

EC-Council

C | C T

Certified Cybersecurity Technician

Module - 15

Data Security

This page is intentionally left blank.



Module Objectives

- 1 Understanding Data Security and its Importance
- 2 Understanding Different Data Security Technologies
- 3 Understanding Various Data Security Controls
- 4 Overview of Disk, File, and Removable-media Encryption Tools
- 5 Understanding the Methods and Tools for Data Backup, Retention, and Destruction
- 6 Understanding Data Loss Prevention (DLP) and DLP Solutions

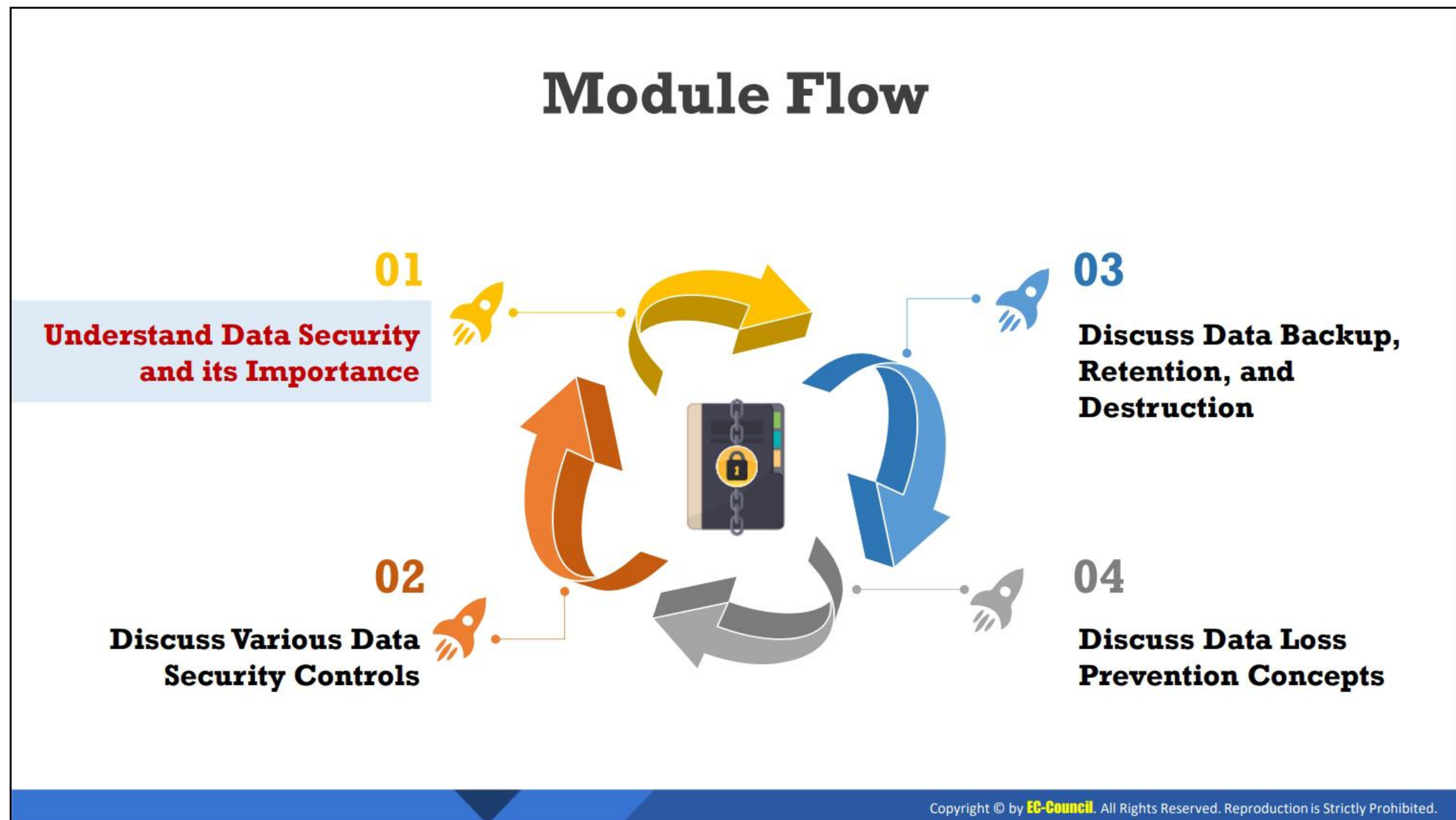
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Objectives

Data breaches can be costly for organizations. Therefore, it is important to keep organization data safe from prying eyes. This module explains the importance of data, and various techniques to protect data.

At the end of this module, you will be able to do the following:

- Understand data security and its importance
- Understand different data security technologies
- Explain various data security controls
- Use different disk, file, and removable-media encryption tools
- Understand methods and tools for data backup, retention, and destruction
- Understand data loss prevention (DLP) and DLP solutions



Understand Data Security and its Importance

The objective of this section is to explain the importance of data security. The module also explains the three states of data, i.e., data at rest, data in use, and data in transit, and introduces various data security technologies.

What is Business Critical Data?



- ❑ Data is the **heart** of any organization
- ❑ Critical data contains information that is important for business operation
- ❑ **Identification** and **classification** of business-critical data is the first step in securing an organization's data

Examples of Critical Data

1 Accounting files	4 Important office documents, spreadsheets, etc.
2 Databases or any business-related data	5 Software downloaded (purchased) from the Internet
3 The operating system files purchased with a computer, software, etc.	6 Contact Information (email address book)

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

What is Business Critical Data?

Data is the heart of any organization. Critical data contains information that is important for business operation. Identification and classification of business-critical data is the first step in securing an organization's data. Every organization has an abundance of data. An organization should identify their critical data or files. The criticality of data is based on its importance to the organization. This requires analyzing and deciding which information is more important for the organization to function properly. Critical data may consist of revenue, emerging trends, market plans, database, files including documents, spreadsheet, emails, etc. Loss of such critical data can significantly affect the organization.

How Can Critical Data Be Identified?

- Conduct a business impact analysis to determine the critical functions and data in an organization. Identify processes and functions that depend on and co-exist with the critical data.
- Evaluate the impact of data damage on the business.

Examples of Critical Data:

- Accounting files
- Databases or any business-related data
- The operating system files purchased with a computer, software, etc.
- Important office documents, spreadsheets, etc.
- Software downloaded (purchased) from the Internet
- Contact Information (email address book)
- Personal photos, music, and videos
- Any other critical file(s)



Need for Data Security

Data is an important asset for an organization, and it is essential to safeguard it from cybercriminals. If an organization's data is exposed or lost by any means, it can damage the organization's business and reputation to a great extent.

Effect of data loss:

- Brand damage and reputation loss
- Competitive advantage loss
- Loss of customers
- Market share loss
- Shareholder value erosion
- Fines and civil penalties
- Litigation/legal actions
- Regulatory fines/sanctions
- Significant cost and effort to notify affected parties and recover from breach

There are numerous causes for data loss, including

- Loss/theft of laptops and mobile devices
- Unauthorized data transfer to USB devices
- Improper sensitive data categorization

- Data theft by employees/external parties
- Printing and copying of sensitive data by employees
- Insufficient response to intrusions
- Unintentional sensitive data transmission

The resulting data loss leads to loss of brand loyalty and trust, decreases the number of customers, and affects market share and shareholder value, regulatory fines, legal proceedings, etc. Data breaches and cyberattacks have increased because of the expansion of computer networks; hence, data security is necessary to protect the data in an organization.

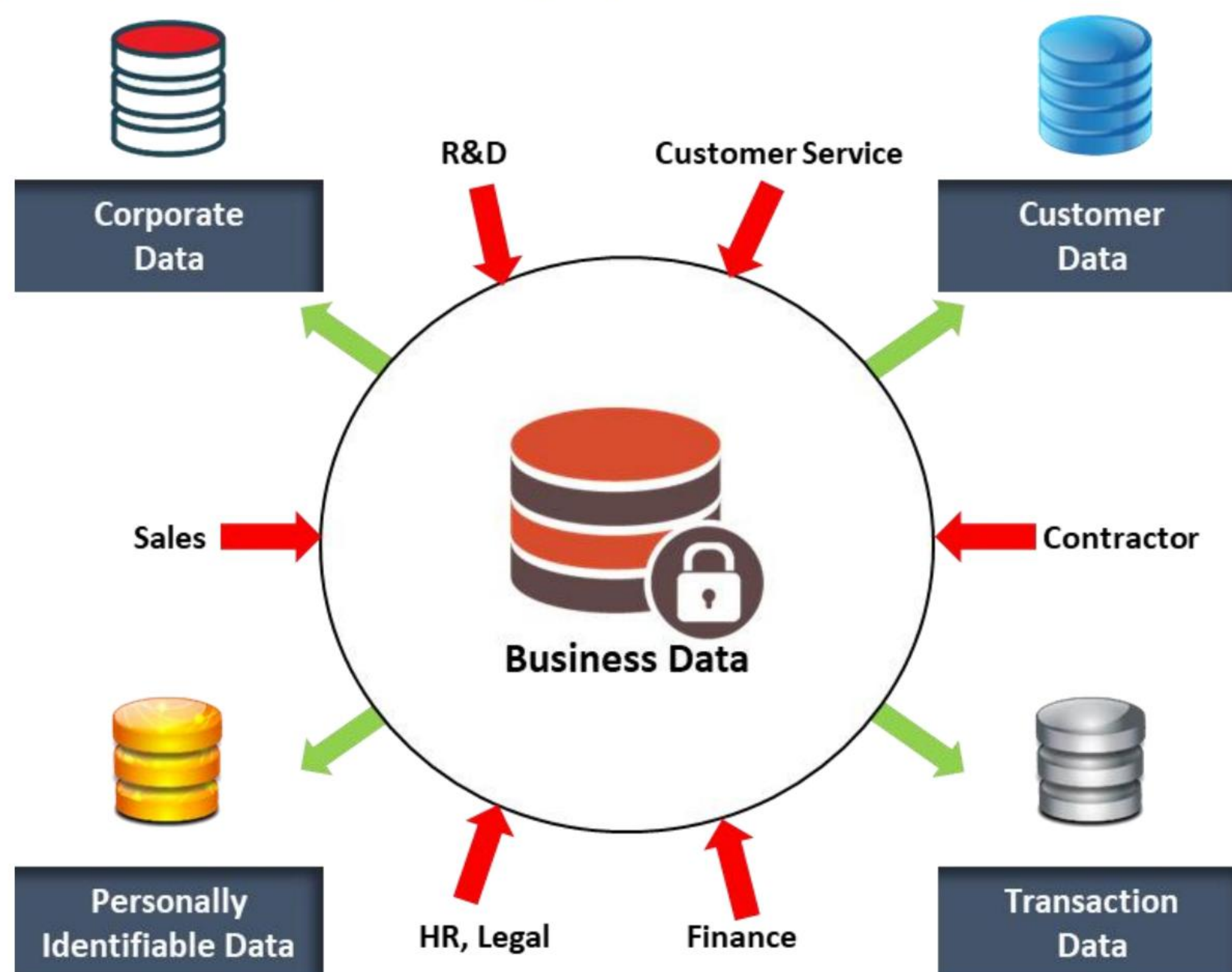
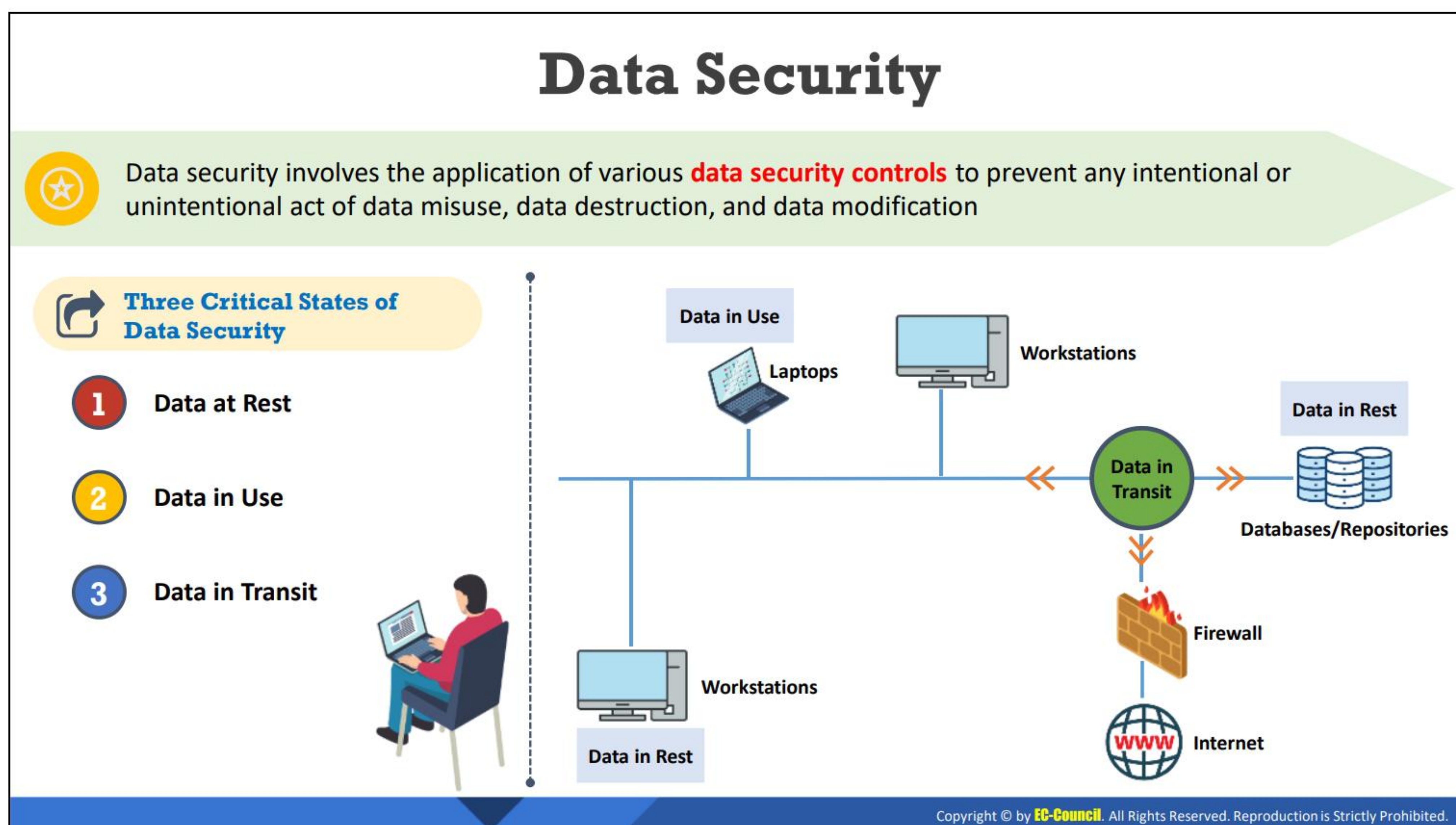


Figure 15.1: Business environment



Data Security

Data security involves the application of various data security controls to prevent any intentional or unintentional act of data misuse, data destruction, and data modification.

An organization's data is considered to be secured when they have sufficient provisions for:

- Restricting data from intentional or accidental destruction, modification, or disclosure
- Recovering lost or modified data following incidents
- appropriate data retention and destruction policies

Three Basic States of Data

- **Data at rest:** This data is inactive and is stored on a device or a backup medium such as hard drives, laptops, backup tapes, mobile devices, or at the offsite cloud backup. Data at rest remains in a stable state. The data at rest will not move actively in a system or network and cannot be accessed by an application or program.
- **Data in use:** This data is stored or processed by RAM, CPUs, or databases. It is not passively stored on the system, but actively moves across IT infrastructure. It is updated, erased, processed, accessed, and/or read by the system.
- **Data in transit:** This data actively moves from one location to another across the network, or is encrypted before moving and/or being transmitted through encrypted connections such as HTTPS, SSL, transport layer security (TLS), FTPS, etc.

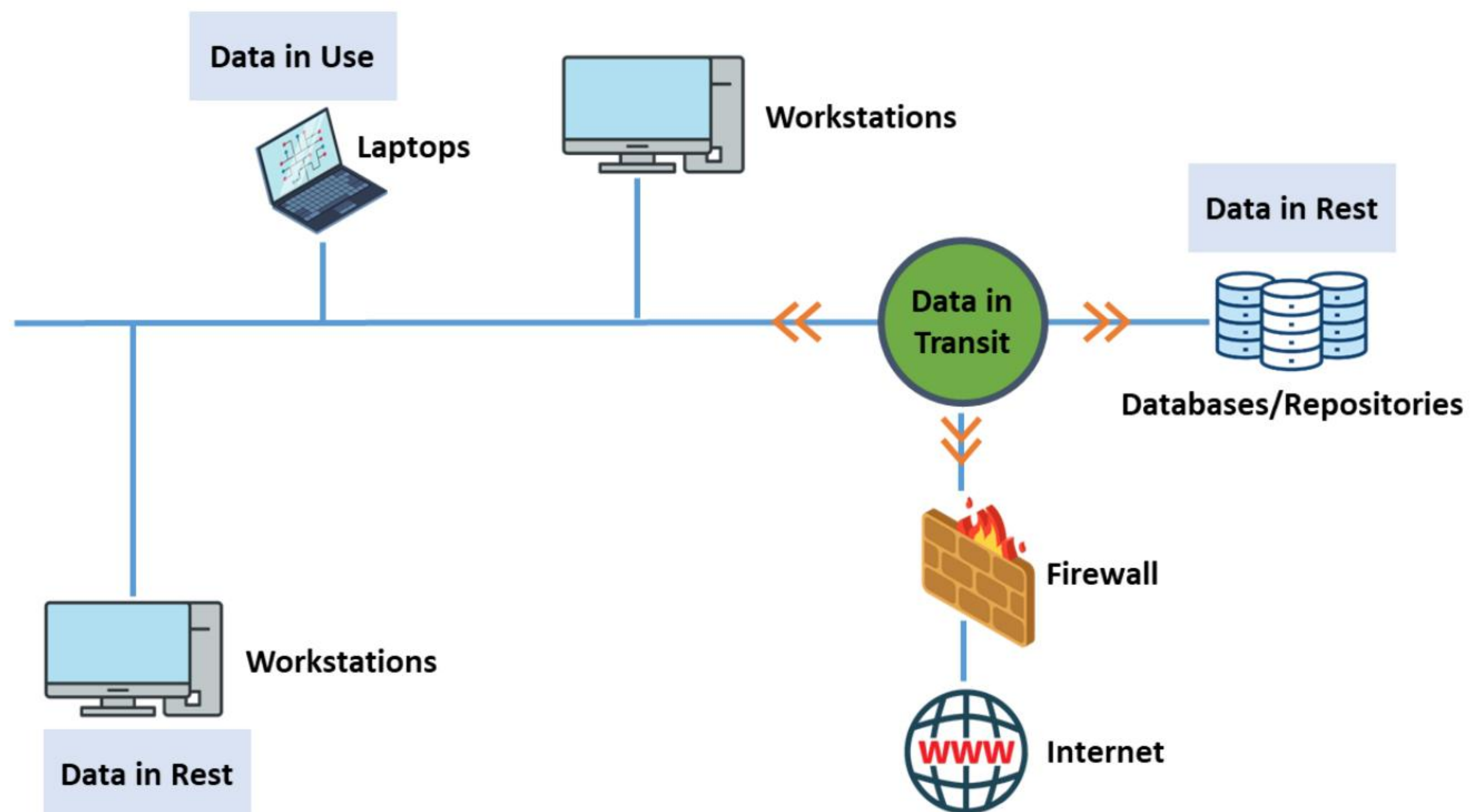


Figure 15.2: Three basic states of data

Example: “Data at Rest” vs “Data in Use” vs “Data in Transit”



Proper implementation of data security measures are required in **each state** to proactively enhance data security

	Data at Rest	Data in Use	Data in Transit
Description	Inactive data stored in digitally at a physical location	Data stored in memory	Data traversing using some means of communication
Examples	Customer bank balance stored in database	Data stored in RAM	An email being sent
Security Controls	- Data encryption - Password protection - Tokenization - Data federation	- Authentication techniques - Tight control on this data's accessibility - Full memory encryption - Strong identity management	- SSL and TLS - Email encryption tools such as PGP or S/MIME - Firewall controls

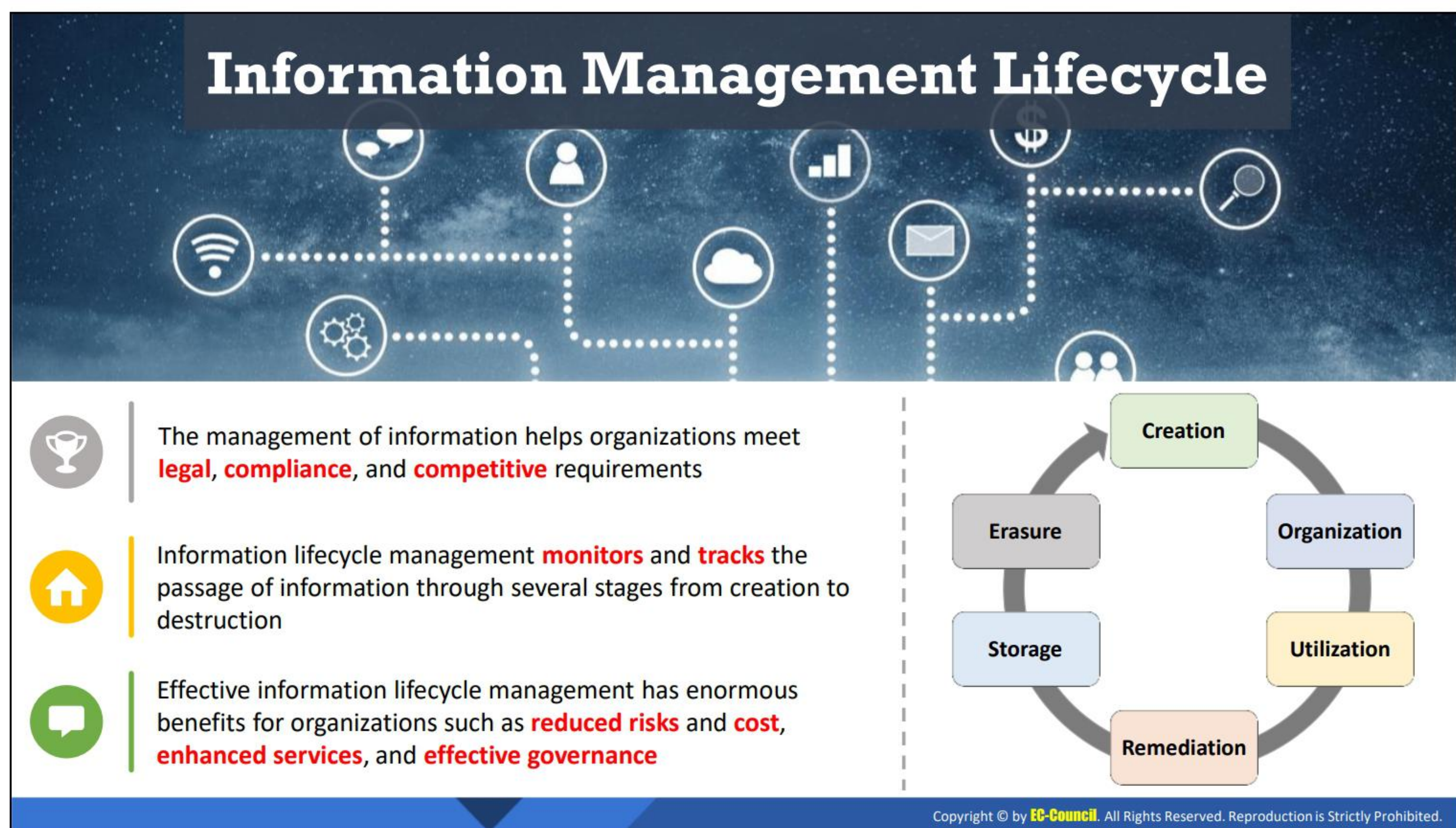
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Example: “Data at Rest” vs “Data in Use” vs “Data in Transit”

A proper implementation of security measures is required in each state to proactively enhance data security. The following table describes the various states of data, their specific examples, and security controls to protect against attacks.

	Data at Rest	Data in Use	Data in Transit
Description	Inactive data stored in digitally at a physical location	Data stored in memory	Data traversing using some means of communication
Examples	Customer bank balance stored in database	Data stored in RAM	An email being sent
Security Controls	- Data encryption - Password protection - Tokenization - Data federation	- Authentication techniques - Tight control on this data's accessibility - Full memory encryption - Strong identity management	- SSL and TLS - Email encryption tools such as PGP or S/MIME - Firewall controls

Table 15.1: Data at rest vs Data in use vs Data in transit



Information Management Lifecycle

The information management lifecycle helps organizations meet legal, compliance, and competitive requirements. Information lifecycle management monitors and tracks the passage of information through several stages from creation to destruction. A lifecycle management policy protects the integrity of data throughout the lifecycle processes. Effective information lifecycle management has enormous benefits for organizations such as reduced risks and cost, enhanced services, and effective governance.

Information passes through a series of stages. Information lifecycle management involves the monitoring and tracking all these stages to verify that the data are managed properly. Although no common list of stages is used, variations include similar operations. The following are the various stages of the information lifecycle.

- **Creation/gathering:** In this stage, the information is gathered in a manageable environment. The data can be generated internally by automated sources or employees as well as by outside sources such as vendors and clients. Metadata creation is also performed in this stage for later identification.
- **Organization:** The information can be stored at one or many locations. In the case of critical information, control over distribution and storage protection is mandatory. The information can also be classified and tagged in this stage.
- **Utilization:** Occasionally, the data need to be transferred to new locations or converted to new formats, or more metadata need to be added. In such cases, all necessary developments and modifications are performed in this stage to ensure that the data are useful and available for authorized users or accounts.

- **Remediation:** Information must often be migrated and converted so that software products can utilize it effectively. It is mandatory to maintain integrity while performing these activities and to follow remediation methods in case of problems.
- **Storage/retention:** Occasionally, information that is not useful at present must be archived. The archived data can be used later for regulatory purposes. Archival policies minimize the amount of data information systems can manage and allow secure retention. The data can be restored from archives when required.
- **Erasure/destruction:** When information is no longer useful and need not be archived, it should be formatted or erased permanently without leaving any residue. Destruction policies need to be followed carefully while performing this activity.

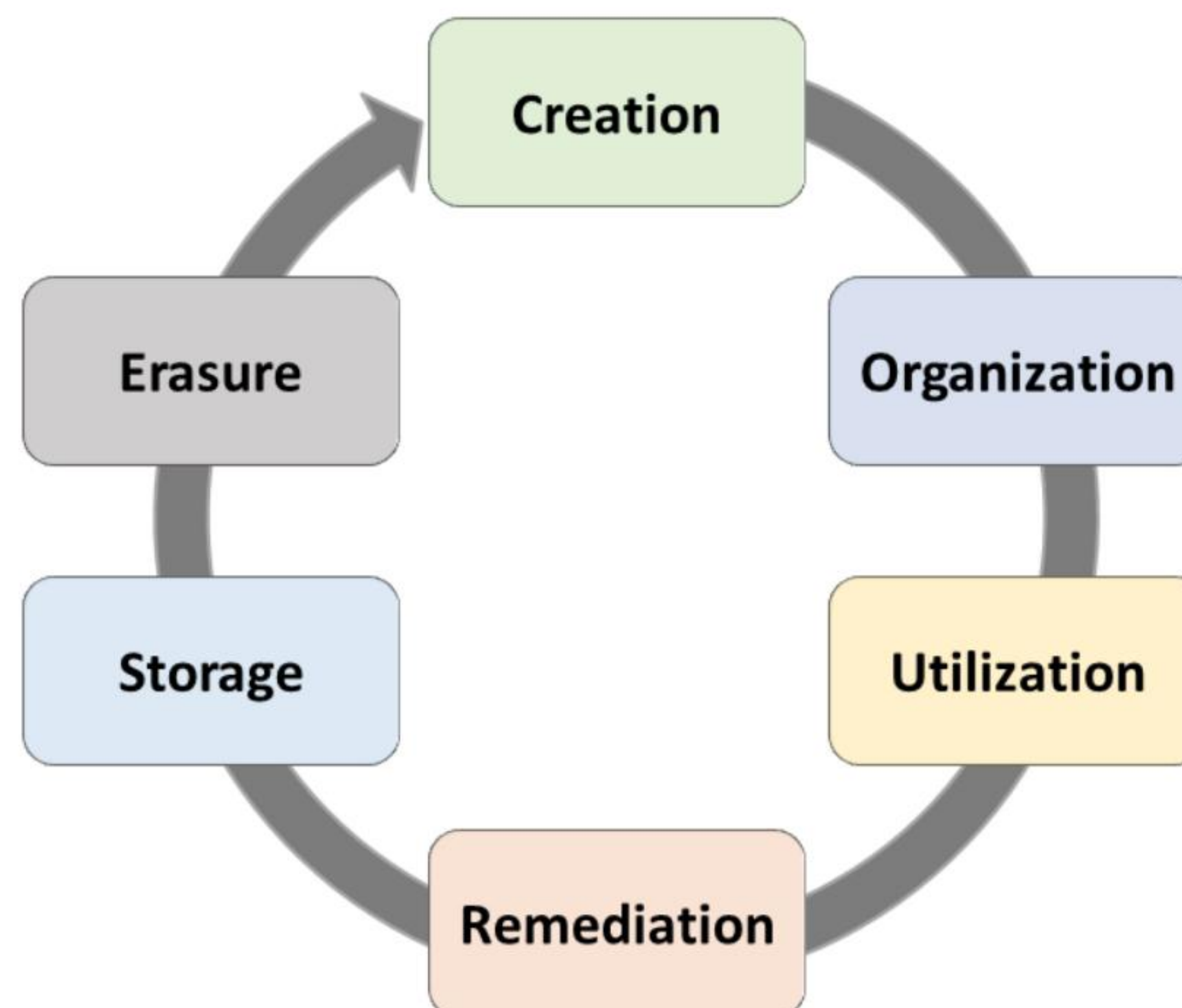


Figure 15.3: Information management lifecycle

Data Roles and Responsibilities

Data Owners

Data owners are individuals or steering committees having **complete control over the data** in an organization; they are solely responsible for the data assets of the organization.

Data Controller

The data controller is a person who **collects** and **controls the processing of data** provided to the data processor

Data Processor

The data processor is a person who **processes the data** given by the data controller for a specific purpose

Data Steward/ Custodian

The data steward is accountable for **business data sets**, and the data custodian is accountable for **technical data assets** for the storage and transport of data

Privacy Officer

- The privacy officer is a senior executive who is responsible for the **privacy of the organization's data**
- They **maintain privacy policies** as well as investigate and track incidents and security loopholes

Data Protection Officer (DPO)

The DPO ensures that sensitive information on the personnel, customers, or any other individual **meets the compliance requirements** of the organization

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Data Roles and Responsibilities

Data roles and responsibilities play an important role in the growth and development of an organization. They help in improving the visibility of duties and tasks assigned to employees based on their roles and responsibilities. Assigning data roles makes the sharing of work and resources easier and helps in collaboration, thereby improving the quality of work. Every organization should follow the General Data Protection Regulation (GDPR) guidelines and focus on data roles as following the specified security guidelines for each role safeguards the organization's data.

Discussed below are various data roles and their responsibilities generally found in an organization.

▪ Data Owners

Data owners are individuals or steering committees having complete control over the data in an organization; they are solely responsible for the data assets of the organization. Only the data owners have the right and authority to make decisions as to who can access or modify data. Only data owners can approve the data glossaries of the organization or initiate quality data events, data requirements, and data solutions. Data owners are also responsible for accountability for data access, defining policies for information assets, creating trusted data, and eliminating redundancies.

▪ Data Controller

The data controller is a person who collects and controls the processing of data provided to the data processor. The data controller determines “how” and “why” personal data are processed in an organization. The responsibilities of the data controller include collecting consent, storing data, and allowing access rights. The data

controller must have the ability to ensure compliance with the principles associated to the processing of personal data.

- **Data Processor**

The data processor is a person who processes the data given by the data controller for a specific purpose or duty that involves the processing of personal data. The processor does not own the personal data. They help controllers in diverse situations such as personal data breach notifications and data protection impact assessment. The main roles of the data processor include maintaining records of data processing activities, following instructions, ensuring compliance with the controller, regularly reviewing data processing instructions, and ensuring that compliance obligations are met.

- **Data Steward/Custodian**

Data steward and data custodian are the two roles given to the subject matter experts responsible for managing the data on a daily basis. The data steward is accountable for business data sets, and the data custodian is accountable for technical data assets for the storage and transport of data. The data custodian is similar to the IT department in that they maintain the infrastructure of the company, data security, configuration, asset management, business rule implementation, etc. The responsibilities of the data custodian include authorizing data access, appointing a data steward for every data set, data integrity, maintaining consistency between new data and the existing data model, and auditing data content.

- **Privacy Officer**

The privacy officer is a senior executive who is solely responsible for the privacy of the organization's data. Their main responsibilities include implementing and maintaining privacy policies with the latest privacy concerns, investigating and tracking incident and security loopholes of the organization, monitoring and managing data protection measures, and conducting privacy awareness programs in the organization.

- **Data Protection Officer (DPO)**

The DPO is the security supervisor in the organization who safeguards the organization's data. The DPO ensures that sensitive information on the personnel, customers, or any other individual meets the compliance requirements of the organization. The DPO should also ensure that the controllers are advised about their data protection rights and responsibilities. The DPO's responsibilities include educating employees about regulatory compliance, performing security audits, performance monitoring, providing advice on data protection, and maintaining a record of all data processing activities.



Data Classification

- Data classification is the process of assigning **sensitivity levels to data** while the data are being generated, modified, saved, or passed over an information system
- Data classification provides organizations a sense of **data criticality** and the **level of security** needed to be implemented for different types of business data

Data can be classified into five levels:

- 01 Top secret
- 02 Highly confidential information
- 03 Proprietary information
- 04 Information for internal use
- 05 Public documents

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Data Classification

Data classification is the process of assigning sensitivity levels to data while the data are being generated, modified, saved, or passed over an information system. Data are a critical business asset; the protection of the confidentiality, integrity, and availability of data is important for business operations and market competitiveness. Data classification provides organizations a sense of data criticality and the level of security needed to be implemented for different types of business data.

While some business data need to be stored and processed only within the organization, other information may be required to be distributed to related third parties. Therefore, confidential and sensitive data must be protected from being exposed. The sensitivity and importance of information determine how confidential it is and how it should be separated from the rest of the data.

Data can be classified into five different levels as follows.

1. **Top secret:** This level includes highly sensitive information such as business plans and financial records. Exposing or leaking such information may cause severe damage to the organization's assets and reputation, further leading to legal consequences.
2. **Highly confidential information:** This level includes confidential information such as corporate or customer data such as bank-account details, credit-card details, and social security numbers. Exposing this information can invite financial or legal risks to the organization. Only the authorized personnel can access this information.
3. **Proprietary information:** This level includes confidential internal information such as customer and employee reviews, third-party details, and technology upgrades of a new

product. This level may also include intellectual property (IP). Exposing such information may have an adverse impact on the organization's business operations.

4. **Information for internal use:** This level includes internal information such as the organization's charts and sales contest rules. Exposing this information may cause reputational damage to the organization. Such data should only be accessible to internal employees of the organization who have authorized access.
5. **Public documents:** This level includes information such as the contact details of the organization, product lists, and price lists, which are freely available to the public. Such data are available on official websites and should be protected from unauthorized modifications.



Data Security Technologies

- **Data Access Control**

Data access controls enable authentication and authorization of users to access the data. It is an important component of security compliance programs that protect unauthorized access to confidential information.

- **Data Encryption**

Protecting information by transforming it so that it becomes unreadable for an unauthorized party. It safeguards corporate secrets, classified information, and personal information. The encrypted data cannot be read by any unauthorized persons or entities.

- **Data Masking**

Protecting information by obscuring specific areas of data with random characters or codes. Data masking protects sensitive data such as personally identifiable information, protected health information, payment card information, intellectual property, etc. Apart from this, data masking also protects against an insider threat. Implementing data masking will bolster the security strategies of an organization.

- **Data Resilience and Backup**

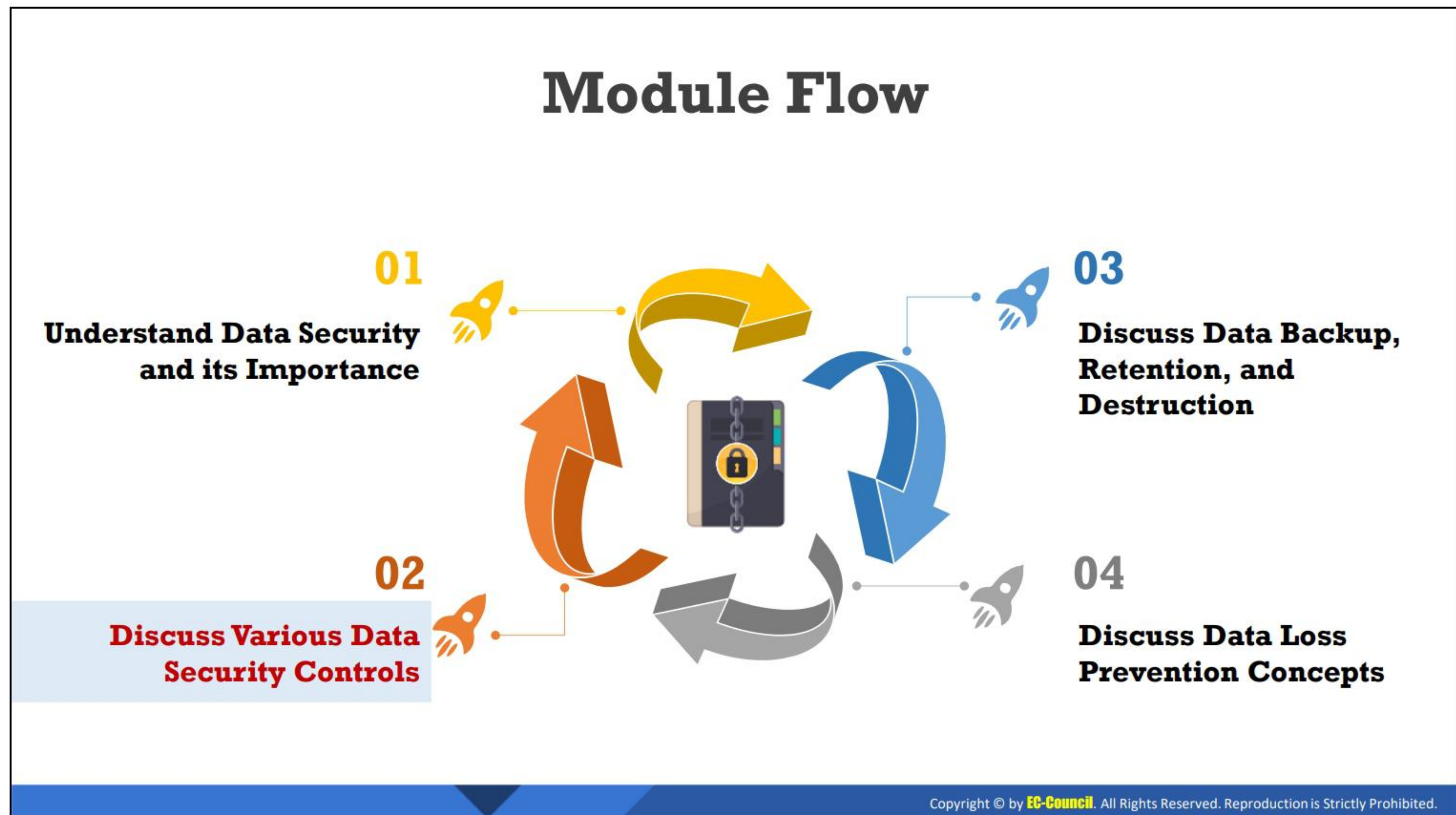
Making a duplicate copy of critical data to be used for restoring and recovery purposes when the primary copy is lost or corrupted, either accidentally or on purpose. Data resilience allows the data to remain available to the applications if there is any failure in the hosted data. Retaining multiple copies of a data backup help in restoring the data with ease and mitigate the risks of data corruption or malicious attacks.

- **Data Destruction**

It involves destroying the data so that it cannot be recovered and used for a wrong motive. The destruction of old hard drives or electronic devices should be done securely and safely. Data destruction helps in physically destroying the old information of customers and employees.

- **Data Retention**

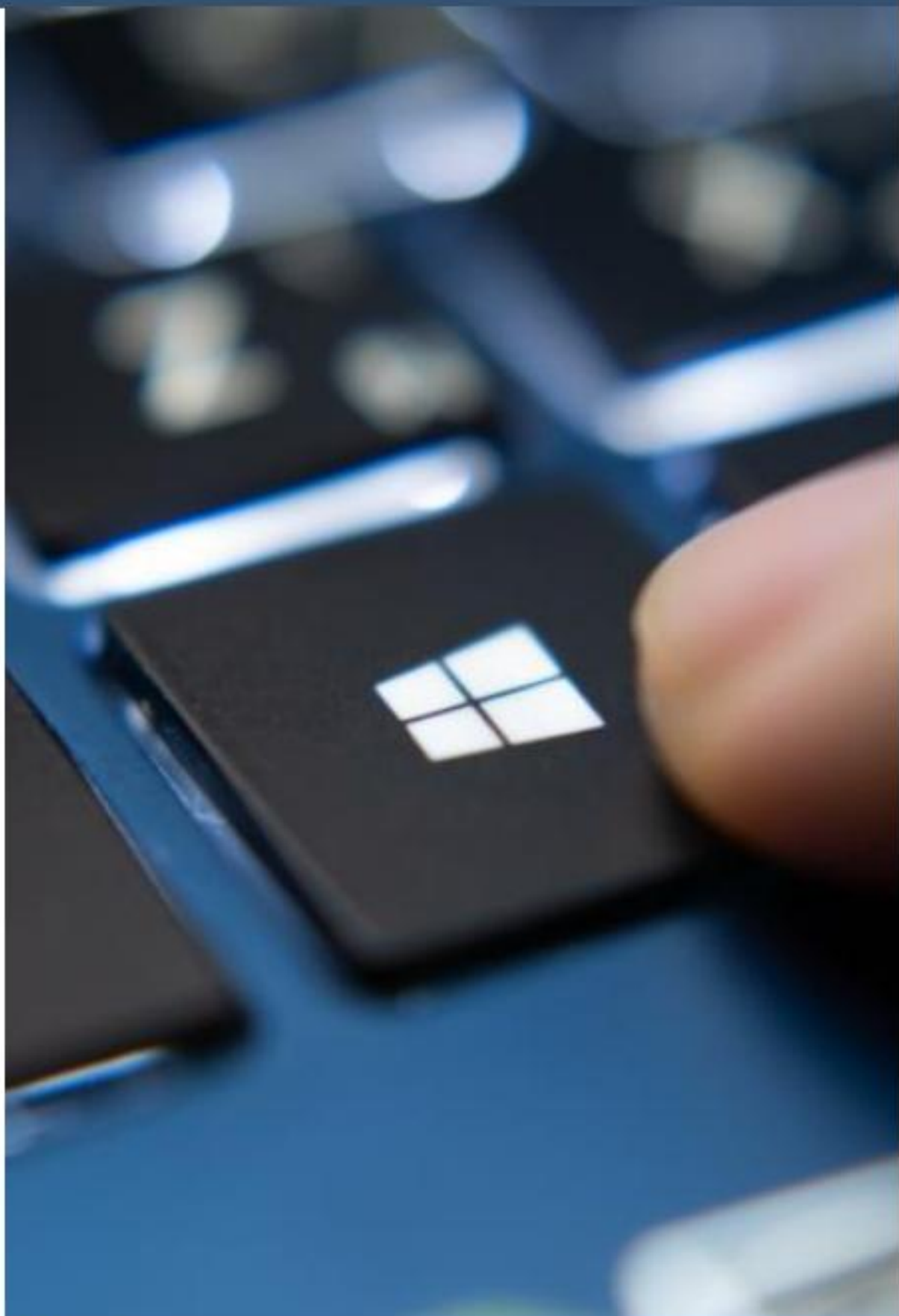
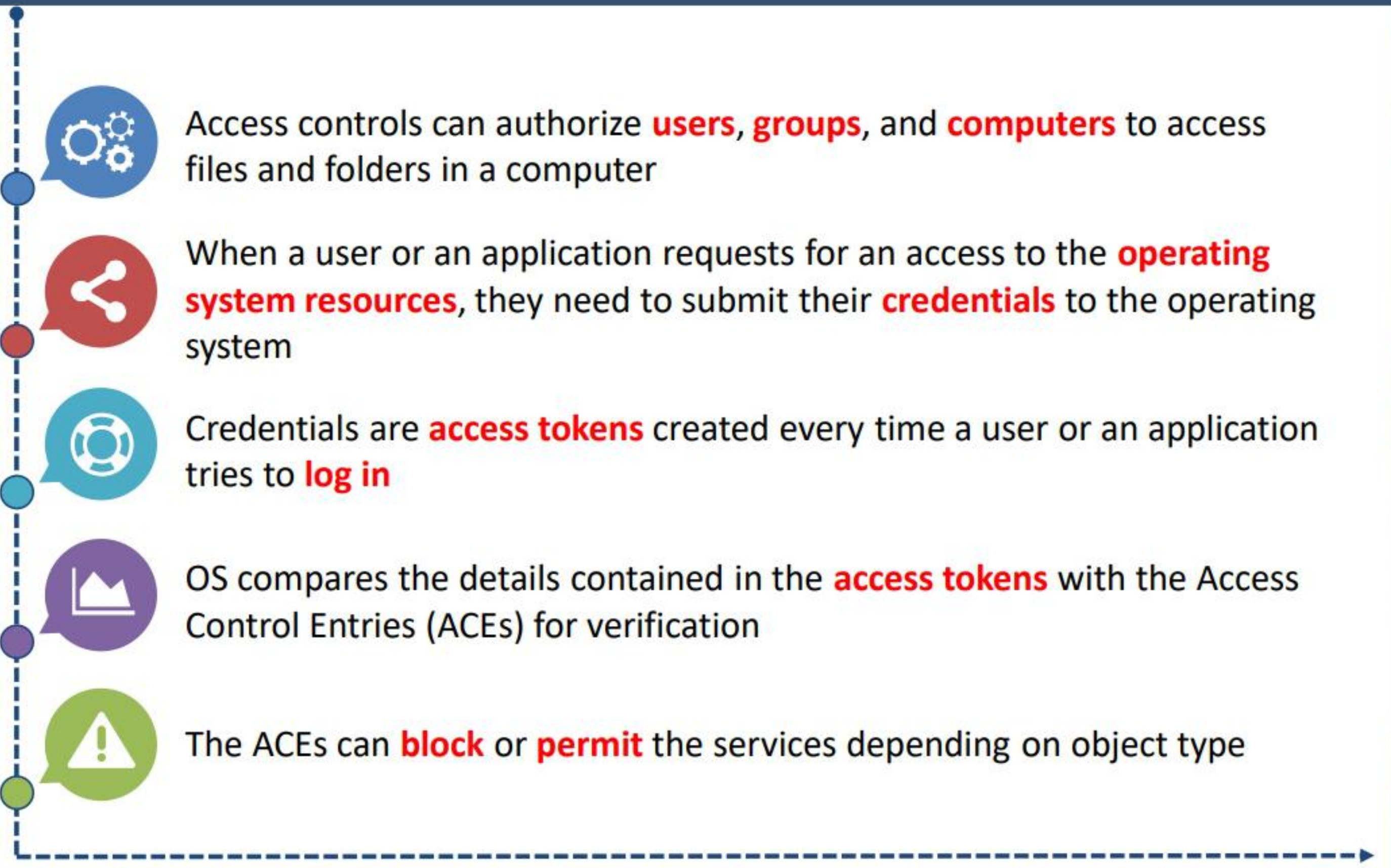
Storing data securely for compliance or business requirements. An organization should have policies and processes for retention and removal of data. Data retention programs have a tremendous impact on data security and can meet the expectations of customers and governments in safeguarding privacy.



Discuss Various Data Security Controls

The objective of this section is to explain the use of various security controls to secure the data.

ACL: Setting Access Controls and Permissions to Files and Folders in Windows



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ACL: Setting Access Controls and Permissions to Files and Folders in Windows (Cont'd)

Applying NTFS permissions to files

- ❑ Typical **file permissions** allowed on the NTFS file system are:
 - Full Control
 - Modify
 - Read and Execute
 - Read
 - Write
- ❑ Each of these permissions includes a **logical group** of special permissions

Special Permissions associated with each NTFS File Permission:

Special Permissions	Full Control	Modify	Read and Execute	Read	Write
Traverse Folder/Execute File	✓	✓	✓		
List Folder/Read Data	✓	✓	✓	✓	
Read Attributes	✓	✓	✓	✓	
Read Extended Attributes	✓	✓	✓	✓	
Create Files/Write Data	✓	✓			✓
Create Folders/Append Data	✓	✓			✓
Write Attributes	✓	✓			✓
Write Extended Attributes	✓	✓			✓
Delete Subfolders and Files	✓				
Delete	✓	✓			
Read Permission	✓	✓	✓	✓	✓
Change Permission	✓				
Take Ownership	✓				
Synchronise	✓	✓	✓	✓	✓

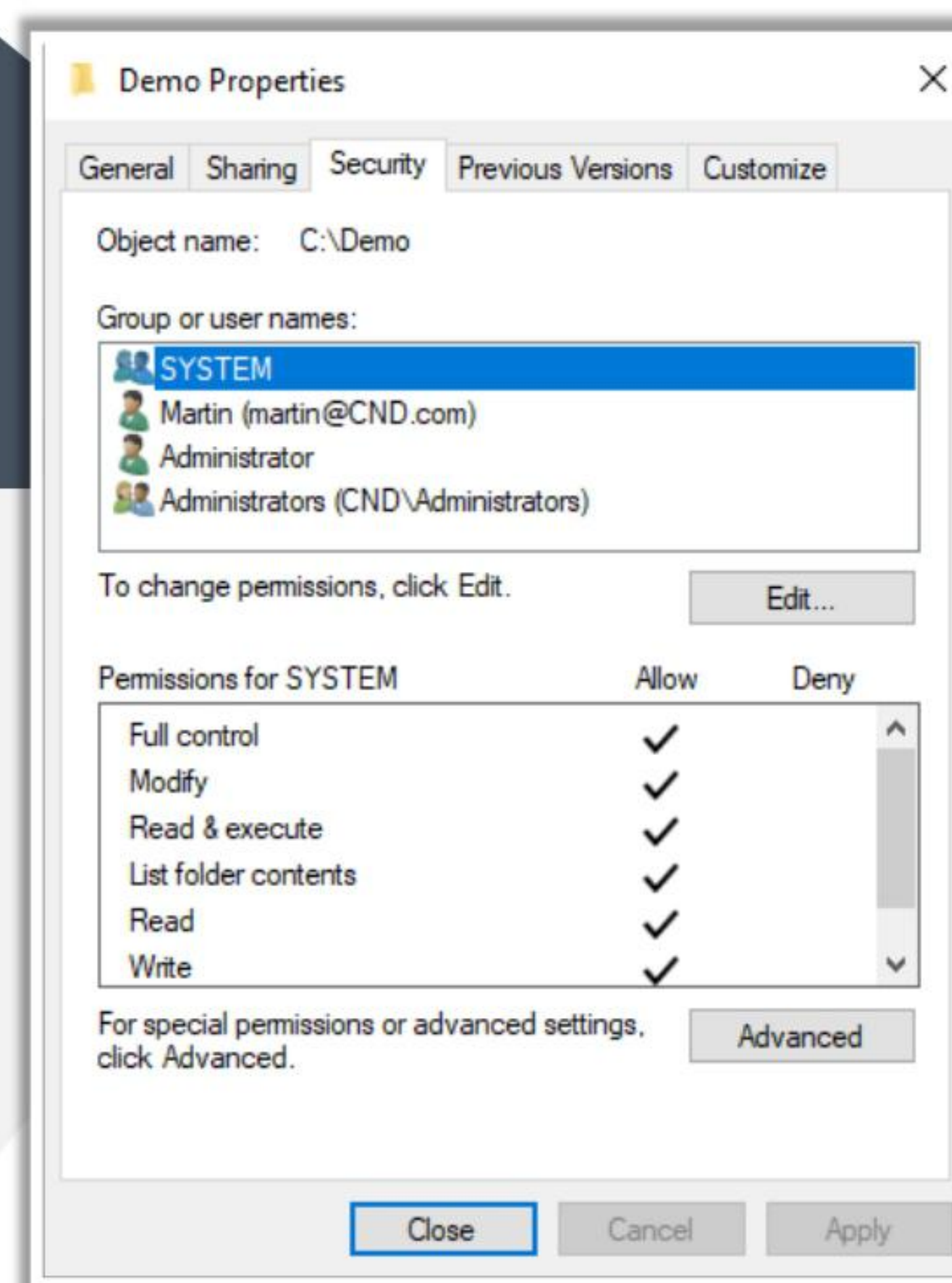
<https://docs.microsoft.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ACL: Setting Access Controls and Permissions to Files and Folders in Windows (Cont'd)

☐ To set, view, edit, or remove **special permissions**:

- 1 Go to the specific file or folder on which you want to set a special permission
- 2 Right-click on the file or folder, click **Properties**, and then click the **Security** tab
- 3 Click **Advanced**
- 4 Click **Add** to set special permissions for a new group or user in Permission Entry Window



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ACL: Setting Access Controls and Permissions to Files and Folders in Windows (Cont'd)

Applying NTFS permissions to folders

- ☐ Typical **folder permissions** allowed on the NTFS file system are
- ❖ Full Control
 - ❖ Modify
 - ❖ Read and Execute
 - ❖ List Folder Contents
 - ❖ Read
 - ❖ Write
- ☐ Each of these permissions include a **logical group** of special permissions

Special Permissions associated with each NTFS Folder Permission

Special Permissions	Full Control	Modify	Read and Execute	List Folder Contents	Read	Write
Traverse Folder/Execute File	✓	✓	✓	✓		
List Folder/Read Data	✓	✓	✓	✓	✓	
Read Attributes	✓	✓	✓	✓	✓	
Read Extended Attributes	✓	✓	✓	✓	✓	
Create Files/Write Data	✓	✓				✓
Create Folders/Append Data	✓	✓				✓
Write Attributes	✓	✓				✓
Write Extended Attributes	✓	✓				✓
Delete Subfolders and Files	✓					
Delete	✓	✓				
Read Permission	✓	✓	✓	✓	✓	✓
Change Permission	✓					
Take Ownership	✓					
Synchronise	✓	✓	✓	✓	✓	✓

<https://docs.microsoft.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ACL: Setting Access Controls and Permissions to Files and Folders in Windows

Access controls can authorize users, groups, and computers to access files and folders in a computer. When a user or an application requests for an access to the operating system resources, they need to submit their credentials to the operating system. Credentials are access tokens created every time a user or an application tries to log in. The operating system verifies whether the access token is created as a permission to access the objects before allowing the user or application to access them. Here, the OS compares the details contained in the access

tokens with the access control entries (ACEs) for verification. The ACEs can block or permit the services depending on object type. For example, the ACEs for a Printer are print, manage printing, and manage documents. The ACLs contain a combination of an object's ACEs.

- **ACEs:** An ACL can have zero or more ACEs, wherein each ACE has the access to an object. Overall, there are six types of ACEs, out of which securable objects support three (generic types), and the other three are directory service objects (object-specified types).
- The three generic types of ACEs are:
 - **Access denied ACE:** Used in a discretionary ACL to prevent access to any user.
 - **Access allowed ACE:** Used in a discretionary ACL to allow access to any user.
 - **System audit ACE:** Used in a system ACL to create an audit log for each attempt by a user while accessing the objects.
- The three object-specified types of ACEs are:
 - **Access denied, object-specific ACEs:** Used in the discretionary access control list to block access to a property or property set. It can even stop the inheritance level of a specified type of child object.
 - **Access allowed, object-specific ACEs:** Used in a discretionary ACL to permit access to a property or property set. It can even stop the inheritance level of a specified type of child object.
 - **System audit, object-specific ACEs:** Used in a system ACL to create an audit log when a user attempts to access the child object.

The object-specific types and generic types differ only in the design of the inheritance level.

- **ACLs:** An ACL is a table that provides a detailed description of the access rights of the users for accessing objects. Every object has an ACL that contains the details of the user rights and privileges for accessing that object. Each OS system has specific ACLs. The ACLs have one or more ACEs that contains the user details.
- **Permissions:** Each container or object has a security descriptor attached to itself. This security descriptor contains a detailed description of the user access rights. The security descriptor is created along with the container or object. An ACE represents the permission to users or user groups, and the entire list or set of permissions is contained in an ACL. There are two types of permissions:
 - **Explicit permissions:** Permissions that are set by default upon creation.
 - **Inherited permissions:** Permissions inherited from the parent object to the child object.

For example, any files and folders in a folder can inherit the permissions applicable to that particular parent folder. Here, the parent folder has an explicit permission, whereas the files and folders have inherited permissions.

- There are two sets of permission entries for accessing a folder on a file server:
 - **Share permission on a folder:** Used for files and folders shared across the network or many user accounts. The permissions can be either denied or granted depending on the users or user accounts. The most commonly used shared permissions are full control, change, and read.
 - **NTFS permissions on a folder:** Control the permissions over a network and local computers. The most commonly used NTFS permissions are full control, modify, read and execute, and read and write.

Applying NTFS Permissions to Files and Folders

Access controls for files and folders can specify which users and user groups can have the access permissions. NTFS files and folder permissions allow users to access files stored on a local computer and also files stored in a shared folder over a network. NTFS also allows the sharing of permissions on shared folders in accordance with file and folder permissions.

- **NTFS permissions for files:**
 - **Full control:** Specifies whether the user has all permissions to access files. Users with full control have the complete access rights to any file even if permission is denied to them.
 - **Modify:** Allows the user to read, write, execute, and traverse.
 - **Read and execute:** Allows the user to go through each directory and read all files.
 - **Read:** Allows the user to list folders, read files, read attributes, and read permissions.
 - **Write:** Allows the user to create files, write data, create folders, and set attributes.

Special Permissions	Full Control	Modify	Read and Execute	Read	Write
Traverse Folder/Execute File	✓	✓	✓		
List Folder/Read Data	✓	✓	✓	✓	
Read Attributes	✓	✓	✓	✓	
Read Extended Attributes	✓	✓	✓	✓	
Create Files/Write Data	✓	✓			✓
Create Folders/Append Data	✓	✓			✓
Write Attributes	✓	✓			✓
Write Extended Attributes	✓	✓			✓
Delete Subfolders and Files	✓				
Delete	✓	✓			
Read Permission	✓	✓	✓	✓	✓
Change Permission	✓				
Take Ownership	✓				
Synchronise	✓	✓	✓	✓	✓

Table 15.2: Special permissions associated with each NTFS file permission

■ **NTFS permissions for folders:**

- **Full control:** Specifies whether the user has complete access to folders.
- **Modify:** This allows the user to read, write, execute, and traverse.
- **Read and execute:** This allows the user to list folders, read files, read attributes, and read permissions.
- **List folder contents:** Specifies if the user can access the folders and sub-folders.
- **Read:** This allows the user to list folders, read files, read attributes, and read permissions.
- **Write:** Allows a user to create files, write data, create folders, and set attributes.

Special Permissions	Full Control	Modify	Read and Execute	List Folder Contents	Read	Write
Traverse Folder/Execute File	✓	✓	✓	✓		
List Folder/Read Data	✓	✓	✓	✓	✓	
Read Attributes	✓	✓	✓	✓	✓	
Read Extended Attributes	✓	✓	✓	✓	✓	
Create Files/Write Data	✓	✓				✓
Create Folders/Append Data	✓	✓				✓
Write Attributes	✓	✓				✓
Write Extended Attributes	✓	✓				✓
Delete Subfolders and Files	✓					
Delete	✓	✓				
Read Permission	✓	✓	✓	✓	✓	✓
Change Permission	✓					
Take Ownership	✓					
Synchronise	✓	✓	✓	✓	✓	✓

Table 15.3: Special permissions associated with each NTFS folder permission

List folder contents permissions can be set only when they are inherited by folders and not files, whereas read and execute can only be set for files and folders.

It is possible to back up and restore data on NTFS files. However, it is not possible to set permissions to individual files and folders for FAT files.

To set, view, change, or remove special permissions for files and folders, go to a specific file or folder on which you want to set the special permission.

1. **Right-click** the file or folder, click **Properties**, and then click the **Security** tab
2. Click **Advanced**
3. Click **Add** to set special permissions for the user or new group in the **Permission Entry** window

In Linux, ACLs are used to implement access control by setting access permissions to a specific file or folder.

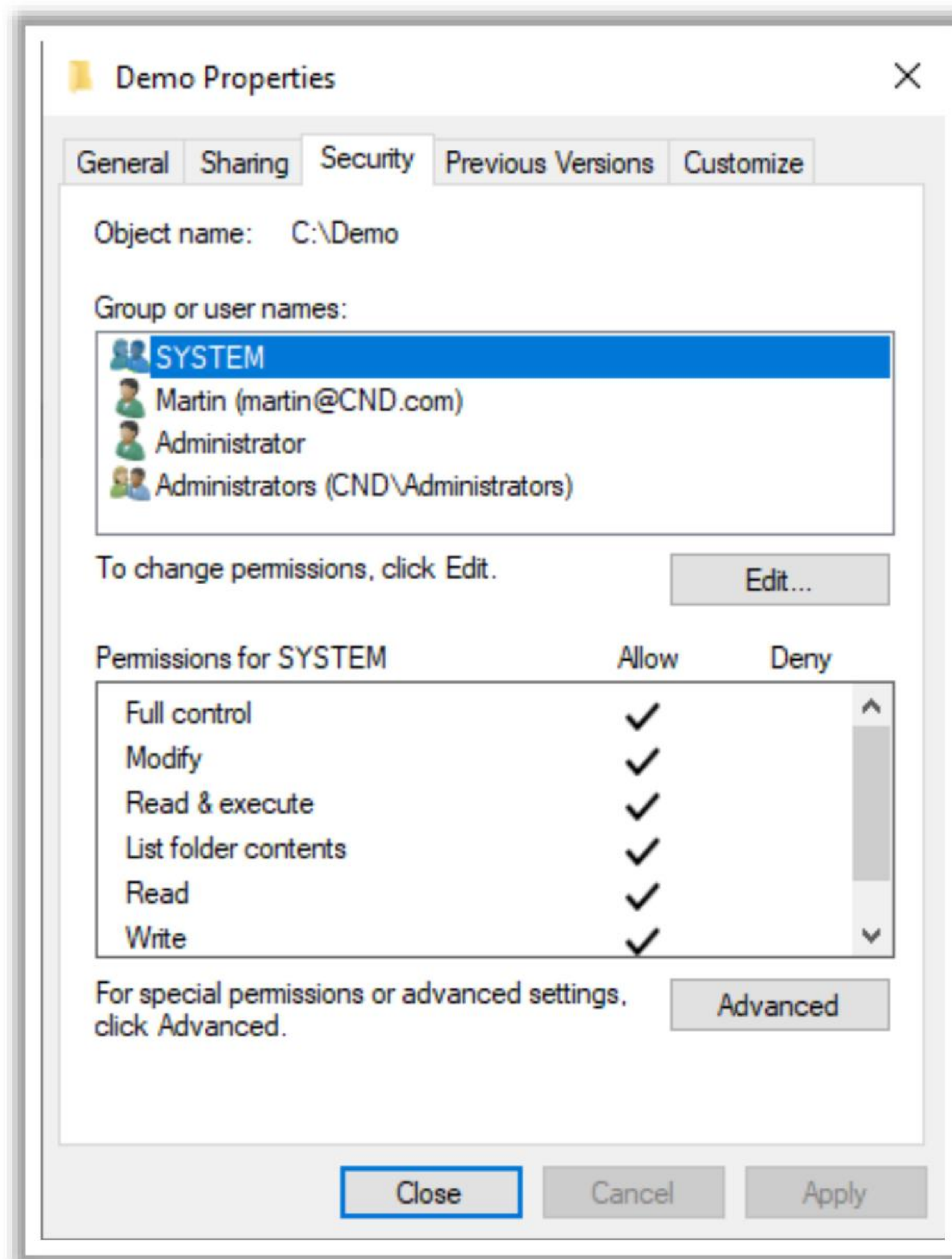


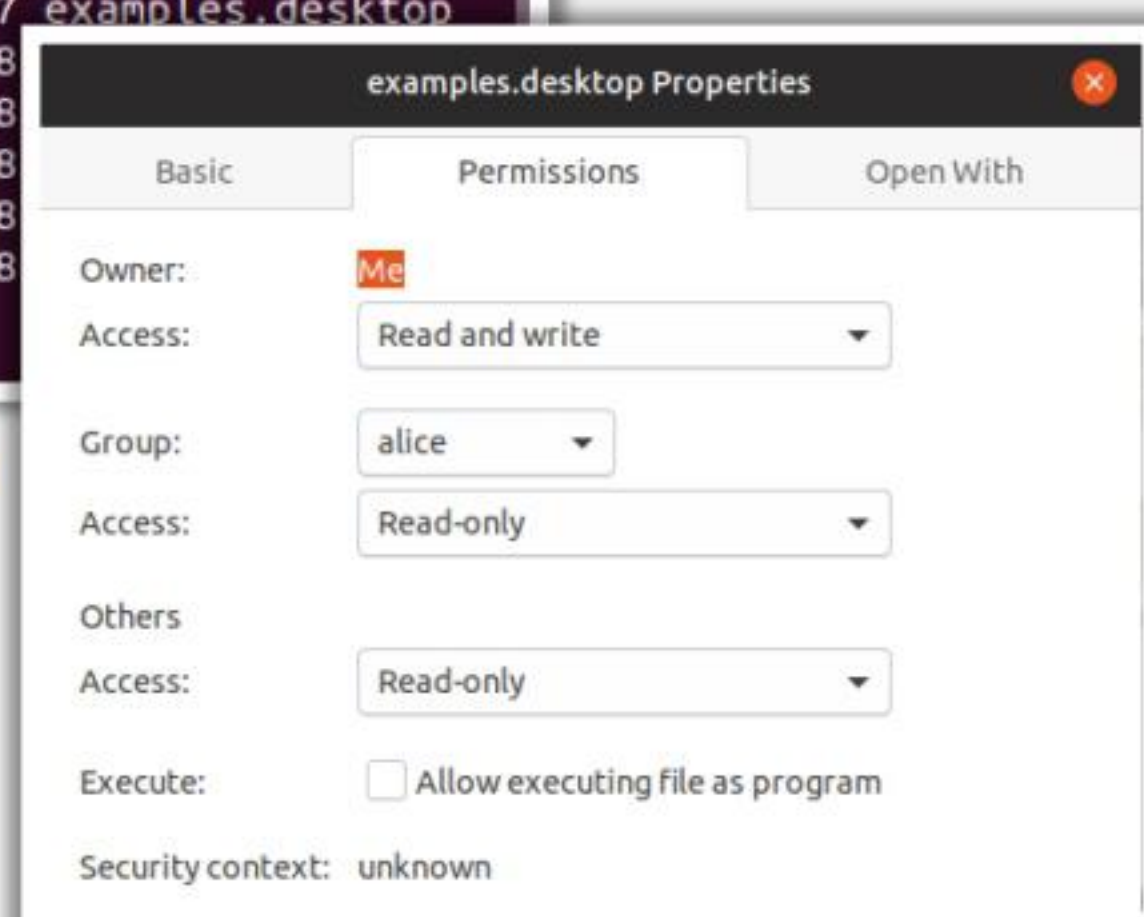
Figure 15.4: Screenshot of Properties window

ACL: Setting Access Controls and Permissions to Files and Folders in Linux

- ❑ In Linux, ACLs are used to implement access control by setting **access permissions** for specific files and folders

```
alice@alice-Virtual-Machine: ~  
alice@alice-Virtual-Machine:~$ ls -l  
total 52  
-rw-r--r-- 1 root root 7 Feb 4 07:45 demo.txt  
-rw-r--r-- 1 root root 85 Feb 4 07:40 demo.txt.gpg  
drwxr-xr-x 2 alice alice 4096 Feb 3 14:38 Desktop  
drwxr-xr-x 2 alice alice 4096 Feb 5 00:05 Documents  
drwxr-xr-x 2 alice alice 4096 Feb 3 14:38 Downloads  
-rw-r--r-- 1 alice alice 8980 Feb 3 11:37 examples.desktop  
drwxr-xr-x 2 alice alice 4096 Feb 3 14:38  
drwxr-xr-x 2 alice alice 4096 Feb 3 14:38  
drwxr-xr-x 2 alice alice 4096 Feb 3 14:38  
drwxr-xr-x 2 alice alice 4096 Feb 3 14:38  
alice@alice-Virtual-Machine:~$
```

Check permissions using **ls** command



Check permissions using **GUI**

- ❖ **setfacl** command: To assign alice read access to demo.txt file

```
root@alice-Virtual-Machine: /home/alice  
root@alice-Virtual-Machine:/home/alice# setfacl -m u:alice:r /home/alice/demo.txt  
root@alice-Virtual-Machine:/home/alice#
```

- ❖ **getfacl** command: To displays the file name, owner, the group, and the access control list (ACL)

```
root@alice-Virtual-Machine: /home/alice  
root@alice-Virtual-Machine:/home/alice# getfacl demo.txt  
# file: demo.txt  
# owner: root  
# group: root  
user::rw-  
user:alice:r--  
group::r--  
mask::r--  
other::r--  
root@alice-Virtual-Machine:/home/alice#
```

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

ACL: Setting Access Controls and Permissions to Files and Folders in Linux

In Linux, a user can use commands such as `chmod`, `chown`, `chgrp`, etc. to set the permissions on files or folders. ACL provides detailed access control features. It can precisely configure permissions on files or folders.

Steps to Configure ACLs to Set File and Folder Permissions

▪ Step 1: Install ACL Package

Install the `acl` package to use ACLs. You can use the below statement to install `acl` package:

```
# yum install acl
```

▪ Step 2: Configure ACL Support on a File System

The file system consisting of the files or directories should be supported. Use the following statement to mount a local `ext3` file system with ACL support:

```
# mount -t ext3 -o acl [device-name] [mount-point]
```

For example,

```
# mount -t ext3 -o acl /dev/mapper/VolGroup00-LogVol100 /data
```

If `/etc/fstab` contains a partition, include the `acl` options:

```
# vi /etc/fstab
```

```
LABEL=/data    /data    ext3    acl    0    0
```


▪ Step 3: ACL Rules

ACL rules define how a specific user or group can access the file or directory. There are two types of ACL rules:

- **Access ACLs:** It specifies user and group access permissions for a specific file or directory
- **Default ACLs:** It is applied only to a directory. It specifies the access permissions that a directory inherits from its parent directory.

Commands for Setting up Access ACL Permission for Files

To set or modify one or more ACL rules on any file or directory, use setfacl command as follows:

```
# setfacl -m [rules] [files]
```

where the **rules** are:

- **u:name:permissions:** It configures access ACL for a specific user [r, w, and x for read, write, and execute, respectively]
- **g:name: permissions:** It configures access ACL for a specific group
- **m:permissions:** It configures the effective rights mask. It is a combination of permissions for user / group.
- **o:permissions:** It configures access ACL for everyone

For example,

To set read and write permission in the ACL of file test for a guest user, use the following statement:

```
# setfacl -m u:user1:rwX test
```

To remove all access ACL rules of the file test for a guest user, use the following statement:

```
# setfacl -x u:guest test
```

To remove all ACL rules of the file test for a guest user, use the following statement:

```
# setfacl -b u:guest test
```

Command for Setting the Default ACLs

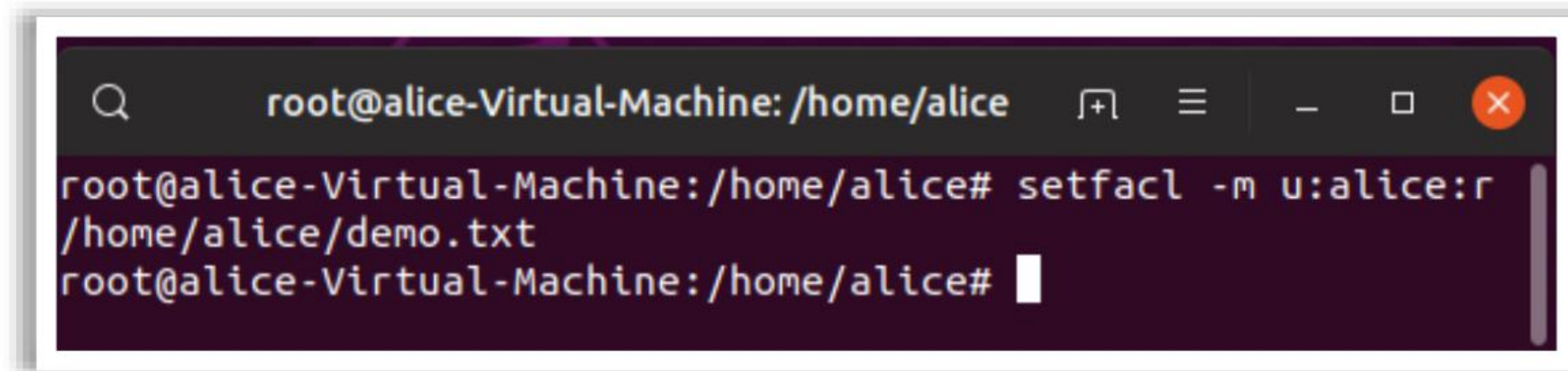
By adding d: before the access rule and defining a directory name in place of a file name, you can configure the default ACL.

```
# setfacl -m d:o:rx /[directory]
```

For example,

To set default ACL for test directory, use the following statement:

```
# setfacl -m d:o:rx /Testdir
```

```
root@alice-Virtual-Machine: /home/alice
root@alice-Virtual-Machine:/home/alice# setfacl -m u:alice:r /home/alice/demo.txt
root@alice-Virtual-Machine:/home/alice#
```

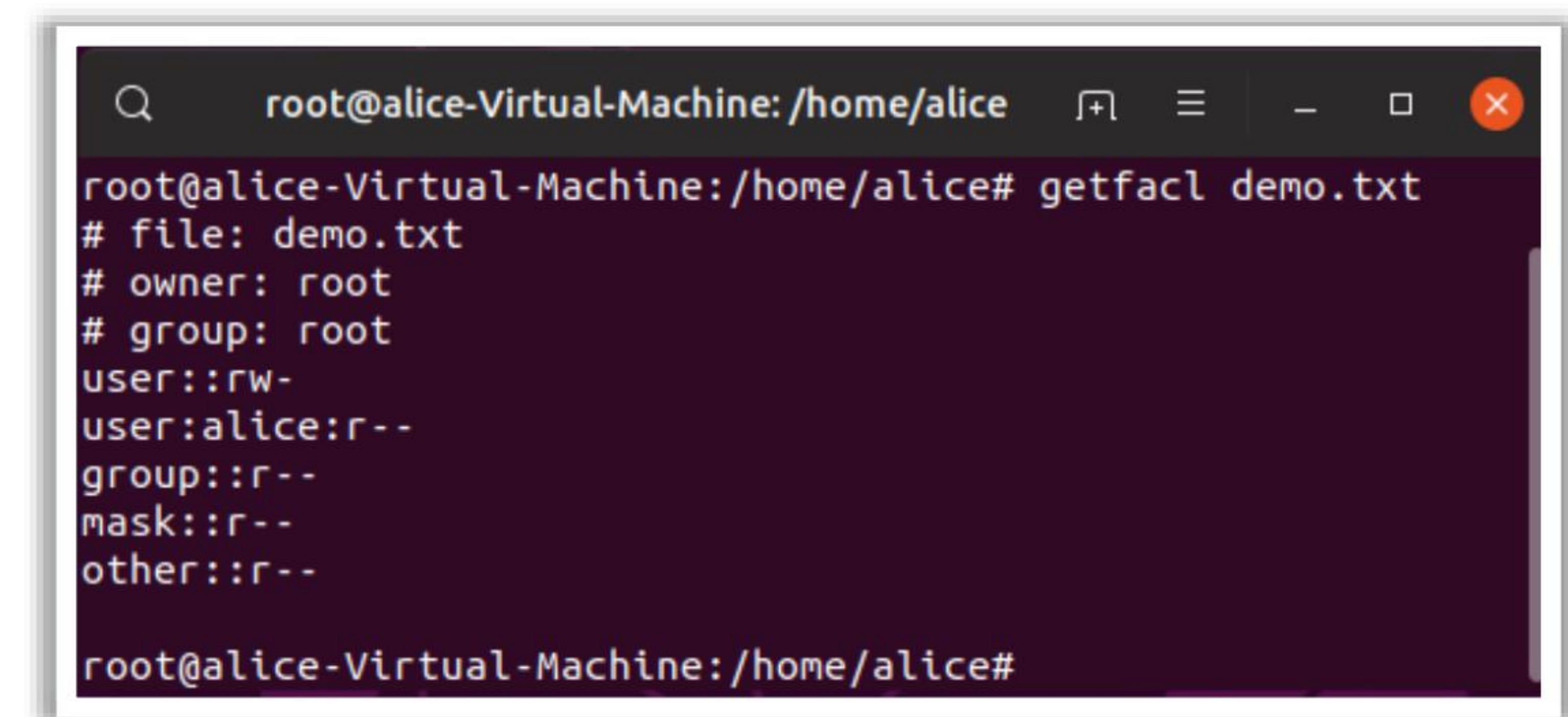
Figure 15.5: setfacl command

Command to Display ACLs Rules on Files

To display ACL on any file or directory, you can use the `getfacl` command, as shown below.

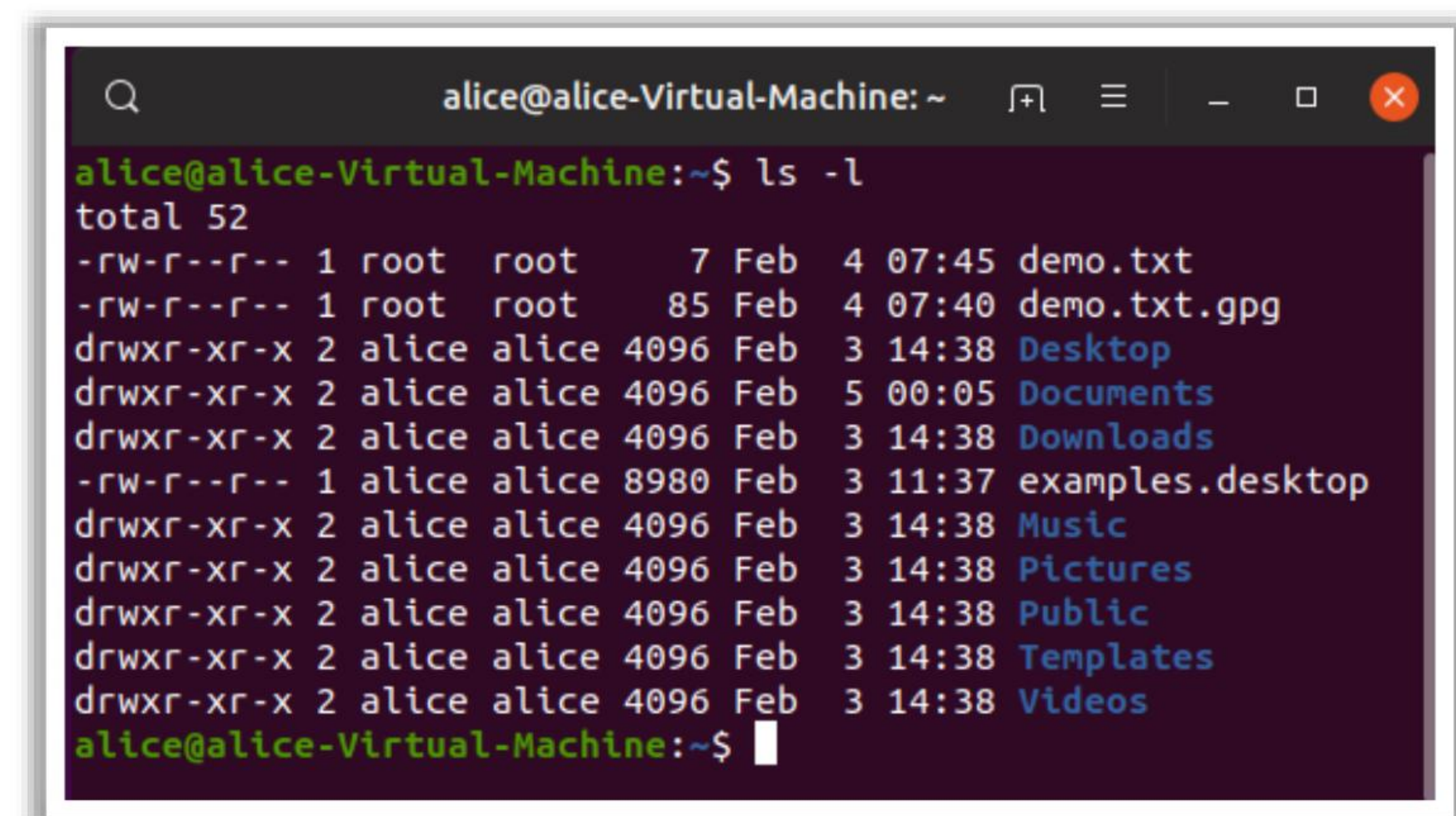
`#getfacl [file/directory]`

For example, `#getfacl test` will display the ACL for the test file



```
root@alice-Virtual-Machine: /home/alice
root@alice-Virtual-Machine:/home/alice# getfacl demo.txt
# file: demo.txt
# owner: root
# group: root
user::rw-
user:alice:r--
group::r--
mask::r--
other::r--
root@alice-Virtual-Machine:/home/alice#
```

Figure 15.6: getfacl command



```
alice@alice-Virtual-Machine: ~
alice@alice-Virtual-Machine:~$ ls -l
total 52
-rw-r--r-- 1 root root 7 Feb 4 07:45 demo.txt
-rw-r--r-- 1 root root 85 Feb 4 07:40 demo.txt.gpg
drwxr-xr-x 2 alice alice 4096 Feb 3 14:38 Desktop
drwxr-xr-x 2 alice alice 4096 Feb 5 00:05 Documents
drwxr-xr-x 2 alice alice 4096 Feb 3 14:38 Downloads
-rw-r--r-- 1 alice alice 8980 Feb 3 11:37 examples.desktop
drwxr-xr-x 2 alice alice 4096 Feb 3 14:38 Music
drwxr-xr-x 2 alice alice 4096 Feb 3 14:38 Pictures
drwxr-xr-x 2 alice alice 4096 Feb 3 14:38 Public
drwxr-xr-x 2 alice alice 4096 Feb 3 14:38 Templates
drwxr-xr-x 2 alice alice 4096 Feb 3 14:38 Videos
alice@alice-Virtual-Machine:~$
```

Figure 15.7: Checking permissions using ls command

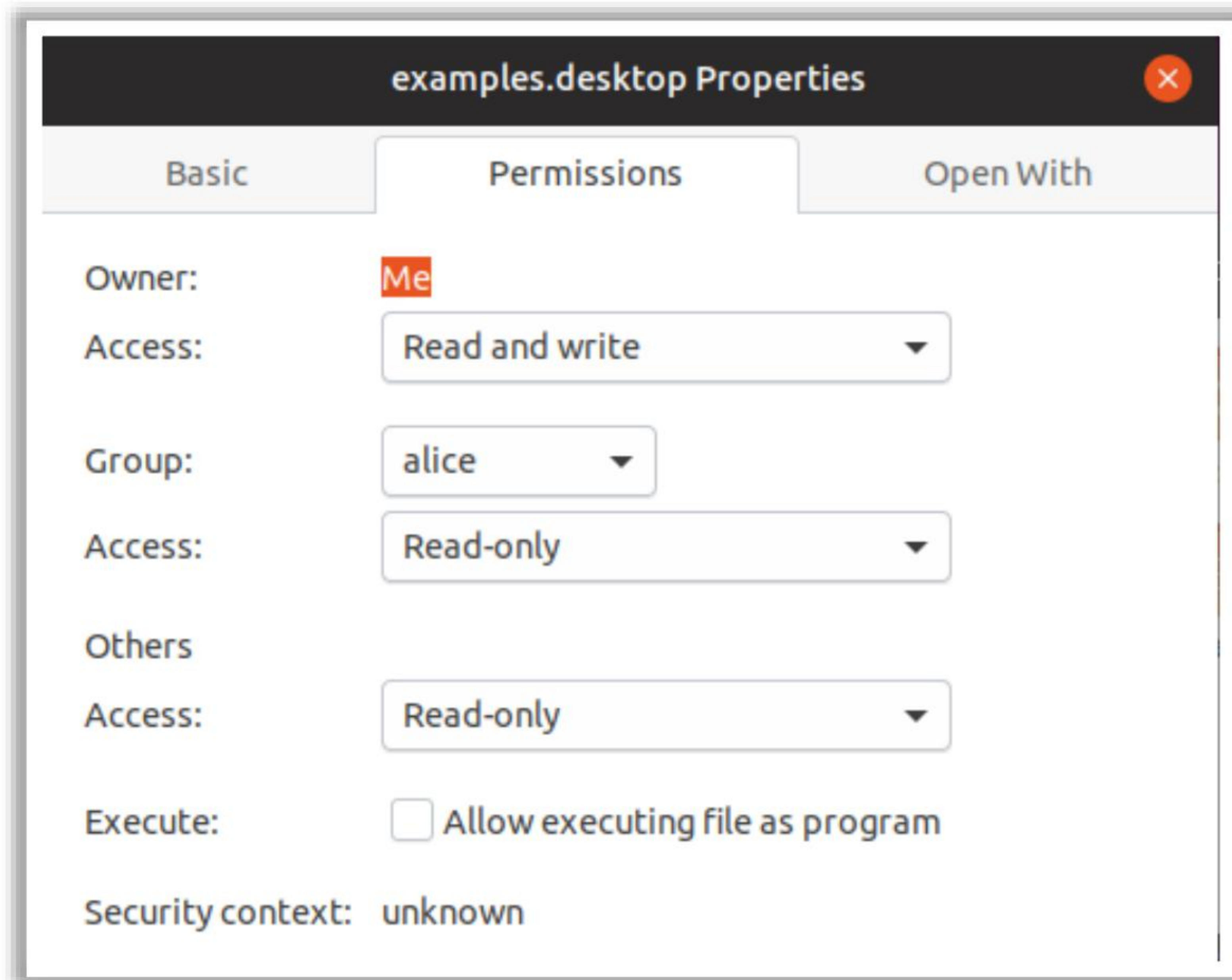
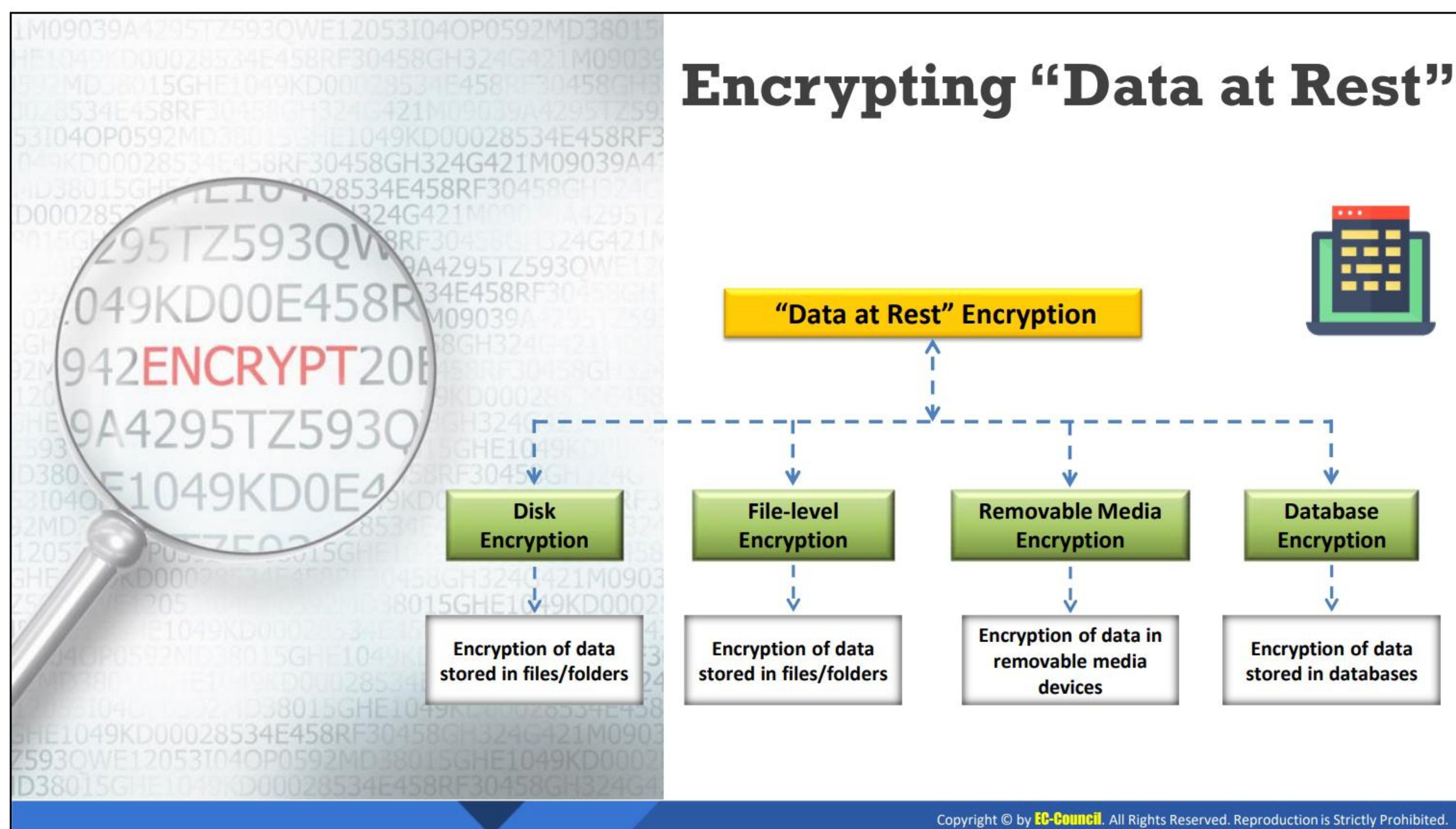


Figure 15.8: Checking permissions using GUI



Encrypting "Data at Rest"

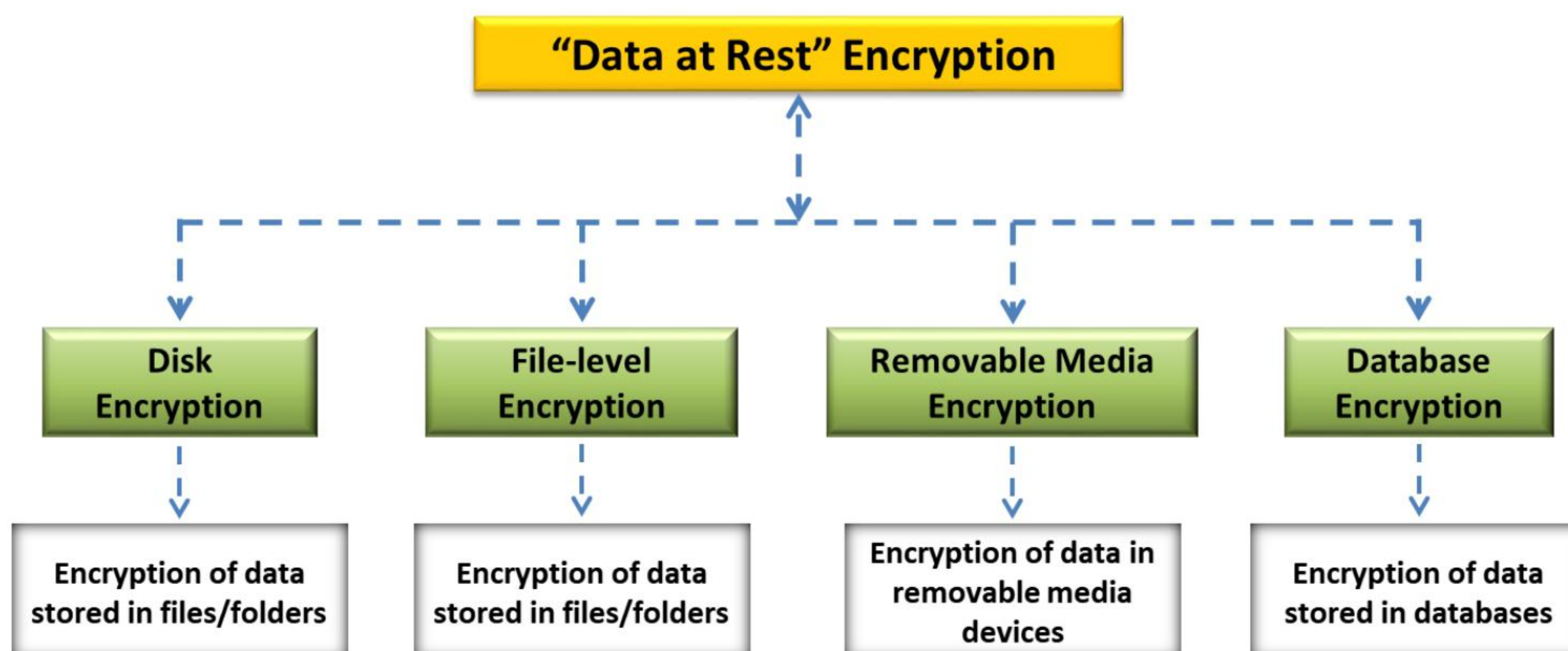


Figure 15.9: "Data at rest" encryption

- **Disk encryption:** Encryption of data stored in a physical or logical disk. Full disk encryption is the encryption of all data in a disk except the master boot record (MBR). The data is automatically converted into a form which cannot be easily deciphered by an unauthorized user. In full disk encryption, the data is encrypted while being written on the disk, and decrypted when the user reads the data from the disk. The benefits of full disk encryption are
 - It is a simple encryption method.
 - The encryption method is clear and coherent to users, applications, and databases.

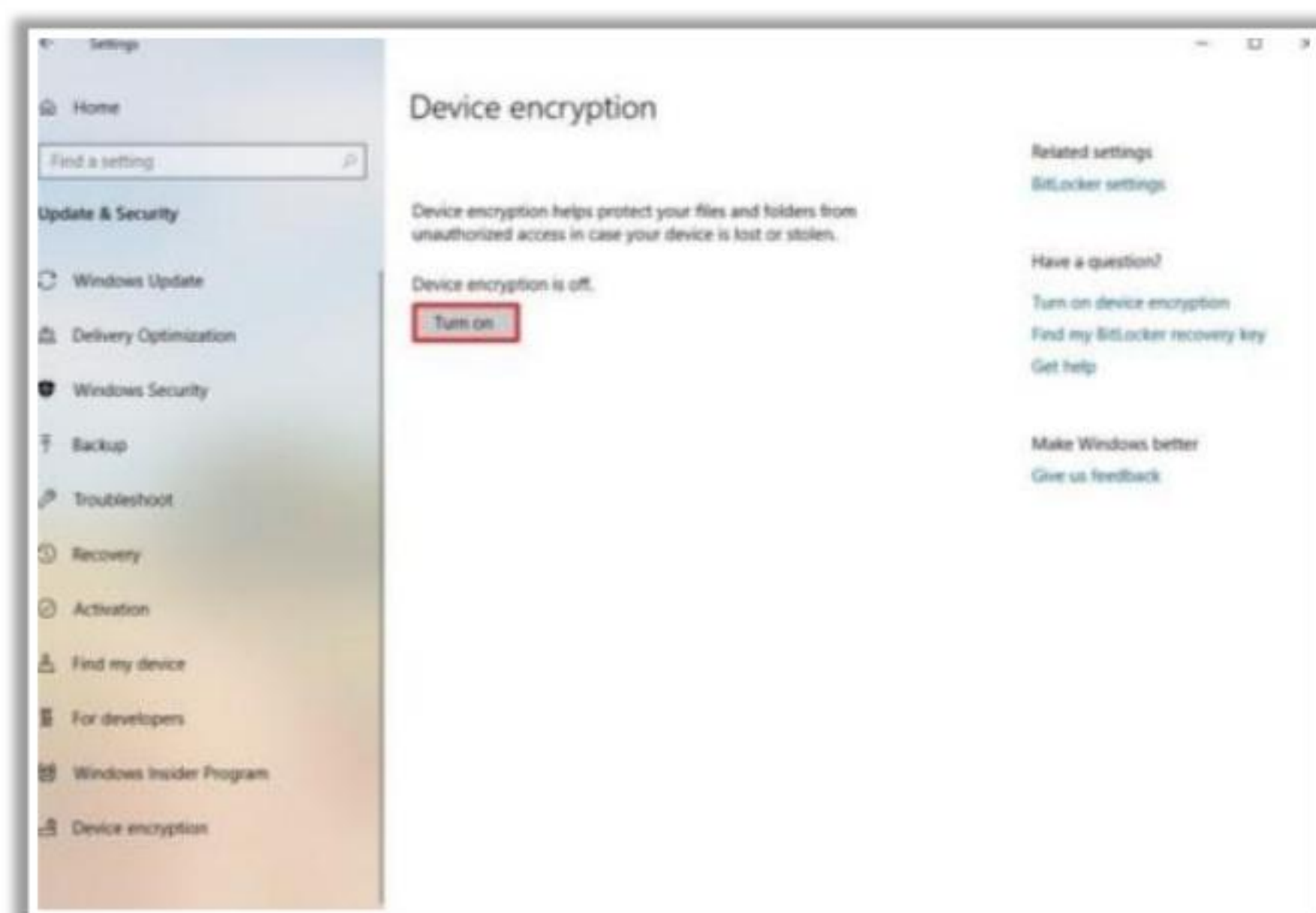
- It is a hardware-based encryption with high performance.
- **File-level encryption:** Encryption of data stored in files/folders. In this type of encryption, the encryption occurs at a filesystem level, and in combination with a cryptographic algorithm, the encrypted data will be extremely secure. File-level encryption regulates the access of unauthorized users to files or folders on networks or shared computers. The advantages of file-level encryption are as follows:
 - Each file is encrypted with a discrete encryption key.
 - Access control is enforced using public key cryptography.
 - Both structured and unstructured data are supported.
- **Removable media encryption:** Removable media encryption prevents removable media devices such as USB flash drives, portable hard disks, digital cameras, smartphones, tablets, etc. from unauthorized access.
- **Database encryption:** Encryption of a specific subset of data or entire data stored in a database. The advantages of database encryption are as follows:
 - It safeguards the data in a database.
 - It protects against a wide range of threats, including malicious insiders.

Disk Encryption: Implementing Built-in Disk Encryption for Windows

1. Enabling Device Encryption

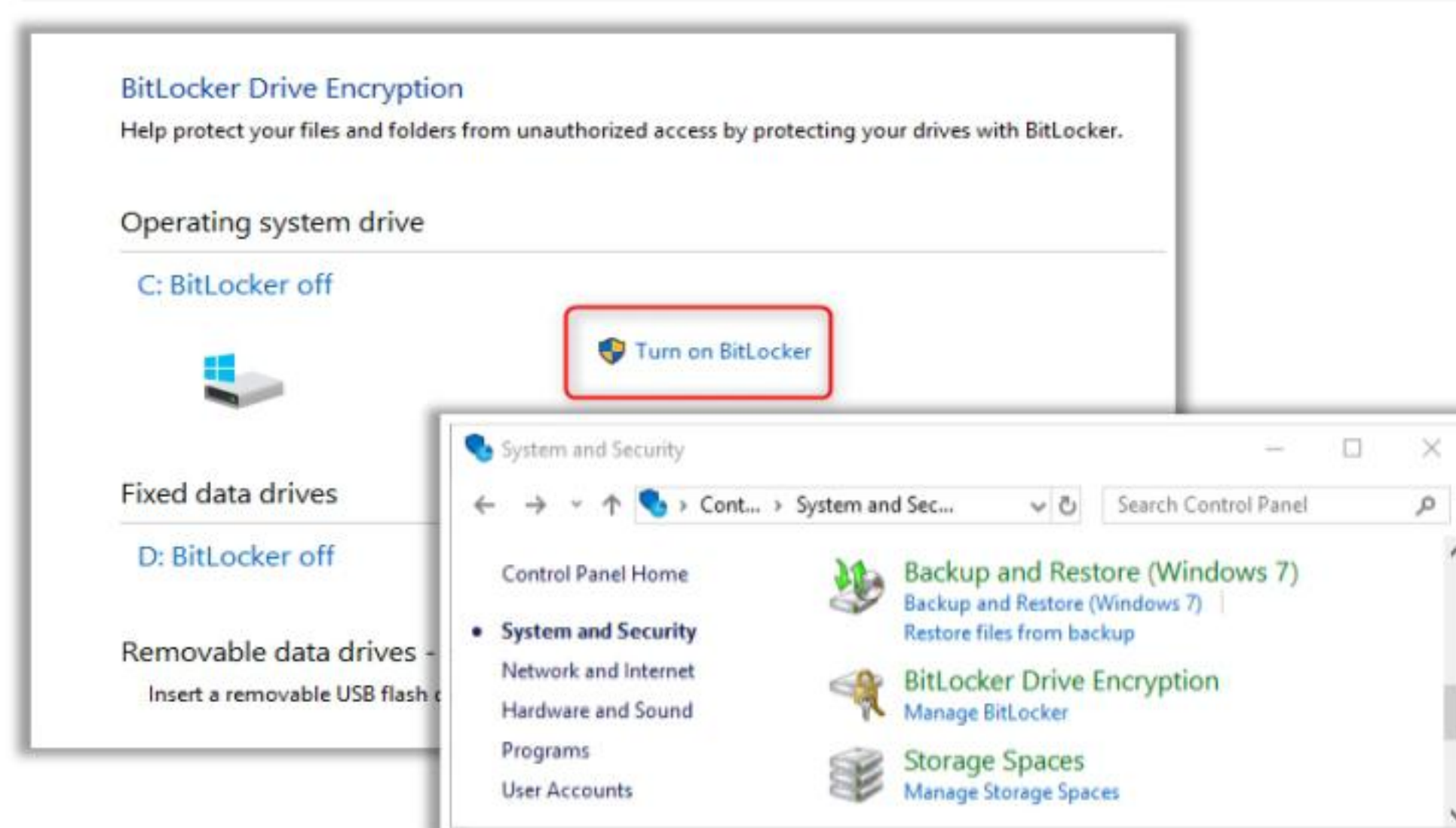


- ✓ Go to **Start** → **Settings** → **Update & Security** → **Device Encryption**
- ✓ **Turn on** Device encryption option



2. Enabling Standard BitLocker Encryption

- ✓ Sign in with an Administrator Account. Select the **Start** button, Choose **Control Panel**, and then click **System and Security**
- ✓ Under **BitLocker Drive Encryption**, choose **Manage BitLocker**
- ✓ Select **Turn on BitLocker**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Disk Encryption: Implementing Built-in Disk Encryption for Windows

Windows 10 has built-in disk encryption methods to encrypt hard drives and safeguard user data. By default, disk encryption is enabled in all devices using Windows 10. There are two methods of disk encryption in Windows 10: device encryption and BitLocker. If the users do not have device encryption, they can enable standard BitLocker encryption; however, BitLocker is not available on Windows 10 Home edition.

Device encryption

It is the simplest encryption method and is available in all editions of Windows 10. If a user loses the device, device encryption can protect the data from unauthorized access. This feature scrambles the entire system drive and secondary drives connected to the device and allows only the user to access the device.

Prerequisites for Device Encryption:

1. Trusted platform module (TPM).
2. Unified extensible firmware interface (UEFI).
3. Checking whether the device meets the device encryption requirements.

Steps to check whether the device meets the device encryption requirements:

- Click the **Start** button.
- Search for **System Information**, right-click on the top result, and choose **Run as administrator**.
- Click **System Summary** on the left pane.

- Search **Device Encryption Support**; the user device support device encryption if it reads **Meets prerequisites**.

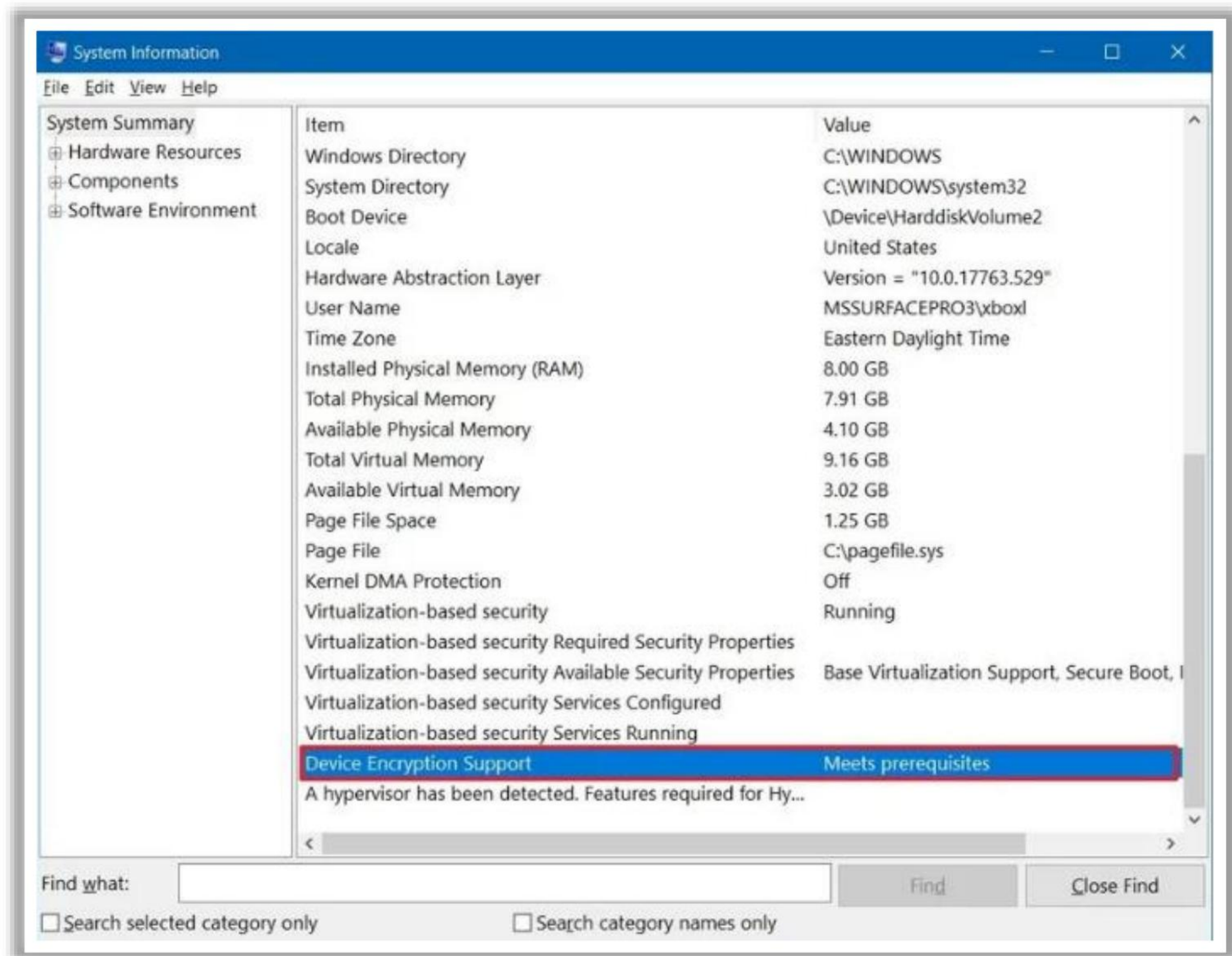


Figure 15.10: Checking whether the device is meeting the device encryption requirements

To enable TPM on UEFI

Follow these steps to enable the TPM chip in the user device if it is in a disabled state.

- Open **Settings**.
- Select **Update & Security**.
- Select **Recovery**.
- Browse to **Advanced start up** section and click **Restart now** button.

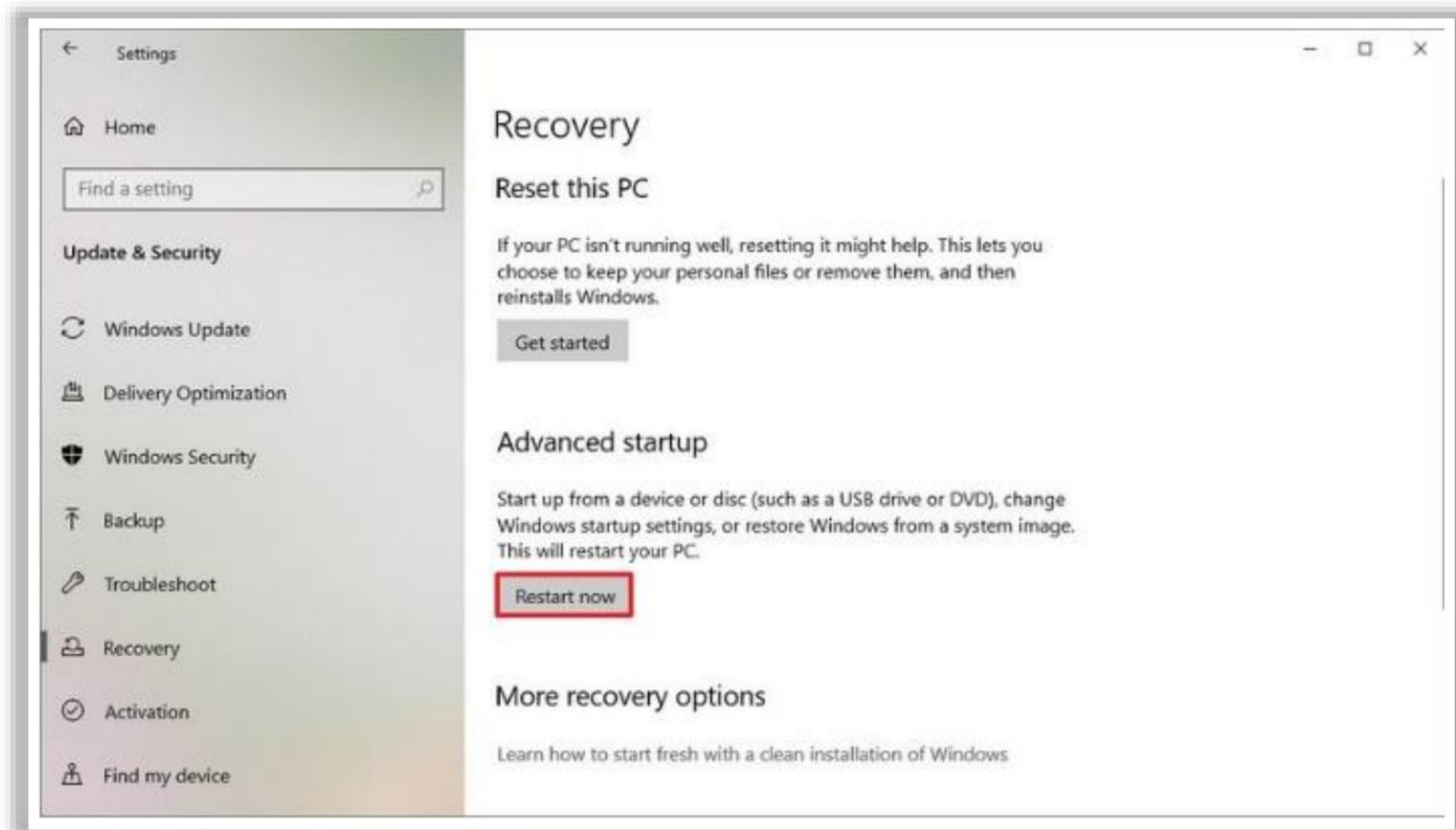


Figure 15.11: Enabling TPM on UEFI

- Click on **Troubleshoot**.

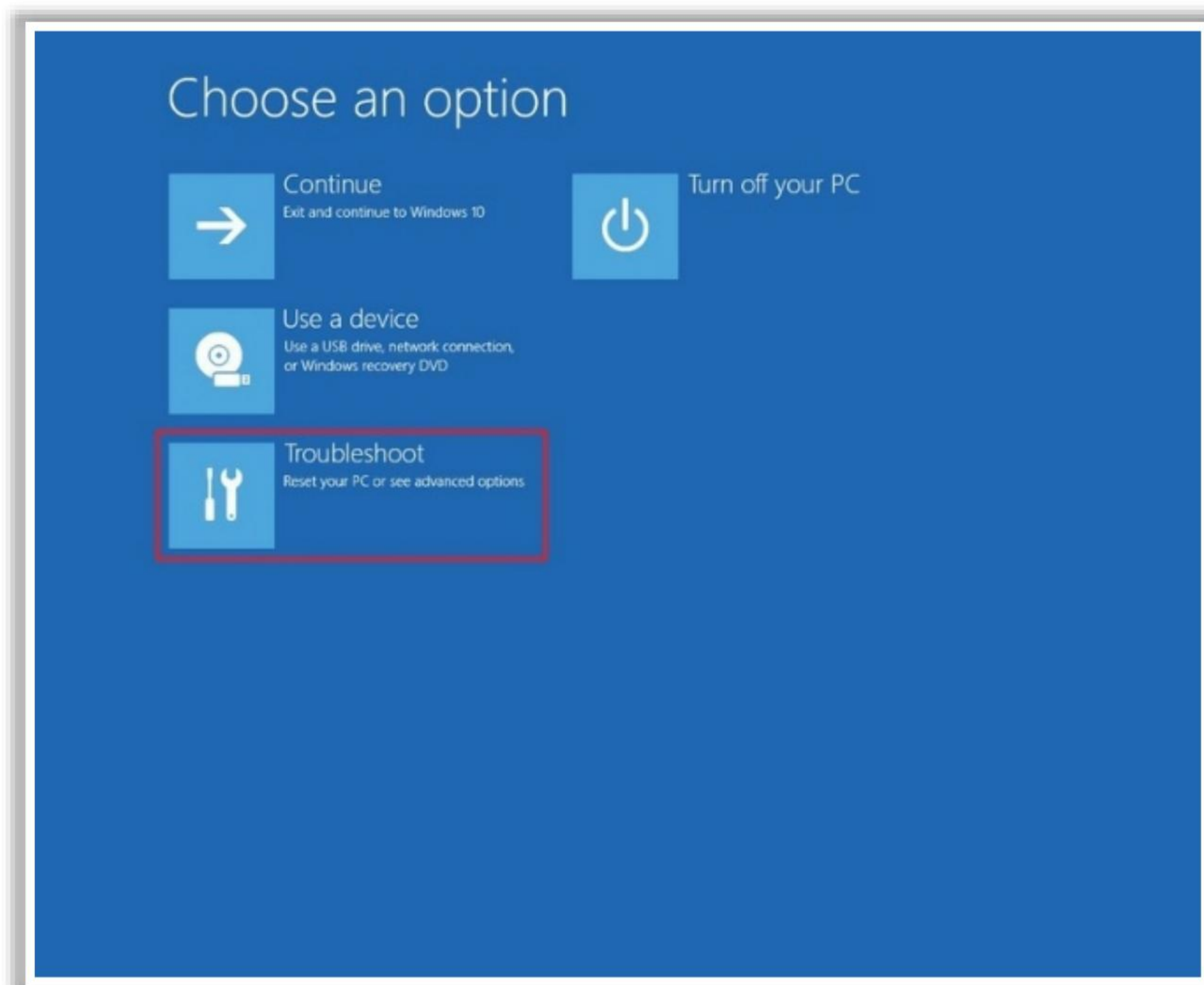


Figure 15.12: Choosing Troubleshoot Option

- Click on **Advanced Options**.

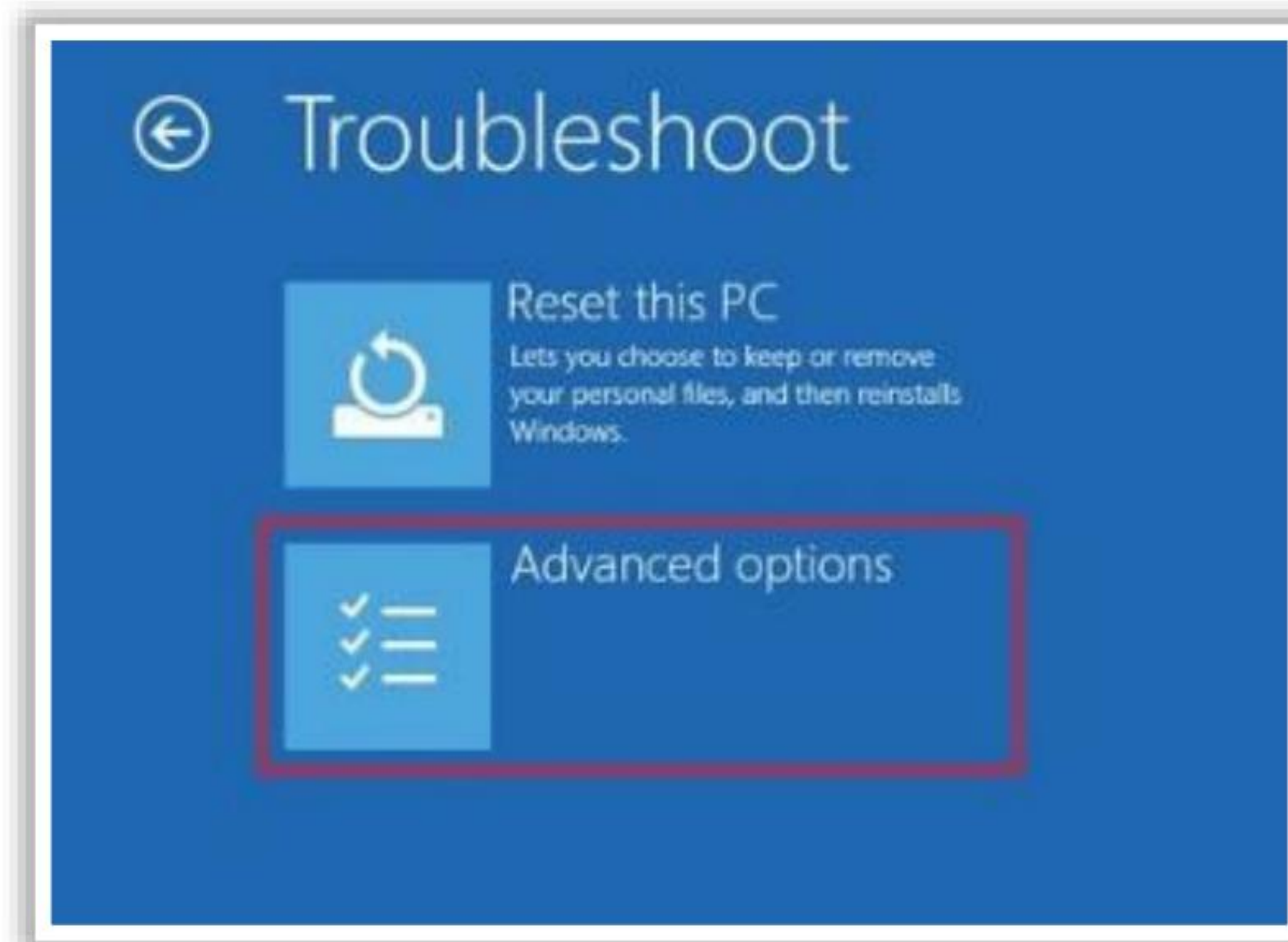


Figure 15.13: Clicking on Advanced Options

- Click on **UEFI Firmware Settings**.

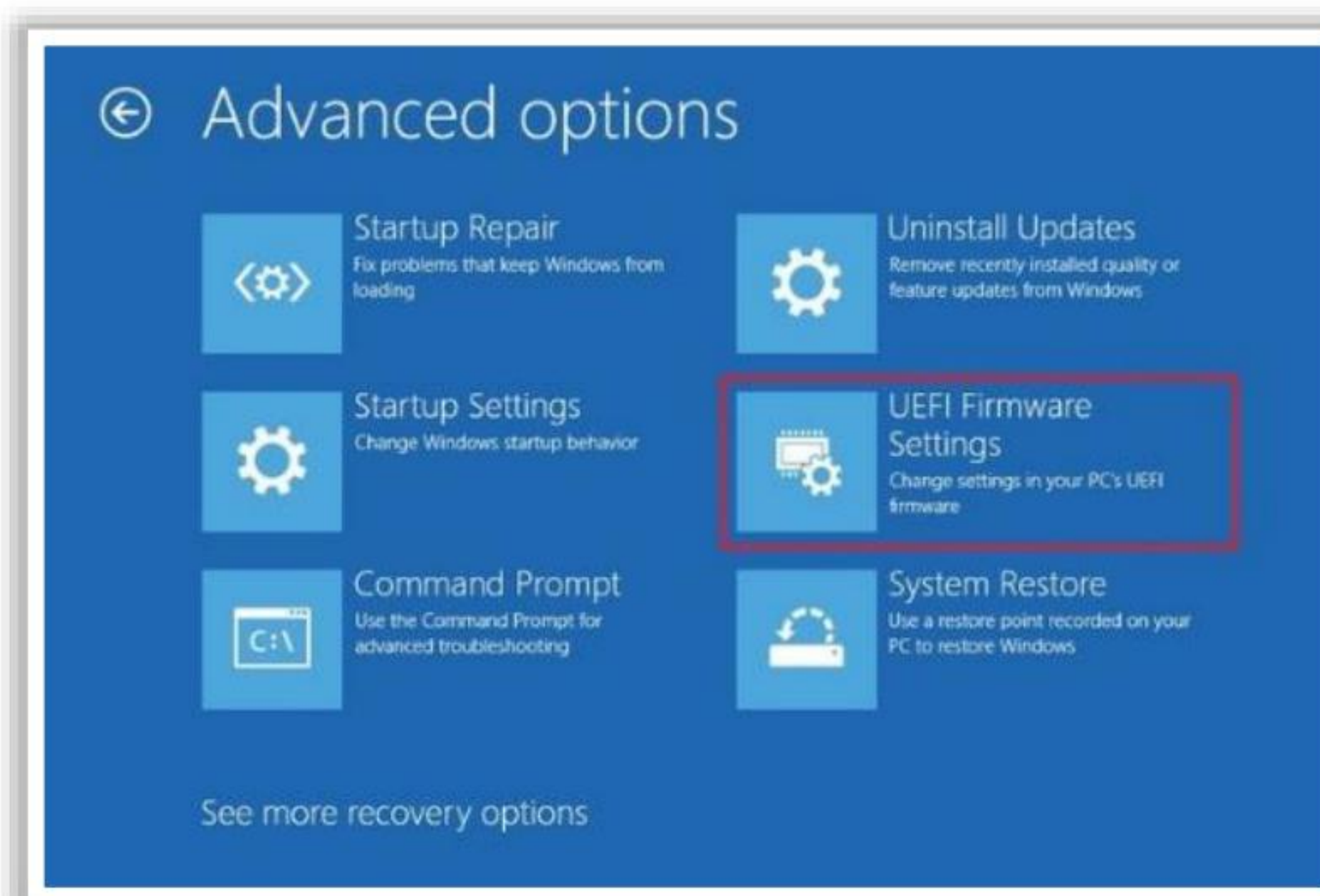


Figure 15.14: Selecting UEFI Firmware Settings

- Click **Restart**.



Figure 15.15: Restarting the System to change the UEFI Firmware Settings

- Navigate to security settings.
- Enable the TPM feature.

To Enable Device Encryption

- Go to **Start → Settings → Update & Security → Device Encryption**.
- **Turn on** the Device encryption option.



Figure 15.16: Enabling Device Encryption

BitLocker encryption

This protects the data by encrypting the entire volume of data using advanced encryption standard (AES) encryption algorithm in cipher block chaining (CBC) or XTS mode with a 128-bit or 256-bit key. BitLocker is available in Windows 10 Pro, Enterprise, or Education editions.

To Enable Standard BitLocker Encryption

- Sign in with an administrator account.
- Select the **Start** button.
- Choose **Control Panel**, then click on **System and Security**.
- Under **BitLocker Drive Encryption**, choose **Manage BitLocker**.
- Select **Turn on BitLocker**.

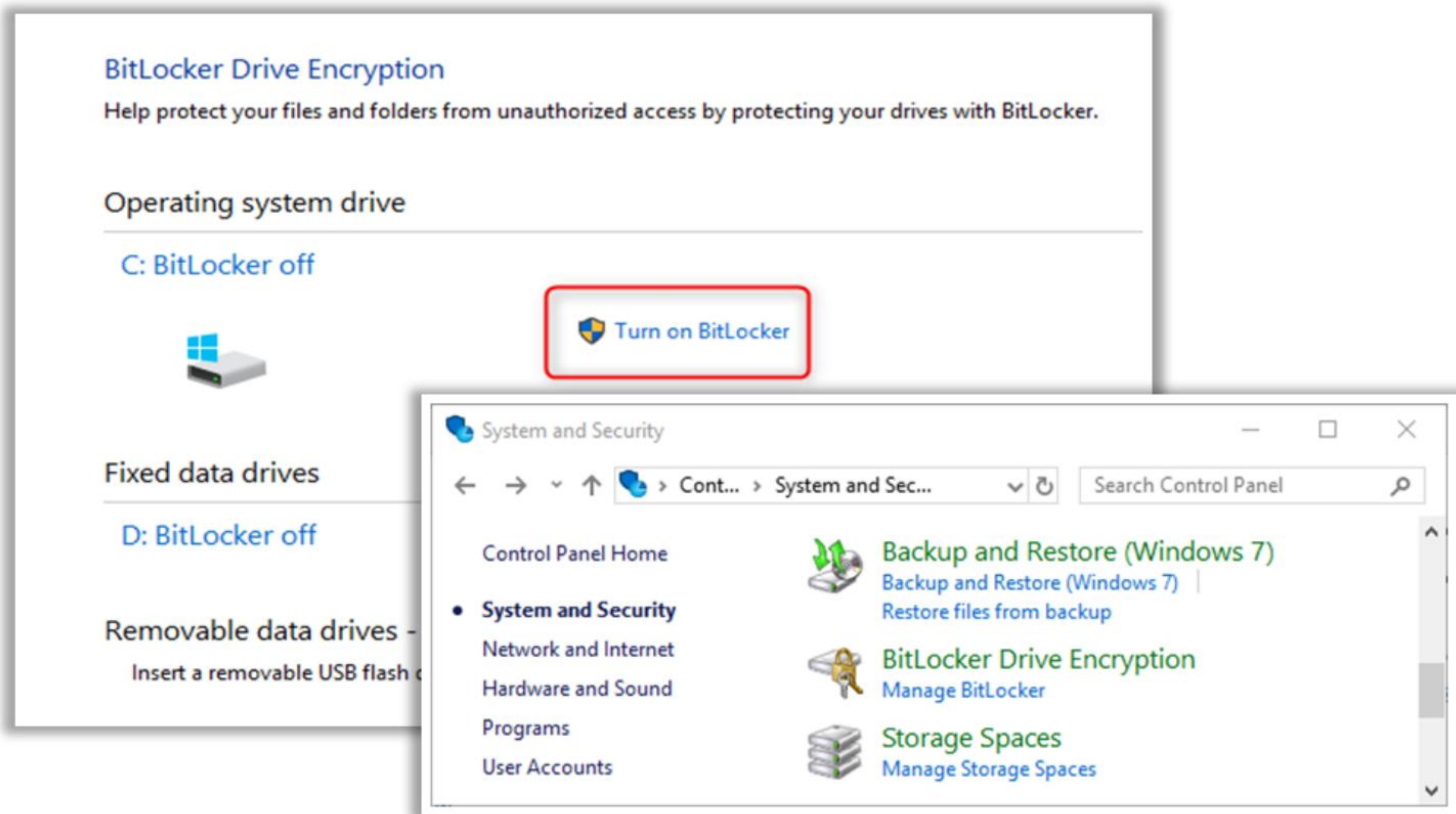
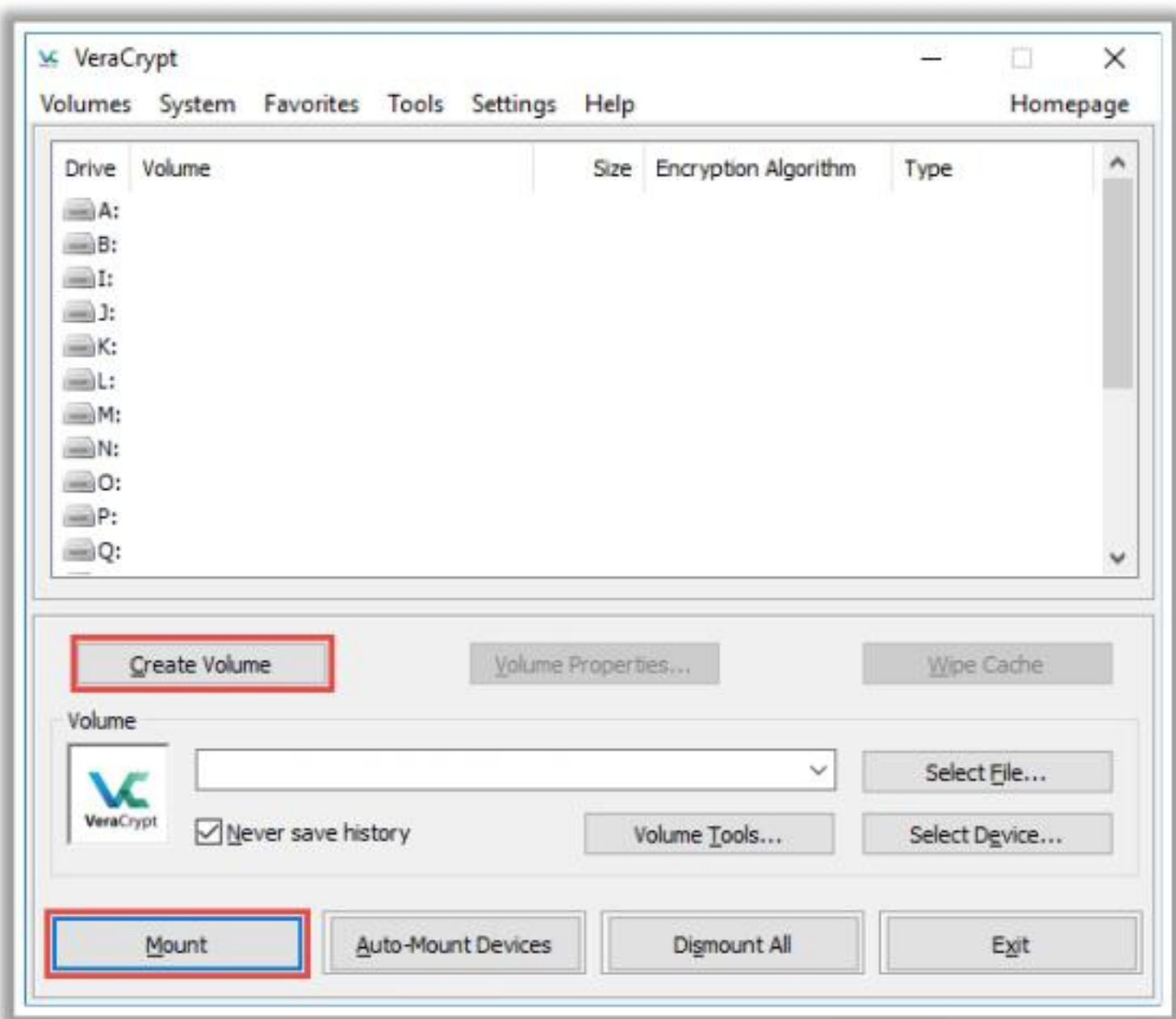


Figure 15.17: Enabling Standard BitLocker Encryption

Disk Encryption Tools

VeraCrypt

- VeraCrypt is a software for establishing and maintaining an **on-the-fly-encrypted volume** (data storage device)
- On-the-fly encryption means that **data is automatically encrypted** immediately before it is saved and decrypted immediately after it is loaded, without any user intervention



<https://www.veracrypt.fr>

 **BitLocker Drive Encryption**
<https://docs.microsoft.com>

 **FinalCrypt**
<https://www.finalcrypt.org>

 **Seqrite Encryption Manager**
<https://www.seqrite.com>

 **FileVault**
<https://support.apple.com>

 **Gilisoft Full Disk Encryption**
<http://www.gilisoft.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Disk Encryption Tools

The common goal of disk encryption tools is to encrypt a disk partition to provide confidentiality to the information stored on it. Some disk encryption tools are discussed below.

- **VeraCrypt**

Source: <https://www.veracrypt.fr>

VeraCrypt is a software for establishing and maintaining an on-the-fly-encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted just before it is saved and decrypted just after it is loaded without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. The entire file system is encrypted (e.g., file names, folder names, free space, metadata, etc.).

Files can be copied to and from a mounted VeraCrypt volume just like they are copied to/from any normal disk (e.g., by simple drag-and-drop operations). Files are automatically decrypted on the fly (in memory/RAM) while they are read or copied from an encrypted VeraCrypt volume. Similarly, files that are written or copied to the VeraCrypt volume are automatically encrypted on the fly (just before they are written to the disk) in RAM.

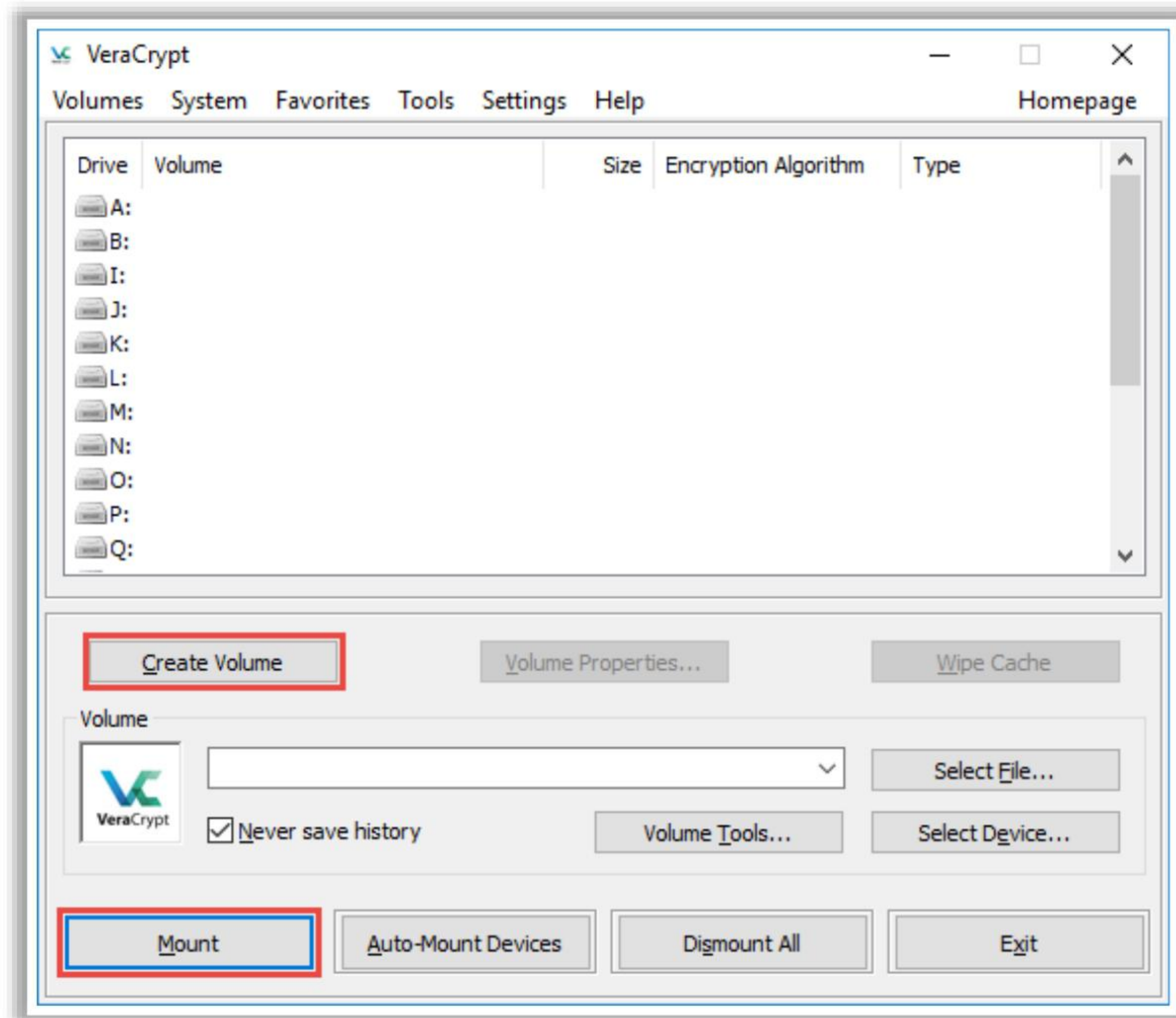


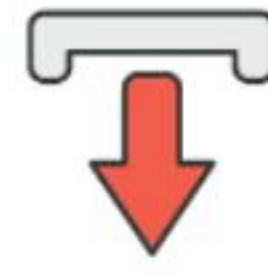
Figure 15.18: Screenshot of VeraCrypt

Some additional disk encryption tools are as follows:

- BitLocker Drive Encryption (<https://docs.microsoft.com>)
- FinalCrypt (<https://www.finalcrypt.org>)
- Seqrite Encryption Manager (<https://www.seqrite.com>)
- FileVault (<https://support.apple.com>)
- Gilisoft Full Disk Encryption (<http://www.gilisoft.com>)

File Level Encryption: Implementing Built-in File System-level Encryption on Windows

 The Encrypting File System (EFS) provides **file system-level encryption** in Windows



C:\Windows\system32\cmd.exe

```
c:\Windows\System32>cipher /e "d:\Demo\Sample.txt"

Encrypting files in d:\Demo\
Sample.txt      [OK]

1 file(s) [or directorie(s)] within 1 directorie(s) were encrypted.

Converting files from plaintext to ciphertext may leave sections of old
plaintext on the disk volume(s). It is recommended to use command
CIPHER /W:directory to clean up the disk after all converting is done.

c:\Windows\System32>
```

Advanced Attributes

Choose the settings you want for this folder.
When you click OK or Apply on the Properties dialog, you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

☒ Folder is ready for archiving

☒ Allow files in this folder to have contents indexed in addition to file properties

Compress or Encrypt attributes

☐ Compress contents to save disk space

☒ Encrypt contents to secure data

[Details](#)

OK Cancel

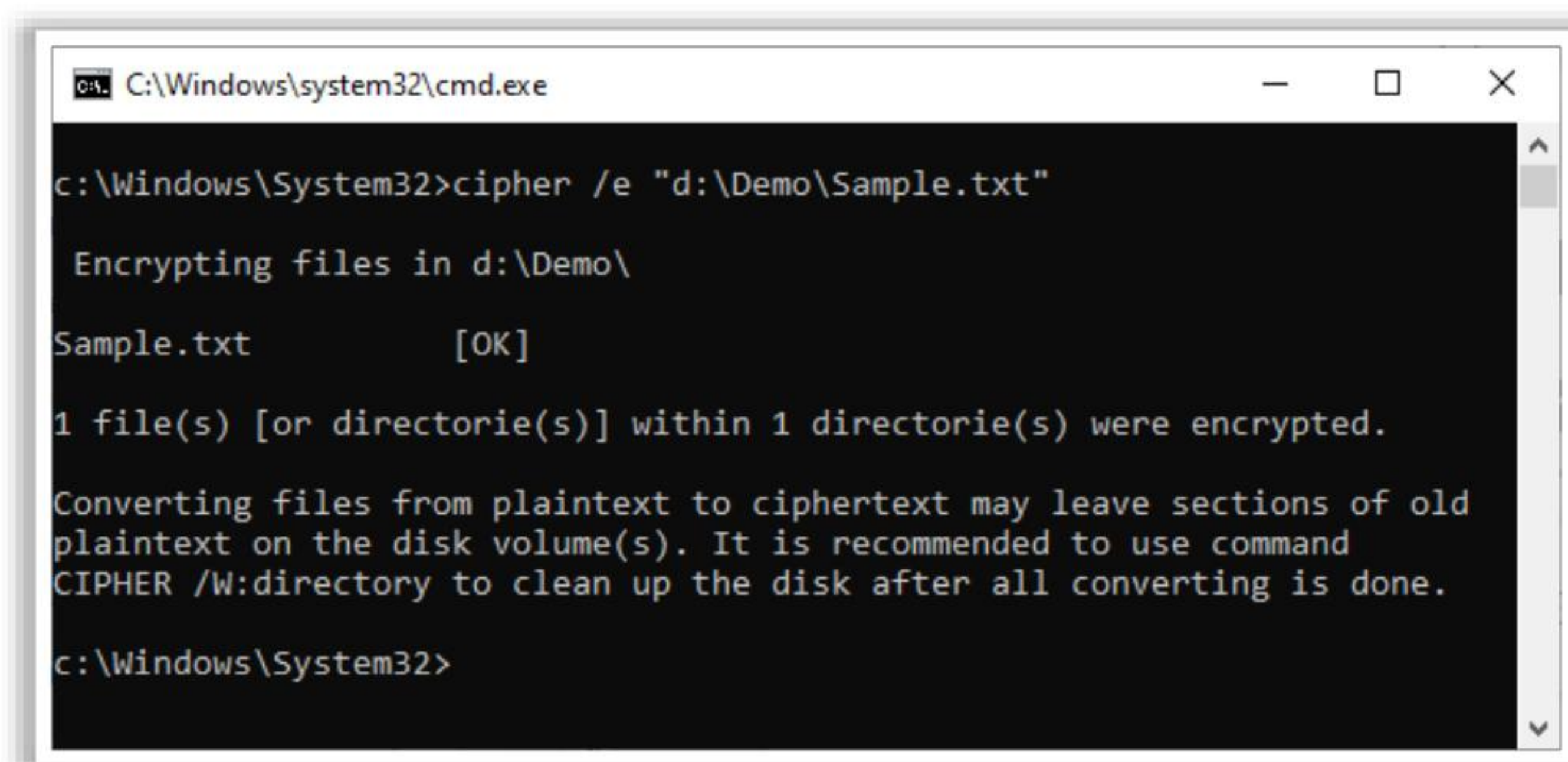
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

File Level Encryption: Implementing Built-in File System-level Encryption on Windows

The Encrypting File System (EFS) provides file system-level encryption in Windows (starting from Windows 2000), except the home version. The user needs to enable this feature on a specific file, directory, or drive. EFS protects the confidential information from unauthorized users who have physical access to a computer.

File Encryption with EPS Using Command Prompt

- Right-click on the Start button and select **Command Prompt (Admin)**.
- Type the following command:
`cipher /e "<PATH>"`
- Enter the file path with extension and hit **Enter**.



```
C:\Windows\system32\cmd.exe

c:\Windows\System32>cipher /e "d:\Demo\Sample.txt"

Encrypting files in d:\Demo\
Sample.txt      [OK]

1 file(s) [or directorie(s)] within 1 directorie(s) were encrypted.

Converting files from plaintext to ciphertext may leave sections of old
plaintext on the disk volume(s). It is recommended to use command
CIPHER /W:directory to clean up the disk after all converting is done.

c:\Windows\System32>
```

Figure 15.19: File encryption with EPS

To enable EPS Using Advanced Attributes in a Selected File/Folder

- Select the file for encryption using EFS.
- Right-click on the file and select **Properties**.

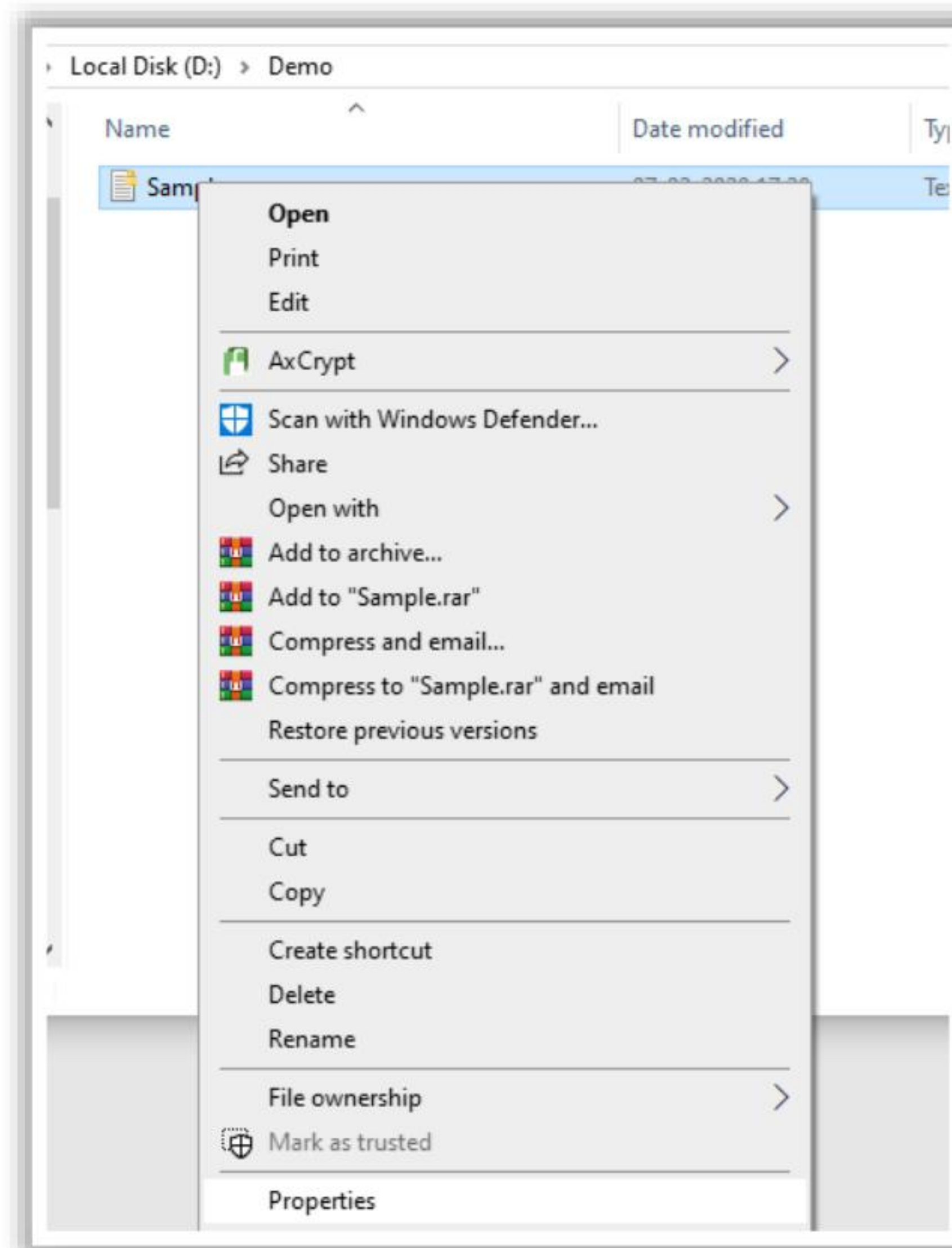


Figure 15.20: Screenshot of Selecting Properties

- Click **Advanced**

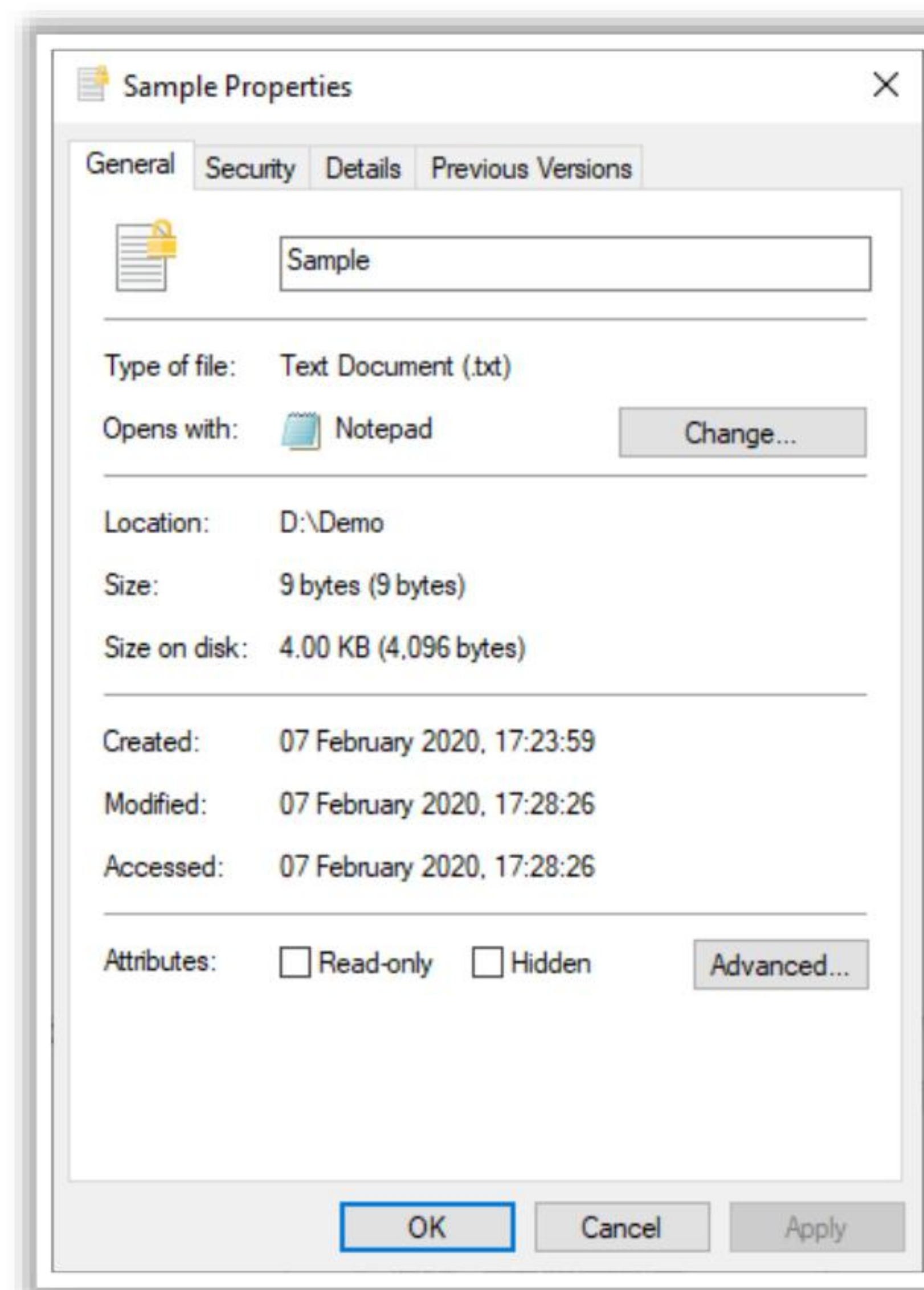


Figure 15.21: Choosing Advanced Option

- Check the box **Encrypt content to secure data** and click **OK**

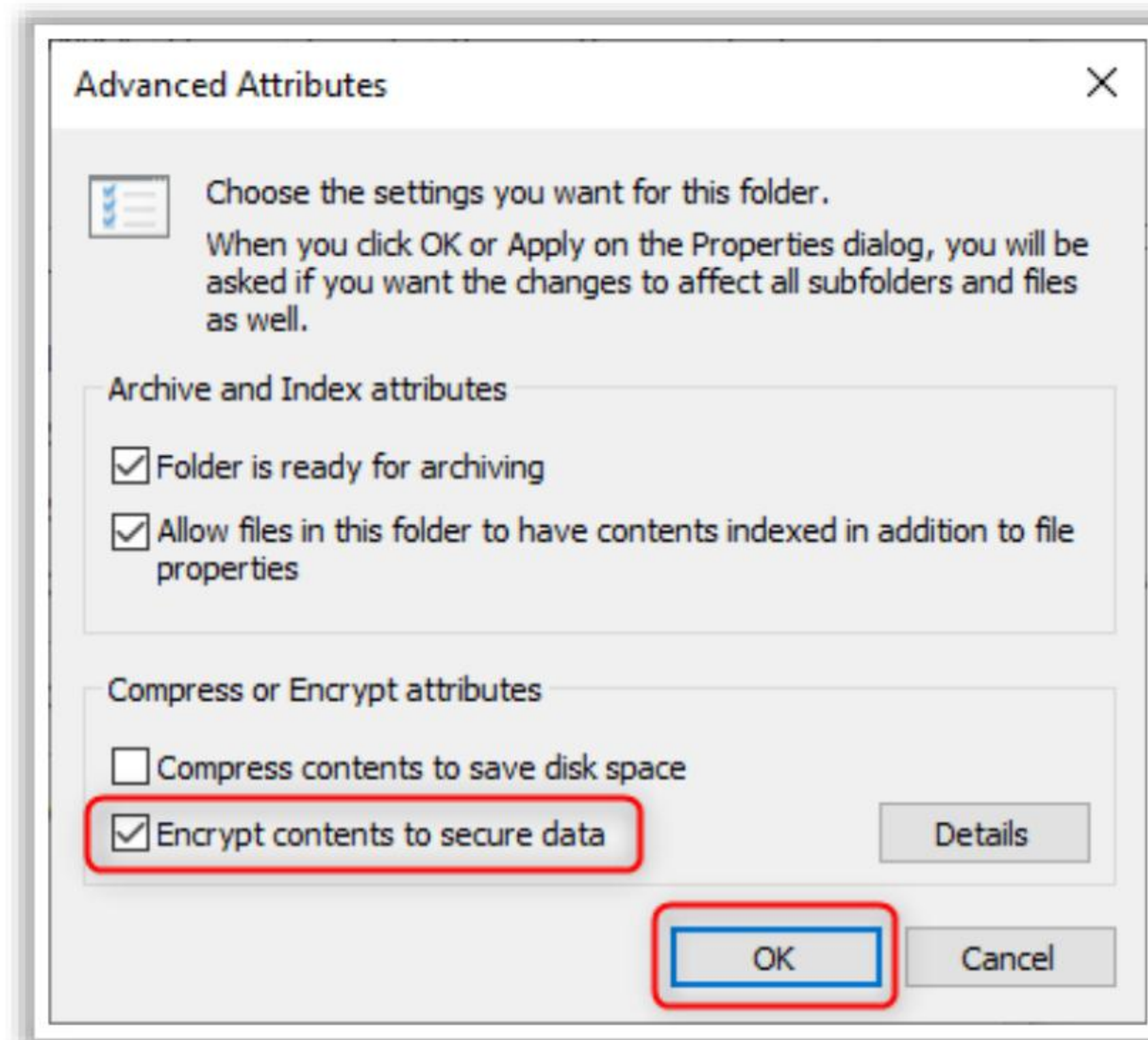


Figure 15.22: Selecting Encrypt Content to Secure Data

- Click **Apply**. A box will appear with the option to encrypt the file only or encrypt the file and its parent folder. Select as per requirements, and click **OK**

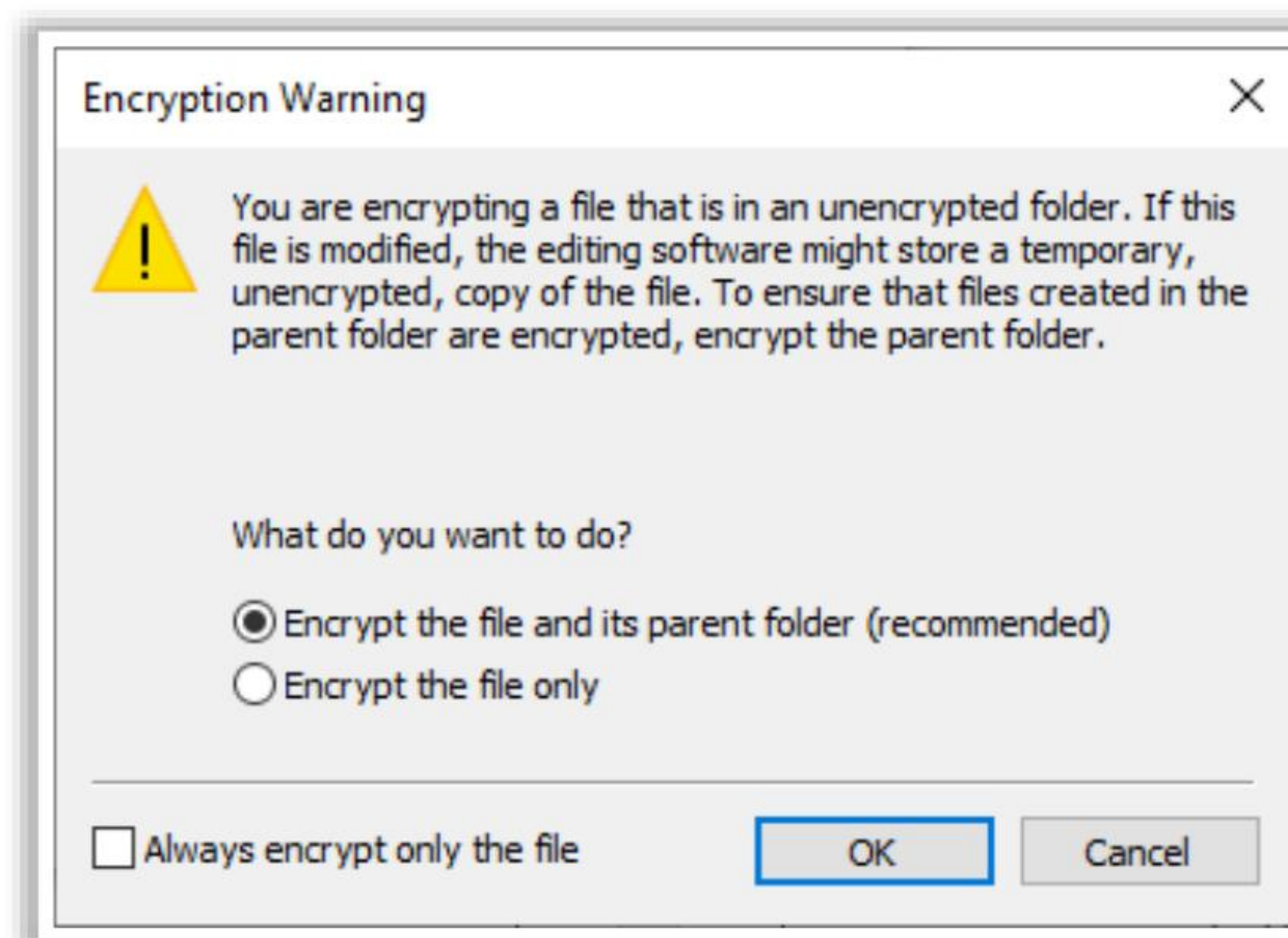


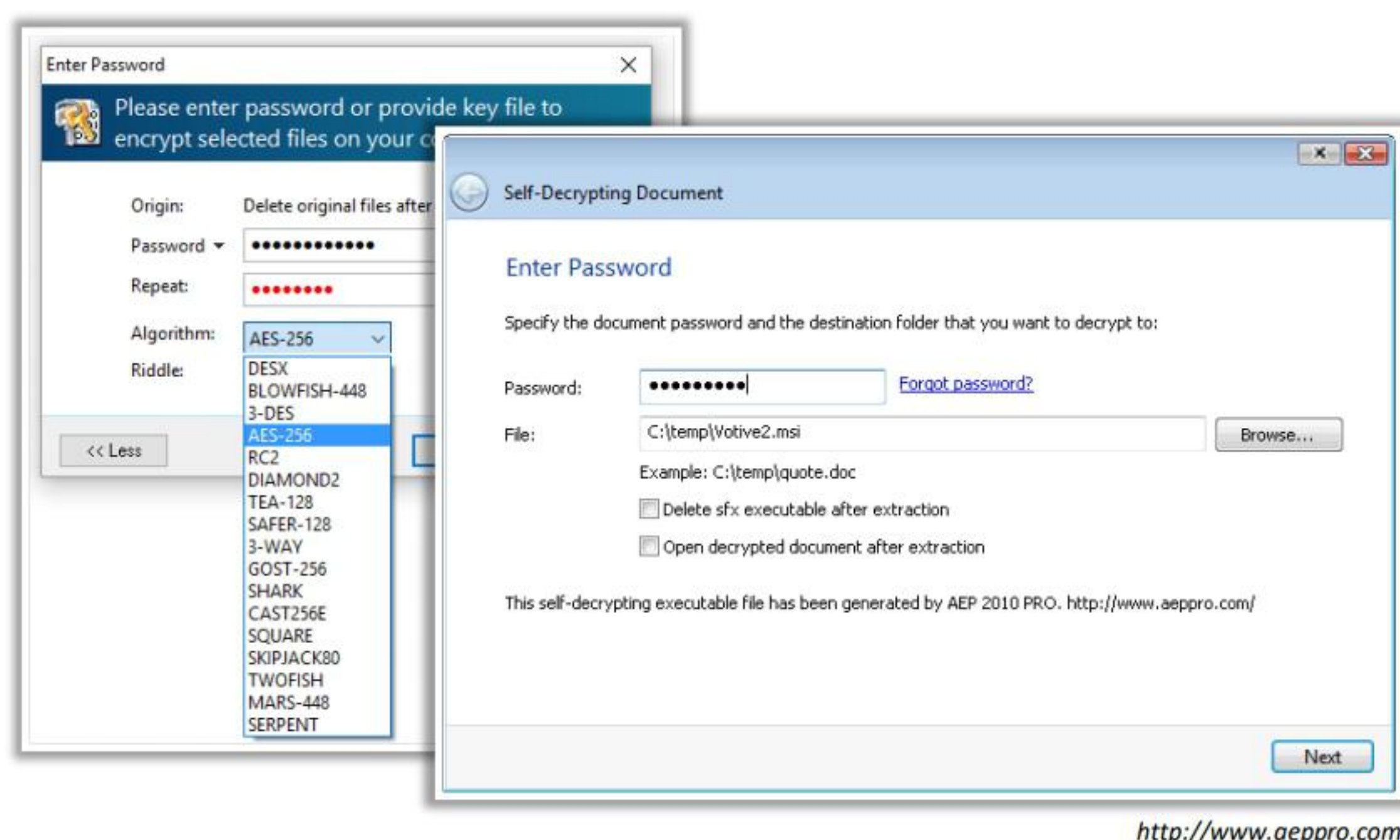
Figure 15.23: Encryption Warning

File Encryption Tools



Advanced Encryption Package

is a file encryption software for Windows 10, 8, and 7. It uses strong and proven algorithms to **protect sensitive documents**



AxCrypt
<https://www.axcrypt.net>



idoo File Encryption
<https://www.idooencryption.com>



Cryptomator
<https://cryptomator.org>



Encrypto
<https://macpaw.com>



AES Crypt
<https://www.aescrypt.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

File Encryption Tools

Advanced Encryption Package

Source: <http://www.aepro.com>

Advanced Encryption Package is a file encryption software for Windows 10, 8, and 7. It uses strong and proven algorithms to protect sensitive documents. It supports both file and text encryption and uses both symmetric and asymmetric algorithms.

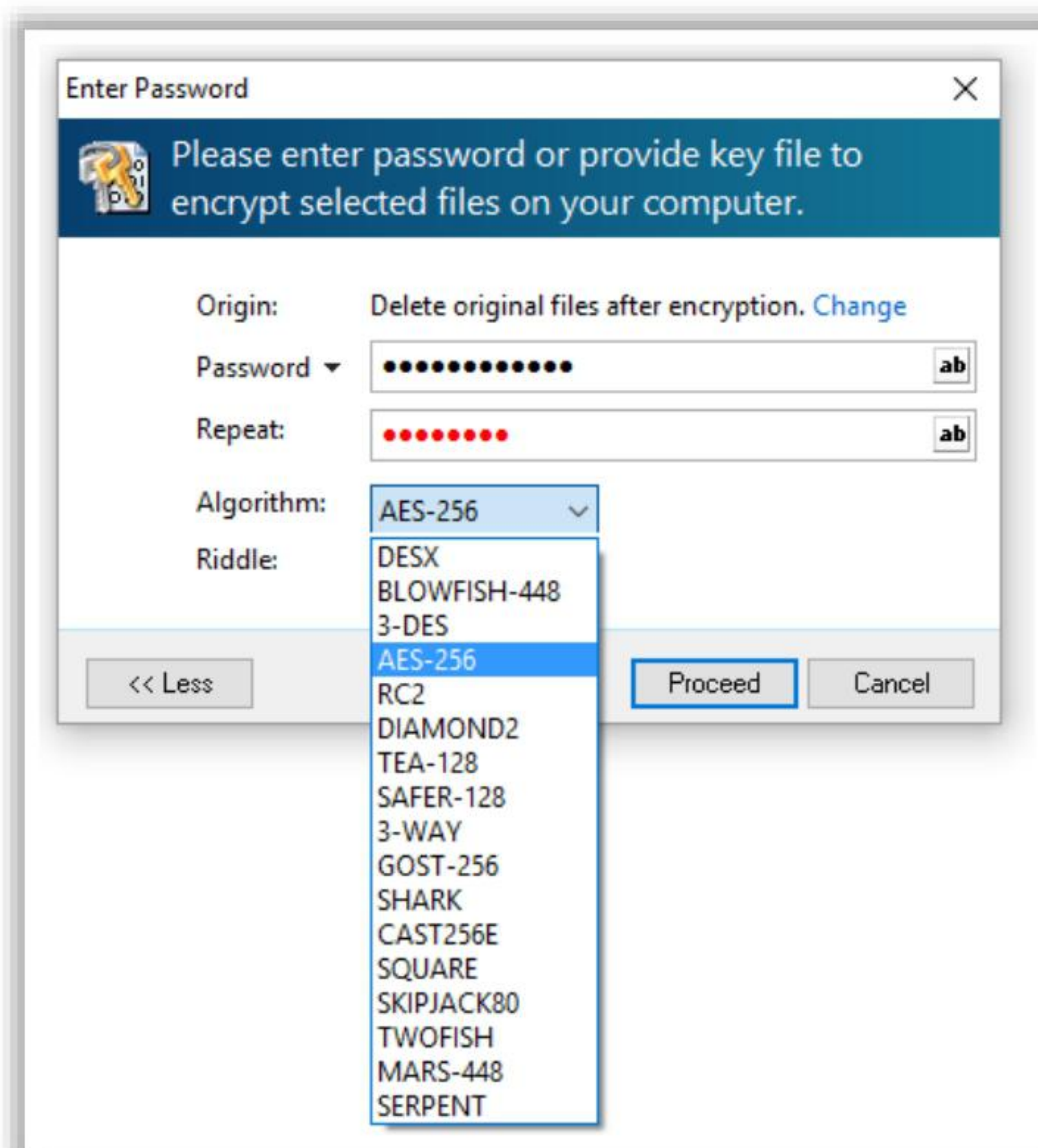


Figure 15.24: Screenshot of Advanced Encryption Package

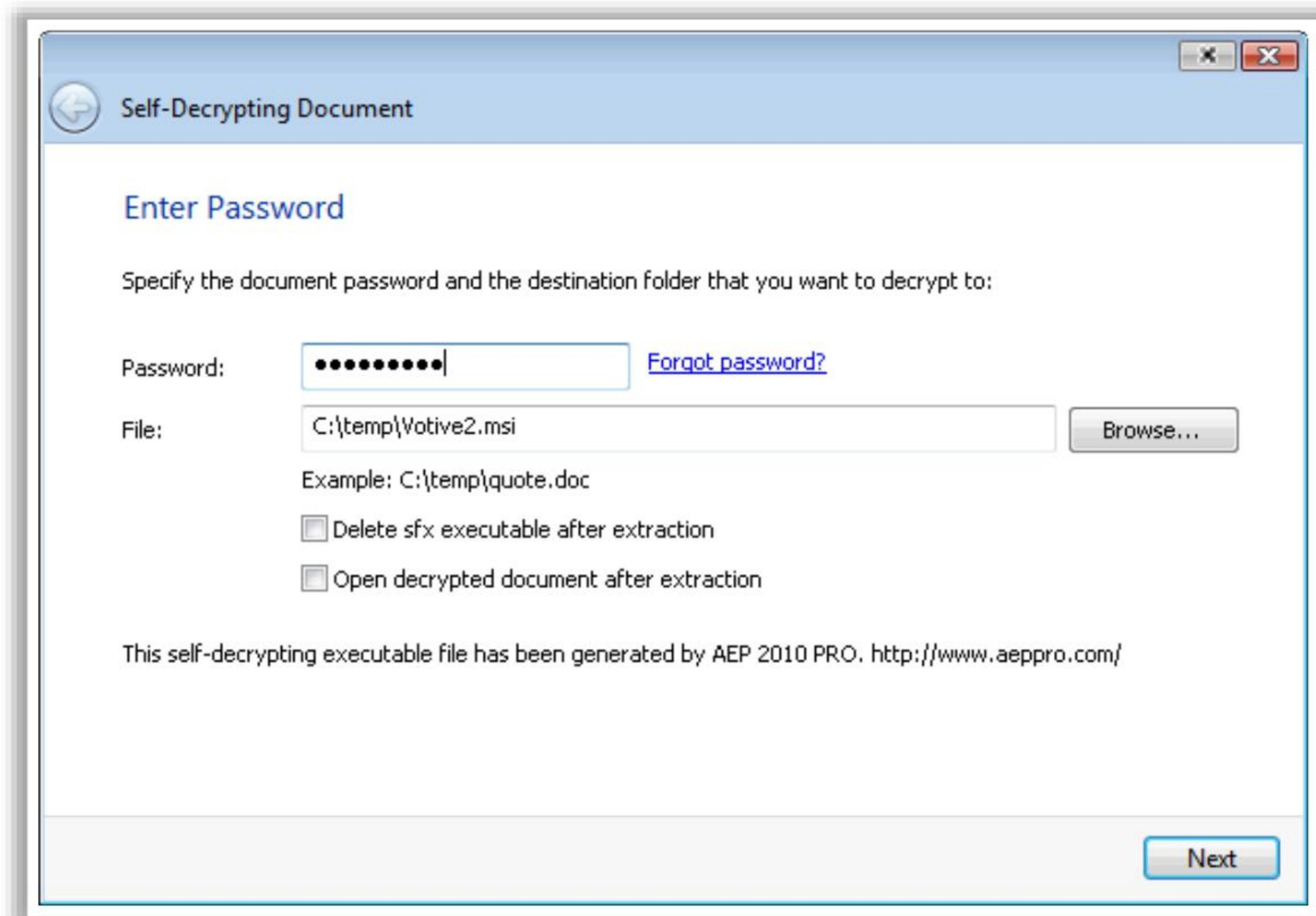


Figure 15.25: Screenshot of Advanced Encryption Package

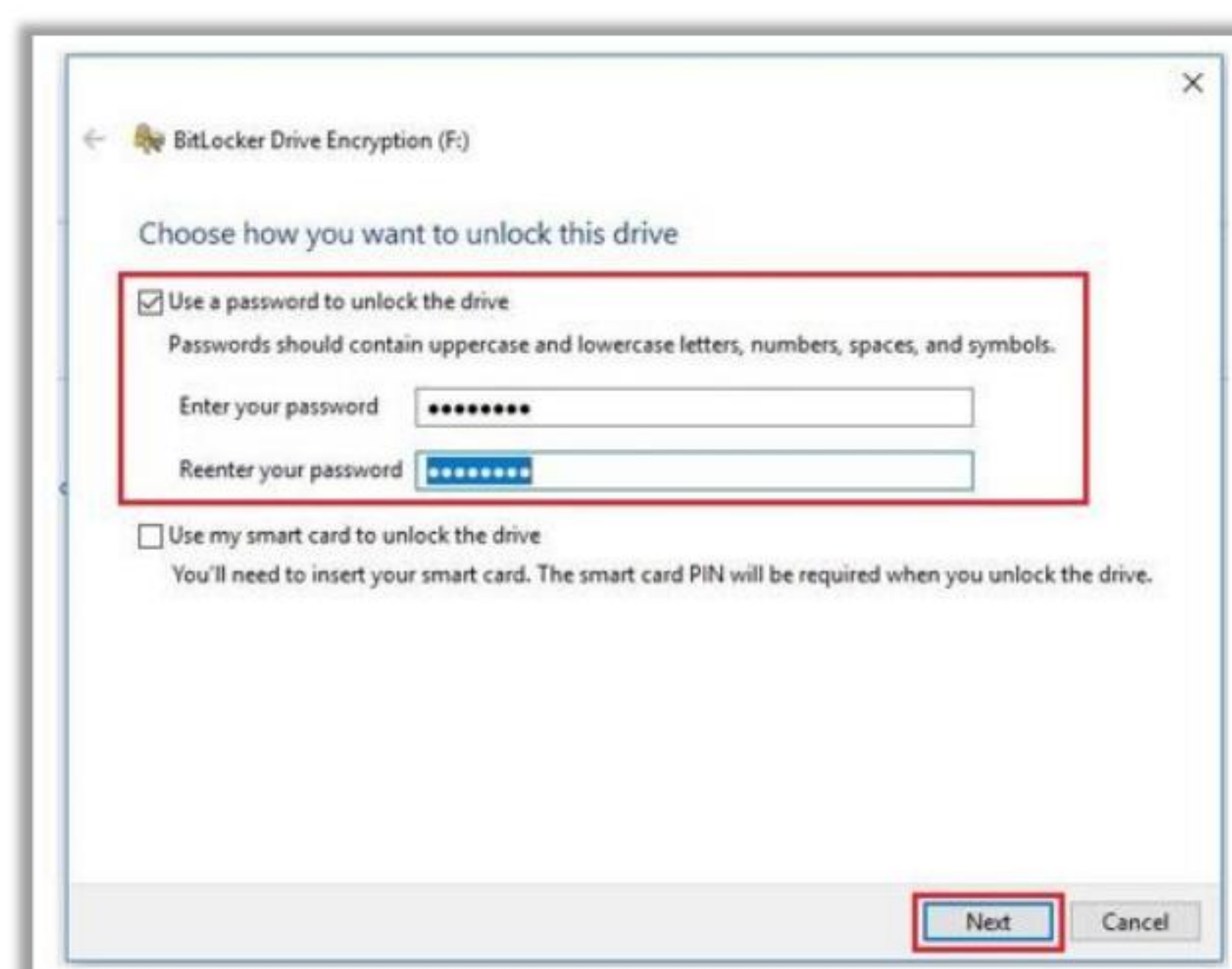
Some additional file encryption tools are as follows:

- AxCrypt (<https://www.axcrypt.net>)
- idoo File Encryption (<https://www.idooencryption.com>)
- Cryptomator (<https://cryptomator.org>)
- Encrypto (<https://macpaw.com>)
- AES Crypt (<https://www.aescrypt.com>)

Removable Media Encryption: Implementing Removable Media Encryption in Windows

 Plug the removable media device into a USB port on your computer

 Go to **Start** → **Control Panel** → **System and Security** → **BitLocker Drive Encryption** (Manage BitLocker)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Removable Media Encryption: Implementing Removable Media Encryption in Windows

Removable media such as USB flash drives, iPods, smartphones, tablets, digital cameras, portable hard disks, etc. are prevalent in a workplace and pose a real threat to an organization. With these devices, the attackers can easily introduce a malicious code in a network or carry sensitive data out of an organization. Hence, encryption is the best way to protect sensitive data from being taken out of an organization.

Encryption can be applied to removable media to prevent it from unauthorized access in case of loss or theft. This will add an extra layer of security to confidential information. Various encryption solutions are available in the market with different features. Some encryption solutions encrypt the data stored on a local drive, but not on USB devices, whereas some encryption solutions automatically encrypt the data stored on removable media. While selecting a removable media encryption solution, it is important to verify how it is configured to restrict access to devices using an authorized list, personal devices, an authorized file copy, and encryption keys.

Operating systems such as Windows, Linux, and Mac use a couple of methods to encrypt removable media such as USB drives. They use either built-in features or third-party encryption solutions to encrypt removable media.

Implementing Removable Media Encryption in Windows: BitLocker

To Enable Removable Media Encryption in Windows 10

- Plug the removable media device into a USB port on the computer.
- Go to **Start** → **Control Panel** → **BitLocker Drive Encryption**.

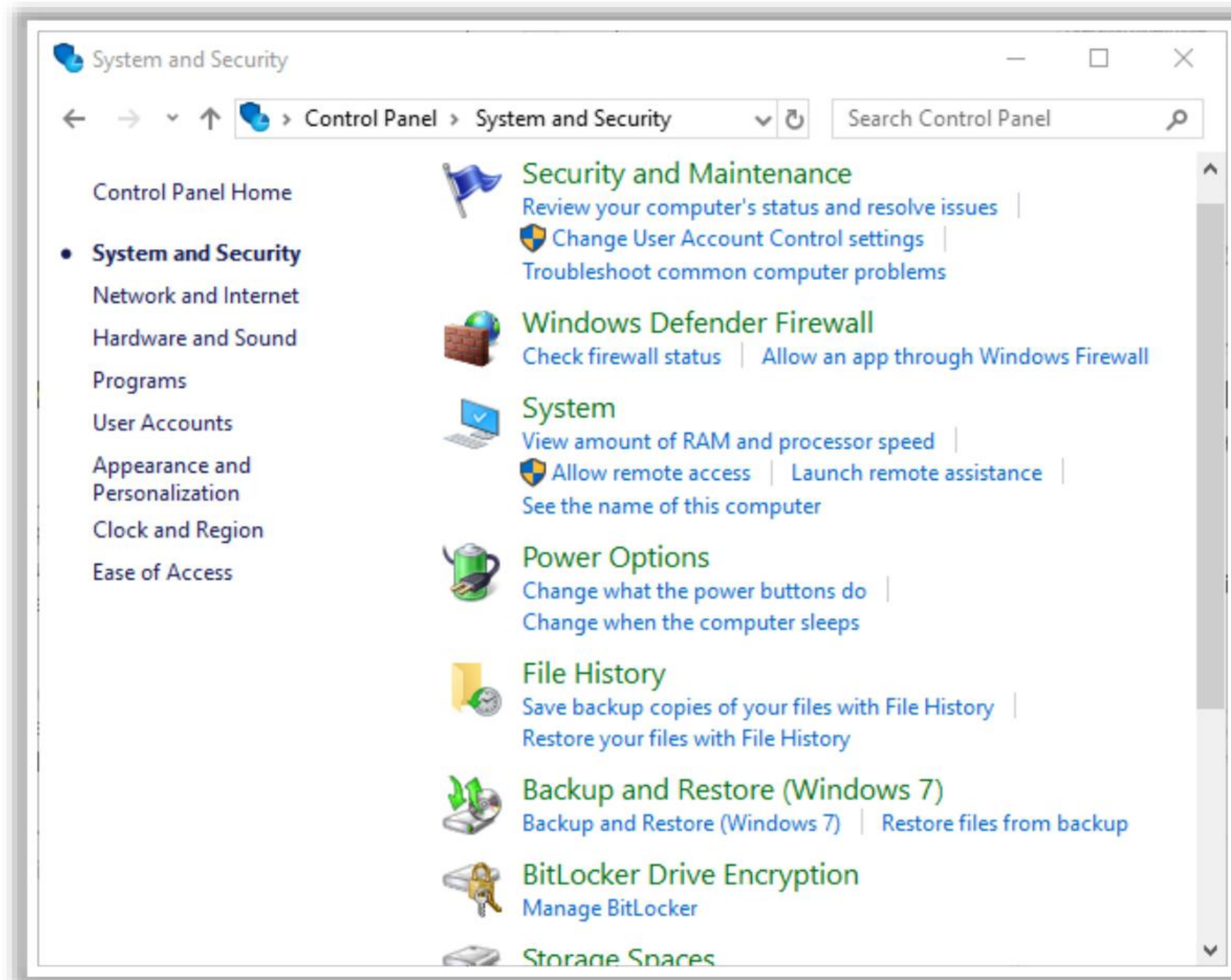


Figure 15.26: Choosing BitLocker Drive Encryption Option

- Select the removable media device to encrypt and click **Turn on BitLocker**.



Figure 15.27: Turning on BitLocker

- BitLocker initialization process will start. Wait for some time to finish the initialization process.

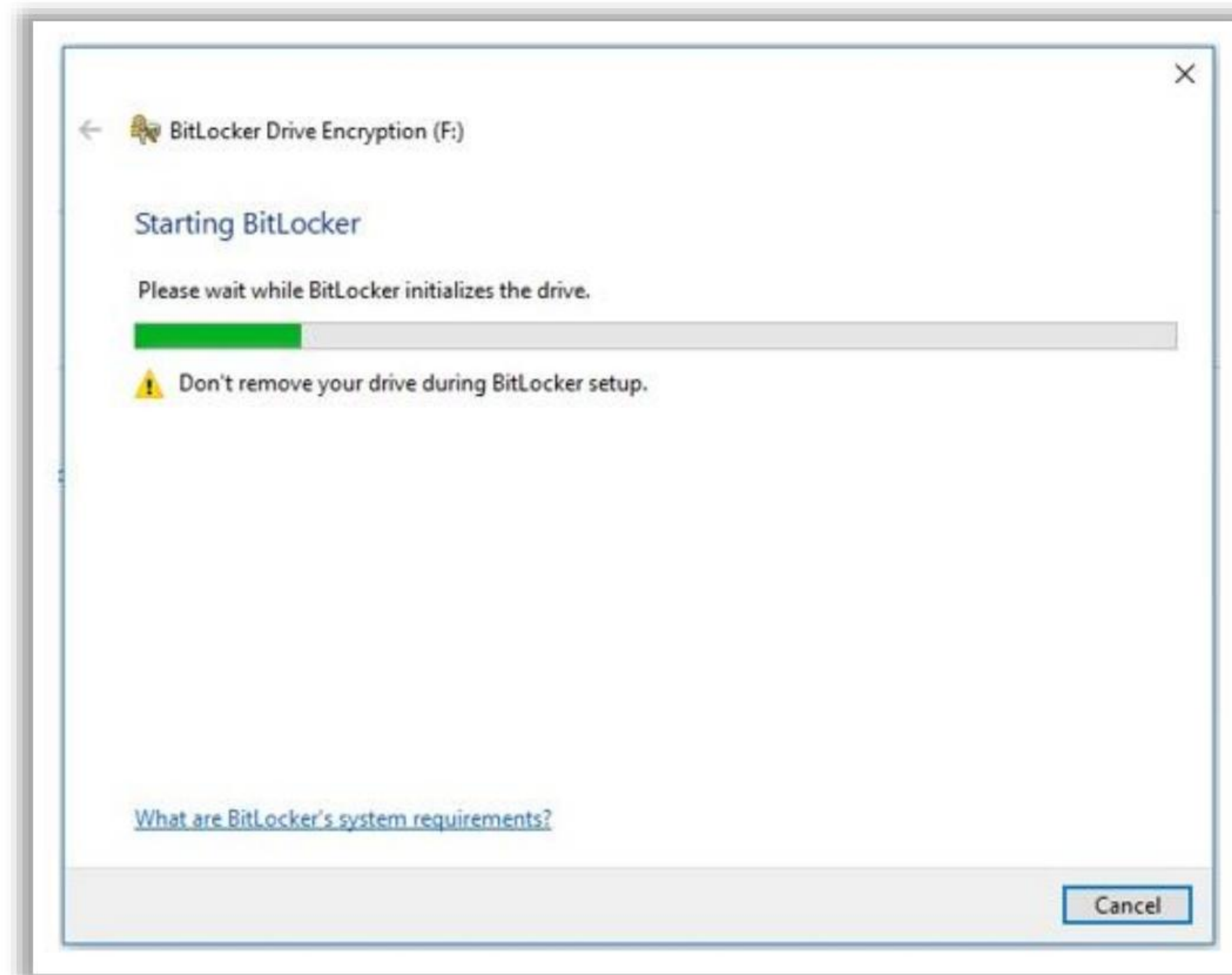


Figure 15.28: BitLocker Initiating the Drive

- In the **Choose how you want to unlock this drive** window, tick the **Use a password to unlock the drive** checkbox and enter a strong password, then click **Next**.

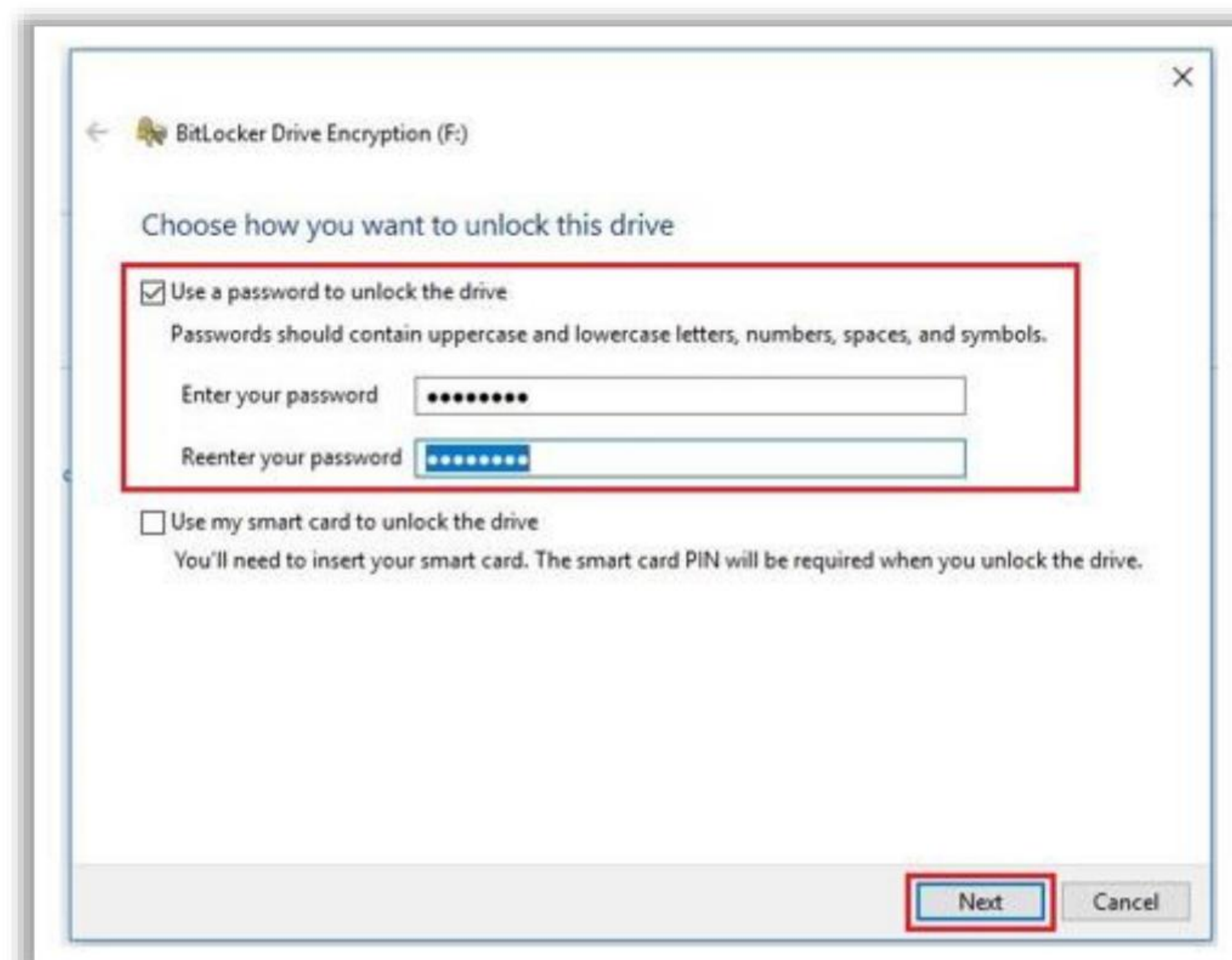


Figure 15.29: Unlocking the Drive

- In **How do you want to back up your recovery key?** window, either choose **Save to a file** or **Print the recovery key**, then click **Next**.

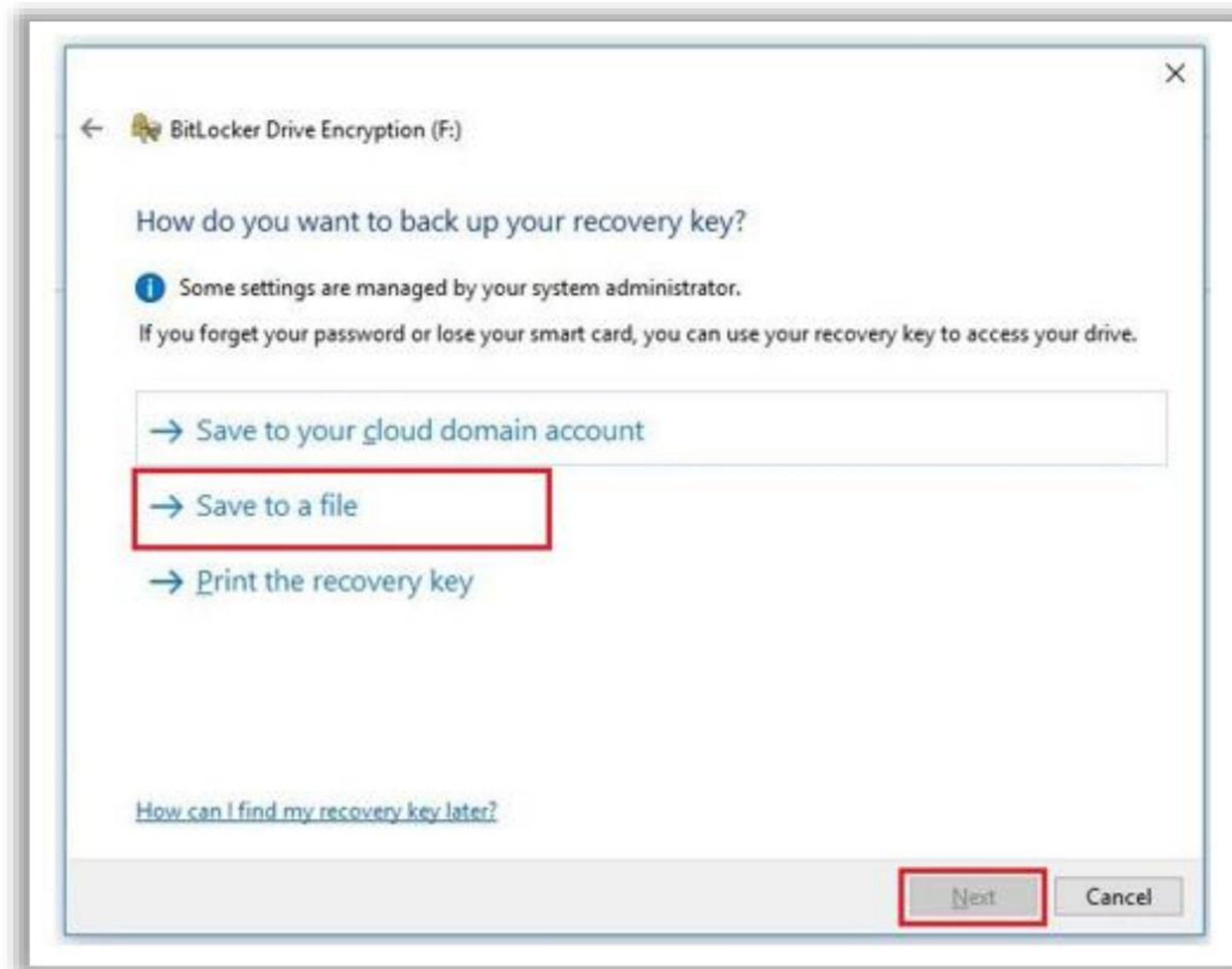


Figure 15.30: Saving to a File

- In the **Choose how much of your drive to encrypt** window, Select **Encrypt used disk space only** if the drive is new or select **Encrypt entire drive** if the drive contains data, then click **Next**.

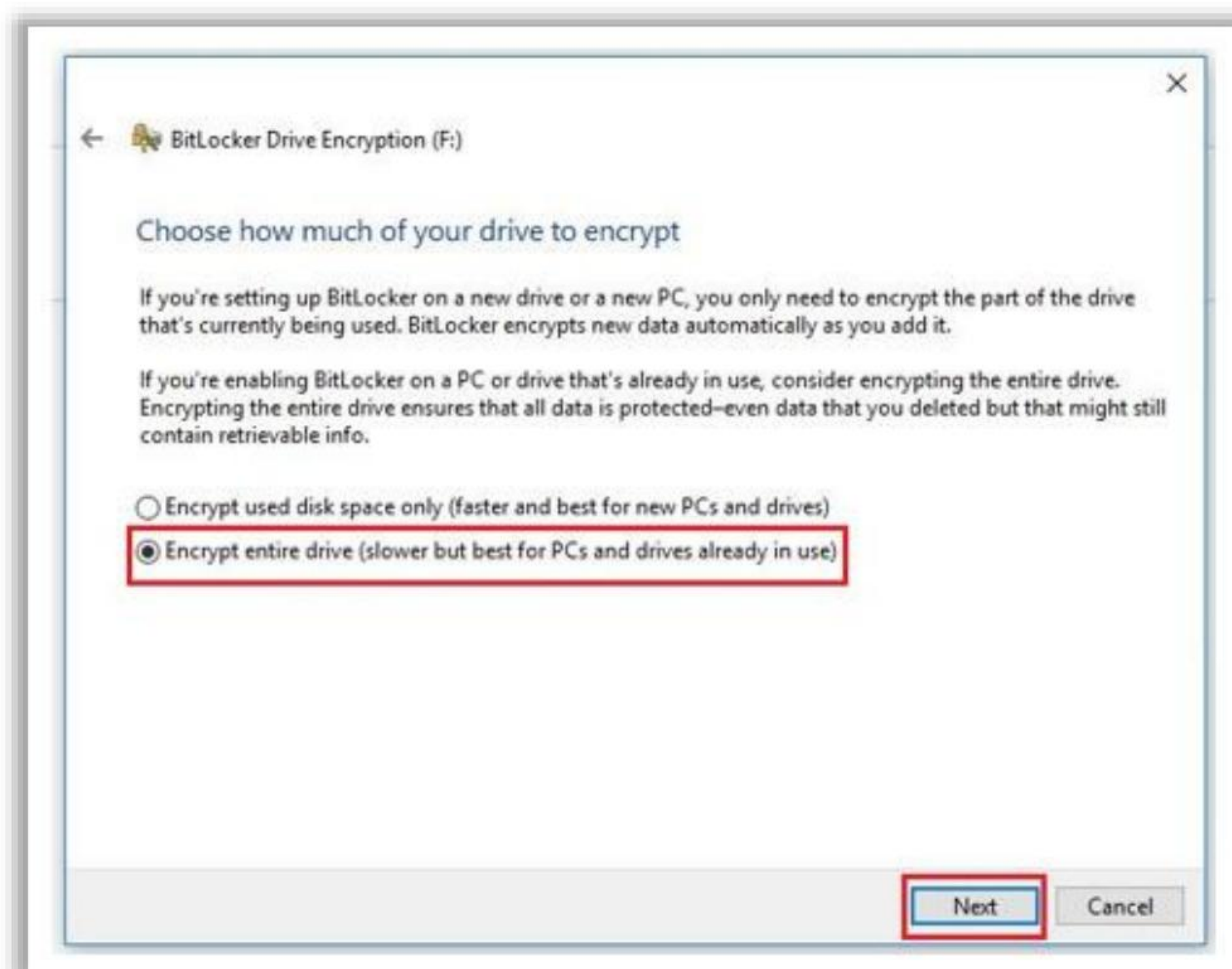


Figure 15.31: Choosing Encrypt Entire Drive Option

- In the **Choose which encryption mode to use** window, select **Compatible mode** if the user wants to use the encrypted drive on older versions of Windows, or select **New encryption mode** if the user wants to use the encrypted drive on Windows 10 only. Then click **Next**.

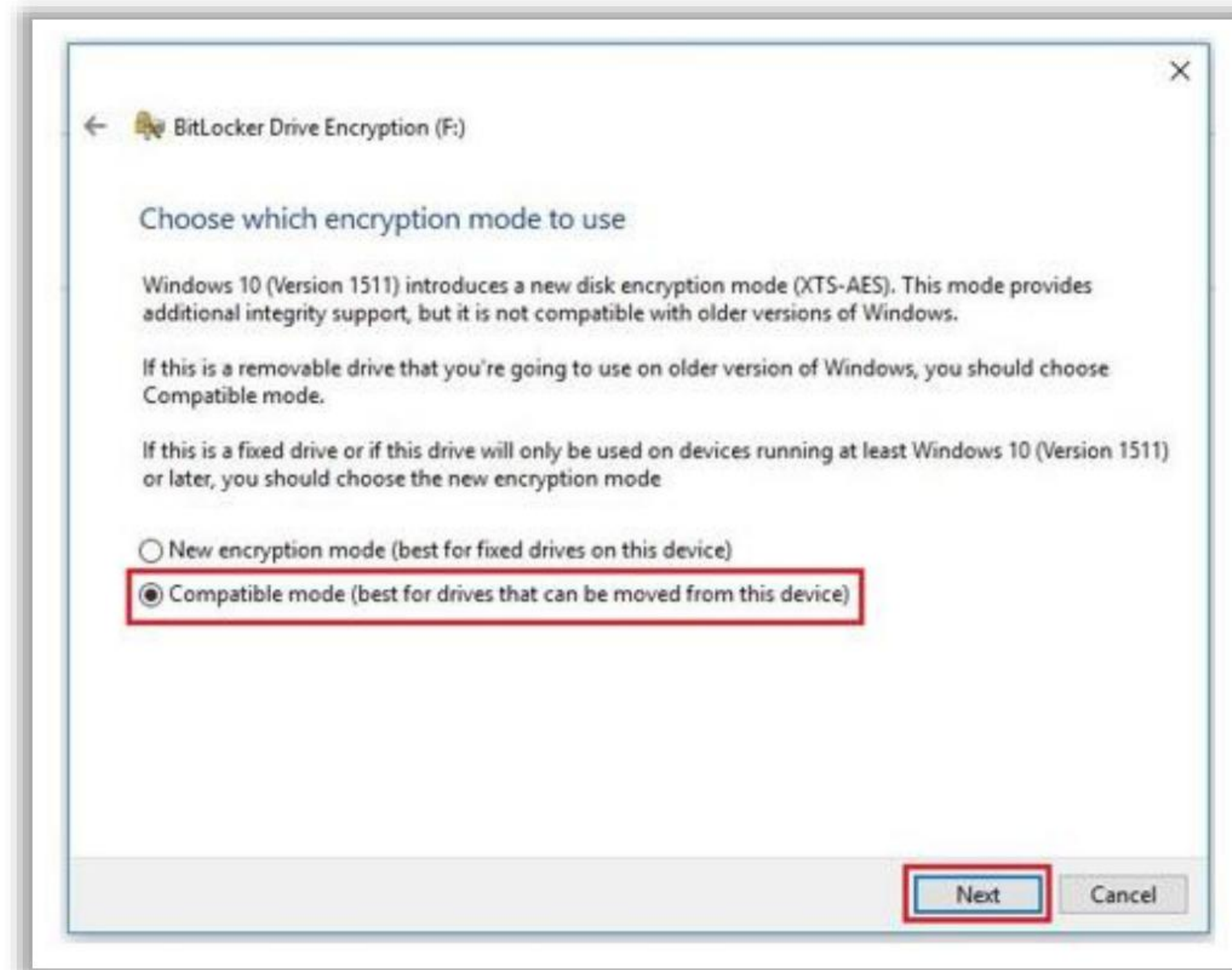


Figure 15.32: Choosing Compatible Mode

- Click **Start encrypting**.

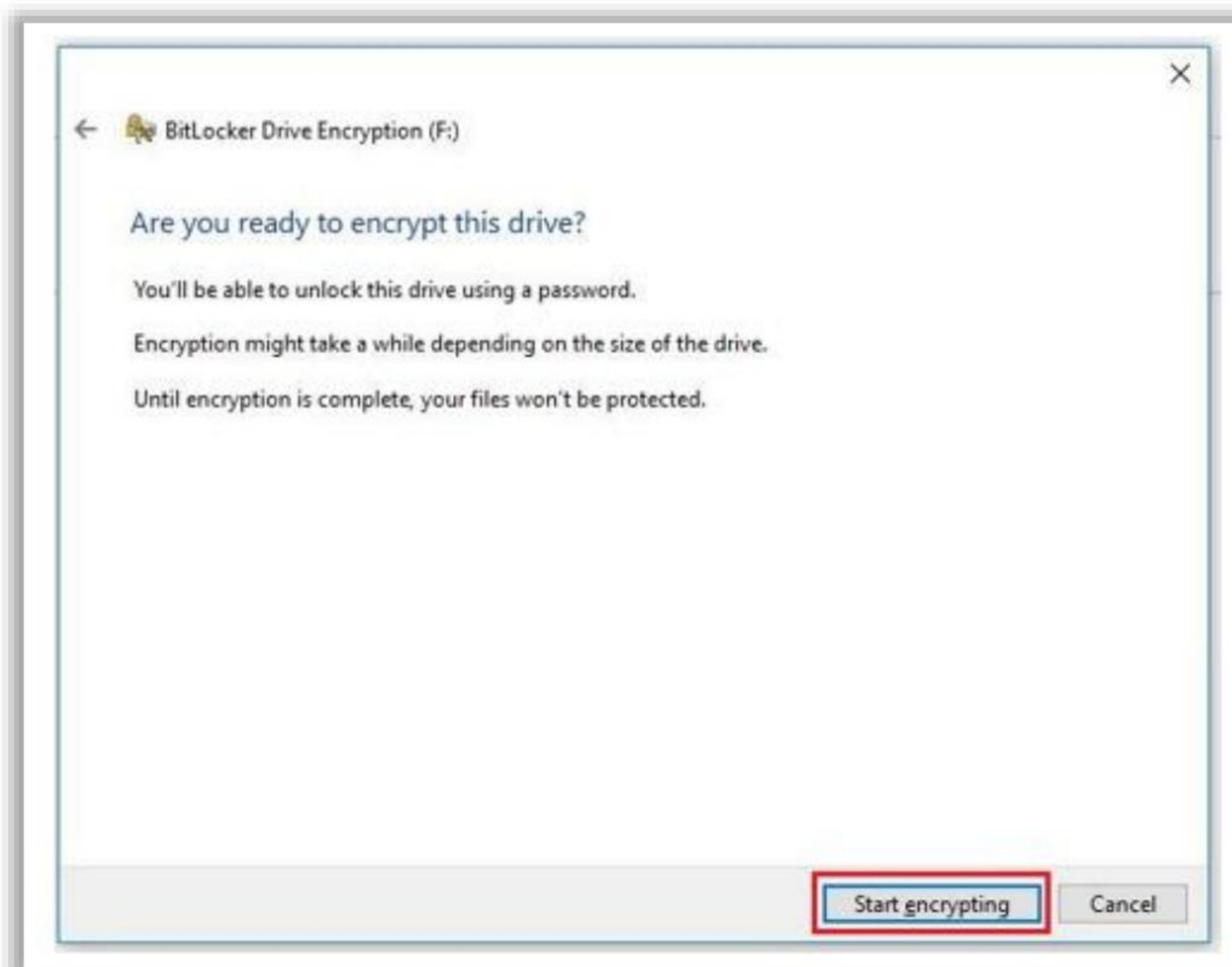


Figure 15.33: Starting the Encryption

- Click **Close** when the encryption process is completed.



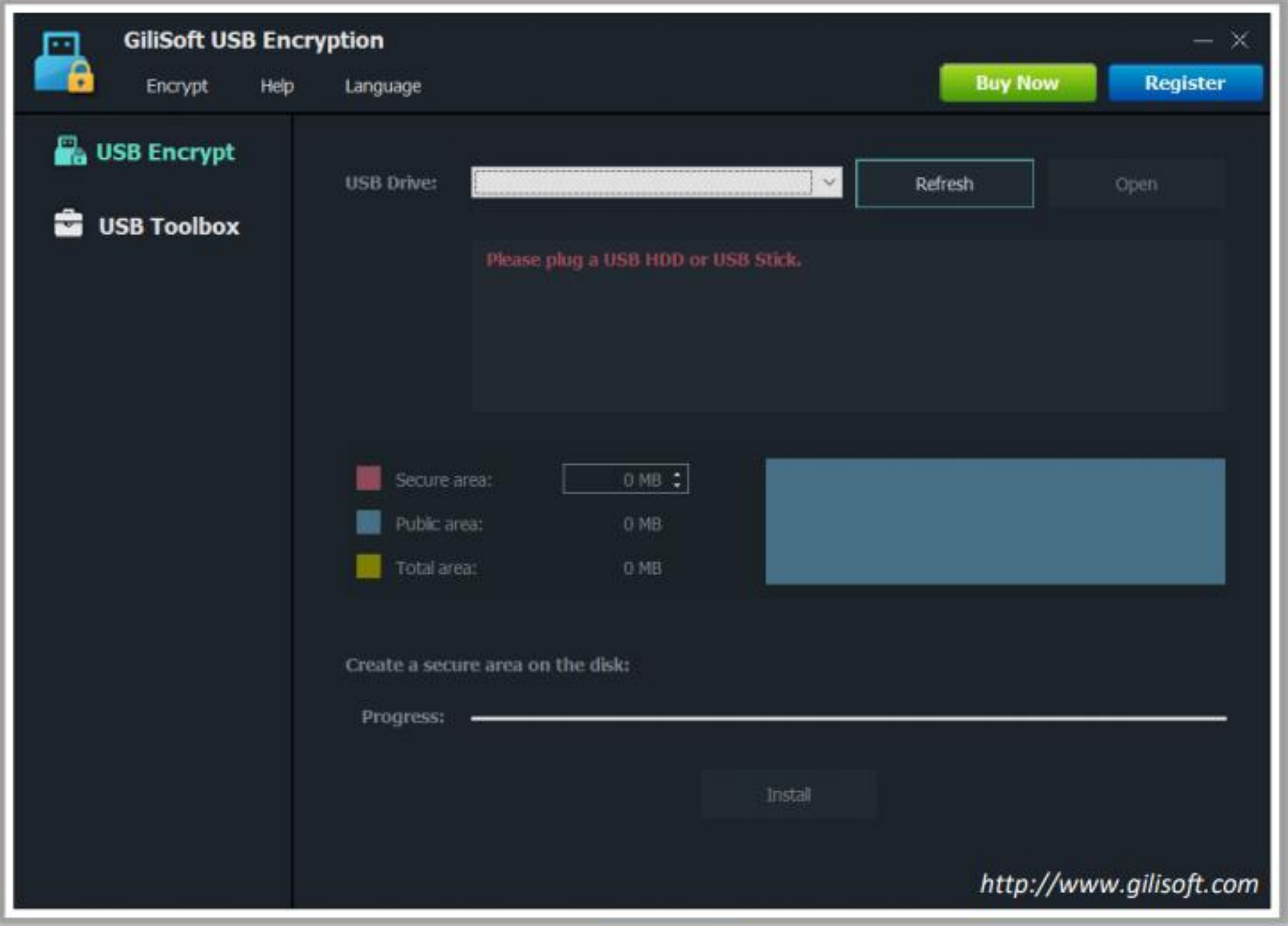
Figure 15.34: Completion of Encryption

Note: Whenever the user tries to connect the encrypted drive, they have to provide the password to unlock it.

Removable Media Encryption Tools



A solution for USB security that supports **encrypting portable storage device** (external drive) and can divide external drive into two parts after encryption: the secure area and public area



The screenshot shows the GiliSoft USB Encryption application window. It has a dark theme with a sidebar on the left containing 'USB Encrypt' and 'USB Toolbox'. The main area shows a 'USB Drive' dropdown menu, 'Refresh' and 'Open' buttons, and a message 'Please plug a USB HDD or USB Stick.' Below this, there are three rows: 'Secure area: 0 MB', 'Public area: 0 MB', and 'Total area: 0 MB'. At the bottom, there is a 'Create a secure area on the disk:' section with a 'Progress:' bar and an 'Install' button. The URL 'http://www.gilisoft.com' is visible in the bottom right corner of the window.

- **idoo USB Encryption**
<https://www.idooencryption.com>
- **Kakasoft USB Security**
<https://www.kakasoft.com>
- **Rohos Mini Drive**
<https://www.rohos.com>
- **McAfee File & Removable Media Protection**
<https://www.mcafee.com>
- **MFG's Removable Media Encryption**
<https://www.managedencryption.co.uk>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Removable Media Encryption Tools

- **GiliSoft USB Encryption**

Source: <http://www.gilisoft.com>

GiliSoft USB Encryption is a solution for USB security that supports the encryption of portable storage devices (external drives) and can divide an external drive into two parts after encryption: a secure area and a public area. It converts a regular USB flash drive into a secured one in less than a minute, and data on the protected area (secure area) is encrypted by a 256-bit AES on-the-fly encryption.

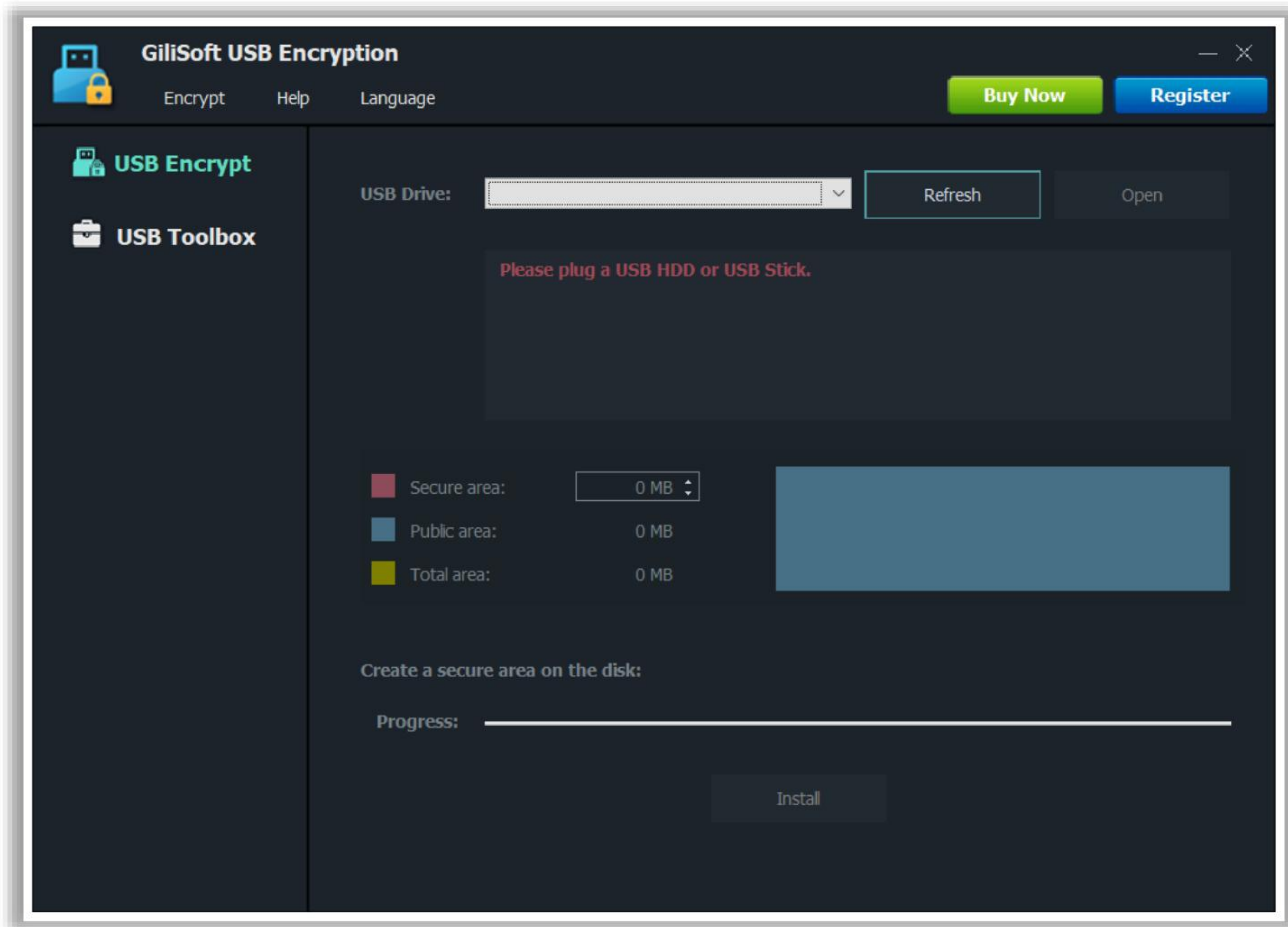
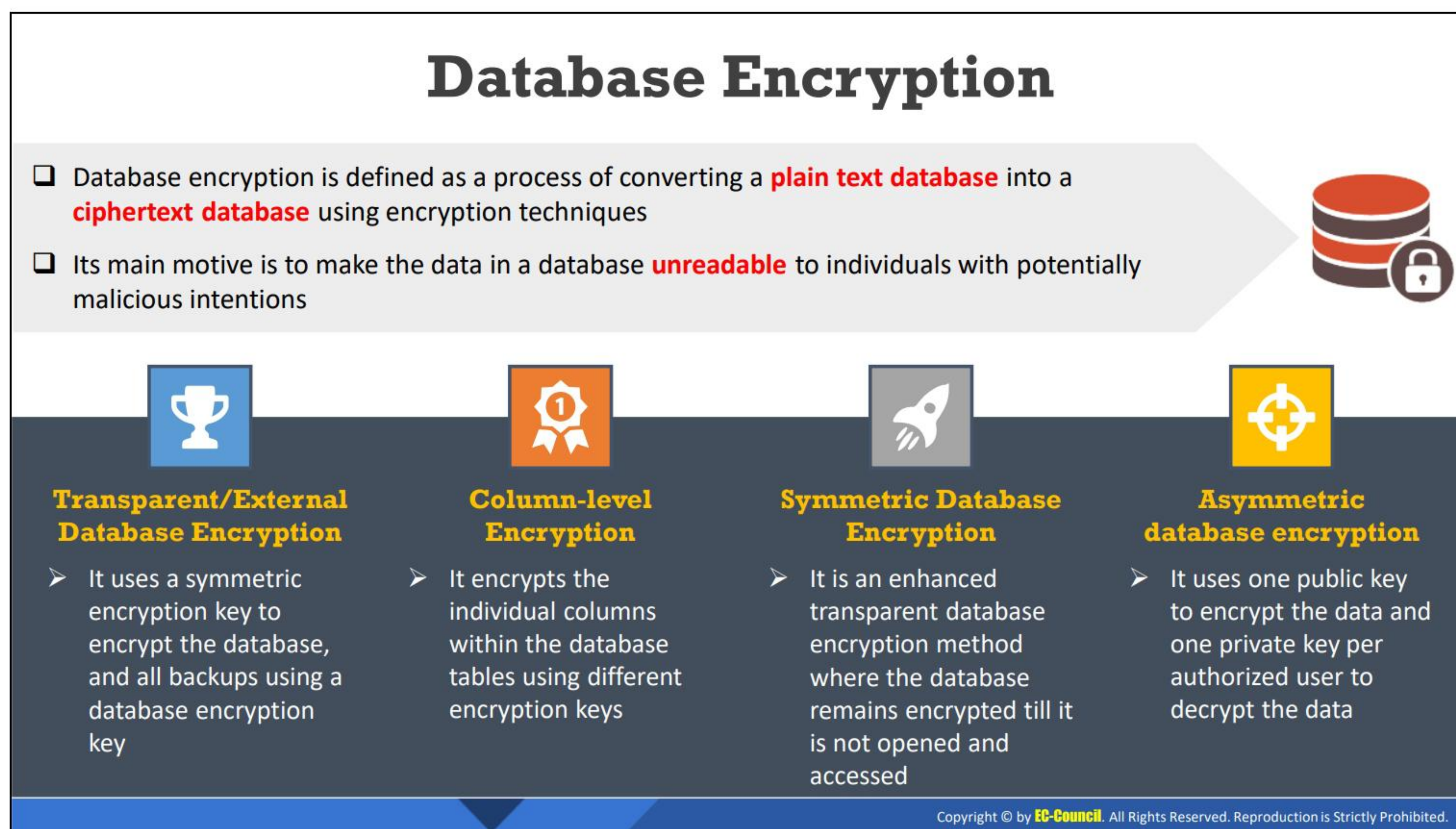


Figure 15.35: Screenshot of GiliSoft USB Encryption

Some additional removable media encryption tools are as follows:

- idoo USB Encryption (<https://www.idooencryption.com>)
- Kakasoft USB Security (<https://www.kakasoft.com>)
- Rohos Mini Drive (<https://www.rohos.com>)
- McAfee File & Removable Media Protection (<https://www.mcafee.com>)
- MFG's Removable Media Encryption (<https://www.managedencryption.co.uk>)



Database Encryption

Database encryption is defined as a process of converting a plain text database into a ciphertext database using encryption techniques. Its main motive is to make the data in a database unreadable to individuals with potentially malicious intentions. It also minimizes the intention of hackers to hack the database as encrypted data cannot be easily deciphered. Several techniques and methods are used by security professionals to implement encryption in the database, such as:

- **Transparent/External database encryption:** This type of database encryption methods encrypts the entire database, that is, it encrypts the “data at rest.” Transparent or external database encryption uses a symmetric encryption key to encrypt the database, and all backups using a database encryption key. A risk with using this method is that the security professional can encrypt only the data that is stored in the database tables; the data that is stored in memory or cache is not encrypted. An individual with a malicious intent may access that data. Access to symmetric encryption key can lead to an access to the database content.
- **Column-level encryption:** This method is a form of partial database encryption. It encrypts the individual columns within the database tables using different encryption keys. This method is more secure, as it needs a separate decryption method for decrypting each encrypted column. However, this method minimizes the database index and search performance. Similarly, partial database encryption can be applied on individual rows, cells, and table spaces of the database table with a separate encryption key.

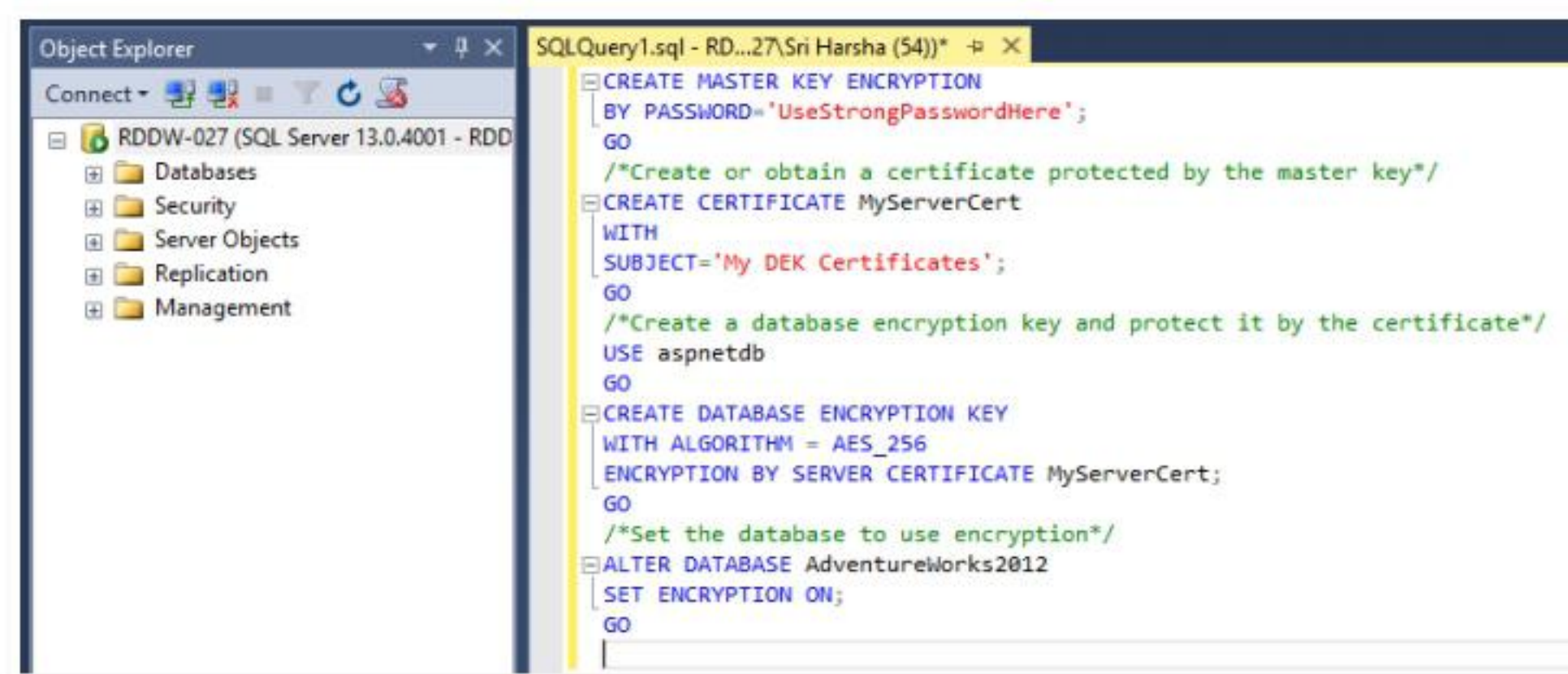
- **Symmetric database encryption:** This method is an enhanced transparent database encryption method where the database remains encrypted till it is not opened and accessed. However, in this method, the user requires a copy of the private key to access the database content. If the security professional uses this method to encrypt the database, then there is a chance that the private key can be leaked or identified by unauthorized users.
- **Asymmetric database encryption:** This method is an improvement over symmetric database encryption, and uses only one private key to encrypt and decrypt data; however, this method uses one public key to encrypt the data and one private key per authorized user to decrypt the data. In case the public key is leaked or accessed by an unauthorized user, they would not be able to read the content of the encrypted file.

Implementation of Transparent Database Encryption in MS SQL Server

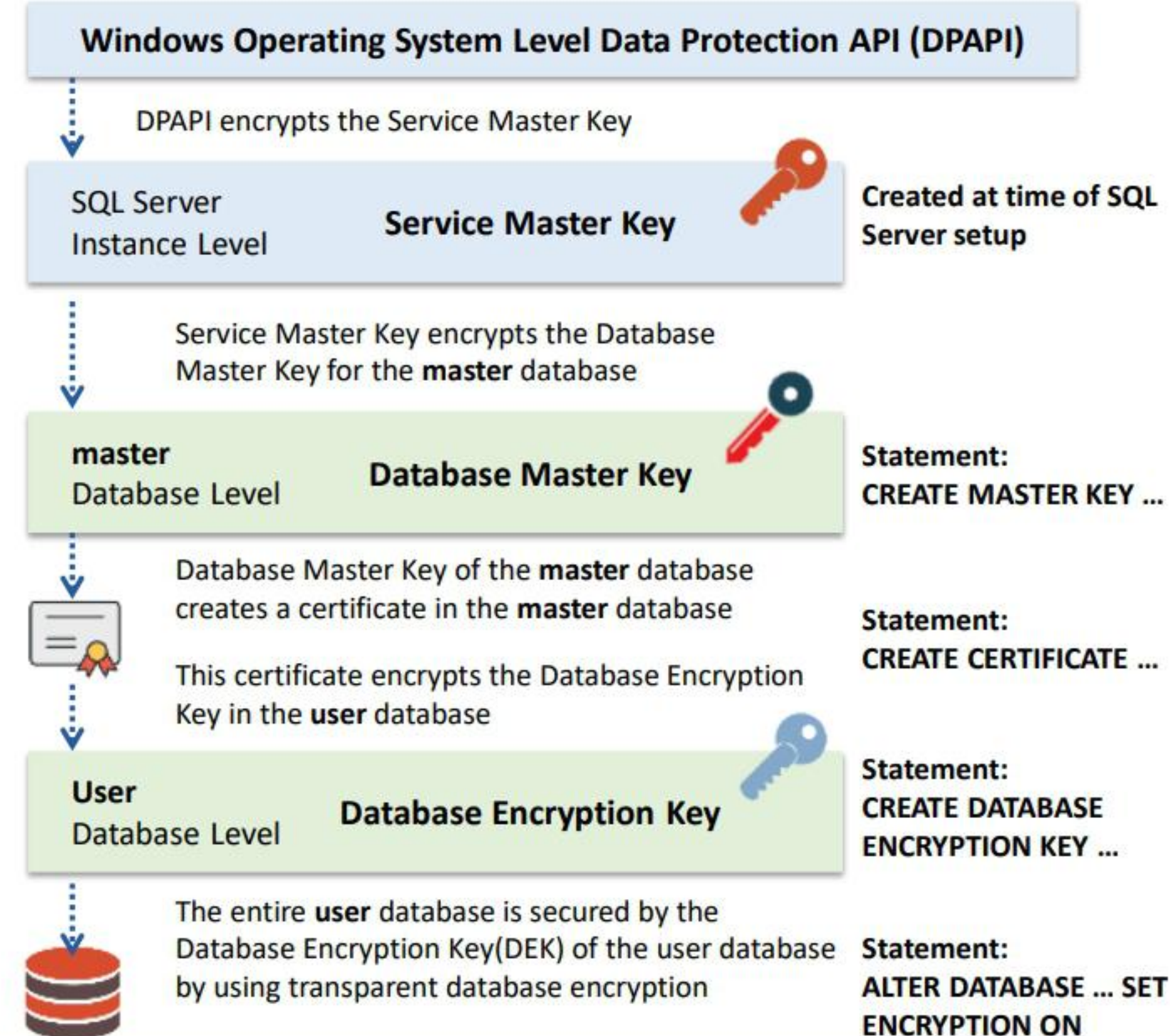
- ❑ Transparent Database Encryption in MS SQL Server (TDE) **encrypts** the physical files of a database

To implement Transparent Database Encryption in SQL Server:

- ✓ Create a master key
- ✓ Create or obtain a certificate protected by the master key
- ✓ Create a database encryption key and protect it using the certificate
- ✓ Set the database to use encryption



Transparent Database Encryption Architecture



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Implementation of Transparent Database Encryption in MS SQL Server

Transparent Database Encryption Architecture

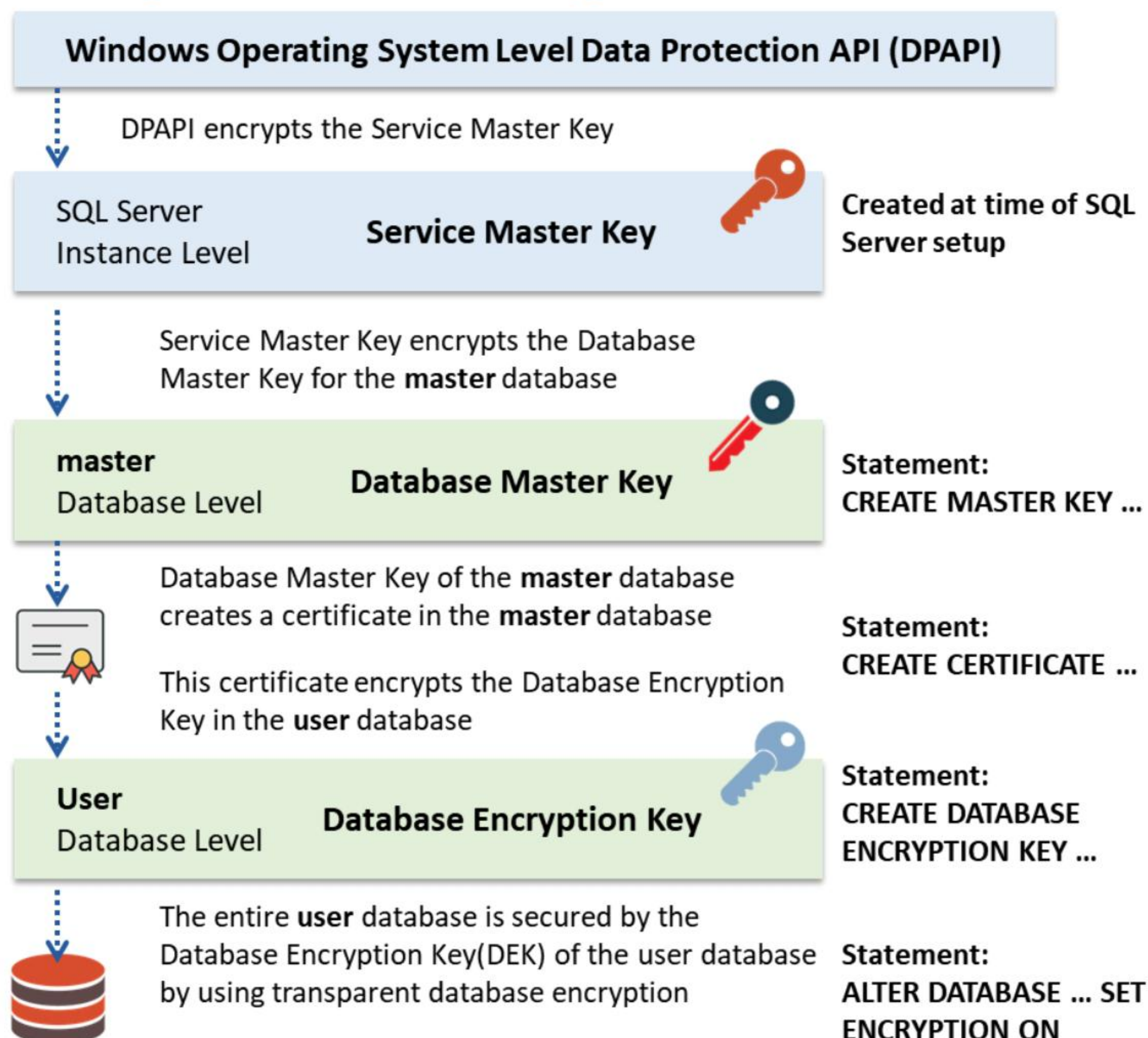


Figure 15.36: Transparent database encryption architecture

Transparent Database Encryption Hierarchy

Transparent database encryption is a built-in feature to protect data at rest. Encrypting the data at rest safeguards it against cybercriminals as an attacker will not be able to decipher the encrypted data.

SQL Server Instance

- A service master key (SMK) is created while setting up an SQL server instance.

Master Database

- Data protection API (DPAPI) encrypts SMK. The DPAPI protects the SMK in the master database.
- SMK encrypts the database master key (DMK). Hence, SMK protects the DMK.
- The DMK creates a certificate. Hence, it protects the certificate's private key.
- The certificate encrypts the database encryption key (DEK). Hence, the certificate protects the DEK in the user database.

User Database

- The entire user database is secured by the DEK using transparent database encryption (TDE). DEK protects the data in the user database.
- TDE executes a page-level encryption; the pages are encrypted before they are written to the disk, and decrypted when the user wants to read them.

To implement Transparent Database Encryption in SQL Server:

- Create a master key
- Create or obtain a certificate protected by the master key
- Create a database encryption key and protect it using the certificate
- Set the database to use encryption

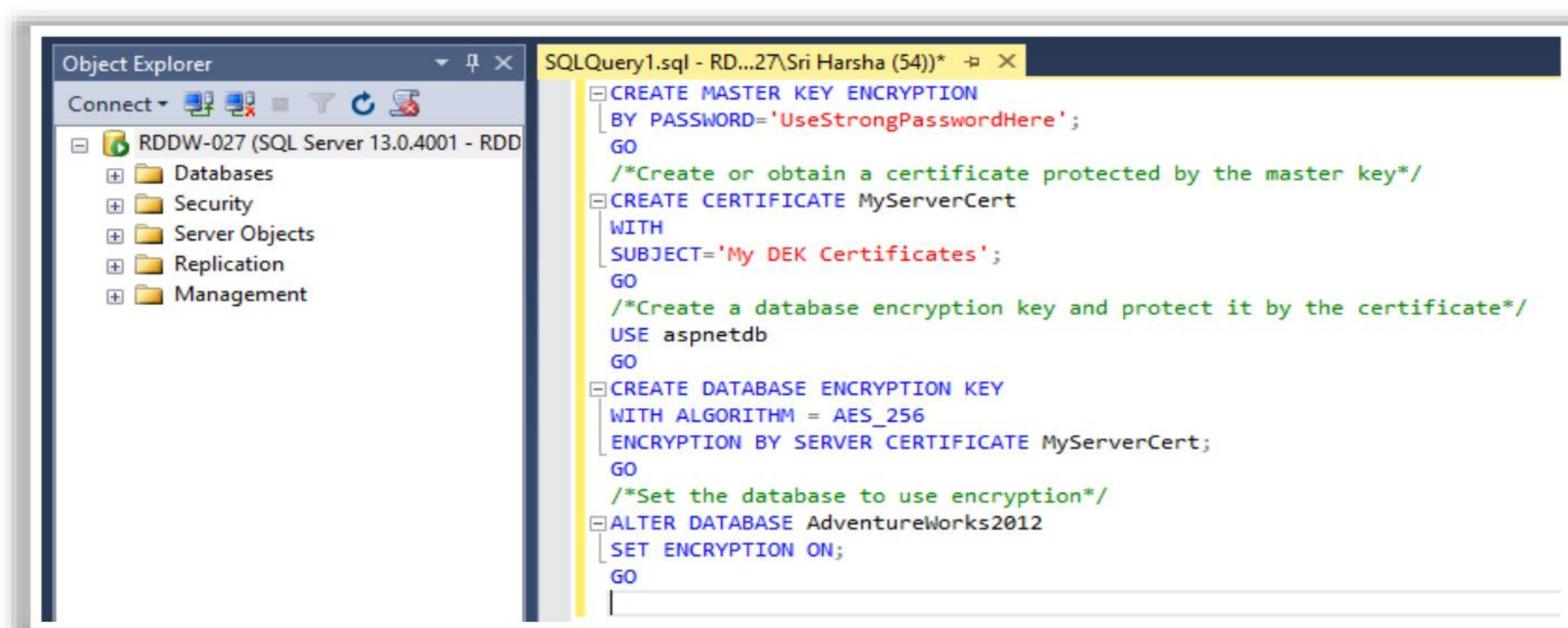


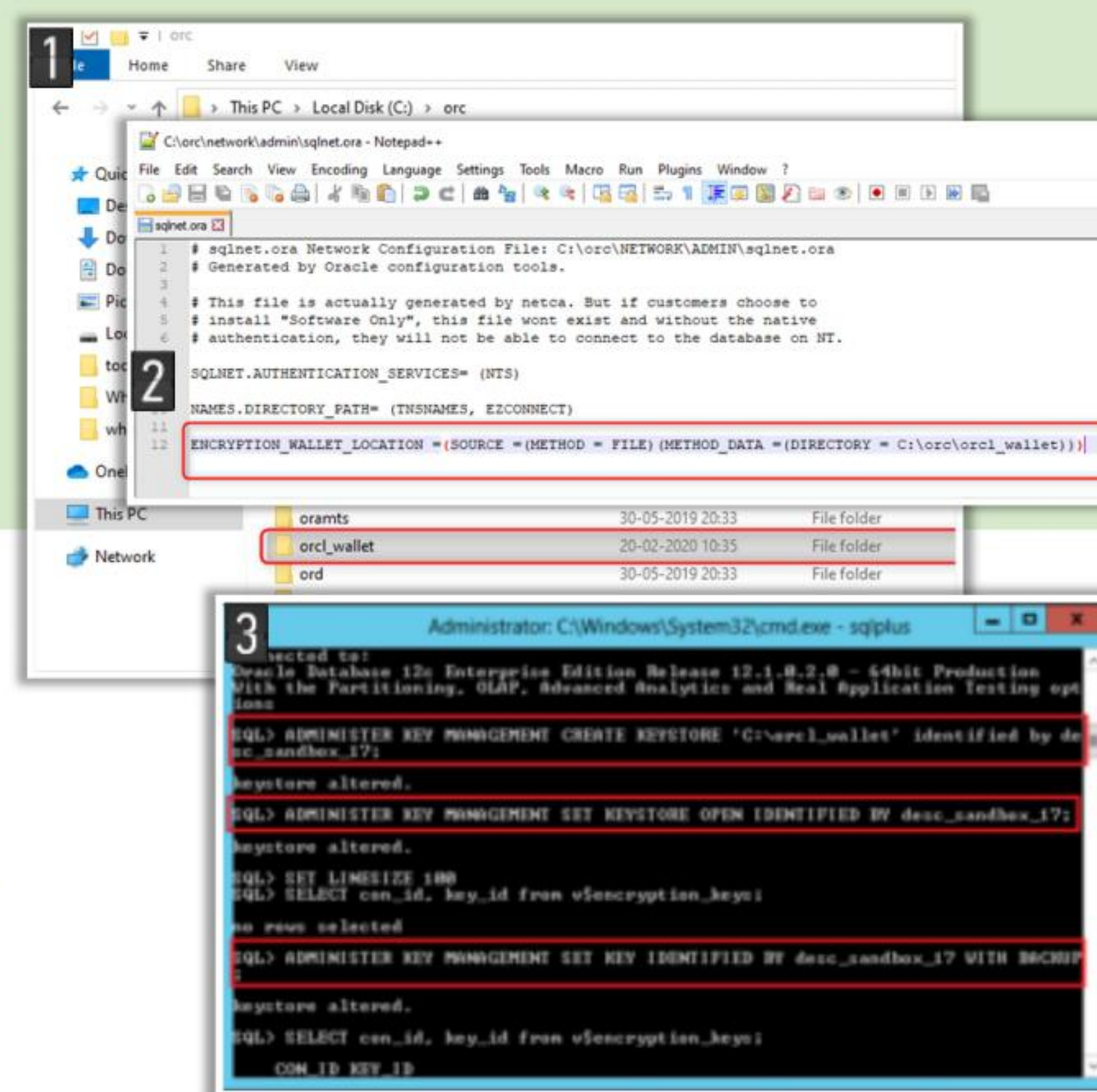
Figure 15.37: Transparent database encryption in MS SQL Server

Implementation of Transparent Data Encryption in Oracle

- ❑ Transparent data encryption (TDE) enables the encryption of **one or more table columns** or a **tablespace**
- ❑ On inserting data in an encrypted column, TDE automatically **encrypts** the data
- ❑ On selecting the encrypted column, the data is automatically decrypted

❖ To implement transparent database encryption:

- ✓ Creating a wallet file location to store all encryption key information
- ✓ Specifying location of the wallet in the sqlnet.ora file located in the NETWORK/admin folder
- ✓ Commands to create, open, and set the master key



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Implementation of Transparent Data Encryption in Oracle

Transparent data encryption (TDE) enables the encryption of one or more table columns, or a tablespace. On inserting data in an encrypted column, TDE automatically encrypts the data. On selecting the encrypted column, the data is automatically decrypted.

To implement TDE in Oracle, the user has to create a Keystore to store the master encryption key and set a master key. The Keystore is a type of operating system file stored outside the database. TDE uses this Keystore to encrypt data in the database.

To implement transparent database encryption:

- Creating a wallet file location to store all encryption key information
- Specifying location of the wallet in the sqlnet.ora file located in the NETWORK/admin folder
- Commands to create, open, and set the master key

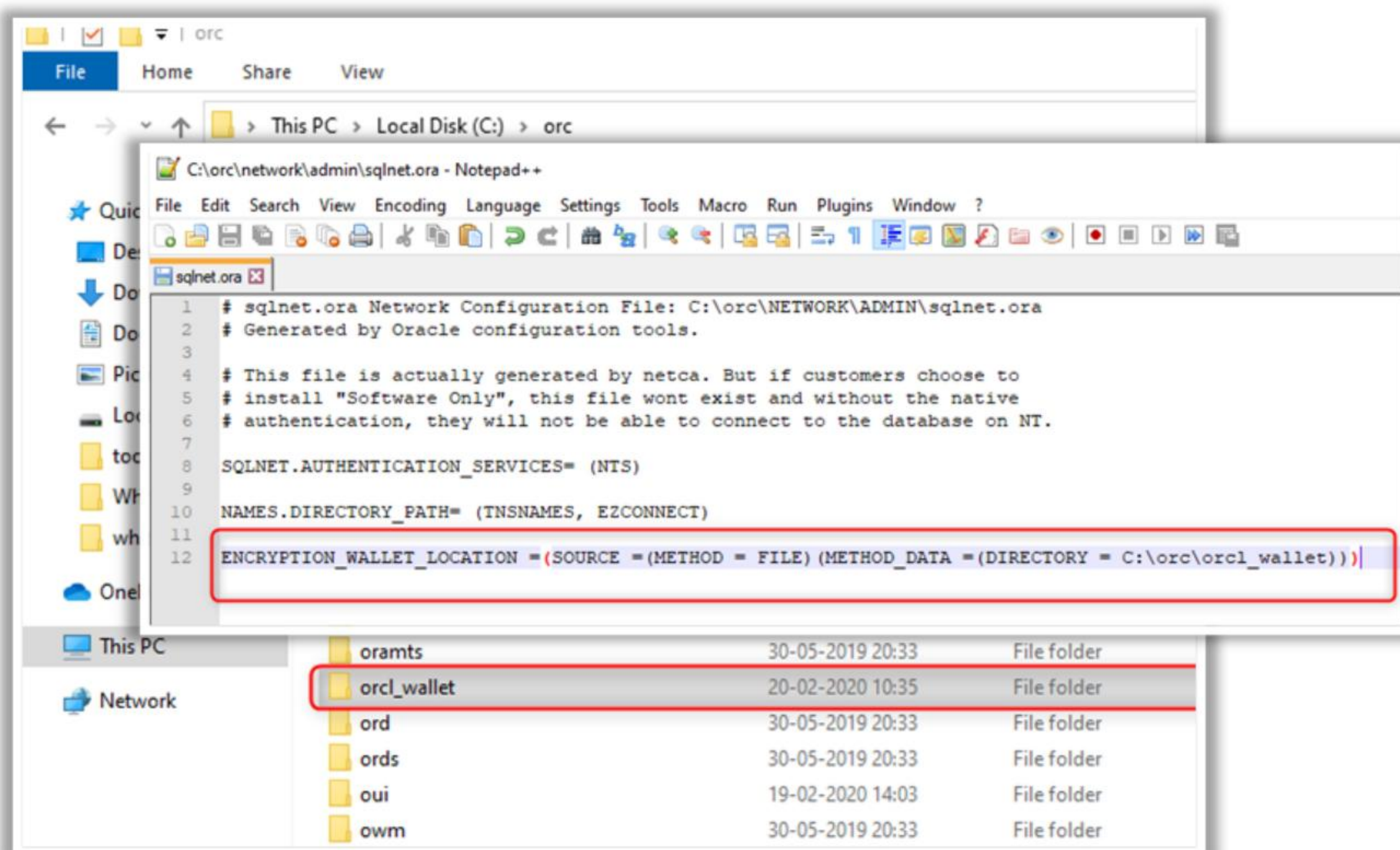


Figure 15.38: Creating a wallet file location

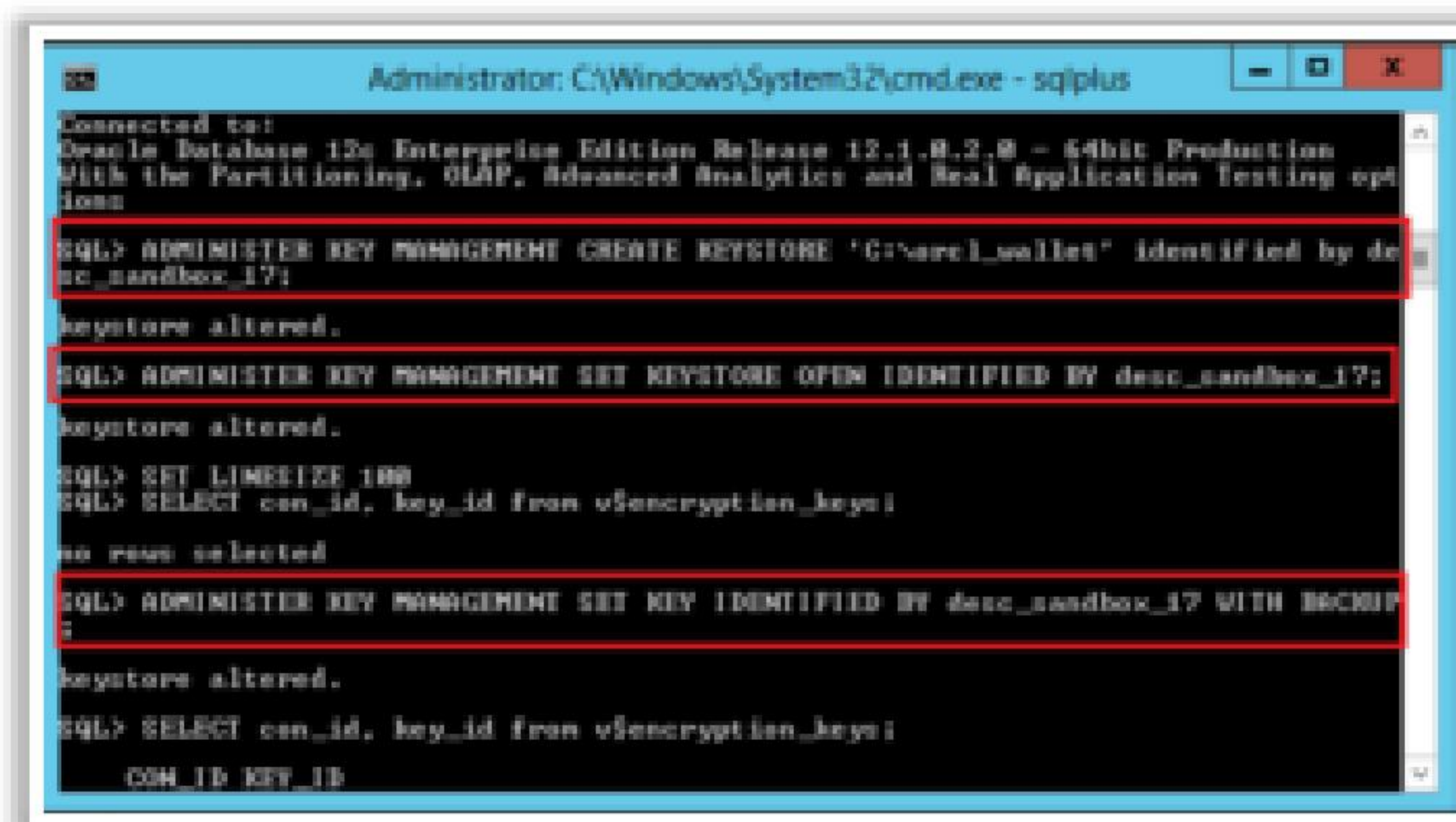


Figure 15.39: Creating and setting the master key

Creating a New Table with an Encrypted Column Using the Default Algorithm (AES192)

```
CREATE TABLE employee ( first_name VARCHAR2(128), last_name
VARCHAR2(128), empID NUMBER, salary NUMBER(6) ENCRYPT );
```

Figure 15.40: Creating new table with an encrypted column

Adding Encrypted Columns to Existing Tables

```
ALTER TABLE employee ADD (ssn VARCHAR2(11) ENCRYPT);
```

Figure 15.41: Adding encrypted column



Encrypting “Data in Transit”

- ☐ Protecting data in transit is **more challenging** than protecting data at rest
- ☐ Data in transit can be secured by encrypting the data prior to sending and using **secured tunnels** such as HTTPS, SSL/TLS, and VPNs

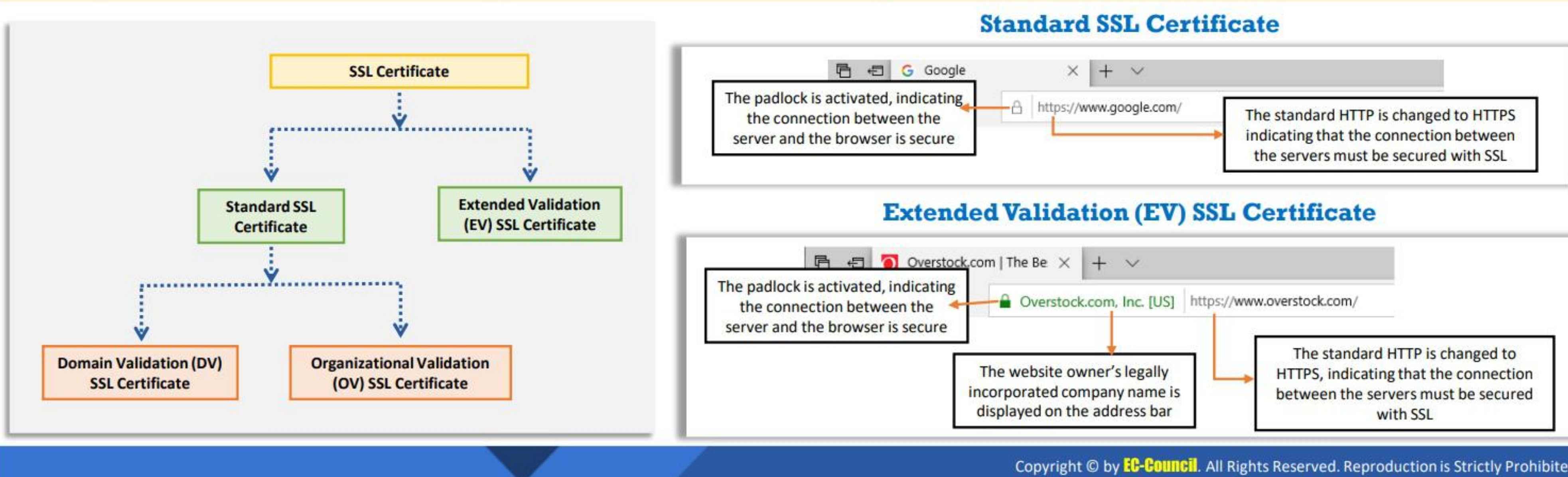
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Encrypting “Data in Transit”

Data are said to be in transit when travelling from one system to another in internal, external, or private networks. Protecting data in transit is more challenging than protecting data at rest. This type of data can be secured by encrypting the data prior to transmitting/sending and using secured tunnels such as HTTPS, SSL/TLS, and VPNs.

Secure HTTP Connection using Digital Certificate

- ☐ The browser connects to a web server by sending a **message** indicating that a **secure session (SSL)** is requested
- ☐ Web server responds by sending a copy of its **root certificate** along with server's public key
- ☐ Browser verifies the **certificate** by checking whether it is valid and has been signed by a **certificate authority (CA)**. It also verifies the certificate's expiry date
- ☐ The browser creates, encrypts, and sends a one-time **session** key along with the server's public key
- ☐ The server uses its **private key** to decrypt the session key, and sends back an acknowledgement encrypted with the session key to begin an encrypted session
- ☐ Now, the browser and server can securely **transmit** data with the session key



Secure HTTP Connection using Digital Certificate

1. The browser makes the connection to a web server by sending it a message, indicating that a secure session (SSL) is requested.
2. The web server responds by sending a copy of its root certificate along with the server's public key.
3. The browser verifies the certificate by checking whether it is valid and has been signed by a certificate authority (CA). It also verifies the certificate's expiry date.
4. The browser creates, encrypts, and sends a one-time session key along with the server's public key.
5. The server uses its private key to decrypt the session key, and sends back an acknowledgment encrypted with the session key to begin an encrypted session.
6. Now, the browser and server can securely transmit data with the session key.

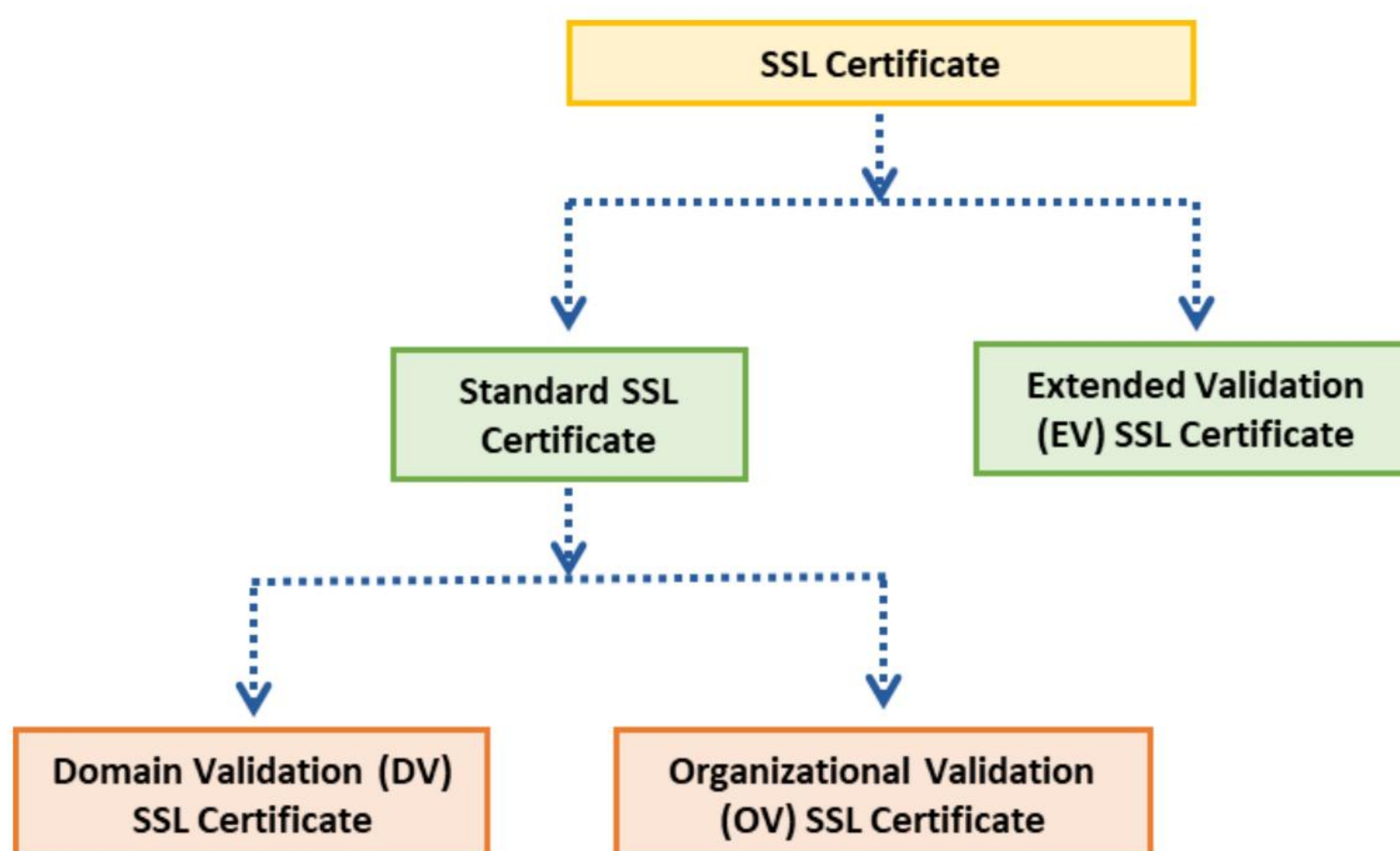


Figure 15.42: SSL certificates

Standard SSL Certificate

This certificate is validated and issued rapidly by the CA, and is ideal for small and medium-sized businesses. A standard SSL certificate displays HTTPS instead of HTTP and a padlock. It is either domain validated or has an organizational validity.

- **Domain-validated (DV) SSL certificate:** The CA verifies only the domain ownership and gives the certificate within a few minutes. This certificate ensures that the website safeguards the user privacy.
- **Organization-validated (OV) SSL certificate:** The CA requires important business documents for validation in order to issue this certificate. This certificate is more trusted than the normal DV SSL certificate. This certificate safeguards user confidentiality and increases the trust on the website.

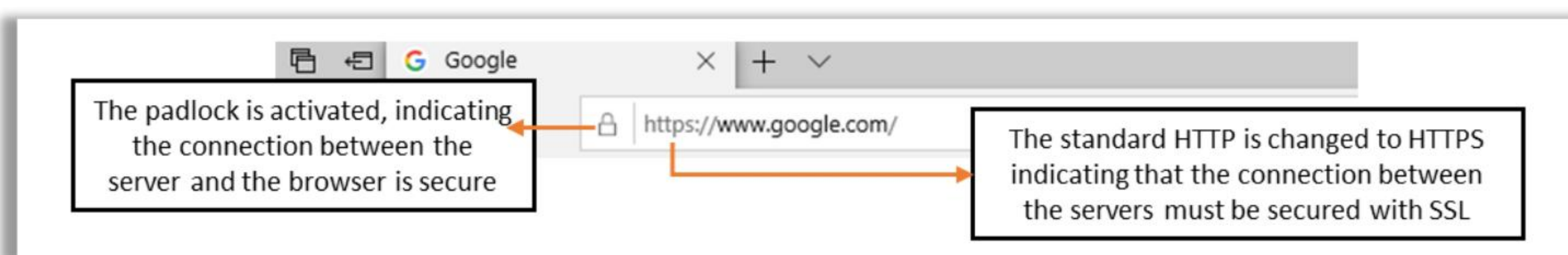


Figure 15.43: Standard SSL Certificate

Extended Validation (EV) SSL Certificate

EV SSL is the most reliable and recommended SSL certificate. It verifies the company name in the URL and delivers a 256-bit robust encryption, which safeguards the confidentiality of the users and increases the trust and confidence in the website.

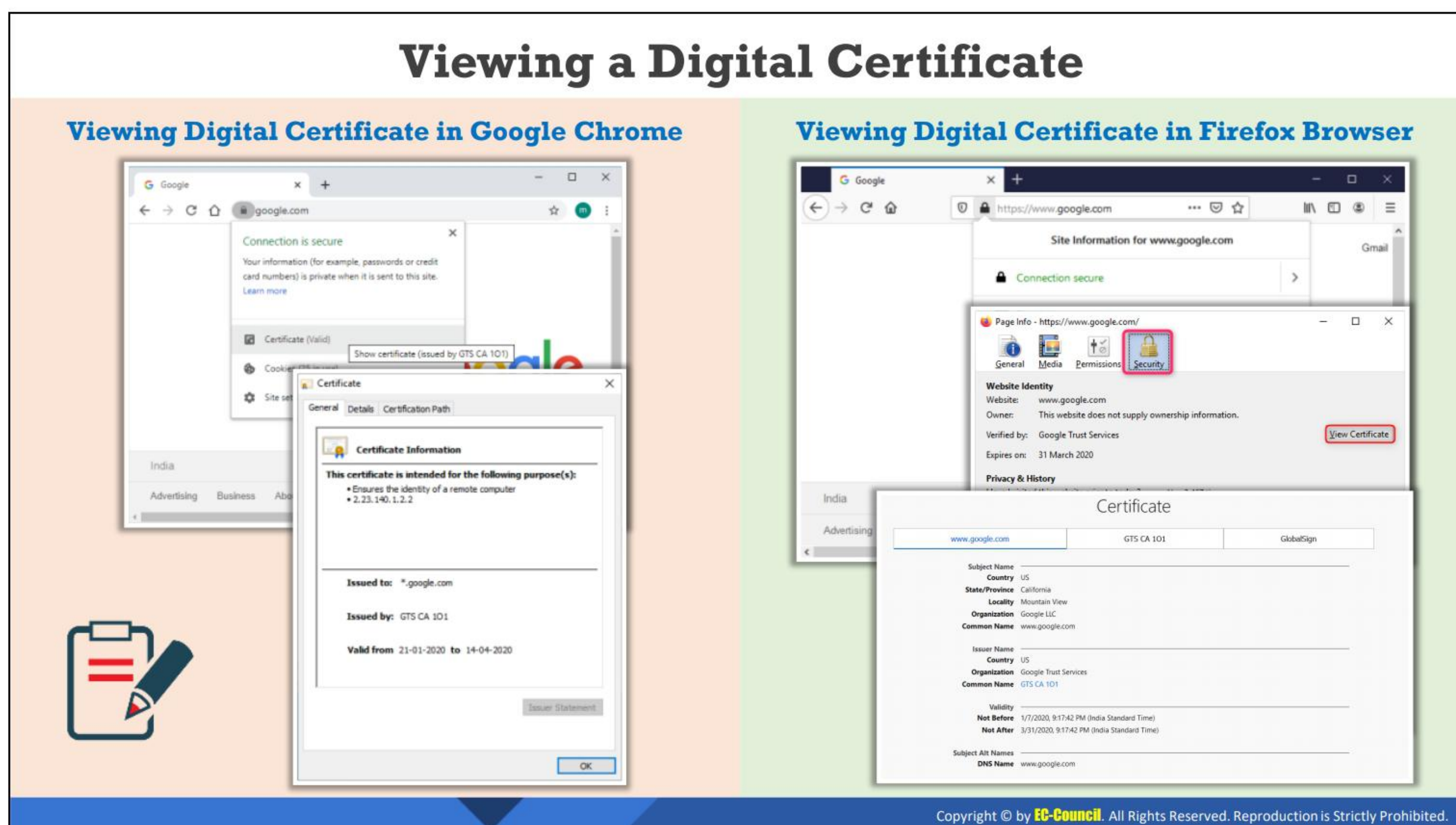
Characteristic Features of EV SSL

- The web address bar should have HTTPS
- The address bar contains the organization name

- The URL contains the company name.
- The certificate information has the CA name.



Figure 15.44: Extended Validation (EV) SSL Certificate



Viewing a Digital Certificate

Viewing a Digital Certificate in Google Chrome

- Type the name of the website whose certificate the user wants to view in Google Chrome browser.
- Click the lock icon in the address bar, then navigate and click on **Certificate**.

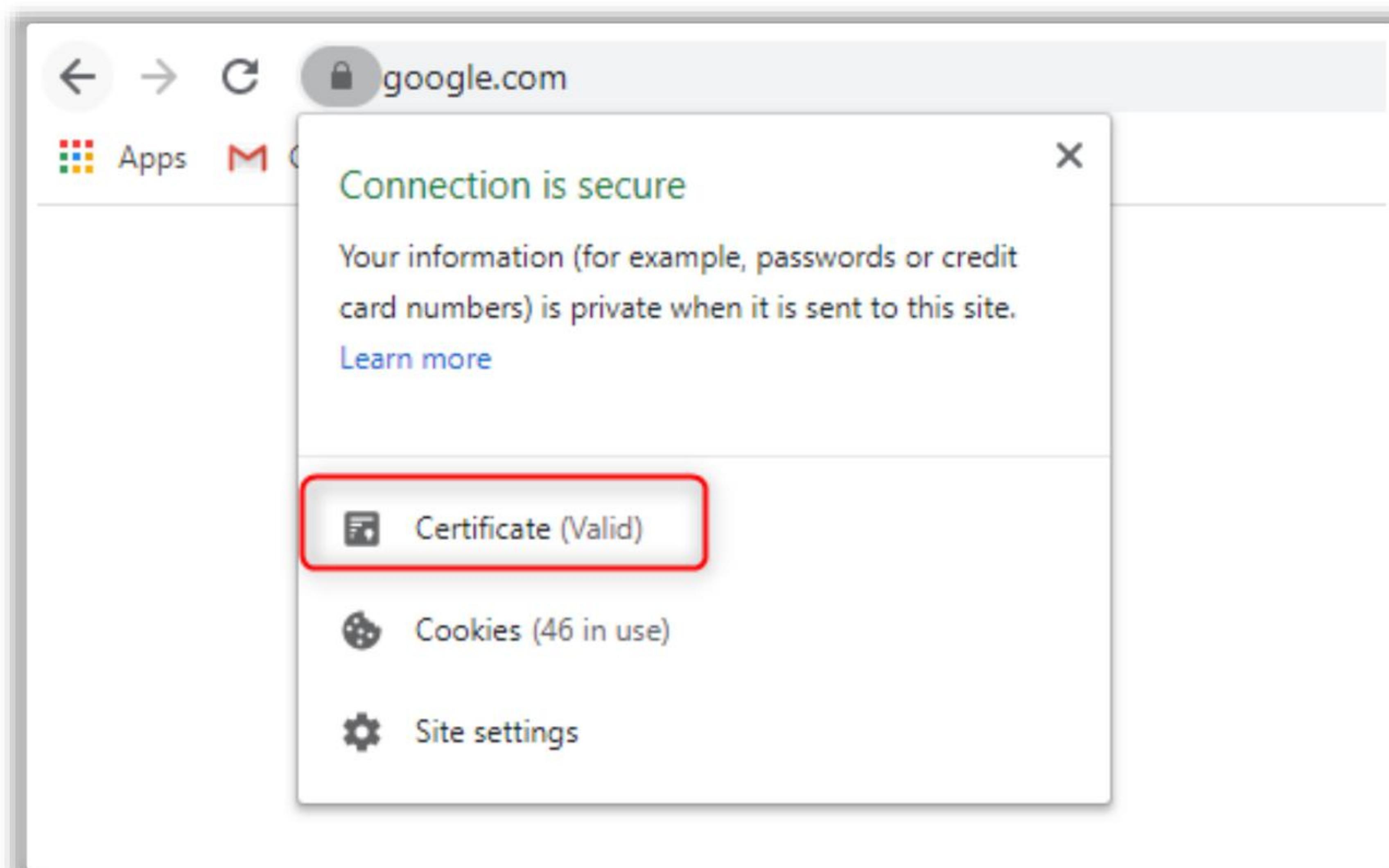


Figure 15.45: Selecting Certificate Option

- A new window will open with **General**, **Details**, and **Certification Path** tabs; click **General**.

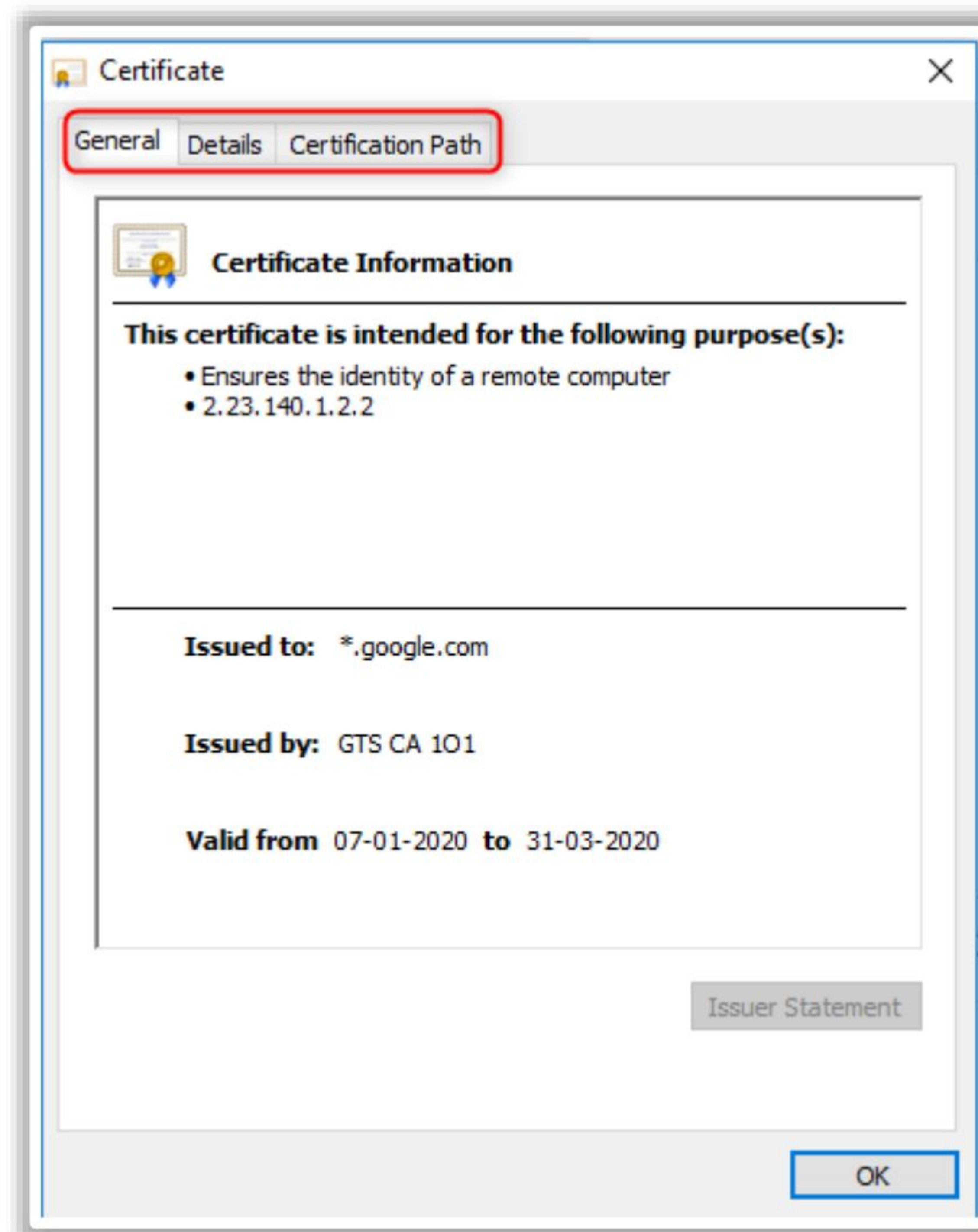


Figure 15.46: Choosing General Tab

Viewing a Digital Certificate in Firefox Browser

- Enter the name of the website whose certificate the user wants to view in Firefox browser.
- Click the lock icon in the address bar.

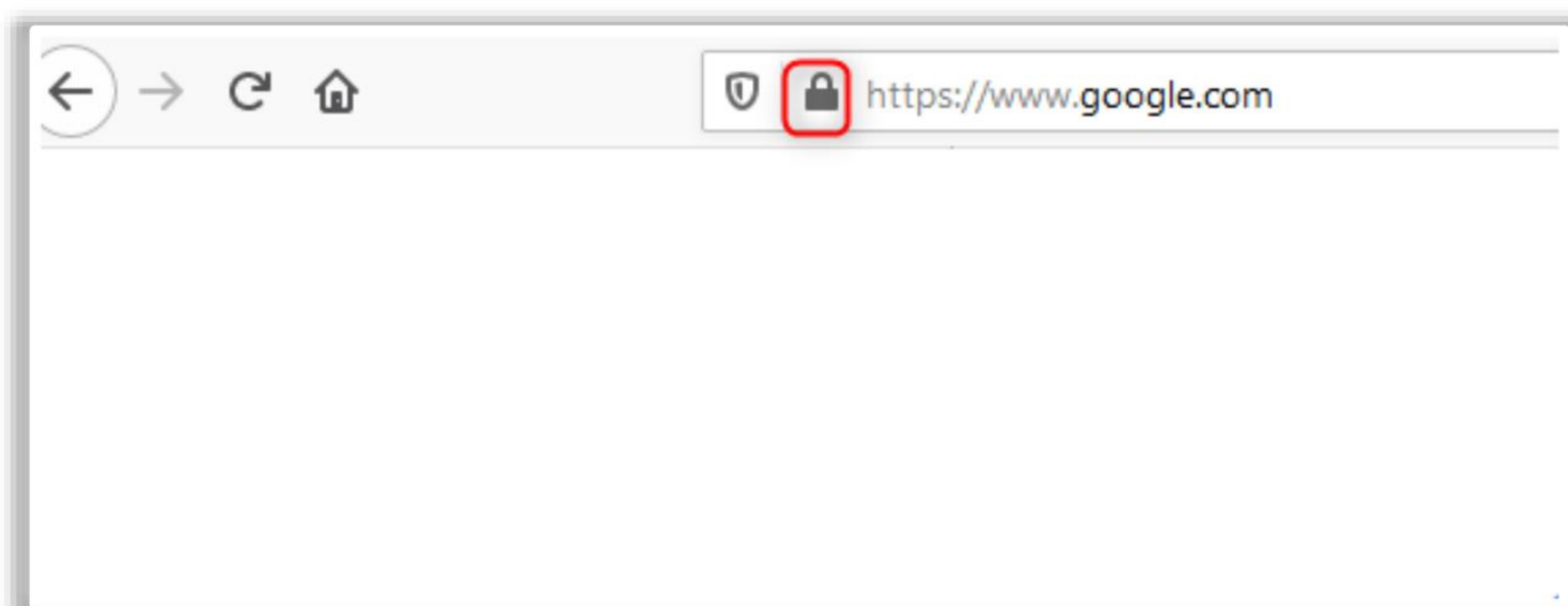


Figure 15.47: Clicking the Lock Icon in the Address Bar

- Click **Connection secure** to see the connection details.

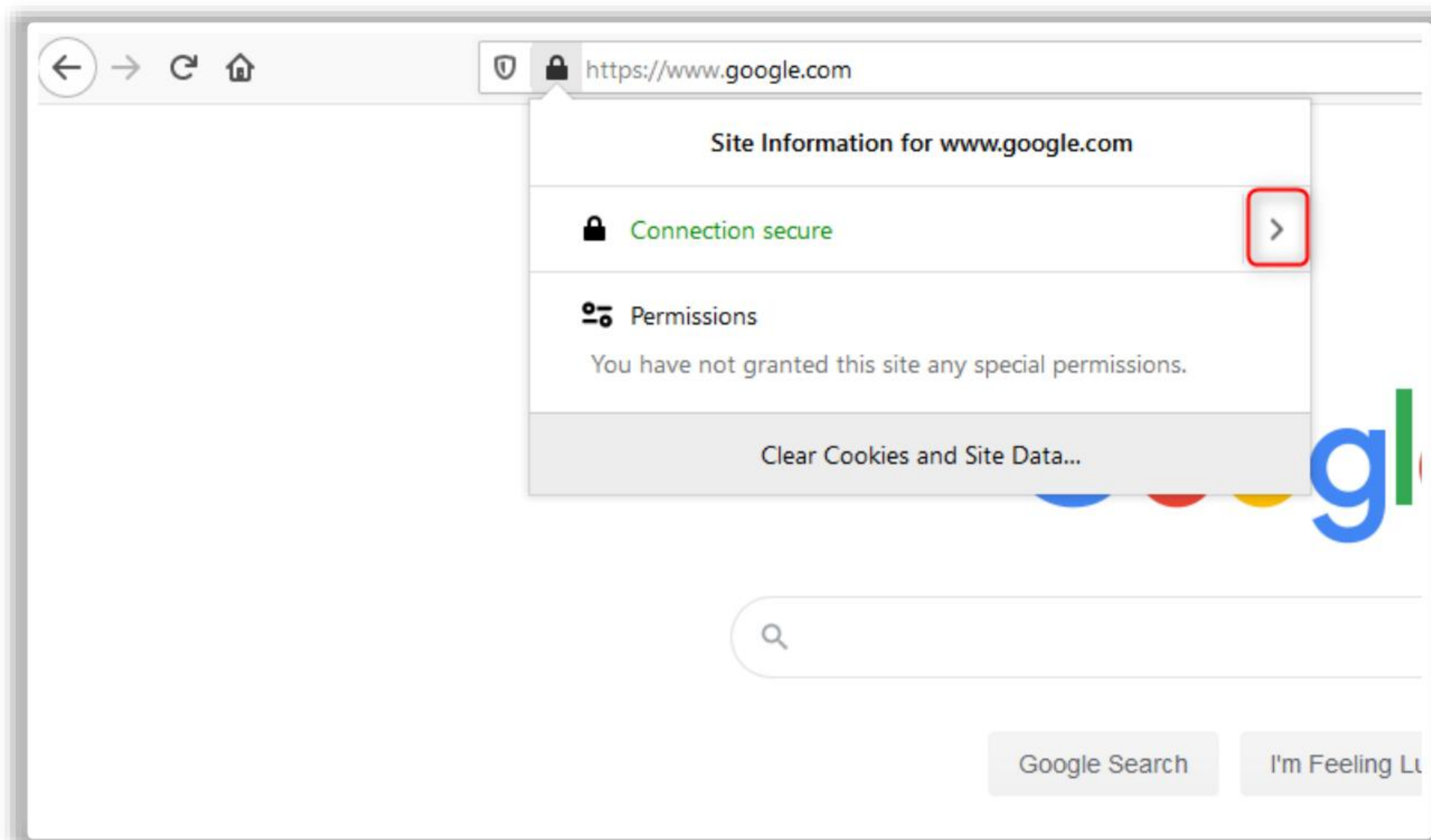


Figure 15.48: Checking the Connection Details

- Navigate to and click **More information**.

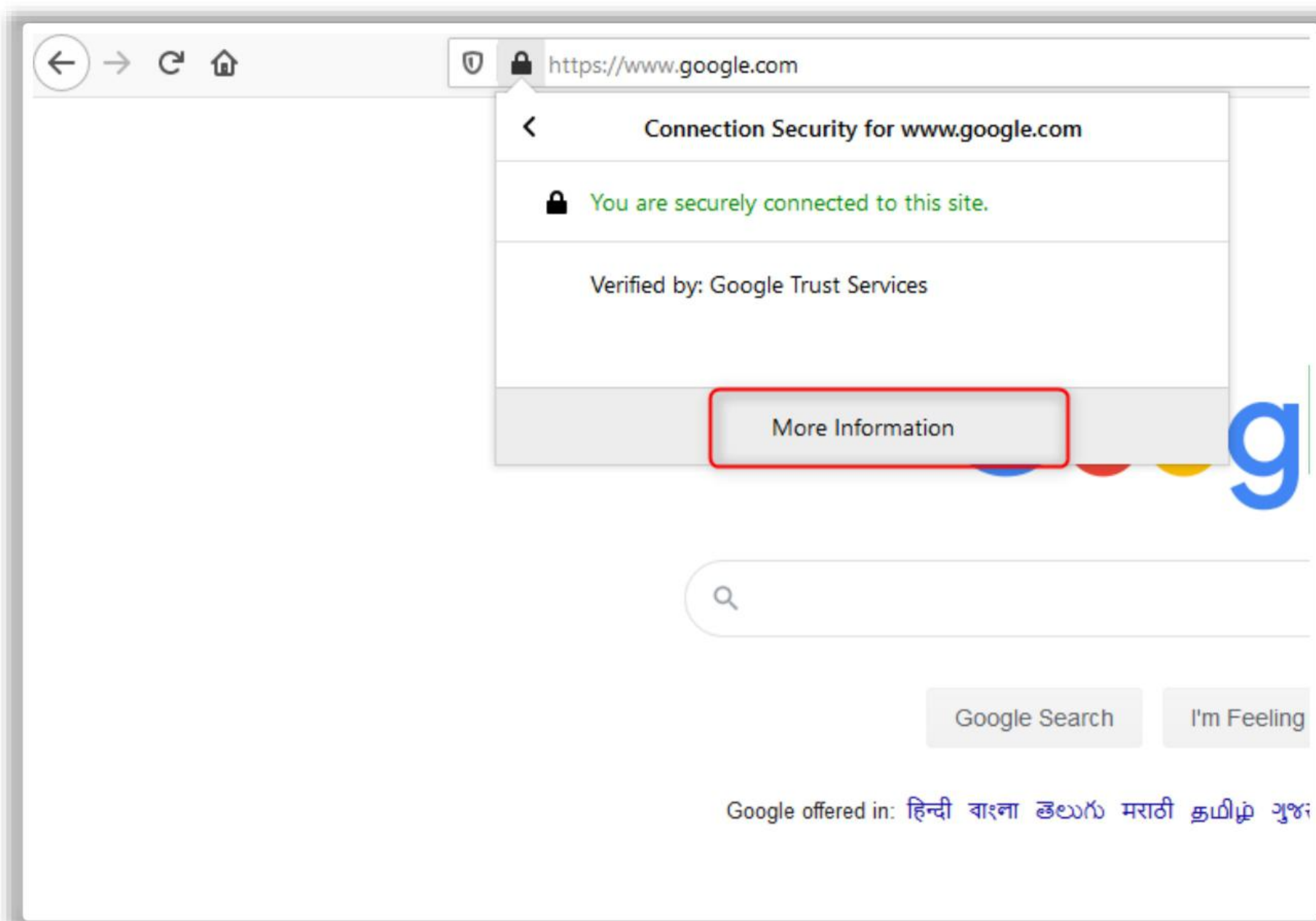


Figure 15.49: Select More Information

- A new **Page Info** window will open; click **Security** tab.
- Click **View Certificate** to view the digital certificate.

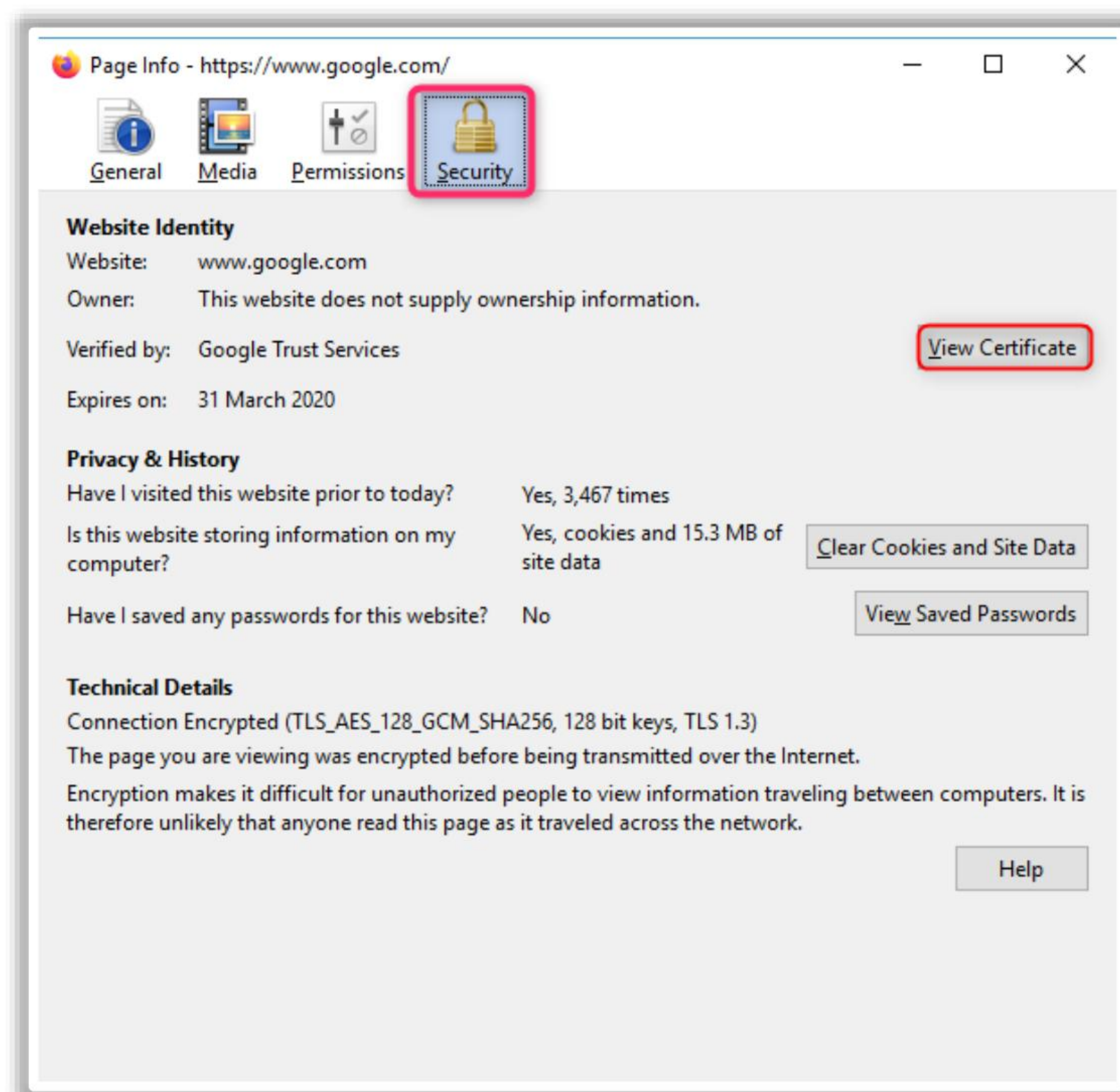


Figure 15.50: Clicking on Security Tab

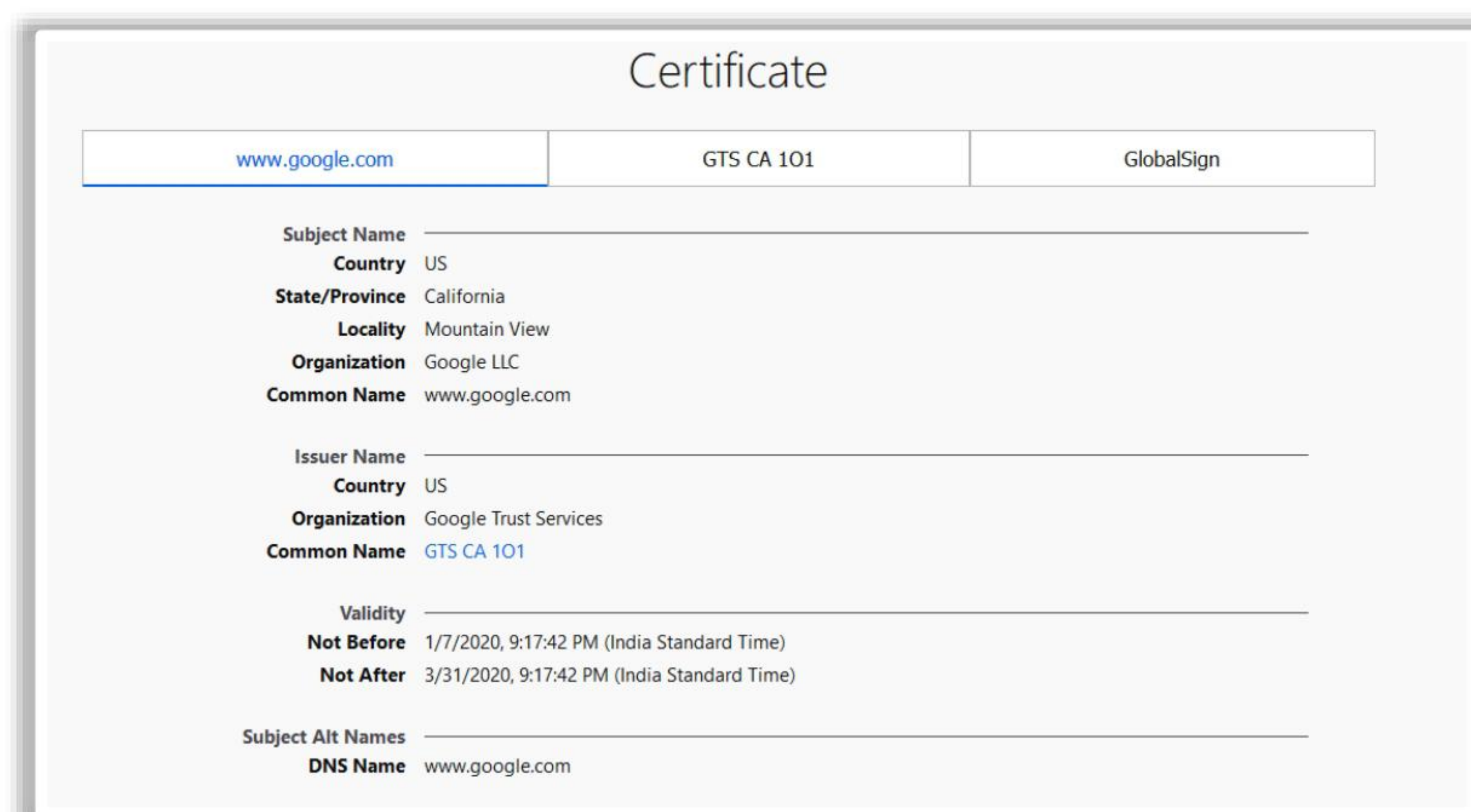


Figure 15.51: Viewing the Digital Certificate

Install and Configure SSL Certificate on Windows Server

1 Create CSR (Certificate Signing Request)

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICvDCCAQCAQAwZELMAkGA1UEBhMCV2xk
MA8GA1UEBxMIW91ckNpdHkxZzA5bG9uYVBA
cGFueSw5LjYyYmYGA1UEAxMPd3d3LmV4
9w0BAQEFAAOCAQAMIBChKCAQEA379BFFx
+/SRxj/KtXVddscKw1obHGpMKPw4meJqOp
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3Lx
RdEdXyHdHk1RAoIVQCfjTwBwGNAD337v
7pVfaDb2PuTgUhw7wksKNFxcG0xcTmz/+
GrciHEu20chq86CBP9RiYlpp2+RMSf
m6zMEYm9o65j7vEaKEJUOJA5MIa/Zja
KfSLjXurLUOnCOQIDAQABoAAwDQYJ
KoZihvNAQEFBQADggEBAK159goyAYOpnr
Q2EvCG1szK1s3D8JjnAiP1NHzjB
/qdTYR+/8Dr/hMcwU5ThGAUf68aMk6t
UNWAdp29C904Js2z+ENEb08GA0Fe4w
ix7vb15vSKe9shGiJRGIzaHVGpR3r7x
QcIuMaDax3x1V8jHbcvZTopX0Kbq6H1G
NLA4CXeOI4KGwu4FXfSazEGb3gEJD8H
aMP8V8er5G0owr/g/9Z/1/b0g97kAcUv
kM2eDsvPhMx/pENGbnLPe4XMy7NP1Eds
FnaYtUy2BDcXj3ZQEWxRWk1ERgg9/Yc
W1obf5ziunM1Df24NBt5tpCNzfGviKI6
/YfWg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

2 Install SSL Certificate

3 Assign SSL Certificate

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Install and Configure SSL Certificate on Windows Server

Step 1: Create a Certificate Signing Request (CSR)

- From windows start menu, type **Internet Information Services (IIS) Manager** and open it.
- In the IIS Manager window's Connections menu, navigate to and select the server name.

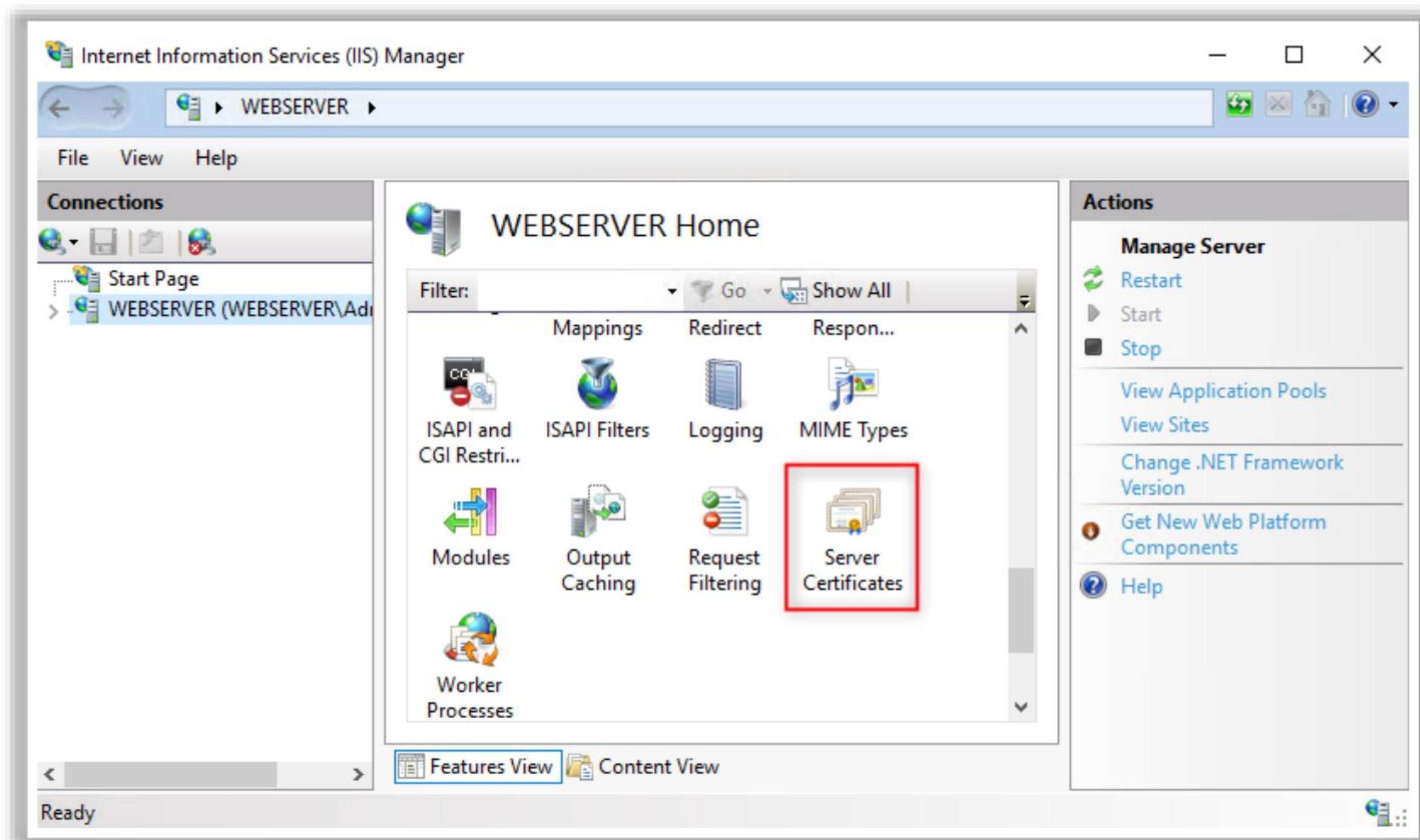


Figure 15.52: Selecting the Name of the Server

- On the server home page's IIS section, double-click on **Server Certificates**.
- On the **Server Certificates** page's **Actions** menu, click on the **Create Certificate Request** link.

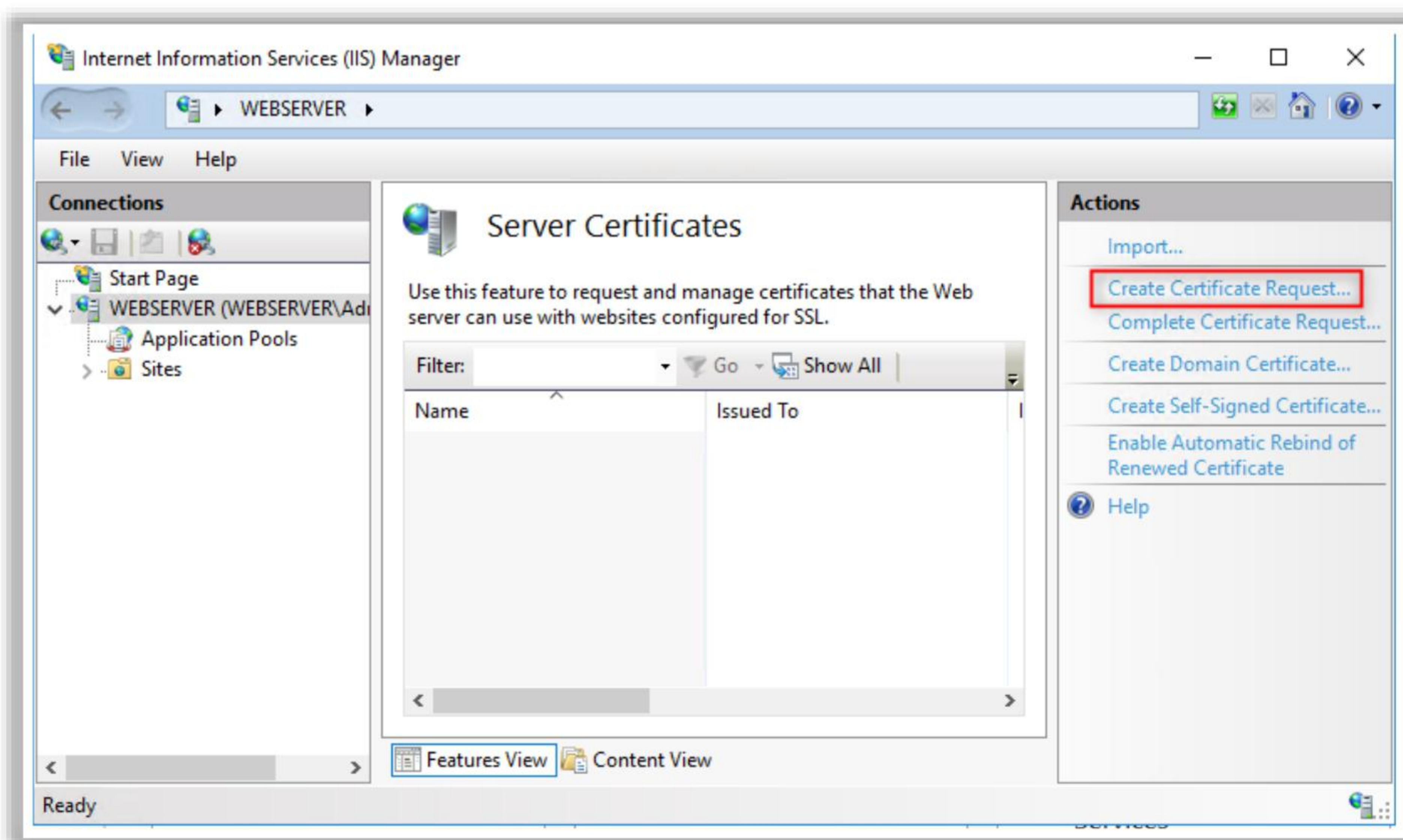


Figure 15.53: Clicking on Create Certificate Request

- In the request certificate's **Distinguished Name Properties** page, fill the following details.
 - **Common name:** Type the domain name
 - **Organization:** Enter the company's legally registered name.
 - **Organization unit:** Type the department name.
 - **City/locality:** Type the name of the city where the company is legally located.
 - **State/Province:** Type the name of the state/province where the company is legally located.
 - **Country:** Select the name of the country where the company is legally located.
- Click **Next** after entering the details.

Request Certificate

Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:

Organization:

Organizational unit:

City/locality:

State/province:

Country/region:

Previous Next Finish Cancel

Figure 15.54: Filling Distinguished Name Properties Page

- On the **Cryptographic Service Provider Properties** page, enter the following details.
- **Cryptographic service provider:** From the drop-down menu, select **Microsoft RSA SChannel Cryptographic Provider** if the user does not have a specific cryptographic provider.
- **Bit length:** From the drop-down menu, select 2048.
- Click **Next**.

Request Certificate

Cryptographic Service Provider Properties

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider:

Bit length:

Previous Next Finish Cancel

Figure 15.55: Filling Details on Cryptographic Service Provider Properties Page

- On the **File Name** page, **Specify a file name for the certificate request**, browse to the location, and save the csr.txt file. Click **Finish**.

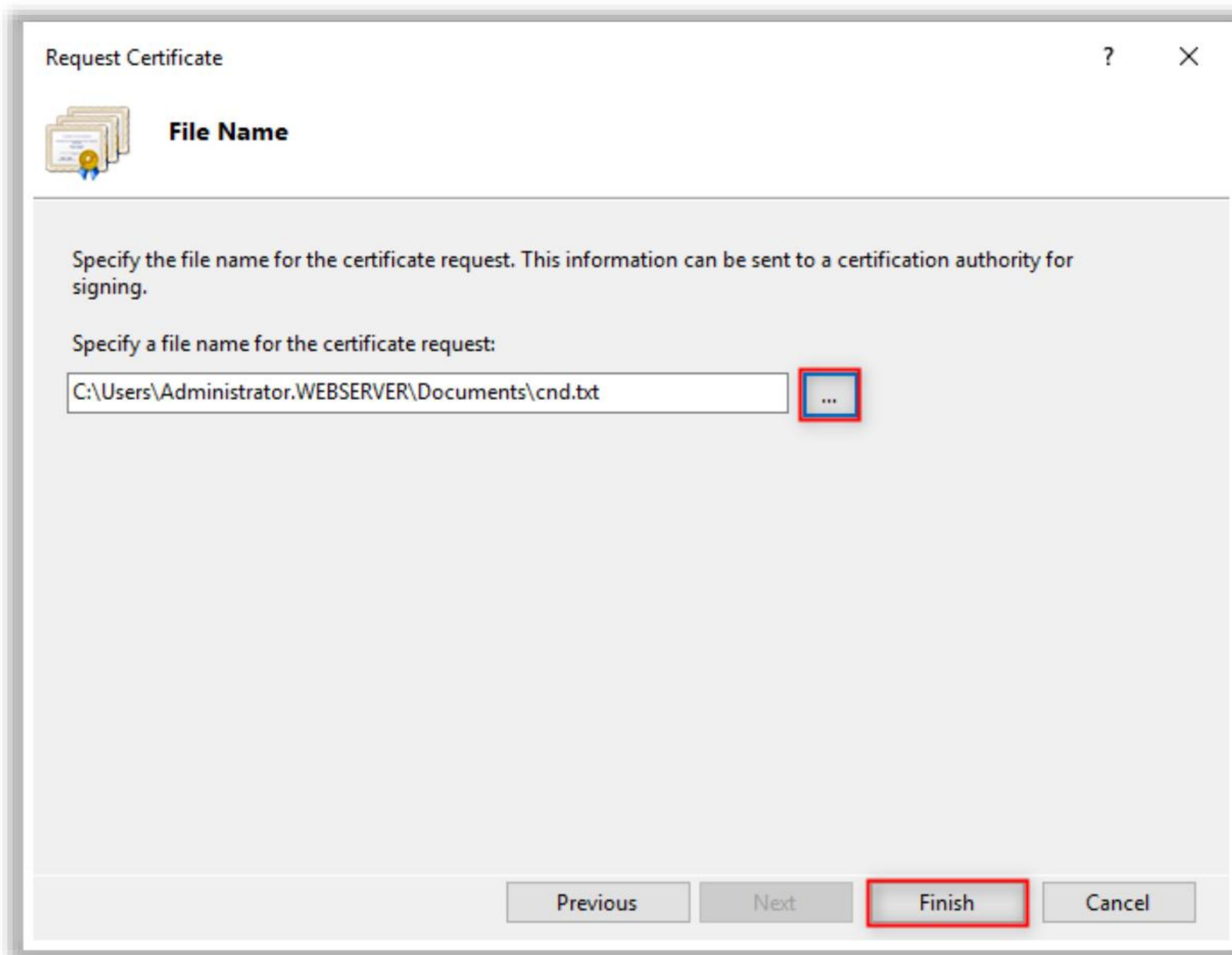


Figure 15.56: Specify a file name for the certificate request

- Open the csr.txt file in a text editor, copy the complete text including the tags, and paste it on the SSL certificate provider form.
- After receiving SSL certificate from the provider, install it.



Figure 15.57: SSL certificate

Step 2. Install SSL Certificate

- Save the SSL certificate sent by the SSL certificate provider.
- From Windows start menu, type **Internet Information Services (IIS) Manager** and open it.
- In the new **IIS Manager** window's **Connections** menu, navigate to and click on the server name.

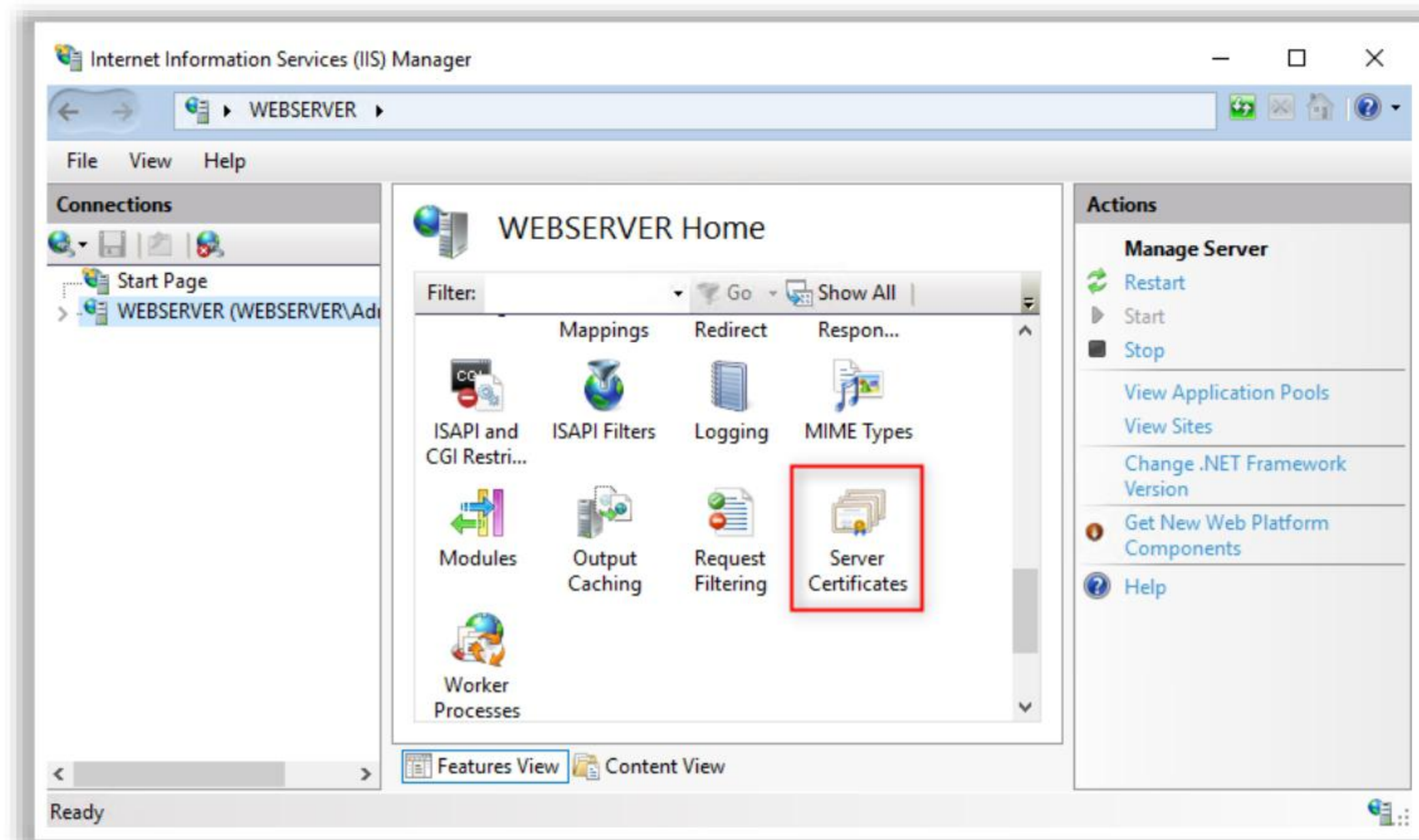


Figure 15.58: Selecting the Name of the Server

- On the server's **Home** page (central pane) in **IIS** section, double-click **Server Certificates**.
- In the right pane's **Actions** menu, click **Complete Certificate Request** link.

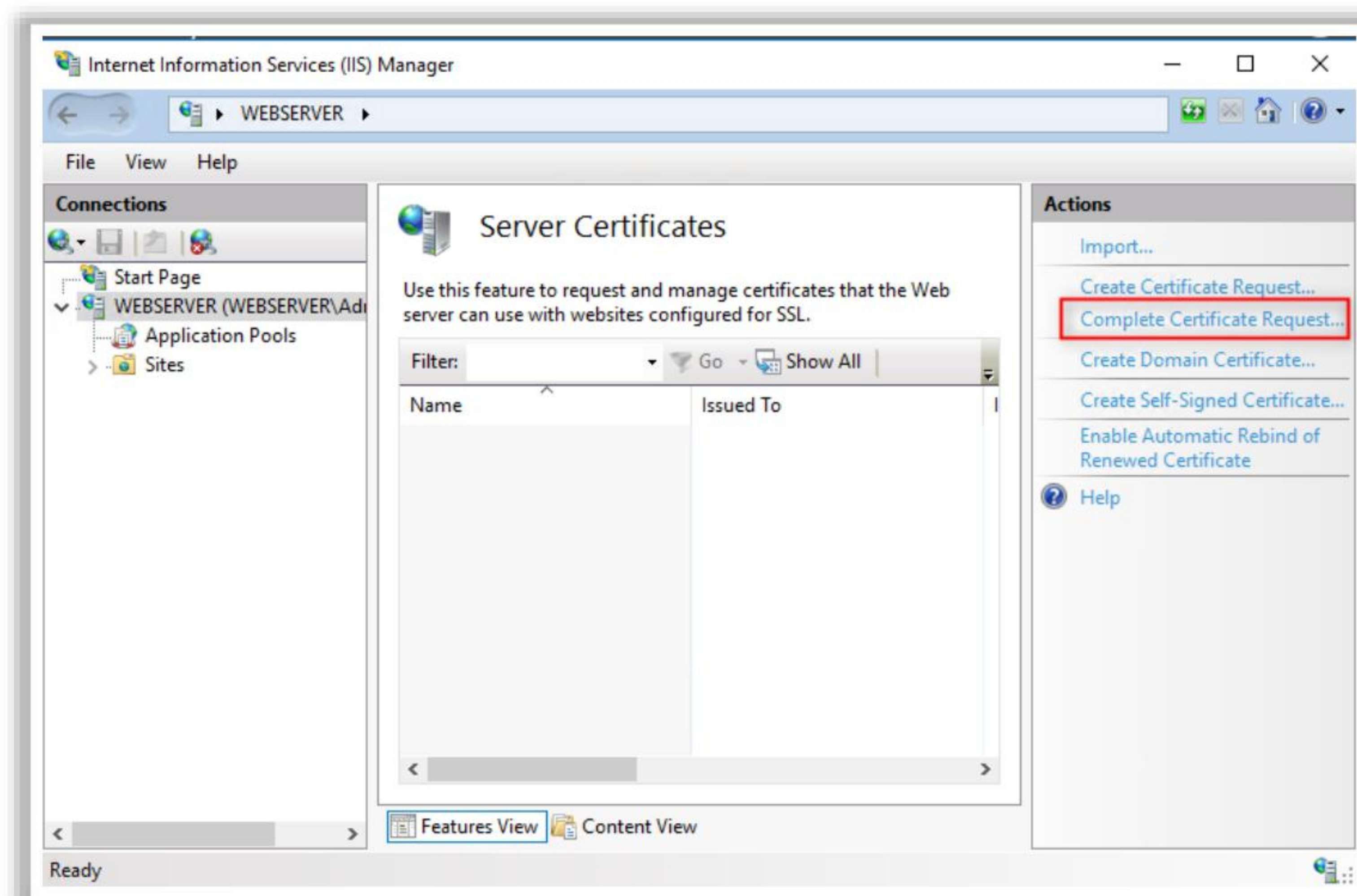


Figure 15.59: Clicking on Complete Certificate Request

- In the **Complete Certificate Request** window, fill the following details
 - **File name containing the certification authority's response:** Browse and select the saved SSL certificate sent by the SSL certificate provider.
 - **Friendly name:** Enter a friendly name for the certificate in order to identify it.
 - **Select a certificate store for the new certificate:** From the drop-down menu, Select **Web Hosting**.
- Click **OK**. Once the SSL certificate is successfully installed, assign it to the appropriate website.

Step 3. Assign SSL Certificate

- From **IIS Manager's Connection** menu, select the name of the server on which the SSL certificate was installed, then select the site on which the user wants to use the SSL certificate.
- On the home page of the website, click the **Bindings** link under **Edit site** section of the **Actions** menu.

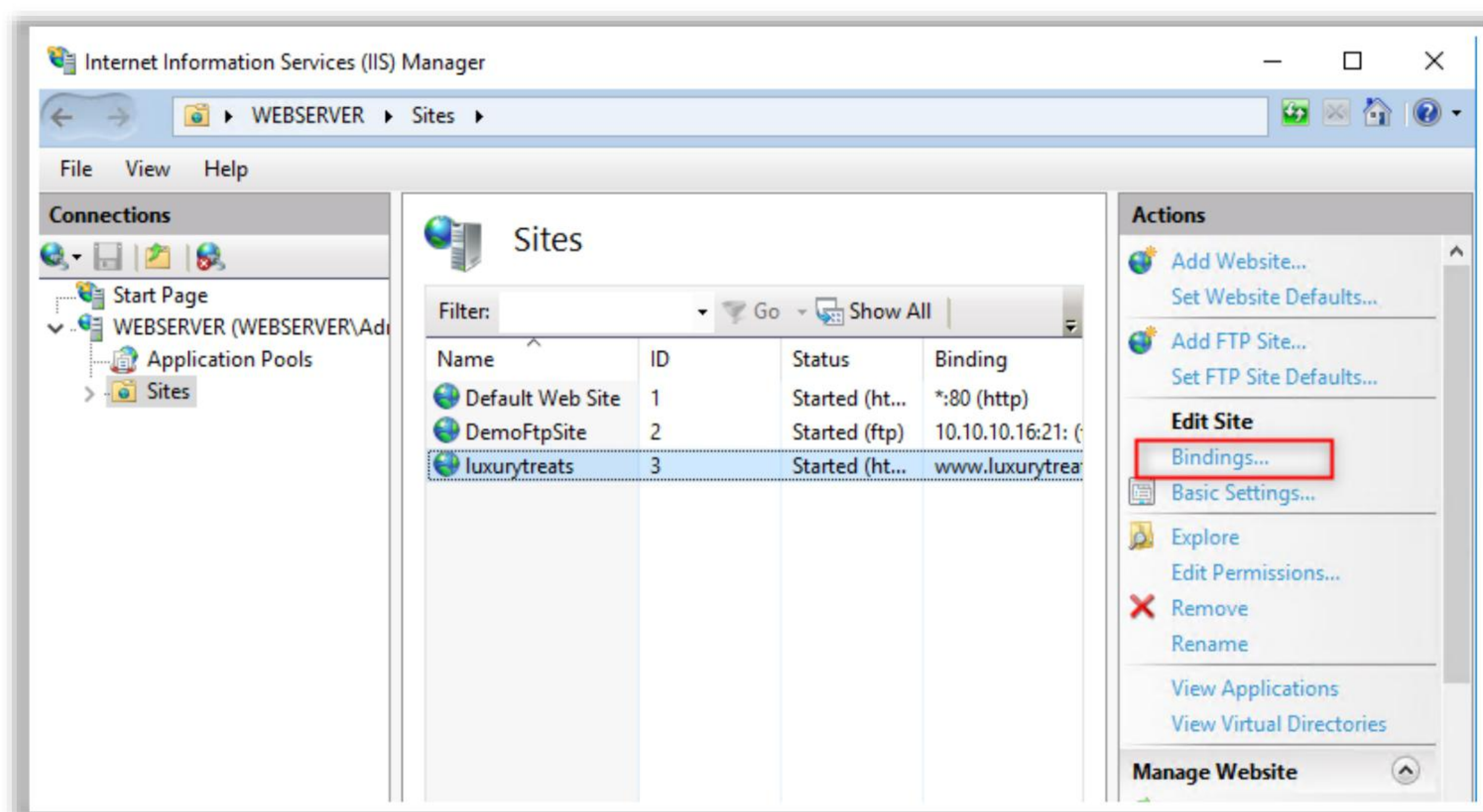


Figure 15.60: Bindings link

- In the new **Binding Site** window, click **Add**.

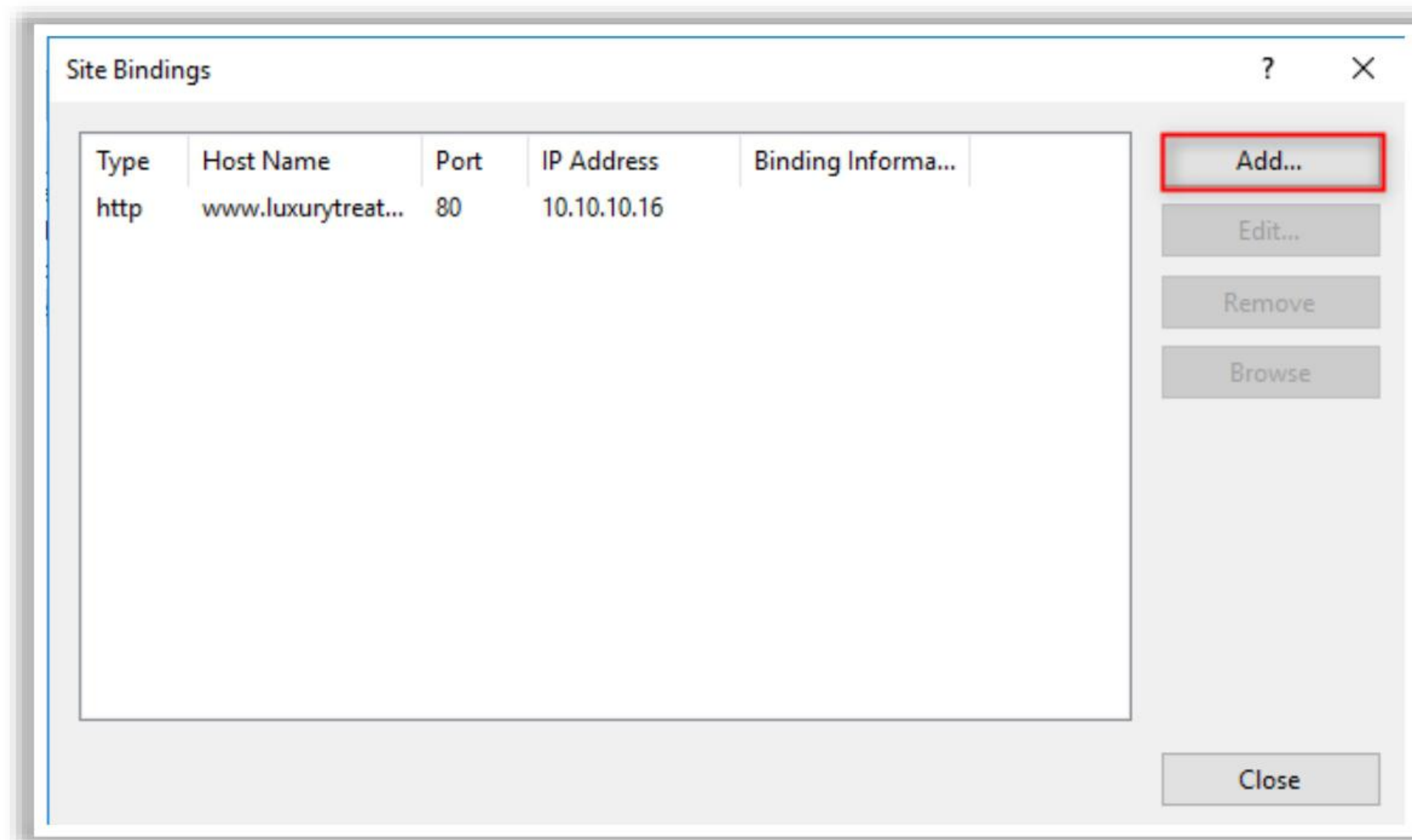


Figure 15.61: Clicking on Add Button

- Enter the following details
 - **Type:** Select **https** from the drop-down menu.
 - **IP Address:** From the drop-down menu, select IP address of the site/ All Unassigned.
 - **Port:** Type 443.
 - **SSL Certificate:** Select the new SSL certificate.
- Click **OK**.

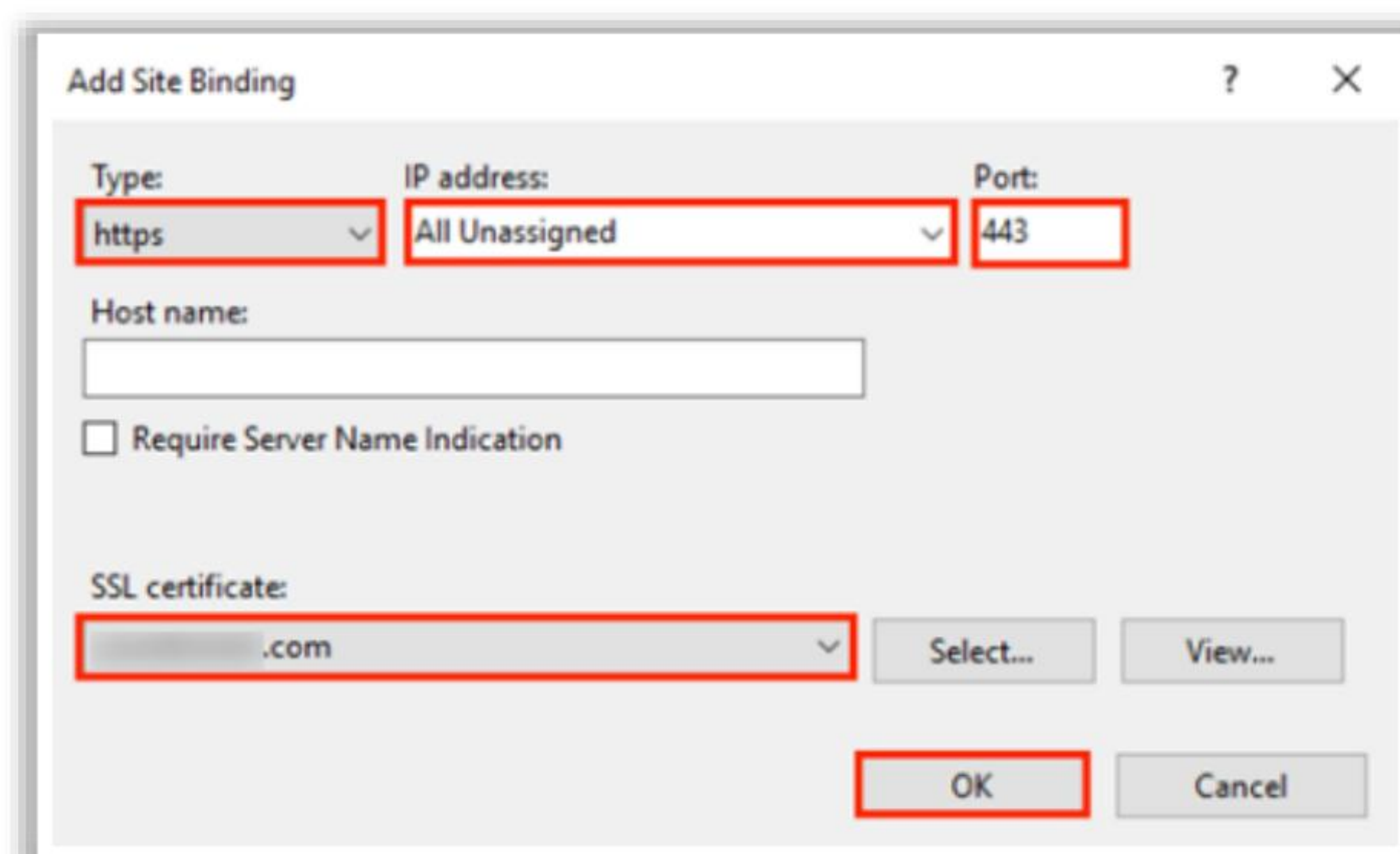


Figure 15.62: Filling Details in Add Site Binding Page

- The SSL certificate is installed, and the website is configured to accept a secure connection.

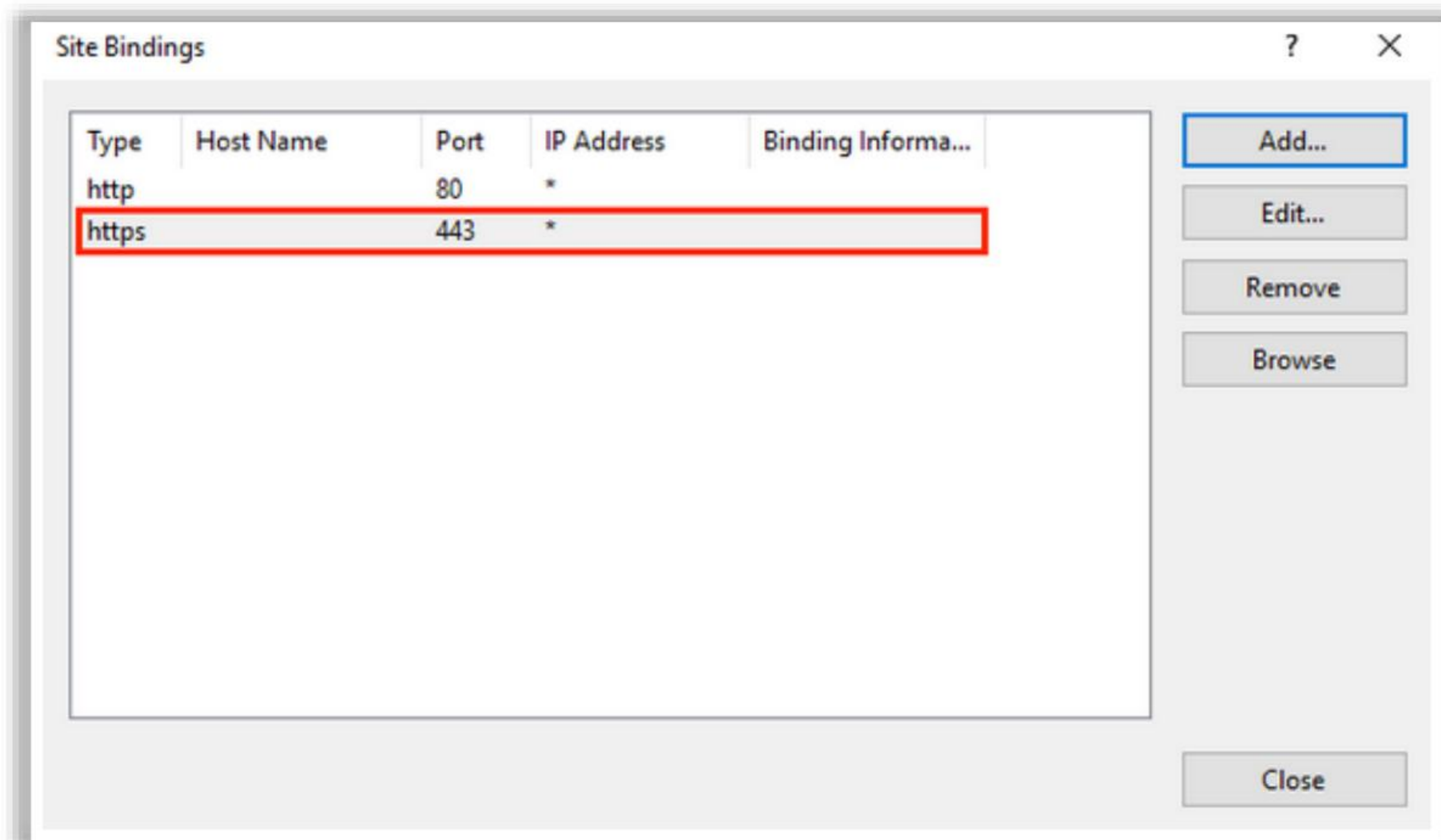
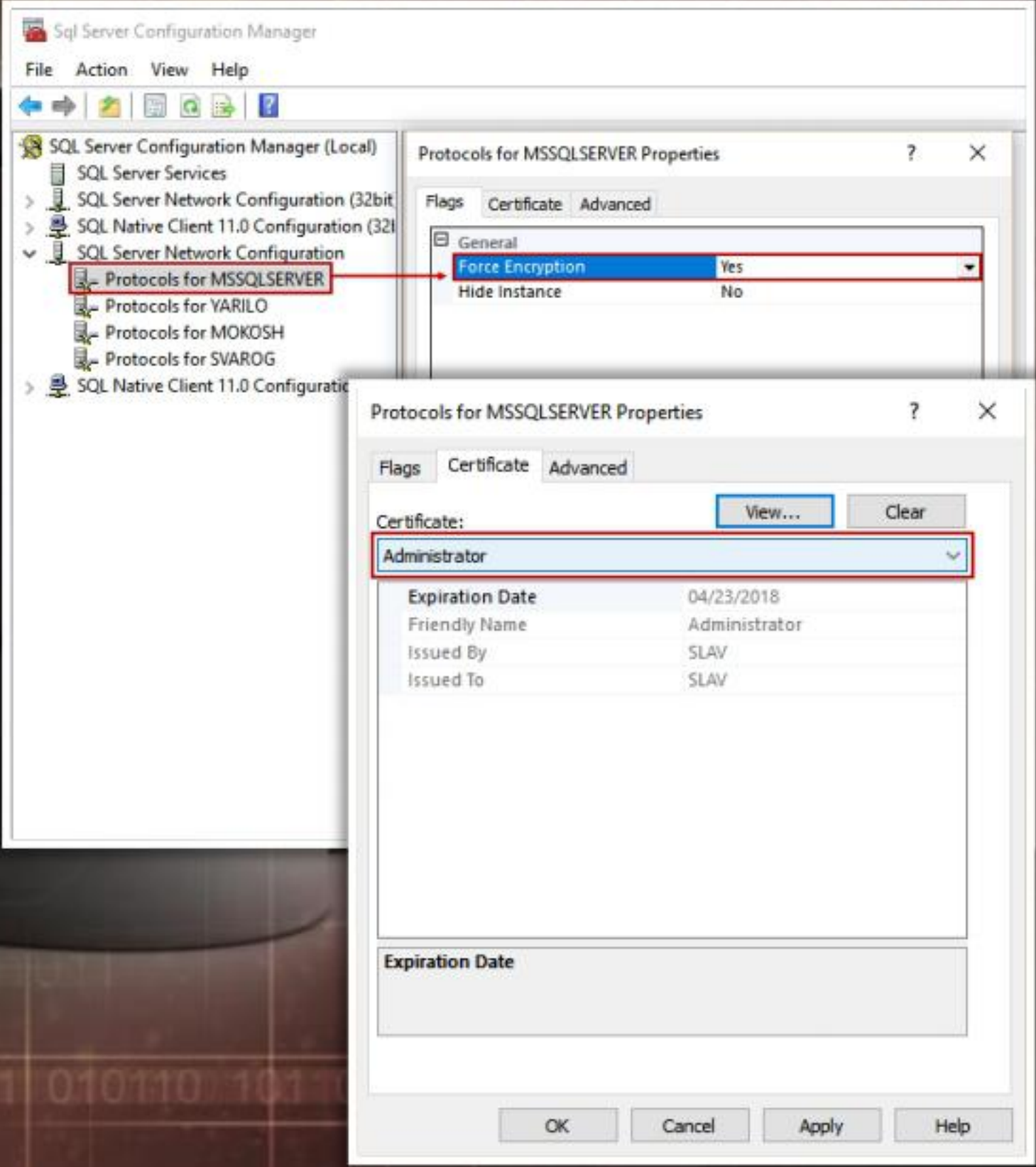


Figure 15.63: Installation of SSL Certificate and Configuration of Website to Establish Secure Connection

Enable Encrypted Connections for an Instance of the SQL Server Database Engine

- ❑ Enable **TLS encryption** to secure the data transmitted between instances of SQL Server and SQL clients/applications
- ❑ TLS encryption is performed within the **protocol layer** and is available to all supported **SQL Server clients**
- ❑ The server computer should contain an installed **certificate**
- ❑ The certificate must be issued for server authentication. The name of the certificate must be the **fully qualified domain name** (FQDN) of the computer
- ❑ The client machine must be set up to trust the certificate's root authority
- ❑ Using a **self-signed certificate** for encryption offers only limited protection
- ❑ The version of Microsoft Windows operating system running on the application and database computers decides the level of encryption used by TLS: 40-bit or 128-bit



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Enable Encrypted Connections for an Instance of the SQL Server Database Engine

- Enable TLS encryption to secure the data transmitted between instances of SQL server and SQL clients/applications.
- TLS encryption is performed within the protocol layer and is available to all supported SQL server clients.
- The server computer should contain an installed certificate.
- The certificate must be issued for server authentication. The name of the certificate must be the fully qualified domain name (FQDN) of the computer.
- The client machine must be set up to trust the certificate's root authority.
- Using a self-signed certificate for encryption offers only limited protection.
- The version of Microsoft Windows operating system running on the application and database computers decides the level of encryption used by TLS: 40-bit or 128-bit.

To Enable Encrypted Connections in SQL Server

- Install the certificate on the SQL server.
- Open **SQL Server Configuration Manager**.
- Navigate to **SQL Server Network Configuration** and Select the required **Protocols** for SQL server instance.

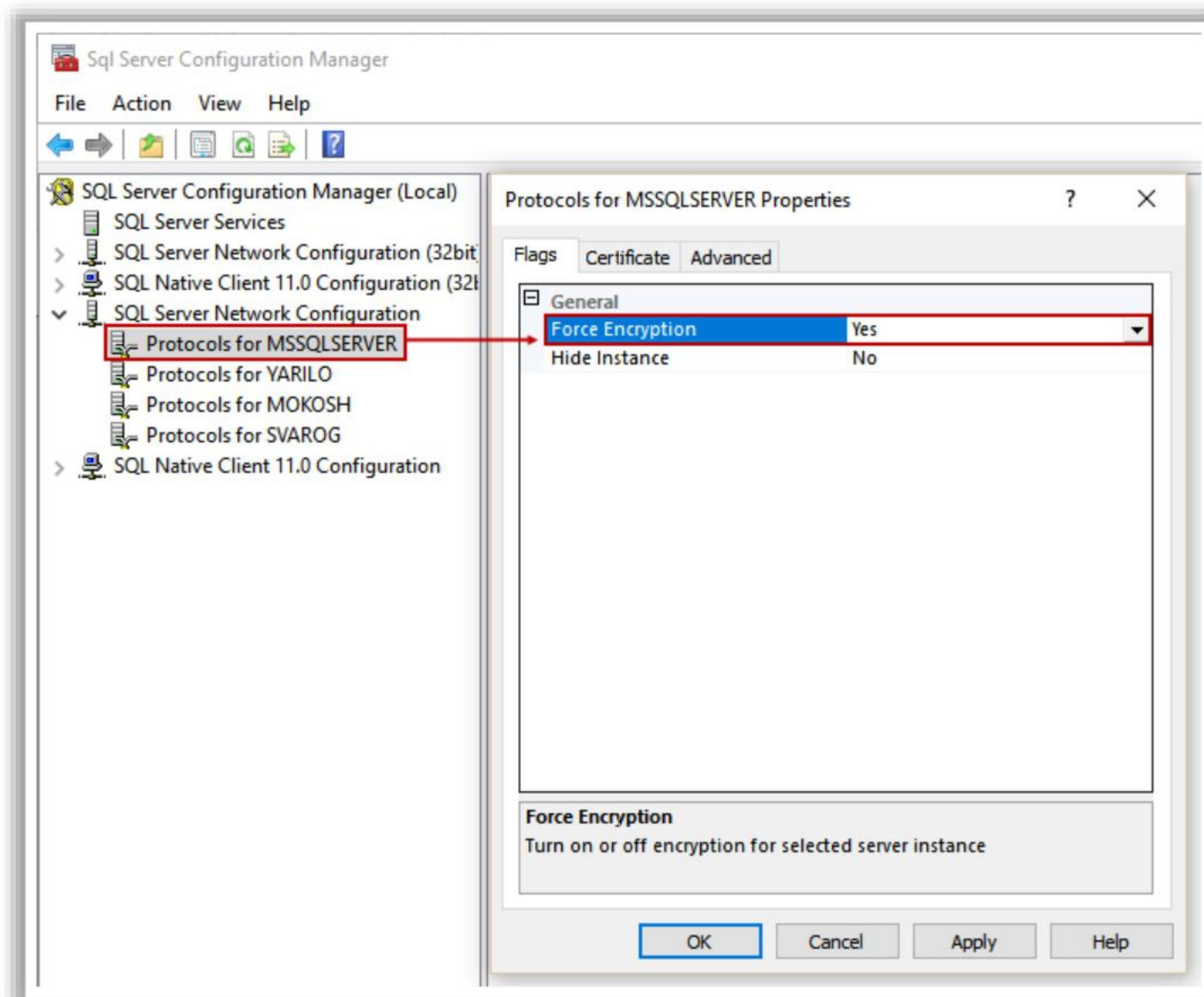


Figure 15.64: SQL Server Configuration Manager

- Right-click on the Protocols and select the **Properties**.
- Click on the **Certificate** tab and select the certificate from the drop-down menu.

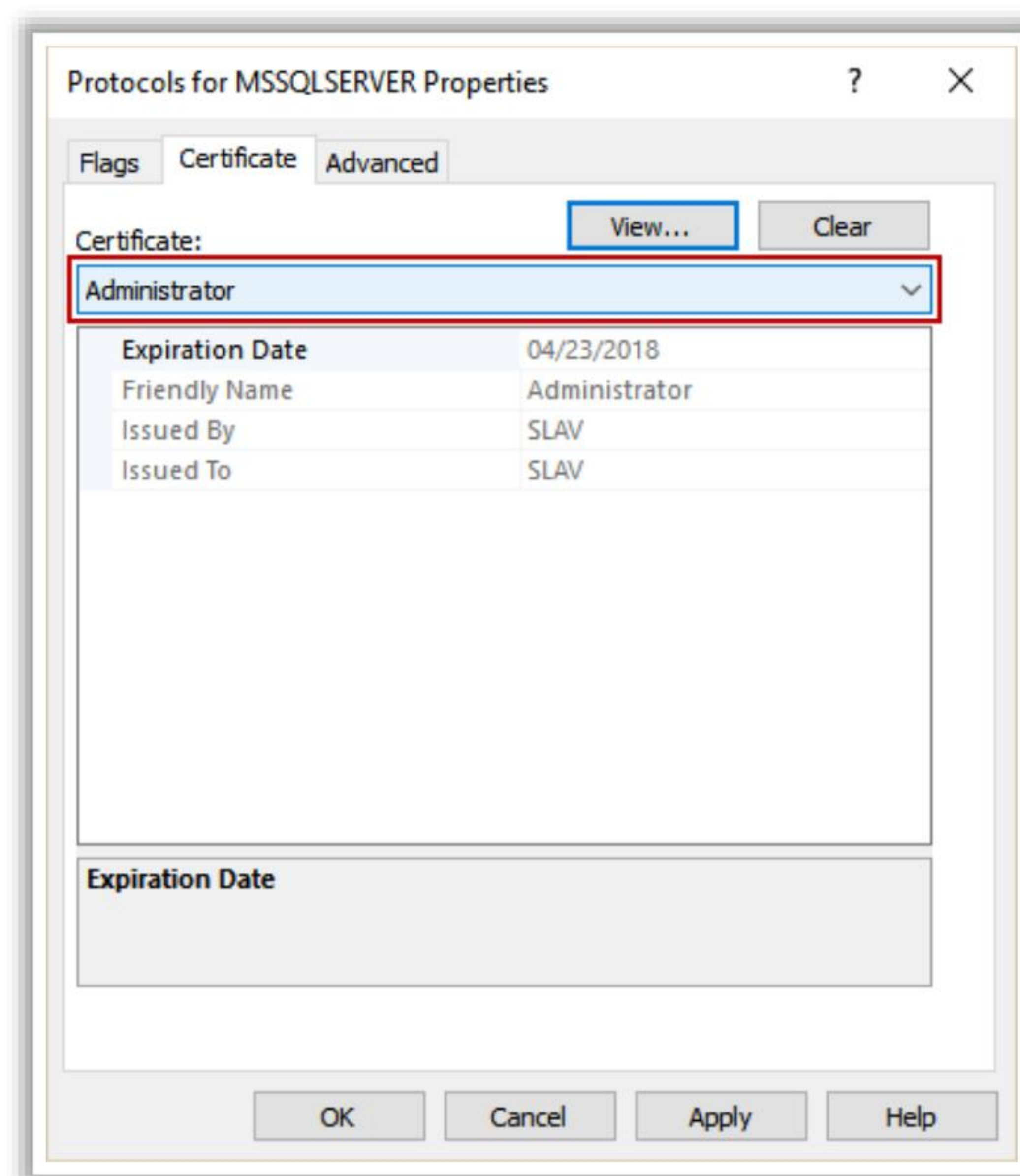


Figure 15.65: Selecting the Required certificate for SQL server instance

- Click **Flags** tab and enable **Force Encryption**.
- Click **Apply**.

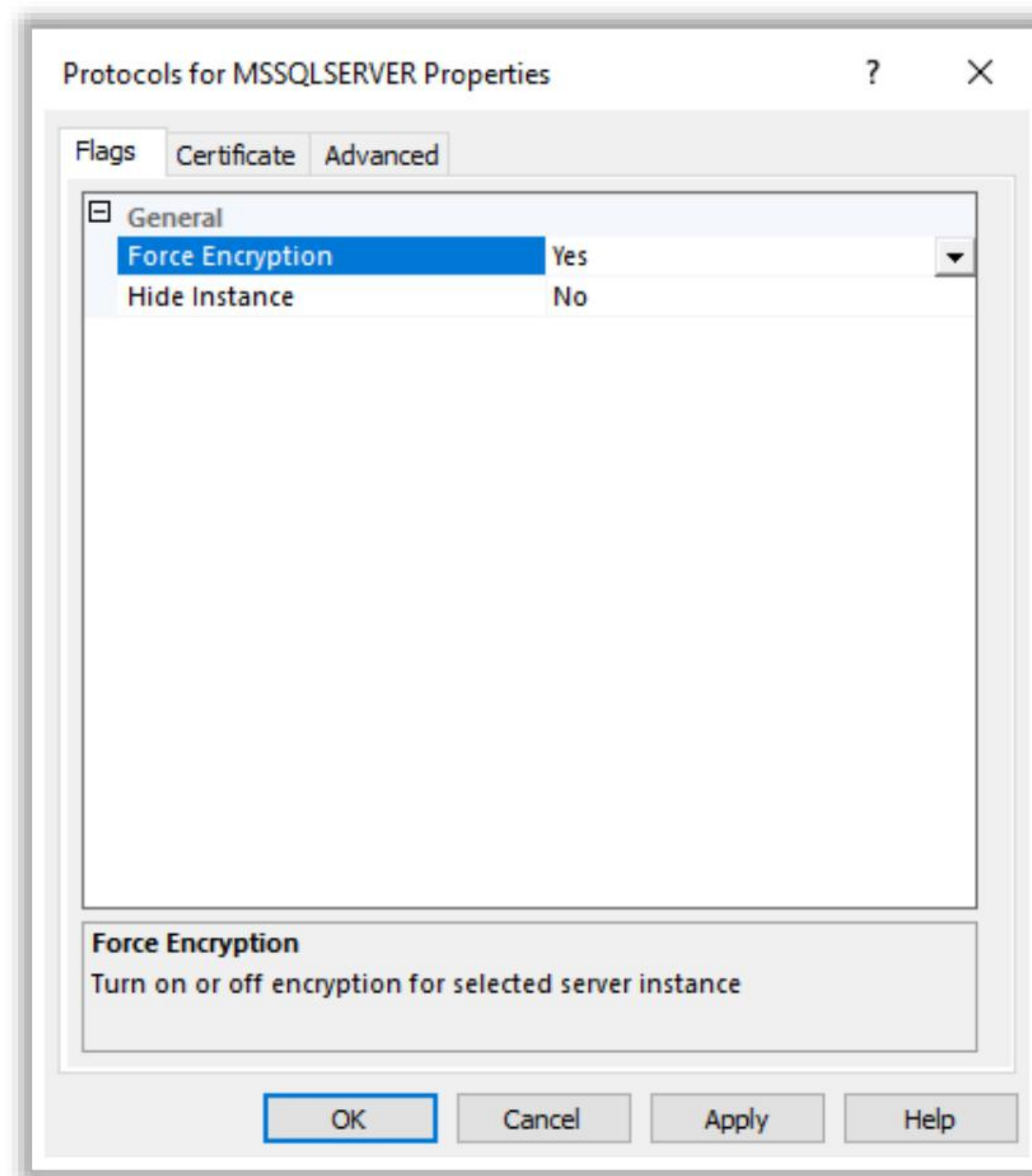


Figure 15.66: Turning on Force Encryption

- Navigate to SQL Server Services, and choose the running instance which was configured. Then, right-click and select **Restart** to apply the changes.

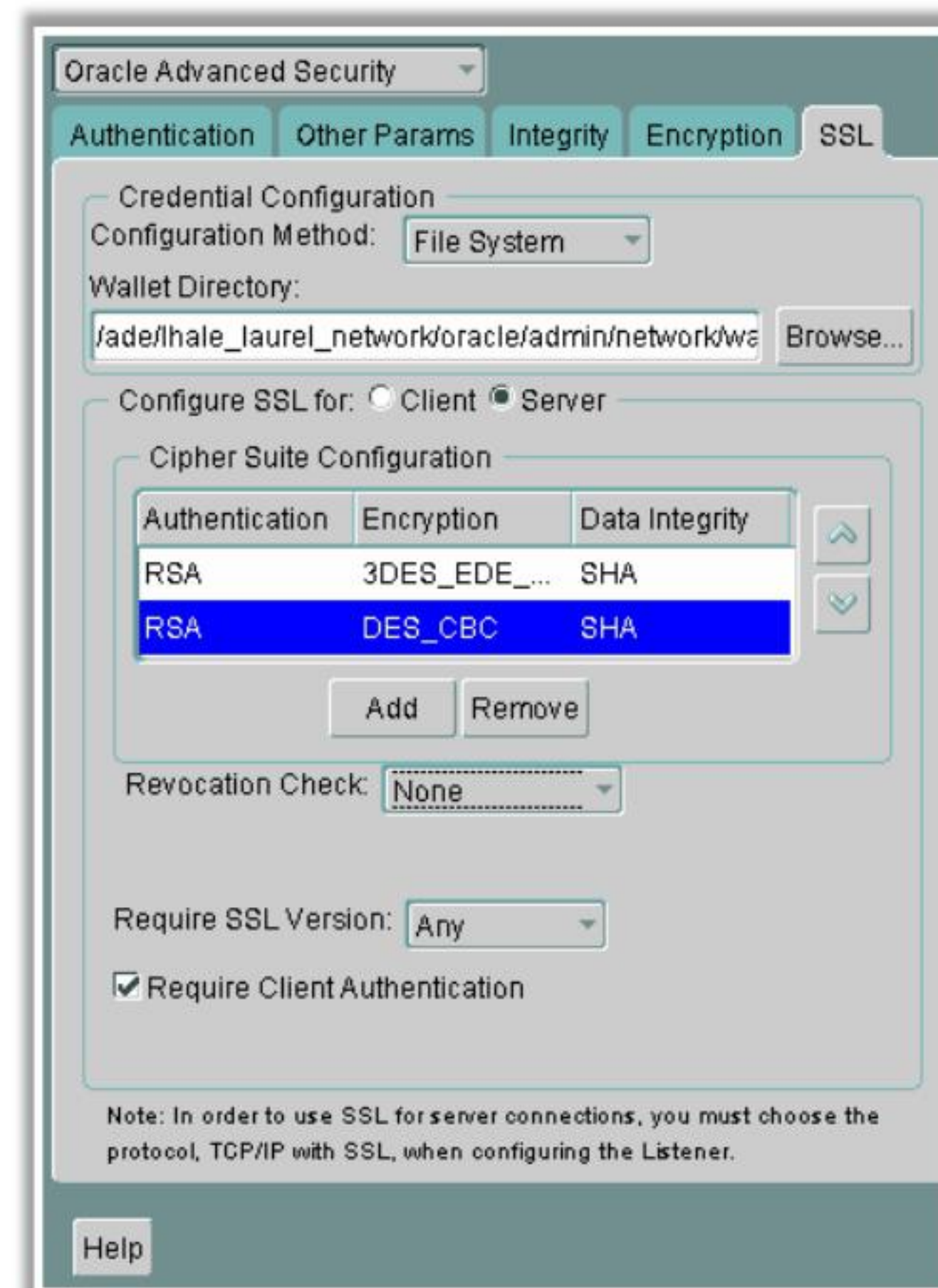
Enable SSL/TLS Encryption in Oracle Server

- ❑ Oracle Advanced Security option implements encryption, and provides **public key authentication** based on the SSL standard for:

- > Any client/ server to one or many Oracle servers
- > An Oracle server to any client

Components of SSL in an Oracle Environment

- **Certificate:** Ensures that the entity's identity is correct
- **Certificate Authority (CA):** A trusted third party which issues digital certificates that are verified for ownership before communicating with another entity
- **Wallet:** A store to manage keys, certificates, and trusted certificates required by SSL



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enable SSL/TLS Encryption in Oracle Server

Oracle Advanced Security option implements encryption, and provides public key authentication based on the SSL standard for

- Any client/ server to one or many Oracle servers.
- An Oracle server to any client.

Components of SSL in an Oracle Environment

- **Certificate:** Ensures that the entity's identity is correct, and the public key belongs to the entity.
- **CA:** A trusted third party which issues digital certificates that are verified for ownership before communicating with another entity.
- **Wallet:** A store to manage keys, certificates, and trusted certificates required by SSL.

Steps to Enable an Encrypted Connection with SQL Server

- **Step 1:** Install Oracle Advanced Security and the Oracle Wallet Manager.
- **Step 2:** Configure SSL on the client.
- **Step 3:** Configure SSL on the server.
- **Step 4:** Start the Oracle Wallet Manager.
- **Step 5:** Create a new wallet.
- **Step 6:** Install a certificate into the new wallet.
- **Step 7:** Add new trusted certificates.

- **Step 8:** Save changes to the wallet.
- **Step 9:** For single sign-on functionality, create an auto-login wallet.
- **Step 10:** Create a user identified globally through certificates on the Oracle server.

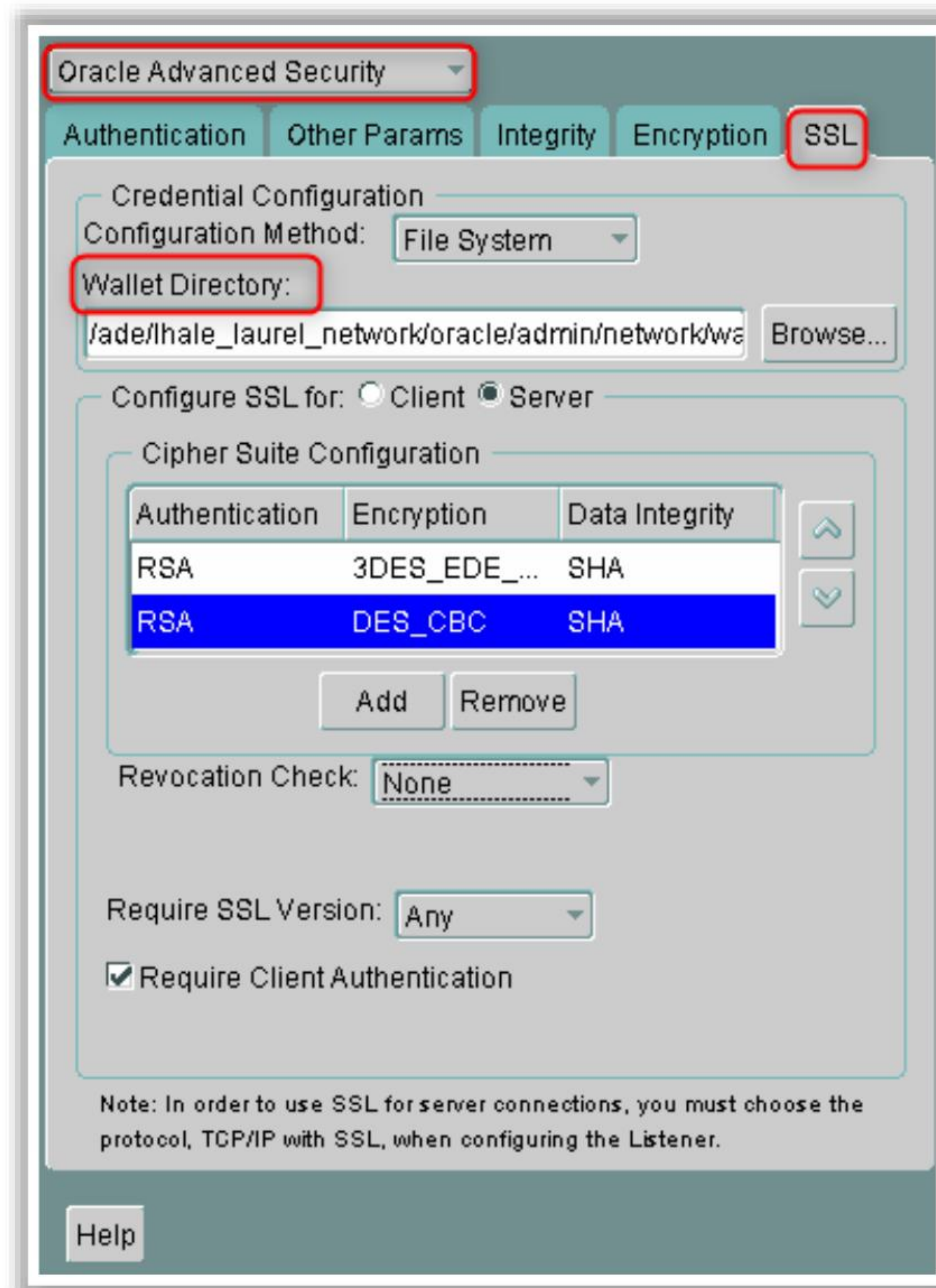


Figure 15.67: Screenshot of Enabling an Encrypted Connection with Oracle Server

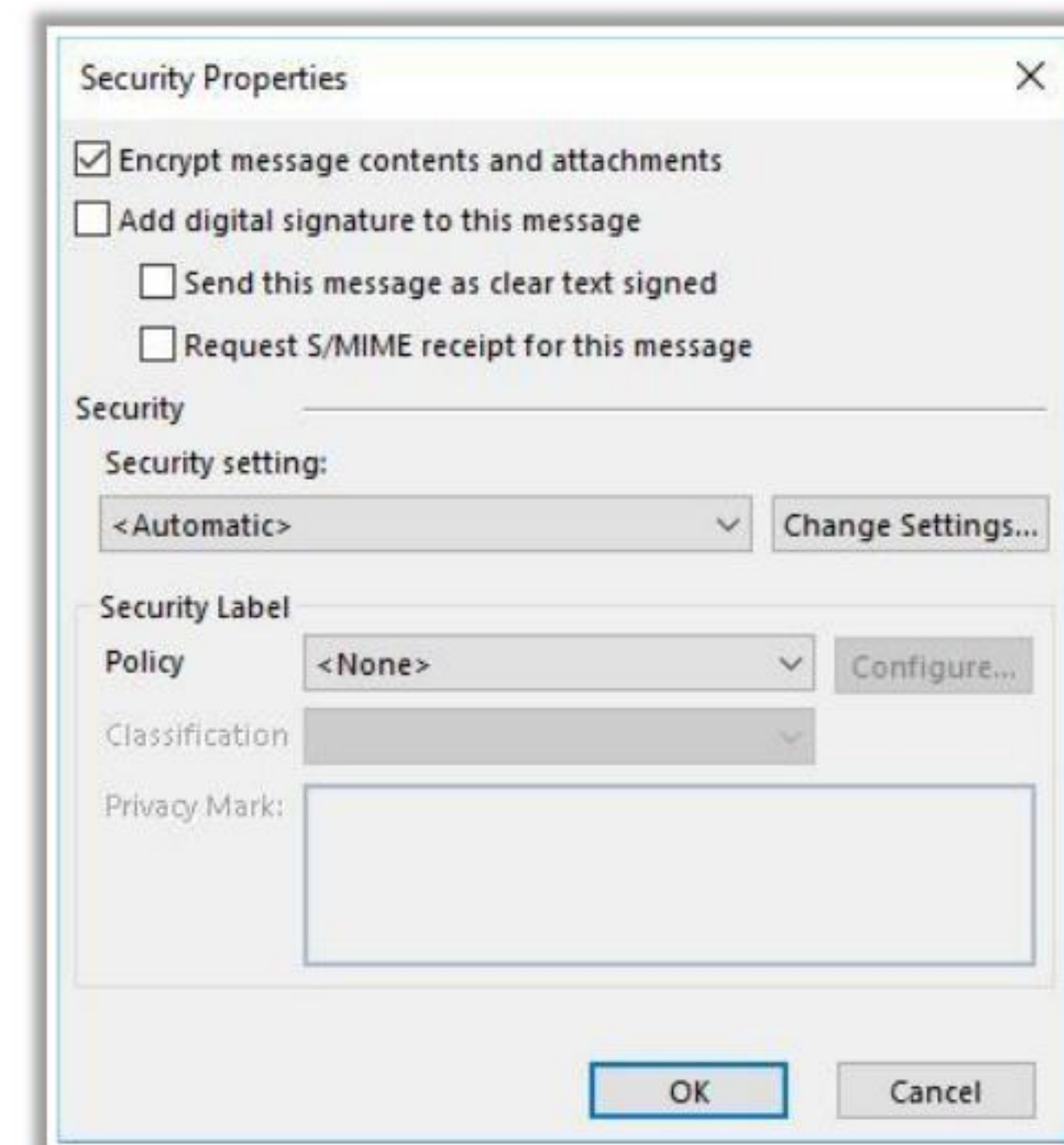
Email Encryption: MS Outlook

- ❑ By default, Outlook supports the **S/MIME standard**
- ❑ To implement S/MIME encryption, the sender and recipient must have a **mail application** that supports the S/MIME standard



Steps to Encrypt a Single Message

- 01** In the message you are composing, click the dialog box launcher in the **More Options** group on the **Options** tab
- 02** Click **Security Settings**, and then select the **Encrypt message contents and attachments** check box
- 03** Compose your message, and then click **Send**

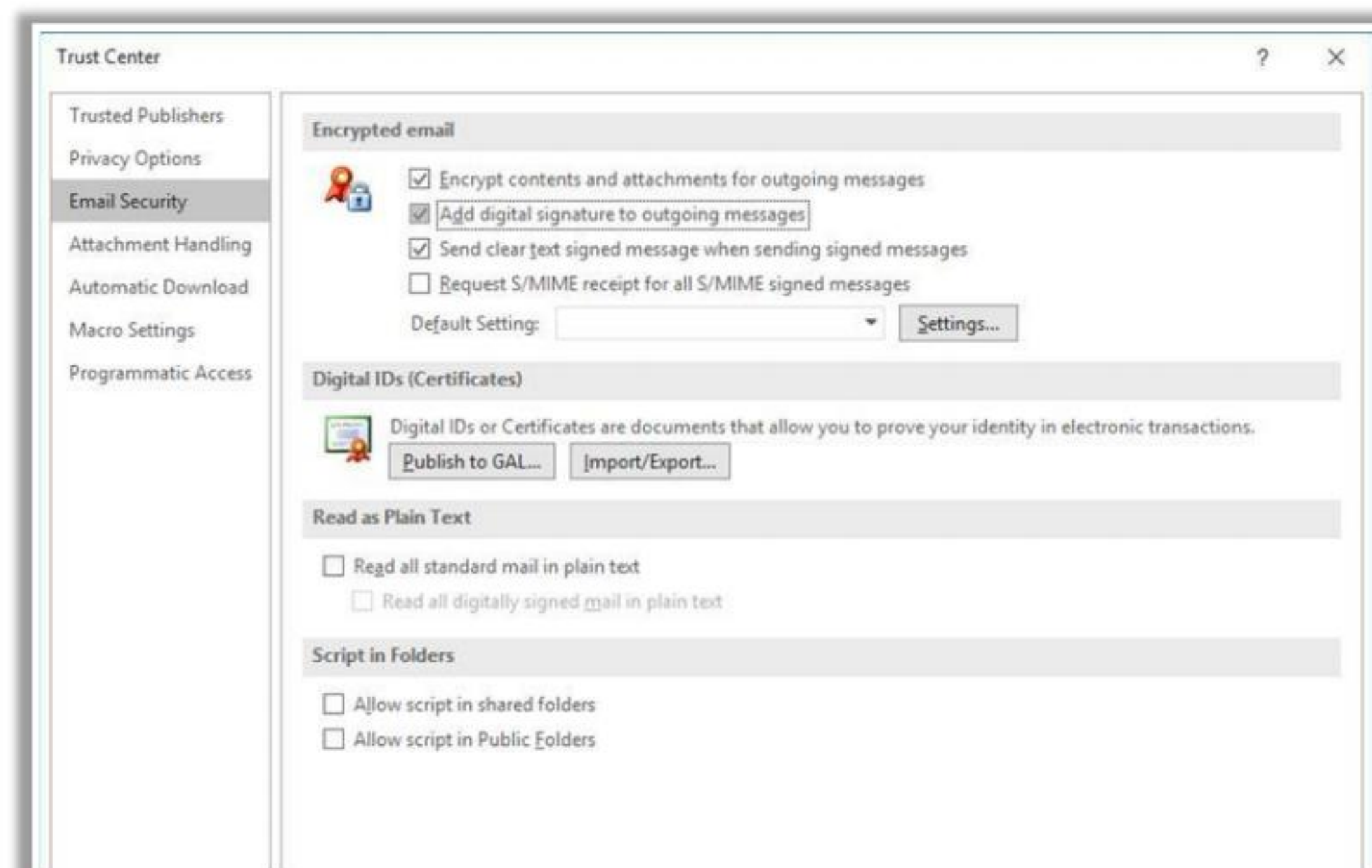


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Email Encryption: MS Outlook (Cont'd)

Steps to Encrypt all Outgoing Messages

- 1** Navigate to **File** tab, click **Options** → **Trust Center** → **Trust Center Settings**
- 2** In **E-mail Security** tab, select the **Encrypt contents and attachments for outgoing messages** check box under **Encrypted e-mail**
- 3** Click **Settings...**, to choose a specific certificate to use for encryption



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Email Encryption: MS Outlook

MS Outlook facilitates the encryption of an email message. Only a recipient who has the secret key that matches the public key can decrypt the email message.

Outlook supports the following encryption options:

- **Secure/multipurpose Internet mail extensions (S/MIME) encryption**

The sender and recipient of the mail should have a mail application that supports the S/MIME standard to use this encryption option.

Steps to Encrypt a Single Message:

- In the message you are composing, click the dialog box launcher in the **More Options** group on the **Options** tab
- Click **Security Settings**, and then select the **Encrypt message contents and attachments** check box

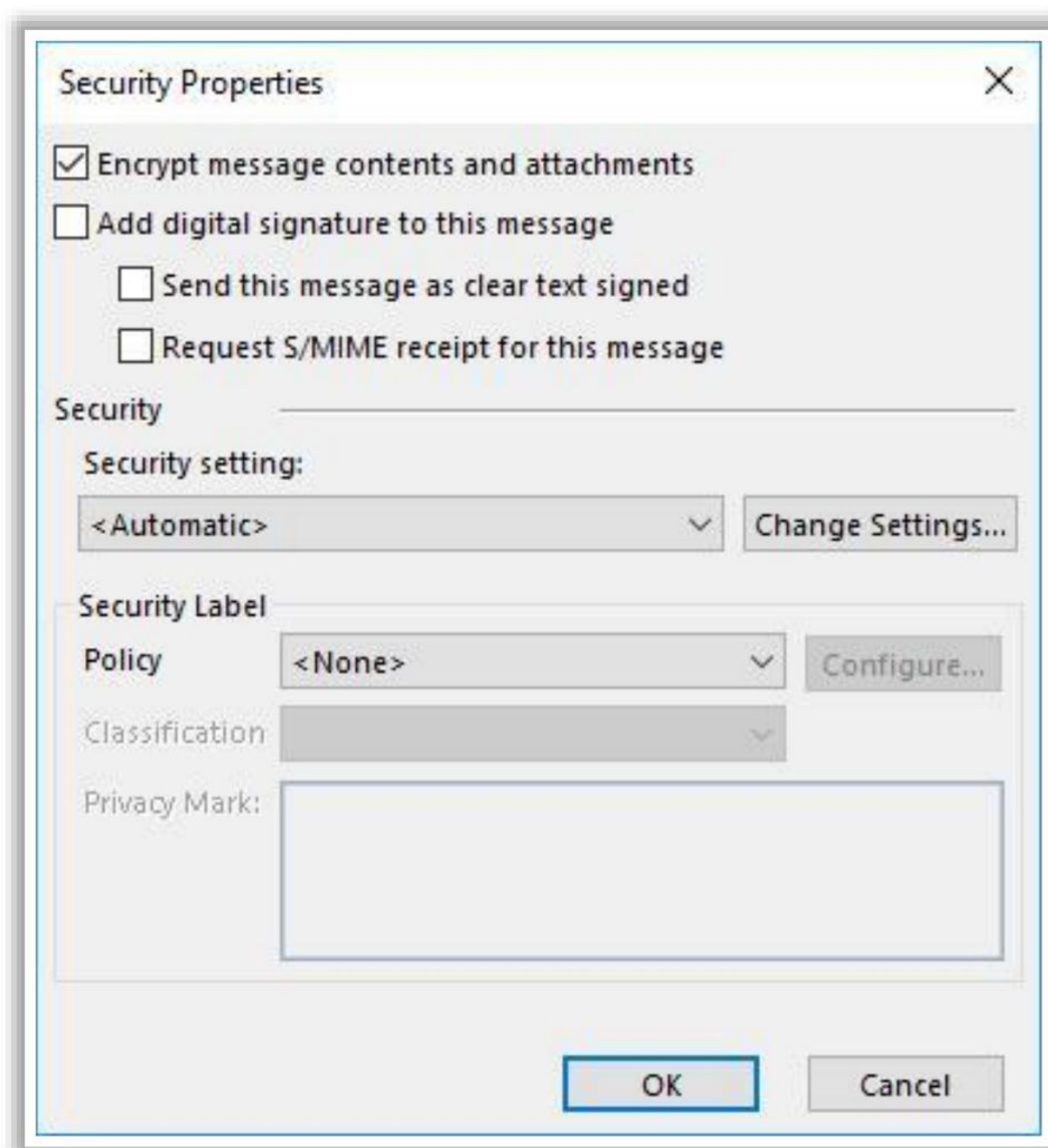


Figure 15.68: Screenshot of MS Outlook Security Properties

- Compose your message, and then click **Send**

Steps to encrypt with S/MIME:

Adding a certificate to the keychain on your computer is necessary. After setting up the signing certificate on your computer, configure it in Outlook.

- Under the **File** menu, Go to **Options > Trust Center > Trust Center Settings**.
- Select **Email Security** from the left pane.
- Select **Settings** under **Encrypted email**.

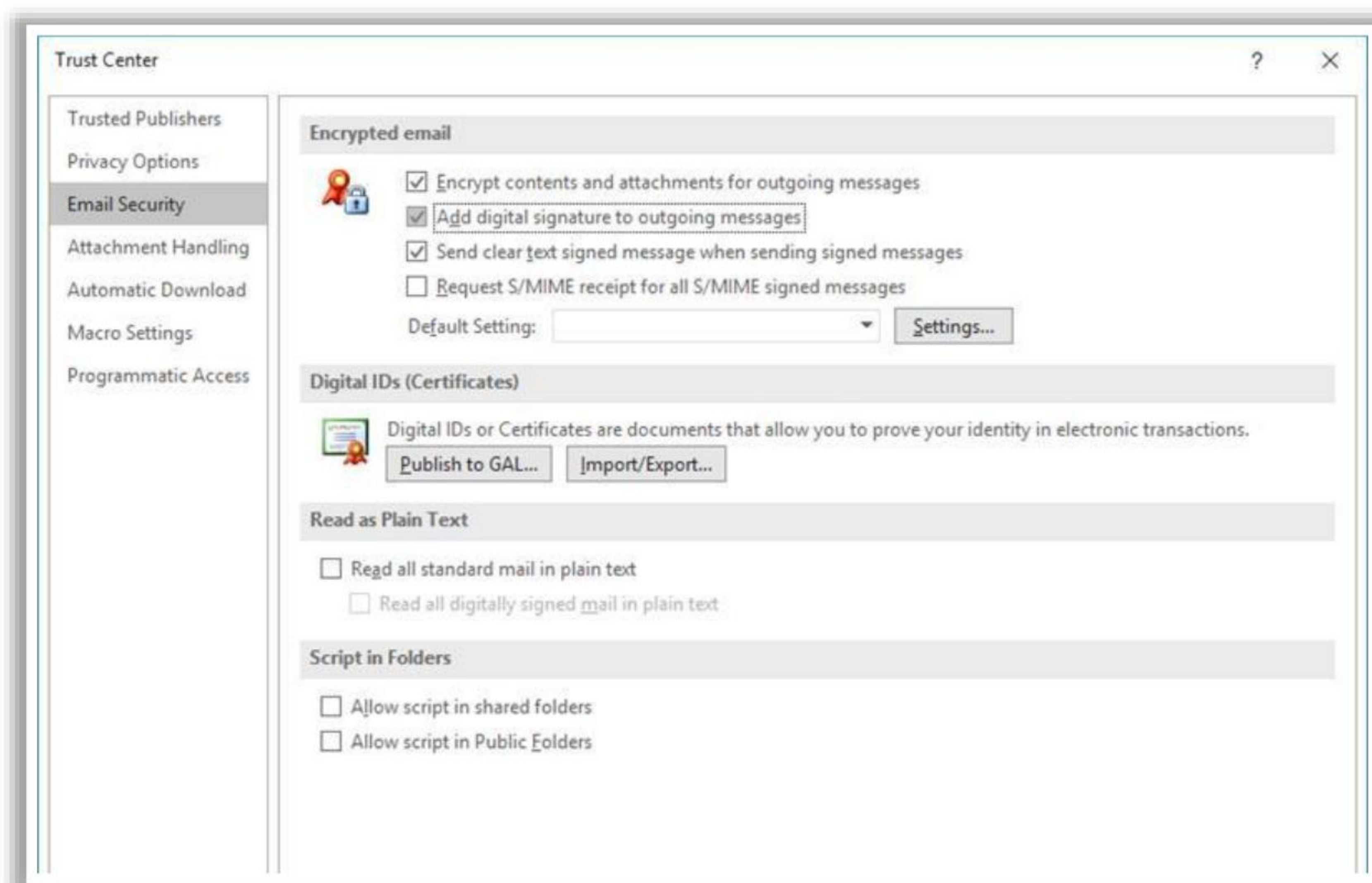


Figure 15.69: Trust Center Window

- Under **Certificates and Algorithms**, click **Choose** and select the **S/MIME** certificate.

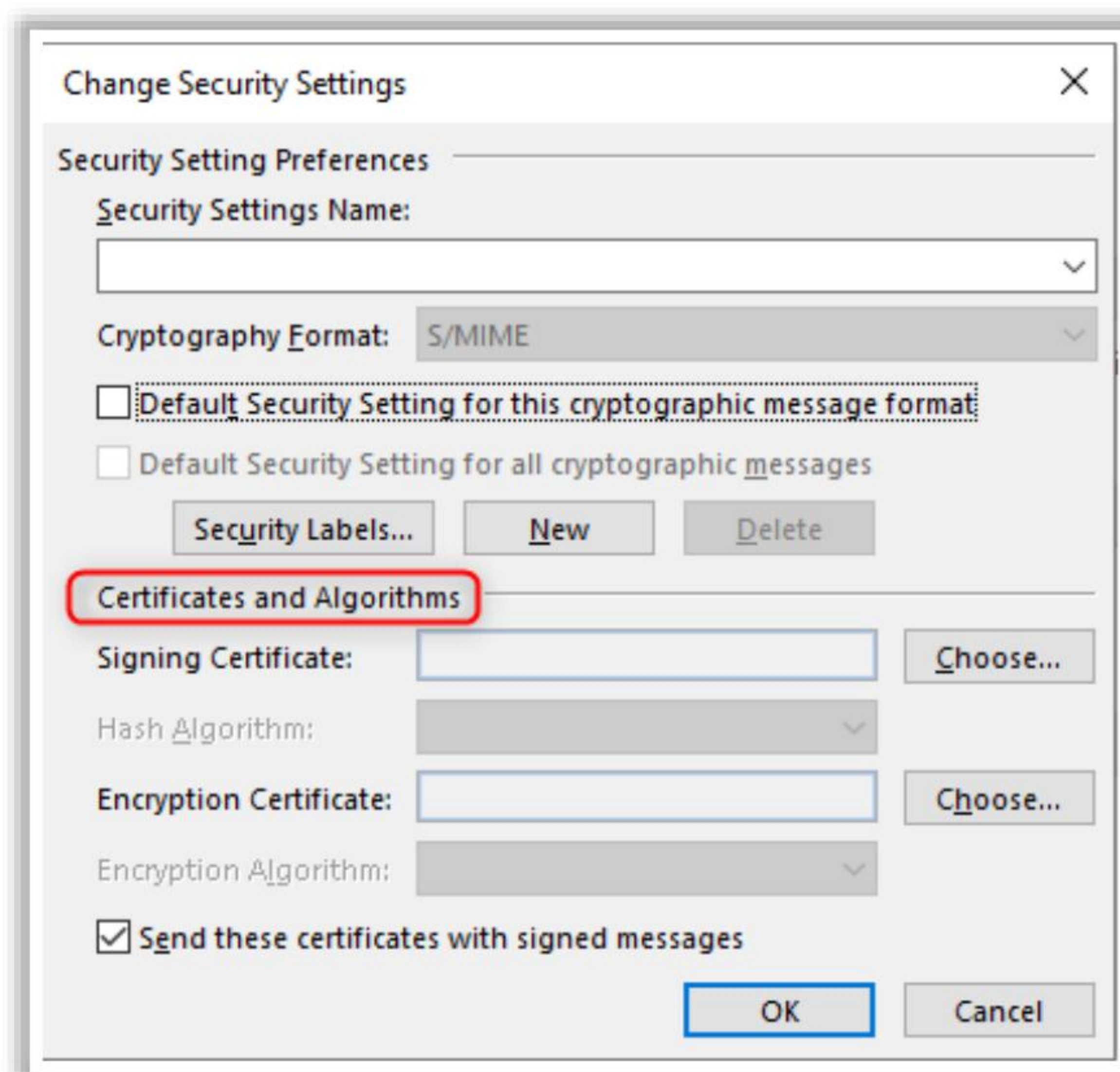


Figure 15.70: Change Security Settings Window

- Select **OK**.
- If you are an Office insider with Office 365 subscription, choose **Options**, select **Encrypt**, and pick **Encrypt with S/MIME** option from the drop-down menu in the email message.

- See **Encrypt with S/MIME** if you have an **S/MIME** certificate installed on your system.
- For **Outlook 2019** and **Outlook 2016**, select **Options**, and then select **Permissions** in the email message.
- Finish composing the email and click **Send**.
- **Office 365 Message Encryption (Information Rights Management)**

The sender should have Office 365 Message Encryption that comes with the Office 365 Enterprise E3 license to use this encryption option.

Steps to encrypt with Office 365 Message Encryption:

- If you are an Office 365 subscriber, select **Options>Encrypt** and pick the encryption that has the restrictions you want to enforce (**Encrypt-Only** or **Do Not Forward**) in the email message.

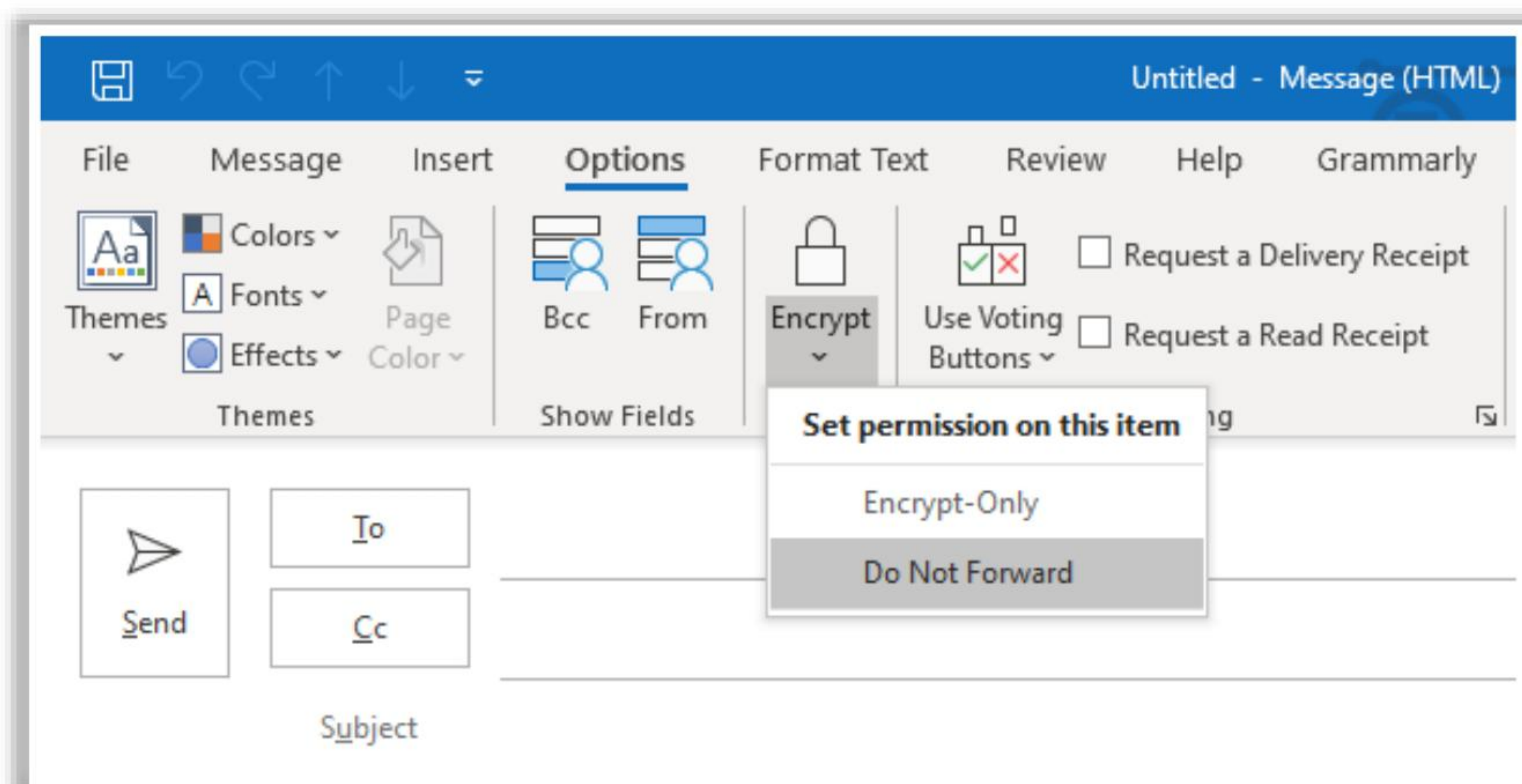


Figure 15.71: Encrypt with Office 365 Message Encryption

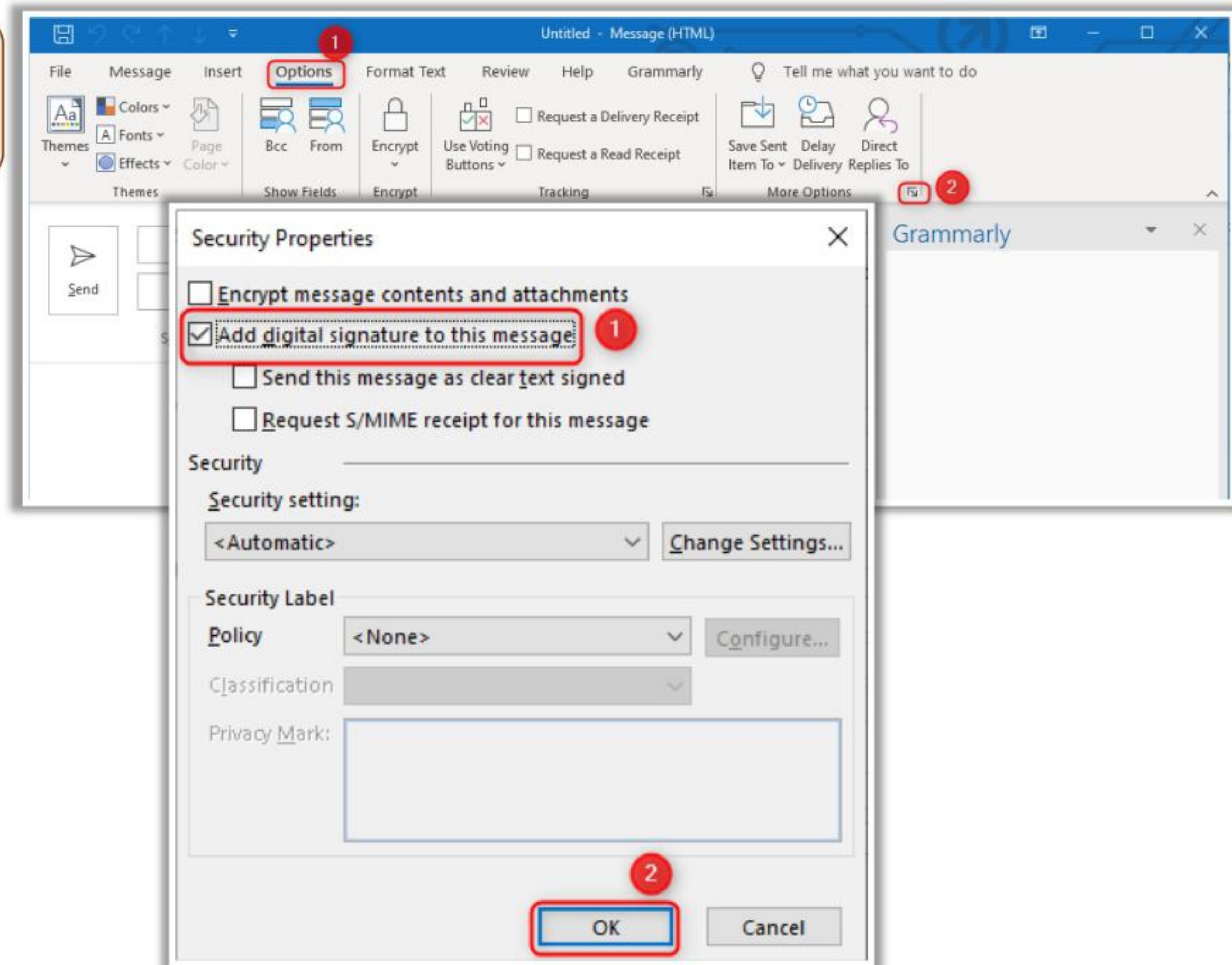
- For **Outlook 2019** and **2016**, select **Options > Permissions** and pick the encryption option that has the restrictions you want to enforce, such as **Do Not Forward**, in the email message.

Email Encryption: MS Outlook using Digital Certificate

- ☐ Encrypting the email transfer with **SSL/TLS** to protect the privacy of an email message

Steps to encrypt email message in MS Outlook using digital certificate

- 1** Get a digital certificate/digital ID
- 2** Send a digitally-signed message
- 3** Encrypt a message with MS Outlook
- 4** Encrypt all outgoing Outlook messages



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Email Encryption: MS Outlook using Digital Certificate

Encrypting the email transfer with SSL/TLS to protect the privacy of an email message. To encrypt and send an email message in MS Outlook, follow the steps given below:

Step 1: Get a digital certificate/digital ID

You can get a digital certificate/Digital ID by following the steps listed below:

- Navigate to **File Tab → Options → Trust Center**.
- Click **Trust Center Settings...** under **Microsoft Outlook Trust Center**.

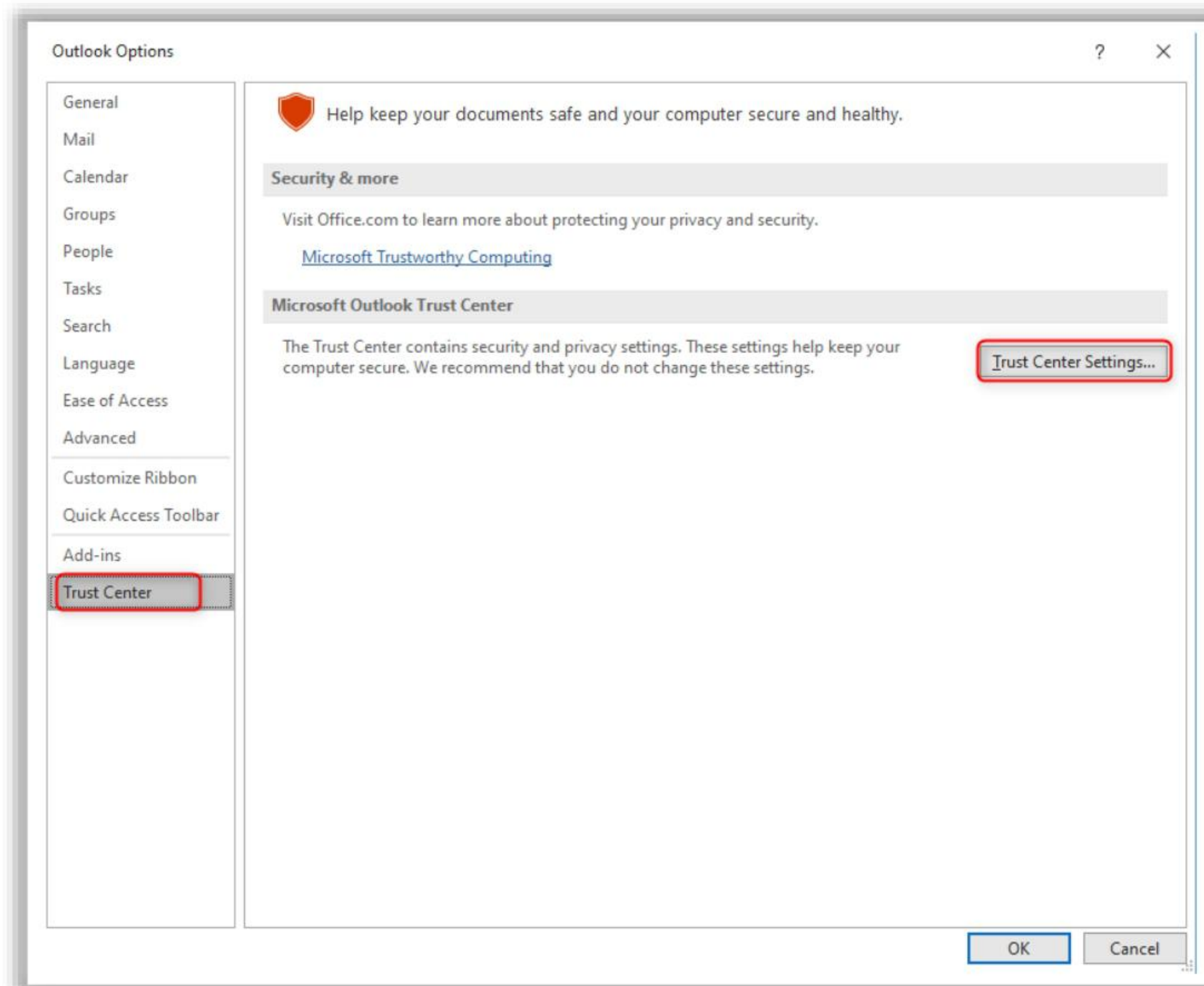


Figure 15.72: Outlook Options Window

- Select **Email Security** from the left pane, and then click **Import/Export...** under **Digital IDs (Certificates)**.

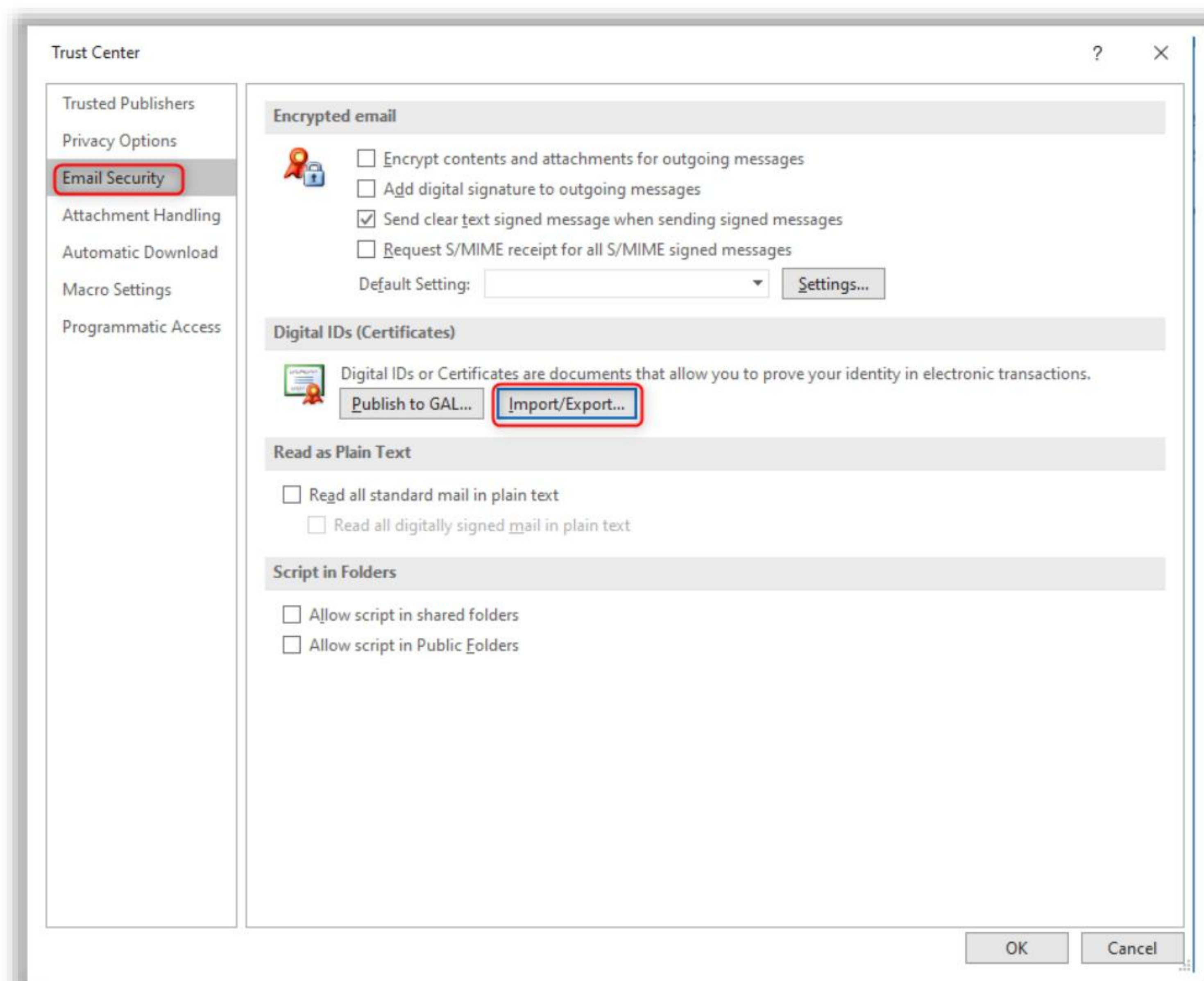


Figure 15.73: Selecting Email Security Option

- Select **Import existing Digital ID from a file** and click **Browse to Import File** by providing **Password**.

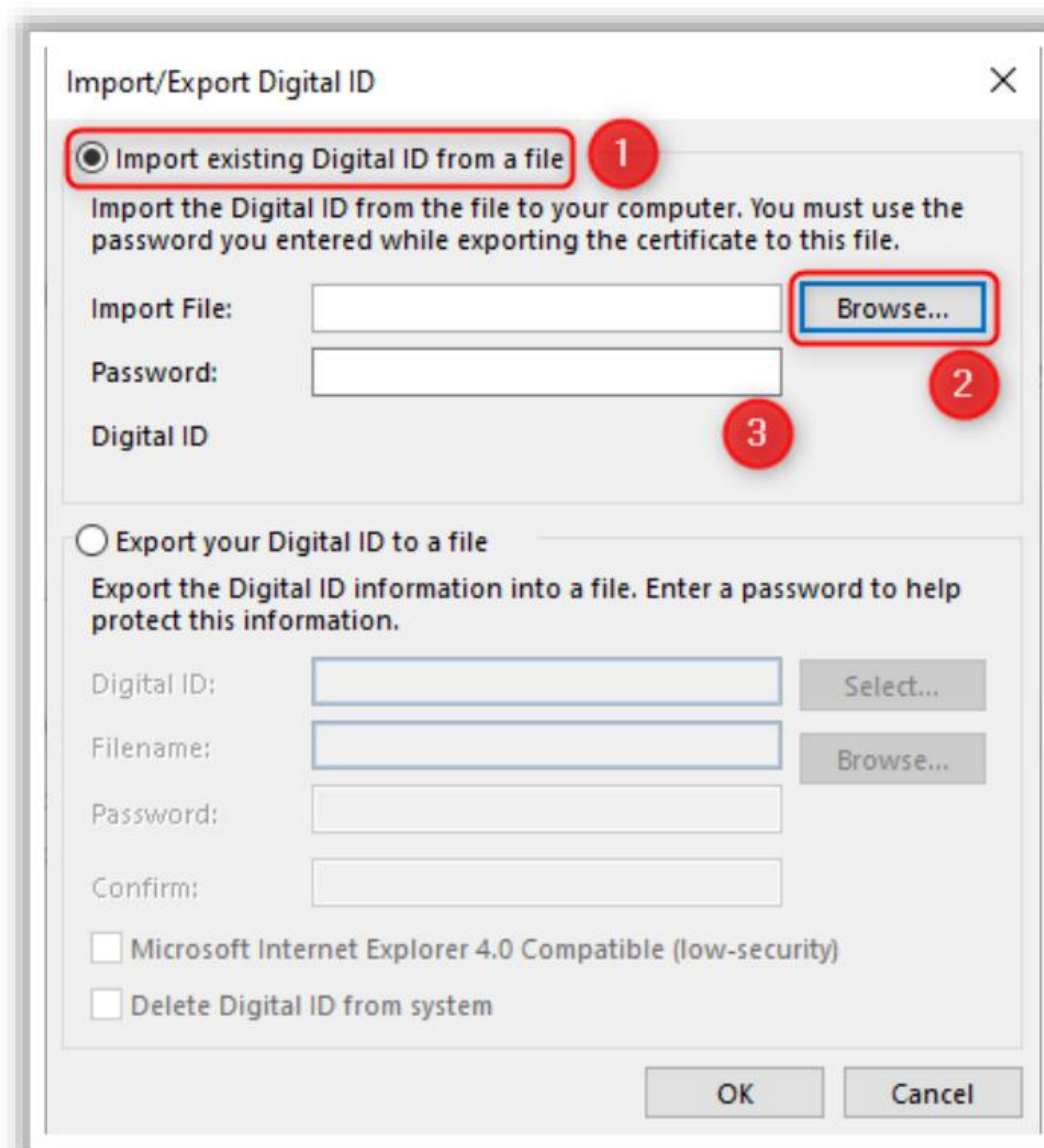


Figure 15.74: Import or Export Digital ID

- Choose an independent CA such as Comodo, DigiCert, GlobalSign, IdenTrust, etc. to get the digital certificate (digital ID), and follow the instructions.
- Once you get a digital certificate, follow the instructions to install it.

Step 2: Send a digitally-signed message

After getting the digital certificate, send the digitally-signed message to the person to whom you wish to send the encrypted message.

- Compose a new message in Outlook.
- Navigate to **Options** → **More Options** icon.

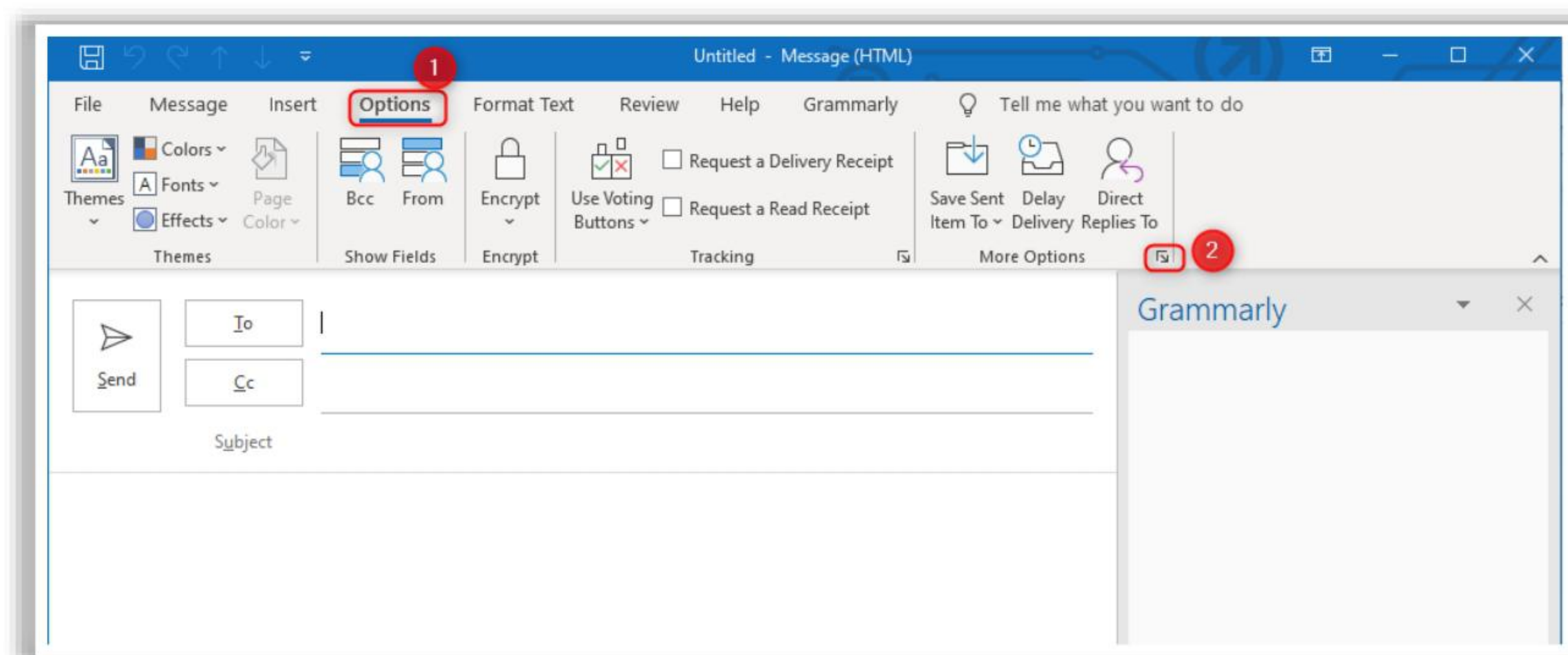


Figure 15.75: Selecting Options Tab in a New Message

- In the **Properties** window, click **Security Settings....**

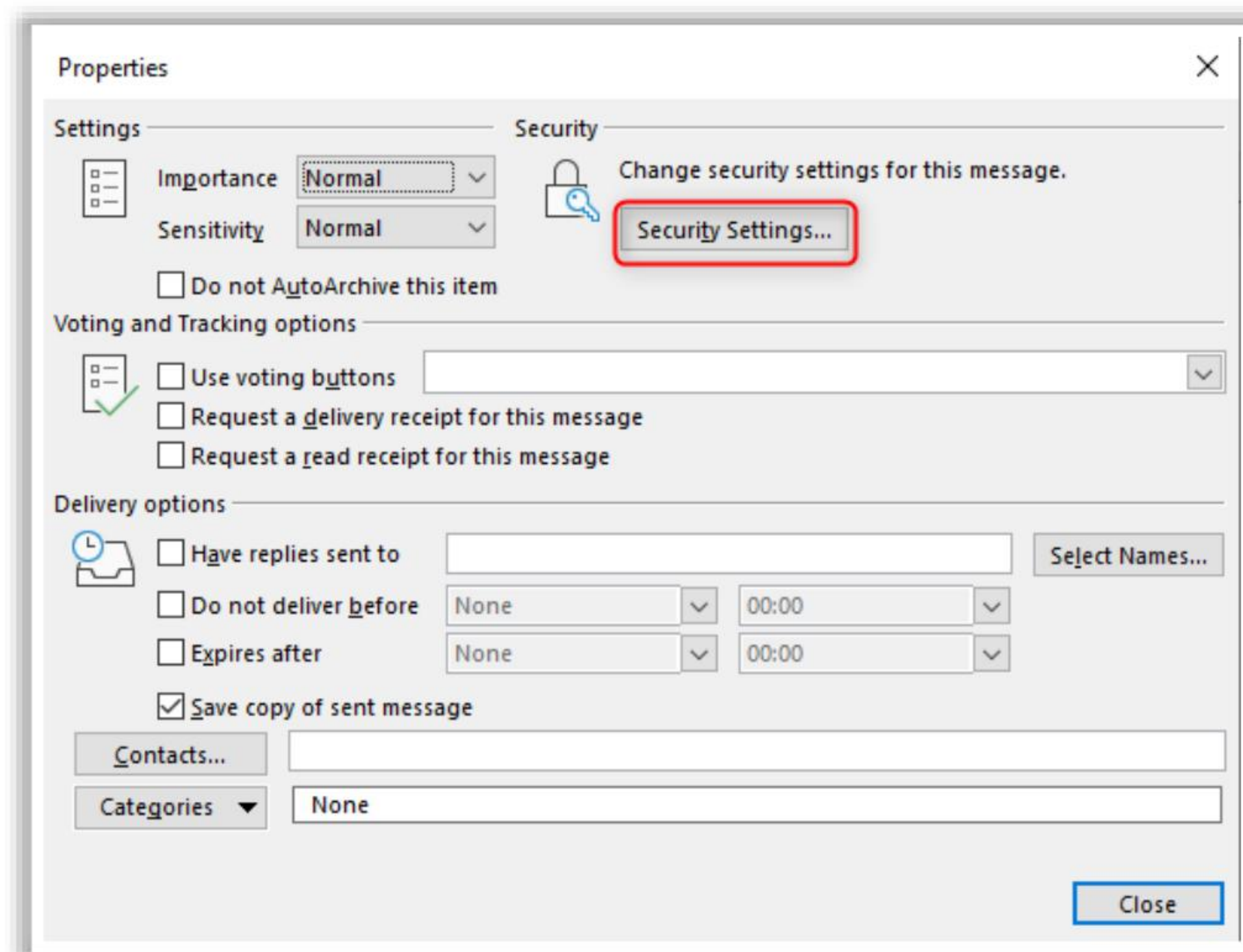


Figure 15.76: Properties Window

- In the **Security Properties** window, check the **Add digital signature to this message** checkbox and click **OK**.

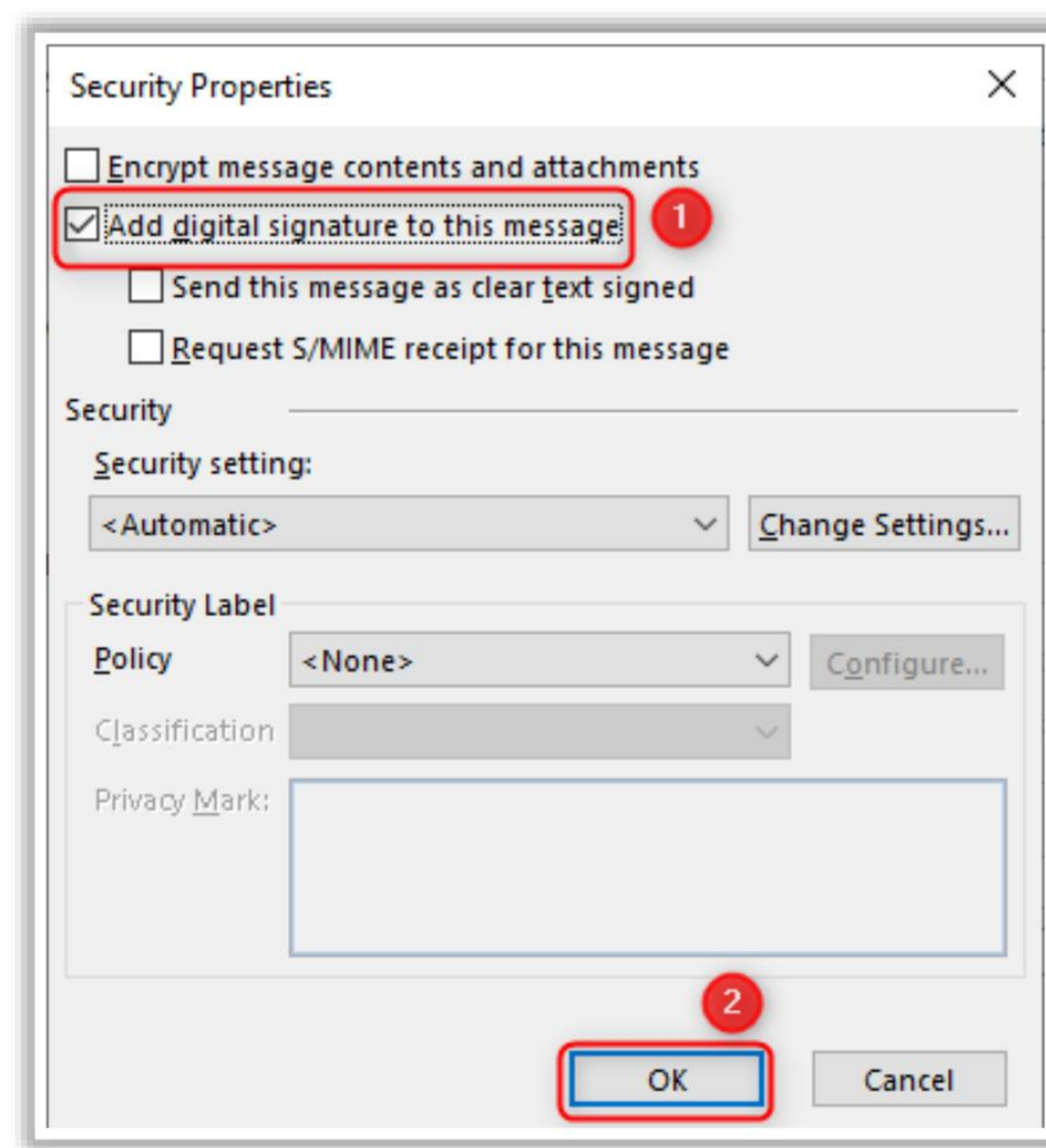


Figure 15.77: Selecting Digital Signature for the Message

- Click **Close** on the **Properties** window.
- Now, a new option will appear in the **Permission** Group: the **Sign Message** button.
- Click **Sign Message** button, and send a message to the recipient.
- Request the recipient to reply to the message with a digitally-signed message of their own.

Step 3: Encrypt a message with MS Outlook

- Compose a message you wish to encrypt in Outlook.
- Click the **File** tab, and then the **Options** tab.

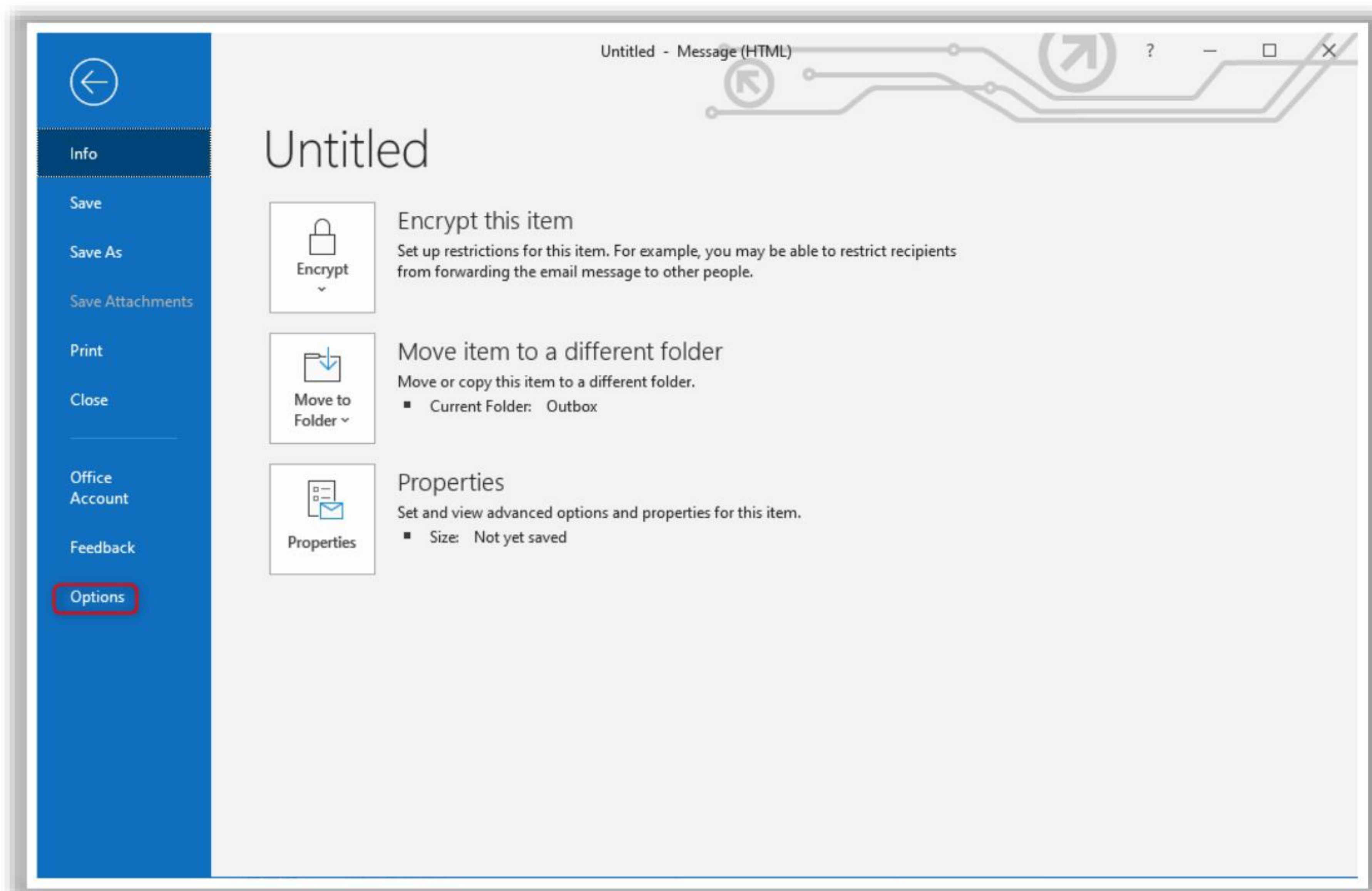


Figure 15.78: Selecting Options Tab

- The **Properties** dialog box will appear.
- Click the **Security Settings** button.

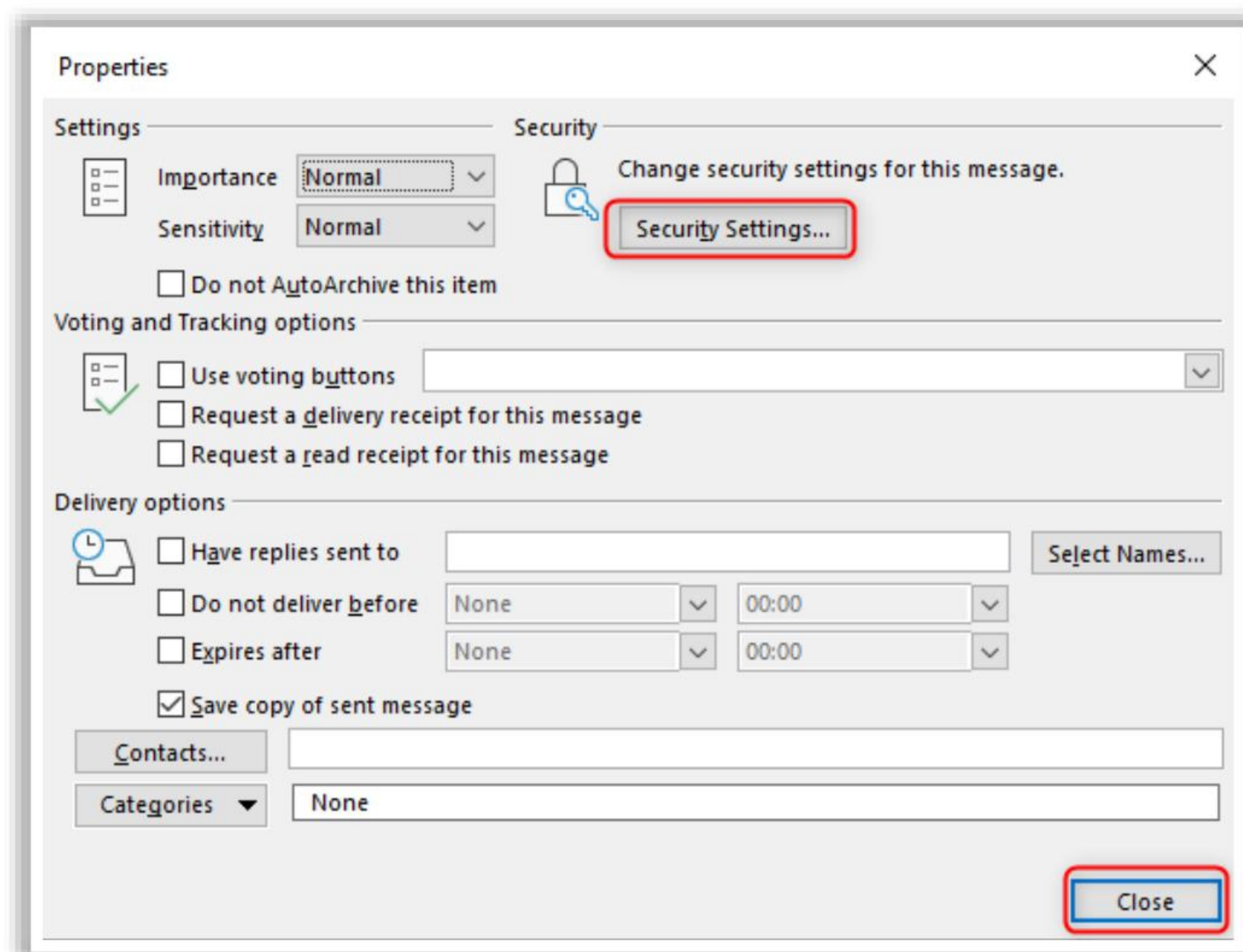


Figure 15.79: Selecting Security Settings in Properties Dialog box

- In the **Security Properties** dialog box, check the **Encrypt message contents and attachments** box and click **OK**.

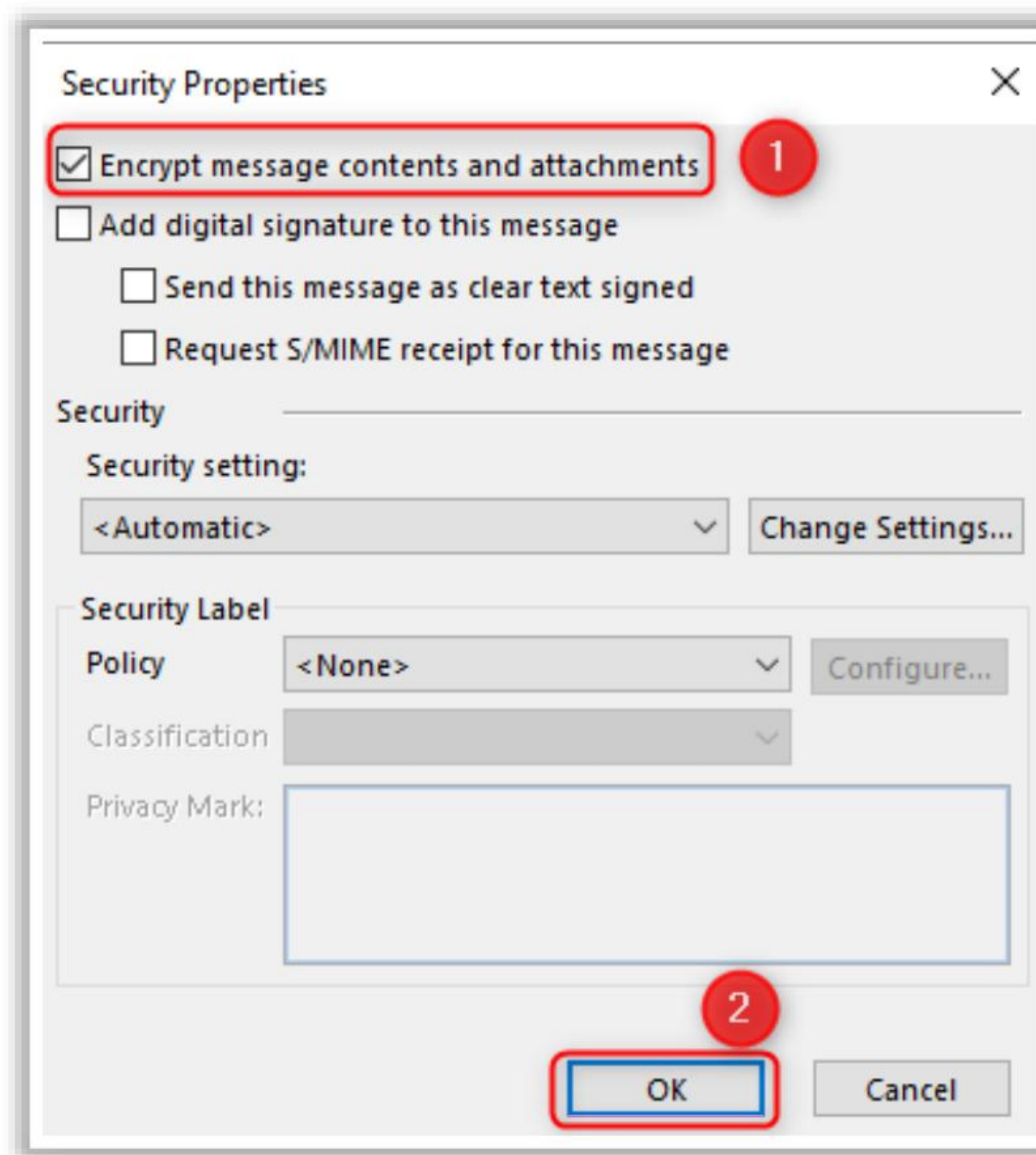


Figure 15.80: Choosing Encrypt Message Contents and Attachments in Security Properties Window

- Click **Close** on the **Properties** dialog box.
- Send the encrypted message.

Step 4: Encrypting all outgoing Outlook messages

Microsoft email account allows the encryption of all outgoing Outlook email messages. Steps to encrypt all outgoing messages are as follows:

- Navigate to **File** tab -> **Options** -> **Trust Center**.
- Click **Trust Center Settings** under **Microsoft Outlook Trust Center**.
- Select **Email Security** from the left pane, and then check the box for **Encrypt contents and attachments for outgoing messages**.

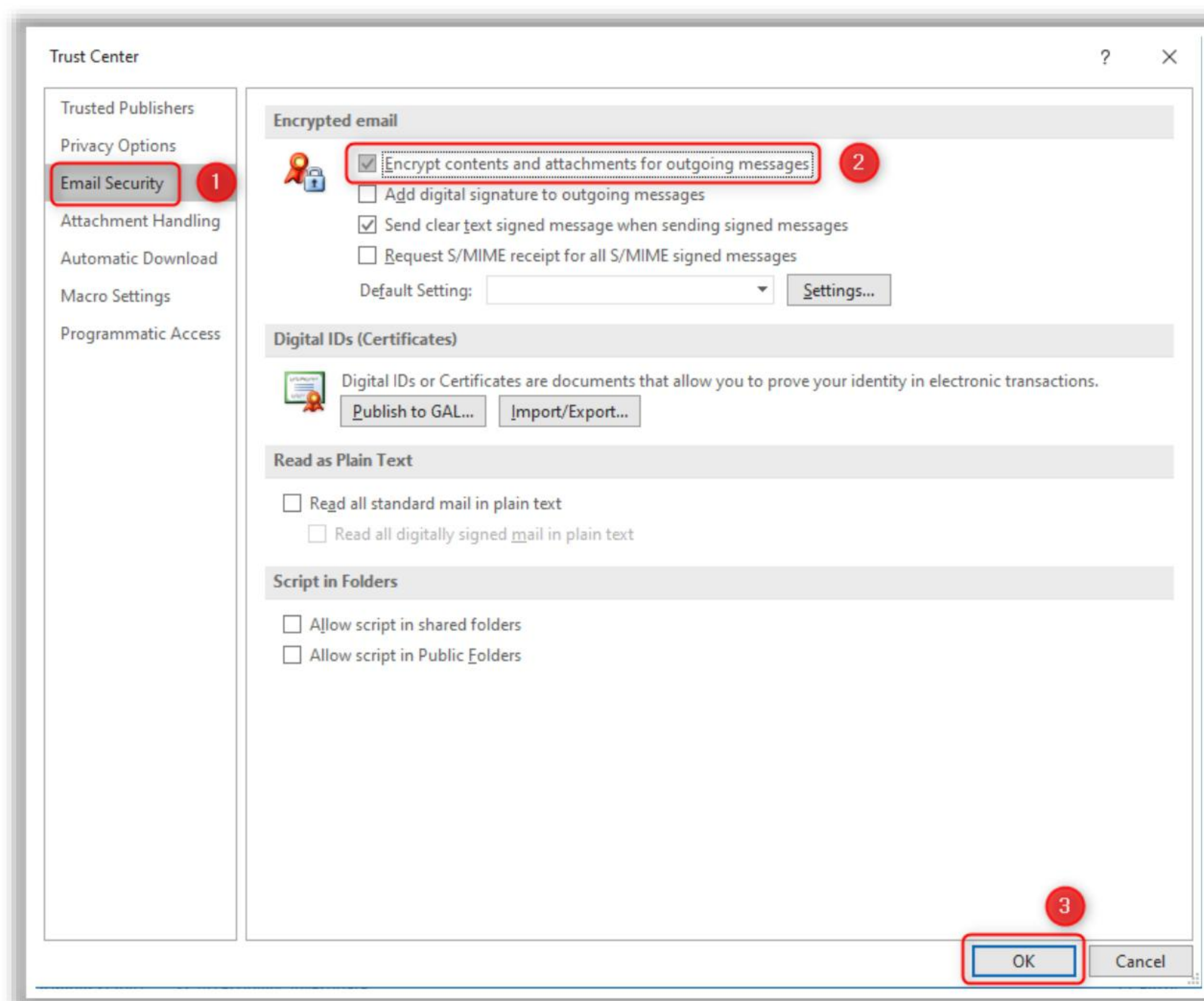


Figure 15.81: Encrypting All Outgoing Outlook messages

- Click **OK**, and then again click **OK**.

Email Encryption: Gmail

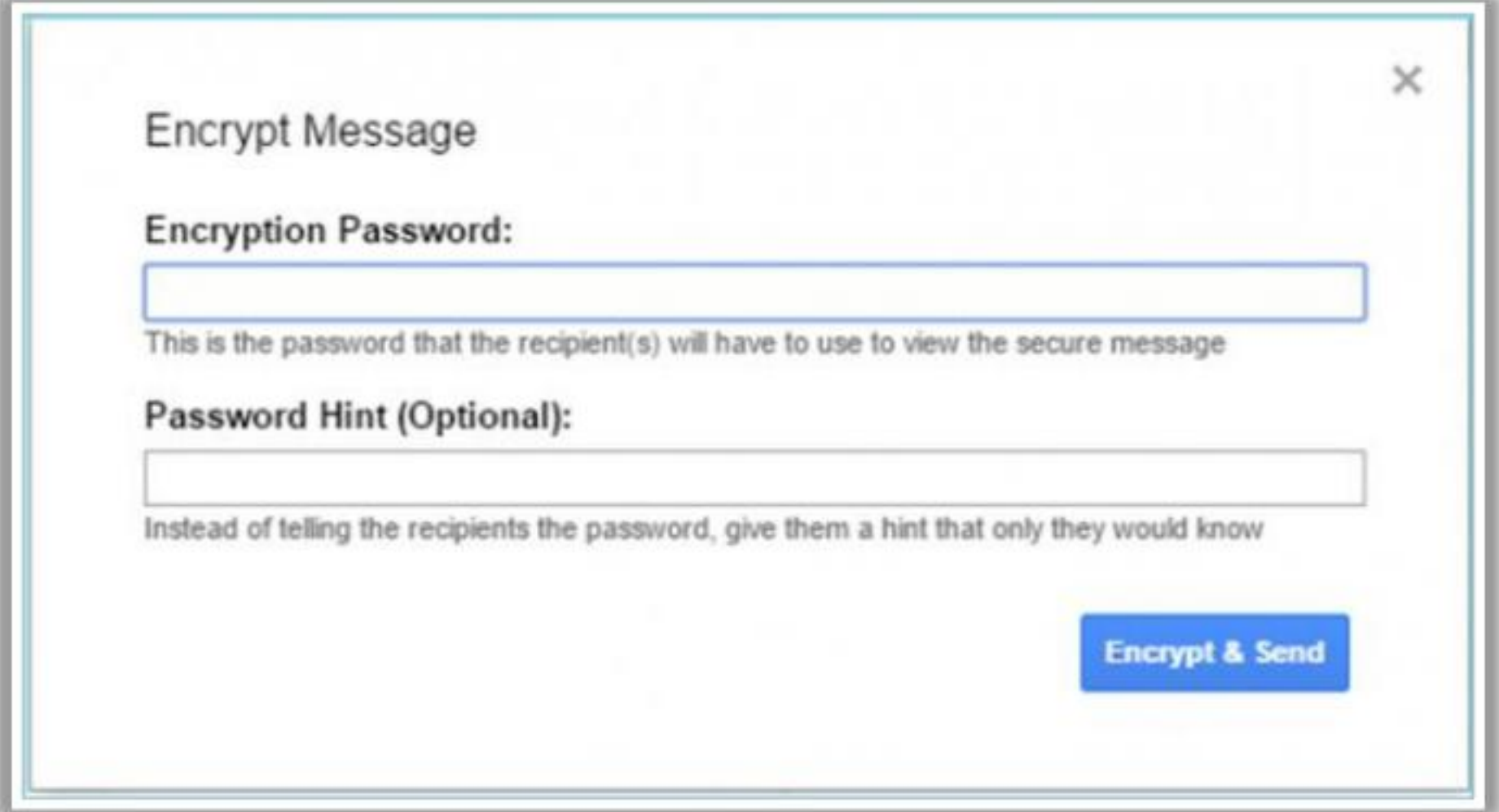
❑ Gmail supports **S/MIME** encryption, along with **SecureGmail** and **Google Chrome extension** to encrypt email messages

Steps to Encrypt an Email Message Using S/MIME

- ➡ Enable S/MIME, and share a key with each other
- ➡ Compose a message, and click the **lock** icon located at the right of the recipient
- ➡ Send the email message

Steps to Encrypt Message using SecureGmail

- ➡ Install SecureGmail from the Chrome Web Store
- ➡ Click the lock button to compose the encrypted email
- ➡ Click the **Send Encrypted** button
- ➡ Provide an Encryption Password and a Password Hint to decrypt the email at the recipient side
- ➡ Click the Encrypt & Send button
- ➡ Manually share the password with the recipient





Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Email Encryption: Gmail

Gmail, the email service offered by Google, is used in many organizations to send and receive emails. Google uses the standard method of Gmail TLS encryption. All messages going through Gmail be encrypted only when both sender's and receiver's email services support TLS (mostly all major mail providers support TLS). Besides offering the basic level of encryption, Gmail also supports S/MIME (secure/multipurpose Internet mail extensions) encryption. SecureGmail (Chrome extension), Firefox, etc. are some other ways of encryption in Gmail. However, these options are available only for paid G Suite Enterprise and G Suite Education accounts, and not for the free Gmail accounts.

Steps to Encrypt an Email Message Using S/MIME

S/MIME encrypts data in transit. Both the sender and receiver have to enable S/MIME for it to work. After enabling S/MIME, they share “keys” to identify each other. Now, S/MIME can be used to send encrypted email messages in the following manner:

- Compose a message.
- Add the name of the recipient to the **To** field.
- Click the **lock** icon located to the right of the recipient.
- Click on **View Details** if you want to change S/MIME settings or view the recipient's encryption level.
- Send the email message.

The S/MIME encryption level is displayed in three colors.

- **Green:** Email message is encrypted with S/MIME encryption.

- **Gray:** Email message is encrypted with TLS encryption.
- **Red:** No encryption. Avoid sending personal information until you have securely encrypted an email.

Steps to Encrypt Messages Using SecureGmail

SecureGmail is a Google Chrome extension by Streak. You can install it from the Chrome Web Store. Once this is done, to the Gmail page to activate it. It is activated if a **lock** is displayed next to the **Compose** button. Now, follow the steps given below to encrypt the email message.

- Click the **lock** button to compose the encrypted email.

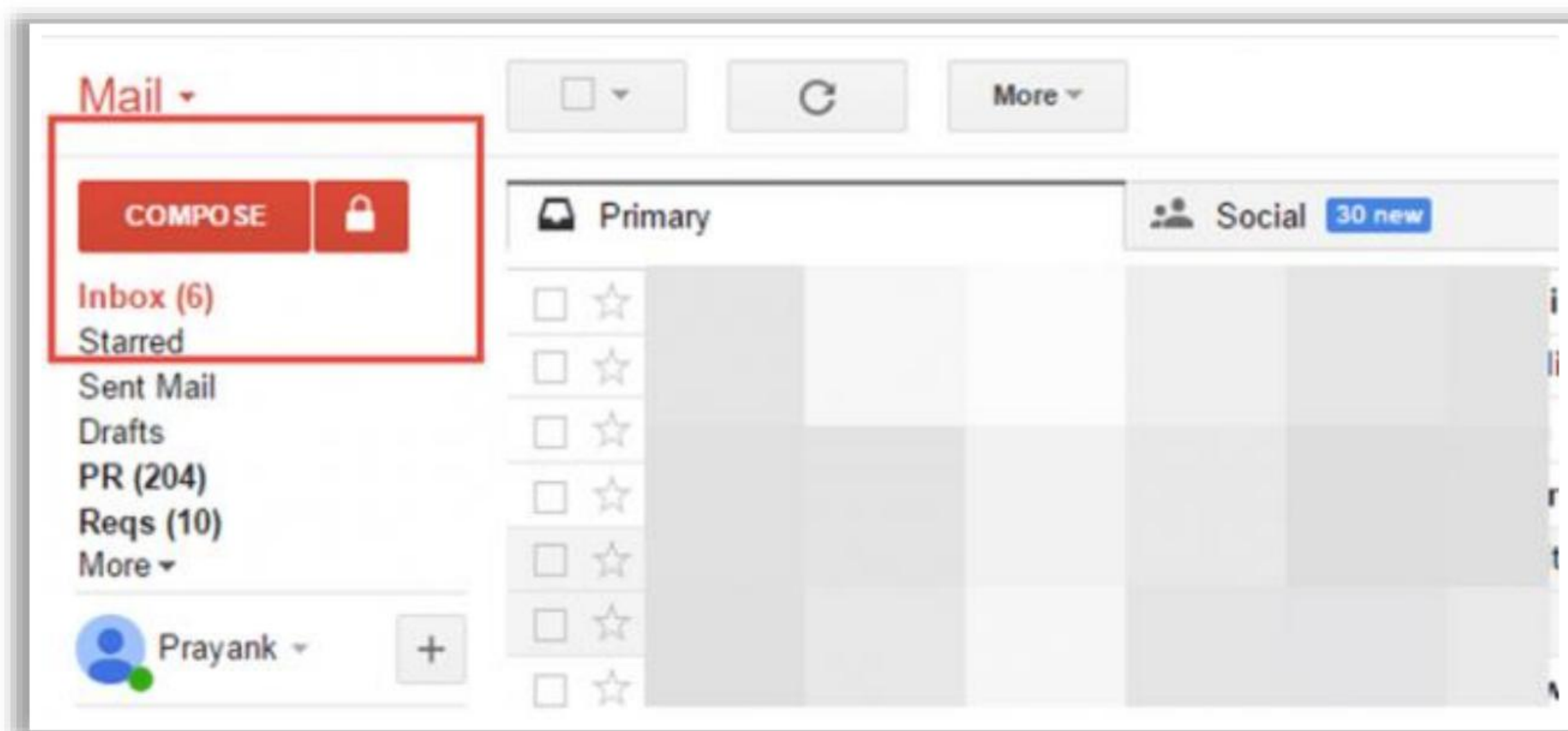


Figure 15.82: Email Composition

- Notice two changes: The header will display **Secured** with a lock symbol, and **Send** button will change to **Send Encrypted**.

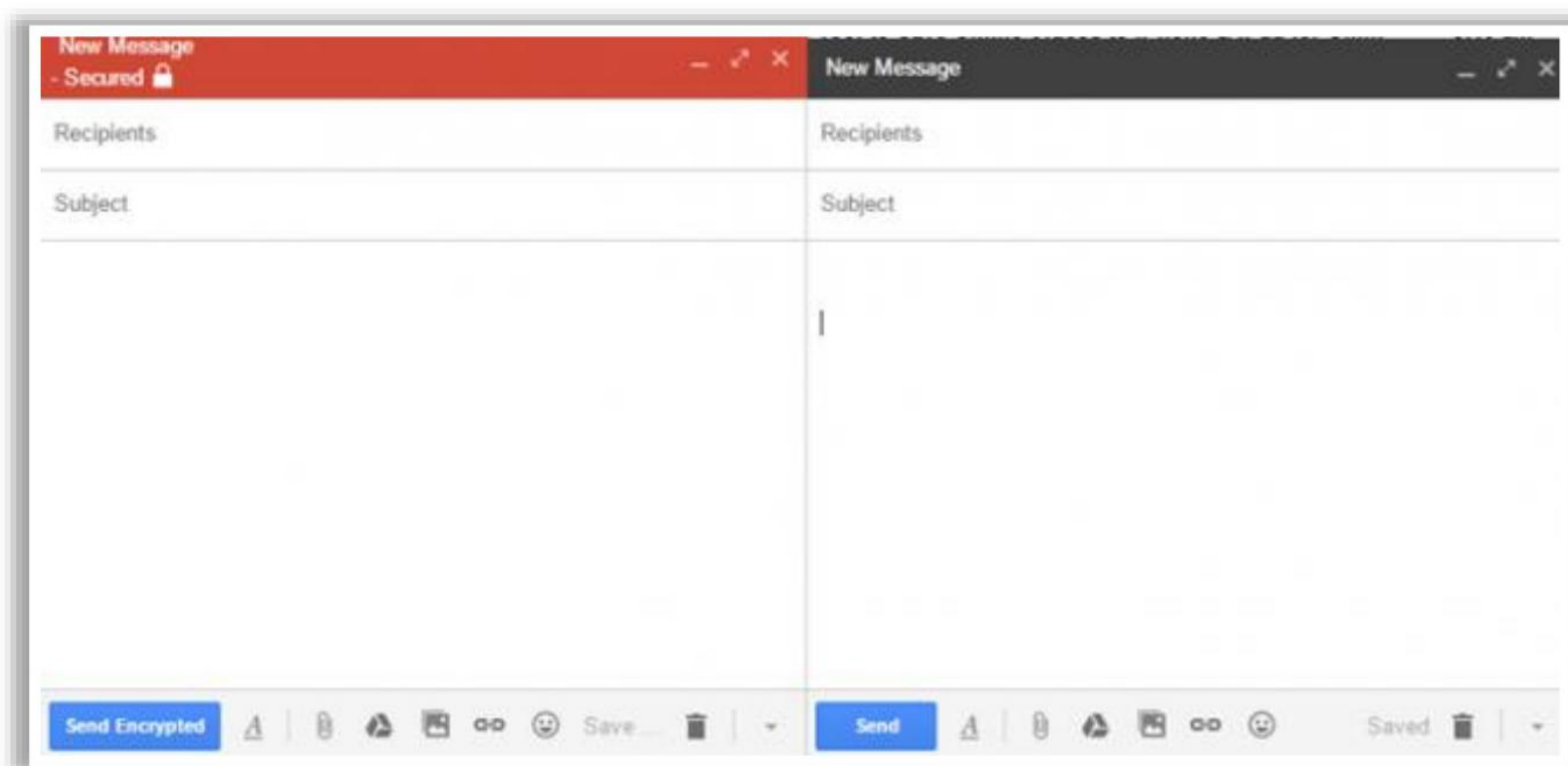


Figure 15.83: New Message - Secured

- Click the **Send Encrypted** button after composing the email.
- Provide an **Encryption Password** and a **Password Hint** to decrypt the email at the recipient side.

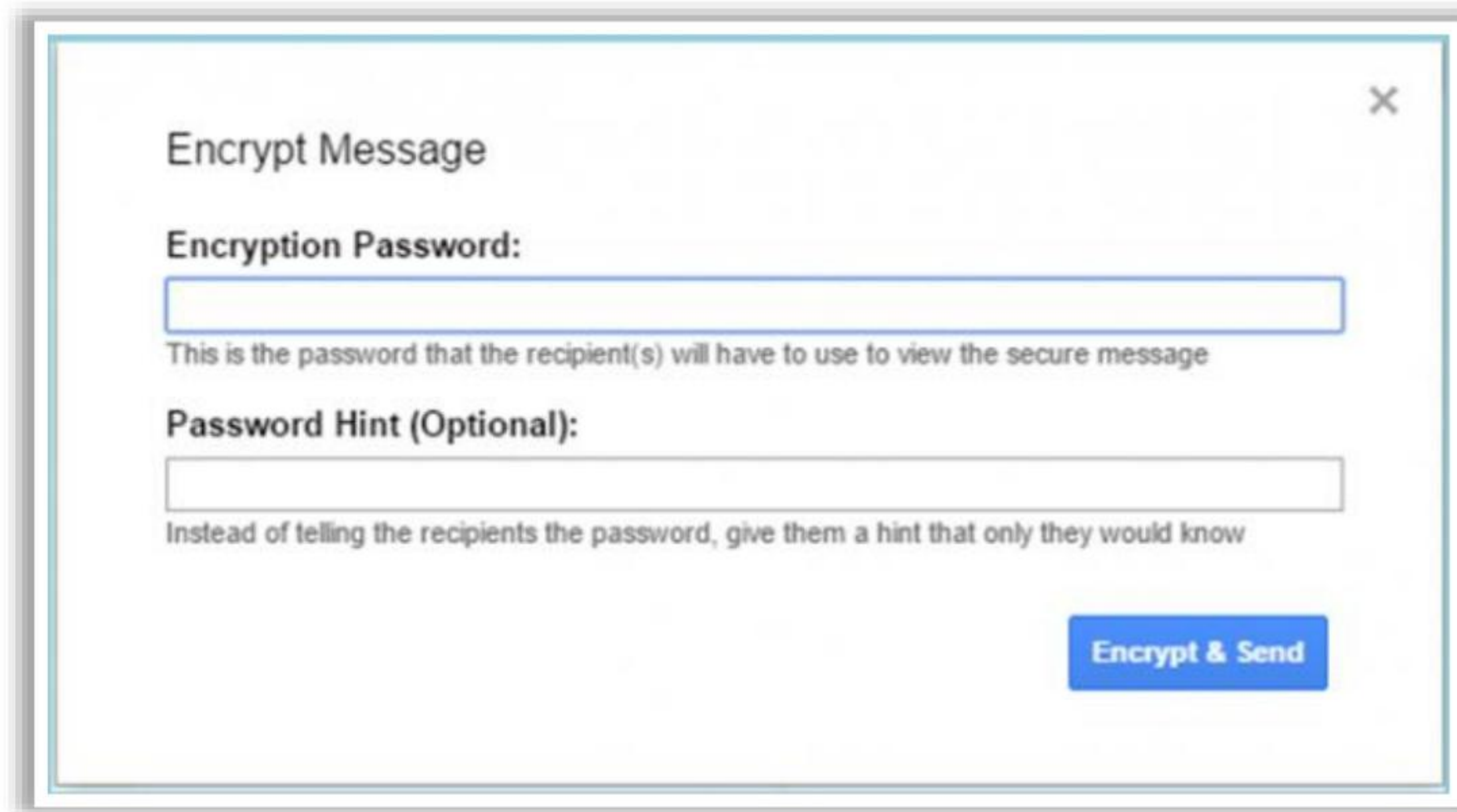


Figure 15.84: Encrypt Message

- Click the **Encrypt & Send** button.
- Manually share the password with the recipient.

Steps to Encrypt Gmail Through Firefox

If Google Chrome is not the primary Internet browser in the system, you can still encrypt mails using Firefox. Add the **Encrypted Communications** Firefox extension and restart your browser to activate it.

- Compose an email.
- Right-click and select **Encrypt Communication**.
- Enter a password and select **OK**.

Steps to open the encrypted email by a recipient:

- You will need the **Encrypted Communications** plug-in.
- Right-click on the message and select **Decrypt Communication**.
- Enter the assigned password.

Data Masking

- ❑ Data masking or data obfuscation is the process of **hiding original data** with random characters

Types of Data Masking		Data Masking Techniques	
Static Data Masking	Dynamic Data Masking	Algorithm	Description
Masks sensitive data at rest, or data stored in an original database environment	Temporarily masks sensitive data in transit without affecting the original data at rest	Character Scrambling	Characters are jumbled into a random order to mask the original data
Its purpose is to provide masked data for the development and testing of applications	Its purpose is to apply role-based security for databases/applications	Lookup Substitution	A lookup table is added to provide an alias for the original value
A series of data transformations is applied on the actual production data to generate high-quality masked data, which is then replicated in different environments.	The database proxy alters the SQL query issued by the analyst before transferring it to the database, to return the masked data to the analyst	Nulling Out or Deletion	Data becomes null for unauthorized users
		Shuffling	Data in an individual column is randomly shuffled or swapped
		Number/Date Variance	A data set is changed by a random percentage of its real value
		Masking Out	Only a part of the data is masked with a mask character. For example: X

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Data Masking

Data masking or data obfuscation is the process of hiding original data with random characters or other data. Its main purpose is to minimize unnecessary exposure of sensitive information like personally identifiable information (PII), protected health information (PHI), payment card information (PCI-DSS), and intellectual property (ITAR). It replaces vulnerable, or sensitive data with fictitious functional data that seems real, allowing it to be safely used in operations where original data is not required. In data masking, the basic format of the data remains the same, but its key values are changed. For example, a long card number is masked as follows:

2424 6789 4545 3421 will be masked as **2424 XXXX 3421**

Reasons to Include Data Masking in Data Security/Data Masking and Security

- **Protecting nonproduction data**

In many organizations, multiple copies of production data are required for nonproduction purposes such as application development and testing, employee training, business analytics modeling, etc. Multiple copies of sensitive data increase their chances of going into malicious hands. While allowing the safe sharing of sensitive data, the data masking techniques also plays a vital role in securing these data sets and meeting compliance requirements without affecting business operations.

- **Protection against insider threats**

Data masking allows employees to access the masked data instead of accessing the real production data to get their jobs done, which can mitigate the risk of a data breach from malicious insiders.

- **Protection against third parties**

Data masking makes it safe to send personal identifiable data, payment card information, or PHI to third parties, such as market researchers.

- **Compliance with regulations**

Data masking helps organizations comply with key regulations such as the general data protection regulation (GDPR) passed by the European Union to make personal more data secure.

Types of Data Masking

There are different types/strategies of data masking. To select a data masking type, consider the size of the organization, the location (cloud vs. on-premise), and the complexity of data you wish to secure. Data masking types include the following:

- 1. Static data masking (SDM)**

SDM masks sensitive **data at rest**, or data stored in an original database environment. SDM is implemented to provide realistic data for the development and testing of applications. Realism is necessary as it helps development and testing teams to detect the defects in the early stages of a development cycle. The SDM also secures data for use in analytics and training, and facilitates compliance with standards and regulations.

SDM applies a series of data transformations on the actual production data to generate high-quality masked data. Various approaches are used to perform SDM.

Statistical Data Masking

Certain alternatives to SDM, such as differential privacy method and DataSifter method, rely on the stochastic perturbations of data to preserve some statistical properties of the original data.

- 2. Dynamic data masking (DDM)**

DDM temporarily masks sensitive **data in transit** without affecting the original **data at rest**. DDM is mainly used to provide role-based security for databases/applications, and it uses database and proxy approaches to mask a database. The database proxy alters an SQL query issued by the analyst before transferring it to the database so that the masked data is returned to the analyst.

- 3. On-the-fly data masking**

Similar to DDM, on-the-fly data masking occurs on demand but for one record at a time. An extract transform load (ETL) process occurs wherever the data is masked within the memory of a given database application, which is helpful for agile companies targeting continuous delivery or continuous deployment practices.

- 4. Data masking and the cloud**

There are different modes for creating test data and moving it from on-premises to the cloud, or among environments inside the cloud. If data is masked before being ingested

into a cloud-native data repository, attackers would not gain anything from the stolen data following a breach. A few cloud-native data services offer built-in masking tools that make the implementation of masking easier in the cloud.

Data Masking Techniques

Some techniques for implementing data masking to obscure confidential data are as follows:

1. Encryption

Different encryption algorithms are used to mask data. Users who have an authorized key can only access the data.

2. Character scrambling

Characters are jumbled into a random order to mask the original data. For example, an emp_id #123456 in a production data set will be masked as #425613.

3. Lookup substitution

A lookup table is added as an alias for the original value. It hides the authentic data to protect it from security breaches.

4. Nulling out or deletion

Data becomes null for unauthorized users. This technique only helps avoid the visibility of the data element.

5. Shuffling

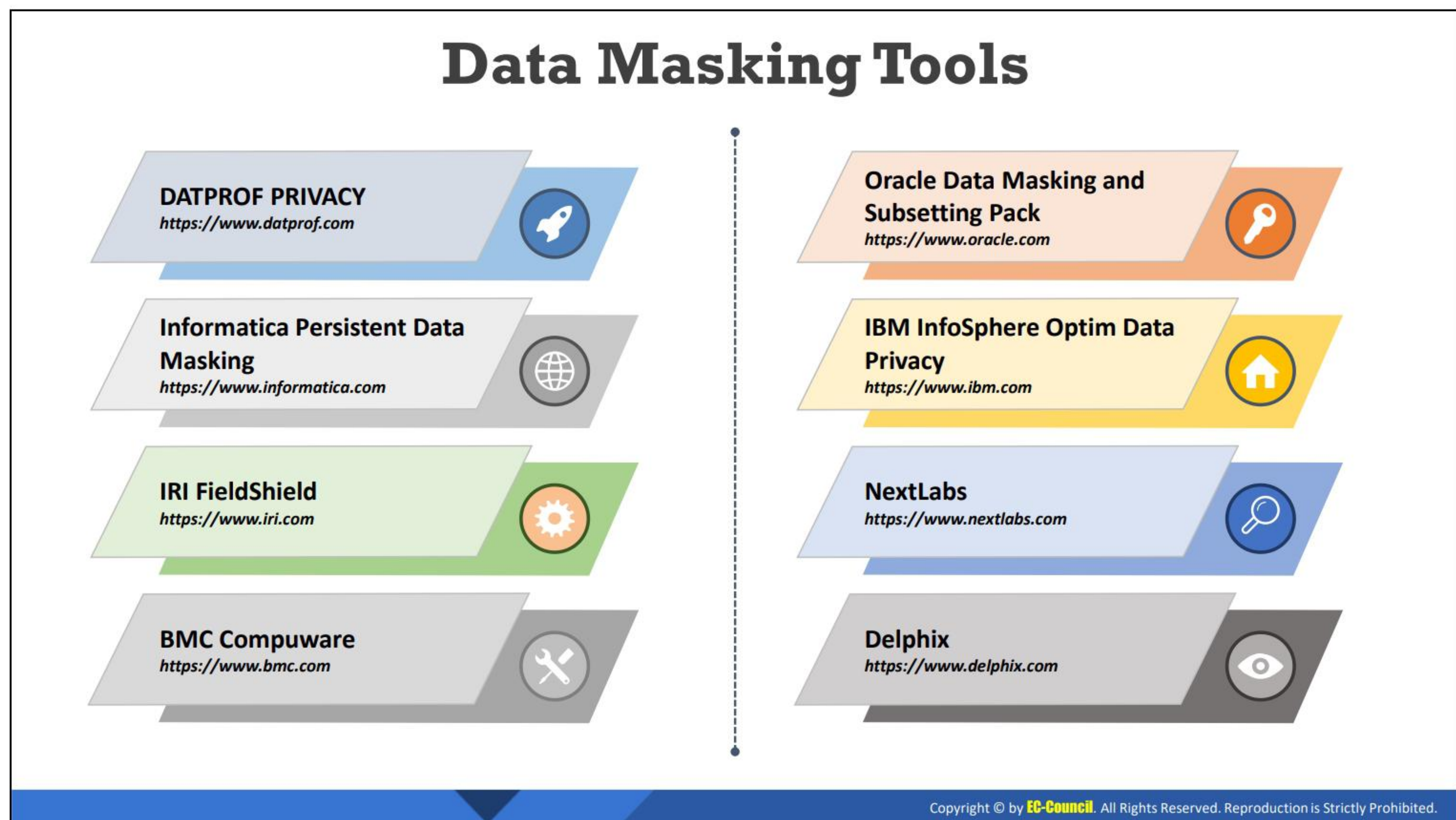
Data in an individual column is randomly shuffled or swapped. The output set appears real but does not disclose any sensitive information.

6. Number and date variance

Number and date variance is helpful in financial and date fields. Each number/date in a data set is masked by a random percentage of its real value.

7. Masking out

Only a part of the data is masked with mask characters (for example, an X). This technique is mainly used to mask credit card details. For example, when an operator bills a customer's credit card for an item, they will see only the last four digits, while all other digits will be masked as XXXX XXXX 7685.



Data Masking Tools

Data masking tools avoid any misuse of complex information and eliminate complex data with false data. The most common tools for masking data for small-, large-, and mid-sized enterprises are as follows:

- DATPROF PRIVACY (<https://www.datprof.com>)
- Informatica Persistent Data Masking (<https://www.informatica.com>)
- IRI FieldShield (<https://www.iri.com>)
- BMC Compuware (<https://www.bmc.com>)
- Oracle Data Masking and Subsetting Pack (<https://www.oracle.com>)
- IBM InfoSphere Optim Data Privacy (<https://www.ibm.com>)
- NextLabs (<https://www.nextlabs.com>)
- Delphix (<https://www.delphix.com>)

Database Deidentification Methods

- ❑ Deidentification is the **process of segregating** or replacing an entity's personal identity from the data stored in a database

01

Masking

- It is the process of **replacing critical information** in database fields with special characters such as asterisks (*) and hashes (#)

03

Tokenization

- It is the process of **replacing sensitive data** in a field with arbitrary tokens. These tokens act as a replacement for encryption keys

02

Bucketing

- It is the process of **replacing unnecessary information** with some common values

04

Hashing/Salting

- Hashing is the process of **transforming any type of data** with a unique fixed string length using hashing algorithms such as MD5 and SHA
- Salting is the process of **attaching random characters** (salt) to a hashed field in a table. It increases complexity and the difficulty of retrieving the hashes



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Database Deidentification Methods

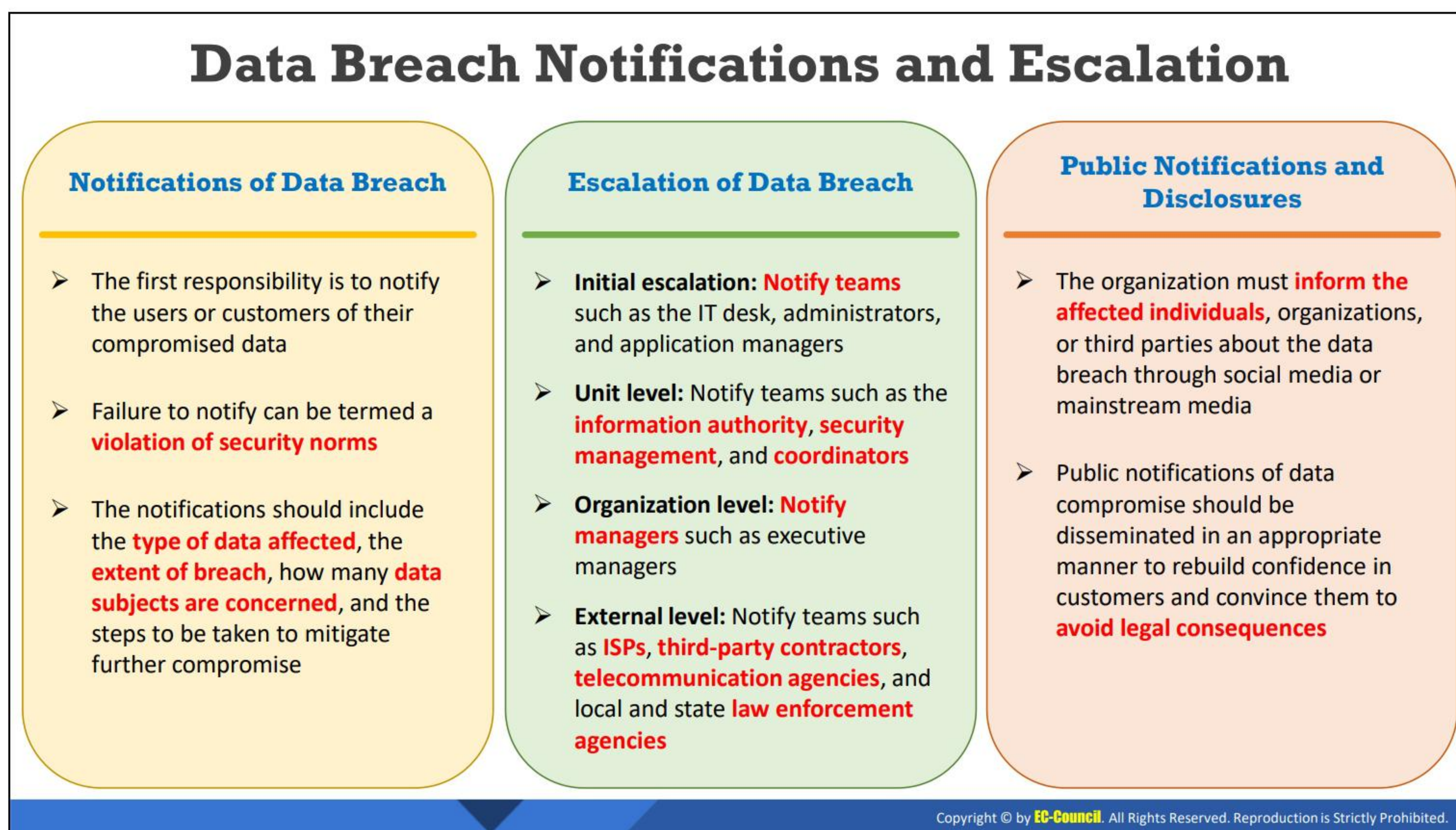
Deidentification is the process of segregating or replacing an entity's personal identity from the data stored in a database. It is important to remove or change personal identifiers from the data before sharing with third parties or keeping aside for reuse. Common personal identifiers include names, phone numbers, and credit/debit card numbers. Critical fields in the database table are labeled separately for the deidentification process whenever the query is executed.

Discussed below are some of the basic techniques used for data deidentification.

- **Masking:** Data masking is the process of replacing critical information in database fields with special characters such as asterisks (*) and hashes (#). For instance, "Michael" can be replaced with the characters "Mi****l" in data masking.
- **Bucketing:** Bucketing is the process of generalizing a field by differentiating it based on values or ranges. This technique is mostly used for generating reports that are later used for evaluation, where unnecessary information is replaced with some common values. For instance, instead of specifying the developer, tester, and administrator, these fields are saved with one common name such as "Engineer."
- **Tokenization:** Tokenization is the process of replacing critical data in a field with arbitrary tokens. These tokens act as the replacement for encryption keys. The token replaces original data with unrecognizable values, and the original data are stored on the token vault. These tokens are reversible, facilitating the reidentification and deidentification of the data when an authorized query is executed to retrieve the original values.
- **Hashing/salting:** Cryptographic hashes transform any type of data with a unique fixed string length using hashing algorithms such as MD5 and SHA. Hashes are generated from

mathematical functions; hence, it is difficult to match or retrieve the corresponding plaintext. In a database, hashing is used to secure passwords, expedite search processes, and offer deidentified references to stored data.

Salting is the process of attaching random characters (salt) to a hashed field in a table. It increases complexity and the difficulty in retrieving the hashes, providing strong defense against dictionary and rainbow table attacks.



Data Breach Notifications and Escalation

Notifications of Data Breach

A data breach refers to illegitimate access to protected or private information. Data breaches can vary in terms of impact and size of theft. They can occur through physical as well as digital media. Examples of physical breaches include stealing documents or leveraging the improper formatting of critical files. Examples of digital data breaches include stealing information by masquerading as a trusted entity and intentionally or deliberately sending private information to an unknown entity via emails.

Many laws and policies exist for organizations to respond appropriately to a breach. The first responsibility is to notify the users or customers of their compromised data. Failure to do so can be termed a violation of security norms. Users or customers can be informed of the data breach within 72 h of attack. If not, companies should prepare a document explaining the reason for the delay. The notification should include the type of data affected, the extent of breach, how many data subjects are concerned, and the steps to be taken to mitigate further compromise (such as forcing users to change passwords).

Escalation of Data Breach

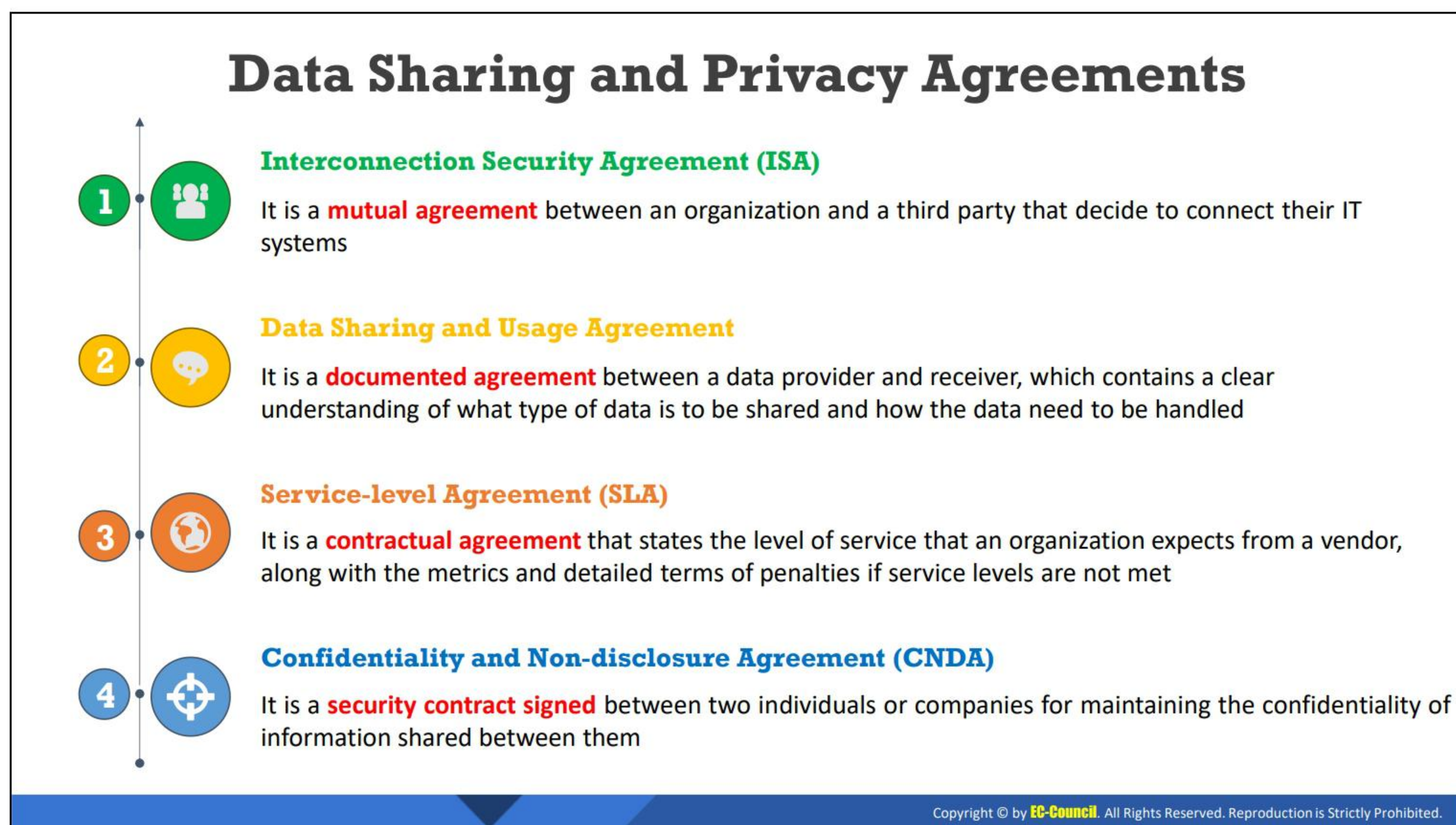
Some independent data breach incidents can be mitigated through minimal effort without informing the initial response team, but some incidents need to be escalated to different levels of security and response teams so that they can inspect and provide countermeasures for preventing the data or network from further compromise.

This escalation can be categorized as follows.

- **Initial escalation:** This type of escalation is crucial when the incident has the capability to take down network services and compromise data. It notifies teams such as the IT desk, administrators, and application managers.
- **Unit level:** This type of escalation is performed when an incident is capable of affecting network services, data confidentiality, and other business services. It notifies teams such as information authority, security management, coordinators, and other unit-wise entities.
- **Organization level:** This type of escalation is performed at the discretion of the security management teams of the organization. It informs managers such as executive managers and other higher authorities.
- **External level:** External escalation is also performed at the discretion or delegation of the information security management team. This type of escalation notifies teams such as ISPs, third-party contractors, telecommunication agencies, and local and state law enforcement agencies.

Public Notifications and Disclosures

Data breach or data compromise can range from password theft to the leak of personal chats, and affected individuals, organizations or third parties must be informed of it through social media or mainstream media. Public notification or disclosure is one of the methods used to disseminate the news of data breach. Public disclosure is the process of providing non-confidential information publicly while hiding important information such as login credentials, account details, and passwords. Public notifications of data compromise should be disseminated in an appropriate manner to rebuild confidence in customers and convince them to avoid legal consequences.



Data Sharing and Privacy Agreements

When an organization wishes to share resources with outsiders such as third-party service vendors, there is a risk associated with data security and privacy. Outsides with access to any internal system could cause a data breach, for which the organization will have to bear the consequences. To protect the confidentiality of data, it is important to make a formal legal agreement with third-party vendors and contractors who use the resources.

The following are some of the common agreements.

- **Interconnection Security Agreements (ISA)**

An ISA is a mutual agreement between an organization and a third party when they decide to connect their IT systems. The ISA is a memorandum of understanding (MOU) for security risk awareness and implementing security controls. It is defined by the NIST SP 800-47 Security Guide for Interconnecting Information Technology Systems.

- **Data Sharing and Usage Agreement**

A data sharing and usage agreement is a documented agreement between a data provider and receiver, which contains a clear understanding of what type of data is to be shared and how the data must be handled. This agreement protects the data from misuse and eliminates miscommunication between the two parties about how to process the shared data.

- **Service-level Agreement (SLA)**

An SLA is a contractual agreement that states the level of service that an organization expects from a vendor, along with the metrics and detailed terms of penalties if service levels are not met. The SLA is a crucial element for every contractual alliance with third

parties. It can be set for all the services or products that a third party offers. A vendor management SLA provides a collection of metrics that indicates to an organization how vendors are performing.

- **Confidentiality and Non-disclosure Agreement (CNDA)**

An NDA is a security contract signed between two individuals or companies for maintaining the confidentiality of information shared between them. The parties sign this agreement when they intend to restrict the use of the shared information. NDAs are also known as confidentiality agreements, proprietary information agreements, and secrecy agreements.

Business experts state that NDAs are the best option when an individual or firm makes a contract with another. NDAs are useful when an individual or firm needs to share its confidential information with third parties but does not want them to disclose it. This confidential information can be the pharmaceutical formulas of a pharmaceutical firm, beverage compositions of a beverage firm, list of customers of an e-commerce firm, or other technical data.

A written NDA is a powerful legal tool stating that neither party will disclose any trade secrets, patents, or other proprietary information to anyone outside the company. A party can initiate legal action against the other for any violation of the documented agreement. The organization can sue for damages and compensation in the case of any violation.

Rights Management Services

Active Directory Rights Management Services

AD RMS is a security solution designed for data security through proper the **implementation of access policies**



SolarWinds Access Rights Manager
<https://www.solarwinds.com/access-rights-manager>



Foxit PDF Security Suite
<https://www.foxit.com>



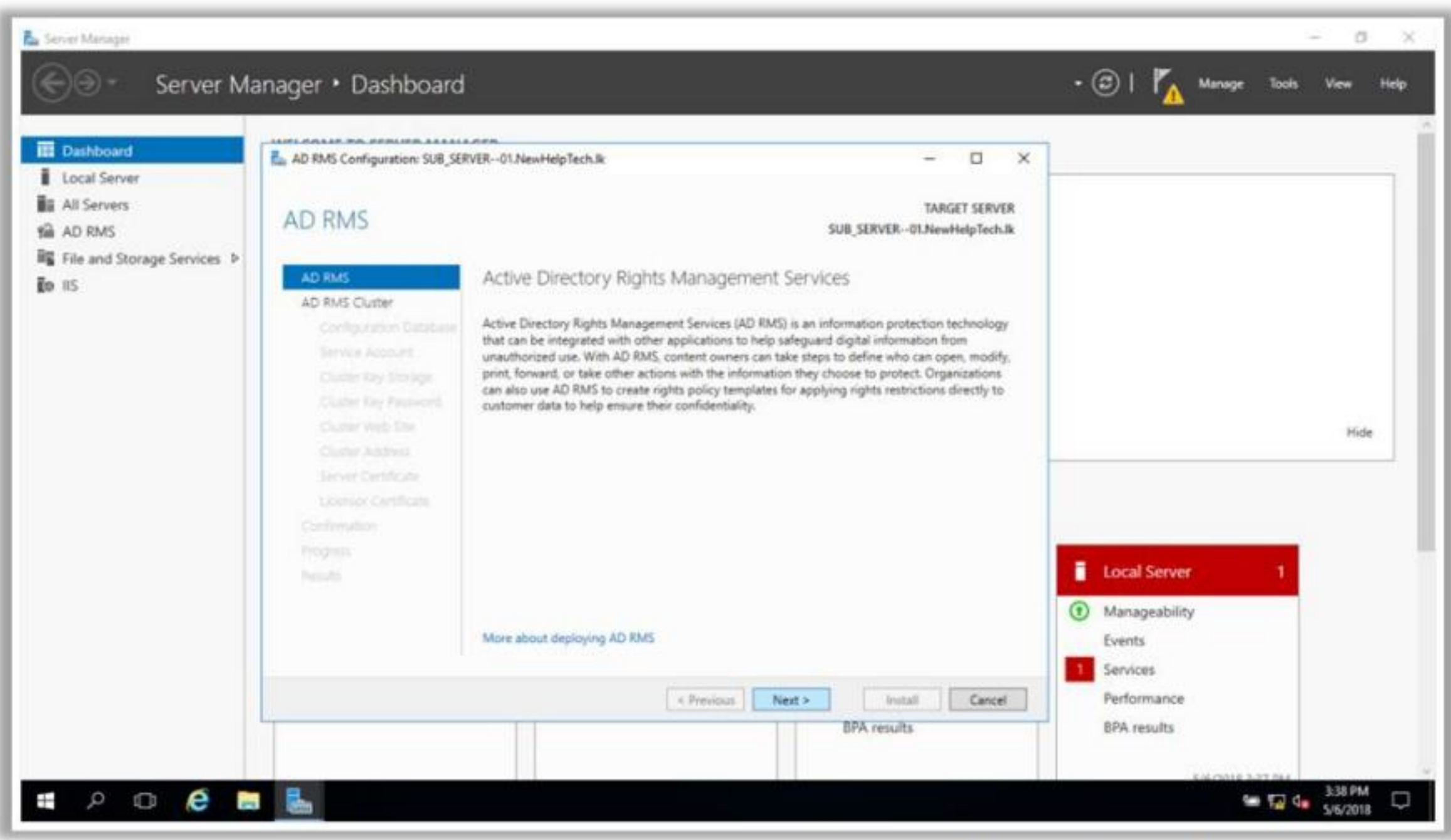
ManageEngine AD360
<https://www.manageengine.com>



Netwrix Auditor
<https://www.netwrix.com>



Microsoft Azure RMS
<https://www.paessler.com>



<https://www.windows-active-directory.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Rights Management Services

Active Directory Rights Management Services (AD RMS)

Source: <https://www.windows-active-directory.com>

RMS is a security tool that has been used since before the release of Windows Server 2008. Currently, RMS is named Active Directory Rights Management Services (AD RMS) and is a security solution designed for data security through the proper implementation of access policies. AD RMS employs encryption techniques and a type of functionality for limiting access to critical organizational data such as MS Word files, emails, web pages, and activities of a legitimate client. AD RMS consists of a server and client units. The server is created from multiple web services, and the client comprises utilities that can be used for encryption and decryption. The client can also procure document licenses and security certificates from the server to perform many other security-related operations; these licenses or certificates can be accessed only by authorized individuals. AD RMS also employs the Information Rights Management (IRM) feature to enhance the security plans for enterprises to secure documents. These IRM policies are used to determine authorized individuals and provide access permissions to documents, presentations, and other services based on specific criteria.

The following are some of the features provided by the AD RMS.

- Provides constant and continuous usage policies
- Provides an additional layer of security to protect sensitive information
- Thwarts unauthorized copying, modifying, and forwarding of documents

- Allows setting file expiration, which makes the content in a document inaccessible after a certain period

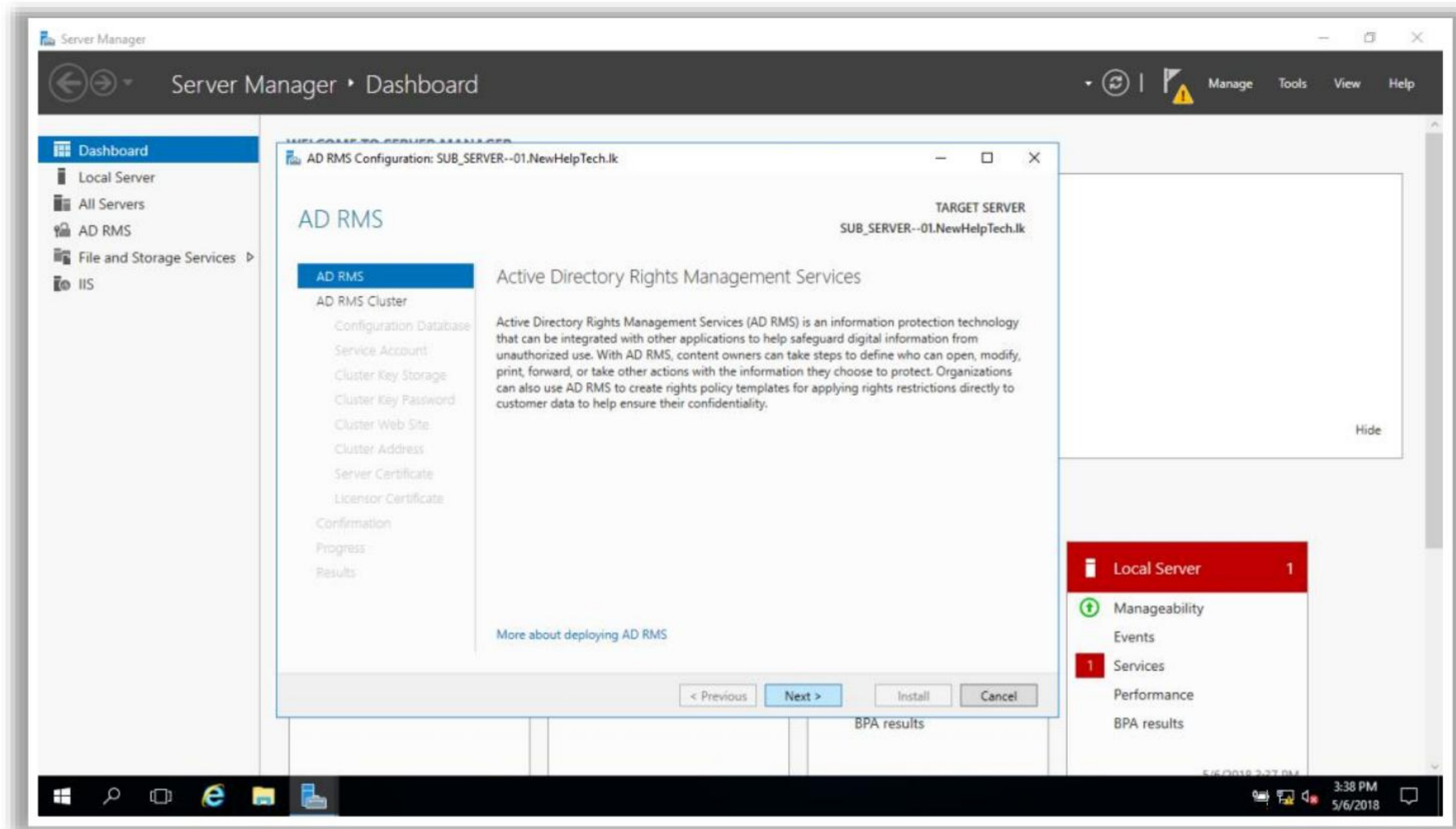
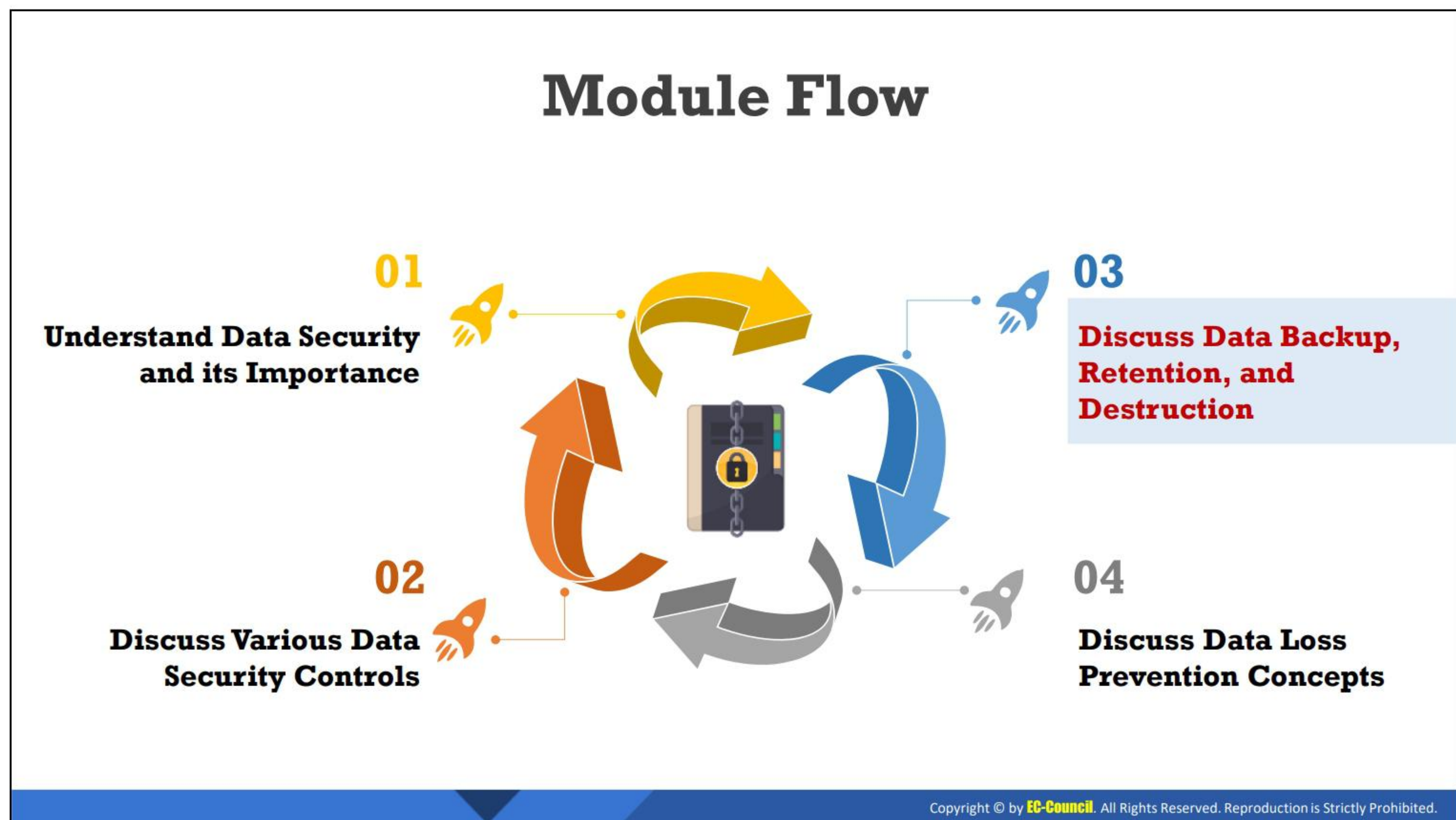


Figure 15.85: Screenshot displaying AD RMS in Windows Server

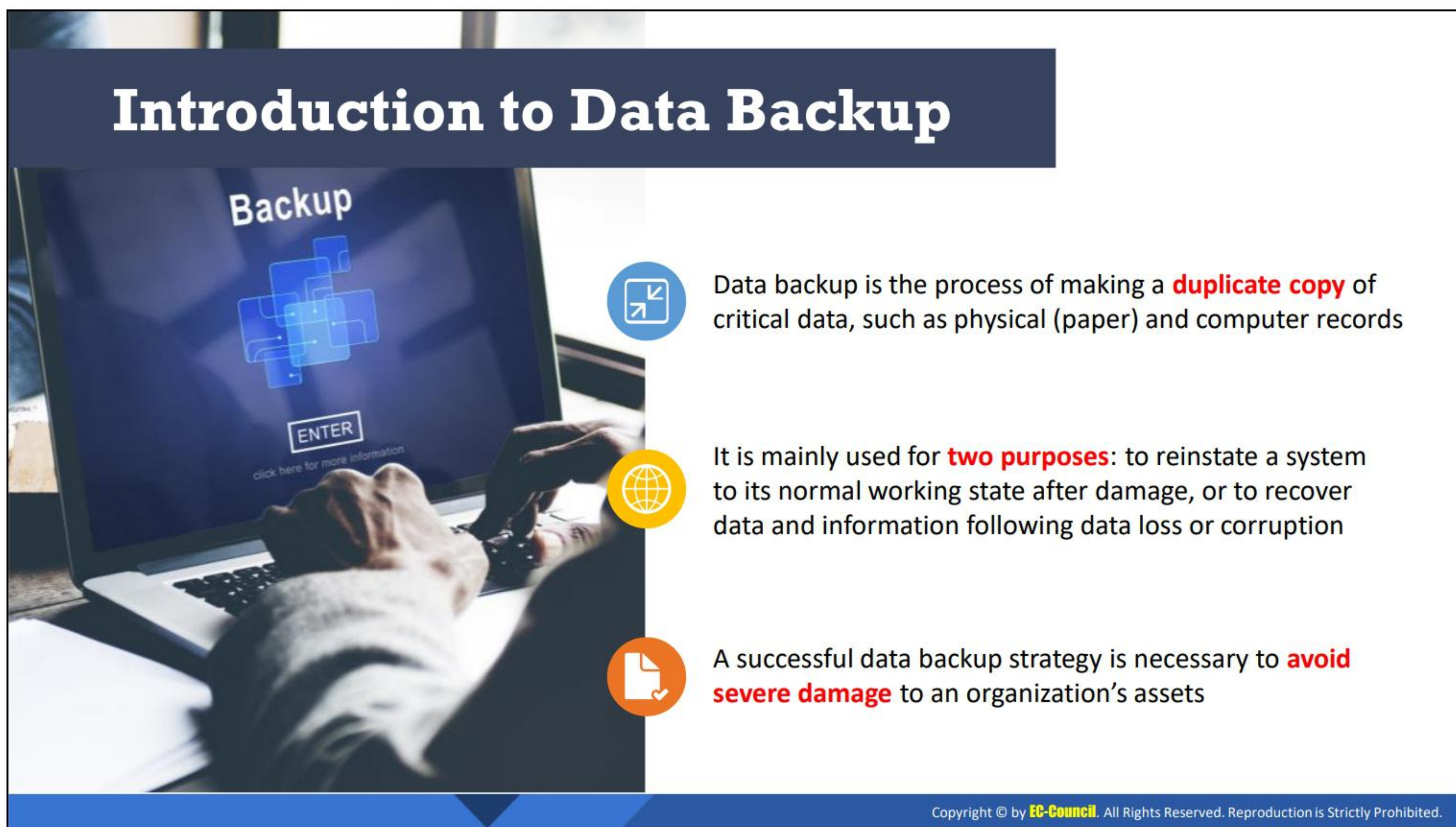
The following are some of the additional rights management services:

- SolarWinds Access Rights Manager (<https://www.solarwinds.com/access-rights-manager>)
- Foxit PDF Security Suite (<https://www.foxit.com>)
- ManageEngine AD360 (<https://www.manageengine.com>)
- Netwrix Auditor (<https://www.netwrix.com>)
- Microsoft Azure RMS (<https://docs.microsoft.com>)



Discuss Data Backup, Retention, and Destruction

Data loss is a major risk that organizations are facing today. Loss of critical data can result in a lot of damage to the organization. Any organization that encounters a critical data loss has a higher probability of facing serious issues later. Therefore, you should have a strong data backup and retention plan in place to deal with such incidents. The objective of this section is to explain the concept of data backup, retention, and destruction.

A graphic titled "Introduction to Data Backup" featuring a laptop screen on the left with a "Backup" interface showing a blue cube icon and an "ENTER" button. To the right of the laptop are three circular icons: a blue square with a white arrow, a yellow circle with a globe, and an orange circle with a document and checkmark. Each icon is followed by a text block explaining a concept of data backup.

Introduction to Data Backup

Backup

Data backup is the process of making a **duplicate copy** of critical data, such as physical (paper) and computer records

It is mainly used for **two purposes**: to reinstate a system to its normal working state after damage, or to recover data and information following data loss or corruption

A successful data backup strategy is necessary to **avoid severe damage** to an organization's assets

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Introduction to Data Backup

Data backup is the process of copying or storing important data. A backup copy will help you restore the original data when data is lost or corrupted. Backup is a mandatory process for all organizations. The process of retrieving lost files from a backup is known as restoring or recovery of files.

The main idea behind data backup is to protect data and information and recover the same after data loss. Data backup is mainly used for two purposes: to reinstate a system to its normal working state after damage, or to recover data and information following data loss or corruption.

Data loss in an organization affects its finances, customer relationship, and company data. Data loss in personal computers may lead to the loss of personal files, images, and other important documents saved in the system.

Reasons for Data Loss

- **Human error:** Deletion of data purposefully or accidentally, misplacement of data storage devices, and errors in administering databases.
- **Crimes:** Stealing or making modifications to critical data in an organization.
- **Natural causes:** Power failures, sudden software changes, or hardware damages.
- **Natural disaster:** Floods, earthquakes, fire, etc.

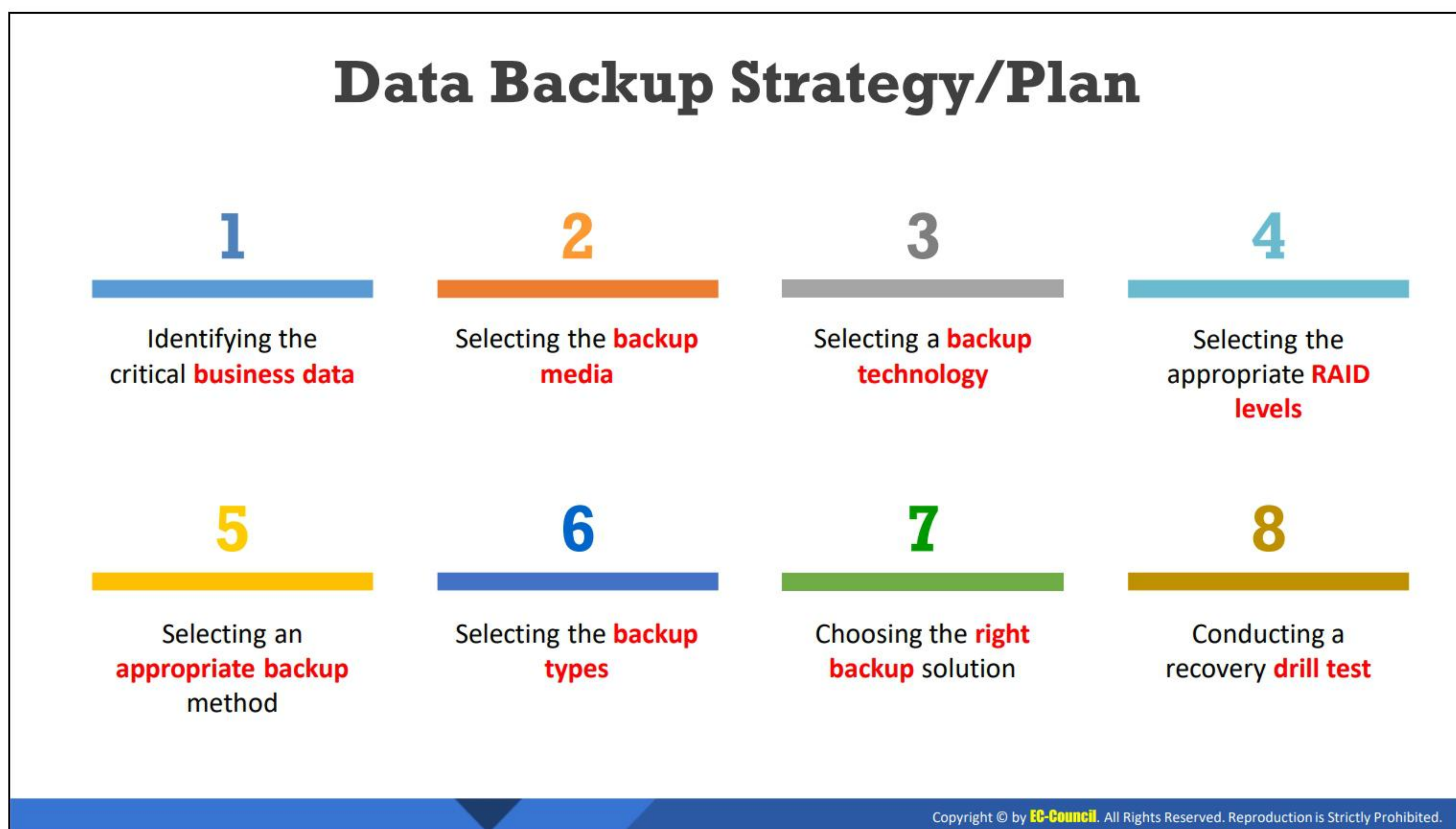
Benefits of Performing a Data Backup

- It offers access to critical data even in the event of a disaster, ensuring peace of mind in a workplace.

- Backup of critical data prevents an organization from losing its business. It also helps them retrieve data anytime.
- Data recovery helps organizations recover lost data and ensure business continuity.

It is recommended that every organization performs a data backup on a regular schedule to run their business successfully and efficiently.

To avoid severe damage to an organization's assets, it is important to design a strategy for a successful data backup process. Going forward, this data backup strategy can act as a blueprint while working on the data backup process for the entire organization. Certain companies also create a data backup policy that is required while implementing a backup strategy.



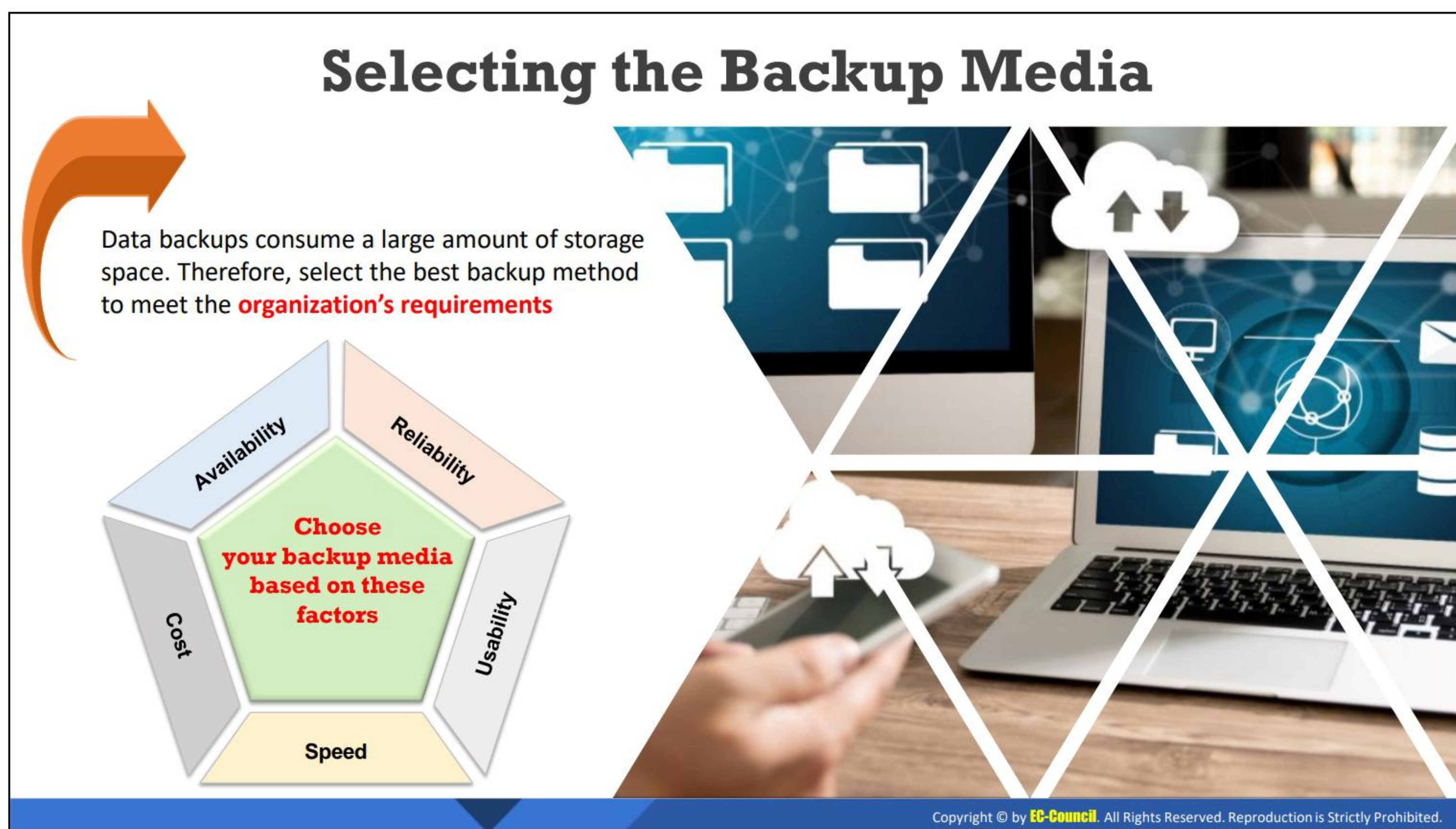
Data Backup Strategy/Plan

An ideal backup strategy includes steps ranging from selecting the right data to conducting a test data restoration drill. Although the backup strategy might differ among organizations, it is important to consider the following features before drafting a backup strategy:

- The backup strategy should have a data recovery feature from any external device. These devices may include servers, host machines, laptops, etc.
- If the data loss is because of a natural disaster, the backup strategy should not be restricted to only a certain number of incidents. The strategy should also cover the methods for recovering the data after a natural disaster.
- The strategy should include the steps to recover data at the earliest.
- The lower the cost for data recovery, the more the financial benefit to the organization.
- Auto recovery options should be included in the backup strategy as well, as they reduce the chances of human error during the recovery process.

Steps involved in data backup strategy/plan:

1. Identifying the critical business data
2. Selecting the backup media
3. Selecting a backup technology
4. Selecting the appropriate RAID levels
5. Selecting an appropriate backup method
6. Selecting the backup types
7. Choosing the right backup solution
8. Conducting a recovery drill test



Selecting the Backup Media

Choosing the best backup media is a common concern within most organizations. The selection of a wrong media device can lead to a segregation of data across different media devices. With a carefully considered plan, selecting an appropriate media will enable a better level of data backup.

Once the data is identified, it is important to choose an appropriate backup media to store the data. Backup media selection depends on the type and amount of data in the backup. At times, data backup consumes a large amount of space; consequently, an increased attention is necessary to select the best backup media for a situation, and to fulfill the organizational needs.

Choosing the best backup media is based on the following factors:

- **Cost:** Organization should have backup storage mediums that best fit their budget. The backup media should have more storage space than the data it will contain.
- **Reliability:** Organizations must be able to rely on the data stored on the backup media without fail. Organizations must select a media that is reliable and not susceptible to damage or loss.
- **Speed:** Organizations should select backup mediums which require reduced number of human interactions during the backup process. Speed becomes a concern if the backup process cannot be completed when a machine is idle.
- **Availability:** The unavailability of the backup medium could be an issue following data loss or data corruption. Organizations should decide on a medium that is always available.
- **Usability:** Organizations should select a media that is easy to use. An easy media type has a greater flexibility during the backup process.

Examples of Data Backup Media Devices

Media	Capacity	Advantages	Disadvantages	Illustrations
Optical disks (DVD)	~200 GB	Affordable, easy to store and transport	- Several manual disk swaps may be required because of the limited data capacity - Recording and verifying a backup is slow	
Portable hard drives/USB flash drives	No limit	- Relatively higher storage capacity than optical disks - Ideal for the home or small offices - Faster recording of backups	- More expensive than DVD backups - Less recommended for small backups	
Tape drives	No limit	- Media for enterprise-level backups - Easy to store and transport	Expensive	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Examples of Data Backup Media Devices

Optical Disks (DVD)

DVD recordable disks can store up to ~200 GB of data and are readily available. DVDs store more data and are available at affordable rates, in bulk if need be. However, they are not used as much as in the past, as external hard drives are available at reasonable prices and can store more data than DVDs.

Advantage:

- Less expensive, easy to store, and transport

Disadvantage:

- Several manual disk swaps may be required because of the limited data capacity
- Recording and verifying a backup is slow

Portable Hard Drives/USB Flash Drives

Portable hard drives are considered a better medium for data backup than a DVD. They are available in high capacities and can also be used for smaller backups. Flash drives are available in different sizes and have the ability to store large backup files.

RAID is another available hard drive option. It contains two or more hard drives. The second drive may be used to copy data stored in the first drive. This process allows important data to be preserved. Any change in the data will be automatically reflected in all other drives as well.

- **Advantages:**

- Relatively higher storage capacity than optical disks
- Ideal for the home or small offices
- Faster recording of backups

- **Disadvantages:**

- Expensive than DVD
- Less recommended for small backups

- **Tape Drives**

A Tape drive is considered as the best media for data backup. It facilitates data backup at an enterprise level. Tape drives are used for storing programs and data. There is no limit in storage capacity and can be used to store large amounts of data.

- **Advantages:**

- Media for enterprise-level backups
- Easy to store and transport
- Requires no user intervention
- Tape backup is completely automatic

- **Disadvantages:**

- Expensive for home users
- Home computers require additional hardware and software updates



Redundant Array Of Independent Disks (RAID) Technology

- 01** A method of combining multiple hard drives into a single unit and writing data across several disk drives, offering fault **tolerance** (if one drive fails, the system can continue operating)
- 02** Placing data on **RAID disks** enables a balanced overlap of input/output (I/O) operations, improving system performance, simplifying storage management, and protecting against data loss
- 03** RAID represents a portion of computer storage that can divide and replicate data among several drives by working as **secondary storage**
- 04** RAID has six levels: RAID 0, RAID 1, RAID 3, RAID 5, RAID 10, and RAID 50, to function effectively. All RAID levels depend on the following storage techniques:



Striping



Parity



Mirroring

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Redundant Array Of Independent Disks (RAID) Technology

Many organizations depend on RAID technology for handling their critical backup needs, especially with the increase in data flow and data volume. Organizations are expanding their networks to improve their productivity. However, this additional increase can cause network bottlenecks. The probability of losing data because of disaster, threats, mistakes, and hardware failures hamper an organization's ability to grow. RAID technology overcomes these situations providing an option for data availability, high performance, efficient and accessible recovery options without a loss of data.

Understanding RAID Technology

RAID technology is used to store data in different places on several disks. Storing the data on multiple disks improves the performance of I/O operations. RAID technology functions by implementing multiple hard disks as a single logical disk. It allows a more balanced storage of the same data across an array of disks. An effective implementation of this technology helps address the complex issues in fault tolerance. The data organized in RAID levels depends on the RAID storage techniques and installation methods. Usually, the implementation of RAID is done on a server. Although personal computers do not necessarily need this technology, they can still setup and utilize it in a smaller environment than an enterprise.

RAID has six levels for functioning effectively: RAID 0, RAID 1, RAID 3, RAID 5, RAID 10, and RAID 50. Each level has the following features:

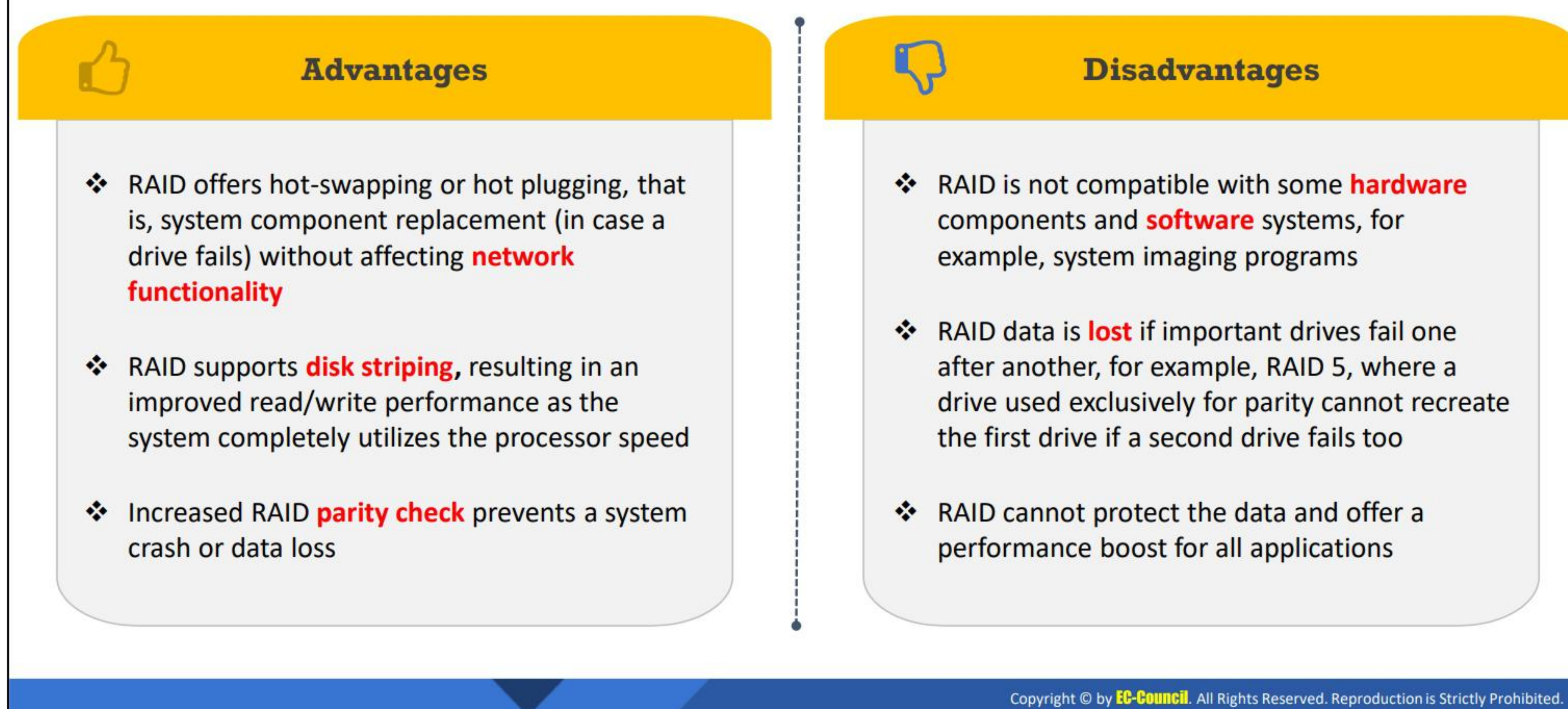
- **Fault tolerance:** Even if a disk fails to work, other disks will continue to function normally.
- **Performance:** RAID achieves high performance during read and write processes across multiple disks.

- **Competence:** This is defined by the amount of data stored. The storage capacity of disks depends on the chosen RAID level. The storage capacity need not be equal the size of the individual RAID disks.

All the RAID levels depend on the storage techniques listed below:

- **Striping:** Striping divides the data into multiple blocks. These blocks are further written across the RAID system. Striping improves the data storage performance.
- **Mirroring:** Data mirroring makes image copies of the data and simultaneously stores this data across the RAID. This affects fault tolerance and data performance.
- **Parity:** Parity uses a striping method to calculate the parity function of a data block. During a drive failure, the parity recalculates the function using a checksum method.

Advantages/Disadvantages of RAID Systems



Advantages/Disadvantages of RAID Systems

Before RAID technology was introduced, many organizations used a single drive to store data. RAID technology is now found across all storage devices in an organization. Advantages and disadvantages RAID depend on the implemented level.

Advantages of RAID Systems

- **Performance and reliability:** RAID technology increases the read/write performance of the data on disks. The speed is much faster than when using a single drive as storage. It improves the performance by distributing the I/O. A RAID controller distributes data over several physical drives, ensuring that a single drive in the RAID system is not overburdened. RAID sustains the reliability of data even if a disk fails. Failed components can be replaced in a RAID system without shutting the system down. This feature is called hot swapping or hot plugging. The replacement process does not affect the network or how the other disks function.
- **Parity check:** Parity check is a process where the RAID system compares the data stored in a crashed system with the data stored in other disks. This check process is accomplished on all drives. The parity check is performed after mirroring the data. Regular parity checks detect the probability of a system crash, thereby preventing data loss.
- **Data redundancy:** A disk can fail anytime. Therefore, data redundancy is important for an organization. RAID provides enhanced data redundancy in case of a hardware failure.
- **Disk striping:** Disk striping improves the read/write performance of data. The data is divided into small chunks and spread over multiple disks. Depending on the

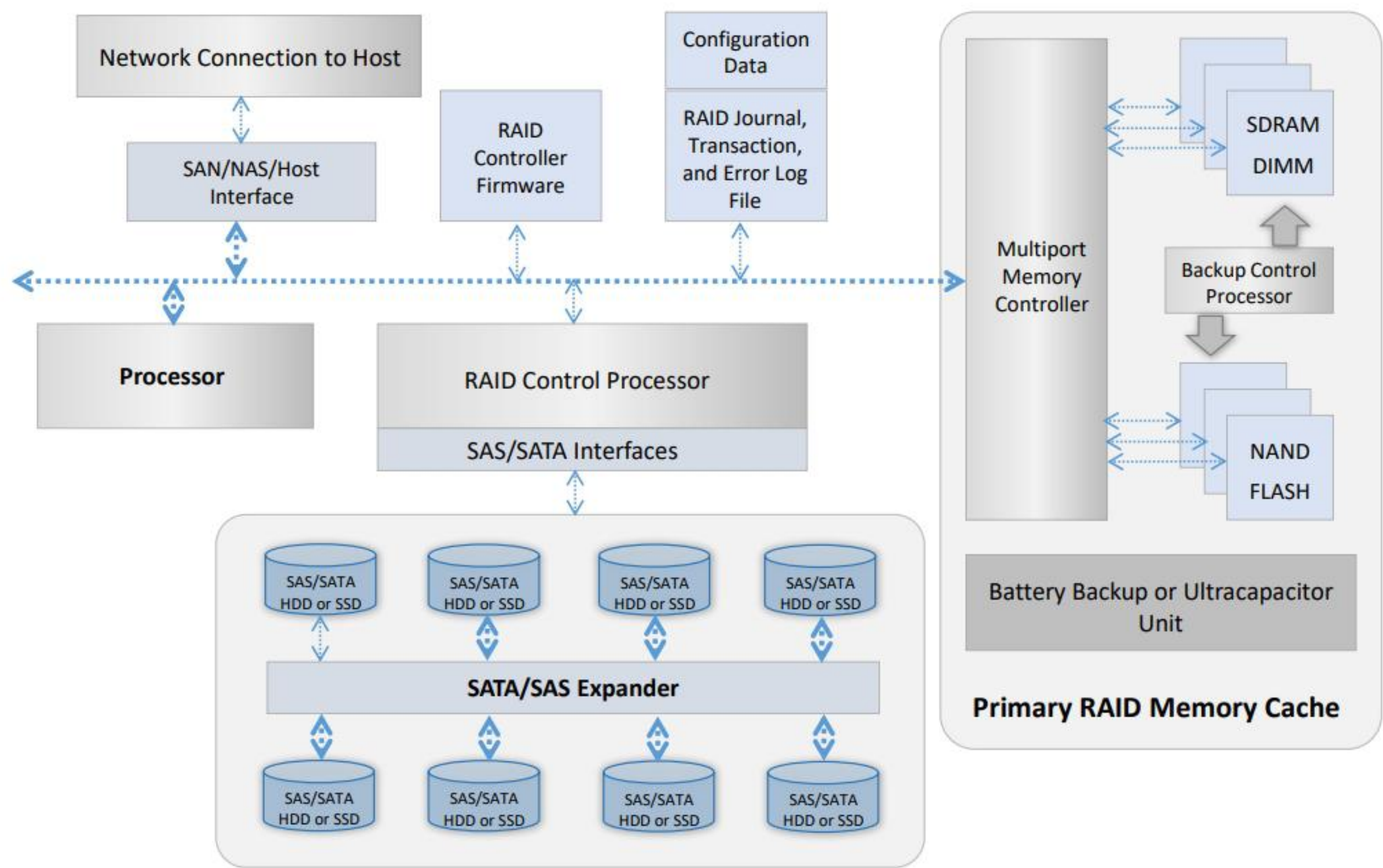
implemented RAID level, the data is divided into bytes, bits, or blocks. Data reading and writing can be done simultaneously on a RAID system.

- **System uptime:** This metric detects the reliability and stability of a computer. System uptime defines the time till which a system can be left unattended without any assistance. Configuring RAID on a system helps enhance system uptime. A high system uptime in an organization signifies a high productivity.

Disadvantages of RAID Systems

- **Writing network drivers:** RAID technology is designed to be widely used on servers. A major disadvantage of RAID technology is the writing of all network drivers. RAID technology is complex, and this process can be time consuming.
- **Non compatibility:** Different systems support different types of RAID drives. Certain hardware or software components may not be compatible with the RAID drive configured on a server. This non compatibility may lead to the RAID not functioning properly. The compatibility between RAID drives, hardware, and software must be checked prior to configuring a system. RAID can protect data for all applications available on the network. For example, RAID is not compatible with system imaging programs.
- **Loss of data:** All RAID drives function in the same environment. They can become nonfunctional because of mechanical issues. Thus, the potential data loss increases if the disks fail one after another. When two drives fail at the same time, recovering the data from the disk becomes difficult. For example, RAID 5, where a drive used exclusively for parity cannot recreate the first drive if a second drive fails too.
- **Time consumed in rebuilding:** The increase in drive capacity has been much more than the increase in transfer speed. Recovering data from drives with a large storage capacity can be time consuming. In such scenarios, rebuilding a failed disk can also be time consuming. Increasing the number of drives does not help increase the data transfer speed.
- **Cost:** Implementation of RAID technology can be costly. Organizations need to hire consultants to sustain its performance. It also requires external RAID controllers and hard drives to function correctly, and this adds to the overall cost.
- RAID cannot protect the data and offer a performance boost for all applications.
- RAID should be maintained by commercial consultants.
- RAID configuration is difficult.

RAID Storage Architecture



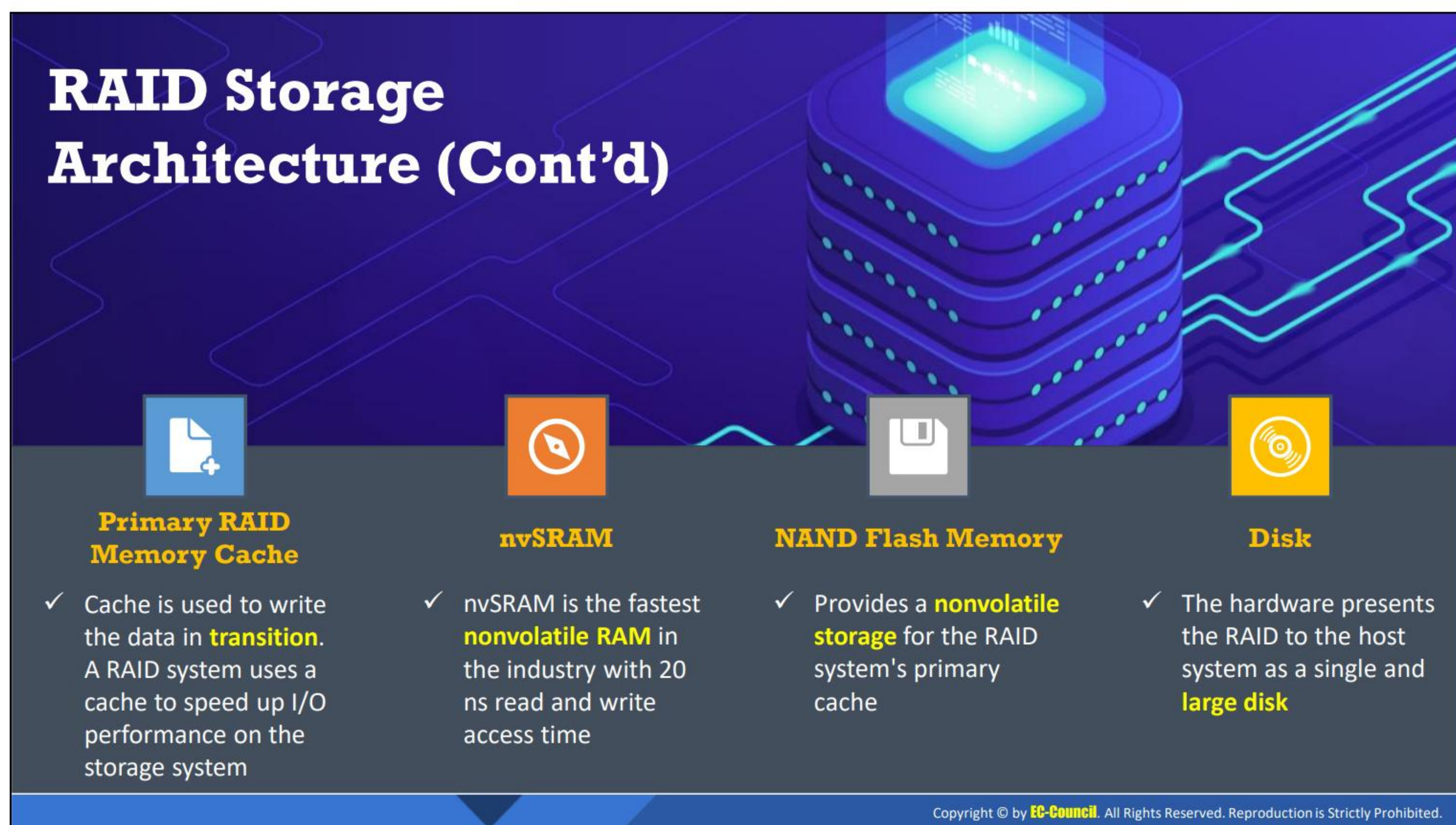
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

RAID Storage Architecture (Cont'd)

- 1 RAID Controller**
Manages an array of **physical disk drives** and presents them to the computer as logical units
- 2 IDE, SATA, or SCSI Interface**
Internal drives are connected using these **interfaces**; Connection to the server is also through one of these interfaces
- 3 Multiport Memory Controller**
Provides access to a memory bank, and helps achieve a **high efficiency** with random address accesses
- 4 SDRAM**
Dynamic random access memory (DRAM) that is **synchronized** with the CPU clock speed



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



RAID Storage Architecture

The RAID architecture depends on two principles: redundancy and parallelism, providing a wide range of storage options with better performance and freedom from disk failures. The Internet's increasing footprint has led to an increase in the use of RAID systems because of their high data storage capabilities and management systems. Many available RAID implementations depend on the following factors: parallelism, duplication, and redundancy.

In a RAID architecture, a switch receives the data from servers connected to the network. The switch then sends the data to the processor at a later stage. The processor transfers the received data to a RAID controller. The RAID controller may be implemented either as a hardware using a RAID-on-Chip (ROC) or in a software. The ROC can contain the I/O interfaces, a processor, a host interface, and a memory controller. The ROC is installed directly in a motherboard using an expansion card, or in an external drive enclosure.

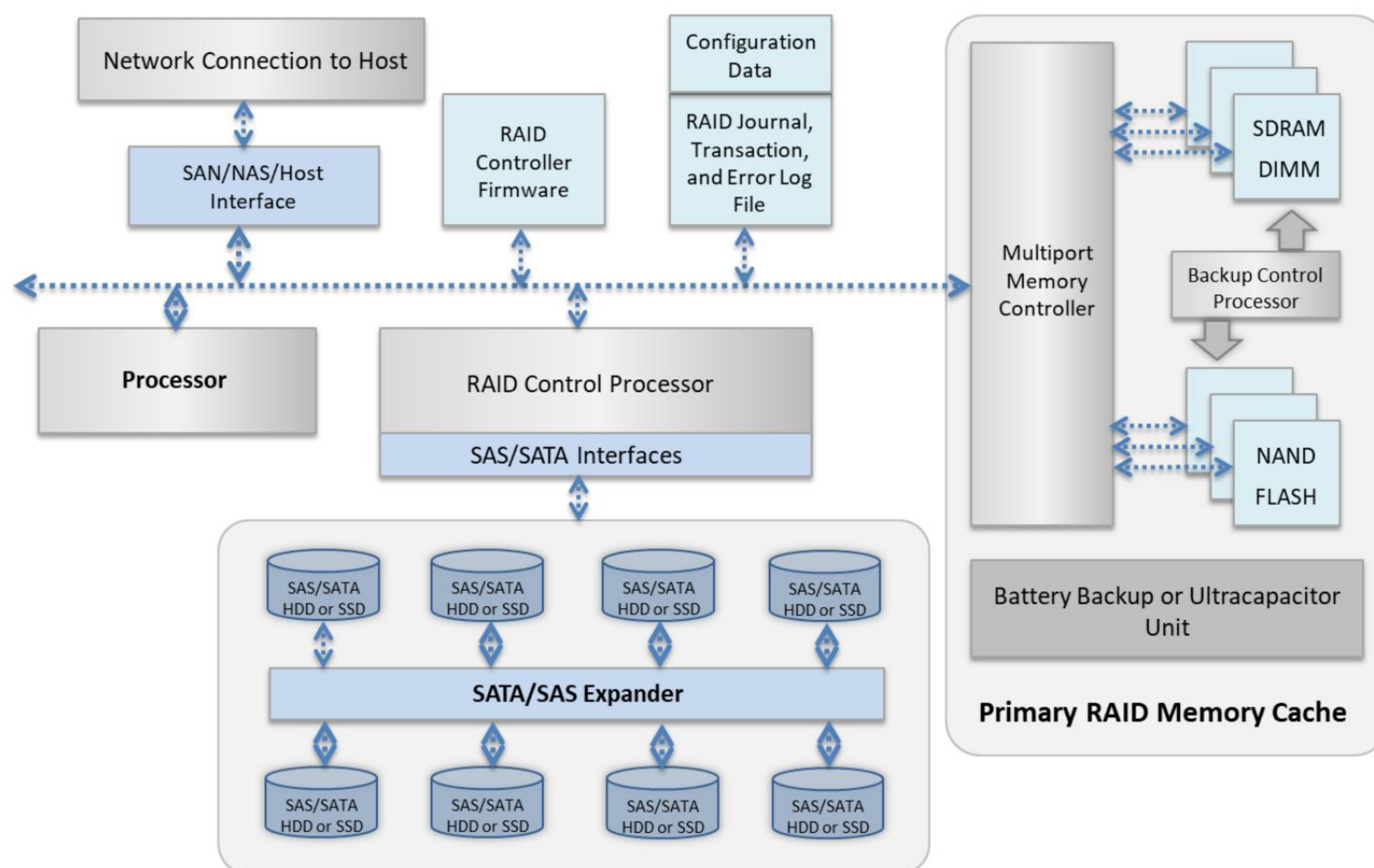


Figure 15.86: RAID storage architecture

The RAID storage architecture outlines how the RAID server functions. The processor controls the entire functioning of the drive arrays and interfaces. It provides flexible and high-performance functions. The architecture in the figure above shows a RAID system can depend on hard disk drives (HDDs) as well as SSDs. The processor requires DRAM and NAND flash memory. The NAND flash memory provides a nonvolatile storage to the primary RAID memory cache.

A battery backup or an ultra-capacitor unit in the primary RAID memory cache is helpful when the RAID control processor suffers from a power failure. In this scenario, the battery backup independently copies the DRAM contents to the NAND flash memory. A battery backup is an inexpensive alternative during a power loss. The architecture shows the requirement of a nonvolatile memory in the RAID controller firmware, RAID journal, and transaction and error log files.

Major Components of a RAID Architecture

- **RAID controller:** This is either hardware- or software-based and contains the HDDs or solid state drives as a single logical unit. A RAID controller has the permission to access multiple copies of files present on multiple disks, thereby preventing damage and increasing the system performance. In a hardware RAID, a physical controller manages the RAID array with a controller in the form of a PCI card that supports SATA or SCSI. A software RAID works similarly to a hardware RAID, except that their performance is lower than the former.
- **Primary RAID memory cache:** The RAID controller has a direct access to the cache memory, enabling faster read and write access to the storage system. The cache is used

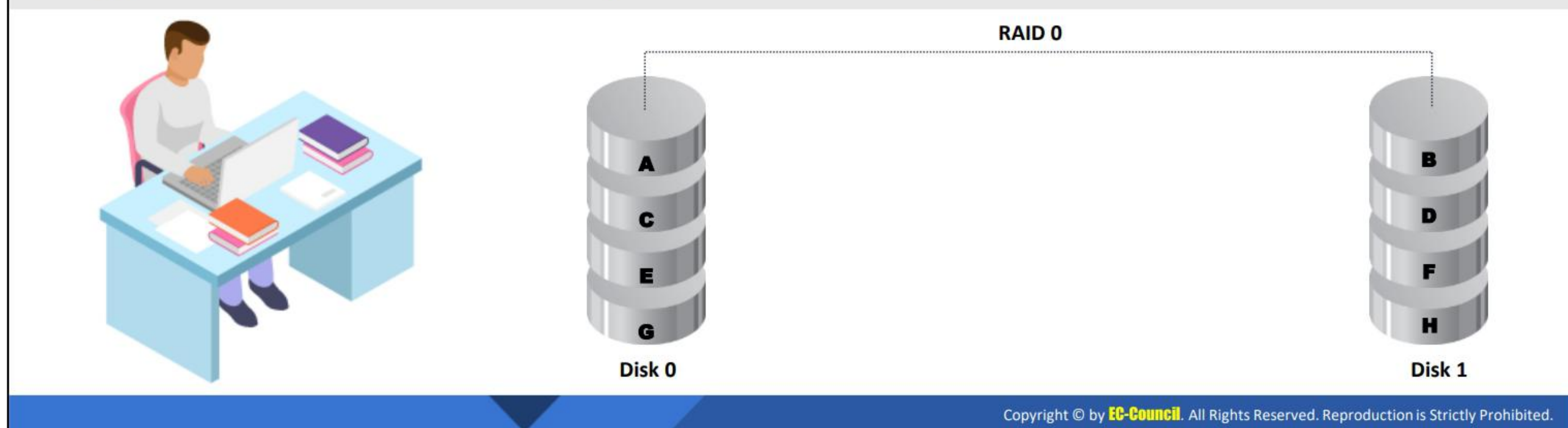
to store the changing data. The cache memory is bigger in size and uses high-speed SDRAMs. A normal cache memory has a write cache and a separate read cache. The read cache decreases the latency of the read process. There are two types of write cache memories:

- **Write-through mode:** This bypasses the cache memory and writes the data directly to the disk after the host sends it. The host sends the next data item after receiving a confirmation that the writing process has been completed.
- **Write-back mode:** Data sent from the host is written to the cache memory. The host may perform other actions while the RAID controller transfers data from the cache to the disk drive. The RAID controller acknowledges the write process to the host soon after writing the data to the cache. Issues may arise if a RAID controller sends an acknowledgment before the data has been completely written on the disk.
- **IDE, SATA, or SCSI interfaces:** IDE, SATA, or SCSI are device cables that transmit read/write signals to and from the drive. These are mostly used for internally connecting the drives. Moreover, servers are connected using these interfaces.
 - **IDE:** Integrated drive electronics (IDE) allows the connection of two devices per channel. It is normally used for internal devices as the cables are large and flat.
 - **SATA:** Serial ATA deals with hot plugging and serial connectivity. The hot plugging technique may be used to replace computer components without shutting down the system. SATA enables only one connection per connector and is not flexible for industrial purposes.
 - **SCSI:** Small computer system interface (SCSI) allows multiple devices to be connected to a single port at the same time. SCSI uses a parallel cable for attaching internal and external devices.
- **nvSRAM:** Nonvolatile SRAM, or nvSRAM, has a faster read and write process (20 ns read and write access time) because of the presence of a standard asynchronous SRAM interface. nvSRAM ensures adequate data storage capabilities without the need for a battery during a shut down. nvSRAM is best used in applications that require high speed and nonvolatile storage at a low cost, such as in the medical industry. nvSRAM backups the data even in the event of a power failure.
- **Multiport memory controller:** An MPMC provides access to memory for up to eight ports. A memory controller can be present as a separate chip or as an integrated memory. It provides access to a memory bank, and helps achieve a high efficiency with random address accesses.
- **NAND flash memory:** Flash memory is a storage medium designed from electrically erasable programmable read-only memory (EEPROM). NAND and NOR are two types of flash memories. It provides a nonvolatile storage for the RAID system's primary cache. Its primary aim is to reduce cost and increase capacity. It does not require power to retain the data. It can improve its read-write cycles with reduced voltage demands.

- **SDRAM:** Synchronous dynamic random access memory or synchronous DRAM (sDRAM) is a memory that is synchronized with the processor's clock speed. This increases the number of instructions the processor can process. SDRAM speed is measured in Mega Hertz (MHz). It is divided into several sections called banks that allow the device to operate on several memory access commands simultaneously.
- **Disk:** The hardware presents the RAID to the host system as a single and large disk.

RAID Level 0: Disk Striping

-  RAID Level 0 splits data into blocks that are written evenly across **multiple hard drives**
-  It improves I/O performance by spreading the **I/O load** across several channels and disk drives
-  Data recovery **is not possible** if a drive fails
-  It requires a minimum of **two drives**
-  It does not provide **data redundancy**



RAID Level 0: Disk Striping

Depending on the requirement of your organization, you can choose any RAID level. RAID levels are based on performance, fault tolerance, or both.

RAID 0 deals with data performance. In this level, data is broken into sections and written across multiple drives. The storage capacity of RAID 0 is equal to the sum of the disks' capacities in the set. RAID 0 does not provide fault tolerance. It requires a minimum of two drives. It does not provide data redundancy. A failure of one disk can lead to the failure of all disks in a level 0 volume. The probability of recovering data from a RAID level 0 is minimal.

The data distribution in a RAID level 0 is equal among all the disk sets, resulting in high performance. With concurrent high performance, the throughput of the read and write operations on multiple disks is equal to the throughput of the array of disks. Increased throughput is an advantage of RAID 0, considering that data recovery is not available. Software and hardware RAID controllers support RAID 0, helping boost server performance.

Example: Assume that the IT infrastructure has a hard disk with high performance. The data in the hard disk is transferred at a remarkably high speed. All the large and critical files are stored in this disk. However, if this disk fails, the entire contents of the files will be affected, leading to the unavailability of the data. It is advisable not to store any critical data in a RAID level 0.

Advantages of RAID Level 0

- **Read and write performance:** RAID level 0 has a good read and write performance. The performance is even better when the controller supports independent reads and writes to different disks in the array.
- **Cost:** RAID level 0 is more cost effective than the other RAID levels.

- **Implementation:** Is easy to implement as the data is divided in a sequential set of blocks. There is no storage loss as the maximum capacity is utilized.

Disadvantages of RAID Level 0

- **No redundancy:** With no data redundancy, data loss is greater.
- **Noncritical data:** Data that is not critical to the organization can be stored on RAID level 0. This level does not use mirroring. Recovery is not possible if critical data is lost on RAID level 0.
- **Unreliable:** If one disk fails, the entire network will be affected.

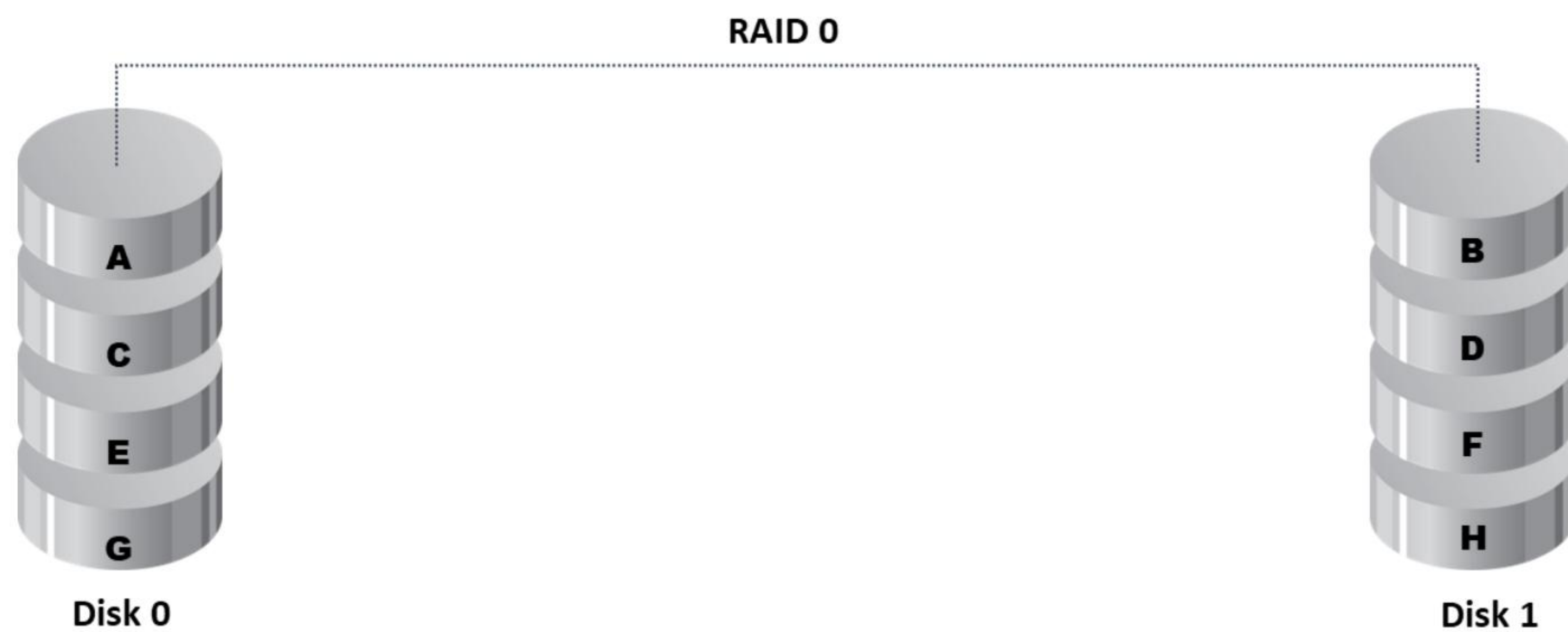
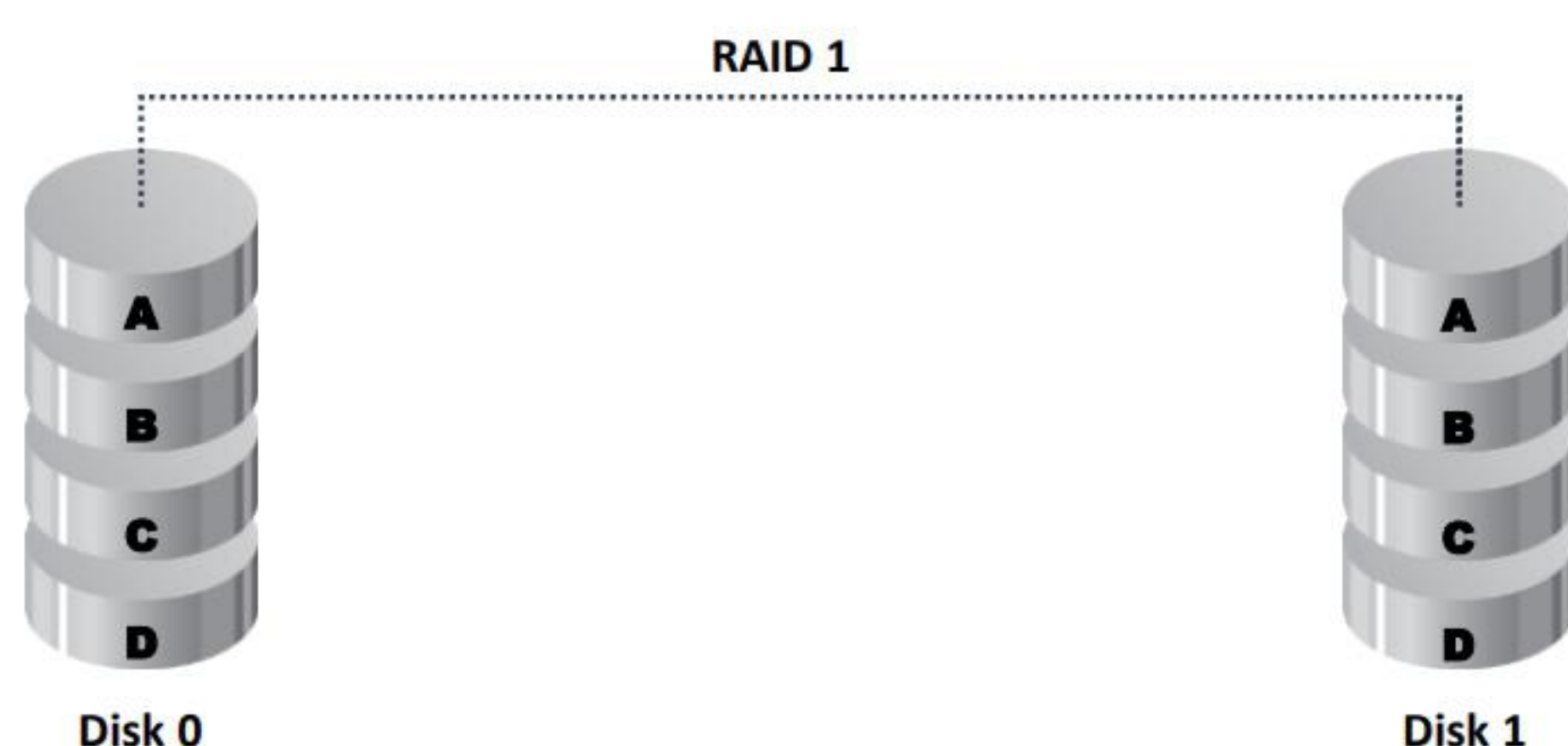


Figure 15.87: RAID level 0

RAID Level 1: Disk Mirroring

-  Multiple copies of data are written to **multiple drives** at the same time
-  It provides data redundancy by **duplicating the drive data** in multiple drives
-  If one drive fails, **data recovery** is possible
-  It requires a minimum of **two drives**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

RAID Level 1: Disk Mirroring

A typical RAID 1 contains an exact copy of the data on two or more disks. RAID 1 writes data on multiple drives and multiple mirror drives at the same time. The failure of one drive does not affect the data on other drives. This allows data retrieval from the mirror drive. Similar to RAID 0, RAID 1 provides no parity, stripping, or spanning of disk space across multiple disks. RAID 1 can be used in accounting, payroll, and other financial applications.

RAID 1 is suitable in environments where read performance matters more than write performance. RAID 1 has improved read performance because the data in a disk can be read at the same time simultaneously.

RAID level 1 provides data reliability in case of a disk failure as it can still provide access to the same data mirrored on other disks. In a RAID 1 hardware implementation, a minimum of two disks are required. In a software RAID 1, data can be copied to a disk volume. RAID 1 reduces the total disk capacity by half.

Example: If a RAID 1 server is configured with two 4 TB drives, the storage capacity will be 4 TB and not 8 TB.

The drive that accesses the data first will service the request. The write throughput in RAID 1 is always slower because every drive needs to be updated. Thus, its performance is limited by the slowest drive. It is only as fast as its slowest drive. RAID 1 will continue to function as long as there is at least one working drive.

Advantages of RAID Level 1

- **High read performance:** Because there are two disks, the read performance is higher in a RAID level 1 system. Data can be read simultaneously while being written on the other disk. Thus, the redundancy is excellent.

- **Compatibility:** RAID 1 is compatible with hardware and software RAID systems, including controllers.
- **Reliability:** The mirroring feature in a RAID 1 ensures the data will be available, making it more reliable than a RAID level 0.

Disadvantages of RAID Level 1

- **Capacity:** RAID level 1 undergoes duplexing, which needs twice the amount of disk space for storage.
- **Hot swapping unavailable:** If a disk fails to run, it cannot be replaced while the server is still in operation. This is called hot swapping. RAID level 1 does not support hot swapping.

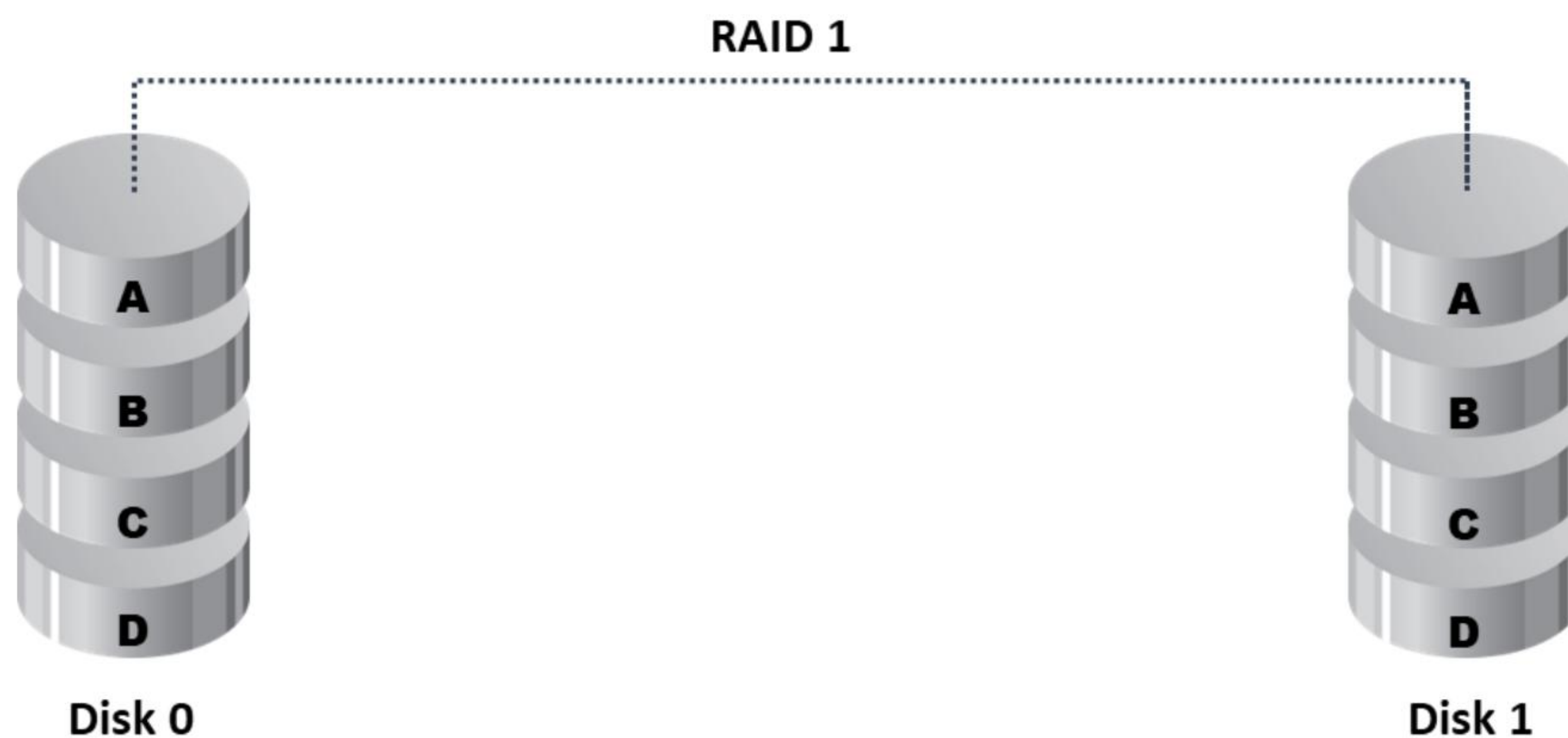
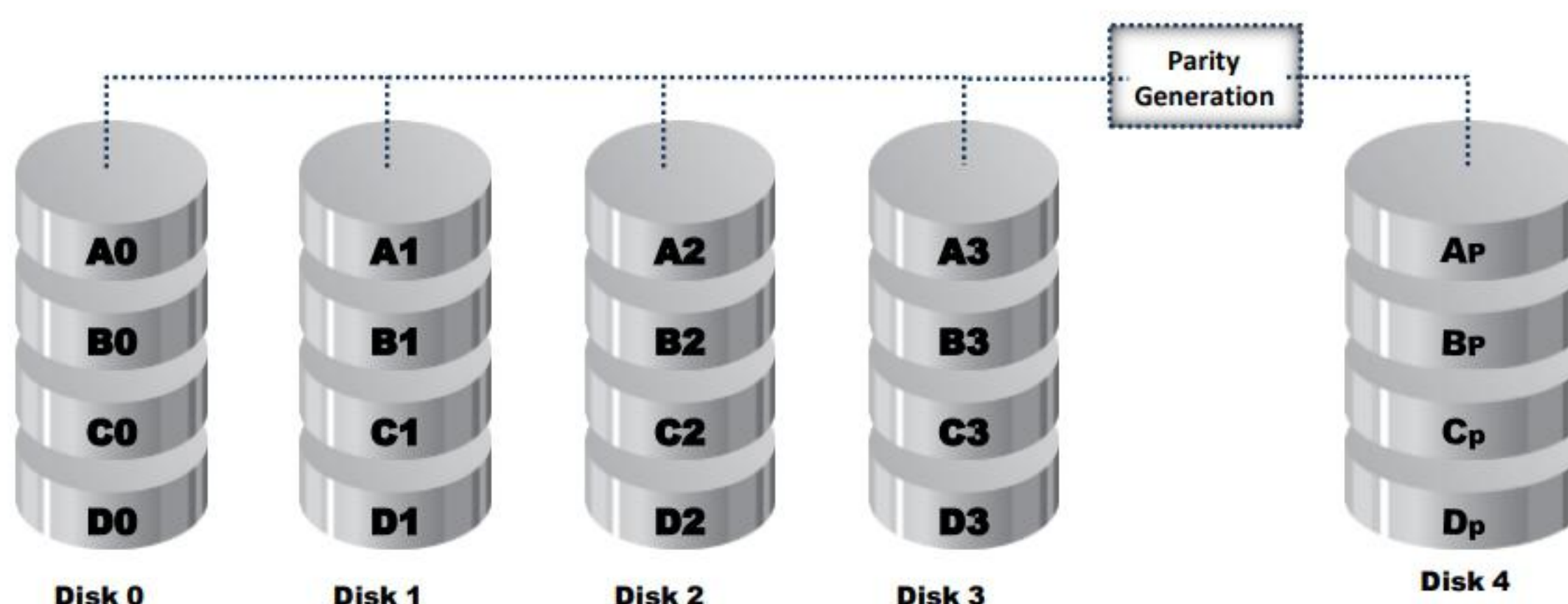


Figure 15.88: RAID level 1



RAID Level 3: Disk Striping with Parity

- 01** Data is striped at the **byte level** across multiple drives. One drive per set is taken up for parity information
- 02** If a drive fails, **data recovery and error correction** is possible using the parity drive in the set
- 03** The **parity drive** stores the information on multiple drives



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

RAID Level 3: Disk Striping with Parity

RAID level 3 is disk striping with parity. It uses striping and parity as its main features to store data. To implement a RAID level 3 system, a minimum of three disks are required. The data is stored on multiple drives at the byte level. This RAID level dedicates one drive to store the parity information. The byte level division allows the drives to work simultaneously. At any point in time, either a read operation or a write operation can take place. RAID 3 is a good choice for specialized databases or single-user systems.

The RAID level 3 has a high transfer data rate along with data security. It can perform data recovery and error correction by calculating an exclusive OR (XOR) of the information recorded on the parity drive.

Advantages of RAID Level 3

- **High throughput:** RAID level 3 provides a high throughput for read and write operations for large data transfers.
- **Resistant:** This RAID level is resistant to disk failures and breakdowns.

Disadvantages of RAID Level 3

- **Complexity:** Installation and configuration of a RAID level 3 system is complex. Its implementation necessitates a larger number of resources.
- **Slow performance:** Random operations affect its performance, thereby reducing its speed.

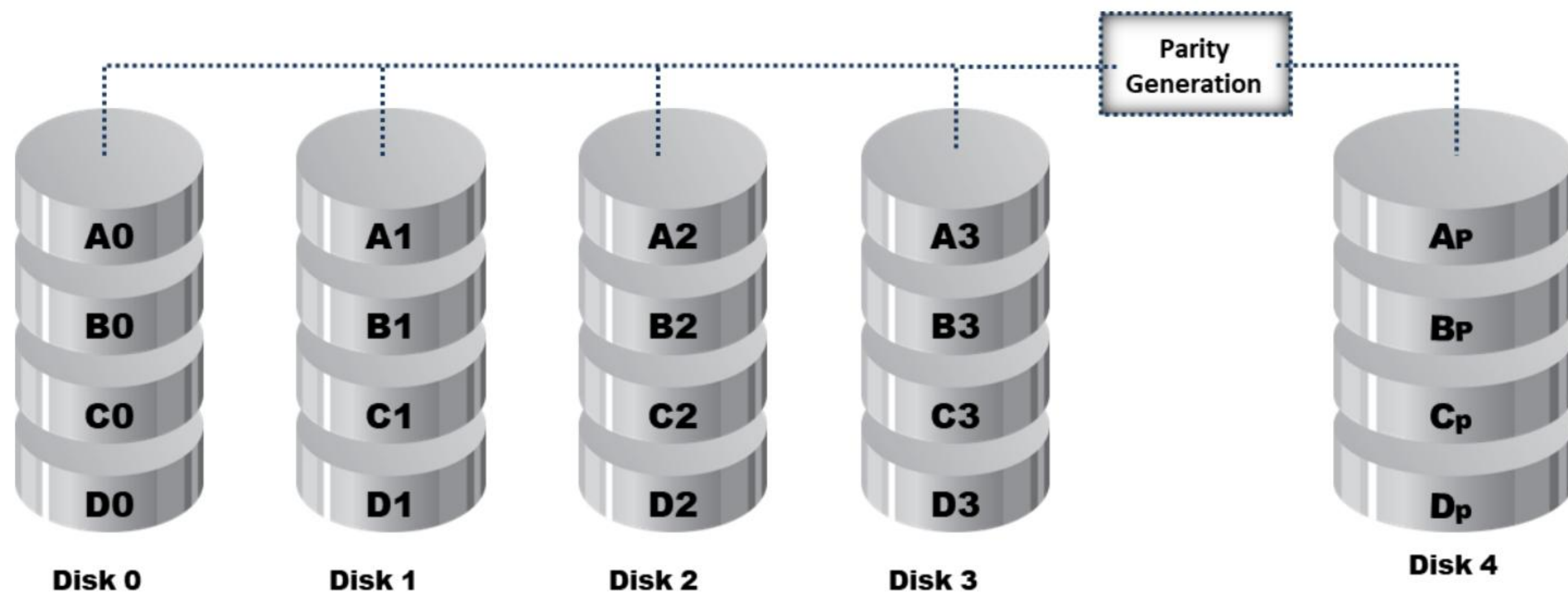
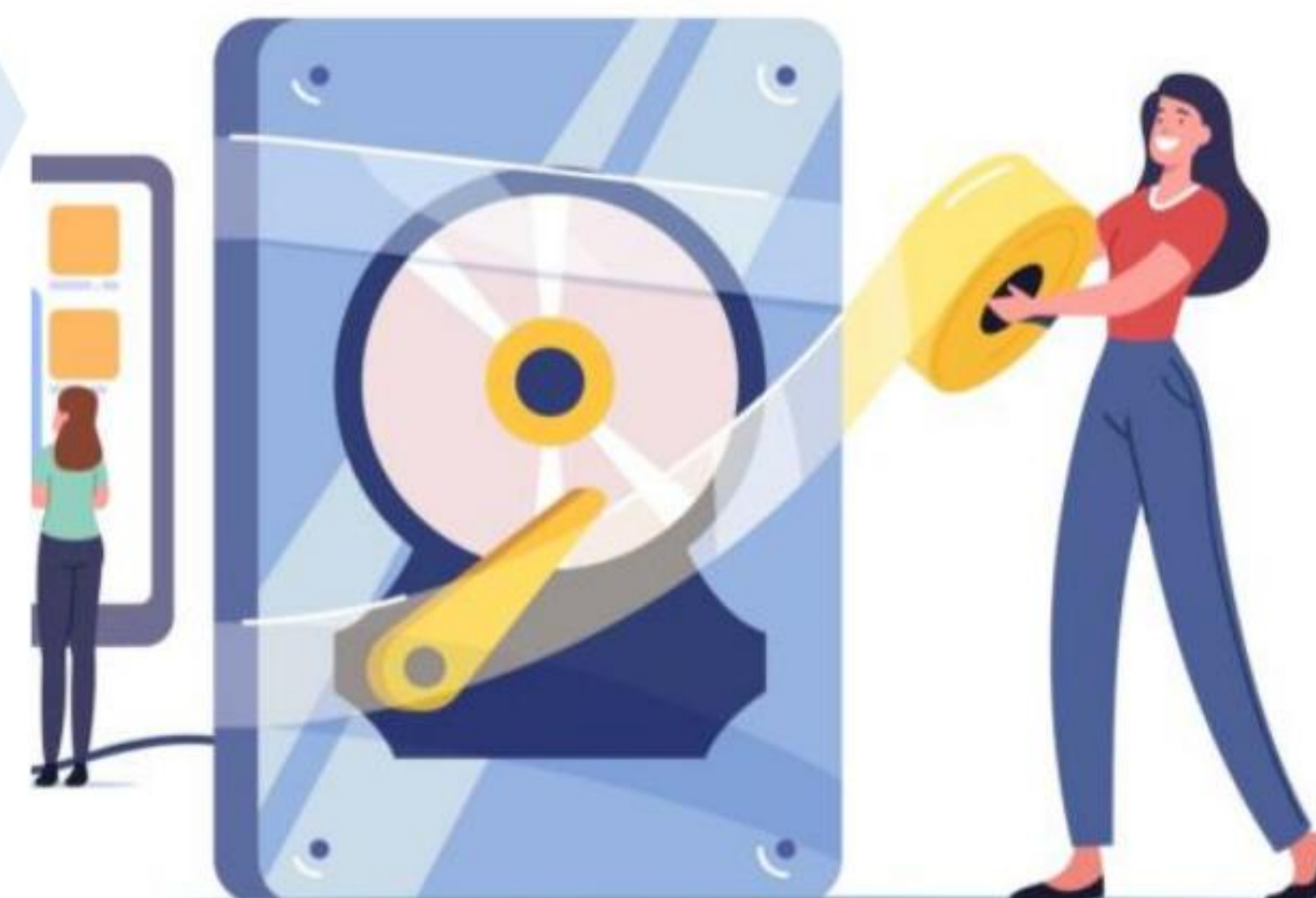
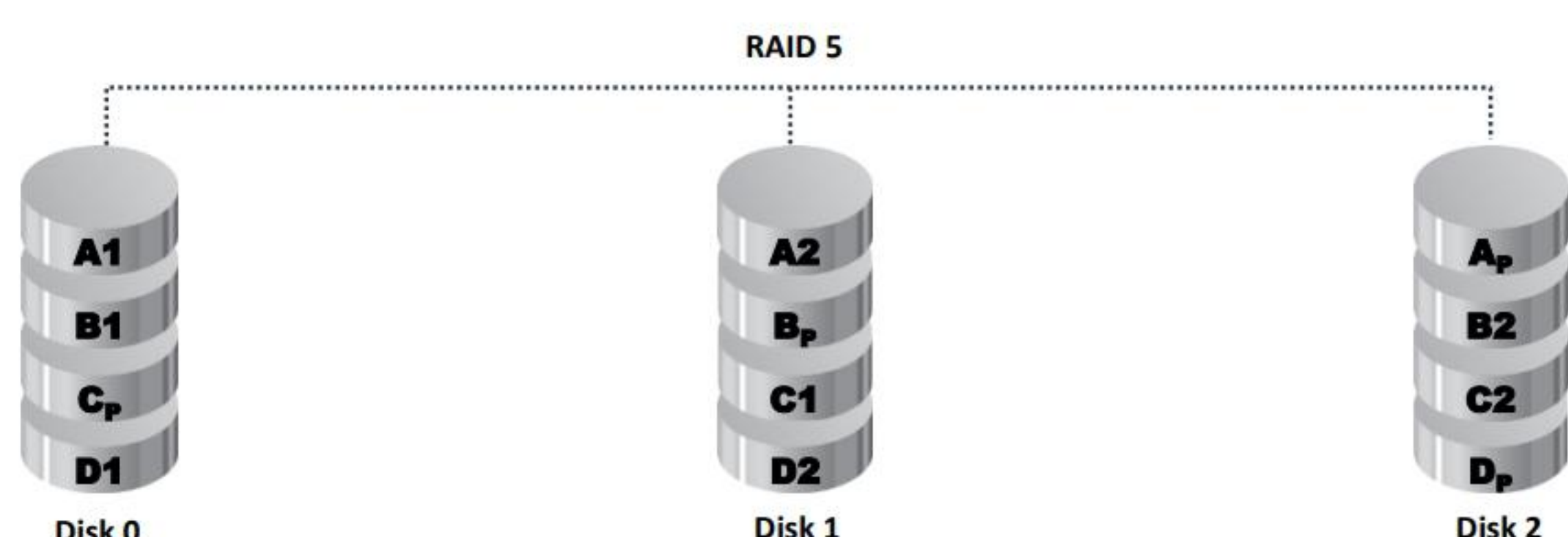


Figure 15.89: RAID level 3

RAID Level 5: Block Interleaved Distributed Parity

- 1 The data is striped at the byte level across multiple drives, and the parity information is distributed among all the member drives
- 2 The **data writing** process is slow
- 3 This level requires a minimum of **three drives** to be set up



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

RAID Level 5: Block Interleaved Distributed Parity

RAID level 5 involves a block-interleaved distributed parity; it includes a block-level striping with a distributed parity. The parity information is distributed among all drives except one. The data chunks in a RAID level 5 system are larger than the regular I/O size, but they can be resized. To prevent data loss following a drive failure, data can be calculated from the distributed parity.

The RAID 5 needs at least three disks; however, more than three disks can be used for a better performance. RAID 5 is not a good choice for write operations on the system. Rebuilding the RAID 5 array following a disk failure takes a long time. The performance can be degraded when the array is being rebuilt, making it vulnerable to additional disk failures. This level offers significantly better read performance as the disks independently process the data requests.

RAID 5 is most often found in file and application servers, database servers, along with web, email, and news servers.

Advantages of RAID Level 5

- **Read data:** Among all RAID levels, level 5 has the highest read data transaction rates.
- **Withstand failure:** RAID 5 can withstand the failure of a single drive and is not affected by the loss of data.
- **Hot swapping:** In case of a disk failure, the failed disk can be replaced with a new one, without a server shutdown.

Disadvantages of RAID Level 5

- **Slow write operation:** Servers built using RAID 5 suffer from performance issues with write operations, and these can eventually result in reduced speeds.

Example: Employees accessing a database on a RAID 5 server will reduce the server's production time.

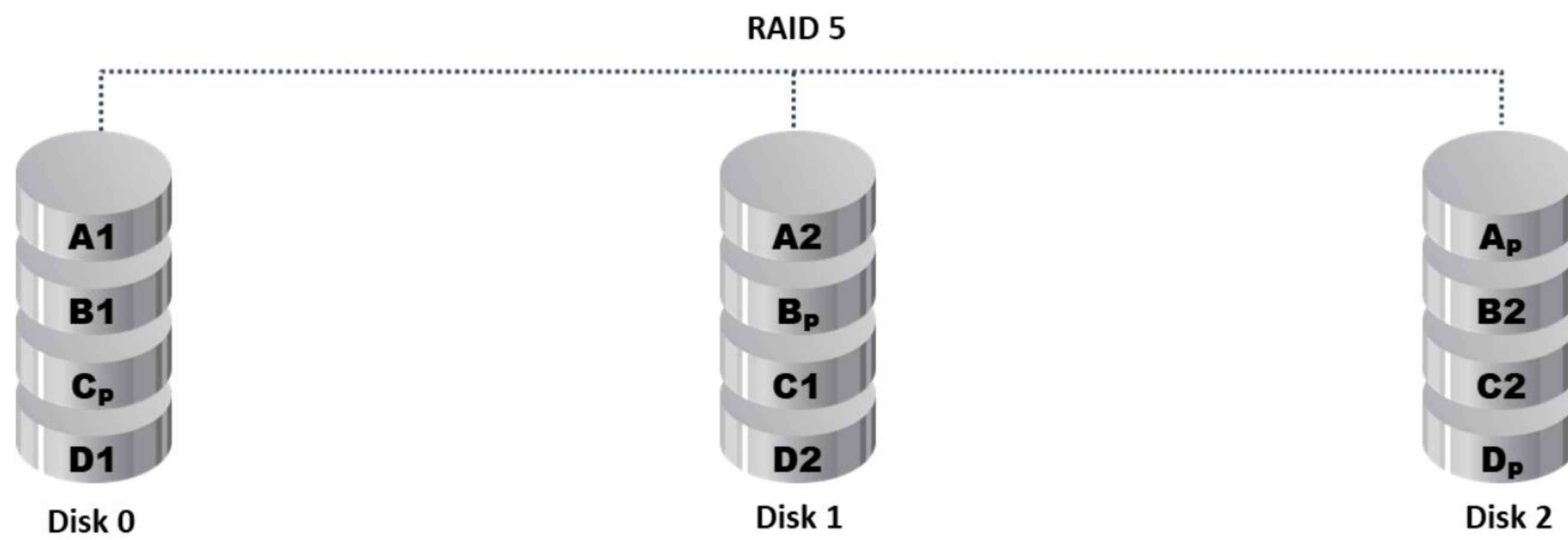
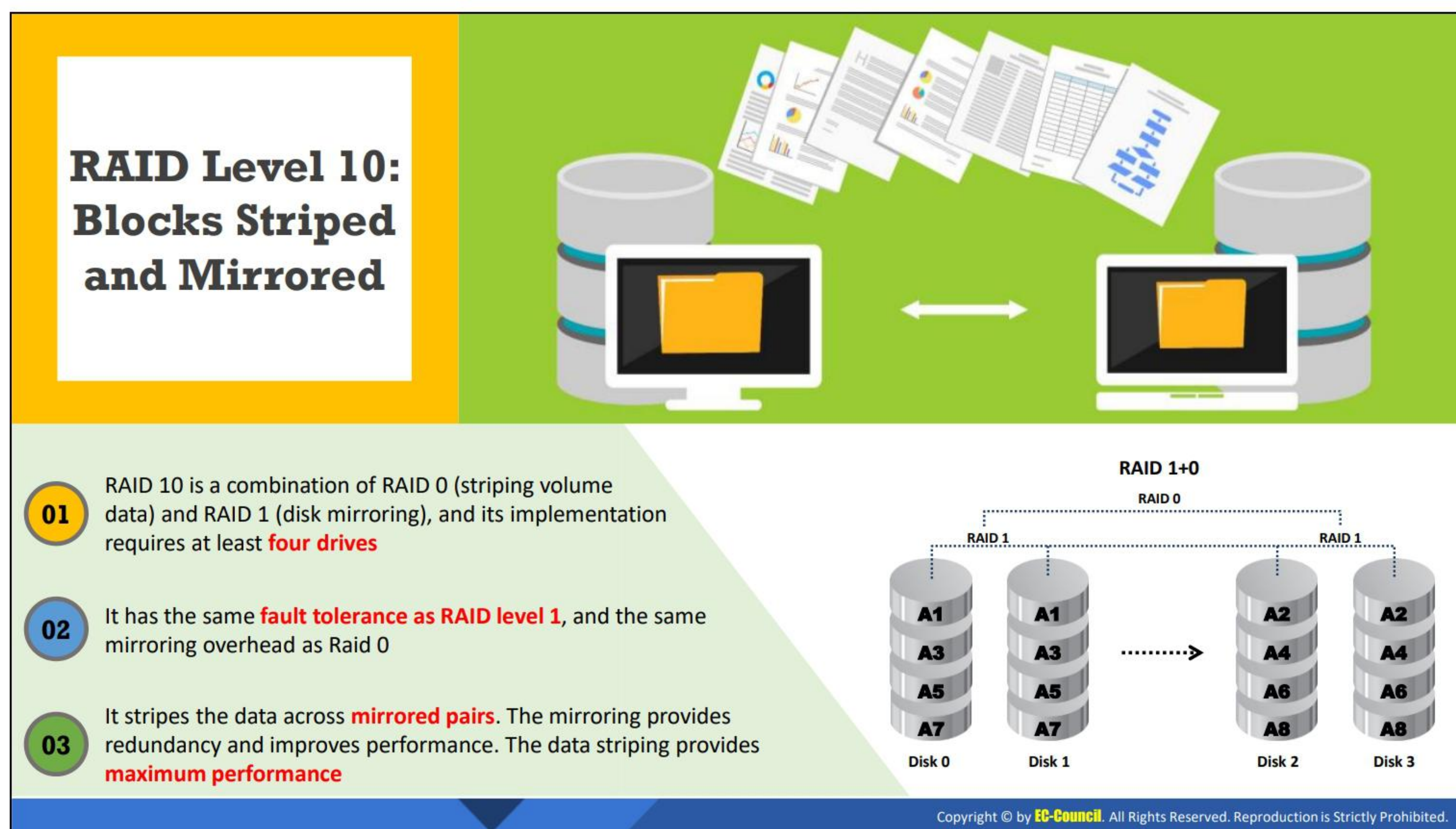


Figure 15.90: RAID level 5



RAID Level 10: Blocks Striped and Mirrored

RAID level 10 includes disk striping and mirroring in a nested hybrid RAID level. It is a combination of RAID level 1 and RAID level 0. It is also called as a “stripe of mirrors.” This level can symbolically be represented as RAID 1+0 or RAID 10. RAID 10 includes the mirroring of RAID 1 without parity and the striping of RAID 0. The performance of RAID 10 is higher than a RAID 1. RAID level 10 has the same fault tolerance as RAID level 1. It requires a minimum of four drives for its operation. RAID 10 is a great choice for database servers, web servers, email servers, etc., and can be implemented on hardware or software. The mirroring provides redundancy and improves performance. The data striping provides maximum performance.

Advantages of RAID Level 10

- **Improved I/O operations:** With a combination of RAID levels 1 and 0, it provides improved I/O operations.
- **Better throughput:** Compared with other RAID levels, RAID 10 provides better throughput and higher latency.
- **Efficient write operations:** The write operations are efficient in this level. Therefore, RAID 10 is often implemented on database servers and other servers that perform write operations.

Disadvantages of RAID Level 10

- **Expensive:** RAID 10 is expensive than other RAID levels as it requires twice as many disks.

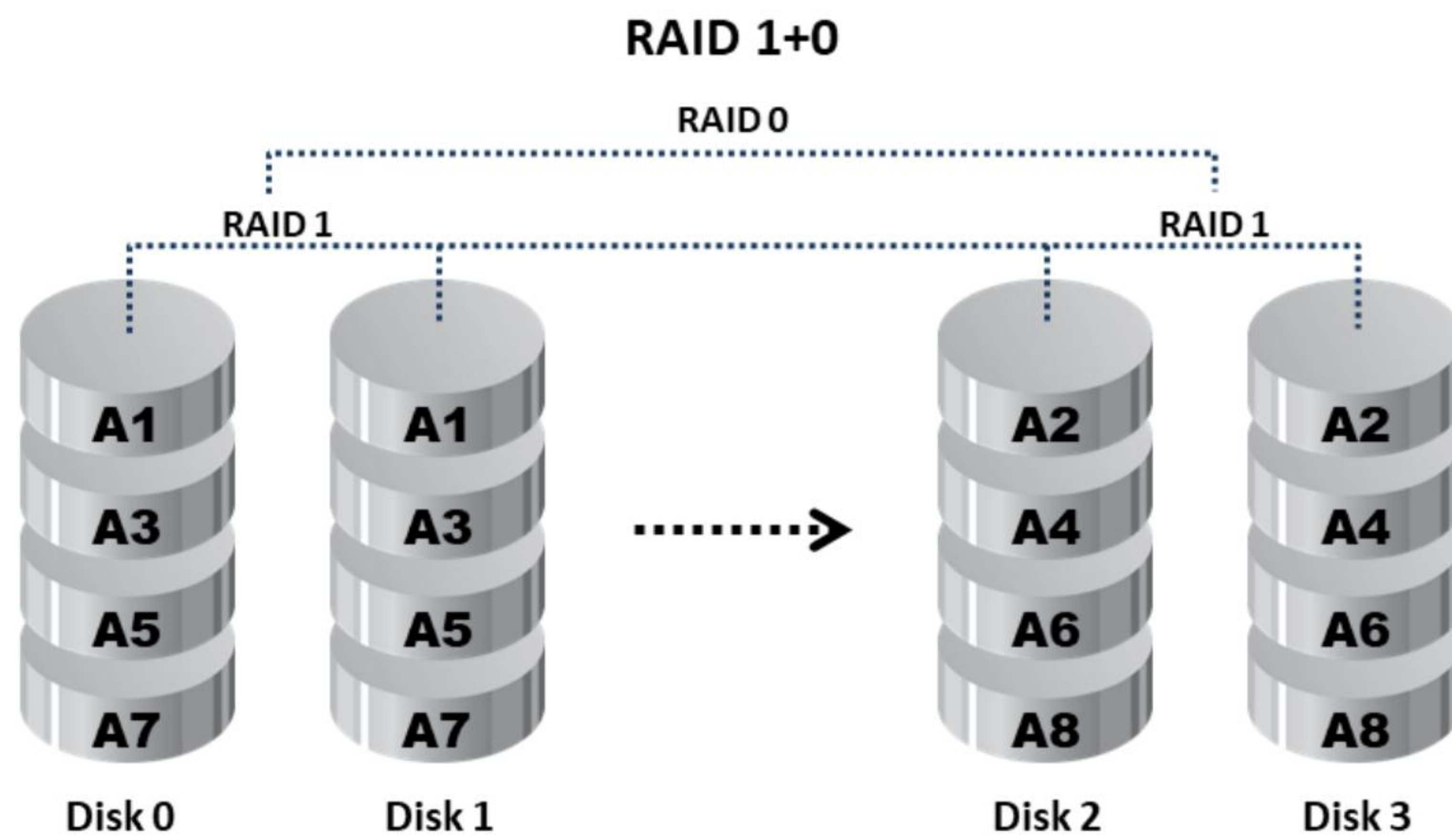
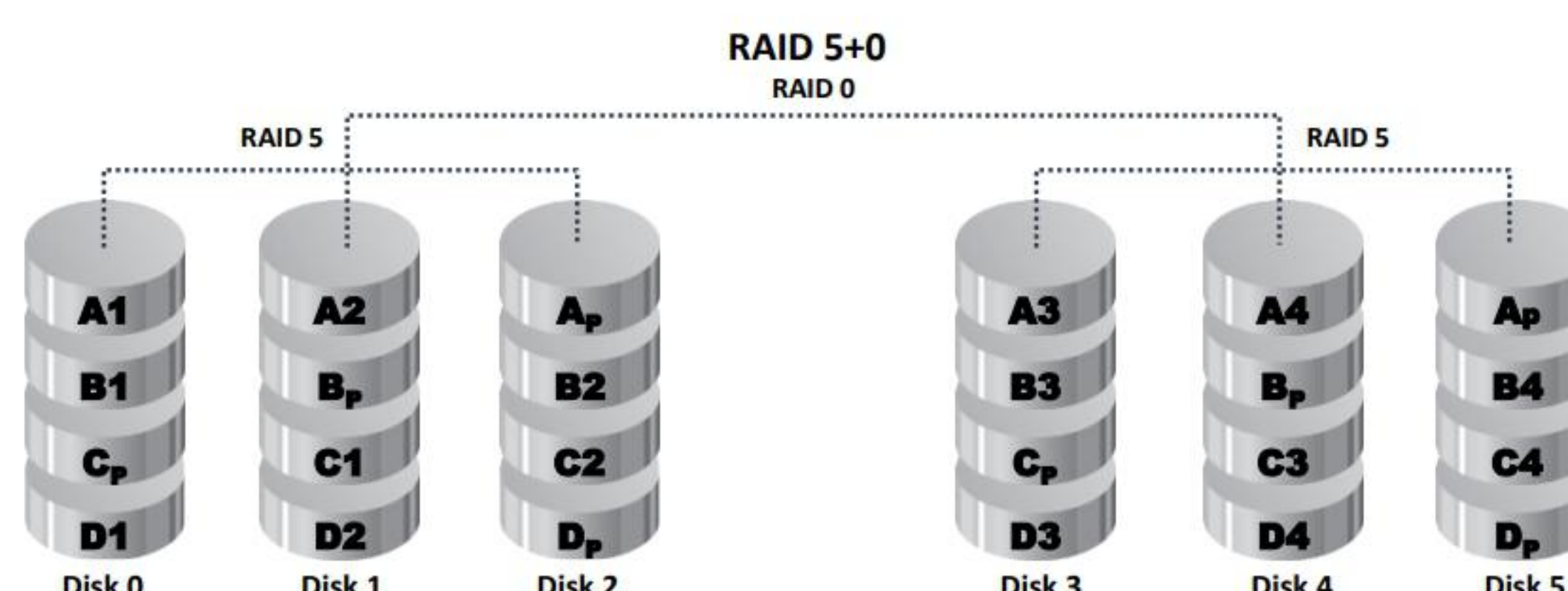


Figure 15.91: RAID level 10

RAID Level 50: Mirroring and Striping across Multiple RAID Levels



- ❑ RAID 50 is a combination of **RAID 0 striping** and the distributed parity of **RAID 5**
- ❑ It is **more fault tolerant** than a RAID 5 but uses twice the parity overhead
- ❑ A minimum of **six drives** are required for setup. A drive from each segment can fail and the array will recover. If more than one drive fails in a segment, the array will stop functioning.
- ❑ This RAID level offers better reads and writes than a RAID 5 and the highest levels of **redundancy** and **performance**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

RAID Level 50: Mirroring and Striping across Multiple RAID Levels

RAID level 50 includes mirroring and striping across multiple RAID levels. This level is a combination of a level 0 block-level striping and a level 5 distributed parity. The configuration of RAID level 50 requires a minimum of six drives. This level undergoes a hot swapping process when a disk fails. A drive from each segment can fail and the array will recover. If more than one drive fails in a segment, the array will stop functioning.

RAID 50 is an improvement over RAID 5, specifically for its write operation and fault tolerance. RAID level 50 can be implemented on servers that run applications requiring higher fault tolerance, capacity, and random access performance. This level offers data protection and faster rebuilds than a RAID 5 system. A failed disk in a segment only affects that segment and not the entire array. Only that segment is then rebuilt. The rest of the array functions normally.

Advantages

- **Security:** The data stored in a RAID 50 is more secured than in a RAID 5. With a larger storage capacity, this level offers better security than RAID 5.
- **Nondegradable:** With the use of a minimum of six drives in the configuration, failure of one disk does not impact the server function on this level.
- **Read and write performance:** The read and write performance of RAID level 50 is far better than RAID level 5.

Disadvantages

- **Controller:** Only a sophisticated controller can handle RAID level 50.

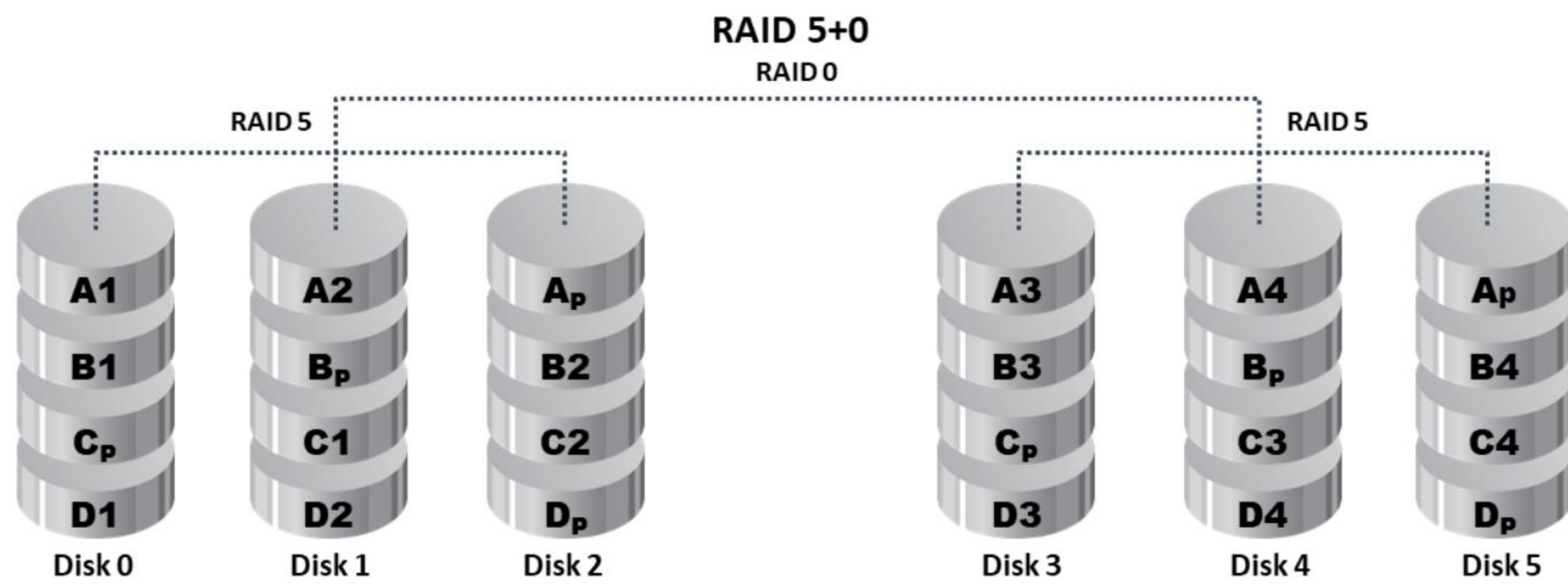
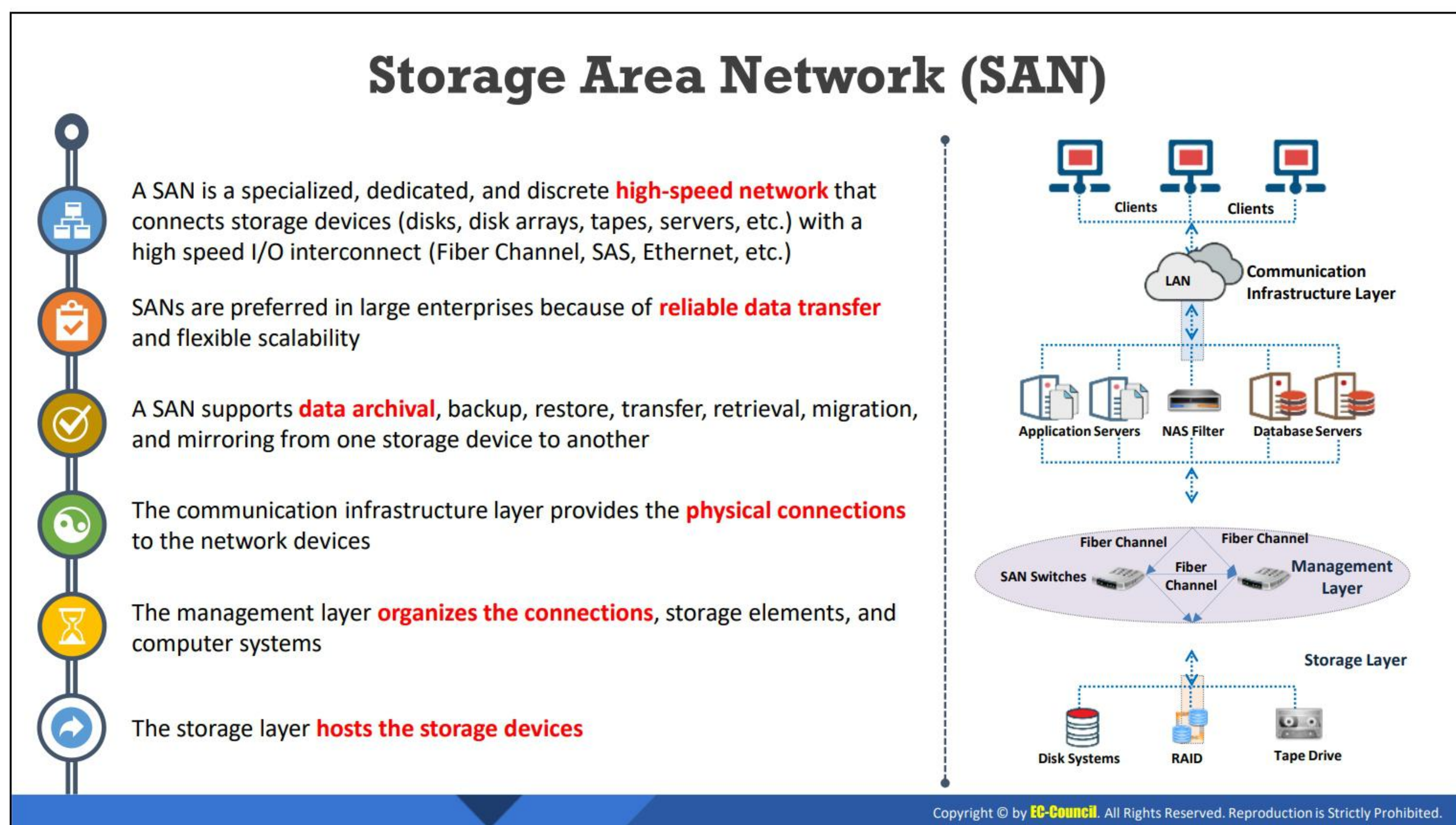


Figure 15.92: RAID level 50



Storage Area Network (SAN)

A storage area network (SAN) is a high performance network that interconnects storage devices with multiple servers. The role of a SAN is to transfer stored resources available on the common network and reorganize them on an independent and high-performance network. This helps the servers to share their storage across the network. Primarily, a SAN enhances storage devices such as tape drives, disk drives, file servers, RAID, etc. A SAN implementation makes disk maintenance controllable and easier. The implementation needs a cable, a switch, and host bus adapters. Each storage system on the SAN must be interconnected, and in case of a physical interconnection, the bandwidth should support extreme data activities.

We know that systems in a network connect to storage devices. However, a SAN implementation is necessary to ensure that all systems in a network are connected to each available storage device on the network. SAN allows these systems to take the ownership of storage devices; systems can exchange the ownership of storage devices among themselves.

Understanding Storage Sharing

The working of a SAN depends on client-server communication. Every organization has multiple servers that are connected to the systems.

Example: If computer A needs some data from computer B, it will need a copy of the data from the server to which computer B is connected. This can be done through file transfer, inter-process communication, and backup. Although the data is transferred from computer B to computer A, it is possible that computer A may encounter untimely data errors, an expensive transfer between the two servers, or other operational processes. SAN architecture is the perfect solution for this issue. In SAN architecture, all servers are connected to storage devices such as tape drives, RAIDs, disk systems, etc. through a fiber channel. Thus, instead of

communicating with computer B for the data, computer A can directly get a copy of the data from the storage devices connected to the servers. For this process to be successful, data storage devices act as a common access point for all the servers.

SAN storage sharing eliminates the scheduling of data transfers among servers. It reduces the cost of data transfer among servers. Storage devices help in timely transfer of data. SAN storage offers only block-level operations that do not provide file abstraction.

However, if the file systems are structured on top of SAN, file access is provided which is known as a SAN file system.

Now-a-days, in large organizations, SAN is a storage pool for servers that are connected via a network. The fiber channel is now replaced by iSCSI, which has become the choice of many mainstream organizations. Whatever be the size of the organization, SAN has become a consolidation of workloads in the network.

A SAN supports data archival, backup, restore, transfer, retrieval, migration, and mirroring from one storage device to another. The communication infrastructure layer provides the physical connections to the network devices. The management layer organizes the connections, storage elements, and computer systems. The storage layer hosts the storage devices.

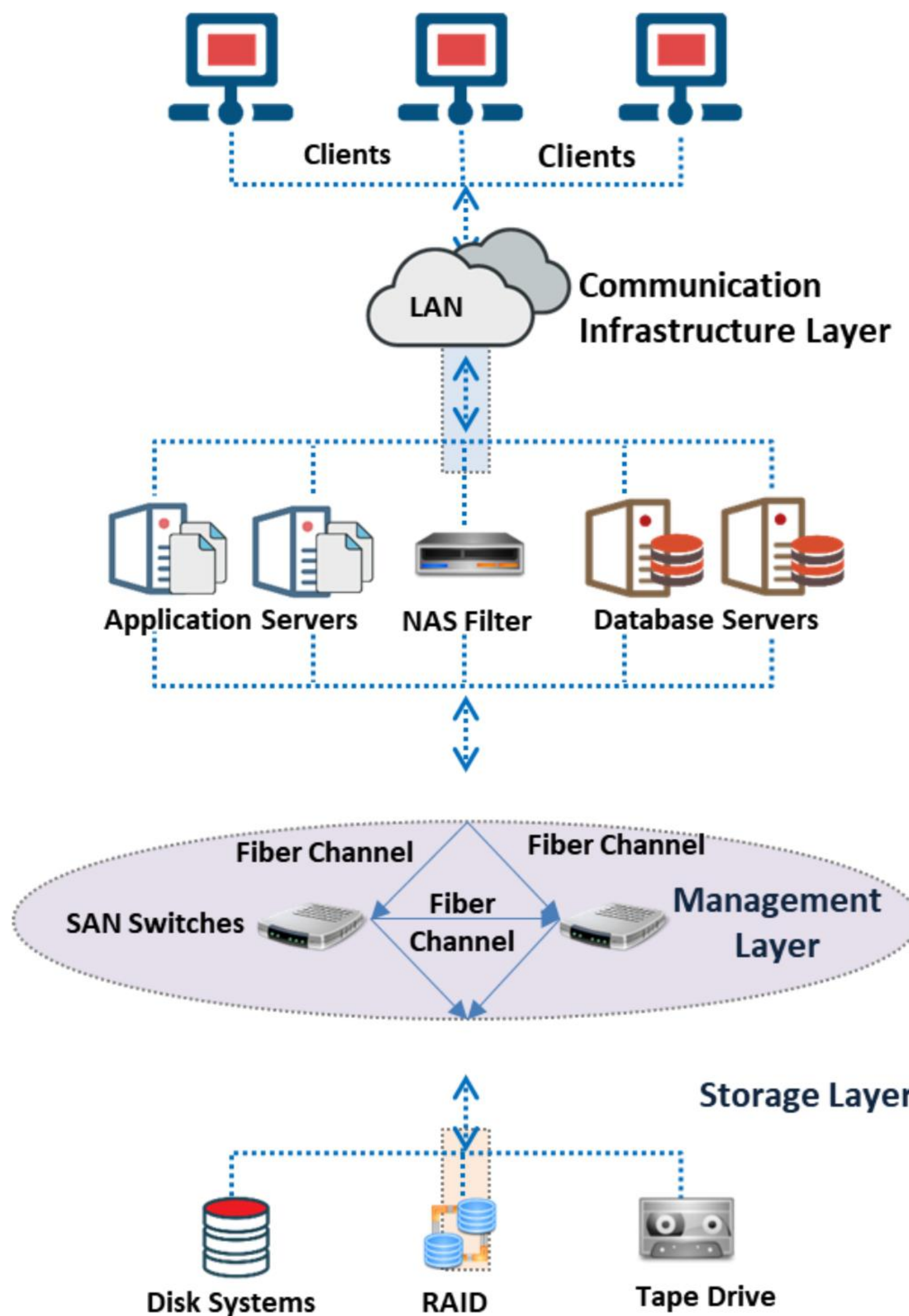
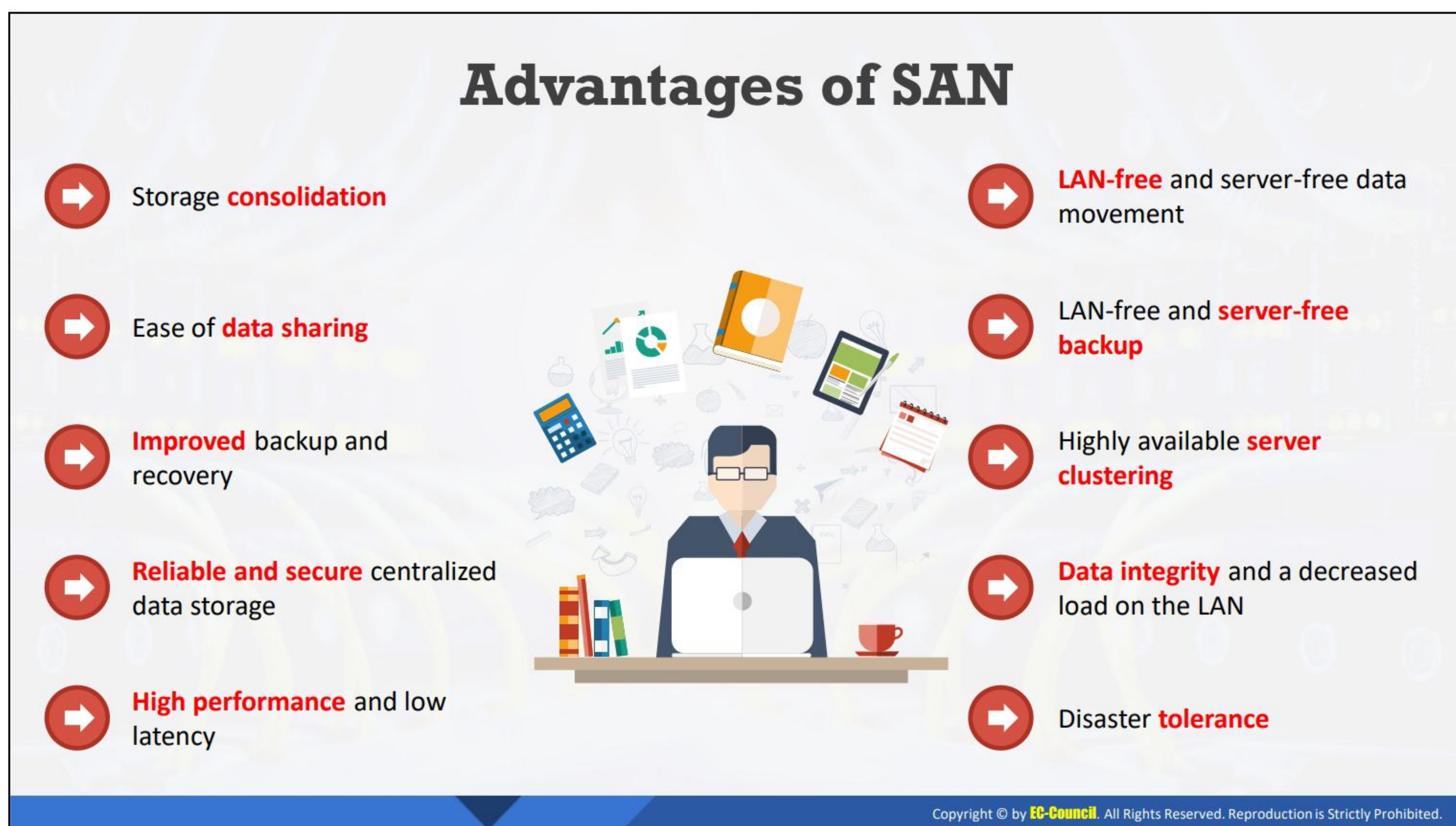


Figure 15.93: SAN



Advantages of SAN

storage device that can fulfill and handle their needs. The below-mentioned advantages of SAN help in its deployment in an IT infrastructure.

Advantages

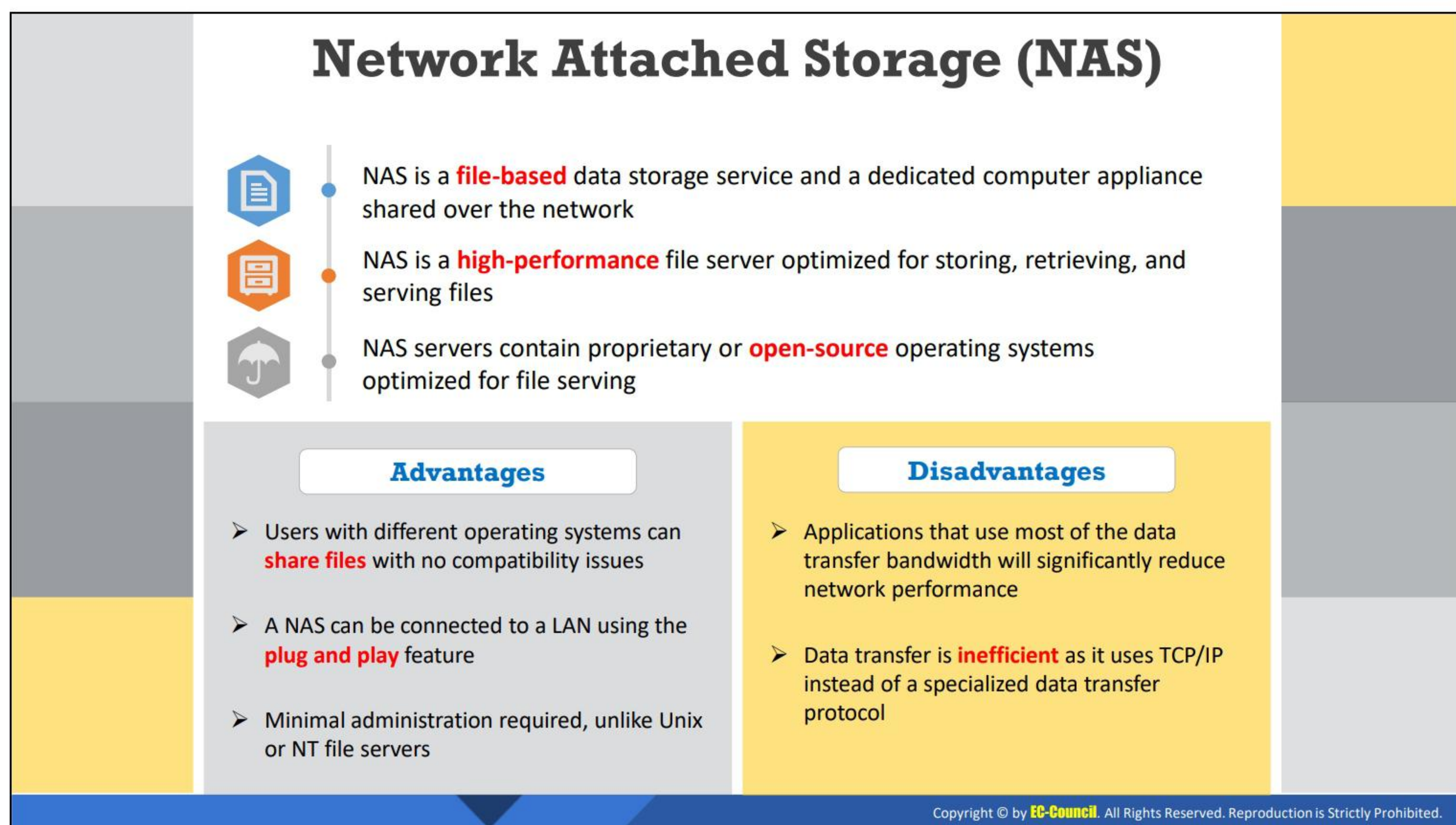
- **Capacity:** SAN performance is directly proportional to the network type. A SAN allows unlimited sharing of data, regardless of the storage capacity. Its capacity can be extended limitlessly to thousands of terabytes.
- **Easy sharing:** SAN data is easily shared between systems as it maintains an isolated traffic. The traffic does not interfere with the normal user traffic, thereby increasing data transfer performance.
- **Fast backup:** A data mirror copy can be created instantly. These mirror images can be used as a backup whenever required.
- **Reliability and Security:** If a SAN is configured correctly, the data is secured. Chances of device intrusion is minimal. Reliable and secure centralized data storage.
- **Productive:** A SAN is scalable; adding a new disk to the network does not stop the SAN's productivity. When adding a new hard disk, a reboot or shut down is not required.
- **Availability of applications:** The algorithms in a SAN storage array offer data protection. This results in the availability of applications at all times.
- **Bootable:** A SAN can run a server without a physical disk, and it can be booted by the SAN. This feature permits access to all page files and applications.

- **Distance connectivity:** For better security, storage devices can be kept at an isolated location. One of the features of a SAN is that it can connect with devices up to a distance of ten kilometers.
- **Recovery:** A SAN is the most reliable data recovery option. Even when the servers are offline a SAN remains available.
- **Effective utilization:** A SAN is an appropriate option for storage space than local disks. If a system requires more storage, a SAN dynamically allocates the required space. This process is similar to virtual machines.
- **Integrity:** Increased data integrity and a decreased load on the LAN.
- LAN-free and server-free data movement and backup
- Effective disaster tolerance

The implementation of a SAN is beneficial to an organization, especially when considering budget constraints, availability, and employee expertise.

Disadvantage

- **Very costly:** The implementation cost of a SAN can significantly exceed the available budget. A SAN is an investment and should only be implemented if it meets the goals of the organization.



Network Attached Storage (NAS)

NAS is a storage device connected to a network. It stores and retrieves data from a centralized location. NAS provides a dedicated shared storage space for a local area network. Implementing a NAS eradicates the server file sharing process on the network. The NAS contains one or more logically arranged storage devices. NAS offers file storage through a standard Ethernet connection.

NAS devices do not use an external device management, and they are operated through a web-based utility. Since it resides on every node on the LAN, it has its own IP address. NAS is similar to a file server. NAS devices are scalable, vertically as well as horizontally. A NAS implementation is accomplished using large and clustered disks.

NAS has evolved from supporting virtualization to data replication and multiprotocol access. A clustered NAS is one such example of the NAS evolution. In a clustered NAS infrastructure, access is provided to all files, irrespective of their physical location. It does not require a closed-source operating system such as Windows. Certain devices run on a stripped down OS such as FreeNAS, or any other open-source solutions.

NAS devices are in high demand in small enterprises because of their effectiveness, low cost, and scalable storage capacity. They are classified into three types based on the number of drives, drive capacity, and scalability.

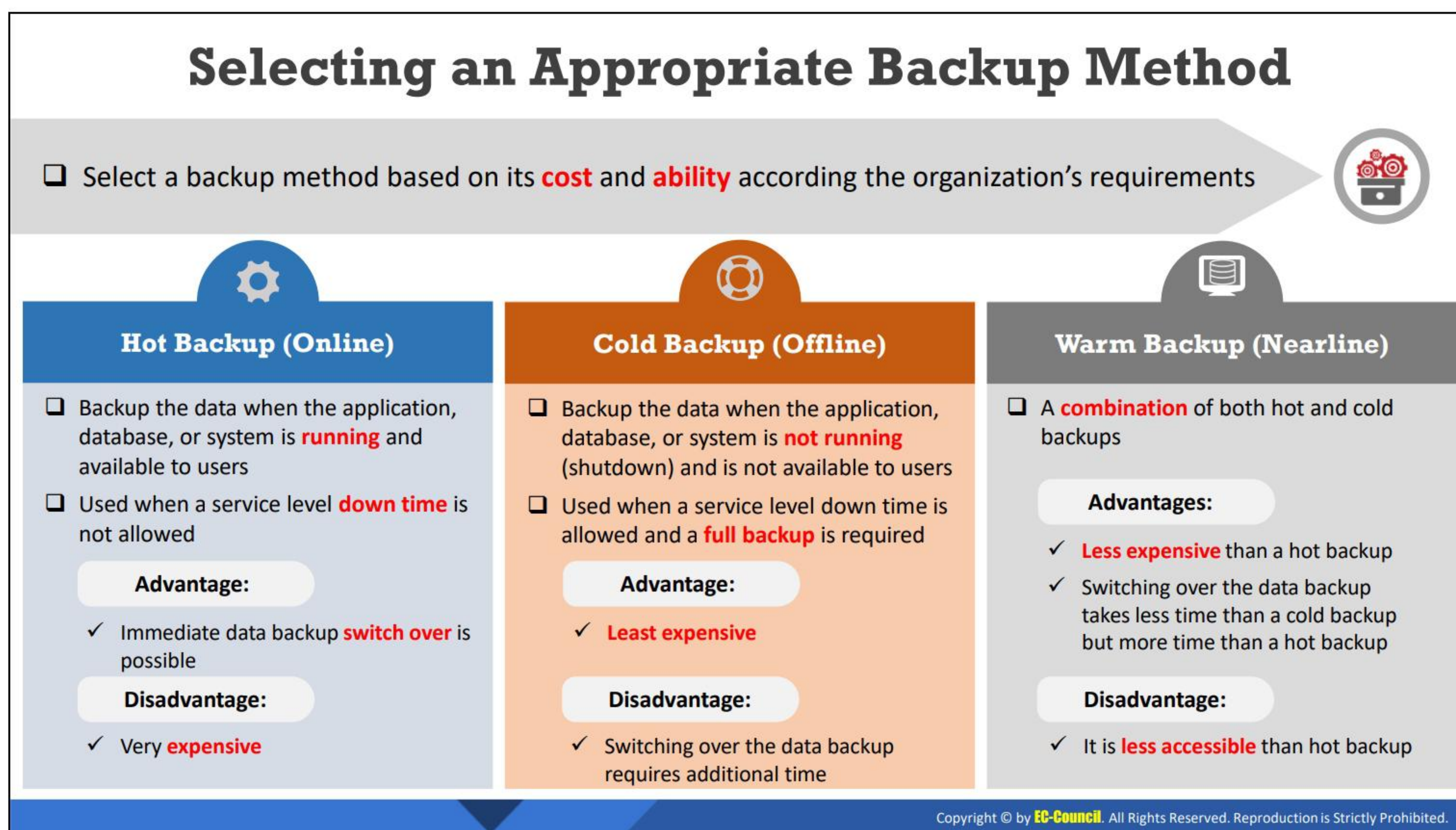
Advantages

- **Accessibility:** A NAS system stores data as files and is compatible with CIFS and NFS protocols. Multiple users can access the files simultaneously using an Ethernet network. Computers in a shared network can access the data either through a wireless or a wired connection.

- **Storage:** NAS deployment in a network increases the amount of storage available to the other systems. A NAS system can store up to 8 TB data. A NAS is most appropriate for storing large applications or video files.
- **Efficient and Reliable:** NAS assures an efficient transfer of data and reliable network access. If a system in a network fails, the functioning of other systems is not affected. A NAS server can also be created to give users the ability to access large files or applications.
- **Automatic backup:** Certain NAS devices are configured with an automatic backup feature. The data is available on the user system as well as on the server hard drive. Changes made on the user system are reflected on the server hard drive as well. Automatic backup is not time consuming and assures the security of data.
- **Compatibility:** Users with different operating systems can share files with no compatibility issues.
- A NAS can be connected to a LAN using the plug and play feature.
- Minimal administration required, unlike Unix or NT file servers.
- Centralized usage, and reduced cost of backup and maintenance than a SAN.
- Faster response than direct attached storage (DAS).

Disadvantages

- **Consumption:** NAS shares the network with other host machines, and this tends to consume a larger amount of network bandwidth. For remote NAS systems, the data transfer performance will depend on the available bandwidth. It is advisable to avoid storing databases on a NAS, as the server response time fluctuates depending on the bandwidth. Applications that use most of the data transfer bandwidth will significantly reduce network performance.
- **Network congestion:** A large backup process can affect the function of an IP network and may lead to network congestion.
- Data transfer is inefficient as it uses TCP/IP instead of a specialized data transfer protocol.
- The storage service cannot be trusted for mission-critical operations.
- Administrators must set user quotas for storage space.



Selecting an Appropriate Backup Method

Organizations can choose any backup method depending on their budget and IT infrastructure. The different types of data backup methods are:

▪ Hot Backup

A hot backup is a popular backup method. It is also called as dynamic backup or active backup. In a hot backup, the system continues to perform the backup even when the user is accessing the system. Implementation of a hot backup in an organization avoids downtime. However, changes made to the data during the backup process is not reflected in the final backup file. In addition, while the backup is in process, the users may find the system to be slow. A hot backup is an expensive process. It is used when a service level down time is not allowed.

Advantage:

- Immediate data backup switch over is possible

Disadvantage:

- Very expensive

▪ Cold Backup

A cold backup is also called an offline backup. A cold backup can take place when the system is not working or is not accessible by users. A cold backup is the safest backup method as it avoids the risk of copying the data. A cold backup involves downtime as the users cannot use the machine until the process is back online. A cold backup is not as expensive as a hot backup. It is used when a service level down time is allowed and a full backup is required.

Advantage:

- Least expensive

Disadvantage:

- Switching over the data backup requires additional time

▪ **Warm Backup**

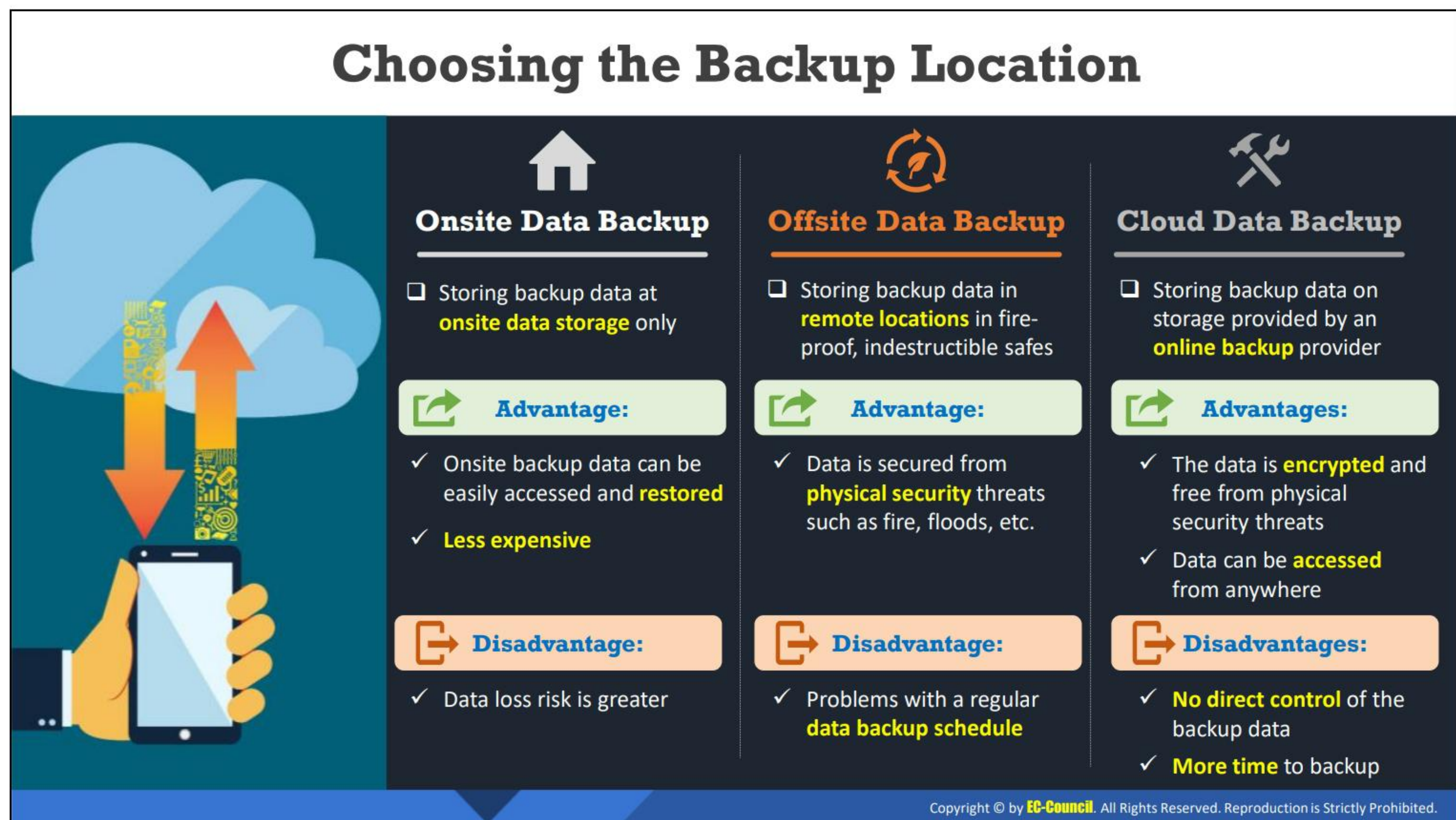
A warm backup is also called a nearline backup. It will have a connectivity to the network. In a warm backup, the system updates are turned on to receive periodic updates. It is beneficial when mirroring or duplicating the data. The warm backup process can take a long time and can be conducted in intervals that can last from days to weeks. It is a combination of both hot and cold backups.

Advantage:

- Less expensive than a hot backup
- Switching over the data backup takes less time than a cold backup but more time than a hot backup

Disadvantage:

- It is less accessible than hot backup



Choosing the Backup Location

Onsite Data Backup

This type of backup is performed within an organization. Onsite backup uses external devices such as a tape drive, DVD, hard disk, etc. The choice of external storage will depend on the amount of data to be backed up.

- **Advantages:**

- Provides immediate access to data.
- Less expensive.
- Media used for onsite backup is readily available and costs less.
- Faster recovery.
- Enhanced scalability.
- Internet access is not required.

- **Disadvantages:**

- Requires direct human interaction to perform the backup.
- Susceptible to theft or natural disasters.
- Data loss risk is greater.

Offsite Data Backup

In an offsite backup, the backup is done at a remote location in fire-proof, indestructible safes. It either stores the data on physical drives, online, or a third-party backup service. Storing the data online helps in having an updated data backup available.

- **Advantages:**

- Implementing offsite backup creates multiple copies that can be stored in multiple locations.
- Human error is minimal as the backup process is automated.
- Data retention is unlimited.
- Data is secured from physical security threats such as fire, floods, etc.

- **Disadvantages:**

- Problems with a regular data backup schedule.
- It is expensive, requiring a third-party service.
- Requires an Internet connection, and the bandwidth consumption will be higher.
- The process is lengthy and time consuming.

Cloud Data Backup

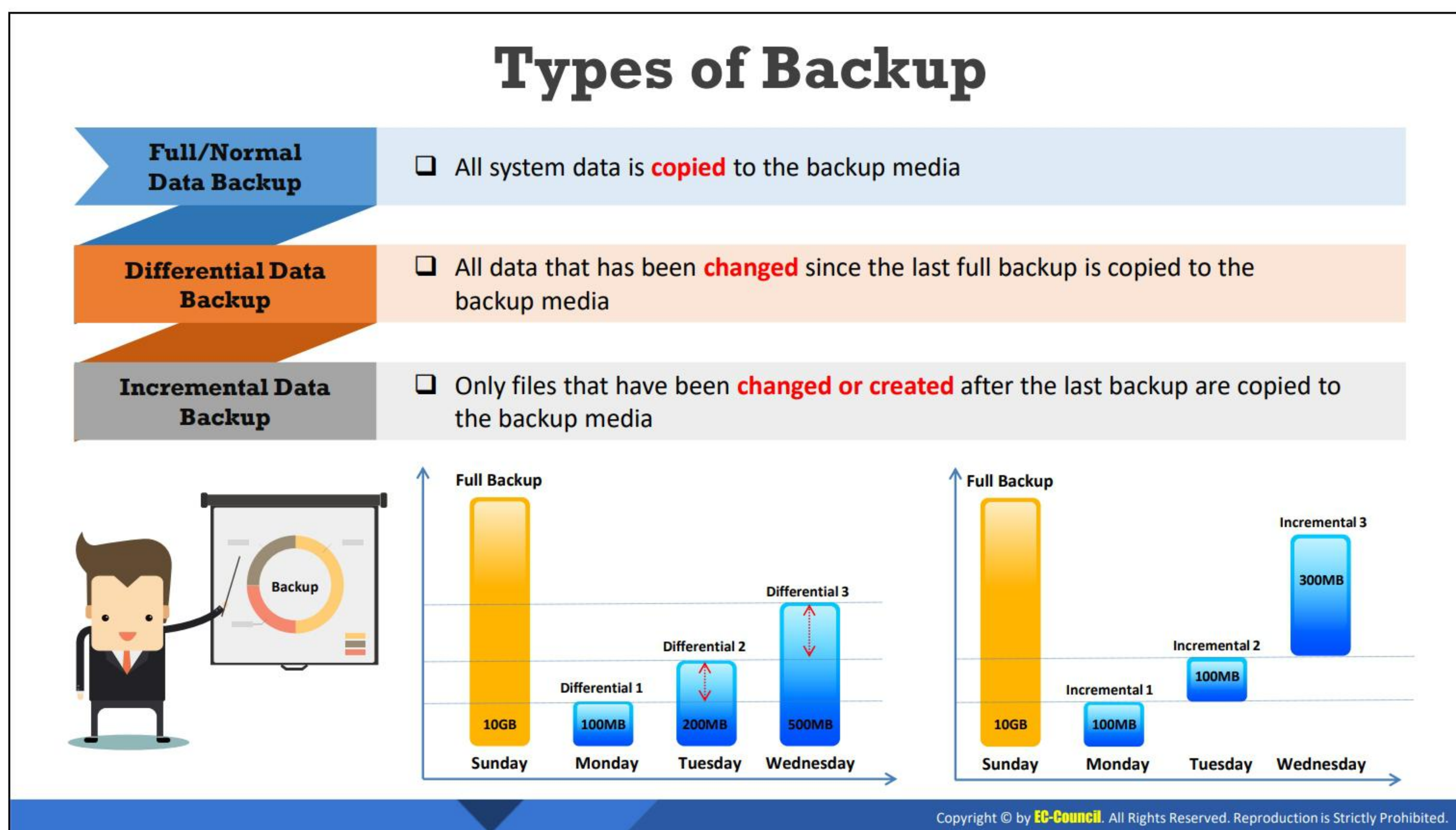
A Cloud backup is also known as online backup. It involves storing the backup on a public network or on a proprietary server. Usually, a third-party service provider hosts the proprietary server. The cloud data backup process works according to the requirements of the organization. If the organization needs a daily backup, the proprietary server will run a daily backup. Usually, any noncritical data is archived using a cloud data backup.

- **Advantages:**

- Cloud data backup is efficient as it uses technologies such as disk-based backup, virtualization, encryption, etc.
- Many proprietors provide data monitoring and create reports for the organization.
- The data in a cloud backup is easily accessed through the Internet.
- The data is encrypted and free from physical security threats.

- **Disadvantages:**

- Data recovery can be time consuming.
- Cloud data backup proprietors do not give any assurances or guarantees on the completion of a backup. The organization is responsible for checking whether the backup process was successful.



Types of Backup

An appropriate backup type is one that does not have a major impact on bandwidth, cost, time required, and the organization's resources. The three most common backup types are full, differential, and incremental.

- **Full backup:** This is also called a normal backup. A full backup occurs automatically according to a set schedule. It copies all files and compresses them to save space. A full backup provides efficient data protection for the copied data.
- **Differential backup:** Differential backup is the combination of a full backup and an incremental backup. A differential backup backs up all the changes made since the last full backup.

Example: Considering the above example, assume a full backup is scheduled for Sunday, and then a differential backup is scheduled to run until Saturday. Once the full backup is completed on Sunday, the differential backup will occur on Monday and the data that was changed will be backed up. On Tuesday, the backup will be for the changes made on Sunday and Monday. Then, on Wednesday, it will include the changes from Sunday, Monday, and Tuesday.

- **Incremental backup:** Backups only files that have been changed or created after the last backup are copied to the backup media. The last backup can be of any type. Before an incremental backup is performed, the system should be backed up using a full or normal backup.

Example: Assume a full backup of the system is scheduled for Sunday, and an incremental backup is scheduled from Tuesday to Saturday. Once the full backup is

performed on Sunday, the incremental backup on Monday will only backup the changes that occurred on Sunday. This process will continue until Saturday.

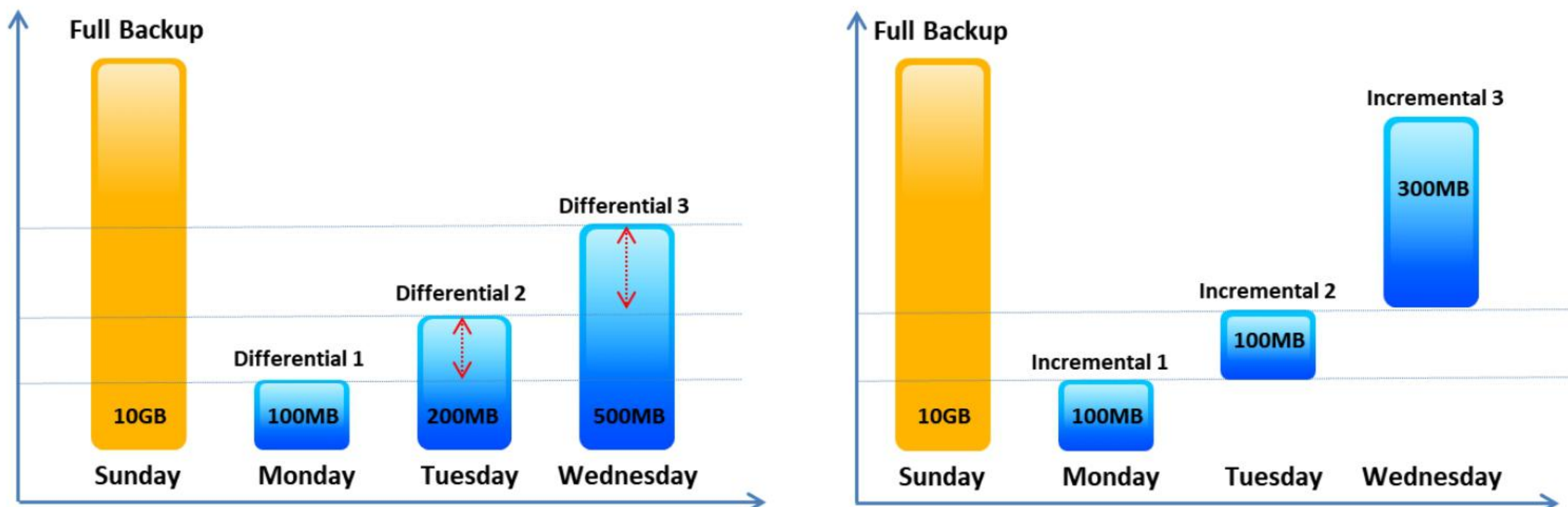


Figure 15.94: Backup types

Backup Types: Advantages and Disadvantages

Type	Advantages	Disadvantages
Full Backup	✓ Restoration is fast	✓ Backup process is slow ✓ High storage requirements
Differential Backup	✓ Faster than a full backup ✓ Restoration faster than an incremental backup ✓ Reduced amount of storage than a full backup	✓ Restoring data is slower than a full backup ✓ Slower than an incremental backup
Incremental Backup	✓ Fastest method ✓ Least amount of storage space among other backup types	✓ Slowest restore speed among other backup types



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Backup Types: Advantages and Disadvantages

Compare the advantages and disadvantages of each backup type, and then select one that is best suited for the organization.

Full Backup

- **Advantages:**
 - It is easy to restore; the process requires a file name and location.
 - Maintains different versions of the data.
- **Disadvantages:**
 - A time-consuming process because each file is backed up every time a full backup is performed.
 - Large storage requirements.

Incremental Backup

- **Advantages:**
 - Faster than a full backup.
 - Uses storage space efficiently, and there is no data duplication.
 - Least amount of storage space among other backup types.
- **Disadvantages:**
 - Data restoration is time consuming and a complex process; first, a full backup is done, which is followed by an incremental backup.

Differential Backup

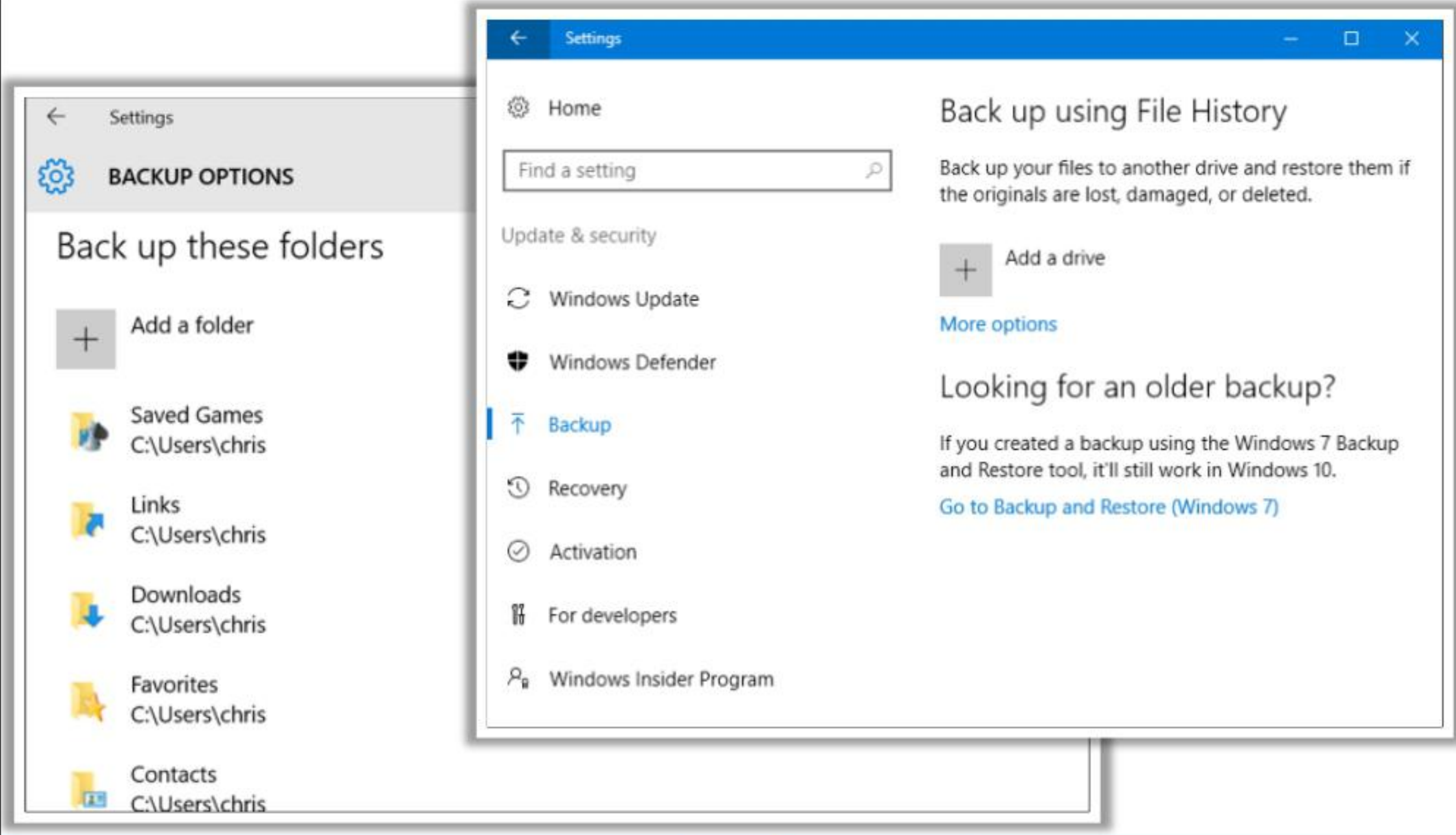
- **Advantages:**
 - Faster than a full backup.
 - Uses storage space more efficiently than a full backup; the backup only contains the changes made at regular intervals.
 - Data restoration is faster than an incremental backup.
 - Reduced amount of storage than a full backup.
- **Disadvantages:**
 - Slower than an incremental backup.
 - Restoration process is slower than a full backup.

Data Backup Tools

File History Tool

- File History is a **built-in backup tool** in Windows
- It regularly backs up important folders like Desktop, Documents, Downloads, Music, Picture, Videos, and parts of AppData folder





**Genie Backup Manager Pro**
<https://www.zoolz.com>

**BullGuard Backup**
<https://www.bullguard.com>

**NTI Backup Now EZ**
<https://www.nticorp.com>

**Power2Go 13**
<https://www.cyberlink.com>

**Backup4all**
<https://www.backup4all.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Data Backup Tools

File History Tool

Use **File History** to backup and restore in Windows. By default, it backs up the system drive. Other drives can be selected for backup if needed. Regular data and settings back up is recommended to prevent data loss.

Steps to Backup your PC with File History

- Select **Start → Settings → Update & Security → Backup → Add a drive +**, and then select an external drive or network location for backups.

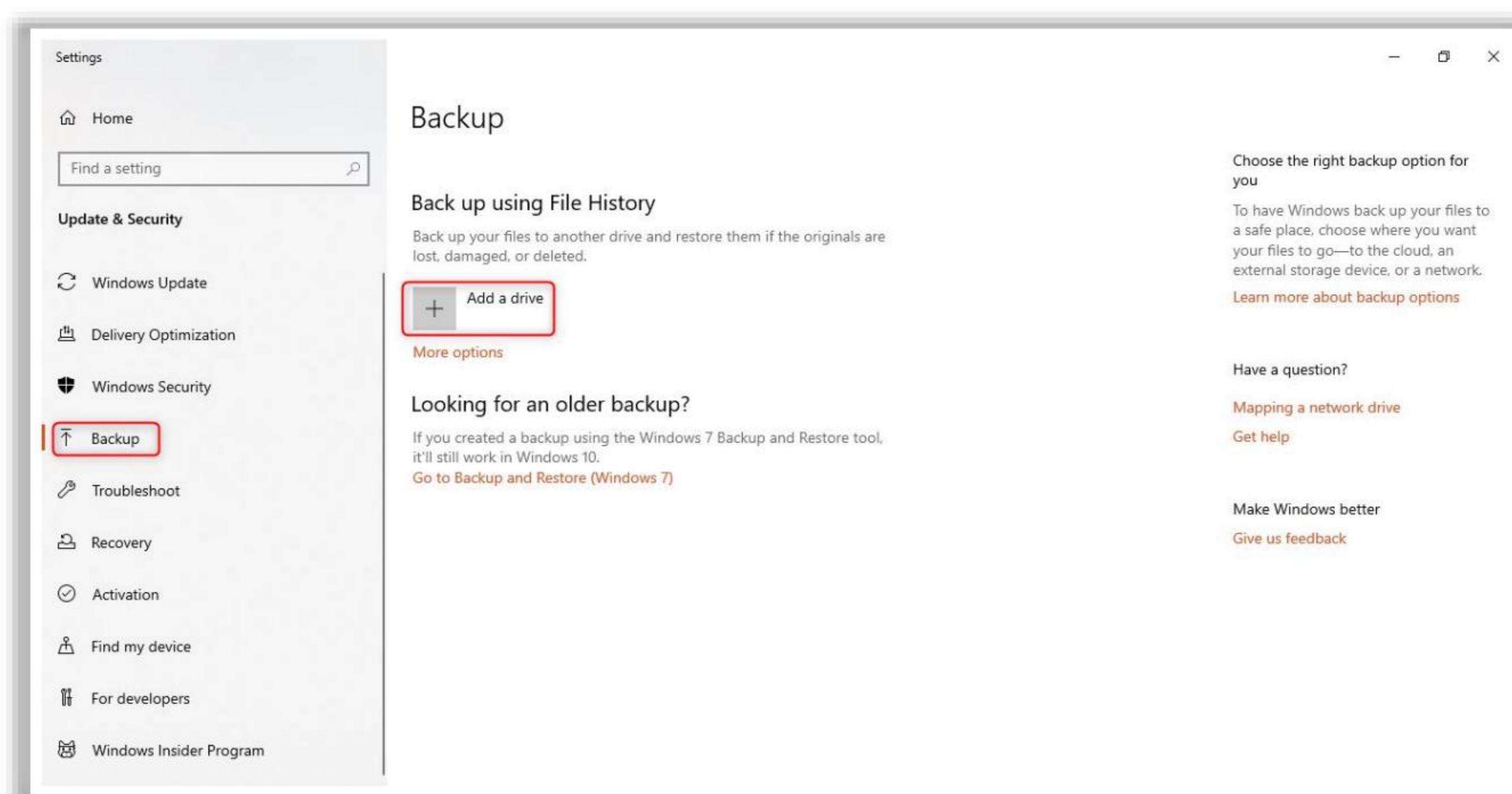


Figure 15.95: Backup PC with File History

File History before it is activated in Windows 10

- Select an external drive. File History is now archiving data. An on/off slider appears under a new heading **Automatically back up my files**.

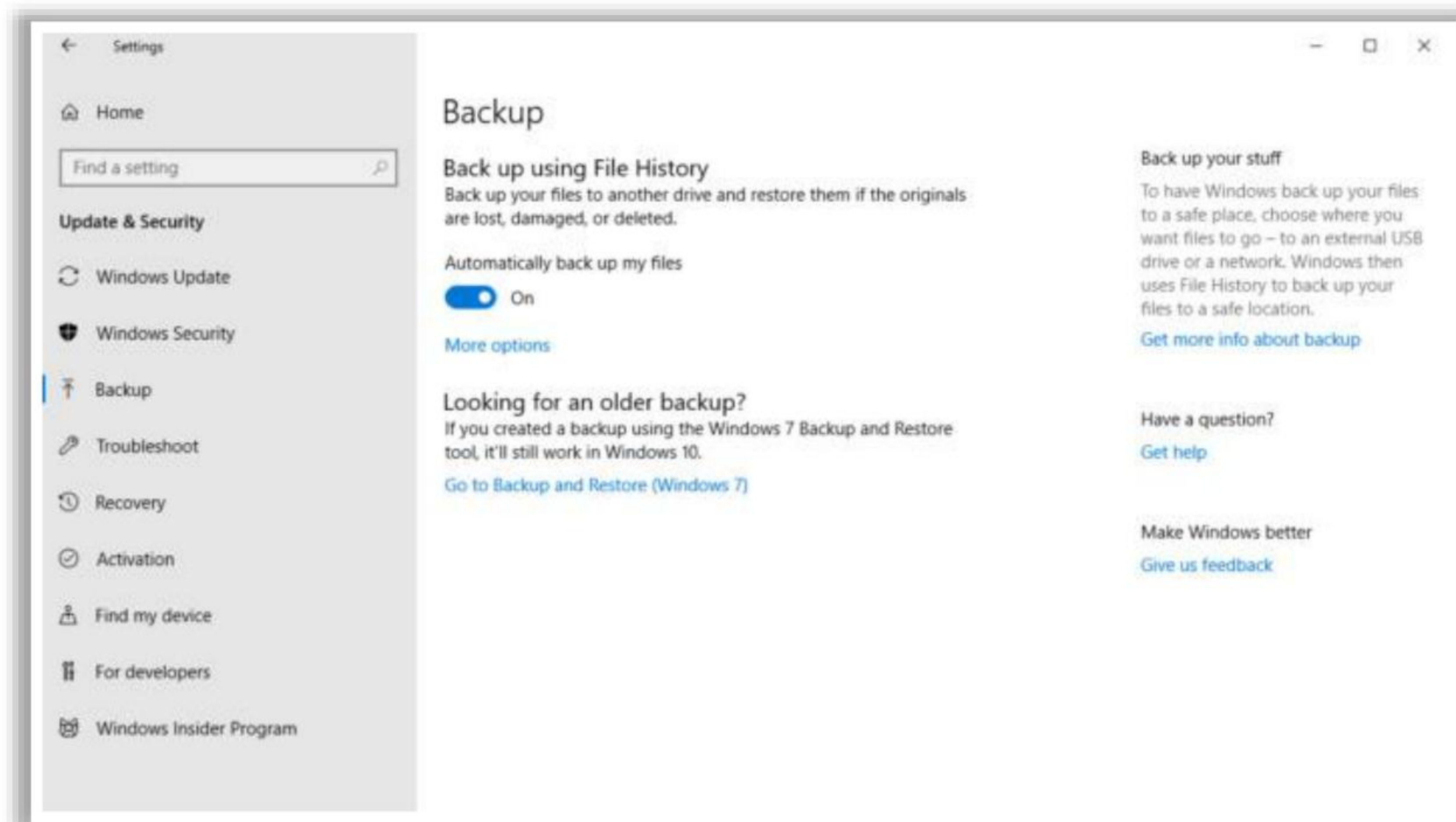


Figure 15.96: Back Up Using File History

- Click **More options** to change the File History defaults.
- By default, Windows 10 File History will back up all folders in the User folder, back up files every hour as long as the backup drive is available and keep previous copies of the files forever. To change any of these settings, click **More options** under the on/off slider.

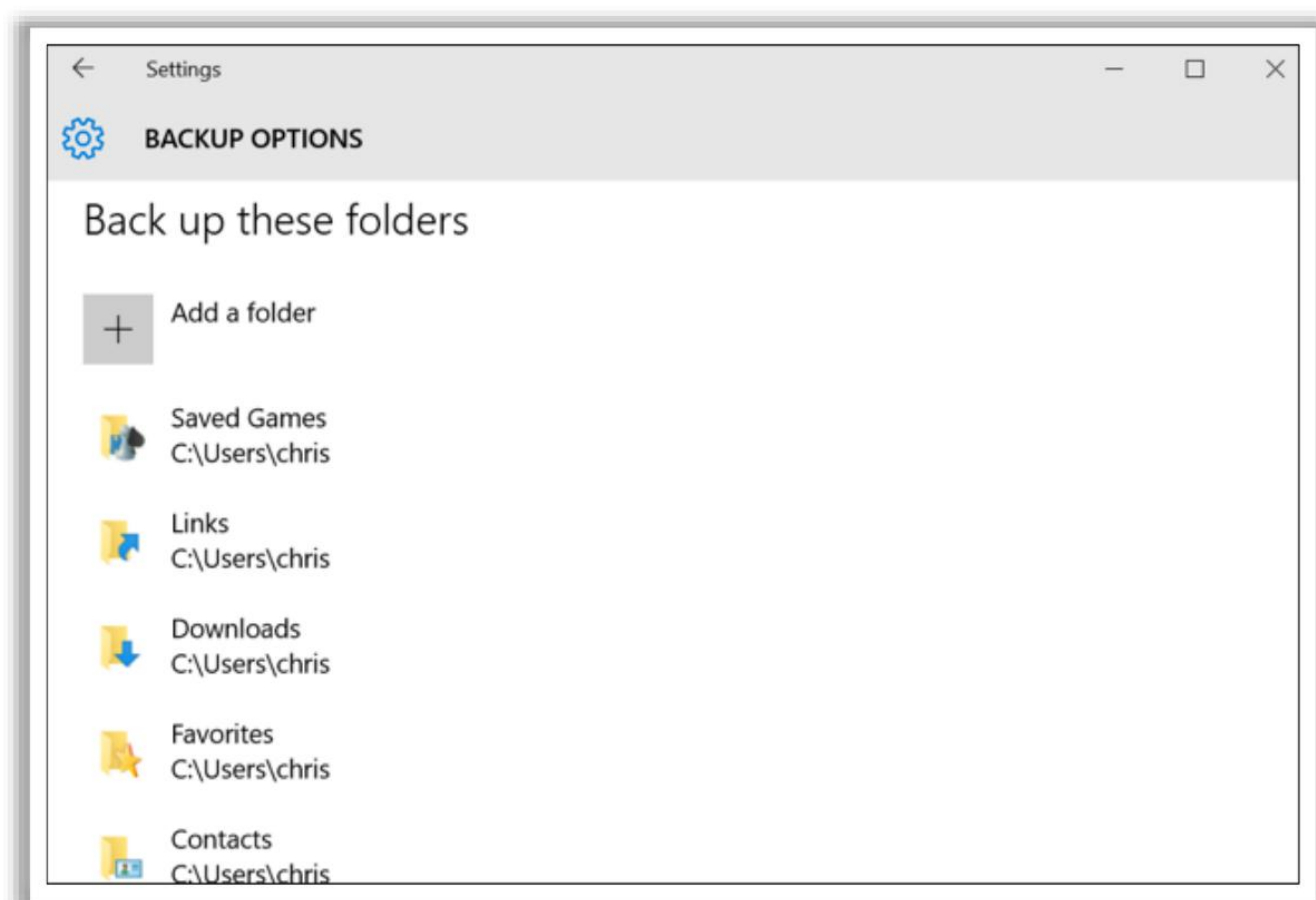


Figure 15.97: Folder Back Up

Some additional data backup tools are as follows:

- Genie Backup Manager Pro (<https://www.zoolz.com>)
- BullGuard Backup (<https://www.bullguard.com>)
- NTI Backup Now EZ (<https://www.nticorp.com>)
- Power2Go 13 (<https://www.cyberlink.com>)
- Backup4all (<https://www.backup4all.com>)

Data Backup Retention

Data Retention



- Data Retention is the process of storing and **maintaining important information** for meeting compliance and business data archival requirements

Data Retention Policy



- Data retention policy is a **set of rules** for preserving and maintaining data for operational or regulatory compliance requirements
- The policy defines the required **retention periods** for different data types, and sets the minimum standards for destroying certain information



Steps for Developing a Data Retention Policy

- ➡ Build a data retention policy development team
- ➡ Understand and determine the applicable legal requirements of the organization
- ➡ Identify and classify the data to be included in data retention policy
- ➡ Develop the data retention policy
- ➡ Ensure that all employees understand the organization's data retention policy



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Data Backup Retention

Data retention is the process of storing and maintaining important information for meeting compliance and business data archival requirements. It helps organizations in recovering business-critical data in case of data loss.

Every organization should develop a data retention policy to ensure that all important data is satisfactorily stored. The data retention policy is a set of rules for preserving and maintaining data for operational or regulatory compliance requirements. The policy defines the required retention periods for different data types, and also sets the minimum standards for destroying certain information.

A data retention policy is applied to all business units, processes, and systems in all countries where an organization operates. It is applied to an organization's officers, directors, employees, agents, affiliates, contractors, consultants, advisors, or service providers who can collect, process, or have access to different data types. Moreover, it is applied to all documents such as emails, hard copy documents, soft copy documents, audio, and video files, etc.

Steps to Create Data a Retention Policy

The following steps are used to create a data retention policy:

1. Build a data retention policy development team

You should build a data retention policy development team that includes the members such as:

- In-house legal counsels
- Departmental managers and supervisors

- Those who receive and manage financial reports
- Those who develop financial reports
- Staff members for managing data retention settings

2. Identify the types of regulatory compliances applicable to your business

Different regulatory compliances specify different data retention durations and data removal conditions. Some of them are listed below:

- The Health Insurance Portability and Accountability Act (HIPAA)
- The Sarbanes-Oxley Act (SOX)
- The Internal Revenue Service (IRS)
- The Children's Online Privacy Protection Act (COPPA)
- The EU's GDPR

3. Specify the types of data to be included in your data retention policy

The following types of data should be included in the data retention policy:

- Documents
- Emails and other electronic documents
- Customer records
- Transactional information
- Spreadsheets
- Contracts
- Correspondence between staff and clients, agents, vendors, shareholders, and the public
- Supplier and partner data
- Employee records
- Customer records
- Sales, invoice, and billing information
- Tax and accounting documentation
- Financial reports
- Healthcare and patient data
- Student and educational data
- Other information produced, collected, and maintained for satisfying regular business activities

4. Develop a data retention policy

Develop a data retention policy considering the following points:

- Purpose
- Applicable laws, regulations, policies, rules, and acts
- Record retention and deletion schedule
- Litigation plan
- Review and update schedule

5. Inform all employees about the data retention policy

All employees should be aware of and comprehensively understand the different aspects of the data retention policy. Provide each employee a copy of the data retention policy and also design training and review sessions to keep them updated.

Data Retention Policy Best Practices

01 Create a data retention policy that fulfils **legal** and **business** requirements

02 Justify the **reasons** behind the policy details

03 Start creating a policy with **minimal requirements** and add new requirements as and when required

04 Create a simple policy which is easy for the employees to implement



05 Create different **data retention policies** for different data types, as per their legal and business impacts

06 Retain **customer, subscriber, and user** information only till they are necessary

07 Implement **software** to manage the data retention tasks

08 Classify **data** and decide if it should be archived or deleted

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Data Retention Policy Best Practices

The following data retention best practices for an organization can help establish and enforce a more compliant and useful data retention policy suited to their needs:

- Create a data retention policy that fulfills legal and business requirements
- Justify the reasons behind the policy details
- Start creating a policy with minimal requirements, and add new requirements as and when required
- Create a simple policy which is easy for the employees to implement
- Create different data retention policies for different data types, as per their legal and business impacts
- Retain customer, subscriber, and user information only till they are necessary
- Implement software to manage the data retention tasks
- Classify data and decide if it should be archived or deleted
- Files which are not accessed frequently should be moved to a lower-level archive
- Organize and store archived data such that it is easily accessible

Data Destruction



 Data destruction is the process of **destroying** data stored on tapes, hard disks, and other forms of electronic media, so that it is completely unreadable and cannot be accessed or used for unauthorized purposes

 The main purpose of data destruction is to restrict **unauthorized disclosure of information** through proper disposal and destruction of devices, equipment, computers, and media that store sensitive data

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Data Destruction

Computers, smartphones, and other devices store a large amount of information, some of which may be sensitive and critical, such as emails, documents, personal photos, etc. Once not in use, the user deletes the data presuming that the information is deleted and cannot be recovered. If not deleted properly, the information still exists on the hard drive or memory chip, and anyone accessing such a system can recover these deleted files. The best way to permanently delete files or sensitive data is by implementing data destruction methods.

Data destruction is the process of destructing the stored data in electronic media such as hard drives, flash drives, tapes, etc. into an unreadable form that cannot be accessed or exploited for unauthorized purposes. The main purpose of data destruction is to restrict the unauthorized disclosure of information through proper disposal and destruction of devices, equipment, computers, and media that store sensitive data.

The various forms of data destruction are:

- Delete/Reformat
- Wipe
- Overwriting data
- Erasure
- Degaussing
- Physical destruction
- Electronic shredding
- Solid-state shredding

Security Benefits of Data Destruction

- Data destruction protects the sensitive information of customers and employees from cybercriminals.
- Hefty fines can be avoided with data destruction as a security breach can lead to various penalties.

Data Destruction Policy

- ❑ Data destruction policy ensures that the data stored on unused tapes, hard disks, and other forms of electronic media is **deleted** or **destroyed** such that they are unreadable and cannot be accessed
- ❑ Every organization must implement a data destruction policy



Data destruction policy for:

Mobile Phones

- Mobile phones have a **hard reset** or **cold reset** button to delete the installed software and restore the device to factory default settings

DVDs and other tape storage drives

- **Physically destroy** the optical and tape media when not required

Hard Drives and Flash Memory Devices

- **Overwrite the data** in hard drives and flash memory devices using programs such as Darik's Boot and Nuke, Wipe, etc.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Data Destruction Policy

A data destruction policy ensures that the data stored on unused tapes, hard disks, and other forms of electronic media are overwritten or destroyed such that they are unreadable and cannot be accessed for unauthorized purposes. Implementation of a data destruction policy reduces the chances of a privacy breach. Companies should spend their time and money on a data destruction policy since they have to safeguard their data and prevent a data breach. Every organization must implement a data destruction policy.

Implementation of a data security policy: For implementing a data security policy, all devices and media no longer used by an organization should be securely removed, destructed, or overwritten.

- **Mobile phones - iPhones, Androids, Blackberries, etc.:** Mobile phones have a hard reset or cold reset button to delete the installed software and restore the device to factory default settings.
- **DVDs and other tape storage drives:** Physically destroy the optical and tape media when not required.
- **Hard drives and flash memory devices:** Overwrite the data in hard drives and flash memory devices using programs such as Darik's Boot and Nuke, Wipe, etc.

Data Destruction Techniques

Technique	Description	Methods
Clearing 	➤ Technique to clear data in all user-addressable storage spaces ➤ Cannot be used for damaged or non-rewritable media	➤ Overwriting ➤ Wiping ➤ Erasure
Purging 	➤ Technique to remove data permanently from a storage space by applying strong magnetic fields ➤ Strong magnetic fields can damage nearby devices	➤ Degaussing
Destroying 	➤ Technique to destroy data by destroying the storage medium ➤ Best method for destroying sensitive data	➤ Disintegration, incineration, pulverizing, and pulping ➤ Shredding

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Data Destruction Techniques

The different data destruction techniques are listed below.

1. Clearing

Clearing is a data destruction technique that protects sensitive information against keyboard attacks. This technique is used to clear the data in all user-addressable storage spaces. The information eliminated by this method will not be recovered through data, disk, or file recovery tools. This technique is not applicable to damaged or non-rewritable media. Overwriting, wiping, and erasure are the methods used for clearing information.

- **Overwriting:** Overwriting is a method of writing new data over old data with the purpose of eliminating the old data completely. Occasionally, this is accomplished in a single attempt. However, if the medium implements strong security, multiple passes may be required. This ensures that all information is destroyed and that no recovery tool will be able to recover it.
- **Wiping:** Data wiping is a method of clearing data from an electronic device so that the data cannot be read any longer. It is performed by physically connecting an electronic device to a wiping device. Once the information is wiped from an electronic device, the device can be reused without losing storage capacity.
- **Erasure:** Erasure is another method used to delete all the data in a hard drive such that the data can no longer be recovered. This method is used by businesses that have leased equipment or wish to reuse hard drives for storing different information.

2. Purging

Purging is a data destruction technique that protects sensitive information against laboratory attacks. This technique is used to remove data permanently from a storage space by applying strong magnetic fields, which can damage nearby devices. A laboratory attack occurs when an unauthorized individual uses signal processing recovery tools in a laboratory environment to recover sensitive information. Degaussing and executing the Secure Erase firmware command are two purging methods.

- **Degaussing:** Degaussing is a method of using high-power magnets to disrupt the magnetic field of magnetic media such as hard disk drives and magnetic tapes. This method cannot be implemented on optical media such as DVDs. Degaussing a hard drive disk typically renders it inoperable, thus making it impossible for a user to check whether all the data have been destroyed. This method is effective in destroying storage media with large amounts of information, but it is inappropriate if the user wishes to reuse the storage device for storing different information.

3. Destroying

Destroying is a data destruction technique of physically destructing the storage media through a variety of methods such as disintegration, incineration, pulverizing, shredding, and pulping. This method is used in circumstances where the complete destruction of data along with physical media is required. This is considered the best method for destroying sensitive data.

- **Disintegration:** This is a physical destruction method that not only destroys the information stored in storage media but also the physical media containing that information.
- **Incineration:** Also known as burning, incineration is an effective technique for depositing information written on white paper. However, destroying compact disks, DVDs, USB devices, or other storage systems via incineration can create environmental issues due to toxic fumes. Hence, this technique is recommended to be employed for erasing data on paper.
- **Pulverizing:** In this method, documents of confidential data are dumped into a pulverizer that uses a hydraulic process to reduce the data objects or documents to shards and loose fibers. Few commercial businesses use this technique owing to the lack of availability and cost concerns.
- **Melting or pulping:** Melting or pulping is the process of liquidizing documents that hold confidential data. It is important to ensure that the data on the documents are securely taken to the pulping facility, and the documents should be closely monitored until the pulping process is completed.
- **Shredding:** This is another physical destruction method used to destroy information stored in storage media such as hard drives, optical drives, smartphones, tablets, and credit-card swipe devices. It breaks the electronic media into multiple pieces not

larger than 2 mm. This method is especially useful to destroy data stored in an organization's data center or in a large stockpile of old hard drives and media.

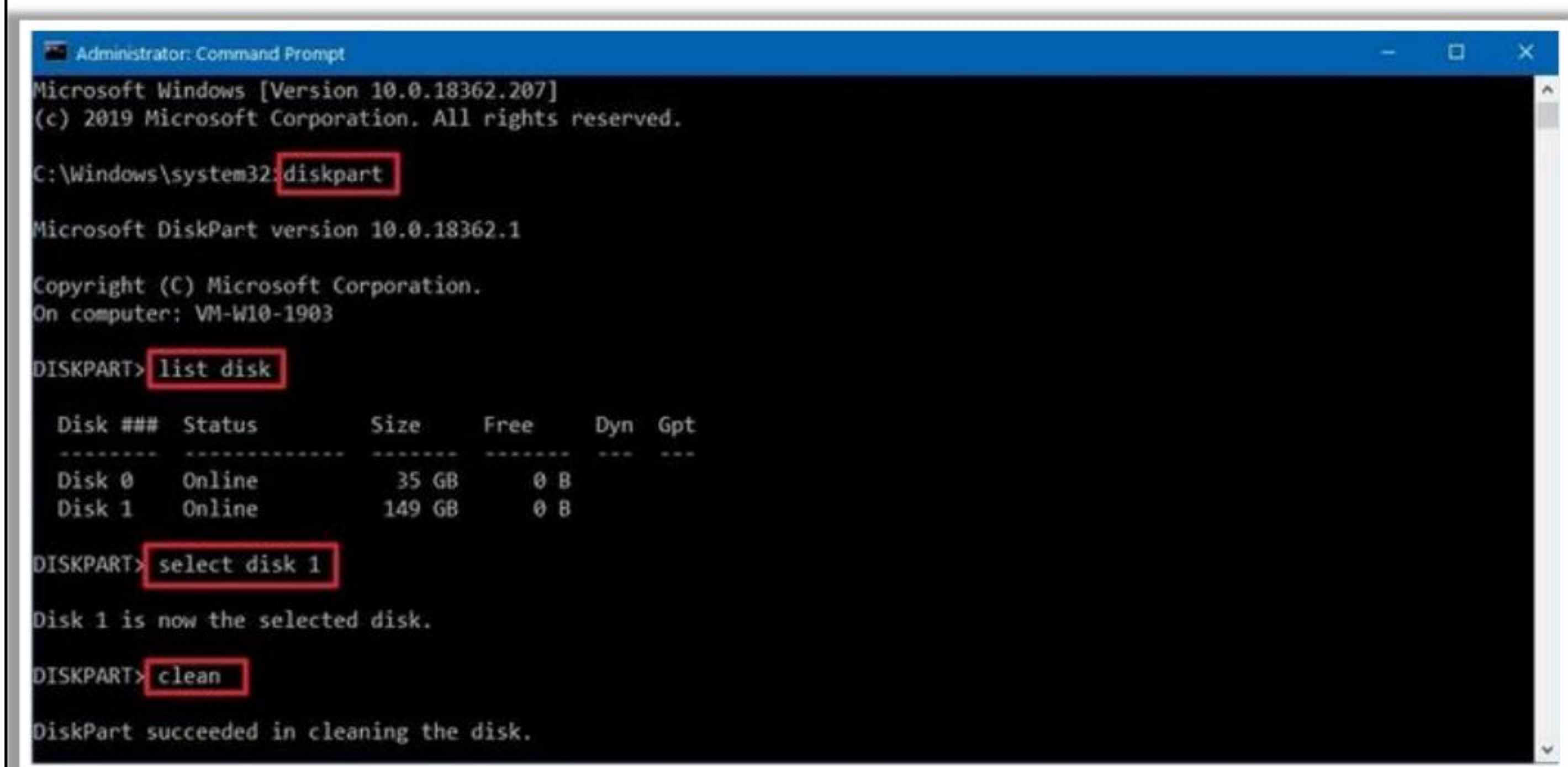
4. Disposal

Disposal is a technique of eliminating information without considering data destruction. This technique is applied to documents containing nonconfidential information. The disclosure of such information will not affect the organization's goals, lead to any financial losses, or harm an individual.

Data Destruction Tools

Disk Wipe: Windows Diskpart Utility

- ☐ DiskPart is a command utility to manage **drives**, **partitions**, and **volumes**
- ☐ It quickly removes data and partitions from a hard drive using the command prompt



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.18362.207]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>diskpart

Microsoft DiskPart version 10.0.18362.1

Copyright (C) Microsoft Corporation.
On computer: VM-W10-1903

DISKPART>list disk

   Disk ###  Status       Size      Free      Dyn  Gpt
   -----  -
   Disk 0    Online        35 GB     0 B
   Disk 1    Online       149 GB     0 B

DISKPART>select disk 1

Disk 1 is now the selected disk.

DISKPART>clean

DiskPart succeeded in cleaning the disk.
```



DBAN
<https://dban.org>



Active@ KillDisk
<https://www.killdisk.com>



Eraser
<https://eraser.heidi.ie>



PC Shredder
<http://www.pcshredder.com>



Macrorit Data Wiper
<https://macrorit.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Data Destruction Tools

Windows DiskPart Utility

- DiskPart is a command utility to manage drives, partitions, and volumes.
- It can be used when other tools such as Disk Management and Format are unable to resolve the problem.
- It quickly removes data and partitions from a hard drive using the command prompt.

Steps to Wipe a Hard Drive with Windows DiskPart

- Open command prompt in Administrator Mode.
- Type diskpart and press **Enter** to launch Diskpart.
- Type list disk for listing all drives connected to the computer, and press **Enter**.
- Type select disk 1 for selecting the drive the user wants to clean, and press **Enter**.
- Type clean to wipe out the drive and press **Enter**.

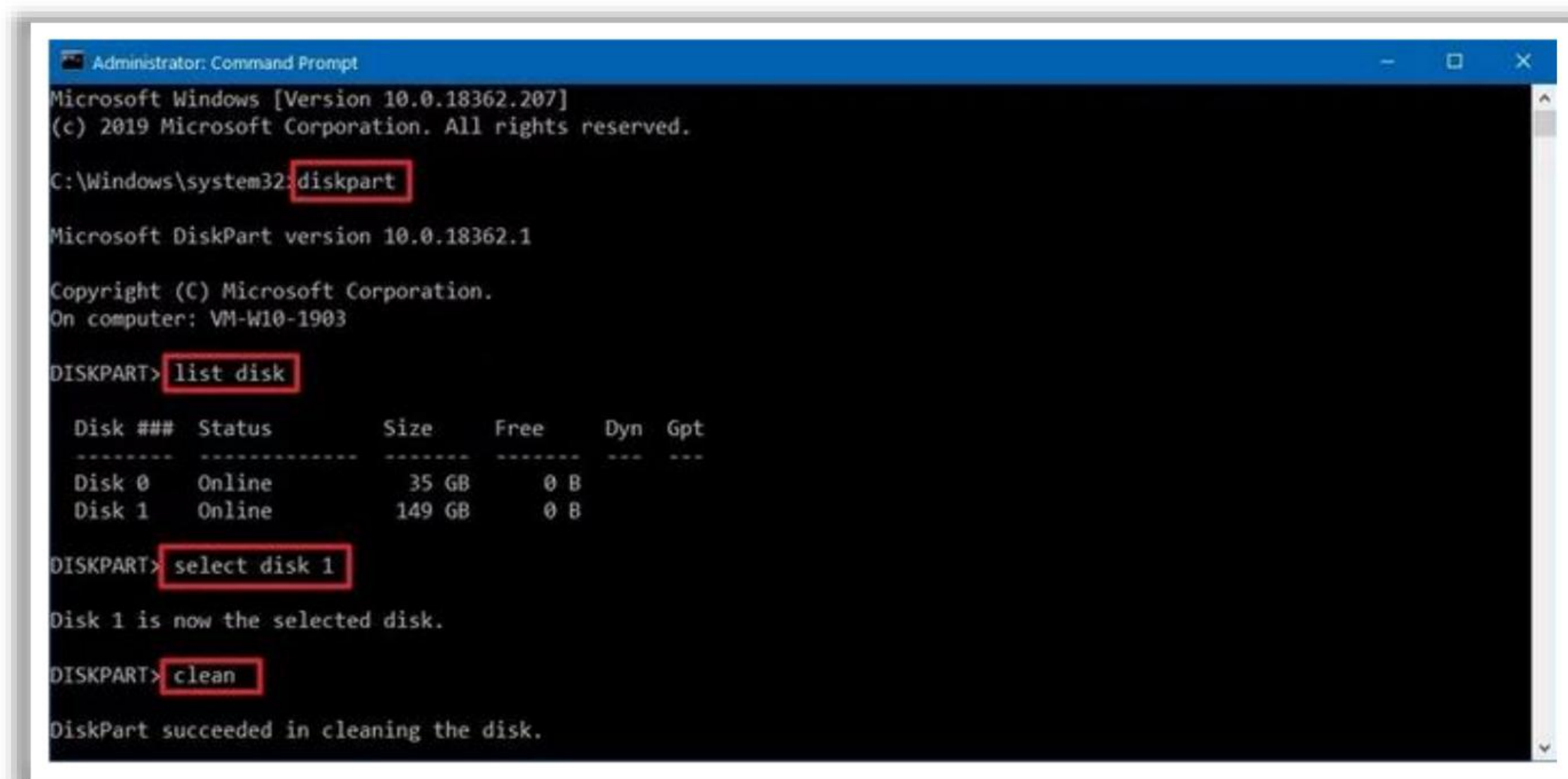


Figure 15.98: Wiping a hard drive with Windows DiskPart

- Type list disk for confirming the selected drive and press **Enter**.
- Type create partition primary command for creating a new partition on the drive and press **Enter**.
- Type select partition 1 command for selecting the new primary partition and press **Enter**.
- Type active for activating the selected partition and press Enter.

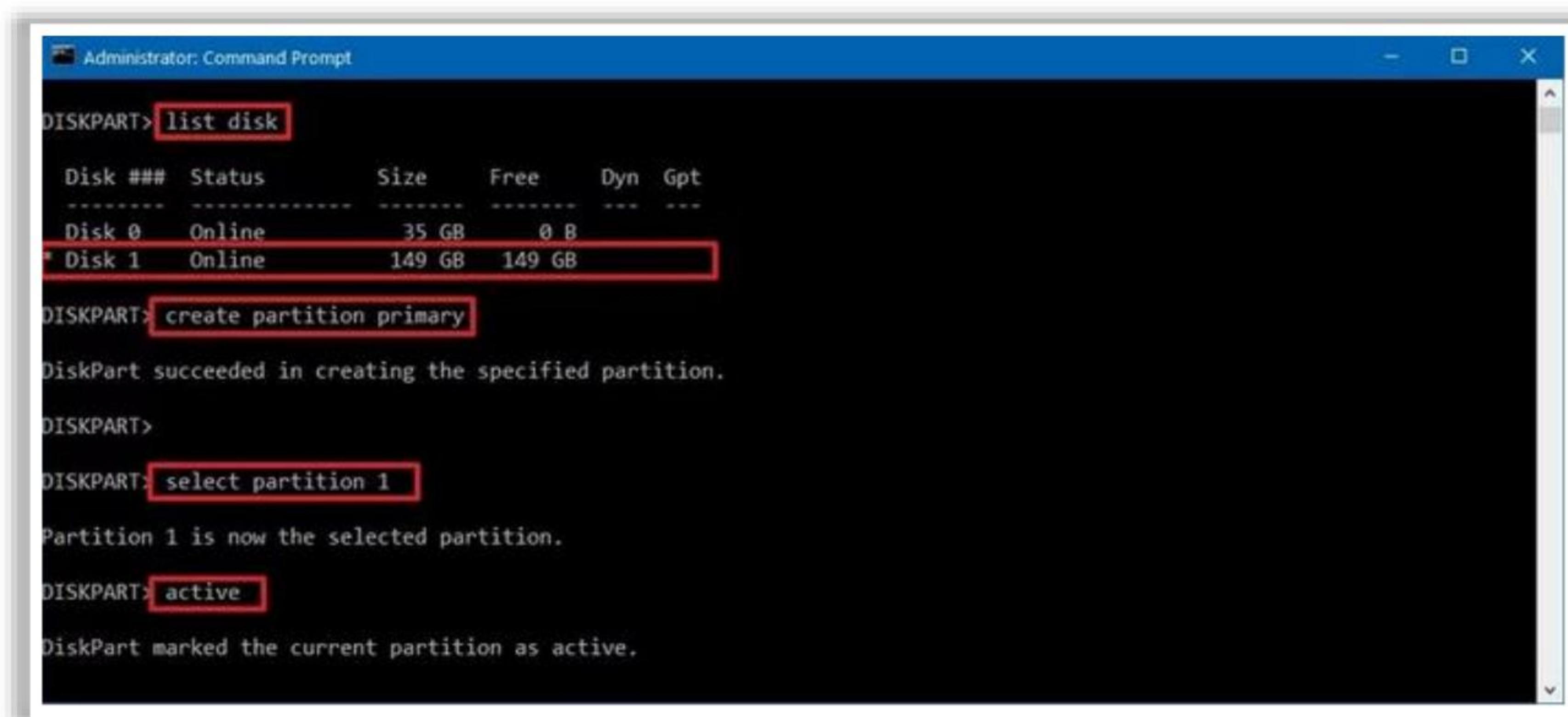


Figure 15.99: Selected partition activation

- Type format FS=NTFS label=Data quick for formatting the partition and setting a drive label, and press **Enter**.
- Type assign letter=w command to assign a letter and make the drive available in File Explorer, then press **Enter**.

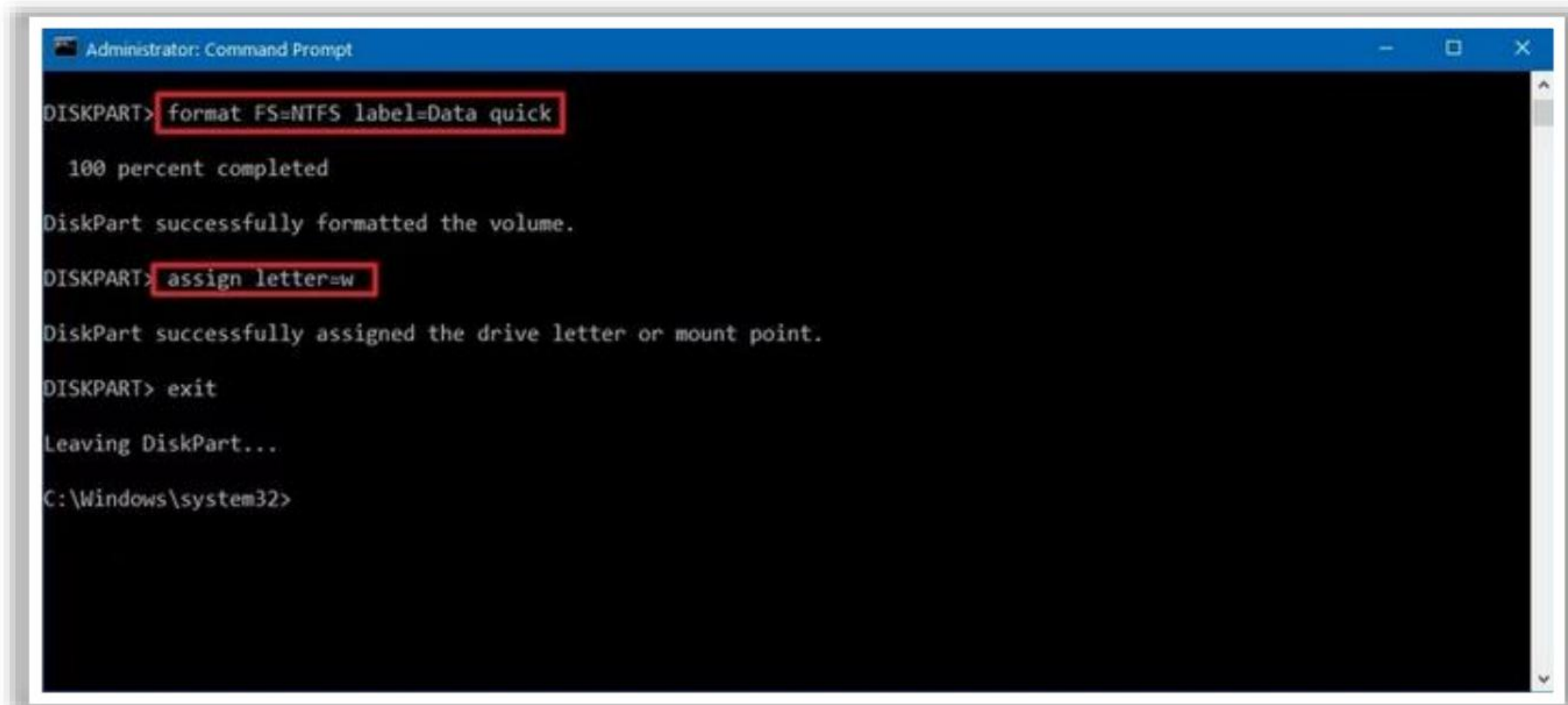
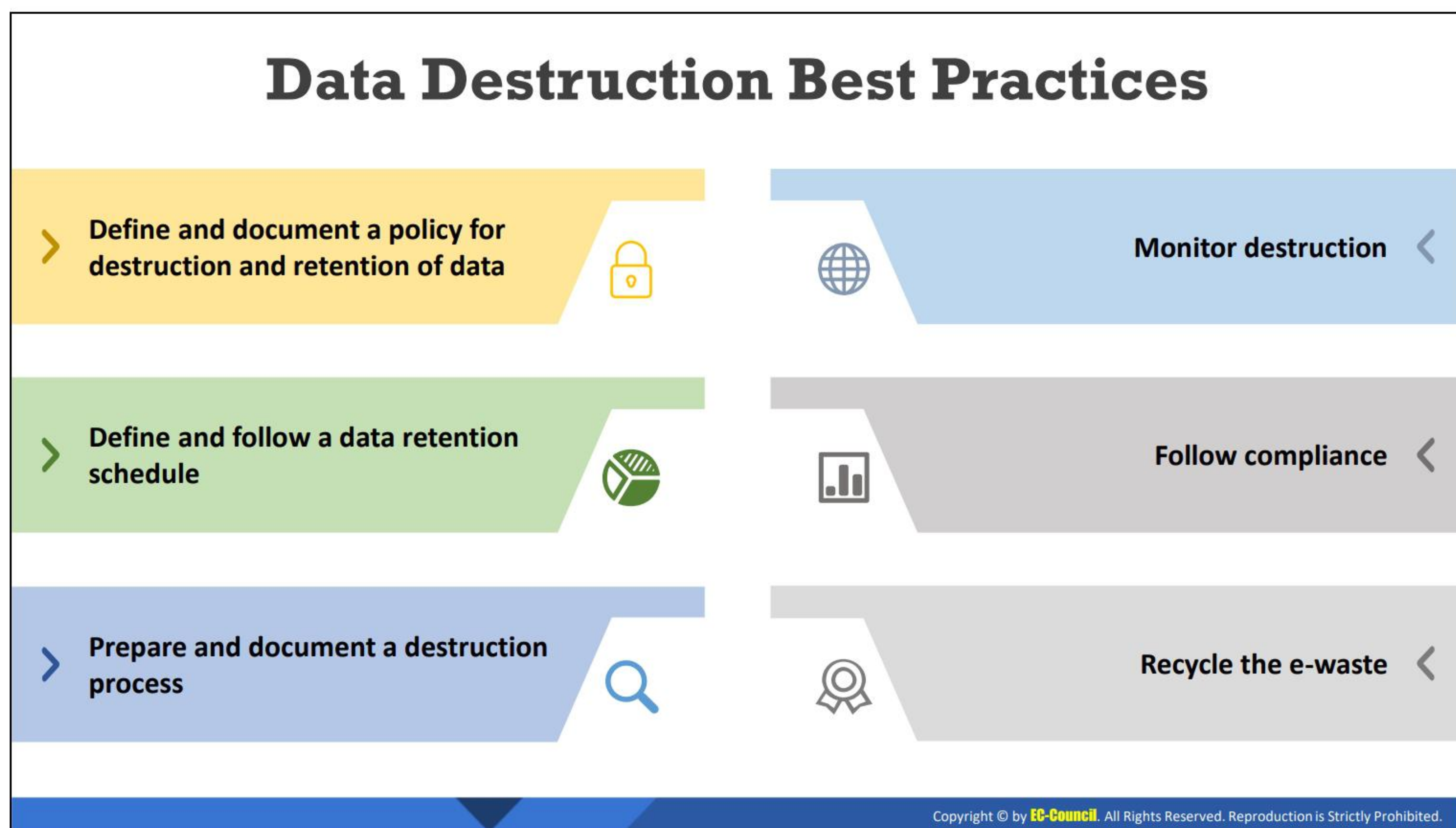


Figure 15.100: Formatting the partition and making the drive available in File Explorer

- Type exit command for terminating DiskPart, and press **Enter**.

Some additional data destruction tools are as follows:

- DBAN (<https://dban.org>)
- Active@ KillDisk (<https://www.killdisk.com>)
- Eraser (<https://eraser.heidi.ie>)
- PC Shredder (<http://www.pcshredder.com>)
- Macrorit Data Wiper (<https://macrorit.com>)



Data Destruction Best Practices

- 1. Define and document a policy for destruction and retention of data:** The policy for retaining data will be based on the record retention schedule. Upon completion of the retention period, the data should be destroyed.
- 2. Define and follow a data retention schedule:** A data retention schedule sets the guidelines on how long the data should remain accessible for future use or reference, and destroys the data when not in use.
- 3. Prepare and document a destruction process:** Accessibility to the confidential information of an organization poses a serious threat; thus, the organization should safeguard its confidential information, recognize the security loopholes, and take measures to avoid them. Best practices in document destruction are divided into three key guidelines for securing customer, employee, and business information, as follows:
 - Shred all and shred regularly.
 - Shred before recycling.
 - Shred using a professional service.
- 4. Monitor destruction:** Depending on the growth and evolution of the organization, the destruction needs will change. Hence, monitor the destruction process to meet the current and future needs.
- 5. Follow compliance:** The company should be in compliance with the laws and regulations pertaining to classified equipment destruction. If there are policies pertaining to the destruction of classified equipment, then they should be complied with. Disposition of

classified equipment requires ethical and legal obligations; therefore, if a company does not dispose equipment properly, they may have to face a number of legal issues.

6. **Recycle the e-waste:** e-waste recycling prevents the reuse or recovery of sensitive information from corporate computers and devices. The proper recycling of e-waste keeps the environment safe.

Data Recovery Tools

EaseUS Data Recovery Wizard

EaseUS data recovery software can quickly **retrieve lost files** after deletion or emptying the recycle bin

Select a location to start recovering

Devices and Drives (12)

Local Disk (C:) 32.68 GB / 108.90 GB

Local Disk (D:) 11.64 GB / 110.16 GB

New Volume (E:) 2.33 GB / 2.35 GB

Local Disk (G:) 38.88 GB / 39.56 GB

Local Disk (H:) 28.67 GB / 29.02 GB

Local Disk (I:) 13.21 GB / 23.75 GB

Local Disk (J:) 501.04 MB / 917.88 MB

System Reser... (K:) 515.52 MB / 549.00 MB

Specify a location

DesktopRecycle BinSelect Folder

<https://www.easeus.com>

**Recuva®**
<https://www.ccleaner.com>

**Puran File Recovery**
<http://www.puransoftware.com>

**Glary Undelete**
<https://www.glarysoft.com>

**SoftPerfect File Recovery**
<https://www.softperfect.com>

**Wise Data Recovery**
<https://www.wisecleaner.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Data Recovery Tools

- **EaseUS Data Recovery Wizard**

Source: <https://www.easeus.com>

EaseUS data recovery software can quickly retrieve lost files after deletion or emptying the recycle bin. It scans for all recoverable files from any inaccessible storage device and completes file recovery safely and efficiently. It is used not only for the recovery of deleted files and formatted drives, but also for overcoming other data-loss issues such as virus attacks, human errors, power failures, system crashes, OS re-installation/upgrade, hard-drive crashes, and software crashes.

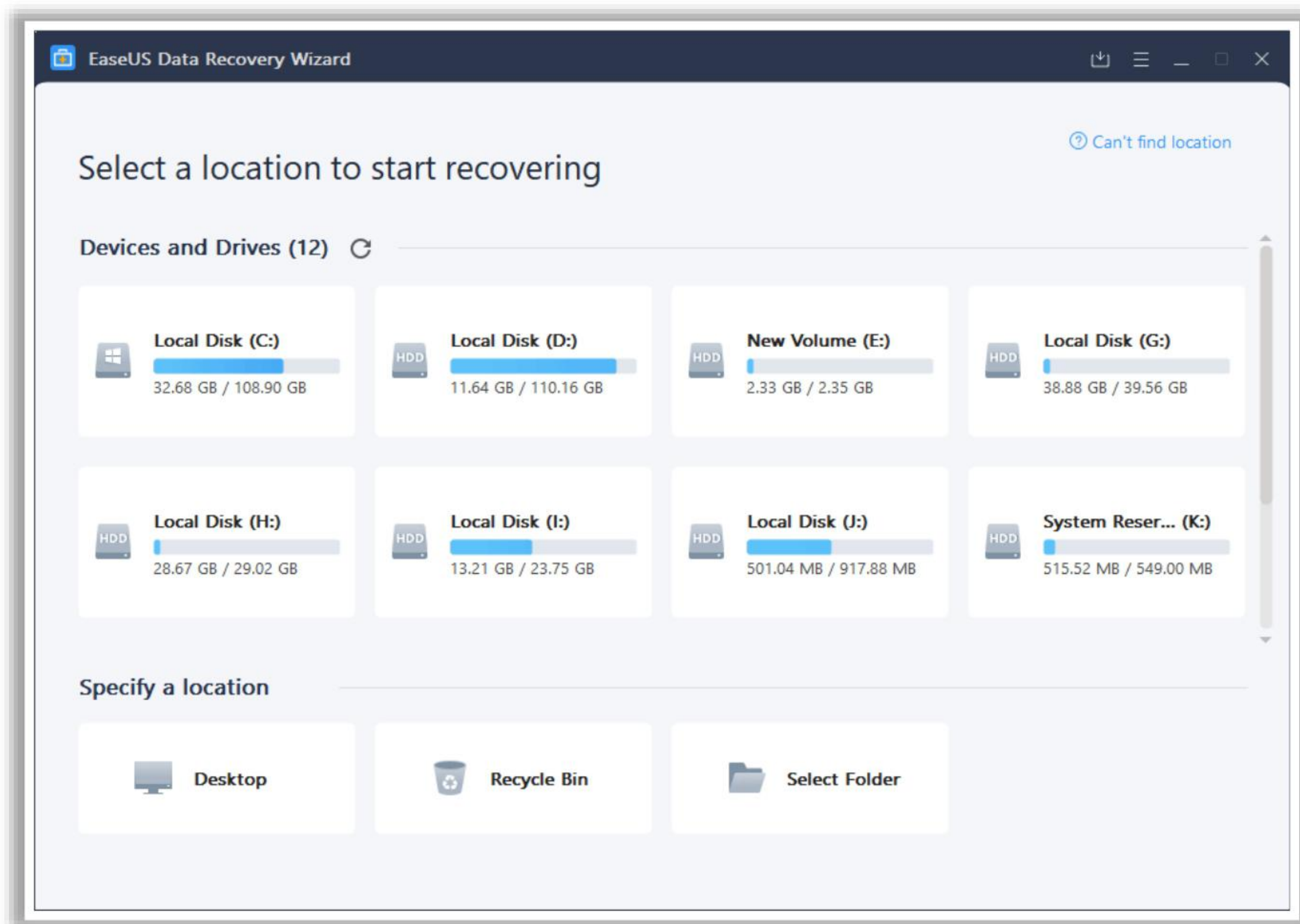
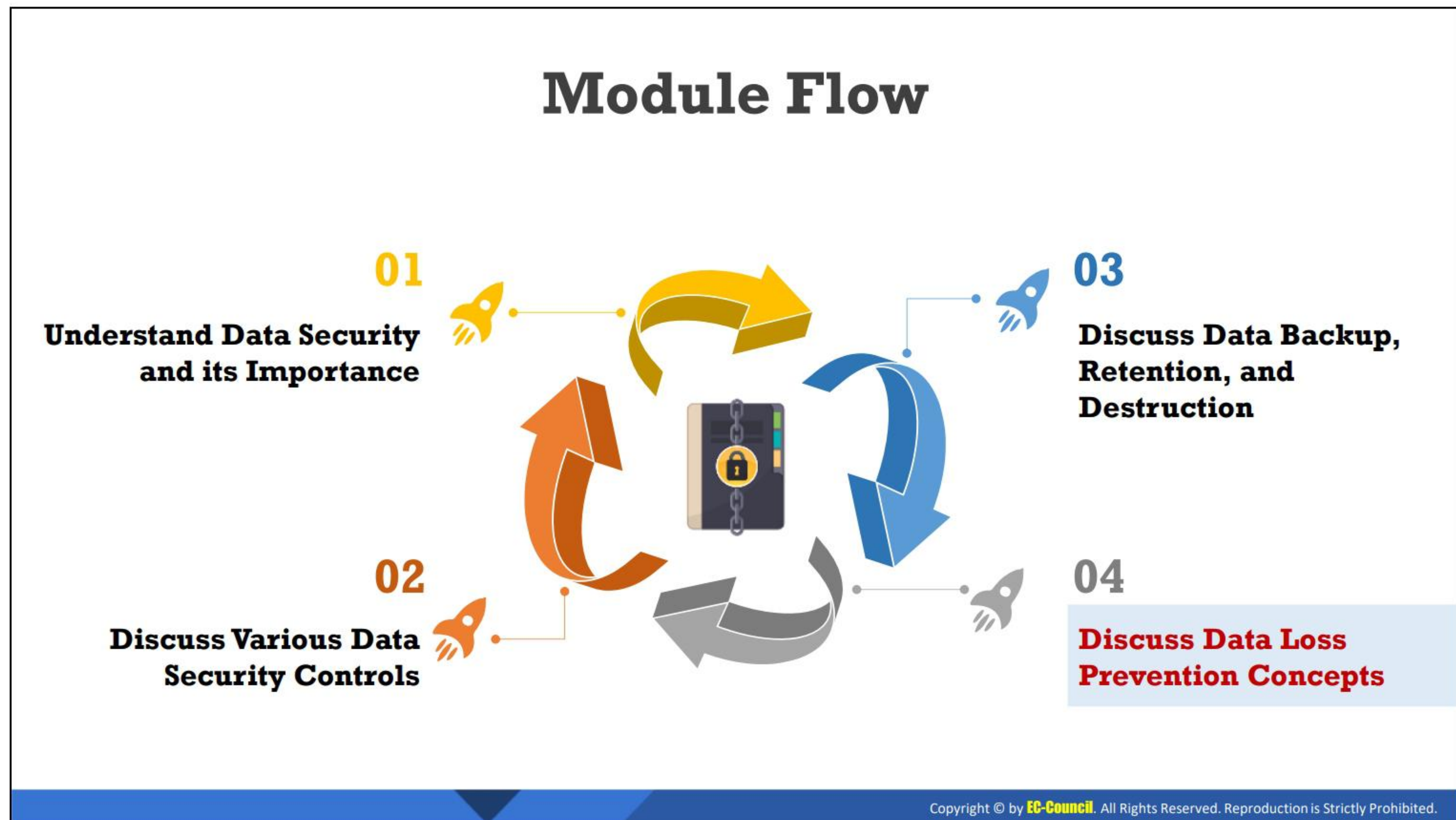


Figure 15.101: Screenshot of EaseUS Data Recovery Wizard

Some additional data recovery tools are as follows:

- Recuva® (<https://www.ccleaner.com>)
- Puran File Recovery (<http://www.puransoftware.com>)
- Glary Undelete (<https://www.glarysoft.com>)
- SoftPerfect File Recovery (<https://www.softperfect.com>)
- Wise Data Recovery (<https://www.wisecleaner.com>)



Discuss Data Loss Prevention Concepts

The objective of this section is to explain the importance of data loss prevention (DLP) in data security.

What is Data Loss Prevention?

- ❑ Data loss prevention (DLP) includes a set of software products and processes that do not allow users to **send confidential corporate data** outside the organization

- ❑ It is used by organizations to:

- ✓ Discover sources of data leaks
- ✓ Monitor the sources of data leakage
- ✓ Protect organization assets and resources
- ✓ Prevent accidental disclosure of sensitive information to unintended parties
- ✓ Manage resources with business rules, security policies, and software



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What is Data Loss Prevention?

Data loss prevention (DLP) includes a set of software products and processes that do not allow users to send confidential corporate data outside the organization. These software products help security professionals in controlling what data end users can transfer. DLP rules block the transfer of any confidential information across external networks. They control any unauthorized access to company information and prevent anyone from sending malicious programs to the organization.

DLP software are implemented according to the organizational rules set by the management. This prevents accidental/malicious data leaks and losses. If an employee tries to forward or even upload company data on cloud storage or on a blog, the access will be denied by the system.

A DLP policy is adopted by the management when internal threats to a company are detected. A DLP policy ensures that none of its employees send sensitive information outside the organization. New emerging DLP tools not only prevent the loss of data but also monitor and control irregular activities from occurring on the system.

Different DLP products are available to help security professionals determine what data users can transfer. DLP products are also known as data leak prevention, information loss prevention, or extrusion prevention products.

DLP is used by organizations to:

- Discover sources of data leaks
- Monitor the sources of data leakage
- Protect organization assets and resources

- Prevent accidental disclosure of sensitive information to unintended parties
- Manage resources with business rules, security policies, and software

Types of Data Loss Prevention (DLP) Solutions

Endpoint DLP

- A solution that **monitors** and **protects PC-based systems** such as tablets, laptops, etc.
- It is used for preventing data leakage through clipboards, removable devices, and sharing applications

Network DLP

- A solution that **monitors**, **protects**, and **reports all data in transit**
- It is installed at the “perimeter” of an organization’s network
- It helps the security professionals in scanning all data moving through the ports and protocols within the organization

Storage DLP

- A solution that **monitors** and **protects data at rest**, that is, the data stored in an organization’s data center infrastructure such as file servers, SharePoint, and databases
- It identifies the location where sensitive information is stored and helps users in determining whether it is stored securely

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Data Loss Prevention (DLP) Solutions

There are various types of DLP solutions that function differently with the same objective, that is, to prevent data leakage.

- **Endpoint DLP:** Endpoint DLP is a solution that monitors and protects PC-based systems such as tablets, laptops, etc. It is used for preventing data leakage through clipboards, removable devices, and sharing applications. The solution includes an agent that monitors specific user operations such as sending an email, copying a file to removable media devices, printing a file, etc. Endpoint DLP protects data in use.
- **Network DLP:** Network DLP is a solution that monitors, protects, and reports all data in transit. It is installed at the “perimeter” of an organization’s network. It helps the security professional in scanning all data moving through the ports and protocols within the organization. It may analyze email traffic, social media interactions, SSL traffic, instant messaging, etc. The solution maintains reports containing information such what data is used, who is using the data, and where the data is sent. Thus, it helps in controlling the flow of data over the organization's network and meets regulatory compliance. Data collected by a Network DLP is stored in a database for retrieval later.
- **Storage DLP:** Storage DLP is a solution that monitors and protects data at rest, that is, the data stored in an organization’s data center infrastructure such as file servers, SharePoint, and databases. It identifies the location where sensitive information is stored and helps users in determining whether it is stored securely. It allows authorized users to view and share sensitive files in the organization’s network.

- ❑ Windows Information Protection (WIP) has an **endpoint data loss prevention** (DLP) capability that can be helpful in protecting local data at rest on endpoint devices
- ❑ WIP can be configured to store business data only on approved devices / within approved applications



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

If the user creates a file on a Windows 10 device, the Windows Defender ATP evaluates its content for sensitive or customized information. In case of file matches, Windows Defender ATP applies DLP at its endpoints. For data discovery, Windows Defender ATP integrates with Azure Information Protection (AIP) and reports the detected sensitive data. Files with sensitive information and sensitivity labels are aggregated by AIP.

- As WIP separates corporate and personal data, there is no need for an employee to switch the applications or environments.
- It reinforces the data protection for existing line-of-business applications.
- WIP can remove the corporate data from Intune MDM enrolled devices.
- For configuration, deployment, and management, WIP integrates with Microsoft Intune, System Center Configuration Manager, or the current mobile device management.

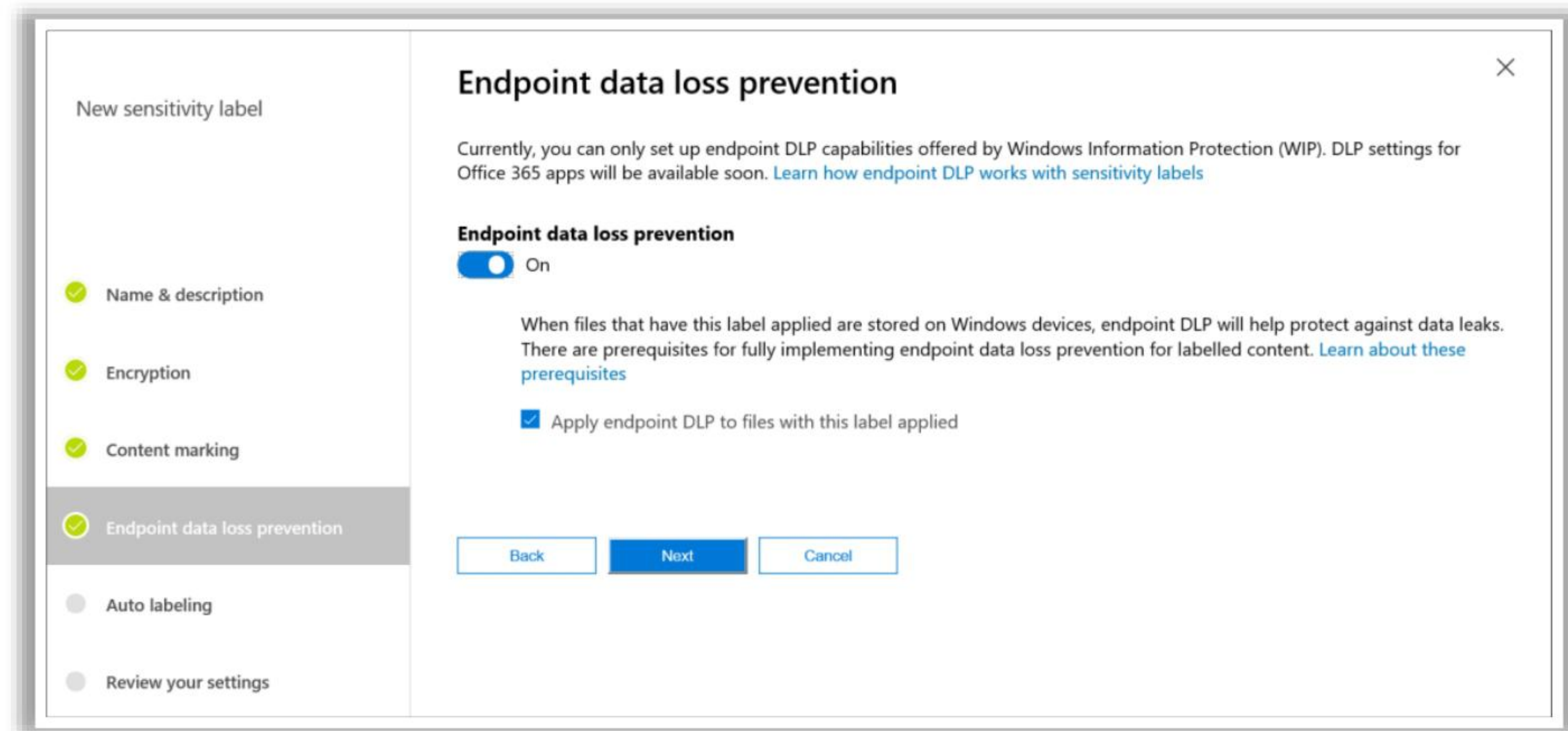
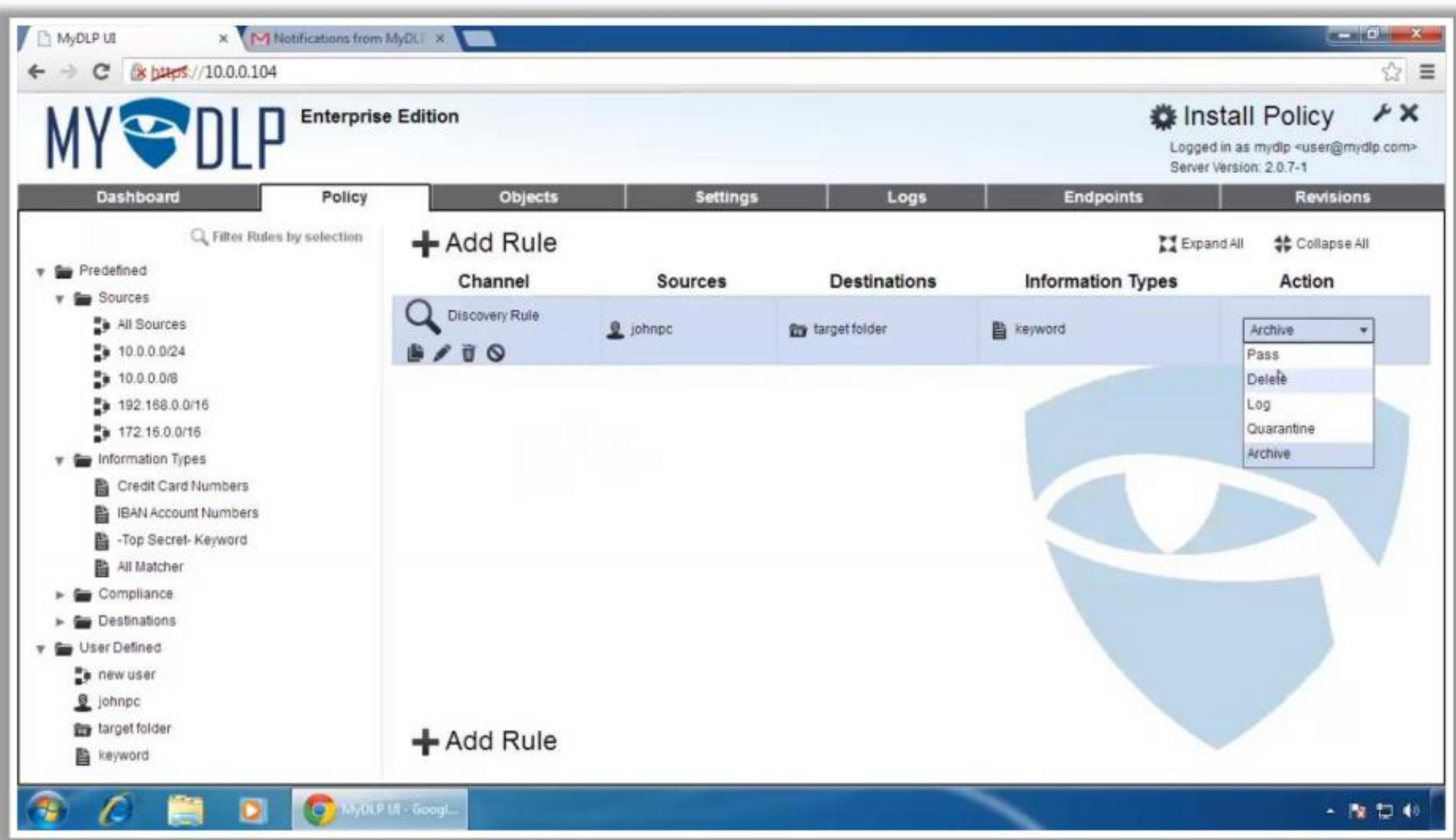


Figure 15.102: Screenshot of WIP

DLP Solutions

**MyDLP**

MyDLP allows the user to monitor, inspect, and **prevent all outgoing confidential data** without any hassle



<https://mydlp.com>



Symantec Data Loss Prevention
<https://www.symantec.com>



SecureTrust Data Loss Prevention
<https://www.securetrust.com>



McAfee Total Protection
<https://www.mcafee.com>



Check Point Data Loss Prevention
<https://www.checkpoint.com>



Digital Guardian Endpoint DLP
<https://digitalguardian.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

DLP Solutions

- **MyDLP**

Source: <https://mydlp.com>

MyDLP is a free and open-source solution that allows organizations to secure confidential data. The supported data inspection channels include web, email, instant messaging, printers, removable storage devices, screenshots, etc. MyDLP allows the user to monitor, inspect, and prevent all outgoing confidential data without any hassle. With its painless deployment and configuration, an easy-to-use policy interface, and great performance, IT administrators and security officers are able to effectively combat data leakage.

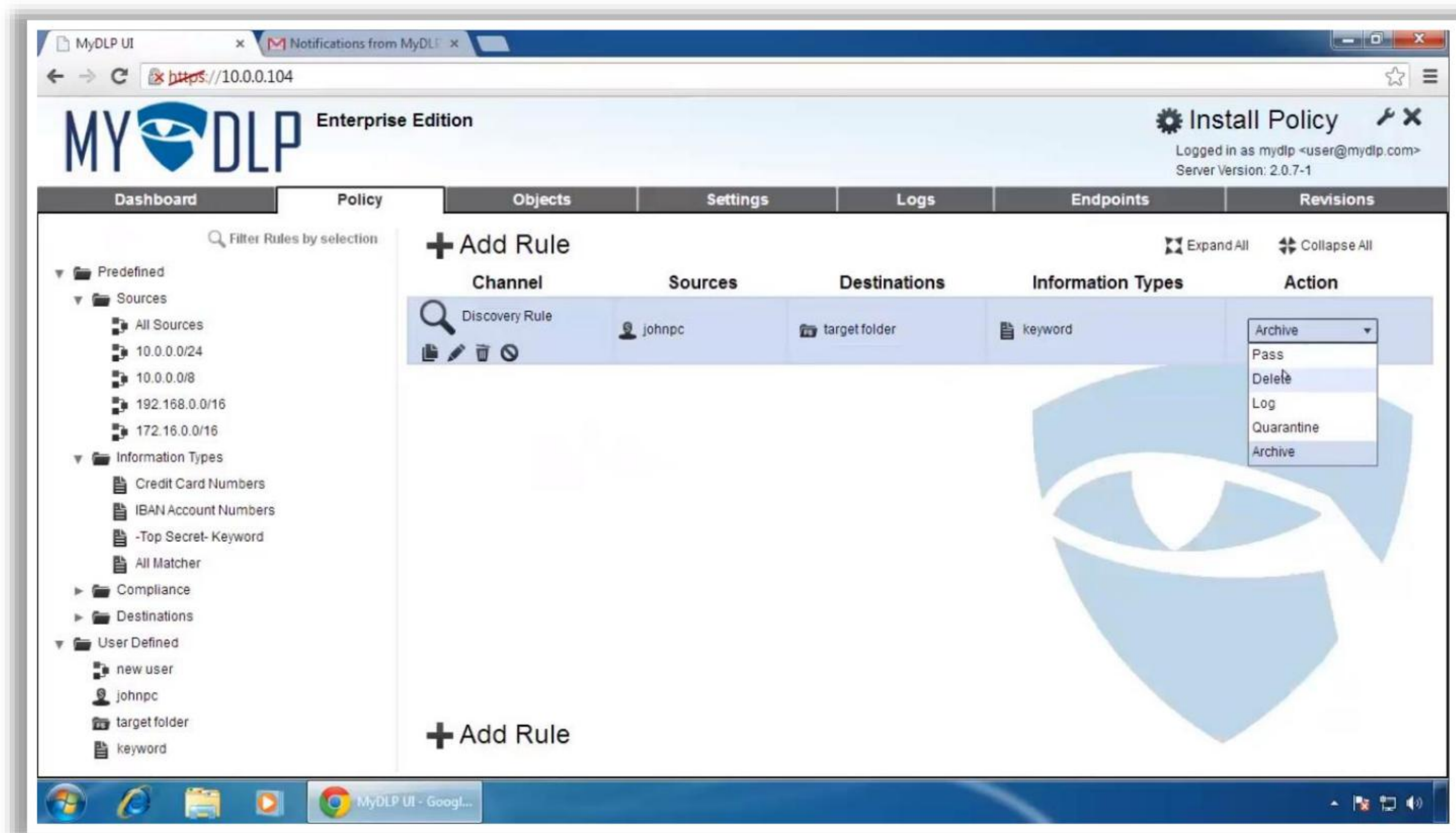


Figure 15.103: Screenshot of MyDLP

Some additional DLP solutions are as follows:

- Symantec Data Loss Prevention (<https://www.symantec.com>)
- SecureTrust Data Loss Prevention (<https://www.securetrust.com>)
- McAfee Total Protection (<https://www.mcafee.com>)
- Check Point Data Loss Prevention (<https://www.checkpoint.com>)
- Digital Guardian Endpoint DLP (<https://digitalguardian.com>)



Best Practices for a Successful DLP Implementation

- ✓ Identify the **main objective** of DLP
- ✓ Identify **sensitive data** for protection
- ✓ Evaluate available **DLP vendors**
- ✓ Ensure that the selected DLP product is **compatible** and supports the required data types and data stores of your organization
- ✓ Identify the **roles** and **responsibilities** of individuals for implementing the DLP solution
- ✓ Implement **DLP** with a minimal base to reduce false positives, and enhance the base gradually by identifying sensitive data
- ✓ Enhance the **DLP policies** to support effective DLP operations and eliminate false positives

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices for a Successful DLP Implementation

DLP safeguards sensitive information in an organization. Implementation of DLP not only prevents the leakage of sensitive data, but also allows the security professional to monitor and control the data accessed and shared by an end user.

Some best practices for a successful DLP implementation are as follows:

- Identify the main objective of DLP.
- Identify sensitive data for protection.
- Evaluate the available DLP vendors.
- Ensure that the selected DLP product is compatible and supports the required data types and data stores of the organization.
- Identify the roles and responsibilities of individuals for the implementation of DLP solution.
- Implement DLP with a minimal base to reduce false positives and enhance the base gradually by identifying sensitive data.
- Enhance the DLP policies to support effective DLP operations and eliminate false positives.

Module Summary



- ➡ This module discussed data security and its importance
- ➡ It discussed different data security technologies
- ➡ It also discussed various data security controls
- ➡ It discussed various disk, file, and removable-media encryption tools
- ➡ This module also discussed methods and tools for data backup, retention, and destruction
- ➡ Finally, this module presented an overview of data loss prevention (DLP) and DLP solutions
- ➡ In the next module, we will discuss network troubleshooting in detail

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

This module discussed data security and its importance. It discussed different data security technologies. It also discussed various data security controls. Furthermore, it demonstrated various disk, file, and removable-media encryption tools. Moreover, this module discussed the methods and tools for data backup, retention, and destruction. Finally, this module presented an overview of data loss prevention (DLP) and DLP solutions.

In the next module, we will discuss network troubleshooting in detail.

This page is intentionally left blank.