapshot replication activities at the same time on the same vSphere virtual machine. This can adversely affect the backup or replication process.

7.9.4 Configuring a VMware vSphere Server backup set

This procedure describes how to configure a VMware vSphere Server backup set.

To configure a VMware vSphere Server backup set

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
   - To create a backup set, click **Create Backup Set**.
   - To edit a backup set, select the DS-System, customer account, and DS-Client number, and then click **Edit Backup Set**.

NOTE: When editing a VMware vSphere Server backup set, you can modify only the user name, password, domain, backup set name, schedule, retention rule, and advanced options.

---

3. In the **Backup set type** box, select **VMware vSphere Server**.
4. In the **DS-System** box, select the DS-System.
5. In the **Customer account** box, select the customer account.
6. In the **DS-Client number** box, select the DS-Client.
7. In the **Source IP address** box, type the IP address of the DS-Client computer from which the VMware vSphere Server will be backed up.
8. To select the items that you want to back up, click **Select Backup Set Items**.

9. In the **Select Backup Set Items** dialog box, select the individual folders or items that you want to back up, and then click **Select**.
10. In the **Backup set name** box, type a name for the backup set.
11. In the **Schedule** box, select a schedule for the backup set.
12. In the **Retention rule** box, select a retention rule for the backup set.
13. To configure advanced options for the backup set, click **Advanced Options.**
    a) Under **Backup set options**, do the following:
       - In the **Compression algorithm** box, select the type of compression algorithm to be used when performing a backup.
       - In the **Stop on errors** box, specify the number of errors that must occur during the backup process before the process is stopped.
       - To record all the files that were backed up in the Activity Log, select the **Enable detailed log** check box.

    b) Under **Virtual machine options**, select the required option(s).
       - **Enable File Level Restore (FLR)** - Select this option to restore individual files or directories of one or more multiple virtual machines.
       - **Back up virtual machine memory** - Select this option to save the virtual machine state (running programs loaded in memory).
       - **Enable Changed Block Tracking (CBT)** - Select this option to verify the disk signature interval (generations).
       - **Verify disk signature interval (generations)** - If you have selected the **Enable Changed Block Tracking (CBT)** option, then type the number of generations after which the system should verify the disk signature.

    c) Under **More options**, do the following:
       - To save the backed up data to a local storage location, select the **Save on a local storage** check box, and then in the **Local storage path** box, type the path for the local storage location.

    d) Click **Save**.
14. Click **Create** or **Save**.

7.10 Managing the list of backup sets

You can narrow your search for a backup set using the search and filter options.

To manage the list of backup sets:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
3. Under **Backup Sets**, do one of the following:
   - Select the DS-System, customer account, and the DS-Client number.
   - To search for a backup item to restore, click and type the name of the backup set that you want to restore.
   - To refine your search, click **Filter**, and in the **Filter** dialog box, use the filters based on status of the backup set, type of backup set, and status of cybersecurity.
   - To select all items in a filter type, click, to clear a selection of items in a filter type, click, and then, click **Reset**.
   - To view a summary of the backup set, click in the **Status** column, and then for more details, click the **SHOW FULL DETAIL** tab.

7.11 Performing an on-demand backup

The system is designed to perform unattended backups at scheduled intervals. In some instances, you may want to back up certain files on demand outside of a schedule. This section provides information on how to perform such on-demand backups.

You can perform on-demand backups at any time. The options available depend on the kind of backup set.

To perform an on-demand backup:

1. On the toolbar, click **Data Management**
2. Click the **Backup Sets** tab.
3. Under **Backup Sets**, select the DS-System, customer account, and the DS-Client number to display a list of backup sets.
4. Select the backup set that you want to back up, and then click **Backup Now**.
5. When the system prompts you to confirm that you want to start the backup, in the **Start Backup** dialog box, click **Yes** to backup the selected item.

7.12 Restoring a backup set

This procedure describes how to restore a backup set.

To restore a backup set:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
3. Under **Backup Sets**, select the DS-System, customer account, and the DS-Client number to display a list of backup sets.
4. Select the backup set that you want to restore, and then click **Restore Backup**.

NOTE: You can restore only one backup set at a time.

---

5. In the **Reason for restoring** box, select a reason for executing the restore.
6. In the **Time** box, click and select the backup session that you want to restore.
7. To scan your files for malware during the restore process, select the check box **Enable cybersecurity scan**.

NOTE: The cybersecurity option is available only for File system backup sets when connected to a Windows DS-Client. If you enable cybersecurity, you must configure the quarantine folder. For more information, see Section 4.1.3, “Configuring the DS-Client cybersecurity settings”.

---

8. Select the restore method for the backup set (applicable only for Microsoft Hyper-V Server backup sets). Your choices are as follows:
   - **Full** - Select this option will restore the entire virtual machine.
   - **File Level** - Select this option to restore individual files or directories of a virtual machine. This option is available only if you have selected **Enable file level restore** when creating the backup set.
9. Select the backup set you want to restore. To search for a backup set you want to restore, click and type the name of the backup set.
   - To search for an item to restore, click and type the name of the item that you want to restore.
   - To sort the items alphabetically, click AZ.
   - To sort the items by session time, click .
10. In the **Restore Location** box, select one of the following options:
    - **Original** - Select this option to restore the item to it’s original source location.

- **Alternate** - Select this option to specify an alternate destination for the restore items, and then do the following:

  a) In the **Server** box, click  . The **Alternate Location** dialog box appears.

  b) Under **Select alternate location**, in the **Server** box, type the IP address of the server to which the backup set will be restored.

  c) Type the user name, password, and domain name for the server in their corresponding boxes.

  d) Under **Rename components**, in the column **Restore to**, click  .

  e) In the **Select the destination folder** dialog box, select the folder to which you want to restore the backup set, and then click **Select.**

  f) If you have selected items to restore with a common path, under **Truncate Restore Path** (available only for Microsoft Office 365), you can select the level by which you can shorten the restore path.

  NOTE: Alternate location security: If the entire path is truncated, the alternate location directory will inherit the security of the truncated parent directory.

  g) Click **Save**.

- **Local** - Select this option to restore the items to the local disk of the DS-Client machine, and then do the following:

  a) Select the items to restore, and then type the path of the destination folder or click  .

  b) In the **Select the destination folder** dialog box, select the folder to which you want to restore the items.

  NOTE: The option **Local** is available only for Microsoft Office 365 backup sets.

11. Click **Restore**.
12. When the system prompts you to confirm that you want to restore the backup set, click **Yes**.

NOTE: Existing data in the target location will be overwritten.

7.13 Synchronizing a backup set

This procedure describes how to synchronize a backup set. The backup log of a Online backup set is a table in the DS-Client database that contains the details of what is backed up, it's attributes and master/delta generations. Due to various reasons, the backup log can fall out of synchronization with the online storage of DS-System.

To synchronize a backup set:

1. On the toolbar, click **Data Management**.
2. Under **Backup Sets**, select the DS-System, the customer account, and the DS-Client number to display a list of backup sets.
3. Select the backup set that you want to synchronize, and then click **More**.
4. Select **Synchronize**.
5. In the **Synchronize Backup Sets** dialog box, select the type of synchronization. Your choices are as follows:
   - **Normal** - Select this option to rectify discrepancies between the DS-Client backup logs and DS-System's online storage. This process can be triggered manually or automatically, by scheduled backup activities, by the orphaned backup sets recovery process, or by Weekly Admin. The DS-Client database is updated to match the DS-System Online Storage contents.
   - **Check-Only** - Select this option to check the synchronization between the backup log of the DS-Client and the online storage of the DS-System.This will only identify whether inconsistencies exist, and no corrective action will be taken. This process can be triggered only manually.
   - **DS-System based** - Select this option to synchronize the DS-Client backup log with the online storage information of DS-System. This process can be triggered manually or automatically. It can also be triggered by backup activities, when the DS-System has undergone a Disaster Recovery process.
   - **Sync with Local Storage** - Select this option to synchronize *Local Only* backup sets or backup sets that have the *Local Storage* option enabled. This process is triggered manually and it compares the records in the DS-Client database with the data existing in the *Local Storage* for a backup set.
6. Click **Synchronize**.

7.14 Deleting a backup set

This procedure describes how to delete a backup set.

To delete a file system backup set:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
3. Under **Backup Sets**, select the DS-System, the customer account, and the DS-Client number to display a list of backup sets
4. Select the backup set(s) that you want to delete, and then click **Delete**.
5. When the system prompts you to confirm that you want to delete the backup set, click **Yes**.

7.15 Performing a selective delete

This procedure describes how to delete files and directories that you select from the online storage using certain selection criteria. After performing a selective delete, the backup set will continue to exist and scheduled backups will continue to run.

To perform a selective delete:

1. On the toolbar, click **Data Management**.
2. Under **Backup Sets**, select the DS-System, the customer account, and the DS-Client number to display a list of backup sets.
3. Select the backup set for which you want to selectively delete items, and then click **More**.
4. Select **Selective Delete**.
5. Under **Time based data selection to delete**, do the following:
   a) In the **Start** box, click to display the **Select Backup Session** with a list of backup sessions, and then select the session with the required start time.
   b) In the **End** box, click to display the **Select Backup Session** with a list of backup sessions, and then select the session with the required end time.
6. Under **Leave generations online**, in the **Generations** box, select the number of latest generations that you want to retain. You will only be able to select files and directories that have more generations, than the number specified in this box.
7. Under **Select the items to delete**, select the item(s) to delete, and then click **Delete**.

8 Monitoring the system

This section describes how to generate various reports and view detailed logs.

8.1 Generating reports

This section provides information on the various reports that you can generate in the Management Console.

8.1.1 About reports

Reports are an important administrative tool that you can use to monitor the effectiveness of your backup and restore processes. All reports can be generated at any time on demand.

8.1.2 Generating a Backup Sets Report

This procedure describes how to generate a Backup Sets report, which contains detailed information about each backup set, including the protected size, stored size, and native size of the data backed up to the DS-System.

To generate a Backup Sets Report:

1. On the toolbar, click **Monitoring**.
2. Click the **Backup Sets Report** tab.
3. Select the DS-System, customer account, and the DS-Client account for which you want to generate the report.
4. To update the report, click **Refresh**.

8.1.3 Generating a Cloud Details Report

This procedure describes how to generate a Cloud Details Report, which displays detailed information about the Microsoft Office 365 cloud domains, including a summary of the Exchange Online mailboxes and SharePoint Online and OneDrive sites for each domain.

To generate a Cloud Details Report:

1. On the toolbar, click **Monitoring**
2. Click the **Cloud Details Report** tab.
3. Expand the domain for which you want to generate a Cloud Details Report.
4. To update the report, click **Refresh**.

8.1.4 Generating a Cybersecurity Scan Report

This procedure describes how to generate a Cybersecurity Scan Report, which displays the results of the cybersecurity scan of your File system backup sets. The information displayed includes the number of files scanned, the number of files that failed to scan, and the number of files detected with malware.

To generate a Cybersecurity Scan Report:

1. On the toolbar, click **Monitoring.**
2. Click the **Cybersecurity Scan Report** tab.
3. Select the DS-System, customer account, and DS-Client account for which you want to generate the report.
   - Under **Today's Backup Summary**, you can view the cybersecurity scan results for all backups performed that day.
   - Under **Today's Restore Summary**, you can view the cybersecurity scan results for all restores performed that day.
   - Under **Backup Trend**, you can view the trend results for all backups over a monthly, weekly, or daily interval
   - Under **Restore Trend**, you can view the trend results for all restores over a monthly, weekly, or daily interval.

   NOTE: The monthly trend report shows monthly data for the past six months, the weekly trend report shows weekly data for the past month, and the daily trend report shows daily data for the past week.
4. To update the report, click **Refresh**.

8.1.5 Generating a GDPR Compliance Report

This procedure describes how to generate a General Data Protection Regulation (GDPR) Compliance Report. GDPR is designed to strengthen and unify data protection and address the export of personal data.

To generate a GDPR Compliance Report:

1. On the toolbar, click **Monitoring**.
2. Click the **GDPR Compliance Report** tab.
3. Select the DS-System, customer account, and the DS-Client account for which you want to generate the report.
4. In the **Start date** and **End date** boxes, specify the period that you want the report to cover.

NOTE: A GDPR report can be generated only for the last 30 days.

5. To generate a GDPR Compliance Report, click **Generate Certificate**.
6. In the **Generate Certificate Request** dialog box, do the following:
   a) In the **Request type** box, type the purpose for which the report is required. (For example, audit, compliance, routine check)
   b) In the **Reason for request** box, type the reason for placing the request.
   c) In the **Phone number** box, type the telephone number of the person making the request.
   d) In the **Requested by (name)** box, type the name of the person requesting for this report.
7. Click **Generate Certificate**.

   The GDPR Certificate Status window informs you that the certificate is being generated and you will be notified when it is ready for download.
8. On the toolbar, click **Notifications**, and then click **Download**.
9. To update the reports list, click **Refresh**.

8.2 Viewing Logs

This section describes how to view various logs in the Management Console. You can view Activity Logs, Event Logs, and the Audit Trail.

8.2.1 About logs

Logs provide a detailed view of all the activities, events, and changes that are occurring in the system.

8.2.2 Viewing the Activity Log

The Activity Log provides a detailed list of all the activities in the system.

To view the Activity Log:

1. On the toolbar, click **Monitoring**.
2. Click the **Logs** tab.
3. Click **Activity Log**.

4. To refine the list of items that appear in the Activity Log, click **Filter**.
5. To select the columns that you want to view in the Activity Log, click **Select Columns**.
6. To update the Activity Log, click **Refresh**.

8.2.3 Viewing the Event Log

The Event Log provides a detailed list of all the errors, warnings, and information messages in the system.

To view the Event Log:

1. On the toolbar, click **Monitoring**.
2. Click the **Logs** tab.
3. Click **Event Log**.
4. To refine the list of items that appear in the Event Log, click **Filter**.
5. To select the columns that you want to view in the Event Log, click **Select Columns**.
6. To update the Event Log, click **Refresh**.

8.2.4 Viewing the Audit Trail

The Audit Trail provides a detailed list of all the changes made to the DS-System and DS-Client databases.

To view the Audit Trail:

1. On the toolbar, click **Monitoring.**
2. Click the **Logs** tab.
3. Click **Audit Trail**.
4. To refine the list of items that appear in the *Audi Trail*, click **Filter**.
5. To select the columns that you want to view in the *Audit Trail*, click **Select Columns**.
6. To update the Audit Trail, click **Refresh**.

8.2.5 Viewing the Grid Log

To view the grid log:

1. On the toolbar, click **Monitoring.**
2. Click the **Logs** tab.
3. Click **Grid Log**.
4. To refine the list of items that appear in the Grid Log, click **Filter**.
5. To select the columns that you want to view in the Grids Log, click **Select Columns**.
6. To update the Grid Log, click **Refresh**.

8.3 Viewing the status of a Grid DS-Client

This section describes how to view the status of a Grid DS-Client.

To view the status of Grid DS-Client:

1. On the toolbar, click **Monitoring**.
2. Click the **Status** tab.
3. Under **Grid Log**, expand a grid to display the status of the grid in detail.
4. To update the status, click **Refresh**.

8.4 Viewing notifications

You can view notifications from other users and the system, including when a Management Console update is available.

For information on how to install a Management Console update, see Section 2.6, “Installing Management Console updates”.