Competency Based Learning Materials

(CBLM)

IT Support Service

Level-3

Module: Performing Basic Data Backup and Recovery

CODE: CBLM-OU-ICT-ITSS-06-L3-V1

National Skills Development Authority
Prime Minister's Office
Government of the People's Republic of Bangladesh

Copyright

National Skills Development Authority
Prime Minister's Office
Level: 10-11, Biniyog Bhaban,
E-6 / B, Agargaon, Sher-E-Bangla Nagar Dhaka-1207, Bangladesh.
Email: ec@nsda.gov.bd
Website: www.nsda.gov.bd.
National Skills Portal: http:\\skillsportal.gov.bd

This Competency Based Learning Materials (CBLM) on "Performing Basic Data Backup and Recovery" under the IT Support Service, Level-3 qualification is developed based on the national competency standard approved by National Skills Development Authority (NSDA)

This document is to be used as a key reference point by the competency-based learning materials developers, teachers/trainers/assessors as a base on which to build instructional activities.

This Competency Based Learning Materials is a document for the development of curricula, teaching and learning materials, and assessment tools. It also serves as the document for providing training consistent with the requirements of industry in order to meet the qualification of individuals who graduated through the established standard via competency-based assessment for a relevant job.

This document has been developed by NSDA in association with industry representatives, academia, related specialist, trainer and related employee.

Public and private institutions may use the information contained in this CBLM for activities benefitting Bangladesh.

List of Abbreviations

CS	- Competency Standard
ISC	- Industry Skills Council
NSDA	- National Skills Development Authority
NSQF	- National Skills Qualifications Framework
BNQF	- Bangladesh National Qualifications Framework
OSH	- Occupational Safety and Health
PPE	- Personal Protective Equipment
SCVC	- Standards and Curriculum Validation Committee
STP	- Skills Training Provider
SOP	- Standard Operating Procedure
UoC	- Unit of Competency
EC	- Executive Committee
CBT&A	- Competency based Training & Assessment
CBC	- Competency based Curriculum
CAD	- Course Accreditation Document
CBLM	- Competency Based Learning Materials
	-
	-
	-
	-

How to use this Competency Based Learning Materials (CBLMs)

The module, Performing Basic Data Backup and Recovery contains training materials and activities for you to complete. These activities may be completed as part of structured classroom activities or you may be required you to work at your own pace. These activities will ask you to complete associated learning and practice activities in order to gain knowledge and skills you need to achieve the learning outcomes.

1. Review the **Learning Activity** page to understand the sequence of learning activities you will undergo. This page will serve as your road map towards the achievement of competence.

2. Read the **Information Sheets.** This will give you an understanding of the jobs or tasks you are going to learn how to do. Once you have finished reading the **Information Sheets** complete the questions in the **Self-Check.**

3. **Self-**Checks are found after each **Information Sheet**. **Self-Checks** are designed to help you know how you are progressing. If you are unable to answer the questions in the **Self-Check** you will need to re-read the relevant **Information Sheet**. Once you have completed all the questions check your answers by reading the relevant **Answer Keys** found at the end of this module.

4. Next move on to the **Job Sheets. Job Sheets** provide detailed information about *how to do the job* you are being trained in. Some **Job Sheets** will also have a series of **Activity Sheets**. These sheets have been designed to introduce you to the job step by step. This is where you will apply the new knowledge you gained by reading the Information Sheets. This is your opportunity to practice the job. You may need to practice the job or activity several times before you become competent.

5. Specification **sheets**, specifying the details of the job to be performed will be provided where appropriate.

6. A review of competency is provided on the last page to help remind if all the required assessment criteria have been met. This record is for your own information and guidance and is not an official record of competency

When working though this Module always be aware of your safety and the safety of others in the training room. Should you require assistance or clarification please consult your trainer or facilitator.

When you have satisfactorily completed all the Jobs and/or Activities outlined in this module, an assessment event will be scheduled to assess if you have achieved competency in the specified learning outcomes. You will then be ready to move onto the next Unit of Competency or Module

Approved by __ th Authority Meeting of NSDA Held on ----------

TABLE OF CONTENTS

MODULE CONTENT

Unit of Competency	**Perform Basic Data Backup and Recovery**
Unit Code	**OU-ICT-ITSS-06-L3-V1**
Module Title	**Performing Basic Data Backup and Recovery**
Module Descriptor	This module discusses the aspects that must be given attention when Performing Basic Data Backup and Recovery. It shows the knowledge and skills requirements for interpreting backup and data recovery, performing OS backup, user data backup, Email backup and backup recovery
Nominal Hours	**60 Hours**
Lerning Outcome	After completion of this module the trainees must be able to: 1. Interpret backup and data recovery 2. Perform OS Backup 3. Perform user data backup 4. Perform email backup 5. Perform backup recovery

Assessment Criteria:

1. Backup is interpreted
2. Data recovery is interpreted
3. Type of backup solutions are stated
4. Disaster recovery plan is interpreted.
5. Partition table is interpreted
6. Backup Plan is prepared
7. Tools for OS backup is identified and collected
8. Target for backup is identified
9. Backup procedure is performed
10. Backup Plan is prepared
11. Tools for user data backup is identified and collected
12. Target for backup is identified
13. Backup procedure is performed
14. Mail client is identified and configured.
15. Local Database file of mail client is identified
16. Email Backup Plan is prepared
17. Target for backup is identified
18. Backup procedure is performed
19. Backup is collected for recovery
20. Tools are identified and selected for recovery.
21. Recovery target is identified
22. Restore point is identified
23. Restore procedure is performed

Learning Outcome 1: Interpret backup and data recovery

Assessment Criteria:

1.1 Backup is interpreted
1.2 Data recovery is interpreted
1.3 Type of backup solutions are stated
1.4 Disaster recovery plan is interpreted

Content:

1. Data Backup
2. Data recovery
3. Type of backup solutions
4. Disaster recovery plan

Resources Required/ Conditions:
The trainees must be provided with the following:

- Handouts or reference materials/books/ CBLMs on the above stated contents
- PCs/printers or laptop/printer with internet access
- Digital projector and Screen
- Bond paper
- Ball pens/pencils and other office supplies and materials
- Relevant learning materials
- Workplace or simulated environment

Methodologies

- Lecture/discussion
- Demonstration/application
- Presentation
- Blended delivery methods

Assessment Methods

- Written test
- Demonstration
- Observation with checklist
- Oral questioning
- Portfolio

Learning Experience 1: Interpret backup and data recovery

In order to achieve the objectives stated in this learning guide, you must perform the learning steps below. Beside each step are the resources or special instructions you will use to accomplish the corresponding activity.

Learning Steps	Resources specific instructions
1. Trainee will ask the instructor about interpreting backup and data recovery	1. Instructor will provide the learning materials "**Performing Basic Data Backup and Recovery"**
2. Read the Information sheet/s	2. Information Sheet No: 1 interpreting backup and data recovery
3. Complete the Self Checks & Check answer sheets.	3. Self-Check/s Self-Check No: 1 interpreting backup and data recovery Answer key No. 1 interpreting backup and data recovery
4. Read the Job Sheet and Specification Sheet and perform job	4. Job- Sheet No: 1- interpreting backup and data recovery Specification Sheet 1 – interpreting backup and data recovery

Information Sheet 1: Interpreting backup and data recovery

Learning Objectives:

After completion of this information sheet, the learners will be able to:

1.1 Interpret Backup
1.2 Interpret Data recovery
1.3 State Type of backup solutions
1.4 Interpret Disaster recovery plan

1.1 Data backup

Data backup refers to the process of duplicating and storing digital information from a computer system onto secondary storage media or remote servers. This backup ensures that critical data is protected against loss, corruption, or unauthorized access. Here's a more detailed explanation:

Purpose: The primary purpose of computer data backup is to safeguard important files, documents, settings, and other digital assets against various threats, including hardware failures, software errors, malware attacks, accidental deletion, theft, and natural disasters. By creating backup copies, users can recover their data in case of any unforeseen events.

Types of Data: Computer data backup can include a wide range of digital information, such as:
Documents: Word files, PDFs, spreadsheets, presentations, etc.
Multimedia: Photos, videos, music files, etc.
System Settings: Configuration files, preferences, customizations, etc.
Applications: Installers, license keys, software configurations, etc.
Databases: Structured data stored in databases or data warehouses.

Backup Methods:
Full Back up: Copies all data from the computer to the backup destination. It provides a complete snapshot of the system at a specific point in time.
Incremental Backup: Copies only the data that has changed since the last backup. This method is faster and requires less storage space compared to a full backup.
Differential Backup: Copies all data that has changed since the last full backup. It requires more storage space than an incremental backup but allows for faster data restoration.
Continuous Data Protection (CDP): Captures every change made to data in real-time or at frequent intervals, ensuring near-continuous backup.
Backup Storage:
Backup data can be stored on various types of storage media, including:
External Hard Drives: Portable storage devices connected to the computer via USB or other interfaces.
Network-Attached Storage (NAS): Dedicated storage devices connected to the local network, providing centralized backup storage for multiple computers.

Cloud Storage: Remote servers accessed via the internet, offering scalable and accessible backup solutions.

Backup Software:

Backup software facilitates the creation, scheduling, and management of backup processes. It may include features such as encryption, compression, deduplication, and remote monitoring.

Examples of backup software include Acronis True Image, EaseUS Todo Backup, Carbonite, Backblaze, and Windows Backup and Restore (built into Windows operating systems).

1.2 Data recovery

Data recovery is the process of retrieving lost, damaged, corrupted, or accidentally deleted digital information from storage media such as hard drives, solid-state drives (SSDs), memory cards, USB drives, and other storage devices. It involves specialized techniques and software to restore inaccessible data and make it usable again. Here's a detailed explanation of data recovery:

Causes of Data Loss:

- Hardware Failures: Malfunctioning hard drives, SSDs, or other storage devices due to mechanical issues, electronic failures, or wear and tear.
- Software Issues: File system corruption, operating system errors, software bugs, or malware infections that render data inaccessible.
- Human Errors: Accidental deletion of files, formatting of drives, or overwriting of data.
- Natural Disasters: Fires, floods, earthquakes, or other catastrophic events that damage storage devices and render data unreadable.
- Theft or Loss: Theft or physical loss of devices containing important data.
- Physical Damage: Physical damage to storage devices caused by drops, impacts, or exposure to extreme temperatures.

Data Recovery Techniques:

File System Reconstruction: Restoring the file system structures to recover lost files and directories.

- Partition Recovery: Reconstructing lost or damaged disk partitions to retrieve data stored on them.
- Deleted File Recovery: Scanning storage media for traces of deleted files and recovering them before they are overwritten.
- Raw Data Recovery: Extracting data directly from the underlying storage media without relying on the file system.
- RAID Recovery: Rebuilding RAID arrays to recover data from multiple disks in case of RAID controller failures or disk failures in RAID configurations.

- Forensic Data Recovery: Employing specialized techniques to recover digital evidence for legal or investigative purposes.

Data Recovery Process:

- Assessment: Evaluating the extent of data loss, identifying the causes, and determining the appropriate recovery techniques.
- Device Preparation: Handling storage devices carefully to prevent further damage and ensuring they are in a stable condition for recovery.
- Data Imaging: Creating a bit-by-bit copy (image) of the original storage device to work from, minimizing the risk of data loss during the recovery process.
- Analysis and Recovery: Using specialized software and tools to scan the storage device, identify recoverable data, and extract it to a safe location.
- Verification: Verifying the integrity and completeness of the recovered data to ensure it is usable and accurate.
- Data Restoration: Restoring the recovered data to its original location or transferring it to a new storage device as needed.

Data Recovery Tools and Software:

There are numerous data recovery tools and software available, ranging from basic file recovery utilities to advanced forensic and enterprise-level solutions.
Examples include Recuva, TestDisk, PhotoRec, EaseUS Data Recovery Wizard, R-Studio, Disk Drill, and specialized tools provided by data recovery service providers.
Data Recovery Services:
In cases where DIY data recovery is not feasible or successful, professional data recovery services can be employed.
Data recovery service providers have specialized expertise, tools, and facilities to handle complex data loss scenarios and recover data from severely damaged or encrypted storage devices.

1.3 Types of Backup:

Backup solutions come in various types, each offering different features, advantages, and suitability for specific use cases. Here are some common types of backup solutions:

Local Backup:

- External Hard Drives: Users manually copy data to external hard drives connected directly to their computer or network-attached storage (NAS) devices. This method provides a straightforward and cost-effective way to create backups, but it requires manual intervention and may not protect against local disasters like fires or floods.
- Network-Attached Storage (NAS): Dedicated storage devices connected to the local network, providing centralized backup storage for multiple computers. NAS devices often offer features such as RAID redundancy, automated backups, and remote access.

Cloud Backup:

- Cloud Storage Services: Data is backed up to remote servers hosted by third-party cloud storage providers such as Google Drive, Dropbox, Microsoft OneDrive, and Amazon S3. Cloud backup offers scalability, accessibility, and off-site protection against local disasters. Users pay for storage space and may benefit from features like automated backups, versioning, and encryption.
- Cloud Backup Services: Managed backup solutions offered by service providers that specialize in cloud backup. These services often include features such as automated backups, deduplication, compression, encryption, and centralized management for businesses.

1.4 Disaster Recovery Plan

A Disaster Recovery Plan (DRP) is a comprehensive strategy that outlines how an organization will respond to and recover from an event that disrupts or destroys computer data. It goes beyond simply having a data backup and considers the entire process of getting back to normal operations after a disaster.

Data Backup and Recovery forms the foundation of a DRP. It's the process of creating copies of your data (documents, emails, databases, etc.) and storing them in a separate location. If your primary data is compromised, you can restore it from the backup.

DRP builds upon data backup and recovery by including additional elements:
Identification of potential threats: This includes natural disasters, power outages, hardware failures, cyberattacks, and human error.
Impact assessment: Analyzing the potential consequences of each threat on your data and operations.
Recovery procedures: Detailed steps for restoring data, applications, and system configurations after a disaster.
Business continuity plan: Ensuring critical business functions can resume even with limited access to data.
Testing and training: Regularly testing your DRP and training employees on their roles in recovery.

Self-Check Sheet 1: Interpreting backup and data recovery

1. What is the purpose of data backup?

2. Define data recovery.

3. Name two types of backup solutions.

4. What does a disaster recovery plan entail?

5. How can data recovery be achieved?

Answer Key 1: Interpreting backup and data recovery

1. What is the purpose of data backup?
   Answer: The purpose of data backup is to create copies of important files and information to protect against data loss caused by various factors such as hardware failures, software errors, accidental deletion, or disasters.

2. Define data recovery.
   Answer: Data recovery is the process of retrieving lost, damaged, or corrupted digital information from storage media such as hard drives, memory cards, or USB drives, with the aim of making the data accessible and usable again.

3. Name two types of backup solutions.
   Answer: Two types of backup solutions are local backup, where data is copied to devices like external hard drives or network-attached storage (NAS), and cloud backup, where data is stored on remote servers accessed via the internet.

4. What does a disaster recovery plan entail?
   Answer: A disaster recovery plan outlines procedures and strategies for restoring IT infrastructure, applications, and data in the event of a disaster or data loss incident, with the goal of minimizing downtime, data loss, and business impact.

5. How can data recovery be achieved?
   Answer: Data recovery can be achieved through various techniques such as file system reconstruction, partition recovery, deleted file recovery, raw data recovery, and RAID recovery, depending on the nature and cause of the data loss.

Learning Outcome 2: Perform OS Backup

Assessment Criteria:

2.1 Partition table is interpreted
2.2 Backup Plan is prepared
2.3 Tools for OS backup is identified and collected
2.4 Target for backup is identified
2.5 Backup procedure is performed

Content:

1. Partition table
    1.1. MBR
    1.2. GPT
2. Backup Plan
3. Tools for OS backup
    3.1. System Provided tools
    3.2. Third party
        3.2.1. Norton
        3.2.2. Acronics
        3.2.3. EASE US
        3.2.4. AOMEI
        3.2.5. Minitool
4. Target for backup
    4.1. Cloud (OneDrive, Google Drive)
    4.2. Local Storage (External Storage Device, Network storage)
5. Backup procedure
    5.1. Manual
    5.2. Scheduled
    5.3. Scheme (Full, incremental, Differential)

Resources Required/ Conditions:

The trainees must be provided with the following:

- Handouts or reference materials/books/ CBLMs on the above stated contents
- PCs/printers or laptop/printer with internet access
- Digital projector and Screen
- Bond paper
- Ball pens/pencils and other office supplies and materials
- Relevant learning materials
- Workplace or simulated environment

Methodologies

- Lecture/discussion
- Demonstration/application

- Presentation
- Blended delivery methods

Assessment Methods

- Written test
- Demonstration
- Observation with checklist
- Oral questioning
- Portfolio

Learning Experience 2: Perform OS Backup

In order to achieve the objectives stated in this learning guide, you must perform the learning steps below. Beside each step are the resources or special instructions you will use to accomplish the corresponding activity.

Learning Steps	Resources specific instructions
1. Student will ask the instructor about Performing OS Backup	1. Instructor will provide the learning materials "**Performing Basic Data Backup and Recovery"**
2. Read the Information sheet/s	2. Information Sheet No: 2 Performing OS Backup
3. Complete the Self Checks & Check answer sheets.	3. Self-Check/s Self-Check No: 2 - Performing OS Backup Answer key No. 2 - Performing OS Backup
4. Read the Job Sheet and Specification Sheet and perform job	4. Job- Sheet No: 2 - Performing OS Backup Specification Sheet: 2- Performing OS Backup

Information Sheet 2: Performing OS Backup

Learning Objectives:

After completion of this information sheet, the learners will be able to:

2.1 Interpret Partition table
2.2 Prepare Backup Plan
2.3 Identify and collect Tools for OS backup
2.4 Identify Target for backup
2.5 Perform Backup procedure

2.1 Partition Table

A partition table is a data structure found on storage devices, such as hard disk drives (HDDs) and solid-state drives (SSDs), that defines the layout and organization of partitions or logical divisions within the storage space. Each partition typically represents a separate section of the disk that can be independently managed and accessed by the operating system and user applications.

Components:
Partition Entries: Each partition entry in the partition table contains metadata about a specific partition, including its starting and ending positions (or sectors), size, type, and file system format.

Partition Types: Partitions can be designated for different purposes, such as primary partitions, extended partitions, logical partitions (within extended partitions), and special-purpose partitions like boot partitions.

Boot Record: The partition table typically includes a boot record or boot sector that contains essential code for bootstrapping the operating system during the system startup process.

Partitioning Schemes:

Master Boot Record (MBR): MBR is one of the oldest and most widely used partitioning schemes. It supports up to four primary partitions or three primary partitions and one extended partition containing multiple logical partitions. MBR has limitations on disk size and does not support drives larger than 2 terabytes (TB).

GUID Partition Table (GPT): GPT is a modern partitioning scheme designed to overcome the limitations of MBR. It supports larger disk sizes (up to 9.4 zettabytes) and allows for up to 128 primary partitions. GPT also provides redundancy and integrity checks for improved data reliability.

Partitioning your hard drive allows you to create separate sections for different purposes. However, it's crucial to have a backup plan in place before making any changes to your disk structure. Here's why and how to prepare:

Why Backup Before Partitioning?

Partitioning involves modifying your hard drive's layout. Even minor mistakes during the process can lead to data loss. Here are some potential risks:

Accidental Deletion: During partitioning, you might accidentally delete existing partitions or data on your drive.

Partitioning Errors: Errors during the partitioning process can corrupt your data or make it inaccessible.
Unexpected Events: Power outages or system crashes during partitioning can lead to data loss.

2.2 Preparing a Backup Plan:

To minimize risks and ensure a smooth recovery in case of any issues, follow these steps before partitioning:

Identify Important Data:
Make a list of all critical files, documents, photos, videos, and applications you need to save.

Choose a Backup Method:

External Hard Drive: The simplest and most reliable option. Connect an external hard drive with enough storage space to hold your data.

Cloud Storage: Services like Google Drive, Dropbox, or OneDrive offer online storage. However, uploading a large amount of data may take time.
Network Attached Storage (NAS): A centralized storage device on your network, good for backing up multiple computers.

Perform the Backup:
Use a reliable backup tool included with your operating system or third-party software.
Select the files and folders you want to back up and choose your chosen backup destination (external drive, cloud, etc.).
Initiate the backup process and ensure it completes successfully.

Verify the Backup:
After the backup finishes, open the backup location and access a few files to confirm they are intact.

2.3 Tools for OS Backup

There are two main categories of tools used for OS backups: built-in operating system tools and third-party backup software.

Built-in Operating System Tools:
Most operating systems come with built-in tools for backing up your data and system.

Windows:

- **File History:** Creates incremental backups of your user files (documents, pictures, etc.) to an external drive.
- **System Restore:** Creates restore points to revert your system files and settings to a previous state. (Not a full system backup)
- macOS:
- **Time Machine:** Creates automatic backups of your entire system, including files, applications, and system settings, to an external drive.
- **Linux:**
  - **dd (command line):** A powerful but complex tool for creating full disk backups. Not recommended for beginners.
  - **cp -r (command line):** Can be used to copy specific directories or partitions to a backup location.

Third-Party Backup Software:
Third-party backup software offers more features and flexibility compared to built-in tools. Here are some popular options:

- Acronis True Image: Creates full system backups, incremental backups, and schedules automated backups.
- Veeam Backup & Replication: Offers comprehensive backup solutions for businesses, including features for virtual machines and cloud backups.
- EaseUS Todo Backup: A user-friendly option with features for full system backups, file/folder backups, and disk cloning.
- Clonezilla: Free and open-source software for creating full disk backups and restoring them.

2.4 Target for Backup

In the context of data backup, a target refers to the destination where your backed-up data is stored. It's the location where copies of your files, folders, system images, or entire partitions are saved for safekeeping. Here are some common types of backup targets:

Local Storage Devices:
External Hard Drives (HDDs) or Solid-State Drives (SSDs): The simplest and most common option. They are readily available, affordable, and offer fast access times for recovery. However, they are susceptible to physical damage like falls or power surges.
USB Flash Drives: Portable and convenient for small backups, but limited storage capacity and prone to loss or damage.

Internal Hard Drives (on a separate partition): An option if you have a large internal drive with enough unused space. However, not ideal for primary backups as a single hardware failure could affect both the original data and the backup.

Network-Attached Storage (NAS):
A centralized storage device on your network, ideal for backing up multiple computers. Offers larger storage capacity than individual external drives but requires some technical setup.

Cloud Storage:
Online storage services like Google Drive, Dropbox, or OneDrive offer convenient and remote backup options.
Advantages: Accessible from anywhere with an internet connection, provides good protection against local disasters (fire, theft).
Disadvantages: Limited free storage space, upload/download speeds can be impacted by internet bandwidth, potential security concerns.

2.5 Backup Procedure:

A backup procedure outlines the steps involved in creating and maintaining copies of your data for safekeeping. Here's a breakdown of a typical backup procedure:

Identify Important Data: Make a list of all critical files, documents, photos, videos, and applications you need to back up.

Choose a Backup Target: Select a suitable destination for your backups (e.g., external hard drive, cloud storage, NAS). Consider factors like storage capacity, security, and accessibility.

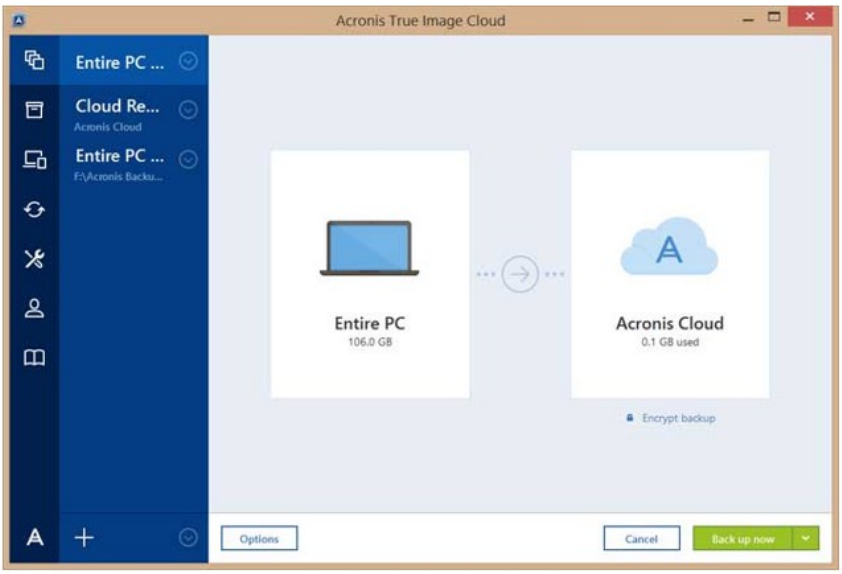
Choose a Backup Method: Decide on the type of backup you want to perform:
Full Back up: Creates a complete copy of all your selected data at a specific point in time.

Incremental Backup: Backs up only the data that has changed since the last backup, saving storage space.

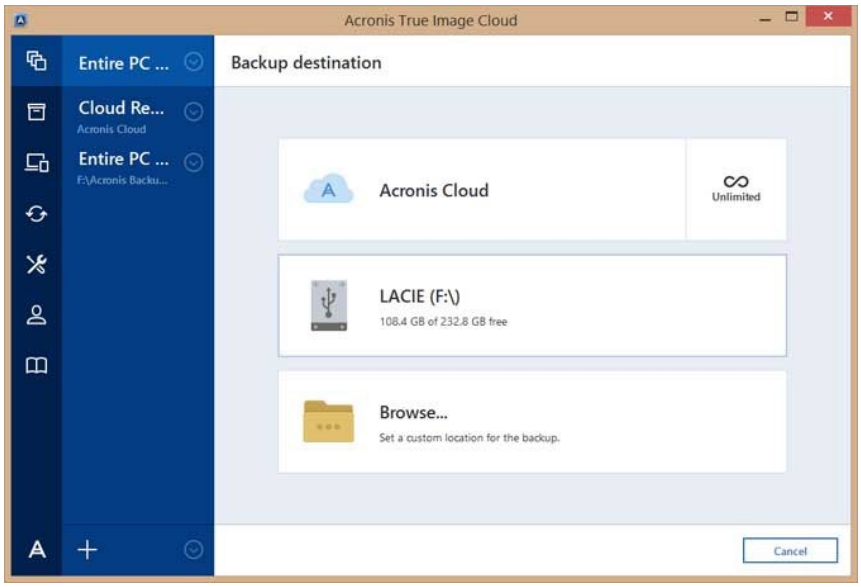
Differential Backup: Backs up data that has changed since the last full backup, faster than a full backup but requires both the differential backup and the last full backup for restoration.

Choose a Backup Tool: Select a suitable software program (built-in OS tools or third-party software) to facilitate the backup process.

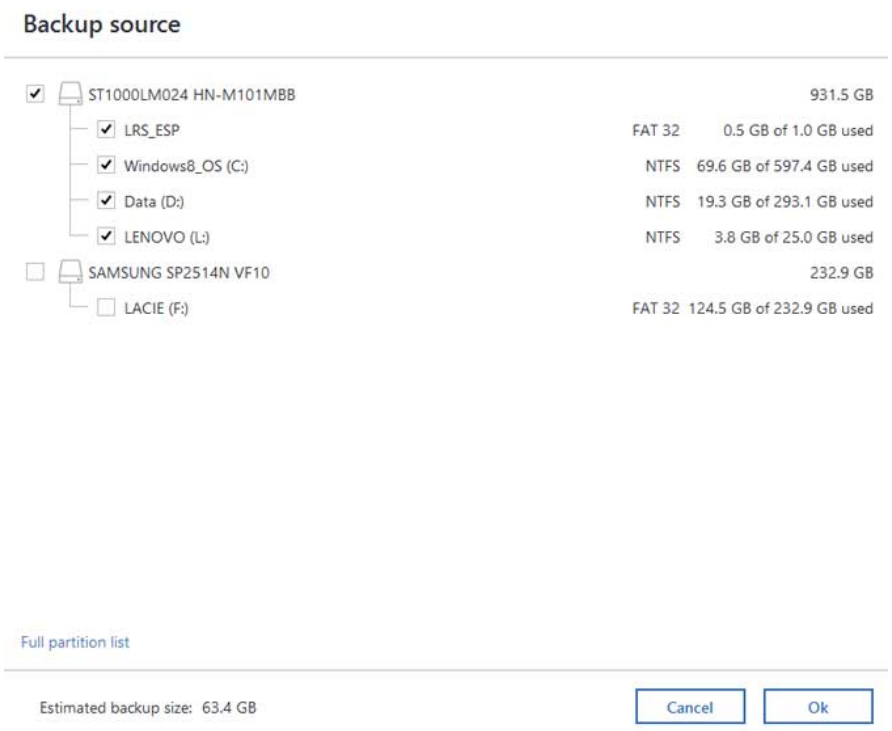
Creating Image using Acronis



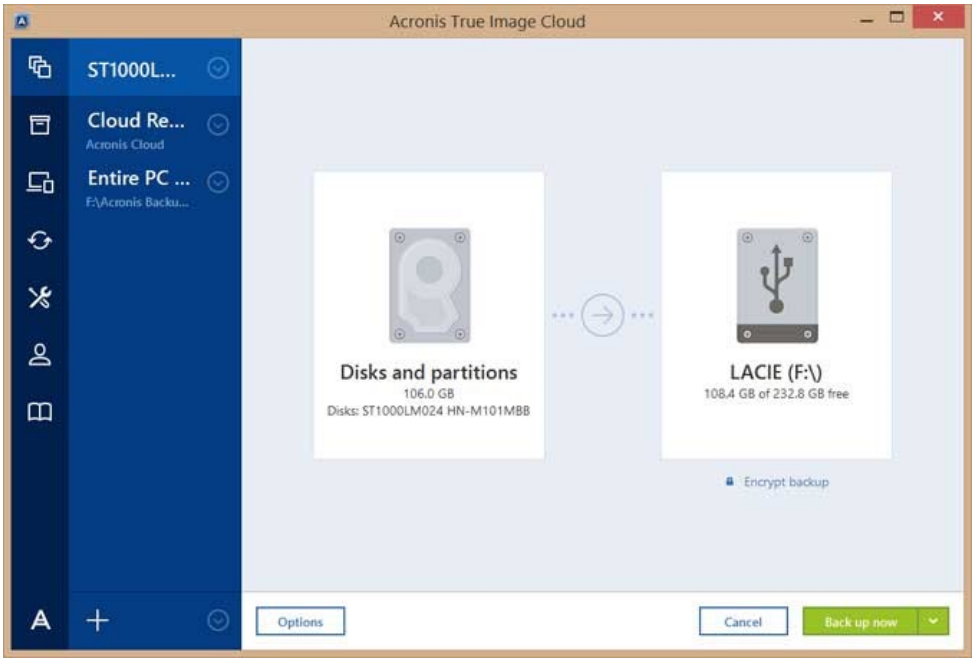
Step 2



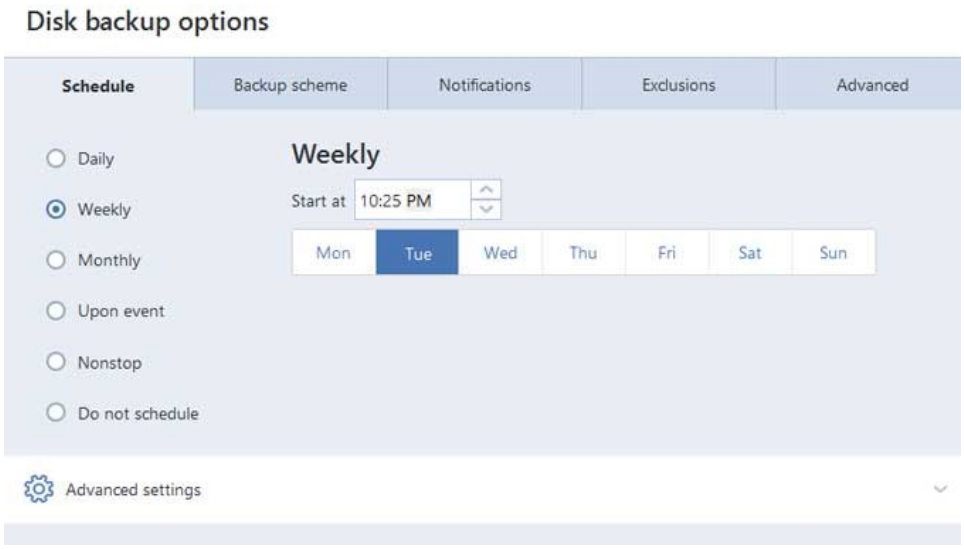
Step 3


Backup source
ST1000LM024 HN-M101MBB
931.5 GB
LRS_ESP
FAT 32
0.5 GB of 1.0 GB used
Windows8_OS (C:)
NTFS
69.6 GB of 597.4 GB used
Data (D:)
NTFS
19.3 GB of 293.1 GB used
LENOVO (L:)
NTFS
3.8 GB of 25.0 GB used
SAMSUNG SP2514N VF10
232.9 GB
LACIE (F:)
FAT 32
124.5 GB of 232.9 GB used
Full partition list
Estimated backup size: 63.4 GB
Cancel
Ok

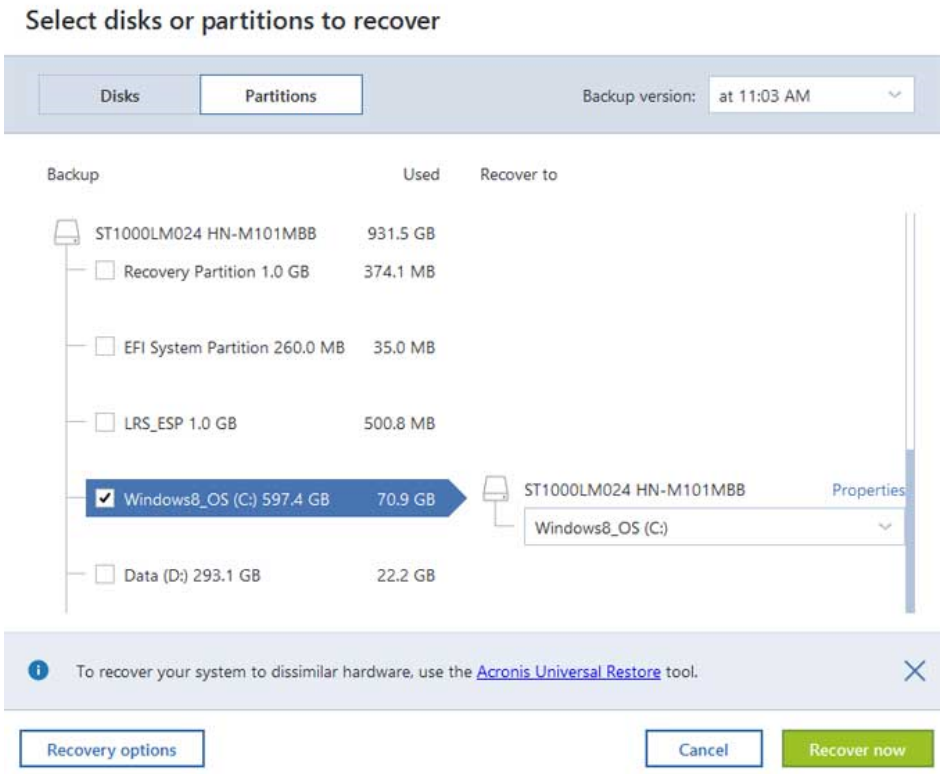
Step 4


Acronis True Image Cloud
ST1000L...
Cloud Re...
Acronis Cloud
Entire PC ...
F:\Acronis Backu...
Disks and partitions
106.0 GB
Disks: ST1000LM024 HN-M101MBB
LACIE (F:\)
108.4 GB of 232.8 GB free
Encrypt backup
Options
Cancel
Back up now

Step 5


Disk backup options
Schedule
Backup scheme
Notifications
Exclusions
Advanced
Daily
Weekly
Monthly
Upon event
Nonstop
Do not schedule
Weekly
Start at 10:25 PM
Mon
Tue
Wed
Thu
Fri
Sat
Sun
Advanced settings

Step 6


Select disks or partitions to recover
Disks
Partitions
Backup version:
at 11:03 AM
Backup
Used
Recover to
ST1000LM024 HN-M101MBB
931.5 GB
Recovery Partition 1.0 GB
374.1 MB
EFI System Partition 260.0 MB
35.0 MB
LRS_ESP 1.0 GB
500.8 MB
Windows8_OS (C:) 597.4 GB
70.9 GB
ST1000LM024 HN-M101MBB
Properties
Windows8_OS (C:)
Data (D:) 293.1 GB
22.2 GB
To recover your system to dissimilar hardware, use the Acronis Universal Restore tool.
Recovery options
Cancel
Recover now

Self-Check Sheet 2: Performing OS Backup

1. What is a partition table?

2. Why is it important to prepare a backup plan before partitioning?

3. What tools are commonly used for operating system backup?

4. What is the target for backup in a backup plan?

5. What does the backup procedure involve?

Answer Key 2: Performing OS Backup

1. What is a partition table?
   Answer: A partition table is a data structure on storage devices that organizes the disk into partitions, defining their size, location, and type.
2. Why is it important to prepare a backup plan before partitioning?
   Answer: Preparing a backup plan before partitioning helps safeguard against data loss or corruption during the process, providing assurance and recovery options in case of unexpected issues.
3. What tools are commonly used for operating system backup?
   Answer: Common tools for operating system backup include built-in utilities like Windows Backup and Restore, Time Machine on macOS, and third-party software such as Acronis True Image and EaseUS Todo Backup.
4. What is the target for backup in a backup plan?
   Answer: The target for backup refers to the destination where backup copies are stored, such as external hard drives, network-attached storage (NAS), cloud storage services, or tape drives.
5. What does the backup procedure involve?
   Answer: The backup procedure involves selecting the data to be backed up, choosing the backup method and target, executing the backup process, monitoring its progress, and verifying the integrity of backup copies.

Task Sheet 2.1: Perform OS Backup

TASK SHEET 2.1
Title: Perform OS Backup
Performance Objective: At the end of this task, the trainee should be able to Identify and gather tools for backing up the operating system (OS) and system files., Determine the destination for storing backup copies of data and system files and Execute the backup process according to the prepared backup plan.
1. Assess the importance of data to determine backup priorities.
2. Choose backup methods and schedule for regular backups.
3. Determine backup destinations and storage options.
4. Document the backup plan, including procedures and schedules.
5. Identify backup tools available for your operating system (e.g., Windows, macOS, Linux).
6. Collect information on built-in backup utilities and third-party software options.
7. Evaluate the features, capabilities, and compatibility of backup tools.
8. Download or acquire selected backup tools for testing and implementation.
9. Consider factors such as storage capacity, accessibility, security, and cost.
10. Select one or more backup targets based on your requirements and preferences.
11. Document the chosen backup targets and their configurations.
12. Identify the data and system files to be backed up, including user data, application settings, and system configurations.
13. Launch the selected backup tool or utility.
14. Configure backup settings, including backup method, schedule, and target destination.
15. Initiate the backup process and monitor its progress.
16. Verify the integrity and completeness of backup copies after the backup procedure completes.

Specification sheet 2.1: Perform OS Backup

A. Tools and Material required:

- Notebook
- Software
- Office Stationeries

B. Equipment:

- Laptop/Computer

Learning Outcome 3: Perform user data backup

Assessment Criteria:

1. Backup Plan is prepared
2. Tools for user data backup is identified and collected
3. Target for backup is identified
4. Backup procedure is performed.

Content:

1. Backup Plan
2. Tools for user data backup
3. Target for backup
4. Backup procedure.

Resources Required/ Conditions:

The trainees must be provided with the following:

- Handouts or reference materials/books/ CBLMs on the above stated contents
- PCs/printers or laptop/printer with internet access
- Digital projector and Screen
- Bond paper
- Ball pens/pencils and other office supplies and materials
- Relevant learning materials
- Workplace or simulated environment

Methodologies

- Lecture/discussion
- Demonstration/application
- Presentation
- Blended delivery methods

Assessment Methods

- Written test
- Demonstration
- Observation with checklist
- Oral questioning
- Portfolio

Learning Experience 3: Perform user data backup

In order to achieve the objectives stated in this learning guide, you must perform the learning steps below. Beside each step are the resources or special instructions you will use to accomplish the corresponding activity.

Learning Steps	Resources specific instructions
1. Student will ask the instructor about Performing user data backup.	1. Instructor will provide the learning materials "**Performing Basic Data Backup and Recovery"**
2. Read the Information sheet/s	2. Information Sheet No 3: Performing user data backup.
3. Complete the Self Checks & Check answer sheets.	3. Self-Check/s Self-Check No 3: Performing user data backup. Answer key No. 3: Performing user data backup.
4. Read the Job Sheet and Specification Sheet and perform job	4. Job- Sheet No 3-1: Performing user data backup. Specification Sheet 3-1: Performing user data backup.

Information Sheet 3: Performing user data backup.

Learning Objectives:

After completion of this information sheet, the learners will be able to:

3.1 Prepare Backup Plan
3.2 Identify and collect Tools for user data backup
3.3 Identify Target for backup
3.4 Perform Backup procedure.

3.1 Backup Plan

A well-defined backup plan is crucial for protecting your valuable user data from potential disasters, hardware failures, or accidental deletion. Here's a guide to help you prepare a comprehensive backup plan:

Identify User Data and Needs:

Data Classification: Categorize user data based on its criticality. This helps prioritize backup frequency and recovery needs.

Critical data (financial records, legal documents) requires more frequent backups and faster recovery times.

Less critical data (personal documents, entertainment media) can have less frequent backups.

User Input: Consider user input and preferences. Some users may require more frequent backups for specific data sets.

3.2 Choose Backup Tools:

Built-in OS tools: Most operating systems offer basic backup utilities.

Third-party backup software: Provides more features like scheduling, encryption, and version control.

Consider factors like ease of use, scalability, and security features when choosing a tool.

3.3 Select Backup Targets:

Local Storage: External hard drives or SSDs offer fast access times for recovery but are susceptible to physical damage.

Network-Attached Storage (NAS): Centralized storage for multiple computers, good for large datasets but requires network setup.

Cloud Storage: Convenient remote backup option, good for disaster recovery but may have bandwidth limitations and potential costs.

3.4 Backups procedure:

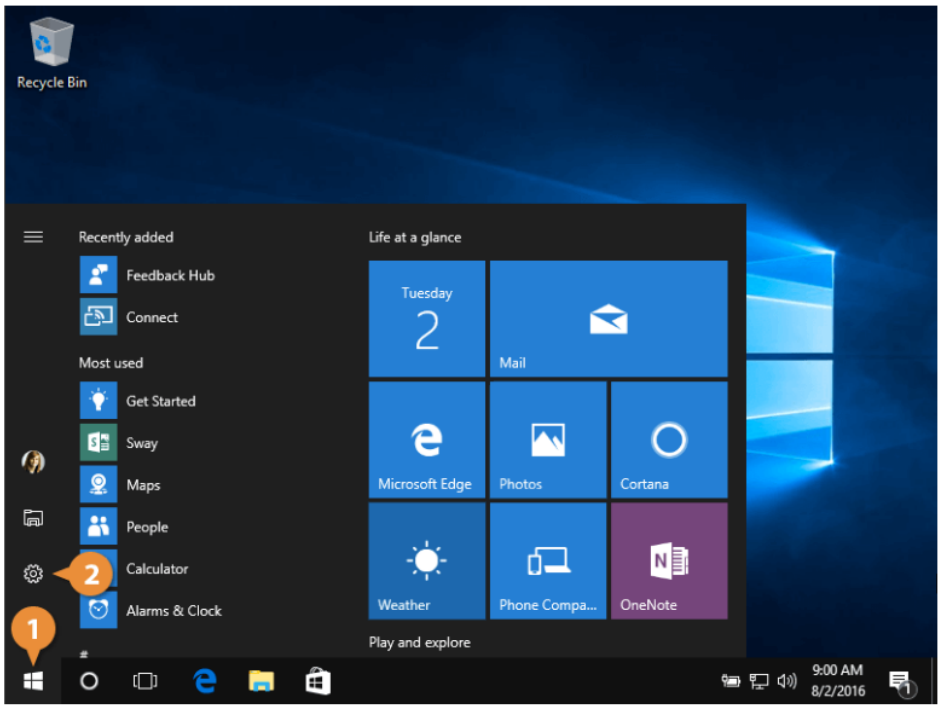
- Run the backup software.
- Select the data sources (user folders, applications).
- Choose the backup target location.
- Initiate the backup process and monitor its progress.

Backup a local Windows 10 user profile and restore it in Windows 10

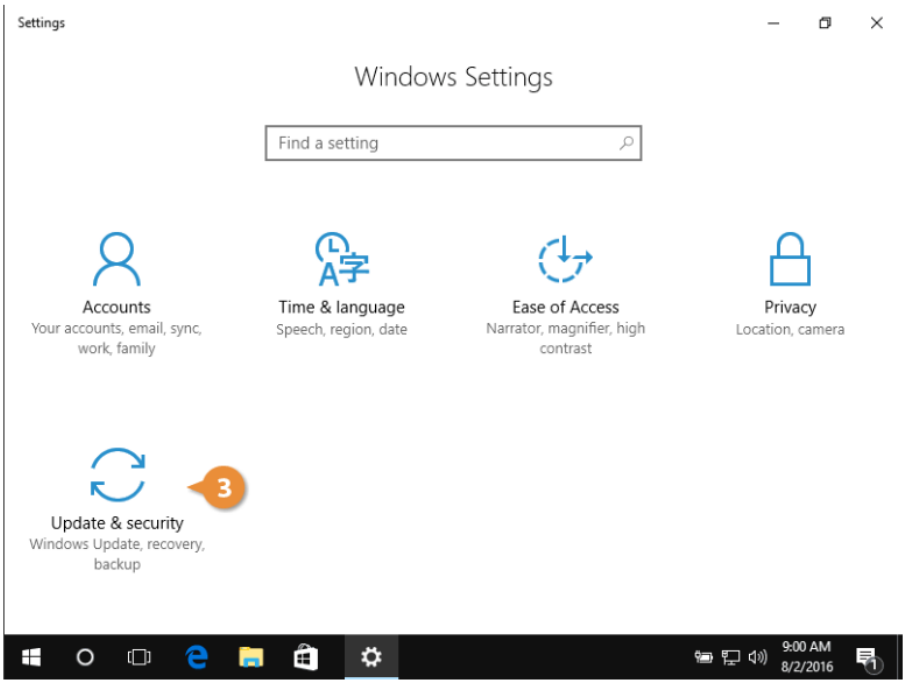
Add a Backup Drive

Click the Start button.

Click the Settings button.



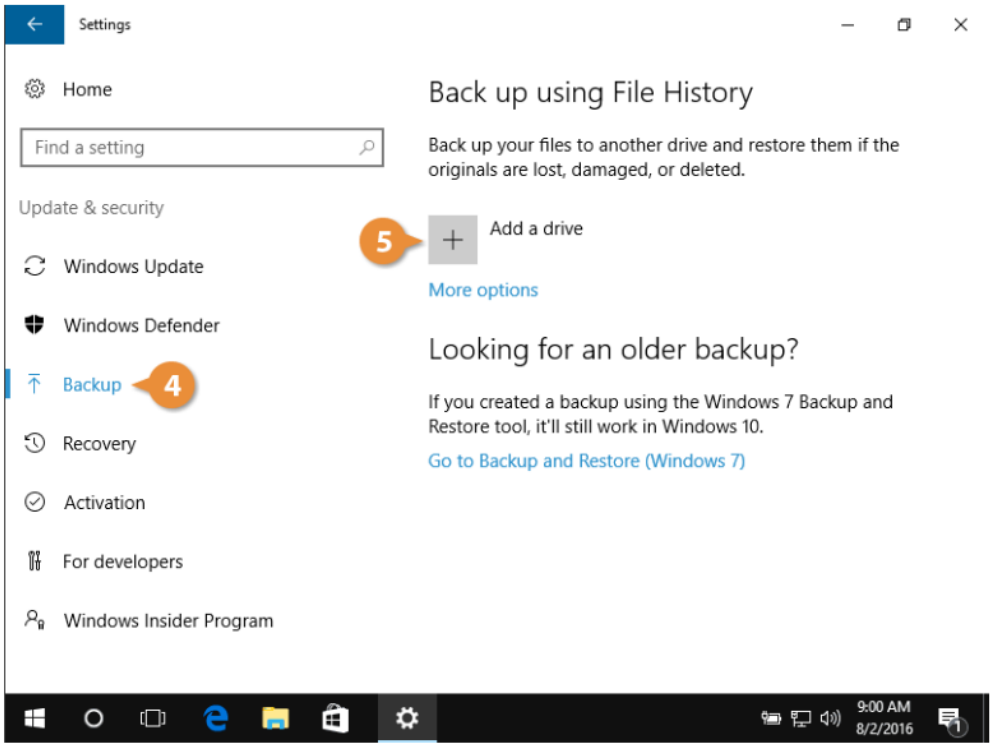
Click Update & security.



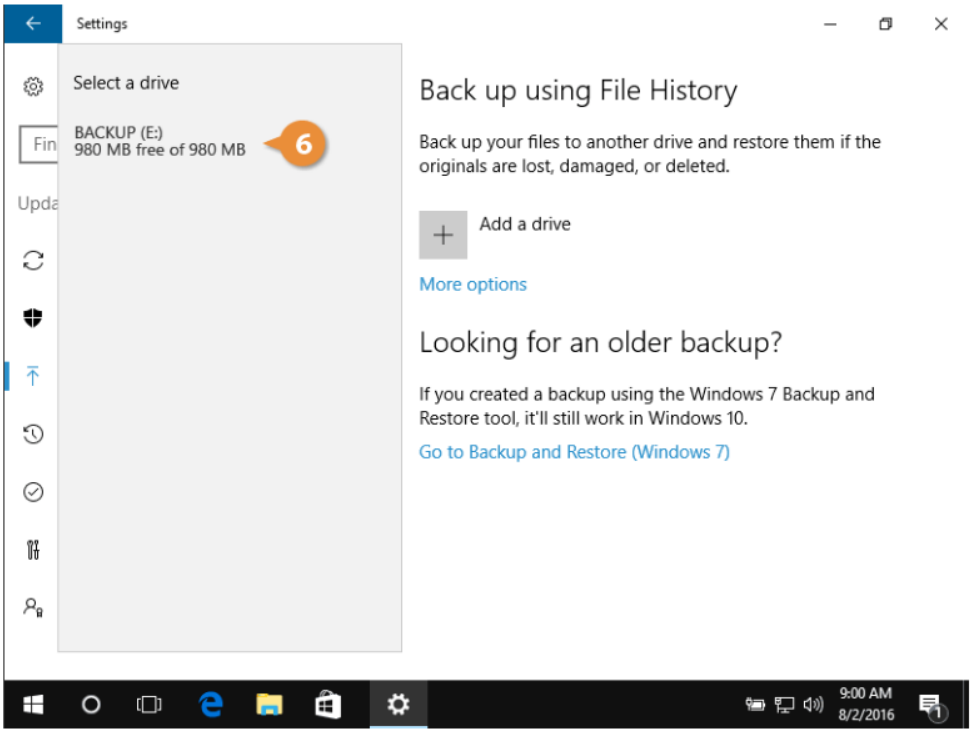
Choose Backup.

(Any connected external hard drives appear.)

Connect an external hard drive, and then click Add a drive.

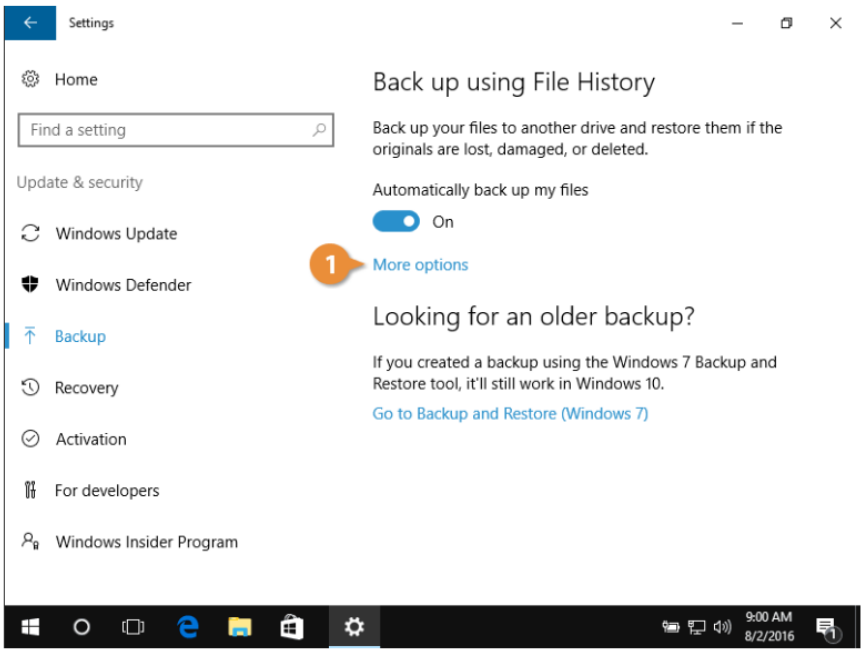


Select a drive from the list.

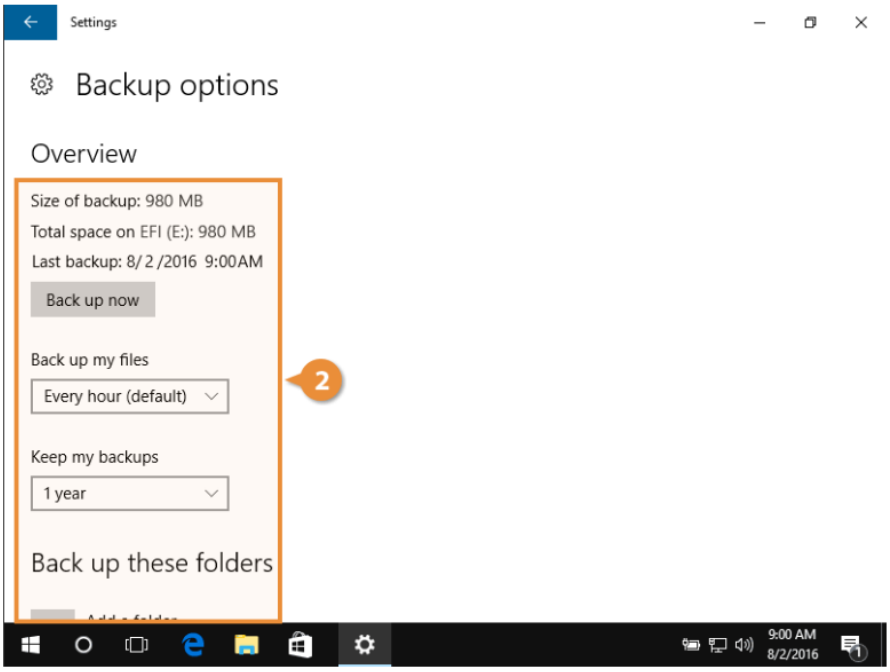


Customize a Backup

Click More options under Back up using File History.

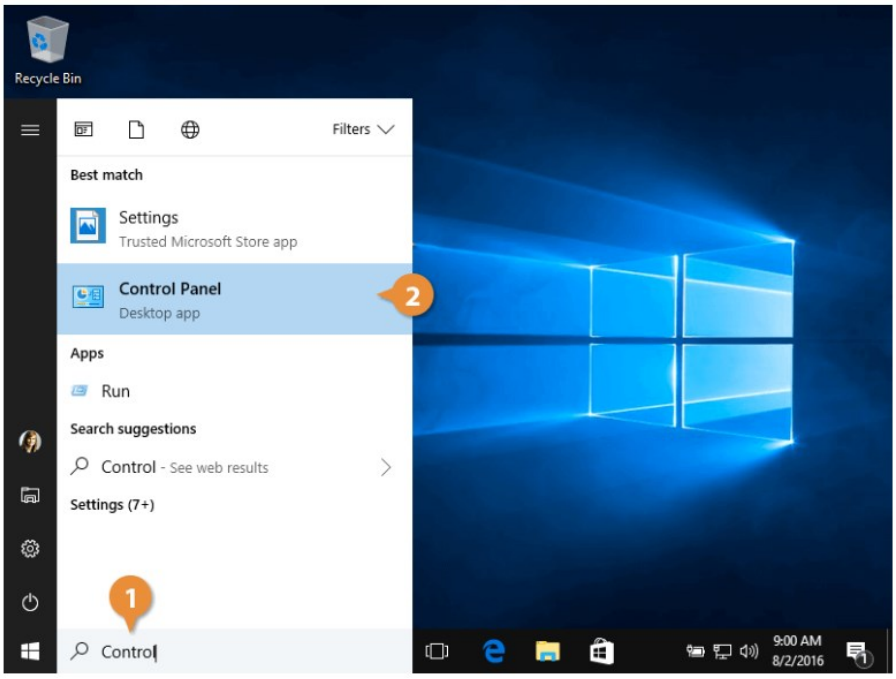


Configure your backup settings according to your specifications.

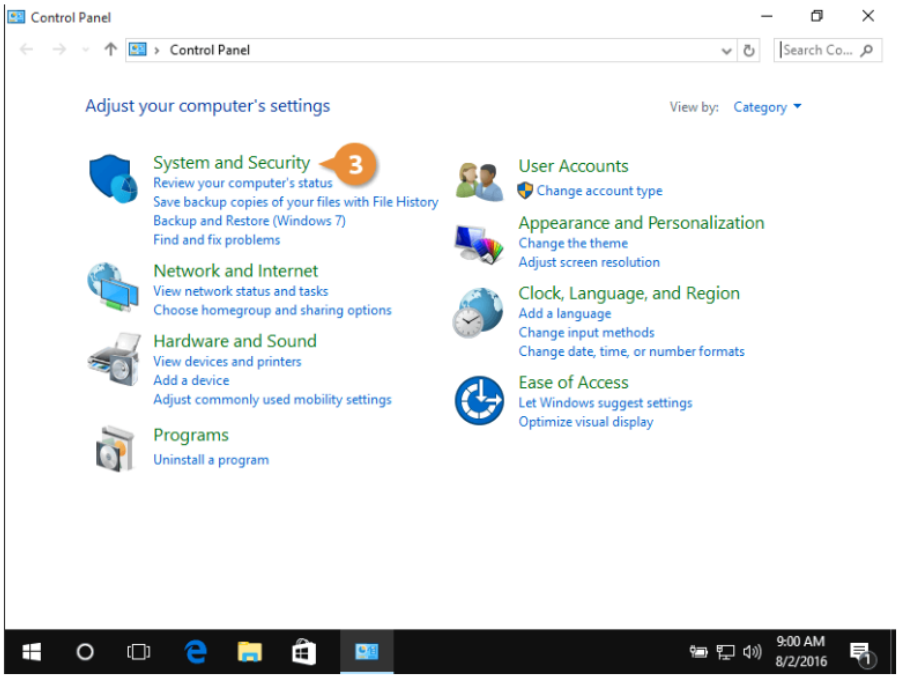


Restore Your Files

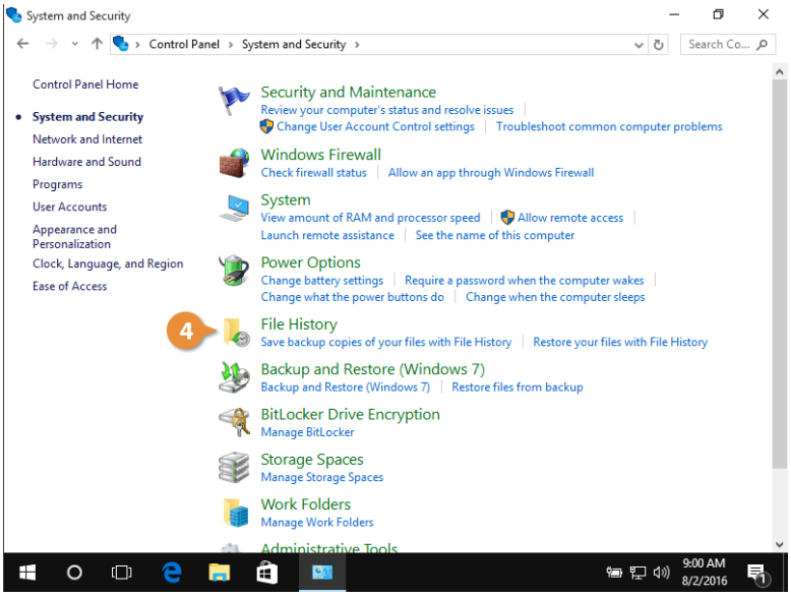
Enter Control in the search field.
Choose Control Panel.



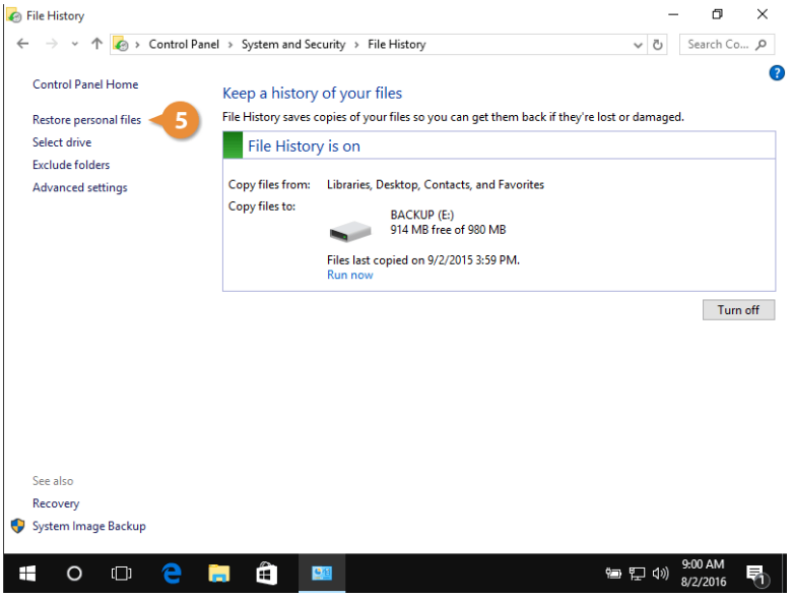
Click System and Security



Click File History



Choose Restore personal files.



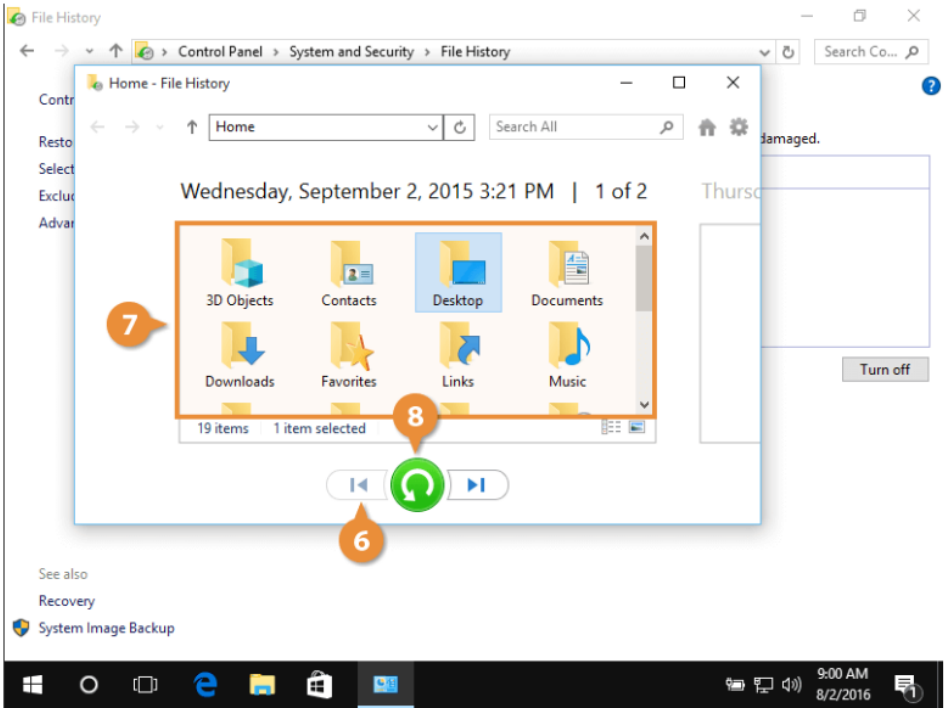
Click the Previous Version button.

System Backup:
Create a system image or full backup of the entire system drive using backup and recovery software.

System backups capture the entire operating system, including installed programs, settings, and files, allowing for complete system restoration if needed.

Select an individual file or entire folder to restore.

Click the Restore button.



Self-Check Sheet 3: Perform user data backup.

1. Why is it important to have a backup plan for user data?

2. What tools can be used to back up user data?

3. Where can you store backed-up user data?

4. What steps are involved in performing a user data backup?

5. How can you ensure the effectiveness of your user data backup plan?

Answer Key 3: Perform user data backup.

1. Why is it important to have a backup plan for user data?
   Answer: A backup plan protects user data from accidental deletion, hardware failures, and disasters. It ensures you can recover information if something goes wrong.

2. What tools can be used to back up user data?
   Answer: There are two main options: built-in operating system tools (basic) and third-party backup software (more features like scheduling and encryption).

3. Where can you store backed-up user data?
   Answer: Common targets include local storage (external hard drives), network-attached storage (NAS), and cloud storage (convenient but may have limitations).

4. What steps are involved in performing a user data backup?
   Answer: The process involves scheduling backups, selecting data and target location, running the backup software, and verifying completion.

5. How can you ensure the effectiveness of your user data backup plan?
   Answer: Regularly test backups by restoring a sample of data, maintain multiple backup copies, and follow secure storage practices.

Task Sheet 3.1: Prepare and Implement a User Data Backup Plan.

Title: Prepare and Implement a User Data Backup Plan
Performance Objective: By the end of this task, the trainee should be able to establish a reliable system for backing up user data and ensure its safety and recoverability.
1. List all types of data stored by users (documents, emails, photos, etc.).
2. Classify data based on criticality (essential documents vs. entertainment media).
3. Choose Backup method
4. Identify backup tools
5. Select backup target
6. Install and configure backup software
7. Perform initial backup
8. Ensure each backup finishes successfully and all data is copied to the target location.

Learning Outcome 4: Perform email backup

Assessment Criteria:

4.1 Mail client is identified and configured.
4.2 Local Database file of mail client is identified
4.3 Email Backup Plan is prepared
4.4 Target for backup is identified
4.5 Backup procedure is performed

Content:

1. Mail client.
   1.1 Outlook (Windows)
   1.2 Thunder Bird (Linux)
2. Local Database file of mail client
3. Email Backup Plan
   3.1. Import/ Export
   3.2. Manual
4. Target for backup is identified
5. Backup procedure is performed

Resources Required/ Conditions:

The trainees must be provided with the following:

- Handouts or reference materials/books/ CBLMs on the above stated contents
- PCs/printers or laptop/printer with internet access
- Digital projector and Screen
- Bond paper
- Ball pens/pencils and other office supplies and materials
- Relevant learning materials
- Workplace or simulated environment

Methodologies

- Lecture/discussion
- Demonstration/application
- Presentation
- Blended delivery methods

Assessment Methods

- Written test
- Demonstration
- Observation with checklist
- Oral questioning
- Portfolio

Learning Experience 4: Perform email backup

In order to achieve the objectives stated in this learning guide, you must perform the learning steps below. Beside each step are the resources or special instructions you will use to accomplish the corresponding activity.

Learning Steps	Resources specific instructions
1. Student will ask the instructor about Performing email backup.	1. Instructor will provide the learning materials "**Performing Basic Data Backup and Recovery"**
2. Read the Information sheet/s	2. Information Sheet No: 4 Performing email backup
3. Complete the Self Checks & Check answer sheets.	3. Self-Check/s Self-Check No: 4 Performing email backup Answer key No. 4 Performing email backup
4. Read the Job Sheet and Specification Sheet and perform job	4. Job- Sheet No: 4 Performing email backup Specification Sheet: 4 Performing email backup

Information Sheet 4: Performing email backup

Learning Objectives:

After completion of this information sheet, the learners will be able to:

4.1 Identify and configure Mail client.
4.2 Identify Local Database file of mail client
4.3 Prepare Email Backup Plan
4.4 Identify Target for backup
4.5 Perform Backup procedure

4.1 Mail Client

A mail client, also known as an email client, message user agent (MUA), or mail user agent, is a software application you use to manage your email. It provides a user interface for you to:

Compose emails: Write new emails, including adding recipients, subject lines, attachments, and body content.

- Send emails: Transmit your composed emails to the intended recipients through an email server.
- Receive emails: Download emails sent to you from other email addresses through an email server.
- Read and organize emails: View received emails, reply to them, forward them, organize them into folders, and delete them as needed.

Types of Mail Clients:

There are two main types of mail clients:

- Desktop Mail Clients: Software applications installed on your computer (Windows, macOS, etc.). Examples include Microsoft Outlook, Mozilla Thunderbird, Apple Mail.
- Webmail Clients: Web-based interfaces accessed through a web browser. Examples include Gmail, Yahoo Mail, Hotmail/Outlook.com.

Configuring a mail client

Configuring a mail client involves setting it up to work with your specific email account. This process allows the client to communicate with your email server and send/receive emails on your behalf. Here's a breakdown of the general steps involved:

Gather Information:

Before you begin configuration, you'll need some information about your email account:

Email Address: Your full email address (e.g., [email address removed]).

Password: The password associated with your email account.

Incoming Mail Server (IMAP or POP3): The server address used to download your emails. This information can be found in your email provider's settings or help

documentation (e.g., [invalid URL removed] or [invalid URL removed]).

Outgoing Mail Server (SMTP): The server address used to send emails. This information can also be found in your email provider's settings or help documentation (e.g., [invalid URL removed]).

Port Numbers (Optional): Some email providers may require specific port numbers for incoming and outgoing mail server connections. These are typically listed alongside the server addresses.

Launch Your Mail Client:
Open your chosen mail client application (e.g., Microsoft Outlook, Mozilla Thunderbird, Apple Mail, Gmail web interface).

Locate Account Settings:
Navigate to the section where you can add or configure email accounts. This might be labeled "Accounts," "Settings," or something similar depending on the client.

Add a New Account:
Look for an option to "Add Account," "Create Account," or something similar. This will initiate the account setup process.

Enter Your Email Address:
Provide your full email address in the designated field.

Select Account Type (Optional):
Some mail clients might ask you to choose the type of account you're setting up. In most cases, select "IMAP" for better email management features like keeping copies of emails on both the server and your device. POP3 is an option if you only need to access emails from one device.

Configure Server Settings:

- Incoming Mail Server: Enter the incoming mail server address (IMAP or POP3 server) obtained in step 1.
- Outgoing Mail Server: Enter the outgoing mail server address (SMTP server) obtained in step 1.
- Port Numbers (Optional): If provided by your email provider, enter the specific port numbers for incoming and outgoing mail server connections.

Enter Login Credentials:

- Username: Enter your full email address again (usually the same as what you entered earlier).
- Password: Enter the password associated with your email account.

Test the Connection (Optional):
Many mail clients offer a "Test Settings" button. This allows you to verify if the configuration is correct and your mail client can successfully connect to the email servers.

Save and Finish:
Once you've entered all the information and (optionally) tested the connection, save the configuration and complete the account setup process.

4.2 Identifying the local database file of a mail client can be tricky because:

Webmail clients like Gmail or Outlook.com function entirely online. Your emails and data reside on the provider's servers, and you access them through a web browser. There's no local database file in this case.

Desktop mail clients like Thunderbird or Outlook might store data locally depending on the configuration and chosen features. However, they often use a specific database format that's not easily readable or accessible without the mail client application itself.

Desktop Mail Clients:

- **Possible Local Storage:** If configured to store emails locally, the mail client might have a designated folder on your device where it keeps email data. However, this data is likely stored in a proprietary format specific to the mail client and not directly accessible as a standard database file (e.g., .sql, .mdb).

- **Challenges in Identifying:** File names and locations can vary depending on the mail client, operating system, and user configuration.
- The data within these files is often not meant to be directly accessed or modified by users. It's designed for the mail client software to use internally.

- **Alternatives to Local Database Access:** Exporting Mail Data: Many mail clients allow you to export your emails to a standard format like .eml or .pst. This can be a more reliable way to access and manage your email data if needed. Explore your mail client's settings or help documentation for export options.

- **Cloud Backups:** Some mail clients offer cloud backup features that store your emails on a remote server. This can be a good option for safeguarding your data and potentially accessing it from other devices.

4.3 Email Backup Plan

Identify Email Accounts and Needs:

- **List all email accounts:** Create a list of all the email accounts you want to back up (personal, work, etc.).
- **Prioritize based on importance:** Categorize accounts based on criticality. High-priority accounts (work emails) might require more frequent backups than less critical ones (personal accounts).

Choose Backup Method:
There are two main methods for email backups:

- Exporting Emails: This involves converting emails to a standard format like .eml or .pst. This creates individual files for each email but doesn't preserve folder structure.
- Backing Up Mail Client Data (if applicable): This involves copying the entire local database file where your mail client stores emails (applicable only for desktop clients with local storage enabled). However, this data is often in a proprietary format and not user-friendly.

4.4 Select Backup Target:

Choose a secure location to store your backups

- Local Storage: External hard drives (fast access but vulnerable to physical damage).
- Cloud Storage: Convenient remote option (bandwidth limitations and potential costs).
- Combination: Consider a hybrid approach, backing up locally for faster access and to the cloud for disaster recovery.

Choose Backup Tools:
The tools you use depend on your chosen backup method:

- Exporting Emails: Use the built-in export functionality of your webmail client (Gmail, Outlook) or desktop mail client (Thunderbird, Outlook).
- Backing Up Mail Client Data: This typically requires specialized tools provided by the mail client or third-party backup software (complex and may not be necessary for most users).

Automate Backups (Optional):
If your chosen method and tools support it, automate backups to ensure consistency and avoid human error.

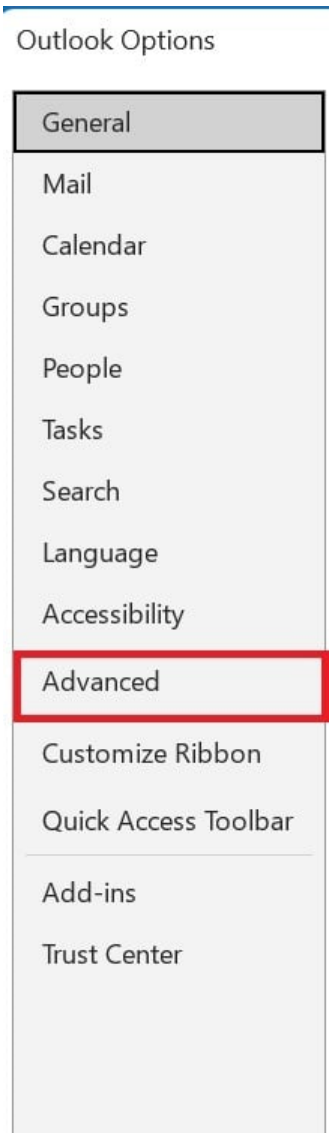
Perform Initial Backup:
Run the chosen method (export or mail client backup) to create an initial backup of your email data.

4.5 Backup Outlook Emails (Outlook Data File PST)

Outlook provides an option to export your emails, calendar, and tasks to a .pst file. This file can then be imported to another email account or used as a backup.
The process involves selecting the desired email account in Outlook and exporting the items to a .pst file. When Outlook exports to a .pst, it creates a copy, ensuring nothing is removed from Outlook.
Use the following steps to backup Outlook emails to a .pst file:

Open Microsoft Outlook.
Go to the File tab in the top menu.

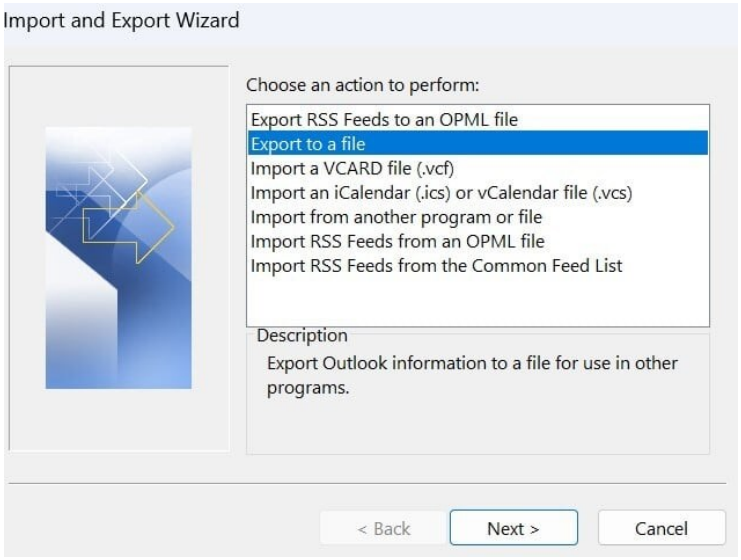
Click on Options > Advanced.



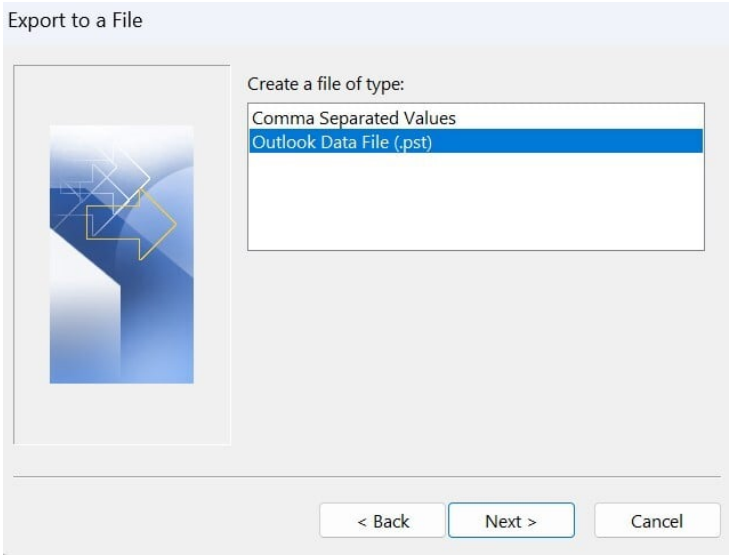
Scroll down to the Export category.

Click on Export.

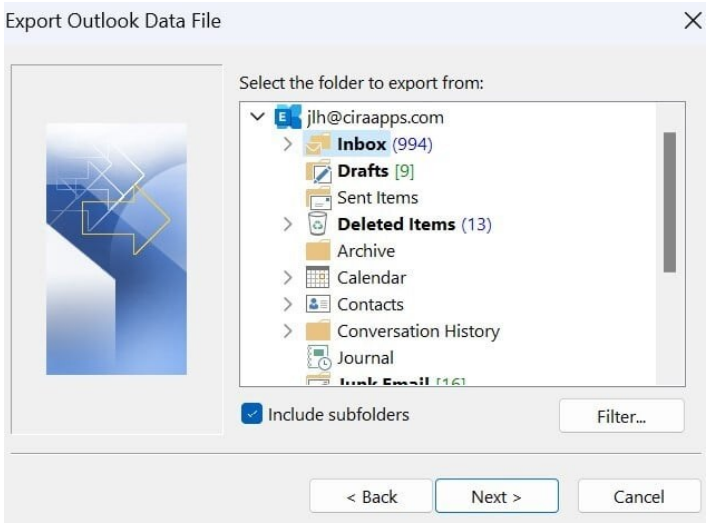
In the Import and Export Wizard, choose “Export to a file” and click Next.



Select Outlook Data File (.pst) and click Next.

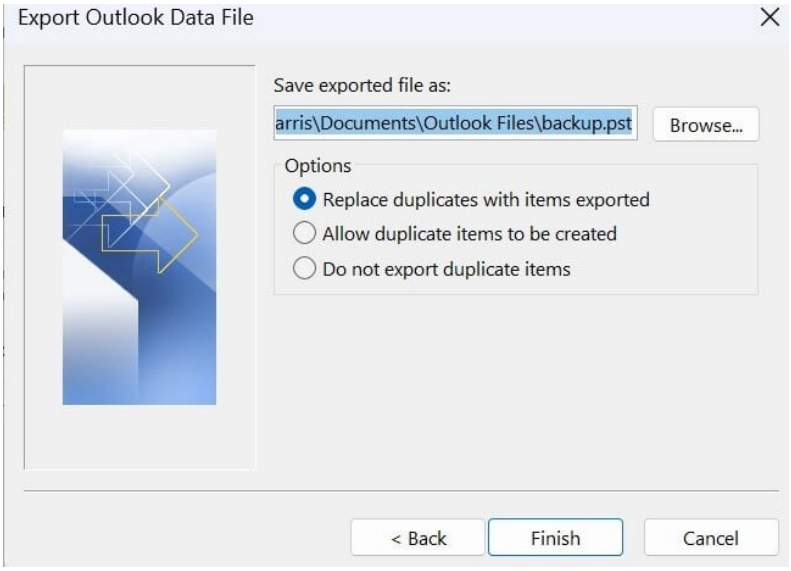


Choose the email folder you wish to back up. Select your email address at the top to back up your entire mailbox.



Click Next.

Choose a location to save your .pst file and provide a name.



Click Finish.

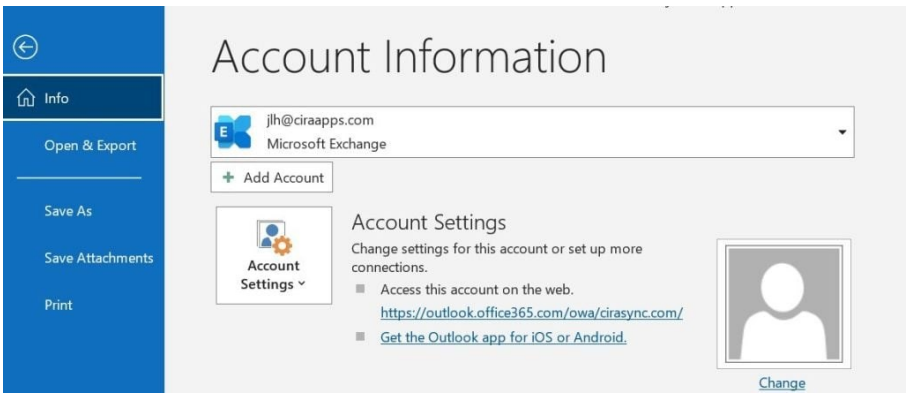
Backup Outlook Emails To Gmail

For people who want to back up their Outlook emails to another email service like Gmail, the process involves adding Outlook and Gmail accounts to the Outlook desktop app. Once both accounts are set up, users can use Outlook to export the emails from the Outlook account to a .pst file and then import this file to the Gmail account.

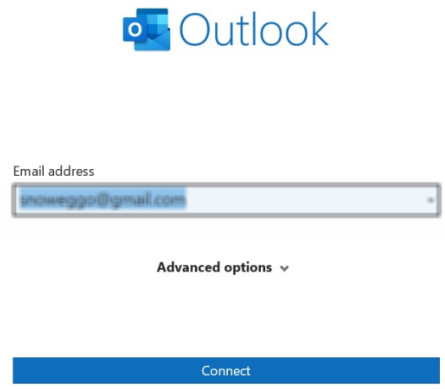
Export your Outlook emails to Gmail using the steps below:

Navigate to the File tab in Microsoft Outlook.

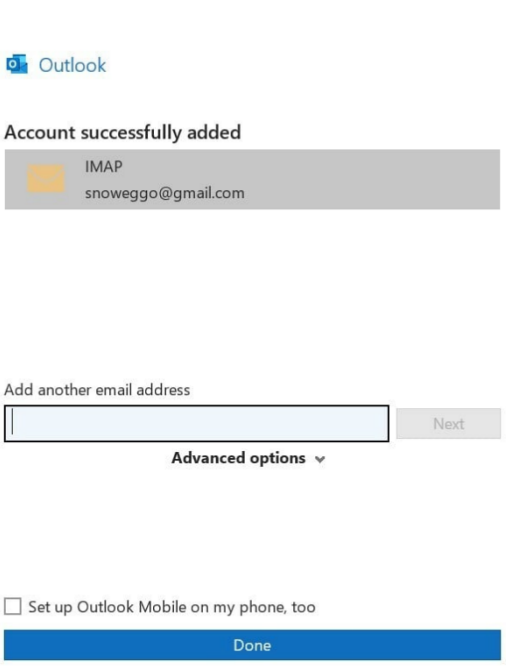
Click Add Account to add your Gmail account.



Follow the prompts to complete the Gmail setup.



4. Once both accounts (Outlook and Gmail) are added, right-click on the desired Outlook



folder or individual emails.

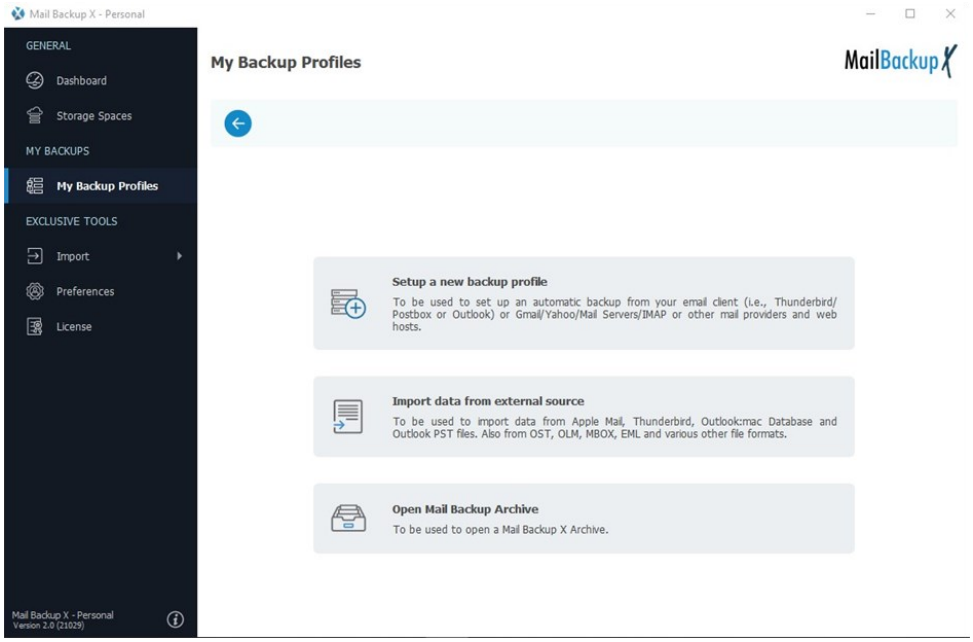
5. Choose Move > Copy to Folder.

6. Select the corresponding folder in your Gmail account.

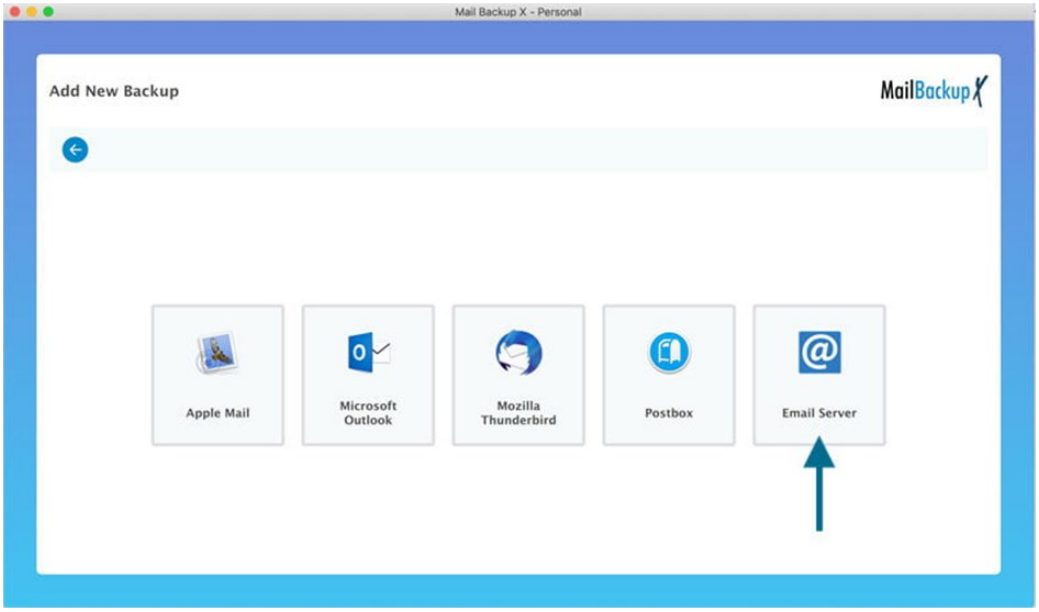
7. Click OK.

Backup Gmail

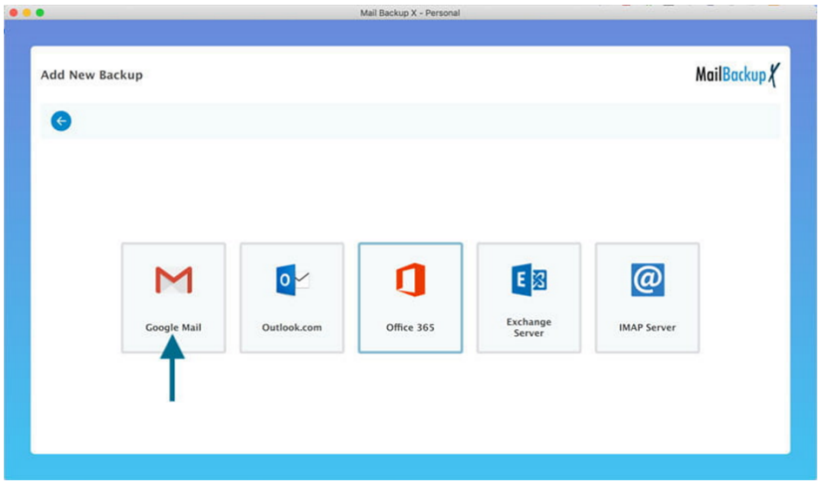
You just need to download the software and launch it. Just double click on the tool icon to launch the tool. Once you launch the tool, you will see a new window. Here you can click on setup a new backup profile



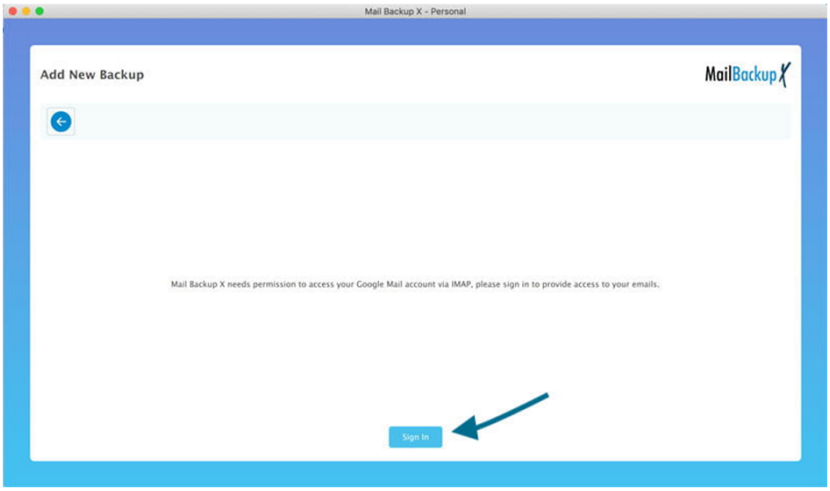
Now you are at the next window. Here you can choose the email services that you wish to back up. Here, you have to choose email server so that you can be taken forward in the process.



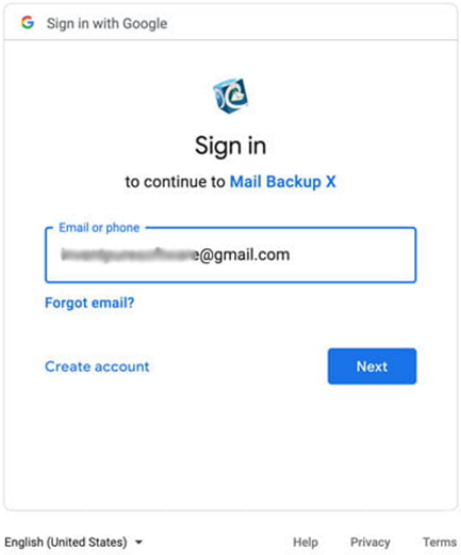
Now, you can see one more window with even more email services. You will find that this window has Google mail as an option. You have to click on it.



You will be taken to the next part of the process where you have to click on the option to sign into your email account.

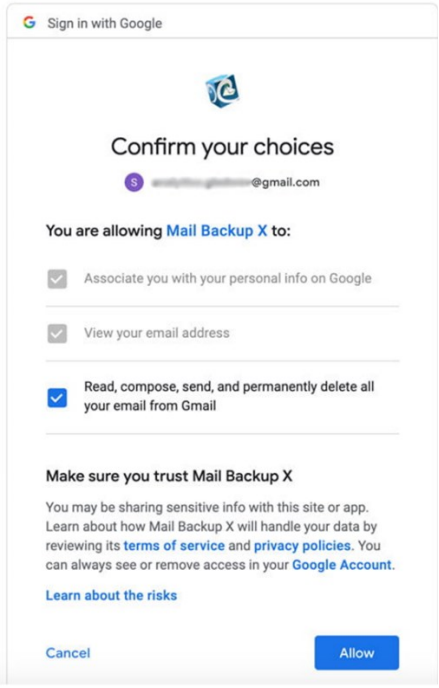


The tool will ask you to enter your Gmail email credentials. Once you are done, you have to click next. Remember, your emails are secure. Click on next.

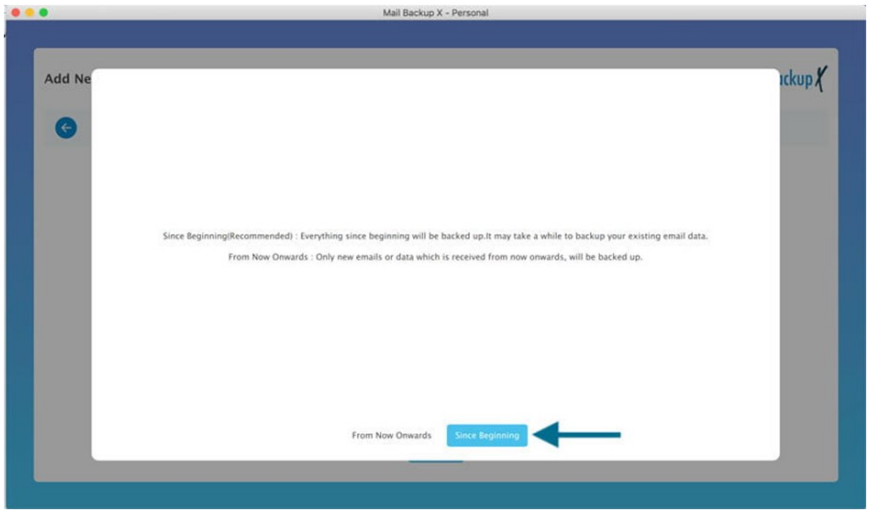


Once you are here, you will be asked to give access to your email data so that the tool can fetch it and help you in managing it. Everything is secure and is done via a Google authenticated log in window.

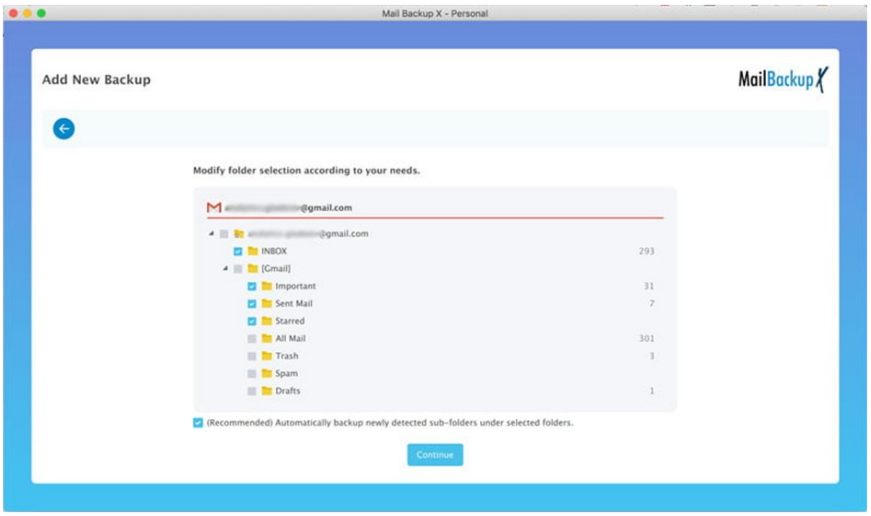
Click on allow.



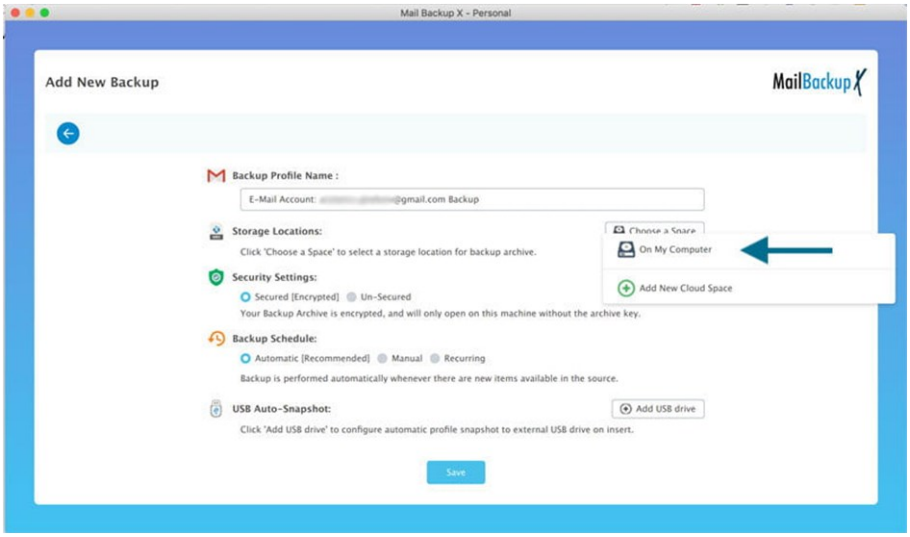
You can select the time period for which you wish your emails to be backed up. You need to click on “Since the beginning” if you want the best results. Clicking on this will take you to the next part in the process.



Now you will see that you are at the filter item window. Here, you get to select only those emails that you wish to back up. Once you are sure that you have selected the emails that you need backed up, click on continue. You can also unselect the email items or folders that you don’t want to include in your backup.



Now, the tool brings you to the advanced settings window. Here, you are asked to change or modify your email profile like you want. You can modify your end results by modifying the settings in this window.



Here are the settings or changes that you get on the advanced settings window.

- Name your email profile

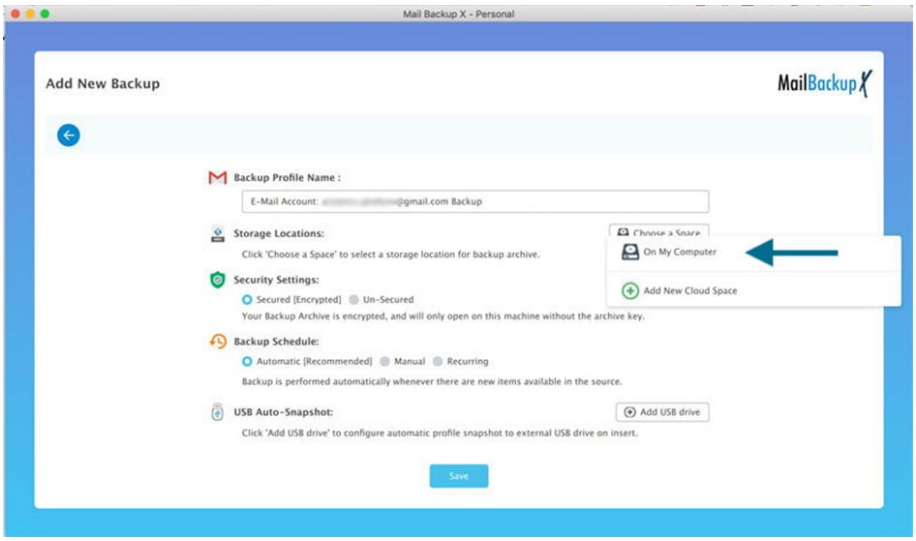
- Choose your desired email backup frequency

- Choose where your emails are stored

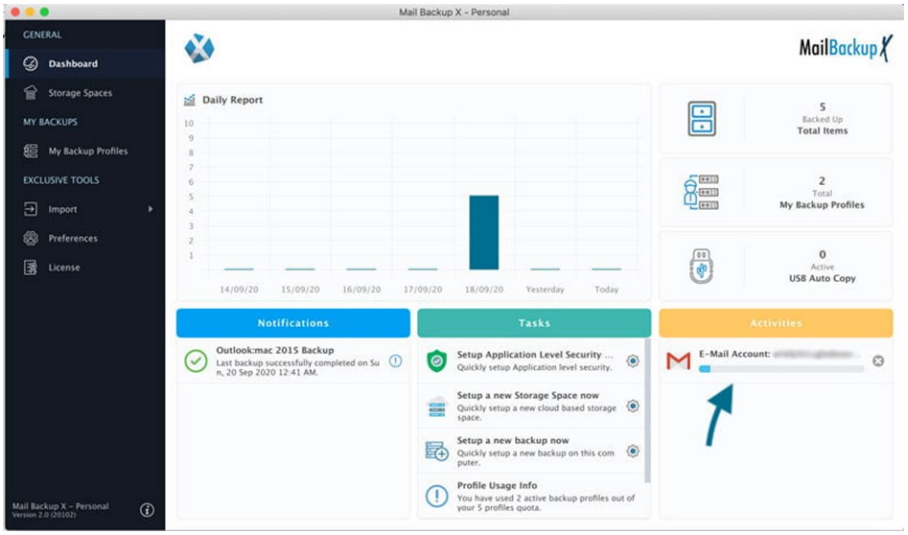
- Choose a cloud service to store your backed up emails

- Map a USB drive to create instant portable backups

- Set up a strong password to protect your backed up email mailboxes



Now, most of the work is done. You just need to hit the save button to initiate the final backup process. The backup will start instantly when you click on save.



As soon as you click on the save button, your backup process will start. You can keep an eye on the whole process after it starts. You can track the live progress of the process once the process is started.

Self-Check Sheet 4: Perform email backup

1. What do I need to configure a mail client?

2. Can I access the local database file of my mail client?

3. How can I back up my emails?

4. Where should I store my email backups?

5. How often should I back up my emails?

Answer Key 4: Perform email backup

1. What do I need to configure a mail client?
   Answer: You'll need your email address, password, and server settings (incoming and outgoing mail server addresses, potentially with port numbers) from your email provider.
2. Can I access the local database file of my mail client?
   Answer: Maybe, but it's not recommended. Webmail clients don't have local files. Desktop clients might store data locally, but it's in a proprietary format and not meant for direct access.
3. How can I back up my emails?
   Answer: There are two main options: export your emails to a standard format like .eml or back up your mail client's data file (if applicable).
4. Where should I store my email backups?
   Answer: Consider local storage (external hard drive) for faster access and cloud storage for disaster recovery. A combination approach can be ideal.
5. How often should I back up my emails?
   Answer: The frequency depends on importance. Back up high-priority accounts more often (daily) and less critical ones less frequently (weekly/monthly).

Task Sheet 4.1: Perform email backup

Performance Objective: By the end of this task, the trainee should be able to Performing email backup:
1. Locate your email address and password.
2. Obtain incoming and outgoing mail server addresses (IMAP/POP3 and SMTP) from your email provider's settings or help documentation. (They may also specify port numbers)
3. Open your chosen mail client application (e.g., Outlook, Thunderbird, Gmail web interface)
4. Locate Account Settings
5. Add a New Account
6. Enter Information:
7. Save and Finish
8. Export emails using your webmail client or desktop mail client's export functionality (if applicable).
9. Use specialized tools (if necessary) to back up mail client data (complex, not common for most users).
10. Ensure the backup process finishes successfully and includes all desired emails

Learning Outcome 5: Perform backup recovery

Assessment Criteria:

5.1 Backup is collected for recovery
5.2 Tools are identified and selected for recovery.
5.3 Recovery target is identified
5.4 Restore point is identified
5.5 Restore procedure is performed

Content:

1. Backup for recovery
2. Tools for recovery.
3. Recovery target
4. Restore point
5. Restore procedure

Resources Required/ Conditions:

The trainees must be provided with the following:

- Handouts or reference materials/books/ CBLMs on the above stated contents
- PCs/printers or laptop/printer with internet access
- Digital projector and Screen
- Bond paper
- Ball pens/pencils and other office supplies and materials
- Relevant learning materials
- Workplace or simulated environment

Methodologies

- Lecture/discussion
- Demonstration/application
- Presentation
- Blended delivery methods

Assessment Methods

- Written test
- Demonstration
- Observation with checklist
- Oral questioning
- Portfolio

Learning Experience 5: Perform backup recovery

In order to achieve the objectives stated in this learning guide, you must perform the learning steps below. Beside each step are the resources or special instructions you will use to accomplish the corresponding activity.

Learning Steps	Resources specific instructions
5. Student will ask the instructor about performing backup recovery	5. Instructor will provide the learning materials "**Performing Basic Data Backup and Recovery"**
6. Read the Information sheet/s	6. Information Sheet No: 5 Performing backup recovery
7. Complete the Self Checks & Check answer sheets.	7. Self-Check/s Self-Check No: 5 Performing backup recovery Answer key No. 5 Performing backup recovery
8. Read the Job Sheet and Specification Sheet and perform job	8. Job- Sheet No: 5 Performing backup recovery Specification Sheet: 5 Performing backup recovery

Information Sheet 5: Performing backup recovery

Learning Objectives:

After completion of this information sheet, the learners will be able to:

5.1 Collect Backup for recovery
5.2 Identify and select Tools for recovery.
5.3 Identify Recovery target
5.4 Identify Restore point
5.5 Perform Restore procedure

5.1 Backup for Recovery: Protecting Your Valuable Data

A backup is a copy of your data stored in a separate location from the original. This copy serves as a safety net in case the original data is lost, corrupted, or accidentally deleted. Recovery refers to the process of restoring your data from a backup to its original location or a functional alternative. Here's a breakdown of the importance of backup and recovery:

Data Loss Prevention: Hardware failures, software malfunctions, cyberattacks, and human errors can all lead to data loss. A backup ensures you have a copy of your data to restore from in such scenarios.

Business Continuity: For businesses, data loss can disrupt operations and cause significant financial losses. A robust backup and recovery plan helps minimize downtime and ensures a quicker return to normal operations after a data loss event.

Peace of Mind: Knowing your data is safeguarded with backups provides peace of mind. You can work and manage your data with confidence, knowing you have a recovery option in case of unforeseen circumstances.

Types of Backups:

There are different types of backups depending on the frequency and how much data you need to capture:

Full Backups: Create a complete copy of all your data at a specific point in time. Good for initial backups or after significant changes.

Incremental Backups: Back up only the data that has changed since the last full backup, saving storage space but requiring the original full backup for restoration.

Differential Backups: Back up data that has changed since the last full backup (faster than full, but requires both differential and full back up for restore).

Backup Methods:

Local Storage: Backups can be stored on external hard drives or solid-state drives (SSDs) for quick access during recovery. However, these are susceptible to physical damage.

Cloud Storage: Backups can be stored in a remote cloud storage service, offering offsite protection and accessibility from anywhere. However, this might depend on internet connectivity and may incur costs.

Network-Attached Storage (NAS): A centralized storage device on your network can be used for backups, offering a balance between local access and redundancy.

Recovery Process:

The recovery process involves retrieving data from your backups and restoring it to its original location or an alternative functional location. The specific steps depend on your backup method and software used. It's crucial to regularly test your backups to ensure they are functional and can be used for successful recovery when needed.

Benefits of a Backup and Recovery Plan:

Improved Data Security: Backups safeguard your data from various threats and ensure its availability.

Reduced Downtime: A good recovery plan allows you to restore data quickly, minimizing disruption to your work or business operations.

Enhanced Business Continuity: By having a recovery plan in place, you can ensure your business can continue functioning even after a data loss event.

5.2 Data Recovery Tools:

These are software applications specifically designed to recover lost or corrupted data from various storage devices like hard drives, SSDs, memory cards, and USB drives. Here are some common types of data recovery software:

File Undelete Tools: These tools can recover recently deleted files that haven't been overwritten by new data.

Data Carving Tools: These tools scan storage devices for specific file signatures even if the file system is damaged or formatted.

Partition Recovery Tools: These tools can recover data from lost or deleted partitions on a storage device.

RAW Data Recovery Tools: These advanced tools attempt to recover data from severely damaged storage devices, often requiring technical expertise.

Features to Consider When Choosing Data Recovery Software:

Supported File Systems: Ensure the software supports the file system used by your storage device (e.g., NTFS, FAT32, exFAT).

Recovery Capabilities: Consider if you need basic file undelete functionality or advanced features like data carving.

Ease of Use: Choose software with a user-friendly interface, especially if you don't have technical expertise.

Data Preview: Look for software that allows you to preview recoverable files before full recovery to avoid wasting time.

Free vs. Paid: Some basic data recovery software might be available for free, while advanced features often come with paid versions.

5.3 Recovery Target:

Here, a recovery target refers to the desired state of your data or system after a disaster or data loss event. It defines the specific point in time or version of your data that you aim to restore during the recovery process.

There are a few ways to define a recovery target in a DR or backup system:

Recovery Point Objective (RPO):This metric specifies the maximum acceptable amount of data loss that can occur before a disaster. It essentially defines how recent the recovery target should be. For example, an RPO of 4 hours means you aim to recover data from a point no more than 4 hours old during a disaster.

Recovery Time Objective (RTO): This metric specifies the targeted timeframe for restoring your systems and data after a disaster. It defines how quickly you want to reach your recovery target. For example, an RTO of 2 hours means you aim to have your systems operational again within 2 hours after a disaster.

5.4 Restore points work:

Creation: Restore points are created automatically by the operating system at various intervals (e.g., daily) or when certain system events occur (e.g., installing new software, updating drivers). You can also manually create restore points before making significant changes to your system.

Content: A restore point typically includes essential system files, registry entries, and some configuration settings. It does not include your personal data files like documents, photos, or music.

Purpose: The primary purpose of restore points is to help you recover your system from unexpected issues. If you experience problems like software conflicts, driver issues, or system instability after making changes, you can use a restore point to revert your system back to a known good state.

Benefits of Using Restore Points:

Easy Recovery: Restore points offer a relatively simple and quick way to undo system changes that might have caused problems.

Non-Destructive: The restore process doesn't affect your personal data files, so you don't have to worry about losing important documents or photos.

Troubleshooting Tool: Restore points can be a valuable troubleshooting tool to isolate the cause of system issues. By reverting to different restore points, you can identify when the problem started and potentially narrow down the culprit.

Limitations of Restore Points:

Not a Backup: Restore points are not a replacement for a full system backup. They only capture system files and settings, not your personal data.

Limited Scope: Restore points don't protect against hardware failures or data loss due to malware or accidental deletion.

Temporary Storage: Operating systems often limit the number of restore points stored. Older restore points might be automatically deleted over time.

5.5 Windows 10 - Backup & Recovery

Windows 10 features several tools to help you perform backups of your documents. Here are some of these tools.

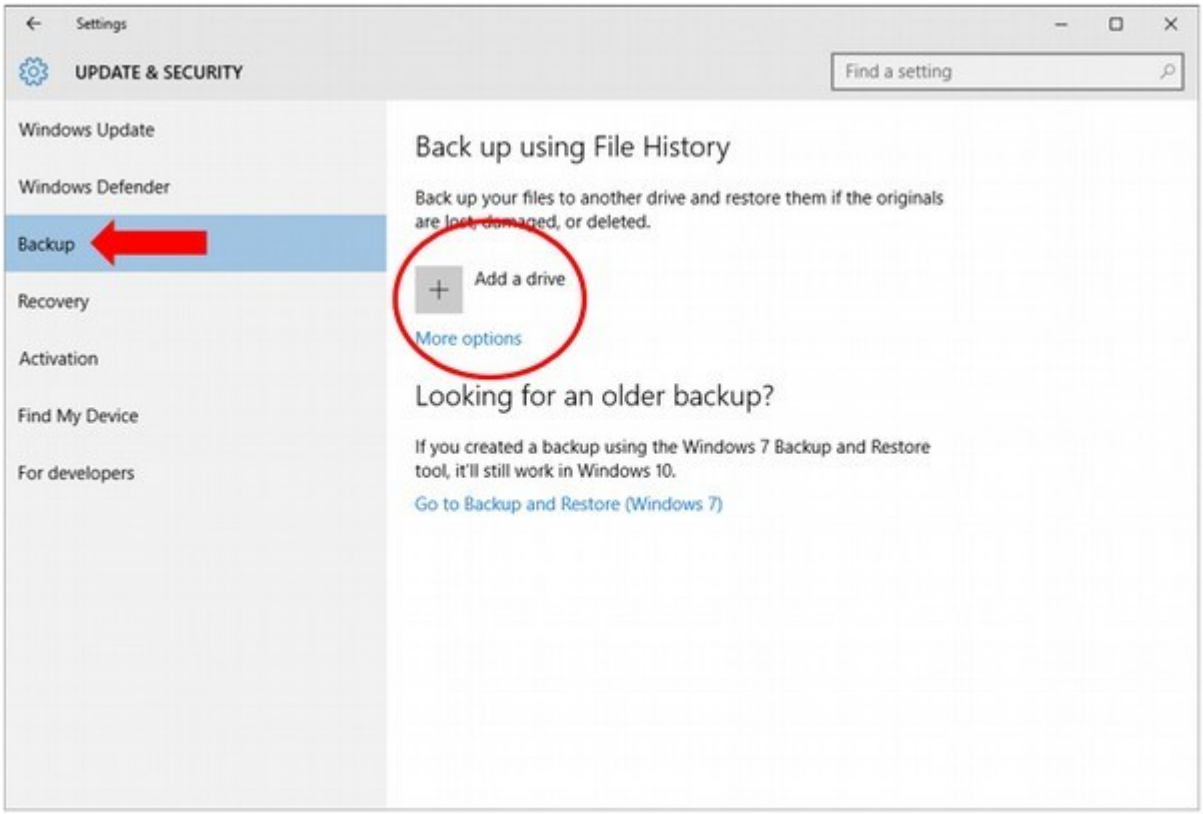
File History

File History will perform a back-up of the files located in your libraries (Documents, Pictures, Music, etc.) It allows you to choose a drive, where you can back-up your files and then asks you when to do it.

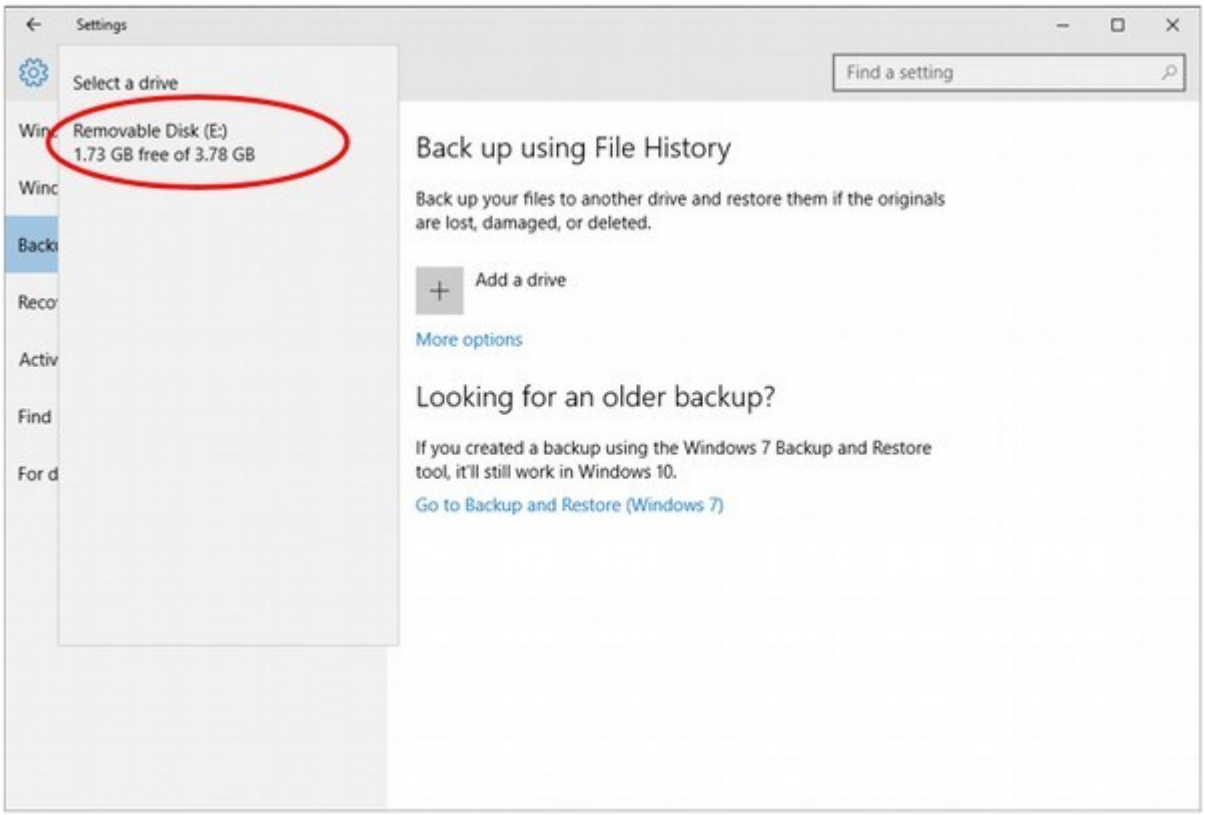
To configure the File History backup, follow these steps −

Step 1 − Go to SETTINGS and select Update & security.

Step 2 − In the UPDATE & SECURITY window, select Backup.



Step 3 − Click “Add a drive” to choose where to store your backup.

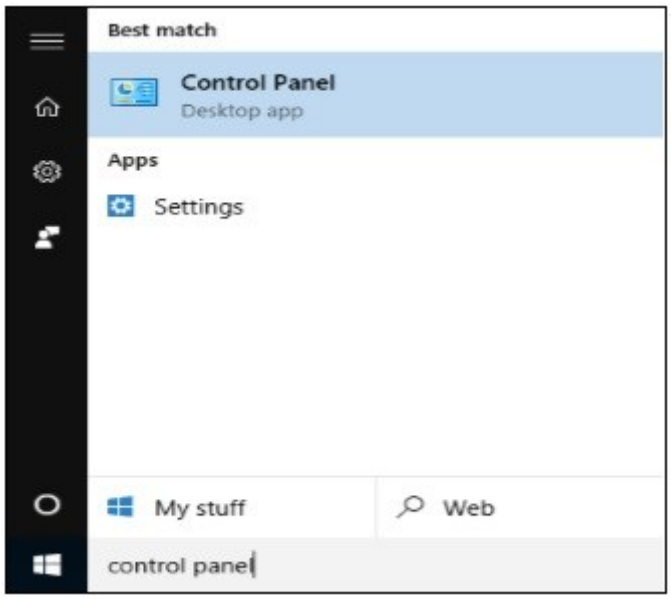


Backup & Restore (Windows 7)

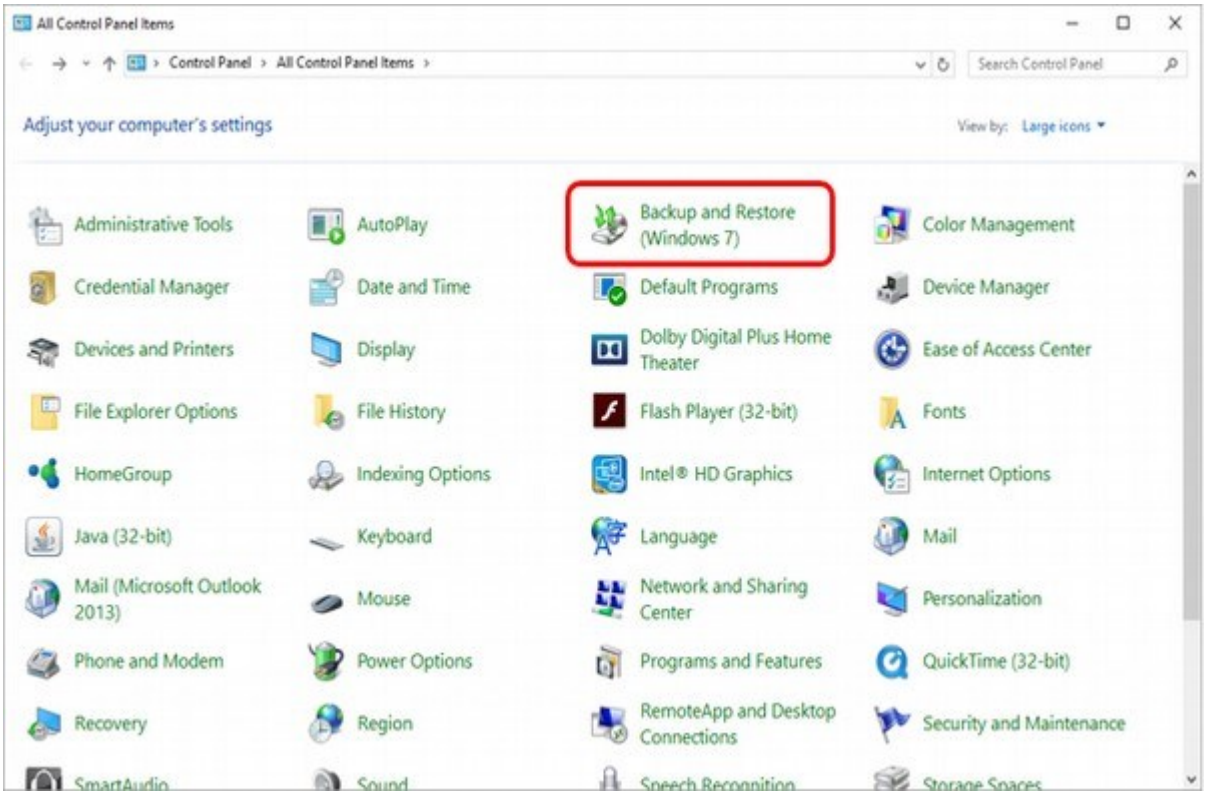
This tool, which was removed in Windows 8 and 8.1, was brought back allowing you to perform back-ups and restore data from old Windows 7 backups. However, it also lets to back-up your regular documents on Windows 10.

To open the Back-up & Restore, follow these steps −

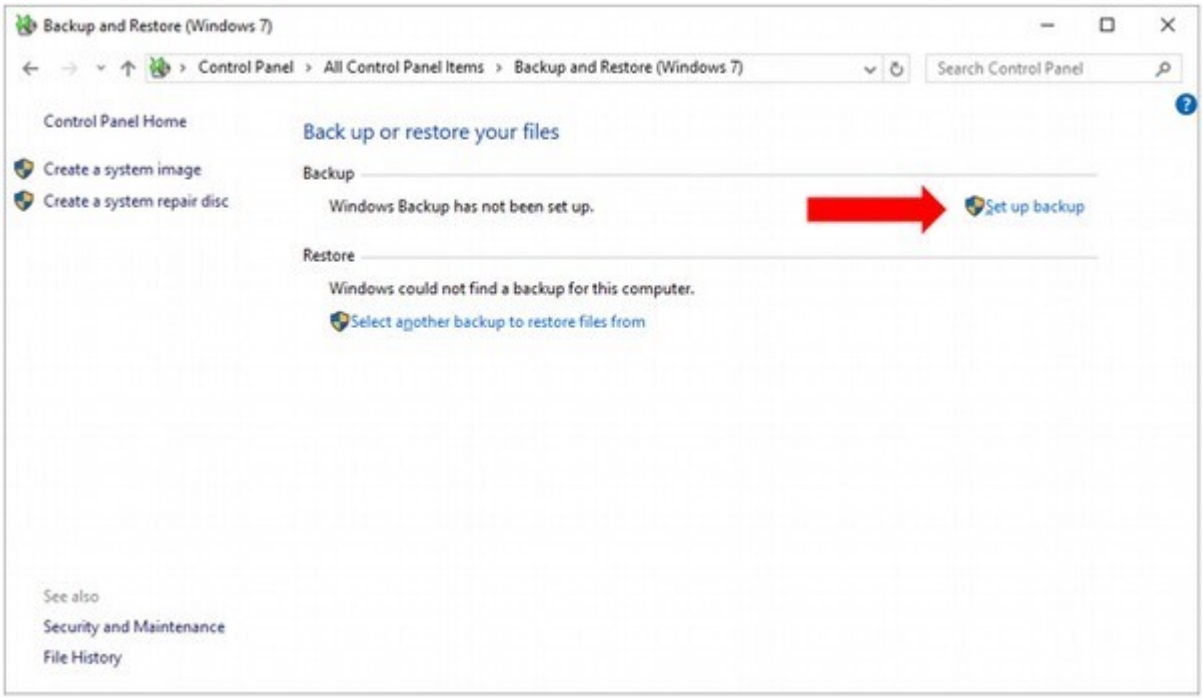
Step 1 − Open the Control Panel by searching for it in the Search bar.



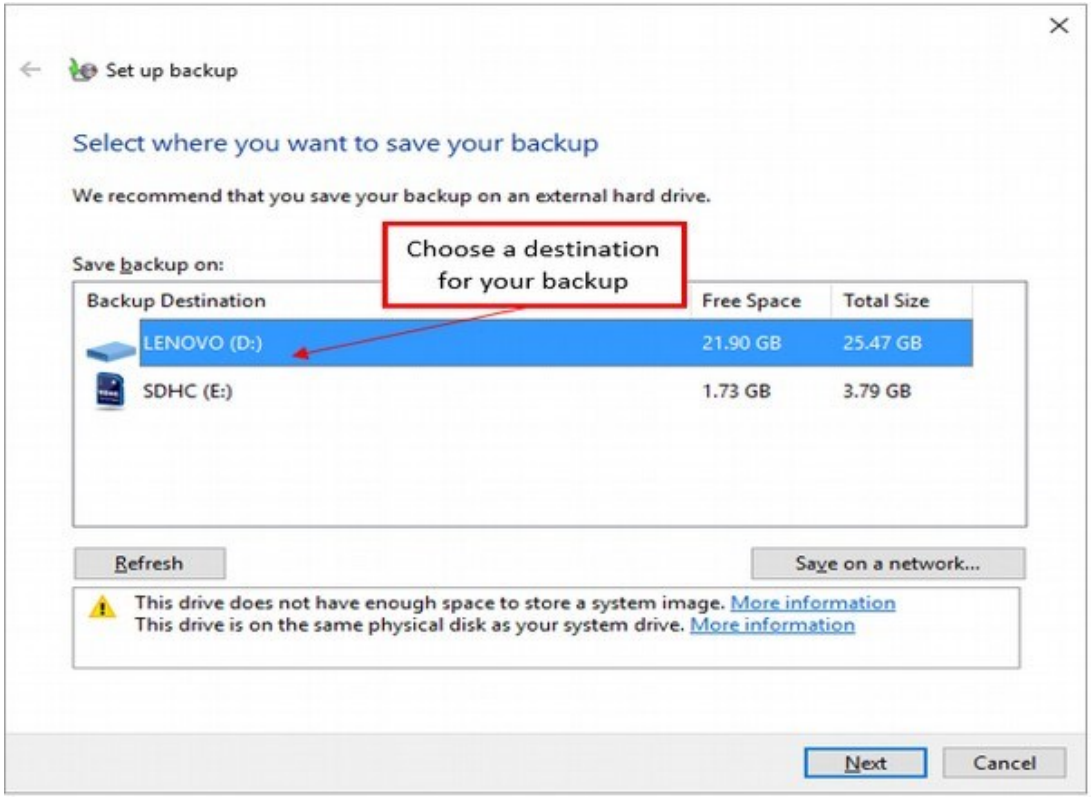
Step 2 − After the Control Panel is open, choose Backup and Restore (Windows 7).



Step 3 − In the Backup and Restore window, you can choose to “Set up backup”.

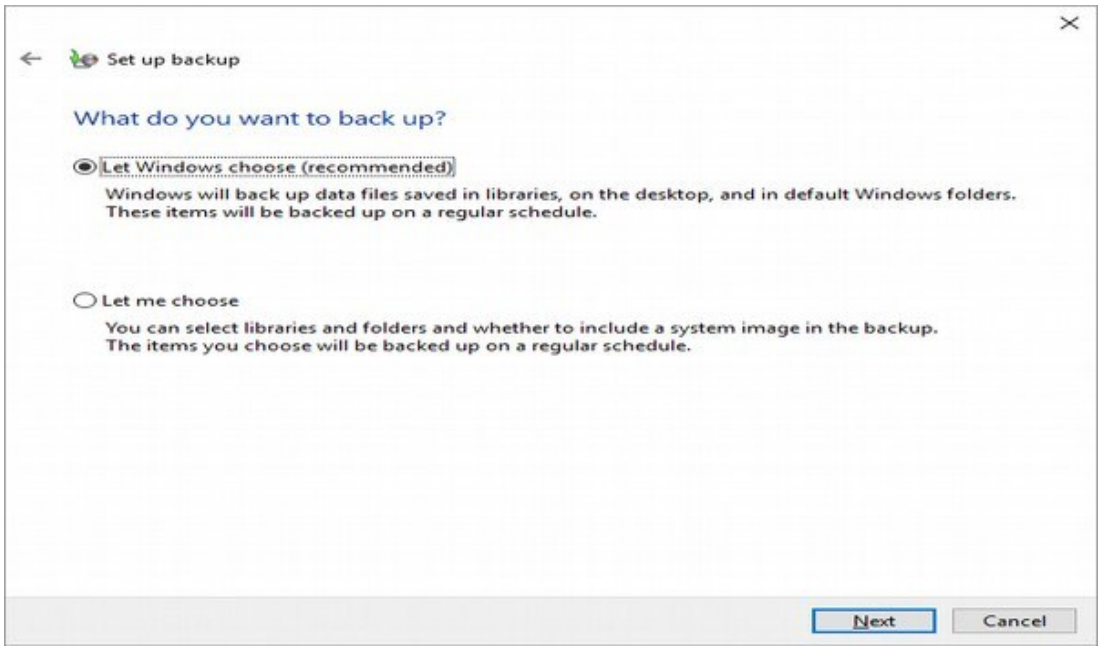


Step 4 − In the Set up backup window, choose where you want to store your backup.



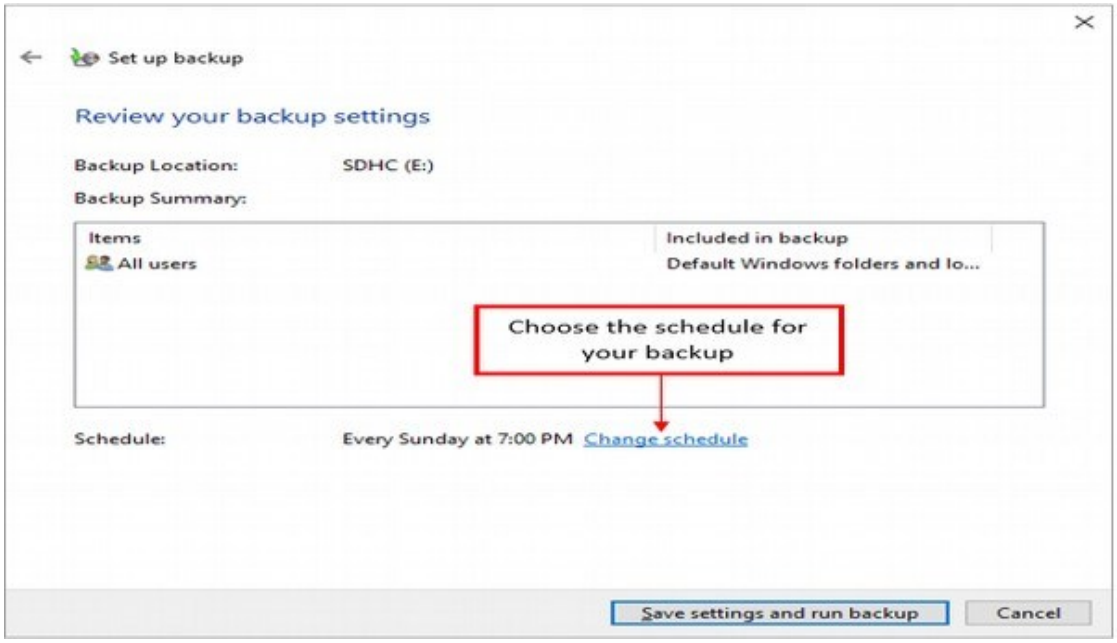
When choosing any of the listed storage devices, Windows 10 will give you information about that specific device. After choosing the desired destination, click Next.

Step 5 − In the next window, you can choose what files you want to backup.



Windows default is to store everything in your libraries (Documents, Pictures, etc.) and in your Desktop, but you can also choose specific files and folders to backup. After making your selection, click Next.

Step 6 − In the last window, you can review the settings of your backup and establish the schedule in which you want to perform it.



Step 7 − In the end, click Save settings and run backup. The backup will perform at the scheduled time.

Self-Check Sheet 5: Perform backup recovery

1. What's the first step before attempting a data recovery?

2. Once I have a backup, how do I choose the right recovery tools?

3. What exactly am I trying to recover to?

4. Is a restore point the same as a backup?

5. How do I actually restore my data from a backup?

Answer Key 5: Perform backup recovery

1. What's the first step before attempting a data recovery?
   Answer: Collect a backup! Having a recent backup is crucial for restoring your data.
2. Once I have a backup, how do I choose the right recovery tools?
   Answer: The tools depend on the situation. Simple data recovery software might work for basic needs, while complex scenarios might require professional services.
3. What exactly am I trying to recover to?
   Answer: The recovery target defines the desired state of your data after recovery. It could be a specific point in time (based on backups) or the latest version of your system.
4. Is a restore point the same as a backup?
   Answer: No. Restore points are snapshots of system files at a specific time, useful for recovering your operating system, but not your personal data (like backups).
5. How do I actually restore my data from a backup?
   Answer: The restore procedure involves using backup software to copy data from the backup to your desired location. The specific steps depend on your software and the type of restore you're performing.

Task Sheet 4.1: Perform backup recovery

Performance Objective: By the end of this task, the trainee should be able to:
1. Briefly describe what data you lost (files, documents, system functionality).
2. Briefly describe what data you lost (files, documents, system functionality).
3. Define the specific point in time or version of your data you want to recover based on your backups.
4. Consider the timeframe of your data loss to choose an appropriate backup.
5. Check if your system has created restore points (usually automatic at intervals or before major changes).
6. Access System Restore through system settings or control panel.
7. If restore points are available, choose one created before you noticed system issues.
8. Use your backup software to initiate the restore process. Select the desired backup and target location for restored data.
9. Follow the software's instructions for a complete restore.
10. Check if your system boots up correctly and functions normally after a system restore.

Review of Competency

Below is yourself assessment rating for module **"Performing Basic Data Backup and Recovery"**

SL no	**Assessment of performance Criteria**	Yes	No
1.	Backup is interpreted		
2.	Data recovery is interpreted		
3.	Type of backup solutions are stated		
4.	Disaster recovery plan is interpreted		
5.	Partition table is interpreted		
6.	Backup Plan is prepared		
7.	Tools for OS backup is identified and collected		
8.	Target for backup is identified		
9.	Backup procedure is performed		
10.	Backup Plan is prepared		
11.	Tools for user data backup is identified and collected		
12.	Target for backup is identified		
13.	Backup procedure is performed		
14.	Mail client is identified and configured.		
15.	Local Database file of mail client is identified		
16.	Email Backup Plan is prepared		
17.	Target for backup is identified		
18.	Backup procedure is performed		
19.	Backup is collected for recovery		
20.	Tools are identified and selected for recovery.		
21.	Recovery target is identified		
22.	Restore point is identified		
23.	Restore procedure is performed		

I now feel ready to undertake my formal competency assessment.

Signed:

Date:

Development of CBLM

The Competency based Learning Material (CBLM) of '**Performing Basic Data Backup and Recovery" (Occupation: IT Support Service, Level-3)** for National Skills Certificate is developed by NSDA with the assistance of SIMEC System Ltd., ECF Consultancy & SIMEC Institute of Technology JV (Joint Venture Firm) in the month of June, 2024 under the contract number of package SD-9B dated 15th January 2024.

SL No.	Name & Address	Designation	Contact Number
1	Mir Rashedul Islam	Writer	01920576687
2	Engr. Md. Zuwel Parves	Editor	01737-278906
3	Engr. Md. Zuwel Parves	Co-Ordinator	01737-278906
4	Md. Saif Uddin	Reviewer	01723-004419

REFERENCE:

1. https://www.ablebits.com/office-addins-blog/backup-outlook-emails/
2. https://gemini.google.com/