CompTIA Security+

Data Encryption

- **Introduction**
- **Exercise 1 - Full Disk Encryption using BitLocker**
- **Exercise 2 - Manage Security for Removable Media**
- **Summary**

Introduction

The **Data Encryption** module provides you with the instruction and Server hardware to develop your hands-on skills. This module includes the following exercises:

- Full Disk Encryption using Bitlocker
- Configure Security for Removable Media
- Using Cryptography Tools

Lab time: It will take approximately 1 hour to complete this lab.

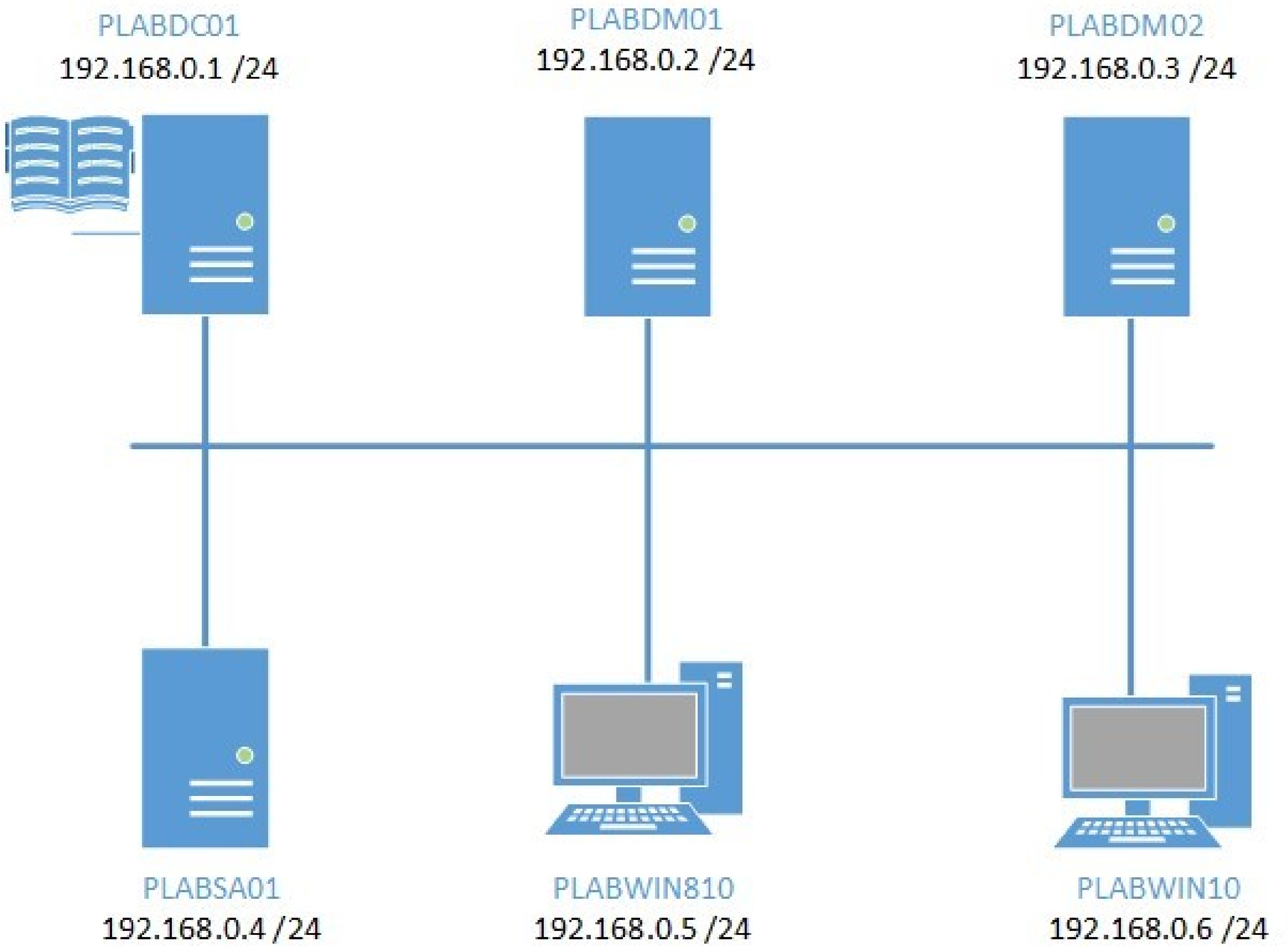
Exam Objectives

The following exam objectives are covered in this lab:

- **SY0-501 3.6:** Summarize secure application development and deployment concepts

Lab Diagram

During your session you will have access to the following lab configuration.



Connecting to your Lab

In this module you will be working on the following equipment to carry out the steps defined in each exercise.

- **PLABDC01** (Windows Server 2012 R2 - Domain Controller)
- **PLABWIN810** (Windows 8.1 - Domain Workstation)

For further information and technical support, please see our Help and Support page.

Exercise 1 - Full Disk Encryption using BitLocker

Windows BitLocker is a storage encryption technology that gives administrators the capability to secure fixed and removable disks including portable USB drives using encryption services built into the operating system.

BitLocker was first introduced in Windows Server 2008 and Windows 7 Enterprise and then carried over to later versions. Disk encryption can be enabled using a local or domain group policy. To unlock an encrypted disk volume, the user must type the password to unlock it. In the event the user forgets the password for unlocking the encrypted volume, the Recovery Keys generated by BitLocker can be used to gain access to the encrypted drive.

To get a better understanding of this technology, please refer to your course material or use your preferred search engine to research this topic in more detail.

Task 1 - Configure BitLocker settings via GPO

In this task, you will create a Group Policy that will enforce BitLocker on the disk volumes of Windows 8.1 devices

To configure BitLocker settings using group policy objects, follow these steps:

Step 1

Ensure you have powered on the required devices in the Introduction of this lab.

Connect to **PLABDC01** server.

The **Server Manager Dashboard** automatically opens upon logon.

Click on **Tools** menu and select **Group Policy Management.**

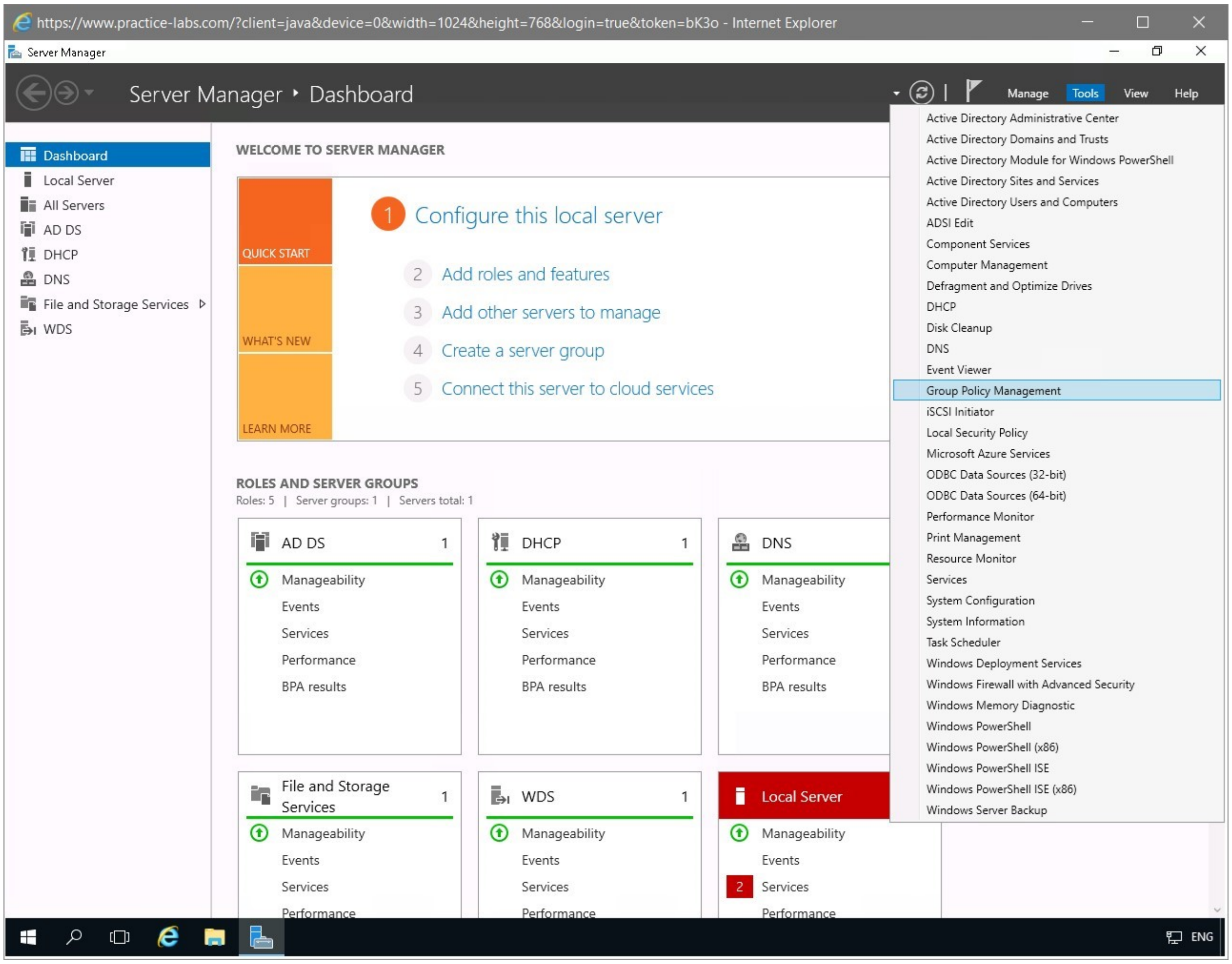

https://www.practice-labs.com/?client=java&device=0&width=1024&height=768&login=true&token=bK3o - Internet Explorer
Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DHCP
DNS
File and Storage Services
WDS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
ROLES AND SERVER GROUPS
Roles: 5 | Server groups: 1 | Servers total: 1
AD DS 1
DHCP 1
DNS
Manageability
Events
Services
Performance
BPA results
File and Storage Services 1
WDS 1
Local Server
2
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
DHCP
Disk Cleanup
DNS
Event Viewer
Group Policy Management
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Print Management
Resource Monitor
Services
System Configuration
System Information
Task Scheduler
Windows Deployment Services
Windows Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell
Windows PowerShell (x86)
Windows PowerShell ISE
Windows PowerShell ISE (x86)
Windows Server Backup
ENG

Figure 1.1 Screenshot of the PLABDC01 desktop: Server Manager Dashboard window is displayed showing the Tools > Group Policy Management menu-options selected.

Step 2

On the **Group Policy Management Console**, expand **Forest: PRACTICELABS.COM > Domains**.

Right-click on **PRACTICELABS.COM** and select **Create a GPO in this domain, and link it here**...

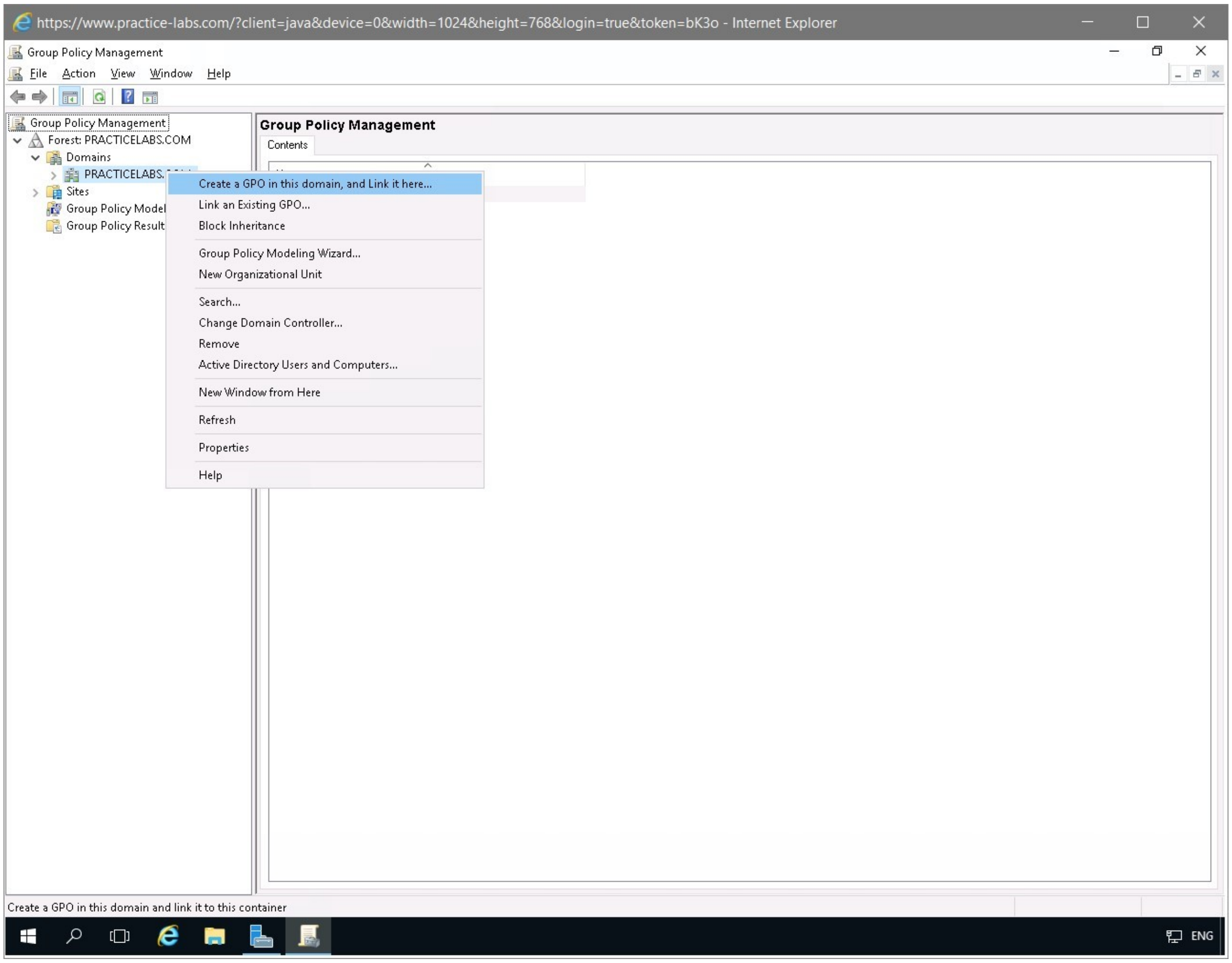

https://www.practice-labs.com/?client=java&device=0&width=1024&height=768&login=true&token=bK3o - Internet Explorer
Group Policy Management
File
Action
View
Window
Help
Group Policy Management
Forest: PRACTICELABS.COM
Domains
PRACTICELABS.
Sites
Group Policy Model
Group Policy Result
Group Policy Management
Contents
Create a GPO in this domain, and Link it here...
Link an Existing GPO...
Block Inheritance
Group Policy Modeling Wizard...
New Organizational Unit
Search...
Change Domain Controller...
Remove
Active Directory Users and Computers...
New Window from Here
Refresh
Properties
Help
Create a GPO in this domain and link it to this container
ENG

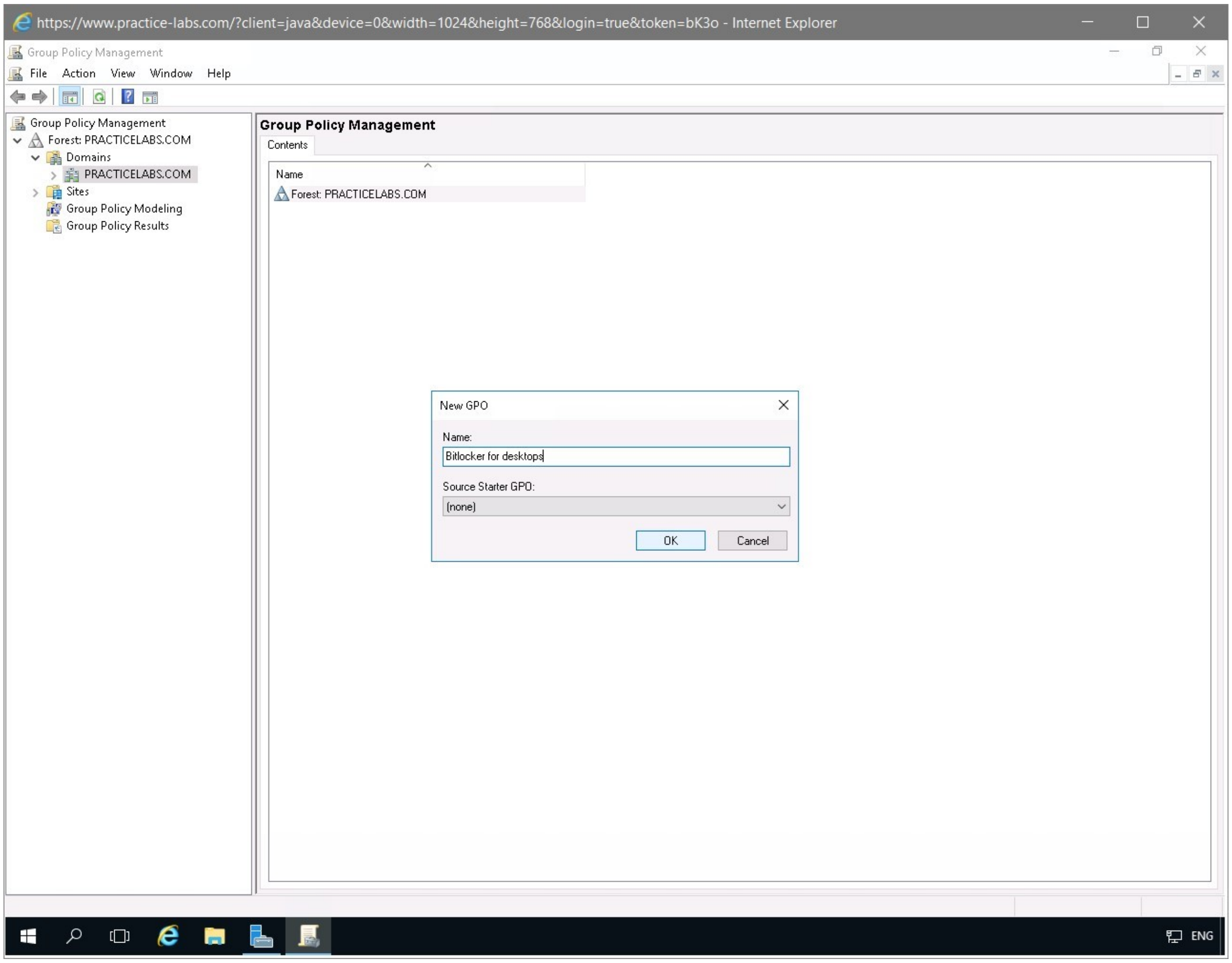
Figure 1.2 Screenshot of the PLABDC01 desktop: Context menu (that appears on right-clicking a domain name) > Create a GPO in this domain, and link it here menu-options are highlighted on the Group Policy Management console.

Step 3

On the **New GPO** dialog box, type the following text in the **Name** textbox:

```
Bitlocker for desktops
```

Click **OK**.



https://www.practice-labs.com/?client=java&device=0&width=1024&height=768&login=true&token=bK3o - Internet Explorer

New GPO

Name: Bitlocker for desktops

Source Starter GPO: (none)

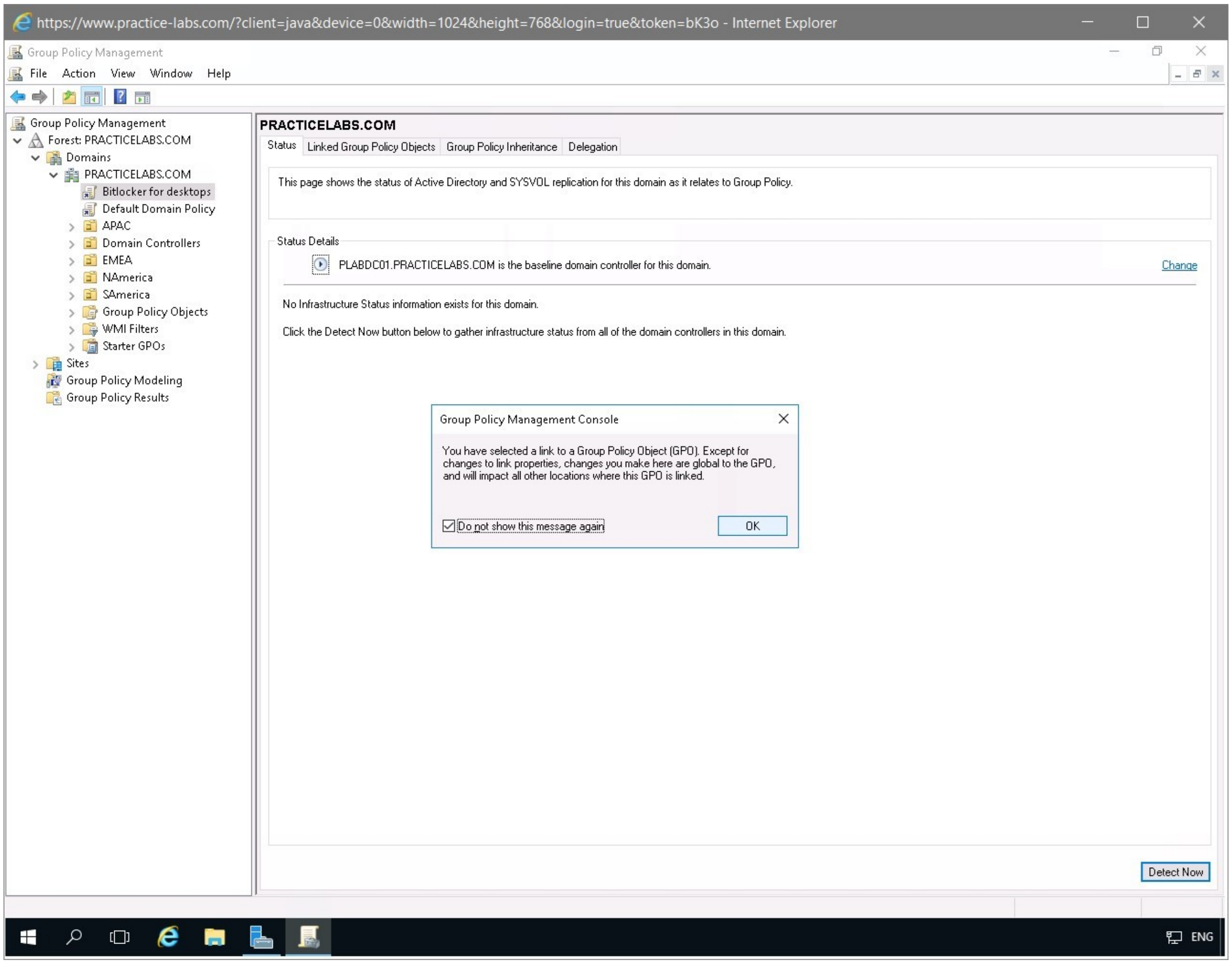
Figure 1.3 Screenshot of the PLABDC01 desktop: New GPO dialog box is displayed showing the required value typed-in and the OK button highlighted.

Step 4

Expand **PRACTICELABS.COM** in the left pane.

When you click the **Bitlocker for desktops** GPO link, you will get a message about changes to GPO link properties, apply to the GPO, select **Do not show this message again** check box.

Click **OK**.



https://www.practice-labs.com/?client=java&device=0&width=1024&height=768&login=true&token=bK3o - Internet Explorer

PRACTICELABS.COM

This page shows the status of Active Directory and SYSVOL replication for this domain as it relates to Group Policy.

Status Details

PLABDC01.PRACTICELABS.COM is the baseline domain controller for this domain.

No Infrastructure Status information exists for this domain.

Click the Detect Now button below to gather infrastructure status from all of the domain controllers in this domain.

Group Policy Management Console

You have selected a link to a Group Policy Object (GPO). Except for changes to link properties, changes you make here are global to the GPO, and will impact all other locations where this GPO is linked.

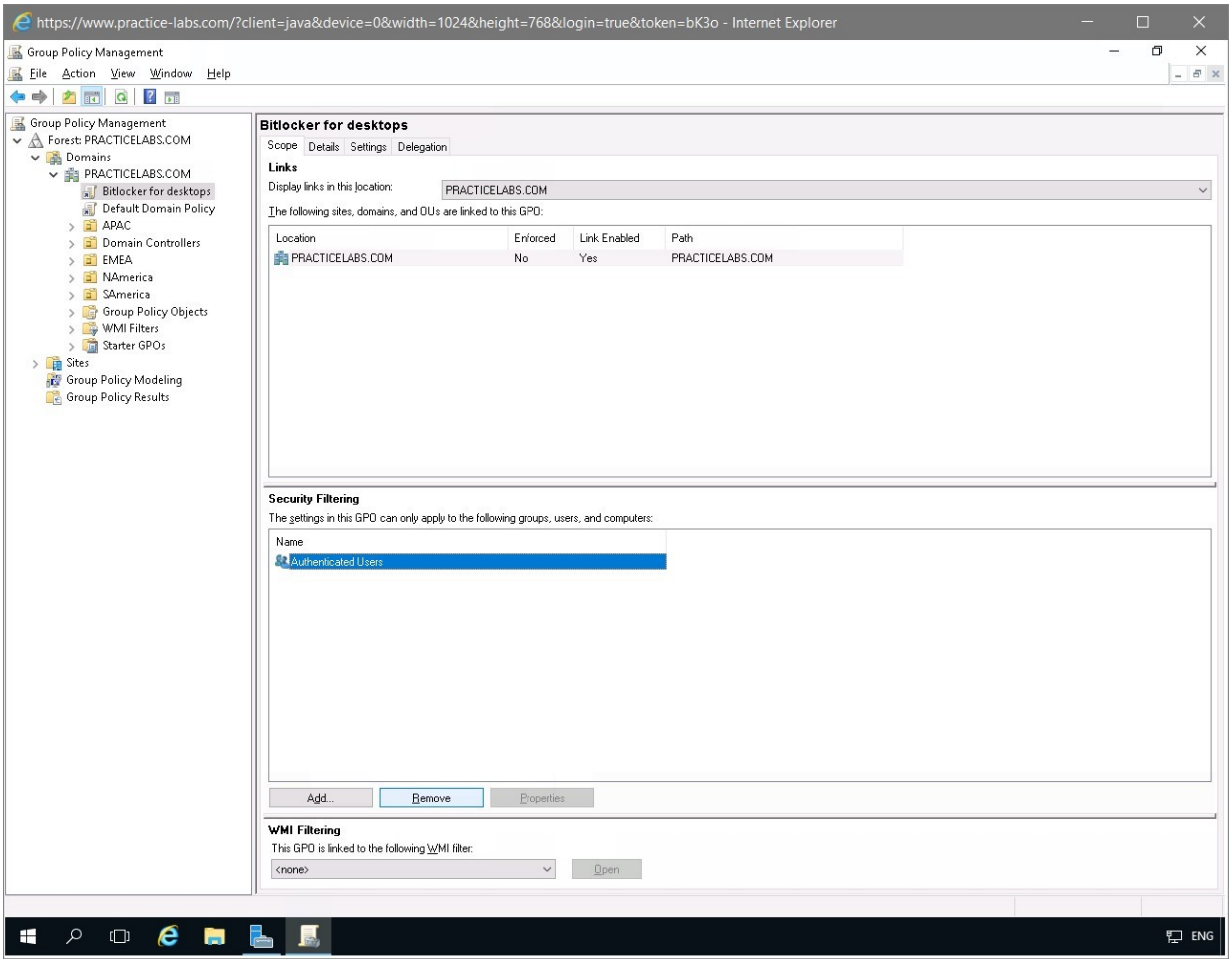
☑ Do not show this message again

Figure 1.4 Screenshot of the PLABDC01 desktop: Group Policy Management Console dialog box is

displayed showing the required settings performed and the OK button highlighted.

Step 5

Select **Authenticated Users** group in the **Security Filtering** section of the bottom right pane and click **Remove**.



Bitlocker for desktops

Links

Display links in this location: PRACTICELABS.COM

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
PRACTICELABS.COM	No	Yes	PRACTICELABS.COM

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
Authenticated Users

WMI Filtering

This GPO is linked to the following WMI filter:

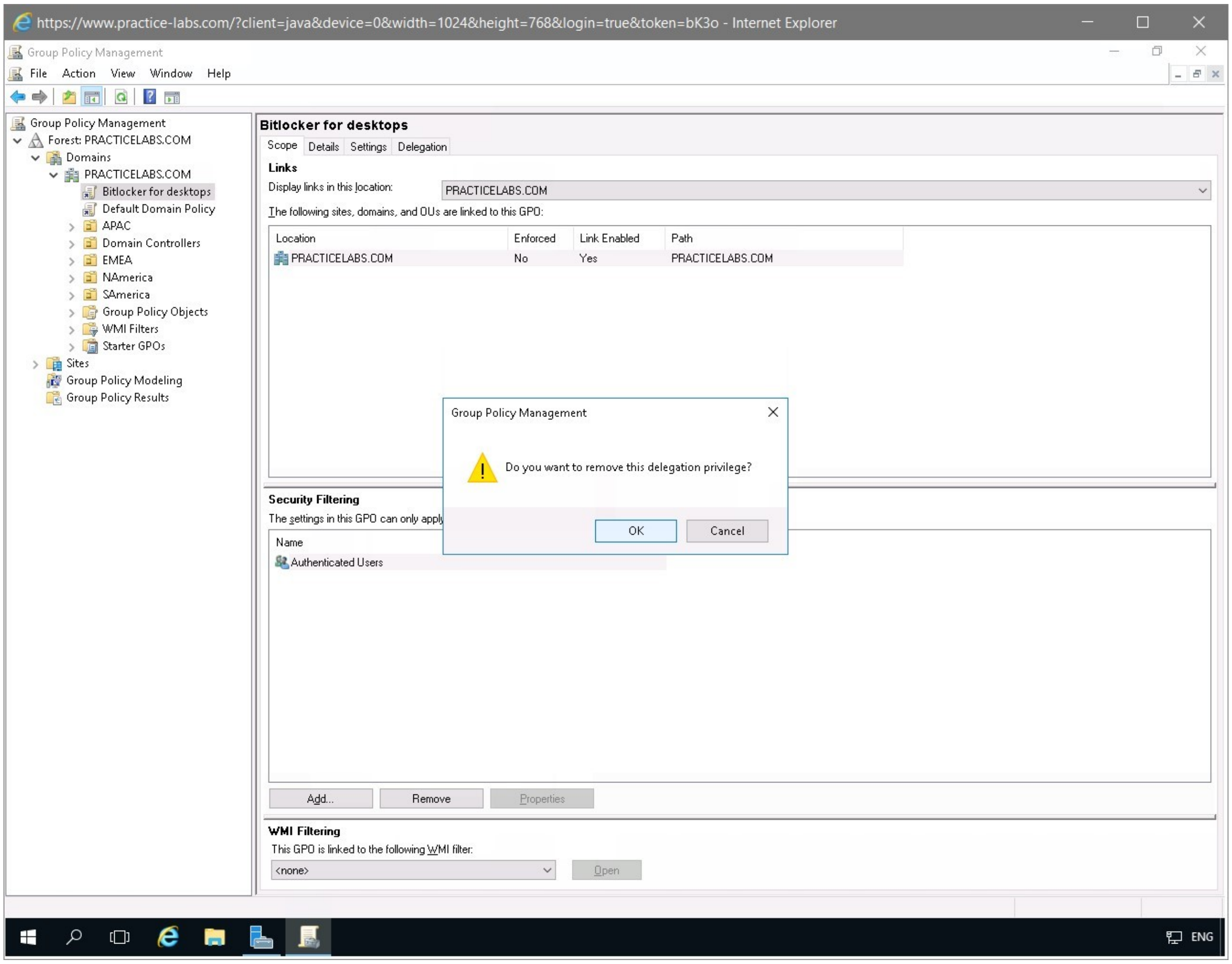
<none>

Figure 1.5 Screenshot of the PLABDC01 desktop: Security Filtering pane showing the required settings performed and the Remove button

highlighted is displayed on the Group Policy Management console with the required node-path selected on the navigation pane at the left.

Step 6

The **Group Policy Management** prompts for confirmation if you want to remove this delegation privilege, click **OK**.



https://www.practice-labs.com/?client=java&device=0&width=1024&height=768&login=true&token=bK3o - Internet Explorer

Bitlocker for desktops

Display links in this location: PRACTICELABS.COM

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
PRACTICELABS.COM	No	Yes	PRACTICELABS.COM

Group Policy Management

Do you want to remove this delegation privilege?

Security Filtering

The settings in this GPO can only apply

Name
Authenticated Users

WMI Filtering

This GPO is linked to the following WMI filter:

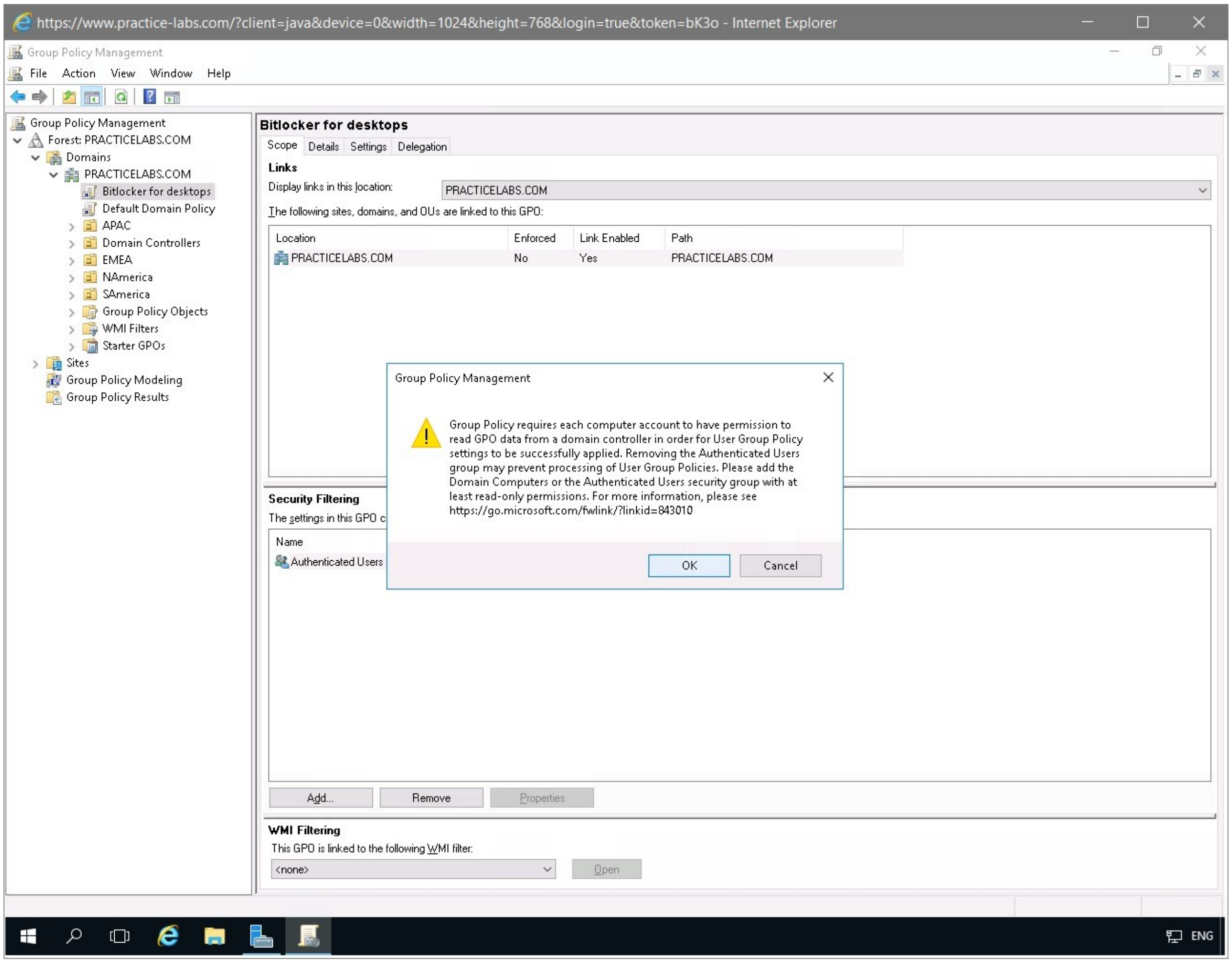
<none>

Figure 1.6 Screenshot of the PLABDC01 desktop: Group Policy Management caution box is

displayed prompting confirmation to remove the delegation privilege and the OK button highlighted.

Step 7

The **Group Policy Management** dialog box displays a message. Read the message and click **OK**.



Location	Enforced	Link Enabled	Path
PRACTICELABS.COM	No	Yes	PRACTICELABS.COM

Group Policy Management

Group Policy requires each computer account to have permission to read GPO data from a domain controller in order for User Group Policy settings to be successfully applied. Removing the Authenticated Users group may prevent processing of User Group Policies. Please add the Domain Computers or the Authenticated Users security group with at least read-only permissions. For more information, please see https://go.microsoft.com/fwlink/?linkid=843010

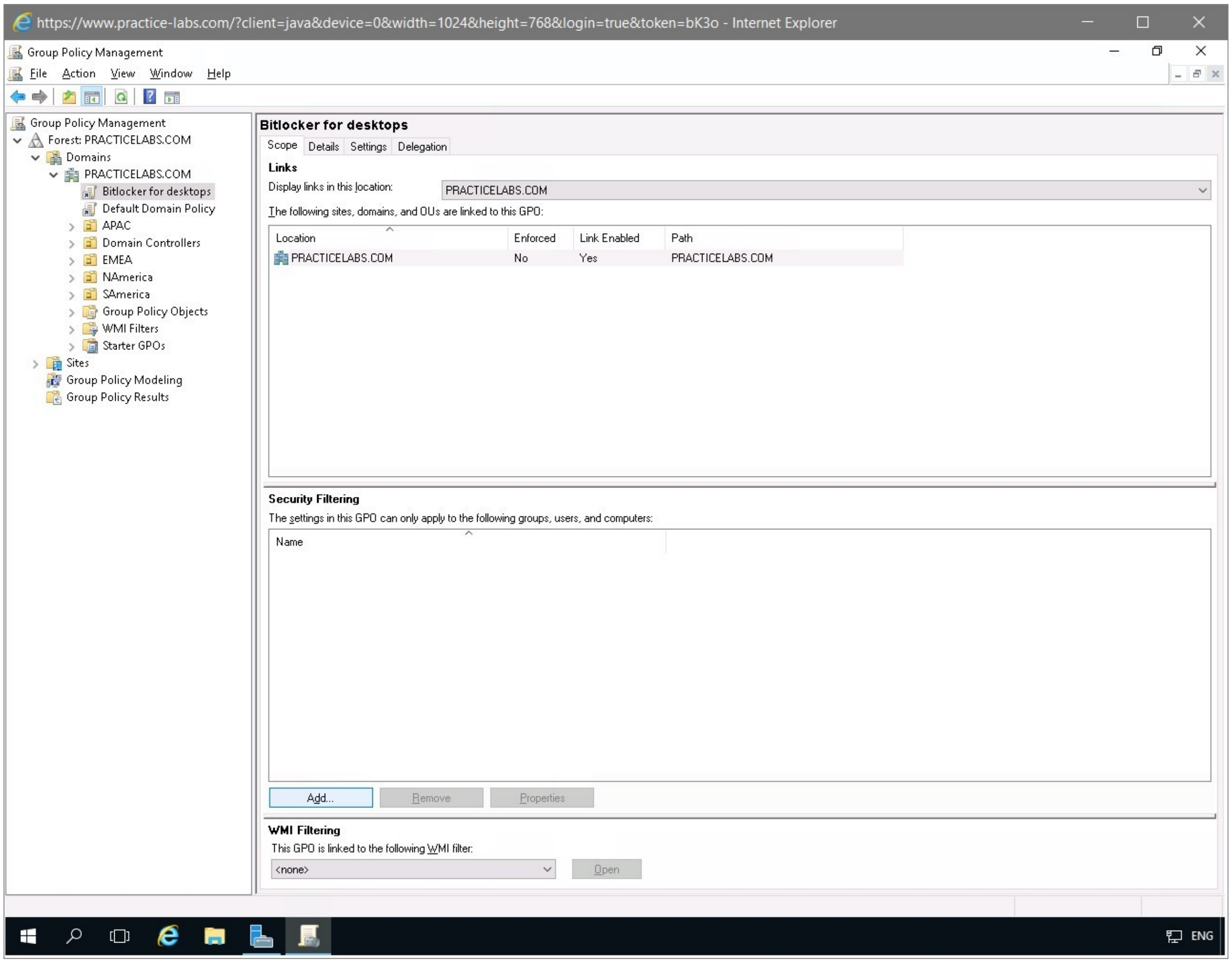
OK Cancel

Figure 1.7 Screenshot of the PLABDC01 desktop: Group Policy Management caution box is displayed listing the fallouts of removing the

delegation privilege and the OK button highlighted.

Step 8

Once again on the **Security Filtering** section, click **Add**.



Bitlocker for desktops

Links

Display links in this location: PRACTICELABS.COM

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
PRACTICELABS.COM	No	Yes	PRACTICELABS.COM

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name

WMI Filtering

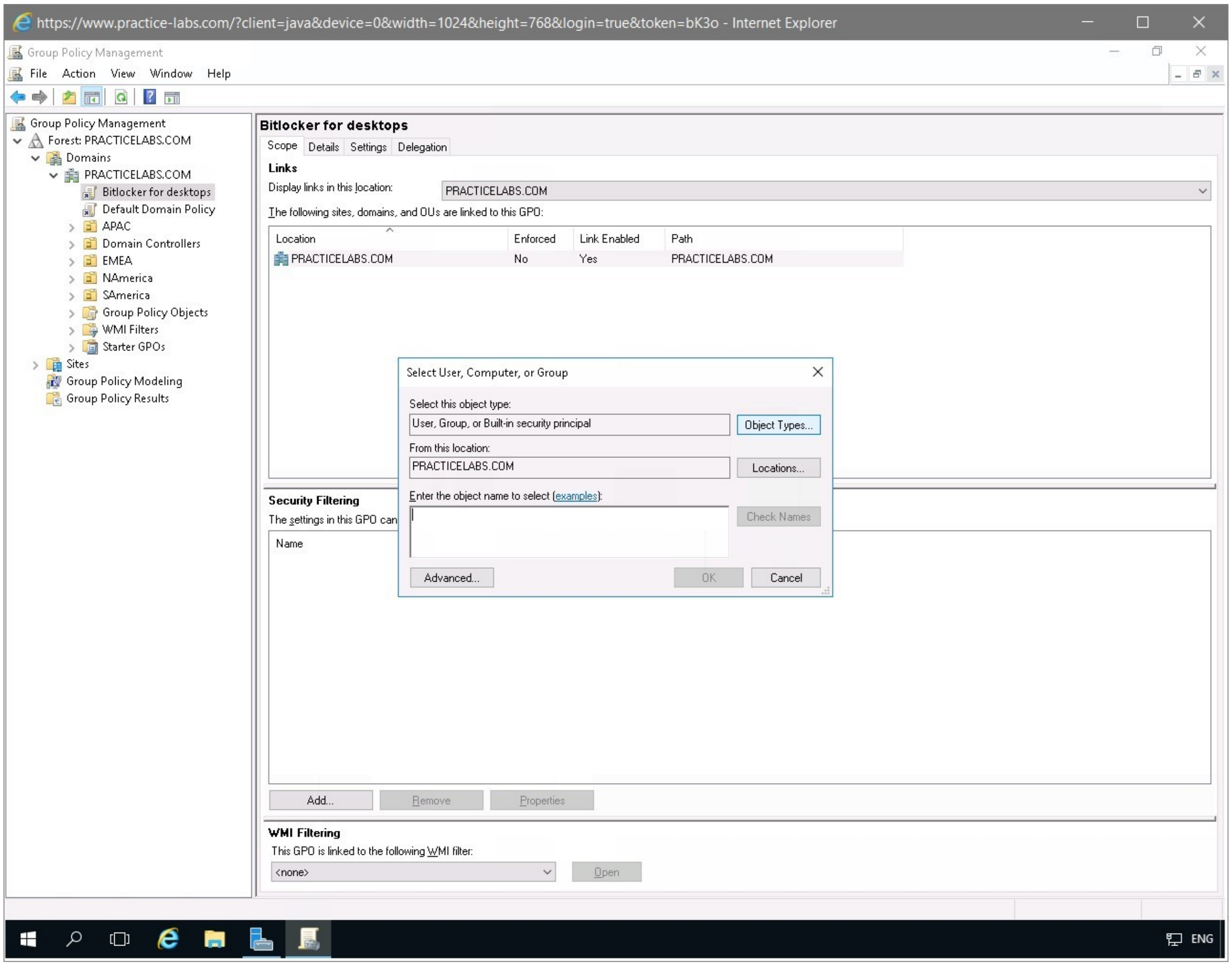
This GPO is linked to the following WMI filter:

<none>

Figure 1.8 Screenshot of the PLABDC01 desktop: Security Filtering pane showing the Add button highlighted is displayed on the Group Policy Management console with the required node-path selected on the navigation pane at the left.

Step 9

On **Select Computer, Computer or Group** dialog box, click **Object Types**.



https://www.practice-labs.com/?client=java&device=0&width=1024&height=768&login=true&token=bK3o - Internet Explorer

Bitlocker for desktops

Display links in this location: PRACTICELABS.COM

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
PRACTICELABS.COM	No	Yes	PRACTICELABS.COM

Select User, Computer, or Group

Select this object type: User, Group, or Built-in security principal

From this location: PRACTICELABS.COM

Enter the object name to select (examples):

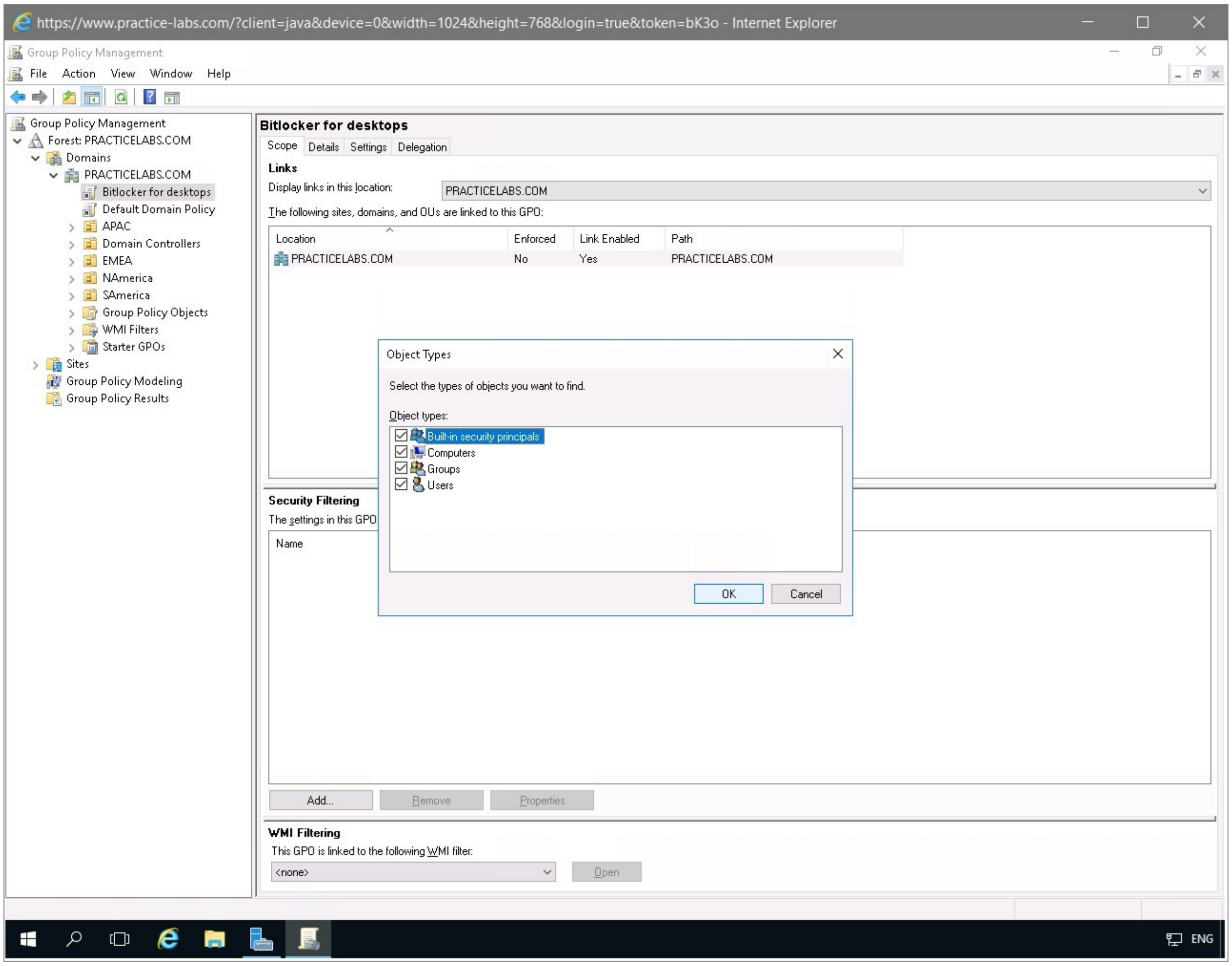
This GPO is linked to the following WMI filter: <none>

Figure 1.9 Screenshot of the PLABDC01 desktop: Select User, Computer, or Group dialog box is displayed showing the Object Types button highlighted.

Step 10

On the **Object Types** dialog box, enable **Computers** check box. Notice that other options are already selected.

Click **OK**.



https://www.practice-labs.com/?client=java&device=0&width=1024&height=768&login=true&token=bK3o - Internet Explorer

Object Types

Select the types of objects you want to find.

Object types:

☑ Built-in security principals
☑ Computers
☑ Groups
☑ Users

Bitlocker for desktops

Display links in this location: PRACTICELABS.COM

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
PRACTICELABS.COM	No	Yes	PRACTICELABS.COM

This GPO is linked to the following WMI filter: <none>

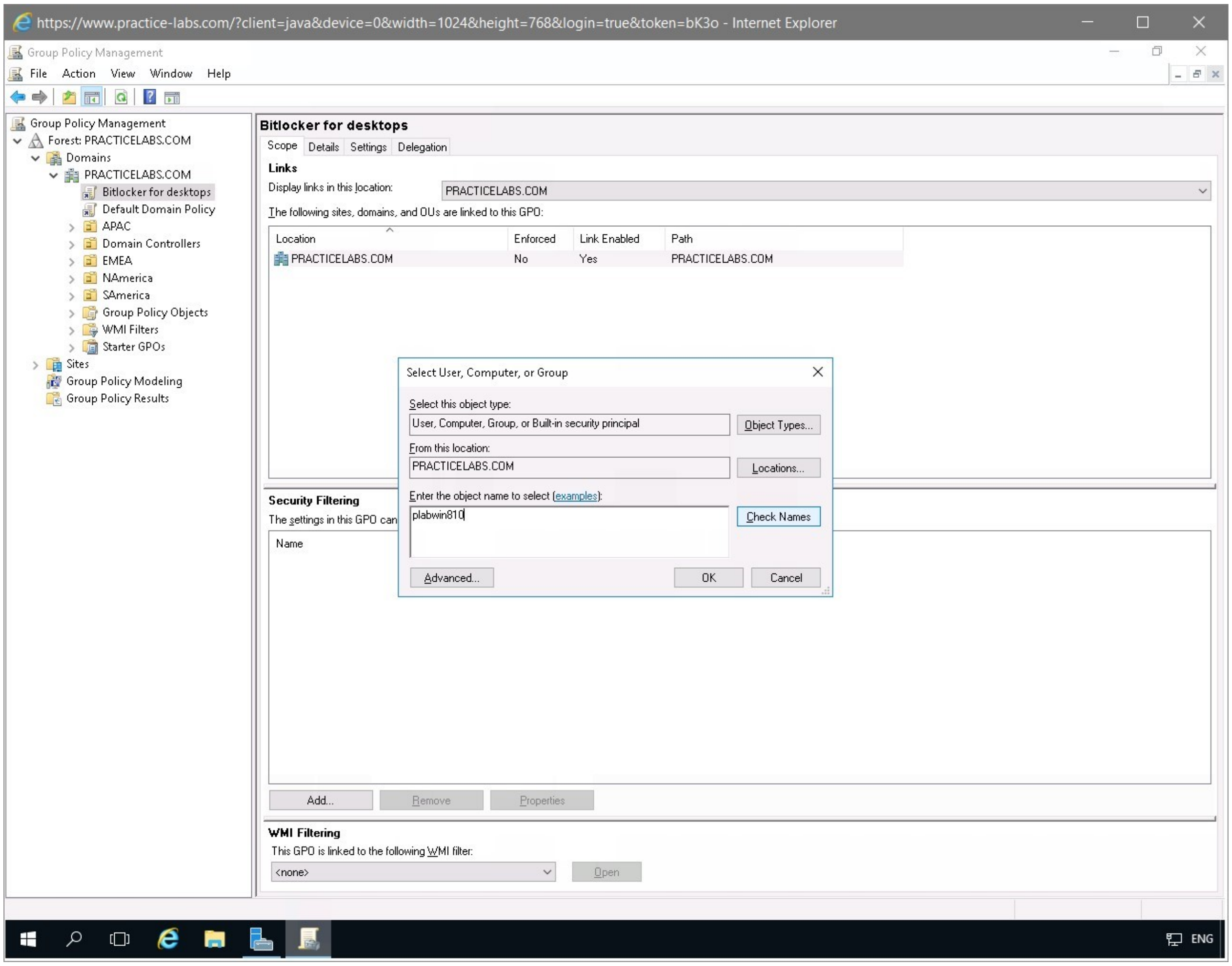
Figure 1.10 Screenshot of the PLABDC01 desktop: Object Types dialog box is displayed showing the required settings performed and the OK button highlighted.

Step 11

Back on the **Select Computer, Computer or Group** dialog box, click in the provided textbox and type:

```
plabwin810
```

Click **Check Names**.



https://www.practice-labs.com/?client=java&device=0&width=1024&height=768&login=true&token=bK3o - Internet Explorer

Select User, Computer, or Group

Select this object type: User, Computer, Group, or Built-in security principal

From this location: PRACTICELABS.COM

Enter the object name to select (examples): plabwin810

Bitlocker for desktops

Display links in this location: PRACTICELABS.COM

The following sites, domains, and OUs are linked to this GPO:

```
Location            Enforced   Link Enabled   Path
PRACTICELABS.COM    No         Yes            PRACTICELABS.COM
```

This GPO is linked to the following WMI filter: <none>

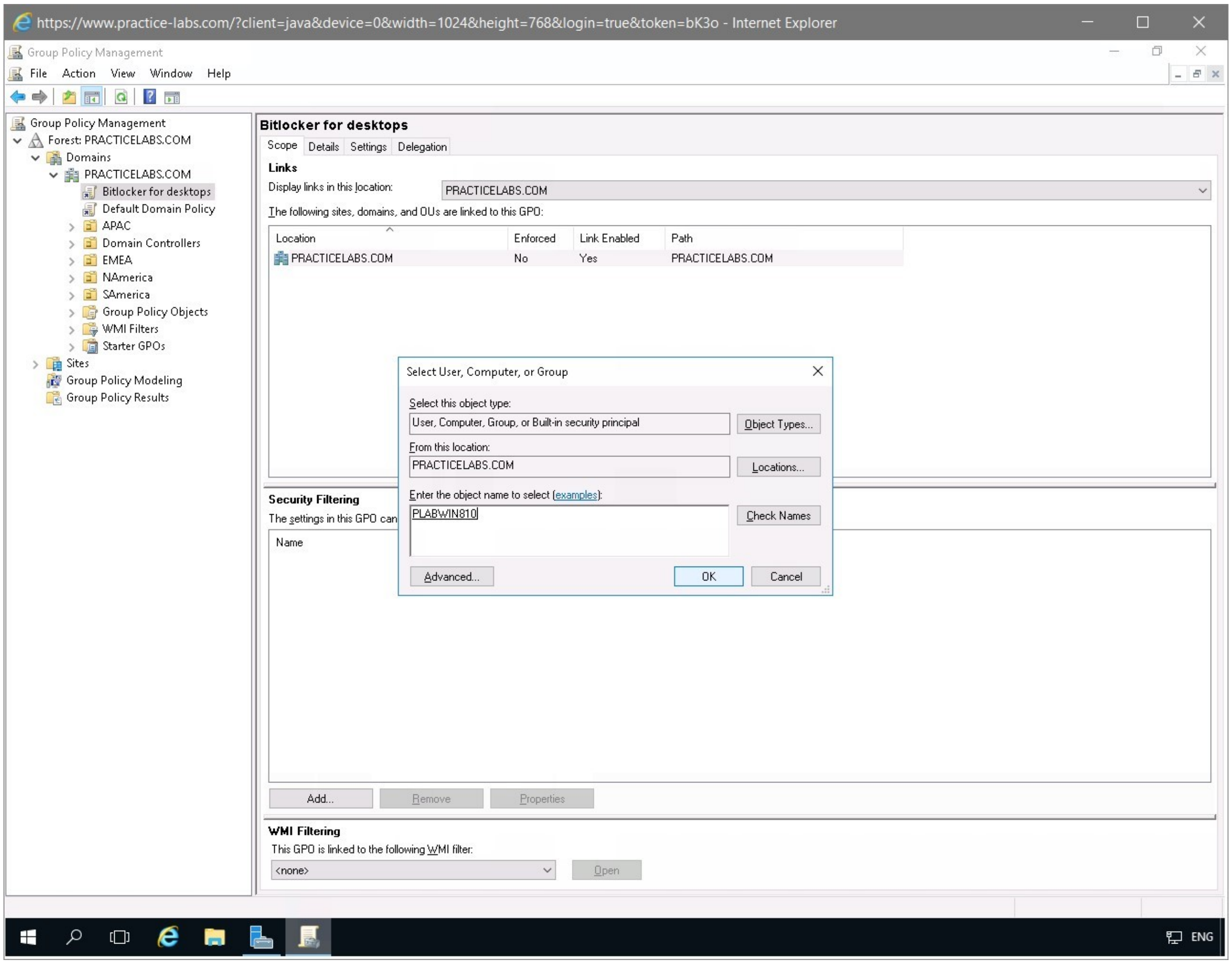
Figure 1.11 Screenshot of the PLABDC01 desktop: Select User, Computer, or Group dialog box is

displayed showing the required value typed-in and the Check Names button highlighted.

Step 12

The computer name **PLABWIN810** is now underlined. This means that the computer account is a member of the **PRACTICELABS.COM** domain.

Click **OK**.



Display links in this location: PRACTICELABS.COM

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
PRACTICELABS.COM	No	Yes	PRACTICELABS.COM

The settings in this GPO can

This GPO is linked to the following WMI filter: <none>

Select this object type: User, Computer, Group, or Built-in security principal

From this location: PRACTICELABS.COM

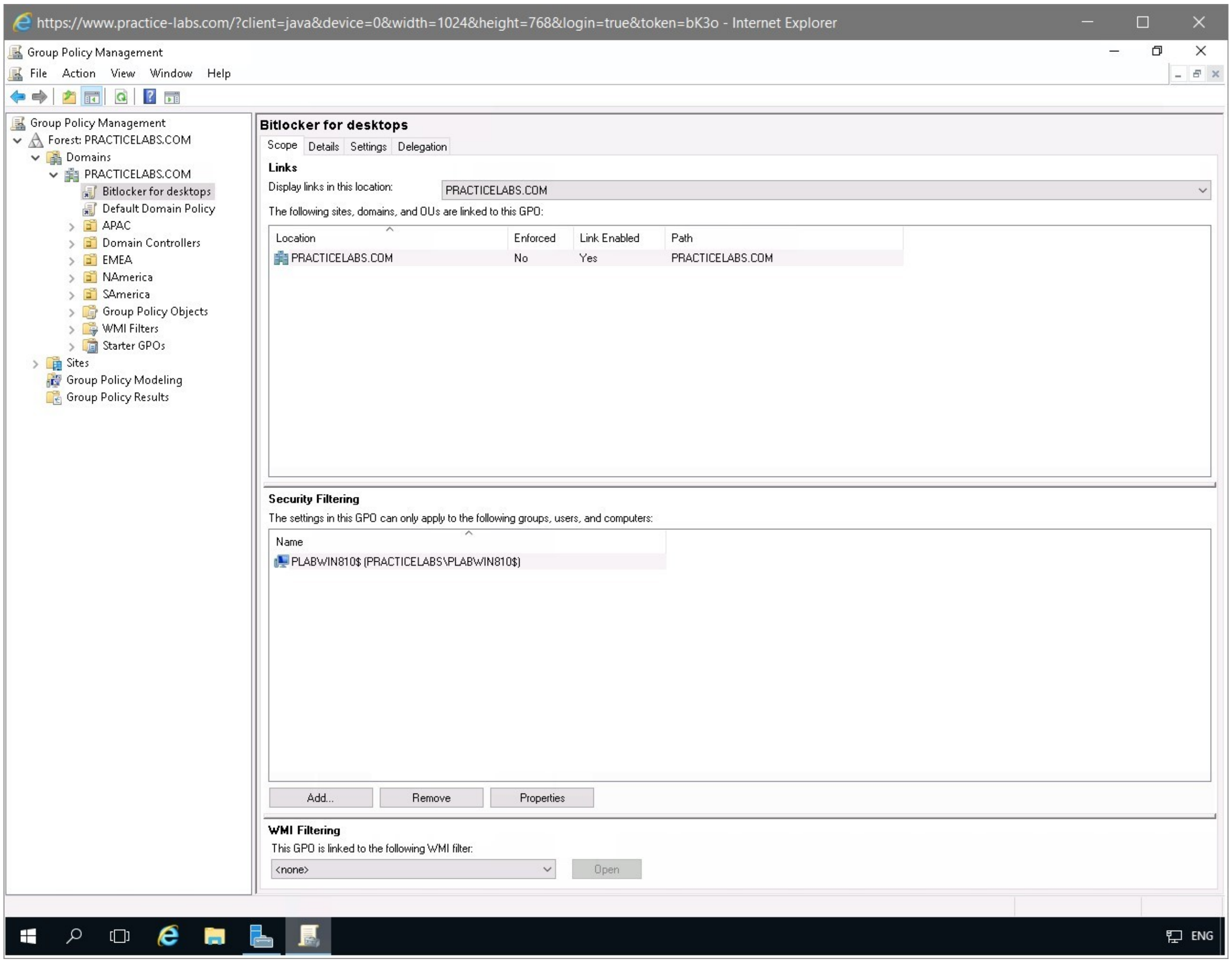
Enter the object name to select (examples): PLABWIN810

Figure 1.12 Screenshot of the PLABDC01 desktop: Select User, Computer, or Group dialog box is displayed showing the object name resolved and the OK button highlighted.

Step 13

PLABWIN810$ (PRACTICELABS\PLABWIN810$) is now added in the **Security Filtering** section.

This means that **Bitlocker for desktops** group policy will apply only to **PLABWIN810** computer.



Bitlocker for desktops

Links

Display links in this location: PRACTICELABS.COM

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
PRACTICELABS.COM	No	Yes	PRACTICELABS.COM

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
PLABWIN810$ (PRACTICELABS\PLABWIN810$)

WMI Filtering

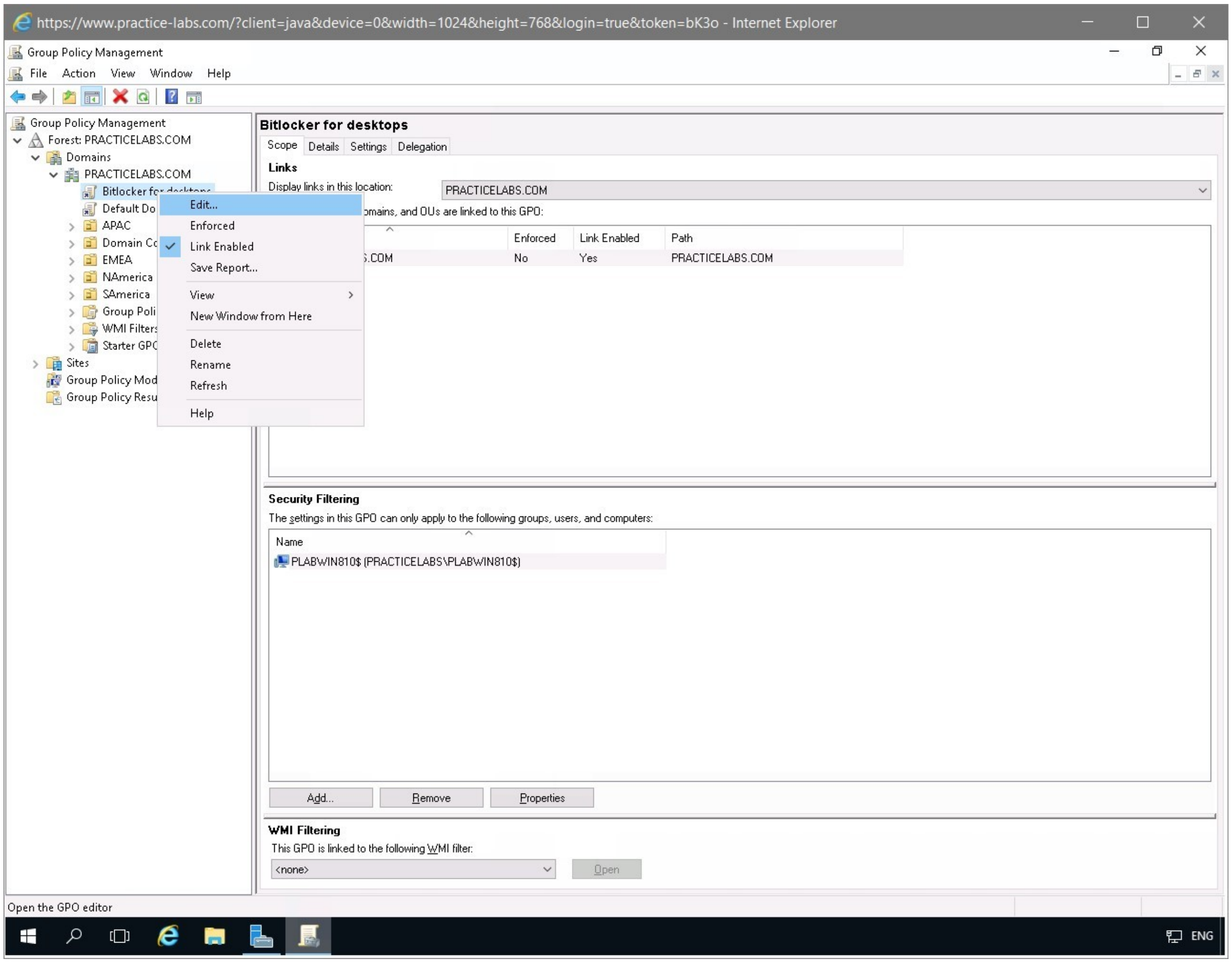
This GPO is linked to the following WMI filter:

<none>

Figure 1.13 Screenshot of the PLABDC01 desktop: Security Filtering pane on the Group Policy Management console is displayed listing the device added for bitlocker security.

Step 14

Under the **PRACTICELABS.COM** node, right-click on **Bitlocker for desktops** GPO link and choose **Edit**.



Bitlocker for desktops

Links

Display links in this location: PRACTICELABS.COM

…omains, and OUs are linked to this GPO:

	Enforced	Link Enabled	Path
…S.COM	No	Yes	PRACTICELABS.COM

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
PLABWIN810$ (PRACTICELABS\PLABWIN810$)

WMI Filtering

This GPO is linked to the following WMI filter:

<none>

Open the GPO editor

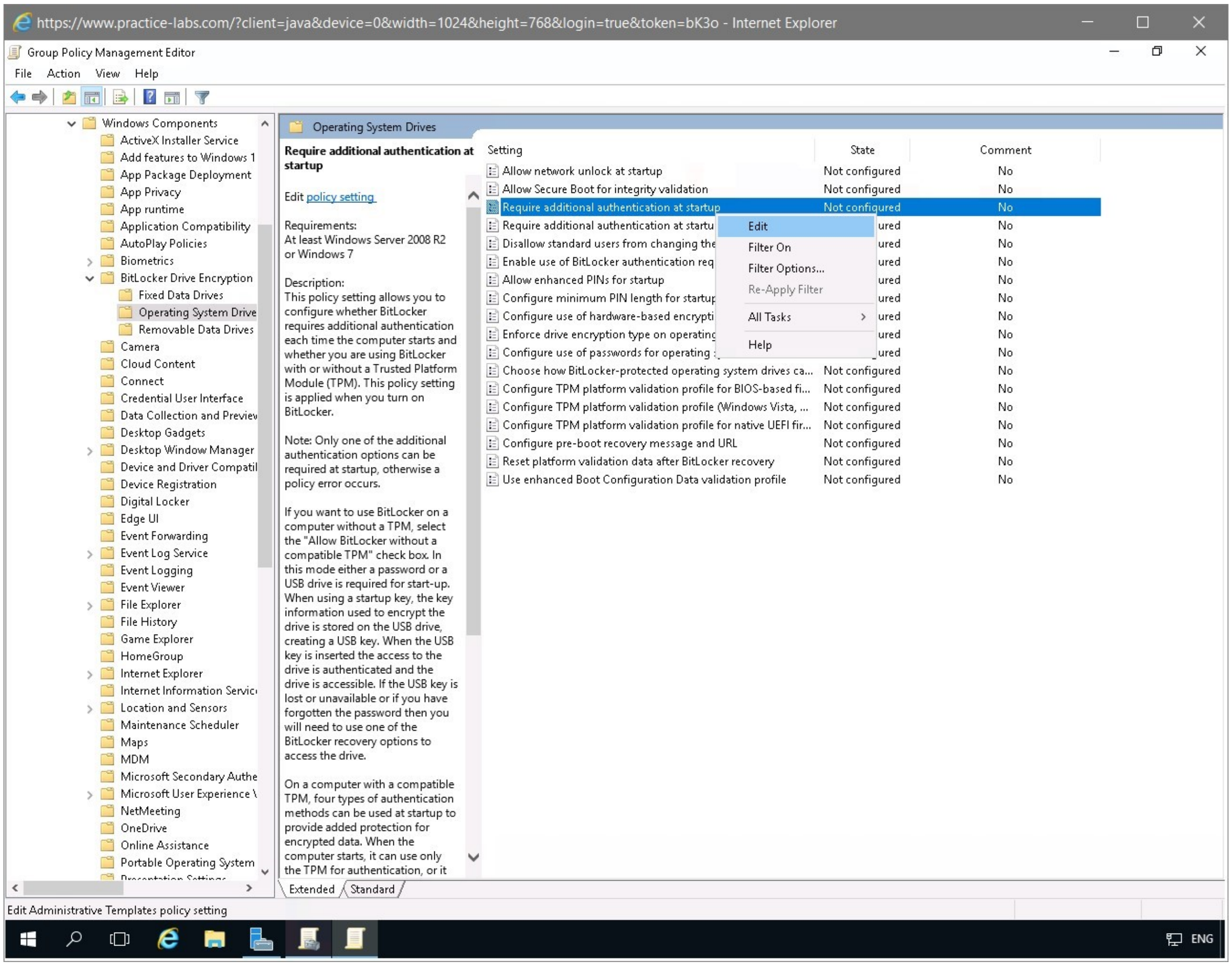
Figure 1.14 Screenshot of the PLABDC01 desktop: Context menu (that appears on right-clicking the Bitlocker for desktops node) > Edit menu-options are displayed on the Group Policy Management console.

Step 15

On the **Group Policy Management Editor** window, expand **Computer Configuration > Policies > Administrative Templates > Windows Components**

> Bitlocker Drive Encryption then click on **Operating System Drives**.

On the details pane on the right side, right-click on **Require additional authentication at startup** and choose **Edit**.



Require additional authentication at startup

Edit policy setting

Requirements:
At least Windows Server 2008 R2 or Windows 7

Description:
This policy setting allows you to configure whether BitLocker requires additional authentication each time the computer starts and whether you are using BitLocker with or without a Trusted Platform Module (TPM). This policy setting is applied when you turn on BitLocker.

Note: Only one of the additional authentication options can be required at startup, otherwise a policy error occurs.

If you want to use BitLocker on a computer without a TPM, select the "Allow BitLocker without a compatible TPM" check box. In this mode either a password or a USB drive is required for start-up. When using a startup key, the key information used to encrypt the drive is stored on the USB drive, creating a USB key. When the USB key is inserted the access to the drive is authenticated and the drive is accessible. If the USB key is lost or unavailable or if you have forgotten the password then you will need to use one of the BitLocker recovery options to access the drive.

On a computer with a compatible TPM, four types of authentication methods can be used at startup to provide added protection for encrypted data. When the computer starts, it can use only the TPM for authentication, or it

Setting	State	Comment
Allow network unlock at startup	Not configured	No
Allow Secure Boot for integrity validation	Not configured	No
Require additional authentication at startup	Not configured	No
Require additional authentication at startu	ured	No
Disallow standard users from changing the	ured	No
Enable use of BitLocker authentication req	ured	No
Allow enhanced PINs for startup	ured	No
Configure minimum PIN length for startup	ured	No
Configure use of hardware-based encrypti	ured	No
Enforce drive encryption type on operating	ured	No
Configure use of passwords for operating	ured	No
Choose how BitLocker-protected operating system drives ca...	Not configured	No
Configure TPM platform validation profile for BIOS-based fi...	Not configured	No
Configure TPM platform validation profile (Windows Vista, ...	Not configured	No
Configure TPM platform validation profile for native UEFI fir...	Not configured	No
Configure pre-boot recovery message and URL	Not configured	No
Reset platform validation data after BitLocker recovery	Not configured	No
Use enhanced Boot Configuration Data validation profile	Not configured	No

Figure 1.15 Screenshot of the PLABDC01 desktop: Context menu (that appears on right-clicking a listed policy setting) > Edit menu-options are displayed on the Group Policy Management Editor console.

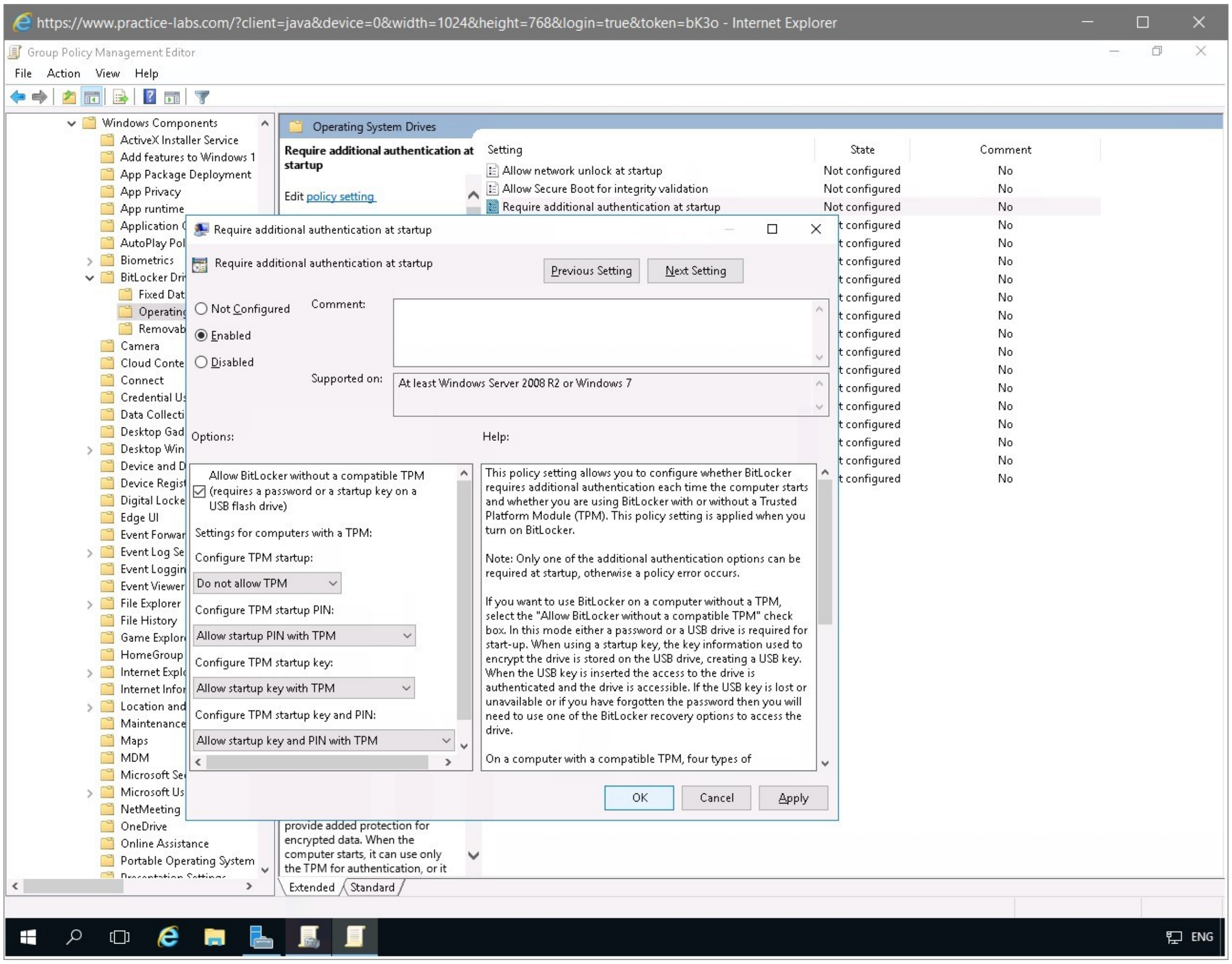
Step 16

From **Require additional authentication at startup**, click **Enabled**.

Under Options, click **Allow BitLocker without a compatible TPM**.

In the **Configure TPM** startup drop-down list, select **Do not allow TPM**.

Click **OK**.



Require additional authentication at startup

Setting	State	Comment
Allow network unlock at startup	Not configured	No
Allow Secure Boot for integrity validation	Not configured	No
Require additional authentication at startup	Not configured	No

Require additional authentication at startup

Previous Setting | Next Setting

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2008 R2 or Windows 7

Options:

☑ Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive)

Settings for computers with a TPM:

Configure TPM startup: Do not allow TPM

Configure TPM startup PIN: Allow startup PIN with TPM

Configure TPM startup key: Allow startup key with TPM

Configure TPM startup key and PIN: Allow startup key and PIN with TPM

Help:

This policy setting allows you to configure whether BitLocker requires additional authentication each time the computer starts and whether you are using BitLocker with or without a Trusted Platform Module (TPM). This policy setting is applied when you turn on BitLocker.

Note: Only one of the additional authentication options can be required at startup, otherwise a policy error occurs.

If you want to use BitLocker on a computer without a TPM, select the "Allow BitLocker without a compatible TPM" check box. In this mode either a password or a USB drive is required for start-up. When using a startup key, the key information used to encrypt the drive is stored on the USB drive, creating a USB key. When the USB key is inserted the access to the drive is authenticated and the drive is accessible. If the USB key is lost or unavailable or if you have forgotten the password then you will need to use one of the BitLocker recovery options to access the drive.

On a computer with a compatible TPM, four types of

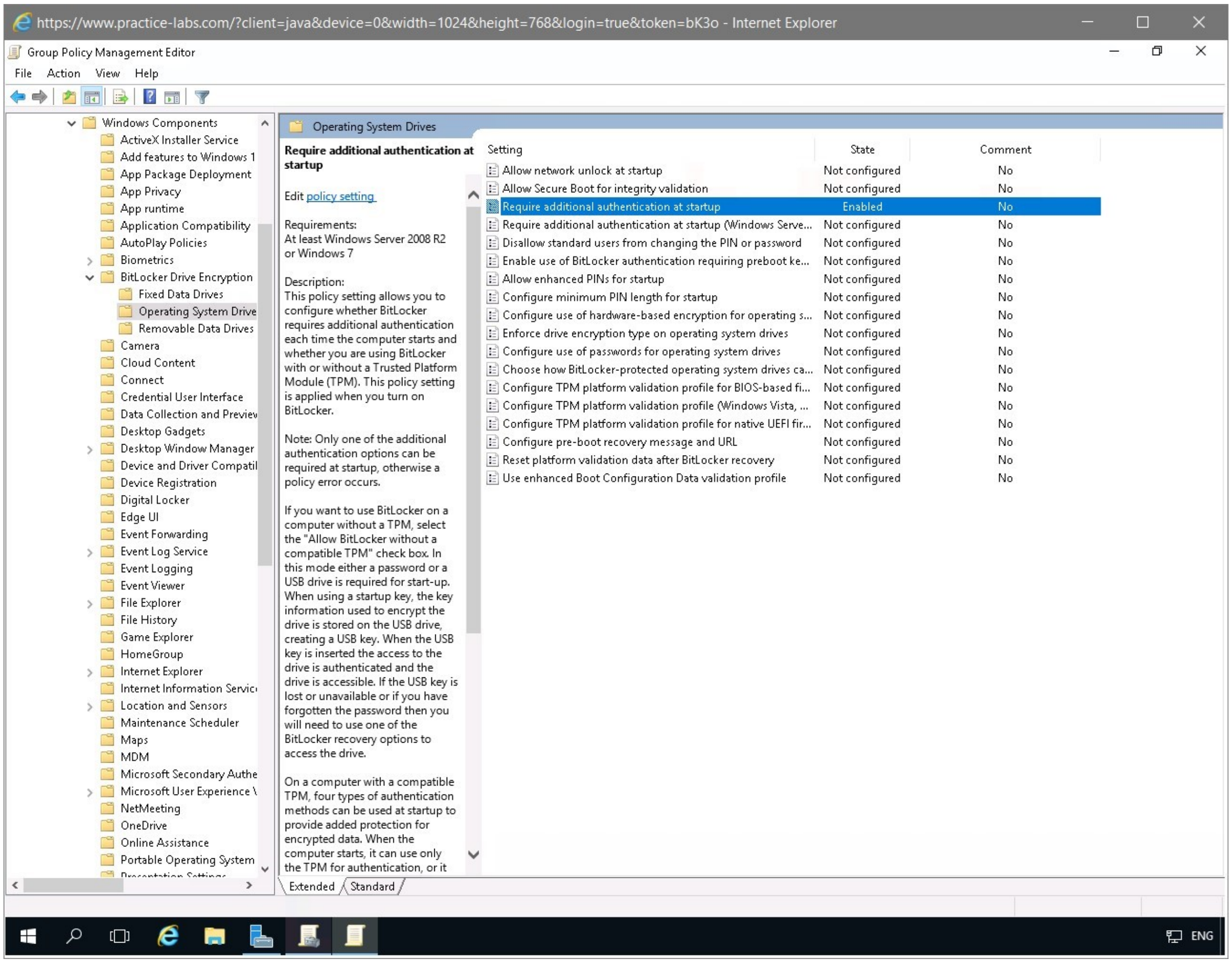
OK | Cancel | Apply

Figure 1.16 Screenshot of the PLABDC01 desktop: Require additional authentication at startup console is displayed showing the required settings performed and the OK button highlighted.

Step 17

Notice that **Require additional authentication at startup setting** is now enabled.

Close **Group Policy Management Editor** and **Group Policy Management console**.



Require additional authentication at startup

Edit policy setting

Requirements:
At least Windows Server 2008 R2 or Windows 7

Description:
This policy setting allows you to configure whether BitLocker requires additional authentication each time the computer starts and whether you are using BitLocker with or without a Trusted Platform Module (TPM). This policy setting is applied when you turn on BitLocker.

Note: Only one of the additional authentication options can be required at startup, otherwise a policy error occurs.

If you want to use BitLocker on a computer without a TPM, select the "Allow BitLocker without a compatible TPM" check box. In this mode either a password or a USB drive is required for start-up. When using a startup key, the key information used to encrypt the drive is stored on the USB drive, creating a USB key. When the USB key is inserted the access to the drive is authenticated and the drive is accessible. If the USB key is lost or unavailable or if you have forgotten the password then you will need to use one of the BitLocker recovery options to access the drive.

On a computer with a compatible TPM, four types of authentication methods can be used at startup to provide added protection for encrypted data. When the computer starts, it can use only the TPM for authentication, or it

Setting	State	Comment
Allow network unlock at startup	Not configured	No
Allow Secure Boot for integrity validation	Not configured	No
Require additional authentication at startup	Enabled	No
Require additional authentication at startup (Windows Serve...	Not configured	No
Disallow standard users from changing the PIN or password	Not configured	No
Enable use of BitLocker authentication requiring preboot ke...	Not configured	No
Allow enhanced PINs for startup	Not configured	No
Configure minimum PIN length for startup	Not configured	No
Configure use of hardware-based encryption for operating s...	Not configured	No
Enforce drive encryption type on operating system drives	Not configured	No
Configure use of passwords for operating system drives	Not configured	No
Choose how BitLocker-protected operating system drives ca...	Not configured	No
Configure TPM platform validation profile for BIOS-based fi...	Not configured	No
Configure TPM platform validation profile (Windows Vista, ...	Not configured	No
Configure TPM platform validation profile for native UEFI fir...	Not configured	No
Configure pre-boot recovery message and URL	Not configured	No
Reset platform validation data after BitLocker recovery	Not configured	No
Use enhanced Boot Configuration Data validation profile	Not configured	No

Figure 1.17 Screenshot of the PLABDC01 desktop: Group Policy Management Editor console is displayed showing the required policy enabled.

Step 18

Keep **Server Manager Dashboard** running on **PLABDC01**.

Keep all devices powered on in their current state and proceed to the next task.

Task 2 - Shrink the Existing Drive

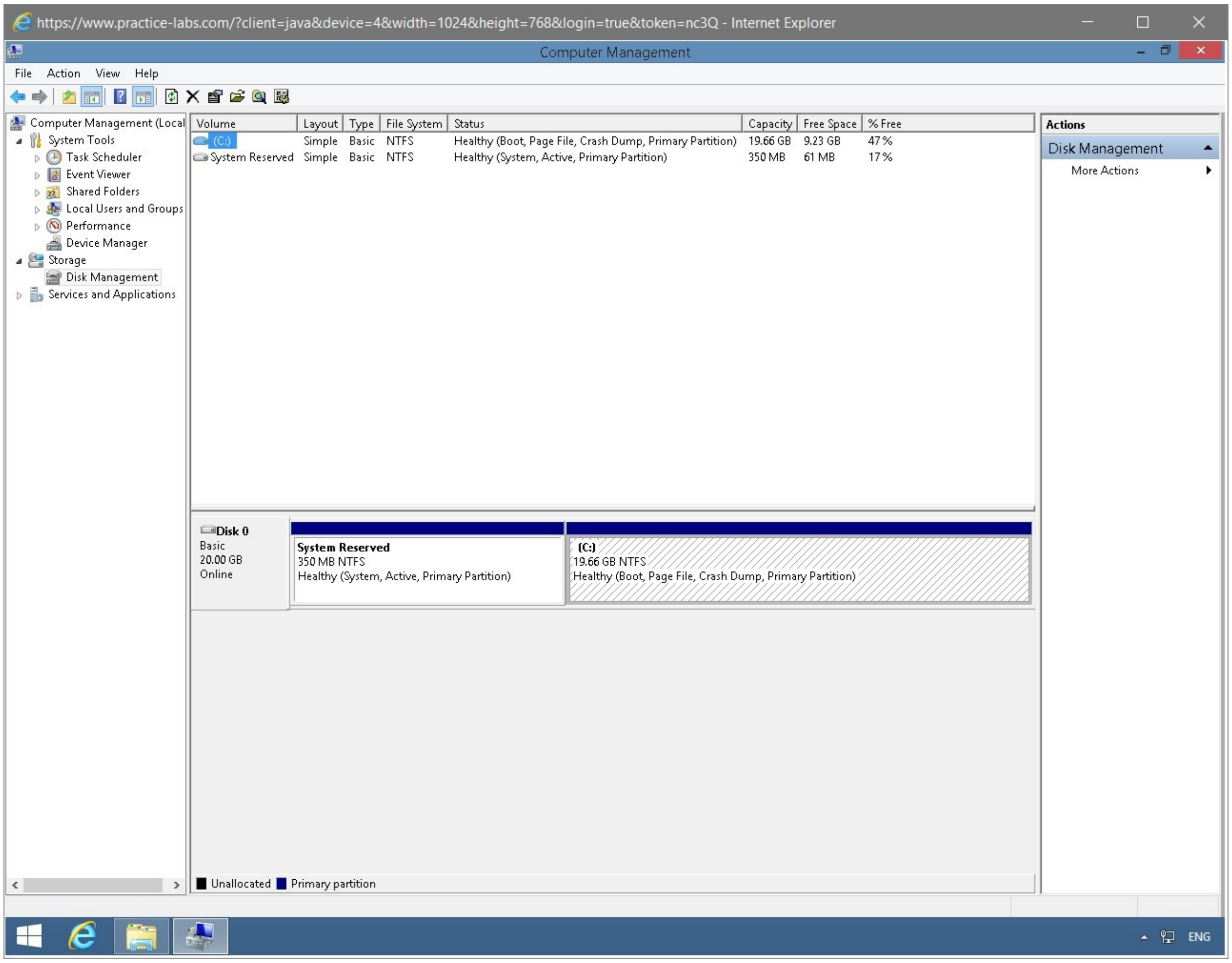
To be able to save the recovery key, you need to partition the existing drive and create a separate partition. This computer has only one drive and Bitlocker does not allow the recovery key to be saved to the encrypted drive. For this step you will be shrinking drive (D).

To partition a drive on Windows 8.1 device, perform the following steps:

Step 1

On **PLABWIN810,** open **Windows Explorer** and right-click **This PC** in the left pane and select **Computer Management**.

In the left pane, expand the **Storage** node and select **Disk Management**.



Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	19.66 GB	9.23 GB	47 %
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	350 MB	61 MB	17 %

Disk 0
Basic
20.00 GB
Online

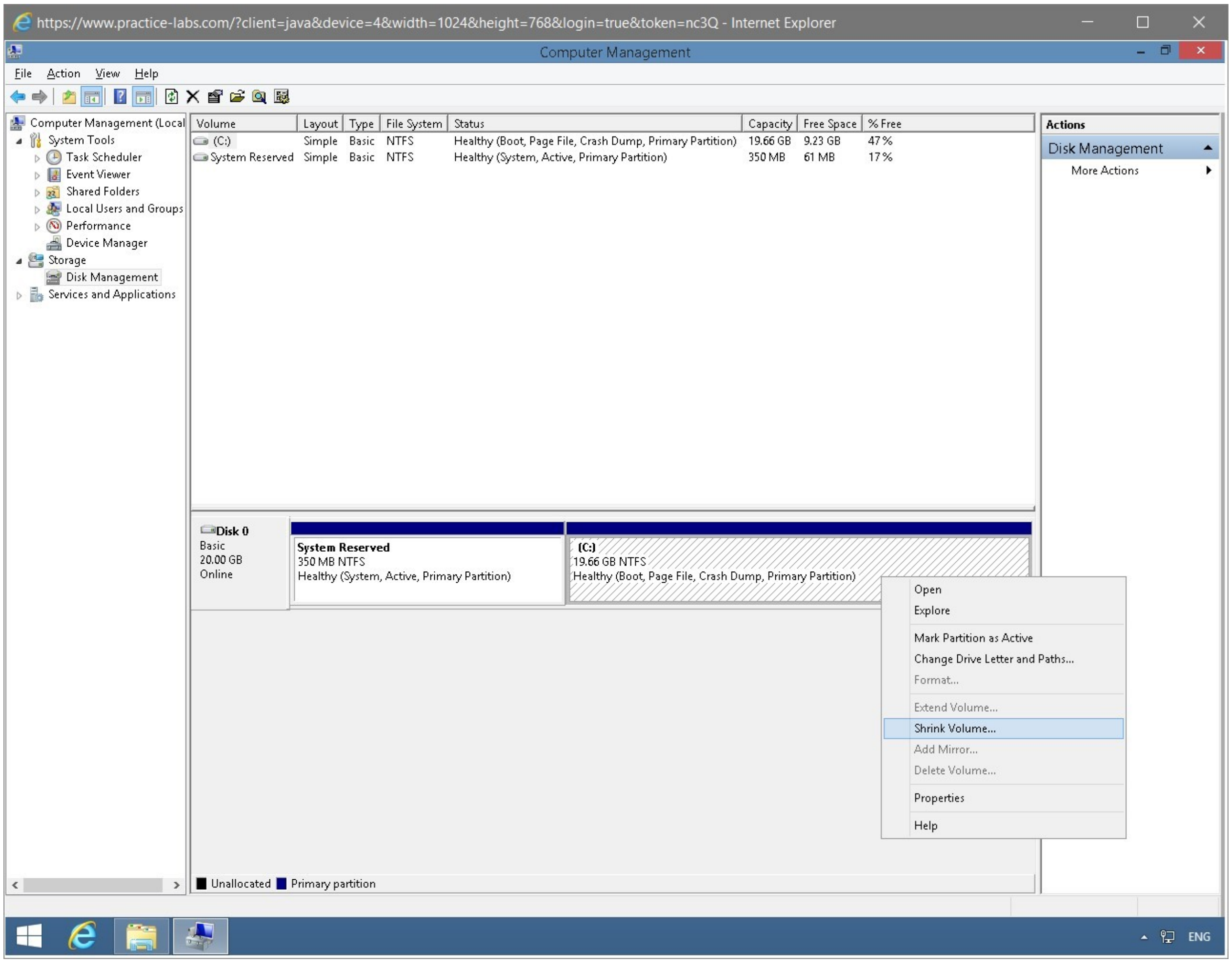
System Reserved
350 MB NTFS
Healthy (System, Active, Primary Partition)

(C:)
19.66 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Figure 1.19 Screenshot of the PLABWIN810 desktop: Computer Management console is displayed showing the Computer Management > Storage > Disk Management node path selected on the navigation pane at the left.

Step 2

In the middle pane, right-click **(C:)** and select **Shrink Volume**.



Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	19.66 GB	9.23 GB	47 %
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	350 MB	61 MB	17 %

Disk 0
Basic
20.00 GB
Online

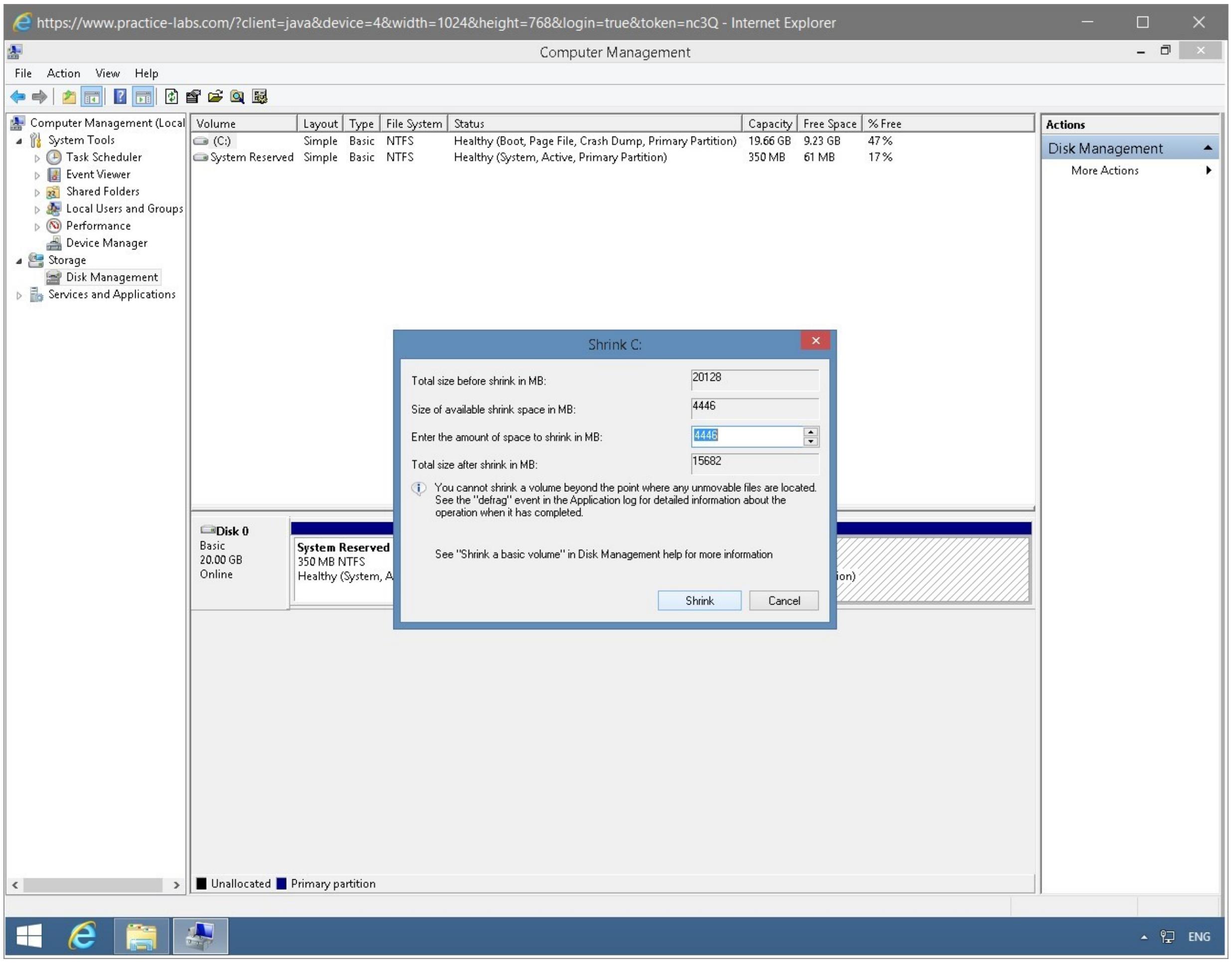
System Reserved
350 MB NTFS
Healthy (System, Active, Primary Partition)

(C:)
19.66 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Figure 1.20 Screenshot of the PLABWIN810 desktop: Context menu (that appears on right-clicking the unallocated area of a disk) > Shrink Volume menu-options are displayed on the Computer Management console.

Step 3

In the **Shrink PC** dialog box, keep the default settings and click **Shrink**.



Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	19.66 GB	9.23 GB	47 %
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	350 MB	61 MB	17 %

Shrink C:

Total size before shrink in MB: 20128

Size of available shrink space in MB: 4446

Enter the amount of space to shrink in MB: 4446

Total size after shrink in MB: 15682

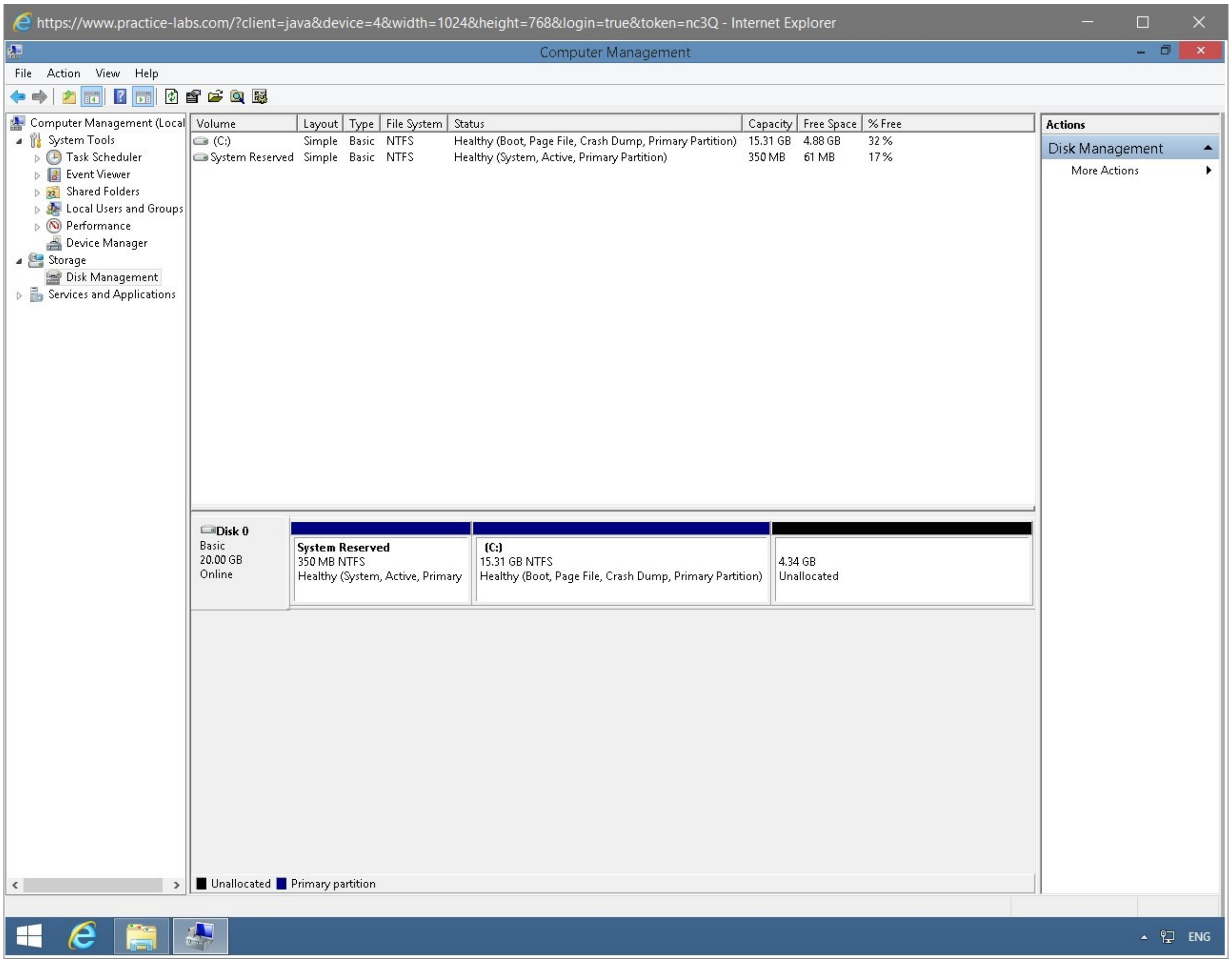
You cannot shrink a volume beyond the point where any unmovable files are located. See the "defrag" event in the Application log for detailed information about the operation when it has completed.

See "Shrink a basic volume" in Disk Management help for more information

Shrink Cancel

Figure 1.21 Screenshot of the PLABWIN810 desktop: Shrink C dialog box is displayed showing default settings and the Shrink button highlighted.

Notice that a new partition is now created.



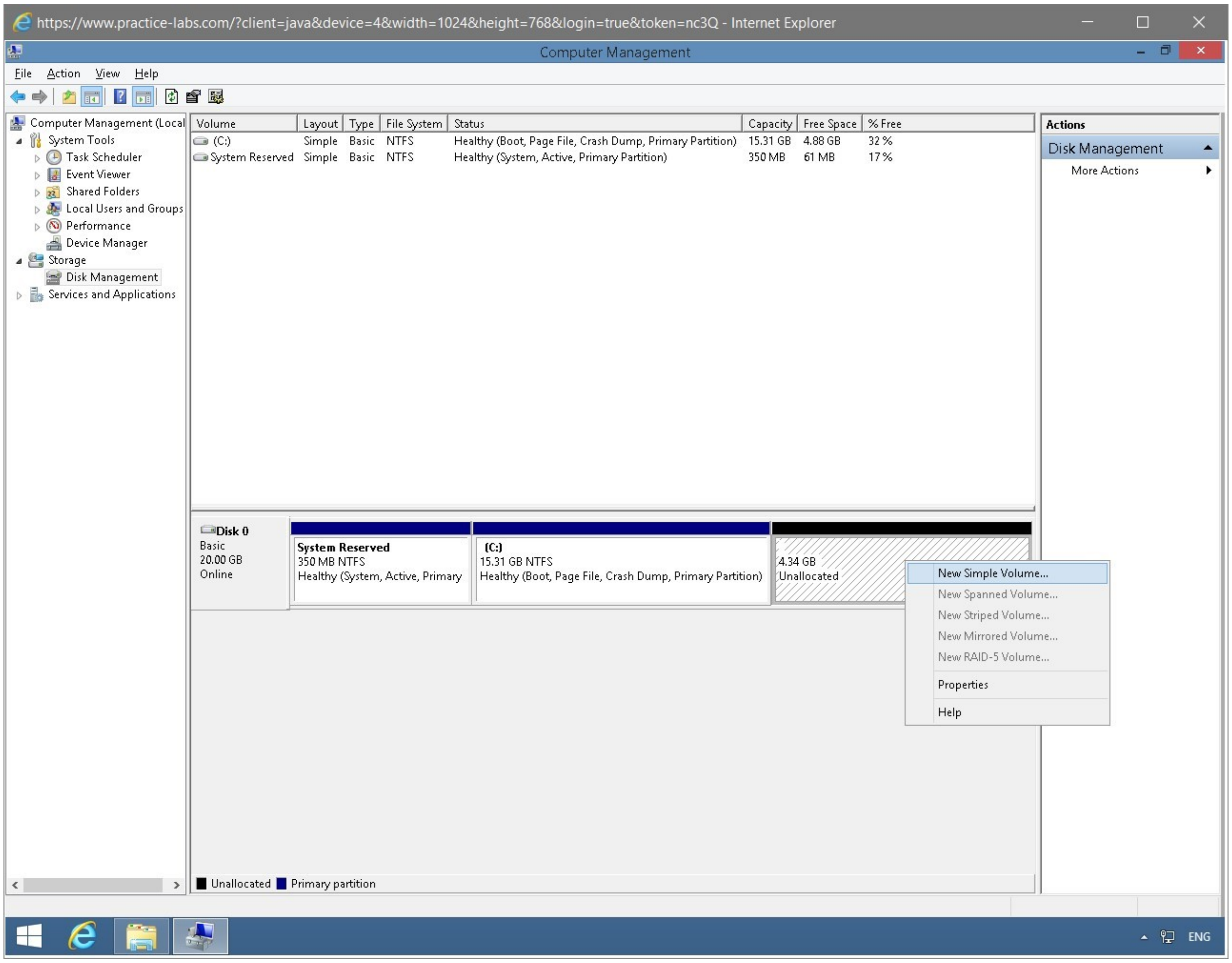
Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	15.31 GB	4.88 GB	32 %
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	350 MB	61 MB	17 %

Disk 0 Basic 20.00 GB Online	**System Reserved** 350 MB NTFS Healthy (System, Active, Primary	**(C:)** 15.31 GB NTFS Healthy (Boot, Page File, Crash Dump, Primary Partition)	4.34 GB Unallocated

Figure 1.22 Screenshot of the PLABWIN810 desktop: Computer Management console is displayed listing the newly created disk partition.

Step 4

You will now need to create a volume on this unallocated partition. Right-click and select **New Simple Volume**.

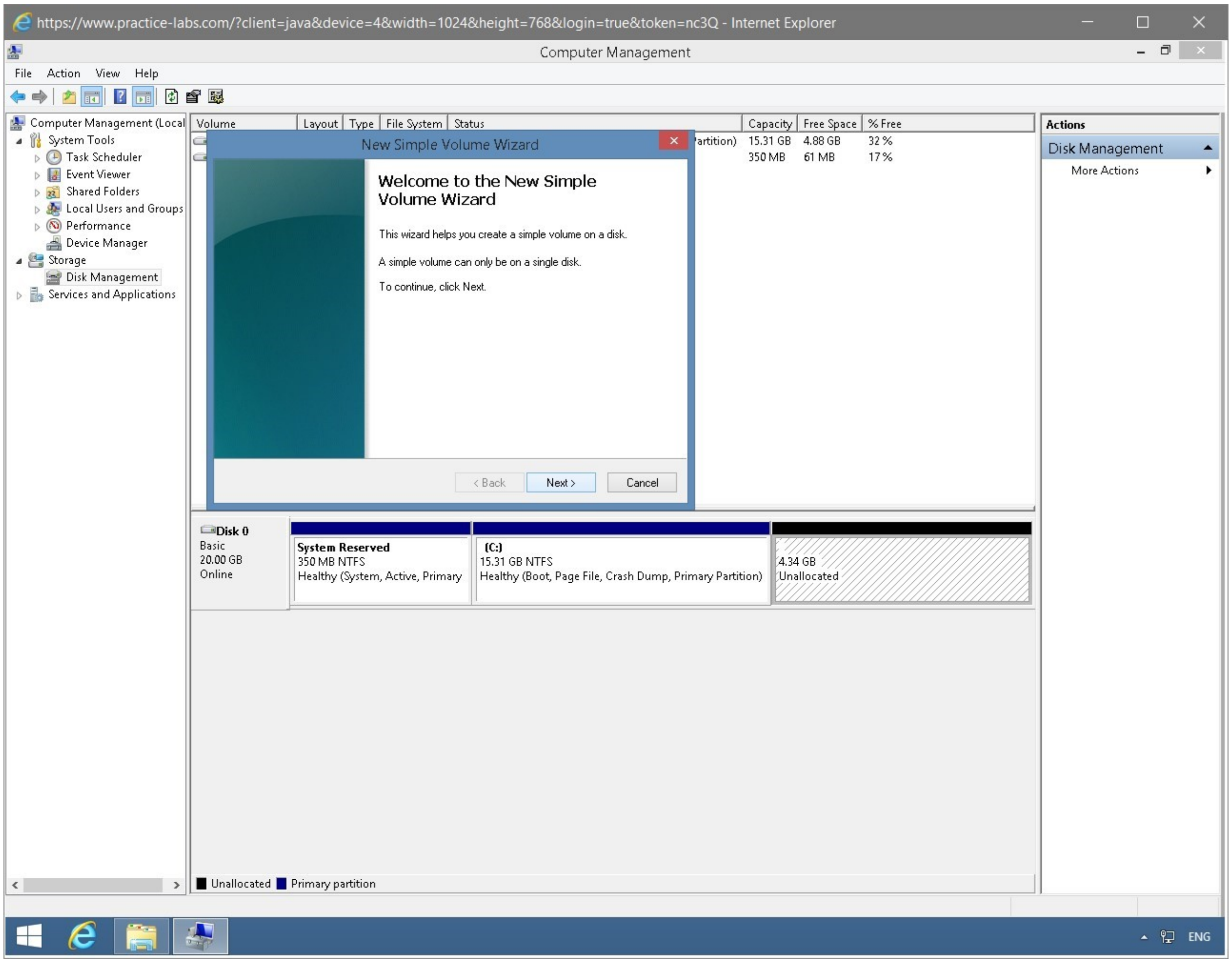


Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	15.31 GB	4.88 GB	32 %
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	350 MB	61 MB	17 %

Figure 1.23 Screenshot of the PLABWIN810 desktop: Context menu (that appears on right-clicking the unallocated area of a disk) > New Simple Volume menu-options are displayed on the Computer Management console.

Step 5

On the **Welcome to the New Simple Volume Wizard** page, read the information and click **Next**.



New Simple Volume Wizard

Welcome to the New Simple Volume Wizard

This wizard helps you create a simple volume on a disk.

A simple volume can only be on a single disk.

To continue, click Next.

< Back | Next > | Cancel

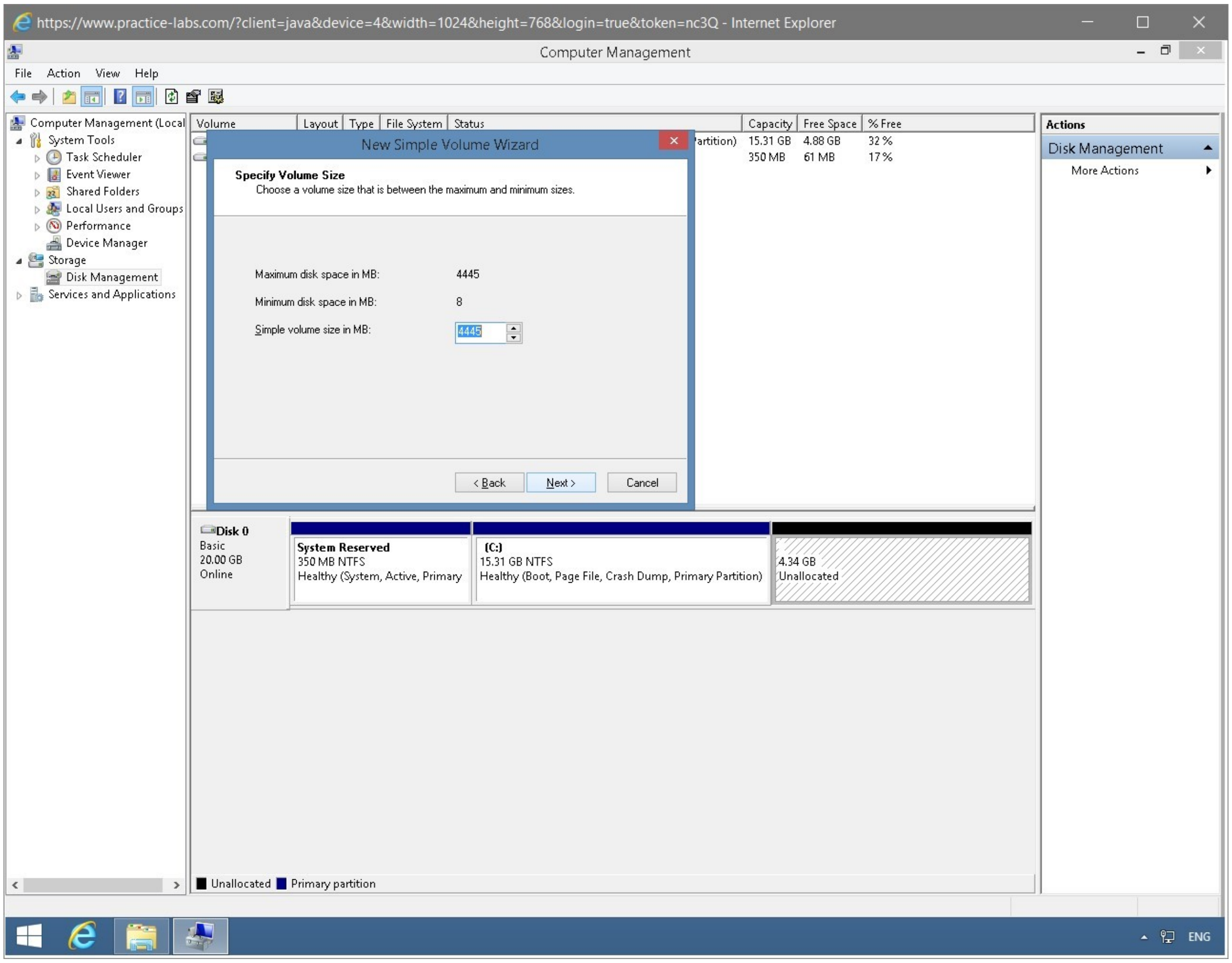
Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free
				Partition)	15.31 GB	4.88 GB	32 %
					350 MB	61 MB	17 %

Disk 0 Basic 20.00 GB Online	System Reserved 350 MB NTFS Healthy (System, Active, Primary	(C:) 15.31 GB NTFS Healthy (Boot, Page File, Crash Dump, Primary Partition)	4.34 GB Unallocated

Figure 1.24 Screenshot of the PLABWIN810 desktop: Welcome page on the New Simple Volume Wizard is displayed showing the Next button highlighted.

Step 6

On the **Specify Volume Size** page, keep the default settings and click **Next**.



Volume	Capacity	Free Space	% Free
artition)	15.31 GB	4.88 GB	32 %
	350 MB	61 MB	17 %

Specify Volume Size

Choose a volume size that is between the maximum and minimum sizes.

Maximum disk space in MB: 4445

Minimum disk space in MB: 8

Simple volume size in MB: 4445

Disk 0
Basic
20.00 GB
Online

System Reserved
350 MB NTFS
Healthy (System, Active, Primary

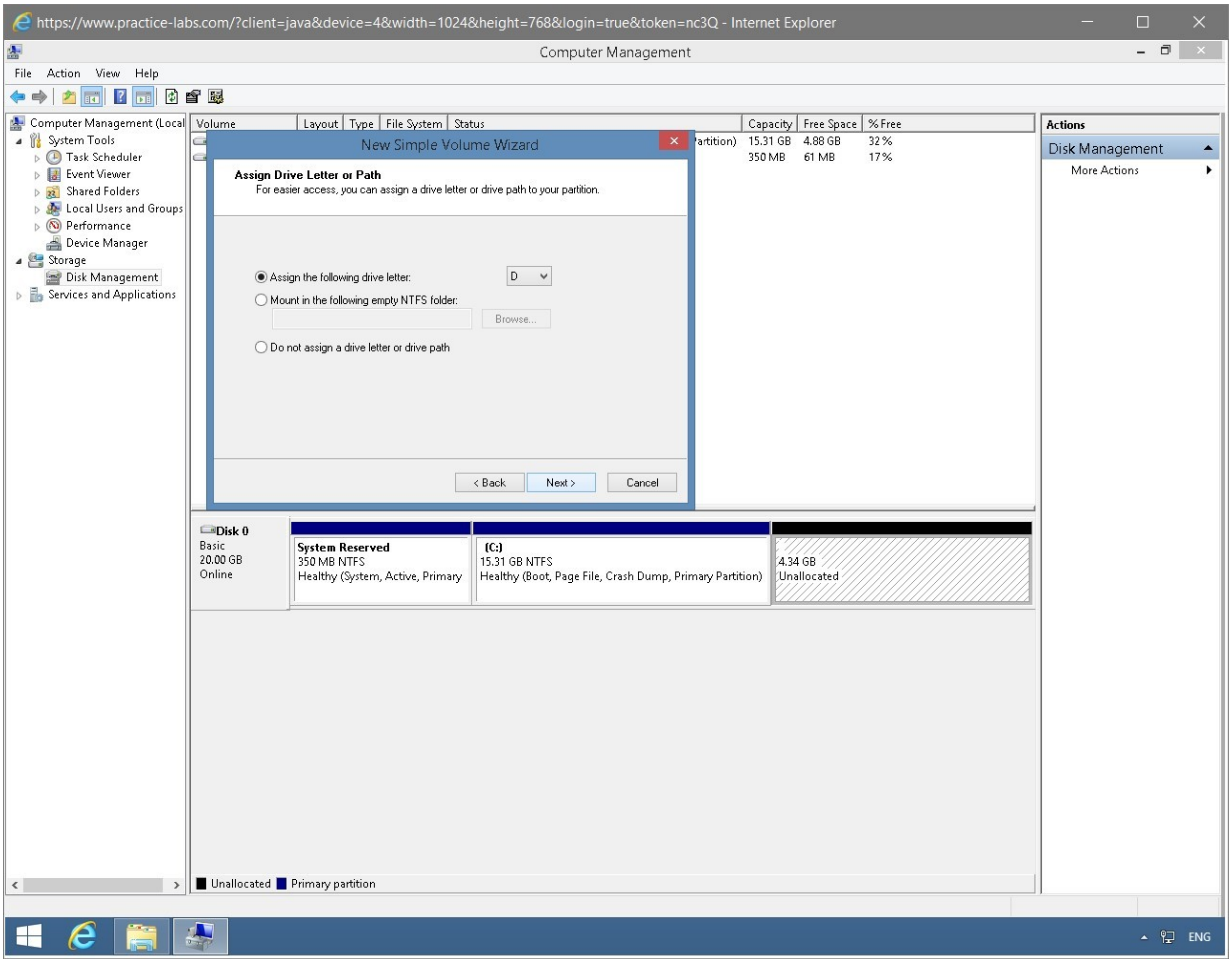
(C:)
15.31 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

4.34 GB
Unallocated

Figure 1.25 Screenshot of the PLABWIN810 desktop: Specify Volume Size page on the New Simple Volume Wizard is displayed showing default settings and the Next button highlighted.

Step 7

On the **Assign Drive Letter or Path** page, keep the default drive letter, **D**, and click **Next**.



Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free
				artition)	15.31 GB	4.88 GB	32 %
					350 MB	61 MB	17 %

Assign Drive Letter or Path

For easier access, you can assign a drive letter or drive path to your partition.

● Assign the following drive letter: D

○ Mount in the following empty NTFS folder:

○ Do not assign a drive letter or drive path

Disk 0
Basic
20.00 GB
Online

System Reserved
350 MB NTFS
Healthy (System, Active, Primary

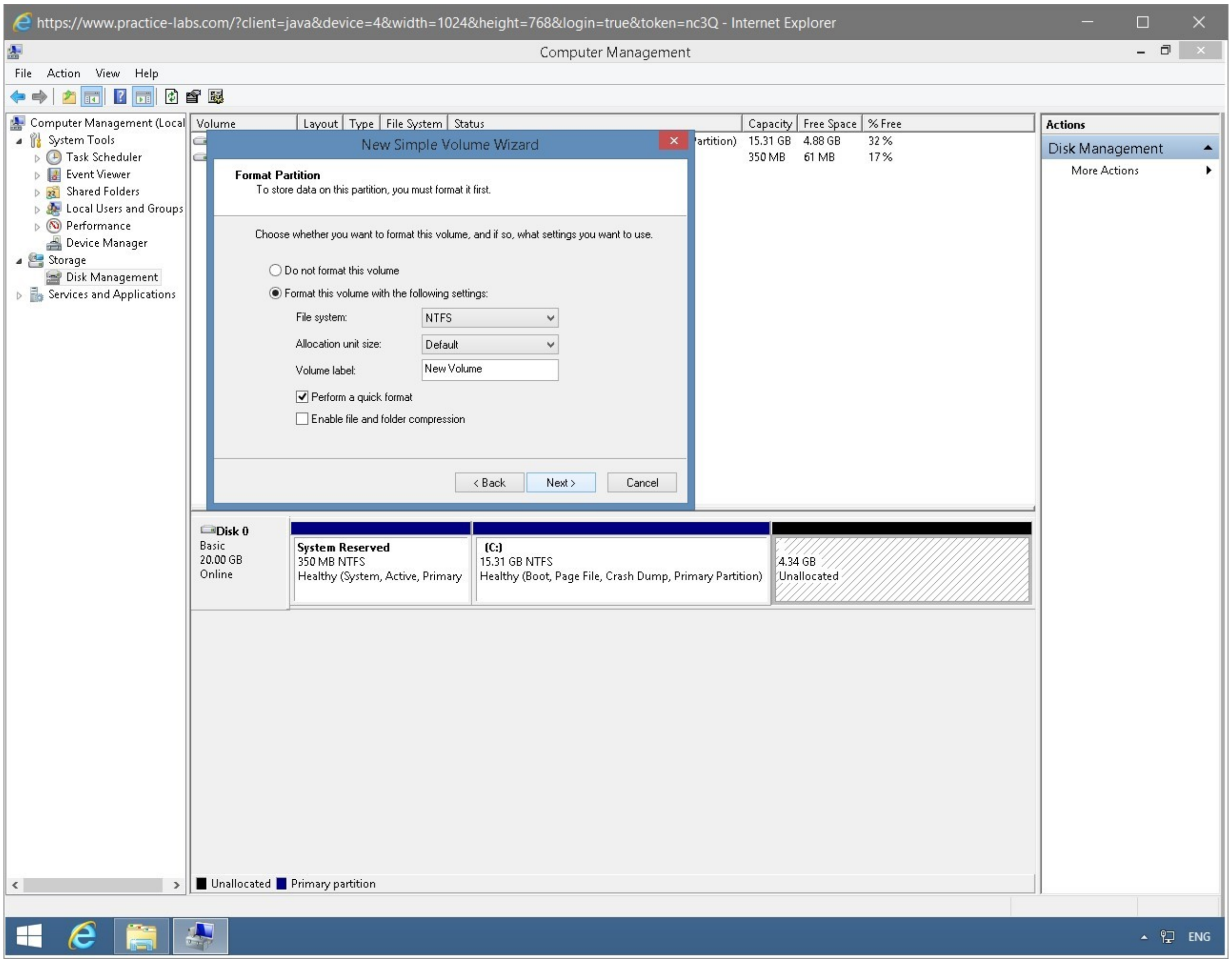
(C:)
15.31 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

4.34 GB
Unallocated

Figure 1.26 Screenshot of the PLABWIN810 desktop: Assign Drive Letter or Path page on the New Simple Volume Wizard is displayed showing the required settings performed and the Next button highlighted.

Step 8

On the **Format Partition** page, keep the default settings and click **Next**.



Format Partition
To store data on this partition, you must format it first.

Choose whether you want to format this volume, and if so, what settings you want to use.

○ Do not format this volume
● Format this volume with the following settings:

File system: NTFS
Allocation unit size: Default
Volume label: New Volume

☑ Perform a quick format
□ Enable file and folder compression

Capacity	Free Space	% Free
15.31 GB	4.88 GB	32 %
350 MB	61 MB	17 %

Disk 0
Basic
20.00 GB
Online

System Reserved
350 MB NTFS
Healthy (System, Active, Primary

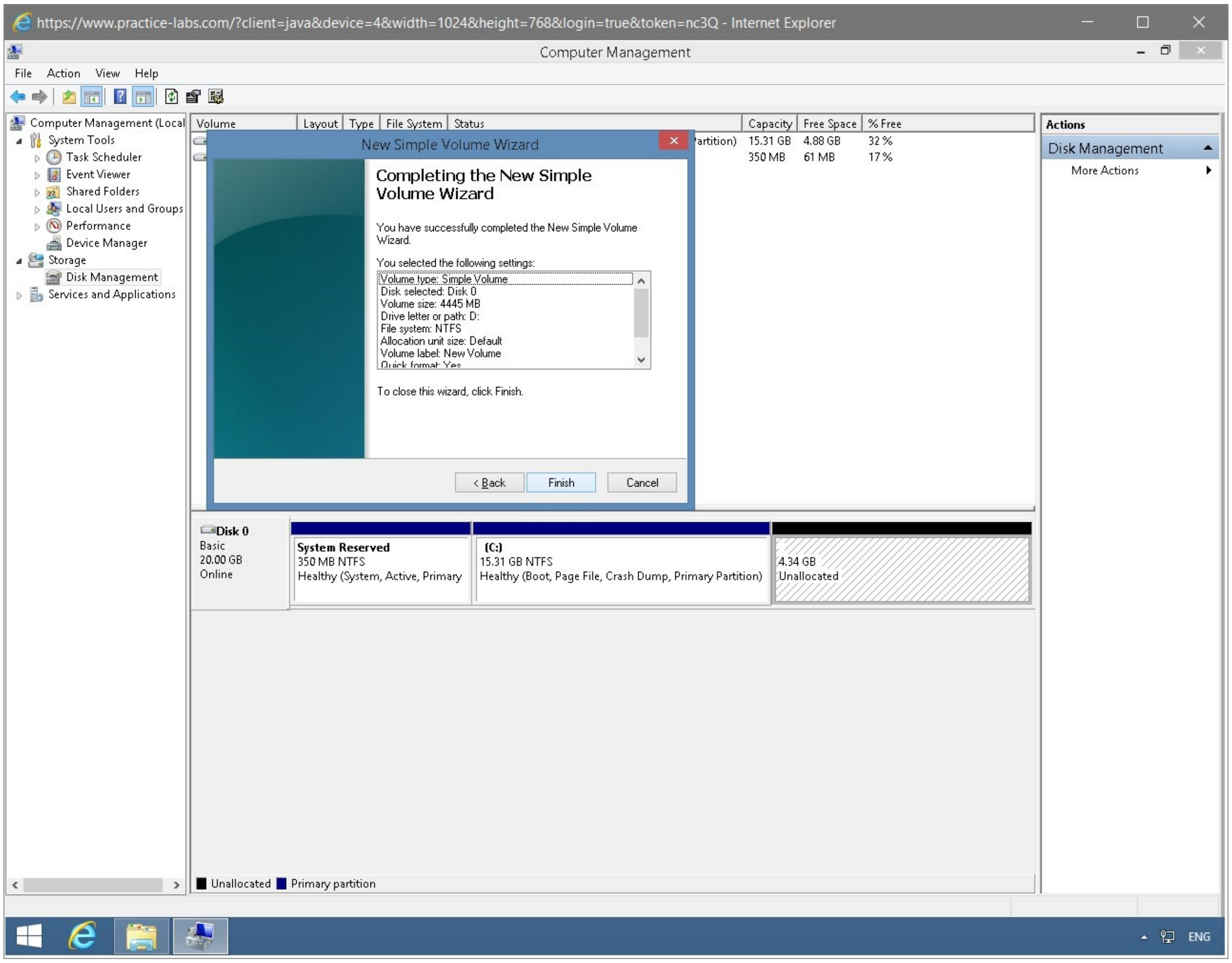
(C:)
15.31 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

4.34 GB
Unallocated

Figure 1.27 Screenshot of the PLABWIN810 desktop: Format Partition page on the New Simple Volume Wizard is displayed showing default settings and the Next button highlighted.

Step 9

On the **Completing the New Simple Volume Wizard** page, review the settings and click **Finish**.



New Simple Volume Wizard

Completing the New Simple Volume Wizard

You have successfully completed the New Simple Volume Wizard.

You selected the following settings:

```
Volume type: Simple Volume
Disk selected: Disk 0
Volume size: 4445 MB
Drive letter or path: D:
File system: NTFS
Allocation unit size: Default
Volume label: New Volume
Quick format: Yes
```

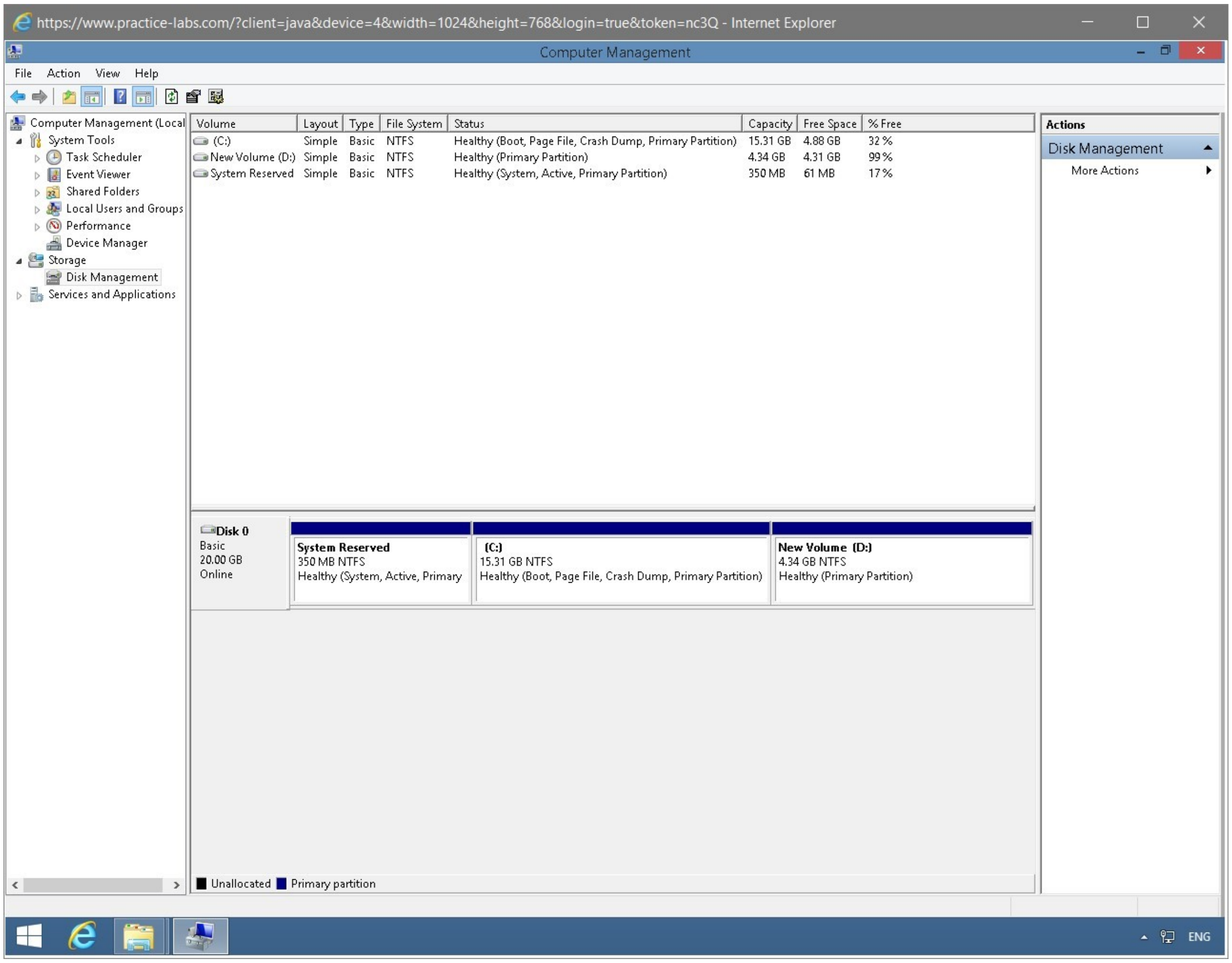
To close this wizard, click Finish.

Figure 1.28 Screenshot of the PLABWIN810 desktop: Completion page on the New Simple Volume Wizard is displayed listing specifications to create the volume and the Finish button highlighted.

Step 10

Notice that the **D** partition is now ready for use. Close the **Computer Management** window.

Note: You may see the a dialog box asking you to format the new partition. Click Cancel.



Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	15.31 GB	4.88 GB	32 %
New Volume (D:)	Simple	Basic	NTFS	Healthy (Primary Partition)	4.34 GB	4.31 GB	99 %
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	350 MB	61 MB	17 %

Disk 0 Basic 20.00 GB Online	System Reserved 350 MB NTFS Healthy (System, Active, Primary	(C:) 15.31 GB NTFS Healthy (Boot, Page File, Crash Dump, Primary Partition)	New Volume (D:) 4.34 GB NTFS Healthy (Primary Partition)

Figure 1.29 Screenshot of the PLABWIN810 desktop: Computer Management console is displayed listing the newly created simple volume.

Keep all devices powered on in their current state and proceed to the next task.

Task 3 - Enable BitLocker

To encrypt the selected disk volume using BitLocker, you must have administrative privileges on the computer.

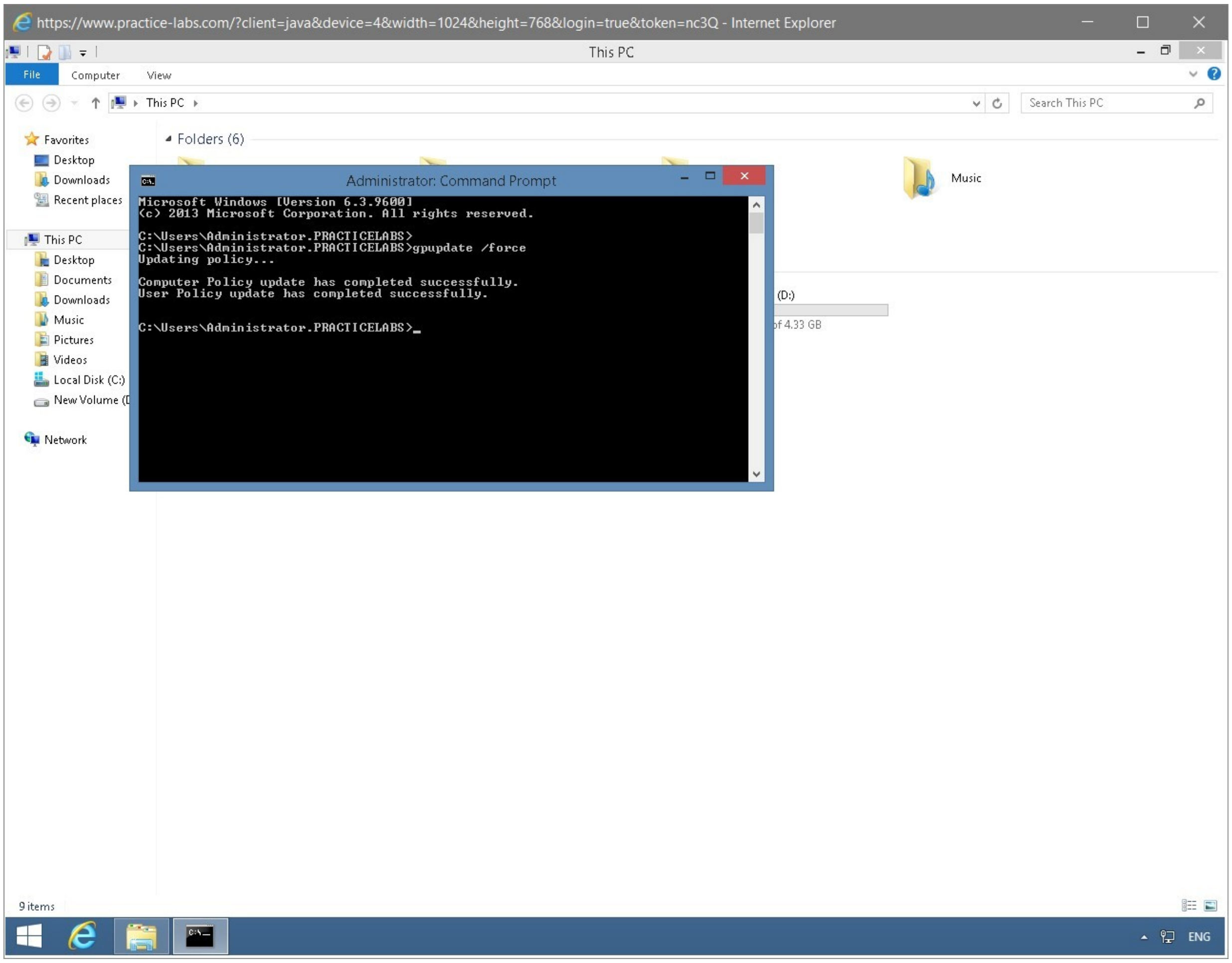
To enable BitLocker on Windows 8.1 device, perform the following steps:

Step 1

On **PLABWIN810,** you need to ensure the **Bitlocker for desktops** policy is applied. You can quickly apply the **Group Policy** using the following command:

```
gpupdate /force
```

Minimize the command prompt window.



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.PRACTICELABS>
C:\Users\Administrator.PRACTICELABS>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.


C:\Users\Administrator.PRACTICELABS>_
```

Figure 1.30 Screenshot of the PLABWIN810 desktop: Command prompt window is displayed showing the command to apply the updated policy completed successfully.

Step 2

Open **Windows Explorer** and select **This PC** in the left pane if already not selected.

Right-click **Local Disk (D:)** and select **Turn on Bitlocker.**

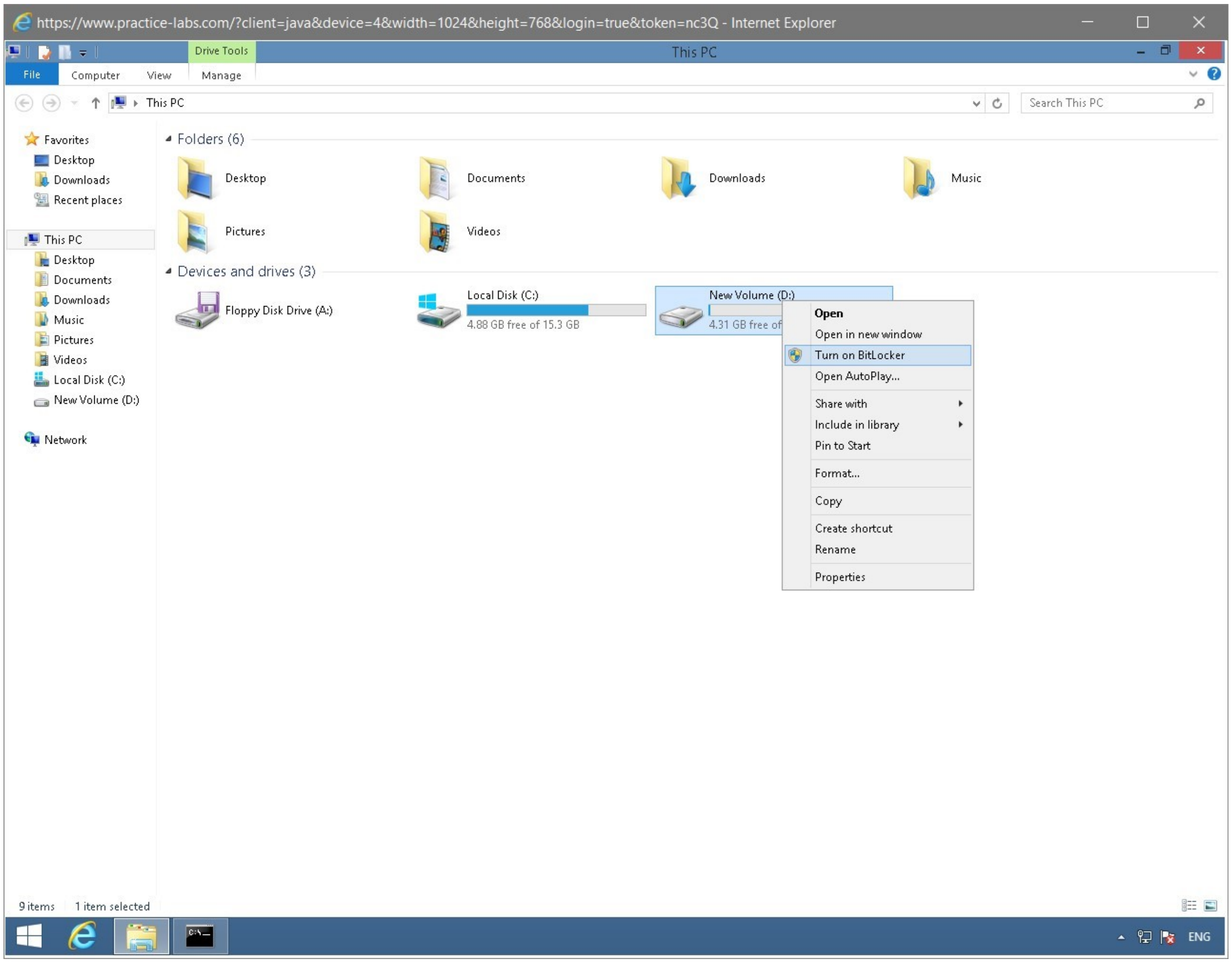


Figure 1.31 Screenshot of the PLABWIN810 desktop: Context menu (that appears on right-clicking a listed volume) > Turn on BitLocker menu-options are highlighted on the file explorer window.

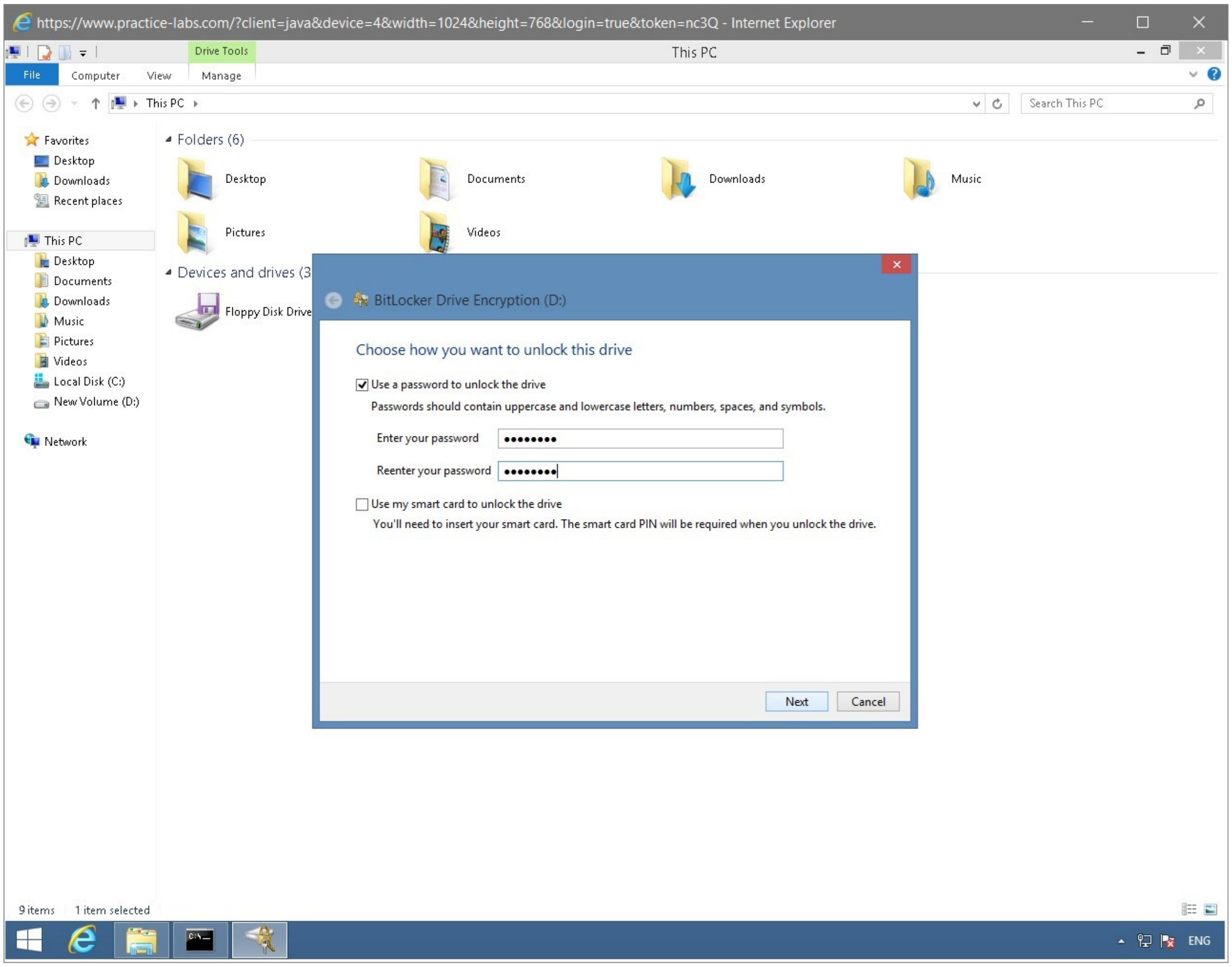
Step 3

On the **Choose how you want to unlock this drive** page, you have two options to select on how you want to unlock **D** drive.

Select **Use a password to unlock this drive** and then in the **Enter your password** and **Reenter your password** textboxes, type:

```
Password
```

Click **Next**.



https://www.practice-labs.com/?client=java&device=4&width=1024&height=768&login=true&token=nc3Q - Internet Explorer

BitLocker Drive Encryption (D:)

Choose how you want to unlock this drive

☑ Use a password to unlock the drive

Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols.

Enter your password ••••••••

Reenter your password ••••••••

☐ Use my smart card to unlock the drive

You'll need to insert your smart card. The smart card PIN will be required when you unlock the drive.

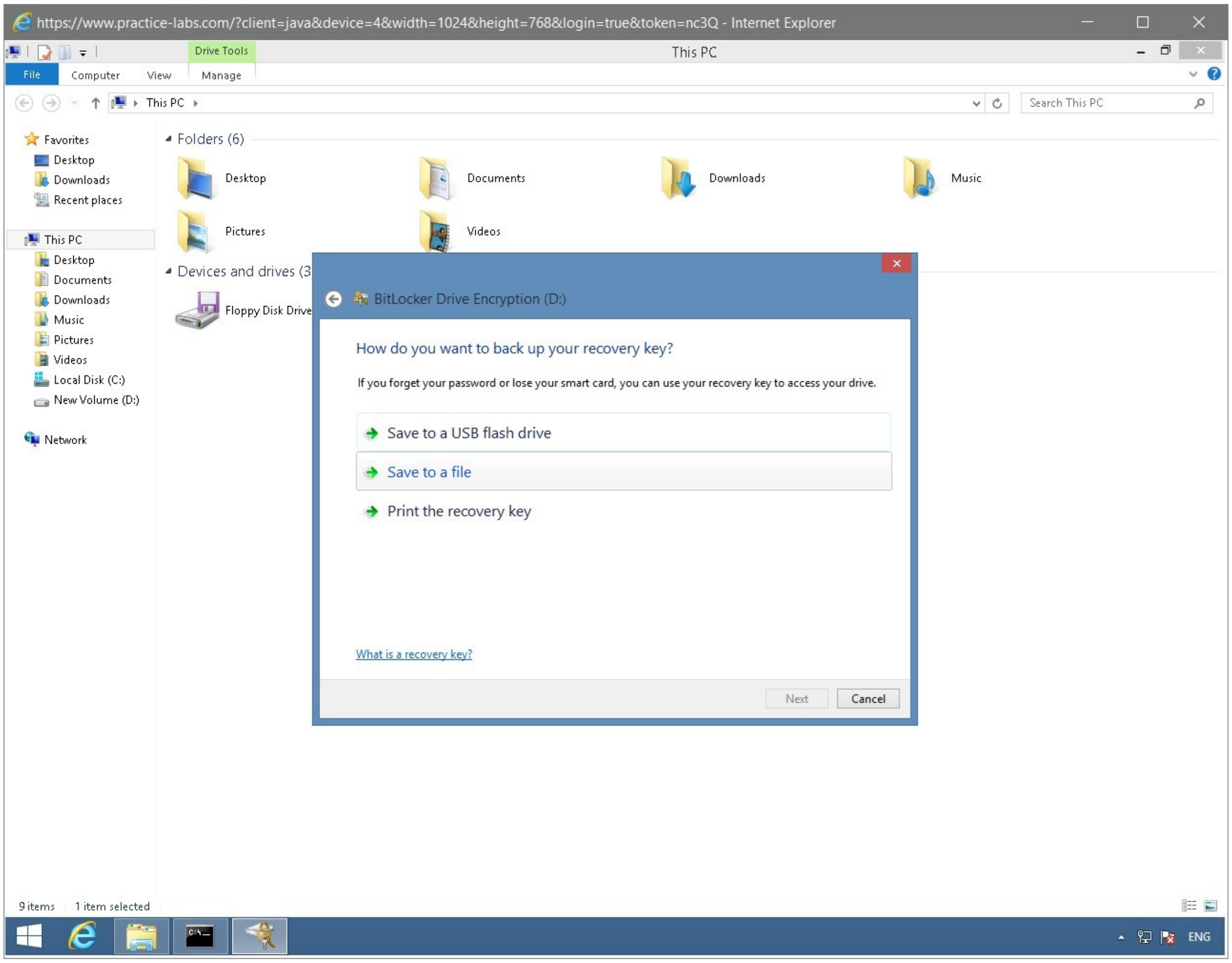
Figure 1.32 Screenshot of the PLABWIN810 desktop: Choose how you want to unlock this

drive page on the BitLocker Drive Encryption (D:) wizard is displayed showing the required values typed-in and the Next button highlighted.

Step 4

On the **How do you want to back up your recovery key?** page, select **Save to a file**.

The Recovery Key is required if the administrator forgets the password or loses the smart card to access the encrypted drive.



BitLocker Drive Encryption (D:)

How do you want to back up your recovery key?

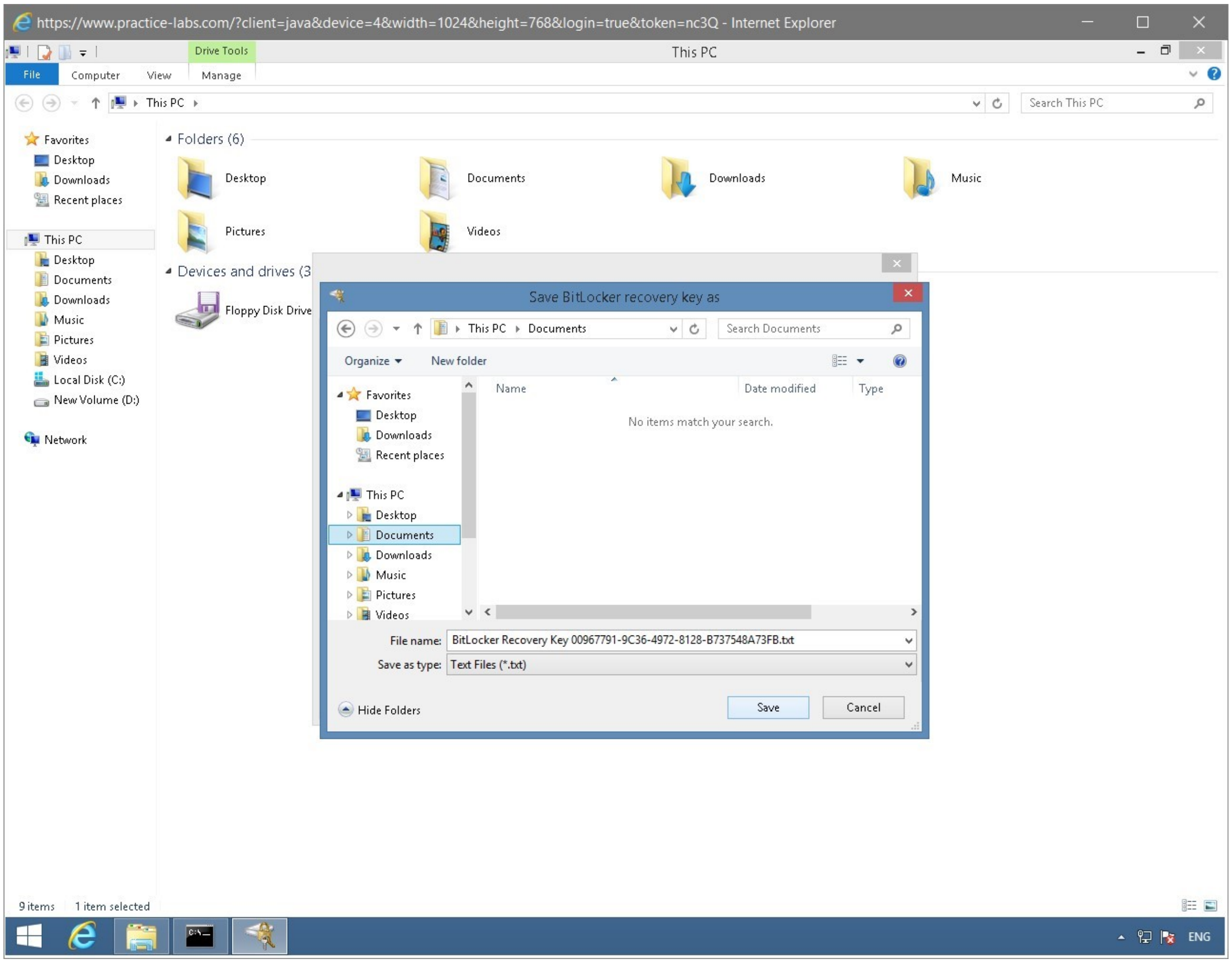
If you forget your password or lose your smart card, you can use your recovery key to access your drive.

Figure 1.33 Screenshot of the PLABWIN810 desktop: How do you want to back up your recovery key page on the BitLocker Drive Encryption (D:) wizard is displayed showing the required option selected.

Step 5

On the **Save Bitlocker recovery key as** dialog box, notice that Windows has assigned the file name as **BitLocker Recovery Key <xxxxxx>**.

Select **Documents** from the left pane if already not selected and then click **Save**.**Note**: In your lab, you will get different recovery key compared to the screen shot. Do NOT change the recovery key given to you as you will need this, if you forget the password used for unlocking this drive.



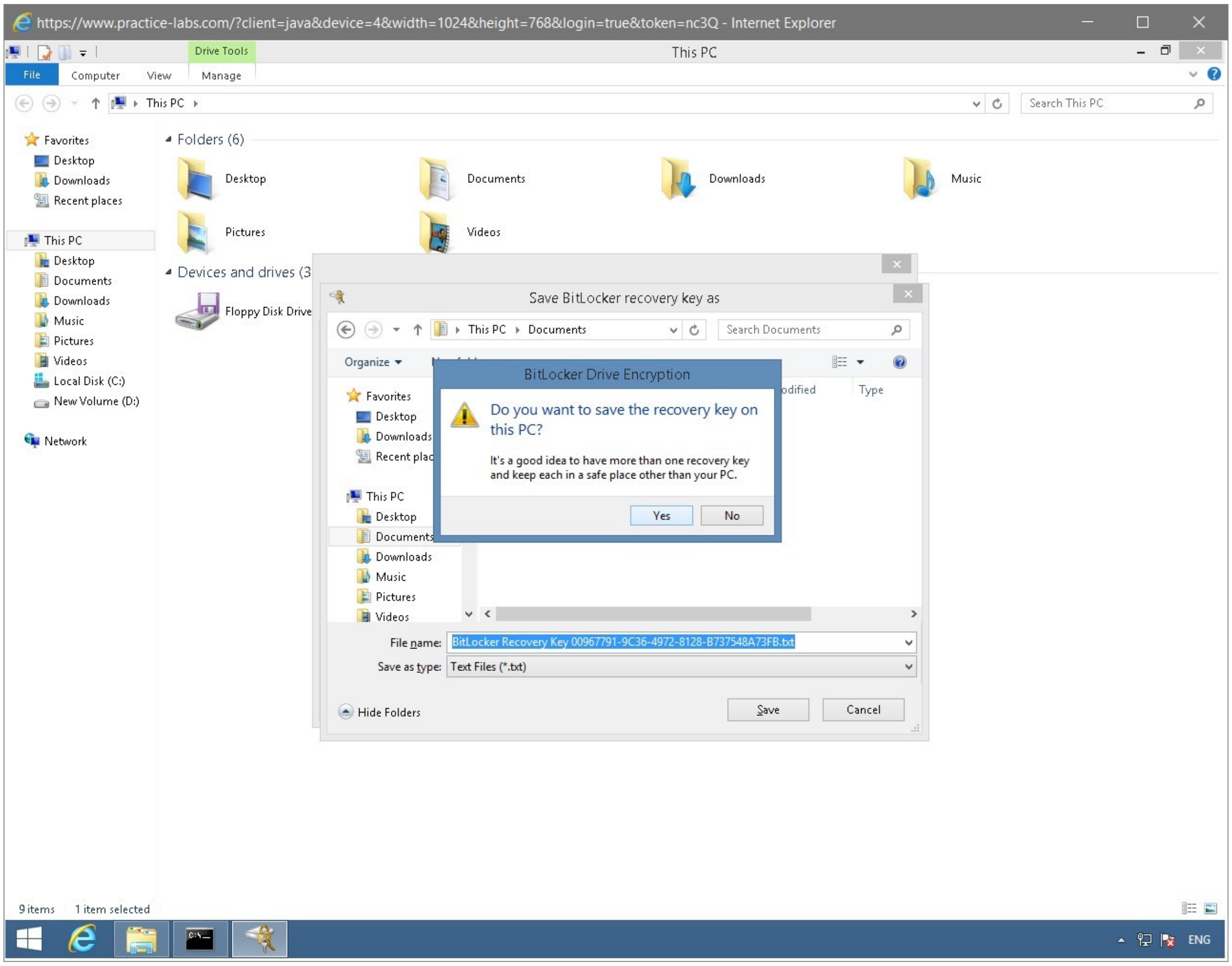
File name: BitLocker Recovery Key 00967791-9C36-4972-8128-B737548A73FB.txt

Save as type: Text Files (*.txt)

Figure 1.34 Screenshot of the PLABWIN810 desktop: Save Bitlocker recovery key as dialog box on the BitLocker Drive Encryption (E:) wizard is displayed showing default settings and the Save button highlighted.

Step 6

On the **BitLocker Drive Encryption** dialog box, click **Yes**.



https://www.practice-labs.com/?client=java&device=4&width=1024&height=768&login=true&token=nc3Q - Internet Explorer
This PC
Save BitLocker recovery key as
Search Documents
Organize
Hide Folders
Save
Cancel

BitLocker Drive Encryption

Do you want to save the recovery key on this PC?

It's a good idea to have more than one recovery key and keep each in a safe place other than your PC.

Yes No

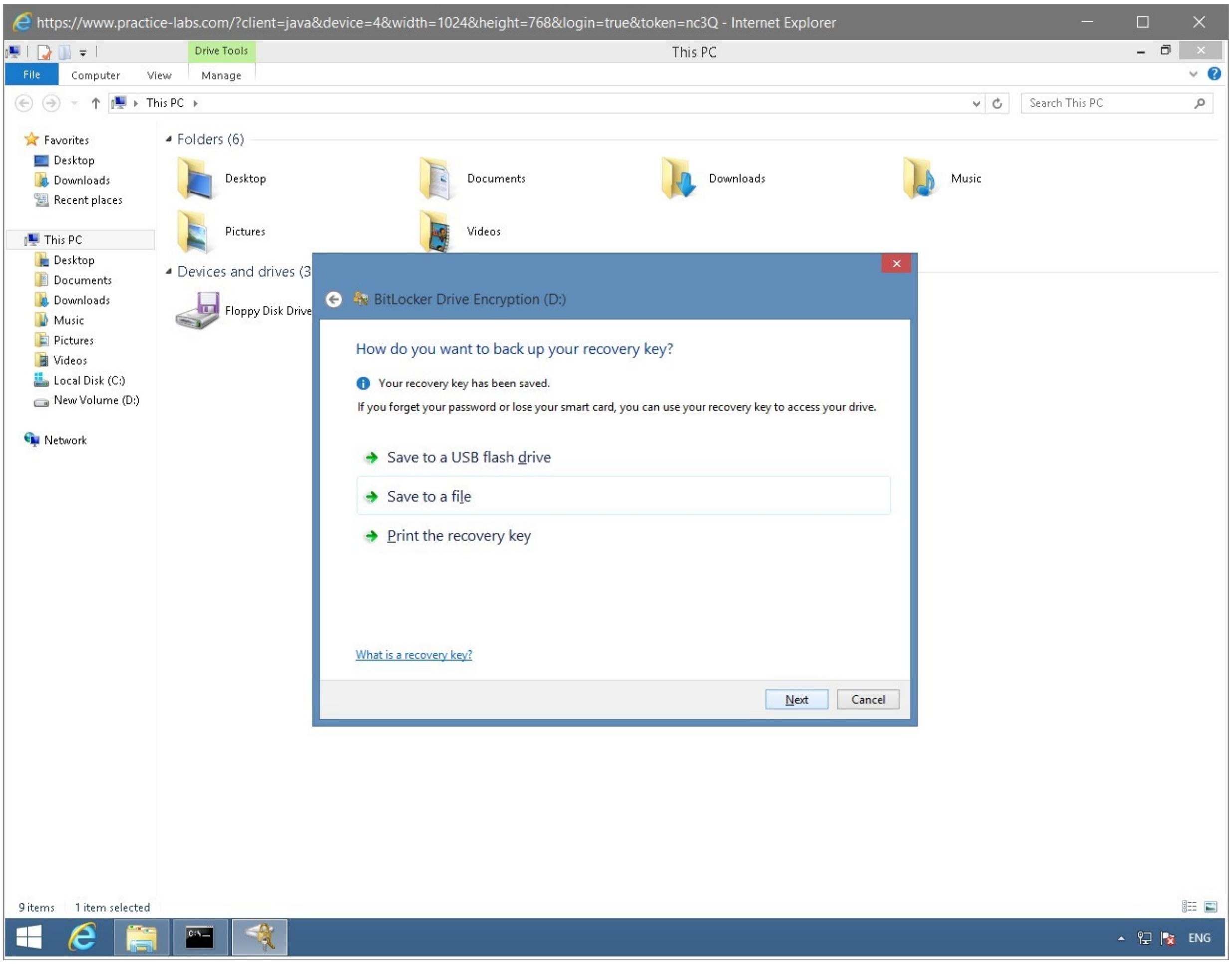
File name: BitLocker Recovery Key 00967791-9C36-4972-8128-B737548A73FB.txt

Save as type: Text Files (*.txt)

Figure 1.35 Screenshot of the PLABWIN810 desktop: BitLocker Drive Encryption caution box cautioning about saving the key in a safe place is displayed on the BitLocker Drive Encryption (E:) wizard with the Yes button highlighted.

Step 7

Back on the wizard, click **Next**.



BitLocker Drive Encryption (D:)

How do you want to back up your recovery key?

Your recovery key has been saved.

If you forget your password or lose your smart card, you can use your recovery key to access your drive.

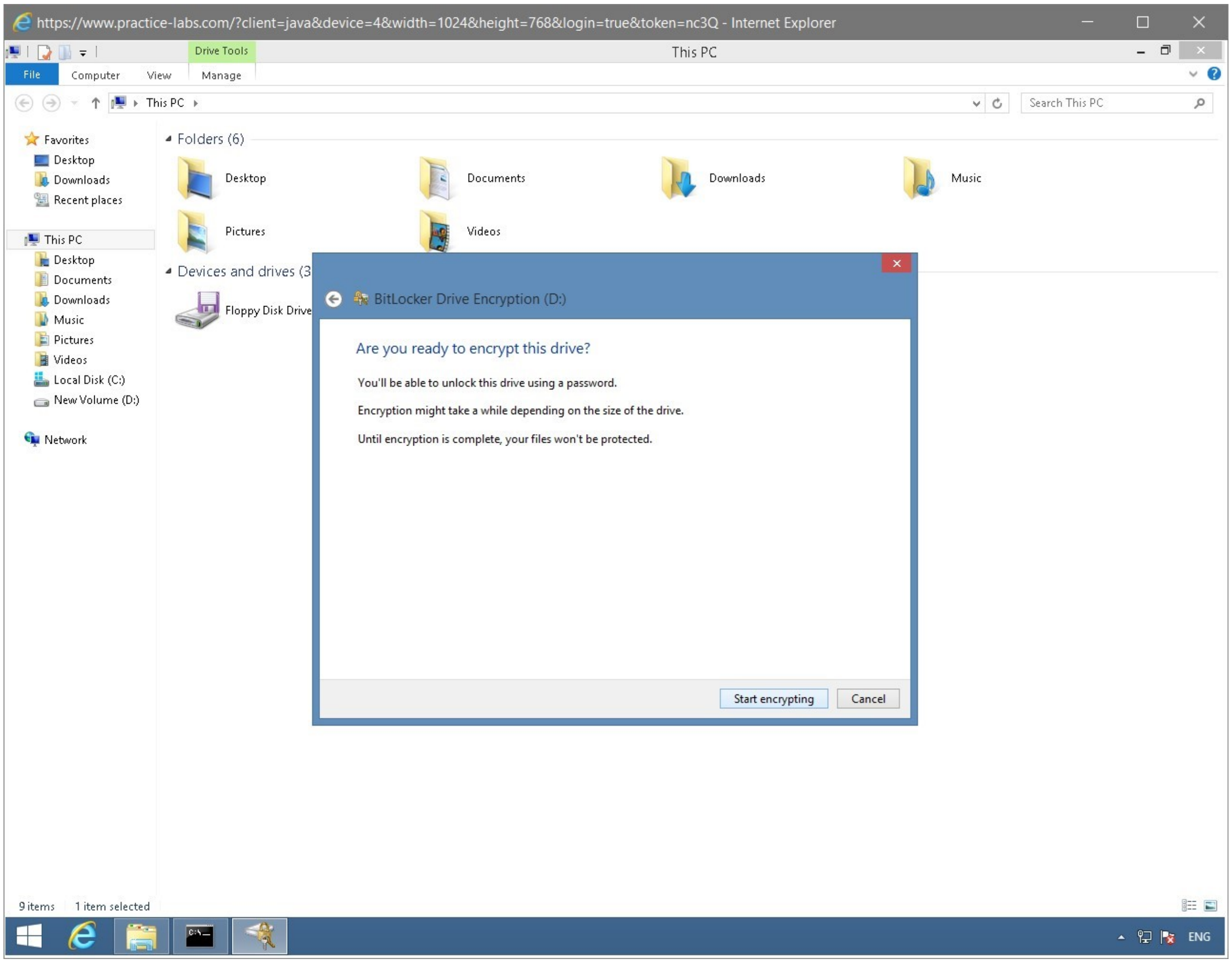
- Save to a USB flash drive
- Save to a file
- Print the recovery key

What is a recovery key?

Figure 1.36 Screenshot of the PLABWIN810 desktop: How do you want to back up your recovery key page on the BitLocker Drive Encryption (D:) wizard is displayed showing the Next button highlighted.

Step 8

On the **Are you ready to encrypt this drive?** page, click **Start encrypting**.



Are you ready to encrypt this drive?

You'll be able to unlock this drive using a password.

Encryption might take a while depending on the size of the drive.

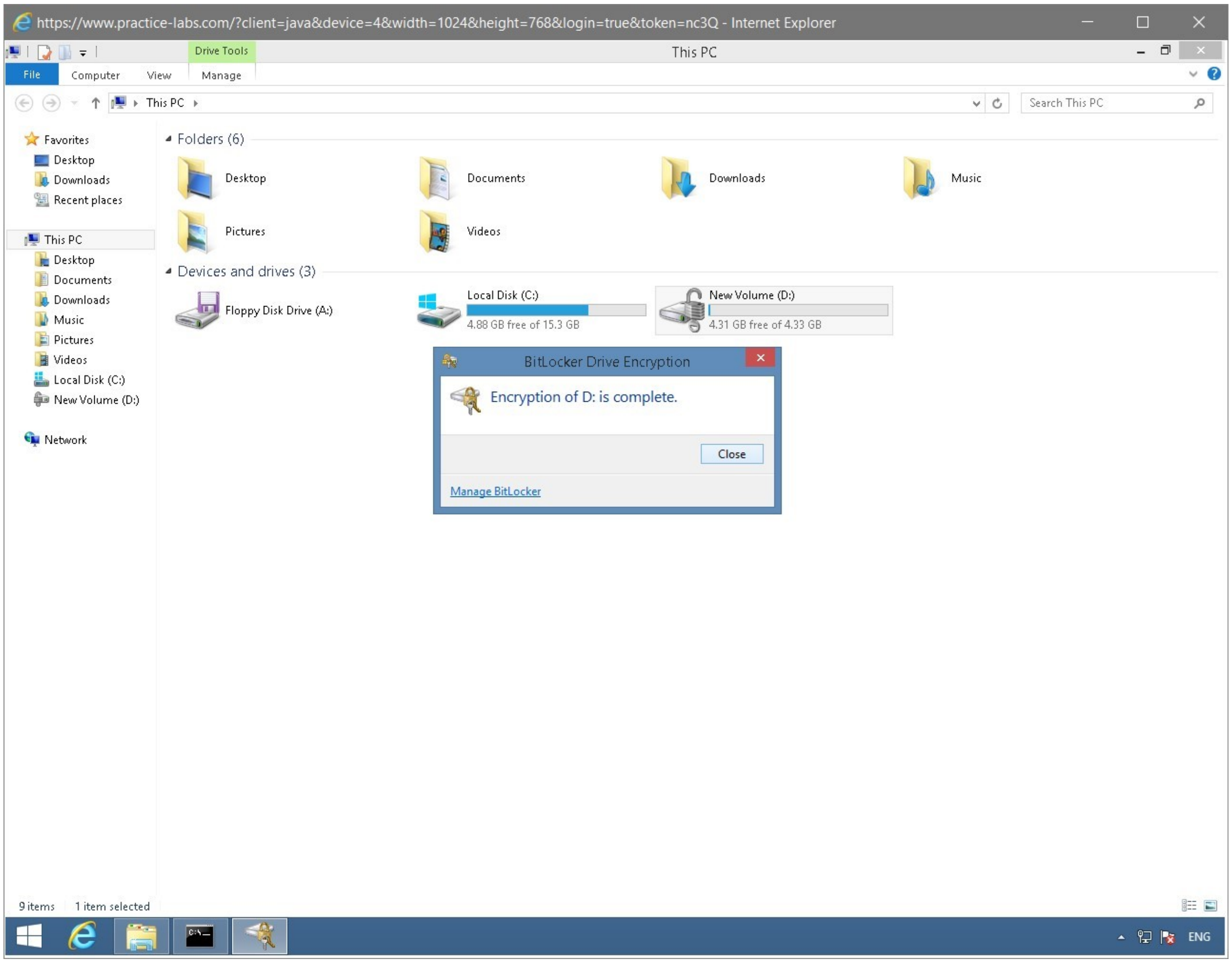
Until encryption is complete, your files won't be protected.

Figure 1.37 Screenshot of the PLABWIN810 desktop: Are you ready to encrypt this drive page on the BitLocker Drive Encryption (D:) wizard is displayed showing the Start encrypting button highlighted.

Step 9

On the **BitLocker Drive Enryption** dialog box, click **Close** when encryption of **D** is complete.

Note: Please be aware this confirmation may not appear. This is expected and you can continue to the next step.



https://www.practice-labs.com/?client=java&device=4&width=1024&height=768&login=true&token=nc3Q - Internet Explorer

BitLocker Drive Encryption

Encryption of D: is complete.

Figure 1.38 Screenshot of the PLABWIN810 desktop: BitLocker Drive Encryption dialog box is displayed indicating that encryption is complete and the Close button highlighted.

Step 10

Notice the BitLocker icon now appended on **Drive Volume D**.

The drive is still in its unlocked state as indicated by the icon.

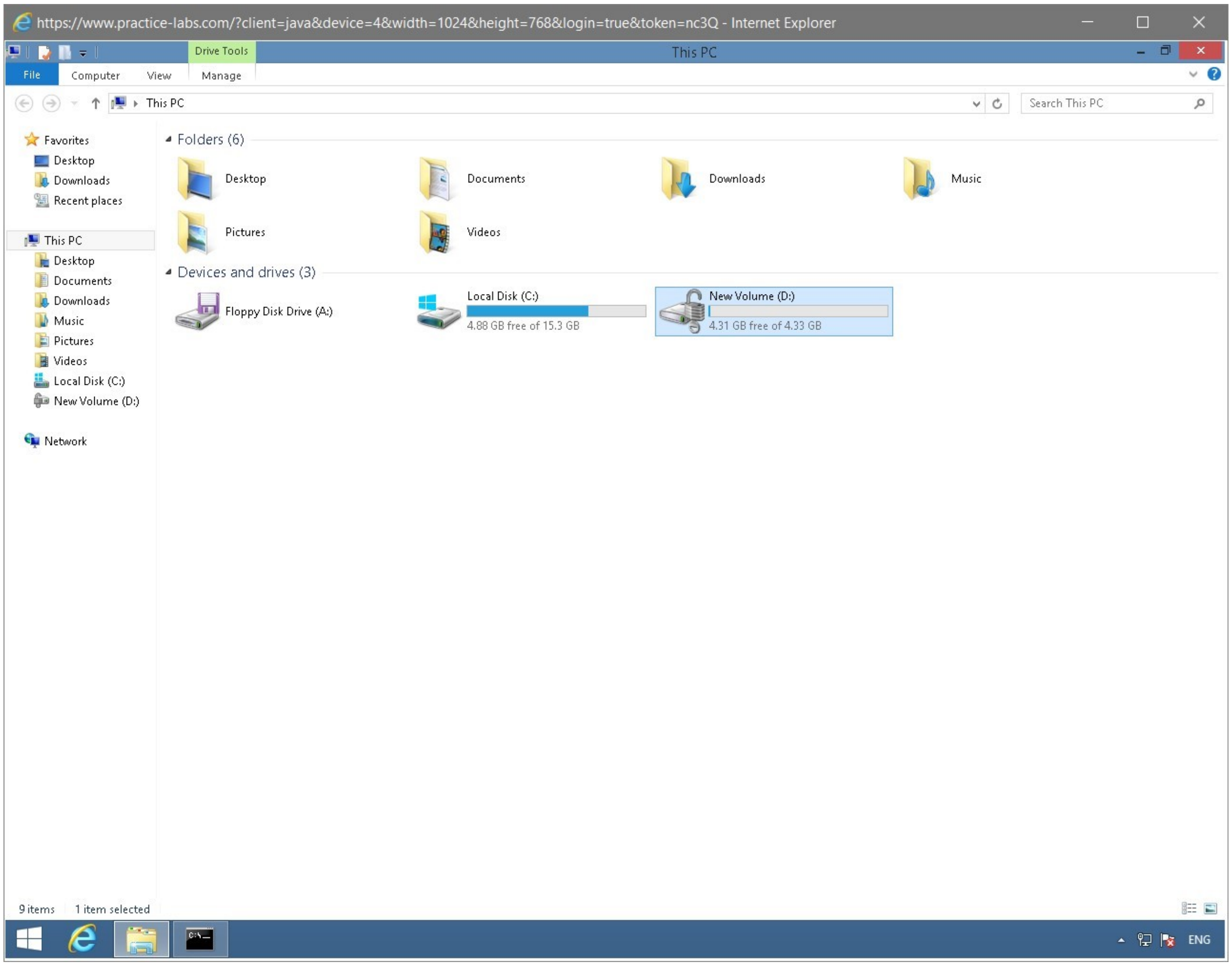


Figure 1.39 Screenshot of the PLABWIN810 desktop: File explorer window is displayed showing the open bitlock icon appended to the encrypted drive.

Step 11

To manage the properties of this newly-encrypted drive, right-click on **Bitlocker volume (D:)** and select **Manage Bitlocker**.

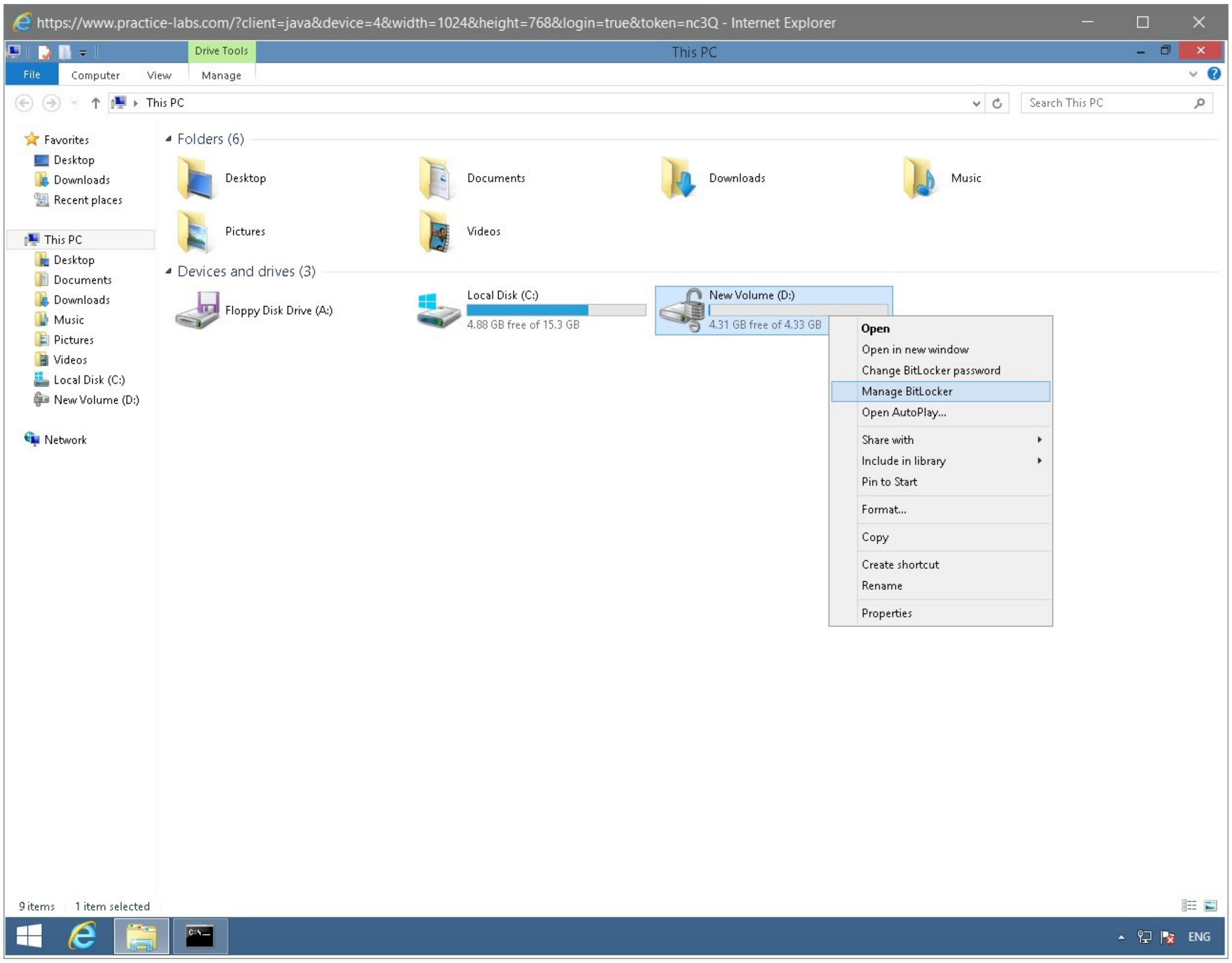


Figure 1.40 Screenshot of the PLABWIN810 desktop: Context menu (that appears on right-clicking an open bitlocked drive) > Manage BitLocker menu-options are displayed on the file explorer window.

Step 12

The **BitLocker Drive Encryption** window opens.

Notice the different options available for managing **New Volume (D:).**

Keep this window open for the next task.

Keep all devices powered on in their current state and proceed to the next task.

Task 4 - Verify BitLocker functionality

The previous task enabled the drive E for BitLocker. To find out how BitLocker works and to test the unlock drive password, perform the following steps:

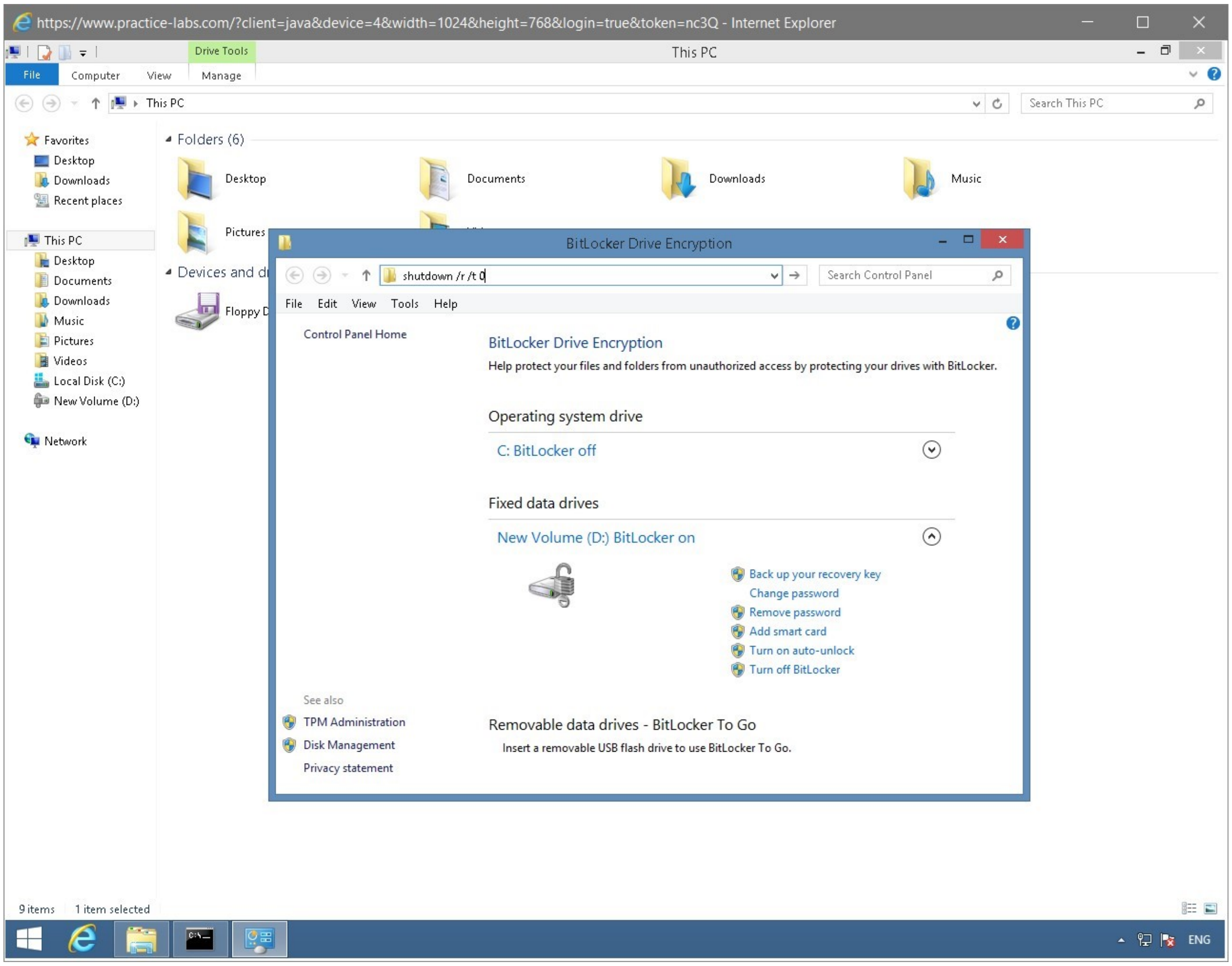
Step 1

While the **BitLocker Drive Encryption** window is open, click in the address bar and type:

```
Shutdown /r /t 0
```

Press **Enter**.

***Note**: Before reconnecting to PLABWIN810, wait for about 1 minute to let PLABWIN810 complete its restart.*



```
shutdown /r /t 0
```

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

C: BitLocker off

Fixed data drives

New Volume (D:) BitLocker on

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

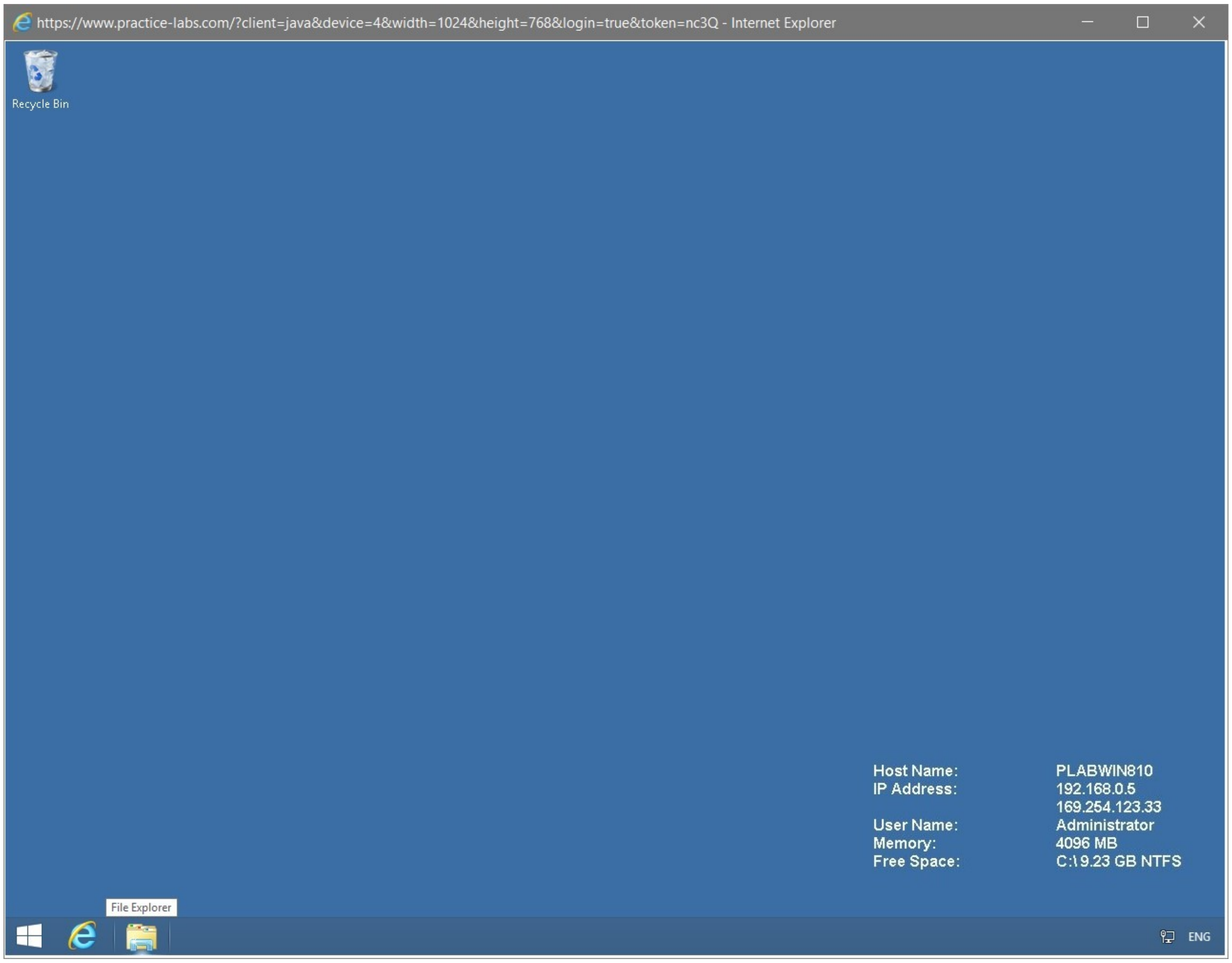
Figure 1.42 Screenshot of the PLABWIN810 desktop: BitLocker Drive Encryption window is displayed with the required command typed in the address bar at the top.

Step 2

On your computer, go to the **Practice Labs** web application.

After **1** minute, reconnect to **PLABWIN810** device.

When signed on to **PLABWIN810** computer, click **File Explorer** on taskbar.


https://www.practice-labs.com/?client=java&device=4&width=1024&height=768&login=true&token=nc3Q - Internet Explorer
Recycle Bin
File Explorer
ENG

```
Host Name:      PLABWIN810
IP Address:     192.168.0.5
                169.254.123.33
User Name:      Administrator
Memory:         4096 MB
Free Space:     C:\ 9.23 GB NTFS
```

Figure 1.43 Screenshot of the PLABWIN810 desktop: PLABWIN810 Windows desktop is

displayed showing the File Explorer icon on taskbar highlighted.

Step 3

Notice that **Local Disk D** is now locked.

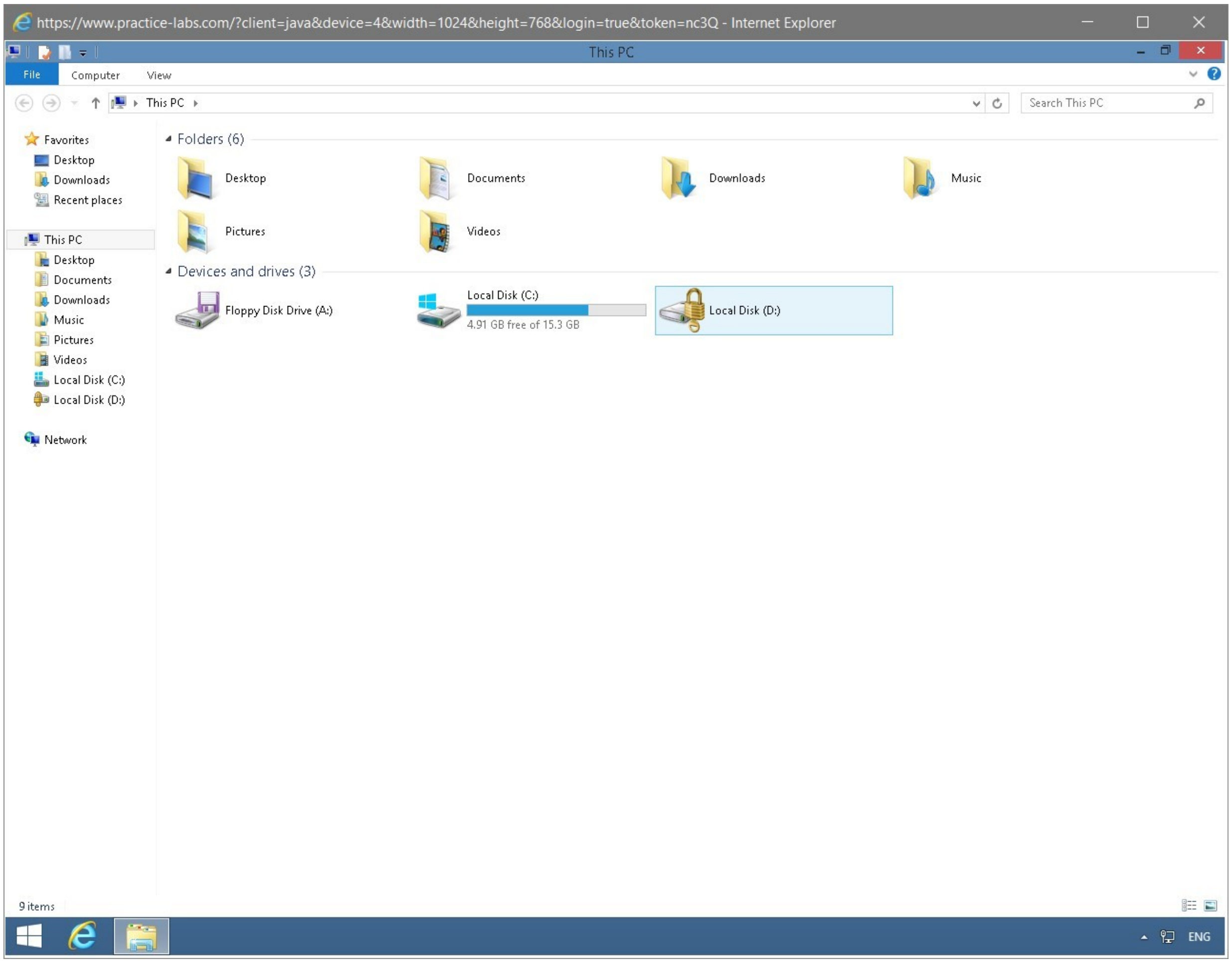


Figure 1.44 Screenshot of the PLABWIN810 desktop: The bitlocked drive is listed on the file explorer window.

Step 4

Right-click on **Local Disk D** and select **Unlock Drive**…

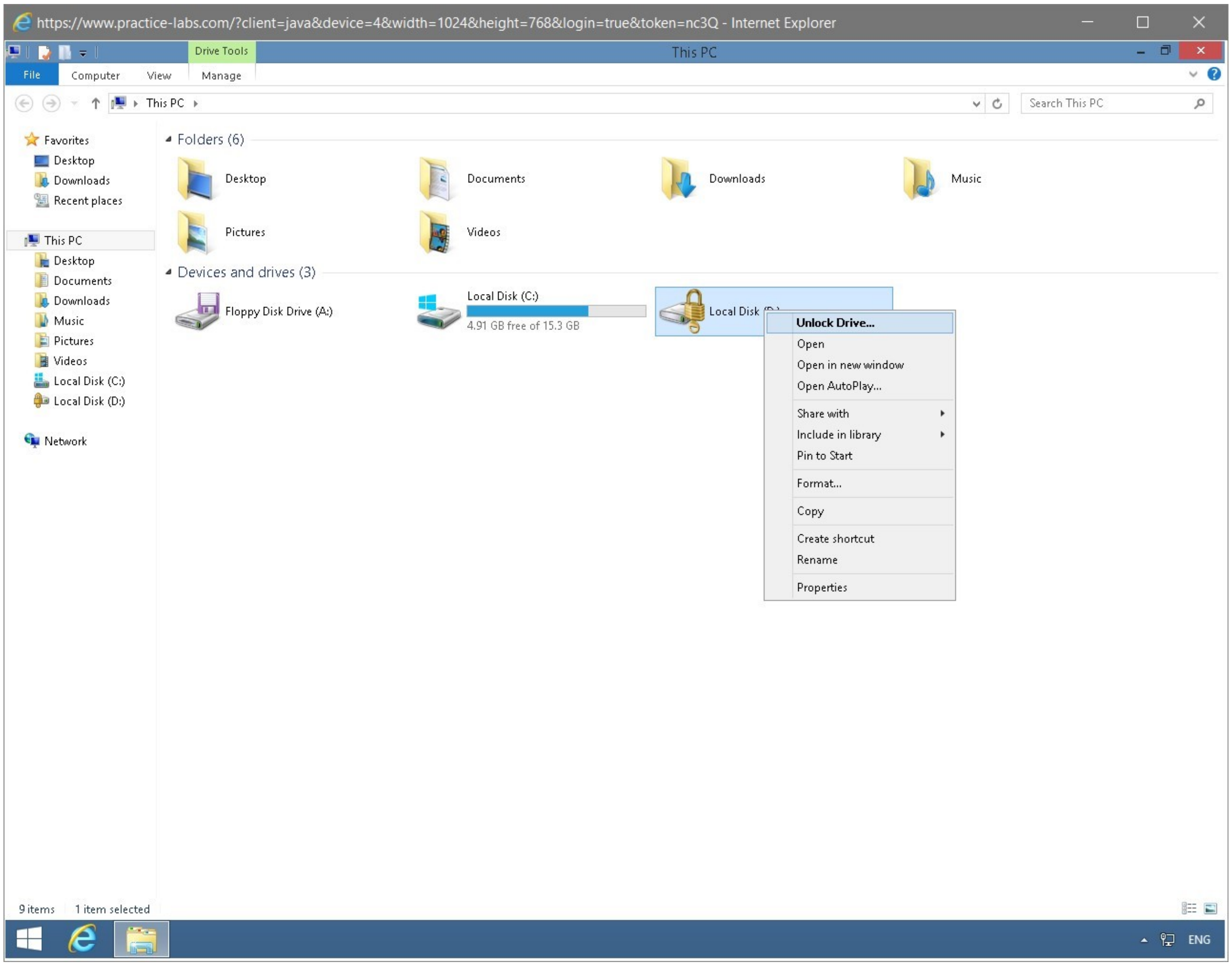


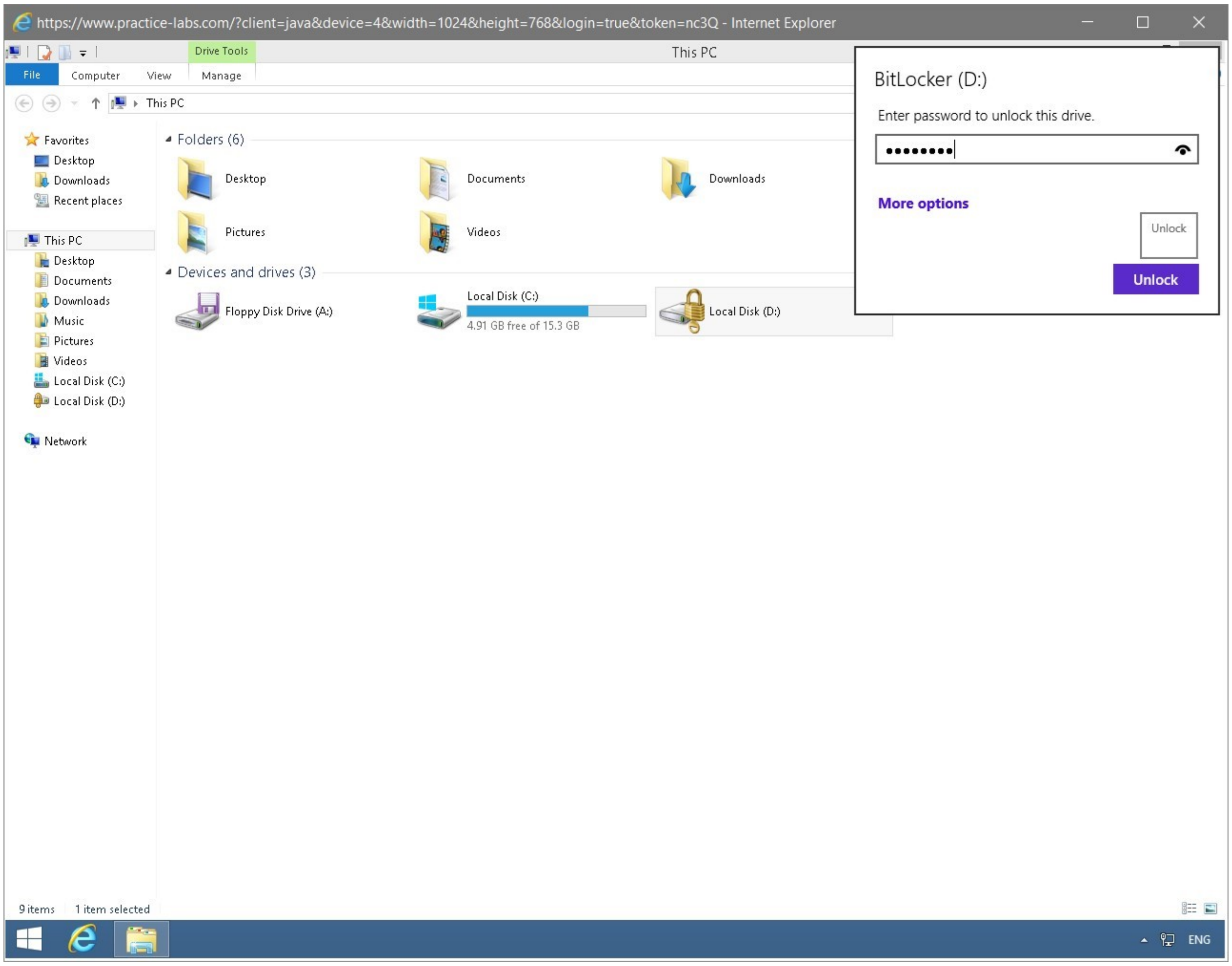
Figure 1.45 Screenshot of the PLABWIN810 desktop: Context menu (that appears on right-clicking a bitlocked drive) > Unlock Drive menu-options are displayed on the file explorer window.

Step 5

On the **BitLocker D** dialog box, type:

```
Password
```

Click **Unlock**.



https://www.practice-labs.com/?client=java&device=4&width=1024&height=768&login=true&token=nc3Q - Internet Explorer

BitLocker (D:)

Enter password to unlock this drive.

•••••••••

Figure 1.46 Screenshot of the PLABWIN810 desktop: BitLocker (D:) dialog box is displayed showing the required credentials typed-in and the Unlock button available.

Step 6

The **Bitlocker Volume D** is now unlocked.

Keep all devices powered on in their current state and proceed to the next task.

Task 5 - Manage BitLocker using the command prompt

Windows BitLocker can managed by using a command prompt tool called **manage-bde.exe**.

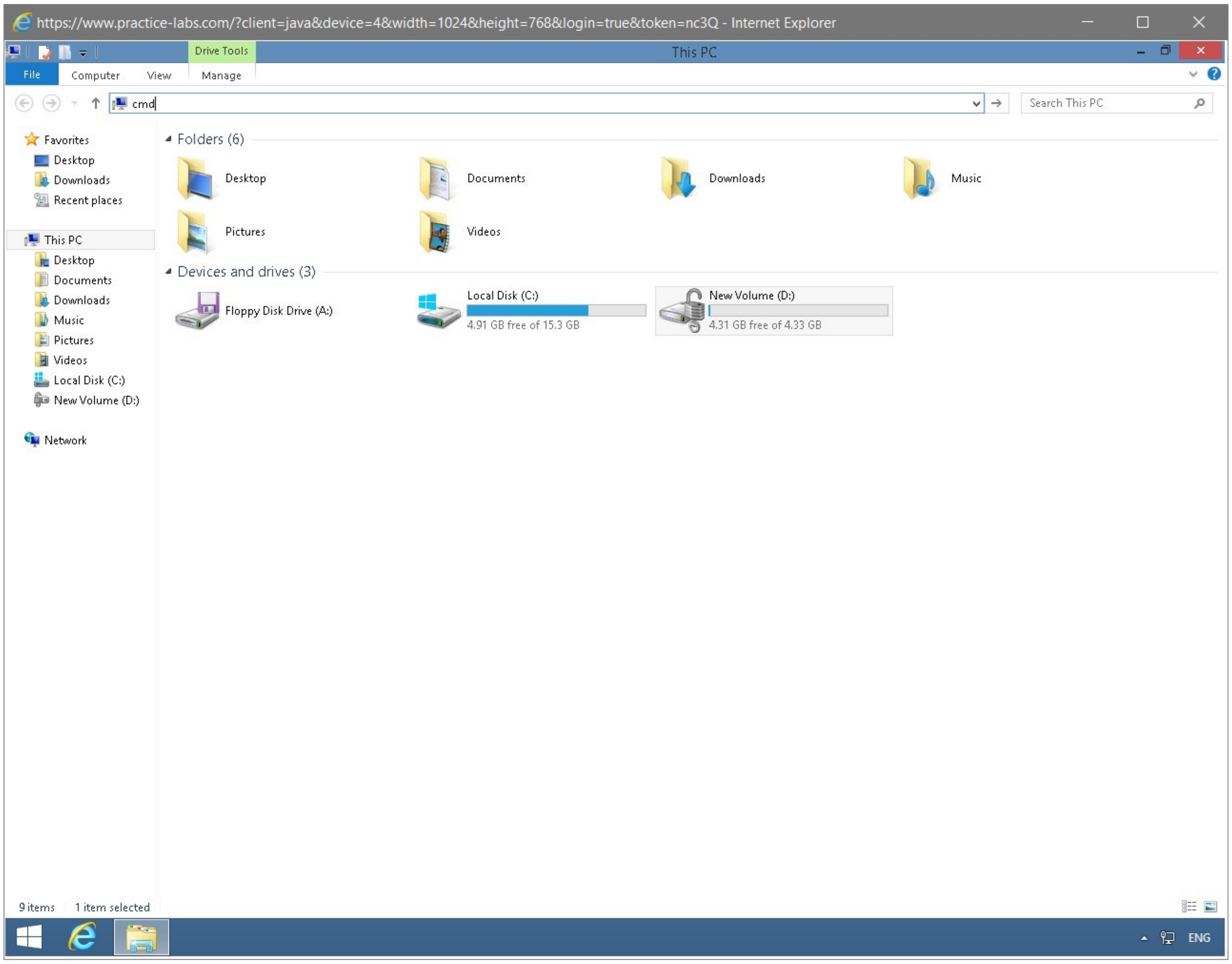
To know how the manage-bde command works, perform the following steps:

Step 1

Connect to **PLABWIN810** while the BitLocker window is open, click in the address bar and type:

```
cmd
```

Press **Enter**.



cmd

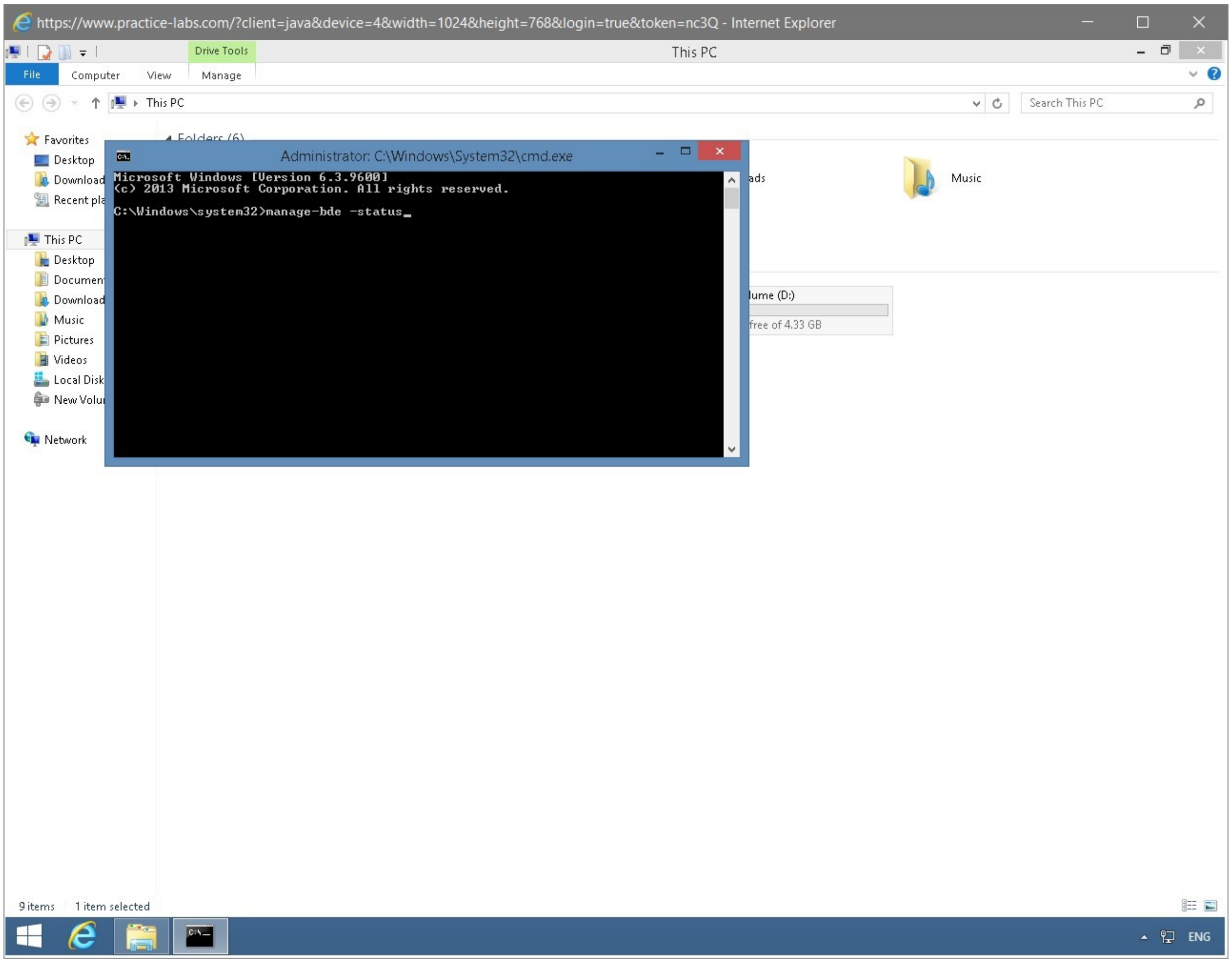
Figure 1.48 Screenshot of the PLABWIN810 desktop: File explorer window is displayed showing the required command typed in the address bar at the top.

Step 2

On the command prompt window, type the following

```
manage-bde -status
```

Press **Enter**.



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>manage-bde -status_
```

Figure 1.49 Screenshot of the PLABWIN810 desktop: Administrator: C:\Windows\System32\cmd.exe window is displayed showing the command to manage a bitlocked device typed-in.

Step 3

The result of **manage-bde** command is now displayed.

Notice that **Drive D** is **Fully Encrypted**.

Keep all devices powered on in their current state and proceed to the next task.

Task 6 - Unlock the Encrypted Drive using Recovery Keys

If the password used for unlocking this bitlocker-enabled drive is forgotten, you can use the Recovery Key that was created earlier to unlock Drive E.

In this task, you will not enter a password and simulate a recovery of the encrypted volume using the Recovery Keys.

To use the recovery keys, perform the following steps:

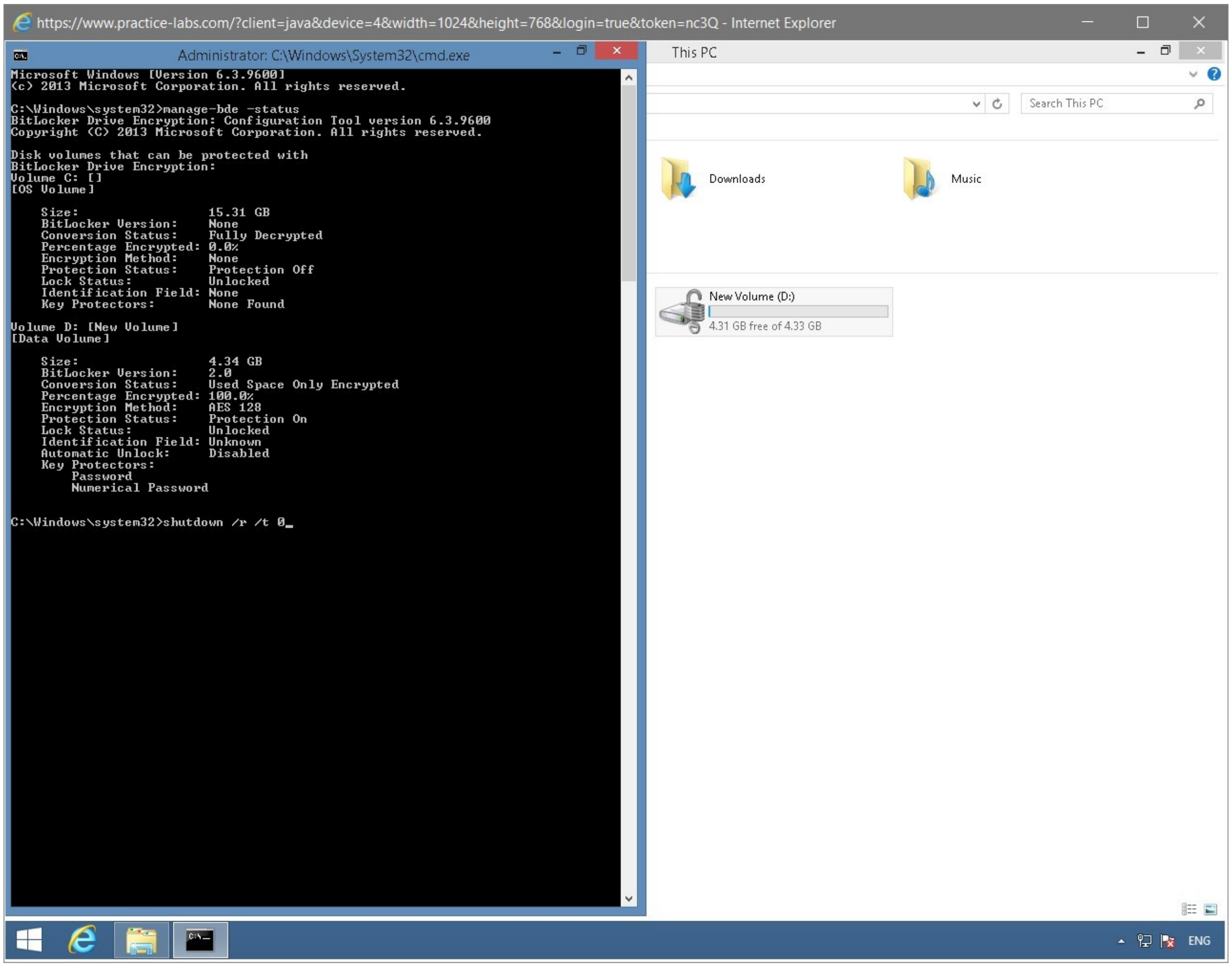
Step 1

On **PLABWIN810**, while the command prompt is still open, type:

```
shutdown /r /t 0
```

Press **Enter**.

***Note**: You need to restart PLABWIN810 computer, as you have unlocked Drive E using the password. You need to restart the computer to lock the encrypted drive.*



https://www.practice-labs.com/?client=java&device=4&width=1024&height=768&login=true&token=nc3Q - Internet Explorer
Administrator: C:\Windows\System32\cmd.exe
This PC
Search This PC
Downloads
Music
New Volume (D:)
4.31 GB free of 4.33 GB
ENG

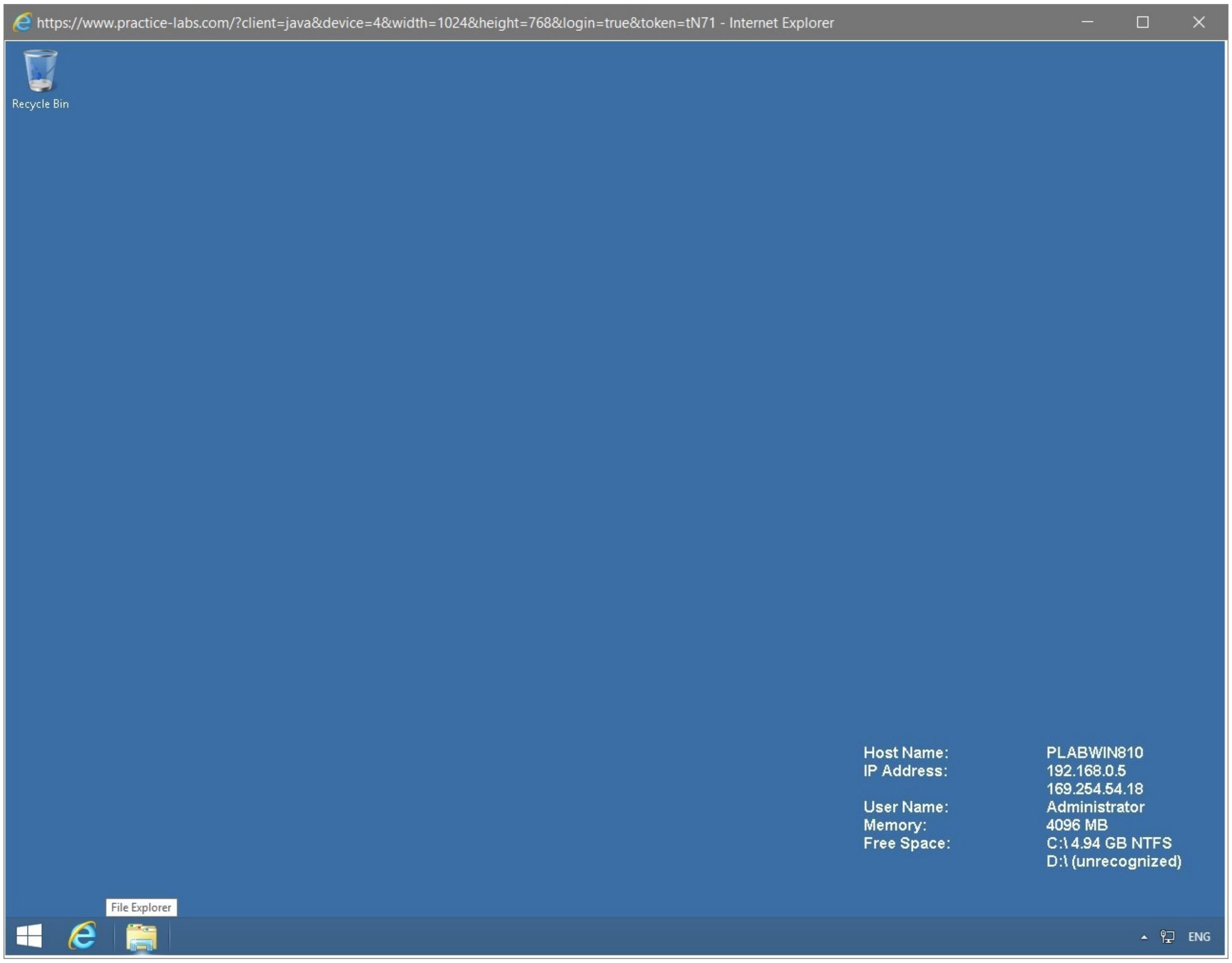
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>manage-bde -status
BitLocker Drive Encryption: Configuration Tool version 6.3.9600
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Disk volumes that can be protected with
BitLocker Drive Encryption:
Volume C: []
[OS Volume]

    Size:                 15.31 GB
    BitLocker Version:    None
    Conversion Status:    Fully Decrypted
    Percentage Encrypted: 0.0%
    Encryption Method:    None
    Protection Status:    Protection Off
    Lock Status:          Unlocked
    Identification Field: None
    Key Protectors:       None Found

Volume D: [New Volume]
[Data Volume]

    Size:                 4.34 GB
    BitLocker Version:    2.0
    Conversion Status:    Used Space Only Encrypted
    Percentage Encrypted: 100.0%
    Encryption Method:    AES 128
    Protection Status:    Protection On
    Lock Status:          Unlocked
    Identification Field: Unknown
    Automatic Unlock:     Disabled
    Key Protectors:
        Password
        Numerical Password


C:\Windows\system32>shutdown /r /t 0_
```

Figure 1.51 Screenshot of the PLABWIN810 desktop: Administrator: C:\Windows\System32\cmd.exe window is displayed showing the command to restart the device typed-in.

Step 2

A minute after the restart, reconnect to the **PLABWIN810** device.

Click **File Explorer** on the taskbar.


https://www.practice-labs.com/?client=java&device=4&width=1024&height=768&login=true&token=tN71 - Internet Explorer
Recycle Bin
File Explorer
ENG

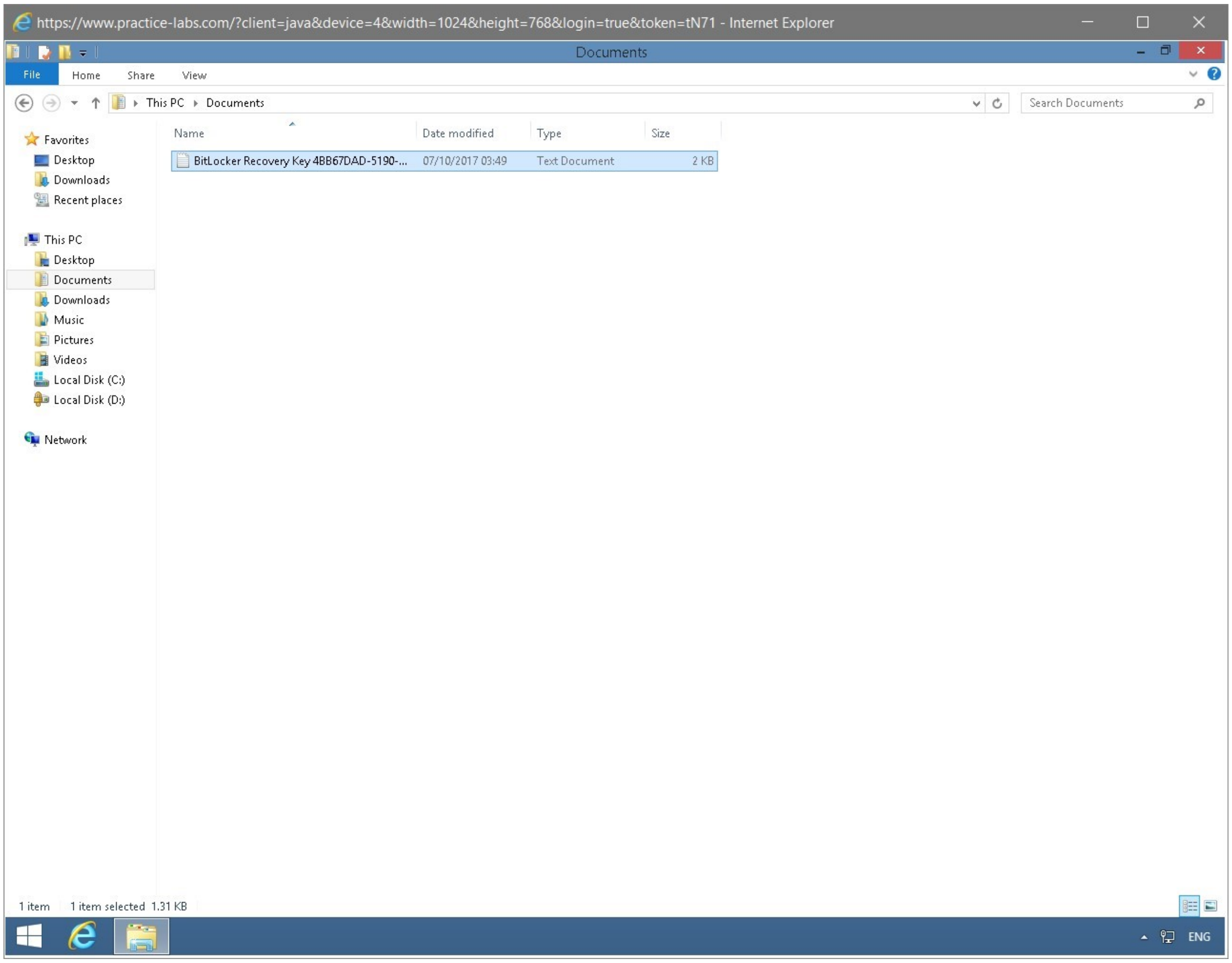
Host Name: PLABWIN810
IP Address: 192.168.0.5
169.254.54.18
User Name: Administrator
Memory: 4096 MB
Free Space: C:\ 4.94 GB NTFS
D:\ (unrecognized)

Figure 1.52 Screenshot of the PLABWIN810 desktop: PLABWIN810 Windows desktop is displayed showing the File Explorer icon on taskbar highlighted.

Step 3

On **File Explorer** window, expand **This PC** and then select **Documents** folder in the right pane.

The contents of **Documents** folder is displayed including the **Bitlocker Recovery Key** file.



Name	Date modified	Type	Size
BitLocker Recovery Key 4BB67DAD-5190-...	07/10/2017 03:49	Text Document	2 KB

1 item 1 item selected 1.31 KB

Figure 1.53 Screenshot of the PLABWIN810 desktop: File explorer window is displayed showing the required node-path selected on the navigation pane at the left and the contents of the selected folder listed on the details pane at the right.

Step 4

Right-click the **BitLocker Recovery Key** file and select **Open**.

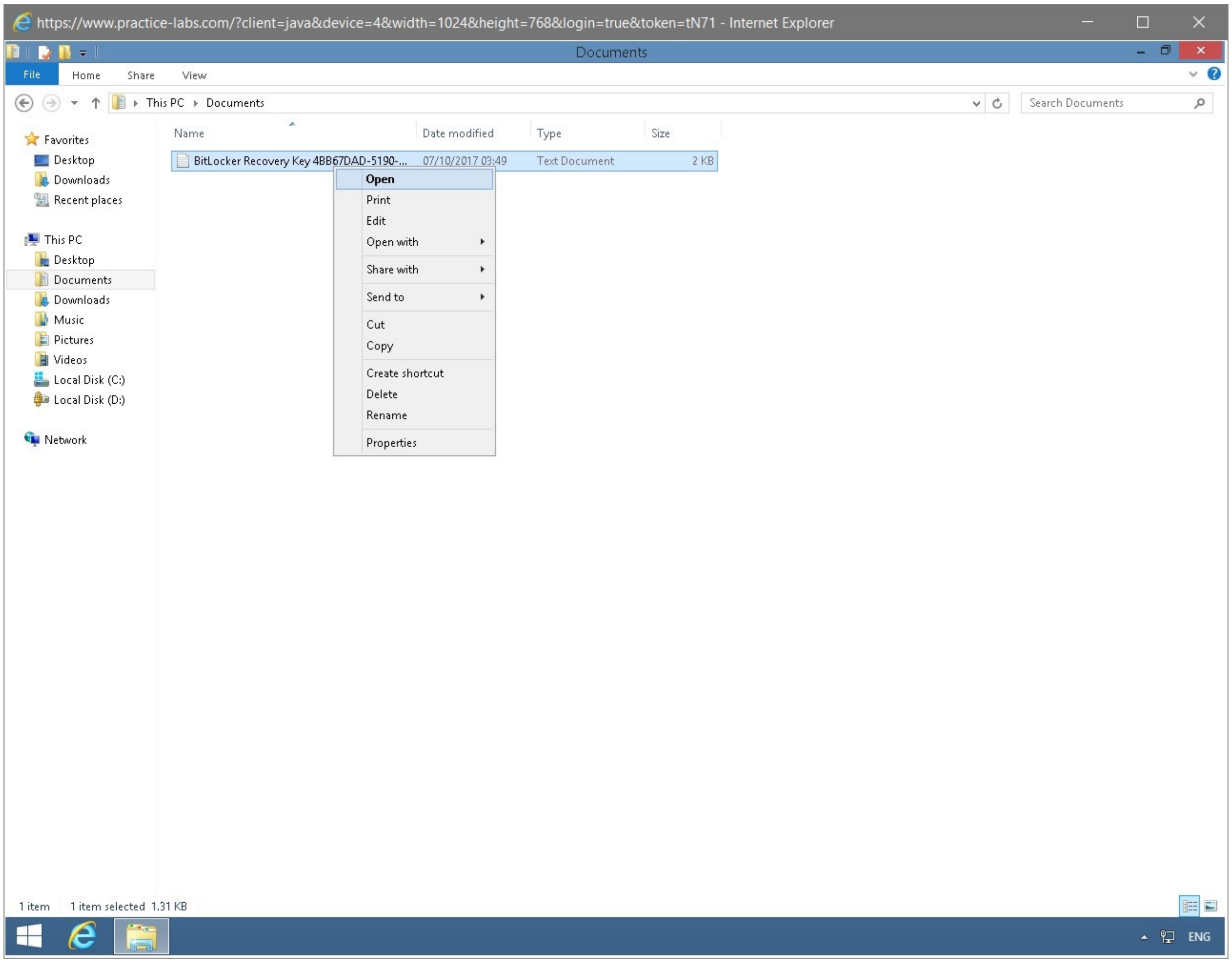


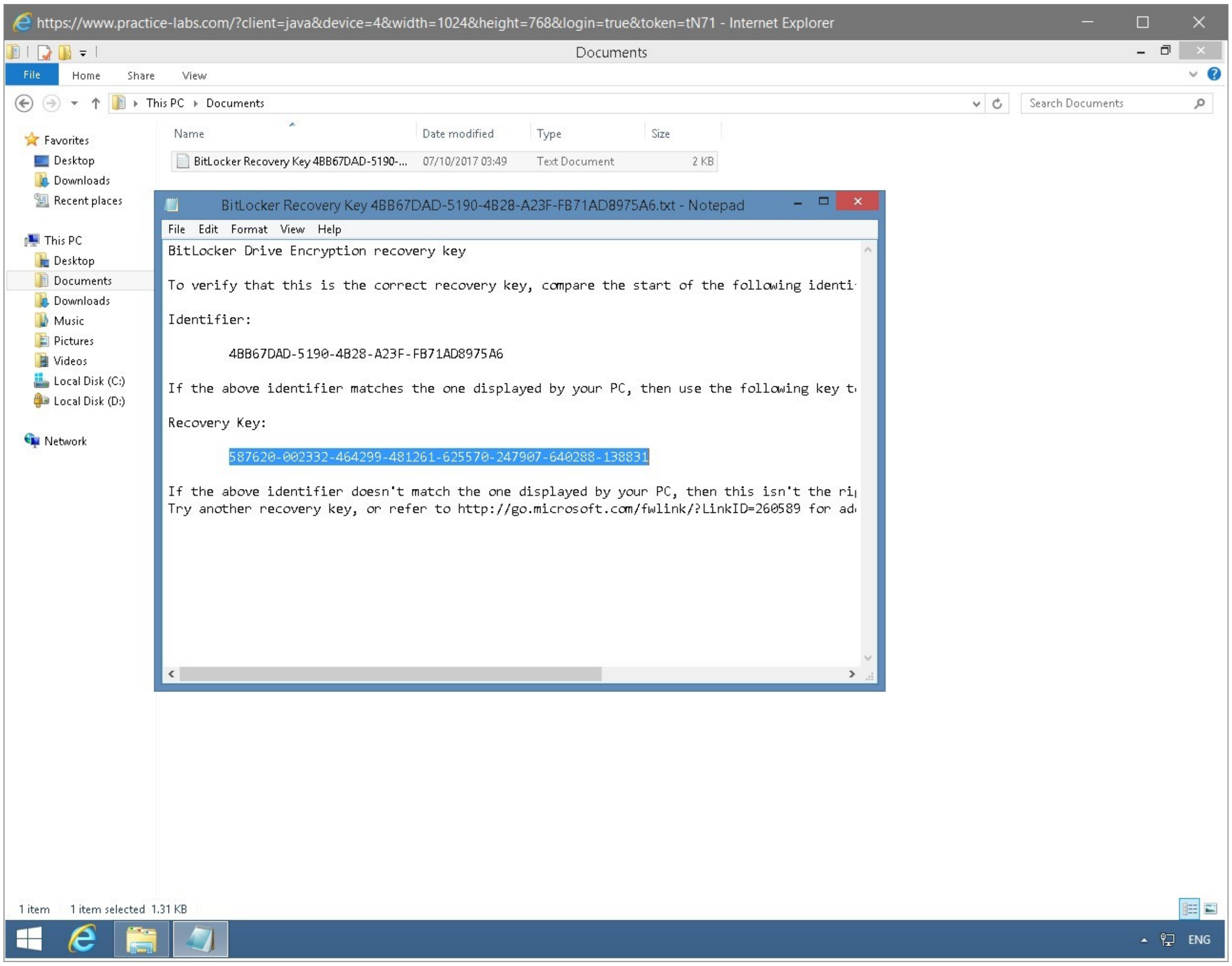
Figure 1.54 Screenshot of the PLABWIN810 desktop: Context menu (that appears on right-clicking the saved bitlocker recovery key) > Open menu-options are displayed on the file explorer window.

Step 5

When **BitLocker Recovery File** is opened, locate the **Recovery Key** section.

> ***Note**: The Recovery Key that you will get in your lab, will be different from the screen shot.*

Keep the **BitLocker Recovery File** window open.



Name	Date modified	Type	Size
BitLocker Recovery Key 4BB67DAD-5190-...	07/10/2017 03:49	Text Document	2 KB

```
BitLocker Drive Encryption recovery key

To verify that this is the correct recovery key, compare the start of the following identi

Identifier:

        4BB67DAD-5190-4B28-A23F-FB71AD8975A6

If the above identifier matches the one displayed by your PC, then use the following key t

Recovery Key:

        587620-002332-464299-481261-625570-247907-640288-138831

If the above identifier doesn't match the one displayed by your PC, then this isn't the ri
Try another recovery key, or refer to http://go.microsoft.com/fwlink/?LinkID=260589 for ad
```

Figure 1.55 Screenshot of the PLABWIN810 desktop: Contents of the BitLocker Recovery Key file showing the recovery key highlighted are displayed.

Step 6

Go back to **File Explorer** window that you opened earlier.

Right-click on **Local Disk (D :)** and select **Unlock Drive...**

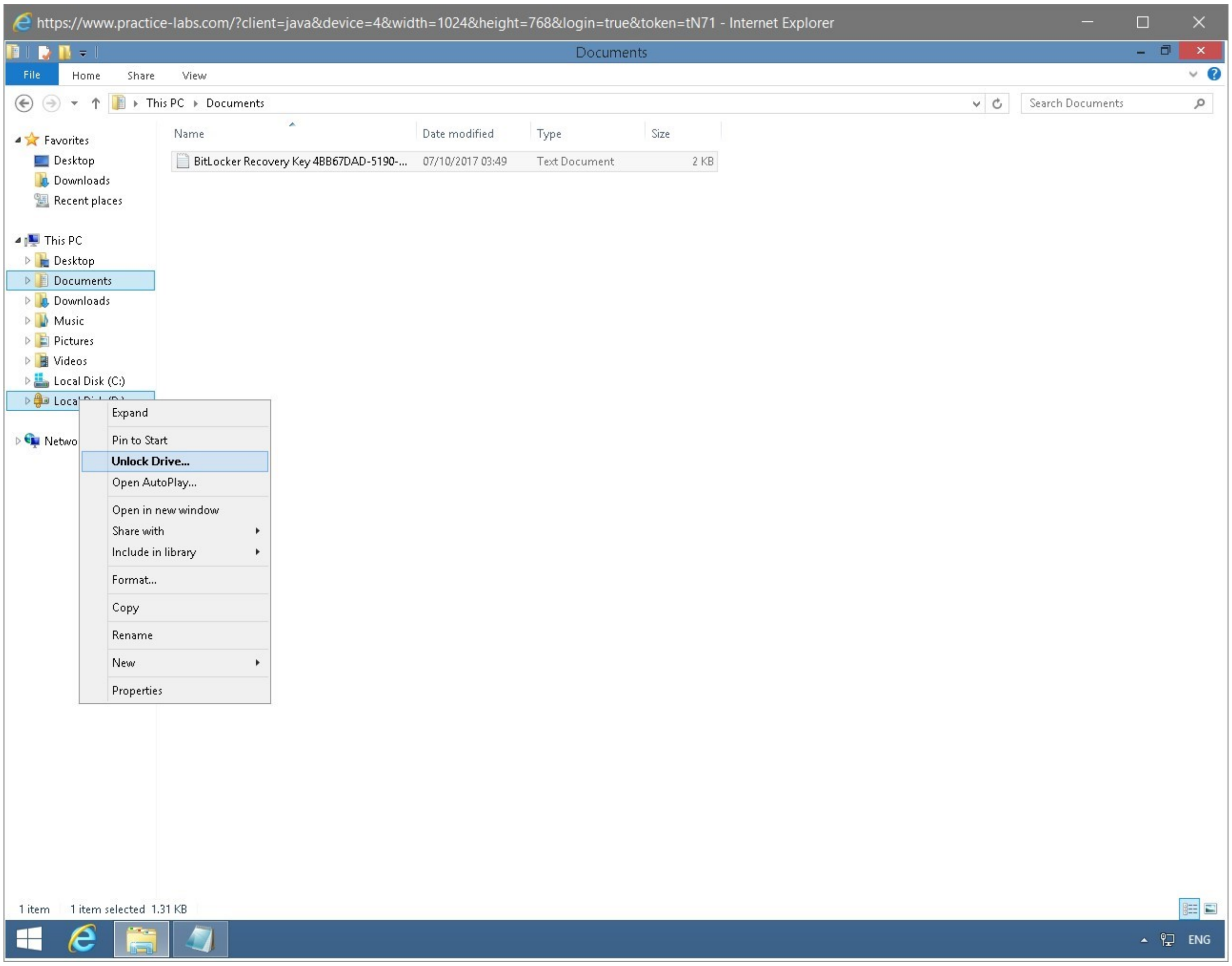
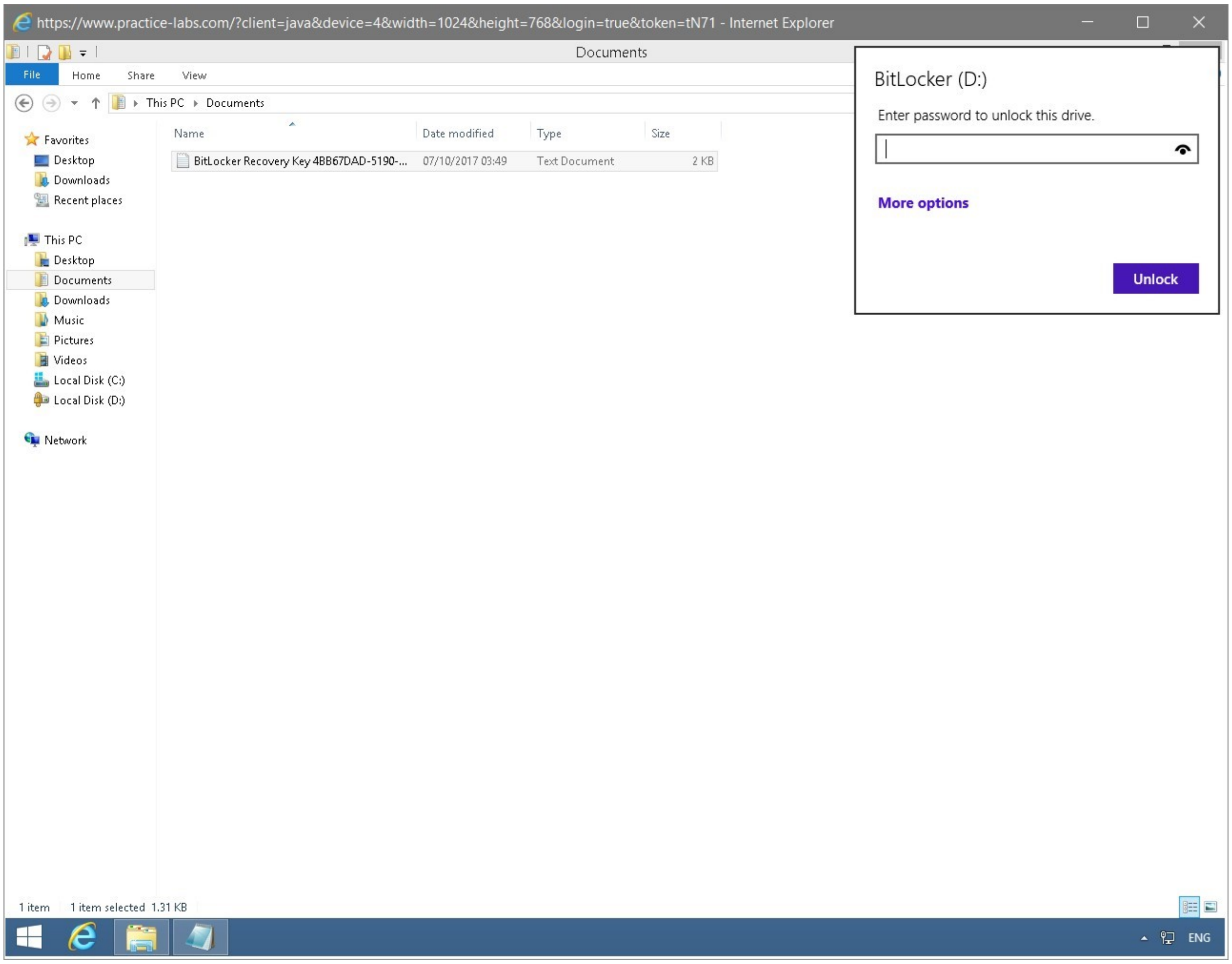


Figure 1.56 Screenshot of the PLABWIN810 desktop: Context menu (that appears on right-clicking the name of a bitlocked drive) > Unlock Drive menu-options are displayed on the file explorer window.

Step 7

On the **BitLocker (E:)** dialog box, click **More options** link.



https://www.practice-labs.com/?client=java&device=4&width=1024&height=768&login=true&token=tN71 - Internet Explorer

BitLocker (D:)

Enter password to unlock this drive.

Name	Date modified	Type	Size
BitLocker Recovery Key 4BB67DAD-5190-...	07/10/2017 03:49	Text Document	2 KB

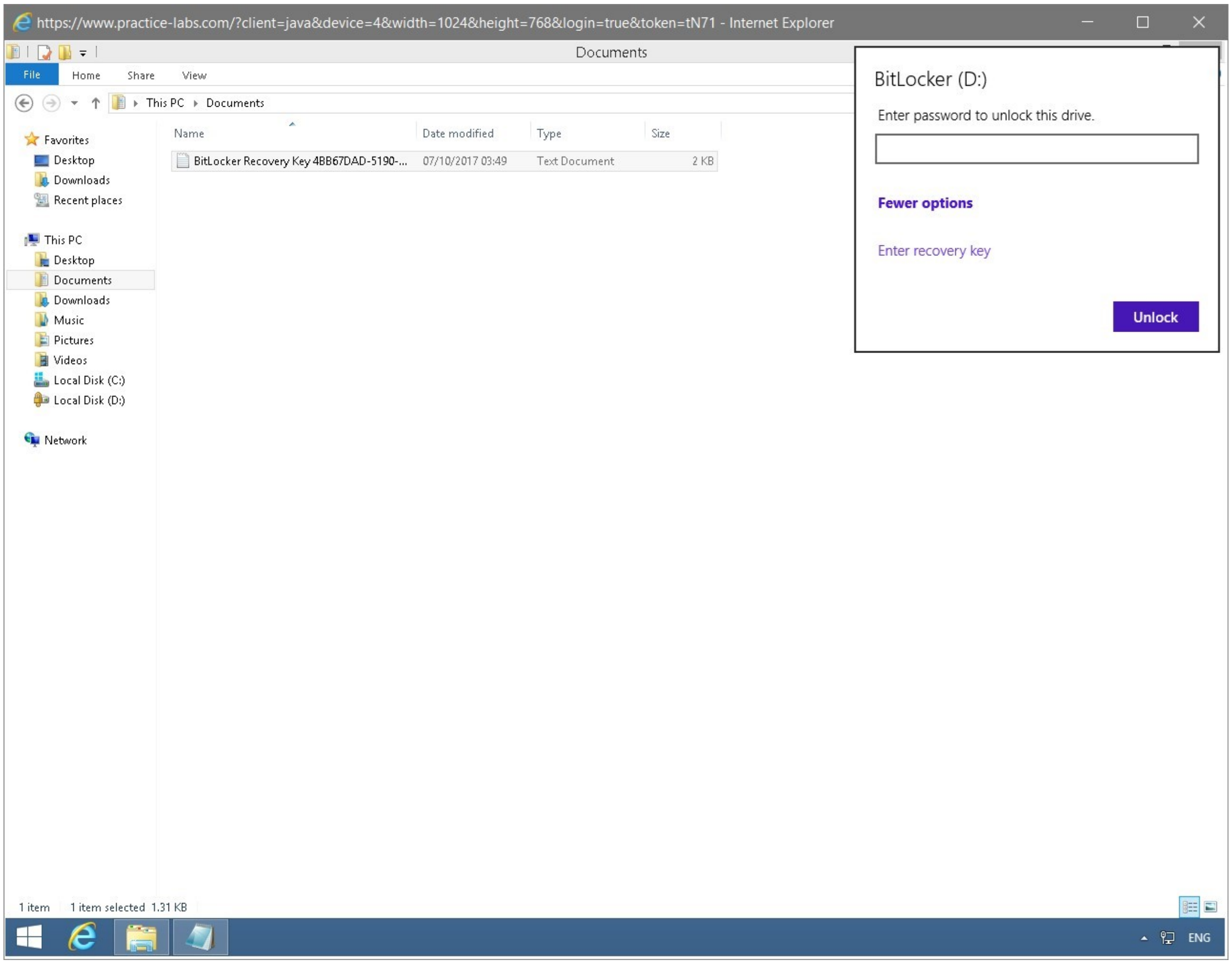
1 item 1 item selected 1.31 KB

Figure 1.57 Screenshot of the PLABWIN810 desktop: BitLocker (D:) dialog box is displayed with the More options link available.

Step 8

The **BitLocker (D:)** dialog box expands and now include **Enter recovery key** link.

Click the **Enter recovery key** link.



Name	Date modified	Type	Size
BitLocker Recovery Key 4BB67DAD-5190-...	07/10/2017 03:49	Text Document	2 KB

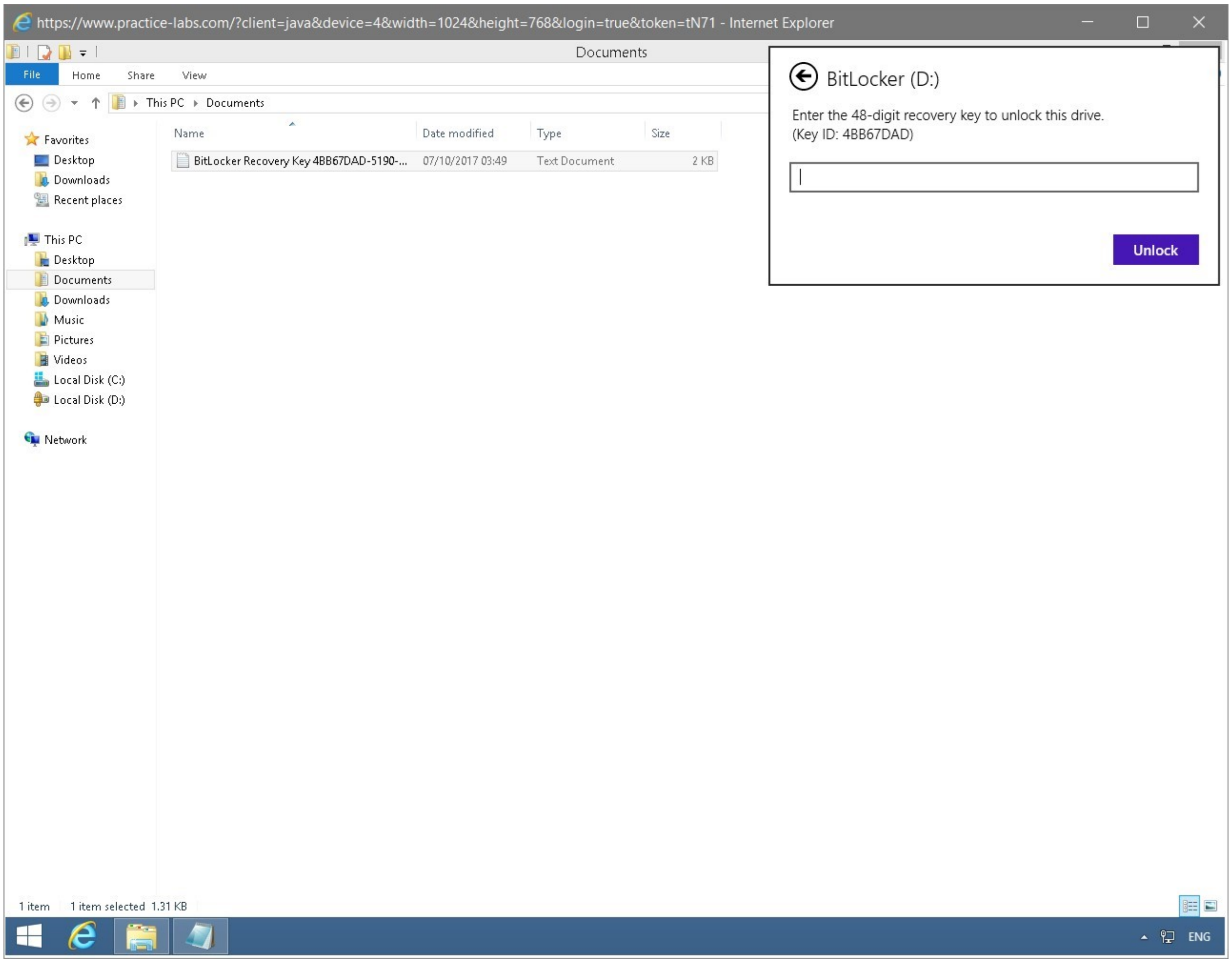
BitLocker (D:)

Enter password to unlock this drive.

Figure 1.58 Screenshot of the PLABWIN810 desktop: Expanded BitLocker (D:) dialog box is displayed showing the Enter recovery key link available.

Step 9

You are now asked to enter the 48-digit recovery key to unlock this drive.



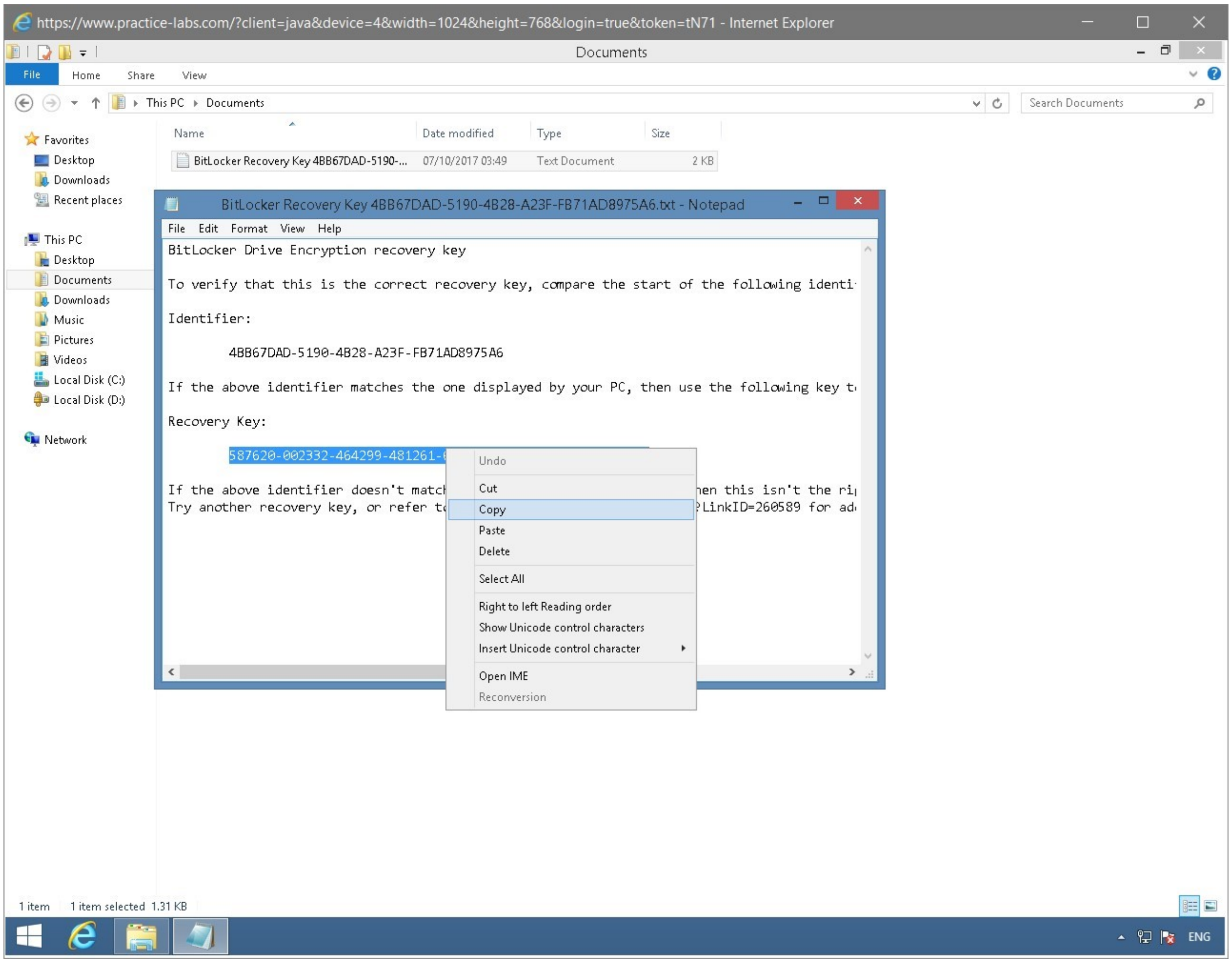
Name	Date modified	Type	Size
BitLocker Recovery Key 4BB67DAD-5190-...	07/10/2017 03:49	Text Document	2 KB

Enter the 48-digit recovery key to unlock this drive.
(Key ID: 4BB67DAD)

Figure 1.59 Screenshot of the PLABWIN810 desktop: BitLocker (D:) dialog box is displayed asking for the 48-digit recovery key.

Step 10

Go back to **BitLocker Recovery Key** text file and copy the **Recovery Key**.



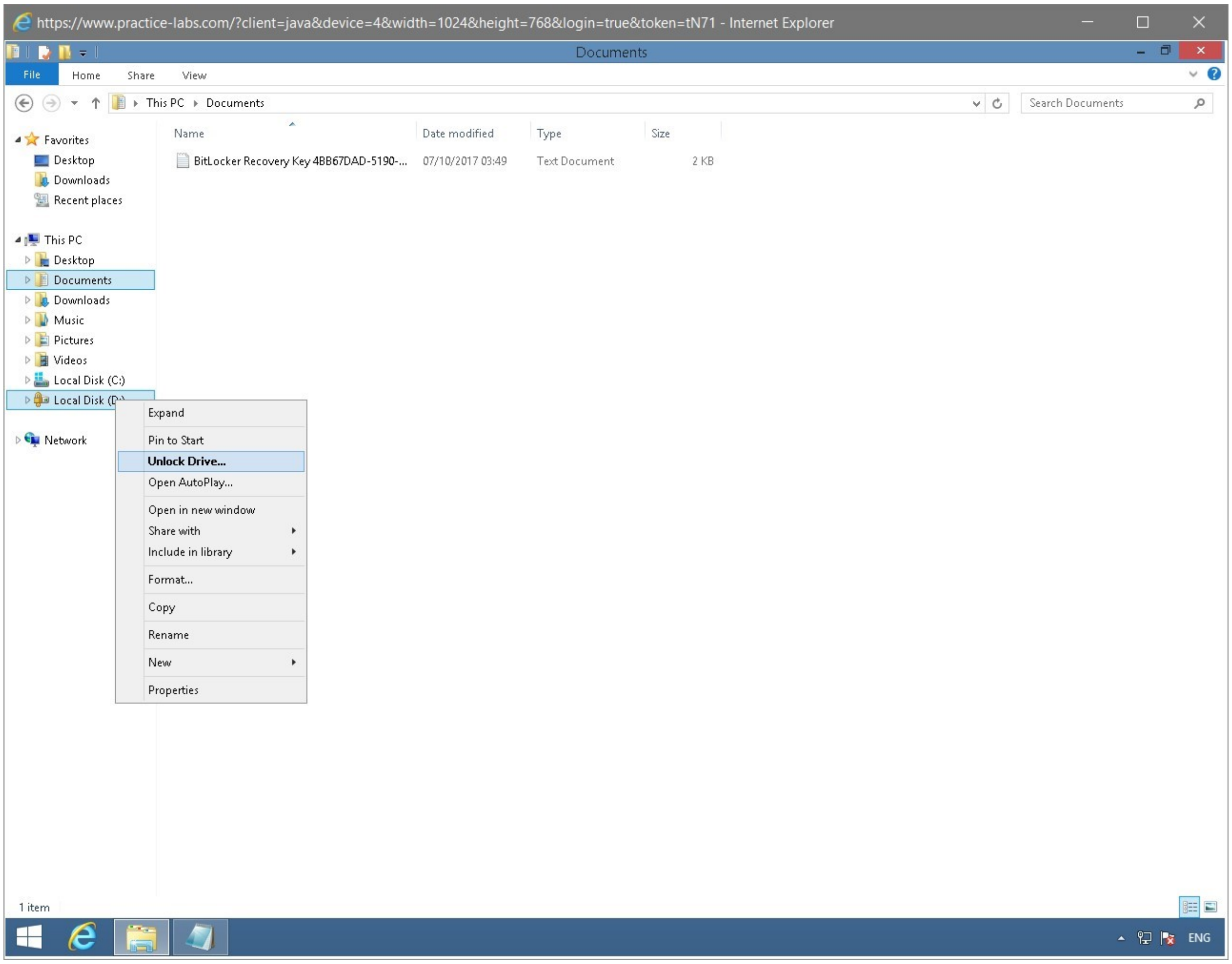
```
BitLocker Drive Encryption recovery key

To verify that this is the correct recovery key, compare the start of the following identi

Identifier:

        4BB67DAD-5190-4B28-A23F-FB71AD8975A6

If the above identifier matches the one displayed by your PC, then use the following key t

Recovery Key:

        587620-002332-464299-481261-(

If the above identifier doesn't match                        hen this isn't the ri
Try another recovery key, or refer t                         ?LinkID=260589 for ad
```

Figure 1.60 Screenshot of the PLABWIN810 desktop: Context menu (that appears on right-clicking the saved recovery key) > Copy menu-options are highlighted on the BitLocker Recovery Key - Notepad file.

Step 11

The dialog box to enter the **Recovery Key** has closed since you clicked outside of it earlier.

Right-click again on **Local Disk D** then select **Unlock Drive...**

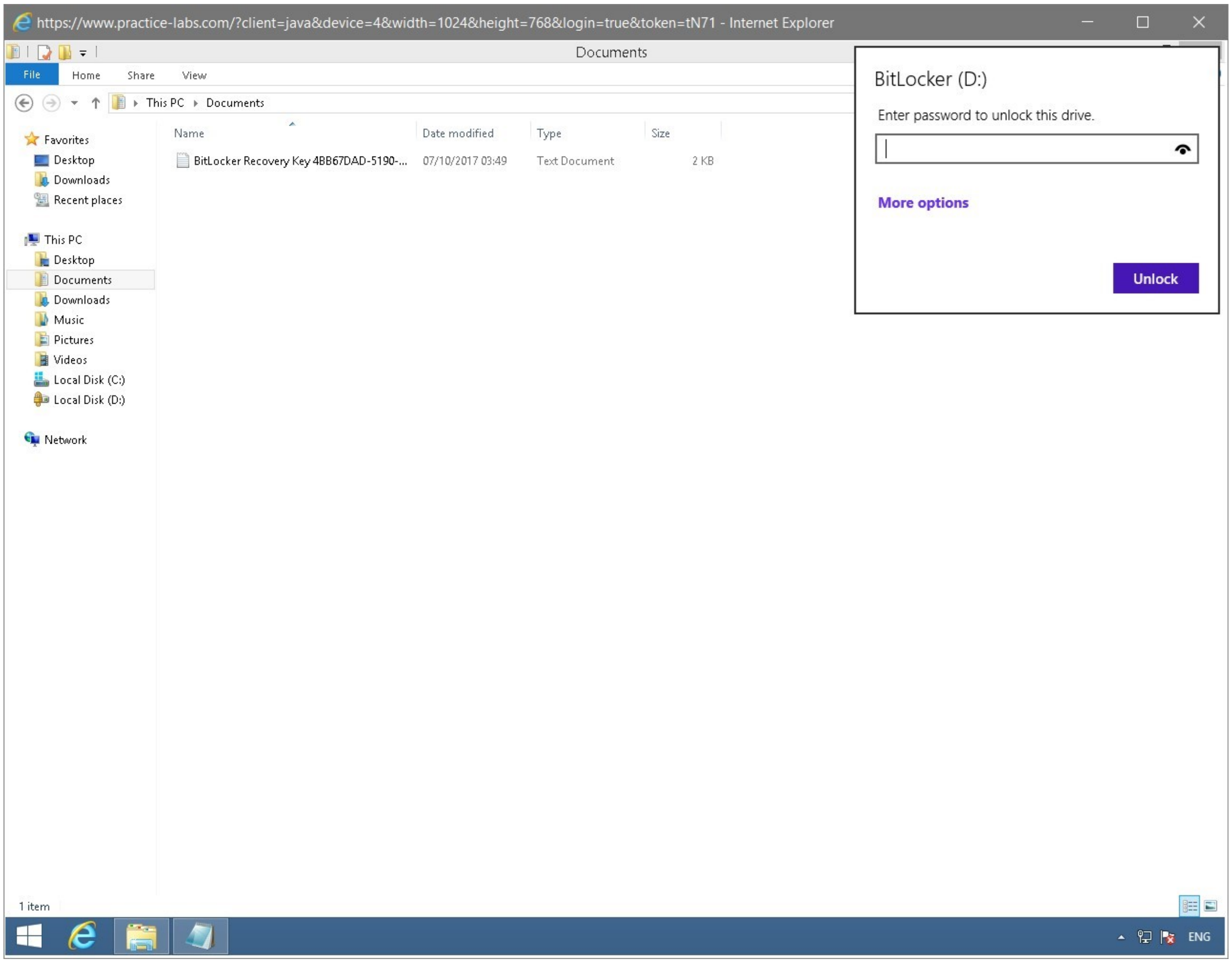


Name	Date modified	Type	Size
BitLocker Recovery Key 4BB67DAD-5190-...	07/10/2017 03:49	Text Document	2 KB

Figure 1.61 Screenshot of the PLABWIN810 desktop: Context menu (that appears on right-clicking the name of a bitlocked drive) > Unlock Drive menu-options are highlighted on the file explorer window.

Step 12

On the **BitLocker D** dialog box, click **More options**.



BitLocker (D:)

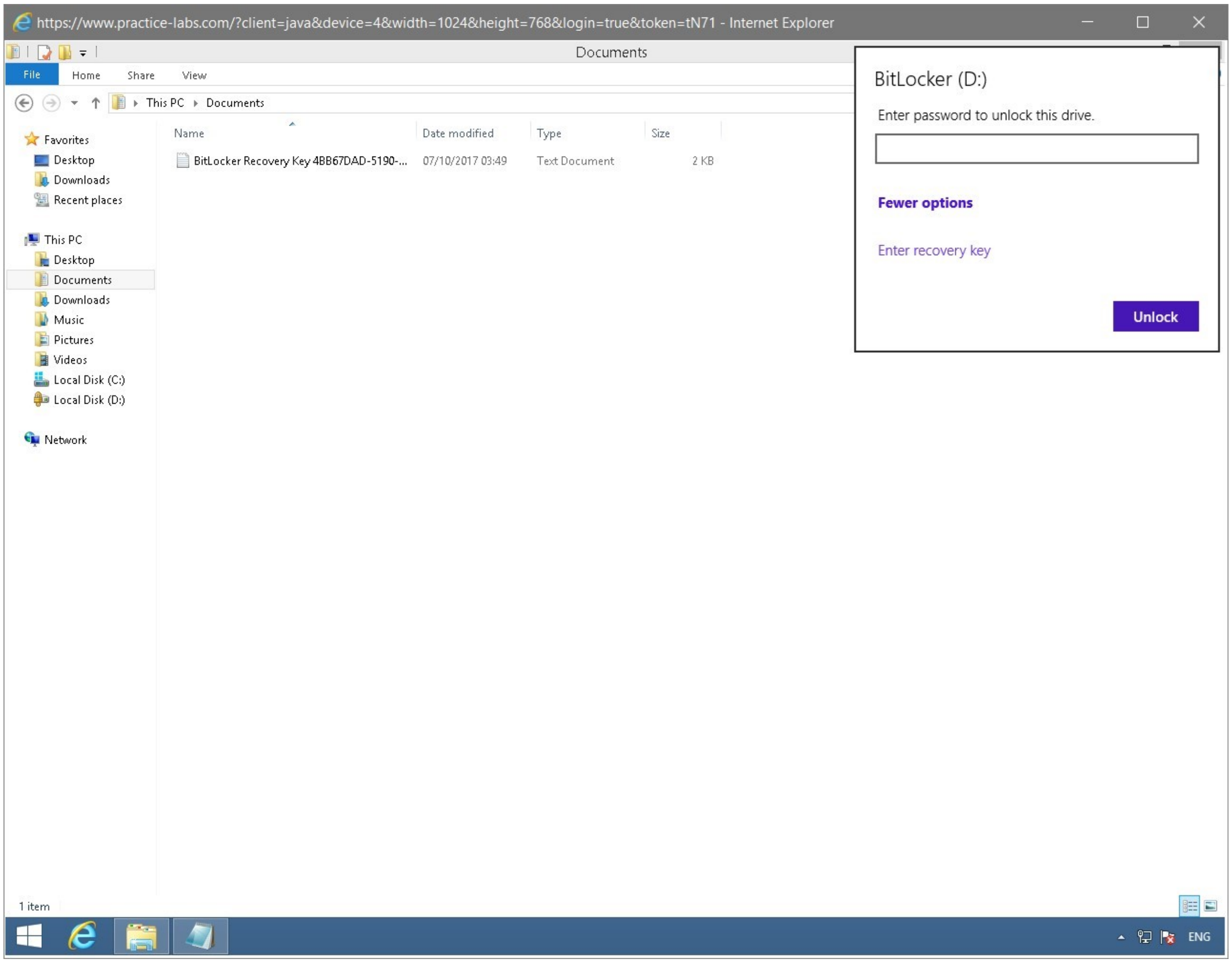
Enter password to unlock this drive.

Name	Date modified	Type	Size
BitLocker Recovery Key 4BB67DAD-5190-...	07/10/2017 03:49	Text Document	2 KB

Figure 1.62 Screenshot of the PLABWIN810 desktop: BitLocker (D:) dialog box is displayed with the More options link available.

Step 13

Still on the **BitLocker D** dialog box, click **Enter recovery key**.



Name	Date modified	Type	Size
BitLocker Recovery Key 4BB67DAD-5190-...	07/10/2017 03:49	Text Document	2 KB

BitLocker (D:)

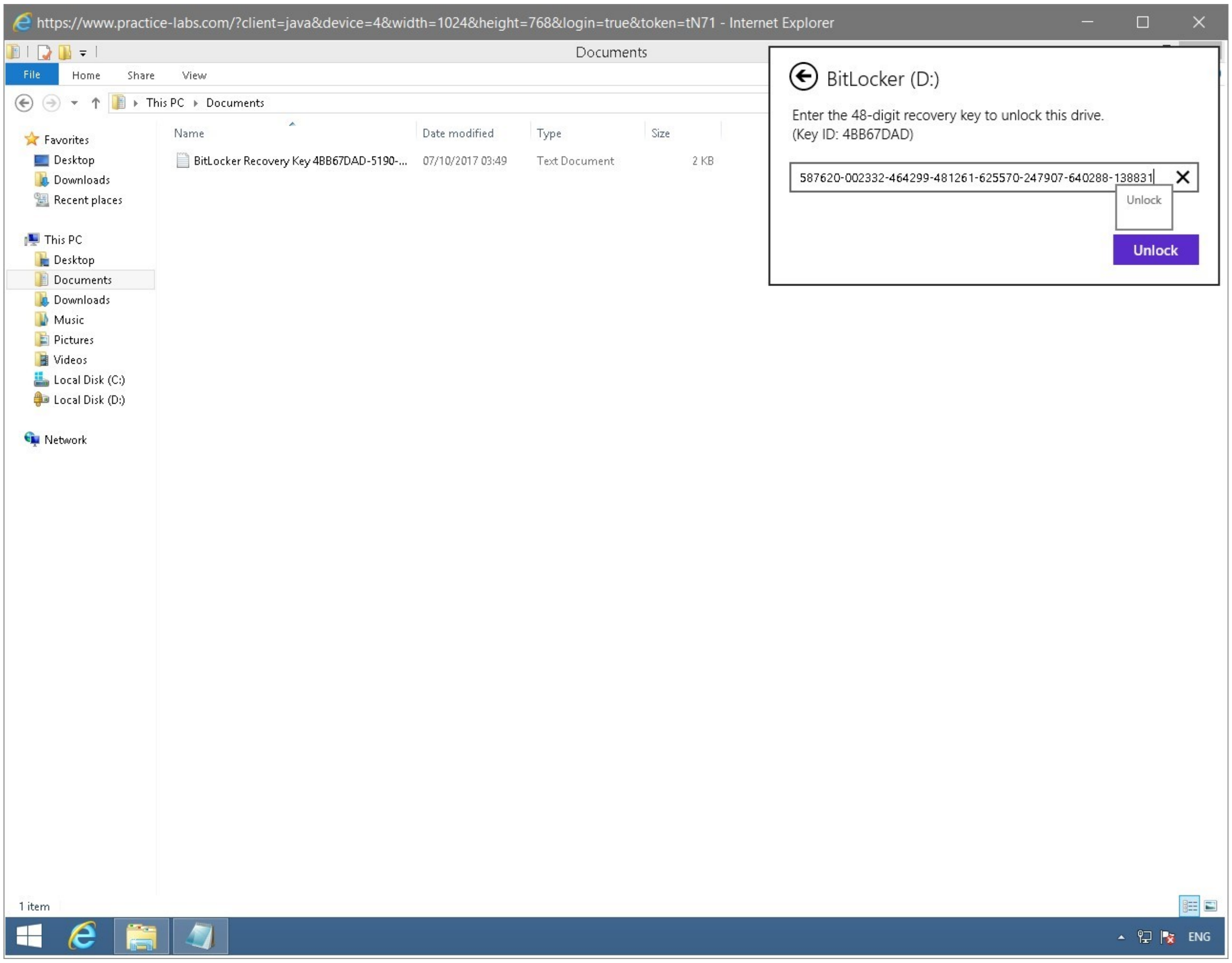
Enter password to unlock this drive.

Figure 1.63 Screenshot of the PLABWIN810 desktop: Expanded BitLocker (D:) dialog box is displayed showing the Enter recovery key link available.

Step 14

Click inside the textbox and press **CTRL+V** to paste the recovery key you copied from the Recovery Key text document.

Click **Unlock**.



Enter the 48-digit recovery key to unlock this drive.
(Key ID: 4BB67DAD)

587620-002332-464299-481261-625570-247907-640288-138831

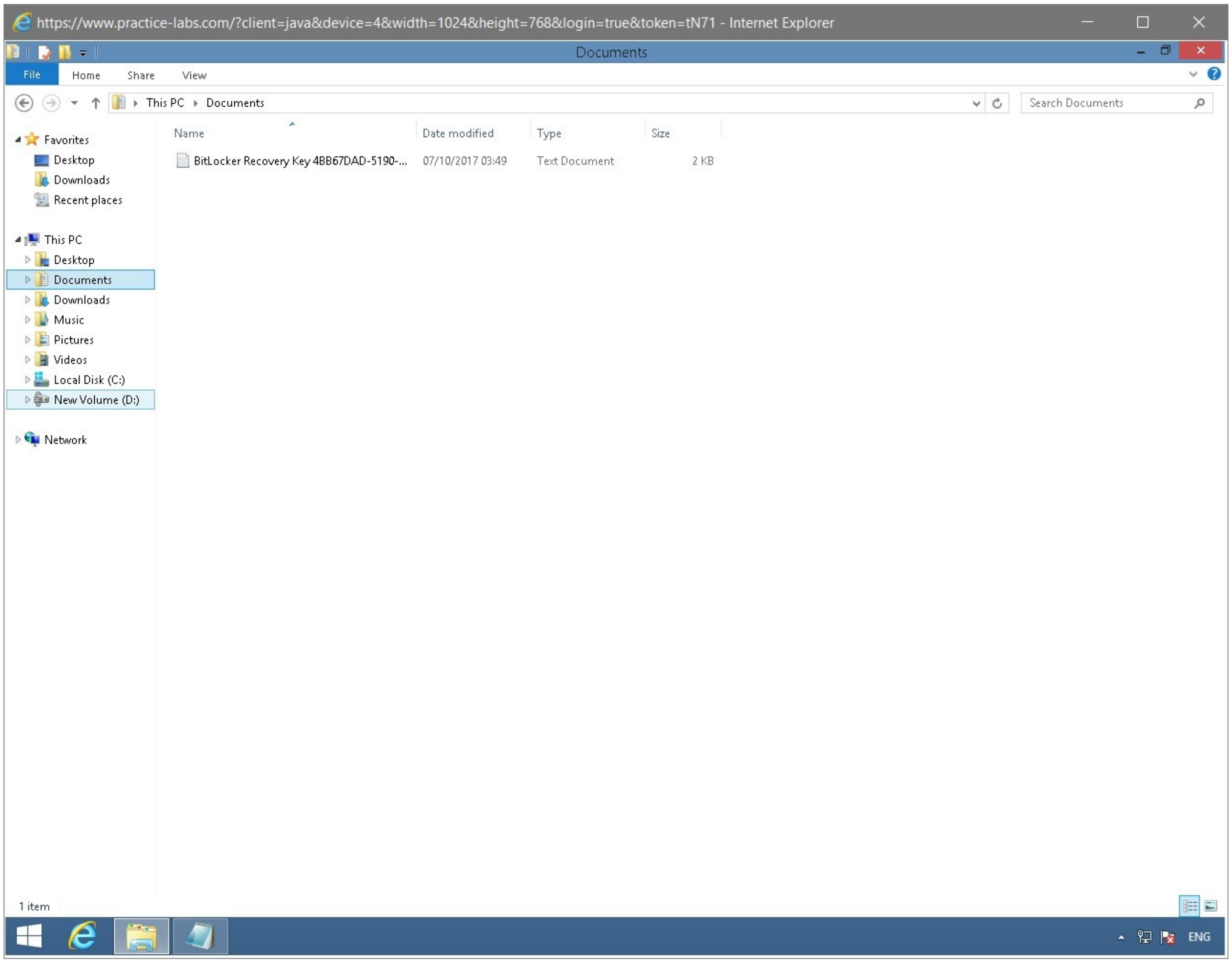
Figure 1.64 Screenshot of the PLABWIN810 desktop: BitLocker (D:) dialog box is displayed showing the 48-digit recovery key copied as required and the Unlock button available.

Step 15

Notice that **BitLocker volume (D:)** is now unlocked.

Therefore, the Recovery Key worked.

Keep the **File Explorer** window open for the next task.



Name	Date modified	Type	Size
BitLocker Recovery Key 4BB67DAD-5190-...	07/10/2017 03:49	Text Document	2 KB

Figure 1.65 Screenshot of the PLABWIN810 desktop: BitLocker volume (D:) node showing the open-lock icon is displayed on the left navigation pane of the file explorer window.

Keep all devices powered on in their current state and proceed to the next task.

Task 7 - Remove BitLocker disk encryption on Drive E

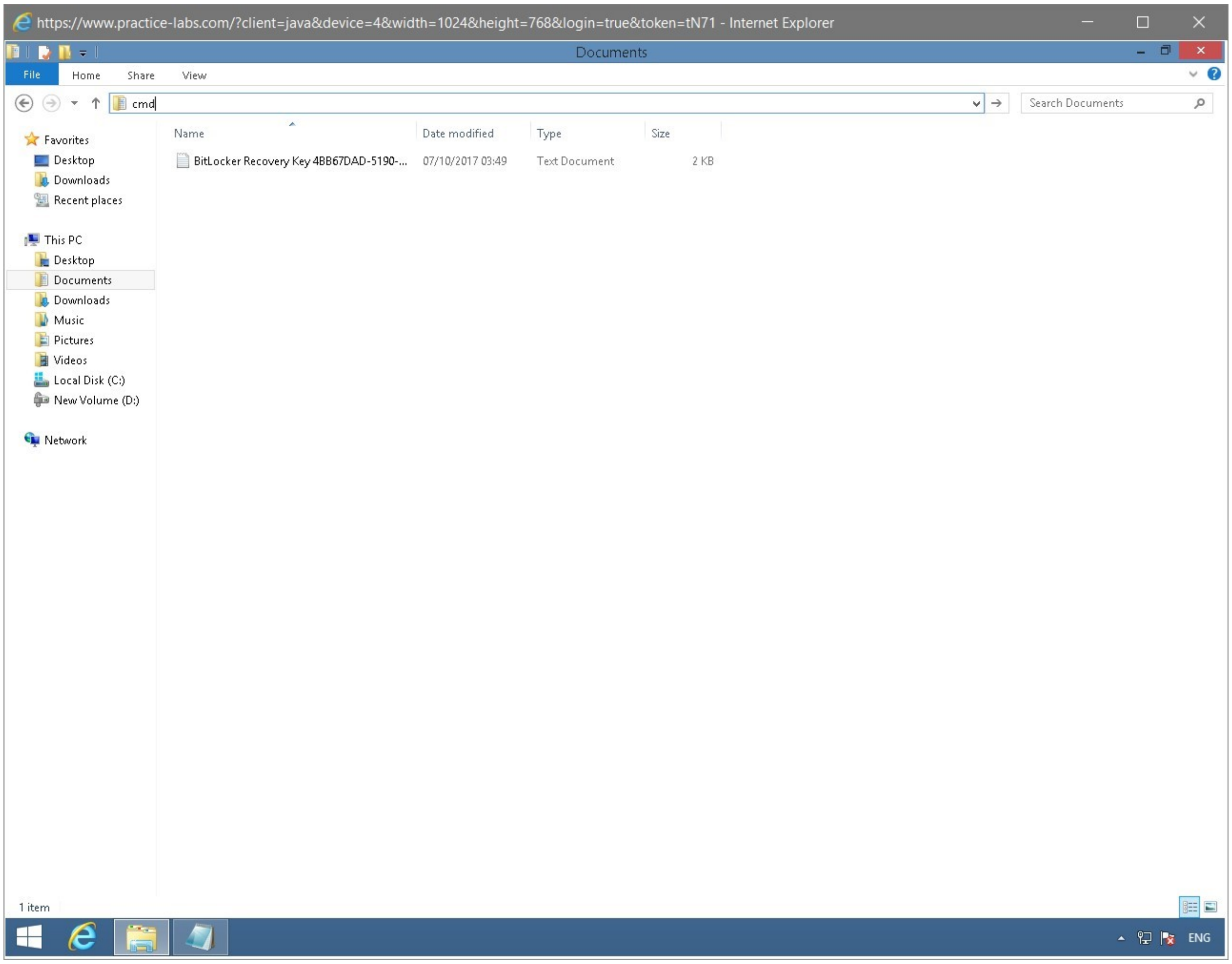
To remove BitLocker encryption on the volume E, follow these steps:

Step 1

On **PLABWIN810**, while **File Explorer** is open, click in the address bar and type:

```
cmd
```

Press **Enter**.



cmd

Name	Date modified	Type	Size
BitLocker Recovery Key 4BB67DAD-5190-...	07/10/2017 03:49	Text Document	2 KB

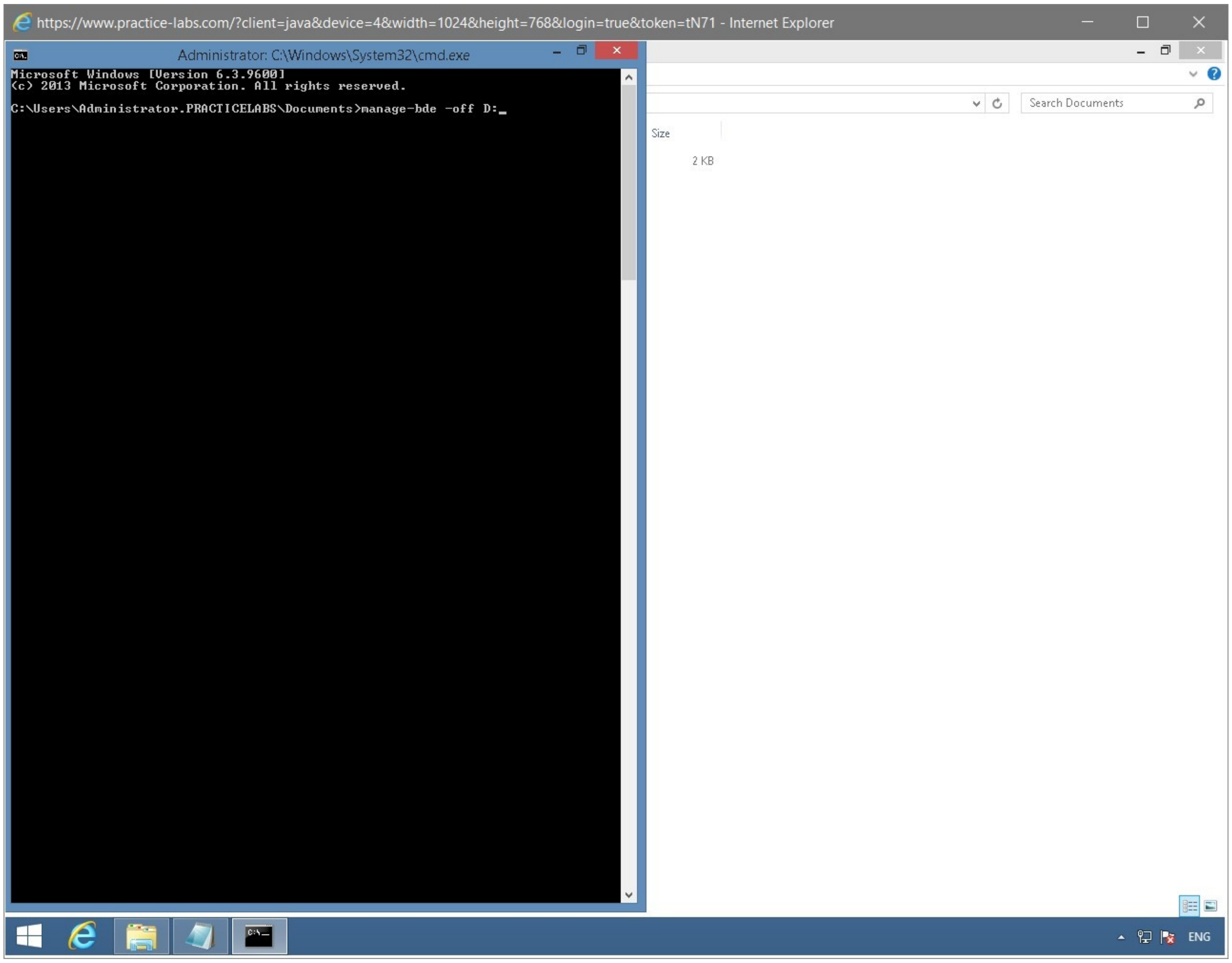
Figure 1.66 Screenshot of the PLABWIN810 desktop: File explorer window is displayed showing the required command typed in the address bar at the top.

Step 2

On the command prompt window, to decrypt **Volume D** type the following:

```
manage-bde -off D:
```

Press **Enter**.



https://www.practice-labs.com/?client=java&device=4&width=1024&height=768&login=true&token=tN71 - Internet Explorer
Administrator: C:\Windows\System32\cmd.exe
Search Documents
Size
2 KB
ENG

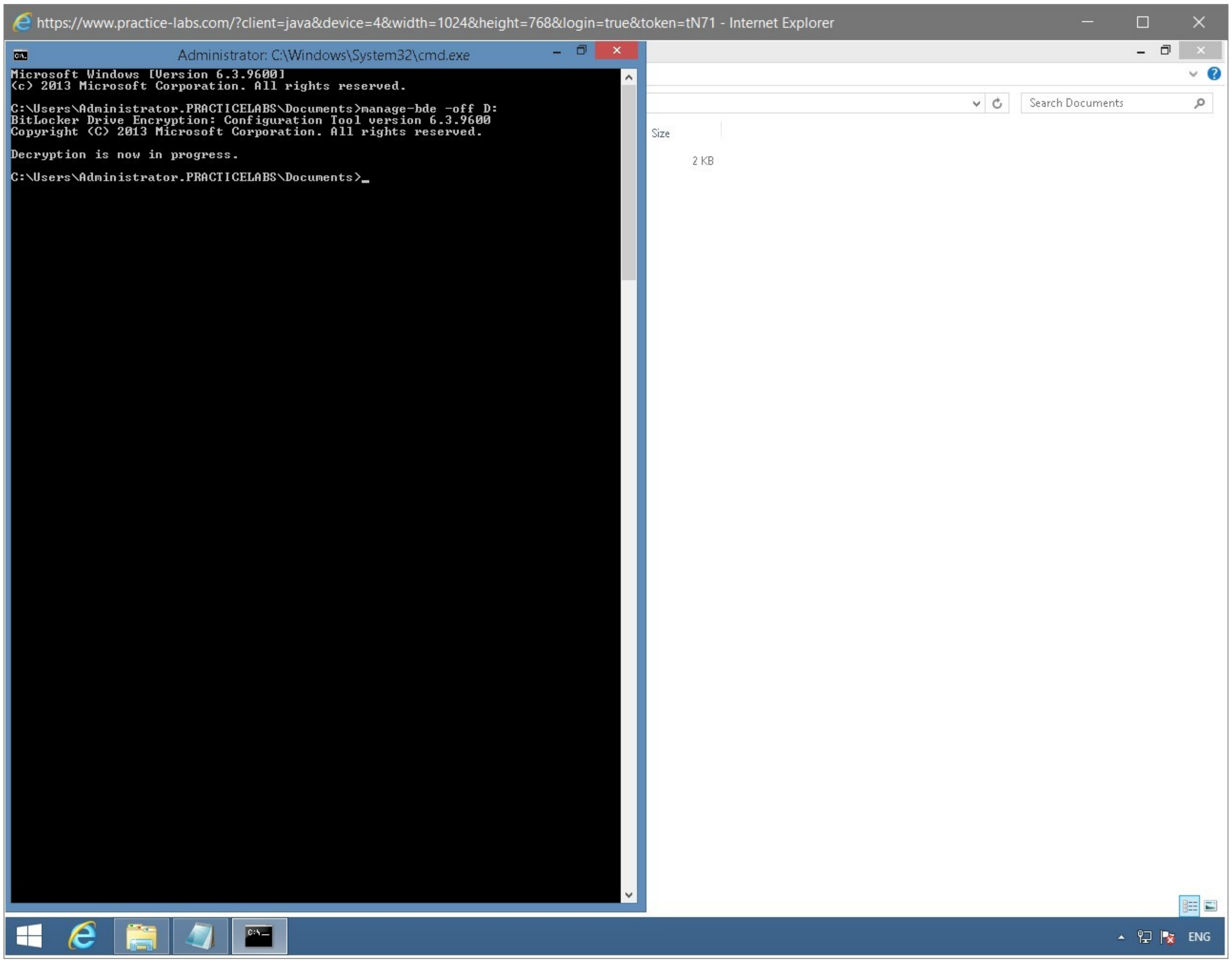
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.PRACTICELABS\Documents>manage-bde -off D:_
```

Figure 1.67 Screenshot of the PLABWIN810 desktop: Administrator: C:\Windows\System32\cmd.exe window is displayed showing the command to manage the bitlocked device typed-in.

Step 3

The system will now indicate that decryption is in progress.

This process will take a few minutes to finish.



https://www.practice-labs.com/?client=java&device=4&width=1024&height=768&login=true&token=tN71 - Internet Explorer
Administrator: C:\Windows\System32\cmd.exe
Search Documents
Size
2 KB
ENG

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.PRACTICELABS\Documents>manage-bde -off D:
BitLocker Drive Encryption: Configuration Tool version 6.3.9600
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Decryption is now in progress.

C:\Users\Administrator.PRACTICELABS\Documents>_
```

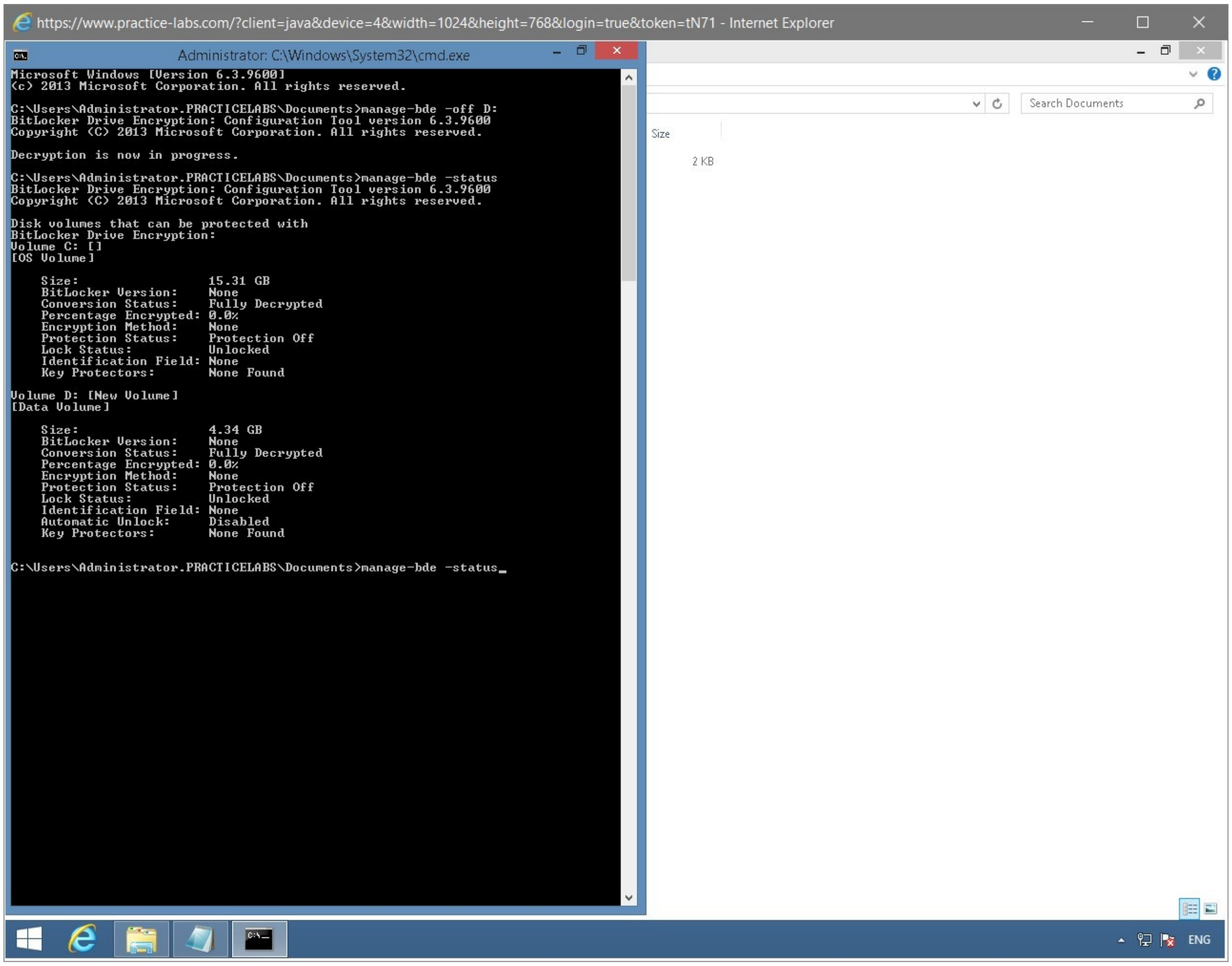
Figure 1.68 Screenshot of the PLABWIN810 desktop: Administrator: C:\Windows\System32\cmd.exe window is displayed indicating that decryption is in progress.

Step 4

To verify the status of Drive D, type:

```
Manage-bde -status
```

Press **Enter**.



https://www.practice-labs.com/?client=java&device=4&width=1024&height=768&login=true&token=tN71 - Internet Explorer
Administrator: C:\Windows\System32\cmd.exe
Search Documents
Size
2 KB
ENG

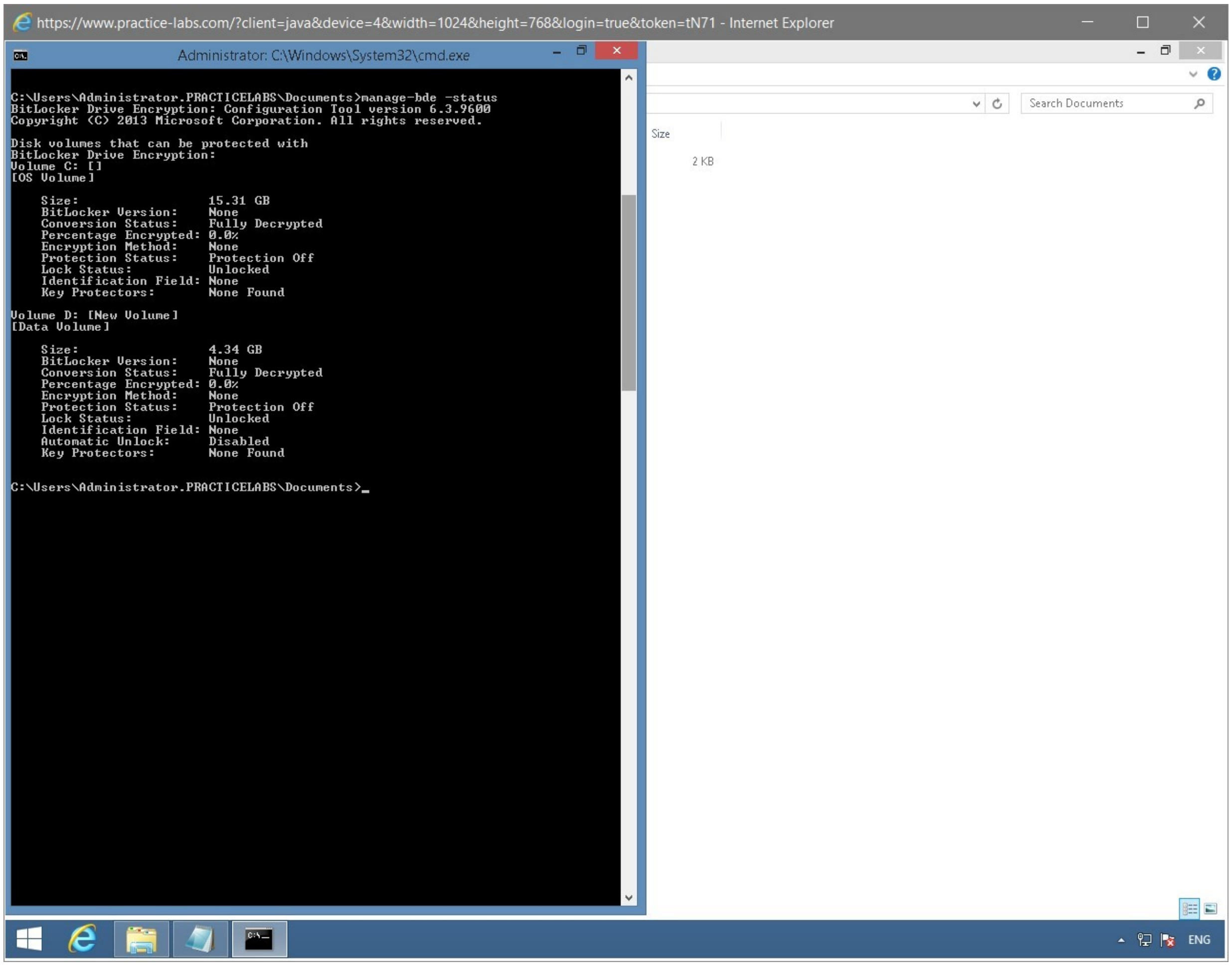
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.PRACTICELABS\Documents>manage-bde -off D:
BitLocker Drive Encryption: Configuration Tool version 6.3.9600
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Decryption is now in progress.

C:\Users\Administrator.PRACTICELABS\Documents>manage-bde -status
BitLocker Drive Encryption: Configuration Tool version 6.3.9600
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Disk volumes that can be protected with
BitLocker Drive Encryption:
Volume C: []
[OS Volume]

    Size:                 15.31 GB
    BitLocker Version:    None
    Conversion Status:    Fully Decrypted
    Percentage Encrypted: 0.0%
    Encryption Method:    None
    Protection Status:    Protection Off
    Lock Status:          Unlocked
    Identification Field: None
    Key Protectors:       None Found

Volume D: [New Volume]
[Data Volume]

    Size:                 4.34 GB
    BitLocker Version:    None
    Conversion Status:    Fully Decrypted
    Percentage Encrypted: 0.0%
    Encryption Method:    None
    Protection Status:    Protection Off
    Lock Status:          Unlocked
    Identification Field: None
    Automatic Unlock:     Disabled
    Key Protectors:       None Found


C:\Users\Administrator.PRACTICELABS\Documents>manage-bde -status_
```

Figure 1.69 Screenshot of the PLABWIN810 desktop: Administrator: C:\Windows\System32\cmd.exe window is displayed showing the command to verify the encryption status of drive D: typed-in.

Step 5

The output of the **manage-bde** command is displayed.

On the following screen, the **Volumes D** and **C** are **Fully Decrypted**.



https://www.practice-labs.com/?client=java&device=4&width=1024&height=768&login=true&token=tN71 - Internet Explorer
Administrator: C:\Windows\System32\cmd.exe
Search Documents
Size
2 KB
ENG

```
C:\Users\Administrator.PRACTICELABS\Documents>manage-bde -status
BitLocker Drive Encryption: Configuration Tool version 6.3.9600
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Disk volumes that can be protected with
BitLocker Drive Encryption:
Volume C: []
[OS Volume]

    Size:                 15.31 GB
    BitLocker Version:    None
    Conversion Status:    Fully Decrypted
    Percentage Encrypted: 0.0%
    Encryption Method:    None
    Protection Status:    Protection Off
    Lock Status:          Unlocked
    Identification Field: None
    Key Protectors:       None Found

Volume D: [New Volume]
[Data Volume]

    Size:                 4.34 GB
    BitLocker Version:    None
    Conversion Status:    Fully Decrypted
    Percentage Encrypted: 0.0%
    Encryption Method:    None
    Protection Status:    Protection Off
    Lock Status:          Unlocked
    Identification Field: None
    Automatic Unlock:     Disabled
    Key Protectors:       None Found


C:\Users\Administrator.PRACTICELABS\Documents>_
```

Figure 1.70 Screenshot of the PLABWIN810 desktop: Administrator: C:\Windows\System32\cmd.exe window is displayed showing system-response to the command typed-in in the previous step.

Step 6

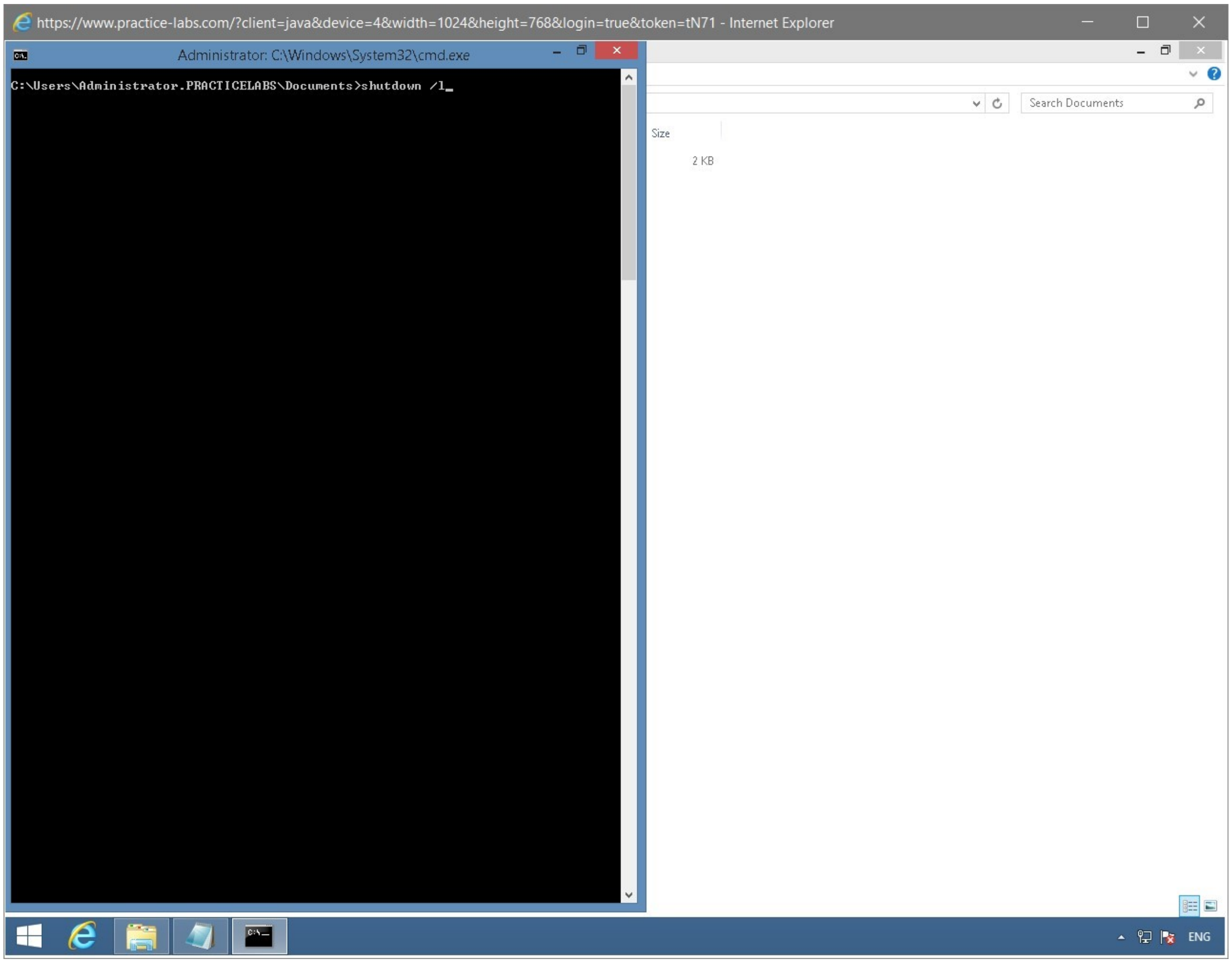
Clear the screen using the following command:

```
 cls
```

To sign out of **PLABWIN810**, type:

```
shutdown /l
```

Press **Enter**.


https://www.practice-labs.com/?client=java&device=4&width=1024&height=768&login=true&token=tN71 - Internet Explorer
Administrator: C:\Windows\System32\cmd.exe
Search Documents
Size
2 KB
ENG

```
C:\Users\Administrator.PRACTICELABS\Documents>shutdown /l_
```

Figure 1.71 Screenshot of the PLABWIN810 desktop: Administrator: C:\Windows\System32\cmd.exe window is displayed showing the command to shutdown the server typed-in.

Leave the devices you have powered on in their current state and proceed to the next exercise.

Exercise 2 - Manage Security for Removable Media

For security reasons, most organizations will prohibit their users from using personal storage devices for transporting proprietary information. This is to avoid theft of confidential data that may put the company's trade secrets at risk. In this exercise, you will configure basic security for portable storage media to disallow their usage by configuring Group Policy Objects or GPO.

To get a better understanding of this technology, please refer to your course material or use your preferred search engine to research this topic in more detail.

Task 1 - Configure restrictions for removable media using GPO

To prevent users from using portable media to save their data files, perform the following steps:

Step 1

Switch back to **PLABDC01** device.

From **Server Manager Dashboard**, go to **Tools > Group Policy Management.**

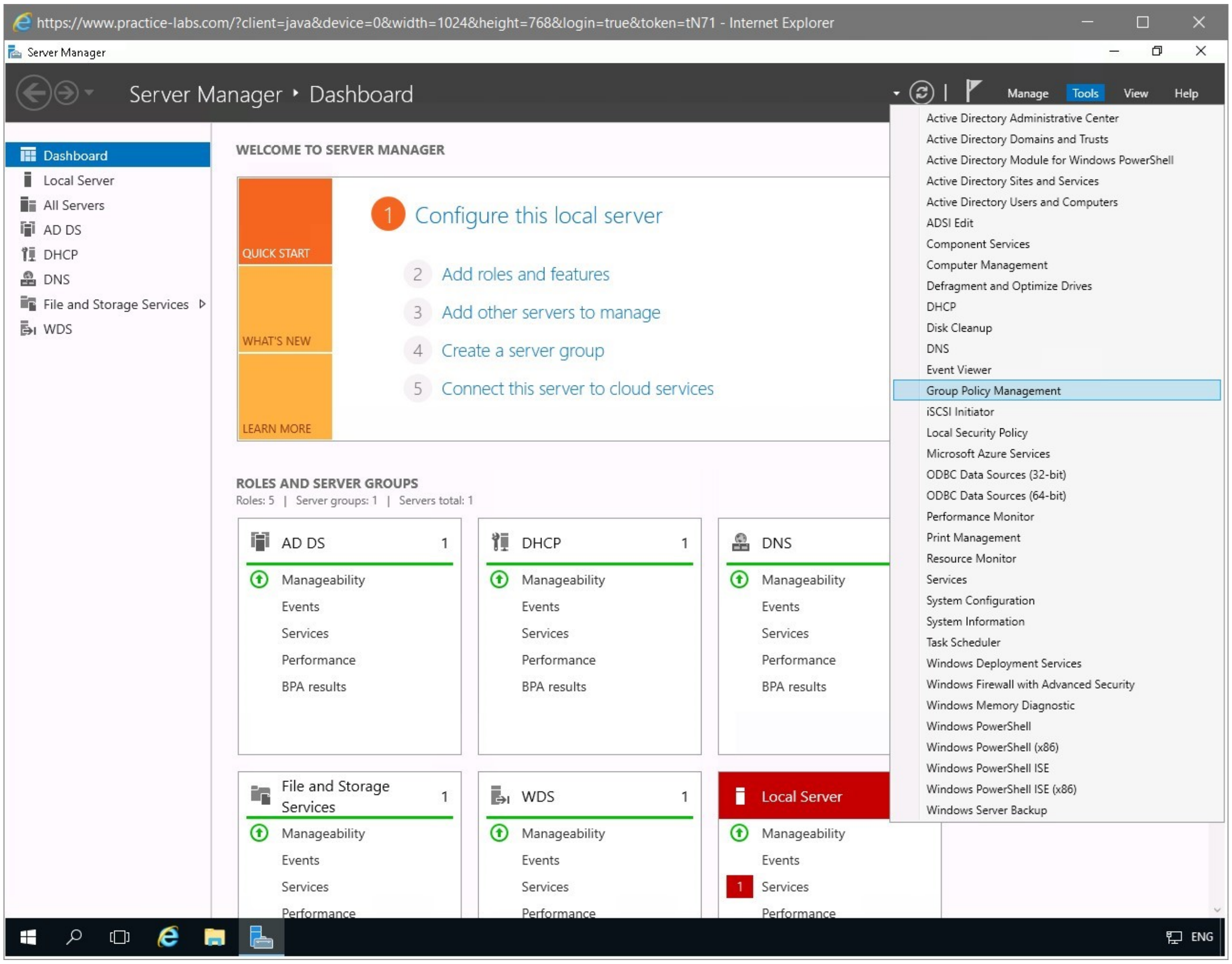
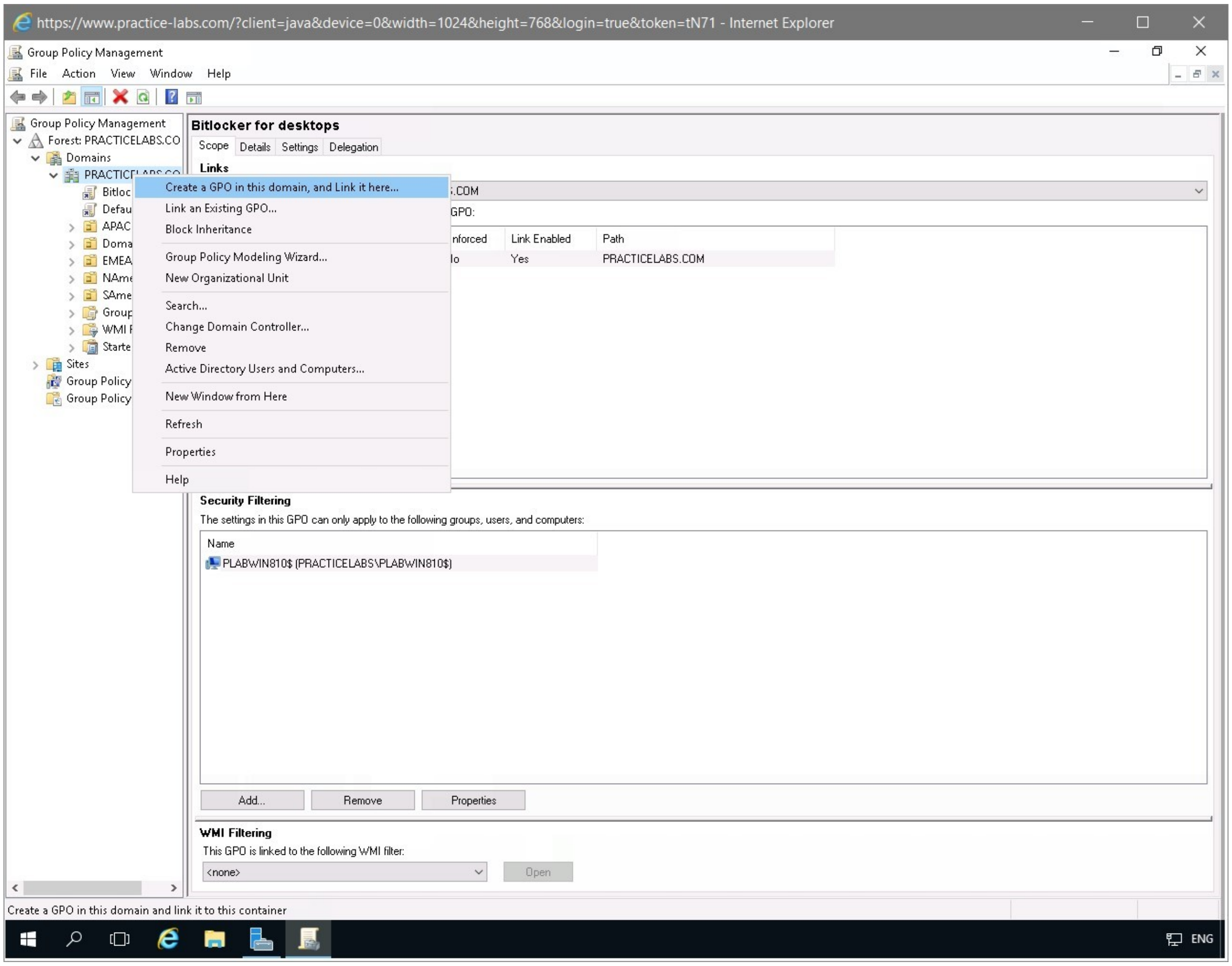

https://www.practice-labs.com/?client=java&device=0&width=1024&height=768&login=true&token=tN71 - Internet Explorer
Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DHCP
DNS
File and Storage Services
WDS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
ROLES AND SERVER GROUPS
Roles: 5 | Server groups: 1 | Servers total: 1
AD DS 1
DHCP 1
DNS
File and Storage Services 1
WDS 1
Local Server
Manageability
Events
Services
Performance
BPA results
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
DHCP
Disk Cleanup
DNS
Event Viewer
Group Policy Management
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Print Management
Resource Monitor
Services
System Configuration
System Information
Task Scheduler
Windows Deployment Services
Windows Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell
Windows PowerShell (x86)
Windows PowerShell ISE
Windows PowerShell ISE (x86)
Windows Server Backup
ENG

Figure 2.1 Screenshot of the PLABDC01 desktop: Tools > Group Policy Management menu-options are highlighted on the Server Manager Dashboard window.

Step 2

On the **Group Policy Management** console, expand **Forest: PRACTICELABS.COM**, then expand **Domains** if already not expanded.

Right-click **PRACTICELABS.COM** and select **Create a GPO in this domain, and link it here**.



Bitlocker for desktops

Links

.COM

GPO:

nforced	Link Enabled	Path
lo	Yes	PRACTICELABS.COM

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
PLABWIN810$ (PRACTICELABS\PLABWIN810$)

WMI Filtering

This GPO is linked to the following WMI filter:

<none>

Create a GPO in this domain and link it to this container

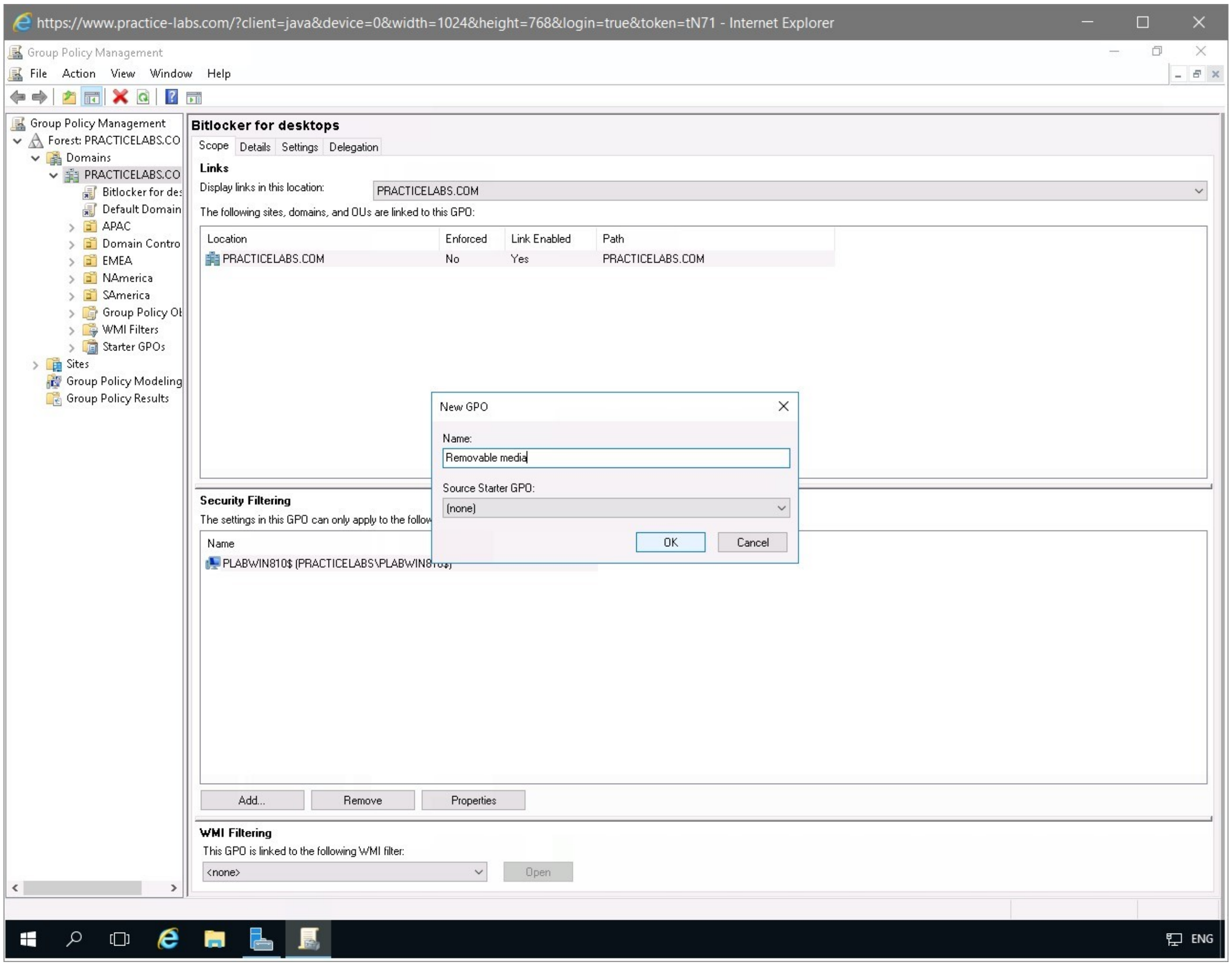
Figure 2.2 Screenshot of the PLABDC01 desktop: Context menu (that appears on right-clicking a domain name) > Create a GPO in this domain, and link it here menu-options are displayed on the Group Policy Management console.

Step 3

On the **New GPO** dialog box, type:

```
Removable media
```

Click **OK**.



Display links in this location: PRACTICELABS.COM

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
PRACTICELABS.COM	No	Yes	PRACTICELABS.COM

Name
PLABWIN810$ (PRACTICELABS\PLABWIN810$)

This GPO is linked to the following WMI filter: <none>

New GPO

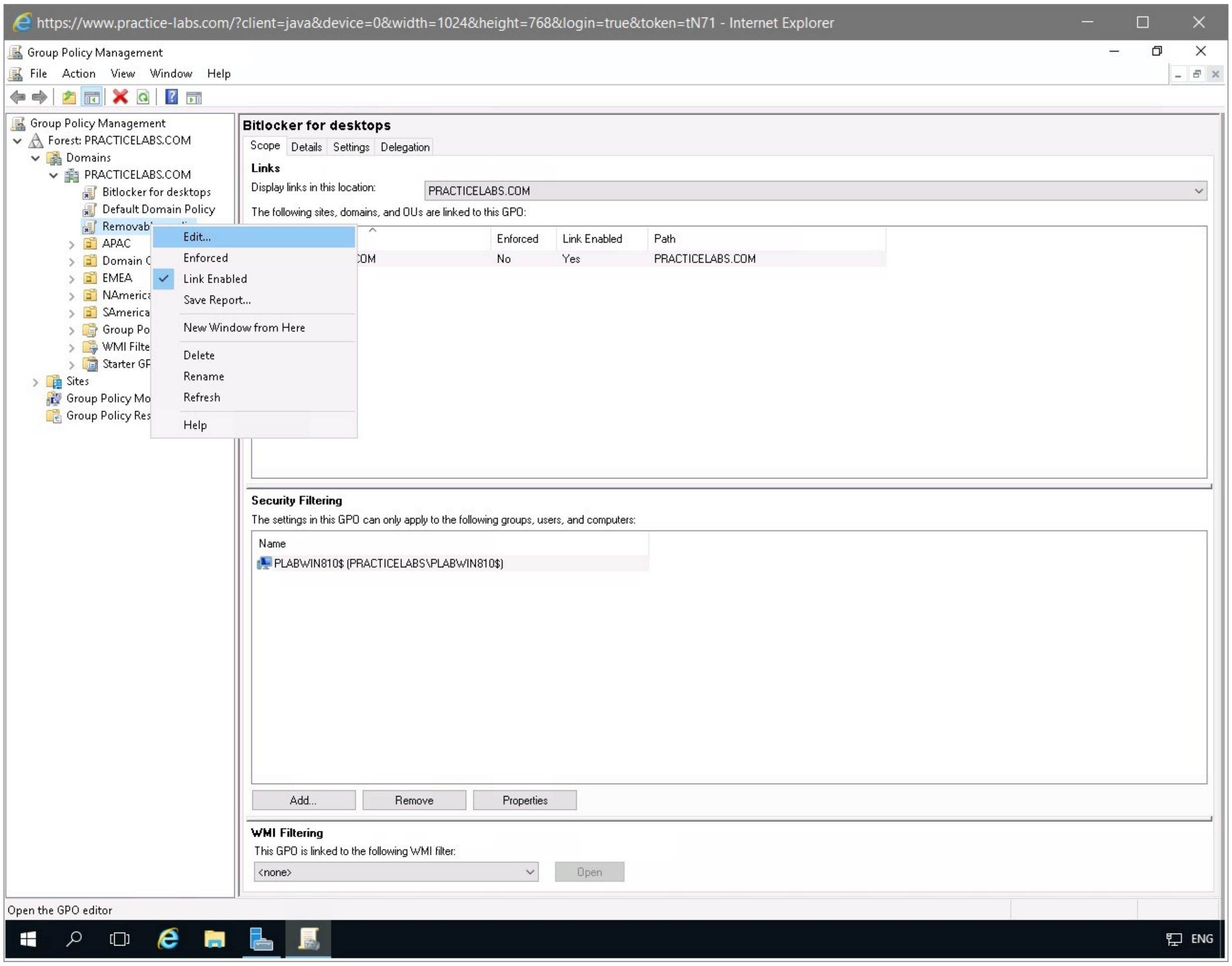
Name: Removable media

Source Starter GPO: (none)

Figure 2.3 Screenshot of the PLABDC01 desktop: New GPO dialog box is displayed showing the required value typed-in and the OK button highlighted.

Step 4

Right-click **Removable media** and select **Edit**.



Bitlocker for desktops

Links

Display links in this location: PRACTICELABS.COM

The following sites, domains, and OUs are linked to this GPO:

	Enforced	Link Enabled	Path
COM	No	Yes	PRACTICELABS.COM

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
PLABWIN810$ (PRACTICELABS\PLABWIN810$)

WMI Filtering

This GPO is linked to the following WMI filter:

<none>

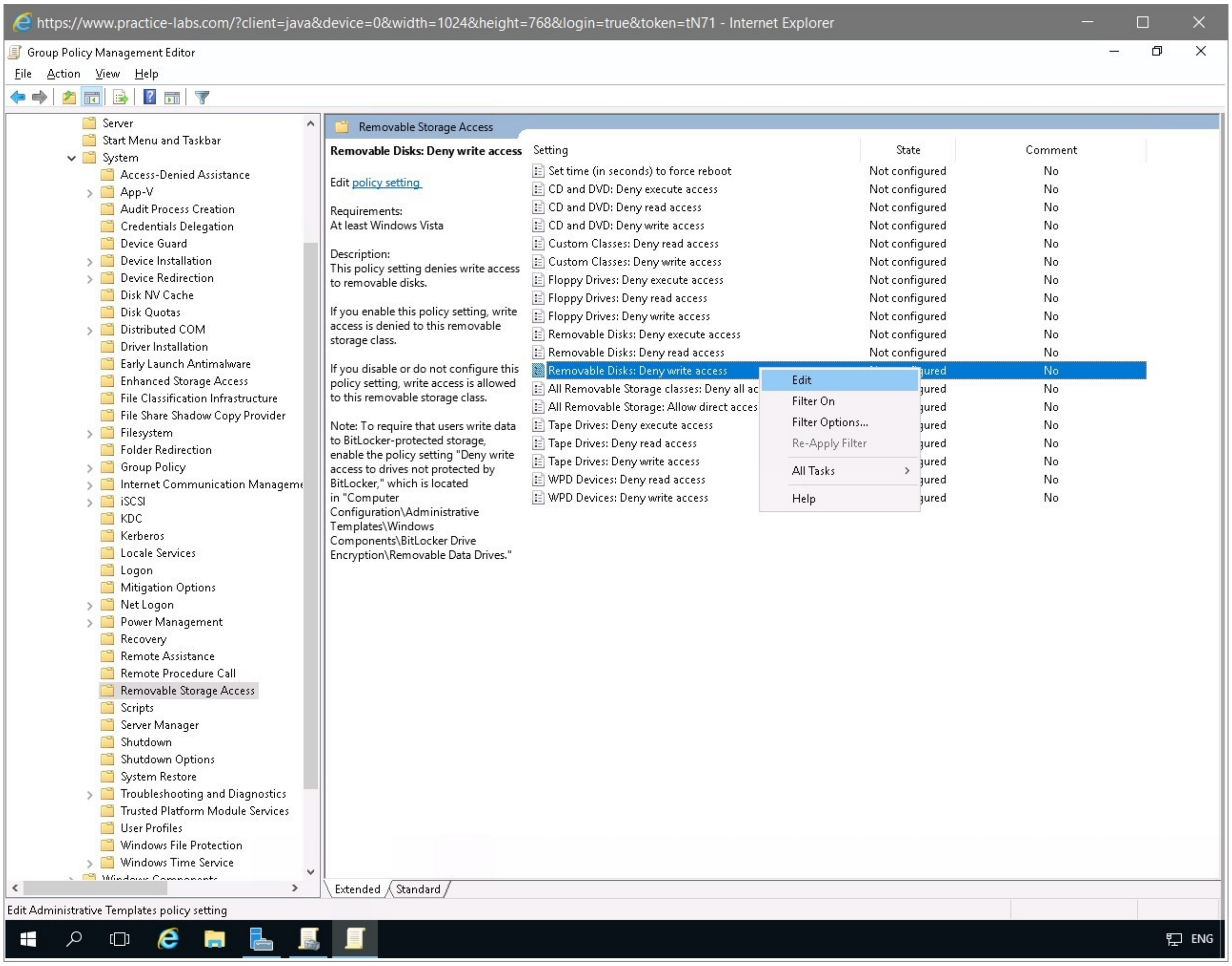
Open the GPO editor

Figure 2.4 Screenshot of the PLABDC01 desktop: Context menu (that appears on right-clicking the Removeable media node) > Edit menu-options are displayed on the Group Policy Management console.

Step 5

On the **Group Policy Management Editor** window, navigate to **Computer Configuration > Policies > Administrative Templates > System** and select **Removable Storage Access**.

On the details pane on the right side, right-click on **Removable Disks: Deny write access** and select **Edit**.



Removable Disks: Deny write access

Edit policy setting

Requirements:
At least Windows Vista

Description:
This policy setting denies write access to removable disks.

If you enable this policy setting, write access is denied to this removable storage class.

If you disable or do not configure this policy setting, write access is allowed to this removable storage class.

Note: To require that users write data to BitLocker-protected storage, enable the policy setting "Deny write access to drives not protected by BitLocker," which is located in "Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives."

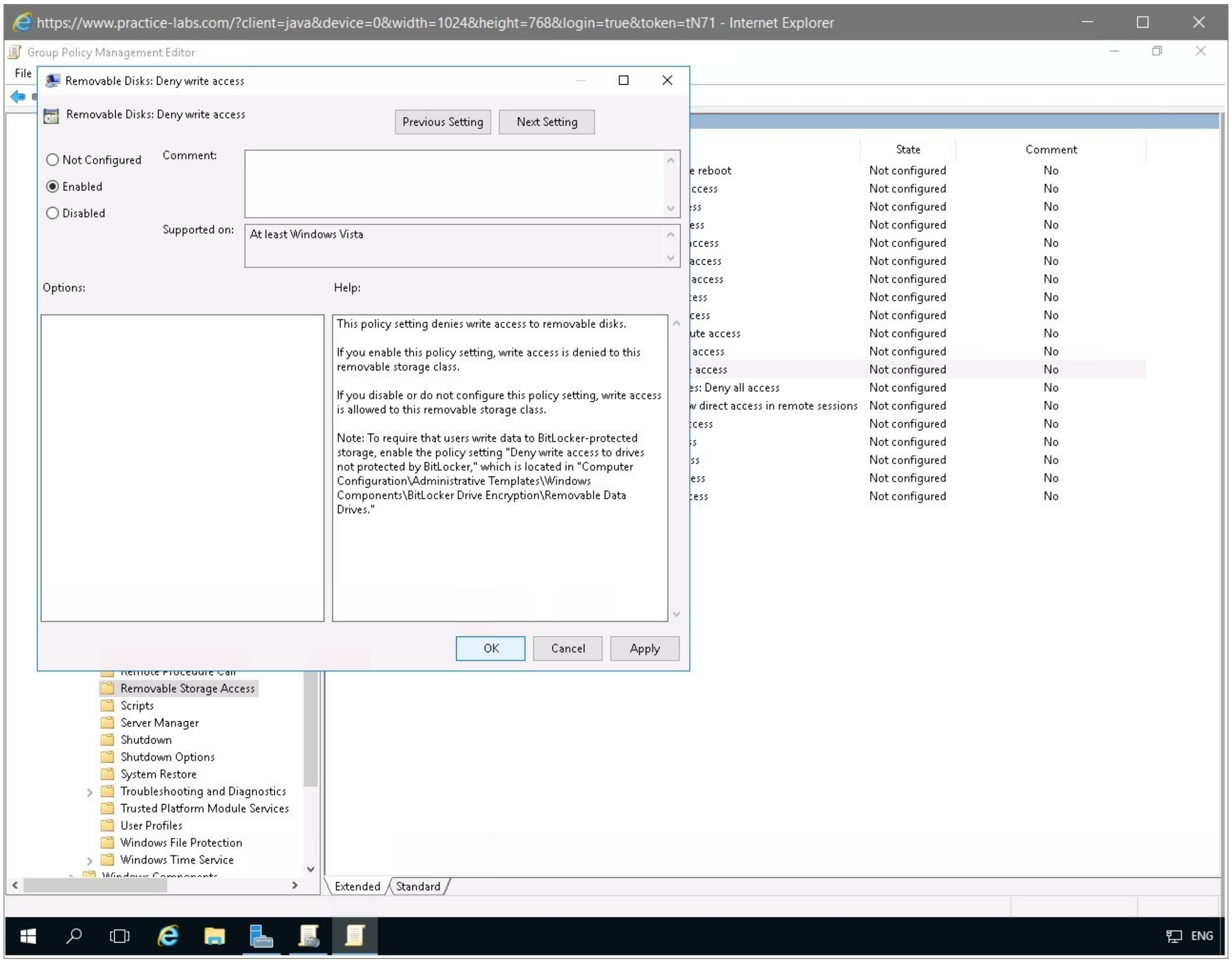
Setting	State	Comment
Set time (in seconds) to force reboot	Not configured	No
CD and DVD: Deny execute access	Not configured	No
CD and DVD: Deny read access	Not configured	No
CD and DVD: Deny write access	Not configured	No
Custom Classes: Deny read access	Not configured	No
Custom Classes: Deny write access	Not configured	No
Floppy Drives: Deny execute access	Not configured	No
Floppy Drives: Deny read access	Not configured	No
Floppy Drives: Deny write access	Not configured	No
Removable Disks: Deny execute access	Not configured	No
Removable Disks: Deny read access	Not configured	No
Removable Disks: Deny write access	gured	No
All Removable Storage classes: Deny all ac	gured	No
All Removable Storage: Allow direct acces	gured	No
Tape Drives: Deny execute access	gured	No
Tape Drives: Deny read access	gured	No
Tape Drives: Deny write access	gured	No
WPD Devices: Deny read access	gured	No
WPD Devices: Deny write access	gured	No

Figure 2.5 Screenshot of the PLABDC01 desktop: Context menu (that appears on right-clicking a listed policy setting) > Edit menu-options are displayed on the Group Policy Management Editor console.

Step 6

From the **Removable Disks: Deny write access** dialog box, select **Enabled**.

Click **OK**.



https://www.practice-labs.com/?client=java&device=0&width=1024&height=768&login=true&token=tN71 - Internet Explorer
Group Policy Management Editor
File
Removable Disks: Deny write access
Previous Setting
Next Setting
OK
Cancel
Apply
State
Comment
Removable Storage Access
Scripts
Server Manager
Shutdown
Shutdown Options
System Restore
Troubleshooting and Diagnostics
Trusted Platform Module Services
User Profiles
Windows File Protection
Windows Time Service
Extended
Standard
ENG

Removable Disks: Deny write access

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

Help:

This policy setting denies write access to removable disks.

If you enable this policy setting, write access is denied to this removable storage class.

If you disable or do not configure this policy setting, write access is allowed to this removable storage class.

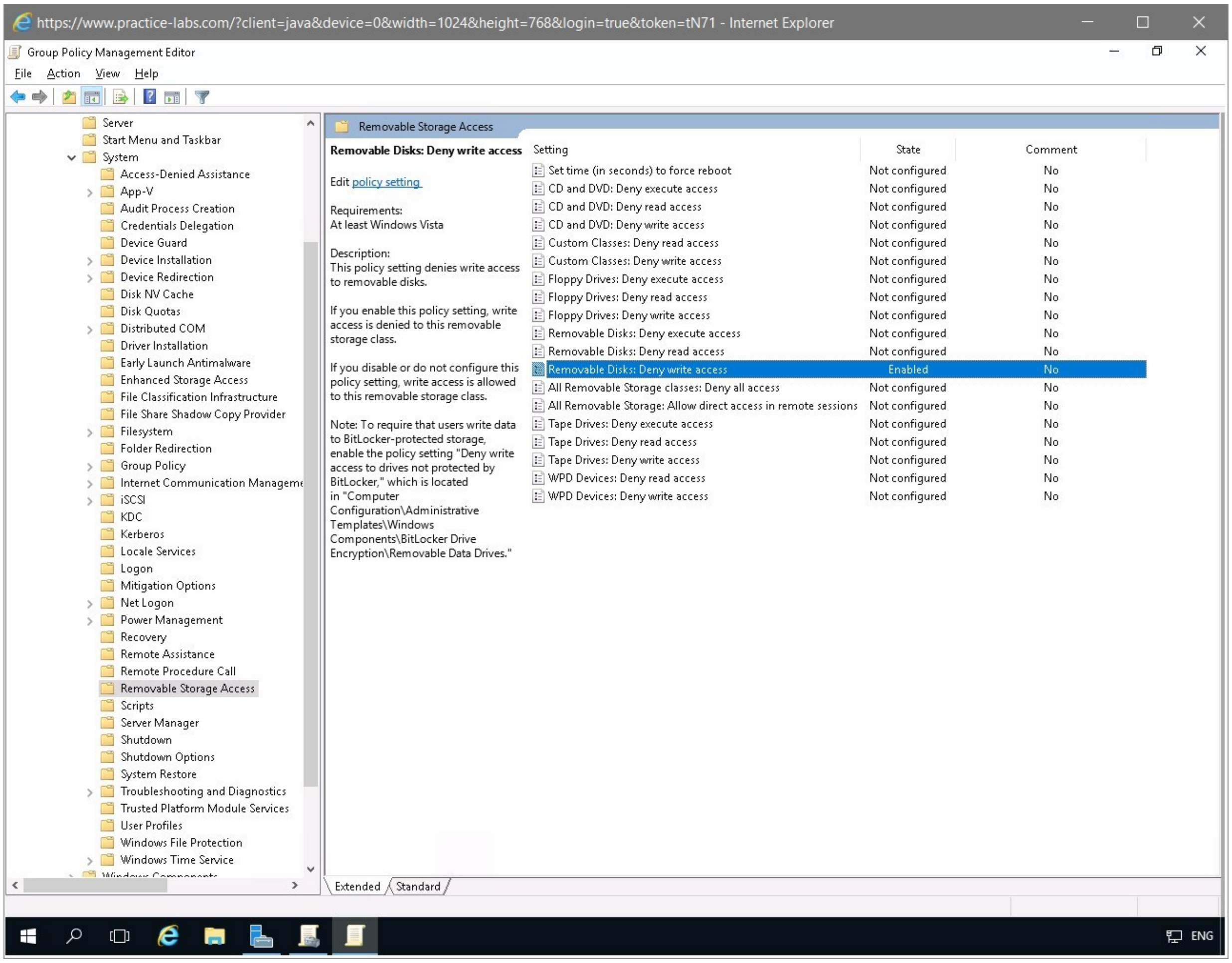
Note: To require that users write data to BitLocker-protected storage, enable the policy setting "Deny write access to drives not protected by BitLocker," which is located in "Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives."

Figure 2.6 Screenshot of the PLABDC01 desktop: Removeable Disks: Deny write access console is displayed showing the required settings performed and the OK button highlighted.

Step 7

Close **Group Policy Management Editor** and **Group Policy Management console**.

> ***Note***: *Due to the system limitations of this lab, it will not show the actual policy of blocking removable storage on the devices.*



Removable Disks: Deny write access

Edit policy setting

Requirements:
At least Windows Vista

Description:
This policy setting denies write access to removable disks.

If you enable this policy setting, write access is denied to this removable storage class.

If you disable or do not configure this policy setting, write access is allowed to this removable storage class.

Note: To require that users write data to BitLocker-protected storage, enable the policy setting "Deny write access to drives not protected by BitLocker," which is located in "Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives."

Setting	State	Comment
Set time (in seconds) to force reboot	Not configured	No
CD and DVD: Deny execute access	Not configured	No
CD and DVD: Deny read access	Not configured	No
CD and DVD: Deny write access	Not configured	No
Custom Classes: Deny read access	Not configured	No
Custom Classes: Deny write access	Not configured	No
Floppy Drives: Deny execute access	Not configured	No
Floppy Drives: Deny read access	Not configured	No
Floppy Drives: Deny write access	Not configured	No
Removable Disks: Deny execute access	Not configured	No
Removable Disks: Deny read access	Not configured	No
Removable Disks: Deny write access	Enabled	No
All Removable Storage classes: Deny all access	Not configured	No
All Removable Storage: Allow direct access in remote sessions	Not configured	No
Tape Drives: Deny execute access	Not configured	No
Tape Drives: Deny read access	Not configured	No
Tape Drives: Deny write access	Not configured	No
WPD Devices: Deny read access	Not configured	No
WPD Devices: Deny write access	Not configured	No

Figure 2.7 Screenshot of the PLABDC01 desktop: Group Policy Management Editor console is

displayed showing the Close icon at the top-right corner available.

Shutdown all virtual machines used in this lab, before proceeding to the next module. Alternatively you can log out of the lab platform.

Summary

In this lab you learned the following skills:

- Full Disk Encryption using Bitlocker
- Configure Security for Removable Media