Asigra Cloud Backup v14.2

Management Console User Guide

April 2023

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: April 2023

Contents

Document history

Version	Date	Summary
1.0	August 31, 2020	- Released for General Availability.
1.1	October 2, 2020	- Management Console users can now scan their Microsoft 365 (Exchange Online) files for malware during the backup and restore process. Requires Windows DS-Client v14.2.0.1 and Management Console v14.2.0.1 or later.
1.2	January 20, 2021	- Management Console users can now scan their Microsoft 365 (Groups and Teams) files for malware during the backup and restore process. Requires Windows DS-Client v14.2.0.2) and Management Console v14.2.0.2 or later. - Management Console users can now remotely manage DS-Clients without opening a port in the firewall on the DS-Client machine. Requires DS-Client v14.2.0.2, DS-System v14.2.0.2, and Management Console v14.2.0.2 or later. - Management Console users can now configure a process to run before and/or after a File system backup to perform actions when a condition is met. Requires Windows DS-Client v14.2.0.2 and Management Console v14.2.0.2 or later.
1.3	February 1, 2022	- The version of the log4j component used by the Asigra software has been updated to the latest version to ensure our software is not flagged by any scanning tools. Requires Windows DS-Client v14.2.0.5, DS-NOC v14.2.0.4, and Management Console v14.2.0.5 or later. - When editing Microsoft 365 credentials in Management Console, updated credentials are now automatically applied to all Microsoft 365 backups that use the credentials. Requires Management Console v14.2.0.5 or later.
1.4	August 29, 2022	- Management Console users can now scan File System backups for potentially malicious or unauthorized content based on predefined policies. Requires Windows DS-License Server RLM v14.2.0.5, Windows DS-System v14.2.0.5, Windows DS-Client v14.2.0.6, and Management Console v14.2.0.6 or later. - Management Console users can now backup and restore Microsoft 365 SharePoint and OneDrive data using Modern authentication credentials. Requires Windows DS-Client v14.2.0.6 and Management Console v14.2.0.6 or later. - When configuring a Microsoft 365 backup, users can now perform folder-level backups of SharePoint and OneDrive Document libraries. Requires Windows DS-Client v14.2.0.5, Windows DS-User v14.2.0.4 or Windows Management Console v14.2.0.6 or later. - Management Console administrators can now configure multifactor authentication (MFA) for a user so that the user requires approval to delete a backup. Requires Management Console v14.2.0.6 or later. - Management Console administrators can now configure multifactor authentication (MFA) for a user so that the user requires approval to perform an on-demand backup. Requires Management Console v14.2.0.6 or later. - Management Console administrators can now configure multifactor authentication (MFA) for a user so that the user requires approval to perform an on-demand restore. Requires Management Console v14.2.0.6 or later.

1.4	August 29, 2022	• Management Console administrators can now configure multifactor authentication (MFA) for a user so that the user requires approval to reassign, edit, or delete a schedule for an existing backup. Requires Management Console v14.2.0.6 or later. • Management Console now integrates with the latest version (v5.0.8) of Secret Double Octopus (SDO) to support the multifactor authentication (MFA) feature. Requires Management Console v14.2.0.6 or later. • When performing backup, restore, or delete operations, Management Console users can now view the contents of folders that contain more than 10,000 items with improved performance. Requires Management Console v14.2.0.6 or later. • Management Console users can now enable or disable the Volume Shadow Copy Service (VSS) option for File system and Permissions backups. The option is enabled by default. Requires Management Console v14.2.0.6 or later. • When configuring Microsoft 365 credentials, Management Console users can now register a single or multitenant application when using Modern authentication (Manual) credentials. Requires Management Console v14.2.0.6 or later. • When configuring a VMware vCenter Server backup, users can now configure the days of the week on which they want to validate the disk signature of a protected virtual machine. Requires DS-User v14.2.0.5 or Management Console v14.2.0.6 and Windows DS-Client v14.2.0.5 or Linux DS-Client v14.2.0.4 or later.
1.5	September 26, 2022	• Management Console users can now migrate their Microsoft 365 Basic authentication credentials to Modern authentication (Automatic or Manual) credentials and update the associated backups to use the migrated Modern authentication credentials. Requires Management Console v14.2.0.7 or later.
1.6	April 10, 2023	• Management Console Global Administrators can now configure Multifactor Authentication (MFA) for users so they must authenticate using a six-digit Time-based one-time password (TOTP) application, such as Google or Microsoft Authenticator when signing in or attempting to perform a potentially destructive action that can result in the loss of data. Requires Management Console 14.2.0.8 or later. • Management Console Global Administrators can now configure Multiperson Approval (MPA) for accounts so users require multiple people to approve a potentially destructive action that can result in the loss of data. Administrators can set a threshold to specify how many approvals are required. Requires Management Console 14.2.0.8, Windows DS-Client 14.2.0.8 or Linux or Mac DS Client 14.2.0.6, DS-System 14.2.0.6, and DS-Operator 14.2.0.6 or later. • Management Console users can now scan their File System backups for malware during the backup and restore process when connected to a Linux or Mac DS-Client. Requires Management Console 14.2.0.8 and Linux or Mac DS-Client 14.2.0.6 or later. • When scanning File System backups for malware during the restore process, Management Console users can now either quarantine the infected files in a password-protected zip file or attempt to clean the infected files and restore them when the remediation is successful. Requires Management Console 14.2.0.8 and Windows DS-Client 14.2.0.8 or Linux or Mac DS-Client 14.2.0.6 or later.

1.6	April 10, 2023	• Management Console users can now select which Microsoft 365 services and DS-Clients use the autodiscover feature to automatically create backups for items added to the Microsoft 365 domain. Users can also automatically suspend backups associated with Microsoft 365 accounts that have been removed from the domain as part of the autodiscover process. Requires Management Console 14.2.0.8 or later. • When restoring Microsoft 365 (Exchange Online) data, Management Console users can now search for specific emails, contacts, calendars, tasks, and/or posts. Requires Management Console 14.2.0.8 or later. • Management Console users can no longer delete Microsoft 365 credentials if there are existing backups using those credentials. Users must first assign new Microsoft 365 credentials to the affected backups sets. Requires Management Console v14.2.0.8 or later. • Management Console users can now view the platform (Windows, Linux, Mac) of each DS-Client, view the IP address or host name of each backup source machine, and search for a specific DS-Client based on the DS-Client number when viewing the list of backups on the Backup Sets tab of the Data Management page. Requires Management Console 14.2.0.8 or later. • Management Console users can now search the Activity Log based on the backup name. Requires Management Console 14.2.0.8 or later. • When creating a VMware Cloud Director backup, if a user with administrator privileges configures the credentials for the Cloud Director server, a regular user can now create the backup using the organization credentials. Requires Management Console 14.2.0.8 or later. • Updated third-party components used by the Management Console to address potential security vulnerabilities. Requires Management Console 14.2.0.8 or later.

1 Getting started

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, backups, schedules, retention rules, and more.

NOTE: Before using Management Console, ensure all required DS-Systems and DS-Clients have been installed and you have the latest version of Java.

The Management Console API is based on the RESTful framework, which allows developers to use their preferred programming languages and tools to integrate with Management Console.

NOTE: To access the Management Console API documentation, add ***/docs*** to the end of your Management Console URL.

1.1 Signing into Management Console

You can sign into Management Console.

- The default IP address is **127.0.0.1** and the default port is **9595**.
- The default user name and password is **admin**.
- You must change your user name and password the first time you sign in.

NOTE: If MFA has been enabled for **Sign in**, you must enter an authentication code to sign into Management Console.

To sign into Management Console:

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

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

4. Click **Sign In**.
5. If MFA has been enabled for sign in, enter the six-digit authentication code you received, and then click **Continue**.

1.2 Performing the initial configuration

The first time you sign into Management Console you are required to perform the initial configuration, including configuring the security policy, changing your password, configuring a DS-System and DS-Client connection, configuring users and permissions, and configuring email notification settings.

To perform the initial configuration:

1. On the **Overview** page, click **Next**.
2. On the **Security Policy** page, do the following:
   a) Under **Password policy**, configure the password policy you want to enforce for users.

   b) Under **Sign in attempts**, configure the number of failed sign in attempts that are allowed before users are locked out of the system and the duration users are locked out.

   c) Under **Session timeout**, configure the period of inactivity after which users are signed out.

   d) Under **Data deletion**, configure whether users are required to enter their password to perform an operation that can result in the loss of data.

   e) Click **Next**.

   NOTE: To configure the security settings after the initial configuration, see Section 2.8.1, “Configuring the security settings”, on page 48.

3. In the **Change Password** dialog box, type your current and new password, and then click **Save**.

   NOTE: To change your password after the initial configuration, see Section 1.4, “Changing your password”, on page 18.

4. On the **Connections** page, click **[+]** to add a DS-System connection, and then do the following:
   a) On the **DS-System Connection** page, do the following:
      1. In the **Name** box, type the name of the DS-System.
      2. In the **User name** box, type the name of the user who will sign in to the DS-System.
      3. In the **Password** box, type the password of the user who will sign in to the DS-System.
      4. In the **Domain/computer name** box, type the domain or computer name to which the DS-System belongs.

   5. In the **Server address** box, type the IP address of the server where the DS-System is installed, and then click **[+]**.
   6. In the **Port** box, enter the port number that will be used by the DS-System.
   7. Click **Next**.

b) On the **License Server** page, to add a production DS-License Server, under **Production License Server**, do the following:

   1. In the **DS-License Server** box, type the IP address or host name of the production DS-License Server.
   2. In the **TCP port** box, enter the communication port number of the production DS-License Server. Do not change the port unless you have a specific requirement.
   3. In the **Verification interval** box, enter the time interval at which the production DS-License Server will verify the validity of the license.

c) On the **License Server** page, to add an emergency DS-License Server, under **Emergency License Server**, do the following:

   1. In the **DS-License Server** box, type the IP address or host name of the emergency DS-License Server.
   2. In the **TCP port** box, enter the communication port number of the emergency DS-License Server. Do not change the port unless you have a specific requirement.
   3. In the **Failover interval** box, enter the time interval after which the emergency DS-License Server should provide failover license authentication for the DS-System if the connectivity to the production DS-License Server is lost.
   4. Click **Next**.

d) On the **DS-System Replication** page, do the following:

   1. To enable DS-System replication, select the **Enable DS-System replication** check box.
   2. In the **Group port number** box, enter the group communication port number required to communicate with the replication group.
   3. In the **Group passcode** box, enter the group passcode. All DS-Systems in the same replication group must have the same passcode.
   4. To enable encryption of the replication group, select the **Enable group encryption** check box.
   5. To enable a bandwidth throttle, select the **Enable bandwidth throttle** check box. In the **Bandwidth limit per system** box, enter the bandwidth limit for each DS-System.

6. Click **Finish**. To view existing DS-System connections, click 👁.

> ***NOTE:*** To add a DS-System connection after the initial configuration, see Section 2.1.1, “Configuring a DS-System connection”, on page 21.

5. On the **Connections** page, click **[+]** to add a DS-Client connection, and then do the following:

   a) On the **DS-Client Connection** page, do the following:

      1. To add a single DS-Client, click **Add single DS-Client**.
      2. In the **Name** box, type a name for the DS-Client connection.
      3. In the **User name** box, type the name of the user who will sign in to the DS-Client.
      4. In the **Password** box, type the password of the user who will sign in to the DS-Client.
      5. In the **Domain/computer name** box, type the domain or computer name to which the DS-Client belongs.
      6. In the **Server address** box, type the IP address of the server where the DS-Client is installed, and then click [+].
      7. In the **Port** box, enter the port number that will be used by the DS-Client to communicate with the DS-System.
      8. Click **Next**.

      > ***NOTE:*** To add multiple DS-Clients, click **Add multiple DS-Clients**, and then click **Browse**. Select the csv file containing the list of DS-Client you want to add, and then click Finish.

   b) On the **DS-Client Registration** page, do the following:

      1. In the **Customer name** box, type the customer name associated with the DS-Client.
      2. In the **Account** box, type the account number associated with the DS-Client.
      3. In the **DS-Client** box, type the DS-Client number associated with the DS-Client.
      4. In the **Server address** box, type the IP address of the DS-System associated with this DS-Client connection, and then click [+].
      5. Click **Next**.

   c) On the **Encryption Keys** page, do the following:

1. Under **Private key**, select a type of encryption algorithm, and then type the encryption key and confirm it.
2. Under **Account key**, select a type of encryption algorithm, and then type the encryption key 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”.

3. To register the DS-Client with the DS-System, select the **Register with DS-System** check box.
4. To allow the DS-Client to send the encryption keys to the DS-System, select the **Forward encryption keys to DS-System** check box.

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

5. Click **Next**.

d) On the **User information** page, do the following:

1. In the **Country** box, select the name of the country where the user is located.
2. In the **Number of employees** box, select the number of employees in the organization.
3. In the **Industry** box, select the industry vertical to which the organization belongs.
4. Click **Finish**. To view existing DS-Client connections, click 👁.

NOTE: To add a DS-Client connection after the initial configuration, see and Section 2.2.1, “Configuring a DS-Client connection”, on page 25.

6. On the **Users & Permissions** page, do the following:

a) To create a user and assign them permissions, click **[+]**.

b) In the **User name** box, type the name of the user.

c) In the **Email address** box, type the email address of the user.

d) In the **Password** box, type the password the user will use to sign into Management Console.

e) In the **Confirm password** box, retype the password.

f) Under **Role**, select the role of the user.

g) Click **Next**.

IMPORTANT: Multifactor authentication (MFA) can be enabled for a user so they must authenticate when they sign in or perform a potentially destructive action that can result in the loss of data. However, this option is disabled by default and cannot be enabled during the initial configuration. This option can only be enabled by a Global Administrator configured with MFA. For more information, see Section 2.3.1, “Configuring a user”, on page 33.

h) Click **Next**.

NOTE: To configure users and permissions after the initial configuration, see Section 2.3, “Managing users and permissions”, on page 31.

7. On the **Email Settings** page, do the following:

a) In the **Protocol** box, select the protocol (SSL, TLS or None) you want to use for establishing encrypted communication between the email server and email client.

b) In the **SMTP host or IP address** box, type the host name or IP address of the email server you want to use for sending email notifications.

c) In the **SMTP port** box, enter the port number you want to use for sending email notifications.

d) In the **Sender’s email address** box, type the email address from which the notification will be sent.

e) To enable a SMTP client to log in using an authentication mechanism supported by the SMTP server, select the **Enable SMTP authentication** check box, and then type the user name and password.

f) To send a test email notification, click **Test**.

g) Click **Finish**.

NOTE: To configure email notification settings after the initial configuration, see Section 2.8.2, “Configuring the email notification settings”, on page 49.

1.3 Viewing the Management Console dashboard

The Management Console includes an interactive dashboard that provides a real-time view of your environment.

To view the Management Console dashboard, click **Dashboard**. The following information is displayed:

- **Component Summary** – Displays the total number of DS-Systems, Accounts, and DS-Clients. If a DS-System or DS-Client has stopped working, it is displayed in a different color.

  NOTE: To view the list of DS-System and DS-Client connections or accounts, click the associated graphic.

- **Activity Summary** – Displays the total number of activities across all accounts on a daily basis. Different colors represent successful activities, activities with warnings, and activities with errors. To view the number of activities in each category, hover the mouse over the corresponding color.

  NOTE: To view detailed information about the activities in the Activity Log, click the associated graphic.

- **Error Summary** – Displays a summary of any errors that have occurred in various areas of the application.
- **Successful** – Displays the most recent activities that were successfully completed. To view all successful activities in the Activity Log, click **See All**.
- **Warnings** – Displays the most recent activities with warnings. To view all the activities with warnings in the Activity Log, click **See All**.
- **Errors** – Displays the most recent activities with errors. To view all the activities with errors in the Activity Log, click **See All**.

1.4 Changing your password

An administrator will provide you with a user name and password for signing into Management Console. When you sign in for the first time, you will be prompted to change your password.

NOTE: Your password must adhere to the password policy defined by the administrator. For more information, see Section 2.8.1, “Configuring the security settings”, on page 48.

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 **Save**.

1.5 Installing a Management Console update

When a Management Console update is available, the 🔔 **Notifications** icon will flash.

To install a Management Console update:

1. On the toolbar, click **Notifications**.
2. To send a notification to all Management Console users that you will be updating the system, click ❗ **Notify Users**. On the **Notifications** page, enter the required details, and then click **Send**.

   NOTE: For more information, see Section 2.8.3, “Configuring the broadcast notification settings”, on page 50.

3. To install the Management Console update, click ⬇ **Updates**.
4. In the **Management Console Updates** window, under **Package Name**, select the package you want to install, and then click **Install**.

   IMPORTANT: After the update has been installed, you must restart your web browser for the update to take effect.

1.6 Rebranding Management Console

You can apply your own company branding to Management Console.

To rebrand Management Console:

1. On the machine where you installed the Management Console software, navigate to the following folder:

   ```
   \Program Files\CloudBackup\Management Console\Branding
   ```

2. Replace the *amc_logo.svg file* with your company logo. The logo must have the same file name and file format.
3. Replace the *favicon.ico* file with your company icon. The icon file must be 16 x 16 pixels and have the same file name and file format.

1.7 Translating Management Console

You can use the Management Console Translation Utility to translate the Management Console interface.

To translate Management Console:

1. Go to https://cloud.google.com and follow the instructions on how 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 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 JSON file 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 you created.

NOTE: For detailed instructions on how to create a Google Cloud Platform, see the *Google* documentation.

1.8 Signing out of Management Console

You can sign out of Management Console at any time.

To sign out of Management Console:

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

2 Configuring the system settings

You can configure DS-Systems, DS-Clients, users and permissions, credentials, and Management Console settings.

2.1 Managing 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.

2.1.1 Configuring a DS-System connection

Before you can configure accounts and DS-Clients, you must first connect to a DS-System. The DS-System must be able to connect to the DS-License Server at all times to validate and receive its capacity license allocation.

To configure a DS-System connection:

1. On the toolbar, click **Settings**.
2. Click the **Connections** tab.
3. Under **DS-Systems Connections**, do one of the following:
   - To add a DS-system connection, click **[+] Add Connection**.
   - To edit a DS-System connection, select the DS-system, and then click ✎ **Edit Connection**.
4. On the **DS-System Connection** page, do the following:

   a) In the **Name** box, type the name of the DS-System.

   b) In the **User name**, type the name of the user who will sign in to the DS-System.

   c) In the **Password** box, type the password of the user who will sign into the DS-System.

   d) In the **Domain/computer name** box, type the domain or computer name to which the DS-System belongs.

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

   f) In the **Port** box, enter the port number that will be used by the DS-System.

   g) Click **Next**.

5. On the **License Server** page, do the following:
   - To add a production DS-License Server, under **Production License Server**, do the following:
     a) In the **DS-License Server** box, type the IP address or host name of the production DS-License Server.

     b) In the **TCP port** box, enter the communication port number of the production DS-License Server. Do not change the port unless you have a specific requirement to do so.

     c) In the **Verification interval** box, enter the time interval at which the production DS-License Server will validate the license.
   - To add an emergency DS-License Server, under **Emergency License Server**, do the following:
     a) In the **DS-License Server** box, type the IP address or host name of the emergency DS-License Server.

     b) In the **TCP port** box, enter the communication port number of the emergency DS-License Server. Do not change the port unless you have a specific requirement to do so.

     c) In the **Failover interval** box, enter the time interval after which the emergency DS-License Server should provide failover license authentication for the DS-System if the connectivity to the production DS-License Server is lost.

     d) Click **Next**.
6. On the **DS-System replication** page, do the following:

   a) To enable DS-System replication, select the **Enable DS-System replication** check box.

   b) In the **Group port number** box, enter the group communication port number required to communicate with the replication group.

   c) In the **Group passcode** box, enter the group passcode. All DS-Systems in the same replication group must have the same passcode.

   d) To enable encryption of the replication group, select the **Enable group encryption** check box.

   e) To enable a bandwidth throttle, select the **Enable bandwidth throttle** check box. In the **Bandwidth limit per system** box, enter the bandwidth limit for each DS-System.
7. Click **Finish**.

2.1.2 Configuring a DS-System replication group

If you enabled DS-System replication when configuring a DS-System connection, you can set up multiple DS-Systems to be a part of a replication group. For more information, see Section 2.1.1, “Configuring a DS-System connection”, on page 21.

To configure a DS-System replication group:

1. On the toolbar, click **Settings**.
2. Click the **Connections** tab.
3. Under **DS-Systems Connections**, click **Create Replication Group**.
4. Under **DS-Systems**, use the icon to drag and drop the DS-Systems to create a DS-System replication group.
5. Click **Create**.

2.1.3 Configuring the DS-System trash settings

You can use the DS-System trash feature to recover data from the trash folder after it has been deleted from the DS-System online storage.

NOTE: If MFA has been enabled for **Configure DS-System trash**, you must enter an authentication code to perform the task.

You can provide an extra layer of security by enabling multiperson approval (MPA) so multiple people must approve when a user enables or disables the DS-System trash setting or configures the number of days deleted data remains in the trash folder before it is permanently deleted.

IMPORTANT: Only a Global Administrator can enable or disable MPA. If MPA is enabled, the Global Administrator must get approval if they attempt to disable MPA or lower the approval threshold.

To configure the DS-System trash settings:

1. On the toolbar, click **Settings**.
2. Click the **Connections** tab.
3. Under **DS-Systems Connections**, select the DS-System for which you want to configure the trash settings, and then click **Advanced Configuration**.
4. To configure multiperson approval (MPA), do the following:
    a) Slide the **Multiperson approval (MPA)** switch to **Enabled**.
    b) Under **Approval threshold**, configure the threshold to determine how many approvals are required to configure the DS-System trash setting.

c) Under **Approvers**, select the approvers from the list of users. The number of approvers is determined by the configured approval threshold.

NOTE: The approval threshold must be met with no denials to be approved.

5. To configure the DS-System trash settings, do the following:

   a) Slide the **DS-System trash** switch to **Enabled**.

   b) Configure the number of days and time after which data in the trash folder is permanently deleted from the DS-System online storage.

6. Click **Next**.

7. Review the DS-System trash settings, click **Save**, and then do one of the following:

   - To confirm you want to configure the DS-System trash settings, click **Continue**.
   - If you are required to enter a password to configure the DS-System trash settings, type your Management Console password, and then click **Continue**.
   - If MFA has been enabled for **Configure DS-System trash**, enter the six-digit authentication code you received, and click **Continue**.
   - If MPA has been enabled for **Configure DS-System trash**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.
   - If MFA and MPA have been enabled for **Configure DS-System trash**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

2.1.4 Deleting a DS-System connection

You can delete a DS-System connection when required.

To delete a DS-System connection:

1. On the toolbar, click **Settings**.
2. Click the **Connections** tab.
3. Under **DS-System connections**, select the DS-System you want to delete, and then click 🗑 **Delete connection**.
4. When the system prompts you to delete the DS-System connection, click **Yes**.

2.2 Managing DS-Clients

The DS-Client is responsible for defining the backups that determine what data is to be backed up from the source computers and for sending the backed up data to the DS-System for storage.

During the backup process, the DS-Client extracts, compresses, and encrypts the data. Only new or modified data is backed up, which accelerates the backup transmission time. Backup data is sent to a secure off-site data center that hosts the DS-System. A restore can be performed on demand via the same DS-Client.

Ease of use comes from the agentless architecture, which allows you to install a DS-Client on only one LAN computer. As long as the DS-Client is on the same network as the source computers, you can back up and restore data as required.

2.2.1 Configuring a DS-Client connection

You must configure a DS-Client and register it with the DS-System so you can send backup data from the DS-Client to the DS-System.

To configure a DS-Client connection:

1. On the **Toolbar**, click **Settings**.
2. Click the **Connections** tab.
3. Under **DS-Client Connections**, do one of the following:
    - To add a DS-Client connection click **[+] Add Connection**.
    - To edit a DS-Client connection, select the DS-Client, and then click ✎ **Edit Connection**. You cannot select the option to add a single DS-Client or multiple DS-Clients.
4. On the **DS-Client Connection** page, do one of the following:
    - To add a single DS-Client, click **Add single DS-Client**, and then do the following:
        a) In the **Name** box, type the name of the DS-Client.
        b) In the **User name** box, type the name of the user who will sign in to the DS-Client.
        c) In the **Password** box, type the password of the user who will sign in to the DS-Client.
        d) In the **Domain/computer name** box, type the domain or computer name to which the DS-Client belongs.
        e) In the **Server address** box, type the IP address of the server where the DS-Client is installed, and then click **[+]**.
        f) In the **Port** box, enter the port number that will be used by the DS-Client to communicate with the DS-System.

g) Click **Nex**t.

- To add multiple DS-Clients, click **Add multiple DS-Clients**, and then click **Browse**. Select the csv file containing the list of DS-Client you want to add, and then click **Finish**.

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

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

   b) In the **Account** box, type the account ID associated with the DS-Client.

   c) In the **DS-Client** box, type the DS-Client number associated with the DS-Client.

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

   e) Click **Next**.

6. On the **Encryption Keys** page, do the following:

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

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

   c) To register the DS-Client with the DS-System, select the **Register with DS-System** check box.

   d) To allow the DS-Client to send the encryption keys to the DS-System, select the **Forward encryption keys to DS-System** check box.

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

   e) Click **Next**.

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

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

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

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

8. Click **Finish**.

2.2.2 Configuring the antimalware and CDR settings

You can configure the antimalware and CDR settings for a DS-Client to scan your data for malware or unauthorized content during the backup and restore process.

Antimalware

The antimalware feature allows you to scan backups for malware during the backup and restore process. A trial version is available for unlicensed DS-Clients that includes 5 free malware detections.

NOTE: The antimalware feature is supported for File system backups when connected to a Windows, Linux, or Mac DS-Client and for Microsoft 365 backups when connected to a Windows DS-Client.

During the backup process, files detected with malware are backed up to the DS-System in encrypted format and a warning message appears in the Event Log.

During the restore process, the process differs depending on the type of backup:

- For File System backups, you have the option to quarantine infected files in a password protected zip file in the quarantine folder or attempt to clean the infected files and restore them if the remediation is successful.
- For Microsoft 365 backups, files detected with malware are not restored. A warning message appears in the Event Log and a copy of the infected files is placed in a password protected zip file in the quarantine folder.

You can generate an Antimalware Scan Report to view the results of the scan, including the number of files scanned, the number of files that failed to scan, and the number of files detected with malware. For more information, see Section 8.1.3, “Generating an Antimalware Scan Report”, on page 138.

IMPORTANT: DS-Clients that are licensed for antimalware must be able to resolve and access cyber.asigra.com to update the antimalware definitions.

Content Disarm & Reconstruction (CDR)

The Content Disarm & Reconstruction (CDR) feature allows you to scan backups for potentially malicious or unauthorized content during the backup and restore process and take remediation actions based on predefined policies.

NOTE: The CDR feature is supported only for File system backups when connected to a Windows DS-Client.

During the backup process, files detected with unauthorized content are backed up to the DS-System in encrypted format and a warning message appears in the Event Log indicating if any files were non-compliant based on the selected policy.

During the restore process, files detected with unauthorized content are filtered, removed, or blocked based on the selected policy. A warning message appears in the Event Log and a copy of the infected files are placed in a password protected zip file in the quarantine folder.

The CDR feature supports the following file types and extensions.

File Type	File Extension	File Size Limitation
Adobe Acrobat	pdf	2 GB
Archives	zip, rar, 7z, cab, wim, swm, tar, gz, tgz, bz2, tbz, xz, txz, emz, kmz, war, jar	150 GB
Certificate revocation list	crl	2 GB
Email messages	msg, eml, tnef, ics, mht, mhtml	2 GB
Executables	exe	2 GB
Extensible Markup	xml, svg, rels, kml	2 GB
Hypertext Markup	html, htm, hta	2 GB
Images	png, bmp, jpeg, jpg, jfif, tif, tiff, gif, wdp, wmf, emf	2 GB
Microsoft Word	doc, docm, doc, rtf, dotx, dotm, dot	2 GB
Microsoft Excel	xlsx, xlsm, xltx, xls, xlt, xlk, xlsb	2 GB
Microsoft PowerPoint	pptx, pptm, ppt, ppsx, ppsm, pps	2 GB
Microsoft Visio	vsdx, vsdm, vssx, vssm, vstx, vstm	2 GB
Multimedia	wav, wma, mp2, mp3, aac, m4a, wmv, mp4, 3gp, amr, mov	50 GB
Scripts	js, vbs, bas, cls	2 GB
Shortcuts	lnk, url	2 GB
Text	txt, csv, lst	2 GB

Table 1 CDR Supported File Types

You can generate a CDR Scan Report to view the results of the scan, including the number of files scanned, the number of files that failed to scan, and the number of files filtered, blocked, or removed. For more information, see Section 8.1.4, “Generating a CDR Scan Report”, on page 139.

To configure the antimalware and CDR settings:

1. On the toolbar, click **Settings**.
2. Click the **Connections** tab.
3. Under **DS-Client Connections**, select the DS-Client for which you want to configure the antimalware and CDR settings, and then click ⚙ **Advanced Configuration**.
4. In the **Configuration settings** box, select **Antimalware/CDR settings**.
5. In the **Server address** box, type the IP address of the computer on which you want to create the quarantine folder.
6. In the **User name** box, type the name of the user who will sign in to the computer where you are creating the quarantine folder.
7. In the **Password** box, type the password of the user who will sign in to the computer where you are creating the quarantine folder.
8. In the **Domain** box, type the domain name of the computer where you are creating the quarantine folder.
9. In the **Quarantine folder** box, specify the location of the quarantine folder. The default location is *C:\Program Files\CloudBackup\DS-Client\Quarantine*.

   NOTE: To configure the quarantine folder on a remote machine when connected to a Linux or Mac DS-Client, you must install a Samba client on the DS-Client machine, install a Samba server on the remote machine, and then configure a Samba share on the remote machine. The parameters required are the remote machine IP address, Samba credentials, and the share folder.

   NOTE: We recommend you specify a location with enough disk space to accommodate the quarantined files. The password for the zip file is “infected”.

10. In the **CDR buffer location** box, specify the location of the CDR buffer where files are scanned by the CDR engine during the backup and restore process. The default location is *C:\Program Files\CloudBackup\DS-Client\CDRBuffer*.

    NOTE: We recommend you specify a location that has enough disk space to accommodate the data. We recommend a 300 GB SSD or NVMe drive.

11. Click **Save**.

2.2.3 Configuring the proxy server settings

You can configure the proxy server settings used by the DS-Client.

To configure the proxy server settings:

1. On the toolbar, click **Settings**.
2. Click the **Connections** tab.
3. Under **DS-Client Connections**, select the DS-Client for which you want configure the proxy server settings, and then click ⚙ **Advanced Configuration**.
4. Under **Configuration settings**, select **Proxy server settings**.
5. In the **DS-Client** box, select the DS-Client whose proxy server settings you want to configure.
6. Under **Proxy server setting**, select one of the following options:
   - No proxy
   - Configure automatically
   - Configure manually
7. If you selected **Configure manually**, type the proxy address and port for the HTTP, HTTPS, and IMAP proxy servers.
8. To use the proxy server settings for all protocols, select the **Use the same proxy server for all protocols** check box.
9. Click **Save**.

2.2.4 Deleting a DS-Client connection

You can delete a DS-Client connection when required.

To delete a DS-Client connection:

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

2.3 Managing users and permissions

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

There are four types of Management Console user roles:

- **Global Administrator** – Can configure and manage a Global Administrator, Custom Administrator, or Regular User on the DS-System and DS-Client. Can share the cloud credentials of any user.
- **Custom Administrator (Service Provider)** – Can configure and manage a Regular User and provide them access to the DS-System functionality. Can assign the following permissions: Administrator, None.
- **Custom Administrator (End User)** – Can configure and manage a Regular User and provide them access to the DS-Client functionality. Can assign the following permissions: Administrator, Operator, Viewer, None.
- **Regular User** – Can access the DS-System or DS-Client functionality depending on who created them and what permissions they were assigned.

NOTE: A regular user created by a custom administrator (Service Provider) can access only DS-Systems. A regular user created by a custom administrator (End User) can access only DS-Clients.

The following table shows the permissions of each user role:

Role	Global Admin	Custom Admin (SP)	Custom Admin (EU)	Regular User (DS-System)		Regular User (DS-Client)		
Permission	**Admin**	**Admin**	**Admin**	**Admin**	**View**	**Admin**	**Operator**	**View**
Data Management								
Backup sets	Full		Full			Full	Limited	View
VM Replication Sets	Full		Full			Full	Limited	View
Schedules	Full		Full			Full	Limited	View
Retention Rules	Full		Full			Full	Limited	View
Account Management								
Accounts	Full	Full		Full	View			
VM Replication Groups	Full	Full		Full	View			
Monitoring								
Backup Sets Storage Report	Full	Full		Full	Full			
Antimalware Scan Report	Full		Full			Full	Full	Full
CDR Scan Report	Full		Full			Full	Full	Full
Cloud Backup Status Report	Full		Full			Full	Full	Full
GDPR Compliance Report	Full	Full		Full	Full			
Grid Status	Full		Full			Full	Full	Full
Logs	Full	Full	Full	Full	Full	Full	Full	Full
Usage Metrics	Full	Full		Full	Full			
Settings								
DS-Client Connections	Full		Full					
DS-System Connections	Full	Full						
Users & Permissions	Full	Full	Full					
Credentials Management	Full		Full			Full	Full	View
Management Console	Full							
Notifications								
Notify Users	Full							
Updates	Full	Full	Full	Full	Full	Full	Full	Full

Table 2 Users and Permissions

- SP = Service Provider
- EU = End User
- Blank = Feature not available.
- Full = Permission to create, edit, view, or delete.
- Limited = Permission to perform a backup or restore, and activate, suspend, or synchronize a backup. Permission to initiate a failover or failback of a replication set. Permission to reassign a schedule or a retention rule.
- View = Permission to view only.

2.3.1 Configuring a user

When configuring a user, you can provide an extra layer of security by configuring multifactor authentication (MFA) so the user must authenticate when they sign in or perform a potentially destructive action that can result in the loss of data.

If MFA is enabled, the user will receive an email with a QR code they must scan using a six-digit time-based one-time password (TOTP) application, such as Google or Microsoft Authenticator.

When the user attempts to perform a task that requires MFA, they will be prompted to enter a randomly generated six-digit authentication code to complete the task.

IMPORTANT: Only a Global Administrator with MFA can enable or disable MFA. If MFA is enabled, the Global Administrator must enter an authentication code if they attempt to disable MFA or disable a previously enabled MFA task.

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: When editing a user, you cannot change the user name or password.

4. In the **User name** box, type the name of the user.
5. In the **Email address** box, type the email address of the user.
6. In the **Password** box, type a password for the user.
7. In the **Confirm password** box, retype the password.
8. Under **Role**, select the role of the user. For more information, see Section 2.3, “Managing users and permissions”, on page 31.
9. Click **Next**.
10. To configure multifactor authentication (MFA) for the user, do the following:
    a) Slide the **Multifactor authentication** switch to **Enabled**.
    b) Configure the following MFA tasks as required:
       - **Sign in** – User must enter an authentication code when signing in.
       - **Edit backup** – User must enter an authentication code when editing a backup or reassigning a schedule or retention rule.

- **On-demand backup** – User must enter an authentication code when performing an on-demand backup.
- **Delete backup** – User must enter an authentication code when deleting a backup.
- **Selective delete** – User must enter an authentication code when deleting data from a backup.
- **On-demand restore** – User must enter an authentication code when performing an on-demand restore.
- **Configure schedule** – User must enter an authentication code when editing or deleting a schedule.
- **Configure retention rule** – User must enter an authentication code when editing or deleting a retention rule.
- **Configure DS-System trash** – User must enter an authentication code when configuring the DS-System trash setting.

NOTE: The list of tasks differs depending on the role of the user.

c) Click **Next**.

11. Review the settings for the user, and then click **Create** or **Save**.

2.3.2 Assigning permissions to a user

After you configure a user, you must assign permissions to the user to enable them to access the DS-System or DS-Client. For more information on user roles and permissions, see Section 2.3, “Managing users and permissions”, on page 31

To assign permissions to a user:

1. On the toolbar, click **Settings**.
2. Click the **Users & Permissions** tab.
3. Under **Users & Permissions**, select the user to which you want to assign permissions.
4. Expand the DS-System and DS-Client and assign the level of permission you want to assign to the user.
5. To save the permission, click 💾.

2.3.3 Deleting a user

When a user is deleted, the ownership of their credentials is transferred to the user who created them.

To delete a user:

1. On the **Toolbar**, click **settings**.
2. Click the **Users & Permissions** tab.
3. Under **Users & Permissions**, select the user you want to delete, and then click **Delete User**.
4. When the system prompts you to confirm you want to delete the credentials, click **Yes**.

2.4 Managing account credentials

Account credentials allow you to have easy access to your credentials. Once the account credentials are created, you can simply select the credentials rather than having to enter them each time.

2.4.1 Configuring account credentials

You can configure and manage your account credentials in one location. When editing account credentials, consider the following:

- A Global Administrator can edit the credentials of any user.
- A Custom Administrator can edit only their own credentials or the credentials of a regular user they created.
- A Regular User can edit only their own credentials.

To configure account credentials:

1. On the toolbar, click **Settings**.
2. Click the **Credentials Management** tab.
3. Click the **Account Credentials** tab, and then do one of the following:
    - To add credentials, click **[+] Add Credentials**.
    - To edit credentials, select the credentials, and then click ✏ **Edit Credentials**.
4. In the **Add/Edit Account Credentials** dialog box, do the following:
    a) In the **User name** box, type the name of the user associated with the credentials.

    b) In the **Password** box, type the password of the user associated with the credentials.

    c) In the **Account credentials name** box, type a name for the credentials.

    d) In the **Description** box, type a description for the credentials.

e) Click **Add/Save**.

2.4.2 Searching for account credentials

If you have multiple account credentials, you can search for the credentials.

To search for account credentials:

1. On the toolbar, click **Settings**.
2. Click the **Credentials Management** tab.
3. Click the **Account Credentials** tab,
4. Click 🔍 **Search**.
5. Type the name of the credentials you want to find, and then press **Enter**.

2.4.3 Sharing account credentials

You can share account credentials with other users. When sharing credentials, consider the following:

- A Global Administrator can share the credentials of any user.
- A Custom Administrator can share only their own credentials or the credentials of a regular user they created.
- A Regular User cannot share their credentials with other users.

To share account credentials:

1. On the toolbar, click **Settings**.
2. Click the **Credentials Management** tab.
3. Click the **Account Credentials** tab.
4. Under **Account Credentials**, select the credentials you want to share, and then click **Share Credentials**.
5. Select the users you want to share the credentials with, and then click **Save**.

2.4.4 Deleting account credentials

When deleting credentials, consider the following:

- A Global Administrator can delete the credentials of any user.
- A Custom Administrator can delete only their own credentials or the credentials of a regular user they created.
- A Regular User can delete only their own credentials.

To delete account credentials:

1. On the toolbar, click **Settings**.
2. Click the **Credentials Management** tab.
3. Click the **Account Credentials** tab.
4. Select the credentials you want to delete, and then click **Delete Credentials**.
5. When the system prompts you to confirm you want to delete the credentials, click **Yes**.

2.5 Managing Microsoft 365 credentials

Microsoft 365 credentials provide you with a secure method to access Microsoft 365 services on a domain to perform backup and restore operations on your data.

The services you can backup or restore depend on your authentication credentials.

If you sign in using	You can back up or restore	You cannot back up or restore
Modern authentication (Automatic or Manual)	• Exchange Mailboxes • Archive Mailboxes • Public Folders • SharePoint Sites • OneDrive Accounts • Groups • Teams	• N/A
Basic authentication	• SharePoint Sites • OneDrive Accounts	• Exchange Mailboxes • Archive Mailboxes • Public Folders • Groups • Teams

Table 3 Microsoft 365 authentication methods

IMPORTANT: You can use Modern authentication credentials to back up Groups or Teams only if the credentials belong to a user who is an owner and member of the Group or Team.

2.5.1 Configuring Microsoft 365 credentials

You can configure the Microsoft 365 credentials required to access Microsoft 365 services hosted in the cloud on a specific domain. The credentials are added separately for each cloud service. When editing credentials, consider the following:

- A Global Administrator can edit the credentials of any user.
- A Custom Administrator can edit only their own credentials or the credentials of a regular user they created.
- A Regular User can edit only their own credentials.

To configure Microsoft 365 credentials:

1. On the toolbar, click **Settings**.
2. Click the **Credentials Management** tab.
3. Click the **Cloud Credentials** tab, and then do one of the following:
   - To add Microsoft 365 credentials, click **[+] Add Credentials**.
   - To edit a Microsoft 365 credentials, select the credentials, and then click ✏ **Edit Credentials**.
4. Select the authentication method you want to use. Your options are as follows:
   - **Modern Authentication** – Authenticates using the secure OAuth 2.0 authorization framework. You have two options: **Automatic** or **Manual**.
   - **Basic Authentication** – Authenticates using a user name and password.
5. If you selected **Modern Authentication (Automatic)**, click **Sign in**. On the **Microsoft Sign In** page, enter your credentials, and then click **Sign In**.
6. If you selected **Modern Authentication (Manual)**, click **Sign In**. In the **Modern Authentication (Manual)** dialog box, do the following:

   NOTE: This procedure must be performed using the Microsoft Azure Active Directory web application, which is subject to change without notice. For more information, see the Microsoft Azure documentation.

   a) Click **Copy** to copy the redirect URI to the clipboard.

   b) Sign in to the Microsoft Azure Active Directory.

   c) Register a new web application as follows:

      1. Under **Manage**, click **App registrations**.
      2. Click **New registration**.
      3. In the **Name** box, type a name for the application.

4. To register a single tenant app, under **Supported account types**, select **Accounts in this organizational directory only (<tenant> only - Single tenant)**.
5. To register a multitenant app, under **Supported account types**, select **Accounts in any organizational directory (Any Azure AD directory - Multitenant)**.
6. Under **Redirect URI**, select **Web**, and then paste the redirect URI from the clipboard into the provided field.
7. Click **Register**.

d) Copy the Application (client) ID to the clipboard and paste it in the **Client ID** box of the **Modern Authentication (Manual)** dialog box.

e) Configure the settings for the web application as follows:

1. On the **App registrations** page, select the app you created.
2. Under **Manage**, click **Certificates & secrets**.
3. Under **Client secrets**, click **New client secret**.
4. Create a client secret key for access to the API, and then click **Add**.
5. Copy the client secret value to the clipboard and paste it in the **Client secret** box of the **Modern Authentication (Manual)** dialog box.

f) Click **Sign In**.

NOTE: When using Modern authentication (Manual), if you don’t grant administrator privileges on behalf of the organization via the consent form, you can do so later by signing into the Microsoft Azure Active Directory Portal. For more information, see the *Microsoft Azure* documentation.

7. If you selected **Basic Authentication**, do the following:

a) In the **User name** box, type the name of the user with permission to access the supported Microsoft 365 services. The user name should be in the format username@domain.com.

b) In the **Password** box, type the password of the user with permission to access the supported Microsoft 365 services.

c) Click **Add** or **Save**.

2.5.2 Configuring the autodiscover settings

You can automatically discover and create backups for items that are added to the domain or suspend backups for items that are removed from the domain.

To configure the autodiscover settings:

1. On the toolbar, click **Settings**.
2. Click the **Credentials Management** tab.
3. Click the **Cloud Credentials** tab.
4. Select the domain for which you want to configure the autodiscover settings, and then click **Autodiscover Settings**.
5. Under **Domain association**, select the DS-System and account you want to associate with the domain.
6. To automatically create backups for items added to the domain, slide the **Autodiscover** switch to **Enabled**.
7. To automatically suspend backups for items removed from the domain, slide the **Autosuspend** switch to **Enabled**.

   NOTE: The autosuspend feature can only be enabled if the autodiscover feature is enabled.

8. Select which Microsoft 365 services you want to use the autodiscover feature.
9. To enable a scan of your files for malware during the backup process, enable **Antimalware**.
10. Select which DS-Clients you want to associate with each Microsoft 365 service when using the autodiscover feature.

    NOTE: Only DS-Clients associated with the selected DS-System and account will appear in the list.

11. Click **Save**.

2.5.3 Sharing Microsoft 365 credentials

You can share Microsoft 365 credentials with other users so they can create Microsoft 365 backups. When sharing credentials, consider the following:

- A Global Administrator can share the credentials of any user.
- A Custom Administrator can share only their own credentials or the credentials of a regular user they created.
- A Regular User cannot share their credentials with other users.

To share Microsoft 365 credentials:

1. On the toolbar, click **Settings**.
2. Click the **Credentials Management** tab, and then click **Cloud Credentials**.
3. Select the user whose credentials you want to share, and then click **Share Credentials**.
4. Select the users you want to share the credentials with, and then click **Save**.

2.5.4 Migrating Microsoft 365 credentials

IMPORTANT: Only a Global Administrator can migrate Microsoft 365 credentials.

You can migrate Microsoft 365 Basic authentication credentials to Modern authentication (Automatic or Manual) credentials and update the associated backups to use the migrated Modern authentication credentials.

NOTE: To migrate Basic authentication credentials to Modern authentication (Automatic or Manual) credentials, you must first create Modern authentication credentials with the same user name.

To migrate Microsoft 365 credentials:

1. On the toolbar, click **Settings**.
2. Click the **Credentials Management** tab.
3. Click the **Cloud Credentials** tab.
4. Select the user whose credentials you want to migrate, and then click **Migrate Credentials**.

   NOTE: You can only migrate the credentials of a user who is configured with Basic authentication.

5. In the **Migrate Credentials** dialog box, do the following:

   a) Under **Credentials**, do the following:

      1. In the **Domain** box, select the Microsoft 365 domain containing the credentials you want to migrate.
      2. In the **From credential type** box, select the type of credential you want to migrate. The only option is **Basic**.
      3. In the **User name** box, select the name of the user whose credentials you want to migrate.
      4. In the **To credential type** box, the credential is automatically selected as either **Modern (Automatic)** or **Modern (Manual)** if a Modern authentication credential with the same user name exists.

   NOTE: You can only migrate Basic authentication credentials to Modern authentication credentials with the same user name.

   b) Under **Backup sets**, do the following:

      1. In the **DS-System** box, select the DS-System.
      2. In the **Account** box, select the account.
      3. In the **DS-Client** box, select the DS-Client.
      4. In the **Services** box, select the services associated with the backups you want to update to use the migrated credentials.
      5. Select the backups sets you want to update to use the migrated credentials, and then click **Migrate**.
      6. When the system prompts you to confirm you want to migrate the credentials for the backups, click **Yes**.
      7. When the credential migration process has completed, review the summary, and then click **Close**.

2.5.5 Deleting Microsoft 365 credentials

You can delete Microsoft 365 credentials if required. When deleting credentials, consider the following:

- A Global Administrator can delete the credentials of any user.
- A Custom Administrator can delete only their own credentials or the credentials of a regular user they created.
- A Regular User can delete only their own credentials.

NOTE: You cannot delete Microsoft 365 credentials that are associated with a backup.

To delete Microsoft 365 credentials:

1. On the toolbar, click **Settings**.
2. Click the **Credentials Management** tab.
3. Click the **Cloud Credentials** tab.
4. Select the user whose credentials you want to delete, and then click 🗑 **Delete Credentials**.
5. When the system prompts you to confirm you want to delete the credentials, click **Yes**.

2.6 Managing VMware vCenter Server credentials

VMware vCenter Server provides a centralized platform and role-based access for controlling your VMware vSphere environments.

2.6.1 Configuring vCenter Server credentials

You can configure the VMware vCenter Server credentials used to access the VMware vCenter Server. When editing credentials, consider the following:

- A Global Administrator can edit the credentials of any user.
- A Custom Administrator can edit only their own credentials or the credentials of a regular user they created.
- A Regular User can edit only their own credentials.

To configure VMware vCenter Server credentials:

1. On the toolbar, click **Settings**.
2. Click the **Credentials Management** tab.
3. Click the **Virtualization Credentials** tab.
4. Select **VMware vCenter Server**, and then do one of the following:
    - To add VMware vCenter Server credentials, click **[+] Add VMware vCenter Server credentials**.
    - To edit VMware vCenter Server credentials, select the credentials, and then click ✏ **Edit VMware vCenter Server credentials**.
5. In the **Host or IP address** box, type the host name or IP address of the VMware vCenter Server.
6. In the **Account credentials** box, select the account credentials for the VMware vCenter Server.

    NOTE: To add or edit account credentials, click **[+]** or ✏.

7. In the **VMware vCenter Server credentials name** box, type a name for the credentials.
8. Click **Add/Save**.
9. To update the list of credentials, click **Refresh**.

NOTE: To enable or disable the VMware vCenter Server credentials, slide the Credentials Status toggle switch to Enabled or Disabled.

2.6.2 Searching for vCenter Server credentials

If you have multiple VMware vCenter Server credentials, you can search for the credentials.

To search for VMware vCenter Server credentials:

1. On the toolbar, click **Settings**.
2. Click the **Credentials Management** tab.
3. Click the **Virtualization Credentials** tab.
4. Select **VMware vCenter Server**, and then click **Search**.
5. Type the name of the VMware vCenter Server credentials you want to find, and then press **Enter**.

2.6.3 Sharing vCenter Server credentials

You can share VMware vCenter Server credentials with other users. When sharing credentials, consider the following:

- A Global Administrator can share the credentials of any user.
- A Custom Administrator can share only their own credentials or the credentials of a regular user they created.
- A Regular User cannot share their credentials with other users.

To share VMware vCenter Server credentials:

1. On the toolbar, click **Settings**.
2. Click the **Credentials Management** tab
3. Click the **Virtualization Credentials** tab.
4. Select **VMware vCenter Server**.
5. Select the credentials you want to share, and then click **Share Credentials**.
6. Select the users you want to share the credentials with, and then click **Save**.

2.7 Managing VMware Cloud Director Server credentials

VMware Cloud Director provides role-based access to a Web console where users in an organization can create and use virtual machines and vApps.

2.7.1 Configuring Cloud Director Server credentials

You can configure the VMware Cloud Director Server credentials used to access the VMware Cloud Director Server.

When editing credentials, consider the following:

- A Global Administrator can edit the credentials of any user.
- A Custom Administrator can edit only their own credentials or the credentials of a regular user they created.
- A Regular User can edit only their own credentials.

NOTE: If a user with administrator privileges configures the Cloud Director Server credentials, a regular user can create backups using the organization credentials.

To configure VMware Cloud Director Server credentials:

1. On the toolbar, click **Settings**.
2. Click the **Credentials Management** tab.
3. Click the **Virtualization Credentials** tab.
4. Select **VMware Cloud Director Server**, and then do one of the following:
   - To add VMware Cloud Director Server Credentials, click **[+] Add Credentials**.
   - To edit VMware Cloud Director Server Credentials, select the credential, and then click ✏ **Edit Credentials**.
5. On the **Add/Edit Cloud Director Server Credentials** tab, do the following:

   a) In the **Host or IP Address** box, type the host name or IP address of the VMware Cloud Director Server.

   b) In the **Account credentials** box, select the account credentials for the VMware Cloud Director Server.

   NOTE: To add or edit account credentials, click **[+]** or ✏.

   c) In the **VMware Cloud Director Server credentials name** box, type a name for the credentials.

d) Click **Next**.

NOTE: The list of VMware vCenter Servers associated with the VMware Cloud Director Server are automatically displayed.

6. On the **Add/Edit vCenter Servers** tab, do the following:
   a) To enable the VMware vCenter Server, slide the toggle switch to **Enabled**.
   b) To edit the account credentials of a VMware vCenter Server, click **Edit**.
   c) Click **Finish**.
7. To update the list of credentials, click **Refresh**.

2.7.2 Searching for Cloud Director Server credentials

If you have multiple VMware Cloud Director Server credentials, you can search for the credentials.

To search for VMware Cloud Director Server credentials:

1. On the toolbar, click **Settings**.
2. Click the **Credentials Management** tab.
3. Click the **Virtualization Credentials** tab.
4. Select **VMware Cloud Director Server**, and then click **Search**.
5. Type the name of the VMware Cloud Director Server credentials you want to find, and then press **Enter**.

2.7.3 Sharing Cloud Director Server credentials

You can share VMware Cloud Director credentials with other users. When sharing credentials, consider the following:

- A Global Administrator can share the credentials of any user.
- A Custom Administrator can share only their own credentials or the credentials of a regular user they created.
- A Regular User cannot share their credentials with other users.

To share VMware Cloud Director Server credentials:

1. On the toolbar, click **Settings**.
2. Click the **Credentials Management** tab.
3. Click the **Virtualization Credentials** tab.

4. Select **VMware Cloud Director Server**.
5. Select the credentials you want to share, and then click **Share Credentials**.
6. Select the users you want to share the credentials with, and then click **Save**.

2.8 Configuring Management Console settings

You can configure the security, email notification, broadcast notification, email report, and proxy server settings for Management Console.

2.8.1 Configuring the security settings

You can configure the password policy, number of sign in attempts after which the user is locked out, period of inactivity after which the user is signed out, and the password policy for data deletion.

To configure the security settings:

1. On the toolbar, click **Settings**.
2. Click the **Management Console** tab.
3. Click the **Security** tab.
4. Under **Password policy**, configure the password policy you want to enforce for users, and then click **Apply**.
5. Under **Sign in attempts**, configure the number of failed sign in attempts that are allowed before users are locked out of the system and the duration that users are locked out, and then click **Apply**.
6. Under **Session timeout**, configure the period of inactivity after which users are automatically signed out, and then click **Apply**.
7. Under **Data deletion**, configure whether users are required to enter their password when attempting to perform an operation that can result in the loss of data, and then click **Apply**.

NOTE: Operations that can result in the loss of data include, deleting an account, deleting a DS-Client, deleting a backup, performing a selective delete, or configuring the DS-System trash settings.

2.8.2 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**.
2. Click the **Management Console** tab.
3. Click the **Email** tab.
4. In the **SMTP host** box, type the host name or IP address of the email server you want to use for the sending email notifications.
5. In the **SMTP port** box, enter the port number you want to use for sending email notifications.
6. In the **Sender's email address** box, type the email address from which the notification will be sent.
7. Select the protocol (**SSL**, **TLS** or **None**) you want to use for establishing encrypted communication between the email server and email client.
8. To enable a SMTP client to log in using an authentication mechanism supported by the SMTP server, select the **Enable SMTP authentication** check box, and then type the user name and password.
9. To send a test email notification, click **Test**.
10. To reset the settings to their defaults, click **Reset**.
11. Click **Save**.

2.8.3 Configuring the broadcast notification settings

You can configure the broadcast settings to send a notification to all Management Console users, which is useful when you need to update the system.

To configure the broadcast notification settings:

1. On the toolbar, click **Settings**.
2. Click the **Management Console** tab.
3. Click the **Broadcast** tab.
4. To email the same notification message to all users, select the **Include email notification** check box.
5. In the **Message** box, type the notification message you want to send.
6. Click **Send**.

NOTE: When the administrator sends a notification to users, their Notification icon 🔔 will flash.

2.8.4 Configuring the email report schedule settings

You can configure a schedule to email a generated report to users.

To configure the email report schedule settings:

1. On the toolbar, click **Settings**.
2. Click the **Management Console** tab.
3. Click the **Report** tab, and then do one of the following:
   - To create an email report schedule, click **[+] Create Email Report Schedule**.
   - To edit an email report schedule, select the schedule, and then click ✏ **Edit Email Report Schedule**.

   NOTE: To delete an email report schedule, select the schedule, and then click **Delete Email Report Schedule**.
4. In the **Schedule name** box, type a name for the schedule.
5. Under **Report Type**, select the report(s) you want to email.
6. If you selected **Backup set status**, do the following:

a) In the **DS-System** box, select the name of the DS-System with the backup for which you want to generate the report.

b) In the **Account** box, select the account associated with the DS-System.

c) In the **DS-Client** box, select the DS-Client associated with the account.

NOTE: You must have an active connection to the selected DS-System or DS-Client to generate the report.

d) In the **Backup status** box, select the status of the backups you want to include in the report.

7. 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 addresses with a comma (,).

8. Under **Schedule details**, select the frequency at which the reports should be emailed.
9. In the **Start date** box, select the date from which data is to be included in the report. No data before this date will be displayed.
10. In the **End date** box, select the date up to which data is to be included in the report. No data after this date will be displayed.
11. Click **Create**/**Save**.

2.8.5 Configuring the proxy server settings

You can configure the proxy server settings for Management Console.

To configure the proxy server settings:

1. On the toolbar, click **Settings**.
2. Click the **Management Console** tab.
3. Click the **Proxy** tab.
4. In the **HTTP proxy address** box, type the IP address of the HTTP proxy server.
5. In the **HTTP proxy port** box, type the port number required to communicate with the HTTP proxy server.
6. In the **HTTPS proxy address** box, type the IP address of the HTTPS proxy server.
7. In the **HTTPS proxy port** box, type the port number required to communicate with the HTTPS proxy server.
8. To use the same settings for both HTTP and HTTPS, select the **Use same proxy server settings for http and https** check box.
9. Click **Save**.

3 Configuring accounts and groups

You can configure accounts, DS-Clients, and VM replication groups.

3.1 Configuring DS-Client remote management

You can configure DS-Clients to be remotely managed by Management Console without opening a port in the firewall on the DS-Client machine.

NOTE: To enable a DS-Client to be remotely managed by Management Console, the **MCRemoteManagement** advanced configuration parameter must be enabled in the DS-User. This parameter is enabled by default.

3.1.1 Configuring at the DS-System level

When you enable DS-Client remote management at the DS-System level, remote management is automatically enabled for all eligible accounts associated with the DS-System.

To configure DS-Client remote management at the DS-System level:

1. On the toolbar, click **Account Management.**
2. Click the **Accounts** tab.
3. In the **DS-System** box, select a DS-System.
4. Select the DS-System for which you want to enable or disable remote management, and then click **DS-Client remote management** ✎.
5. In the **DS-Client Remote Management** dialog box, do the following:
   a) Slide the toggle switch to **Enabled**.
   b) In the **Host name or IP address** box, type the host name or IP address of Management Console.
   c) In the **Port number** box, enter the port number for Management Console.
   d) In the **Remote management port range** boxes, enter the range of ports from which a port can be automatically assigned to the DS-Clients.
   e) Click **Save**.

3.1.2 Configuring at the account level

When you enable DS-Client remote management at the account level, remote management is automatically enabled for all eligible DS-Clients associated with the account.

NOTE: You can enable or disable DS-Client remote management for multiple accounts at the same time or for an individual account. For more information see, Section 3.2.1, “Configuring an account”, on page 55.

To configure DS-Client remote management at the account level:

1. On the toolbar, click **Account Management.**
2. Click the **Accounts** tab.
3. In the **DS-System** box, select a DS-System.
4. Select the accounts for which you want to enable or disable remote management, and then click 🔗 **Edit Customer Remote Management**.
5. Slide the toggle switch to enable or disable DS-Client remote management.
6. Click **Save**.

3.1.3 Configuring at the DS-Client level

You can enable DS-Client remote management only for eligible DS-Clients.

NOTE: You can enable or disable DS-Client remote management for multiple DS-Clients at the same time or for an individual DS-Client. For more information, see Section 3.3.1, “Configuring a DS-Client”, on page 58.

To configure DS-Client remote management at the DS-Client level:

1. On the toolbar, click **Account Management.**
2. Click the **Accounts** tab.
3. In the **DS-System** box, select a DS-System.
4. Select the DS-Clients for which you want to enable or disable remote management, and then click 🔗 **Edit Customer Remote Management**.
5. Slide the toggle switch to enable or disable DS-Client remote management.
6. Click **Save**.

3.2 Configuring accounts

You must configure an account to back up data from a DS-Client to the DS-System.

IMPORTANT: To configure an account, you must be a Global Administrator and have a DS-System connection.

You can provide an extra layer of security by configuring multiperson approval (MPA) so users require multiple people to approve a potentially destructive action that can result in the loss of data.

If MPA is enabled, you must configure a threshold to determine how many approvals are required and select the approvers from a list of users.

When a user attempts to perform a task that requires approval, the approvers receive an email with the name of the user and a description of the task and must approve or deny the request. The approval link expires after 30 minutes. A task must meet the configured approval threshold with no denials to be approved.

IMPORTANT: Only a Global Administrator can enable or disable MPA. If MPA is enabled, the Global Administrator must get approval if they attempt to disable MPA, disable a previously enabled MPA task, or lower the approval threshold.

3.2.1 Configuring an account

When configuring an account, consider the following:

- The first DS-Client that registers an account encryption key for an account sets the key and it cannot be changed.
- Since encryption keys are entered by the person installing the DS-Client, you should create a DS-Client immediately after the account is created.
- Ensure all users who install a DS-Client belonging to the same account use the same account encryption key. If any other key or key type is selected, the DS-Client will fail to connect to the DS-System.

NOTE: If you are using DS-Billing as part of your implementation, you should use the DS-Billing application to create and maintain accounts. For more information, see the *DS-Billing User Guide*.

To configure an account:

1. On the toolbar, click **Account Management.**
2. Click the **Accounts** tab.
3. Under **Accounts**, do one of the following:
   - To add an account, click **[+] Add Account**.
   - To edit an existing account, select the account, and then click 🖉 **Edit Account**.

NOTE: When editing an account, you cannot change the DS-System or account ID.

---

4. To configure the account settings, do the following:

   a) In the **DS-System** box, select the name of the DS-System to which you want to associate the account.

   b) In the **Account ID** box, type a unique ID for the account.

   c) In the **Account name** box, type a unique name for the account.

   d) In the **Contact name** box, type the name of the contact for the account.

   e) In the **Contact email address** box, type the email address of the contact for the account.

   f) To define a storage limit for the account, slide the **Storage quota management** switch to **Enabled**, and then enter the quota in GB or MB.

   g) To enable DS-Client remote management for the account, slide the **DS-Client remote management** switch to **Enabled**.

   NOTE: When enabled, remote management is automatically enabled for all eligible DS-Clients associated with the account.

   ---

   h) To enable DS-System replication for the account, slide the **DS-System replication** switch to **Enabled**.

   i) Click **Next**.

5. To configure multiperson approval (MPA), do the following:

   a) Slide the **Multiperson approval** switch to **Enabled**.

   b) Configure the following MPA tasks as required:

   - **Edit backup** – Users require approval to edit a backup or reassign a schedule or retention rule.

- **On-demand backup** – Users require approval to perform an on-demand backup.
- **On-demand restore** – Users require approval to perform an on-demand restore.
- **Delete backup** – Users require approval to delete a backup.
- **Selective delete** – Users require approval to delete data from a backup.
- **Configure schedule** – Users require approval to edit or delete a schedule.
- **Configure retention rule** – Users require approval to edit or delete a retention rule.

NOTE: Users inherit the MPA settings based on the account they are associated with and their role.

c) Click **Next**.

6. Review the settings for the account, and then click **Create** or **Save**.

3.2.2 Deleting an account

You can delete an account when required.

To delete an account:

1. On the toolbar, click **Account Management.**
2. Click the **Accounts** tab.
3. In the **DS-System** box, select a DS-System.
4. Select the account you want to delete, and then click 🗑 **Delete Account**.
5. In the **Account ID** box, type the account ID.
6. If you are required to enter a password to delete an account, type your Management Console password, and then click **Continue**.

3.3 Configuring DS-Clients

Each DS-System can support multiple accounts and multiple DS-Clients per account. The initial group of DS-Clients can be identified by the prefix “DSC” and a unique system ID that contains 4 alphanumeric characters followed by a generated DS-Client number. Additional groups of DS-Clients can be identified by the prefix “D00”, “D01”, and so on.

3.3.1 Configuring a DS-Client

You can configure a DS-Client for each account associated with a DS-System.

To configure a DS-Client:

1. On the toolbar, click **Account Management**.
2. Click the **Accounts** tab.
3. In the **DS-System** box, select a DS-System, expand the required DS-System and account, and then do one of the following:
    - To add a DS-Client, click **[+] Add DS-Client**.
    - To edit an existing DS-Client, select the DS-Client, and then click ✎ **Edit DS-Client**.
4. In the **Description** box, type a name or description of the DS-Client.
5. Under **Storage quota settings**, do the following:

    a) To limit the online storage quota, select the **Limit online storage quota** check box, and then enter the quota.

    b) To limit the VM replication quota, select the **Limit VM Replication quota** check box, and then enter the quota for the VM replication count, VM replication capacity, or both.
6. To scan files for malware or unauthorized content during backup and restore, slide the **Antimalware/CDR Scan** switch to **Enabled**.
7. To register the DS-Client as a template for mass deployment, under **Mass deployment settings**, select the **Enable auto-registration counter** check box, and then enter the number of DS-Clients that can be created.
8. To enable DS-Client remote management of the DS-Client, slide the **Remote management** switch to **Enabled**.

    NOTE: You can enable remote management only for eligible DS-Clients.
9. Click **Add** or **Save**.

3.3.2 Deleting a DS-Client

You can delete a DS-Client account when required.

To delete a DS-Client account:

1. On the toolbar, click **Account Management**.
2. Click the **Accounts** tab.
3. In the **DS-System** box, select a DS-System, expand the required DS-System and account
4. Select the DS-Client you want to delete, and then click **Delete DS-Client**.
5. In the **DS-Client** box, type the number of the DS-Client account.
6. If you are required to enter a password to delete a DS-Client, type your Management Console password, and then click **Continue**.

3.4 Configuring VM replication groups

The VM replication feature can be licensed to a DS-System from a DS-License Server RLM to allow DS-Clients to replicate virtual machines from one VMware vCenter Server to another and initiate failover and failback.

When configuring a VM replication group, you must add at least two DS-Clients. The source DS-Client must point to the IP addresses of the destination DS-Client in the replication group. This allows for the reverse transmission of data on failback. To optimize your networking configuration and avoid potential conflicts between multiple DS-Clients that share the same IP address, you can specify the ports used by the source DS-Client and the destination DS-Client.

Unlike backups, VM replication does not send any data to the DS-System. Replication data is transferred between the source DS-Client and destination DS-Client. The DS-Client on which you create a VM replication set is the source DS-Client.

When a replication set is run, the source DS-Client instructs the source VMware vCenter Server to snapshot the selected virtual machines. The source DS-Client then sends the replication data to the destination DS-Client, which creates the replication virtual machine on the target VMware vCenter Server.

When a virtual machine is replicated by the DS-Client for the first time, full replication is performed. All subsequent replication processes are incremental.

NOTE: VM replication is based on the number of replicated virtual machines or the native capacity of the virtual machines. The source DS-Client must have sufficient VM replication capacity to cover the size of its VM replication sets.

3.4.1 Configuring a VM replication group

You must configure a VM replication group to perform VM replication.

IMPORTANT: After you have modified the VM replication port settings for multiple DS-Clients, you must stop and restart the DS-Client service on each affected computer one at a time. Wait until the DS-Client service has successfully restarted on one computer before you stop and restart the DS-Client service on another.

To configure a VM replication group:

1. On the toolbar, click **Account Management**.
2. Click the **VM Replication Groups** tab.
3. Under **VM Replication Groups**, do one of the following:
   - To add a VM replication group, click **[+] Add VM Replication Group**.
   - To edit a VM replication group, select the group, and then click ✎ **Edit VM Replication Group**.
4. In the **DS-System** box, select the DS-System for which you want to configure a VM replication group.
5. Under **Source DS-Client**, do the following:

   a) In the **Account** box, select the account containing the DS-Client you want to use as the source DS-Client.

   b) In the **DS-Client** box, select the DS-Client account that will be the source DS-Client for the VM replication group.

   c) In the **IP address** box, type the IP address of the source DS-Client.

   d) In the **Port number** box, enter the port number that will be used by the source DS-Client.
6. Under **Destination DS-Client**, do the following:

   a) In the **Account** box, select the account containing the DS-Client you want to use as the destination DS-Client.

   b) In the **DS-Client** box, select the DS-Client account that will be the destination DS-Client for the VM replication group.

   c) In the **IP address** box, type the IP address of the destination DS-Client.

   d) In the **Port number** box, enter the port number that will be used by the destination DS-Client.

   e) To add another destination DS-Client, click ⊕ Add destination.
7. Click **Add** or **Save**.

3.4.2 Deleting a VM replication group

You can delete a VM replication group when required.

To delete a VM replication group:

1. On the toolbar, click **Account Management**.
2. Click the **VM Replication Groups** tab.
3. Select the VM replication group you want to delete, and then click 🗑 **Delete VM Replication Group**.
4. When the system prompts you to delete the VM replication group, click **Yes**.

4 Working with schedules

You can create a schedule to perform automatic or unattended activities.

4.1 Configuring a schedule

When configuring a schedule, each detail determines when and how often a scheduled task is performed. You can add as many details as required to a schedule. A default schedule is available that you can edit if required.

NOTE: If MFA and/or MPA has been enabled for **Configure schedule**, you must enter an authentication code and/or require approval to edit a schedule.

To configure a schedule:

1. On the toolbar, click **Data Management**.
2. Click the **Schedules** tab, and then do one of the following:
   - To add a schedule, select the DS-Client, and then click [**+**] **Create Schedule**.
   - To edit a schedule, select the schedule, and then click ✎ **Edit Schedule**.
3. In the **Schedule name** box, type a name for the schedule.
4. In the **Schedule detail name** box, type a name for the schedule detail.
5. Select the tasks for the schedule detail. The options are as follows:
   - To schedule a backup, select the **Backup** check box.
   - To schedule replication, select the **Replication** check box.
   - To schedule retention, select the **Retention** check box.
   - To schedule a restore, select the **Restore** check box.
6. In the **Select interval** box, select the frequency at which you want the schedule to run. The options are as follows:
   - **One time** – The schedule runs only once. Specify the date on which you want the schedule to run.
   - **Daily** – The schedule runs every specified number of days. Specify the daily interval at which you want the schedule to run.
   - **Weekly** – The schedule runs every specified number of weeks. Specify the weekly interval at which you want the schedule to run, and then select the days of the week on which you want the schedule to run.
   - **Monthly** – The schedule runs every specified number of months. Specify the day and monthly interval at which you want the schedule to run.

7. If you selected the daily, weekly, or monthly interval, under **Schedule Frequency**, select one of the following:
    - **Occurs once** - The schedule runs only once.
    - **Occurs every** - Specify the interval at which you want the schedule to run.
8. Under **Time selection**, do the following:
    a) In the **Schedule start date** box, specify the date when you want the schedule to start.

    b) In the **Schedule end date** box, specify the date when you want the schedule to end.

    c) In the **Task start time** box, specify the time when you want the schedule to start.

    d) In the **Task duration** box, specify the duration you want the schedule to run.

    e) In the **Task end time** box, specify the time when you want the schedule to end.
9. To add a new schedule detail, click +.
10. Click **Create** or **Save**.
11. If you have edited a schedule, do one of the following:
    - To confirm you want to edit the schedule, click **Continue**.
    - If MFA has been enabled for **Configure schedule**, enter the six-digit authentication code you received, and click **Continue**.
    - If MPA has been enabled for **Configure schedule**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.
    - If MFA and MPA have been enabled for **Configure schedule**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

4.2 Reassigning a schedule

You can reassign a schedule to a different backup or multiple backups.

NOTE: If MFA and/or MPA has been enabled for **Edit backup**, you must enter an authentication code and/or require approval to complete the task.

To reassign a schedule:

1. On the toolbar, click **Data Management**.
2. Click the **Schedules** tab.
3. Select the schedule you want to reassign, and then click **Reassign Schedule.**
4. On the **Schedule** page, select the backups to which you want to reassign the schedule, and then click **Reassign**.
5. On the **Reassign to Schedule** page, select the schedule you want to reassign to the backup.
6. Click **Save**, and then do one of the following:
   - To confirm you want to reassign the schedule, click **Continue**.
   - If MFA has been enabled for **Edit backup**, enter the six-digit authentication code you received, and click **Continue**.
   - If MPA has been enabled for **Edit backup**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.
   - If MFA and MPA have been enabled for **Edit backup**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

4.3 Deleting a schedule

You can delete a schedule if required.

NOTE: If MFA and/or MPA has been enabled for **Configure schedule**, you must enter an authentication code and/or require approval to complete the task.

To delete a schedule:

1. On the toolbar, click **Data Management**.
2. Click the **Schedules** tab.
3. Select the schedule you want to delete, click **Delete Schedule**, and then do one of the following:
   - To confirm you want to delete the schedule, click **Continue**.
   - If MFA has been enabled for **Configure schedule**, enter the six-digit authentication code you received, and click **Continue**.
   - If MPA has been enabled for **Configure schedule**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.
   - If MFA and MPA have been enabled for **Configure schedule**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

5 Working with retention rules

You can use Retention rules to implement granularity in your backed up generations. If you do not use retention rules, your backup data will remain in the DS-System online storage based on the settings for the backup generation.

After assigning a retention rule to an individual backup, you need to enforce the rule either on demand or via 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 only applies the options that retain more data.

5.1 Configuring a retention rule

You can configure a retention rule to determine how much data is retained online. A default retention rule is available that you can edit if required.

NOTE: If MFA and/or MPA has been enabled for **Configure retention rule**, you must enter an authentication code and/or require approval to edit a retention rule.

To configure a retention rule:

1. On the toolbar, click **Data Management**.
2. Click the **Retention Rules** tab, and then do one of the following:
   - To create a retention rule, select the DS-Client account, and then click [**+**] **Create Retention Rule**.
   - To edit a retention rule, select the retention rule, and then click ✎ **Edit Retention Rule**.
3. In the **Retention rule name** box, type a name for the retention rule.
4. To create a time-based retention rule, select the **Time based retention** check box, and then do the following:

   a) In the **Keep most recent generations** box, enter the number of generations of a file you want to retain in the DS-System online storage.

   b) To keep all generations of a file for a specific time period, select the **Keep all generations for the last** check box, and then enter the time period.

   NOTE: Any generations not within the specified time period will be deleted unless they qualify for another retention option.

c) To add a time-based retention rule, click **[+]**, and then enter the interval for which you want to retain the most recent generation.

NOTE: When the retention rule is enforced, the most resent generation is retained for as many intervals that can fit into the retention period.

5. To delete files that have been removed from the source, select the **Delete files removed from source**, and then do the following:

   a) In the **After...** box, enter the time period after which files removed from source should be deleted.

   b) In the **Keep generation** box, enter the number of generations of a file you want to retain in the DS-System online storage.

6. Click **Create** or **Save**.

7. If you have edited a retention rule, do one of the following:

   - To confirm you want to edit the retention rule, click **Continue**.
   - If MFA has been enabled for **Configure retention rule**, enter the six-digit authentication code you received, and click **Continue**.
   - If MPA has been enabled for **Configure retention rule**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.
   - If MFA and MPA have been enabled for **Configure retention rule**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

5.2 Reassigning a retention rule

You can reassign a different retention rule to a backup as required.

NOTE: If MFA and/or MPA has been enabled for **Edit backup**, you must enter an authentication code and/or require approval to complete the task.

To reassign a retention rule:

1. On the toolbar, click **Data Management**.
2. Click the **Retention Rules** tab.
3. Select the DS-Client account for which you want to reassign a retention rule.
4. Select the retention rule you want to reassign, and then click **Reassign Retention Rule**.
5. Select the backup(s) to which you want to reassign the retention rule, and then click **Reassign**.
6. On the **Reassign to Retention Rule** page, select a retention rule.
7. Click **Save**, and then do one of the following:
   - To confirm you want to reassign the retention rule, click **Continue**.
   - If MFA has been enabled for **Edit backup**, enter the six-digit authentication code you received, and click **Continue**.
   - If MPA has been enabled for **Edit backup**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.
   - If MFA and MPA have been enabled for **Edit backup**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

5.3 Deleting a retention rule

You can delete a retention rule if required.

NOTE: If MFA and/or MPA has been enabled for **Configure retention rule**, you must enter an authentication code and/or require approval to complete the task.

To delete a retention rule:

1. On the toolbar, click **Data Management**.
2. Click the **Retention Rules** tab.
3. Select the retention rule you want to delete, click **Delete Retention Rule**, and then do one of the following:
   - To confirm you want to delete the retention rule, click **Continue**.
   - If MFA has been enabled for **Configure retention rule**, enter the six-digit authentication code you received, and click **Continue**.
   - If MPA has been enabled for **Configure retention rule**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.
   - If MFA and MPA have been enabled for **Configure retention rule**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

6 Working with backups

A backup consists of a list of items, that need to be backed up and the settings that define how to perform the backup.The following backups are supported:

Backup Type	Windows	Linux	Mac
File Systems			
File System	✓	✓	✓
Permissions	✓	✓	✓
Cloud			
Microsoft 365	✓		
Databases			
Microsoft SQL Server (Classic)	✓		
Microsoft SQL Server (VSS aware)	✓		
Servers			
Microsoft Exchange Server (VSS aware)	✓		
Microsoft SharePoint Server (VSS aware)	✓		
Virtual Machines			
Microsoft Hyper-V Server (VSS-aware)	✓		
VMware vCenter Server	✓	✓	
VMware Cloud Director Server	✓	✓	

Table 4 Supported backup types

6.1 File system backups

You can create a File system backup to back up individual files, folders, or drives at various levels of the tree structure in a file system.

6.1.1 Configuring a File system backup

You can configure a File system backup.

NOTE: If MFA and/or MPA has been enabled for **Edit backup**, you must enter an authentication code and/or require approval to complete the task.

To configure a File system backup:

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

   NOTE: To search for a specific DS-Client based on the DS-Client number, type the DS-Client number in the search field, and then press **Enter**.
3. On the **Type & Components** page, do the following:
   a) In the **Backup set type** box, select **File System**.
   b) In the **Backup set name** box, type a name for the backup.
   c) In the **DS-System** box, select the DS-System.
   d) In the **Account** box, select the account.
   e) In the **DS-Client** box, select the DS-Client.
   f) Click **Next**.
4. On the **Credentials & Items** page, do the following:
   a) In the **Source IP address** box, type the IP address of the source computer containing the files you want to back up.
   b) To use the DS-Client credentials to connect to the local DS-Client computer, select **Use DS-Client credentials**.

c) To use other credentials, select **Use network credentials** and then type the user name, password, and domain name.

NOTE: You must connect using an Administrator or equivalent account.

d) Under **Backup set items**, select the items you want to back up.

5. To configure advanced options, click **Advanced Options**, and then do the following:

a) On the **General** tab, do the following:

1. In the **Compression algorithm** box, select the compression method you want to use. The options are as follows:

- **LZOP** – A faster compression rate than ZLIB, but with less compression. This is a good default compression method when the network is not the bottleneck.
- **ZLIB** – A slower compression rate than LZOP, but with better compression. This is a good default compression method when the network is the bottleneck.

NOTE: There are four levels of ZLIB compression. ZLIB Global compresses global data that remains static during the life cycle of the application. ZLIB High = 9, ZLIB Medium = 6, ZLIB Low = 3.

2. In the **Stop on errors** box, enter the number of errors that must occur before the backup process is stopped. A value of 0 means DS-Client will not stop a backup process regardless of the number of errors.
3. To record all the files that were backed up in the Activity Log, select the **Enable detailed log** check box.
4. To back up data using the Microsoft VSS (Volume Shadow Copy Service), select the **Use Volume Shadow Copy Service (VSS)** check box.

NOTE: To ensure backup consistency and avoid conflicts with files in use, we recommend enabling this option on source machines running a supported version of Windows if you have administrative credentials.

5. To scan files for malware during the backup process, under **Antimalware scan**, slide the switch to **Enabled**.

NOTE: Files detected with malware are backed up to the DS-System in encrypted format and a warning message appears in the Event Log.

6. To scan files for potentially malicious or unauthorized content during the backup process, under **CDR scan**, slide the switch to **Enabled**. In the **Policy** box, select one of the following policies:

   - **Filter** – Filters non-compliant content from the file based on a static analysis by the CDR engine. This is the default option.
   - **Remove** – Removes non-compliant content from the file.
   - **Block** – Blocks the file if it contains non-compliant content.

NOTE: Files detected with non-compliant content are backed up to the DS-System in encrypted format and a warning message appears in the Event Log.

7. To back up file permissions, select the **Back up permissions** check box.
8. To copy the backed up data to the DS-Client buffer, select the **Use buffer** check box. DS-Client sends files from the DS-Client buffer to the DS-System, which frees up the backup source as fast as possible.
9. To save a copy of the backed up data to a local storage location, select the **Save on local storage** check box. In the **Local storage path** box, type the path for the local storage location.

b) On the **Preprocessing** tab, do the following:

1. To enable preprocessing so you can configure a process to run before the backup, slide the switch to **Enabled**.
2. To execute a process on a remote machine where the backup files are located, select the **Execute on remote system** check box.This option is available only if the backup is on a remote machine.
3. To run a command before the backup, in the **Process** box, select **Run command**. In the **Command** box, type the command you want to run. To test the command, click **Test**.

   You must type “cmd /c” before the command if it is not the name of an executable file.

   - On a local Windows machine, the DS-Client will terminate the process if the command requires user input.
   - On a remote Windows machine, the credentials must have administrator privileges.

NOTE: To use the Run command on a Windows or Linux machine, the **AllowLocal** advanced parameter must be enabled in DS-User.

4. To start a service before the backup, in the **Process** box, select **Start service**. In the **Service** box, type the name of the service or click **Browse** to select the service. To test the process, click **Test**.

5. To stop a service before the backup, in the **Process** box, select **Stop service**. In the **Service** box, type the name of the service or click **Browse** to select the service. To test the process, click **Test**.

6. Under **Condition**, select the condition that must be met to perform the activity. The options are as follows:

   - **On exit code** – The condition is applied if the exit code is equal or not equal to the specified exit code.

   - **On file existence** – The condition is applied if the specified file exists or not. Enter the full path. Include the drive on local machines or the share but not the server on remote machines.

   - **On output string** – The condition is applied if the specified string in the command output exists or not (local commands or Linux only). For a large output string, only the first 16K is checked.

   - **On execution success** – The condition is applied if the command is executed successfully.

   - **On execution failure** – The condition is applied if the command fails to execute.

NOTE: To combine the On execution failure condition with the On exit code, On file existence, or On output string conditions, select the **Or execution failure** check box.

7. Under **Action**, select the action that you want to be performed if the specified condition is met. The options are as follows:

   - **Do not perform the post-process activity** - The post-processing activity will not be performed if the condition has been met.

   - **Do not perform backup** - The backup will not be performed if the condition has been met.

   - **Delay backup** (Windows only) - The backup will be delayed by the specified number of seconds if the condition has been met.

NOTE: The **Delay backup** option is useful if the command activates a background process responsible for creating data for a backup. This allows time for the preprocessing activity to terminate properly.

c) On the **Postprocessing** tab, do the following:

1. To enable postprocessing so you can configure a process to run after the backup, slide the switch to **Enabled**.

2. To execute a process on a remote machine where the backup files are located, select the **Execute on remote system** check box. This option is available only if the backup is on a remote machine.

3. To run a command after the backup, in the **Process** box, select **Run command**. In the **Command** box, type the command you want to run. To test the command, click **Test**.

   You must type “cmd /c” before the command if it is not the name of an executable file.

   - On a local Windows machine, the DS-Client will terminate the process if the command requires user input.

   - On a remote Windows machine, the credentials must have administrator privileges.

NOTE: To use the Run command on a Windows or Linux machine, the **AllowLocal** advanced parameter must be enabled in DS-User.

4. To start a service after the backup, in the **Process** box, select **Start service**. In the **Service** box, type the name of the service or click **Browse** to select the service. To test the process, click **Test**.

5. To stop a service after the backup, in the **Process** box, select **Stop service**. In the **Service** box, type the name of the service or click **Browse** to select the service. To test the process, click **Test**.

6. Under **Action**, select the action that you do not want to be performed if the specified condition is met. The options are as follows:

   - **Backup is successful** (Windows only) - The postprocessing activity will not be performed if the backup was successful.

   - **Backup completes with errors** (Windows only) – The postprocessing activity will not be performed if the backup completed with errors.

   - **Backup is incomplete** (Windows only) – The postprocessing activity will not be performed if the backup is incomplete.

   - **Execute after data has been copied to DS-Client Buffer** (Linux only) - Executes the command after the backup data has been copied to the DS-Client buffer.

7. Click **OK**.

6. Click **Next or Save**.

7. On the **Schedule & Retention** page, do the following:

a) In the **Schedule** box, select a schedule for the backup.

   - To view the details of the schedule, click 👁 **View**.
   - To add a schedule, click + **Create Schedule**.
   - To edit a schedule, select the schedule, and then click ✏ **Edit Schedule**.

b) In the **Retention rule** box, select a retention rule for the backup.

   - To view details of the retention rule, click 👁 **View**.
   - To add a retention rule, click + **Create Retention Rule**.
   - To edit a retention rule, select the retention rule, and then click ✏ **Edit Retention Rule**.

c) If the schedule has an associated restore task, you can schedule when the backup is restored. To schedule a restore, click ⟲ **Restore**.

d) Click **Next** or **Save**.

8. On the **Summary** page, review the settings for the backup.
   - To edit the name of the backup, click ✏.
   - To edit the advanced options, click ⚙ **Advanced Options.**
   - To view the details of the schedule, click 👁 **View**.
   - To view details of the retention rule, click 👁 **View**.
9. Click **Create** or **Save**.
10. If you have edited the backup, do one of the following:
    - To confirm you want to edit the backup, click **Continue**.
    - If MFA has been enabled for **Edit backup**, enter the six-digit authentication code you received, and click **Continue**.
    - If MPA has been enabled for **Edit backup**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.
    - If MFA and MPA have been enabled for **Edit backup**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

6.1.2 Restoring a File system backup

You can restore data from a File system backup.

NOTE: If MFA and/or MPA has been enabled for **On-demand restore**, you must enter an authentication code and/or require approval to complete the task.

To restore a File system backup:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
3. Select the DS-System, account, and DS-Client.

   NOTE: To search for a specific DS-Client based on the DS-Client number, type the DS-Client number in the search field, and then press **Enter**.

4. Select the File system backup you want to restore, and then click **Restore Backup Set**. You can restore only one backup at a time.
5. Beside **Backup session**, select the generation(s) of the backup you want to restore. By default, the latest generation is selected for restore.
6. To configure advanced options, click . Select the file overwrite restore option you want to use, and then click **Save**. The options are as follows:
   - **Restore all** – All selected files are restored to the destination folder. Files with the same name are overwritten.
   - **Restore newer** – Only files newer than those in the destination folder are restored.
   - **Restore older** – Only files older than those in the destination folder are restored.
   - **Restore different** – Only files with different dates/sizes than those in the destination directory are restored.
   - **Skip existing** – Existing files with the same name in the destination folder are not restored.
7. To restore the backup without deleted data, select the **Exclude deleted data** check box.
8. Select the items you want to restore. To search for items, click **Search,** and then type the name of the backup.
9. In the **Restore Location** box, select one of the following options:
   - **Original** – Select this option to restore the item to its original source location.

- **Alternate** – Select this option to restore the items to an alternate location, and then do the following:

    a) In the **Server** box, click ✏.

    b) In the **Server** box, type the IP address of the server to which the backup will be restored.

    c) Type the user name, password, and domain name for the server.

    d) Under **Destination details**, in the column **Destination Folder**, click 📁.

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

    f) Click **Save**.

10. To scan files for malware during the restore process, do the following:

    e) Slide the **Antimalware Scan** switch to **Enabled**.

    f) In the **Policy** box, select one of the following policies:

    - **Quarantine only** – Files detected with malware are not restored. A copy of the infected files is placed in a password protected zip file in the quarantine folder. This is the default policy.

    - **Clean and restore** – Attempts to clean the infected files and restore them if remediation is successful. This overwrites the original file. A copy of the original infected files is placed in a password protected zip file in the quarantine folder.

11. To scan files for malicious or unauthorized content during the restore process, do the following:

    a) Slide the **CDR Scan** switch to **Enabled**.

    b) In the **Policy** box, select one of the following policies:

    - **Filter** – Filters non-compliant content from the file based on a static analysis by the CDR engine. This is the default policy.

    - **Remove** – Removes non-compliant content from the file.

    - **Block** – Blocks the file if it contains non-compliant content.

NOTE: Files detected with non-compliant content are filtered, removed, or blocked based on the selected policy. A warning message appears in the Event Log and a copy of the infected files is placed in a password protected zip file in the quarantine folder.

12. To restore the permissions for the items, select the **Restore permissions** check box.

IMPORTANT: If you are restoring to an alternate location and selected Microsoft Azure storage, you must clear the **Restore permissions** check box.

---

13. Click **Restore**, and then do one of the following:
    - To confirm you want to restore the backup, click **Continue**.
    - If MFA has been enabled for **On-demand restore**, enter the six-digit authentication code you received, and click **Continue**.
    - If MPA has been enabled for **On-demand restore**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.
    - If MFA and MPA have been enabled for **On-demand restore**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

NOTE: To view the progress of the restore activity, click ⚙. For more information, see Section 8.5, “Viewing the Activity Monitor”, on page 145.

6.2 Microsoft 365 backups

You can back up and restore Microsoft 365 Exchange mailboxes, public folders, archive mailboxes, SharePoint sites, OneDrive accounts, Groups, and Teams.

NOTE: For information on managing Microsoft 365 credentials, see Section 2.5, “Managing Microsoft 365 credentials”, on page 37.

- In Microsoft 365 Small Business domains, you can only backup and restore Exchange Online data.
- A Microsoft 365 license is required for every user whose Exchange mailbox or SharePoint site you want to backup and restore, for every user who administer the backup and restore process in the Microsoft 365 Portal, and for every user whose credentials will be used by the DS-Client to access the backup source.

IMPORTANT: To back up Exchange mailboxes or SharePoint sites, you must have the Microsoft 365 Exchange Online license or a Microsoft 365 license that includes equivalent permissions. The user performing the backup must be a Global admin or SharePoint admin as well as a Site admin.

- Exchange data must be in a user mailbox, shared mailbox, or resource mailbox. Backed up data can be restored to the same mailbox or a different mailbox of the source domain or of a different domain using DS-Client. You cannot back up Exchange distribution groups.
- The '%' and '#' characters are supported for SharePoint Online names. The following strings are not supported: "%25", "%2f", and "%3a".

  NOTE: This is applicable when the aforementioned strings are used as a name by themselves or as part thereof. These strings are reserved by DS-Client to properly process SharePoint Online paths and their ASCII equivalents '%', '/', and ':' are supported. Microsoft does not automatically convert these URI-encoded strings and treats them as distinct and valid.

- You can back up and restore OneDrive data under personal sites. OneDrive data for each user is backed up as a Documents List of each personal site.

6.2.1 Configuring a Microsoft 365 backup

You can configure a Microsoft 365 backup.

NOTE: If MFA and/or MPA has been enabled for **Edit backup**, you must enter an authentication code and/or require approval to complete the task.

To configure a Microsoft 365 backup:

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

   NOTE: To search for a specific DS-Client based on the DS-Client number, type the DS-Client number in the search field, and then press **Enter**.

3. On the **Types & Components** page, do the following:

   a) In the **Backup set type** box, select **Microsoft 365**, and then do one of the following:
      - To create a single backup, disable **Multiple backup set creation**, and then type a name for the backup in the **Backup set name** box.
      - To create multiple backups for each Microsoft 365 service, enable **Multiple backup set creation**. This is the default option.

b) In the **DS-System** box, select the DS-System.

c) In the **Account** box, select the account.

d) In the **DS-Client** box, select the DS-Client.

e) Click **Next**.

4. On the **Credentials & Items** page, do the following:

a) In the **Domain** box, select the domain name where the Microsoft 365 items are located.

b) In the **User name** box, select the user name associated with the domain containing the Microsoft 365 items you want to back up.

c) Under **Backup set items**, click the tab containing the Microsoft 365 items you want to back up, and then select the items.

NOTE: If the user doesn’t have credentials to backup or restore a specific service, the associated tab is disabled.

- To search for an item, click 🔍 **Search,** and type the name of the item.
- To sort the items alphabetically, click AZ **Sort list by names**.
- To update the list if items, click ↻.

5. To configure advanced options, click ⚙ **Advanced Options**, and then do the following:

a) In the **Compression algorithm** box, select the compression method you want to use for the backup. The options are as follows:

- **LZOP** – A faster compression rate than ZLIB, but with less compression. This is a good default compression method when the network is not the bottleneck.
- **ZLIB** – A slower compression rate than LZOP, but with better compression. This is a good default compression method when the network is the bottleneck.

NOTE: There are four levels of ZLIB compression. ZLIB Global compresses global data that remains static during the life cycle of the application. ZLIB High = 9, ZLIB Medium = 6, ZLIB Low = 3.

b) In the **Stop on errors** box, enter the number of errors that must occur before the backup process is stopped. A value of 0 means DS-Client will not stop a backup process regardless of the number of errors.

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

d) To scan files for malware during the backup process, under **Antimalware scan**, slide the switch to **Enabled**.

NOTE: Files detected with malware are backed up to the DS-System in encrypted format and a warning message appears in the Event Log.

---

e) To save a copy of the backed up data to a local storage location, select the **Save on local storage** check box. In the **Local storage path** box, type the path for the local storage location.

f) Click **OK**.

6. Click **Next or Save**.

7. On the **Schedule & Retention** page, do the following:

   a) In the **Schedule** box, select a schedule for the backup.

   - To view the details of the schedule, click 👁 **View**.
   - To add a schedule, click + **Add Schedule**.
   - To edit a schedule, select the schedule, and then click ✎ **Edit Schedule**.

   b) In the **Retention rule** box, select a retention rule for the backup.

   - To view details of the retention rule, click 👁 **View**.
   - To add a retention rule, click + **Add Retention Rule**.
   - To edit a retention rule, select the retention rule, and then click ✎ **Edit Retention Rule**.

   c) If the schedule you selected has an associated restore task, you can schedule when the backup is restored. To schedule a restore, click ⟲ .

   d) Click **Next** or **Save**.

8. On the **Summary** page, review the settings for the backup.

   - To edit the name of the backup, click ✎.
   - To edit the advanced options, click ⚙ **Advanced Options.**
   - To view the details of the schedule, click 👁 **View**.
   - To view details of the retention rule, click 👁 **View**.

9. Click **Create** or **Save**.

10. If you have edited the backup, do one of the following:

   - To confirm you want to edit the backup, click **Continue**.
   - If MFA has been enabled for **Edit backup**, enter the six-digit authentication code you received, and click **Continue**.

- If MPA has been enabled for **Edit backup**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.
- If MFA and MPA have been enabled for **Edit backup**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

6.2.2 Restoring a Microsoft 365 backup

You can restore data from a Microsoft 365 backup.

NOTE: If MFA and/or MPA has been enabled for **On-demand restore**, you must enter an authentication code and/or require approval to complete the task.

To restore a Microsoft 365 backup:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
3. Select the DS-System, account, and DS-Client.

   NOTE: To search for a specific DS-Client based on the DS-Client number, type the DS-Client number in the search field, and then press **Enter**.

4. Select the Microsoft 365 backup you want to restore, and then click ⟲ **Restore Backup Set**. You can restore only one backup at a time.
5. Beside **Backup session**, select the generation(s) of the backup you want to restore. By default, the latest generation is selected for restore.
6. Select the items you want to restore. To sort the items alphabetically, click AZ.
7. To search for items in Exchange mailboxes, archive mailboxes, and public folders, click 🔍 **Search,** and then do the following.

   a) In the **Search for** box, type the name of the item you want to find.

   b) In the **Modified** box, select the time period to which you want to restrict your search. The options are **Last 30 days** (default), **Last 6 months**, **Last year**, or **Custom**.

   c) Under **Filters**, specify where you want to search **Emails**, **Contacts**, **Calendars**, **Tasks**, and/or **Posts**.

   NOTE: You can refine the search criteria further by adding a **From address** for email and a **Company name** or **Email address** for contacts.

d) Select the items you want to restore, and then click **Select**.

8. To search for items in SharePoint sites and OneDrive accounts, click 🔍 **Search,** and then do the following.

   a) In the **Search for** box, type the name of the item you want to find.

   b) In the **Modified** box, select the time period to which you want to restrict your search. The options are **Last 30 days** (default), **Last 6 months**, **Last year**, or **Custom**.

   c) Select the items you want to restore, and then click **Select**.

9. In the **Restore Location** box, select one of the following options:

   - **Original** – Select this option to restore the item to its original source location.

   - **Alternate** – Select this option to restore the items to an alternate location, and then do the following:

     NOTE: Restoring to an alternate location is supported only for Exchange. Groups and Teams can be restored only to the original location.

     a) In the **Server** box, click ✏.

     b) In the **Server** box, type the IP address of the server to which the backup will be restored.

     c) Type the user name, password, and domain name for the server.

     d) In the **Destination Folder** column, type the path of the folder to which you want to restore the backup or click 📁 to select the folder.

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

     f) Under **Truncate destination folder path**, select the level by which you want to shorten the length of the destination folder path.

     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.

     c) Click **Save**.

10. To scan files for malware during the restore process, under **Antimalware scan**, slide the switch to **Enabled**.

> ***NOTE:*** Files detected with malware are not restored. A warning message appears in the Event Log and a copy of the infected files is placed in a password protected zip file in the quarantine folder.

11. Click **Restore**, and then do one of the following:
    - To confirm you want to restore the backup, click **Continue**.
    - If MFA has been enabled for **On-demand restore**, enter the six-digit authentication code you received, and click **Continue**.
    - If MPA has been enabled for **On-demand restore**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.
    - If MFA and MPA have been enabled for **On-demand restore**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

NOTE: To view the progress of the restore activity, click ⚙. For more information, see Section 8.5, “Viewing the Activity Monitor”, on page 145.

6.3 Microsoft Exchange Server backups

You can backup data on a Microsoft Exchange Server using the Microsoft VSS (Volume Shadow Copy Service) component on the destination computer to perform the online backup.

IMPORTANT: For a VSS aware backup, remote UAC is enabled by default. The local admin other than the built in admin, must have access to admin$ on the source machine. Failing to do this will display an error message.

6.3.1 Configuring a Microsoft Exchange Server backup

You can configure a Microsoft Exchange Server backup.

NOTE: If MFA and/or MPA has been enabled for **Edit backup**, you must enter an authentication code and/or require approval to complete the task.

To configure a Microsoft Exchange Server backup:

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

   NOTE: To search for a specific DS-Client based on the DS-Client number, type the DS-Client number in the search field, and then press **Enter**.

3. On the **Type & Components** page, do the following:
   a) In the **Backup set type** box, select **Microsoft Exchange Server (VSS aware)**.
   b) In the **Backup set name** box, type a name for the backup.
   c) In the **DS-System** box, select the DS-System.
   d) In the **Account** box, select the account.
   e) In the **DS-Client** box, select the DS-Client.
   f) Click **Next**.
4. On the **Credentials & Items** page, do the following:
   a) In the **Source IP address** box, type the IP address of the source computer containing the files you want to back up.
   b) Type the user name, password, and domain name.
   c) Under **Backup set items**, select the items you want to back up.
5. To configure advanced options, click ⚙ **Advanced Options**, and then do the following:
   a) In the **Compression algorithm** box, select the compression method you want to use for the backup. The options are as follows:
      - **LZOP** – A faster compression rate than ZLIB, but with less compression. This is a good default compression method when the network is not the bottleneck.

- **ZLIB** – A slower compression rate than LZOP, but with better compression. This is a good default compression method when the network is the bottleneck.

NOTE: There are four levels of ZLIB compression. ZLIB Global compresses global data that remains static during the life cycle of the application. ZLIB High = 9, ZLIB Medium = 6, ZLIB Low = 3.

b) In the **Stop on errors** box, enter the number of errors that must occur before the backup process is stopped. A value of 0 means the DS-Client will not stop a backup process regardless of the number of errors.

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

d) Under **Database backup policy**, in the **Full dump** box, select the method for the database dump. The options are as follows:

- **Always** – Performs a full dump of each database during each backup of the target server. This is the default option.
- **Plus Differential** – Performs 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** – Performs a full dump of the database on the first backup followed by incremental backups until another full dump is required. Specify the time interval between the database dumps.

e) To save the backed up data to a local storage location, select the **Save on local storage** check box. In the **Local storage path** box, type the path for the local storage location.

f) Click **OK**.

6. Click **Next or Save**.
7. On the **Schedule & Retention** page, do the following:

a) In the **Schedule** box, select a schedule for the backup.

- To view the details of the schedule, click 👁 **View**.
- To add a schedule, click + **Add Schedule**.
- To edit a schedule, select the schedule, and then click ✎ **Edit Schedule**.

b) In the **Retention rule** box, select a retention rule for the backup.

- To view details of the retention rule, click 👁 **View**.
- To add a retention rule, click + **Add Retention Rule**.

        - To edit a retention rule, select the retention rule, and then click ✏ **Edit Retention Rule**.

    c) If the schedule you selected has an associated restore task, you can schedule when the backup is restored. To schedule a restore, click 🕘 .

    d) Click **Next** or **Save**.

8. On the **Summary** page, review the settings for the backup.

    - To edit the name of the backup, click ✏.
    - To edit the advanced options, click ⚙ **Advanced Options.**
    - To view the details of the schedule, click 👁 **View**.
    - To view details of the retention rule, click 👁 **View**.

9. Click **Create** or **Save**.

10. If you have edited the backup, do one of the following:

    - To confirm you want to edit the backup, click **Continue**.
    - If MFA has been enabled for **Edit backup**, enter the six-digit authentication code you received, and click **Continue**.
    - If MPA has been enabled for **Edit backup**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.
    - If MFA and MPA have been enabled for **Edit backup**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

6.3.2 Restoring a Microsoft Exchange Server backup

You can restore data from a Microsoft Exchange Server backup.

NOTE: If MFA and/or MPA has been enabled for **On-demand restore**, you must enter an authentication code and/or require approval to complete the task.

To restore a Microsoft Exchange Server backup:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
3. Select the DS-System, account, and DS-Client.

   NOTE: To search for a specific DS-Client based on the DS-Client number, type the DS-Client number in the search field, and then press **Enter**.

4. Select the Microsoft Exchange Server backup you want to restore, and then click **Restore Backup Set**. You can restore only one backup at a time.
5. Beside **Backup session**, select the generation(s) of the backup you want to restore.By default, the latest generation is selected for restore.
6. Select the items you want to restore. To search for items, click 🔍 **Search,** and type the name of the backup.
7. In the **Restore Location** box, select one of the following options:
   - **Original** – Select this option to restore the item to its original source location.
   - **Alternate** – Select this option to restore the items to an alternate location, and then do the following:

     a) In the **Server** box, click ✎.

     b) In the **Server** box, type the IP address of the server to which the backup will be restored.

     c) Type the user name, password, and domain name for the server.

     d) Under **Destination details**, in the column **Destination Folder**, click 📁.

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

     f) Click **Save**.
8. To retain the database in restoring mode after the restore is complete, select the **Leave database in restoring state** check box.

9. Click **Restore**, and then do one of the following:
    - To confirm you want to restore the backup, click **Continue**.
    - If MFA has been enabled for **On-demand restore**, enter the six-digit authentication code you received, and click **Continue**.
    - If MPA has been enabled for **On-demand restore**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.
    - If MFA and MPA have been enabled for **On-demand restore**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

NOTE: To view the progress of the restore activity, click ⚙. For more information, see Section 8.5, “Viewing the Activity Monitor”, on page 145.

6.4 Microsoft Hyper-V Server backups

You can back up data on a Microsoft Hyper-V Server using the Microsoft VSS (Volume Shadow Copy Service) component on the destination computer to perform the online backup.

Each Microsoft Hyper-V virtual machine is presented as a component by the VSS writer. A component must be restored with all its contents, based on the rules specified in its metadata. For more information, see the *DS-Client User Guide*.

When performing a backup of a Microsoft Hyper-V Server (VSS-aware) backup, consider the following:

- 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).
- The backup unit is the Microsoft Hyper-V Server virtual machine (not individual files within the virtual machine). A Microsoft Hyper-V Server virtual machine is a group of files governed with strong data integration.
- 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.
- The GUID of the Microsoft Hyper-V Server virtual machine is the identifier for the virtual machine and is considered the name of the virtual machine. The name of the virtual machine can be saved as a description of the virtual machine. The virtual machine name might not be unique for all virtual machines in a host.

- Microsoft Hyper-V Server WMI APIs allow you to search for the virtual machines in a host server you want to back up. You can also select all virtual machines to be backed up.
- VSS provides a consistent interface that allows online backup of a Microsoft Hyper-V Server virtual machine.
- VSS-related metadata is saved with the backup data to provide the rules for data integration in each backed up virtual machine.
- Master, delta, and library files are supported for this type of backup.

IMPORTANT: When creating a VSS-aware backup, the source database cannot reside on an SMB remote share as this is currently not supported and can result in VSS snapshot failure.

6.4.1 Configuring a Microsoft Hyper-V Server backup

You can configure a Microsoft Hyper-V backup to back up a Microsoft Hyper-V Server in a standalone or cluster configuration. You must specify the type when you create the backup.

NOTE: If MFA and/or MPA has been enabled for **Edit backup**, you must enter an authentication code and/or require approval to complete the task.

To configure a Microsoft Hyper-V Server backup:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
   - To create a backup, click + **Create Backup Set**.
   - To edit a backup, select the DS-System, account, and DS-Client. Select the backup you want to edit, and then click ✎ **Edit Backup Set**.

   NOTE: To search for a specific DS-Client based on the DS-Client number, type the DS-Client number in the search field, and then press **Enter**.

3. On the **Type & Components** page, do the following:

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

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

c) In the **DS-System** box, select the DS-System.

d) In the **Account** box, select the account.

e) In the **DS-Client** box, select the DS-Client.

f) Click **Next**.

4. On the **Credentials & Items** page, do the following:

   a) In the **Source IP address** box, type the IP address of the source computer containing the files you want to back up.

   b) Type the user name, password, and domain name.

   c) Under **Backup set items**, select the items you want to back up.

5. To configure advanced options, click ⚙ **Advanced Options**, and then do the following:

   a) In the **Compression algorithm** box, select the compression method you want to use for the backup. The options are as follows:

      - **LZOP** – A faster compression rate than ZLIB, but with less compression. This is a good default compression method when the network is not the bottleneck.
      - **ZLIB** – A slower compression rate than LZOP, but with better compression. This is a good default compression method when the network is the bottleneck.

   NOTE: There are four levels of ZLIB compression. ZLIB Global compresses global data that remains static during the life cycle of the application. ZLIB High = 9, ZLIB Medium = 6, ZLIB Low = 3.

   b) In the **Stop on errors** box, type the number of errors that must occur before the backup process is stopped. A value of 0 means the DS-Client will not stop a backup process regardless of the number of errors.

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

   d) Under **Database backup policy**, in the **Full dump** box, select the method for the database dump. The options are as follows:

      - **Always** – Performs a full dump of each database during each backup of the target server. This is the default option.
      - **Plus Incremental** – Performs a full dump of the database on the first backup followed by incremental backups until another full dump is required. Specify the time interval between the database dumps.

   e) To restore individual files or directories of a virtual machine, select the **Enable File Level Restore (FLR)** check box.

   f) To save a copy of the backed up data to a local storage location, select the **Save on local storage** check box. In the **Local storage path** box, type the path for the local storage location.

   g) Click **OK.**

6. Click **Next** or **Save**.

7. On the **Schedule & Retention** page, do the following:

   a) In the **Schedule** box, select a schedule for the backup.

      - To view the details of the schedule, click 👁 **View**.
      - To add a schedule, click + **Add Schedule**.
      - To edit a schedule, select the schedule, and then click ✎ **Edit Schedule**.

   b) In the **Retention rule** box, select a retention rule for the backup.

      - To view details of the retention rule, click 👁 **View**.
      - To add a retention rule, click + **Add Retention Rule**.
      - To edit a retention rule, select the retention rule, and then click ✎ **Edit Retention Rule**.

   c) If the schedule you selected has an associated restore task, you can schedule when the backup is restored. To schedule a restore, click 🕓 .

   d) Click **Next** or **Save**.

8. On the **Summary** page, review the settings for the backup.

   - To edit the name of the backup, click ✎.
   - To edit the advanced options, click ⚙ **Advanced Options.**
   - To view the details of the schedule, click 👁 **View**.
   - To view details of the retention rule, click 👁 **View**.

9. Click **Create** or **Save**.

10. If you have edited the backup, do one of the following:

    - To confirm you want to edit the backup, click **Continue**.
    - If MFA has been enabled for **Edit backup**, enter the six-digit authentication code you received, and click **Continue**.
    - If MPA has been enabled for **Edit backup**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.
    - If MFA and MPA have been enabled for **Edit backup**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

6.4.2 Restoring a Microsoft Hyper-V Server backup

You can restore data from a Microsoft Hyper-V Server backup.

NOTE: If MFA and/or MPA has been enabled for **On-demand restore**, you must enter an authentication code and/or require approval to complete the task.

To restore a Microsoft Hyper-V Server backup:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
3. Select the DS-System, account, and DS-Client.

   NOTE: To search for a specific DS-Client based on the DS-Client number, type the DS-Client number in the search field, and then press **Enter**.

4. Select the Microsoft Hyper-V Server backup you want to restore, and then click **Restore Backup Set**. You can restore only one backup at a time.
5. Beside **Backup session**, select the generation(s) of the backup you want to restore. By default, the latest generation is selected for restore.
6. Beside **Restore method**, select a method to restore the backup. The options are as follows:
   - To restore the entire Microsoft Hyper-V Server, select **Full**.
   - To restore individual files or folders of a virtual machine, select **File-level**.

   NOTE: File-level restore is available if the backup was backed up with the Enable File Level Restore (FLR) option.

7. Select the items you want to restore. To search for items, click 🔍 **Search,** and then type the name of the backup.
8. In the **Restore Location** box, select one of the following options:
   - **Original** – Select this option to restore the item to its original source location.
   - **Alternate** – Select this option to restore the items to an alternate location, and then do the following:
     a) In the **Server** box, click ✎.
     b) In the **Server** box, type the IP address of the server to which the backup will be restored.

c) Type the user name, password, and domain/computer name for the server.

d) To change the destination folder, under **Rename components**, select a component, click ✏, and then type the path.

e) Click **Save**.

9. Click **Restore**, and then do one of the following:

    - To confirm you want to restore the backup, click **Continue**.
    - If MFA has been enabled for **On-demand restore**, enter the six-digit authentication code you received, and click **Continue**.
    - If MPA has been enabled for **On-demand restore**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.
    - If MFA and MPA have been enabled for **On-demand restore**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

NOTE: To view the progress of the restore activity, click ⚙. For more information, see Section 8.5, “Viewing the Activity Monitor”, on page 145.

6.5 Microsoft SharePoint Server backups

You can backup and restore from a Microsoft SharePoint Server using the Microsoft Volume Shadow Copy Service (VSS) component on the target computer.

Before working with Microsoft SharePoint server (VSS-aware) backups, ensure the following requirements are met.

- The account running the VSS writers on all target server instances for backup and restore must be a member of the Domain Administrators group.
- The account must have permission to issue BACKUP DATABASE and RESTORE DATABASE commands to the target database servers.
- The account must have permission to access the Microsoft SQL Server, which requires it to be a member of the SQL Server administrator group with db_creator and sysadmin roles.
- The VSS writer must be registered in the Windows registry by running the following command:

```
STSADM -o registerwsswriter
```

IMPORTANT: For a VSS aware backup, remote UAC is enabled by default. The local admin other than the built in admin, must have access to admin$ on the source machine. Failing to do this will display an error message.

6.5.1 Configuring a Microsoft SharePoint Server backup

You can configure a Microsoft SharePoint Server backup.

NOTE: If MFA and/or MPA has been enabled for **Edit backup**, you must enter an authentication code and/or require approval to complete the task.

To configure a Microsoft SharePoint Server backup:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
   - To create a backup, click + **Create Backup Set**.
   - To edit a backup, select the DS-System, account, and DS-Client. Select the backup you want to edit, and then click ✎ **Edit Backup Set**.

   NOTE: To search for a specific DS-Client based on the DS-Client number, type the DS-Client number in the search field, and then press **Enter**.

3. On the **Type & Components** page, do the following:
   a) In the **Backup set type** box, select **Microsoft SharePoint Server (VSS aware)**.
   b) In the **Backup set name** box, type a name for the backup.
   c) In the **DS-System** box, select the DS-System.
   d) In the **Account** box, select the account.
   e) In the **DS-Client** box, select the DS-Client.
   f) Click **Next**.
4. On the **Credentials & Items** page,
   a) In the **Source IP address** box, type the IP address of the source computer containing the files you want to back up.
   b) Type the user name, password, and domain name.

5. Under **Backup set items**, select the items you want to back up.

6. To configure advanced options, click **Advanced Options**, and then do the following:

   a) In the **Compression algorithm** box, select the compression method you want to use for the backup. The options are as follows:

      - **LZOP** – A faster compression rate than ZLIB, but with less compression. This is a good default compression method when the network is not the bottleneck.

      - **ZLIB** – A slower compression rate than LZOP, but with better compression. This is a good default compression method when the network is the bottleneck.

   NOTE: There are four levels of ZLIB compression. ZLIB Global compresses global data that remains static during the life cycle of the application. ZLIB High = 9, ZLIB Medium = 6, ZLIB Low = 3.

   b) In the **Stop on errors** box, enter the number of errors that must occur before the backup process is stopped. A value of 0 means the DS-Client will not stop a backup process regardless of the number of errors.

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

   d) Under **Database backup policy**, in the **Full dump** box, select the method for the database dump. The options are as follows:

      - **Always** – Performs a full dump of each database during each backup of the target server. This is the default option.

      - **Plus Differential** – Performs 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.

   e) To save a copy of the backed up data to a local storage location, select the **Save on local storage** check box. In the **Local storage path** box, type the path for the local storage location.

   f) Click **OK**.

7. Click **Next** or **Save**.

8. On the **Schedule & Retention** page, do the following:

   a) In the **Schedule** box, select a schedule for the backup.

      - To view the details of the schedule, click **View**.

      - To add a schedule, click **Add Schedule**.

      - To edit a schedule, select the schedule, and then click **Edit Schedule**.

   b) In the **Retention rule** box, select a retention rule for the backup.

      - To view details of the retention rule, click 👁 **View**.
      - To add a retention rule, click ➕ **Add Retention Rule**.
      - To edit a retention rule, select the retention rule, and then click ✏ **Edit Retention Rule**.

   c) If the schedule you selected has an associated restore task, you can schedule when the backup is restored. To schedule a restore, click 🕓 .

   d) Click **Next** or **Save**.

9. On the **Summary** page, review the settings for the backup.

   - To edit the name of the backup, click ✏.
   - To edit the advanced options, click ⚙ **Advanced Options.**
   - To view the details of the schedule, click 👁 **View**.
   - To view details of the retention rule, click 👁 **View**.

10. Click **Create** or **Save**.

11. If you have edited the backup, do one of the following:

    - To confirm you want to edit the backup, click **Continue**.
    - If MFA has been enabled for **Edit backup**, enter the six-digit authentication code you received, and click **Continue**.
    - If MPA has been enabled for **Edit backup**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.
    - If MFA and MPA have been enabled for **Edit backup**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

6.5.2 Restoring a Microsoft SharePoint Server backup

You can restore data from a Microsoft SharePoint Server backup.

NOTE: If MFA and/or MPA has been enabled for **On-demand restore**, you must enter an authentication code and/or require approval to complete the task.

To restore a Microsoft SharePoint Server backup:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
3. Select the DS-System, account, and DS-Client.

   NOTE: To search for a specific DS-Client based on the DS-Client number, type the DS-Client number in the search field, and then press **Enter**.

4. Select the Microsoft SharePoint Server backup you want to restore, and then click **Restore Backup Set**. You can restore only one backup at a time.
5. Beside **Backup session**, select the generation(s) of the backup you want to restore. By default, the latest generation is selected for restore.
6. Select the backup or individual files/directories you want to restore. To search for items, click **Search,** and type the name of the backup.
7. In the **Restore Location** box, select one of the following options:
   - **Original** – Select this option to restore the item to its original source location.
   - **Alternate** – Select this option to restore the items to an alternate location, and then do the following:
     a) In the **Server** box, click .
     b) In the **Server** box, type the IP address of the server to which the backup will be restored.
     c) Type the user name, password, and domain name for the server.
     d) To change the destination folder, under **Rename components**, select a component, click , and then type the path.
     e) Click **Save**.
8. Click **Restore**, and then do one of the following:
   - To confirm you want to restore the backup, click **Continue**.
   - If MFA has been enabled for **On-demand restore**, enter the six-digit authentication code you received, and click **Continue**.

- If MPA has been enabled for **On-demand restore**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.
- If MFA and MPA have been enabled for **On-demand restore**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

NOTE: To view the progress of the restore activity, click ⚙. For more information, see Section 8.5, “Viewing the Activity Monitor”, on page 145.

6.6 Microsoft SQL Server backups

You can back up a Microsoft SQL Server database.The first backup is always a full database dump and subsequent backups are incremental forever.

IMPORTANT: For a VSS aware backup, remote UAC is enabled by default. The local admin other than the built in admin, must have access to admin$ on the source machine. Failing to do this will display an error message.

6.6.1 Configuring a Microsoft SQL Server backup

You can configure a Microsoft SQL server backup.

NOTE: If MFA and/or MPA has been enabled for **Edit backup**, you must enter an authentication code and/or require approval to complete the task.

To configure a Microsoft SQL server backup:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
   - To create a backup, click + **Create Backup Set**.
   - To edit a backup, select the DS-System, account, and DS-Client. Select the backup you want to edit, and then click ✎ **Edit Backup Set**.

   NOTE: To search for a specific DS-Client based on the DS-Client number, type the DS-Client number in the search field, and then press **Enter**.

3. On the **Type & Components** page, do the following:

4. In the **Backup set type** box, select a database from the following:

   - **Microsoft SQL Server (Classic)**
   - **Microsoft SQL Server (VSS aware)**

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

   b) In the **DS-System** box, select the DS-System.

   c) In the **Account** box, select the account.

   d) In the **DS-Client** box, select the DS-Client.

5. Click **Next**.

6. On the **Credentials & Items** page, do the following:

   a) In the **Source IP address** box type the IP address of the source computer containing the files you want to back up.

   b) For Microsoft SQL Server (Classic), do one of the following:

      - To use the DS-Client credentials to connect to the local DS-Client computer, select **Use DS-Client credentials**, and then type the database user name and database password.
      - To use other credentials, select **Use network credentials**, and then type the user name, password, domain, database user name, and database password.
      - In the **Database Dump Path** box, select a location for the database dump. To save the dump file on the local storage of the DS-Client computer, select **DS-Client Buffer**.To dump large databases to a file, select **DS-Client Pipe**. During a backup, the DS-Client reads from the pipe on the source database.To dump the database in a directory on the remote database server computer, select **Database Server**, 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.

   c) For Microsoft SQL Server (VSS-aware), type the user name, password, and domain name.

   d) Under **Backup set items**, select the items you want to back up.

7. To configure advanced options, click **Advanced Options**, and then do the following:

   a) In the **Compression algorithm** box, select the compression method you want to use for the backup. The options are as follows:

      - **LZOP** – A faster compression rate than ZLIB, but with less compression. This is a good default compression method when the network is not the bottleneck.

- **ZLIB** – A slower compression rate than LZOP, but with better compression. This is a good default compression method when the network is the bottleneck.

NOTE: There are four levels of ZLIB compression. ZLIB Global compresses global data that remains static during the life cycle of the application. ZLIB High = 9, ZLIB Medium = 6, ZLIB Low = 3.

---

b) In the **Stop on errors** box, type the number of errors that must occur before the backup process is stopped. A value of 0 means the DS-Client will not stop a backup process regardless of the number of errors.

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

d) Under **Database backup policy**, in the **Full dump** box, select the method for the database dump. The options are as follows:

- **Always** – Performs a full dump of each database during each backup of the target server. This is the default option.
- **Plus Differential** – Performs 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.
- **Transaction log only** – Performs a back up of transaction logs for selected databases to be used in combination with full dumps taken by another Microsoft SQL Server (Classic) backup.

NOTE: To dump the transaction log and send it to DS-System, select the **Backup Transaction Log** check box.

---

e) To save a copy of the backed up data to a local storage location, select the **Save on local storage** check box. In the **Local storage path** box, type the path for the local storage location.

f) Click **OK**.

8. Click **Next** or **Save**.

9. On the **Schedule & Retention** page, do the following:

a) In the **Schedule** box, select a schedule for the backup.

- To view the details of the schedule, click 👁 **View**.
- To add a schedule, click + **Add Schedule**.
- To edit a schedule, select the schedule, and then click ✎ **Edit Schedule**.

b) In the **Retention rule** box, select a retention rule for the backup.

        - To view details of the retention rule, click 👁 **View**.
        - To add a retention rule, click + **Add Retention Rule**.
        - To edit a retention rule, select the retention rule, and then click ✏ **Edit Retention Rule**.

    c) If the schedule you selected has an associated restore task, you can schedule when the backup is restored. To schedule a restore, click 🕓 .

    d) Click **Next** or **Save**.

10. On the **Summary** page, review the settings for the backup.
    - To edit the name of the backup, click ✏.
    - To edit the advanced options, click ⚙ **Advanced Options.**
    - To view the details of the schedule, click 👁 **View**.
    - To view details of the retention rule, click 👁 **View**.
11. Click **Create** or **Save**.
12. If you have edited the backup, do one of the following:
    - To confirm you want to edit the backup, click **Continue**.
    - If MFA has been enabled for **Edit backup**, enter the six-digit authentication code you received, and click **Continue**.
    - If MPA has been enabled for **Edit backup**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.
    - If MFA and MPA have been enabled for **Edit backup**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

6.6.2 Restoring a Microsoft SQL Server backup

You can restore data from a Microsoft SQL Server backup.

NOTE: If MFA and/or MPA has been enabled for **On-demand restore**, you must enter an authentication code and/or require approval to complete the task.

To restore a Microsoft SQL Server backup:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
3. Select the DS-System, account, and DS-Client.

   NOTE: To search for a specific DS-Client based on the DS-Client number, type the DS-Client number in the search field, and then press **Enter**.

4. Select the Microsoft SQL Server backup you want to restore, and then click ⟲ **Restore Backup Set**. You can restore only one backup at a time.
5. Beside **Backup session**, select the generation(s) of the backup you want to restore. By default, the latest generation is selected for restore.
6. Select the items you want to restore. To search for items, click 🔍 **Search,** and type the name of the backup.
7. In the **Restore Location** box, select one of the following options:
   - **Original** – Select this option to restore the item to its original source location.
   - **Alternate** – Select this option to specify an alternate destination for the restore items, and then do the following: When restoring to an alternate location, you have three options:

     a) In the **Server** box, click ✎.

     b) In the **Server** box, type the IP address of the server to which the backup will be restored.

     c) Type the user name, password, and domain name or computer name for the server.

     d) Type the credentials for the database in the **Database user name** and **Database password** boxes.

     e) Under **Destination details**, in the column **Destination Folder**, click 📁, and select the folder to which you want to restore the backup.

     f) Click **Save**.
8. Click **Restore**, and then do one of the following:

- To confirm you want to restore the backup, click **Continue**.
- If MFA has been enabled for **On-demand restore**, enter the six-digit authentication code you received, and click **Continue**.
- If MPA has been enabled for **On-demand restore**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.
- If MFA and MPA have been enabled for **On-demand restore**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

NOTE: To view the progress of the restore activity, click ⚙. For more information, see Section 8.5, “Viewing the Activity Monitor”, on page 145.

6.7 Permissions backups

You can 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 you back up an online File system backup, the files are saved with the current permissions and attributes. If the permissions or attributes change but the content of the files remains the same, DS-Client does not backup the changes to DS-System. With a Permissions backup, changes to attributes such as Compress, Read-Only, Hidden, Archive, and Index are detected and backed up.

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

6.7.1 Configuring a permissions backup

You can configure a permissions backup.

> ***NOTE:*** If MFA and/or MPA has been enabled for **Edit backup**, you must enter an authentication code and/or require approval to complete the task.

To configure a permissions backup:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
   - To create a backup, click ⊕ **Create Backup Set**.
   - To edit a backup, select the DS-System, account, and DS-Client. Select the backup you want to edit, and then click ✎ **Edit Backup Set**.

   > ***NOTE:*** To search for a specific DS-Client based on the DS-Client number, type the DS-Client number in the search field, and then press **Enter**.

3. On the **Type & Components** page, do the following:

   a) In the **Backup set type** box, select **Permissions**.

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

   c) In the **DS-System** box, select the DS-System.

   d) In the **Account** box, select the account.

   e) In the **DS-Client** box, select the DS-Client.

   f) Click **Next**.

4. On the **Credentials & Items** page, do the following:

   a) In the **Source IP address** box, type the IP address of the source computer containing the files you want to back up.

   b) To use the DS-Client credentials to connect to the local DS-Client computer, select **Use DS-Client Credentials**.

   c) To use other credentials, select **Use network credentials** and then type the user name and password.

   > ***NOTE:*** You must connect using an Administrator or equivalent account.

   d) Under **Backup set items**, select the items you want to back up.

5. To configure advanced options, click ⚙ **Advanced Options**, and then do the following:

   a) In the **Compression algorithm** box, select the compression method you want to use for the backup. The options are as follows:

      - **LZOP** – A faster compression rate than ZLIB, but with less compression. This is a good default compression method when the network is not the bottleneck.

      - **ZLIB** – A slower compression rate than LZOP, but with better compression. This is a good default compression method when the network is the bottleneck.

   NOTE: There are four levels of ZLIB compression. ZLIB Global compresses global data that remains static during the life cycle of the application. ZLIB High = 9, ZLIB Medium = 6, ZLIB Low = 3.

   b) In the **Stop on errors** box, enter the number of errors that must occur before the backup process is stopped. A value of 0 means the DS-Client will not stop a backup process regardless of the number of errors.

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

   d) 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 sends the files from the DS-Client buffer to the DS-System.

   e) To save a copy of the backed up data to a local storage location, select the **Save on local storage** check box. In the **Local storage path** box, type the path for the local storage location.

   f) Click **OK**.

6. Click **Next** or **Save**.

7. On the **Schedule & Retention** page, do the following:

   a) In the **Schedule** box, select a schedule for the backup.

      - To view the details of the schedule, click 👁 **View**.

      - To add a schedule, click + **Add Schedule**.

      - To edit a schedule, select the schedule, and then click ✎ **Edit Schedule**.

   b) In the **Retention rule** box, select a retention rule for the backup.

      - To view details of the retention rule, click 👁 **View**.

      - To add a retention rule, click + **Add Retention Rule**.

      - To edit a retention rule, select a retention rule, and then click ✎ **Edit Retention Rule**.

c) If the schedule you selected has an associated restore task, you can schedule when the backup is restored. To schedule a restore, click ⟲ .

d) Click **Next** or **Save**.

8. On the **Summary** page, review the settings for the backup.
   - To edit the name of the backup, click ✎.
   - To edit the advanced options, click ⚙ **Advanced Options.**
   - To view the details of the schedule, click 👁 **View**.
   - To view details of the retention rule, click 👁 **View**.
9. Click **Create** or **Save**.
10. If you have edited the backup, do one of the following:
    - To confirm you want to edit the backup, click **Continue**.
    - If MFA has been enabled for **Edit backup**, enter the six-digit authentication code you received, and click **Continue**.
    - If MPA has been enabled for **Edit backup**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.
    - If MFA and MPA have been enabled for **Edit backup**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

6.7.2 Restoring a permissions backup

You can restore data from a permissions backup.

NOTE: If MFA and/or MPA has been enabled for **On-demand restore**, you must enter an authentication code and/or require approval to complete the task.

To restore a permissions backup:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
3. Select the DS-System, account, and DS-Client.

   NOTE: To search for a specific DS-Client based on the DS-Client number, type the DS-Client number in the search field, and then press **Enter**.

4. Select the permissions backup you want to restore, and then click **Restore Backup Set**. You can restore only one backup at a time.
5. Beside **Backup session**, select the generation(s) of the backup you want to restore. By default, the latest generation is selected for restore.
6. Select the items you want to restore. To search for items, click 🔍 **Search,** and then type the name of the backup.
7. In the **Restore Location** box, select one of the following options:
   - **Original** – Select this option to restore the item to its original source location.
   - **Alternate** – Select this option to specify an alternate destination for the restore items, and then do the following: When restoring to an alternate location, you have three options:
     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 will be restored.
     c) Type the user name, password, and domain name or computer name for the server.
     d) Under **Destination details**, in the column **Destination Folder**, click 📁.
     e) In the **Select the destination folder** dialog box, select the folder to which you want to restore the backup, and then click **Select**.
     f) Click **Save**.

8. Click **Restore**, and then do one of the following:

   - To confirm you want to restore the backup, click **Continue**.
   - If MFA has been enabled for **On-demand restore**, enter the six-digit authentication code you received, and click **Continue**.
   - If MPA has been enabled for **On-demand restore**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.
   - If MFA and MPA have been enabled for **On-demand restore**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

NOTE: To view the progress of the restore activity, click ⚙. For more information, see Section 8.5, “Viewing the Activity Monitor”, on page 145.

6.8 VMware vCenter Server backups

You can back up and restore virtual machines on a VMware vCenter Server using the native VMware vCenter Storage APIs - Data Protection (VADP).

Before working with VMware vCenter Server backups, ensure the following requirements are met:

- For application consistent backups, ensure VMware Tools is installed on the guest operating system of the virtual machine.
- Firewalls are configured correctly and allow the DS-Client to communicate with the vCenter and the each ESXi host of the cluster via port #902.
- If an ESXi host is added with the DNS name of the VMware vCenter Server, the DS-Client machine must have name resolution to the ESXi host to back up or restore the virtual machines.
- To restore to an alternate location, the DS-Client must have network access to the destination VMware vCenter Server and all involved ESXi hosts.

To perform a backup or restore of a VMware vCenter Server backup, you must create a user role with the following permissions:

- Datastore: Allocate space
- Datastore: Browse datastore
- Datastore: Low level file operation
- Folder: Create folder
- Global: Disable methods
- Global: Enable methods

- Global: Licenses
- Network: Assign network
- Resource: Assign virtual machine to resource pool
- Resource: Create resource pool
- Virtual machine: Change Configuration (with all sub-options)
- Virtual machine: Edit Inventory: Create new
- Virtual machine: Edit Inventory: Register
- Virtual machine: Edit Inventory: Unregister
- Virtual machine: Interaction: Power off
- Virtual machine: Interaction: Power on
- Virtual machine: Provisioning: Allow disk access
- Virtual machine: Provisioning: Allow read-only disk access
- Virtual machine: Provisioning: Allow virtual machine download
- Virtual machine: Provisioning: Allow virtual machine files upload
- Virtual machine: Snapshot management (with all sub-options)

Each user assigned to this role requires access to the following levels of the VMware vCenter Server:

- vCenter
- Datacenter
- Cluster
- Host
- Datastore
- Network interface

Under VMs and Templates, select the folder containing the virtual machines to be backed up, and then add the user and assign the Administrator role to allow Web GUI full control access to the folder. To be able to back up subfolders, select the "Propagate to children" option.

NOTE: To prevent users from having access to all underlying levels, clear the “Propagate to children” option for each level.

6.8.1 Configuring a VMware vCenter Server backup

You can configure a VMware vCenter Server backup.

NOTE: If MFA and/or MPA has been enabled for **Edit backup**, you must enter an authentication code and/or require approval to complete the task.

To configure a VMware vCenter Server backup:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
    - To create a backup, click ⊕ **Create Backup Set**.
    - To edit a backup, select the DS-System, account, DS-Client. Select the backup you want to edit, and then click ✎ **Edit Backup Set**.

    NOTE: To search for a specific DS-Client based on the DS-Client number, type the DS-Client number in the search field, and then press **Enter**.

3. On the **Type & Components** page, do the following:
    a) In the **Backup set type** box, select **VMware vCenter Server**.
    b) In the **Backup set name** box, type a name for the backup.
    c) In the **DS-System** box, select the DS-System.
    d) In the **Account** box, select the account.
    e) In the **DS-Client** box, select the DS-Client.
    f) Click **Next**.
4. On the **Credentials & Items** page, do the following:
    a) In the **VMware vCenter Server credentials** box, select the source computer containing the files you want to back up.
        - To add a VMware vCenter Server credential, click +. Enter the host IP address, select an account credential, type the VMware vCenter Server credential name, and then click **Add**.
        - To edit a VMware vCenter Server credential, click ✎. You can only add or edit an account credential.

    b) Under **Backup set items**, select the items you want to back up.
5. To configure advanced options, click ⚙ **Advanced Options**, and then do the following:

a) In the **Compression algorithm** box, select the compression method you want to use for the backup. The options are as follows:

- **LZOP** – A faster compression rate than ZLIB, but with less compression. This is a good default compression method when the network is not the bottleneck.
- **ZLIB** – A slower compression rate than LZOP, but with better compression. This is a good default compression method when the network is the bottleneck.

NOTE: There are four levels of ZLIB compression. ZLIB Global compresses global data that remains static during the life cycle of the application. ZLIB High = 9, ZLIB Medium = 6, ZLIB Low = 3.

b) In the **Stop on errors** box, enter the number of errors that must occur before the backup process is stopped.A value of 0 means the DS-Client will not stop a backup process regardless of the number of errors.

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

d) To restore individual files or directories of one or more multiple virtual machines, select the **Enable File Level Restore (FLR)** check box.

e) To back up the virtual machine state, including running programs loaded in memory, select the **Backup Virtual Machine Memory** check box.

NOTE: This ensures the state of the target machine matches the state of the source machine. The target machine is automatically powered off and functions as a standby machine to avoid network conflicts.

f) To use Changed Block Tracking (CBT), select the **Enable Changed Block Tracking (CBT)** check box.

g) To specify the number of generations after which the system should verify the disk signature, select the **Verify disks signature interval (generations)** check box, and then enter the number of generations.

h) To specify on which days the system should verify the disk signature, clear the **Verify disks signature interval (generations)** check box, and then select the days on which you want the process to be performed.

NOTE: This Verify disks signature option is available only if you have enabled Changed Block Tracking (CBT).

i) To save a copy of the backed up data to a local storage location, select the **Save on local storage** check box. In the **Local storage path** box, type the path for the local storage location.

> ***NOTE:*** To perform FLR from a local storage location on a Linux DS-Client, you must enable both the FLR and CBT options.

j) Click **OK**.

6. Click **Next** or **Save**.
7. On the **Schedule & Retention** page, do the following:

   a) In the **Schedule** box, select a schedule for the backup.

   - To view the details of the schedule, click **View**.
   - To add a schedule, click + **Add Schedule**.
   - To edit a schedule, select the schedule, and then click **Edit Schedule**.

   b) In the **Retention rule** box, select a retention rule for the backup.

   - To view details of the retention rule, click **View**.
   - To add a retention rule, click + **Add Retention Rule**.
   - To edit a retention rule, select the retention rule, and then click **Edit Retention Rule**.

   c) If the schedule you selected has an associated restore task, you can schedule when the backup is restored. To schedule a restore, click .

   d) Click **Next** or **Save**.

8. On the **Summary** page, review the settings for the backup.

   - To edit the name of the backup, click .
   - To edit the advanced options, click **Advanced Options.**
   - To view the details of the schedule, click **View**.
   - To view details of the retention rule, click **View**.

9. Click **Create** or **Save**.
10. If you have edited the backup, do one of the following:

    - To confirm you want to edit the backup, click **Continue**.
    - If MFA has been enabled for **Edit backup**, enter the six-digit authentication code you received, and click **Continue**.
    - If MPA has been enabled for **Edit backup**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

- If MFA and MPA have been enabled for **Edit backup**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

6.8.2 Restoring a VMware vCenter Server backup

You can restore data from a VMware vCenter Server backup.

NOTE: If MFA and/or MPA has been enabled for **On-demand restore**, you must enter an authentication code and/or require approval to complete the task.

To restore a VMware vCenter Server backup:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
3. Select the DS-System, account, and DS-Client.

   NOTE: To search for a specific DS-Client based on the DS-Client number, type the DS-Client number in the search field, and then press **Enter**.

4. Select the VMware vCenter Server backup you want to restore, and then click **Restore Backup Set**.

   NOTE: We recommend restoring only one backup at a time. Restoring multiple backups concurrently can affect performance.

5. Beside **Backup session**, select the generation(s) of the backup you want to restore. By default, the latest generation is selected for restore.
6. Beside **Restore method**, select a restore level. The options are as follows:
   - To restore an entire virtual machine, select **VM-level**.
   - To restore files, select **File-level**.
7. Select the items you want to restore. To search for items, click **Search,** and then type the name of the backup.
8. In the **Restore Location** box, select one of the following options:
   - **Original** – Select this option to restore the item to its 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 **VMware Cloud Director** box, select the VMware Cloud Director to which you want to restore the backup. Click + to add a VMware Cloud Director Server, or click ✎ to edit a VMware vCenter Server.

   c) In the **Account credentials** box, select the corresponding cloud credential for the selected VMware Cloud Director. Click + to add an account credential or click ✎ to edit an account credential.

   d) Under **Destination details**, select the source VM, the organization, the vApp, the destination VM, and the network to which you want to restore the backup.

   e) Click **Save**.

9. To power on the virtual machine after the restore is complete, select the **Power on virtual machine after restore** check box. For more information, see Section 6.8.3, “Powering on a virtual machine after restore”, on page 118.

10. To add a time stamp of the restore process to the name of the virtual machine, select the **Add time stamp to virtual machine name** check box.

11. Click **Restore**, and then do one of the following:

    - To confirm you want to restore the backup, click **Continue**.
    - If MFA has been enabled for **On-demand restore**, enter the six-digit authentication code you received, and click **Continue**.
    - If MPA has been enabled for **On-demand restore**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.
    - If MFA and MPA have been enabled for **On-demand restore**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

NOTE: To view the progress of the restore activity, click ⚙. For more information, see Section 8.5, “Viewing the Activity Monitor”, on page 145.

6.8.3 Powering on a virtual machine after restore

A virtual machine can be powered on after restore using the **Power on virtual machine after restore** option and manually performing either pre-configuration on the source virtual machine or post-configuration on the restored virtual machine.

Performing pre-configuration on the source virtual machine:

1. On the VMware vCenter Server, do the following:

   a) Click **Network adapter** of the virtual machine and then select the **Distributed Switch** network configured on the VMware vCenter Server.

   b) Set the MAC address allocation to **Automatic**.

2. On the VMware vCenter Server, do the following:

   a) Click **Properties** for the virtual machine and then select the **Network** mapped to the VMware vCenter Server.

   b) Power on the virtual machine and ensure it gets powered on successfully.

Performing post-configuration on the restored virtual machine:

1. On the VMware vCenter Server, do the following:

   a) Click **Network adapter** of the restored virtual machine and then select the **Distributed Switch** network configured on the VMware vCenter Server.

   b) Set the MAC address allocation to **Automatic**.

2. On the VMware vCenter Server, do the following:

   a) Click **Properties** for the virtual machine and then select the **Network** mapped to the VMware vCenter Server.

   b) Under **MAC Address**, select **Reset**.

3. Power on the restored virtual machine.

6.9 VMware Cloud Director backups

You can back up virtual data centers. When creating or performing a backup or restore of a VMware Cloud Director backup, you require the following permissions.

- General: Administration View
- Organization VDC Network: View Properties
- Organization VDC: View Organization VDCs
- Organization VDC: View Compute Policies for an Organization VDC
- Organization: View Organizations
- Organization: View Organization Networks
- vApp: Create/Reconfigure a vApp
- vApp: Edit vApp Properties
- vApp: Edit VM Network
- vApp: Edit VM Properties
- vApp: Start/Stop/Suspend/Reset a vApp

The DS-Client automatically places the vApp in maintenance mode to perform a backup or restore and automatically takes the vApp out of maintenance mode when the backup or restore process has completed.

If there is an issue during the backup or restore process that causes the vApp to remain in maintenance mode, you can run the **test_libvcd** utility to exit vApp maintenance mode. The utility is located in the following folder:

```
\Program Files\CloudBackup\DS-Client\
```

To exit vApp maintenance mode, run the following command with the utility:

- On Windows:

  ```
  <DS-Client Path>\libvcd_test.exe -leave-maintenance-mode
  -address <vCloud Address> -user <USER> -password <PASSWORD>
  ```

- On Linux:

  ```
  /<DS-Client Path>/lib/test_libvcd -leave-maintenance-mode
  -address <vCloud Address> -user <USER> -password <PASSWORD>
  ```

6.9.1 Configuring a VMware Cloud Director backup

You can configure a VMware Cloud Director backup.

NOTE: If MFA and/or MPA has been enabled for **Edit backup**, you must enter an authentication code and/or require approval to complete the task.

To configure a VMware Cloud Director backup:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
   - To create a backup, click ⊕ **Create Backup Set**.
   - To edit a backup, select the DS-System, account, DS-Client, the backup, and then click ✎ **Edit Backup Set**.
3. On the **Type & Components** page, do the following:

   a) In the **Backup set type** box, select **VMware Cloud Director**.

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

   NOTE: Quotation marks **[“]** are not supported in the VMware Cloud Director name.

   ---

   c) In the **DS-System** box, select the DS-System.

   d) In the **Account** box, select the account.

   e) In the **DS-Client** box, select the DS-Client.
4. On the **Credentials & Items** page, do the following:

   a) In the **VMware Cloud Director Server Credentials** box, select a VMware Cloud Director.

   - To add a VMware Cloud Director, click + **Add Cloud Director**. Type the host or IP address of the source computer from which the VMware Cloud Director will be backed up, account credential, VMware Cloud Director name, and then click **Next**.
   - To edit a VMware Cloud Director, click ✎ **Edit Cloud Director**.

   NOTE: The credentials must have administrator privileges for the VMware Cloud Director.

   ---

   b) In the **Account credentials** box, select an account credential with system or organization administrator privileges.

- To add an account credential, click + **Add Account Credential**. Type the user name, password for the DS-Client computer from which the VMware Cloud Director will be backed up, credential name, description, and then click **Add**.

- To edit an account credential, click ✎ **Edit Account Credential**.

c) Under **Backup set items**, select the items you want to back up.

5. To configure advanced options, click ⚙ **Advanced Options**, and then do the following:

   a) In the **Compression algorithm** box, select the compression method you want to use for the backup. The options are as follows:

      - **LZOP** – A faster compression rate than ZLIB, but with less compression. This is a good default compression method when the network is not the bottleneck.

      - **ZLIB** – A slower compression rate than LZOP, but with better compression. This is a good default compression method when the network is the bottleneck.

   NOTE: There are four levels of ZLIB compression. ZLIB Global compresses global data that remains static during the life cycle of the application. ZLIB High = 9, ZLIB Medium = 6, ZLIB Low = 3.

   b) In the **Stop on errors** box, enter the number of errors that must occur before the backup process is stopped. A value of 0 means the DS-Client will not stop a backup process regardless of the number of errors.

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

   d) To restore individual files or directories of one or more multiple virtual machines, select the **Enable File Level Restore (FLR)** check box.

   e) To use Changed Block Tracking (CBT), select the **Enable Changed Block Tracking (CBT)** check box.

   f) To specify the number of generations after which the system should verify the disk signature, select the **Verify disks signature interval (generations)** check box, and then enter the number of generations.

   g) To specify on which days the system should verify the disk signature, clear the **Verify disks signature interval (generations)** check box, and then select the days on which you want the process to be performed.

   NOTE: This Verify disks signature option is available only if you have enabled Changed Block Tracking (CBT).

h) To save a copy of the backed up data to a local storage location, select the **Save on local storage** check box. In the **Local storage path** box, type the path for the local storage location.

> ***NOTE:*** To perform FLR from a local storage location on a Linux DS-Client, you must enable both the FLR and CBT options.

i) Click **OK**.

6. Click **Next** or **Save**.
7. On the **Schedule & Retention** page, do the following:

   a) In the **Schedule** box, select a schedule for the backup.

   - To view the details of the schedule, click 👁 **View**.
   - To add a schedule, click + **Add Schedule**.
   - To edit a schedule, select the schedule, and then click ✎ **Edit Schedule**.

   b) In the **Retention rule** box, select a retention rule for the backup.

   - To view details of the retention rule, click 👁 **View**.
   - To add a retention rule, click + **Add Retention Rule**.
   - To edit a retention rule, select the retention rule, and then click ✎ **Edit Retention Rule**.

   c) If the schedule you selected has an associated restore task, you can schedule when the backup is restored. To schedule a restore, click ⟲ .

   d) Click **Next** or **Save**.

8. On the **Summary** page, review the settings for the backup.
   - To edit the name of the backup, click ✎.
   - To edit the advanced options, click ⚙ **Advanced Options.**
   - To view the details of the schedule, click 👁 **View**.
   - To view details of the retention rule, click 👁 **View**.
9. Click **Create** or **Save**.
10. If you have edited the backup, do one of the following:
    - To confirm you want to edit the backup, click **Continue**.
    - If MFA has been enabled for **Edit backup**, enter the six-digit authentication code you received, and click **Continue**.
    - If MPA has been enabled for **Edit backup**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

- If MFA and MPA have been enabled for **Edit backup**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

6.9.2 Restoring a VMware Cloud Director backup

You can restore data from a VMware Cloud Director backup.

NOTE: If MFA and/or MPA has been enabled for **On-demand restore**, you must enter an authentication code and/or require approval to complete the task.

To restore a VMware Cloud Director backup:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
3. Select the DS-System, account, and DS-Client.

   NOTE: To search for a specific DS-Client based on the DS-Client number, type the DS-Client number in the search field, and then press **Enter**.

4. Select the VMware Cloud Director backup you want to restore, and then click **Restore Backup Set**.

   NOTE: We recommend restoring only one backup at a time. Restoring multiple backups concurrently can affect performance.

5. To restore an individual virtual machine to a VMware Cloud Director, select **Virtual machines**, and then do the following:

   a) Beside **Backup session**, select the generation(s) of the backup you want to restore. By default, the latest generation is selected for restore.

   b) Beside **Restore method**, select **VM-level** to restore the entire virtual machine, or **File-level** to restore individual files from the backup of the virtual machine.

6. To restore an entire VMware vApp, containing one or more virtual machines to a VMware Cloud Director, select **vApp**.
7. Select the items you want to restore. To search for items, click **Search,** and type the name of the backup.
8. In the **Restore Location** box, select one of the following options:

   - **Original** – Select this option to restore the item to its 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 ✏.

  b) Under **Select alternate location**, in the **VMware Cloud Director** box, select the VMware Cloud Director to which you want to restore the backup. Click + to add a VMware Cloud Director Server, or click ✏ to edit a VMware vCenter Server.

  c) In the **Account credentials** box, select the corresponding cloud credential for the selected VMware Cloud Director. Click + to add an account credential or click ✏ to edit an account credential.

  d) Under **Destination details**, select the source VM, the organization, the vApp, the destination VM, and the network to which you want to restore the backup.

  e) Click **Save**.

9. To power on the virtual machine after the restore is complete, select the **Power on virtual machine after restore** check box. For more information, see Section 6.9.3, “Powering on the virtual machine after restore”.

10. To add a time stamp of the restore process to the name of the virtual machine, select the **Add time stamp to virtual machine name** check box.

11. Click **Restore**, and then do one of the following:

    - To confirm you want to restore the backup, click **Continue**.

    - If MFA has been enabled for **On-demand restore**, enter the six-digit authentication code you received, and click **Continue**.

    - If MPA has been enabled for **On-demand restore**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

    - If MFA and MPA have been enabled for **On-demand restore**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

NOTE: To view the progress of the restore activity, click ⚙. For more information, see Section 8.5, “Viewing the Activity Monitor”, on page 145.

6.9.3 Powering on the virtual machine after restore

A virtual machine can be powered on after restore using the **Power on virtual machine after restore** option and manually performing either pre-configuration on the source virtual machine or post-configuration on the restored virtual machine.

Performing pre-configuration on the source virtual machine:

1. On the VMware Cloud Director, do the following:

   a) Click **Network adapter** of the virtual machine and then select the **Distributed Switch** network configured on the VMware Cloud Director.

   b) Set the MAC address allocation to **Automatic**.

2. On the VMware Cloud Director, do the following:

   a) Click **Properties** for the virtual machine and then select the **Network** mapped to the VMware Cloud Director.

   b) Power on the virtual machine and ensure it gets powered on successfully.

Performing post-configuration on the restored machine:

1. On the VMware Cloud Director, do the following:

   a) Click **Network adapter** of the restored virtual machine and then select the **Distributed Switch** network configured on the VMware Cloud Director.

   b) Set the MAC address allocation to **Automatic**.

2. On the VMware Cloud Director, do the following:

   a) Click **Properties** for the virtual machine and then select the **Network** mapped to the VMware Cloud Director..

   b) Under **MAC Address**, select **Reset**.

3. Power on the restored virtual machine.

6.10 Managing the list of backups

You can manage the list of backups, including using search and filter options.

To manage the list of backups:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
3. Select the DS-System, account, and DS-Client.

> ***NOTE:*** To search for a specific DS-Client based on the DS-Client number, type the DS-Client number in the search field, and then press **Enter**.

4. To search for a backup, click 🔍, and then type the name of the backup.
5. To refine the list of items that appear, click ☰ **Filter**.

> ***NOTE:*** To select all items in a filter, click ⬚. To clear all items in a filter, click ✕.To reset the filters, click **Reset**.

6. To select the columns you want to view, click ▮▮▮ **Select Columns**.

> ***NOTE:*** To view details about the status of a backup, click the status in the Status column. To view the Event Log for the backup, click Event Log.

6.11 Configuring antimalware and CDR for multiple backups

You can configure the antimalware or CDR scan for multiple backups.

NOTE: The antimalware feature is supported for File system backups when connected to a Windows, Linux, or Mac DS-Client and for Microsoft 365 backups when connected to a Windows DS-Client. The CDR feature is supported for File system backups when connected to a Windows DS-Client. For more information, see Section 2.2.2, “Configuring the antimalware and CDR settings”, on page 27.

To configure antimalware and CDR for multiple backups:

1. On the toolbar, click **Data Management**.
2. Select the DS-System, account, and DS-Client.

   NOTE: To search for a specific DS-Client based on the DS-Client number, type the DS-Client number in the search field, and then press **Enter**.

3. To enable or disable the Antimalware scan for multiple backups, do the following:
   a) Select the Windows File System and/or Microsoft 365 backups you want to configure, and then click 🛡.
   b) Under **Antimalware Scan**, slide the switch to enable or disable the antimalware scan.

   NOTE: You can only enable or disable the Antimalware scan for Windows File System or Microsoft 365 backups that belong to a DS-Client that has been licensed for the Antimalware/CDR feature.

4. To enable the CDR scan for multiple backups, do the following:
   a) Select the Windows File System backups you want to configure, and then click 🛡.
   b) Under **CDR Scan**, slide the switch to enable or disable the CDR scan.

   NOTE: You can only enable or disable the CDR scan for Windows File System backups that belong to a DS-Client that has been licensed for the Antimalware/CDR feature.

5. Click **Save**.

6.12 Performing an on-demand backup

The system is designed to perform unattended backups at scheduled intervals. However, you can perform on-demand backups at any time. The options available depend on the kind of backup.

NOTE: If MFA and/or MPA has been enabled for **On-demand backup**, you must enter an authentication code and/or require approval to complete this task.

To perform an on-demand backup:

1. On the toolbar, click **Data Management**
2. Click the **Backup Sets** tab.
3. Select a DS-System, account, and DS-Client.
4. Select the backup(s) you want to back up, click ☁ **Start Backup**, and then do one of the following:
   - To confirm you want to perform an on-demand backup, click **Continue**.
   - If MFA has been enabled for **On-demand backup**, enter the six-digit authentication code you received, and click **Continue**.
   - If MPA has been enabled for **On-demand backup**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.
   - If MFA and MPA have been enabled for **On-demand backup**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

NOTE: To view the progress of the backup activity, click ⚙. For more information, see Section 8.5, “Viewing the Activity Monitor”, on page 145.

6.13 Synchronizing a backup

The first time you perform a backup, the DS-Client retrieves the files from the backup source and sends the files to the DS-System. Information pertaining to the files is saved in both the DS-Client database and the DS-System online storage.

The information in the DS-Client database can fall out of synchronization with the DS-System online storage. If this occurs, a Normal synchronization process is automatically run during the next Weekly Admin process or scheduled backup. However, you can perform a manual synchronization of a backup.

To synchronize a backup:

1. On the toolbar, click **Data Management**.
2. Select a DS-System, account, and DS-Client.
3. Select the backup you want to synchronize, and then click ⋯ **More**.
4. Under **Backup set options**, select **Synchronize**.
5. Select the type of synchronization you want to perform. The options are as follows:
   - **Normal** - Compares the DS-Client database with the DS-System online storage and updates the DS-Client database as required.
   - **Check only** - Checks the synchronization between the DS-Client database and the DS-System online storage and identifies if inconsistencies exist. No corrective action is taken.
   - **DS-System based** - Synchronizes the DS-Client database with the DS-System online storage.
6. To synchronize backups that have the local storage option enabled, select the **Sync with Local Storage check box.**
7. Click **Synchronize**.

NOTE: To view the progress of the synchronization activity, click ⚙. For more information, see Section 8.5, “Viewing the Activity Monitor”, on page 145.

6.14 Suspending or activating a backup

When a backup is active, the DS-Client performs the scheduled tasks assigned to the backup. When a backup is suspended, the DS-Client no longer performs the scheduled tasks assigned to the backup.

To suspend an active backup:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
3. Select a DS-System, account, and DS-Client.
4. Select the active backups you want to suspend, and then click ⋯ **More**.
5. Under **Backup set options**, click **Suspend**.
6. When prompted to confirm you want to suspend the backup, click **Yes**.

To activate a suspended backup:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
3. Select a DS-System, account, and DS-Client.
4. Select the suspended backups you want to activate, and then click ⋯ **More**.
5. Under **Backup set options**, click **Activate**.
6. When prompted to confirm you want to activate the backup, click **Yes**.

6.15 Performing a selective delete

You can delete specific items from online storage. After performing a selective delete, the backup still exists, and scheduled backups will continue to run.

NOTE: If MFA and/or MPA has been enabled for **Selective delete**, you must enter an authentication code and/or require approval to complete the task.

To perform a selective delete:

1. On the toolbar, click **Data Management**.
2. Select a DS-System, account, and DS-Client.
3. Select the backup containing the items you want to delete, and then click ••• **More**.
4. Under **Backup set data,** click **Selective Delete**.
5. Beside **Backup session**, select the generation(s) of the backup containing the items you want to delete. By default, the latest generation is selected.
6. In the **Leave generations online** box, enter the number of generations you want to retain in the DS-System online storage. You can only select items that have more generations than the value specified.
7. Select the items you want to delete, click **Delete**, and then do one of the following:
   - To confirm you want to perform the selective delete, click **Continue**.
   - If you are required to enter a password to perform a selective delete, type your Management Console password, and then click **Continue**.
   - If MFA has been enabled for **Selective delete**, enter the six-digit authentication code you received, and click **Continue**.
   - If MPA has been enabled for **Selective delete**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.
   - If MFA and MPA have been enabled for **Selective delete**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

NOTE: To view the progress of the selective delete activity, click ⚙. For more information, see Section 8.5, “Viewing the Activity Monitor”, on page 145.

6.16 Deleting a backup

You can delete a backup. Apply caution when performing this process because data cannot be recovered after it has been deleted.

NOTE: If MFA and/or MPA has been enabled for **Delete backup**, you must enter an authentication code and/or require approval to complete this task.

To delete a backup:

1. On the toolbar, click **Data Management**.
2. Click the **Backup Sets** tab.
3. Select a DS-System, account, and DS-Client.
4. Select the backup(s) you want to delete, click 🗑 **Delete Backup Set**, and then do one of the following:
    - To confirm you want to delete the backup, click **Continue**.
    - If you are required to enter a password to delete a backup, type your Management Console password, and then click **Continue**.
    - If MFA has been enabled for **Delete backup**, enter the six-digit authentication code you received, and click **Continue**.
    - If MPA has been enabled for **Delete backup**, click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.
    - If MFA and MPA have been enabled for **Delete backup**, enter the six-digit authentication code you received, and click **Continue**. The task is not completed until you get approval, which can take up to 30 minutes.

7 Working with VM replication

You can use VM replication to replicate virtual machines from one VMware vCenter Server to another and initiate failover and failback.

7.1 Configuring VMware vCenter Server replication

You can configure a VMware vCenter Server replication to replicate virtual machines from one VMware vCenter Server to another and initiate failover and failback.

To configure VMware vCenter Server replication:

1. On the toolbar, click **Data Management**.
2. Click the **VM Replication Sets** tab.
   - To create a VM replication set, click + **Create Replication Set**.
   - To edit a VM replication set, select the DS-System, account, and DS-Client. Select the replication set you want to edit, and then click ✎ **Edit Replication Set**.
3. On the **Type & Components** page, do the following:

   a) In the **Replication set name** box, type a name for the replication set.

   b) In the **DS-System** box, select the DS-System.

   c) In the **Account** box, select the source account.

   d) In the **DS-Client number** box, select the source DS-Client account.

   e) In the **IP address** box, select the IP address of the destination DS-Client to which the virtual machine will be replicated.

   f) Click **Next**.
4. On the **Credentials & Items** page, do the following:

   a) In the **Source Host or IP address** box, type the IP address of the source VMware vCenter Server from which the virtual machine will be replicated, and then type the user name and password required to connect to the VMware vCenter Server.

   b) In the **Destination Host or IP address** box, type the IP address of the destination VMware vCenter Server to which the virtual machine will be replicated, and then type the user name and password required to connect to the VMware vCenter Server.

   c) In the **Maximum generations** box, enter the maximum number of generations you want to be available for failover and failback.

   d) Under **Source VMware vCenter items**, drag and drop the items you want to replicate to the **Destination VMware vCenter** section.

e) To edit the host IP address, datastore, or name of the virtual machine, click ✎ **Edit replication configuration**.

f) Click **Next**.

5. On the **Schedule** page, do the following:

a) In the **Schedule** box, select a schedule for the replication set.

- To view the details of the schedule, click 👁 **View**.
- To add a schedule, click + **Add Schedule**.
- To edit a schedule, select the schedule, and then click ✎ **Edit Schedule**.

b) Click **Next**.

NOTE: For more information, see Section 4.1, “Configuring a schedule”, on page 63.

6. On the **Summary** page, review the settings for the replication set.
   - To edit the name of the backup set, click ✎.
   - To view the details of the schedule, click 👁 **View**.
7. Click **Create** or **Save**.

7.2 Managing the list of replication sets

You can manage the list of replication sets, including using the search and filter options.

To manage the list of replication sets:

1. On the toolbar, click **Data Management**.
2. Click the **VM Replication Sets** tab.
3. Select the DS-System, account, and DS-Client containing the replication sets you want to manage.
4. To search for a replication set, click 🔍, and then type the name of the replication set you want to find.
5. To select the columns you want to view for the replication sets, click ▥ **Select Columns**.
6. To update the list of replication sets, click ↻ **Refresh**.

7.3 Performing on-demand replication

You can perform on-demand replication at any time.

To perform on-demand replication:

1. On the toolbar, click **Data Management**.
2. Click the **VM Replication Sets** tab.
3. Select the replication set on which you want to perform replication, and then click **Replicate**.
4. On the **Start Replication** page, select the items you want to replicate, and then click **Start**.
5. When the system prompts you to confirm you want to start replication, click **Yes**.

7.4 Performing a failover

After a virtual machine on the source server has been replicated to the destination server, the replicated virtual machine is ready for failover.

Before performing a failover, you can select from multiple replicated generations. When a target virtual machine is used after failover, it is available for failback.

To perform a failover:

1. On the toolbar, click **Data Management**.
2. Click the **VM Replication Sets** tab.
3. Click **Initiate Failover or Failback**.
4. Select a DS-System, account, and DS-Client.
5. Under **Ready for failover**, select the replication set on which you want to perform a failover.
6. Click **Initiate**.

7.5 Performing a failback

You can perform a failback on a replicated virtual machine. You must always perform a failback from the destination DS-Client.

IMPORTANT: Before performing a failback, ensure the existing source virtual machine has already been deleted and all notifications are resolved. If you want to retain the existing source virtual machine, clone the virtual machine before deleting it. Do not delete a partially restored source virtual machine from a previously attempted failback that has been stopped or has failed.

To perform a failback:

1. On the toolbar, click **Data Management**.
2. Click the **VM Replication Sets** tab.
3. Click **Initiate Failover or Failback**.
4. Select a DS-System, account, and DS-Client.
5. Under **Ready for failback**, select the replication set on which you want to perform a failback.
6. Click **Initiate**.

7.6 Deleting a replication set

You can delete a replication set if required.

To delete a replication set:

1. On the toolbar, click **Data Management**.
2. Click the **Replication Sets** tab.
3. Select a DS-System, account, and DS-Client.
4. Select the replication sets you want to delete, and then click **Delete Replication set**.
5. When the system prompts you to confirm you want to delete the replication set, click **Yes**.

8 Monitoring the system

You can generate various reports and view detailed logs to monitor the system.

8.1 Generating reports

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

8.1.1 Generating a Backup Sets Storage Report

You can generate a Backup Sets Storage Report to view the total protected size, stored size, and native size of the data backed up to the DS-System online storage at the DS-System, account, and DS-Client level.

To generate a Backup Sets Storage Report:

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

8.1.2 Generating a Cloud Backup Status Report

You can generate a Cloud Backup Status Report to view a summary of the Microsoft 365 data backed up for the various services, including Exchange mailboxes, public folders, archive mailboxes, SharePoint sites, OneDrive files, Groups, and Teams.

To generate a Cloud Backup Status Report:

1. On the toolbar, click **Monitoring**.
2. Click the **Cloud Backup Status** tab.
3. Select the Microsoft 365 domain for which you want to generate the report.
4. Select the Microsoft 365 service for which you want to view the information.
5. To update the report, click **Refresh**.

8.1.3 Generating an Antimalware Scan Report

You can generate an Antimalware Scan Report to view the results of the antimalware scan, including the number of files scanned, the number of files that failed to scan, and the number of files detected with malware.

NOTE: The antimalware feature is supported only for Windows File system and Microsoft 365 backups. For more information, see Section 2.2.2, “Configuring the antimalware and CDR settings”, on page 27.

To generate an Antimalware Scan Report:

1. On the toolbar, click **Monitoring.**
2. Click the **Antimalware Scan** tab.
3. Select the DS-System, account, and DS-Client account for which you want to generate the report.
4. Under **Antimalware Scan Backup Summary (24 hours)**, you can view the antimalware scan results for all backups performed in the past 24 hours.
5. Under **Antimalware Scan Restore Summary (24 hours)**, you can view the antimalware scan results for all restores performed in the past 24 hours.
6. Under **Antimalware Scan Backup Trend**, you can view the antimalware trend results for all backups performed over a daily, weekly, or monthly period.
7. Under **Antimalware Scan Restore Trend**, you can view the antimalware trend results for all restores performed over a daily, weekly, or monthly period.

   NOTE: The daily trend report shows data for the past week, the weekly trend report shows data for the past month, and the monthly trend report shows data for the past six months.

8. To update the report, click ↻ **Refresh**.

8.1.4 Generating a CDR Scan Report

You can generate a CDR Scan Report to view the results of the CDR scan, including the number of files scanned, the number of files that failed to scan, and the number of files filtered, removed, or blocked.

NOTE: The CDR feature is supported only for Windows File system backups. For more information, see Section 2.2.2, "Configuring the antimalware and CDR settings", on page 27.

To generate a CDR Scan Report:

1. On the toolbar, click **Monitoring.**
2. Click the **CDR Scan** tab.
3. Select the DS-System, account, and DS-Client account for which you want to generate the report.
4. Under **CDR Scan Backup Summary (24 hours)**, you can view the CDR scan results for all backups performed in the past 24 hours.
5. Under **CDR Scan Restore Summary (24 hours)**, you can view the CDR scan results for all restores performed in the past 24 hours.
6. Under **CDR Scan Backup Trend**, you can view the CDR trend results for all backups performed over a daily, weekly, or monthly period.
7. Under **CDR Scan Restore Trend**, you can view the CDR trend results for all restores performed over a daily, weekly, or monthly period.

   NOTE: The daily trend report shows data for the past week, the weekly trend report shows data for the past month, and the monthly trend report shows data for the past six months.

8. To update the report, click ↻ **Refresh**.

8.1.5 Generating a GDPR Compliance Report

You can generate a GDPR Compliance Report to view who deleted data, what data was deleted, and when the data was deleted. You can also generate a GDPR Compliance Certificate that can be downloaded in PDF format.

The GDPR solution allows you to protect your data, regardless of where it resides, by controlling how different types and tiers of data are securely stored or deleted as regulations demand.

To generate a GDPR Compliance Report:

1. On the toolbar, click **Monitoring**.
2. Click the **GDPR Compliance** tab.
3. Select the DS-System, account, and DS-Client for which you want to generate the report.
4. In the **Start date** and **End date** boxes, specify the period you want the report to cover. You can generate a GDPR report for the past 30 days only.
5. To update the list of items, click ⟳ **Refresh**.
6. Select the deleted items you want to include in the GDPR Report, and then click **Generate Certificate**.
7. In the **Request type** box, type the purpose for which the report is required. For example, audit, compliance, routine check.
8. In the **Reason for request** box, type the reason for making the request.
9. In the **Phone number** box, type the telephone number of the person making the request.
10. In the **Requested by (name)** box, type the name of the person making the request.
11. Click **Generate Certificate**. The GDPR Certificate Status window informs you the certificate is being generated and you will be notified when it is ready for download. Click **Close.**
12. When the certificate has been generated, click 🔔 **Notifications**, and then click **Download**.

8.2 Viewing Logs

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

8.2.1 Viewing the Activity Log

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

To view the Activity Log:

1. On the toolbar, click **Monitoring**.
2. Click the **Logs** tab.
3. In the **Select Component** box, select the component for which you want to view the Activity Log, and then do the one of the following:
   - If you selected **DS-System**, select the DS-System.
   - If you selected **DS-Client**, select the DS-System, account, and DS-Client.
4. Click the **Activity Log** tab.
5. To search the activity log, click 🔍. Type the description in the search field, and then press **Enter**.
6. To refine the list of items that appear in the Activity Log, click ≡ **Filter**.
7. To select the columns you want to view in the Activity Log, click ▥ **Select Columns**.
8. To update the Activity Log, click ⟳ **Refresh**.

8.2.2 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. In the **Select Component** box, select the component for which you want to view the Event Log, and then do the one of the following:
   - If you selected **DS-System**, select the DS-System.
   - If you selected **DS-Client**, select the DS-System, account, and DS-Client.
4. Click the **Event Log** tab.
5. To refine the list of items that appear in the Event Log, click ☰ **Filter**.
6. To select the columns you want to view in the Event Log, click ▥ **Select Columns**.
7. To update the Event Log, click ↻ **Refresh**.

8.2.3 Viewing the Audit Log

The Audit Log provides a detailed list of all the changes made to the DS-System, DS-Client, and Management Console databases.

To view the Audit Log:

1. On the toolbar, click **Monitoring.**
2. Click the **Logs** tab.
3. In the **Select Component** box, select the component for which you want to view the Audit Log, and then do the one of the following:
   - If you selected **DS-System**, select the DS-System.
   - If you selected **DS-Client**, select the DS-System, account, and DS-Client.
4. Click the **Audit Log** tab.
5. To refine the list of items that appear in the Audit Log, click ☰ **Filter**.
6. To select the columns you want to view in the Audit Log, click ▥ **Select Columns**.
7. To update the Audit Log, click ↻ **Refresh**.

8.2.4 Viewing the Grid Log

The Grid Log displays all events specific to a Grid DS-Client configuration.

NOTE: The Grid Log is available only if you have configured a Grid DS-Client.

To view the Grid Log:

1. On the toolbar, click **Monitoring.**
2. Click the **Logs** tab.
3. In the **Component name** box, select **DS-Client**, and then select the DS-System, account, and DS-Client.
4. Click the **Grid Log** tab.
5. To refine the list of items that appear in the Grid Log, click **Filter**.
6. To select the columns you want to view in the Grids Log, click **Select Columns**.
7. To update the Grid Log, click **Refresh**.

8.3 Viewing the status of a Grid DS-Client

You can 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 Status**, view the status of the grid.
4. To update the status, click **Refresh**.

8.4 Viewing usage metrics

You can view the average usage metrics at the DS-System, account, and DS-Client account level for a selected period.

To view the usage metrics:

1. On the toolbar, click **Monitoring**.
2. Click the **Usage Metrics** tab.
3. Select a DS-System, account, and DS-Client.
4. In the **Start date** and **End date** boxes, specify the period you want to cover. You can view the average usage metrics for the past 365 days.
5. To refresh the list, click ↻ **Refresh**.
6. Expand the account for which you want to view the usage metrics. The following information is displayed:

Column	Description
Physical Environment	• **Online Capacity** – Online capacity used for physical machines. • **Physical Machines** – Physical machines backed up.
Virtual Environment	• **Online Capacity** – Online capacity used for virtual machines. • **Virtual Machines** – Virtual machines backed up.
Cloud Environment	• **Online Capacity** – Online capacity used for Cloud backups. • **Users** – Total Cloud users backed up.
VMware Replication	• **Native Capacity** – Total VM replication capacity used for virtual machines. • **Virtual Machines** – Total virtual machines replicated.
Local-only Storage	• **Local-only Capacity** – Total local-only capacity used.
Antimalware/CDR	• **Antimalware/CDR Count** – Total number of DS-Clients licensed for the Antimalware/CDR feature.

Table 5 Usage metrics

8.5 Viewing the Activity Monitor

You can use the Activity Monitor to view the progress and status of on-demand backup, restore, synchronization, and delete activities you have started.

To view the Activity Monitor:

1. On the toolbar, click **Data Management**.
2. Click **View Activity Monitor**. The On-Demand Activity Monitor displays the name of the process, type of activity, and activity status.
3. To search for an activity, click 🔍, and then type the name of the activity.
4. To refine the list of activities, click **Filter**.
5. To view the details of an activity, click **View details**.

> ***NOTE:*** To view more information about the activity, click **Event Log**.

6. To stop an activity, select the activity, and then select the **Stop Running Activities** check box.
7. To remove an individual activity, click **Clear activity**. To remove all completed activities, click **Clear Completed Activities.**
8. To minimize the Activity Monitor, click **Minimize**.