24 - Implement Azure Information Protection

Introduction

Modern Desktops
Azure AD
Office 365
Custom Label
Confidential Label
AIP Policy

Welcome to the **Implement Azure Information Protection** Practice Lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

> ***Note:*** *Microsoft Edge has been updated to the latest version to keep in line with all the technology changes with Azure and Microsoft 365 platforms. Hence the Edge icon and screenshots may differ slightly to the experience in the lab environment.*

Learning Outcomes

In this module, you will complete the following exercises:

- Exercise 1 - Configure Prerequisites for Azure Information Protection
- Exercise 2 - Implement Azure Information Protection Labels

After completing this lab, you will be able to:

- Remove Device from Azure AD
- Remove Domain Computer from Active Directory
- Join the Computer to Azure AD
- Generate Default Policies and Labels
- Migrate AIP Labels to Office 365 Security and Compliance Center
- Create a Custom Label
- Edit the Confidential Label
- Publish the Labels
- Install Azure Information Protection Client Unified Labeling
- Enable Remote Desktop
- Configure Proxy Server Settings for a New User
- Verify AIP Policy

Exam Objectives

The following exam objectives are covered in this lab:

- Implement mobile application management - Implement Azure Information Protection templates

Alert: To be able to complete this Practice Lab successfully, a free 30-day Microsoft Office 365 account needs to be created. This account will be used to complete specific tasks in the lab.

To create a free trial account, please use the following link:

https://www.microsoft.com/en-us/microsoft-365/business/office-365-enterprise-e5-business-

software?activetab=pivot%3aoverviewtab ***Note:** Our main focus is to cover the practical, hands-on aspects of the exam objectives. We recommend referring to course material or a search engine to research theoretical topics in more detail.*

Lab Duration

It will take approximately **1 hour** to complete this lab.

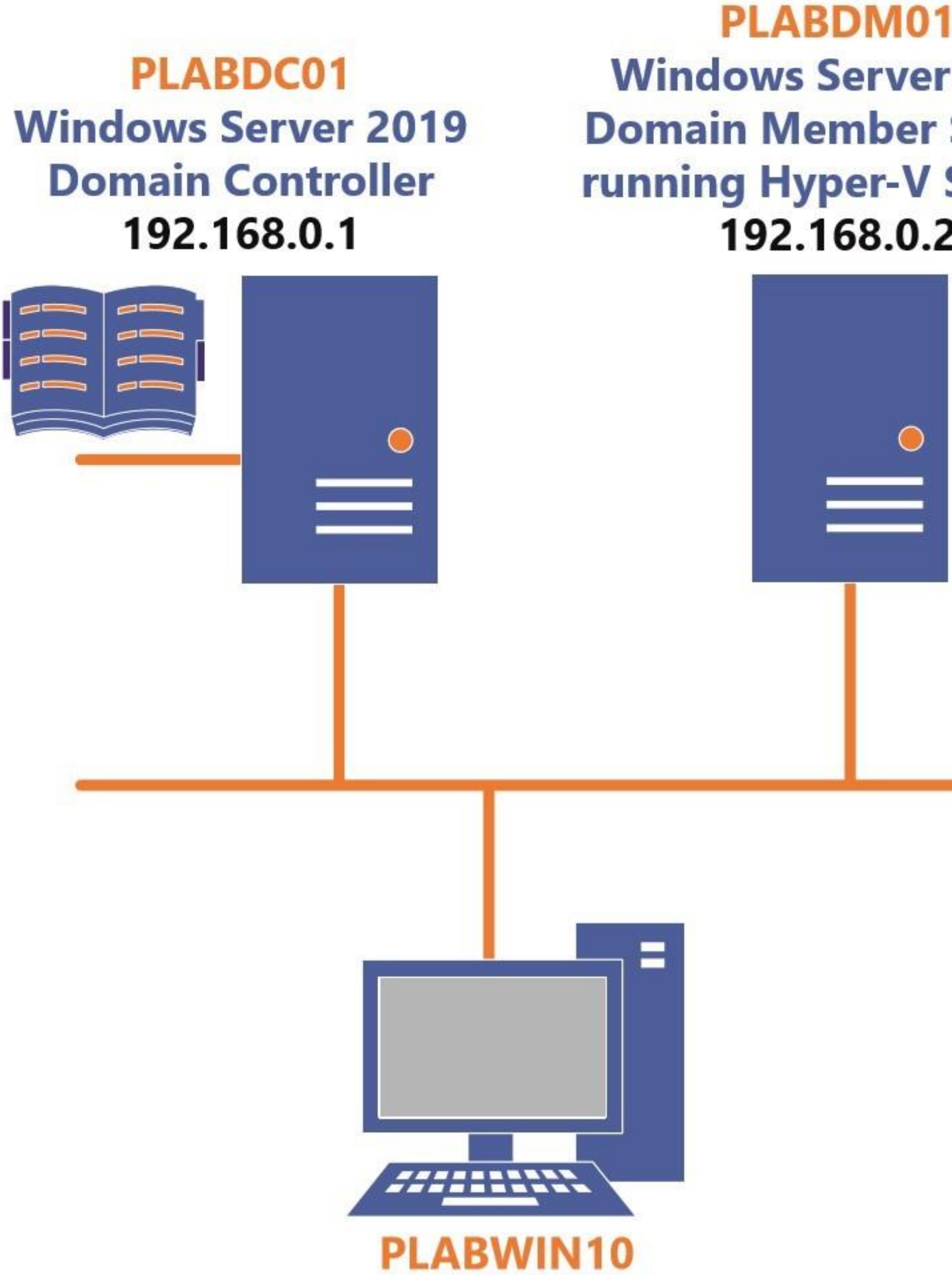
Help and Support

For more information on using Practice Labs, please see our **Help and Support** page. You can also raise a technical support ticket from this page.

Click **Next** to view the Lab topology used in this module.

Lab Topology

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


PLABDC01
Windows Server 2019
Domain Controller
192.168.0.1
PLABDM01
Windows Server
Domain Member
running Hyper-V
192.168.0.2
PLABWIN10

Depending on the exercises, you may or may not use all of the devices, but they are shown here in the layout to get an overall understanding of the topology of the lab.

- **PLABDC01 -** (Windows Server 2019 - Domain Controller)
- **PLABDM01 -** (Windows Server 2019 - Domain Member Server, running Hyper-V Service)
- **PLABDM02 -** (Windows Server 2019 - Domain Member Server, running Windows Deployment Services)
- **PLABWIN10 -** (Windows 10 Enterprise - Domain Member Workstation)
- **PLABWIN810 -** (Windows 8.1 Enterprise - Domain Member Workstation)

Click **Next** to proceed to the first exercise.

Exercise 1 - Configure Prerequisites for Azure Information Protection

The disclosure of proprietary information to unauthorized parties is a risk that is addressed with the use of technologies like encryption, signed e-mail, and password-protected files. These encryption methods require the use of certificates from issuing authorities called a public key infrastructure. Managing a PKI service calls for administrative overhead as it entails the management of certificates for users and external users. Also, end-user training is a requirement to ensure that employees make informed decisions on whether to apply for document protection or otherwise when managing work-related files.

Azure Information Protection included in Microsoft 365 Business Premium or Azure Premium P1 subscription provides the framework to classify user-created documents and apply for protection.

This exercise will demonstrate how to prepare a Windows 10 computer by removing it from a local Active Directory domain and joining it to Azure AD. This is a requirement as you will sign in to an Azure AD tenant where the Azure Information Protection template will be created in another activity.

To learn more about preparing the prerequisites for Azure Information Protection, please refer to your course material or use your favorite search engine to research for more information about this topic.

Learning Outcomes

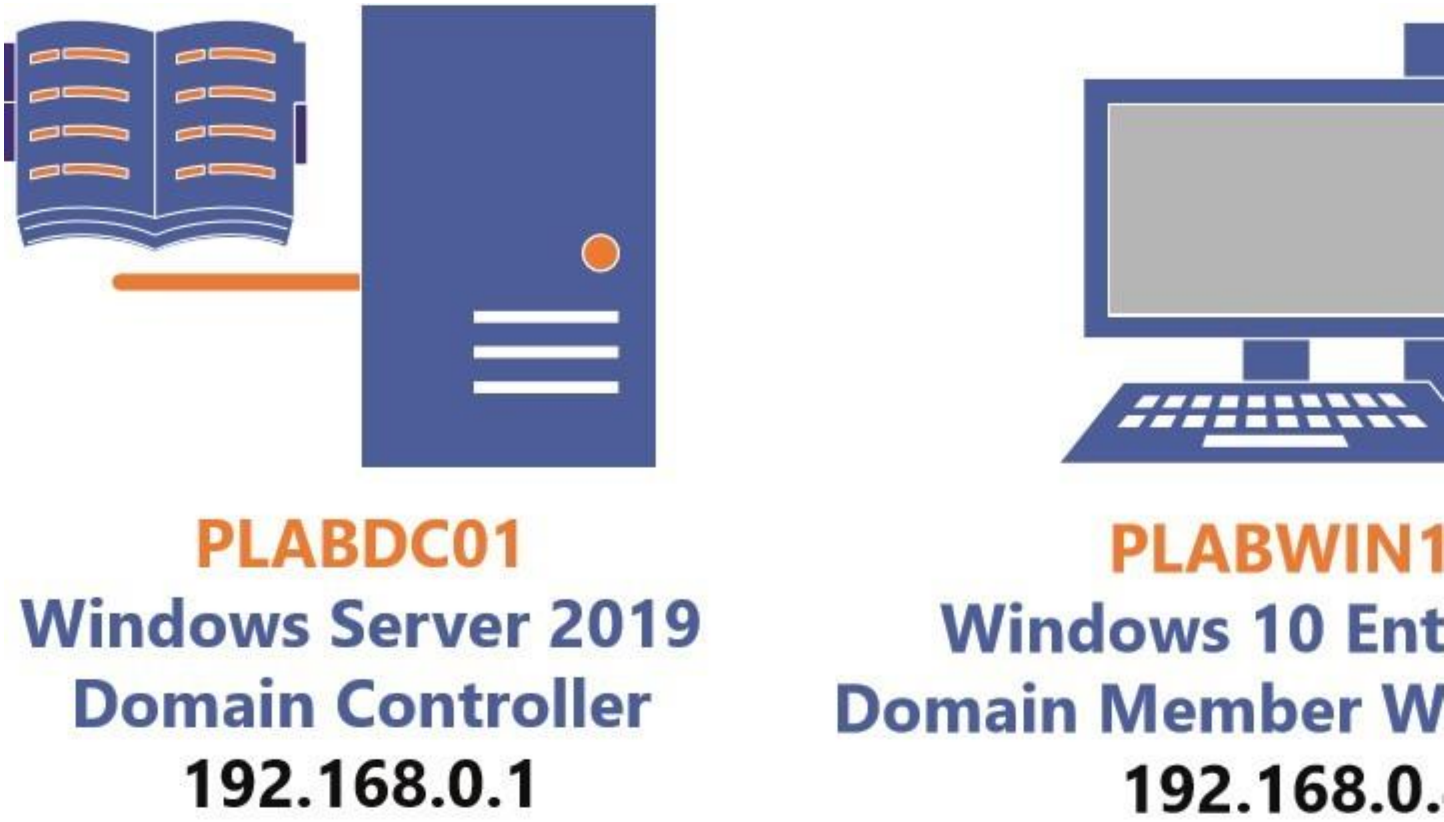
After completing this exercise, you will be able to:

- Remove Device from Azure AD
- Remove Domain Computer from Active Directory
- Join the Computer to Azure AD

Your Devices

You will be using the following devices in this lab. Please power these on now.

- **PLABDC01 -** (Windows Server 2019 - Domain Controller)
- **PLABWIN10 -** (Windows 10 Enterprise - Domain Member Workstation)



Task 1 - Remove Device from Azure AD

In this task, you will remove devices that you have added in the earlier exercises of this MD-101 lab. Please note that when you sign out of Practice Labs platform, devices rollback to their default settings and subsequently remove all system changes made while working on the exercises.

This task is essential to prevent errors about Azure AD, reaching the maximum limit of devices joined in the directory. Likewise, this will prevent errors, as devices are configured to receive deployed apps in Intune.

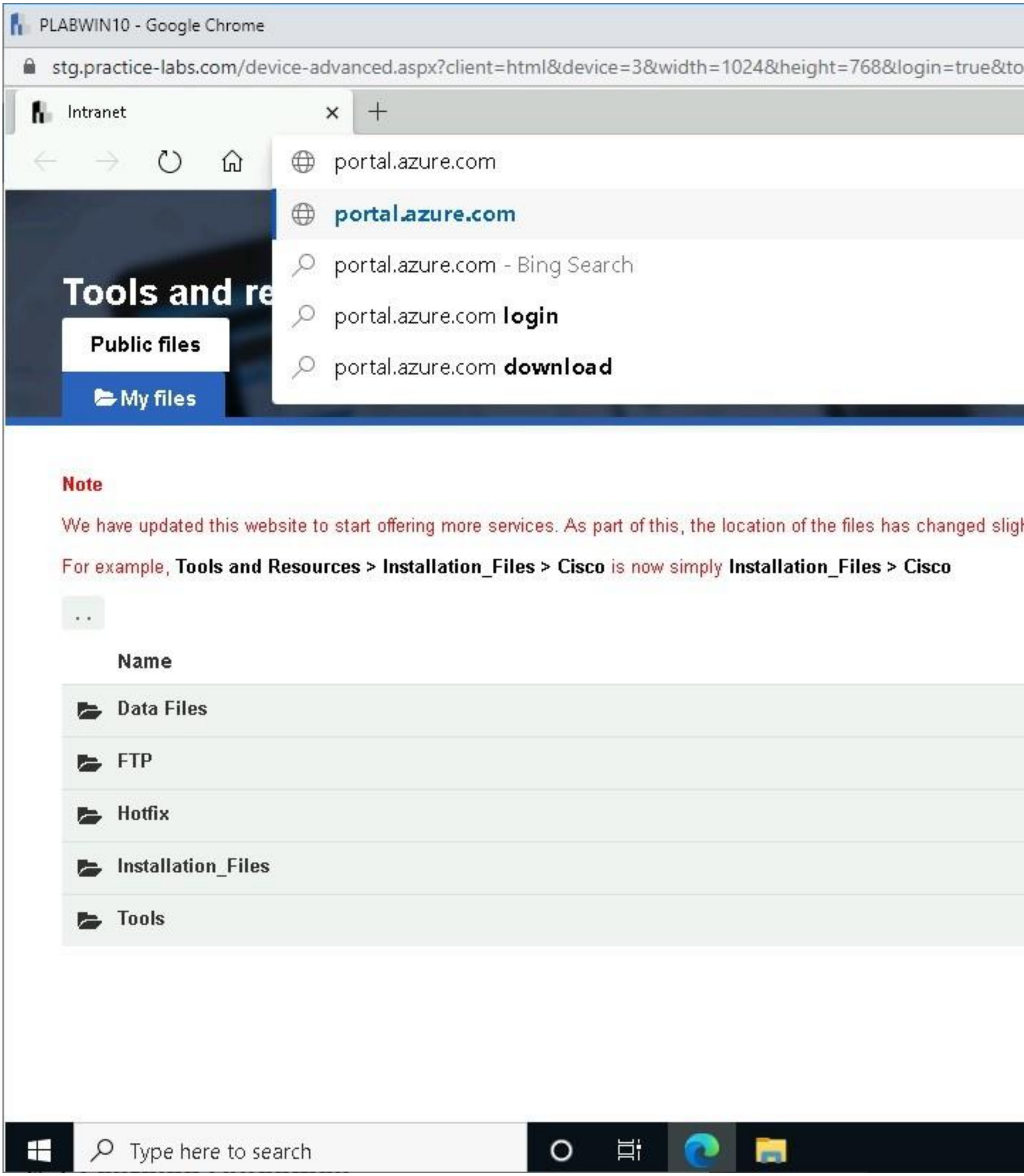
Step 1

Click Microsoft Edge on the taskbar.

Click in the browser’s address bar and type:

https://portal.azure.com

Press **Enter**.



stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&to

portal.azure.com

portal.azure.com

portal.azure.com - Bing Search

portal.azure.com **login**

portal.azure.com **download**

Note

We have updated this website to start offering more services. As part of this, the location of the files has changed sligh

For example, **Tools and Resources > Installation_Files > Cisco** is now simply **Installation_Files > Cisco**

..

Name
Data Files
FTP
Hotfix
Installation_Files
Tools

Figure 1.1 Screenshot of PLABWIN10 desktop: Required URL is typed into

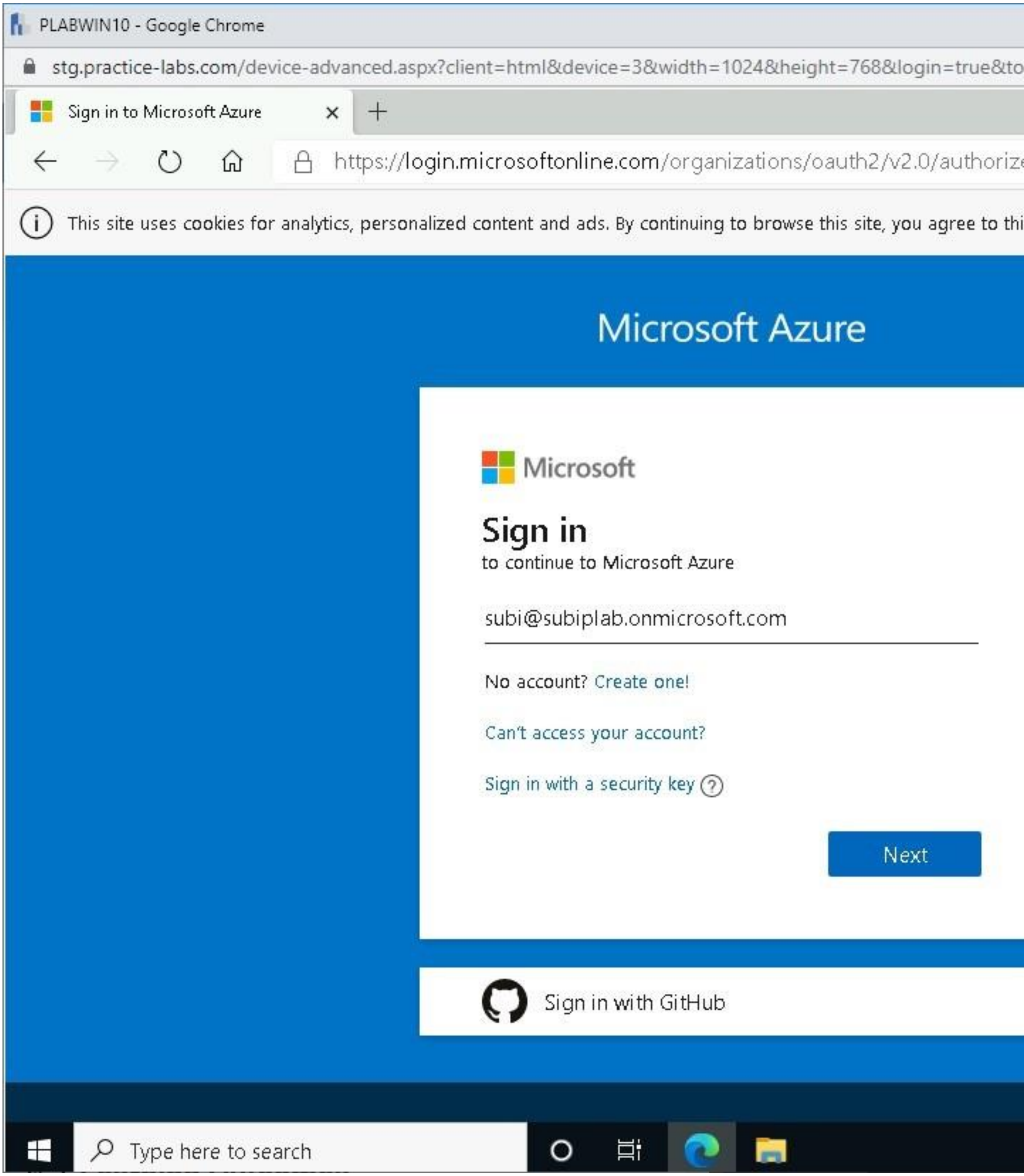
the address bar on the web browser window.

Step 2

Sign-in to Microsoft Azure using an account with a global administrator role in the Azure tenant.

Type the user account’s e-mail address.

Press **Enter**.



PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&to

https://login.microsoftonline.com/organizations/oauth2/v2.0/authorize

This site uses cookies for analytics, personalized content and ads. By continuing to browse this site, you agree to thi

subi@subiplab.onmicrosoft.com

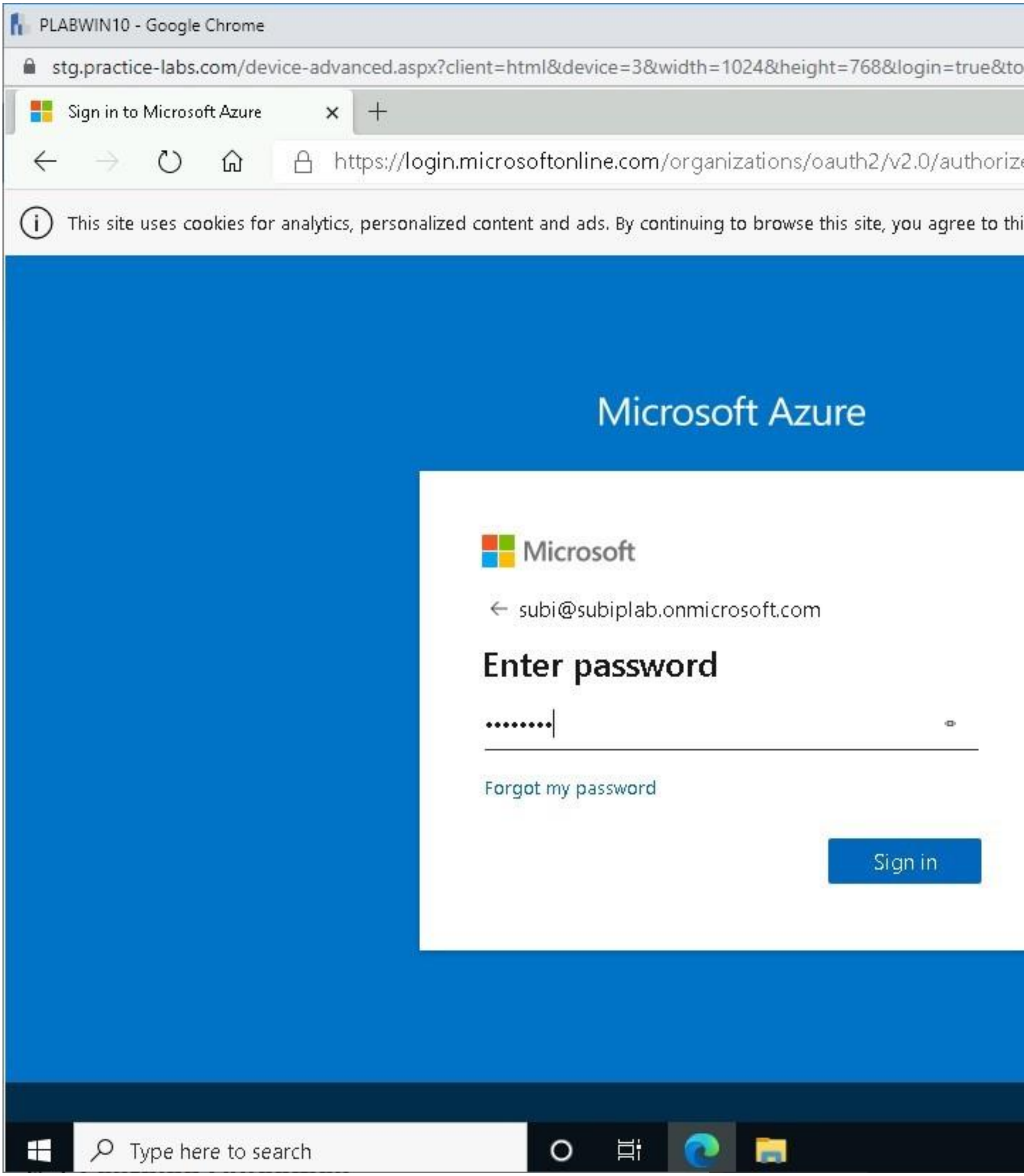
Sign in to Microsoft Azure
Microsoft Azure
Microsoft
Sign in
to continue to Microsoft Azure
No account? Create one!
Can't access your account?
Sign in with a security key
Next
Sign in with GitHub
Type here to search

Figure 1.2 Screenshot of PLABWIN10 desktop: Microsoft Sign in pane on

the Microsoft Azure screen is displayed showing the login credentials typed-in, and the Next button highlighted.

Step 3

Enter the required password and press **Enter**.



stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&to

https://login.microsoftonline.com/organizations/oauth2/v2.0/authorize

This site uses cookies for analytics, personalized content and ads. By continuing to browse this site, you agree to thi

subi@subiplab.onmicrosoft.com

Enter password

••••••••

Forgot my password

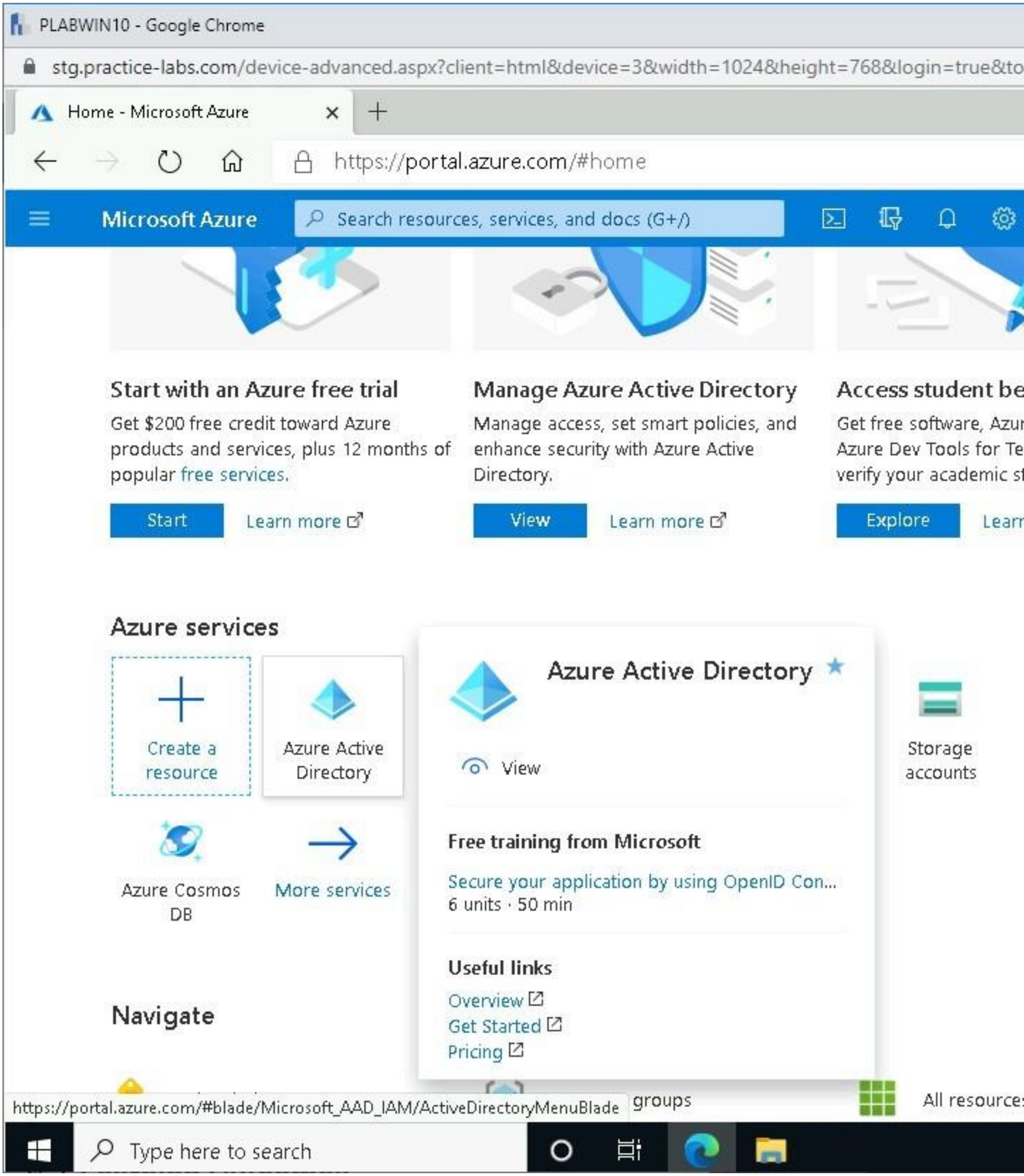
Figure 1.3 Screenshot of PLABWIN10 desktop: Microsoft Enter password

pane on the Microsoft Azure screen is displayed showing the required password typed-in, and the Sign in button highlighted.

Step 4

If the **Would you like to save password for microsoftonline.com** notification toolbar appears, click **Never**.

From the **Microsoft Azure** home page, select **Azure Active Directory** tile.


PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&to
Home - Microsoft Azure
https://portal.azure.com/#home
Microsoft Azure
Search resources, services, and docs (G+/)
Start
Learn more
View
Learn more
Explore
Learr
Azure services
Create a resource
Azure Active Directory
Storage accounts
Azure Cosmos DB
More services
View
Useful links
Overview
Get Started
Pricing
Navigate
groups
All resource
https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade
Type here to search

Start with an Azure free trial

Get $200 free credit toward Azure products and services, plus 12 months of popular free services.

Manage Azure Active Directory

Manage access, set smart policies, and enhance security with Azure Active Directory.

Access student be

Get free software, Azur
Azure Dev Tools for Te
verify your academic st

Azure Active Directory

Free training from Microsoft

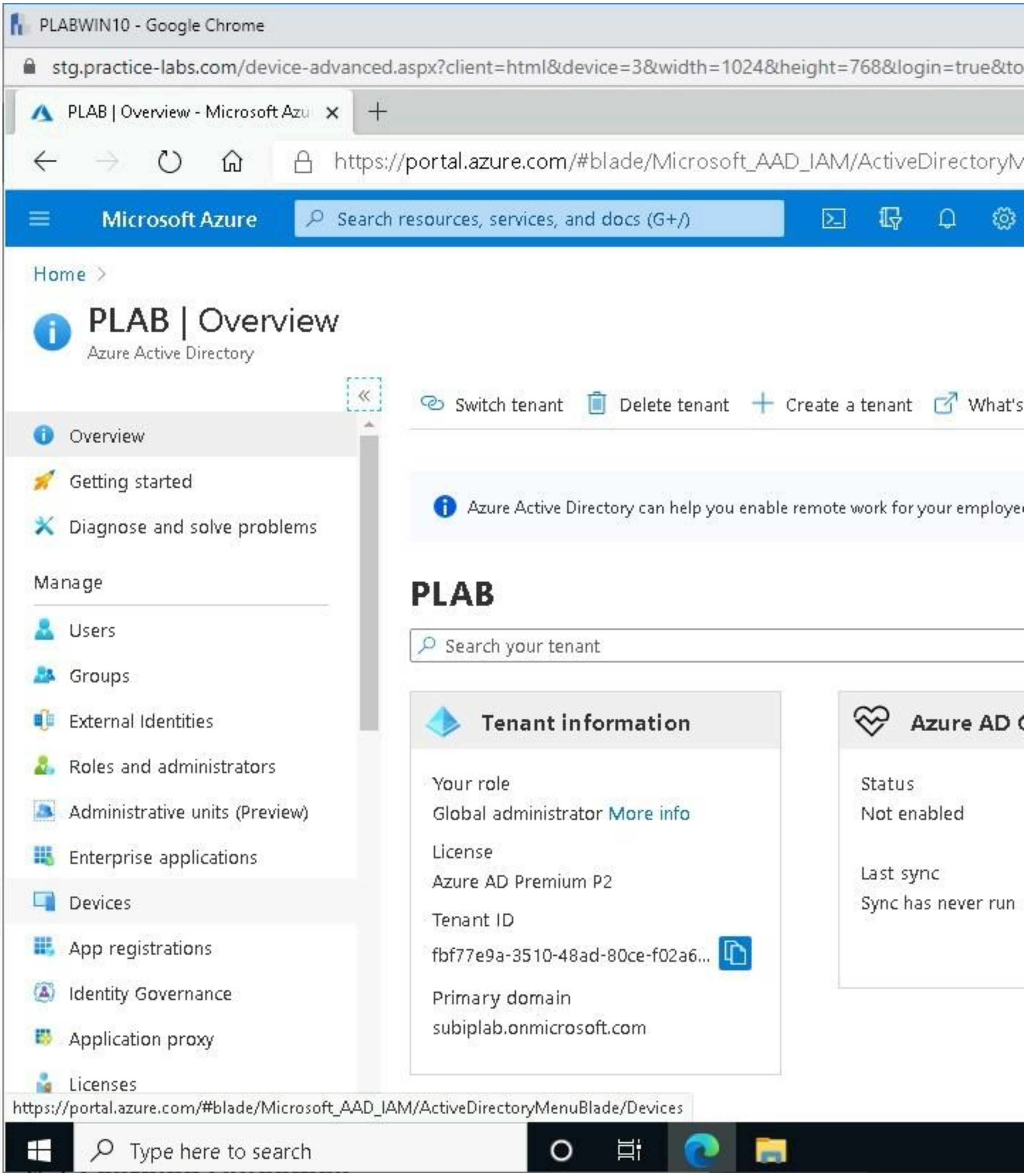
Secure your application by using OpenID Con...
6 units · 50 min

Figure 1.4 Screenshot of PLABWIN10 desktop: Azure Active Directory

option on the Microsoft Azure screen is selected.

Step 5

From the **<Organization Name> | Overview**, click **Devices** on the left pane.


PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&to
PLAB | Overview - Microsoft Azu
https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryM
Microsoft Azure
Search resources, services, and docs (G+/)
Home
PLAB | Overview
Azure Active Directory
Overview
Getting started
Diagnose and solve problems
Manage
Users
Groups
External Identities
Roles and administrators
Administrative units (Preview)
Enterprise applications
Devices
App registrations
Identity Governance
Application proxy
Licenses
Switch tenant
Delete tenant
Create a tenant
What's
Azure Active Directory can help you enable remote work for your employe
PLAB
Search your tenant
Tenant information
Azure AD C
https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Devices
Type here to search

Your role
Global administrator More info

License
Azure AD Premium P2

Tenant ID
fbf77e9a-3510-48ad-80ce-f02a6...

Primary domain
subiplab.onmicrosoft.com

Status
Not enabled

Last sync
Sync has never run

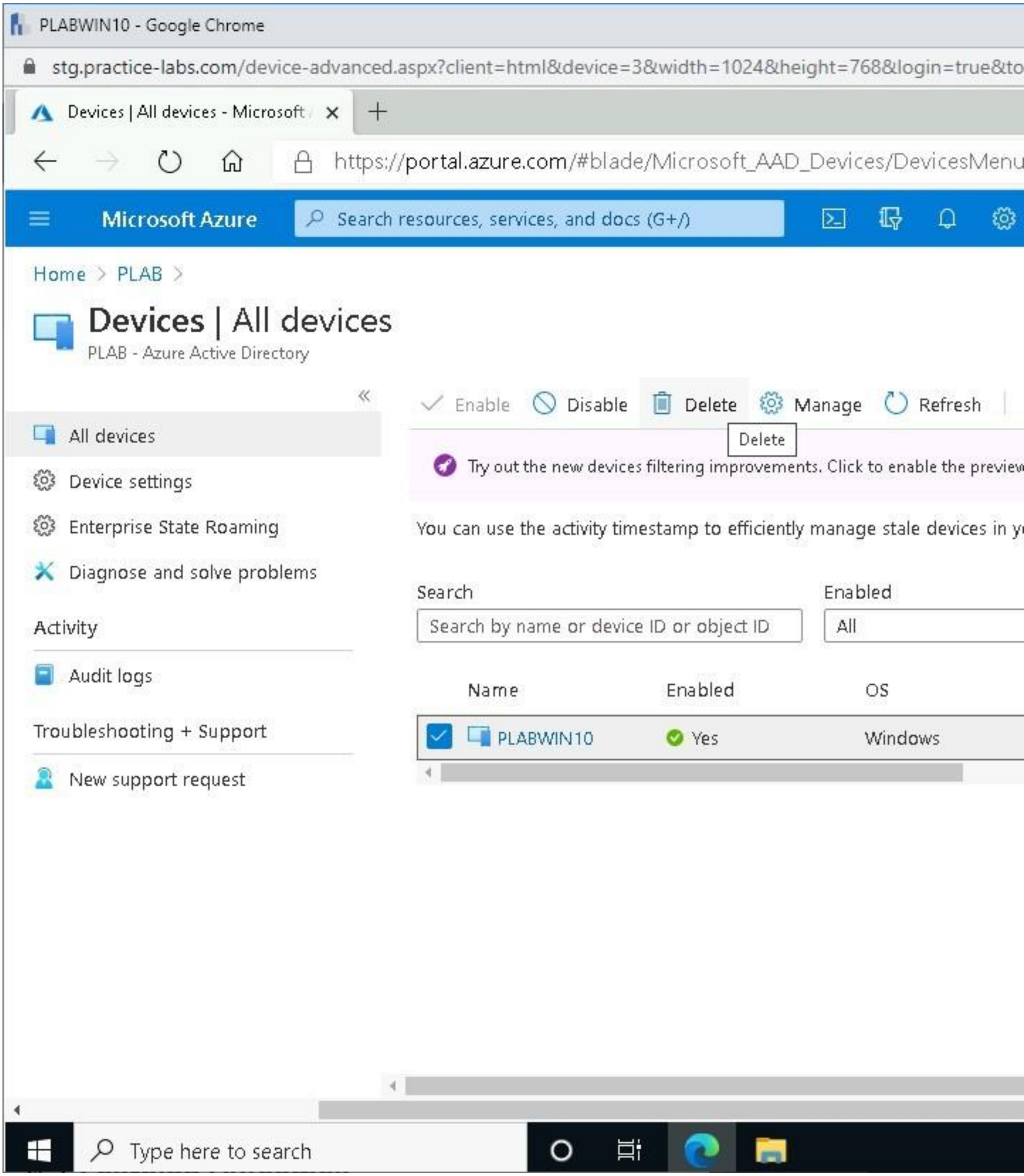
Figure 1.5 Screenshot of PLABWIN10 desktop: Devices option on the

navigation pane at the left on the Microsoft Azure - PLAB | Overview screen is selected.

Step 6

On the **Devices | All devices** page, click the **PLABWIN10** box and select **Delete**.

> ***Note***: *If there is more than one instance of **PLABWIN10** device, select all of them and click **Delete**.*


PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&to
Devices | All devices - Microsoft
https://portal.azure.com/#blade/Microsoft_AAD_Devices/DevicesMenu
Microsoft Azure
Search resources, services, and docs (G+/)
Home > PLAB >
Devices | All devices
PLAB - Azure Active Directory
All devices
Device settings
Enterprise State Roaming
Diagnose and solve problems
Activity
Audit logs
Troubleshooting + Support
New support request
Enable
Disable
Delete
Manage
Refresh
Delete
Search
Search by name or device ID or object ID
Enabled
All
Type here to search

Try out the new devices filtering improvements. Click to enable the preview

You can use the activity timestamp to efficiently manage stale devices in y

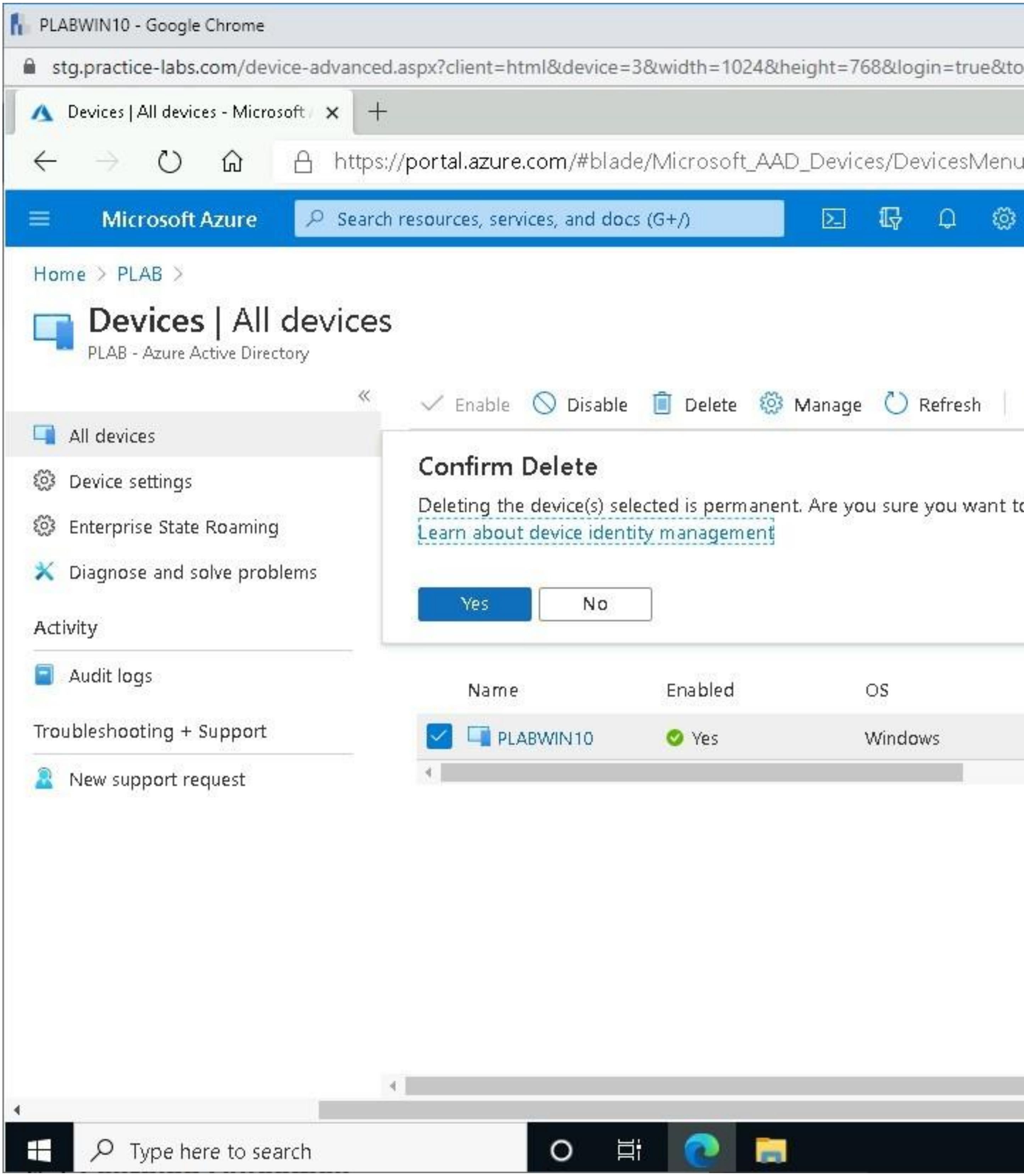
	Name	Enabled	OS
☑	PLABWIN10	✓ Yes	Windows

Figure 1.6 Screenshot of PLABWIN10 desktop: Microsoft Azure - Devices |

All devices screen is displayed showing the required selection performed, and the Delete option highlighted.

Step 7

Click **Yes** on the **Confirm Delete** notification bar.



Confirm Delete

Deleting the device(s) selected is permanent. Are you sure you want tc

Learn about device identity management

	Name	Enabled	OS
☑	PLABWIN10	✓ Yes	Windows

PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&to
Devices | All devices - Microsoft
https://portal.azure.com/#blade/Microsoft_AAD_Devices/DevicesMenu
Microsoft Azure
Search resources, services, and docs (G+/)
Home > PLAB >
Devices | All devices
PLAB - Azure Active Directory
Enable
Disable
Delete
Manage
Refresh
All devices
Device settings
Enterprise State Roaming
Diagnose and solve problems
Activity
Audit logs
Troubleshooting + Support
New support request
Yes
No
Type here to search

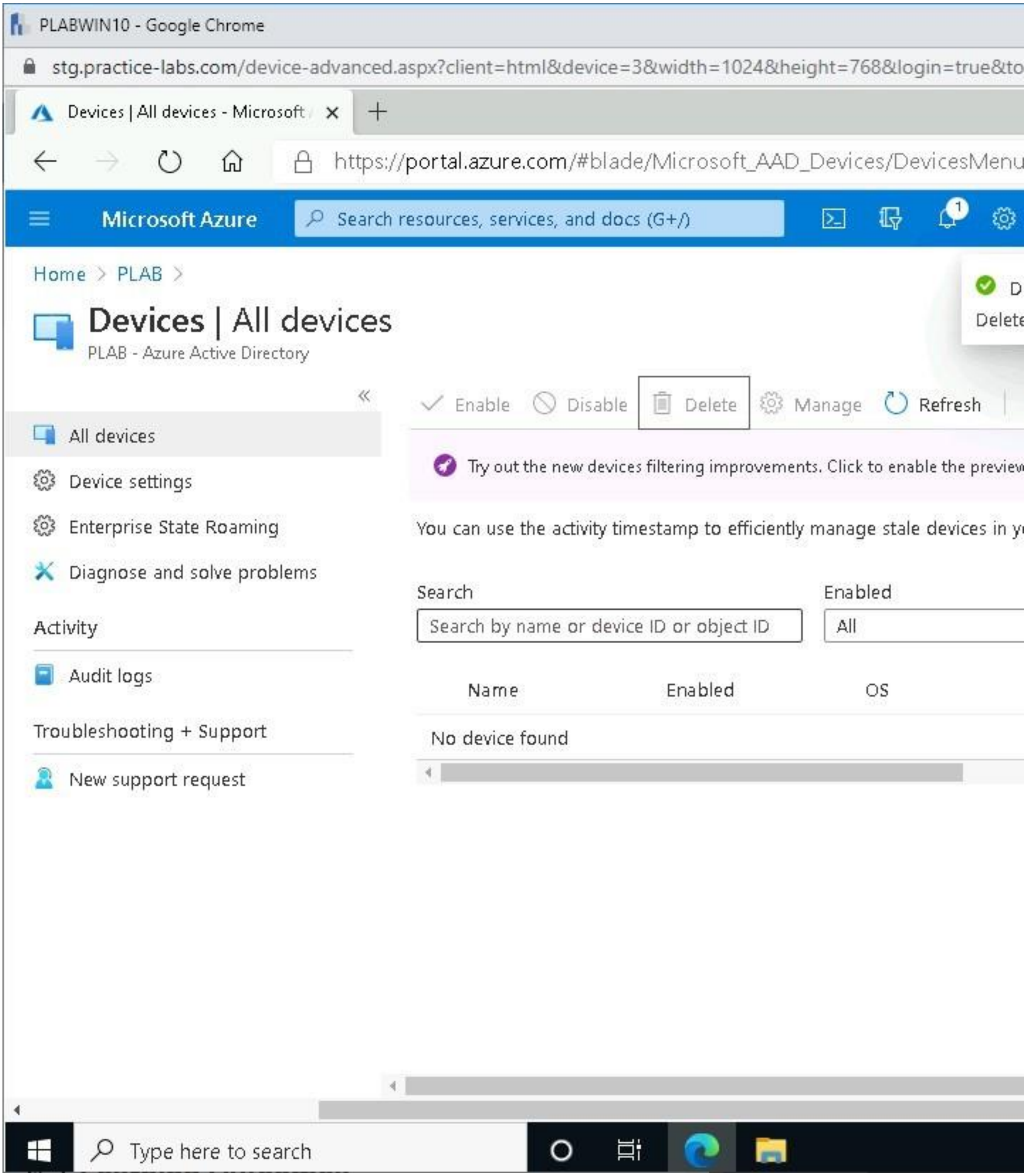
Figure 1.7 Screenshot of PLABWIN10 desktop: Confirm Delete notification

is displayed prompting for confirmation to delete the selected device and showing the Yes button highlighted.

Step 8

Please wait while deletion of **PLABWIN10** device is in progress.

Once the device is successfully deleted, close **Microsoft Edge** without signing out.



PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&to
Devices | All devices - Microsoft
https://portal.azure.com/#blade/Microsoft_AAD_Devices/DevicesMenu
Microsoft Azure
Search resources, services, and docs (G+/)
Home > PLAB >
D
Delete
Devices | All devices
PLAB - Azure Active Directory
Enable
Disable
Delete
Manage
Refresh
All devices
Device settings
Enterprise State Roaming
Diagnose and solve problems
Activity
Audit logs
Troubleshooting + Support
New support request
Search
Enabled
All
Name
Enabled
OS
Type here to search

Try out the new devices filtering improvements. Click to enable the preview

You can use the activity timestamp to efficiently manage stale devices in y

Search by name or device ID or object ID

No device found

Figure 1.8 Screenshot of PLABWIN10 desktop: Delete devices notification

is displayed on the Microsoft Azure - Devices | All devices screen confirming deletion of the specified device.

Task 2 - Remove Domain Computer from Active Directory

PLABWIN10 is a computer joined to an on-premise Active Directory domain called PRACTICELABS.COM. Removal of **PLABWIN10** from the local Active Directory is mandatory as this enables the device to join an Azure AD. In this task, you will remove **PLABWIN10** from the local Active Directory domain and restart the device.

Step 1

Connect to **PLABWIN10**.

Right-click the **Start** charm, and select **Windows PowerShell (Admin**).

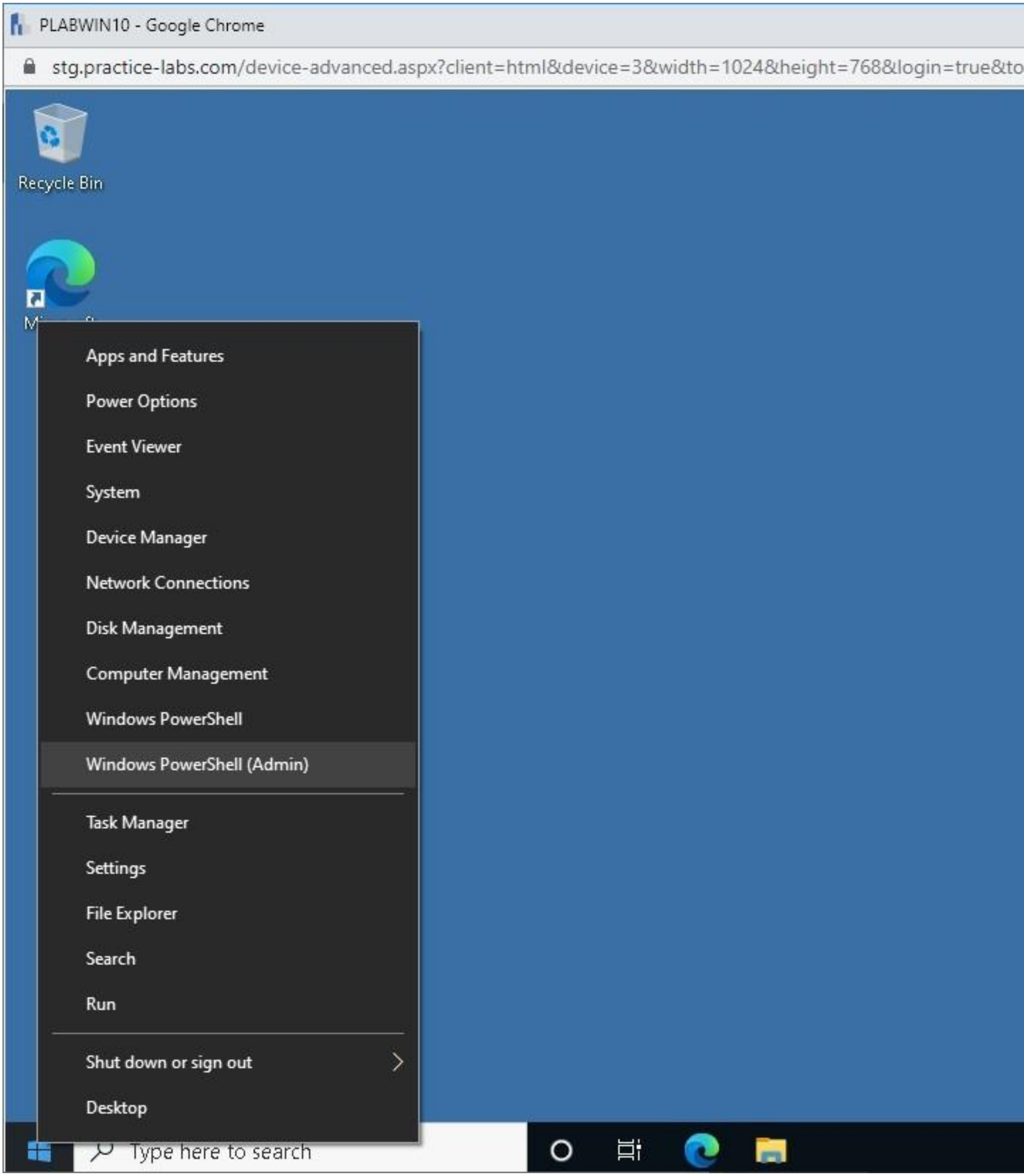
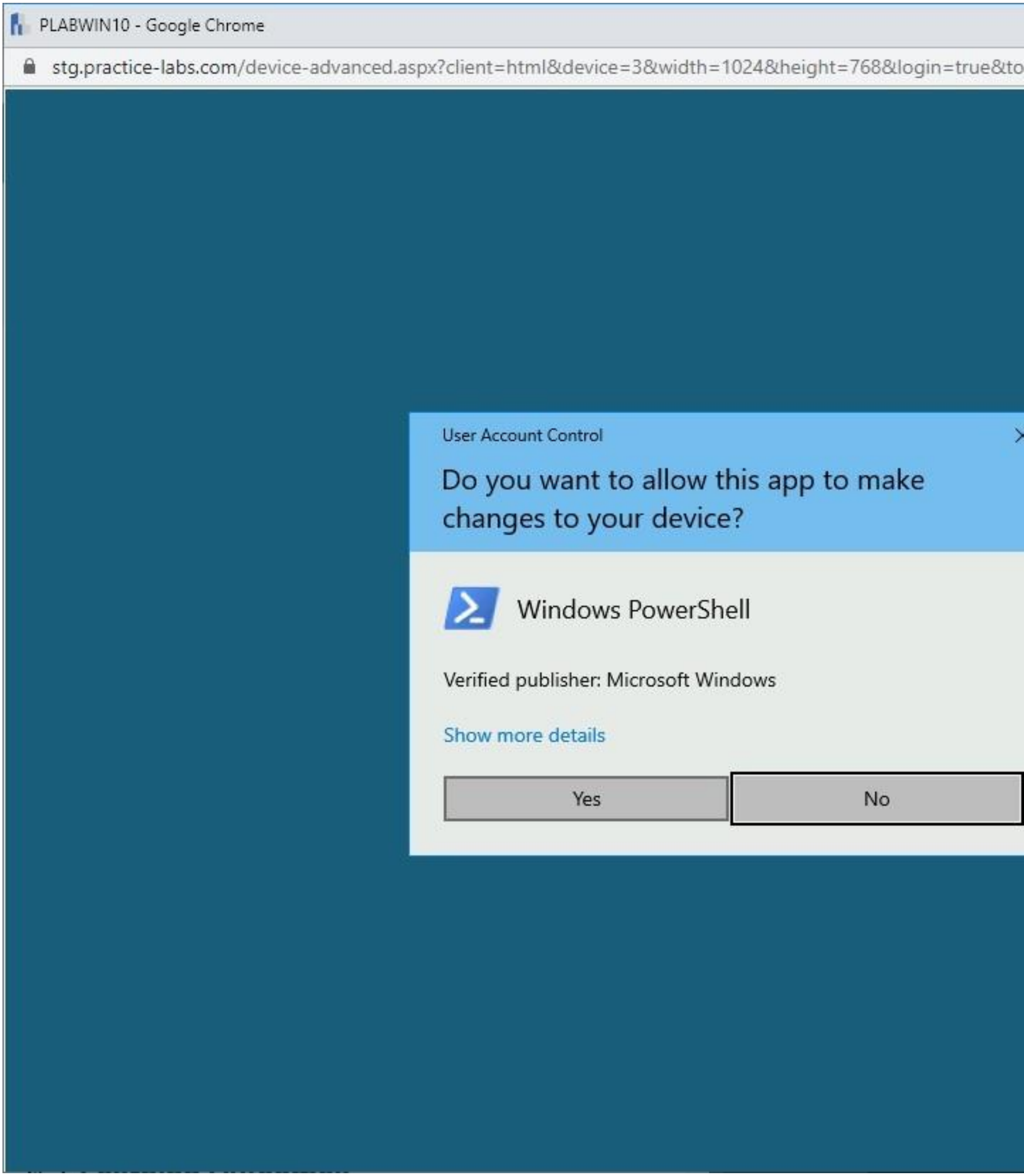


Figure 1.9 Screenshot of PLABWIN10 desktop: Context menu (that appears

on right-clicking the Start charm) > Windows PowerShell (Admin) menu-options are selected.

Step 2

Select **Yes** in the **User Account Control** message box.


PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&to
User Account Control
Yes
No

Do you want to allow this app to make changes to your device?

Windows PowerShell

Verified publisher: Microsoft Windows

Show more details

Figure 1.10 Screenshot of PLABWIN10 desktop: User Account Control

dialog box is displayed prompting for confirmation to allow the app to make changes to the device and showing the Yes button highlighted.

Step 3

To remove this computer from the on-premise PRACTICELABS.COM domain, type the following commands:

```
Remove-Computer
```

Press **Enter**.

On the next prompt, type:

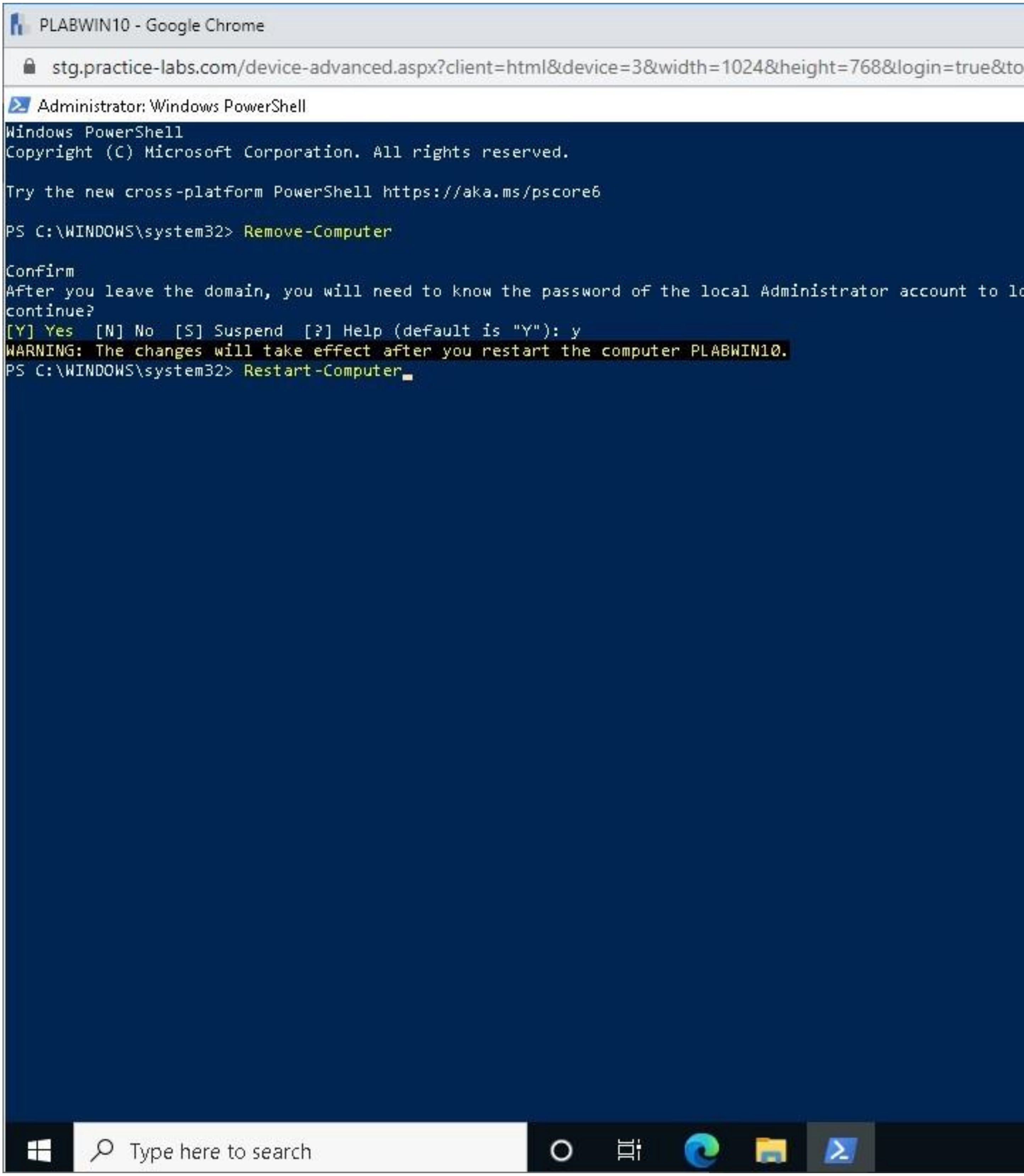
```
y
```

Press **Enter**.

To restart the device, type:

```
Restart-Computer
```

Press **Enter**.



PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&to
Administrator: Windows PowerShell
Type here to search

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> Remove-Computer

Confirm
After you leave the domain, you will need to know the password of the local Administrator account to lo
continue?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y
WARNING: The changes will take effect after you restart the computer PLABWIN10.
PS C:\WINDOWS\system32> Restart-Computer
```

Figure 1.11 Screenshot of PLABWIN10 desktop: Administrator Windows

PowerShell window is displayed showing the command to remove the virtual machine from the current domain executed.

Please wait while the **PLABWIN10** device restarts.

Task 3 - Join the Computer to Azure AD

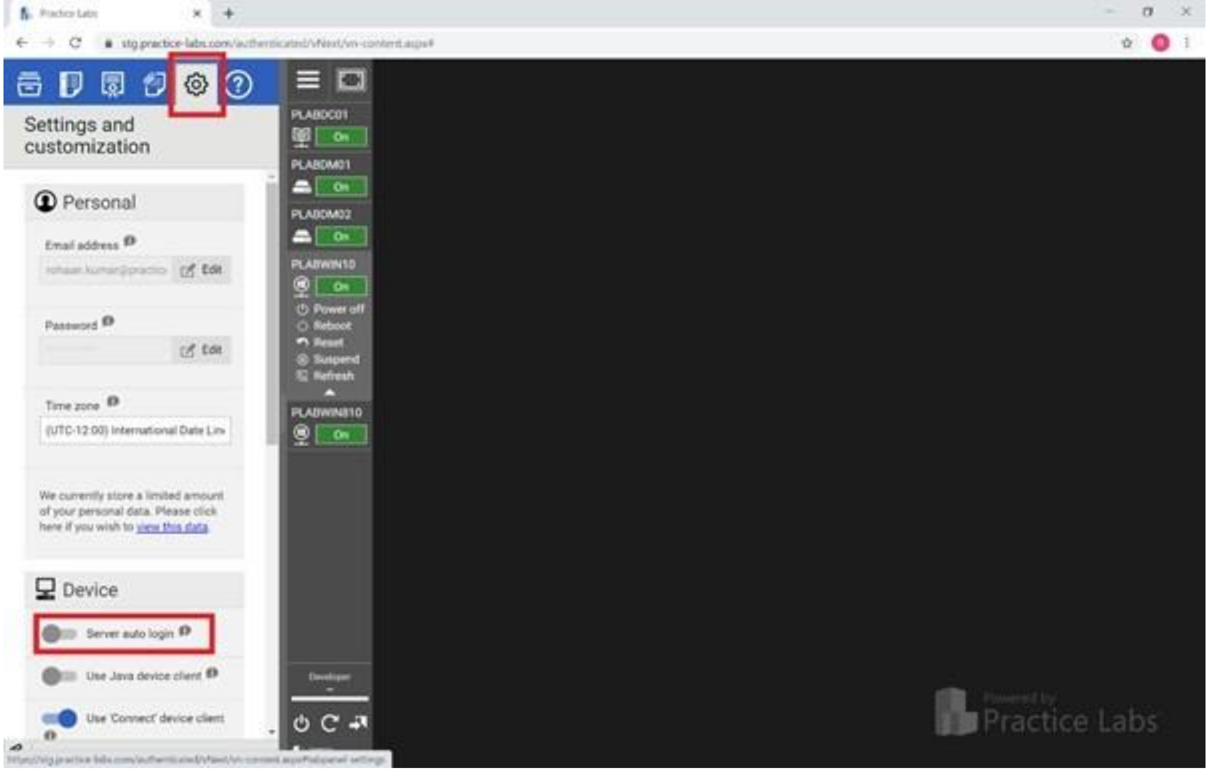
After successfully removing **PLABWIN10** from Active Directory, the device is ready to be joined to Azure AD.

This task will demonstrate how to join a computer to a cloud directory service.

Step 1

For this step, you will need to disable the **Auto login** feature. Click on settings and then move the slider for **Server auto login** to the off position.

Note: *Please see our help and support page for more information on how to do this.*



Settings and customization

Personal

Email address: rohaan.kumar@practice… Edit

Password: Edit

Time zone: (UTC-12:00) International Date Line

We currently store a limited amount of your personal data. Please click here if you wish to view this data.

Device

Server auto login: off

Use Java device client: off

Use 'Connect' device client: on

Figure 1.12 Screenshot of Practice Labs application interface: Server auto login option on the Device section of the Settings pane on the left is switched off.

Step 2

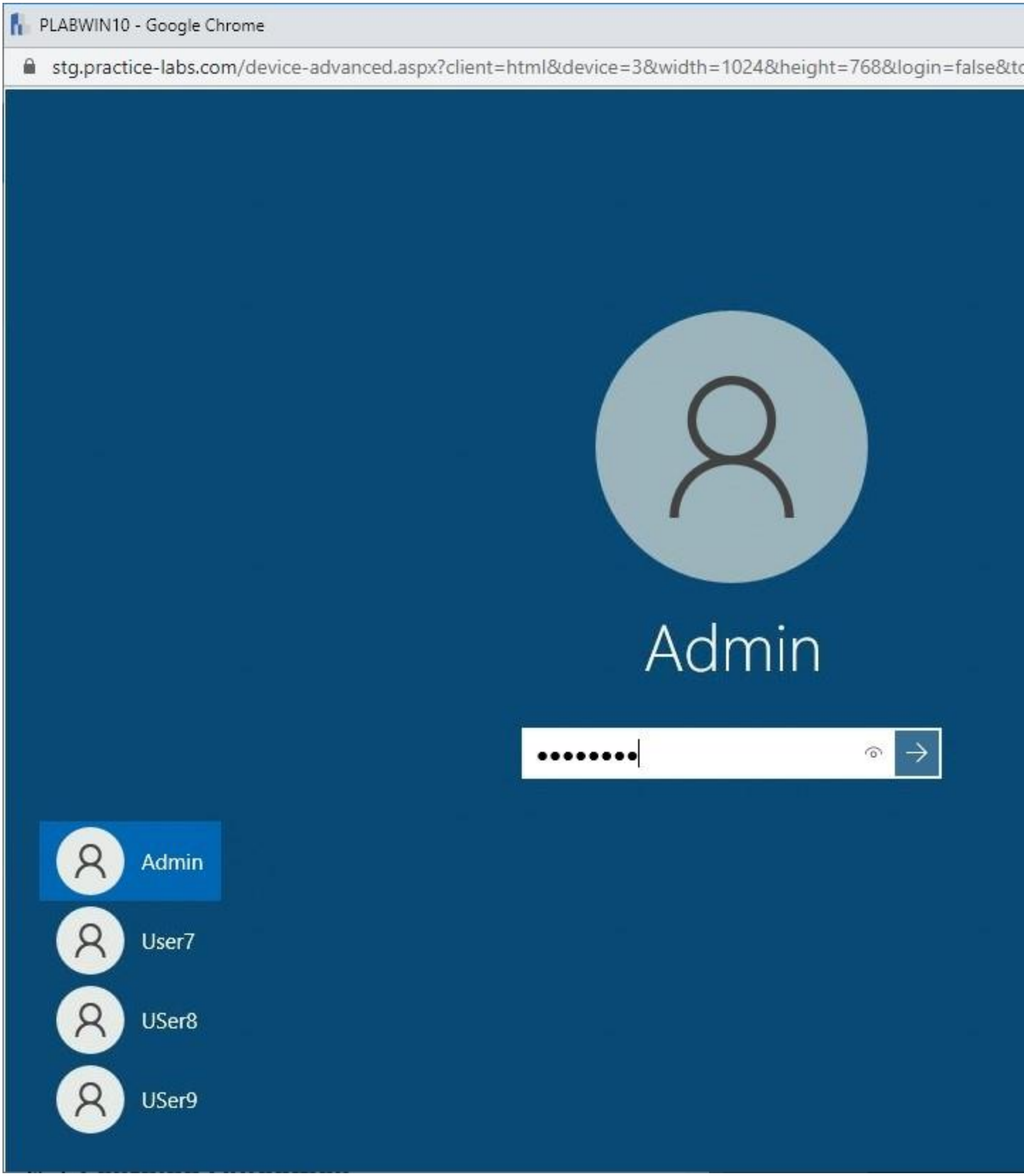
Connect to **PLABWIN10** 1 minute after restart.

Select **Admin** from the sign-in screen.

Use the password:

```
Passw0rd
```

Press **Enter**.



PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc
Admin
••••••••
Admin
User7
USer8
USer9

Figure 1.13 Screenshot of PLABWIN10 desktop: Required password is

typed in on the Admin login screen.

Step 3

Select **Install** in the **Application Install - Security Warning** message box.

Click **Start** type:

```
access work
```

Select **Access work or school**.

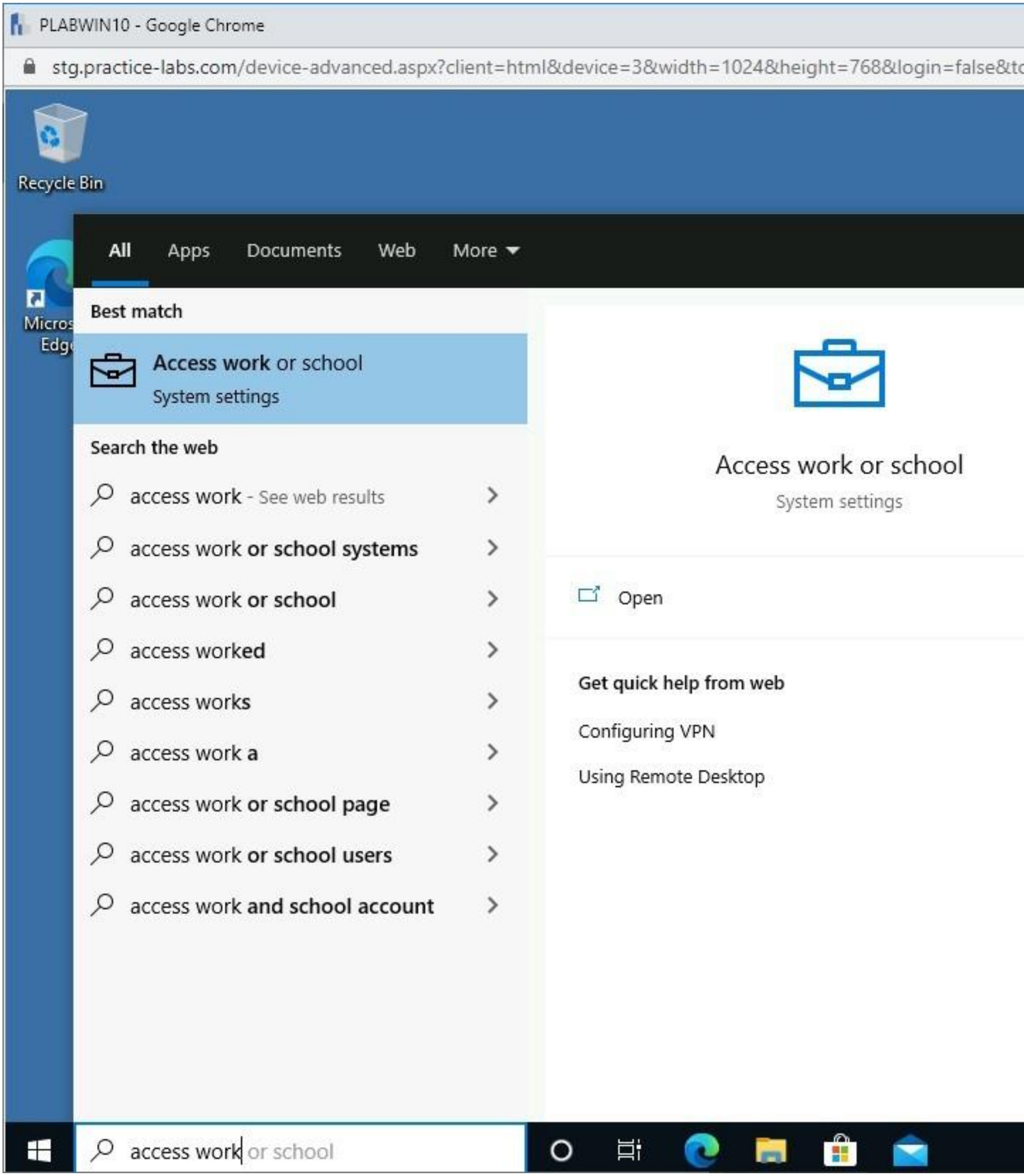
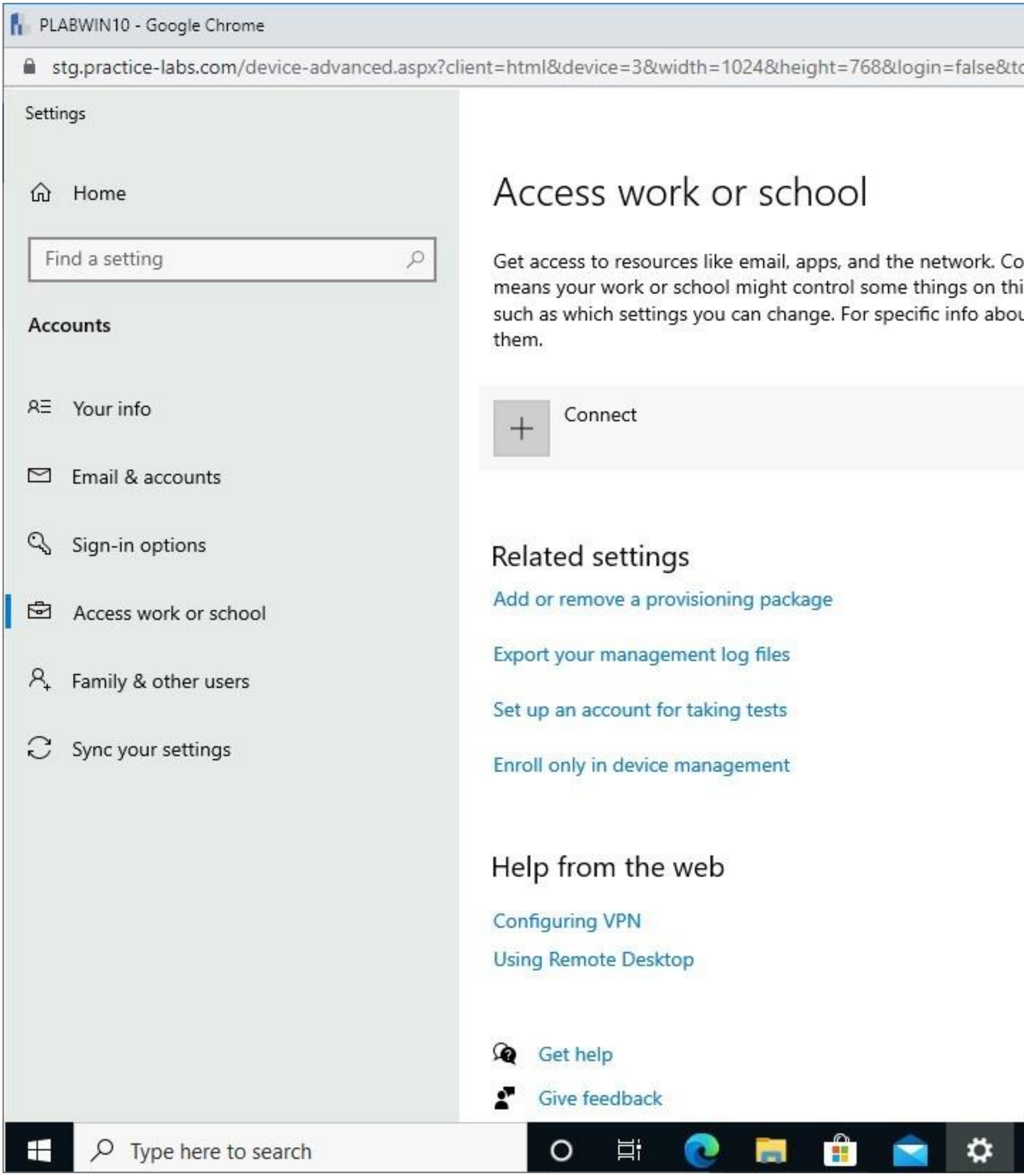


Figure 1.14 Screenshot of PLABWIN10 desktop: Required option on the

Best match popup menu is selected.

Step 4

Under **Access work or school**, click **[+]** beside **Connect**.



PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc
Settings
Home
Find a setting
Accounts
Your info
Email & accounts
Sign-in options
Access work or school
Family & other users
Sync your settings
Connect
Related settings
Add or remove a provisioning package
Export your management log files
Set up an account for taking tests
Enroll only in device management
Help from the web
Configuring VPN
Using Remote Desktop
Get help
Give feedback
Type here to search

Access work or school

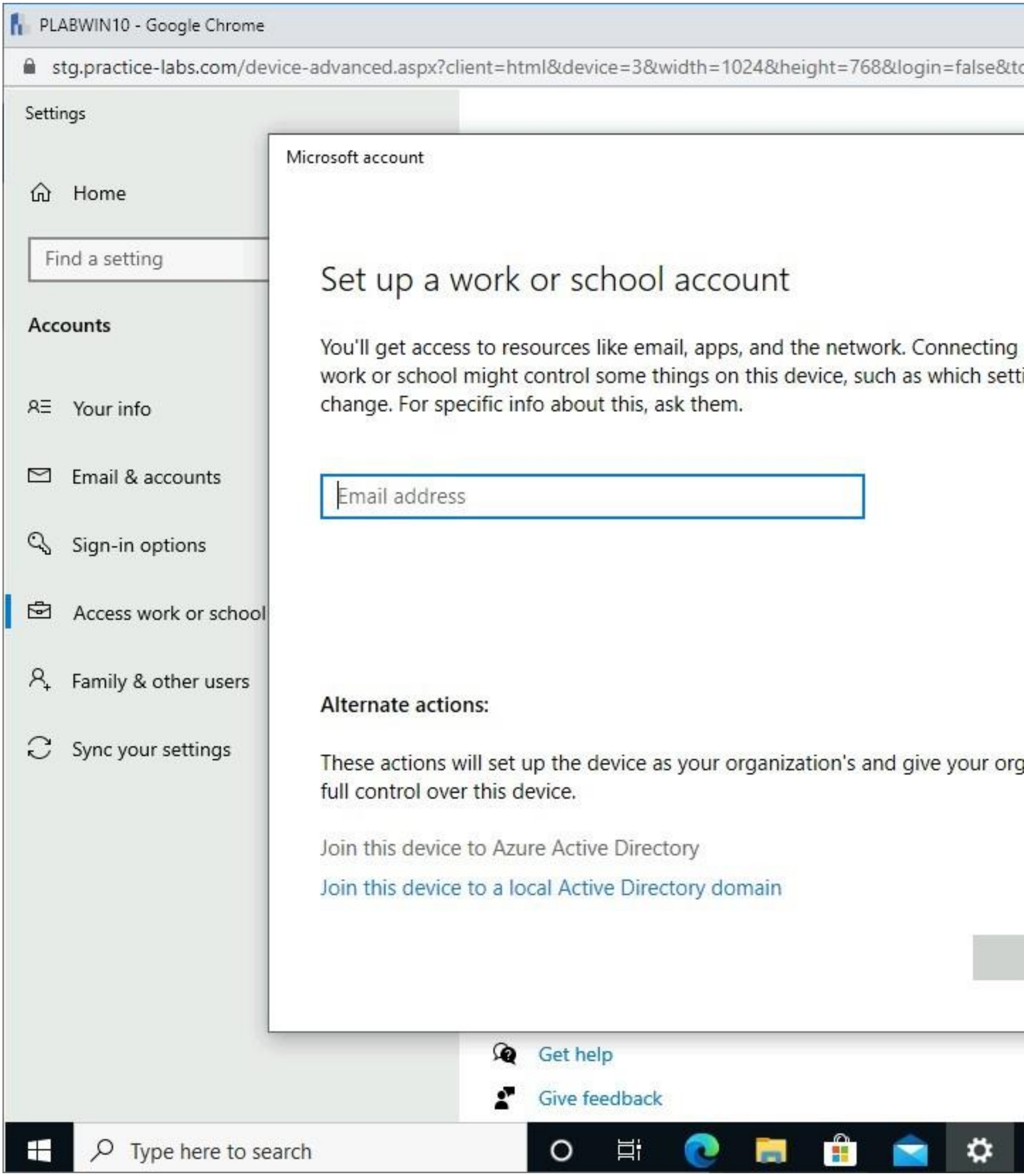
Get access to resources like email, apps, and the network. Co means your work or school might control some things on thi such as which settings you can change. For specific info abou them.

Figure 1.15 Screenshot of PLABWIN10 desktop: Connect option on the

Settings - Access work or school screen is highlighted.

Step 5

On the **Microsoft Account - Set up a work or school account**, select **Join this device to Azure Active Directory** hyperlink.



Set up a work or school account

You'll get access to resources like email, apps, and the network. Connecting work or school might control some things on this device, such as which setti change. For specific info about this, ask them.

Email address

Alternate actions:

These actions will set up the device as your organization's and give your org full control over this device.

Join this device to Azure Active Directory

Join this device to a local Active Directory domain

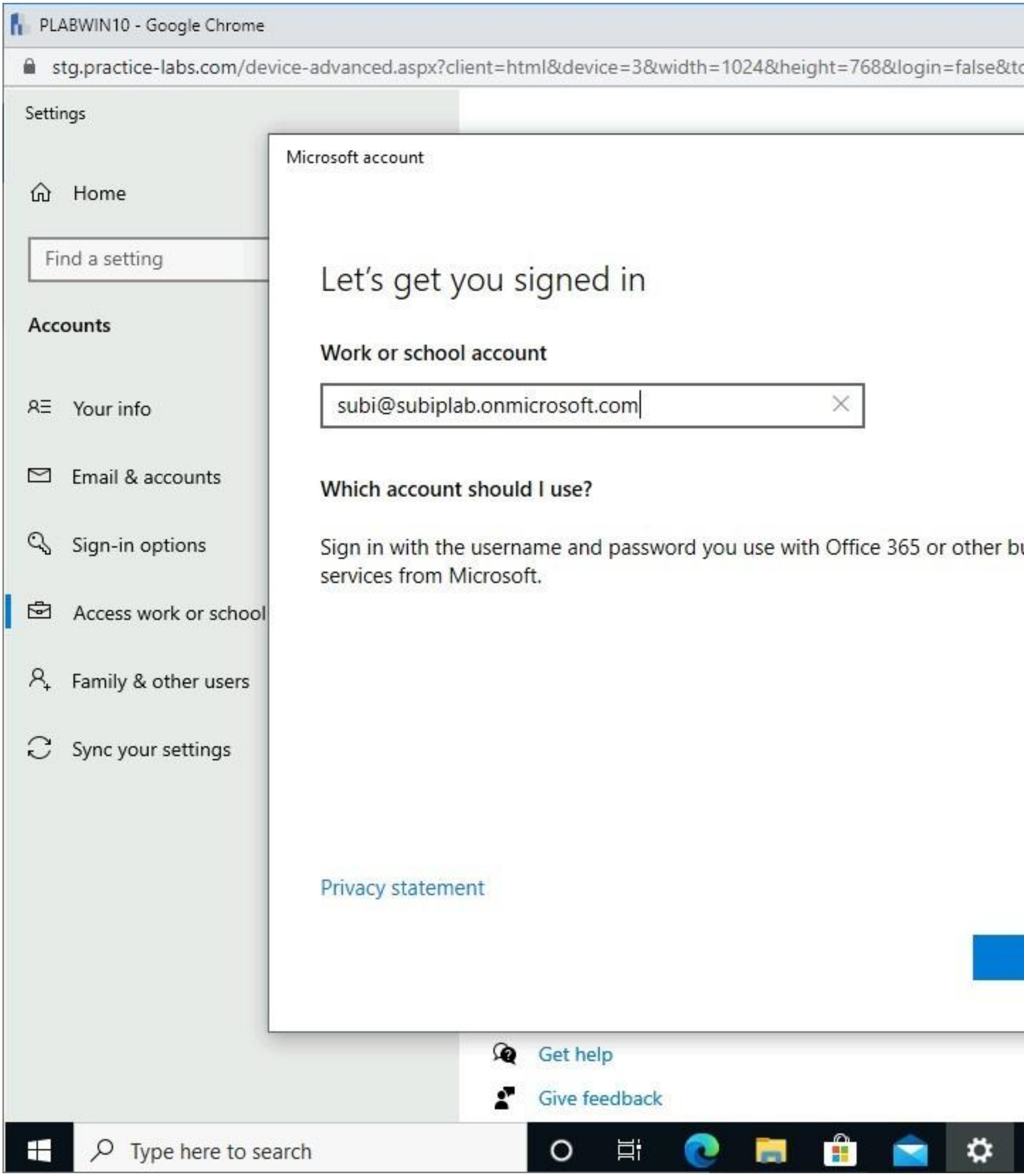
Figure 1.16 Screenshot of PLABWIN10 desktop: Join this device to Azure

Active Directory link on the Set up a work or school account page of the Microsoft account wizard is selected.

Step 6

On the **Let’s get you signed in**, type an Azure AD user account with a global administrator role in the Azure tenant.

Click **Next**.



PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc

Microsoft account

Let's get you signed in

Work or school account

subi@subiplab.onmicrosoft.com

Which account should I use?

Sign in with the username and password you use with Office 365 or other bu services from Microsoft.

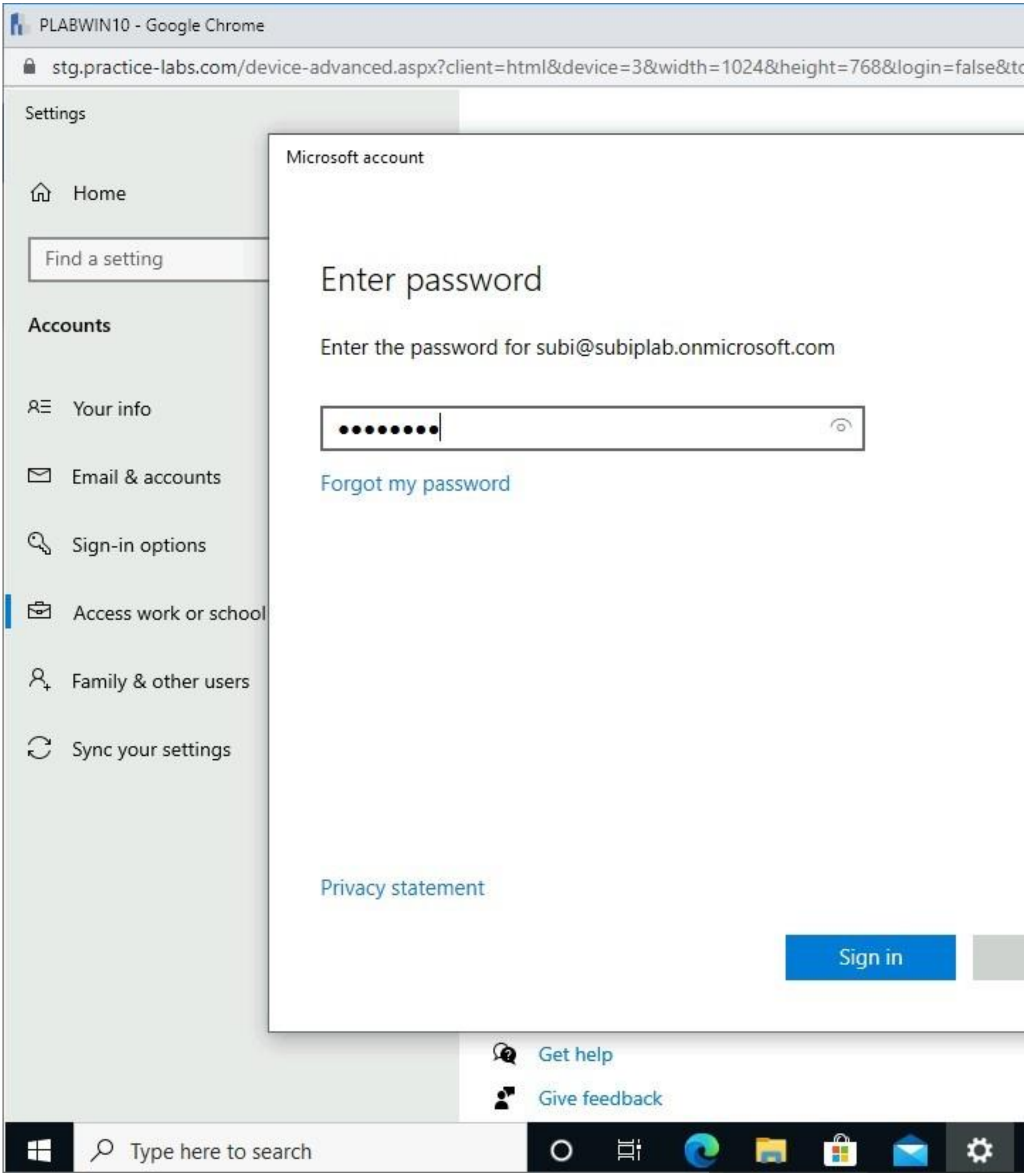
Privacy statement

Figure 1.17 Screenshot of PLABWIN10 desktop: Let's get you signed in page

on the Microsoft account wizard is displayed showing the required user account information typed-in and the Next button selected.

Step 7

Enter the appropriate password for the user account, click **Sign in**.



PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc

Microsoft account

Enter password

Enter the password for subi@subiplab.onmicrosoft.com

••••••••

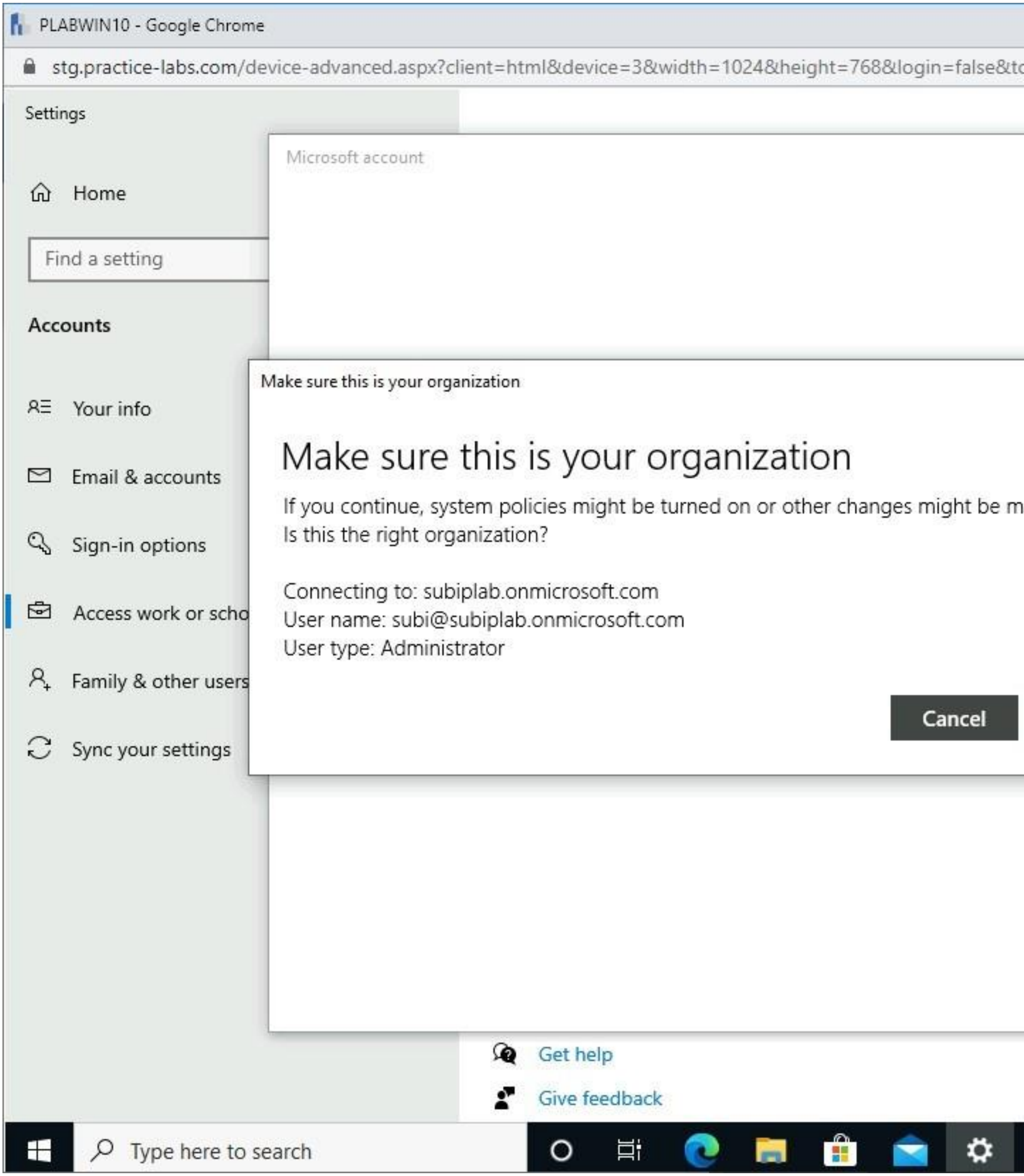
Figure 1.18 Screenshot of PLABWIN10 desktop: Enter password page on

the Microsoft account wizard is displayed showing the required password typed-in and the Sign in button selected.

Step 8

Please wait while the device is currently set up with Azure AD.

Click **Join** in the **Make sure this is your organization** message box.



Make sure this is your organization

If you continue, system policies might be turned on or other changes might be m
Is this the right organization?

Connecting to: subiplab.onmicrosoft.com
User name: subi@subiplab.onmicrosoft.com
User type: Administrator

Figure 1.19 Screenshot of PLABWIN10 desktop: Make sure this is your

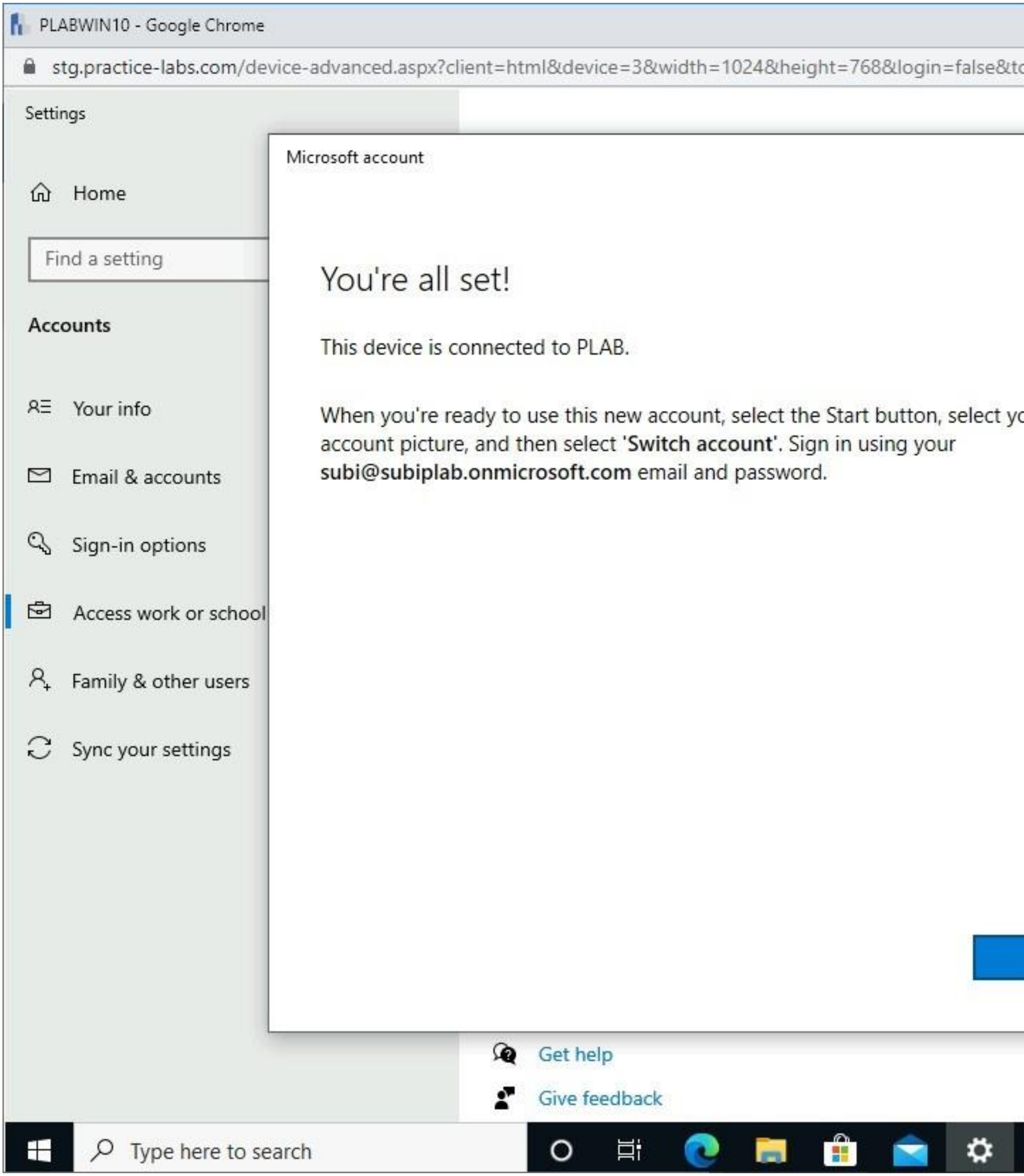
organization dialog box is displayed prompting for confirmation to join the specified active directory and showing the Join button selected.

Step 9

Please wait while the device setup runs.

A confirmation message appears, saying, “**You’re all set**!”

Click **Done**.



You're all set!

This device is connected to PLAB.

When you're ready to use this new account, select the Start button, select yc account picture, and then select '**Switch account**'. Sign in using your **subi@subiplab.onmicrosoft.com** email and password.

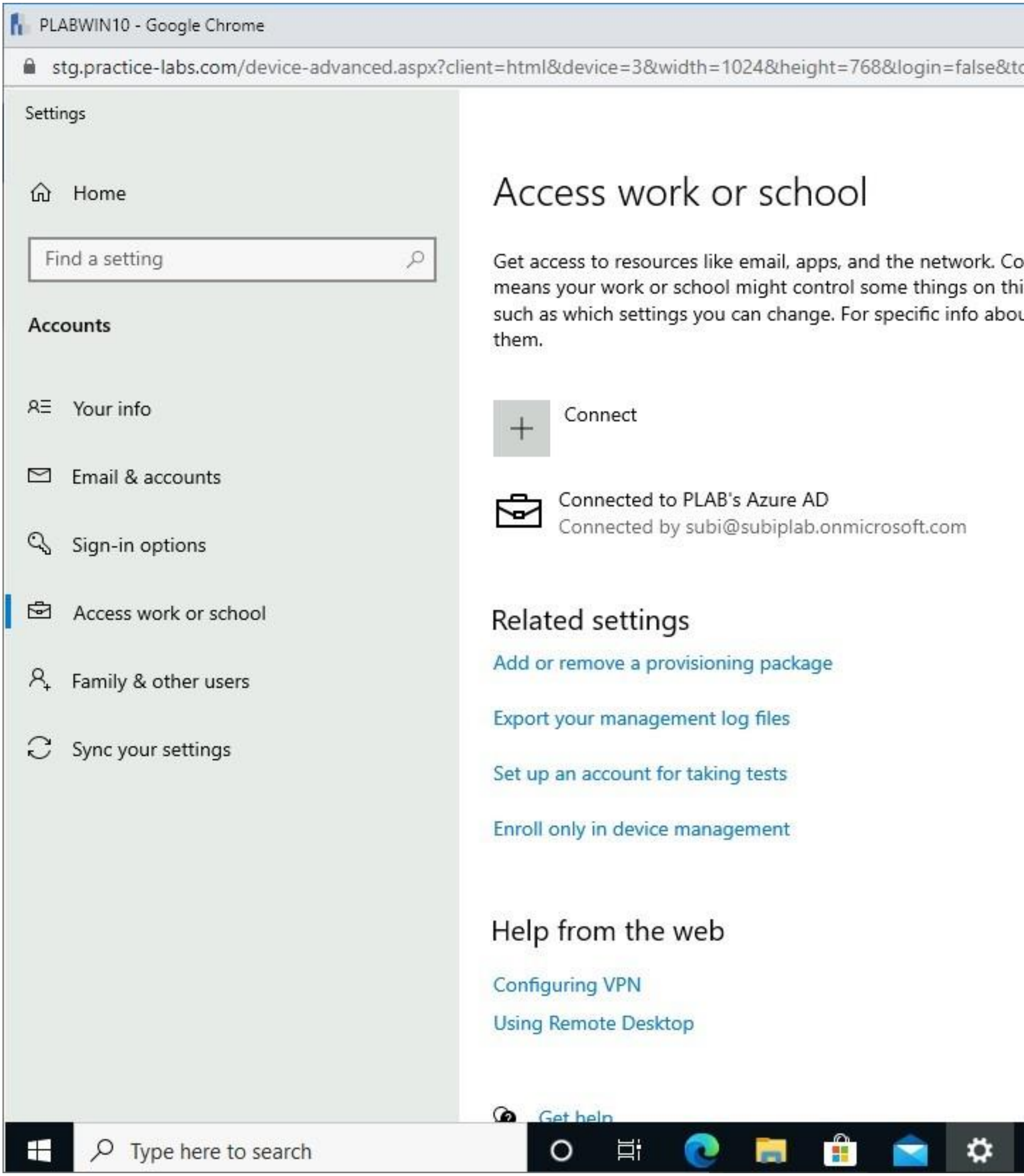
Figure 1.20 Screenshot of PLABWIN10 desktop: You're all set page on the

Microsoft account wizard is displayed confirming status of the specified connection and showing the Done button selected.

Step 10

Back in the **Access work or school** page, observe that **Connected to Your <Organization Name> Azure AD** indicates this device is now joined to the cloud directory service.

Close **Settings** window.



Access work or school

Get access to resources like email, apps, and the network. Co means your work or school might control some things on thi such as which settings you can change. For specific info abou them.

Connect

Connected to PLAB's Azure AD
Connected by subi@subiplab.onmicrosoft.com

Related settings

Add or remove a provisioning package

Export your management log files

Set up an account for taking tests

Enroll only in device management

Help from the web

Configuring VPN

Using Remote Desktop

Get help

Figure 1.21 Screenshot of PLABWIN10 desktop: Settings - Access work or

school screen is displayed listing status of the specified connection.

Keep devices in their current state and proceed to the next exercise.

Exercise 2 - Implement Azure Information Protection Labels

Azure Information Protection is a cloud-based document protection feature that provides classification, labeling, and data protection. Emails and documents created in Microsoft Office use AIP to classify, label, and protect data. Compared to data encryption, AIP has mechanisms to recognize sensitive information as it alerts users when they work with such data types. Default labels lay the groundwork from which Azure administrators can use data protection. Also, custom labels are supported where you can create rules based on data types, phrases entered by users in their documents.

To successfully implement AIP, you will need to first create rules and policies for classification. You will then configure labeling and data protection. For instance, you can specify data types such as personally identifiable information (PII) like social security or financial information such as credit card numbers or bank account numbers. Moreover, custom keywords like “salary” are conditions for automatic or recommended classification.

AIP is included in Azure Premium P1 or P2 subscription for your Azure tenant. On the client-side, Windows 10 is the preferred operating system that runs Microsoft Office 2013 or later. To use the sensitivity labels to classify documents, you must install the Azure Information Protection client on Windows 10.

For this exercise, you will enable the Azure Information Protection (AIP) label service and generate the default labels. The generated labels will be copied to Office 365 and Security Compliance Center to support AIP unified labeling feature. AIP supports the creation of custom labels by adding keywords that denote confidentiality or secrecy. These keywords add to the conditions in the AIP policy. Similarly, you can edit the properties of the default labels by adding keywords to it. After customizing the labels, publish the labels to enable detection by AIP-aware apps such as Microsoft Office. You must sign-in to Windows 10 device joined to Azure AD to verify the application of AIP policy.

To learn more about implementing Azure Information Protection labels, please refer to your course material or use your favorite search engine to research for more information about this topic.

Learning Outcomes

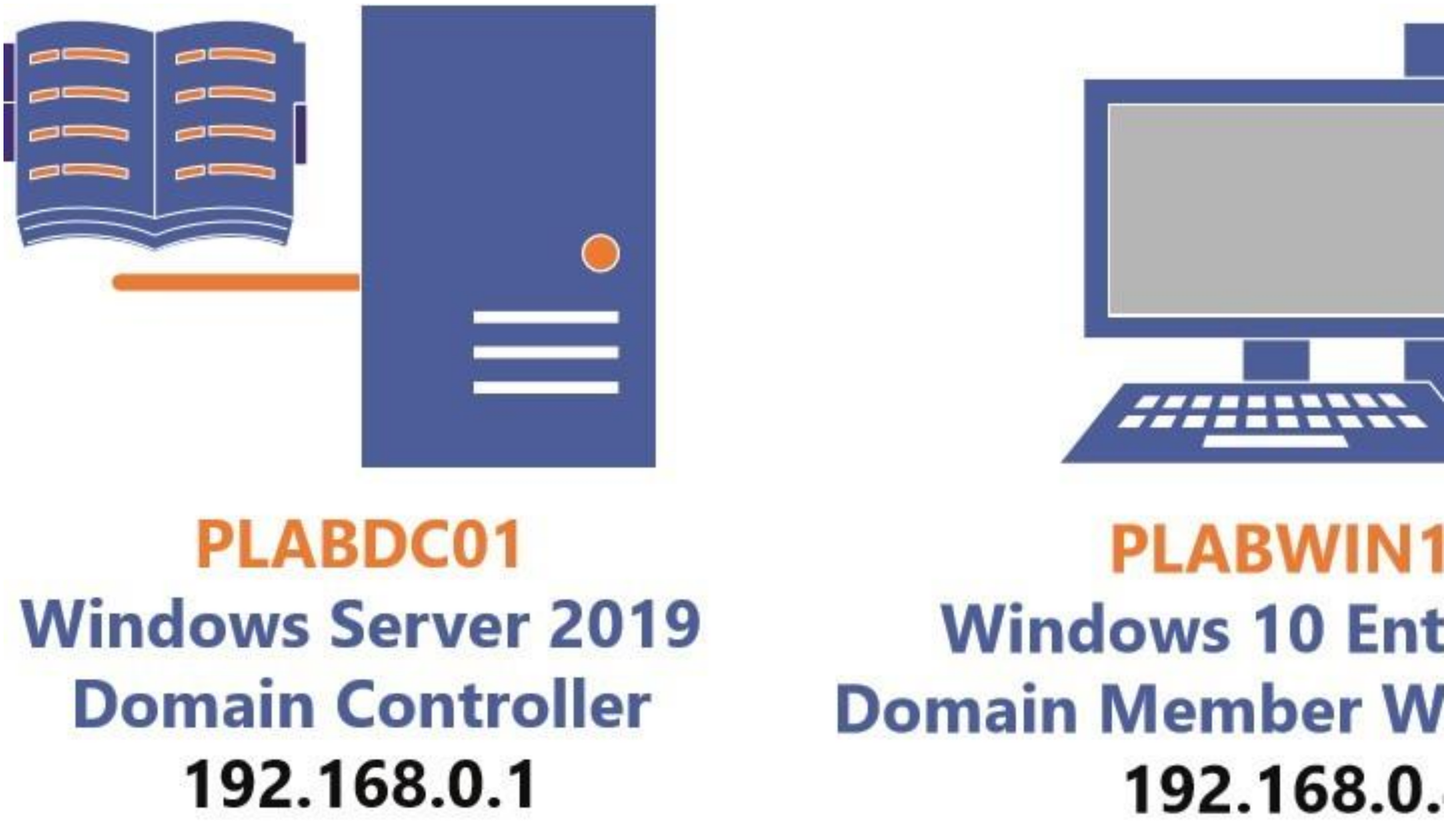
After completing this exercise, you will be able to:

- Generate Default Policies and Labels
- Migrate AIP Labels to Office 365 Security and Compliance Center
- Create a Custom Label
- Edit the Confidential Label
- Publish the Labels
- Install Azure Information Protection Client Unified Labeling
- Enable Remote Desktop
- Configure Proxy Server Settings for a New User
- Verify AIP Policy

Your Devices

You will be using the following devices in this lab. Please power these on now.

- **PLABDC01 -** (Windows Server 2019 - Domain Controller)
- **PLABWIN10 -** (Windows 10 Enterprise - Domain Member Workstation)



Task 1 - Generate Default Policies and Labels

To make it easier for the Azure administrator to classify Microsoft Office documents, AIP provides default labels, namely: Personal, Public, General, Confidential, and Highly Confidential. These labels have necessary description and provide the foundation where you can create conditions to classify and subsequently protect documents.

In this task, you will generate built-in labels in AIP.

Step 1

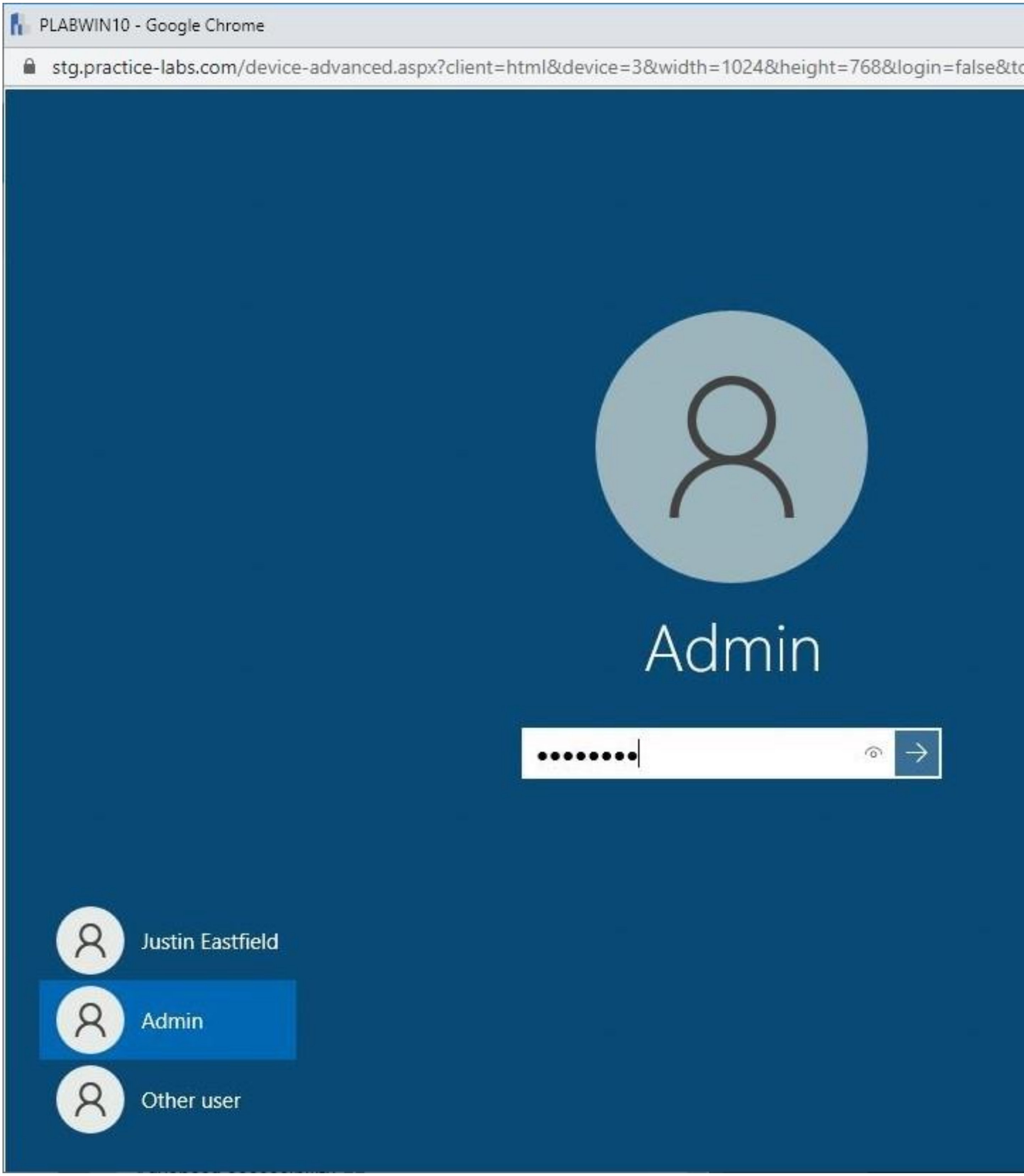
Connect to **PLABWIN10**.

Select **Admin** from the sign-in screen.

Use the password:

```
Passw0rd
```

Press **Enter**.



PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc

Figure 2.1 Screenshot of PLABWIN10 desktop: Required password is typed

in on the Admin login screen.

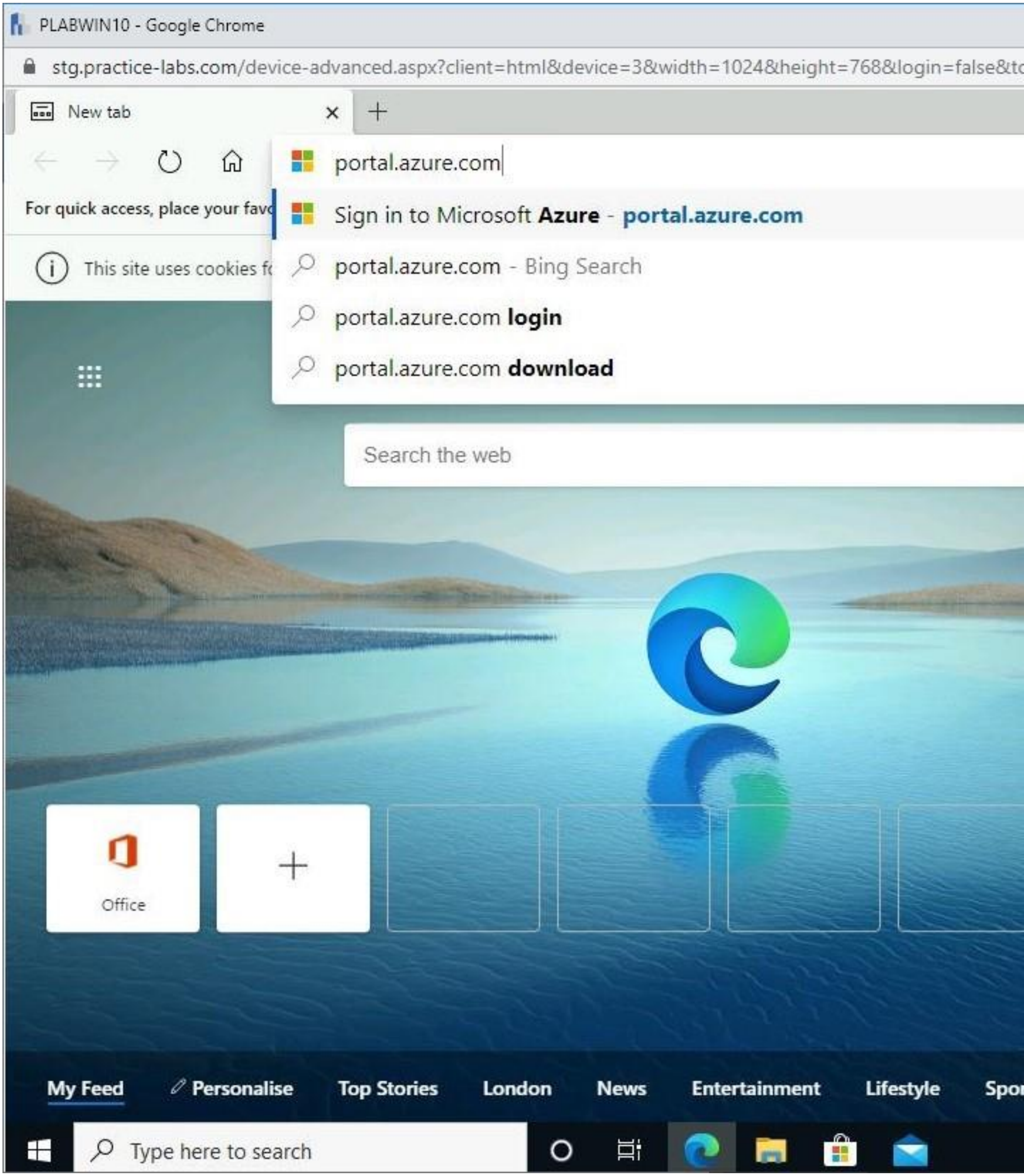
Step 2

Click **Microsoft Edge** on the taskbar.

Click in the browser’s address bar and type:

https://portal.azure.com

Press **Enter**.


PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc
New tab
For quick access, place your fav
This site uses cookies fo
Sign in to Microsoft Azure - portal.azure.com
portal.azure.com - Bing Search
portal.azure.com login
portal.azure.com download
Search the web
Office
My Feed
Personalise
Top Stories
London
News
Entertainment
Lifestyle
Spor
Type here to search

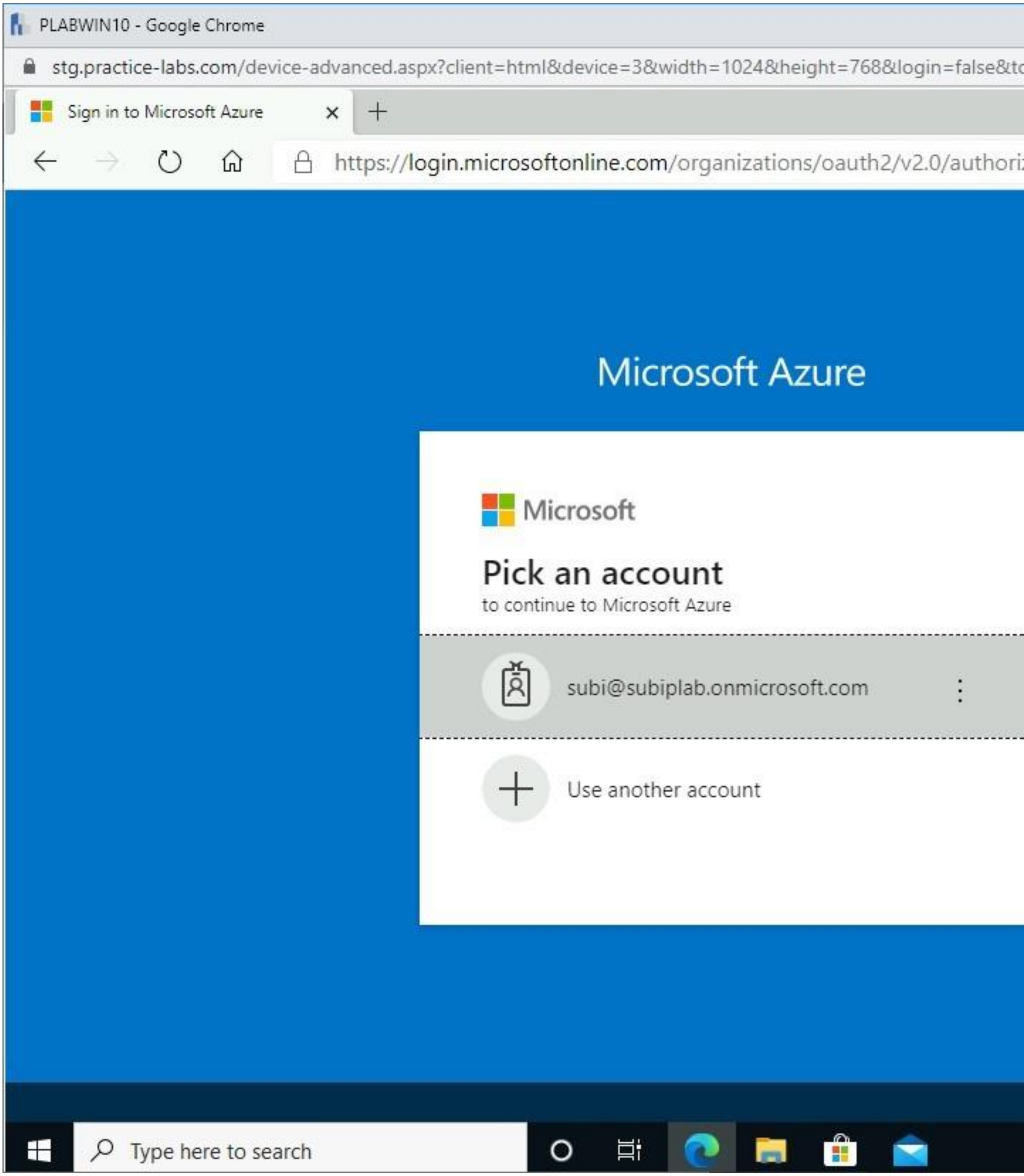
portal.azure.com

Figure 2.2 Screenshot of PLABWIN10 desktop: Required URL is typed into

the address bar on the web browser window.

Step 3

On the **Pick an account** message box, select your user account.


PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc
Sign in to Microsoft Azure
https://login.microsoftonline.com/organizations/oauth2/v2.0/authori
Type here to search

Microsoft Azure

Microsoft

Pick an account

to continue to Microsoft Azure

subi@subiplab.onmicrosoft.com

Use another account

Figure 2.3 Screenshot of PLABWIN10 desktop: Microsoft Pick an account

pane on the Microsoft Azure screen is displayed, showing the required login credentials selected.

Step 4

Enter the password for the account.

Press **Enter.**

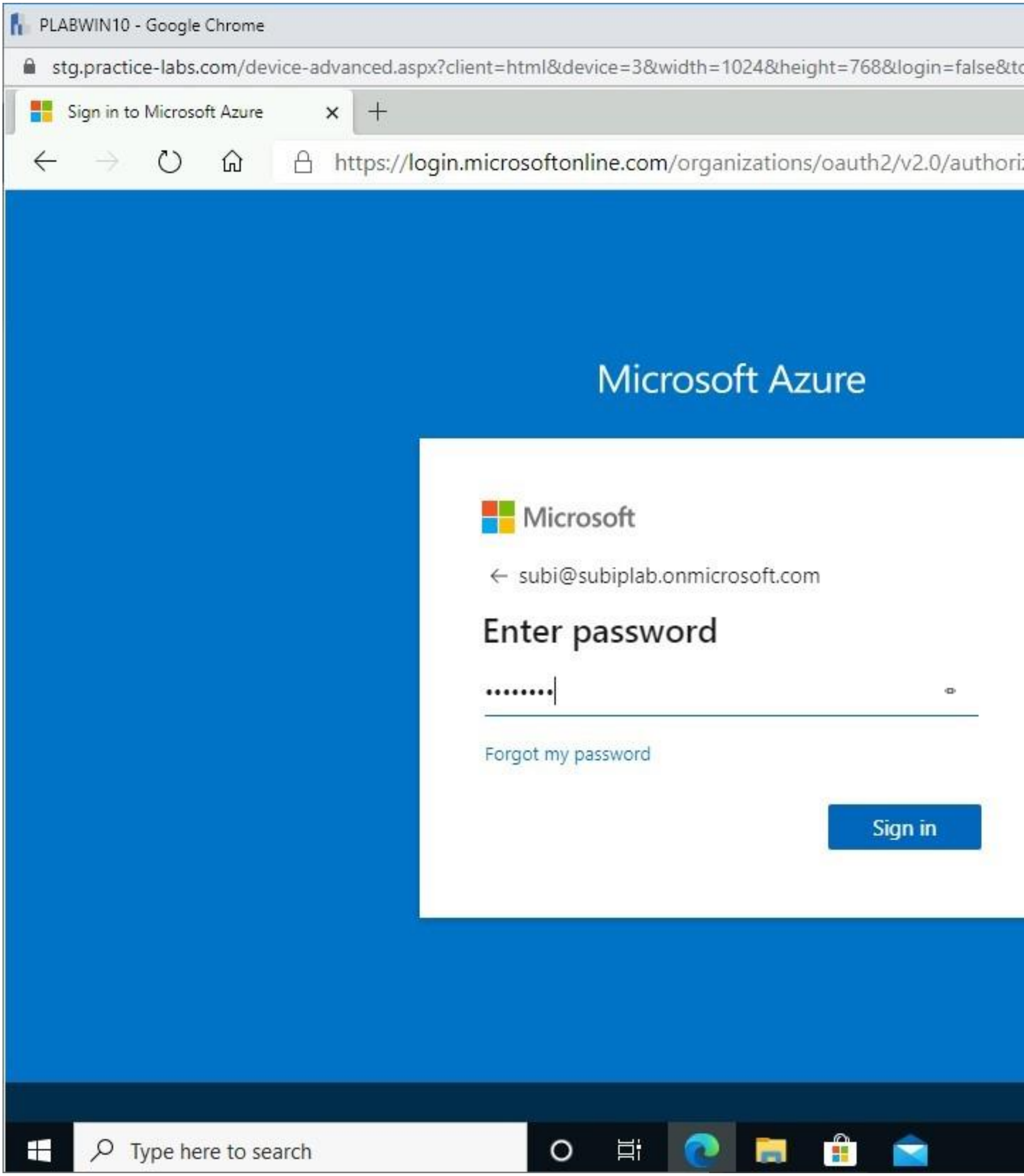

PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&to
Sign in to Microsoft Azure
https://login.microsoftonline.com/organizations/oauth2/v2.0/authori
Microsoft Azure
Microsoft
subi@subiplab.onmicrosoft.com
Enter password
Forgot my password
Sign in
Type here to search

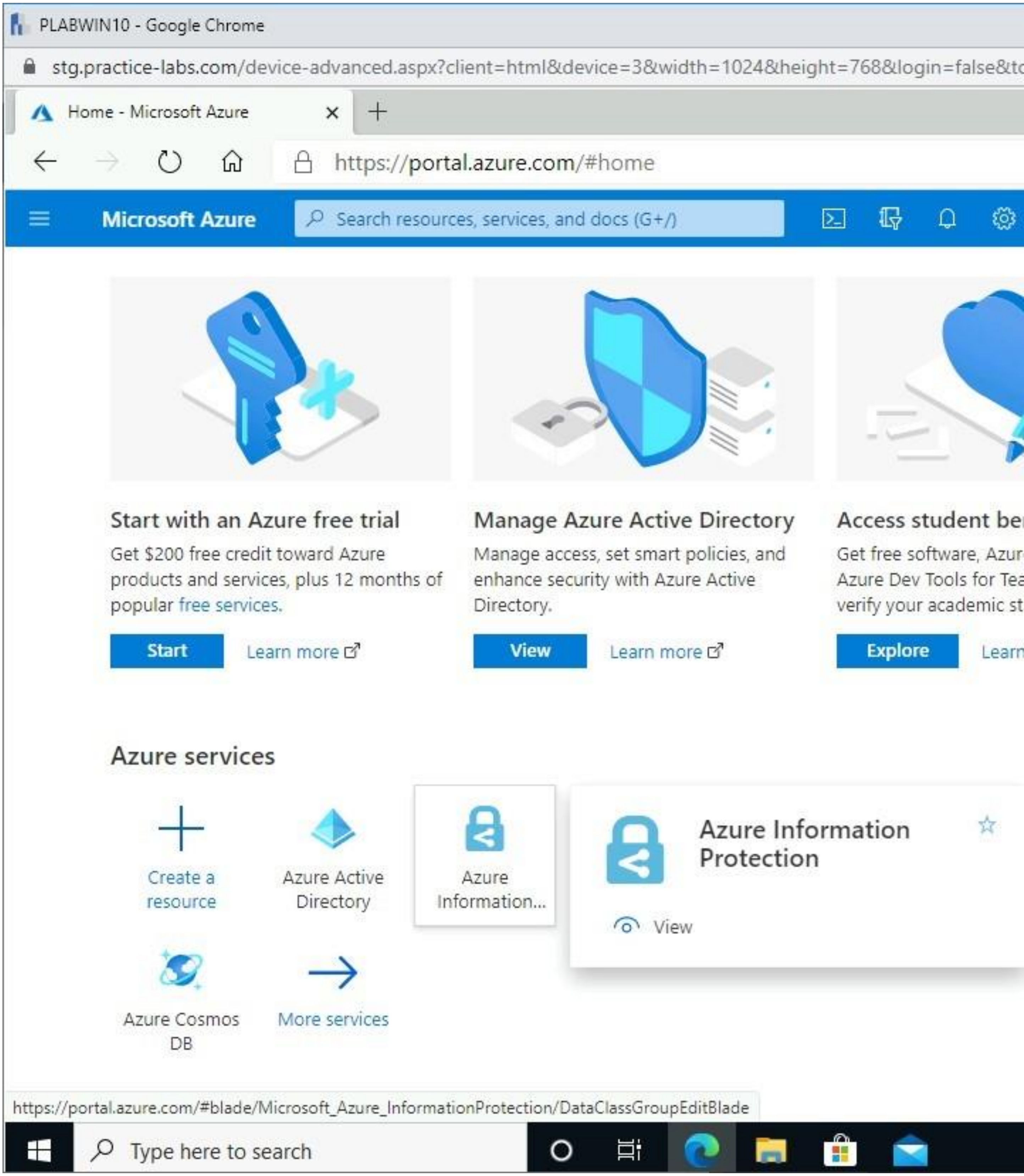
Figure 2.4 Screenshot of PLABWIN10 desktop: Microsoft Enter password

pane on the Microsoft Azure screen is displayed showing the required password typed-in, and the Sign in button highlighted.

Step 5

Select **Azure Information Protection** tile.

> ***Note:*** *If **Azure Information Protection** tile is not displayed, click on **More Services** or search for **Azure Information Protection** on the **Search resources, services, and docs** text box.*



PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&to
Home - Microsoft Azure
https://portal.azure.com/#home
Microsoft Azure
Search resources, services, and docs (G+/)
Start with an Azure free trial
Get $200 free credit toward Azure products and services, plus 12 months of popular free services.
Start
Learn more
Manage Azure Active Directory
Manage access, set smart policies, and enhance security with Azure Active Directory.
View
Learn more
Access student be
Get free software, Azur
Azure Dev Tools for Tea
verify your academic st
Explore
Learn
Azure services
Create a resource
Azure Active Directory
Azure Information...
Azure Information Protection
View
Azure Cosmos DB
More services
https://portal.azure.com/#blade/Microsoft_Azure_InformationProtection/DataClassGroupEditBlade
Type here to search

Figure 2.5 Screenshot of PLABWIN10 desktop: Azure Information

Protection option on the Microsoft Azure screen is selected.

Step 6

On the **Azure Information Protection | Labels** page, click **Generate default labels** from the middle pane.

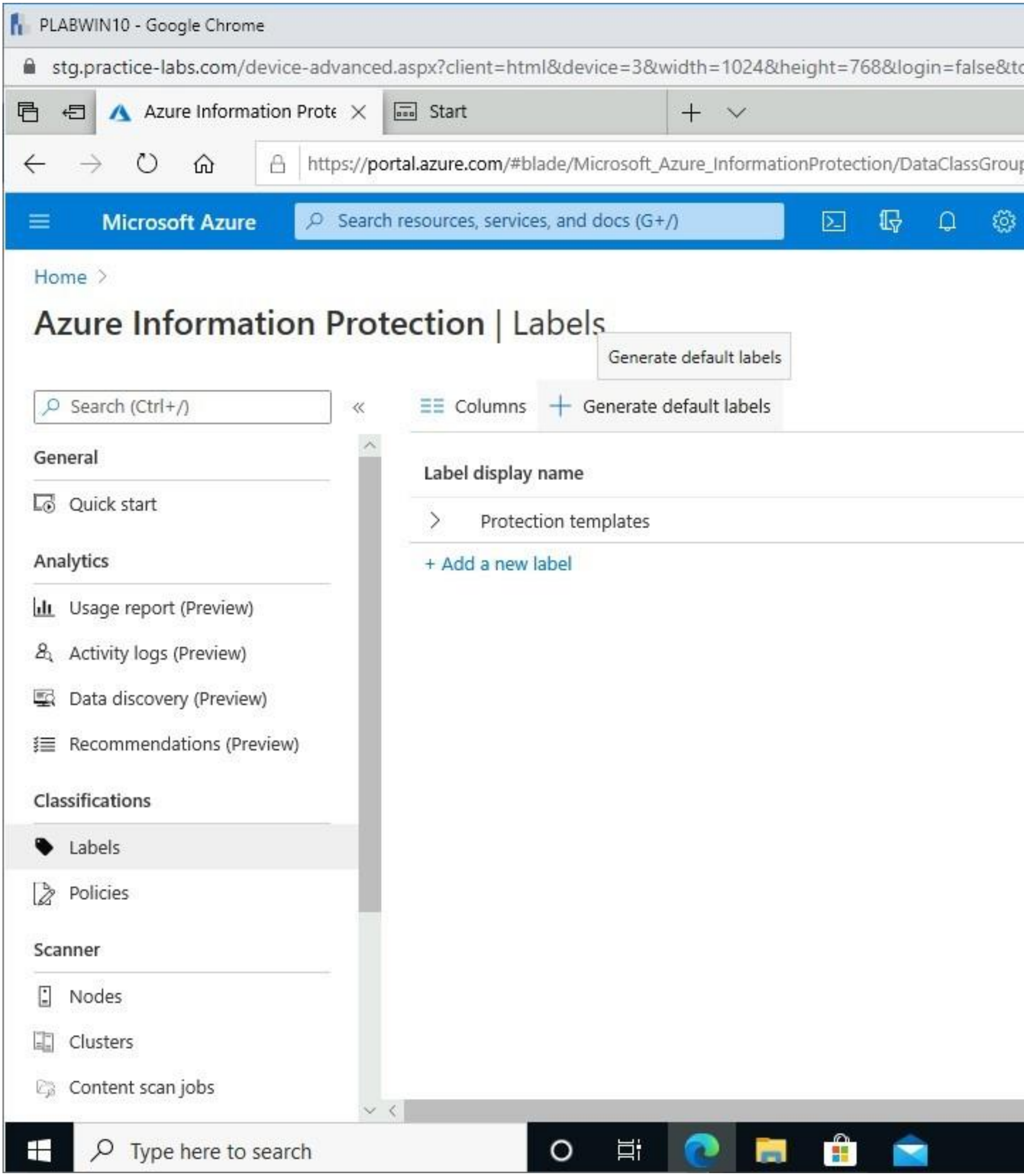


Figure 2.6 Screenshot of PLABWIN10 desktop: Generate default labels

option on the Microsoft Azure - Azure Information Protection | Labels screen is highlighted.

Step 7

There will be a momentary pause while **Microsoft Azure** generates the default labels, please wait.

A confirmation appears thereafter, indicating the successful generation of default labels.

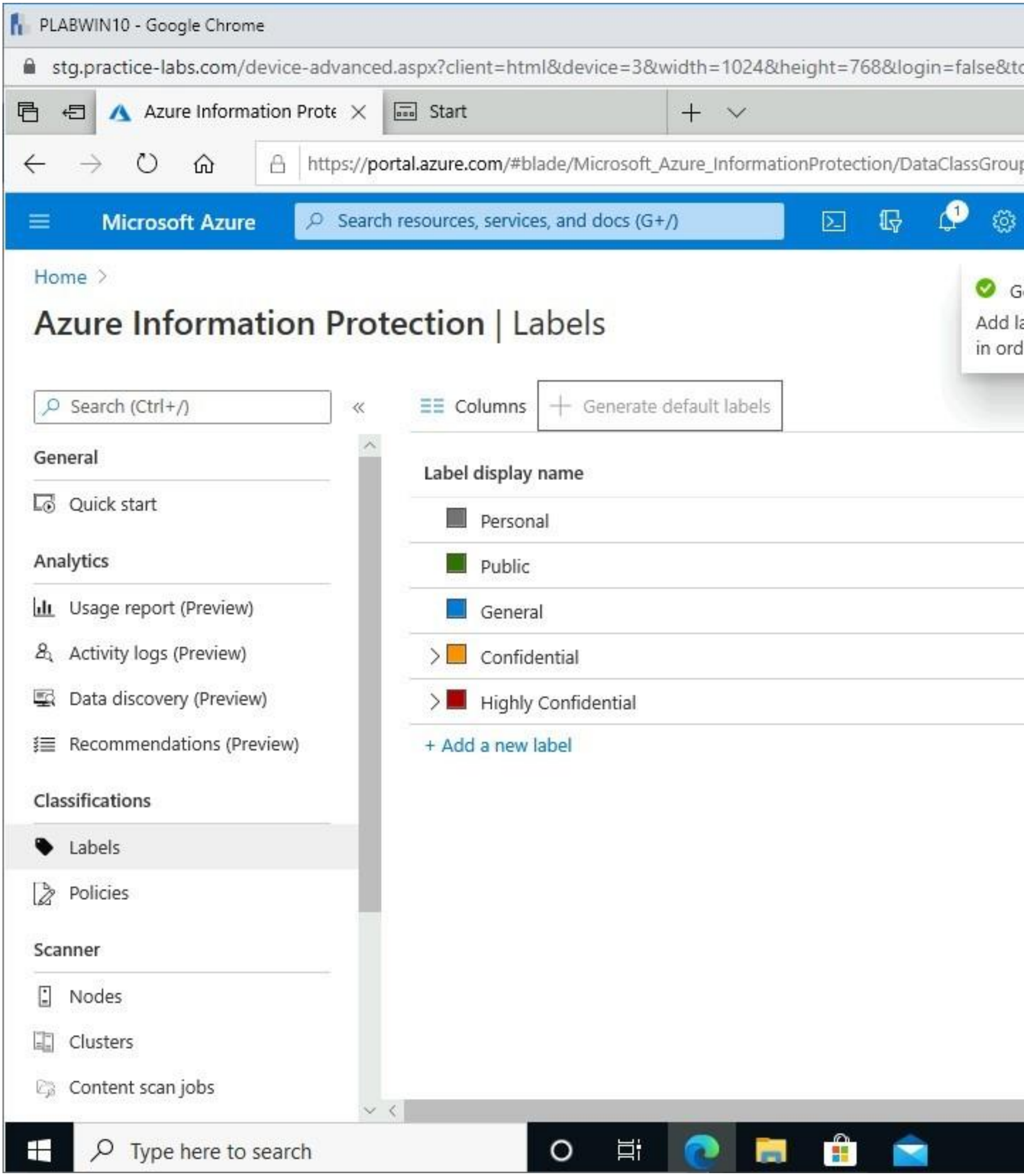
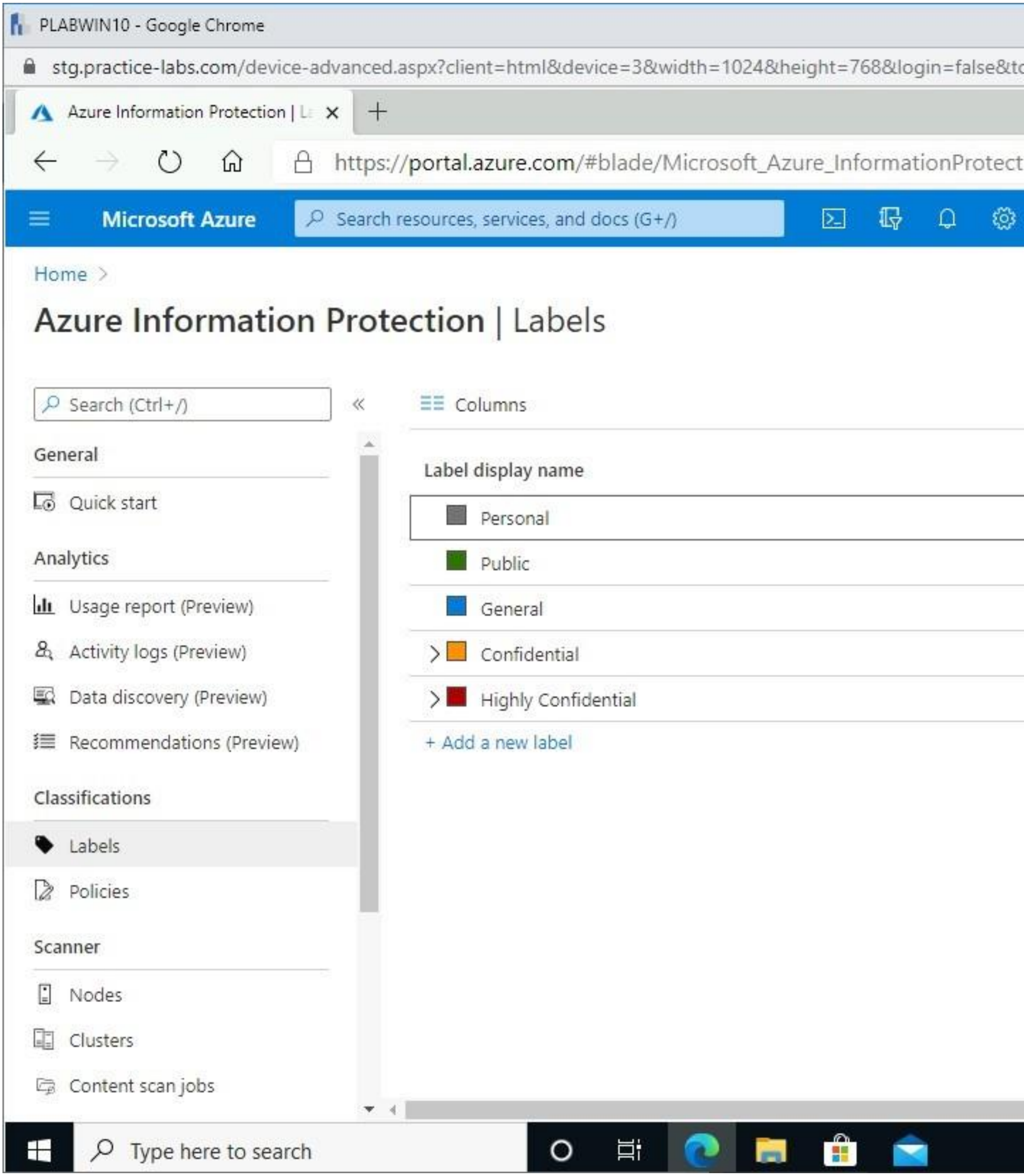


Figure 2.7 Screenshot of PLABWIN10 desktop: Generating default labels

completed notification is displayed on the Microsoft Azure - Azure Information Protection | Labels screen.

Step 8

Personal, **Public**, **General**, **Confidential** and **Highly Confidential** appear as default labels.


PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&t
Azure Information Protection | L
https://portal.azure.com/#blade/Microsoft_Azure_InformationProtect
Microsoft Azure
Search resources, services, and docs (G+/)
Home >
Azure Information Protection | Labels
Search (Ctrl+/)
General
Quick start
Analytics
Usage report (Preview)
Activity logs (Preview)
Data discovery (Preview)
Recommendations (Preview)
Classifications
Labels
Policies
Scanner
Nodes
Clusters
Content scan jobs
Columns
+ Add a new label
Type here to search

Label display name
Personal
Public
General
> Confidential
> Highly Confidential

Figure 2.8 Screenshot of PLABWIN10 desktop: Newly created default labels

are listed on the Microsoft Azure - Azure Information Protection | Labels screen.

Step 9

On the **Azure Information Protection** | **Labels** page, select **Policies** under the **Classifications** section.

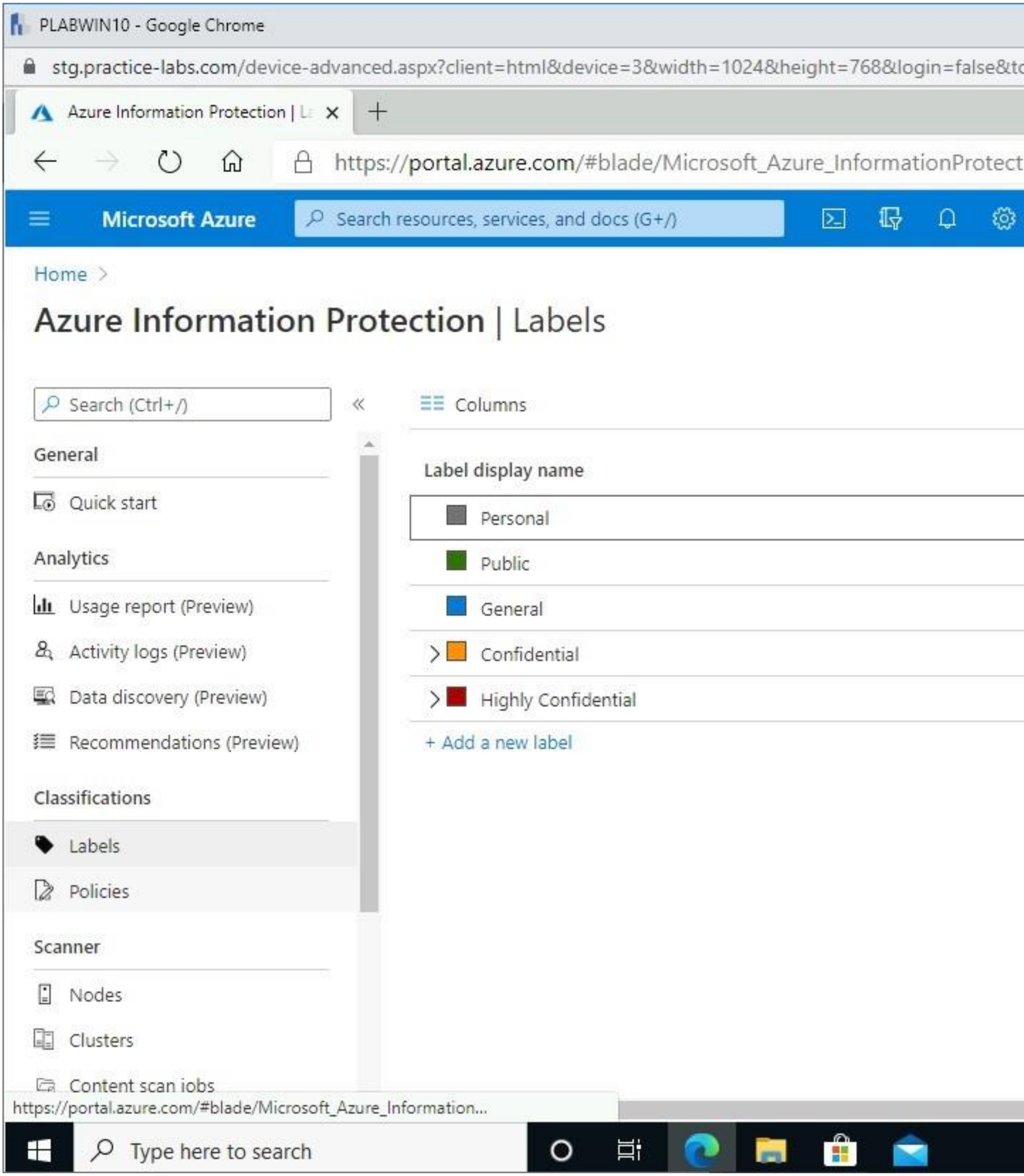

PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc
Azure Information Protection | La
https://portal.azure.com/#blade/Microsoft_Azure_InformationProtect
Microsoft Azure
Search resources, services, and docs (G+/)
Home >
Azure Information Protection | Labels
Search (Ctrl+/)
Columns
General
Quick start
Analytics
Usage report (Preview)
Activity logs (Preview)
Data discovery (Preview)
Recommendations (Preview)
Classifications
Labels
Policies
Scanner
Nodes
Clusters
Content scan jobs
Label display name
Personal
Public
General
Confidential
Highly Confidential
+ Add a new label
https://portal.azure.com/#blade/Microsoft_Azure_Information...
Type here to search

Figure 2.9 Screenshot of PLABWIN10 desktop: Policies option on the

navigation pane at the left on the Microsoft Azure - Azure Information Protection | Labels screen is selected.

Step 10

On the **Azure Information Protection | Policies** page, click on **Global.**

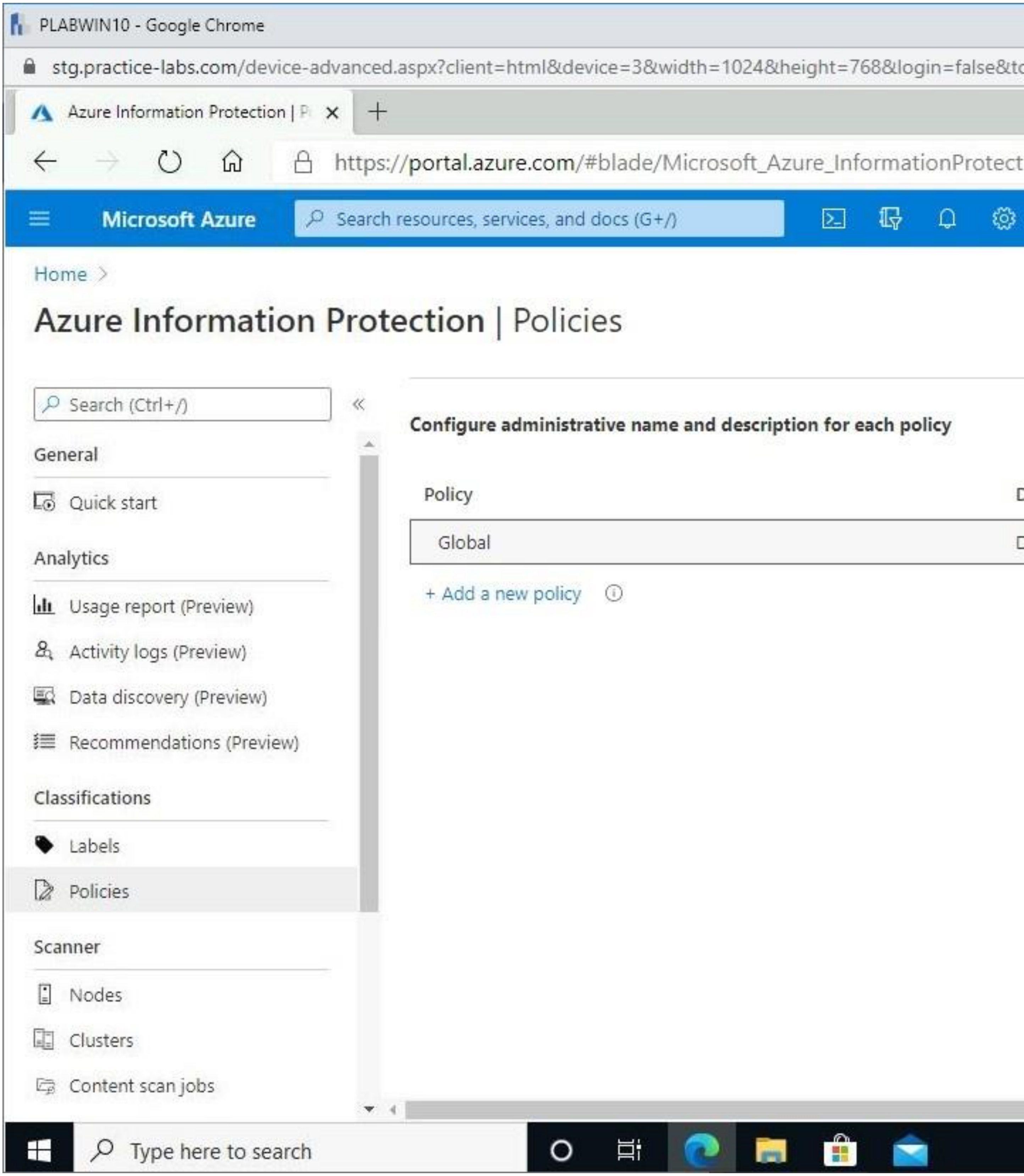
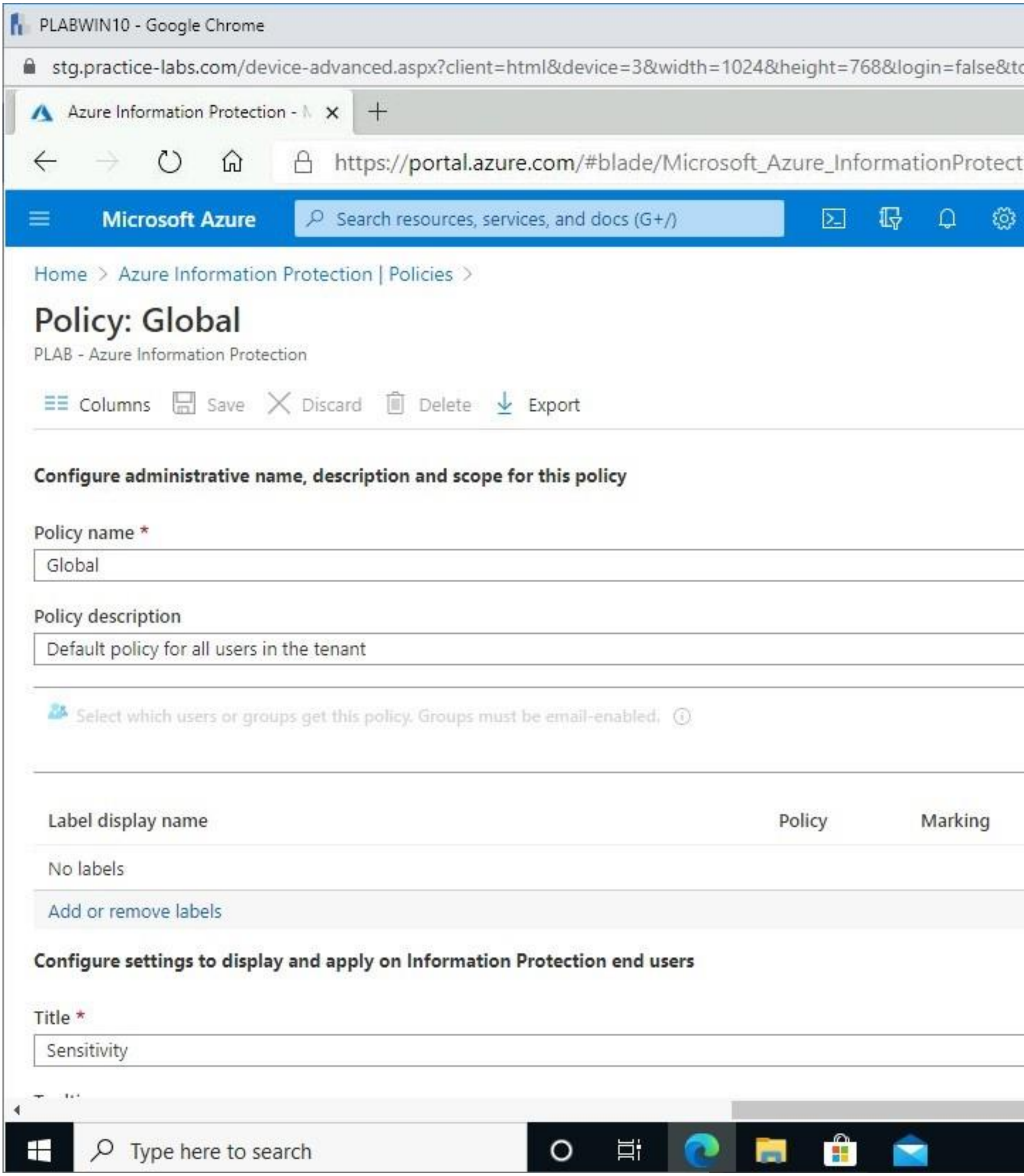

PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc
Azure Information Protection | P
https://portal.azure.com/#blade/Microsoft_Azure_InformationProtect
Microsoft Azure
Search resources, services, and docs (G+/)
Home >
Azure Information Protection | Policies
Search (Ctrl+/)
General
Quick start
Analytics
Usage report (Preview)
Activity logs (Preview)
Data discovery (Preview)
Recommendations (Preview)
Classifications
Labels
Policies
Scanner
Nodes
Clusters
Content scan jobs
Configure administrative name and description for each policy
Policy
Global
+ Add a new policy
Type here to search

Figure 2.10 Screenshot of PLABWIN10 desktop: Required list item on the

Microsoft Azure - Azure Information Protection | Policies screen is selected.

Step 11

On the **Policy: Global** page, under **Label display name,** click **Add or remove labels.**



PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc

Azure Information Protection - M

https://portal.azure.com/#blade/Microsoft_Azure_InformationProtect

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Azure Information Protection | Policies >

Policy: Global

PLAB - Azure Information Protection

Columns Save Discard Delete Export

Configure administrative name, description and scope for this policy

Policy name *

Global

Policy description

Default policy for all users in the tenant

Select which users or groups get this policy. Groups must be email-enabled.

Label display name	Policy	Marking
No labels		
Add or remove labels		

Configure settings to display and apply on Information Protection end users

Title *

Sensitivity

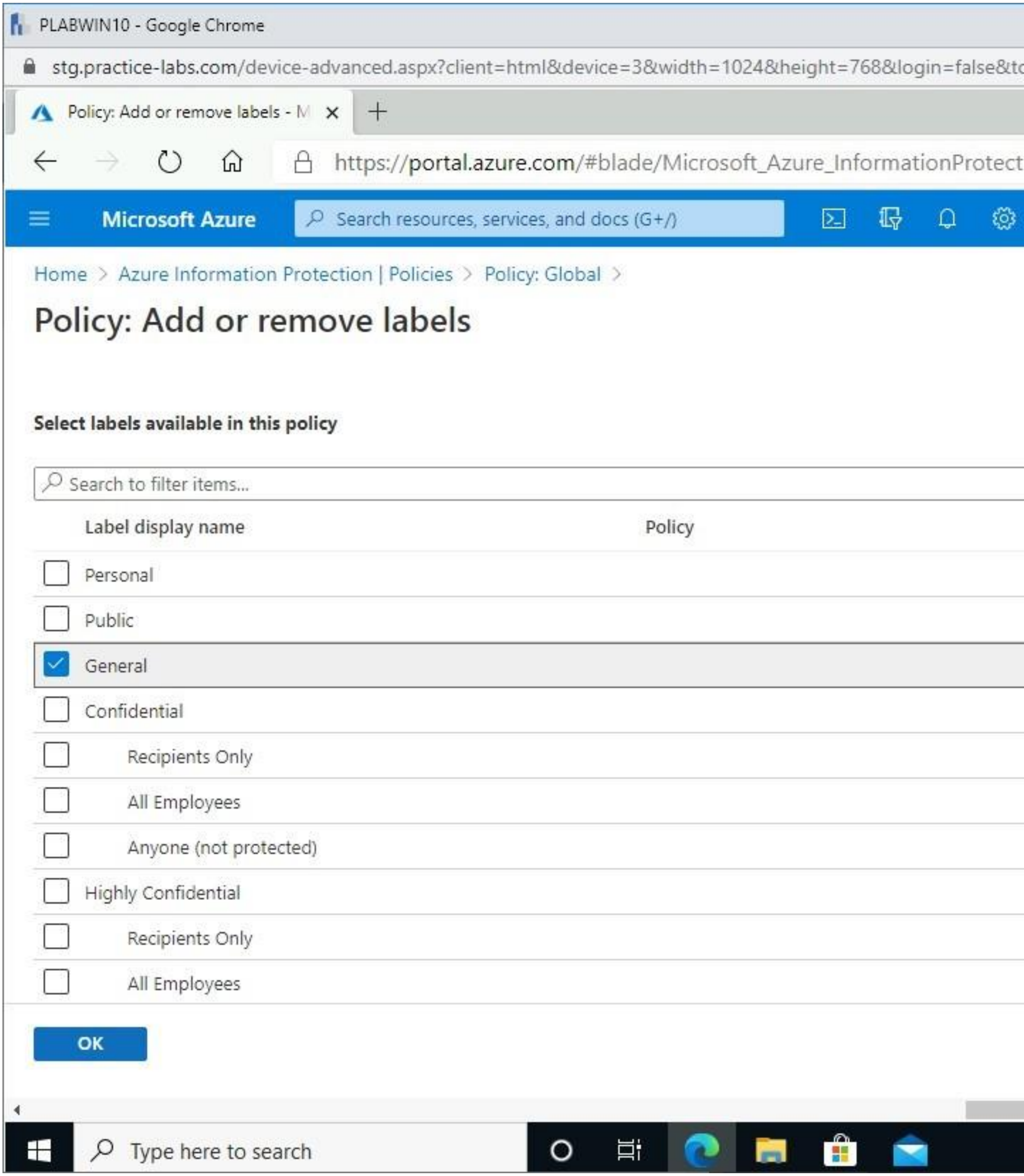
Figure 2.11 Screenshot of PLABWIN10 desktop: Add or remove labels link

on the Microsoft Azure - Policy: Global screen is selected.

Step 12

On the **Policy: Add or remove labels** page, select the **General** checkbox.

Click **OK.**



PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc
Policy: Add or remove labels - M
https://portal.azure.com/#blade/Microsoft_Azure_InformationProtect
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Azure Information Protection | Policies > Policy: Global >
Search to filter items...
OK
Type here to search

Policy: Add or remove labels

Select labels available in this policy

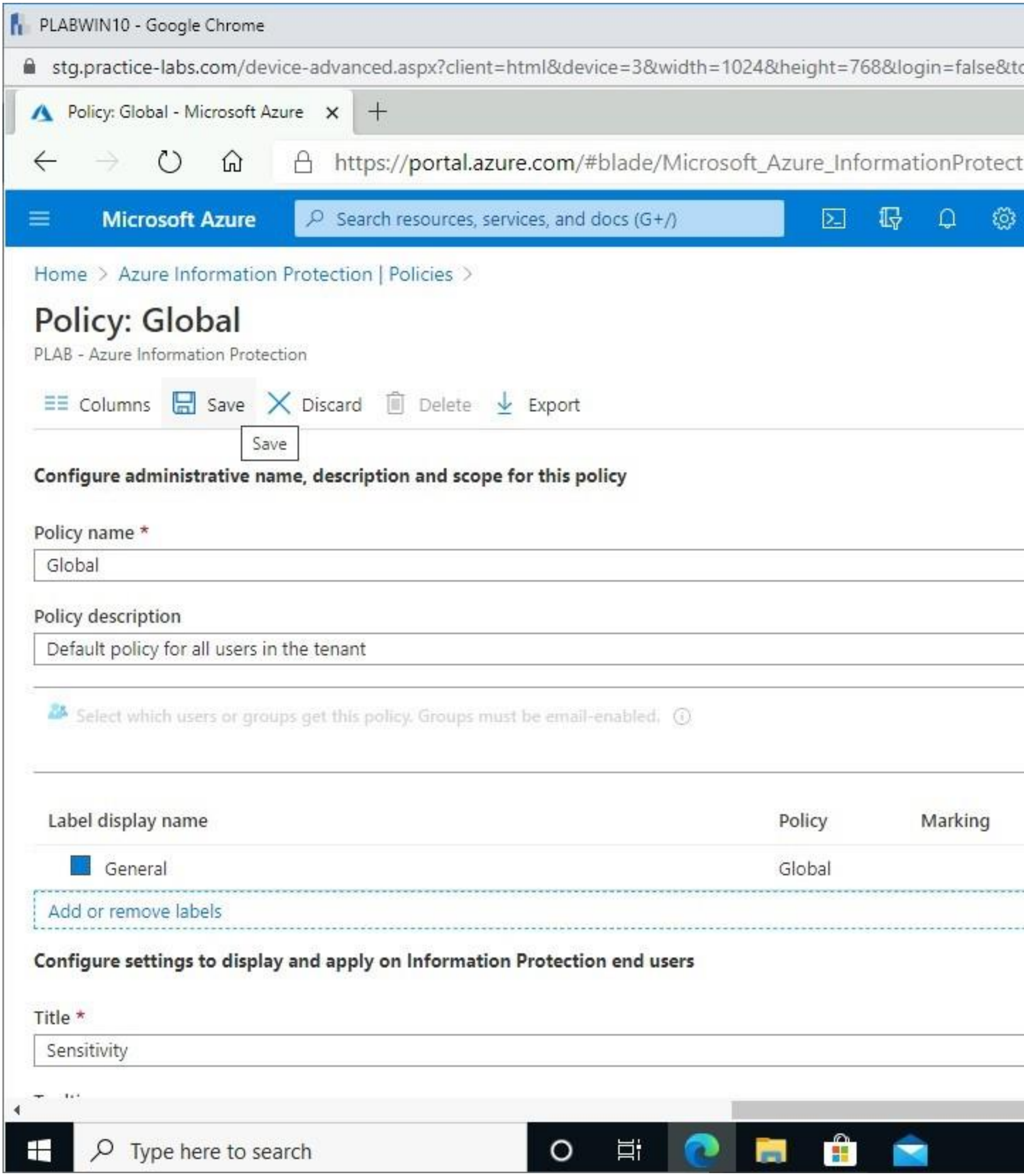
	Label display name	Policy
□	Personal	
□	Public	
☑	General	
□	Confidential	
□	Recipients Only	
□	All Employees	
□	Anyone (not protected)	
□	Highly Confidential	
□	Recipients Only	
□	All Employees	

Figure 2.12 Screenshot of PLABWIN10 desktop: Required selection is

performed on the Microsoft Azure - Policy: Add or remove labels screen.

Step 13

You are back on the **Policy: Global** page. Click **Save.**


PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc
Policy: Global - Microsoft Azure
https://portal.azure.com/#blade/Microsoft_Azure_InformationProtect
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Azure Information Protection | Policies >
Columns
Save
Discard
Delete
Export
Save
Add or remove labels
Type here to search

Policy: Global

PLAB - Azure Information Protection

Configure administrative name, description and scope for this policy

Policy name *

Global

Policy description

Default policy for all users in the tenant

Select which users or groups get this policy. Groups must be email-enabled.

Label display name	Policy	Marking
🟦 General	Global	

Configure settings to display and apply on Information Protection end users

Title *

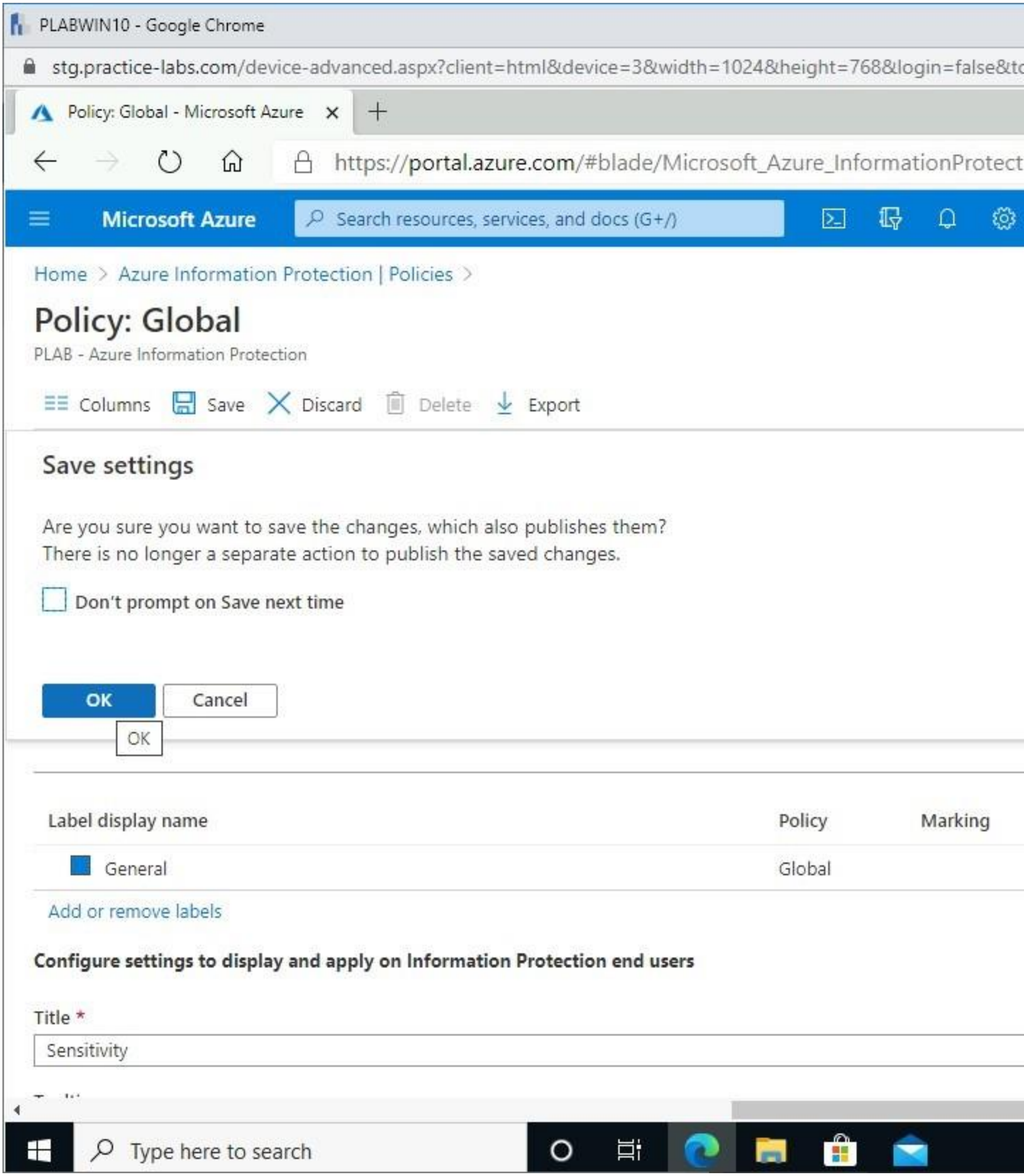
Sensitivity

Figure 2.13 Screenshot of PLABWIN10 desktop: Save option on the

Microsoft Azure - Policy: Global screen is highlighted.

Step 14

On the **Save settings** message box, click **OK.**



PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc
Policy: Global - Microsoft Azure
https://portal.azure.com/#blade/Microsoft_Azure_InformationProtect
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Azure Information Protection | Policies >
Columns
Save
Discard
Delete
Export
OK
Cancel
OK
Add or remove labels
Type here to search

Policy: Global

PLAB - Azure Information Protection

Save settings

Are you sure you want to save the changes, which also publishes them? There is no longer a separate action to publish the saved changes.

□ Don't prompt on Save next time

Label display name	Policy	Marking
General	Global	

Configure settings to display and apply on Information Protection end users

Title *

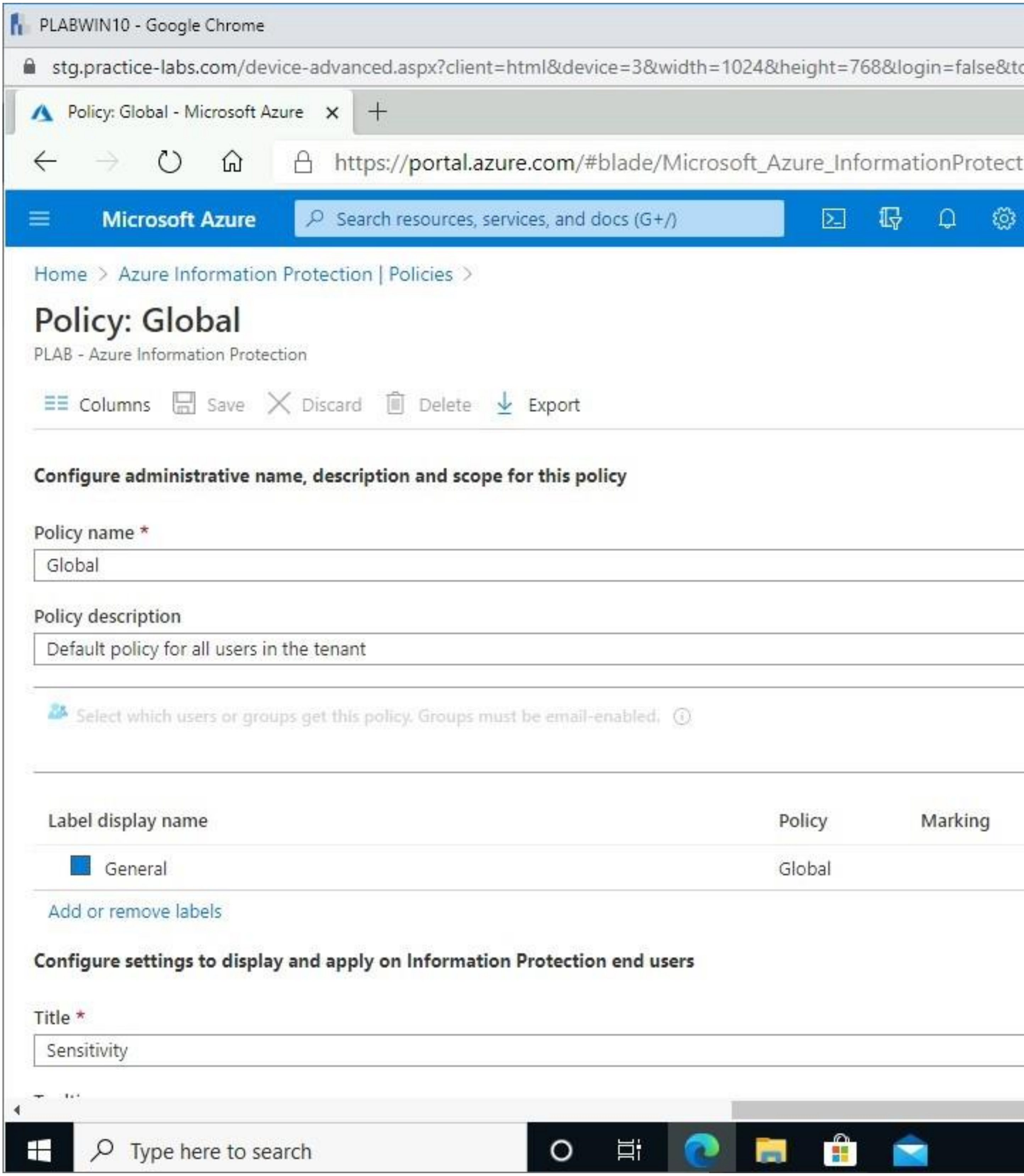
Sensitivity

Figure 2.14 Screenshot of PLABWIN10 desktop: OK button on the Save

settings notification displayed on the Microsoft Azure - Policy: Global screen is highlighted.

Step 15

Once you’ve saved the policy, click **Close.**



PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc

Policy: Global - Microsoft Azure

https://portal.azure.com/#blade/Microsoft_Azure_InformationProtect

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Azure Information Protection | Policies >

Policy: Global

PLAB - Azure Information Protection

Columns Save Discard Delete Export

Configure administrative name, description and scope for this policy

Policy name *

Global

Policy description

Default policy for all users in the tenant

Select which users or groups get this policy. Groups must be email-enabled.

Label display name	Policy	Marking
🟦 General	Global	

Add or remove labels

Configure settings to display and apply on Information Protection end users

Title *

Sensitivity

Type here to search

Figure 2.15 Screenshot of PLABWIN10 desktop: Close icon at the top-right

corner of the Microsoft Azure - Policy: Global screen is highlighted.

Step 16

Back on the **Azure Information Protection | Policies** page, scroll down the navigation pane on the left, and under the **Manage** section, select **Unified labeling**.

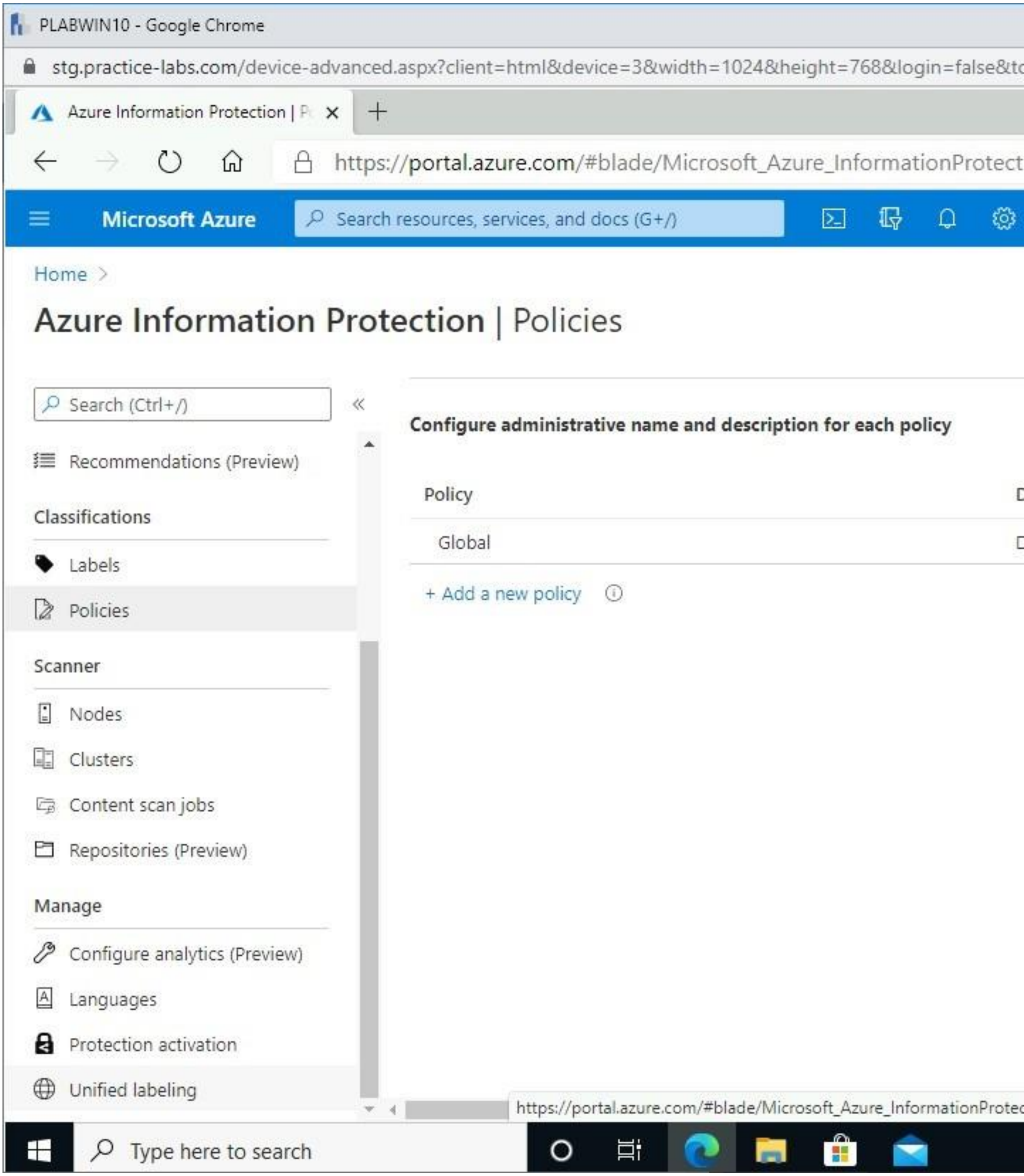

PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&to
Azure Information Protection | P
https://portal.azure.com/#blade/Microsoft_Azure_InformationProtect
Microsoft Azure
Search resources, services, and docs (G+/)
Home >
Azure Information Protection | Policies
Search (Ctrl+/)
Recommendations (Preview)
Classifications
Labels
Policies
Scanner
Nodes
Clusters
Content scan jobs
Repositories (Preview)
Manage
Configure analytics (Preview)
Languages
Protection activation
Unified labeling
Configure administrative name and description for each policy
Policy
Global
+ Add a new policy
https://portal.azure.com/#blade/Microsoft_Azure_InformationProtec
Type here to search

Figure 2.16 Screenshot of PLABWIN10 desktop: Unified labeling option on

the navigation pane at the left on the Microsoft Azure - Azure Information Protection | Policies screen is selected.

Task 2 - Migrate AIP Labels to Office 365 Security and Compliance Center

AIP labels are manageable either in Microsoft Azure or Office 365 Security and Compliance. Beginning March 2021, however, unified labeling will be the new method for managing labels in Azure tenant. Unified labeling is managed in Office 365 Security and Compliance.

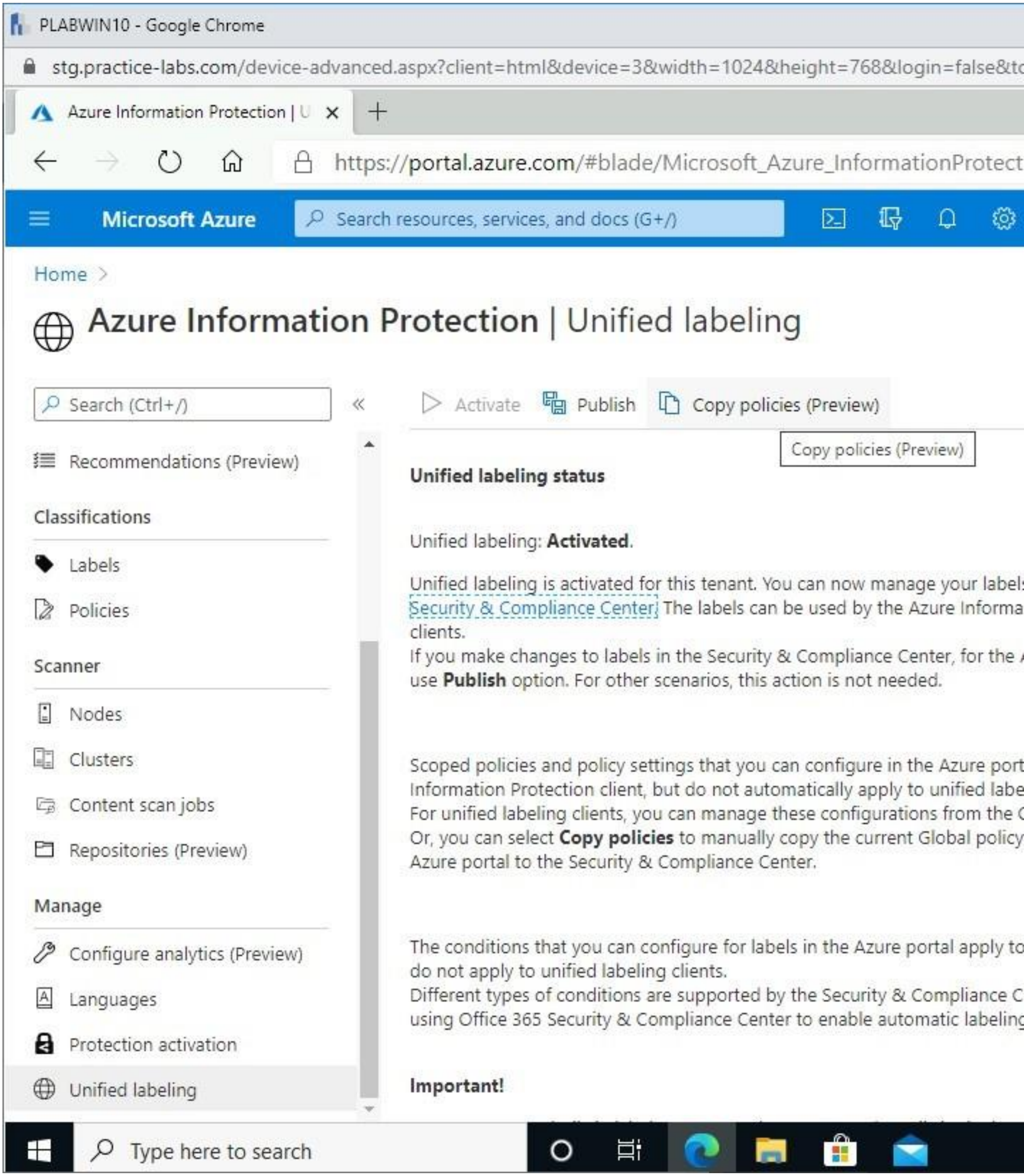
In the previous task, you generated the default labels in Microsoft Azure. It is recommended that these default labels be copied to Office 365 Security and Compliance first before creating the conditions that will classify Office documents.

In this task, you will migrate AIP labels from Microsoft Azure to Office 365 Security and Compliance.

Step 1

Ensure you are connected to **PLABWIN10** and are in the **Azure Information Protection | Unified Labeling** page.

Select **Copy policies (Preview**).


PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&t
Azure Information Protection | U ×
https://portal.azure.com/#blade/Microsoft_Azure_InformationProtect
Microsoft Azure
Search resources, services, and docs (G+/)
Home >
Azure Information Protection | Unified labeling
Search (Ctrl+/)
«
Activate
Publish
Copy policies (Preview)
Copy policies (Preview)
Recommendations (Preview)
Classifications
Labels
Policies
Scanner
Nodes
Clusters
Content scan jobs
Repositories (Preview)
Manage
Configure analytics (Preview)
Languages
Protection activation
Unified labeling
Type here to search

Unified labeling status

Unified labeling: **Activated**.

Unified labeling is activated for this tenant. You can now manage your label
Security & Compliance Center. The labels can be used by the Azure Informa
clients.
If you make changes to labels in the Security & Compliance Center, for the
use **Publish** option. For other scenarios, this action is not needed.

Scoped policies and policy settings that you can configure in the Azure port
Information Protection client, but do not automatically apply to unified labe
For unified labeling clients, you can manage these configurations from the
Or, you can select **Copy policies** to manually copy the current Global policy
Azure portal to the Security & Compliance Center.

The conditions that you can configure for labels in the Azure portal apply to
do not apply to unified labeling clients.
Different types of conditions are supported by the Security & Compliance C
using Office 365 Security & Compliance Center to enable automatic labeling

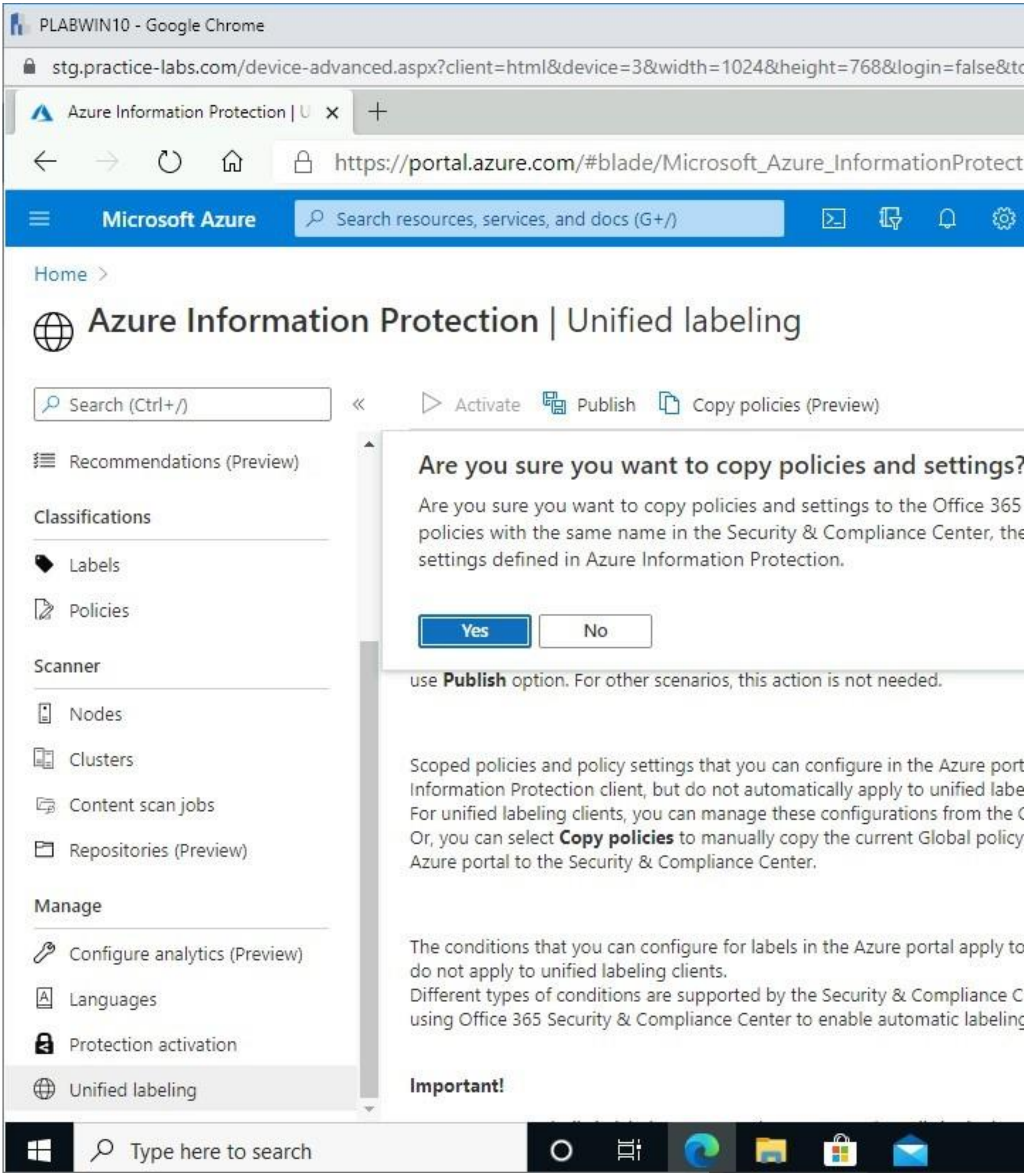
Important!

Figure 2.17 Screenshot of PLABWIN10 desktop: Copy policies (Preview)

option on the Microsoft Azure - Azure Information Protection | Unified labeling screen is selected.

Step 2

Click **Yes** in the **Are you sure you want to copy policies and settings?** prompt.


PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&to
Azure Information Protection | U
https://portal.azure.com/#blade/Microsoft_Azure_InformationProtect
Microsoft Azure
Search resources, services, and docs (G+/)
Home >
Azure Information Protection | Unified labeling
Search (Ctrl+/)
Activate
Publish
Copy policies (Preview)
Recommendations (Preview)
Classifications
Labels
Policies
Scanner
Nodes
Clusters
Content scan jobs
Repositories (Preview)
Manage
Configure analytics (Preview)
Languages
Protection activation
Unified labeling
Yes
No
Type here to search

Are you sure you want to copy policies and settings?

Are you sure you want to copy policies and settings to the Office 365
policies with the same name in the Security & Compliance Center, the
settings defined in Azure Information Protection.

use **Publish** option. For other scenarios, this action is not needed.

Scoped policies and policy settings that you can configure in the Azure port
Information Protection client, but do not automatically apply to unified labe
For unified labeling clients, you can manage these configurations from the C
Or, you can select **Copy policies** to manually copy the current Global policy
Azure portal to the Security & Compliance Center.

The conditions that you can configure for labels in the Azure portal apply to
do not apply to unified labeling clients.
Different types of conditions are supported by the Security & Compliance C
using Office 365 Security & Compliance Center to enable automatic labeling

Important!

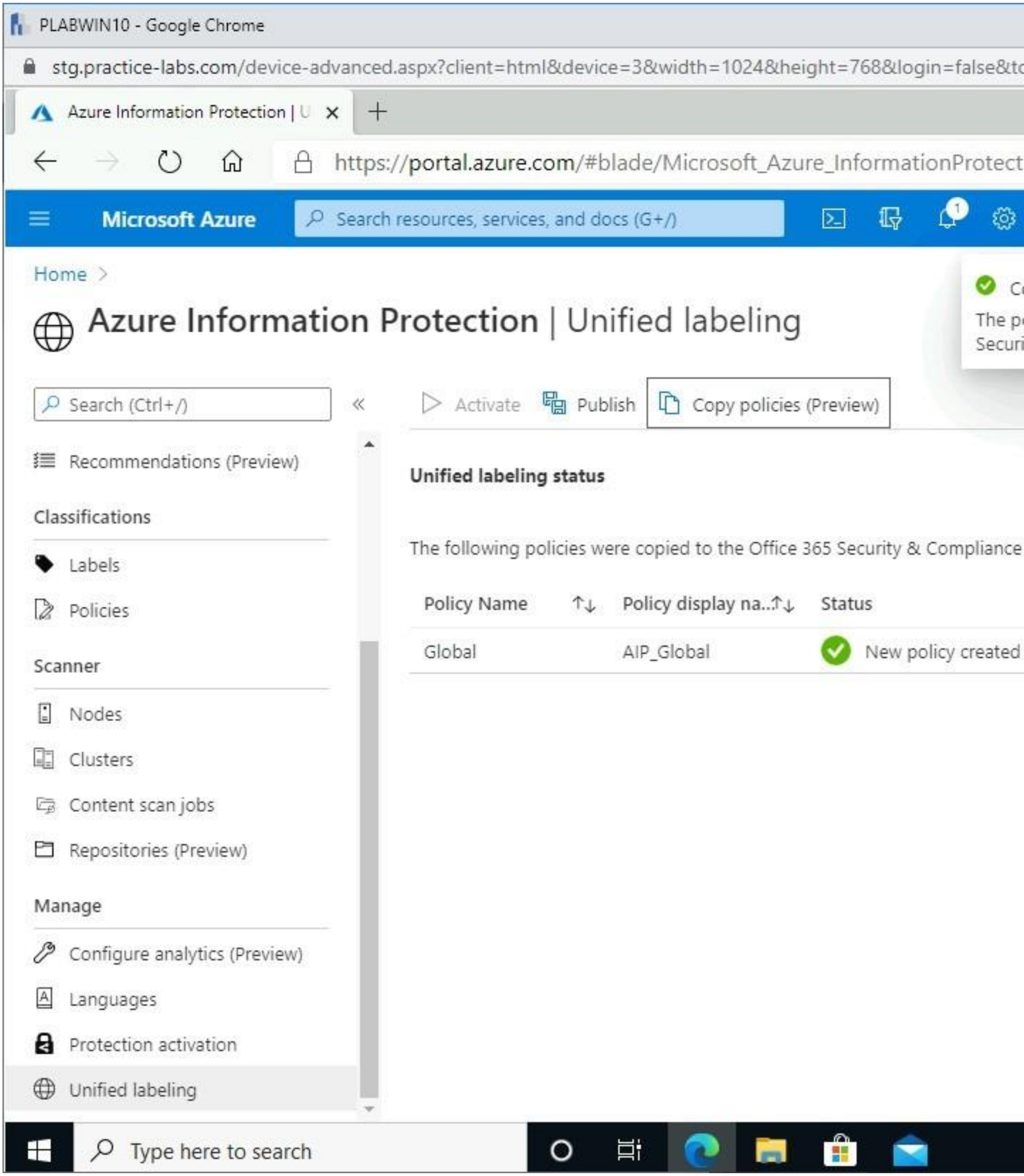
Figure 2.18 Screenshot of PLABWIN10 desktop: Yes button on the Are you

sure you want to copy policies and settings notification is highlighted.

Step 3

There will be a momentary pause while the default labels are copied.

Microsoft Azure confirms a successful copy of the policies to **Office 365 Security and Compliance Center**.



PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc
Azure Information Protection | U
https://portal.azure.com/#blade/Microsoft_Azure_InformationProtect
Microsoft Azure
Search resources, services, and docs (G+/)
Home >
Search (Ctrl+/)
Recommendations (Preview)
Classifications
Labels
Policies
Scanner
Nodes
Clusters
Content scan jobs
Repositories (Preview)
Manage
Configure analytics (Preview)
Languages
Protection activation
Unified labeling
Activate
Publish
Copy policies (Preview)
Type here to search

Azure Information Protection | Unified labeling

Unified labeling status

The following policies were copied to the Office 365 Security & Compliance

Policy Name	Policy display na...	Status
Global	AIP_Global	✓ New policy created

Co

The p

Securi

Figure 2.19 Screenshot of PLABWIN10 desktop: Copy policies completed

successfully notification is displayed on the Microsoft Azure - Azure Information Protection | Unified labeling screen.

Task 3 - Create a Custom Label

Although the default labels supplied by AIP encompass a wide variety of sensitive information, you can create a custom label to further test the full capability of AIP.

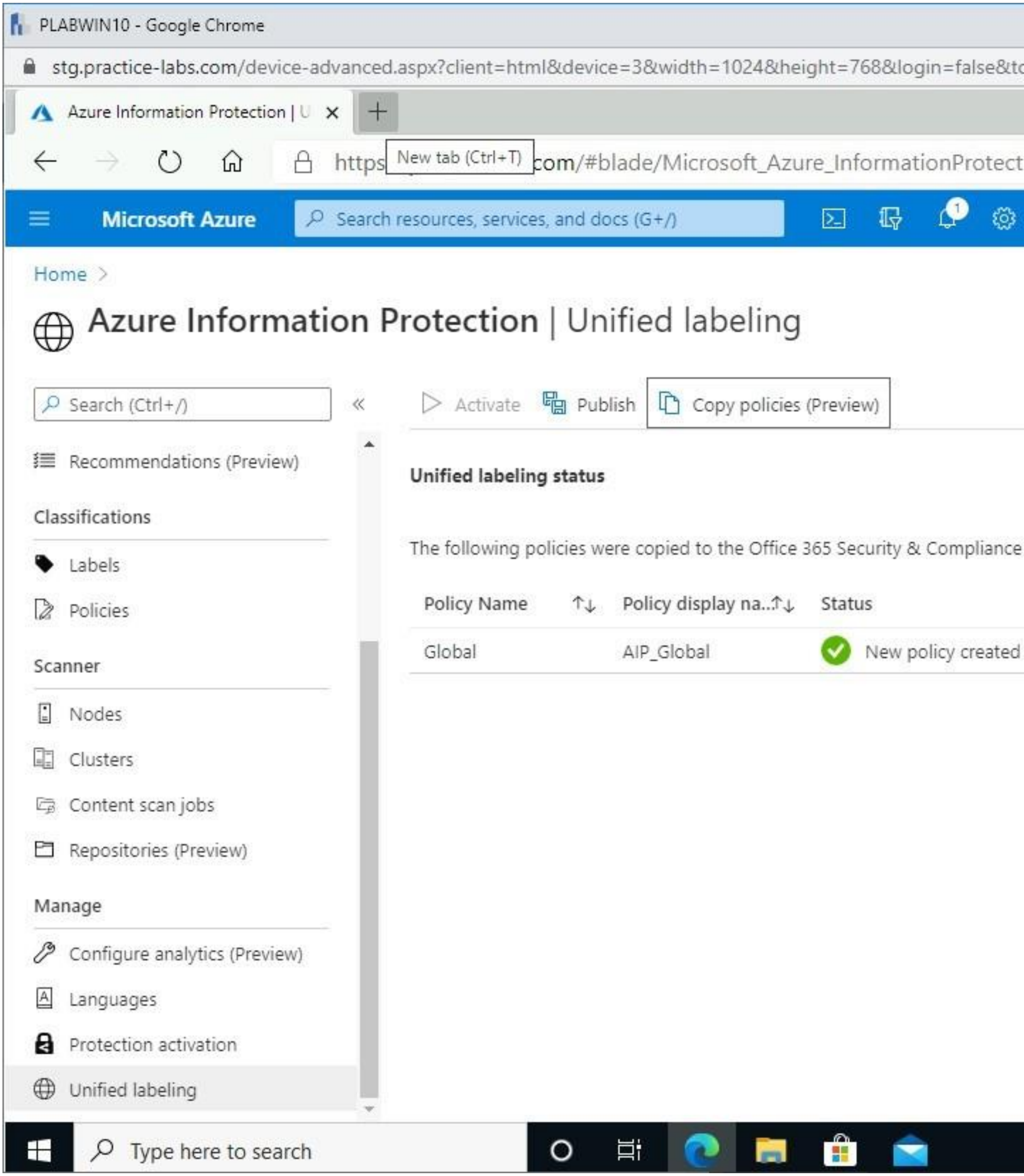
With a custom label, you can automatically classify and protect Office documents with phrases or keywords.

In this task, you will create a custom label with its own set of conditions.

Step 1

Ensure you are connected to **PLABWIN10,** and the **Azure Information Protection | Unified Labeling** page is open.

Click the **New tab (+)** button to open a new browser tab.


PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&to
Azure Information Protection | U
New tab (Ctrl+T)
https
com/#blade/Microsoft_Azure_InformationProtect
Microsoft Azure
Search resources, services, and docs (G+/)
Home >
Search (Ctrl+/)
Activate
Publish
Copy policies (Preview)
Recommendations (Preview)
Classifications
Labels
Policies
Scanner
Nodes
Clusters
Content scan jobs
Repositories (Preview)
Manage
Configure analytics (Preview)
Languages
Protection activation
Unified labeling
Type here to search

Azure Information Protection | Unified labeling

Unified labeling status

The following policies were copied to the Office 365 Security & Compliance

Policy Name ↑↓	Policy display na..↑↓	Status
Global	AIP_Global	✓ New policy created

Figure 2.20 Screenshot of PLABWIN10 desktop: New tab icon on the web

browser window is highlighted.

Step 2

In the new browser tab, type:

portal.office.com

Press **Enter**.

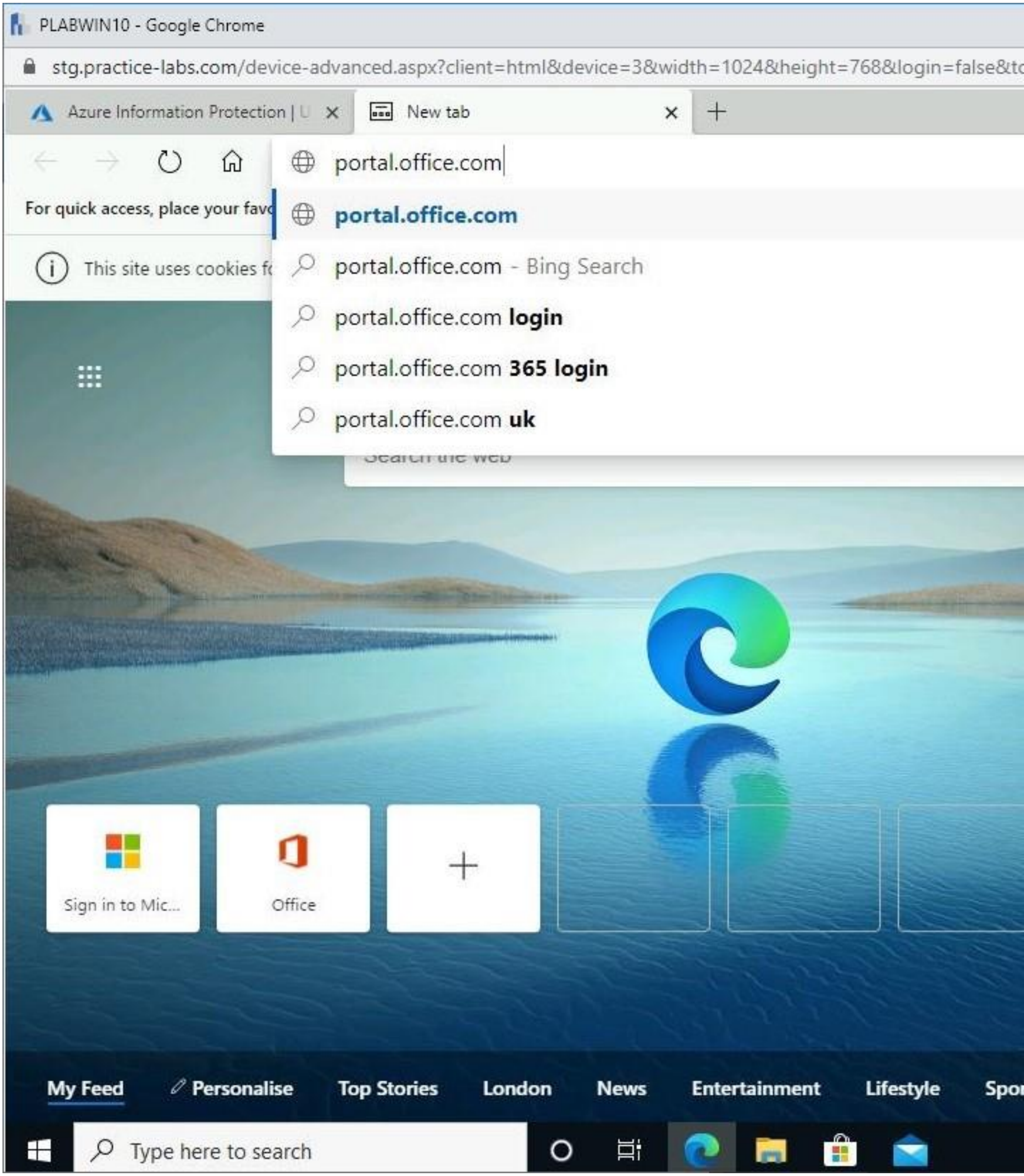

PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc
Azure Information Protection | U
New tab
portal.office.com
portal.office.com
portal.office.com - Bing Search
portal.office.com login
portal.office.com 365 login
portal.office.com uk
For quick access, place your fav
This site uses cookies fo
Sign in to Mic...
Office
My Feed
Personalise
Top Stories
London
News
Entertainment
Lifestyle
Spor
Type here to search

Figure 2.21 Screenshot of PLABWIN10 desktop: Required URL is typed

into the address bar on the web browser window.

Step 3

You will automatically sign in to Office 365 portal.

Click the **Admin** tile.

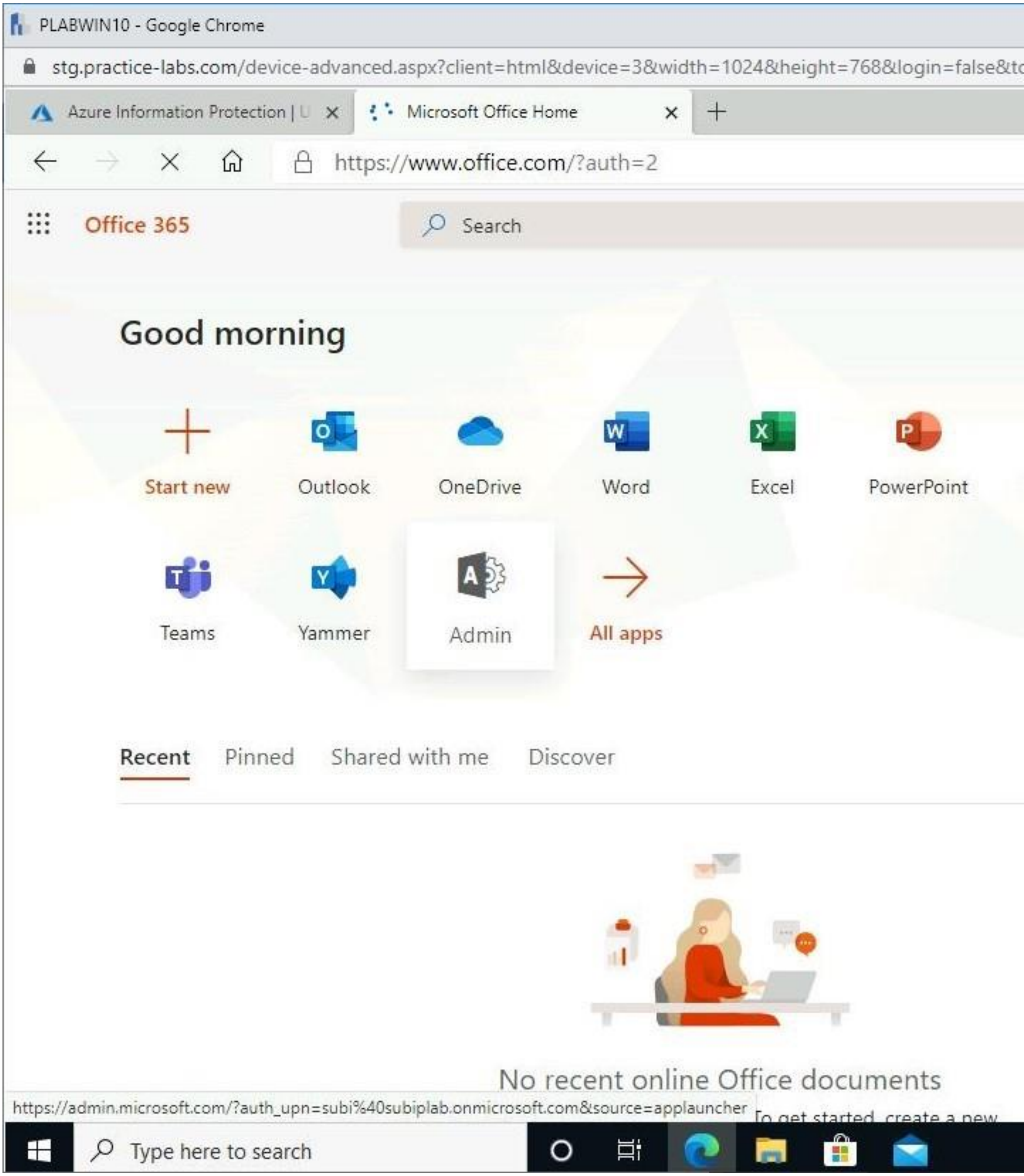

PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc
Azure Information Protection | U
Microsoft Office Home
https://www.office.com/?auth=2
Office 365
Search
Good morning
Start new
Outlook
OneDrive
Word
Excel
PowerPoint
Teams
Yammer
Admin
All apps
Recent
Pinned
Shared with me
Discover
No recent online Office documents
To get started, create a new
https://admin.microsoft.com/?auth_upn=subi%40subiplab.onmicrosoft.com&source=applauncher
Type here to search

Figure 2.22 Screenshot of PLABWIN10 desktop: Admin option on the

Office 365 home screen is selected.

Step 4

Click **Show all** from the left navigation pane in the **Microsoft 365 admin center**.

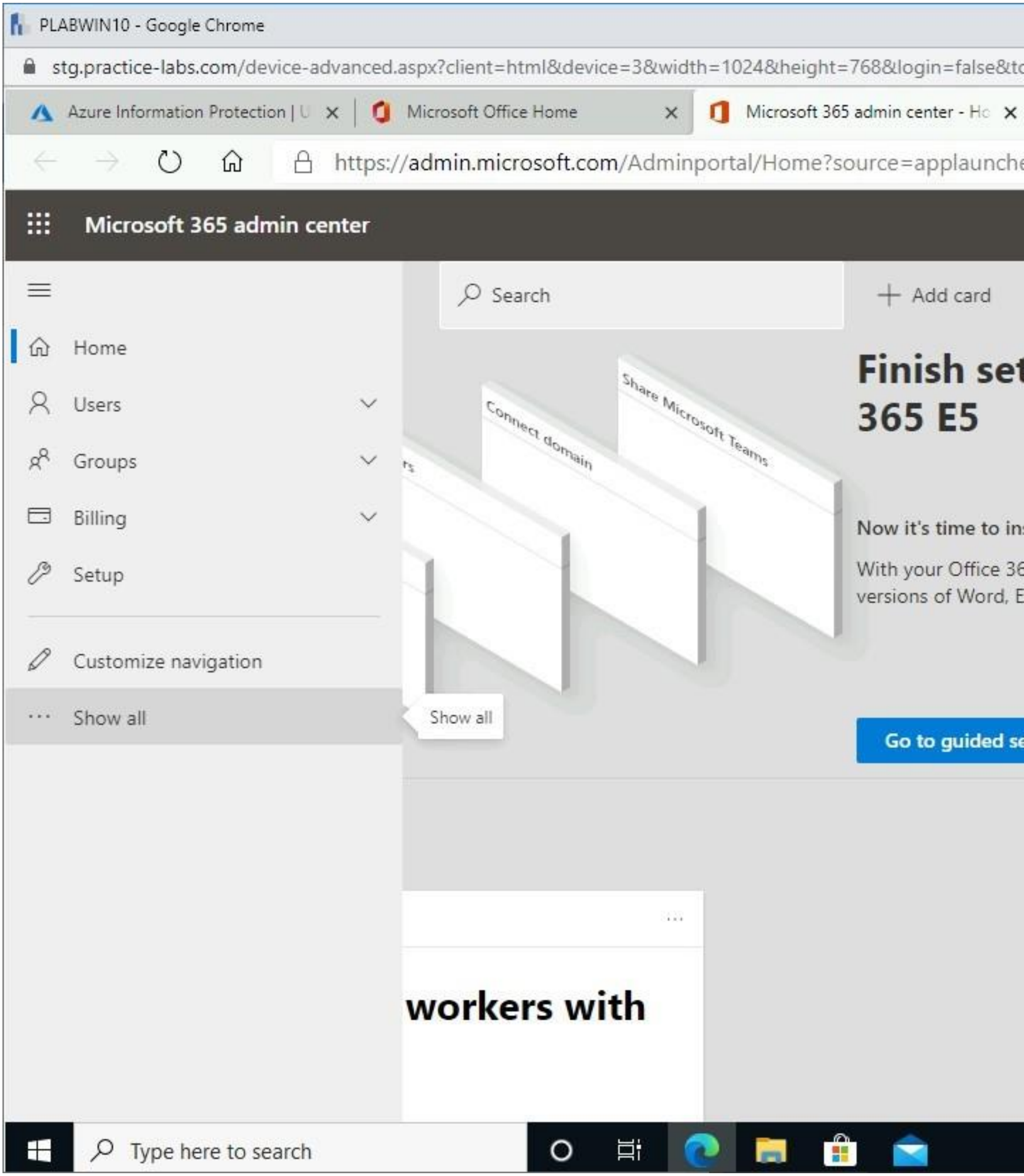

PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc
Azure Information Protection | U
Microsoft Office Home
Microsoft 365 admin center - Ho
https://admin.microsoft.com/Adminportal/Home?source=applaunche
Microsoft 365 admin center
Home
Users
Groups
Billing
Setup
Customize navigation
Show all
Search
Add card
Share Microsoft Teams
Connect domain
Show all
Finish set
365 E5
Now it's time to in
With your Office 36
versions of Word, E
Go to guided se
workers with
Type here to search

Figure 2.23 Screenshot of PLABWIN10 desktop: Show all menu-option on

the navigation pane at the left on the Microsoft 365 admin center screen is selected.

Step 5

Scroll down to **Admin centers** and select **Security**.

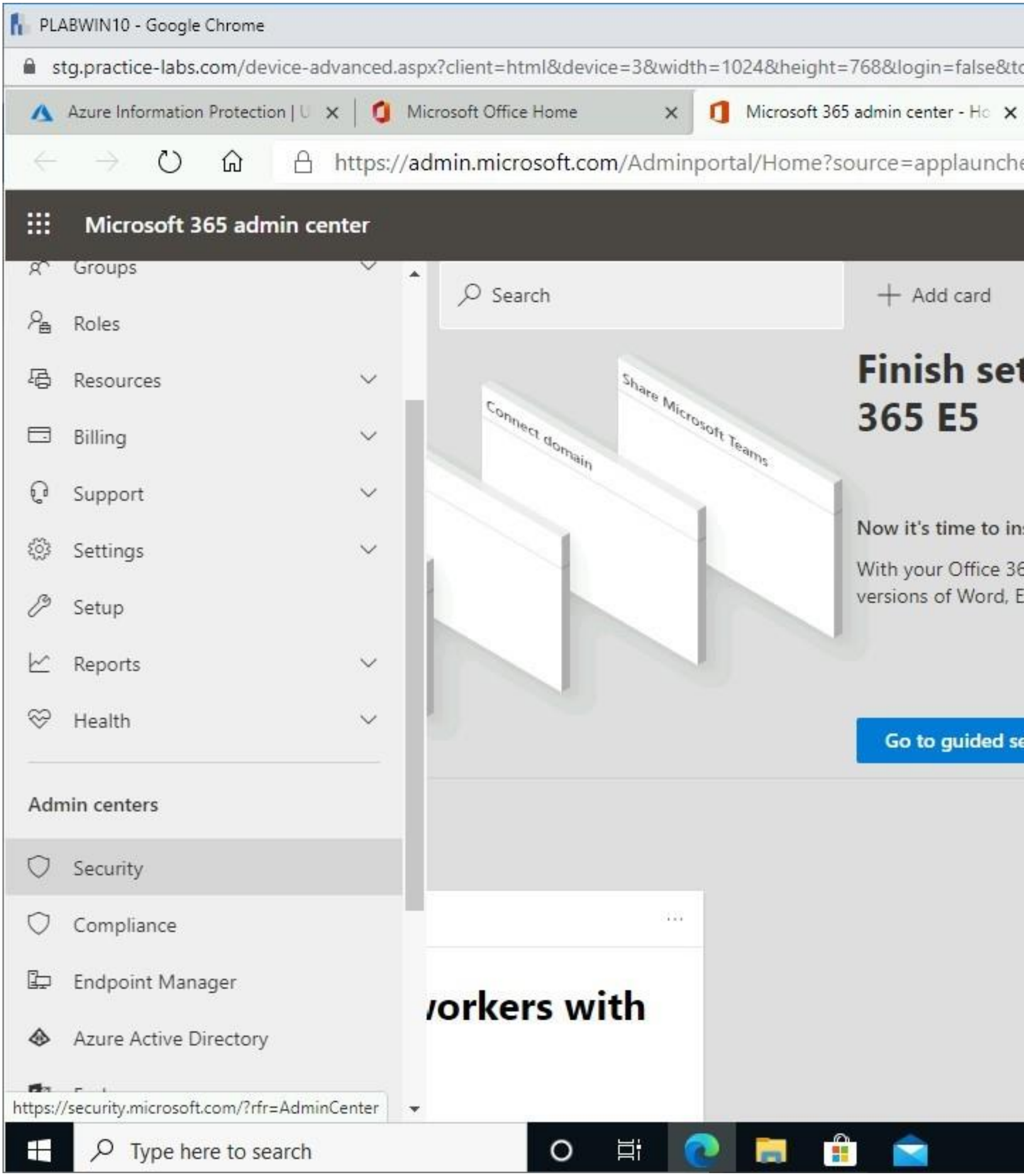

PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc
Azure Information Protection | U
Microsoft Office Home
Microsoft 365 admin center - Ho
https://admin.microsoft.com/Adminportal/Home?source=applaunche
Microsoft 365 admin center
Groups
Roles
Resources
Billing
Support
Settings
Setup
Reports
Health
Admin centers
Security
Compliance
Endpoint Manager
Azure Active Directory
https://security.microsoft.com/?rfr=AdminCenter
Search
Add card
Connect domain
Share Microsoft Teams
Finish set
365 E5
Now it's time to ins
With your Office 36
versions of Word, E
Go to guided se
vorkers with
Type here to search

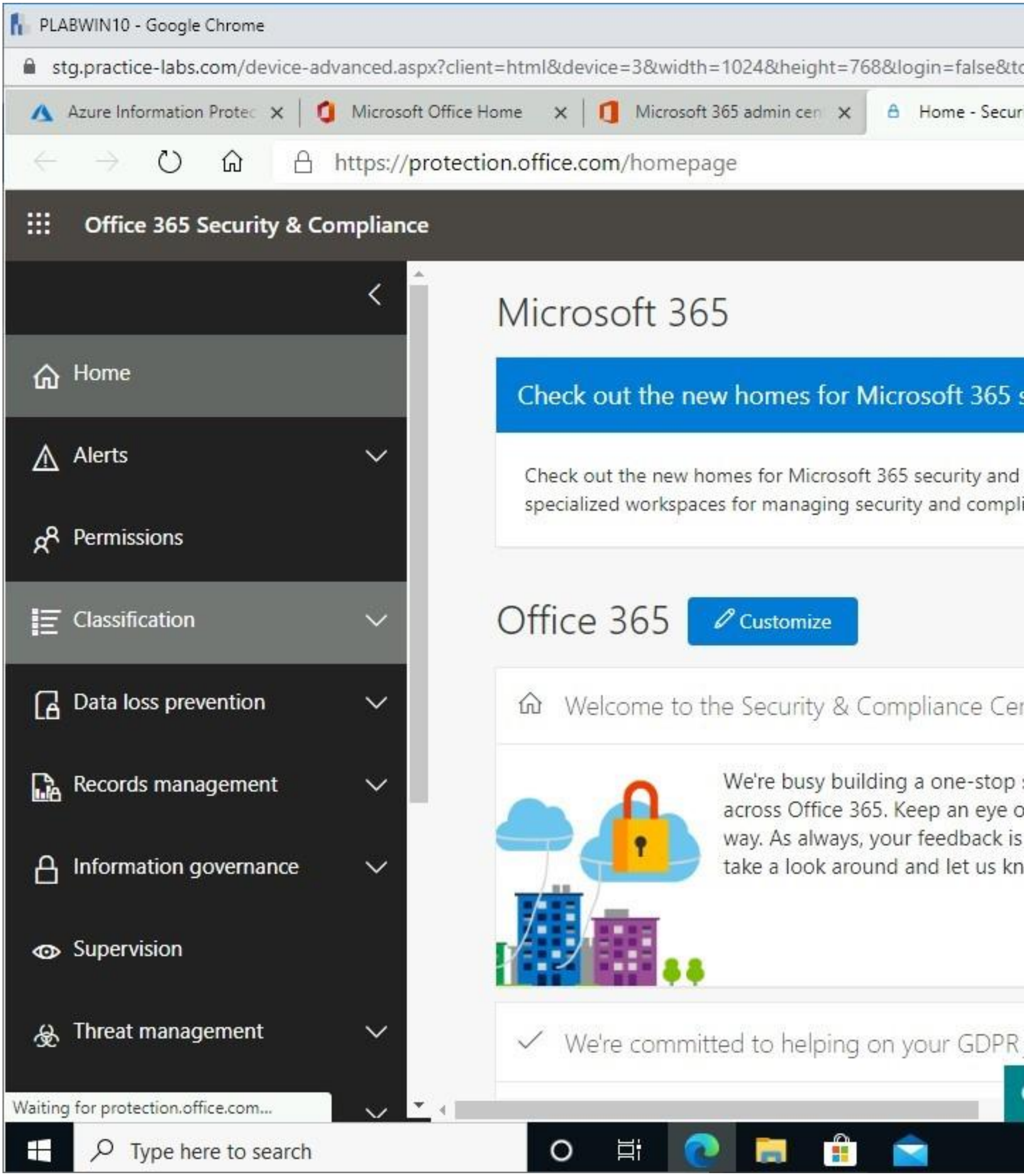
Figure 2.24 Screenshot of PLABWIN10 desktop: Security menu-option on

the navigation pane at the left on the Microsoft 365 admin center screen is selected.

Step 6

A new browser tab opens for the **Office 365 Security & Compliance** page.

Click **Classification** on the navigation pane to expand it.



Check out the new homes for Microsoft 365 s

Check out the new homes for Microsoft 365 security and
specialized workspaces for managing security and compli

Welcome to the Security & Compliance Cen

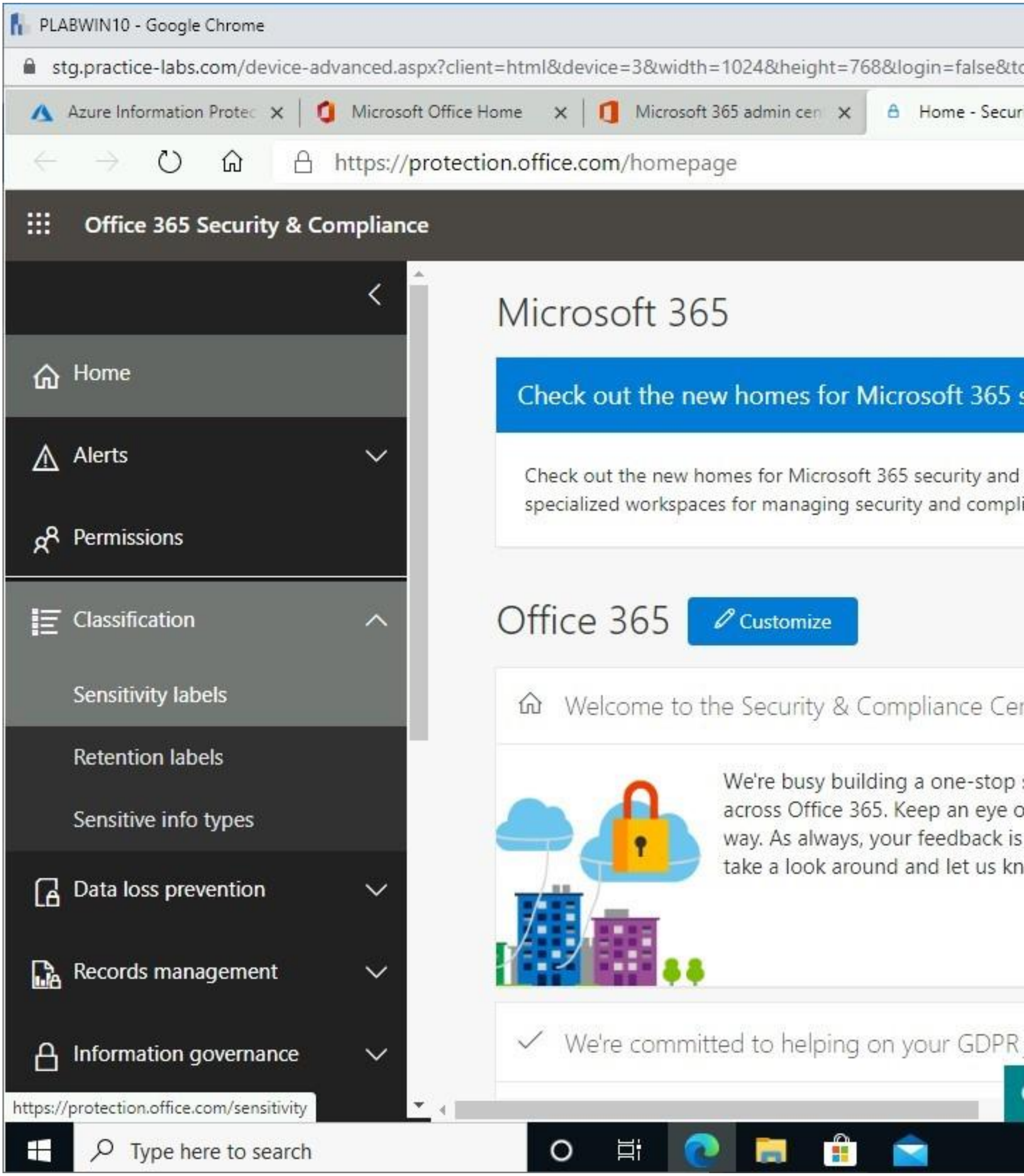
We're busy building a one-stop s
across Office 365. Keep an eye o
way. As always, your feedback is
take a look around and let us kn

We're committed to helping on your GDPR

Figure 2.25 Screenshot of PLABWIN10 desktop: Classification menu-option on the navigation pane at the left on the Office 365 Security & Compliance screen is selected.

Step 7

Under **Classification**, select **Sensitivity labels**.



Microsoft 365

Check out the new homes for Microsoft 365 s

Check out the new homes for Microsoft 365 security and
specialized workspaces for managing security and compli

Office 365

Welcome to the Security & Compliance Cer

We're busy building a one-stop s
across Office 365. Keep an eye o
way. As always, your feedback is
take a look around and let us kn

We're committed to helping on your GDPR

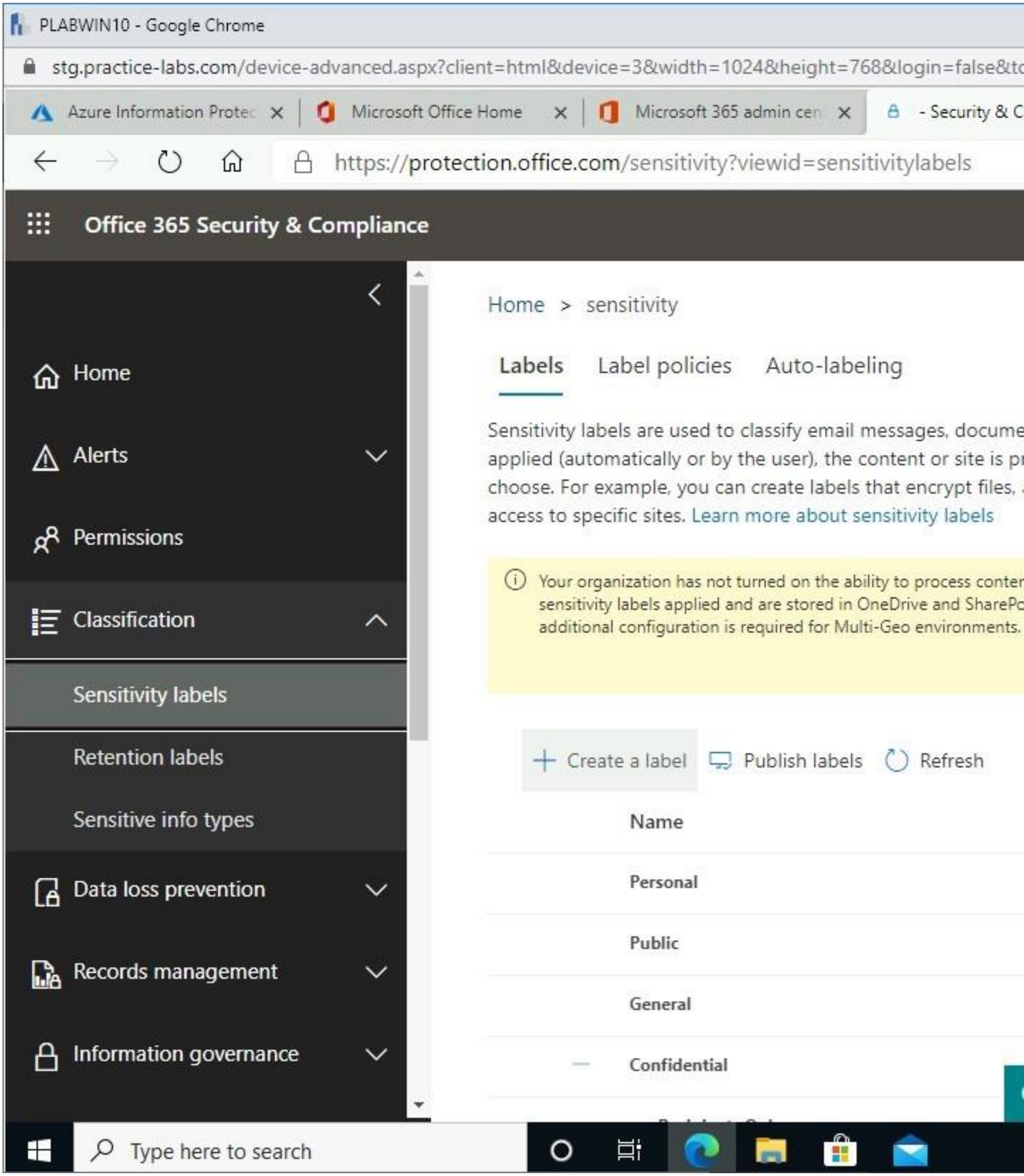
Figure 2.26 Screenshot of PLABWIN10 desktop: Classification > Sensitivity

labels menu-options on the navigation pane at the left on the Office 365 Security & Compliance screen are selected.

Step 8

The AIP copied labels from Microsoft Azure appears on the list.

Click **Create a label**.



Sensitivity labels are used to classify email messages, docume
applied (automatically or by the user), the content or site is pr
choose. For example, you can create labels that encrypt files,
access to specific sites. Learn more about sensitivity labels

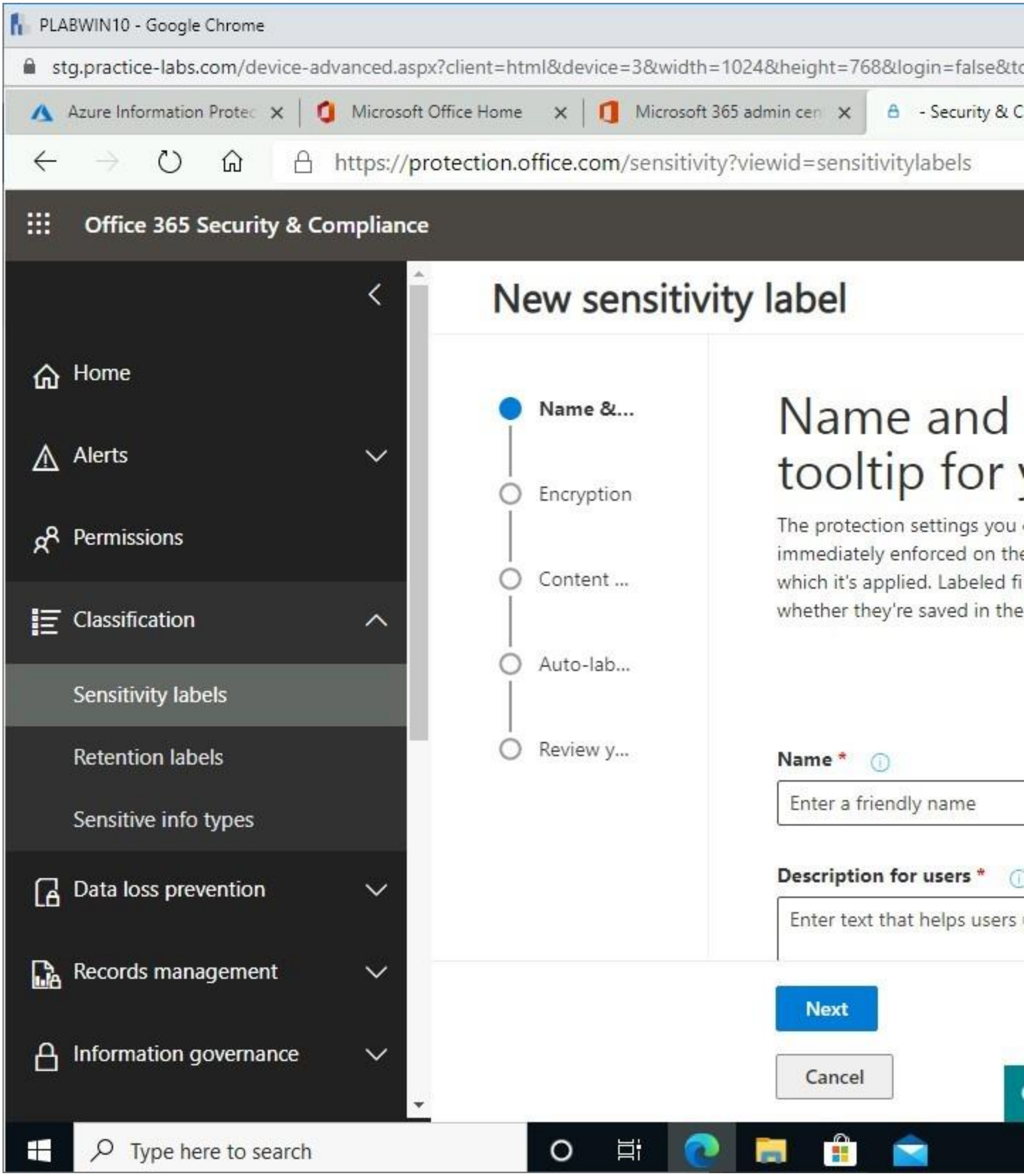
Your organization has not turned on the ability to process conter
sensitivity labels applied and are stored in OneDrive and SharePo
additional configuration is required for Multi-Geo environments.

Figure 2.27 Screenshot of PLABWIN10 desktop: Create a label option on

the Office 365 Security & Compliance screen is highlighted.

Step 9

On the **Name and create a tooltip for your label** page, scroll down to view the other fields.



Name and
tooltip for y

The protection settings you
immediately enforced on the
which it's applied. Labeled fi
whether they're saved in the

Name *

Enter a friendly name

Description for users *

Enter text that helps users

Figure 2.28 Screenshot of PLABWIN10 desktop: Name and create a tooltip

for your label tab on the Office 365 Security & Compliance - New sensitivity label screen is displayed.

Step 10

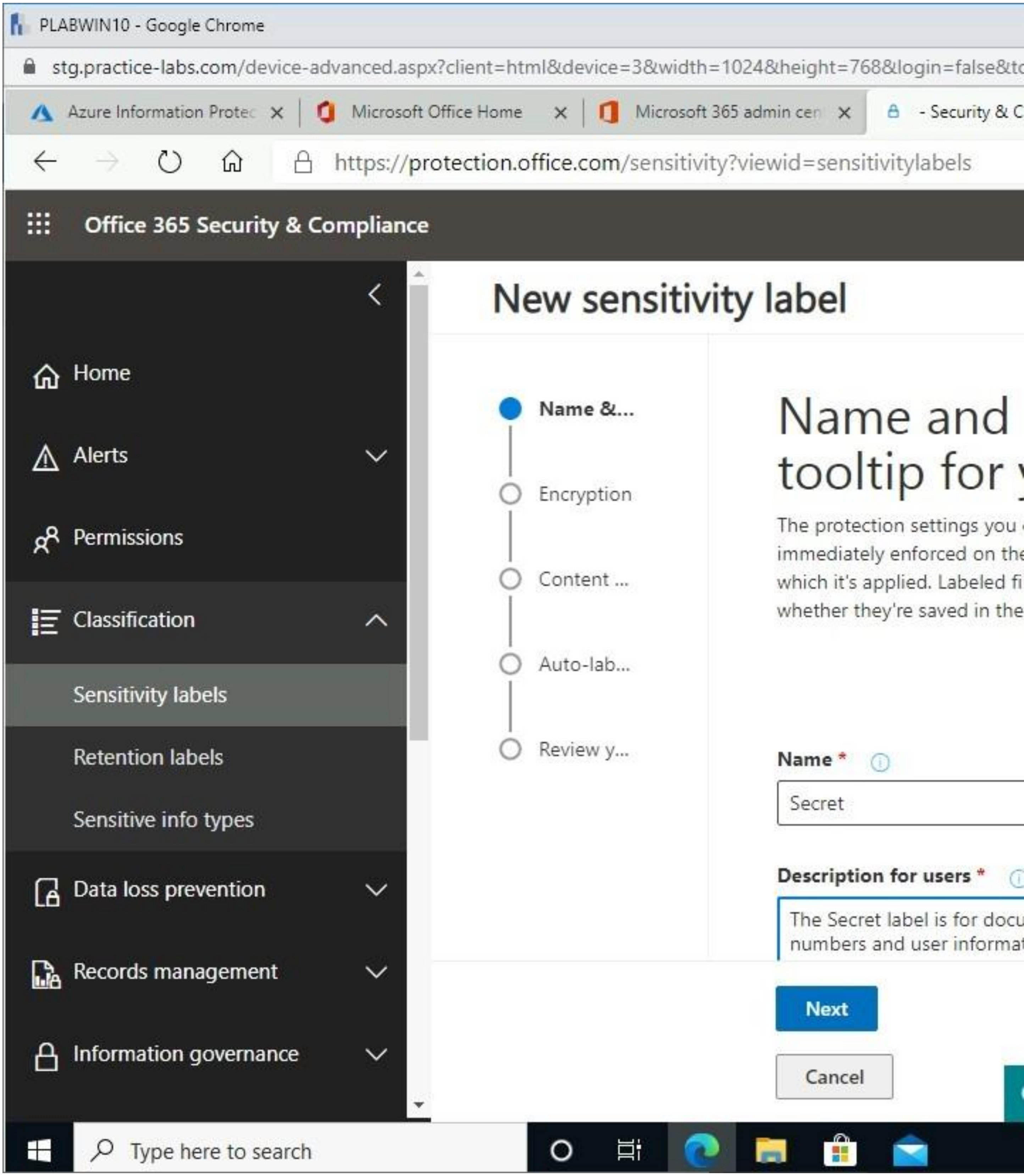
In the **Name** box, type:

```
Secret
```

Click in the **Description for users** text box and type:

```
The Secret label is for documents that contain
credit card numbers and user information.
```

Click **Next**.



Name * Secret

Description for users * The Secret label is for docu numbers and user informat

Figure 2.29 Screenshot of PLABWIN10 desktop: Name and create a tooltip

for your label tab on the Office 365 Security & Compliance - New sensitivity label screen is displayed showing the required values typed-in and the Next button selected.

Step 11

On the **Encryption** page, no encryption will be applied at this time.

Click **Next**.

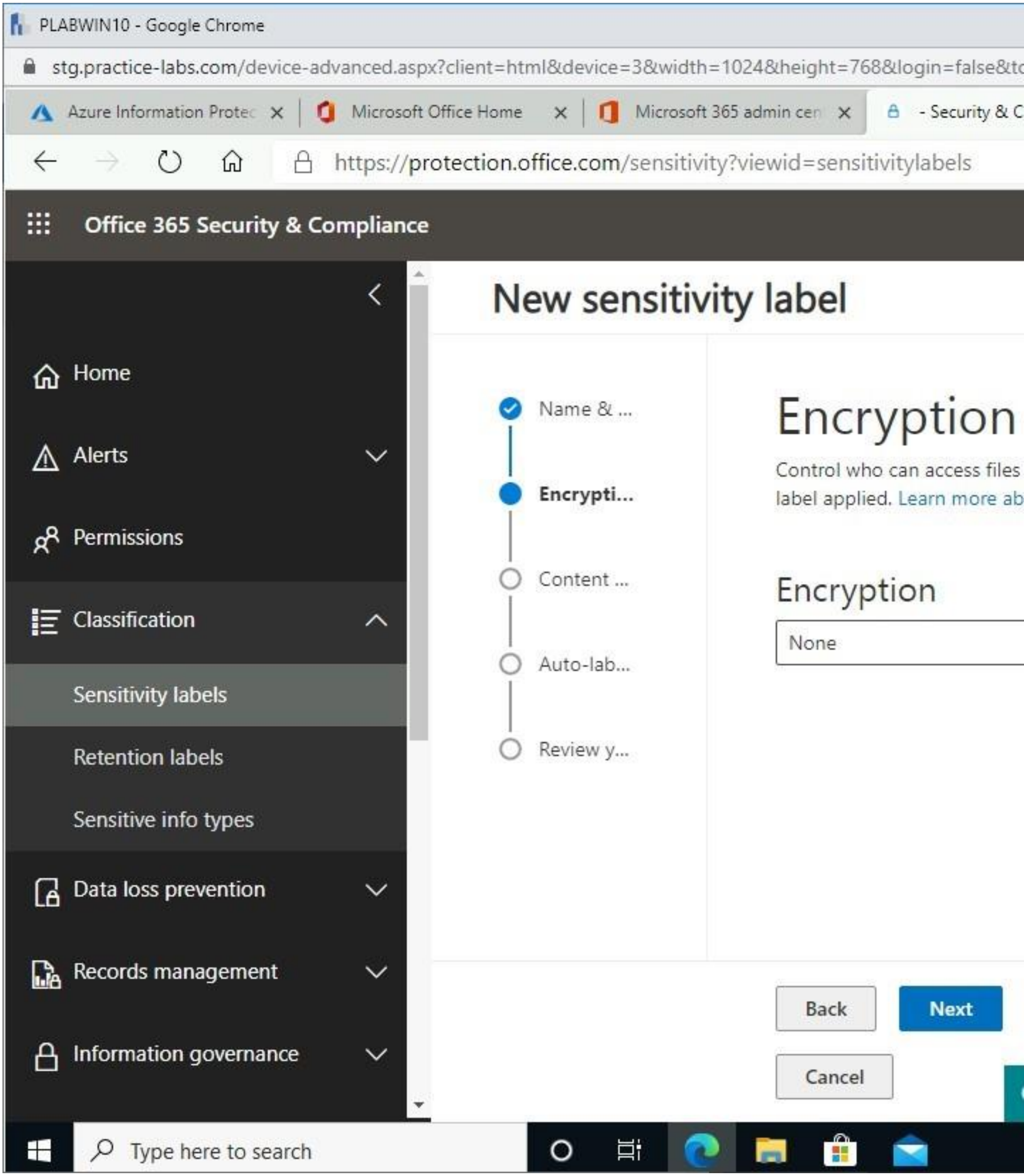


Figure 2.30 Screenshot of PLABWIN10 desktop: Encryption tab on the

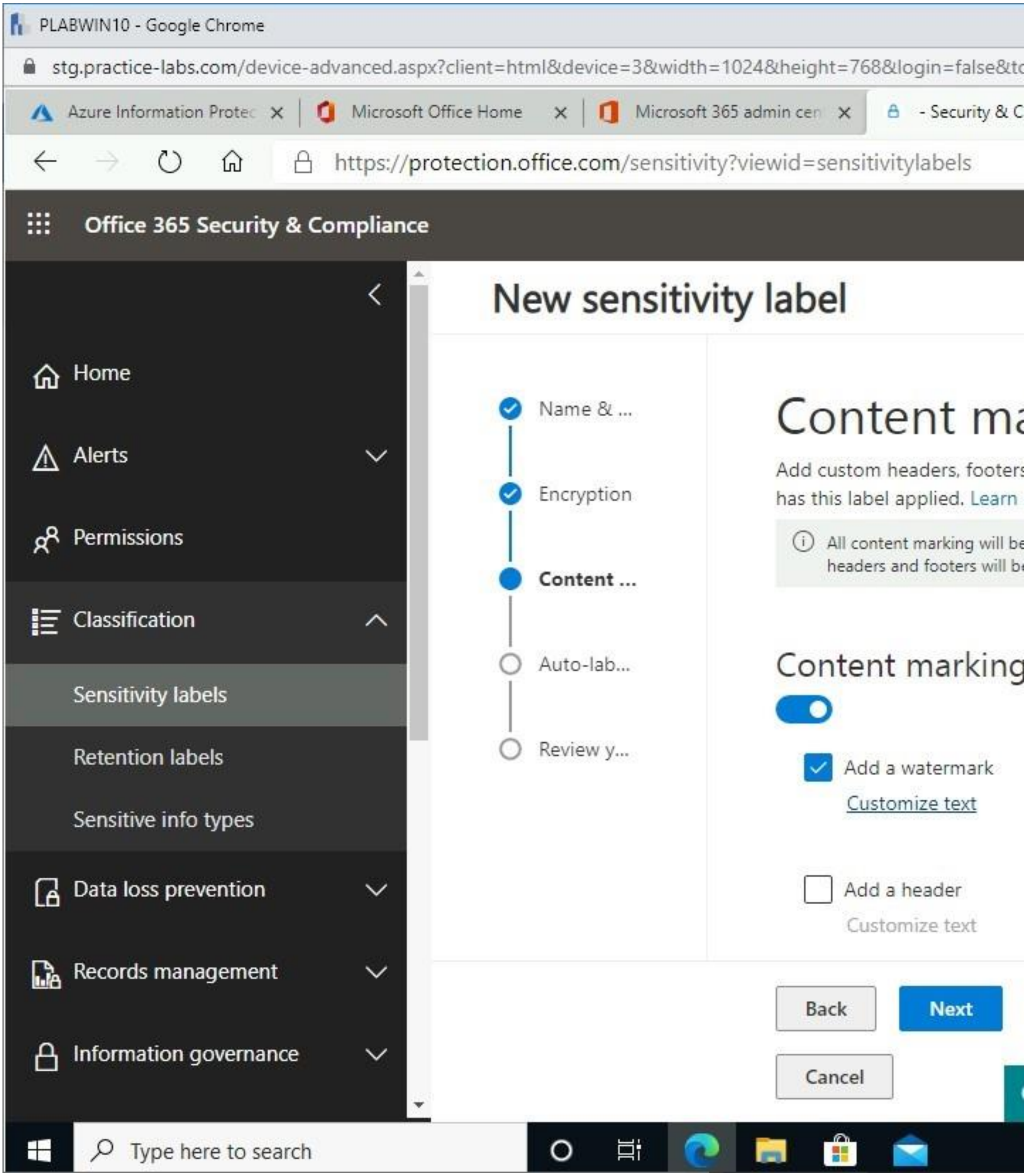
Office 365 Security & Compliance - New sensitivity label screen is displayed showing default settings and the Next button selected.

Step 12

On the **Content marking** page, access the **Content marking** slider and switch it to **On**.

Enable **Add a watermark** checkbox.

Click **Customize text**.


PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&to

https://protection.office.com/sensitivity?viewid=sensitivitylabels

Office 365 Security & Compliance

New sensitivity label

Content ma

Add custom headers, footers
has this label applied. Learn

All content marking will be
headers and footers will b

Content marking

☑ Add a watermark

Customize text

□ Add a header

Customize text

Figure 2.31 Screenshot of PLABWIN10 desktop: Content marking tab on

the Office 365 Security & Compliance - New sensitivity label screen is displayed showing the required settings performed and the Customize text link highlighted.

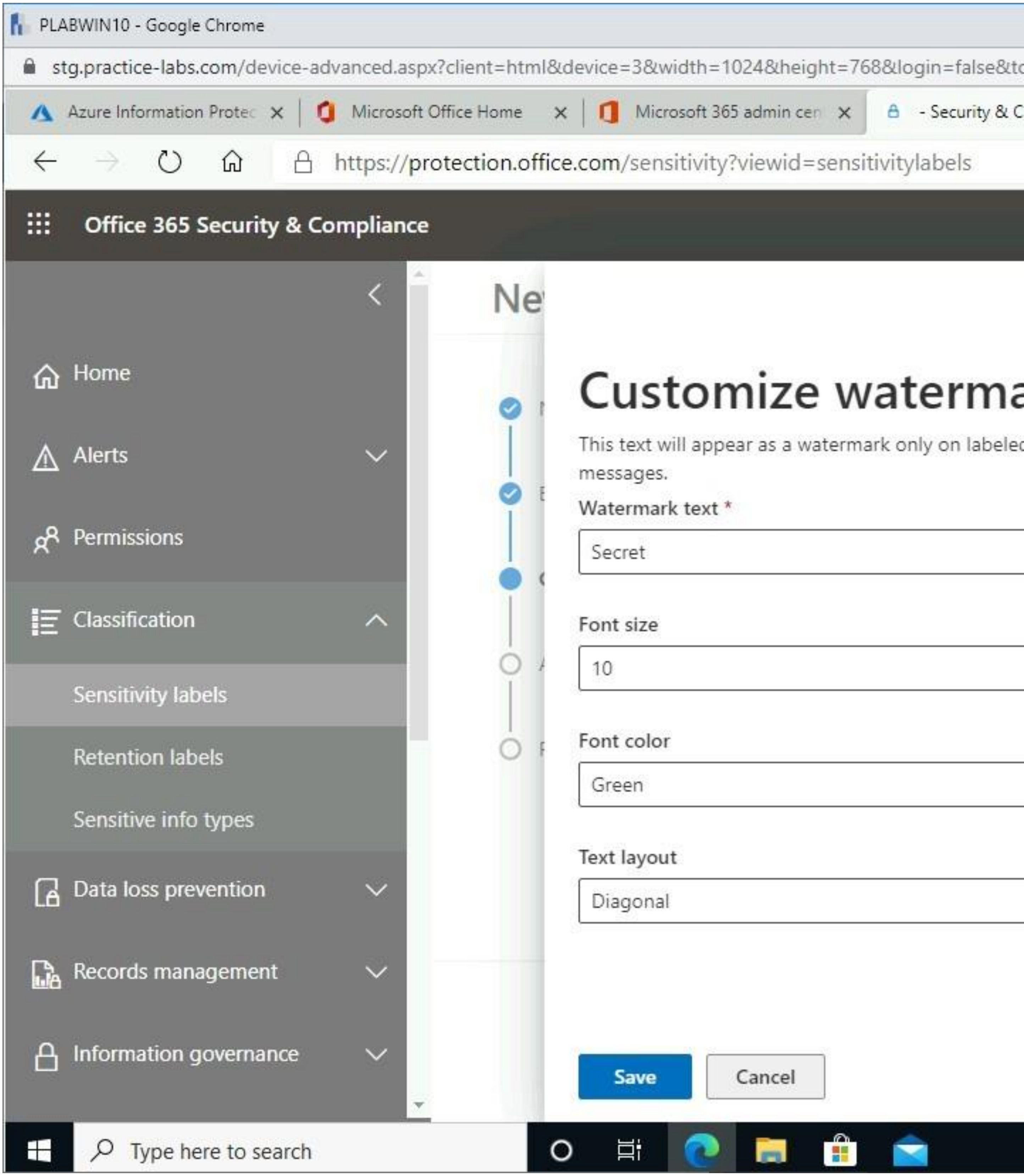
Step 13

From the **Customize watermark** text menu, click in the **Watermark text** box then type:

```
Secret
```

Click the **Font** color drop-down list and select **Green**.

Click **Save**.



Customize waterma

This text will appear as a watermark only on labelec messages.

Watermark text *

Secret

Font size

10

Font color

Green

Text layout

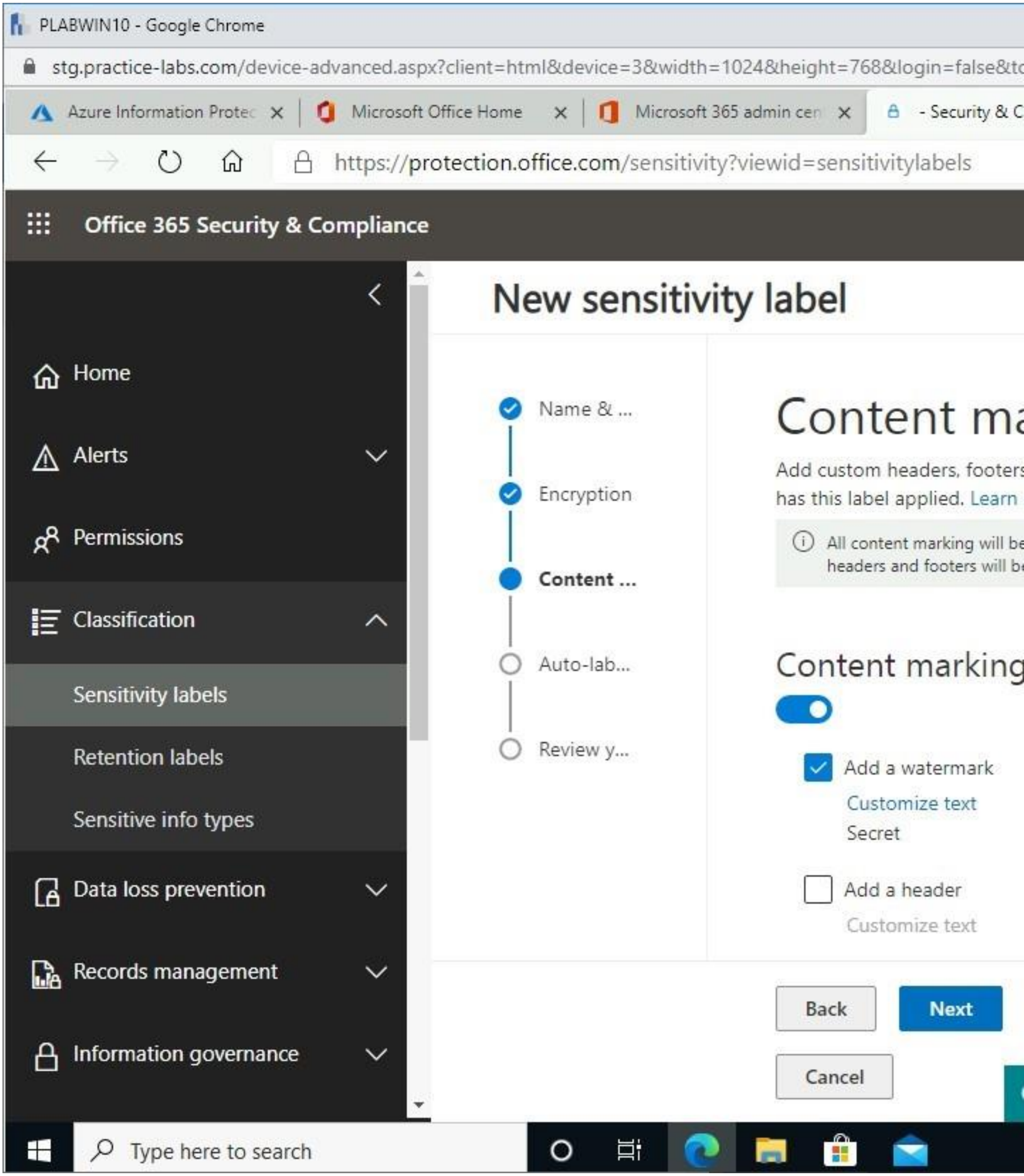
Diagonal

Figure 2.32 Screenshot of PLABWIN10 desktop: Customize watermark text

flyout menu is displayed showing the required settings performed and the Save button selected.

Step 14

Back in the **Content marking** page, click **Next**.



New sensitivity label

Content ma

Add custom headers, footers
has this label applied. Learn

All content marking will be
headers and footers will b

Content marking

☑ Add a watermark
Customize text
Secret

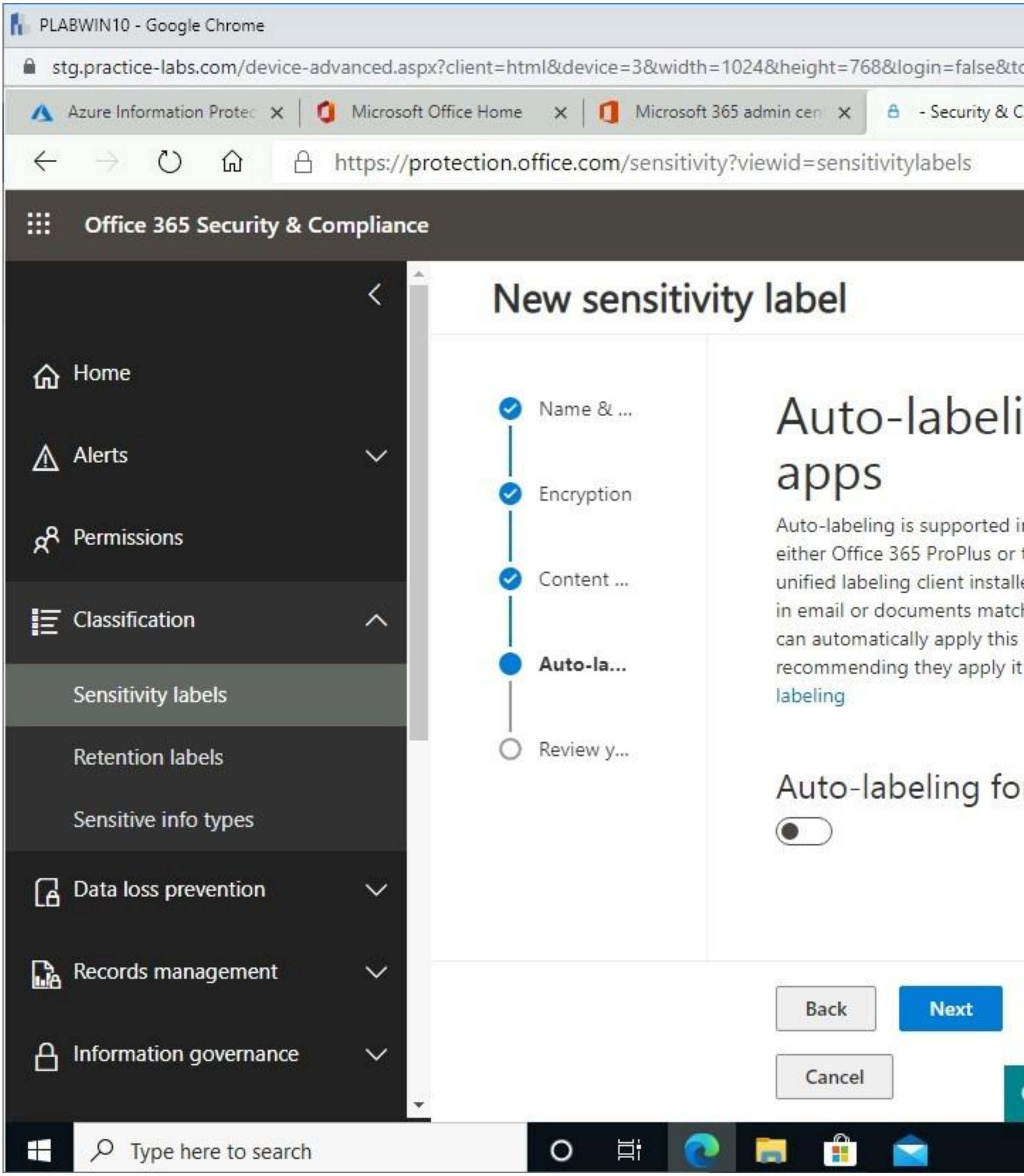
□ Add a header
Customize text

Figure 2.33 Screenshot of PLABWIN10 desktop: Content marking tab on

the Office 365 Security & Compliance - New sensitivity label screen is displayed listing the required settings performed and showing the Next button selected.

Step 15

Scroll down **Auto-labeling for Office apps** to view the relevant settings.



PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc

https://protection.office.com/sensitivity?viewid=sensitivitylabels

New sensitivity label

Auto-labeli
apps

Auto-labeling is supported i
either Office 365 ProPlus or t
unified labeling client installe
in email or documents matcl
can automatically apply this
recommending they apply it
labeling

Auto-labeling fo

Figure 2.34 Screenshot of PLABWIN10 desktop: Auto-labeling for Office

apps tab on the Office 365 Security & Compliance - New sensitivity label screen is displayed.

Step 16

Access the **Auto-labeling for Office apps** slider and set it to **On**.

Other options become available.

Expand **Detect content that matches these conditions > Add condition** and click **Content contains**.

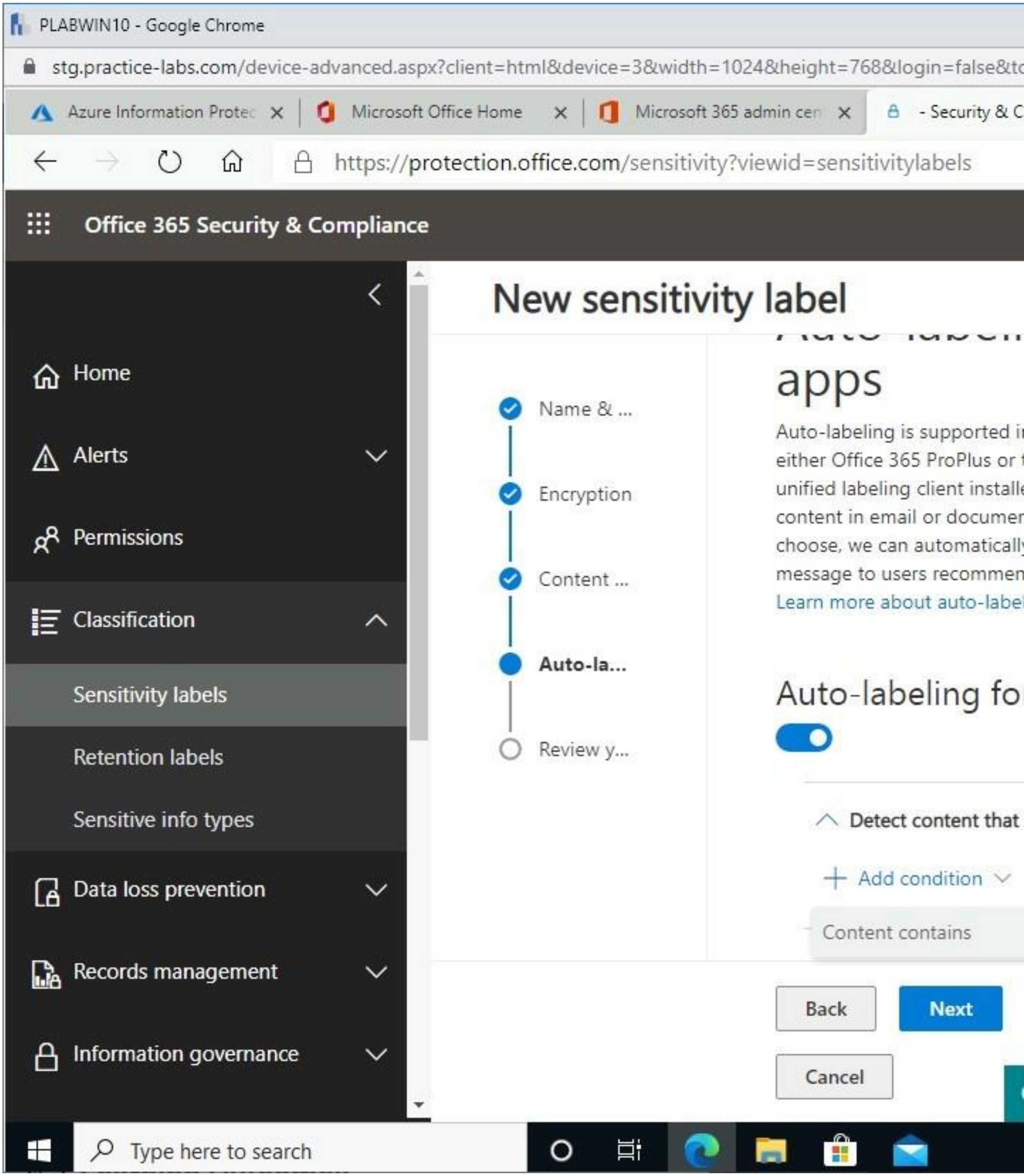
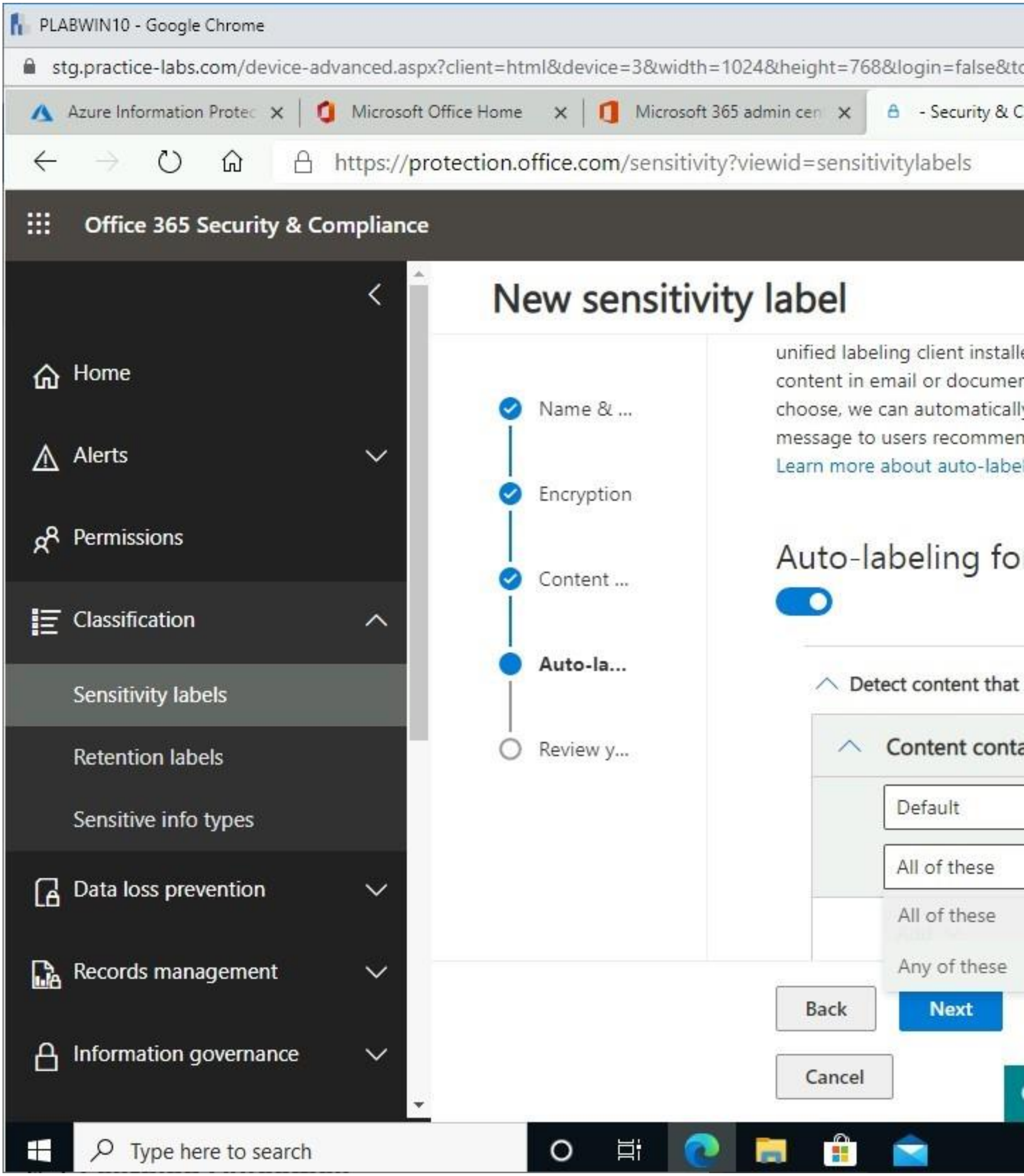

PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&t
Azure Information Protec
Microsoft Office Home
Microsoft 365 admin cen
- Security & C
https://protection.office.com/sensitivity?viewid=sensitivitylabels
Office 365 Security & Compliance
Home
Alerts
Permissions
Classification
Sensitivity labels
Retention labels
Sensitive info types
Data loss prevention
Records management
Information governance
New sensitivity label
Name & ...
Encryption
Content ...
Auto-la...
Review y...
apps
Auto-labeling is supported i
either Office 365 ProPlus or
unified labeling client installe
content in email or documen
choose, we can automatically
message to users recommen
Learn more about auto-labe
Auto-labeling fo
Detect content that
Add condition
Content contains
Back
Next
Cancel
Type here to search

Figure 2.35 Screenshot of PLABWIN10 desktop: Auto-labeling for Office

apps tab on the Office 365 Security & Compliance - New sensitivity label screen is displayed showing the required settings performed and the Content contains section-head selected.

Step 17

From the **Content contains** section, click **Any of these**.



unified labeling client installe
content in email or documen
choose, we can automatically
message to users recommen
Learn more about auto-label

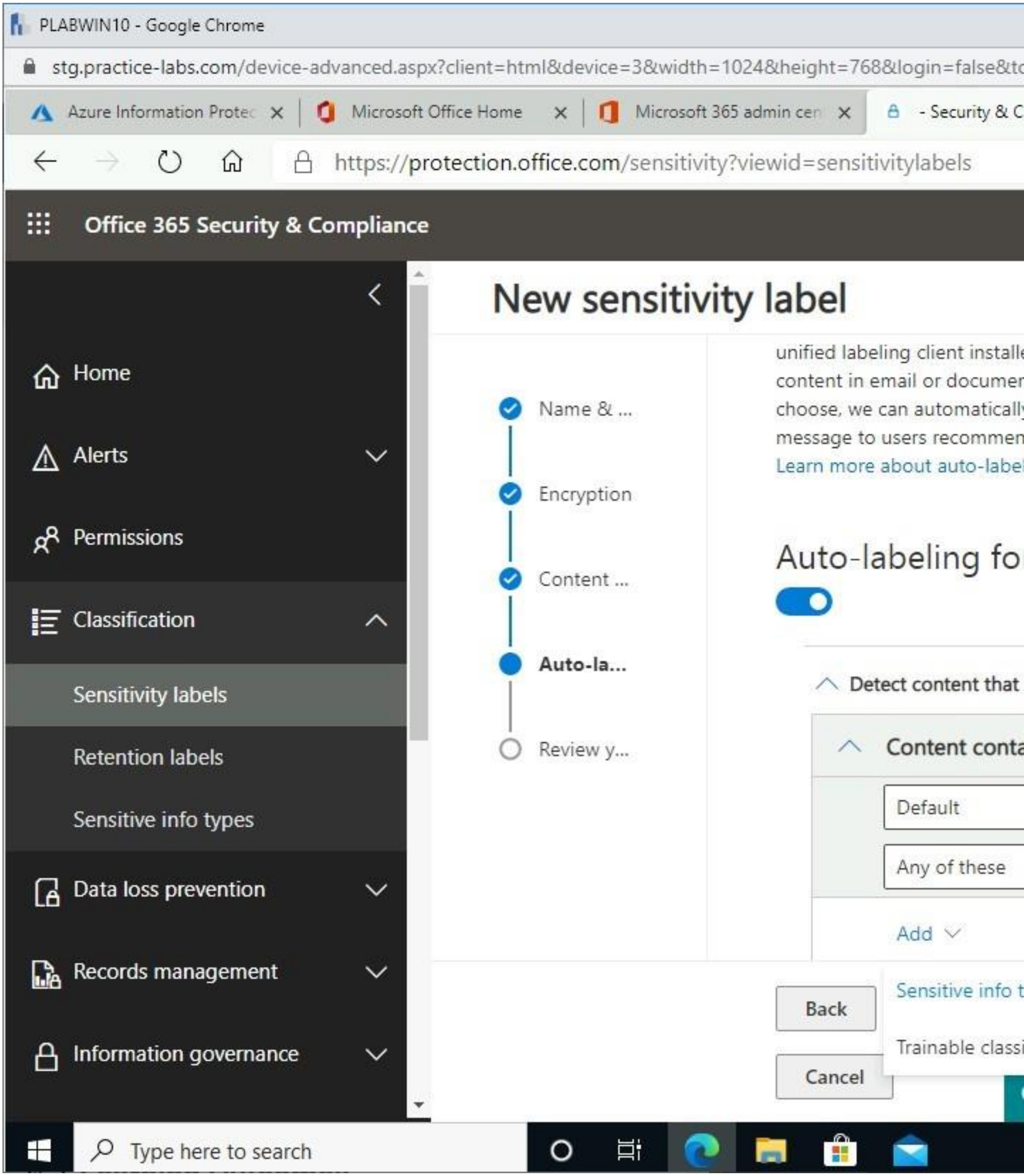
Auto-labeling fo

Figure 2.36 Screenshot of PLABWIN10 desktop: Auto-labeling for Office

apps tab on the Office 365 Security & Compliance - New sensitivity label screen is displayed showing the Content contains section set to Any of these.

Step 18

Click **Add** and select **Sensitive info** types.



unified labeling client installe
content in email or documer
choose, we can automatically
message to users recommen
Learn more about auto-label

Figure 2.37 Screenshot of PLABWIN10 desktop: Auto-labeling for Office

apps tab on the Office 365 Security & Compliance - New sensitivity label screen is displayed showing the required settings performed and the Add section-head selected.

Step 19

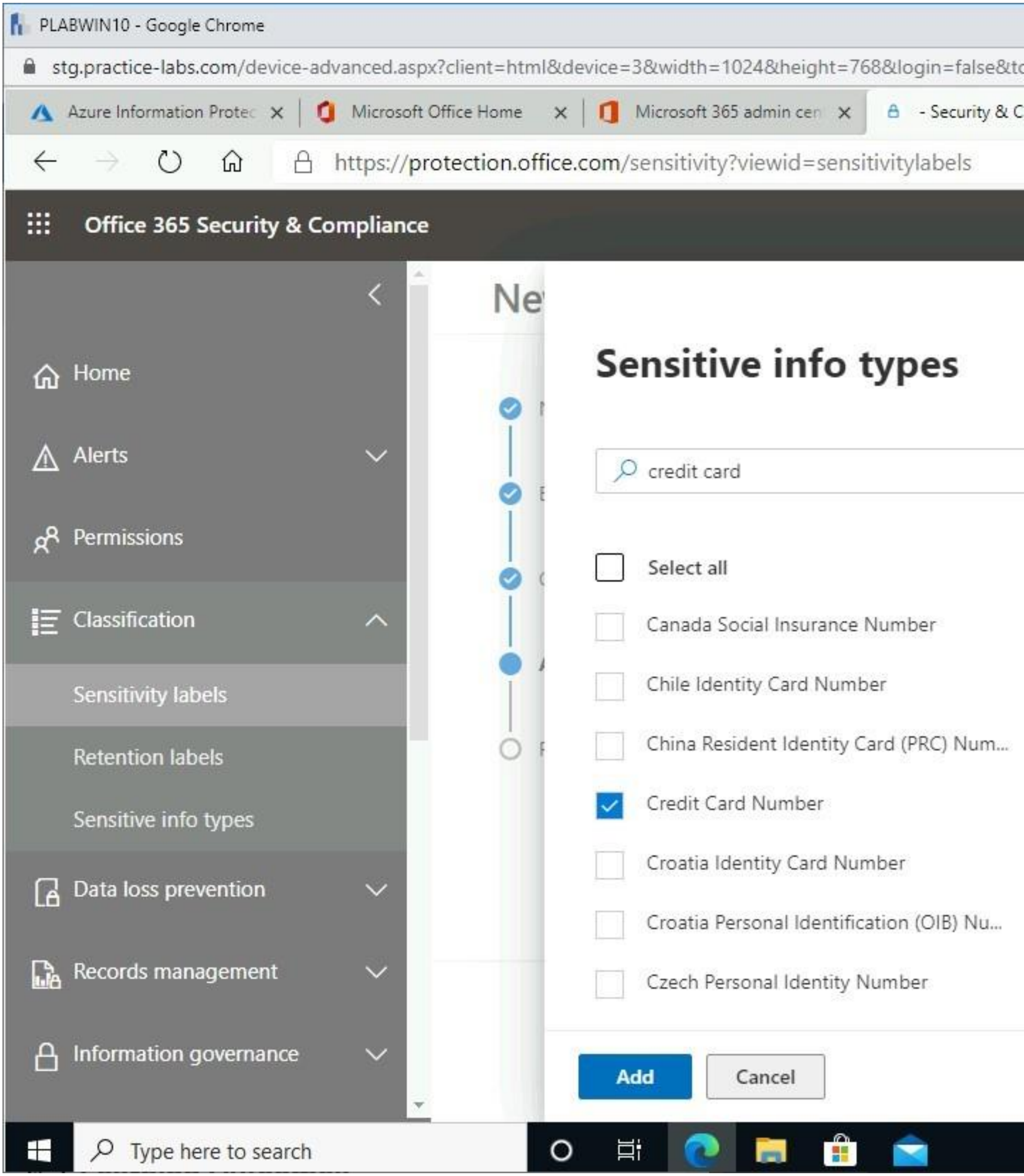
From the **Sensitive info types** menu, click in the search box and type:

```
credit card
```

Press **Enter**.

Enable **Credit Card Number** checkbox.

Click **Add**.



Sensitive info types

credit card

□ Select all

□ Canada Social Insurance Number

□ Chile Identity Card Number

□ China Resident Identity Card (PRC) Num...

☑ Credit Card Number

□ Croatia Identity Card Number

□ Croatia Personal Identification (OIB) Nu...

□ Czech Personal Identity Number

Figure 2.38 Screenshot of PLABWIN10 desktop: Sensitive info types flyout

menu is displayed showing the required settings performed and the Add button selected.

Step 20

Scroll down further.

From the **When content matches these conditions**, select **Recommend that users apply the label**.

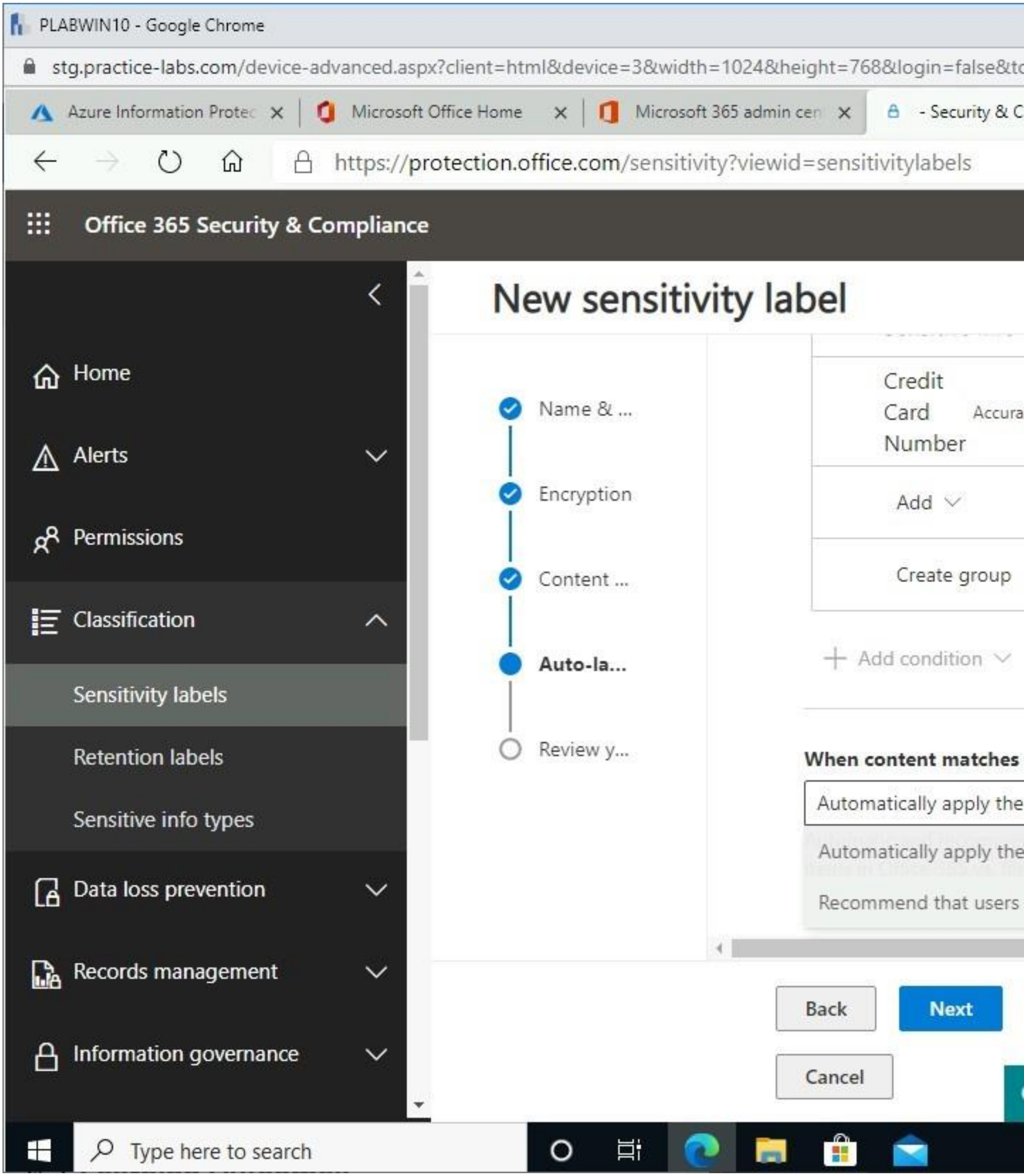


Figure 2.39 Screenshot of PLABWIN10 desktop: Auto-labeling for Office

apps tab on the Office 365 Security & Compliance - New sensitivity label screen is displayed showing the When content matches these conditions set to Recommend that users apply the label.

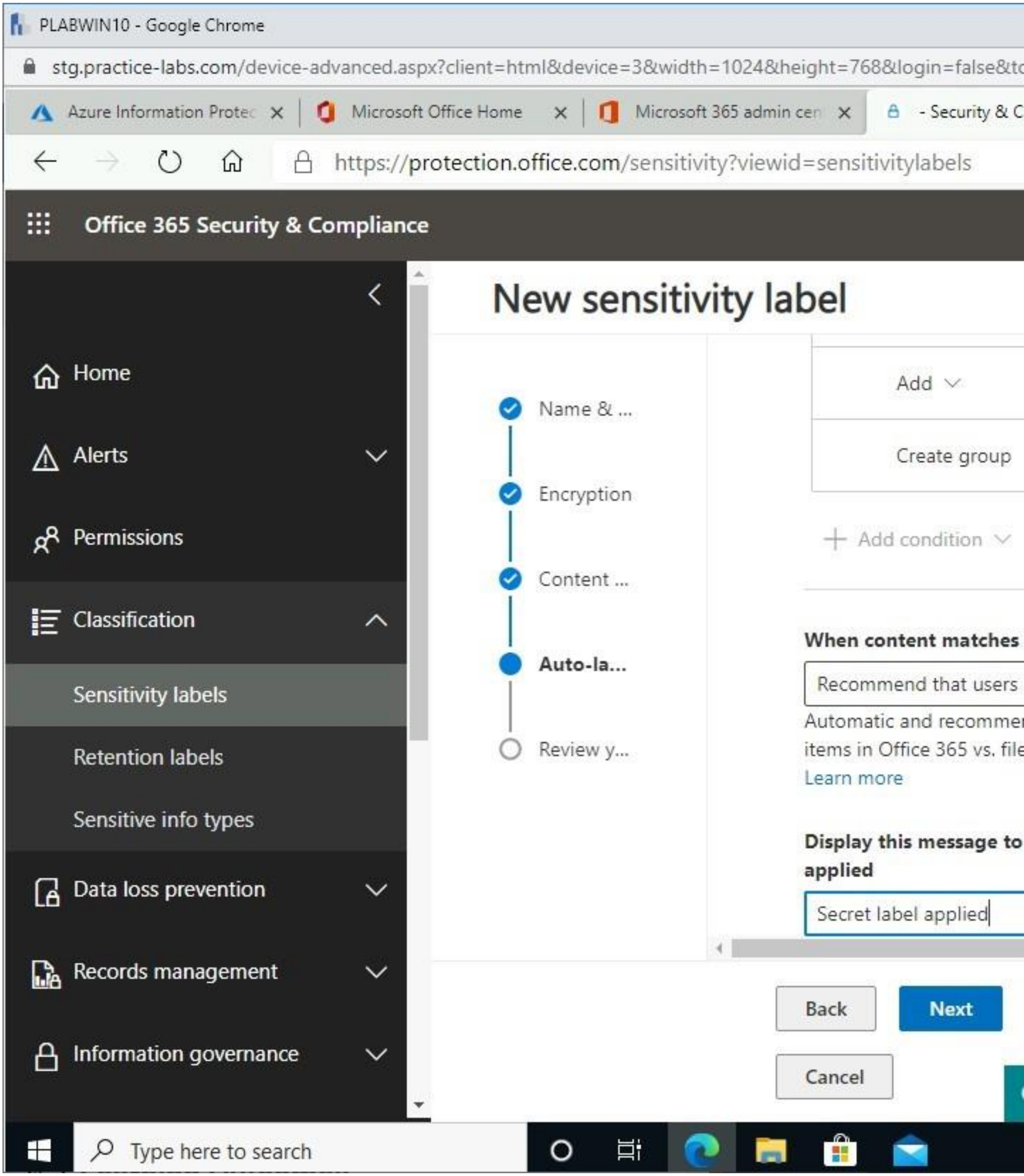
Step 21

Click in the **Display this message to users when the label is applied** box.

Then type:

```
Secret label applied
```

Click **Next**.



New sensitivity label

When content matches

Recommend that users

Automatic and recommen
items in Office 365 vs. file
Learn more

Display this message to
applied

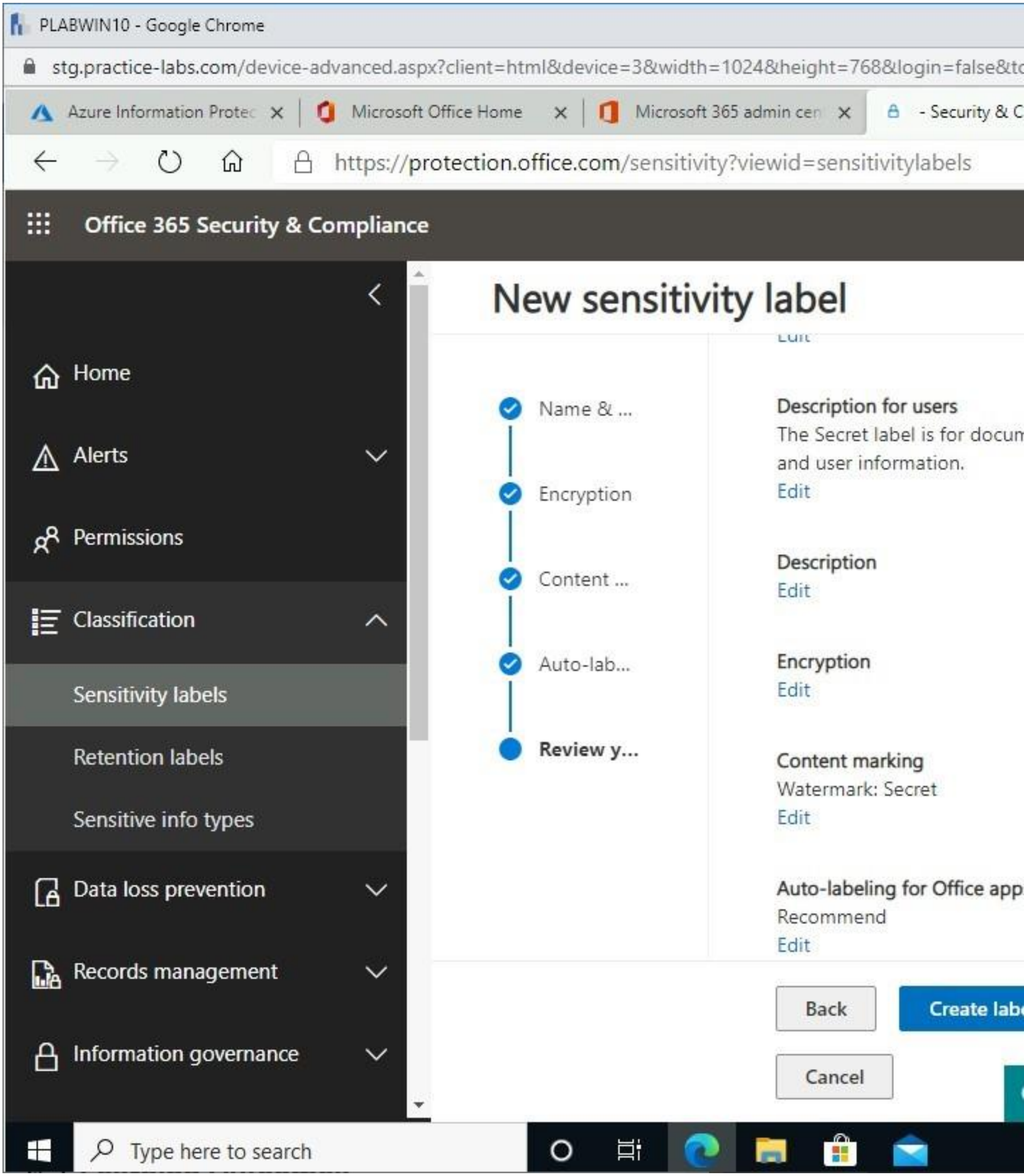
Secret label applied

Figure 2.40 Screenshot of PLABWIN10 desktop: Auto-labeling for Office

apps tab on the Office 365 Security & Compliance - New sensitivity label screen is displayed showing the required settings applied to the Display this message to users when the label is applied section.

Step 22

Click **Create label** on the **Review your settings** page.



New sensitivity label

Description for users
The Secret label is for docum
and user information.
Edit

Description
Edit

Encryption
Edit

Content marking
Watermark: Secret
Edit

Auto-labeling for Office app
Recommend
Edit

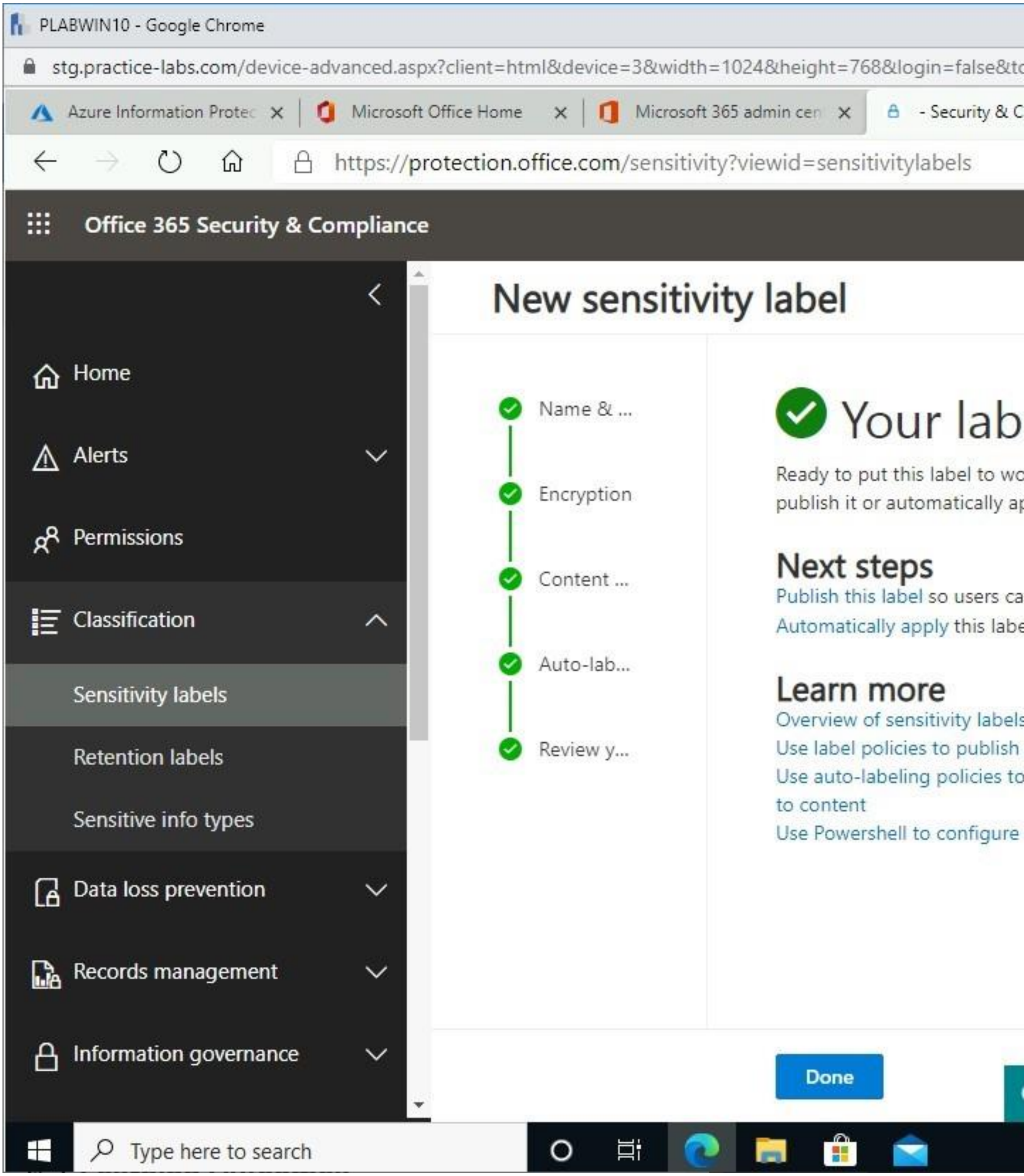
Figure 2.41 Screenshot of PLABWIN10 desktop: Review your settings tab

on the Office 365 Security & Compliance - New sensitivity label screen is displayed listing the settings performed and showing the Create label button selected.

Step 23

The message “**Your label was created**” appears.

Click **Done**.



New sensitivity label

Your lab

Ready to put this label to wo
publish it or automatically ap

Next steps

Publish this label so users ca
Automatically apply this labe

Learn more

Overview of sensitivity labels
Use label policies to publish
Use auto-labeling policies to
to content
Use Powershell to configure

Figure 2.42 Screenshot of PLABWIN10 desktop: Your label was created

message is displayed on the Office 365 Security & Compliance - New sensitivity label screen.

Task 4 - Edit the Confidential Label

The Confidential label is one of the default labels provided by AIP. Default labels provide conditions that make it easier for organizations to apply labels and subsequently classify the document.

In this task, you will edit the default Confidential label by customing the watermark and footer text.

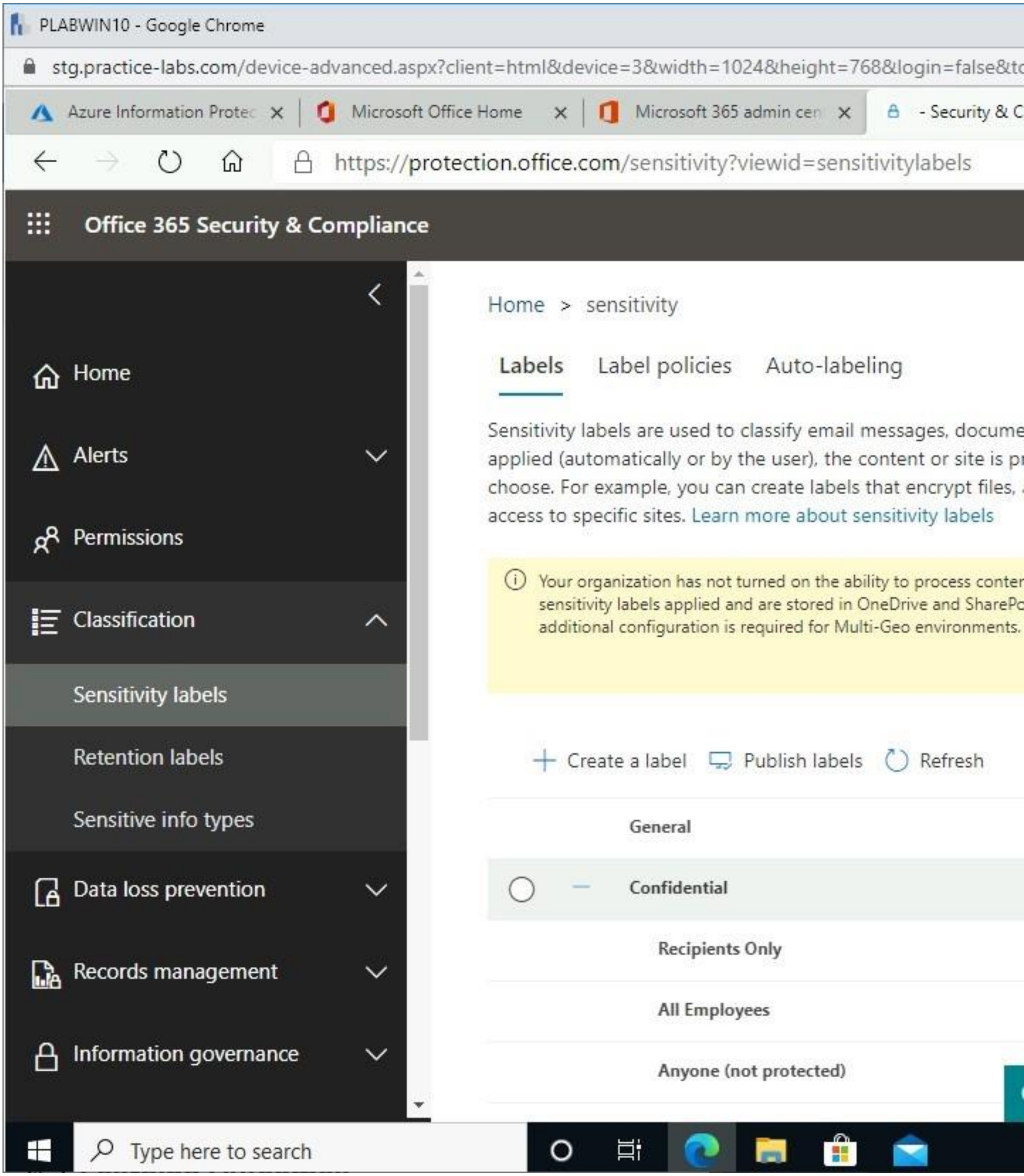
Step 1

Ensure you are connected to **PLABWIN10** and are in **Office 365 Security & Compliance** page.

You are on the **Classification** > **Sensitivity labels** page.

On the **Home** > **sensitivity** path, click the **Labels** tab.

Scroll down and click **Confidential**.



Sensitivity labels are used to classify email messages, docume applied (automatically or by the user), the content or site is pr choose. For example, you can create labels that encrypt files, access to specific sites. Learn more about sensitivity labels

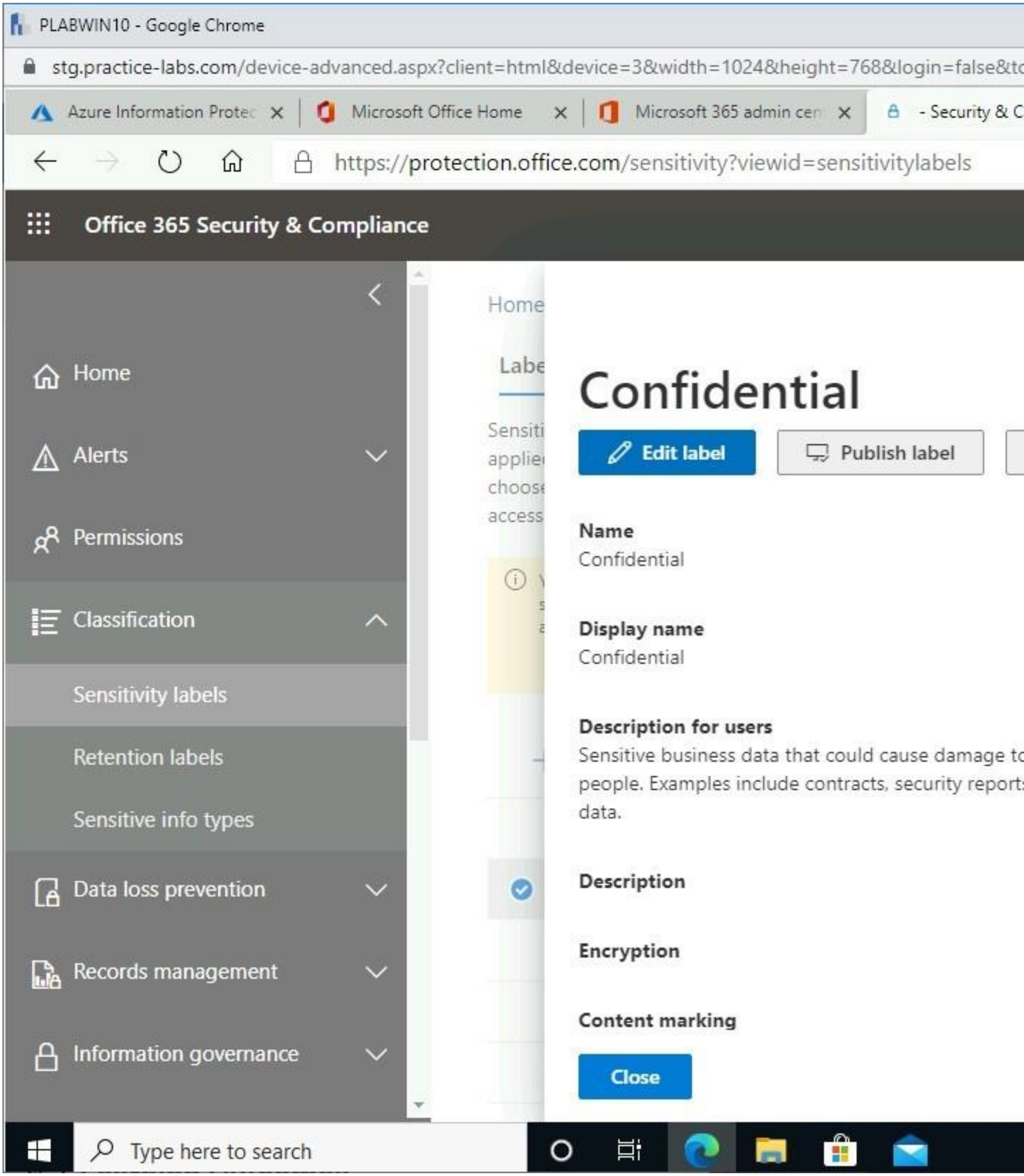
Your organization has not turned on the ability to process conter sensitivity labels applied and are stored in OneDrive and SharePo additional configuration is required for Multi-Geo environments.

Figure 2.43 Screenshot of PLABWIN10 desktop: Required option on the

Labels tab of the Office 365 Security & Compliance - Sensitivity screen is selected.

Step 2

From the **Confidential** menu, click **Edit label**.



Confidential

Name
Confidential

Display name
Confidential

Description for users
Sensitive business data that could cause damage to people. Examples include contracts, security reports data.

Description

Encryption

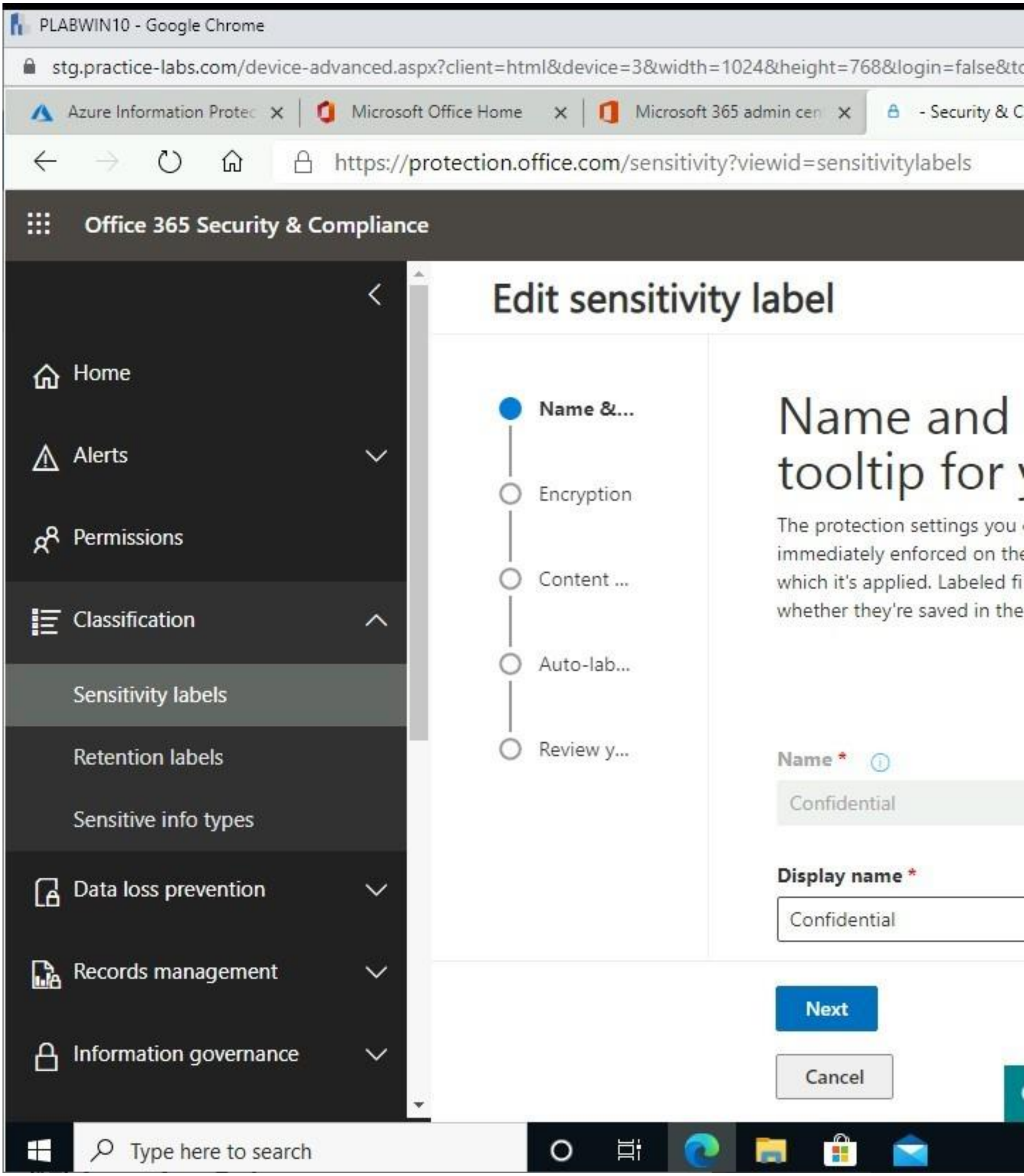
Content marking

Figure 2.44 Screenshot of PLABWIN10 desktop: Edit label button on the

Confidential flyout menu is selected.

Step 3

Click **Next** in the **Name and create a tooltip for your label** page.



Name and tooltip for y

The protection settings you
immediately enforced on the
which it's applied. Labeled fi
whether they're saved in the

Name * Confidential

Display name * Confidential

Figure 2.45 Screenshot of PLABWIN10 desktop: Name and create a tooltip

for your label tab on the Office 365 Security & Compliance - Edit sensitivity label screen is displayed showing default settings, and the Next button highlighted.

Step 4

Select **Next** in the **Encryption** page.

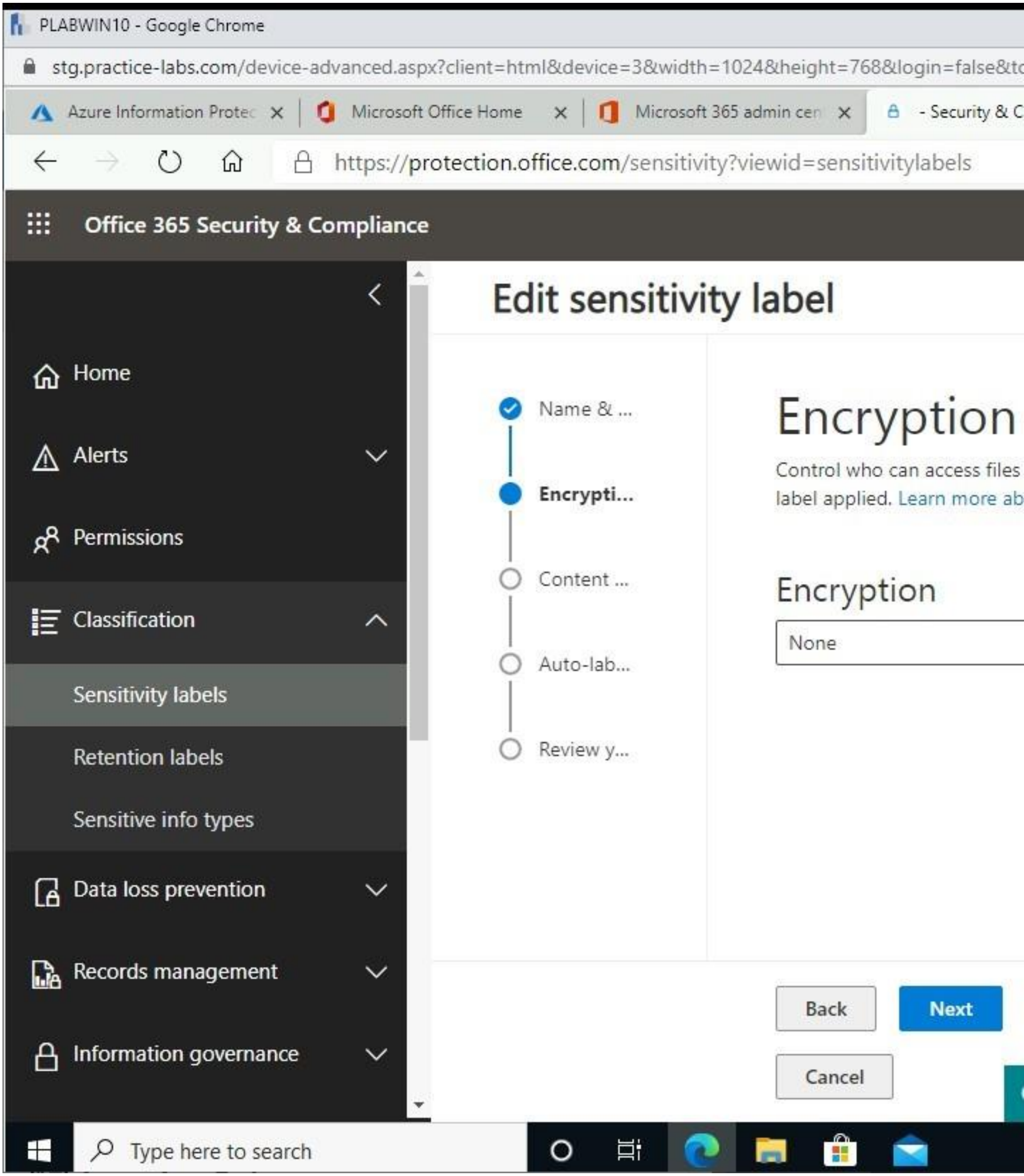


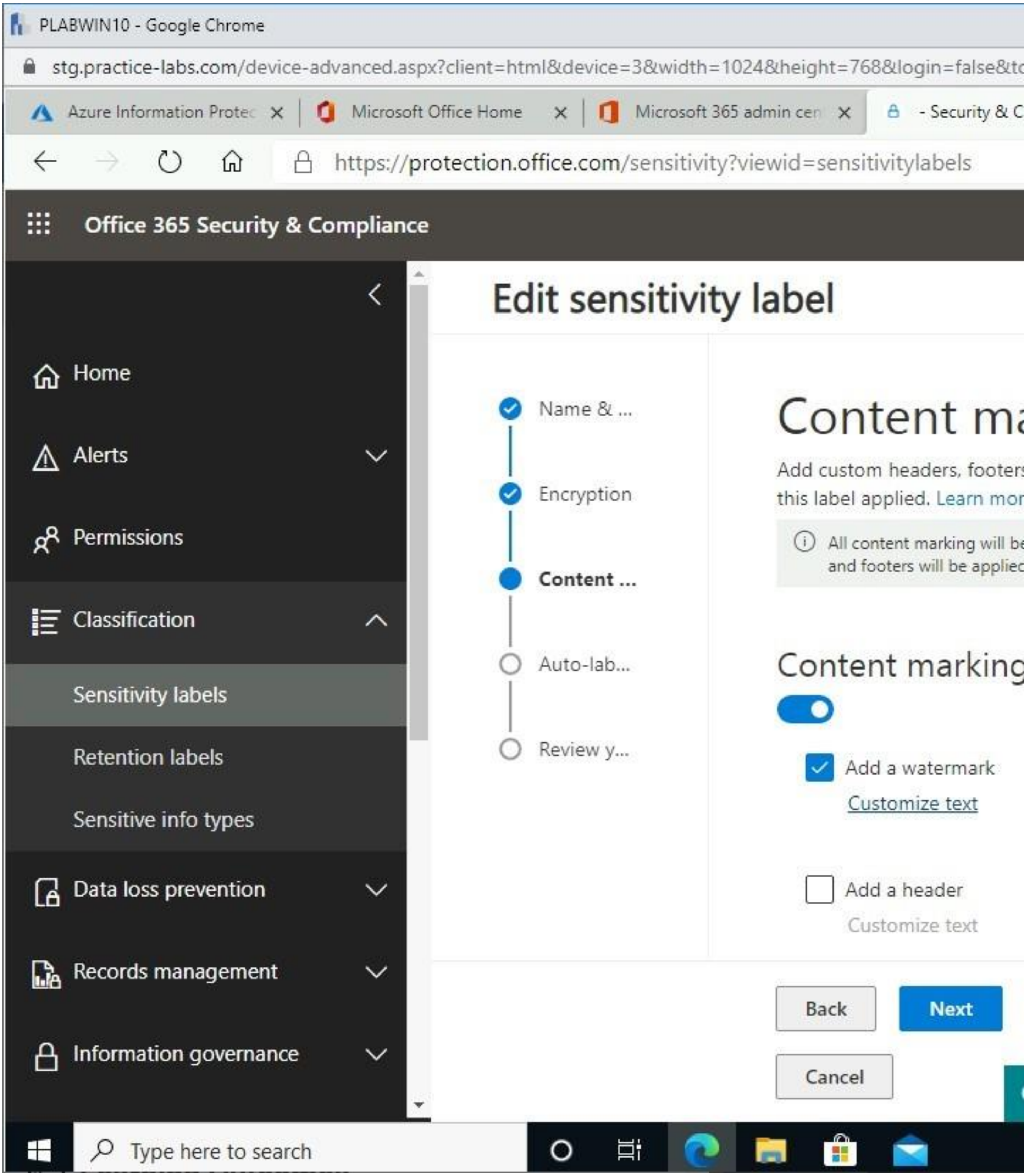
Figure 2.46 Screenshot of PLABWIN10 desktop: Encryption tab on the

Office 365 Security & Compliance - Edit sensitivity label screen is displayed showing default settings and the Next button highlighted.

Step 5

On the **Content marking** page, move the **Content marking** slider to **On**.

Select **Add a watermark** checkbox and click **Customize text**.



Edit sensitivity label

Content ma

Add custom headers, footers
this label applied. Learn mor

All content marking will be
and footers will be appliec

Content marking

☑ Add a watermark

Customize text

□ Add a header

Customize text

Figure 2.47 Screenshot of PLABWIN10 desktop: Content marking tab on

the Office 365 Security & Compliance - Edit sensitivity label screen is displayed showing the required settings performed and the Customize text link for the Add a watermark section highlighted.

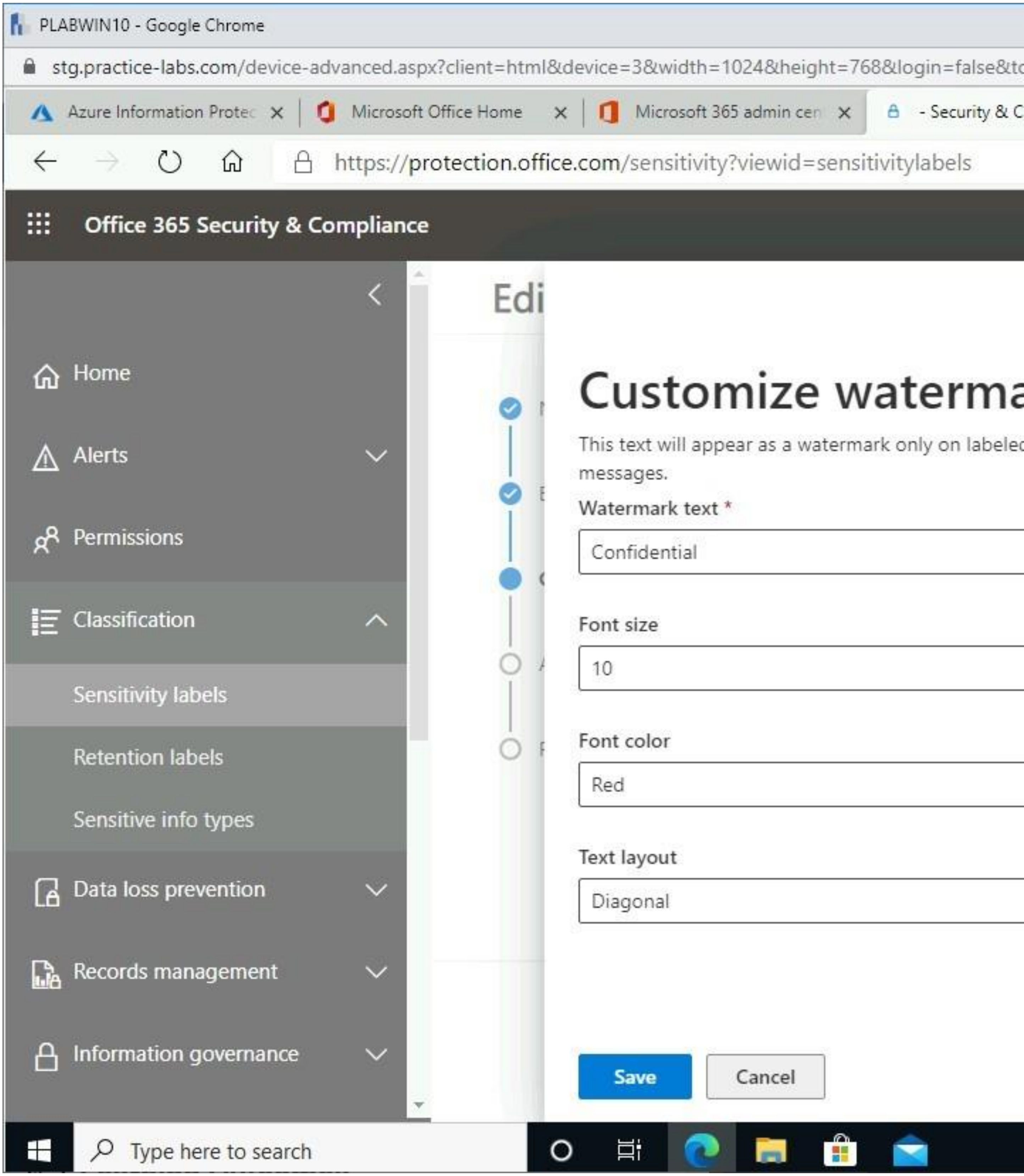
Step 6

On the **Customize watermark text** menu, click in the **Watermark text** box and type:

```
Confidential
```

Access the **Font color** drop-down list and select **Red**.

Click **Save**.



Customize waterma

This text will appear as a watermark only on labelec messages.

Watermark text *

Confidential

Font size

10

Font color

Red

Text layout

Diagonal

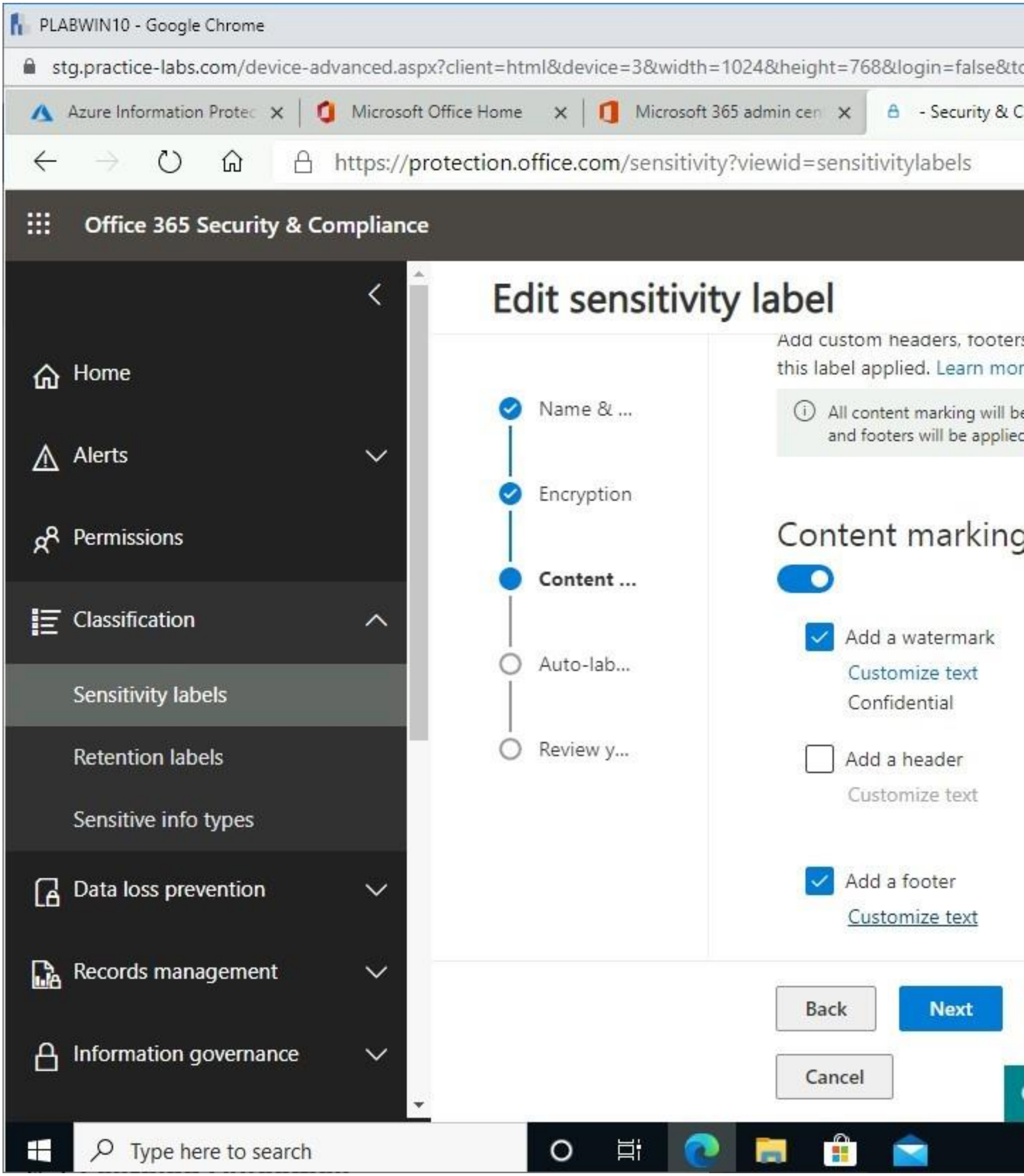
Figure 2.48 Screenshot of PLABWIN10 desktop: Customize watermark text

flyout menu is displayed showing the required settings performed and the Save button selected.

Step 7

Back on the **Content marking** page, scroll down further.

Select **Add a footer** and click **Customize text**.



Edit sensitivity label

Add custom headers, footers
this label applied. Learn mor

All content marking will be
and footers will be applied

Content marking

☑ Add a watermark
Customize text
Confidential

□ Add a header
Customize text

☑ Add a footer
Customize text

Figure 2.49 Screenshot of PLABWIN10 desktop: Content marking tab on

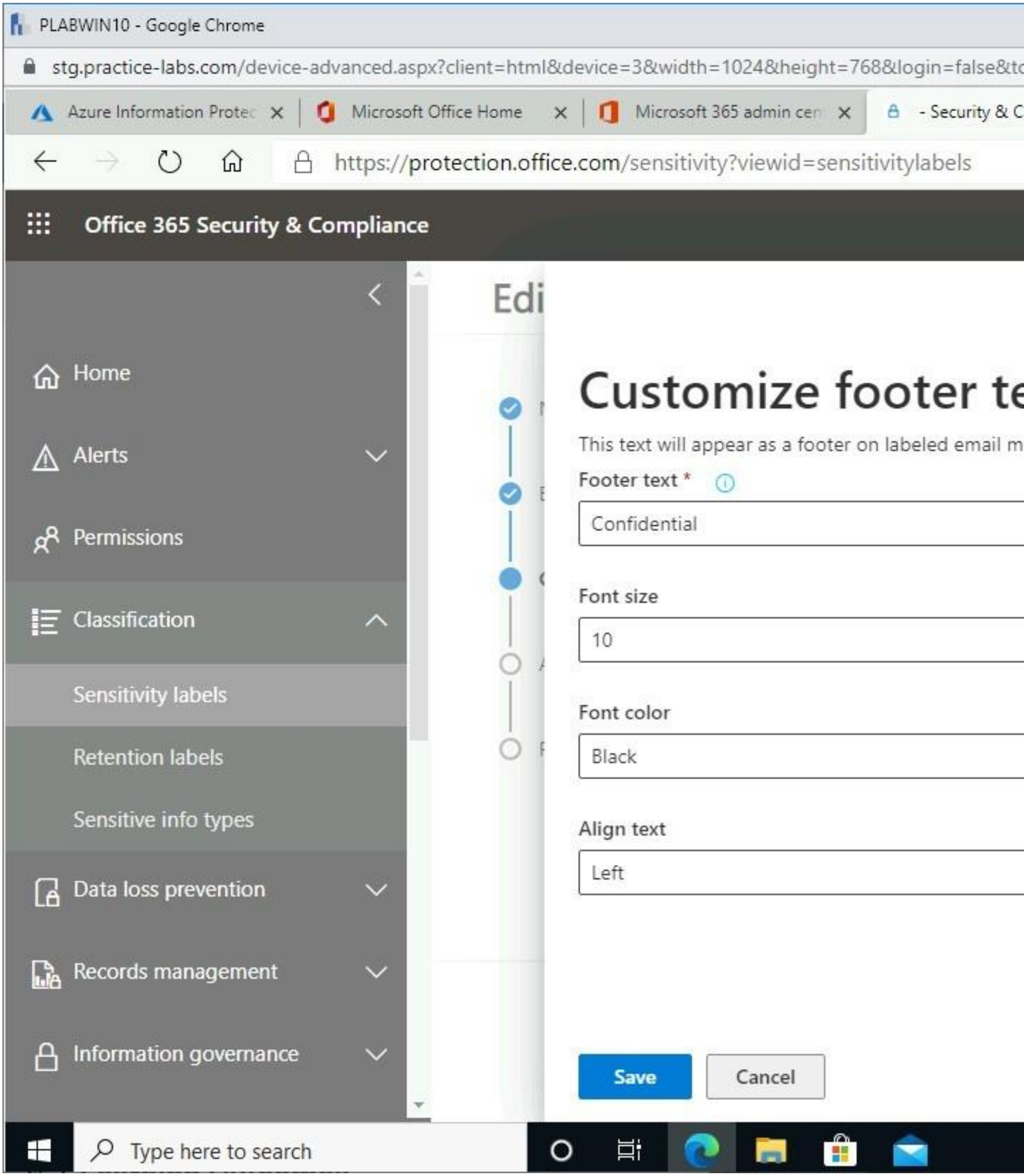
the Office 365 Security & Compliance - Edit sensitivity label screen is displayed showing the required settings performed and the Customize text link for the Add a footer section highlighted.

Step 8

On the **Customize footer text** menu, click in the **Footer** text box and type:

```
Confidential
```

Click **Save**.



Customize footer te

This text will appear as a footer on labeled email m

Footer text * Confidential

Font size 10

Font color Black

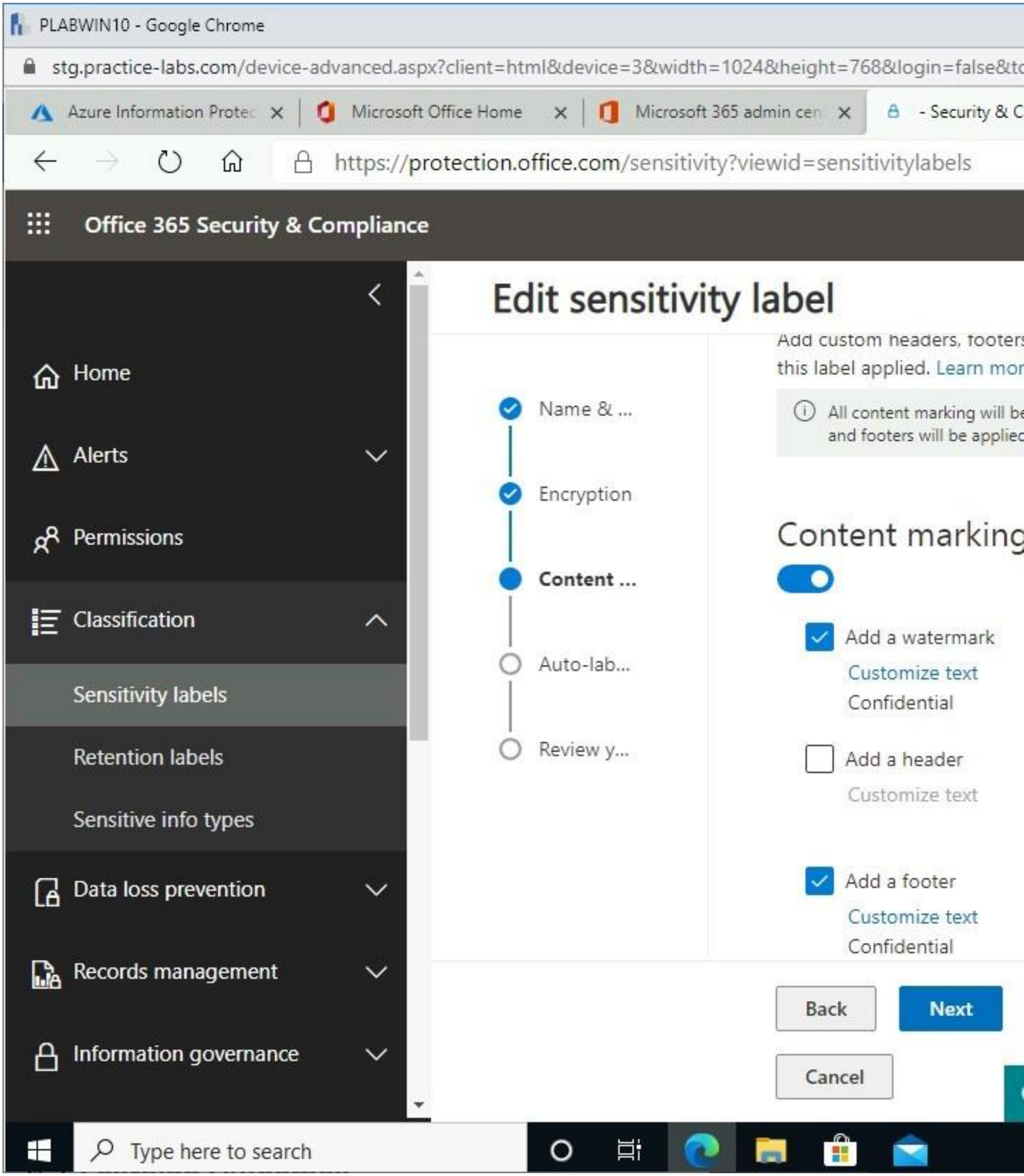
Align text Left

Figure 2.50 Screenshot of PLABWIN10 desktop: Customize footer text

flyout menu is displayed showing the required settings performed and the Save button selected.

Step 9

Click **Next** in the **Content marking** page.



Edit sensitivity label

Add custom headers, footers
this label applied. Learn mor

All content marking will be
and footers will be applied

Content marking

☑ Add a watermark
Customize text
Confidential

□ Add a header
Customize text

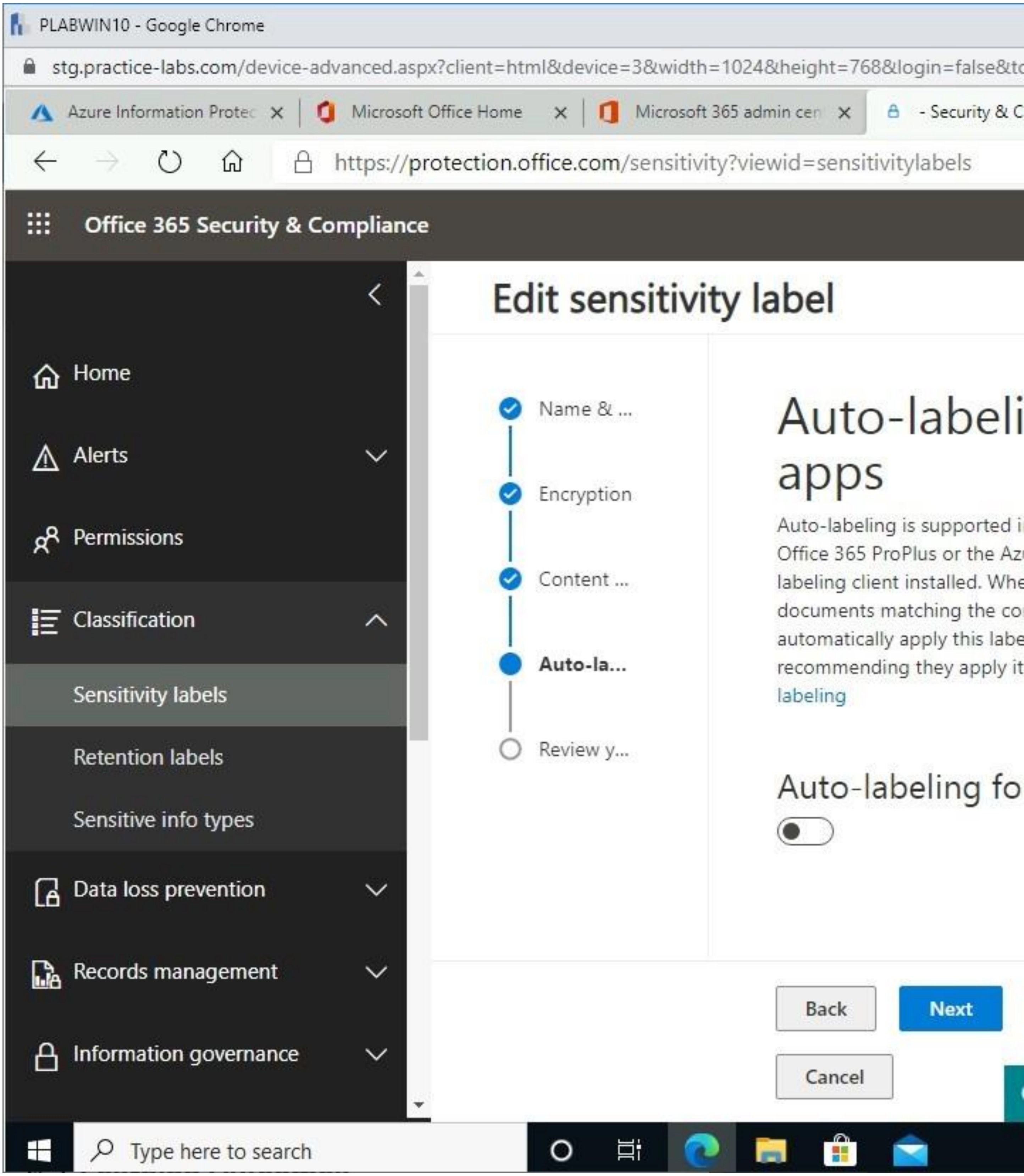
☑ Add a footer
Customize text
Confidential

Figure 2.51 Screenshot of PLABWIN10 desktop: Content marking tab on

the Office 365 Security & Compliance - Edit sensitivity label screen is displayed showing the required settings performed, and the Next button highlighted.

Step 10

Scroll down **Auto-labeling for Office apps** page to see other settings.



PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc

https://protection.office.com/sensitivity?viewid=sensitivitylabels

Edit sensitivity label

Auto-labeli
apps

Auto-labeling is supported i
Office 365 ProPlus or the Az
labeling client installed. Whe
documents matching the co
automatically apply this labe
recommending they apply it
labeling

Auto-labeling fo

Figure 2.52 Screenshot of PLABWIN10 desktop: Auto-labeling for Office

apps tab on the Office 365 Security & Compliance - Edit sensitivity label screen is displayed.

Step 11

Access the **Auto-labeling for Office apps** slider and set it to **On**.

***Note**: The "**Default**" field is useful for designating a keyword such as salary, wages, etc., considered as sensitive information. Then pair this keyword with Office 365-supplied sensitive info like Bank Account number and others.*

Under **Detect content that matches these conditions > Add condition > Content contains** click the drop-down list then select **Any of these**.

Click **Add** and select **Sensitive info types**.

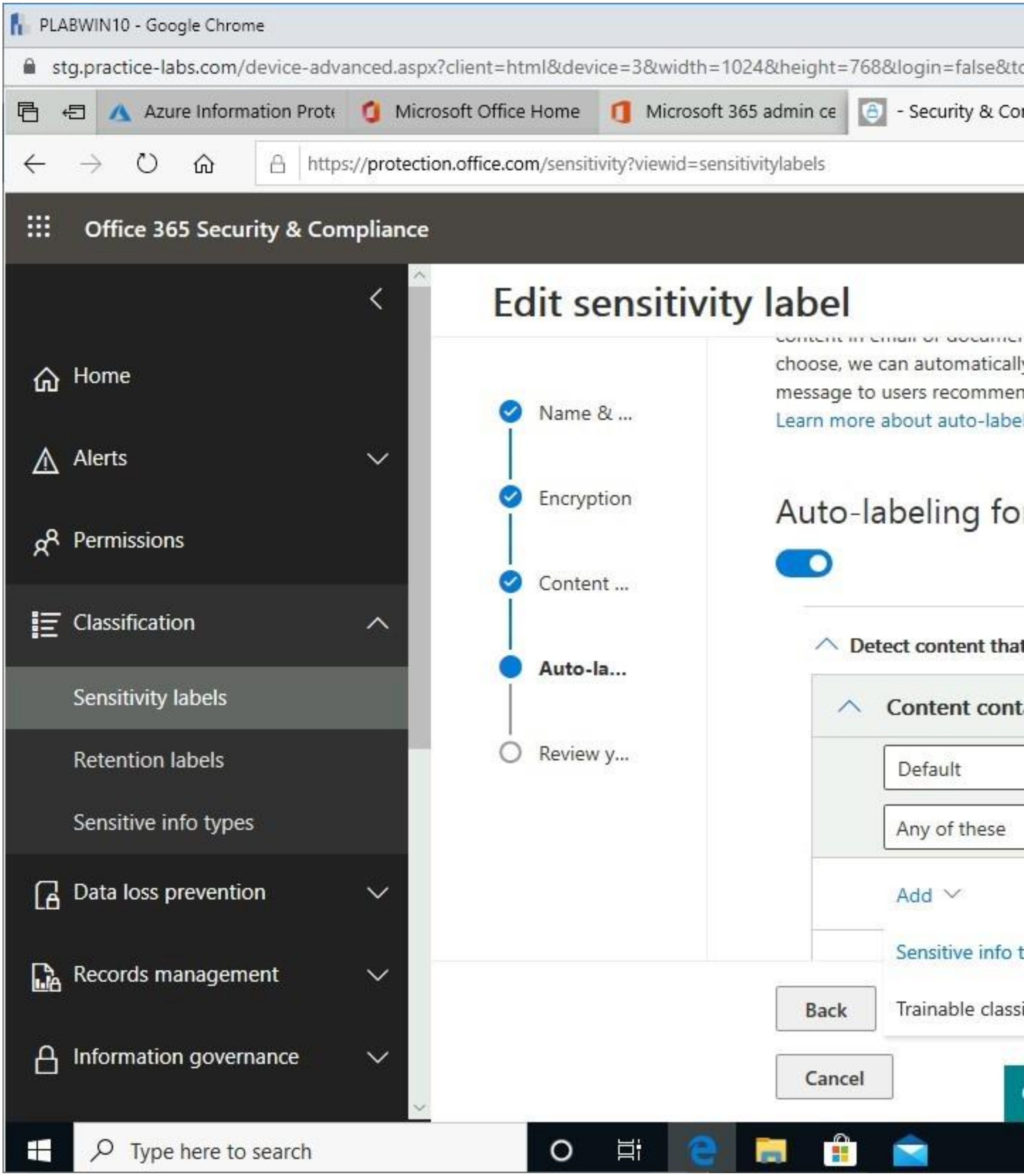


Figure 2.53 Screenshot of PLABWIN10 desktop: Auto-labeling for Office

apps tab on the Office 365 Security & Compliance - Edit sensitivity label screen is displayed showing the required settings performed for the Detect content that matches these conditions option.

Step 12

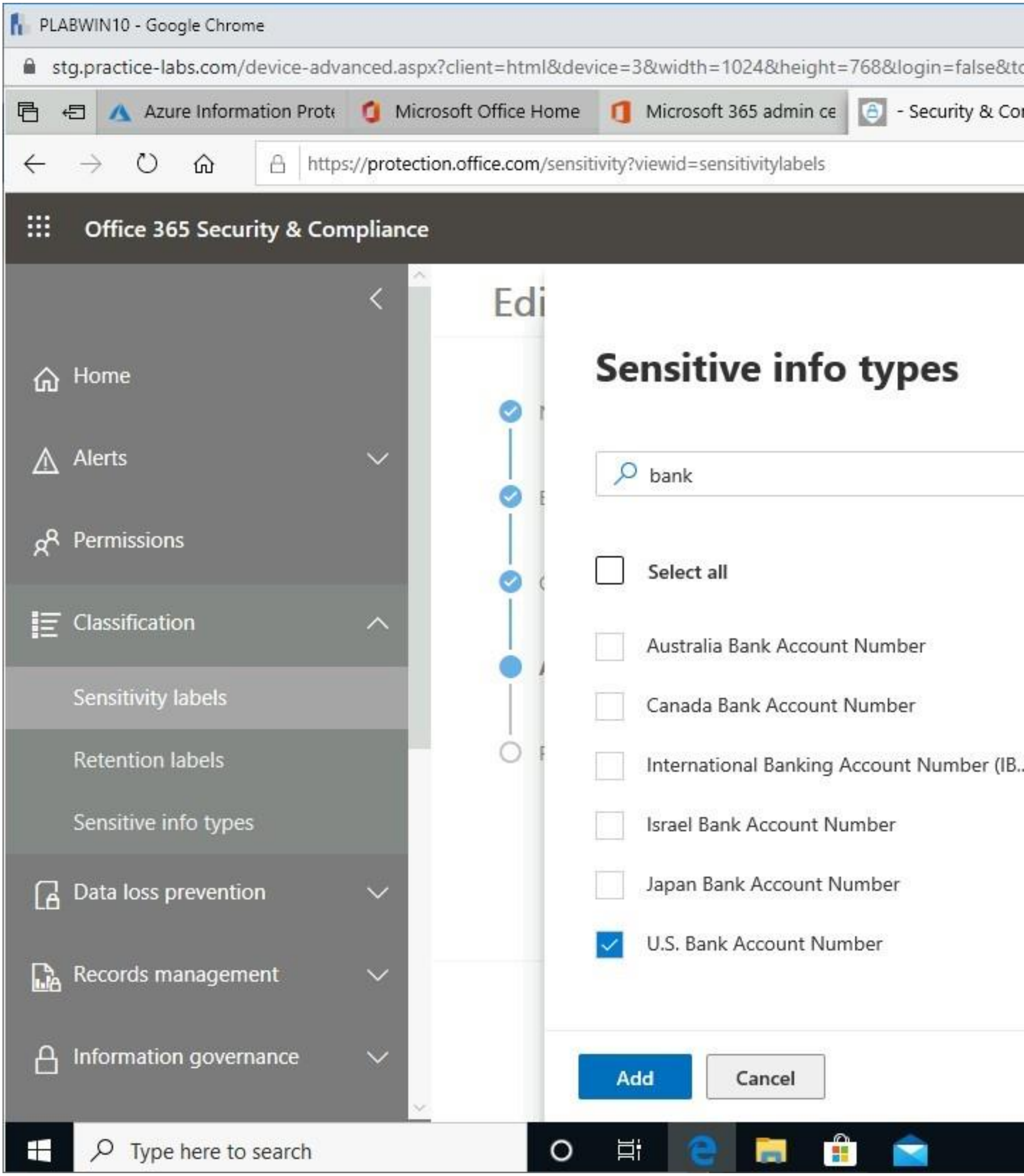
From the **Sensitive info types** menu, click in the search box and type:

```
bank
```

Press **Enter**.

Select **U.S. Bank Account Number** checkbox.

Click **Add**.



Sensitive info types

bank

☐ Select all

☐ Australia Bank Account Number

☐ Canada Bank Account Number

☐ International Banking Account Number (IB...

☐ Israel Bank Account Number

☐ Japan Bank Account Number

☑ U.S. Bank Account Number

Figure 2.54 Screenshot of PLABWIN10 desktop: Sensitive info types flyout

menu is displayed showing the required settings performed and Add button selected.

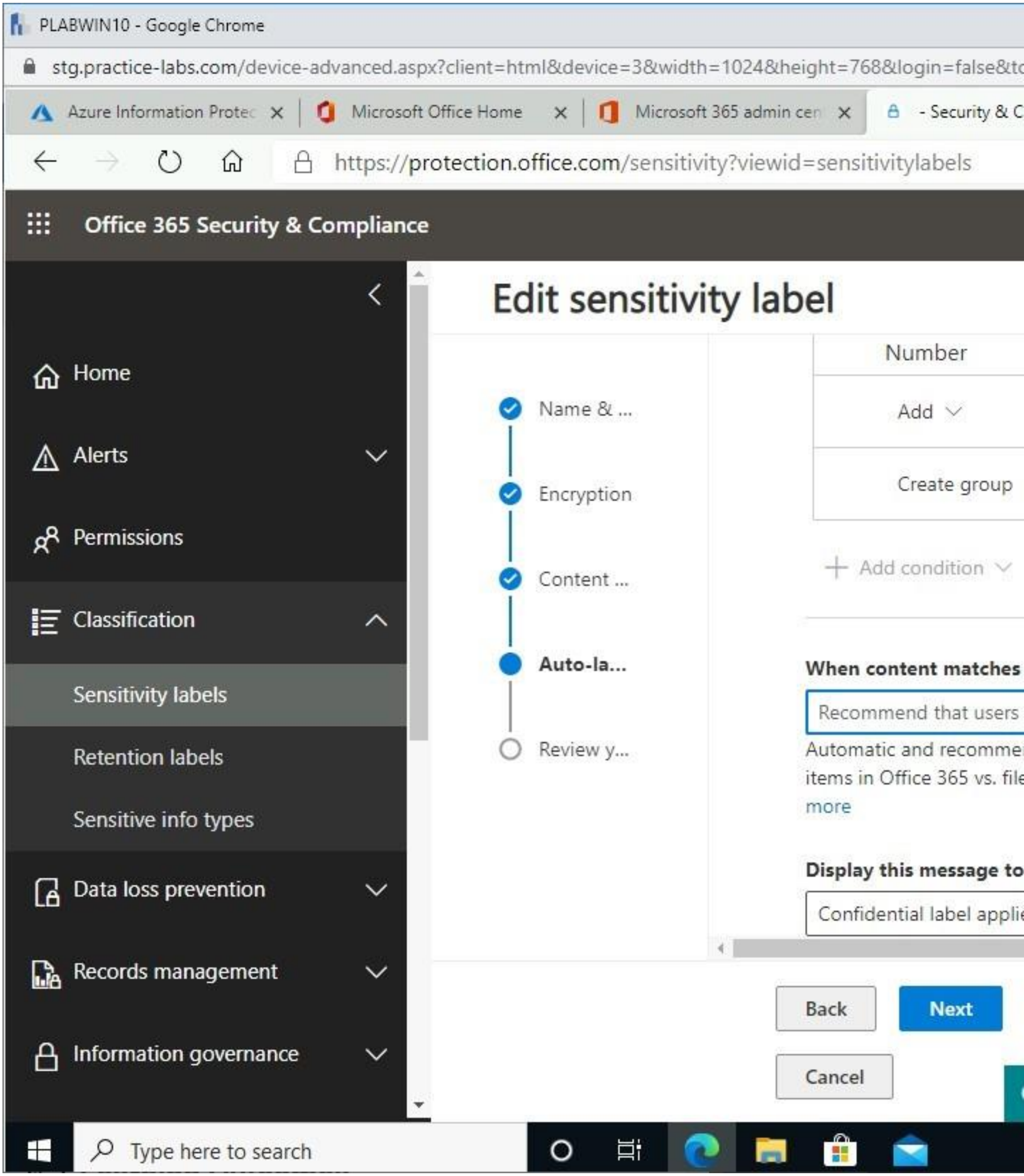
Step 13

Back in the **Auto-labeling for Office apps** page, scroll down to **When content matches these conditions** drop-down list, select **Recommend that users apply the label**.

Click in the **Display this message to users when the label is applied** box and type:

```
Confidential label applied.
```

Click **Next**.



When content matches

Recommend that users

Automatic and recomme items in Office 365 vs. file more

Display this message to

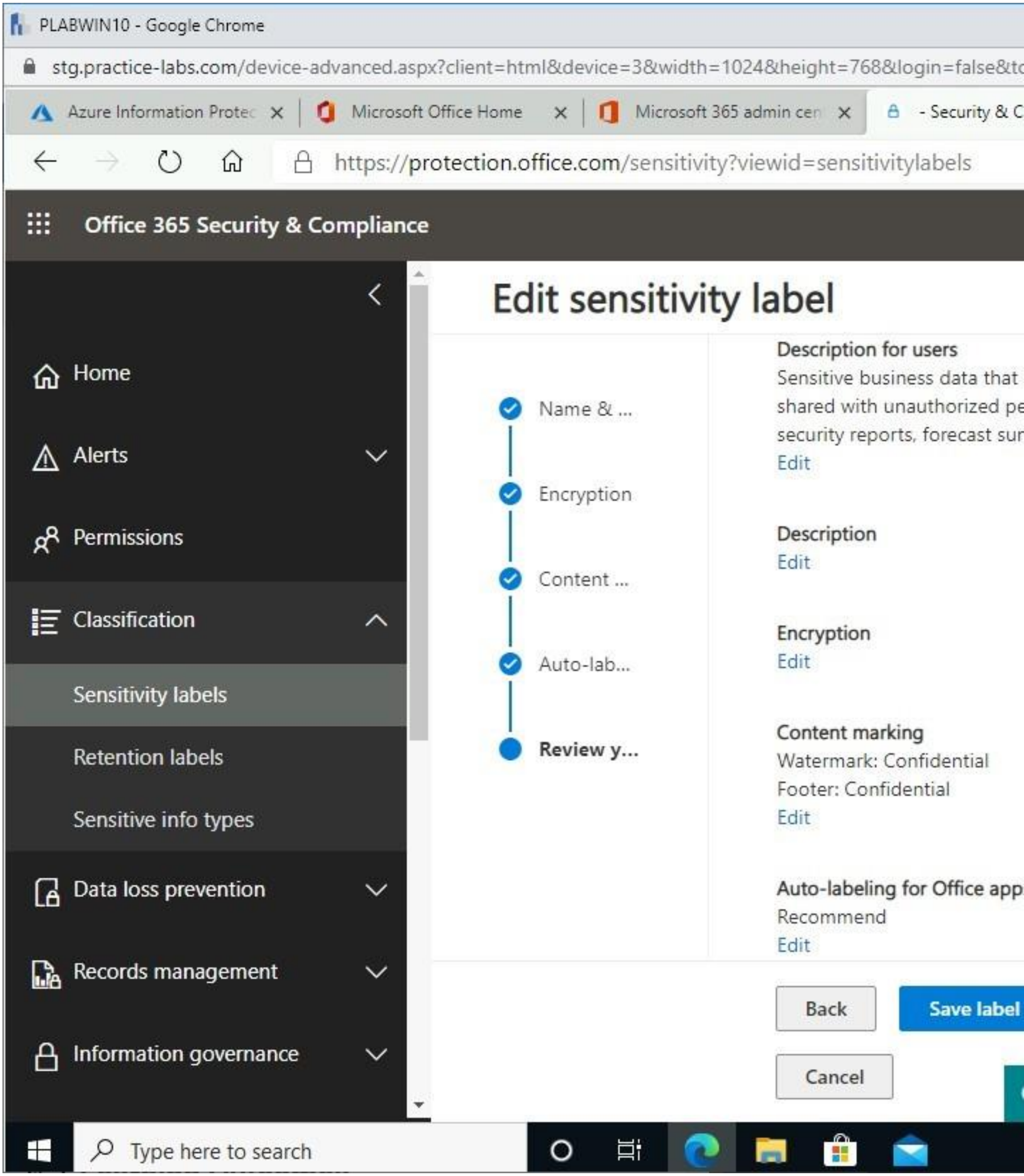
Confidential label applie

Figure 2.55 Screenshot of PLABWIN10 desktop: Auto-labeling for Office

apps tab on the Office 365 Security & Compliance - Edit sensitivity label screen is displayed showing the required settings performed and the Next button highlighted.

Step 14

On the **Review your settings** page, click **Save label**.



Edit sensitivity label

Description for users
Sensitive business data that
shared with unauthorized pe
security reports, forecast sur
Edit

Description
Edit

Encryption
Edit

Content marking
Watermark: Confidential
Footer: Confidential
Edit

Auto-labeling for Office app
Recommend
Edit

Figure 2.56 Screenshot of PLABWIN10 desktop: Review your settings tab

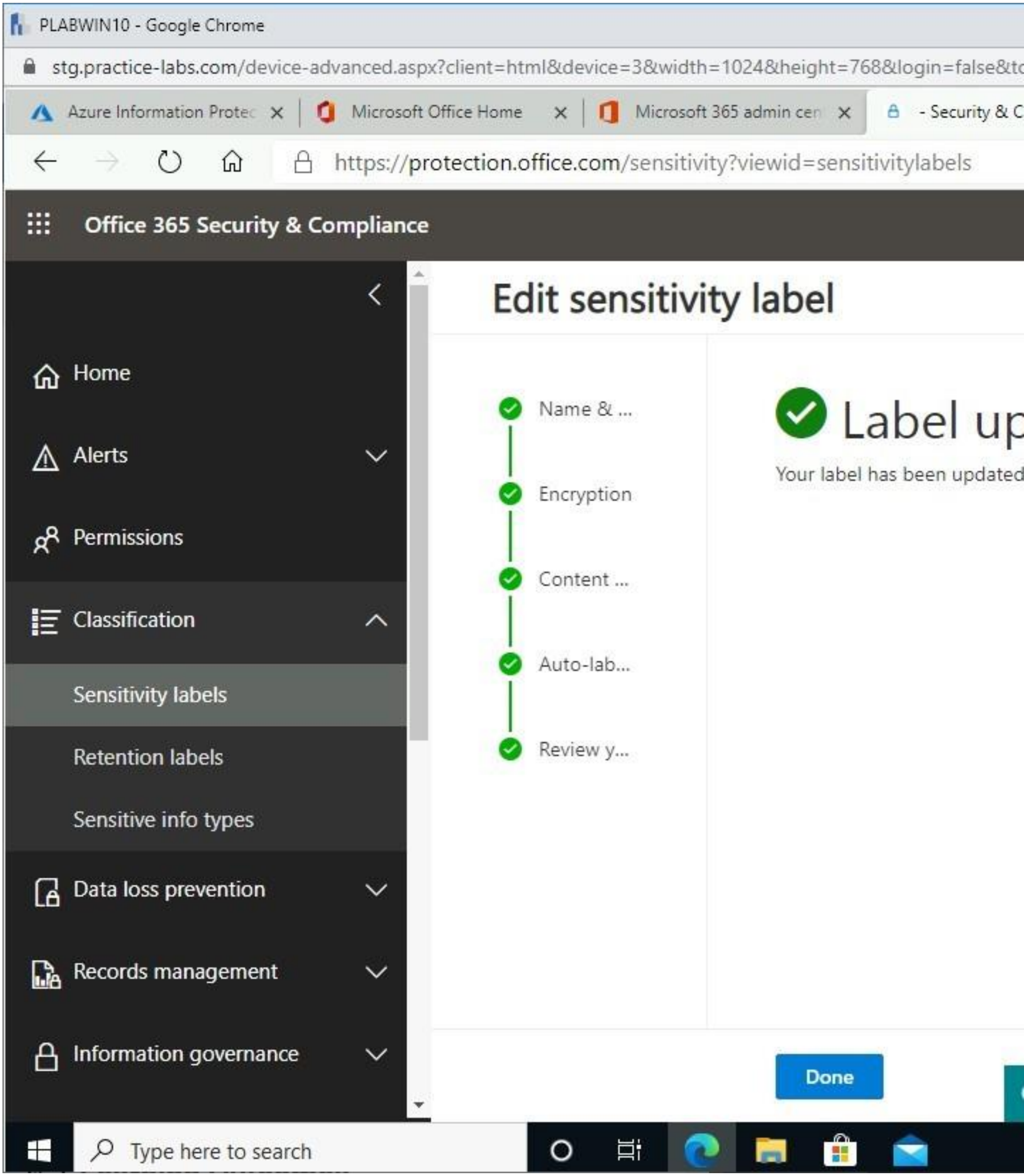
on the Office 365 Security & Compliance - Edit sensitivity label screen is displayed listing the settings performed and showing the Save label button selected.

Step 15

Please wait while the changes on the label save.

You will get a successful confirmation when the label gets updated.

Click **Done**.



Edit sensitivity label

- Name & ...
- Encryption
- Content ...
- Auto-lab...
- Review y...

Label up

Your label has been updated

Done

Figure 2.57 Screenshot of PLABWIN10 desktop: Label updated message is

displayed on the Office 365 Security & Compliance - Edit sensitivity label screen.

Task 5 - Publish the Labels

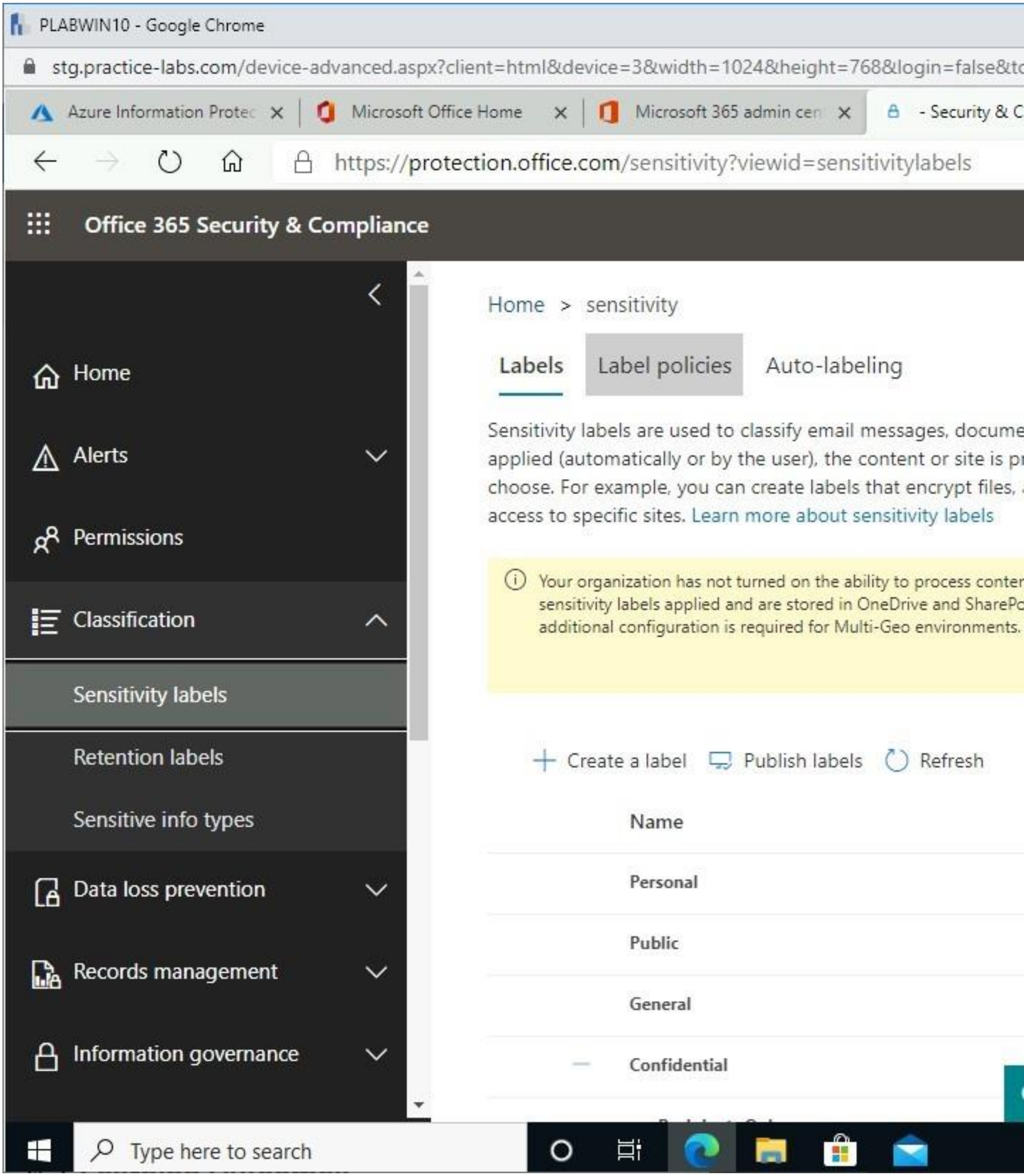
In order to make the labels available to Office apps, the labels, whether they are default or custom, must be published to all or specific users and groups in the Azure tenant.

For this task, you will publish the AIP labels to make them available to AIP-aware applications like Microsoft Office.

Step 1

Ensure you are connected to **PLABWIN10** and are in the **Sensitivity labels** section.

Select **Label policies**.



Sensitivity labels are used to classify email messages, docume applied (automatically or by the user), the content or site is pr choose. For example, you can create labels that encrypt files, access to specific sites. Learn more about sensitivity labels

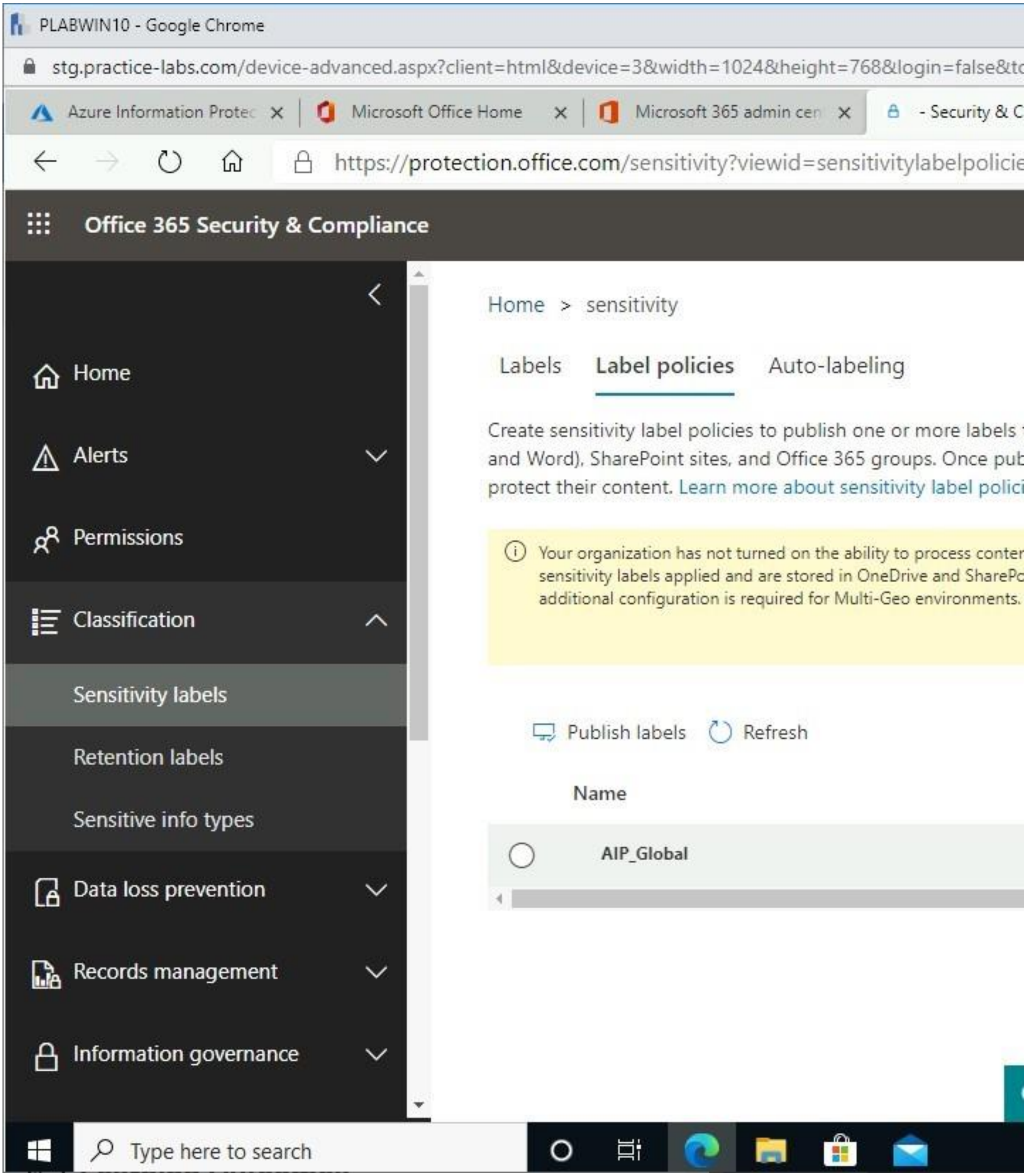
Your organization has not turned on the ability to process conte sensitivity labels applied and are stored in OneDrive and SharePo additional configuration is required for Multi-Geo environments.

Figure 2.58 Screenshot of PLABWIN10 desktop: Required option on the

Office 365 Security & Compliance - Sensitivity screen is selected.

Step 2

Select **AIP_Global** policy.



Create sensitivity label policies to publish one or more labels
and Word), SharePoint sites, and Office 365 groups. Once pub
protect their content. Learn more about sensitivity label polici

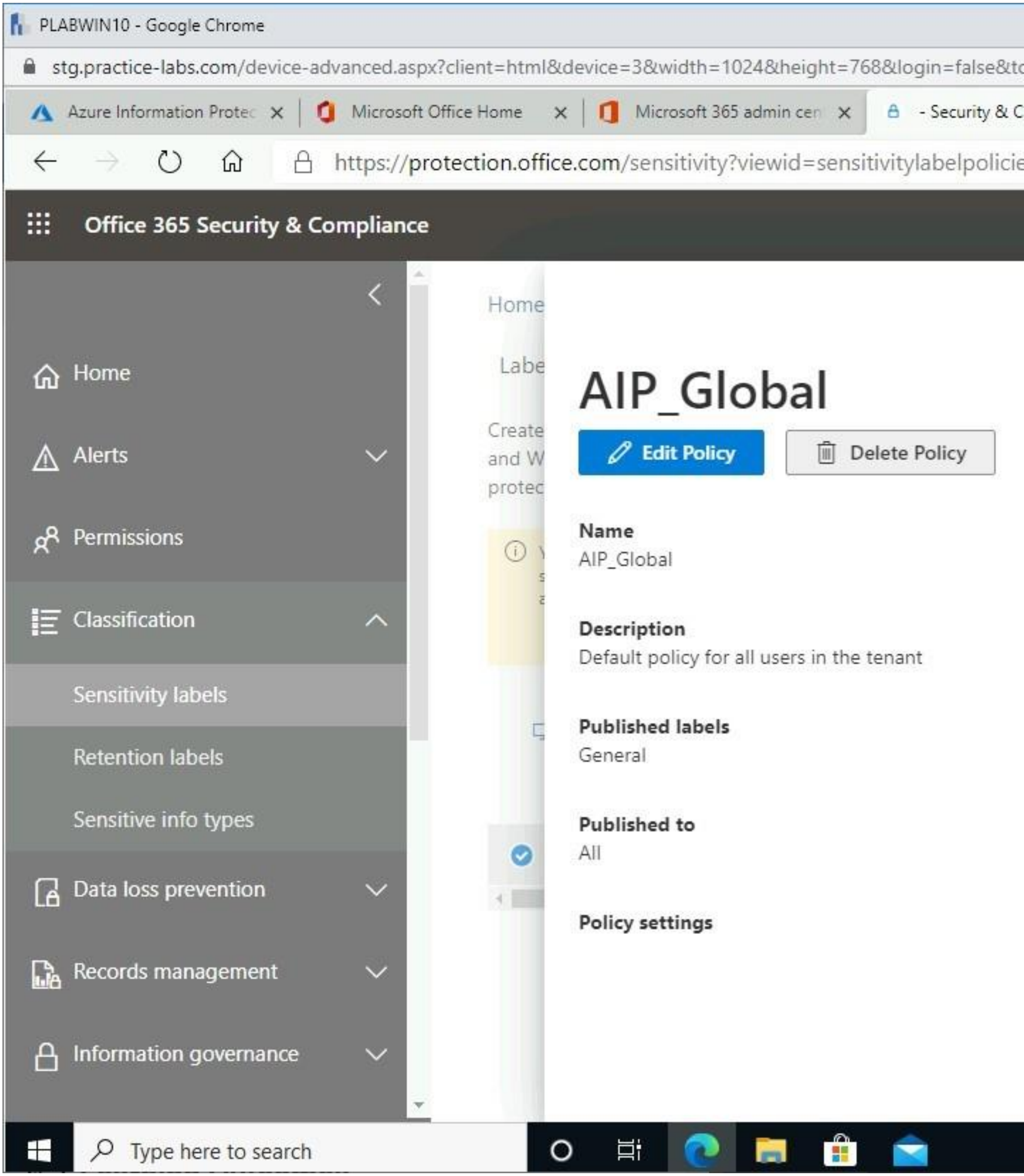
Your organization has not turned on the ability to process conter
sensitivity labels applied and are stored in OneDrive and SharePo
additional configuration is required for Multi-Geo environments.

Figure 2.59 Screenshot of PLABWIN10 desktop: Required option on the

Label policies tab of the Office 365 Security & Compliance - Sensitivity screen is selected.

Step 3

On the **AIP_Global** menu, click **Edit policy**.



AIP_Global

Name
AIP_Global

Description
Default policy for all users in the tenant

Published labels
General

Published to
All

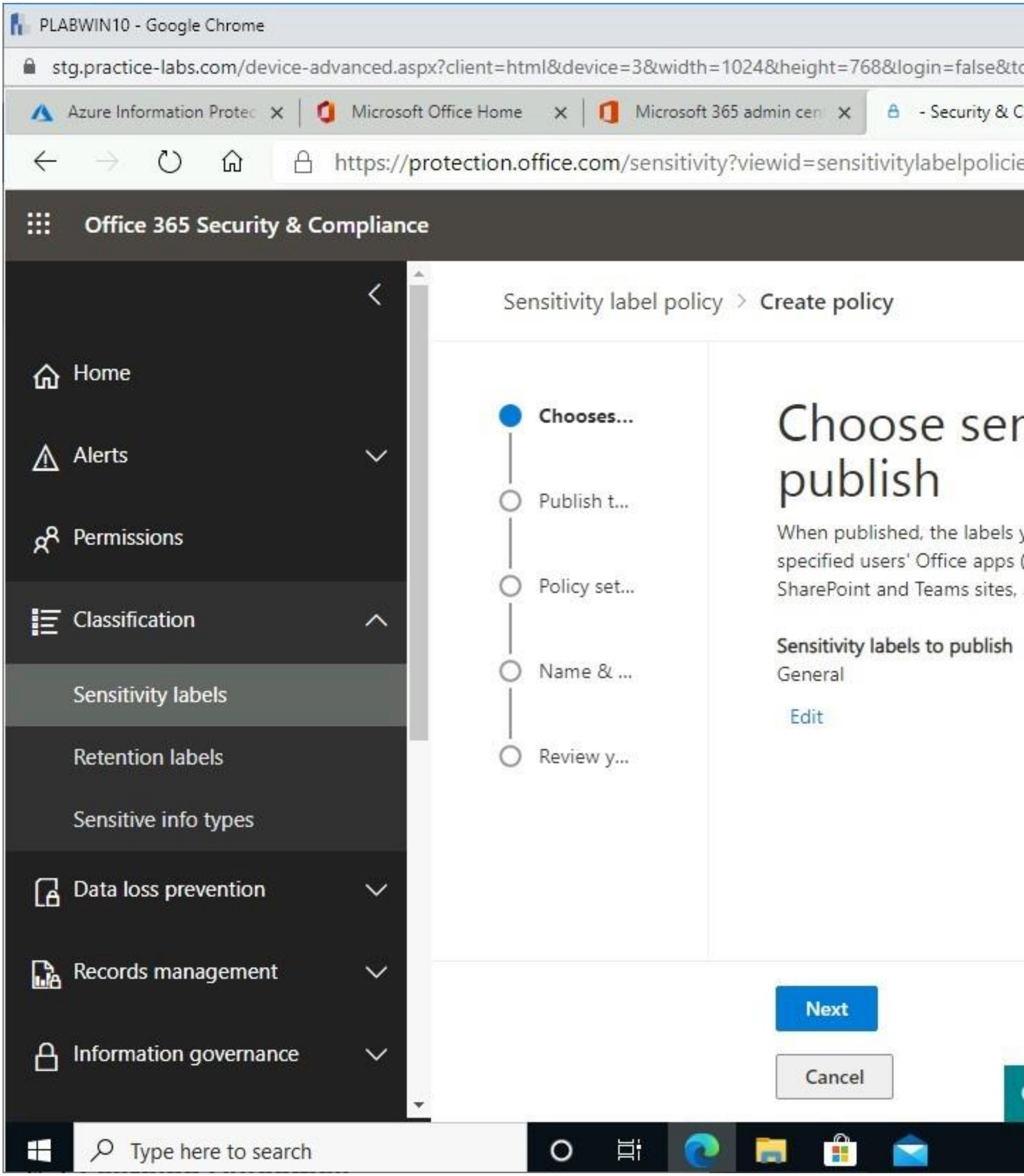
Policy settings

Figure 2.60 Screenshot of PLABWIN10 desktop: Edit Policy button on the

AIP_Global flyout menu is selected.

Step 4

From the **Choose sensitivity labels to publish** page, go to **Sensitivity labels to publish** section, and click **Edit**.



Choose ser
publish

When published, the labels y
specified users' Office apps (
SharePoint and Teams sites,

Sensitivity labels to publish
General

Edit

Figure 2.61 Screenshot of PLABWIN10 desktop: Choose sensitivity labels to

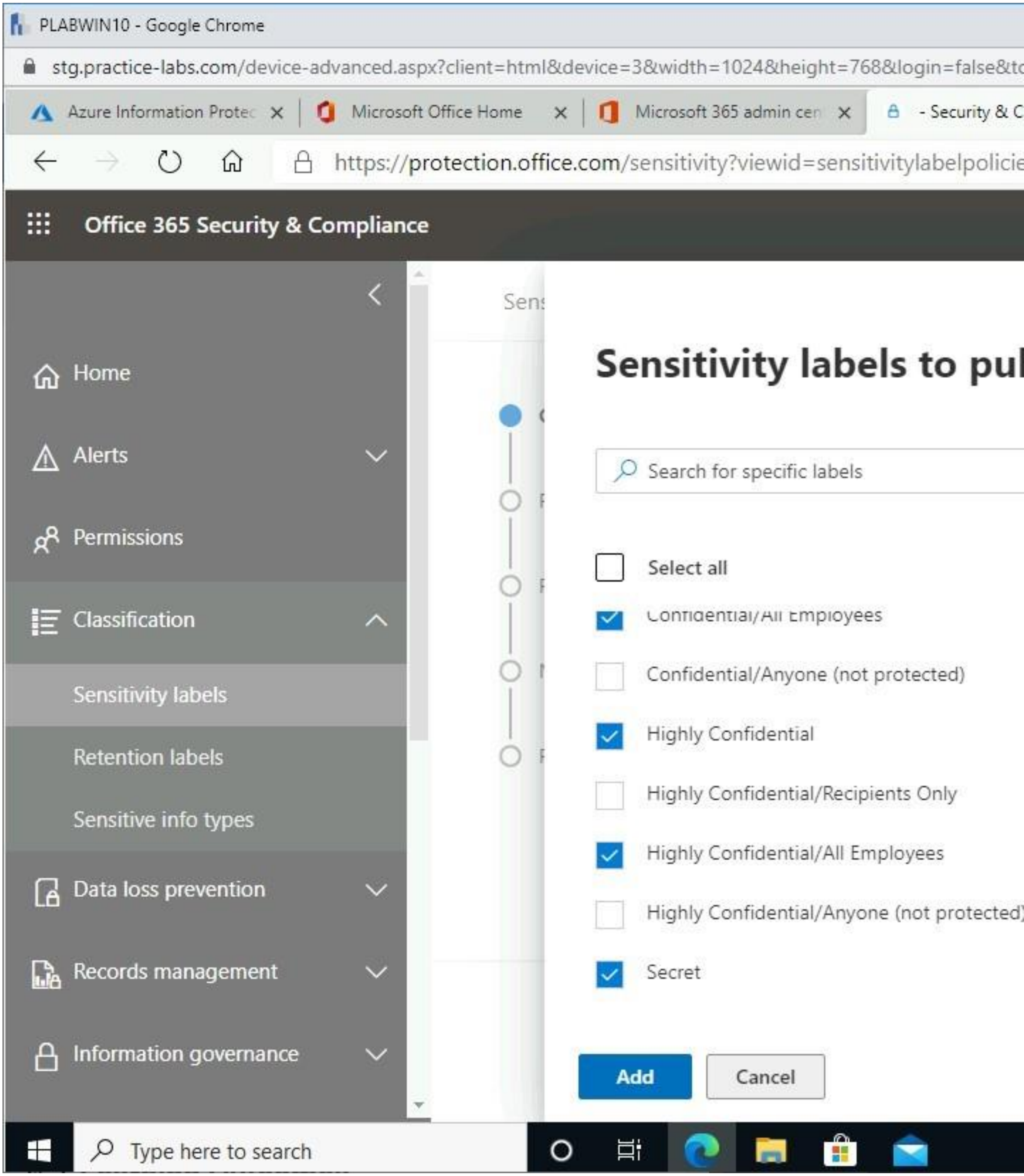
publish tab on the Office 365 Security & Compliance - Sensitivity label policy > Create policy screen is displayed showing the Edit link highlighted.

Step 5

On the **Sensitivity labels to publish** menu, select the following checkboxes:

- General
- Confidential
- Confidential/All Employees
- Highly Confidential
- Highly Confidential/All Employees
- Secret

Click **Add**.



Sensitivity labels to pul

Search for specific labels

☐ Select all

☑ Confidential/All Employees

☐ Confidential/Anyone (not protected)

☑ Highly Confidential

☐ Highly Confidential/Recipients Only

☑ Highly Confidential/All Employees

☐ Highly Confidential/Anyone (not protected)

☑ Secret

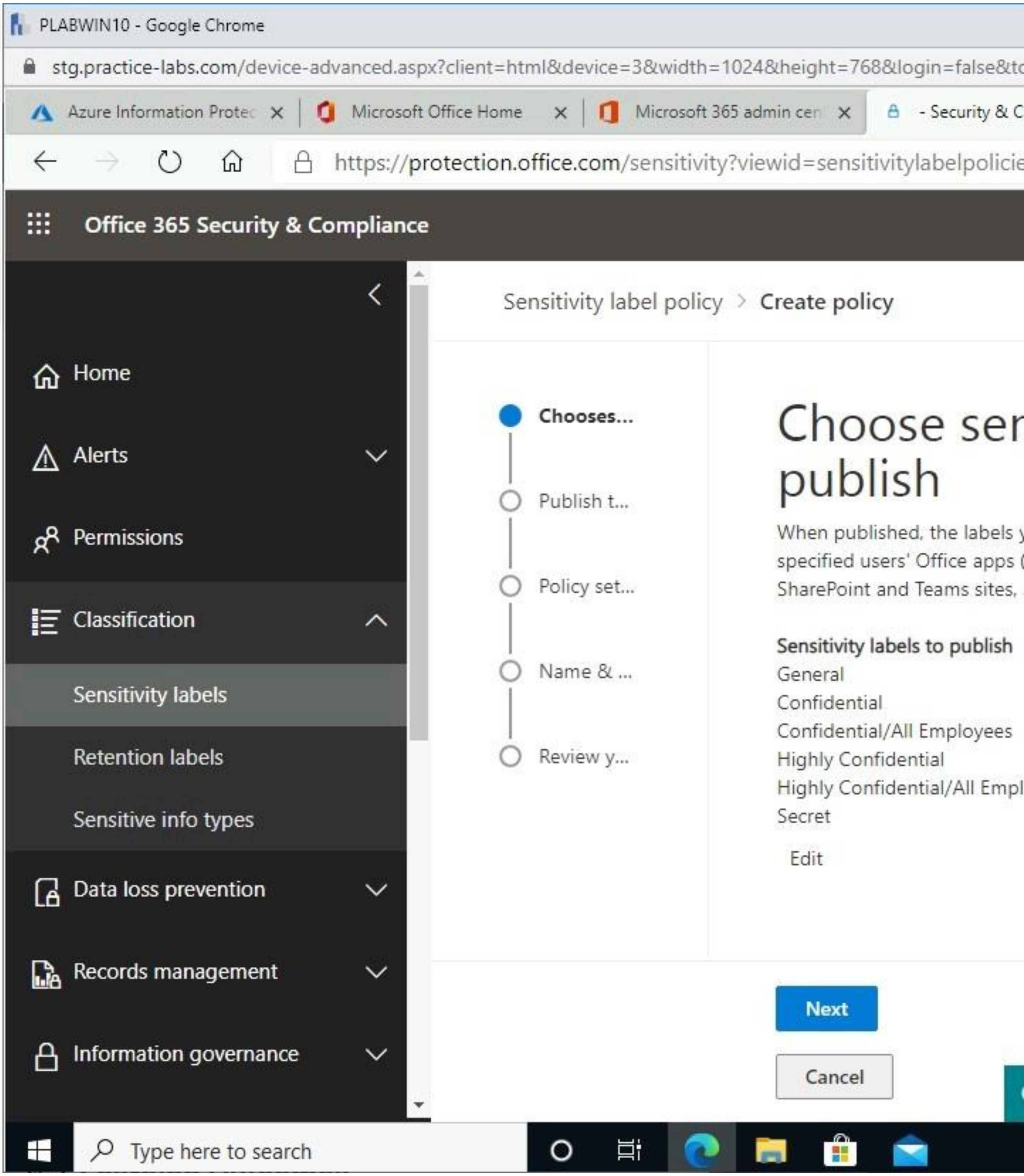
Add   Cancel

Figure 2.62 Screenshot of PLABWIN10 desktop: Sensitivity labels to

publish flyout menu is displayed showing the required selections performed and the Add button selected.

Step 6

Back on the **Choose sensitivity labels to publish** page, click **Next**.



Sensitivity label policy > Create policy

- Chooses...
- Publish t...
- Policy set...
- Name & ...
- Review y...

Choose ser
publish

When published, the labels y
specified users' Office apps (
SharePoint and Teams sites,

Sensitivity labels to publish

General
Confidential
Confidential/All Employees
Highly Confidential
Highly Confidential/All Empl
Secret

Edit

Next

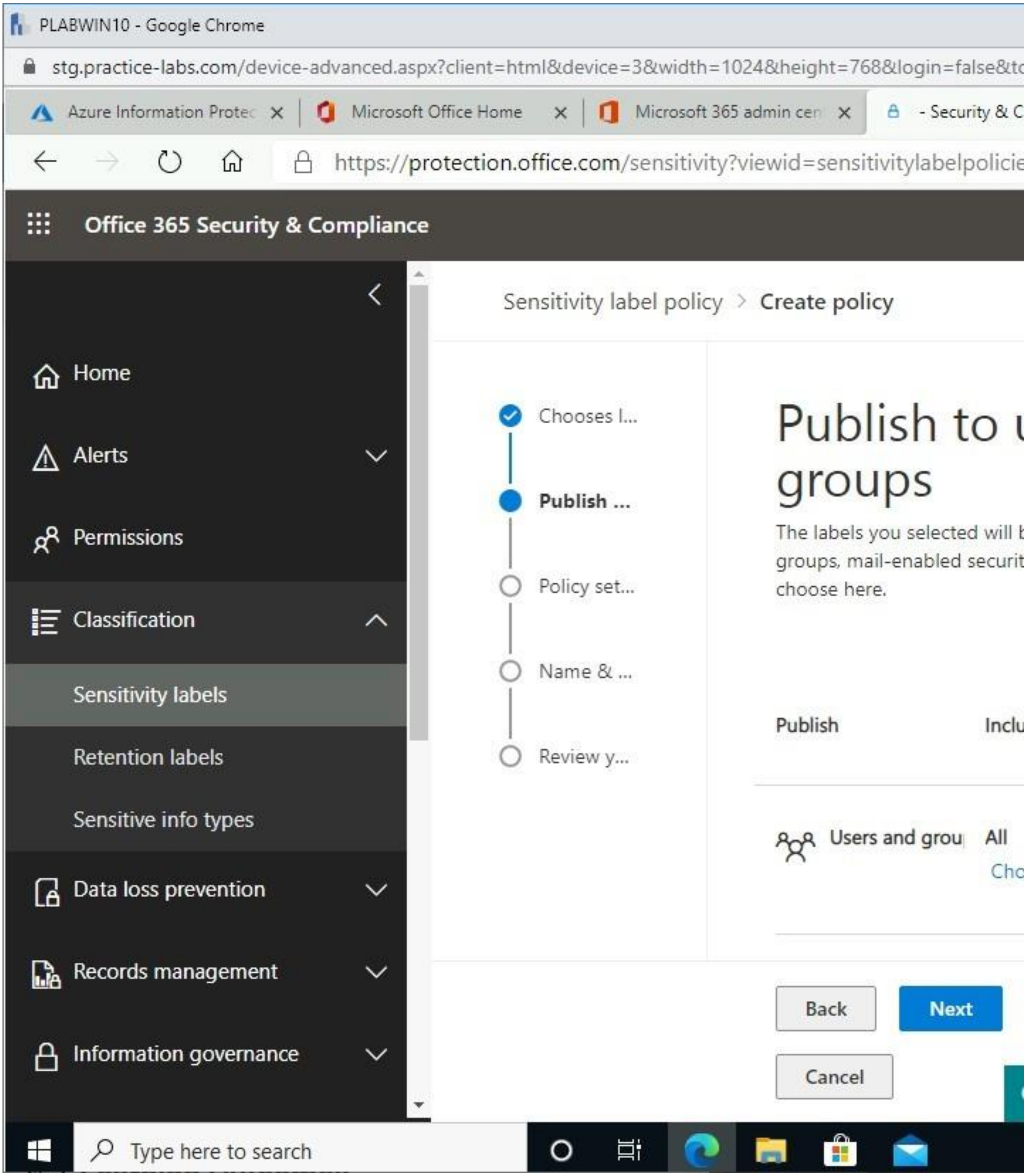
Cancel

Figure 2.63 Screenshot of PLABWIN10 desktop: Choose sensitivity labels to

publish tab on the Office 365 Security & Compliance - Sensitivity label policy > Create policy screen is displayed showing the required settings performed and the Next button selected.

Step 7

From the **Publish to users and groups** page, scroll down to view other settings.



Publish to u
groups

The labels you selected will b
groups, mail-enabled securit
choose here.

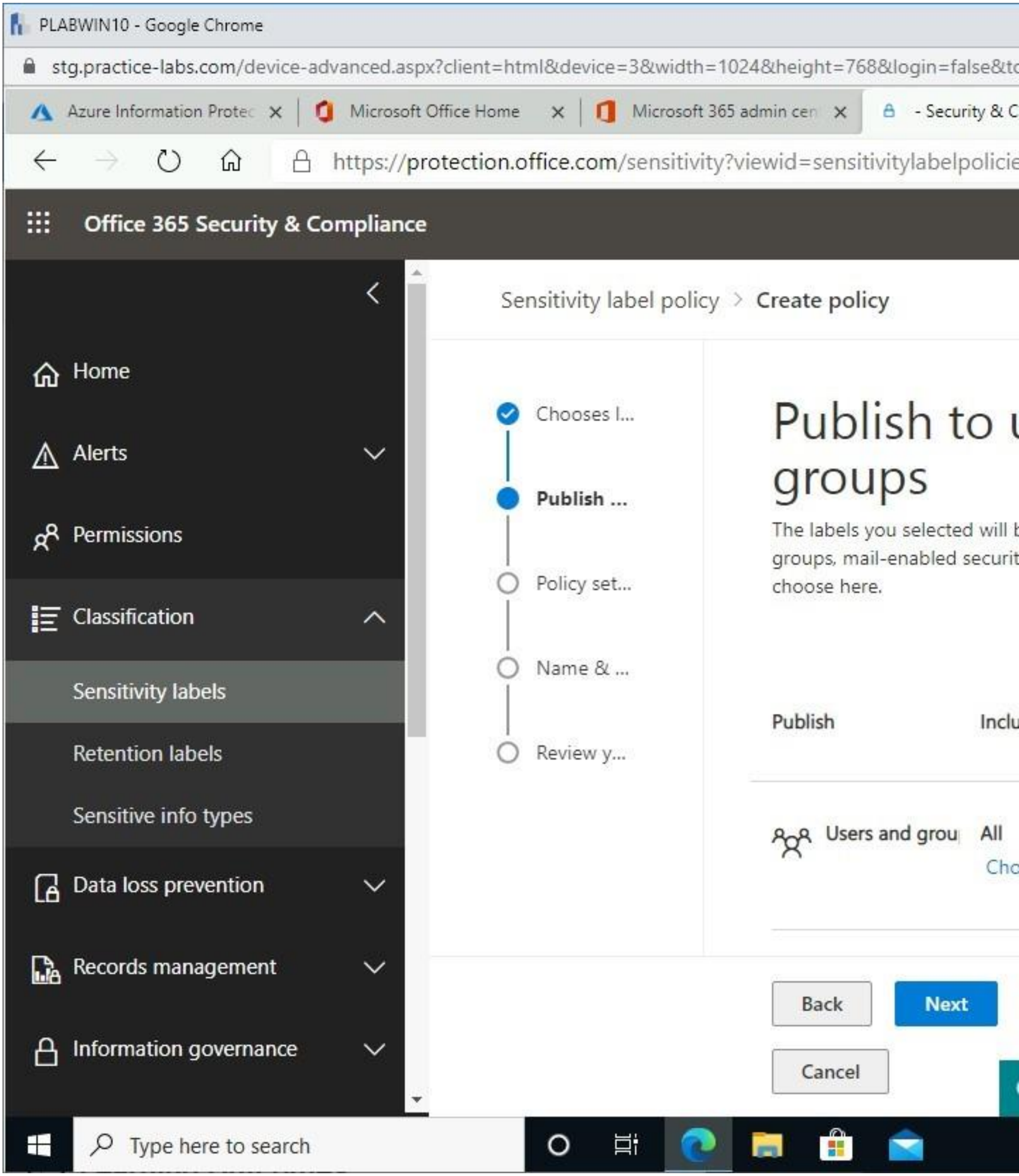
Publish	Inclu
Users and grou	All Cho

Figure 2.64 Screenshot of PLABWIN10 desktop: Publish to users and

groups tab on the Office 365 Security & Compliance - Sensitivity label policy > Create policy screen is displayed.

Step 8

From the **Publish to users and groups**, select **Choose users or groups**.



The labels you selected will b
groups, mail-enabled securit
choose here.

Figure 2.65 Screenshot of PLABWIN10 desktop: Publish to users and

groups tab on the Office 365 Security & Compliance - Sensitivity label policy > Create policy screen is displayed.

Step 9

Select **Add** in the **Edit locations** page.

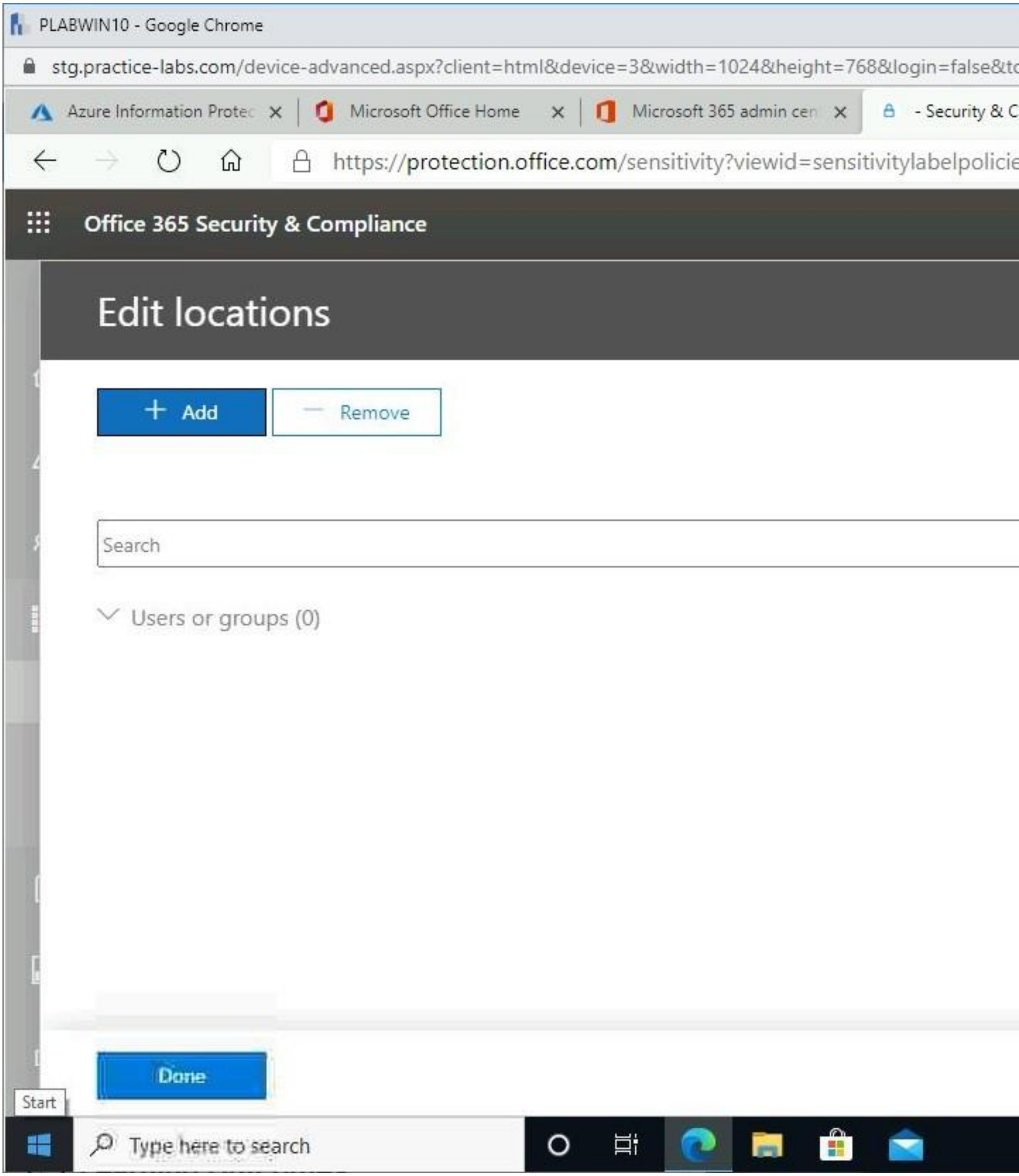

PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc
Azure Information Protec
Microsoft Office Home
Microsoft 365 admin cen
- Security & C
https://protection.office.com/sensitivity?viewid=sensitivitylabelpolicie
Office 365 Security & Compliance
Edit locations
+ Add
— Remove
Search
Users or groups (0)
Done
Start
Type here to search

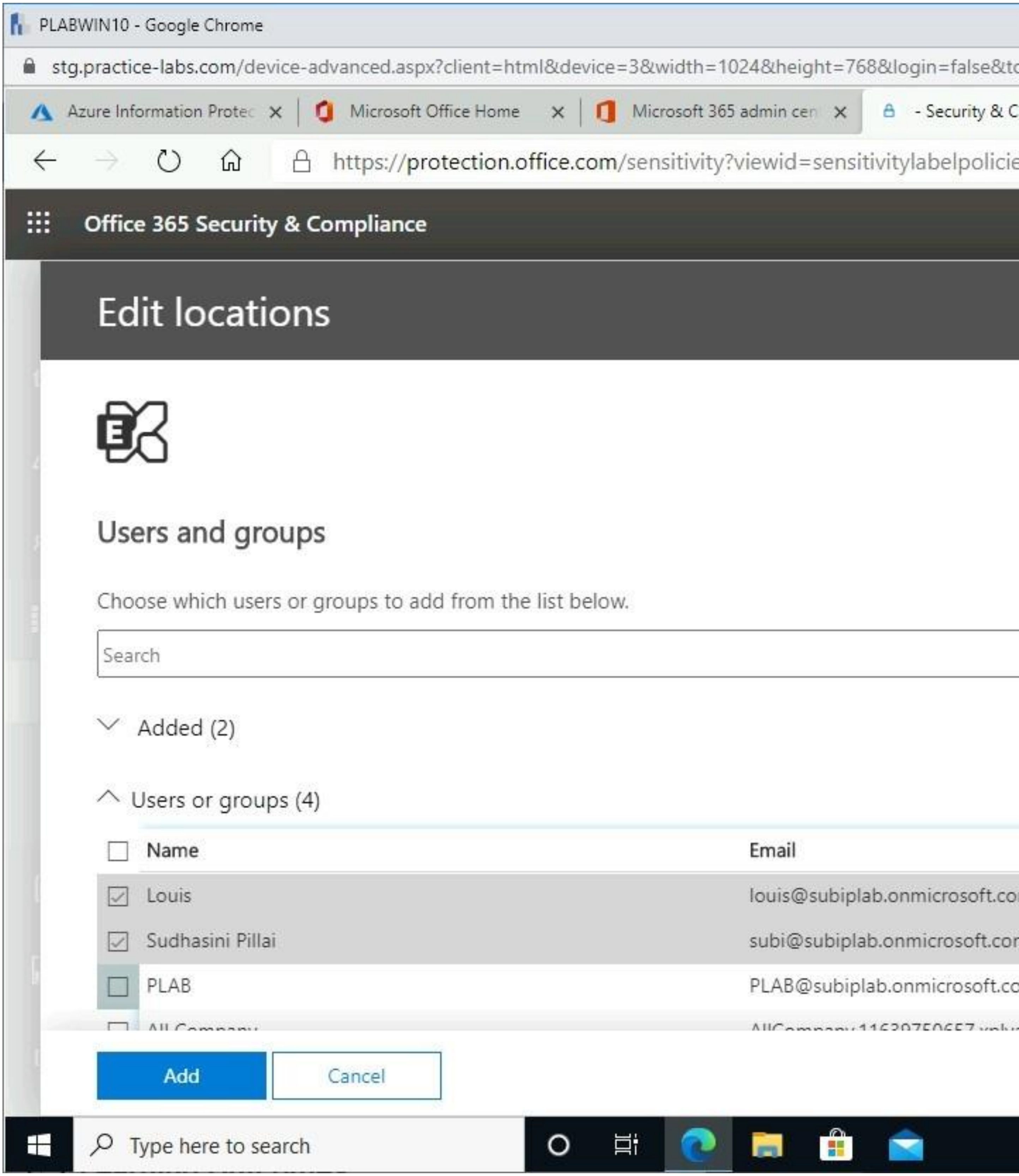
Figure 2.66 Screenshot of PLABWIN10 desktop: Add button on the Edit

locations flyout menu is highlighted.

Step 10

Select all the users in your Azure AD tenant.

Click **Add**.


PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc
Azure Information Protec
Microsoft Office Home
Microsoft 365 admin cen
- Security & C
https://protection.office.com/sensitivity?viewid=sensitivitylabelpolicie
Office 365 Security & Compliance
Type here to search

Edit locations

Users and groups

Choose which users or groups to add from the list below.

Search
Added (2)
Users or groups (4)

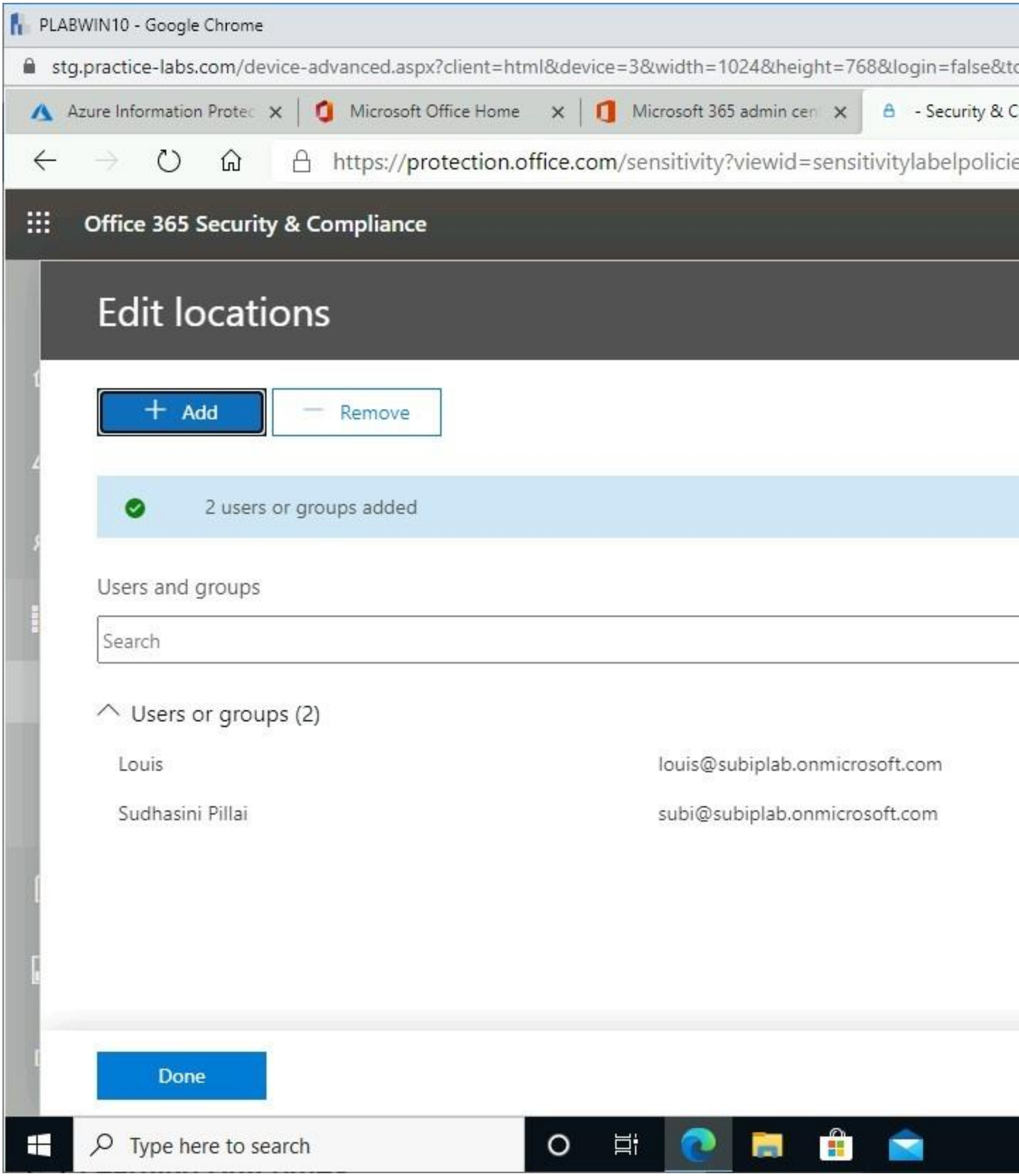
□	Name	Email
☑	Louis	louis@subiplab.onmicrosoft.co
☑	Sudhasini Pillai	subi@subiplab.onmicrosoft.cor
□	PLAB	PLAB@subiplab.onmicrosoft.co
□	All Company	AllCompany.116

Figure 2.67 Screenshot of PLABWIN10 desktop: Edit locations flyout menu

is displayed showing the required selections performed, and the Add button highlighted.

Step 11

Click **Done** when the selected users are successfully added.


PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc
Azure Information Protec
Microsoft Office Home
Microsoft 365 admin cen
- Security & C
https://protection.office.com/sensitivity?viewid=sensitivitylabelpolicie
Office 365 Security & Compliance
Edit locations
+ Add
— Remove
Search
Done
Type here to search

2 users or groups added

Users and groups

Users or groups (2)

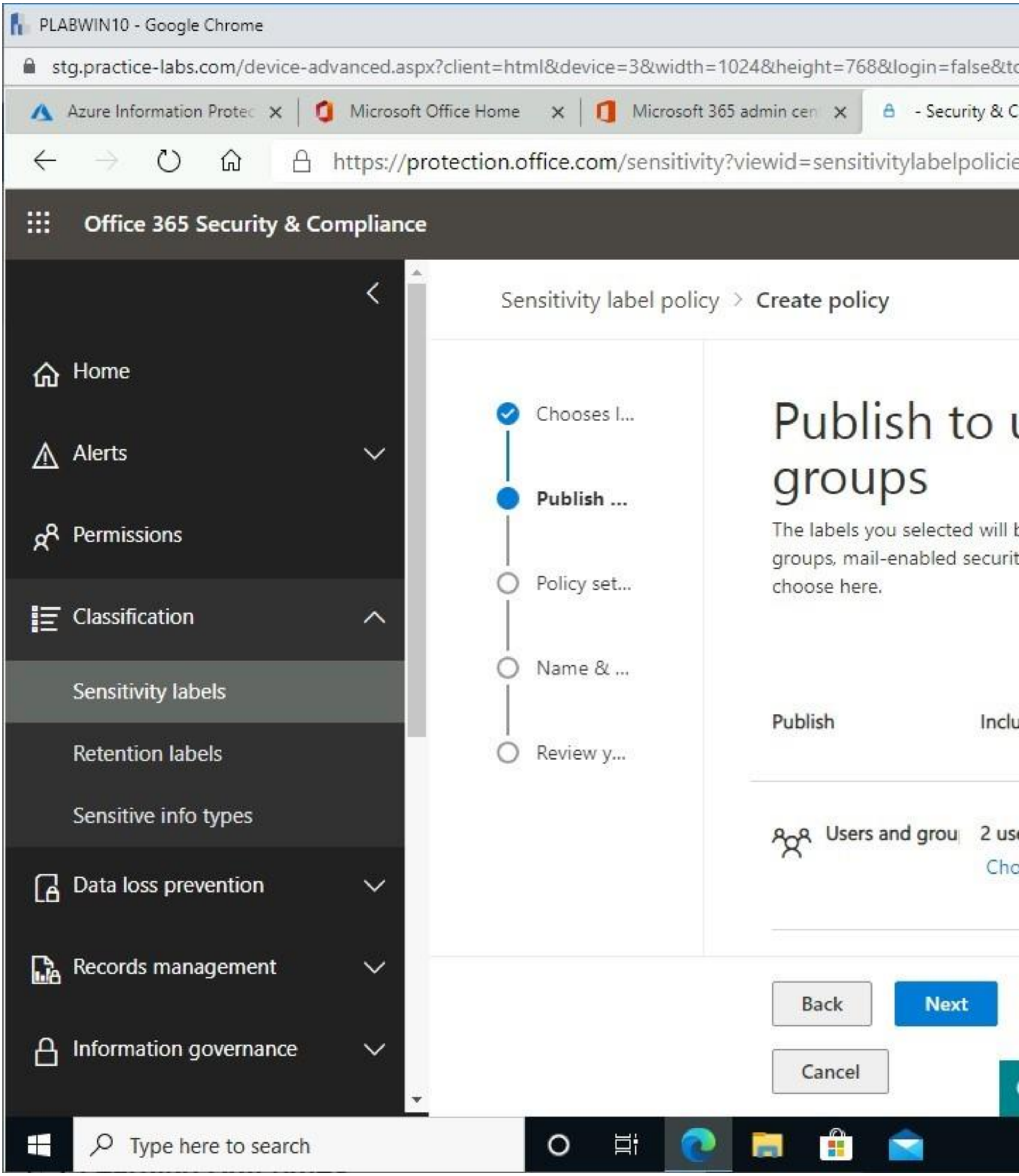
Louis	louis@subiplab.onmicrosoft.com
Sudhasini Pillai	subi@subiplab.onmicrosoft.com

Figure 2.68 Screenshot of PLABWIN10 desktop: Edit locations flyout menu

is displayed showing the required selections performed and the Done button highlighted.

Step 12

Click **Next** on the **Publish to users and groups** page.



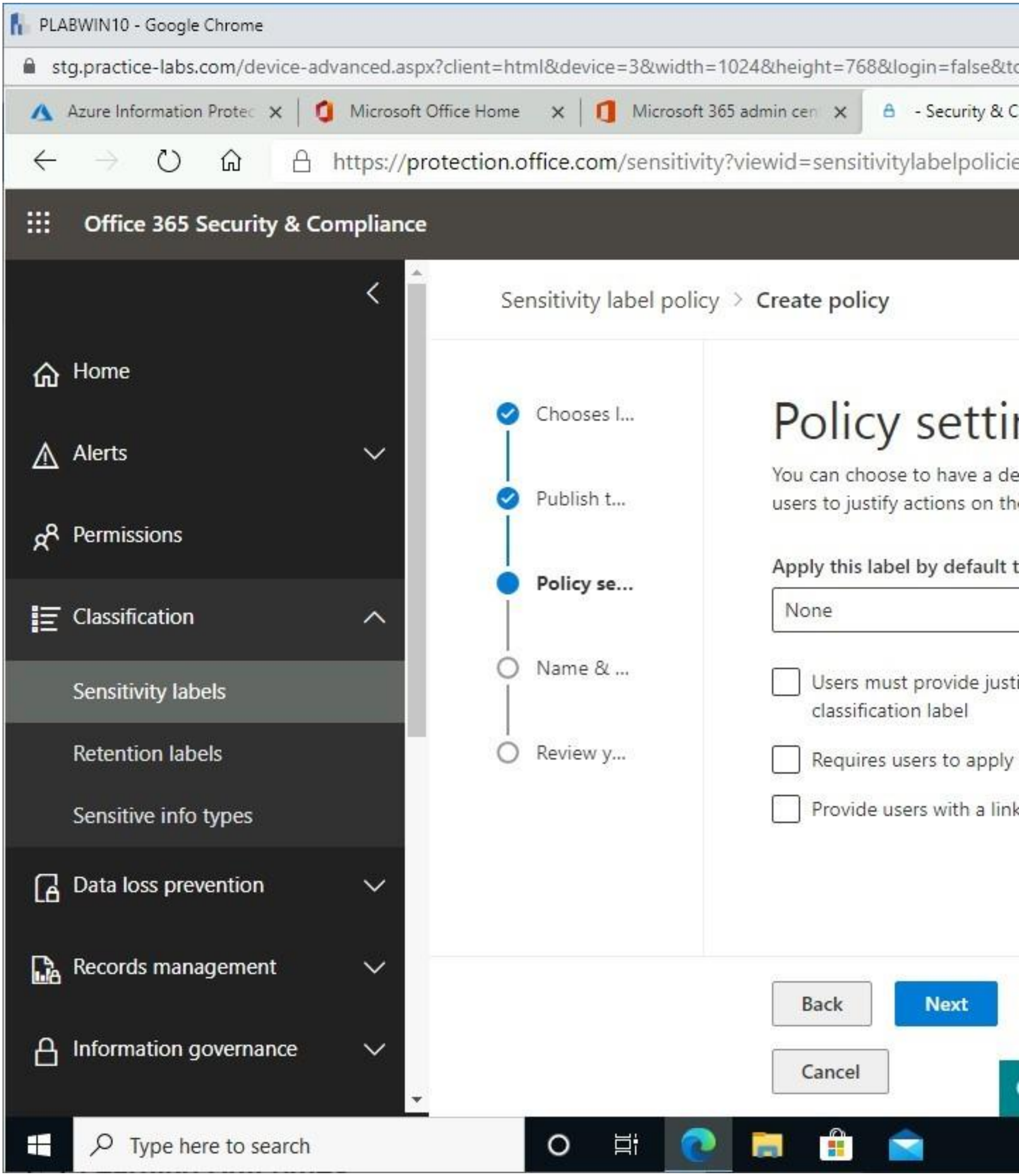
The labels you selected will b
groups, mail-enabled securit
choose here.

Figure 2.69 Screenshot of PLABWIN10 desktop: Publish to users and

groups tab on the Office 365 Security & Compliance - Sensitivity label policy > Create policy screen is displayed listing the settings performed and the Next button selected.

Step 13

From the **Policy settings** page, scroll down a bit to see other settings.



Policy settir

You can choose to have a de
users to justify actions on th

Apply this label by default t

None

□ Users must provide justi
classification label

□ Requires users to apply

□ Provide users with a link

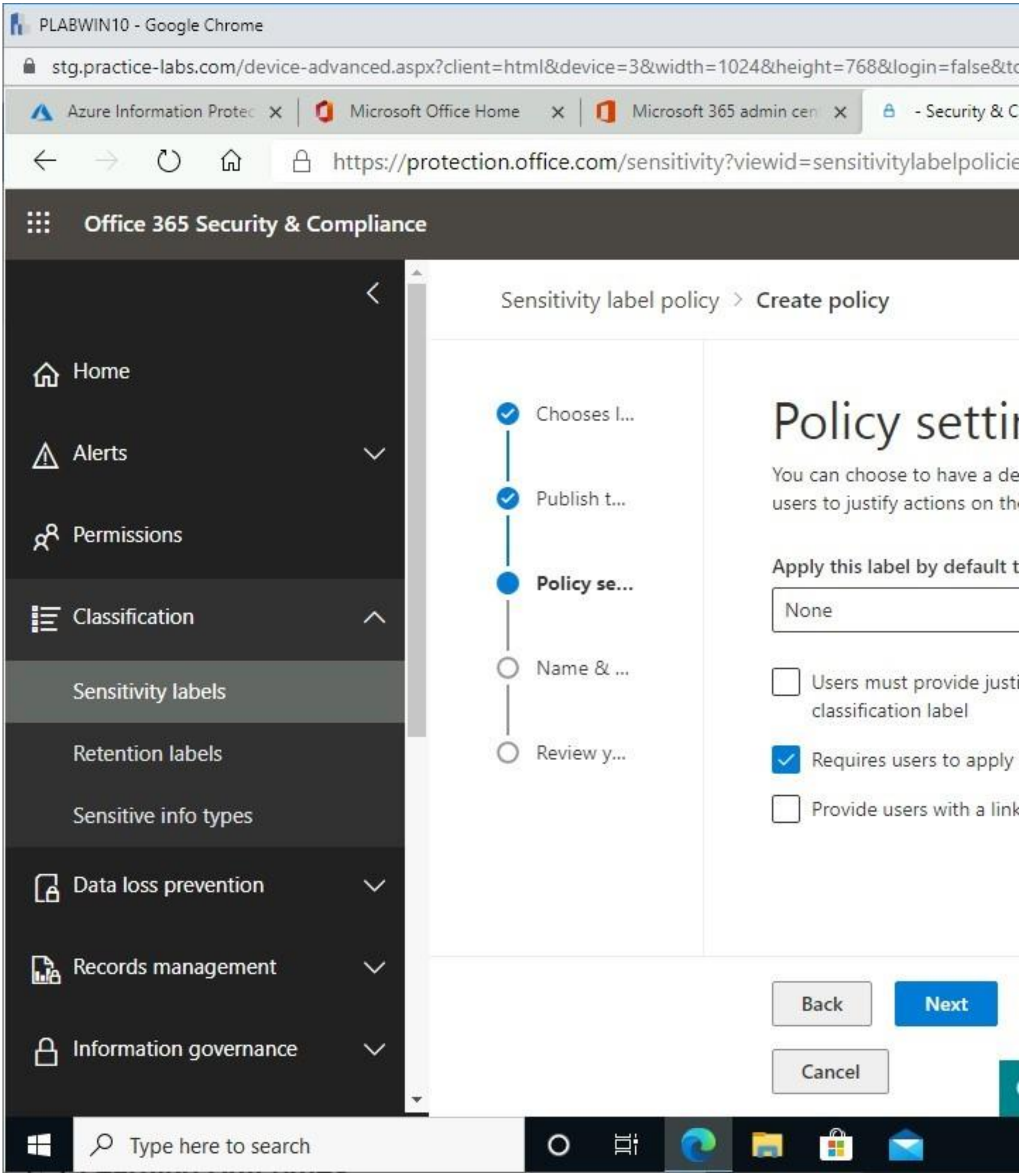
Figure 2.70 Screenshot of PLABWIN10 desktop: Policy settings tab on the

Office 365 Security & Compliance - Sensitivity label policy > Create policy screen is displayed.

Step 14

On the **Policy settings** page, click the **Requires users to apply a label to their email or documents** checkbox.

Click **Next**.



Policy settir

You can choose to have a de
users to justify actions on th

Apply this label by default t

None

□ Users must provide justi
classification label

☑ Requires users to apply

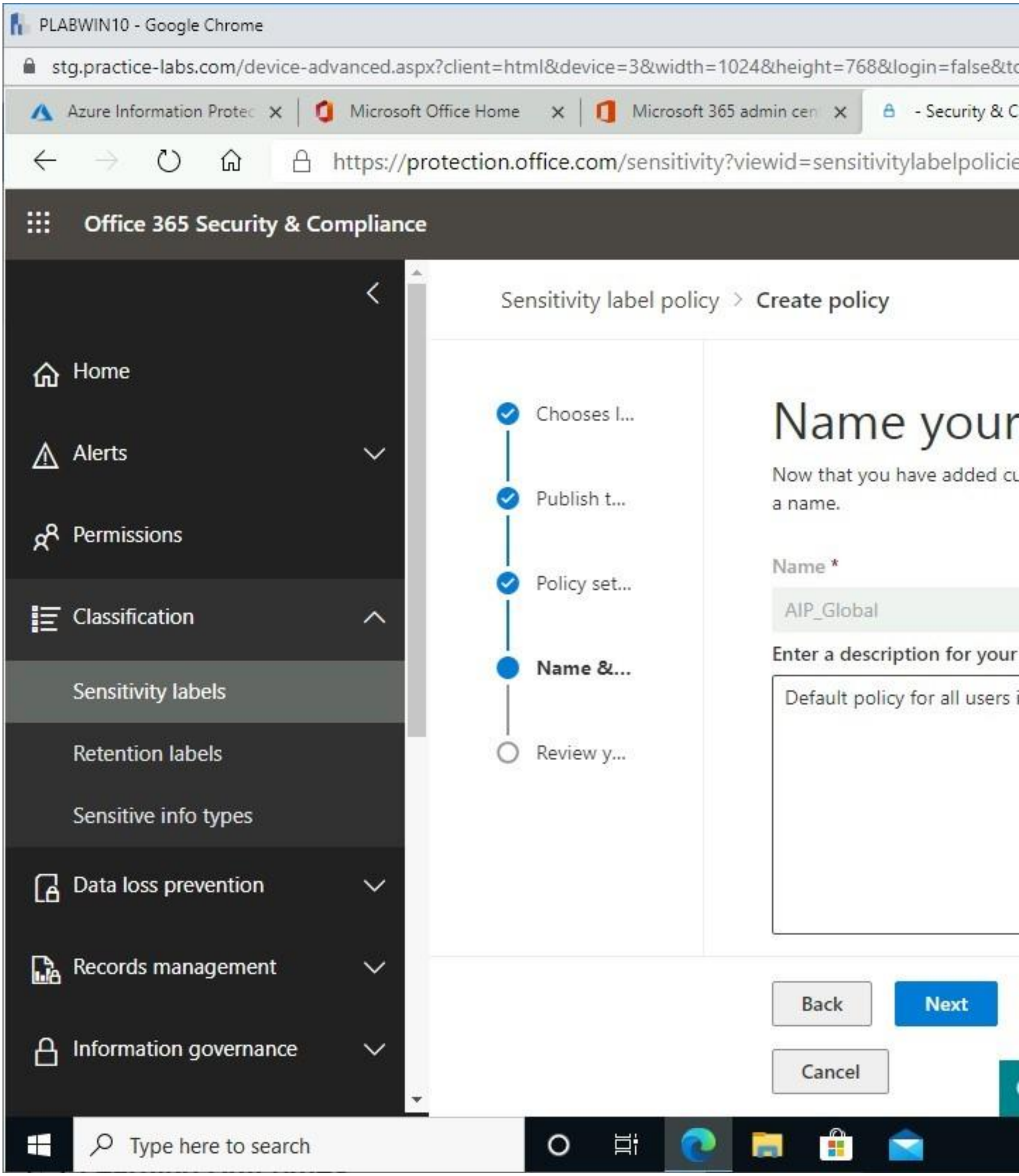
□ Provide users with a link

Figure 2.71 Screenshot of PLABWIN10 desktop: Policy settings tab on the

Office 365 Security & Compliance - Sensitivity label policy > Create policy screen is displayed with the required option enabled and the Next button selected.

Step 15

Select **Next** in the **Name your policy** page.



Name your

Now that you have added cu
a name.

Name *

AIP_Global

Enter a description for your

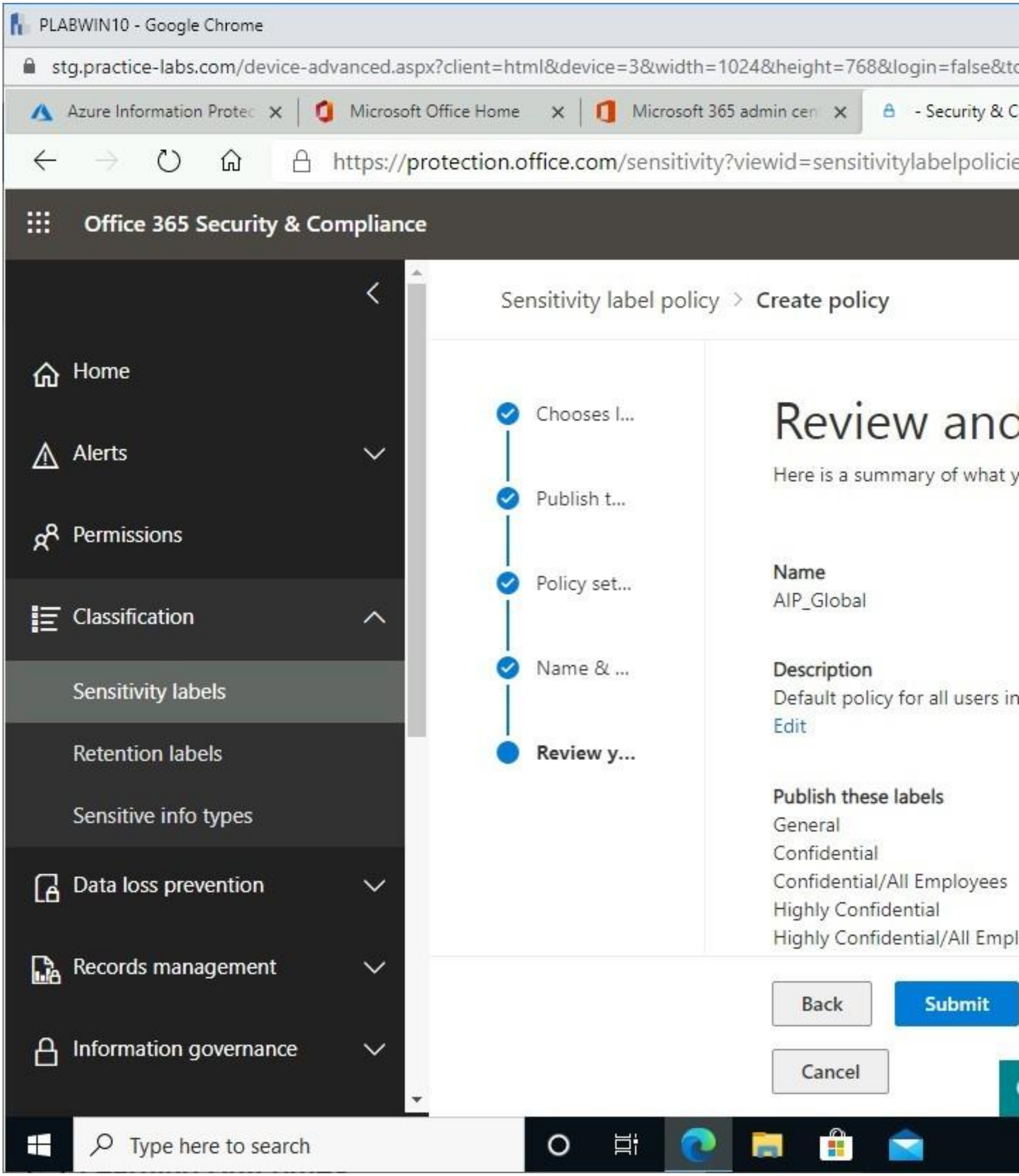
Default policy for all users i

Figure 2.72 Screenshot of PLABWIN10 desktop: Name your policy tab on

the Office 365 Security & Compliance - Sensitivity label policy > Create policy screen is displayed showing default settings and showing the Next button selected.

Step 16

From **Review and finish** page, click **Submit**.



Review anc

Here is a summary of what y

Name
AIP_Global

Description
Default policy for all users in
Edit

Publish these labels
General
Confidential
Confidential/All Employees
Highly Confidential
Highly Confidential/All Empl

Figure 2.73 Screenshot of PLABWIN10 desktop: Review and finish tab on

the Office 365 Security & Compliance - Sensitivity label policy > Create policy screen is displayed listing the settings performed and showing the Submit button selected.

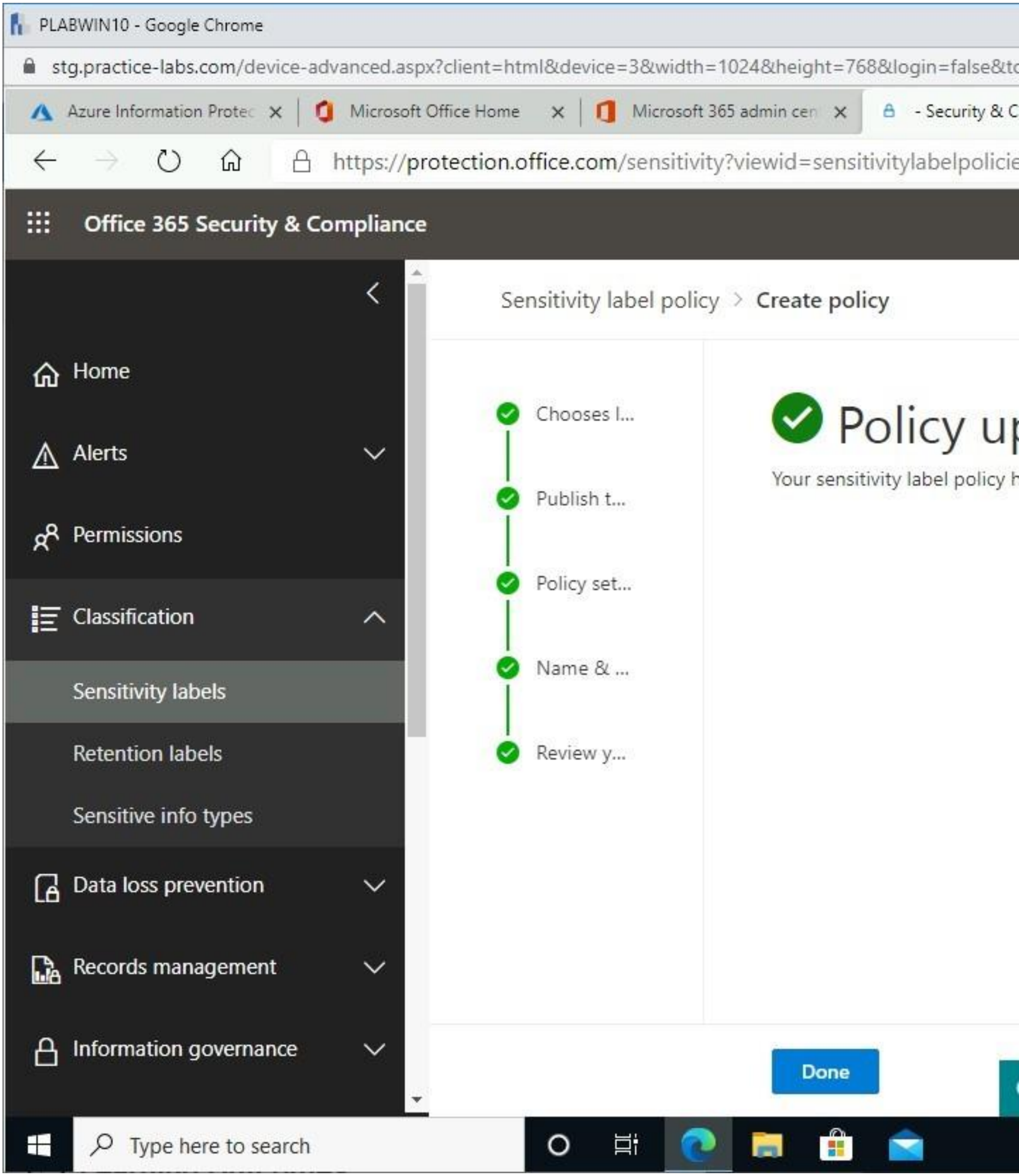
Step 17

Please wait while Office 365 publishes the policy.

You will get a successful confirmation when the publication completes.

Click **Done**.

Then minimize **Microsoft Edge**.



Policy up

Your sensitivity label policy h

Figure 2.74 Screenshot of PLABWIN10 desktop: Policy updated message is

displayed on the Office 365 Security & Compliance - Sensitivity label policy > Create policy screen.

Task 6 - Install Azure Information Protection Client Unified Labeling

Azure Information Protection (classic) client uses the labels published in Microsoft Azure, while Azure Information Protection Unified Labeling (UL) client uses the labels published in Office 365 Security & Compliance. Unified labeling will be the new method for managing labels in Azure Information Protection starting March 2021.

To support this transition, you can copy labels created in Microsoft Azure to Office 365 Security& Compliance. This was illustrated in an earlier activity in this exercise.

In this task, you will install AIP-UL to make published labels available to users' Office apps.

Step 1

Ensure you are connected to **PLABWIN10**. Click **File Explorer** on the taskbar.

In the **File Explorer** window, expand **This PC > Local Disk (C:)** drive and click the **AIP** folder.

From the details pane, right-click **AzInfoProtection_UL** and select **Run as administrator**.

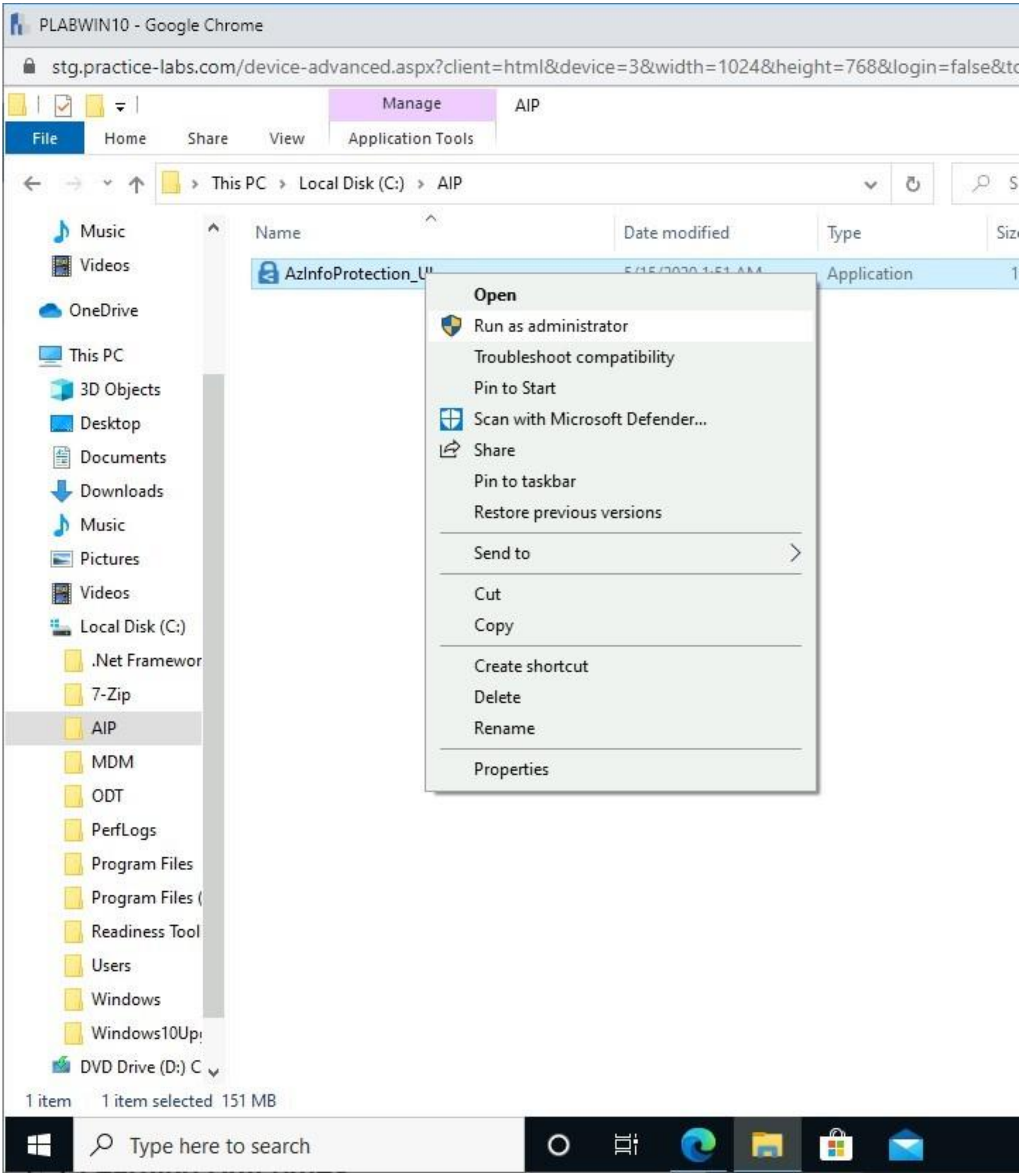
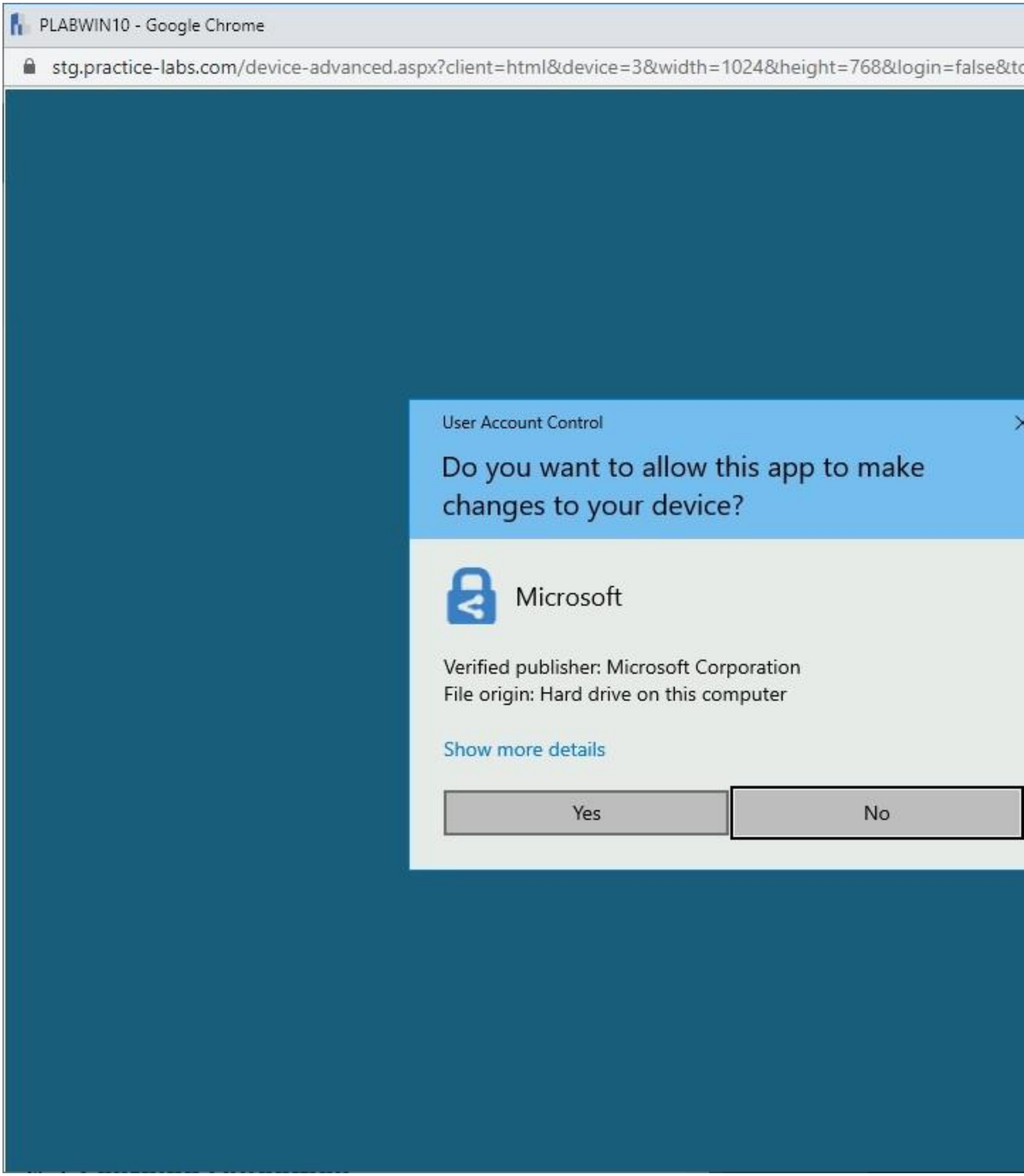


Figure 2.75 Screenshot of PLABWIN10 desktop: Context menu (that

appears on right-clicking a listed app) > Run as administrator menu-options are selected on the file explorer window.

Step 2

Click **Yes** in the **User Account Control** message box.



PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc

User Account Control

Do you want to allow this app to make changes to your device?

Microsoft

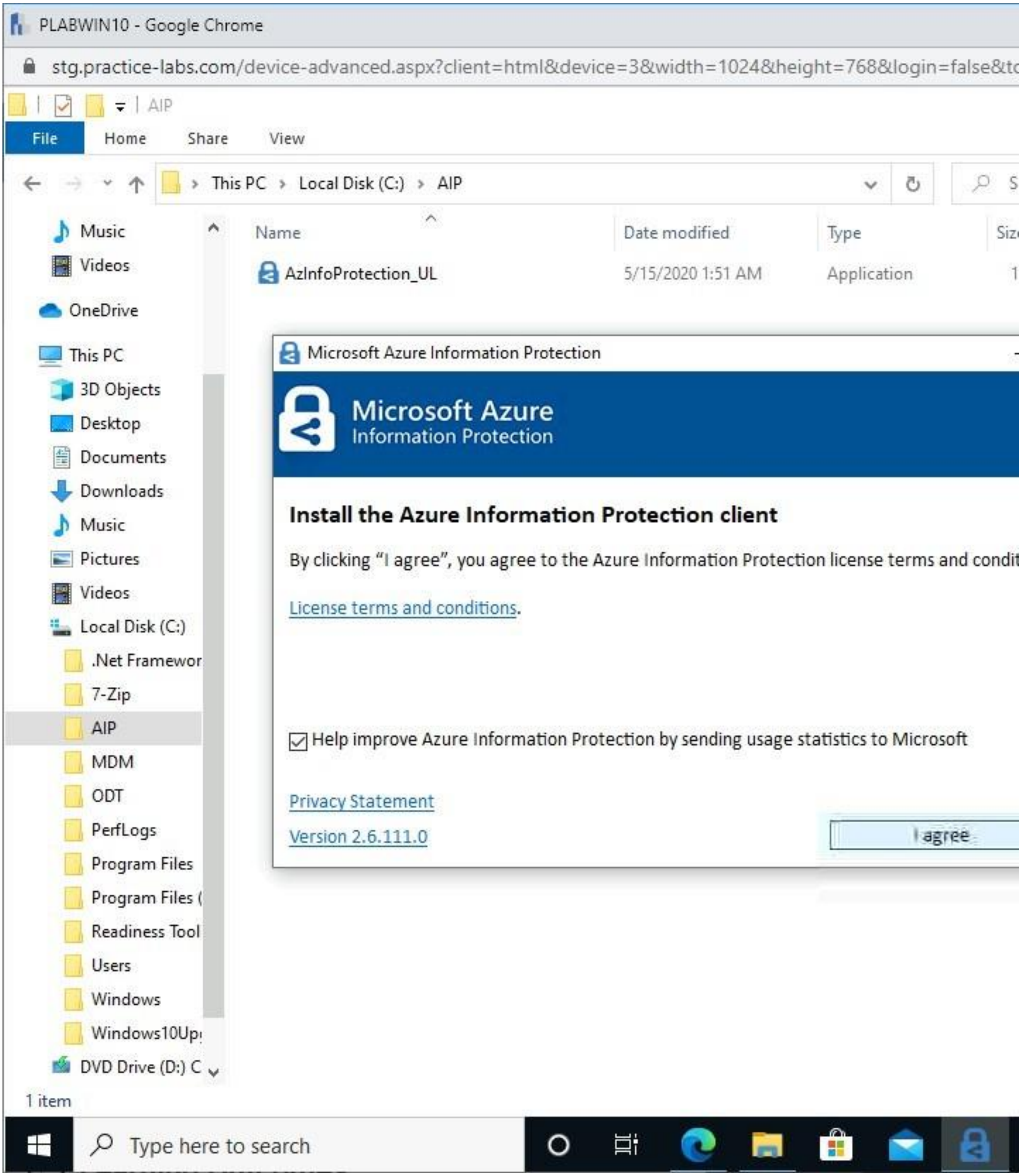
Verified publisher: Microsoft Corporation
File origin: Hard drive on this computer

Figure 2.76 Screenshot of PLABWIN10 desktop: User Account Control

dialog box is displayed prompting for confirmation to allow the app to make changes to the device and showing the Yes button highlighted.

Step 3

Click **I agree** in the **Install the Azure Information Protection client** message box.



Install the Azure Information Protection client

By clicking “I agree”, you agree to the Azure Information Protection license terms and condit

License terms and conditions.

☑ Help improve Azure Information Protection by sending usage statistics to Microsoft

Privacy Statement

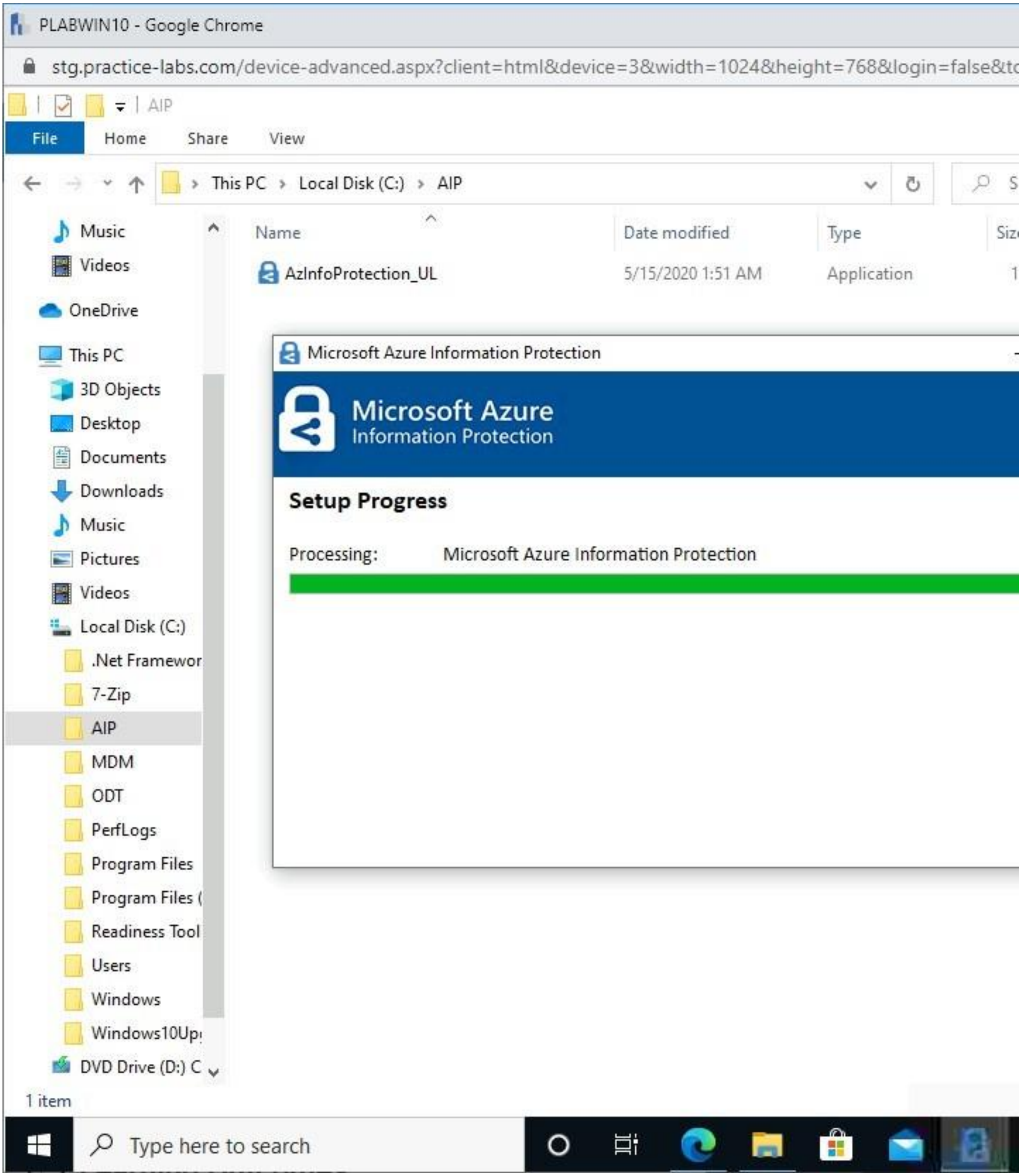
Version 2.6.111.0

Figure 2.77 Screenshot of PLABWIN10 desktop: Install the client page on

the Microsoft Azure Information Protection wizard is displayed showing default settings, and the I agree button highlighted.

Step 4

Please wait while the installation is in progress.



Microsoft Azure Information Protection

Microsoft Azure
Information Protection

Setup Progress

Processing: Microsoft Azure Information Protection

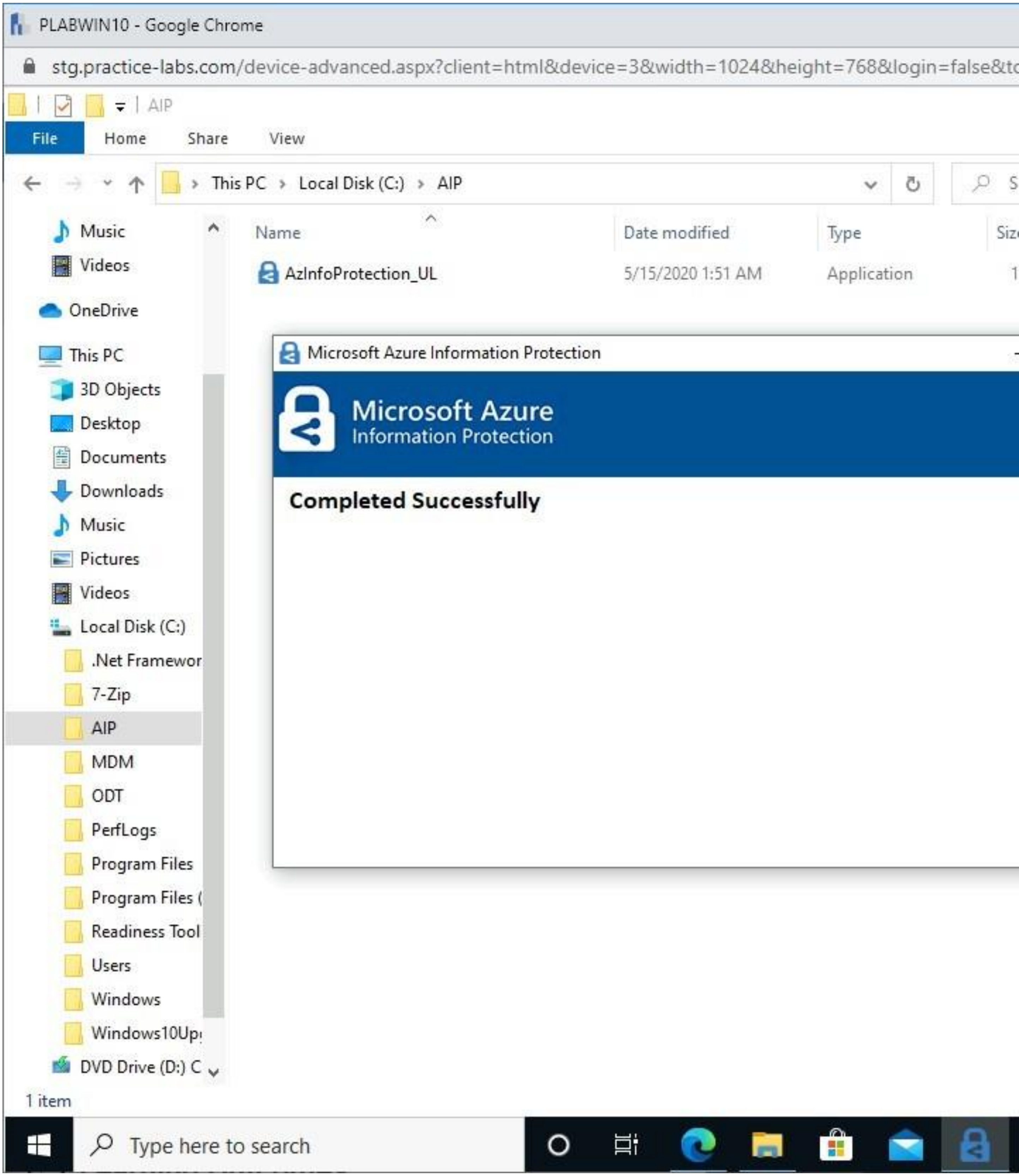
Figure 2.78 Screenshot of PLABWIN10 desktop: Setup Progress page on

the Microsoft Azure Information Protection wizard is displayed showing progress bar on the installation of the client.

Step 5

Click **Close** when **Microsoft Azure Information Protection** successfully installs.

Close **File Explorer** window as well.



Name	Date modified	Type	Siz
AzInfoProtection_UL	5/15/2020 1:51 AM	Application	1

Microsoft Azure Information Protection

Microsoft Azure
Information Protection

Completed Successfully

Figure 2.79 Screenshot of PLABWIN10 desktop: Completed Successfully

page on the Microsoft Azure Information Protection wizard is displayed showing the Close button highlighted.

Task 7 - Enable Remote Desktop

Regular user accounts must be able to connect to Practice Labs devices with Remote Desktop protocol.

In this task, you will enable Remote Desktop for all users in the **PLABWIN10** so that you can test the Azure Information Protection unified labeling client.

Step 1

Ensure you are connected to **PLABWIN10**.

Click the **File Explorer** icon on the taskbar.

Right-click **This PC** and select **Properties.**

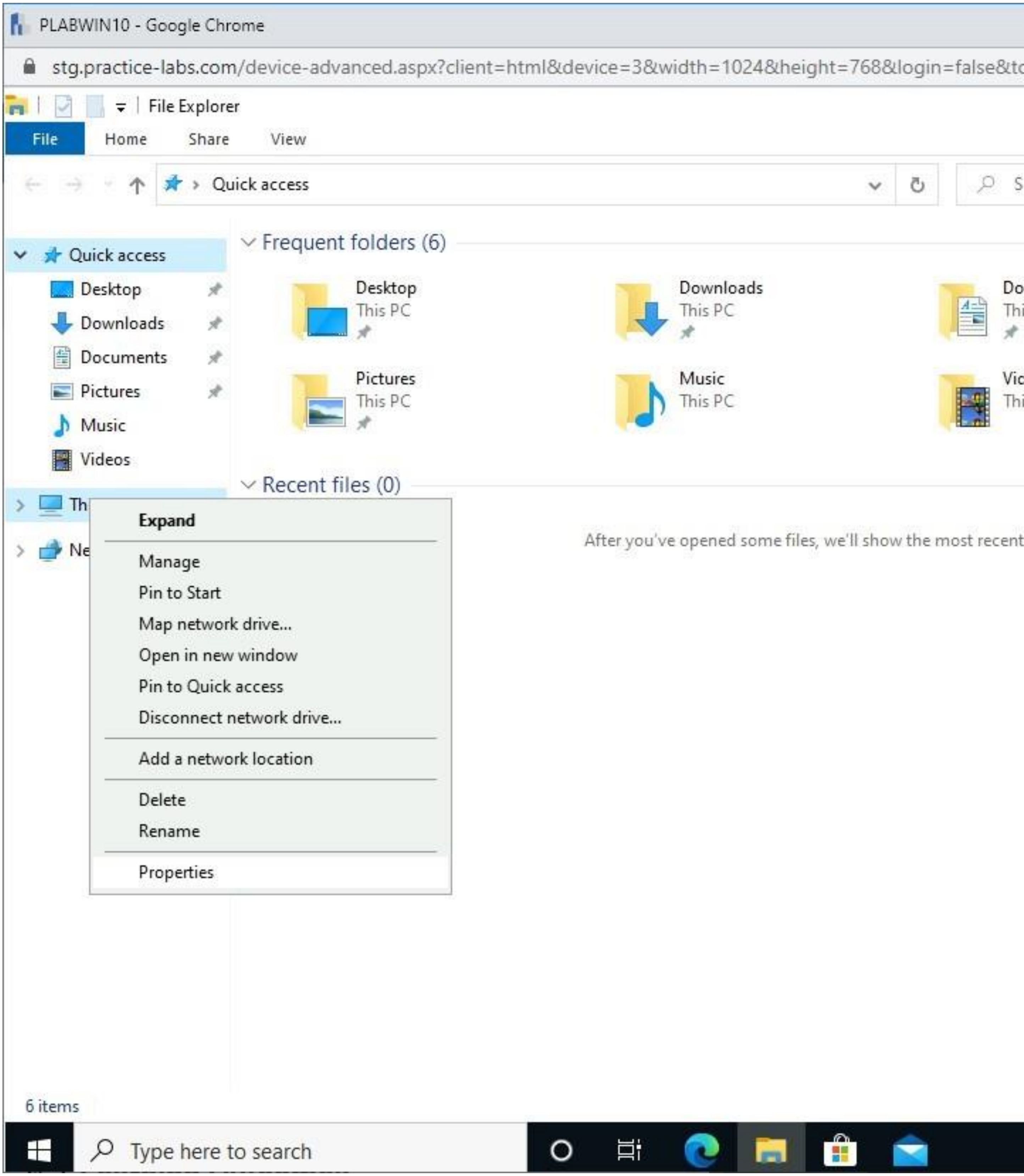
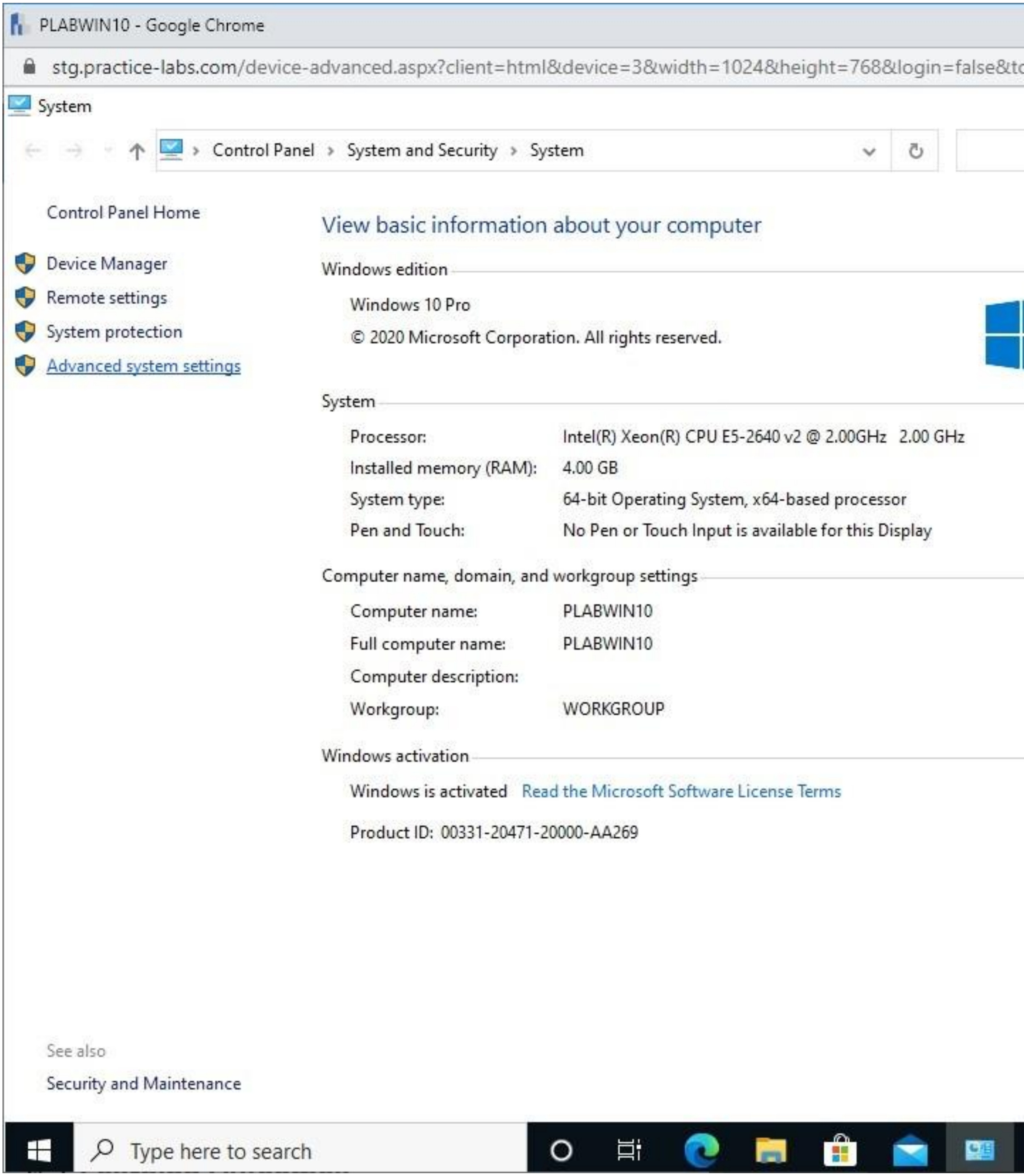


Figure 2.80 Screenshot of PLABWIN10 desktop: Context menu (that

appears on right-clicking the This PC node) > Properties menu-options are selected on the File Explorer window.

Step 2

Select **Advanced system settings.**


PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&t
System
Control Panel › System and Security › System
Control Panel Home
Device Manager
Remote settings
System protection
Advanced system settings
See also
Security and Maintenance
Type here to search

View basic information about your computer

Windows edition

Windows 10 Pro

© 2020 Microsoft Corporation. All rights reserved.

System

Processor:	Intel(R) Xeon(R) CPU E5-2640 v2 @ 2.00GHz 2.00 GHz
Installed memory (RAM):	4.00 GB
System type:	64-bit Operating System, x64-based processor
Pen and Touch:	No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name:	PLABWIN10
Full computer name:	PLABWIN10
Computer description:	
Workgroup:	WORKGROUP

Windows activation

Windows is activated Read the Microsoft Software License Terms

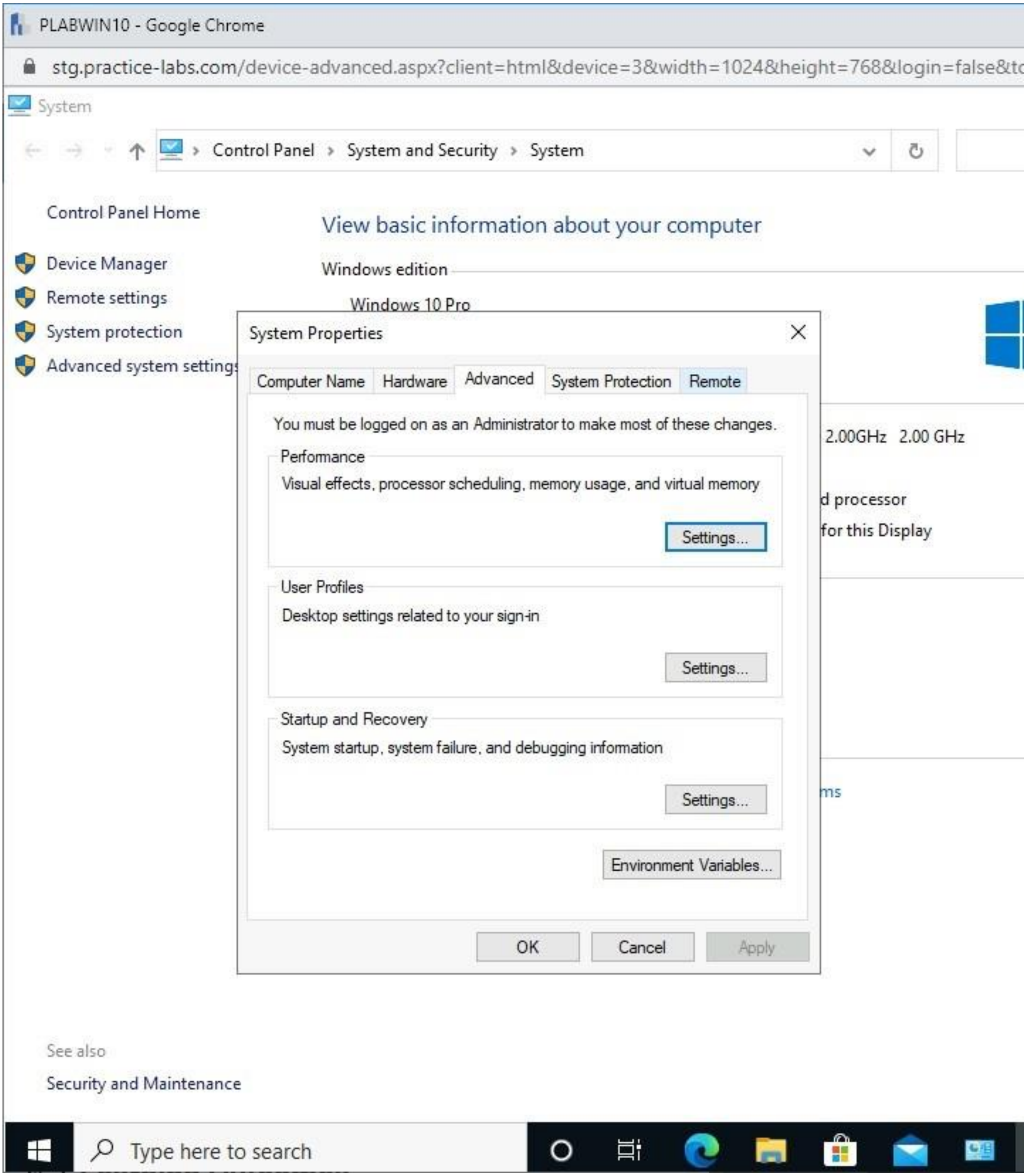
Product ID: 00331-20471-20000-AA269

Figure 2.81 Screenshot of PLABWIN10 desktop: Advanced system settings

link on the navigation pane at the left on the System screen is highlighted.

Step 3

On the **System Properties** dialog box, click the **Remote** tab.



System Properties

Computer Name | Hardware | Advanced | System Protection | Remote

You must be logged on as an Administrator to make most of these changes.

Performance

Visual effects, processor scheduling, memory usage, and virtual memory

Settings...

User Profiles

Desktop settings related to your sign-in

Settings...

Startup and Recovery

System startup, system failure, and debugging information

Settings...

Environment Variables...

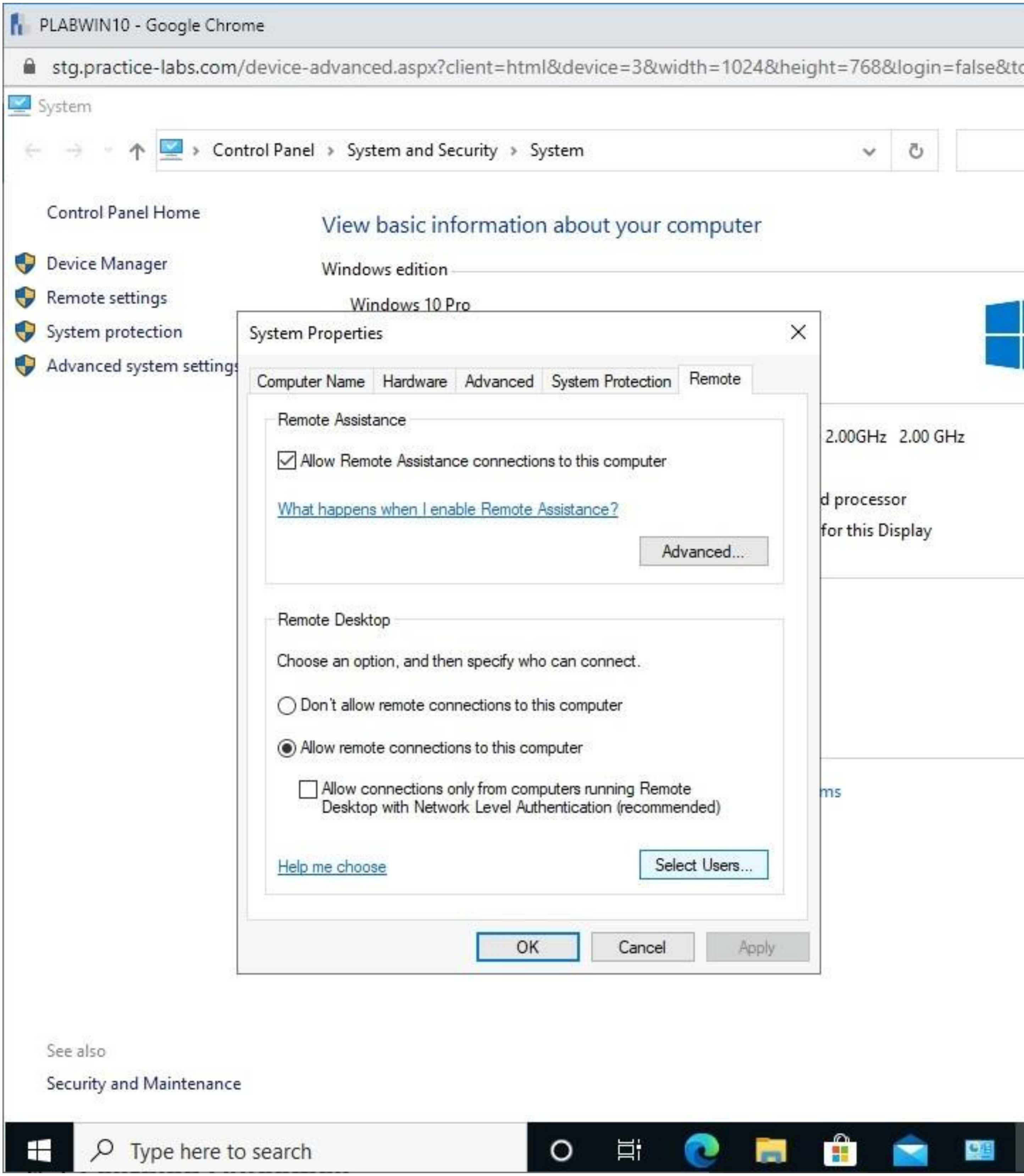
OK | Cancel | Apply

Figure 2.82 Screenshot of PLABWIN10 desktop: Remote tab on the System

Properties dialog box is highlighted.

Step 4

Under **Remote Desktop**, click **Select Users**.



PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc

System

Control Panel › System and Security › System

Control Panel Home

Device Manager

Remote settings

System protection

Advanced system settings

View basic information about your computer

Windows edition

Windows 10 Pro

2.00GHz 2.00 GHz

d processor

for this Display

ms

See also

Security and Maintenance

System Properties

Computer Name | Hardware | Advanced | System Protection | Remote

Remote Assistance

☑ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Advanced...

Remote Desktop

Choose an option, and then specify who can connect.

○ Don't allow remote connections to this computer

● Allow remote connections to this computer

□ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

Help me choose

Select Users...

OK | Cancel | Apply

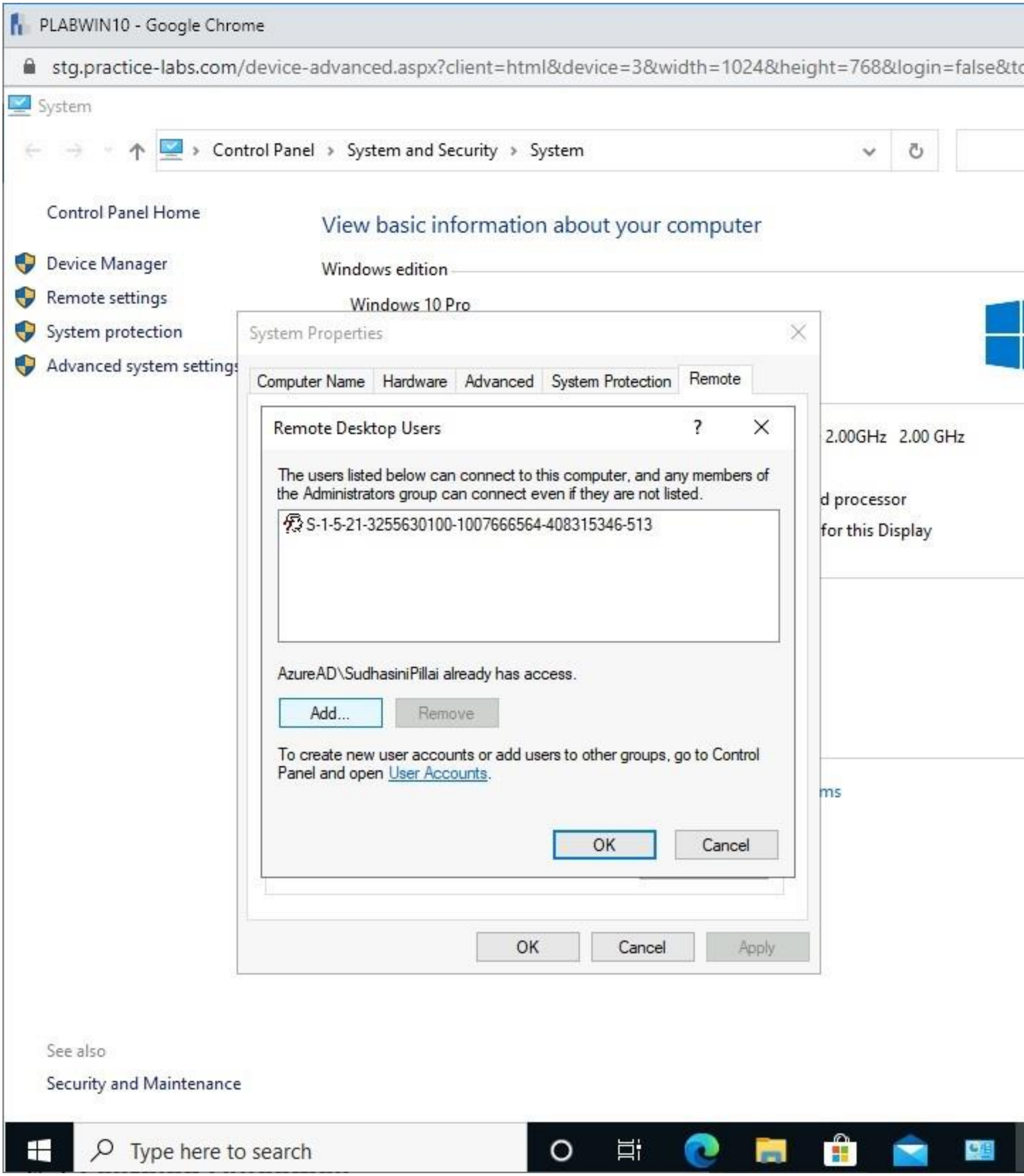
Type here to search

Figure 2.83 Screenshot of PLABWIN10 desktop: Remote tab on the System

Properties dialog box is displayed showing default settings and the Select Users button highlighted.

Step 5

On the **Remote Desktop Users** dialog box, click **Add**.



Remote Desktop Users

The users listed below can connect to this computer, and any members of the Administrators group can connect even if they are not listed.

S-1-5-21-3255630100-1007666564-408315346-513

AzureAD\SudhasiniPillai already has access.

To create new user accounts or add users to other groups, go to Control Panel and open User Accounts.

Figure 2.84 Screenshot of PLABWIN10 desktop: Remote Desktop Users

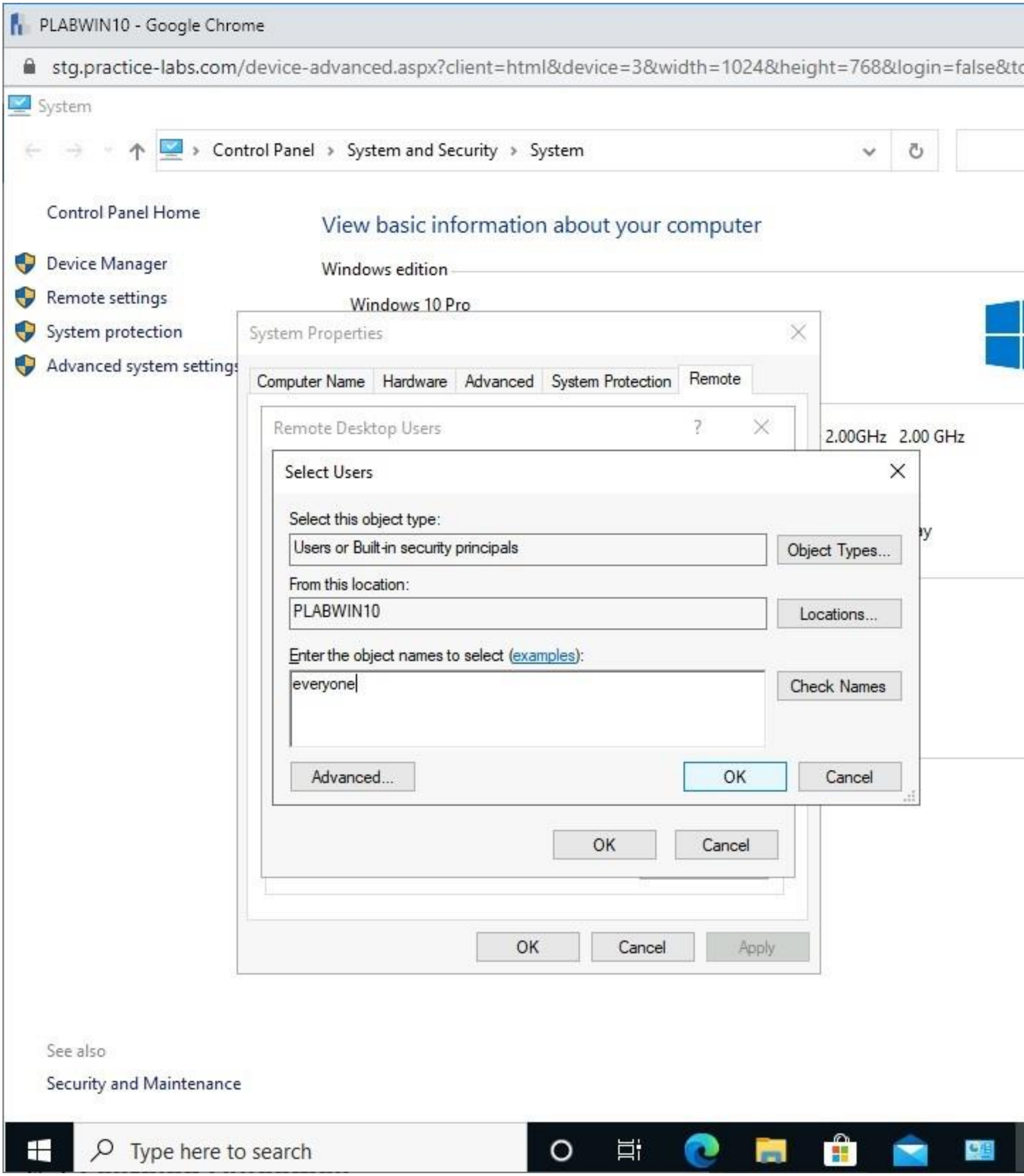
dialog box is displayed showing the Add button highlighted.

Step 6

From the **Select Users** dialog box, click in the **Enter the object names to select** text box and enter:

```
everyone
```

Click **OK**.



Select Users

Select this object type:
Users or Built-in security principals
Object Types...

From this location:
PLABWIN10
Locations...

Enter the object names to select (examples):
everyone
Check Names

Advanced...
OK
Cancel

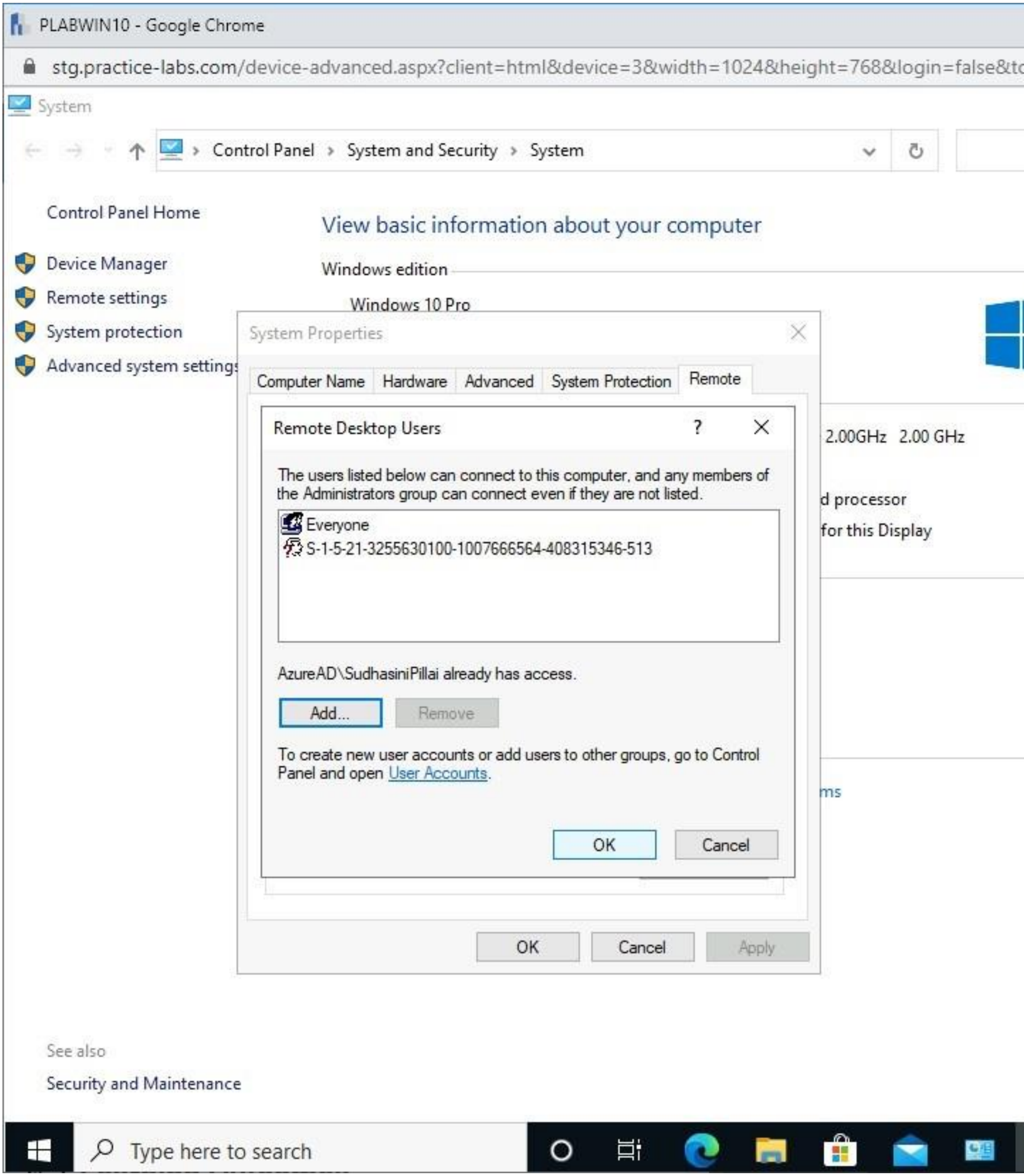
Figure 2.85 Screenshot of PLABWIN10 desktop: Select Users dialog box is

displayed showing the required object name typed-in and the OK button highlighted.

Step 7

Click **OK** on the **Remote Desktop Users** dialog box.

Similarly, select **OK** on the **System Properties** then close **File Explorer**.



The users listed below can connect to this computer, and any members of the Administrators group can connect even if they are not listed.

Everyone
S-1-5-21-3255630100-1007666564-408315346-513

AzureAD\SudhasiniPillai already has access.

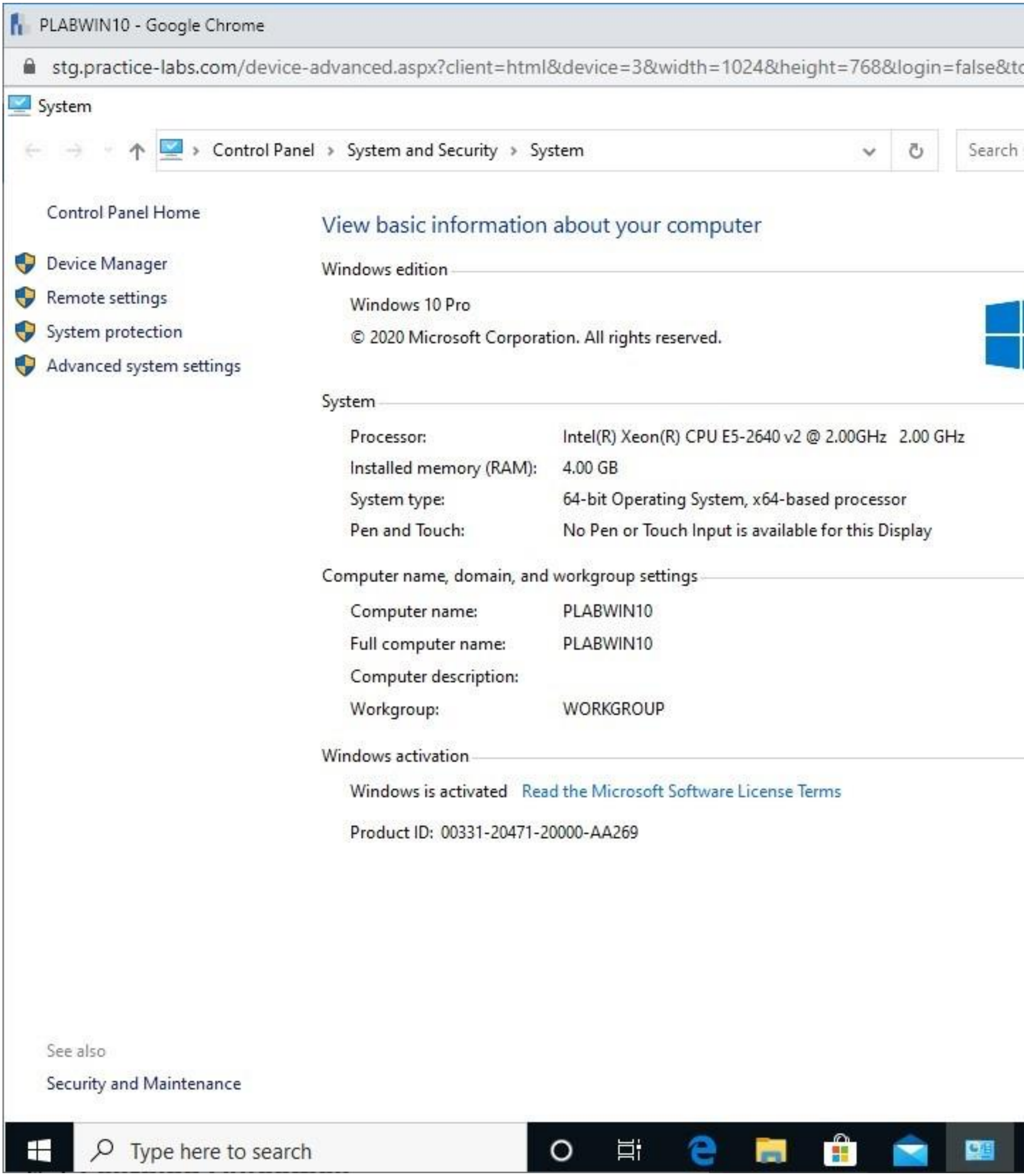
To create new user accounts or add users to other groups, go to Control Panel and open User Accounts.

Figure 2.86 Screenshot of PLABWIN10 desktop: Remote Desktop Users

dialog box is displayed showing the required settings performed and the OK button highlighted.

Step 8

Close **System** and **File Explorer** windows.


PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc
System
Control Panel › System and Security › System
Search
Control Panel Home
Device Manager
Remote settings
System protection
Advanced system settings
See also
Security and Maintenance
Type here to search

View basic information about your computer

Windows edition

Windows 10 Pro

© 2020 Microsoft Corporation. All rights reserved.

System

Processor: Intel(R) Xeon(R) CPU E5-2640 v2 @ 2.00GHz 2.00 GHz

Installed memory (RAM): 4.00 GB

System type: 64-bit Operating System, x64-based processor

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: PLABWIN10

Full computer name: PLABWIN10

Computer description:

Workgroup: WORKGROUP

Windows activation

Windows is activated Read the Microsoft Software License Terms

Product ID: 00331-20471-20000-AA269

Figure 2.87 Screenshot of PLABWIN10 desktop: Close icon at the top-right

corner of the System window is highlighted.

Step 9

Right-click **Start**, point to **Shut down or sign out** and select **Sign out**.

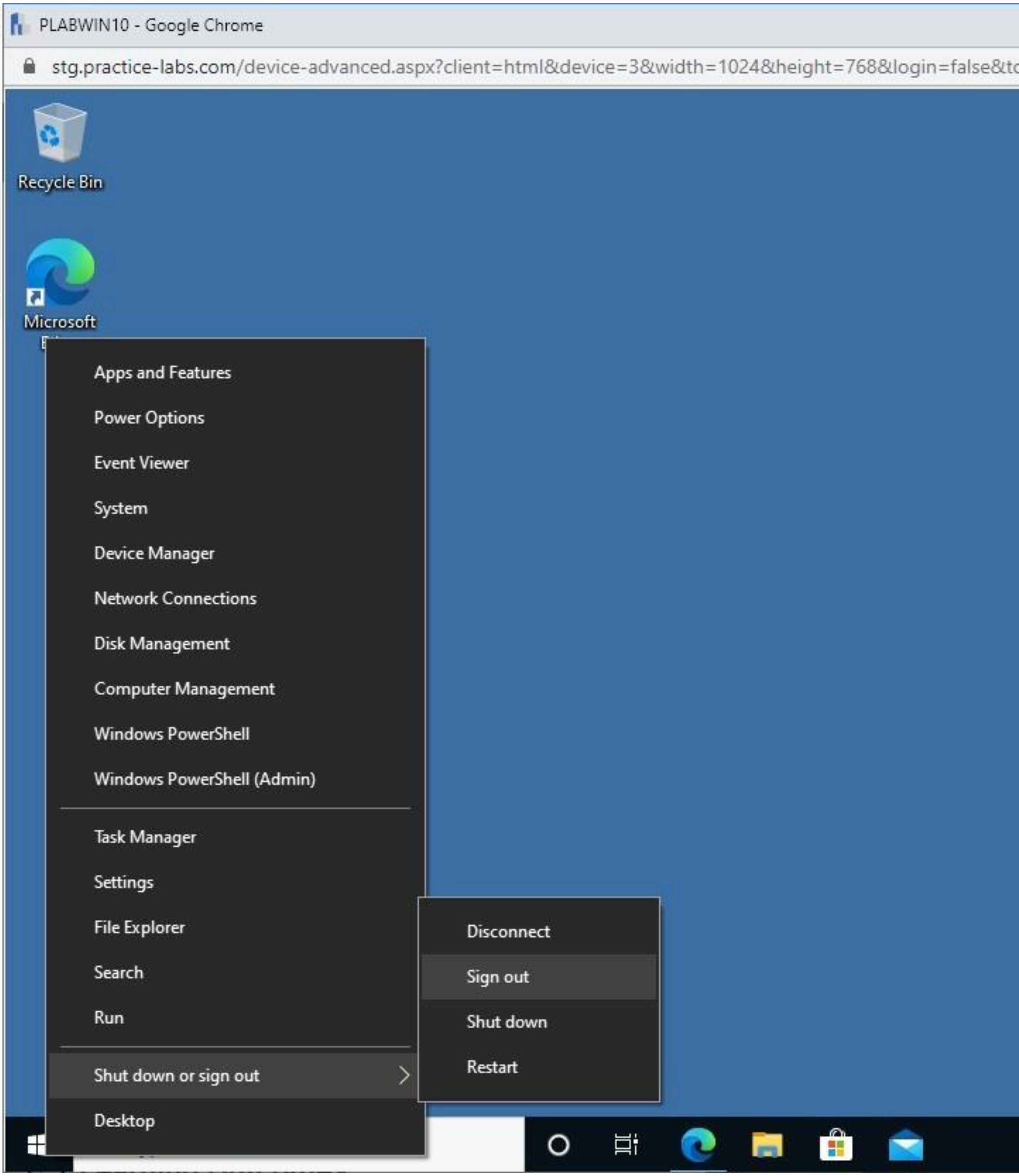


Figure 2.88 Screenshot of PLABWIN10 desktop: Context menu (that

appears on right-clicking the Start charm) > Shut down or sign out > Sign out menu-options are selected.

Task 8 - Configure Proxy Server Settings for a New User

Devices in Practice Labs connect to a proxy server to access the Internet. You need to configure a device to connect to a proxy server if a new user signs in to a Windows computer. Connection to the Internet is essential to ensure that **PLABWIN10** synchronizes with Azure and Office 365 policies and settings.

For this task, you will sign-in as a regular Azure AD user and enable connection to a proxy server.

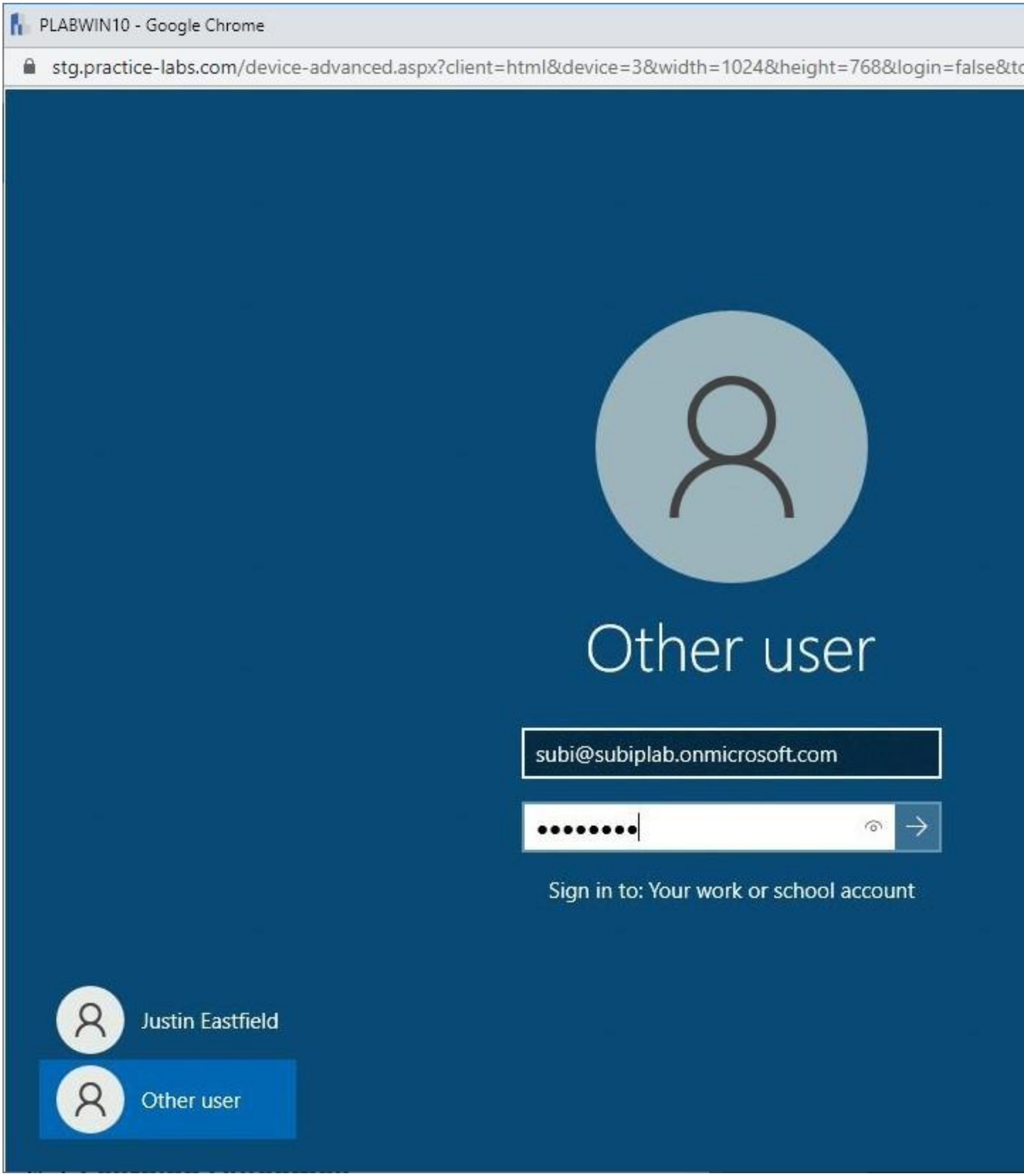
Step 1

Connect to **PLABWIN10**.

Click **Other user**.

Type the username and password of the account with a global administrator role in the Azure tenant.

Press **Enter**.



PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc

Other user

subi@subiplab.onmicrosoft.com

•••••••••

Sign in to: Your work or school account

Figure 2.89 Screenshot of PLABWIN10 desktop: Required login credentials

are typed into the Other user login screen.

Step 2

Please wait while the user desktop environment continues to initialize.

Click **Agree** in the **BGInfo License Agreement** dialog box.

On the **Application Install - Security Warning** message box, click **Install**.

Right-click the network icon on the system tray and select **Open Network & Internet Settings**.

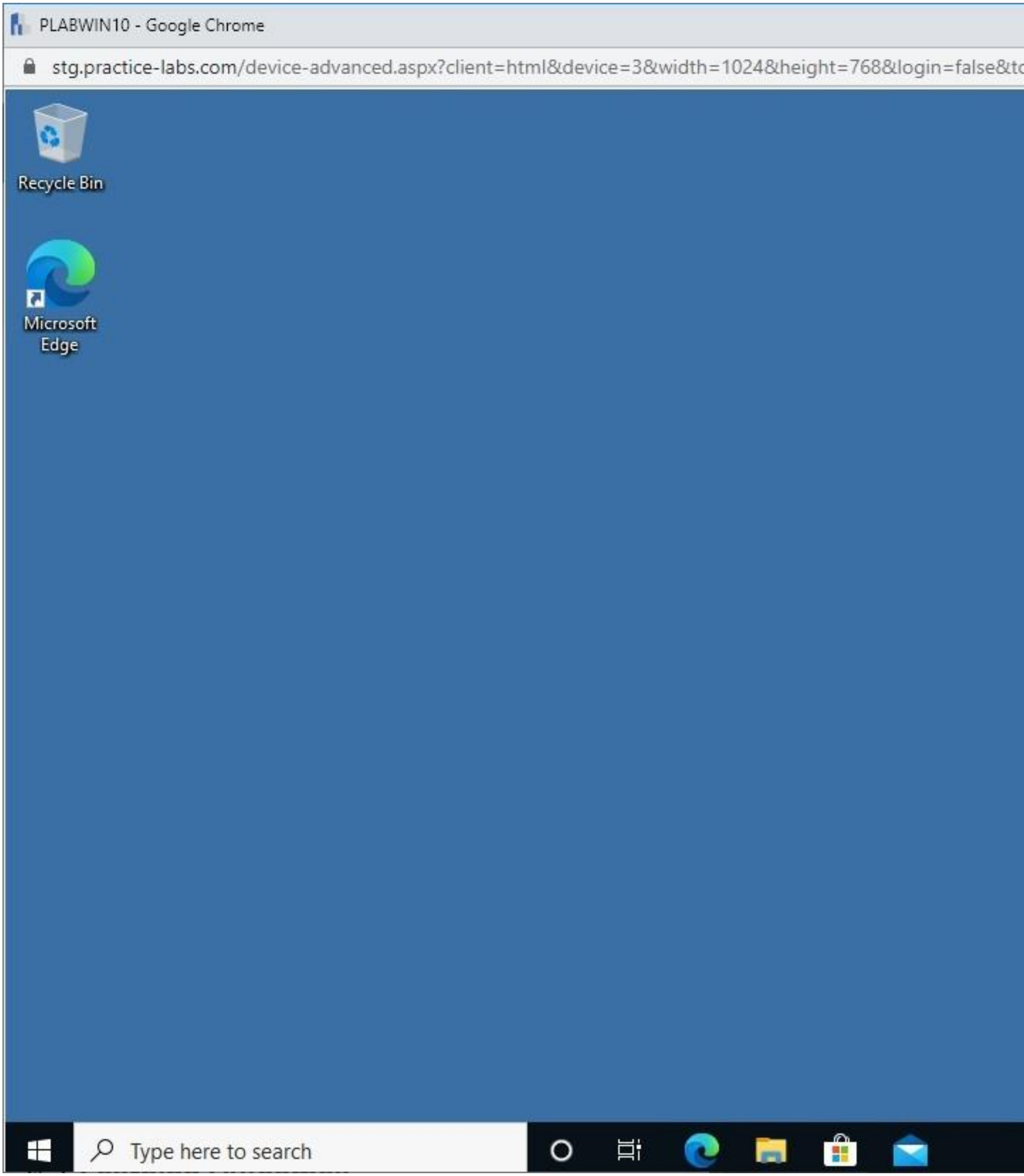
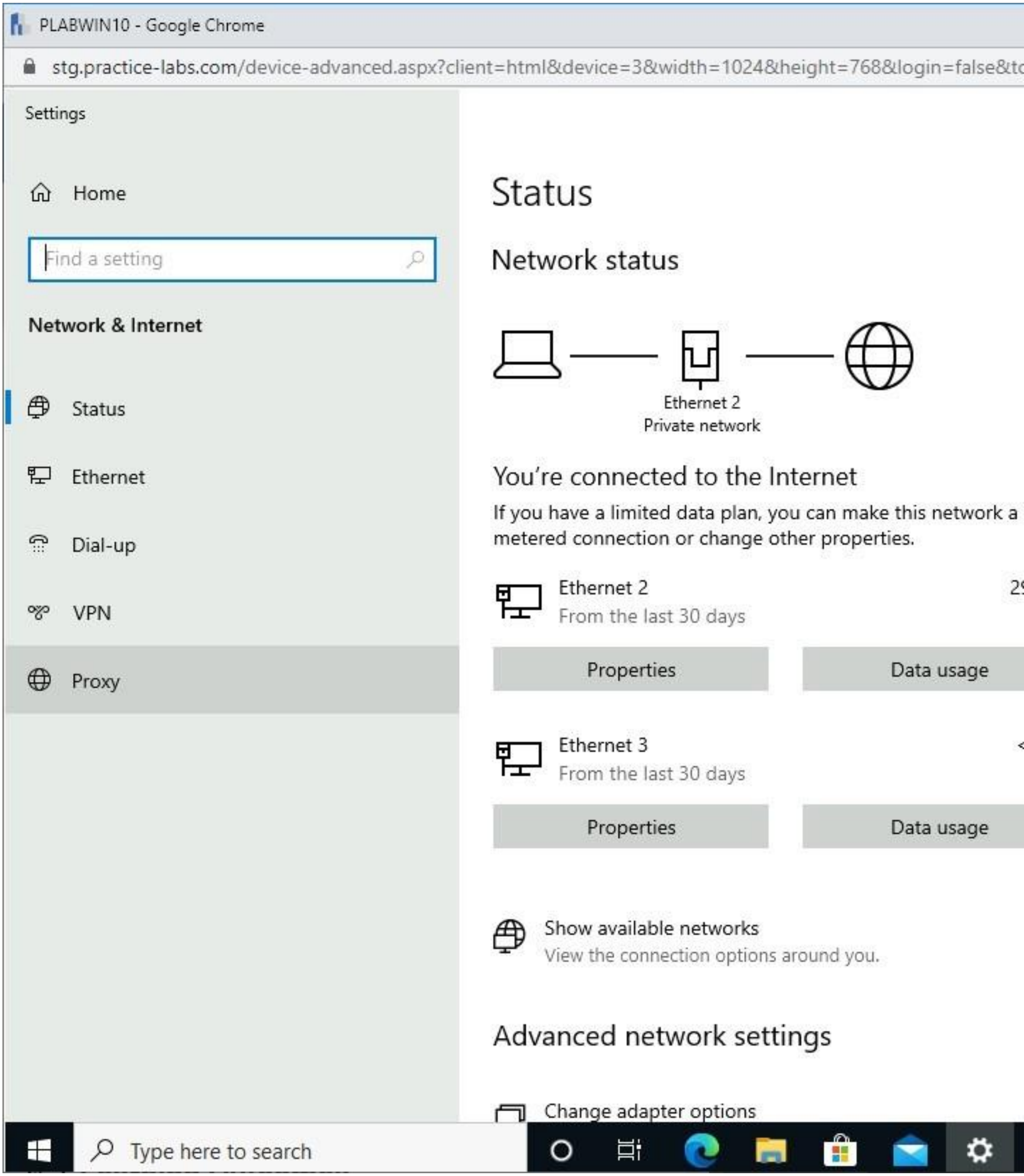

PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc
Recycle Bin
Microsoft Edge
Type here to search

Figure 2.90 Screenshot of PLABWIN10 desktop: Context menu (that

appears on right-clicking the network icon) > Open Network & Internet settings menu-options are selected.

Step 3

On the **Settings** page, click **Proxy** from the left pane.



PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&to

Settings

Status

Network status

You're connected to the Internet

If you have a limited data plan, you can make this network a metered connection or change other properties.

Ethernet 2
From the last 30 days

Ethernet 3
From the last 30 days

Show available networks
View the connection options around you.

Advanced network settings

Figure 2.91 Screenshot of PLABWIN10 desktop: Proxy option on the

navigation pane at the left on the Settings - Status screen is highlighted.

Step 4

Under the **Manual proxy setup** section, slide the **Use a proxy server** to **On**.

In the **Address** box, type:

```
http://proxy
```

In the **Port** box, type:

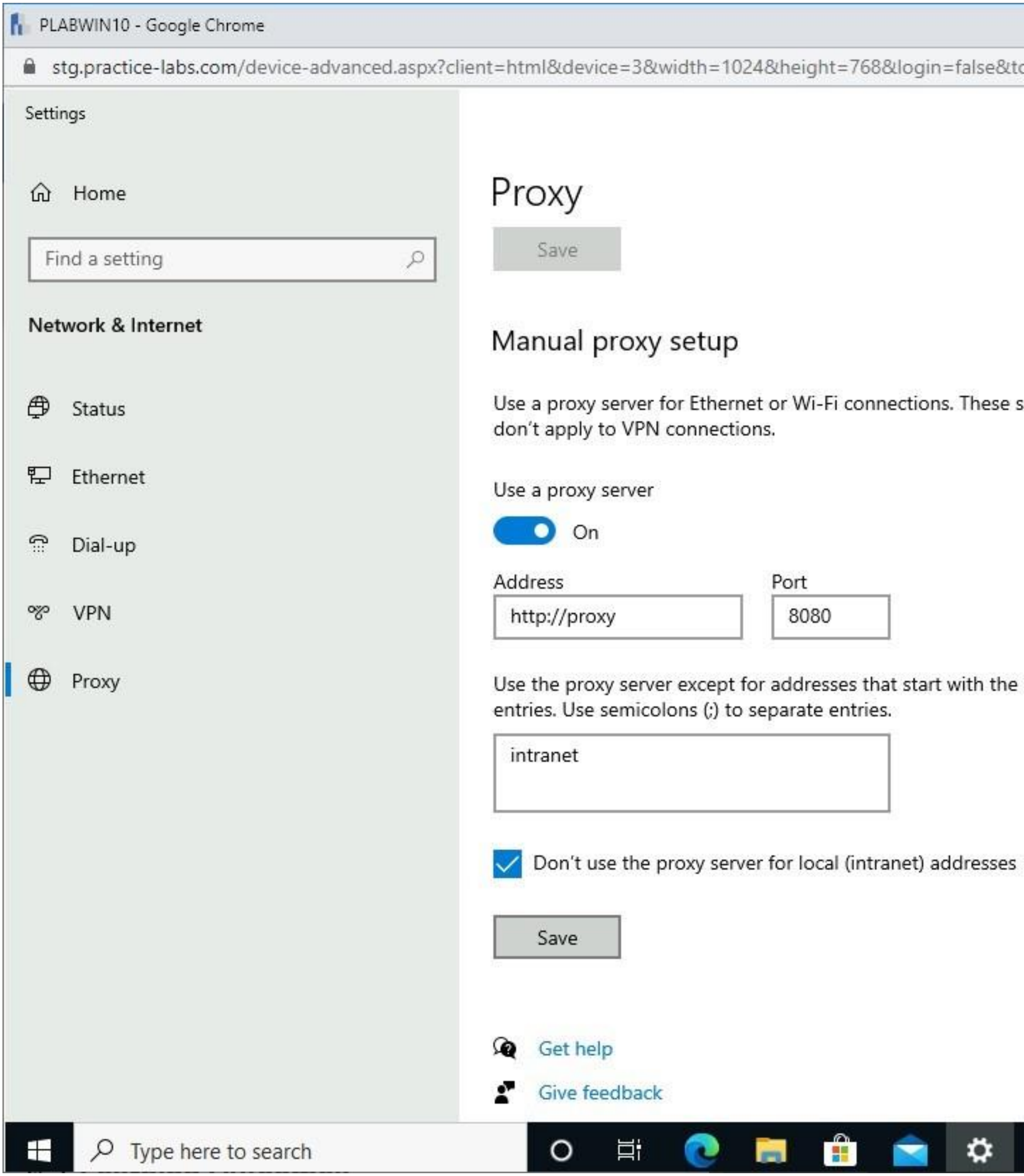
```
8080
```

Click in the **Use proxy server except**…. box, and type:

```
intranet
```

Enable **Don’t use the proxy server for local (intranet) address** box.

Click **Save**.


PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc
Settings
Home
Find a setting
Network & Internet
Status
Ethernet
Dial-up
VPN
Proxy
Save
Get help
Give feedback
Type here to search

Proxy

Manual proxy setup

Use a proxy server for Ethernet or Wi-Fi connections. These s
don't apply to VPN connections.

Use a proxy server

On

Address: http://proxy

Port: 8080

Use the proxy server except for addresses that start with the
entries. Use semicolons (;) to separate entries.

intranet

☑ Don't use the proxy server for local (intranet) addresses

Save

Figure 2.92 Screenshot of PLABWIN10 desktop: Settings - Proxy screen is

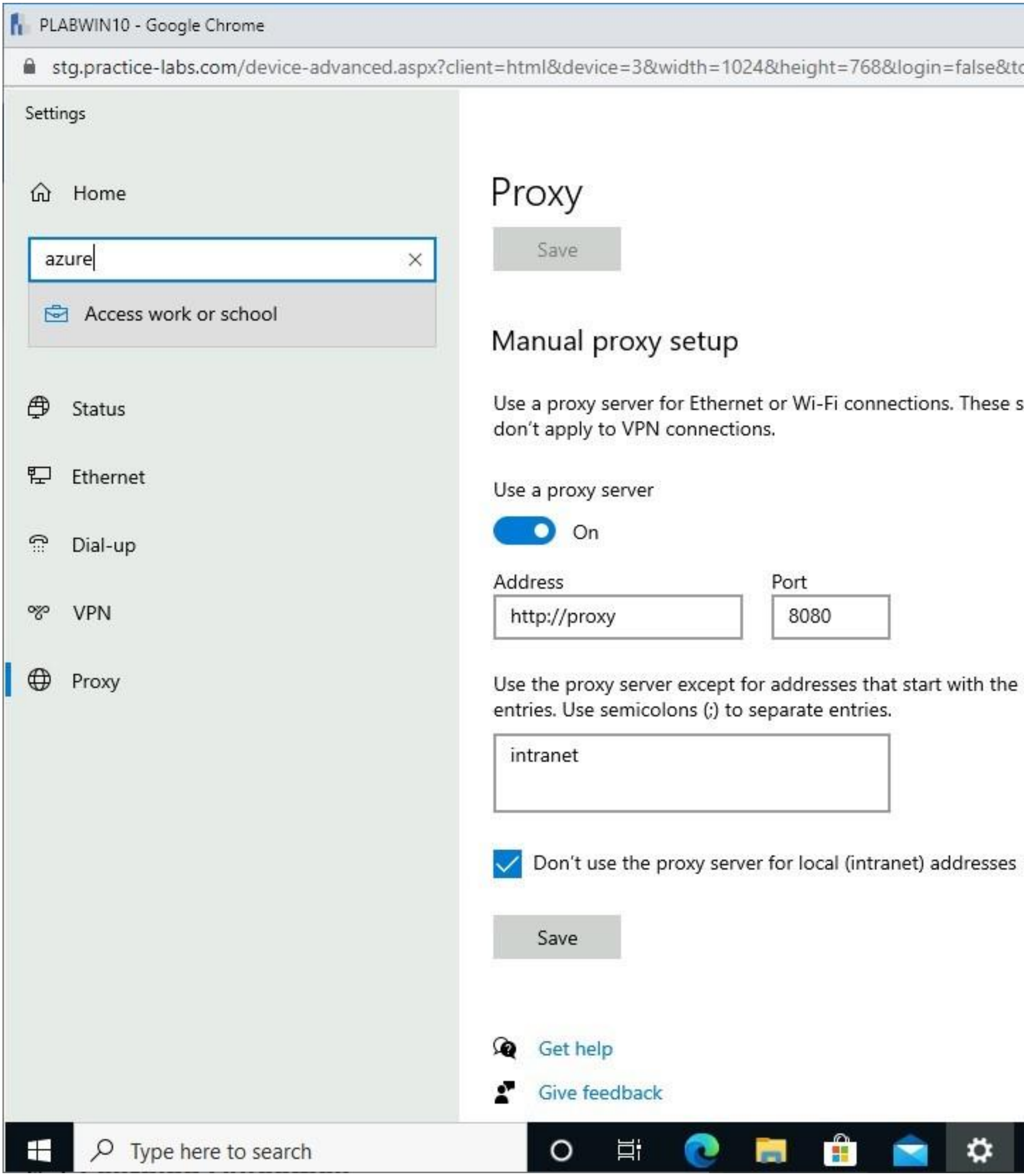
displayed showing the required settings performed and the Save button available.

Step 5

Click in the **Search** box on the left pane, and type:

```
azure
```

Select **Access work or school**.



PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc

Settings

Proxy

Manual proxy setup

Use a proxy server for Ethernet or Wi-Fi connections. These s
don't apply to VPN connections.

Use a proxy server

On

Address: http://proxy

Port: 8080

Use the proxy server except for addresses that start with the
entries. Use semicolons (;) to separate entries.

intranet

☑ Don't use the proxy server for local (intranet) addresses

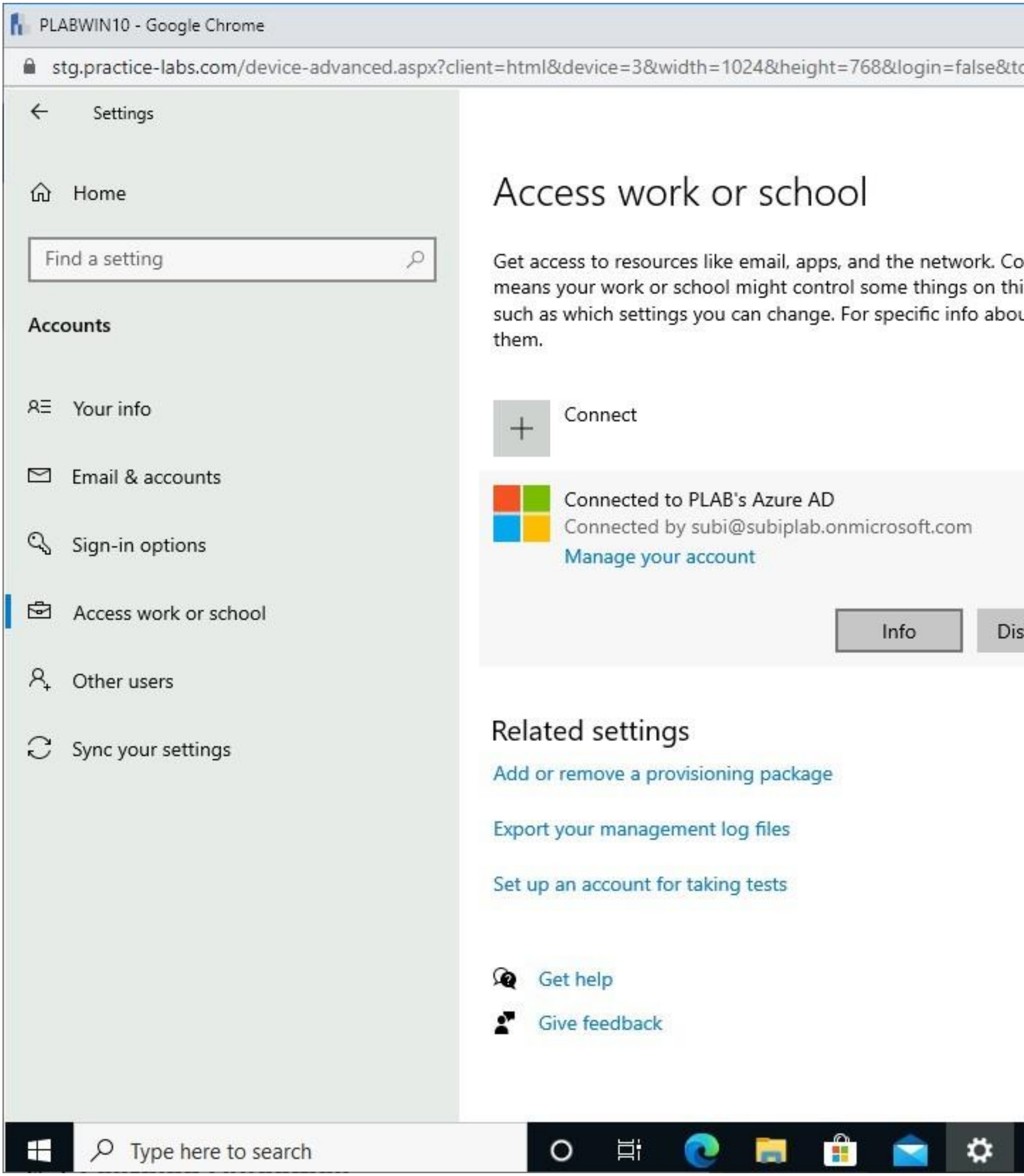
Figure 2.93 Screenshot of PLABWIN10 desktop: Access work or school

option on the search menu of the Settings -Proxy screen is highlighted.

Step 6

Under **Access work or school** section, click **Connected to <Organization Name> Azure AD.**

Click **Info**.



PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc

Access work or school

Get access to resources like email, apps, and the network. Co means your work or school might control some things on thi such as which settings you can change. For specific info abou them.

Connected to PLAB's Azure AD
Connected by subi@subiplab.onmicrosoft.com

Related settings

Add or remove a provisioning package
Export your management log files
Set up an account for taking tests
Get help
Give feedback
Type here to search

Figure 2.94 Screenshot of PLABWIN10 desktop: Info button on the

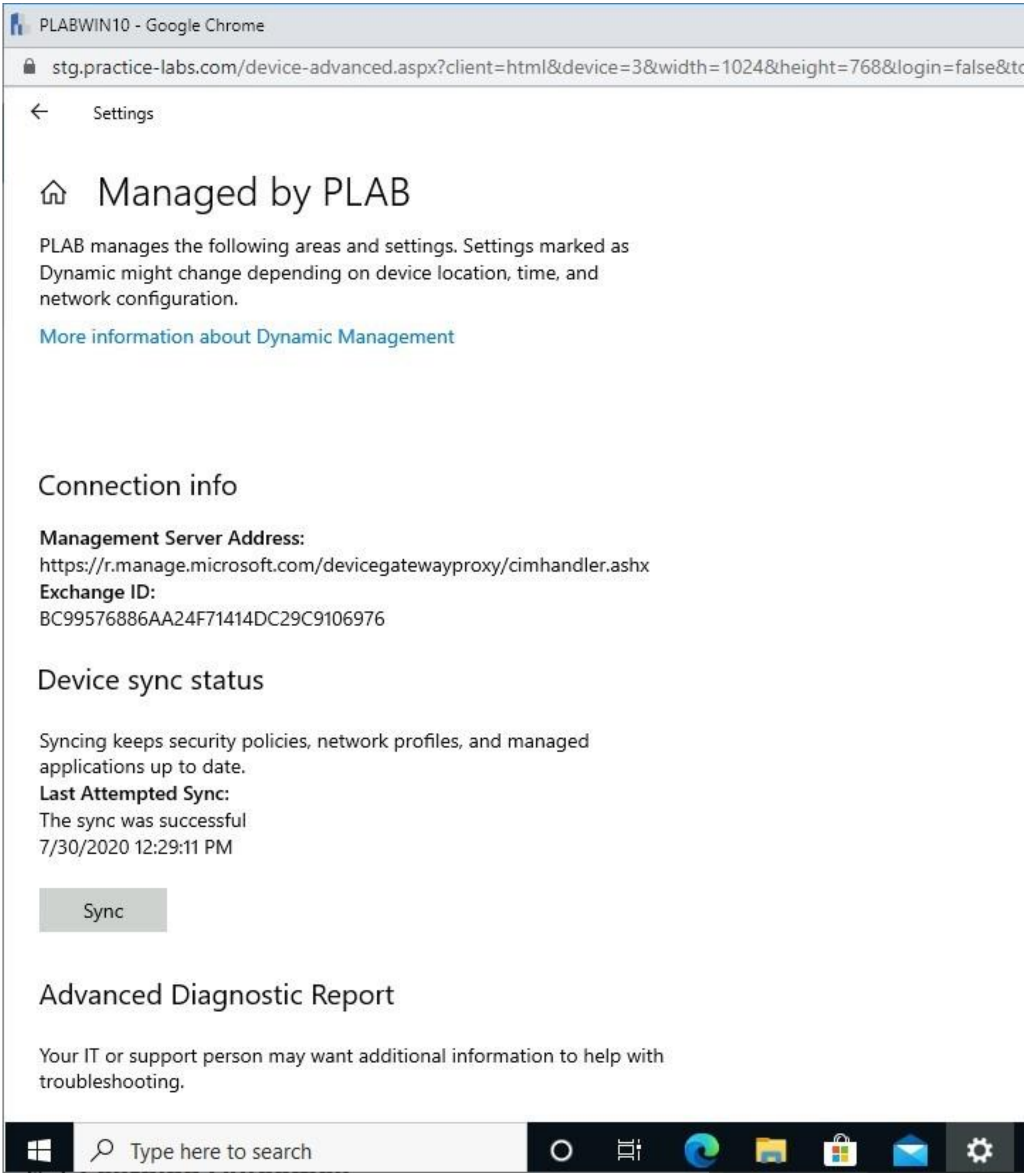
Connected to PLAB's Azure AD pane displayed on the Settings - Access work or school screen is highlighted.

Step 7

The last attempted sync was recorded successfully.

> ***Note****: If there is sync error message, click Sync.*

Close the **Settings** window.



PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc
Settings

Managed by PLAB

PLAB manages the following areas and settings. Settings marked as Dynamic might change depending on device location, time, and network configuration.

More information about Dynamic Management

Connection info

Management Server Address:
https://r.manage.microsoft.com/devicegatewayproxy/cimhandler.ashx
Exchange ID:
BC99576886AA24F71414DC29C9106976

Device sync status

Syncing keeps security policies, network profiles, and managed applications up to date.
Last Attempted Sync:
The sync was successful
7/30/2020 12:29:11 PM

Advanced Diagnostic Report

Your IT or support person may want additional information to help with troubleshooting.

Figure 2.95 Screenshot of PLABWIN10 desktop: Status of the last sync

attempt is listed on the Device sync status section of the Settings - Managed by PLAB screen.

Task 9 - Verify AIP Policy

You will now test the functionality of the AIP labels by creating a Word document and typing the required information to classify documents using labels.

In this task, you will create a Word document and enter the keywords defined in the AIP policy. This is to verify the application of the AIP policy.

Step 1

Ensure you are connected to **PLABWIN10**.

Click the **Start** charm, and start typing:

```
word
```

Select **Word** from the menu.

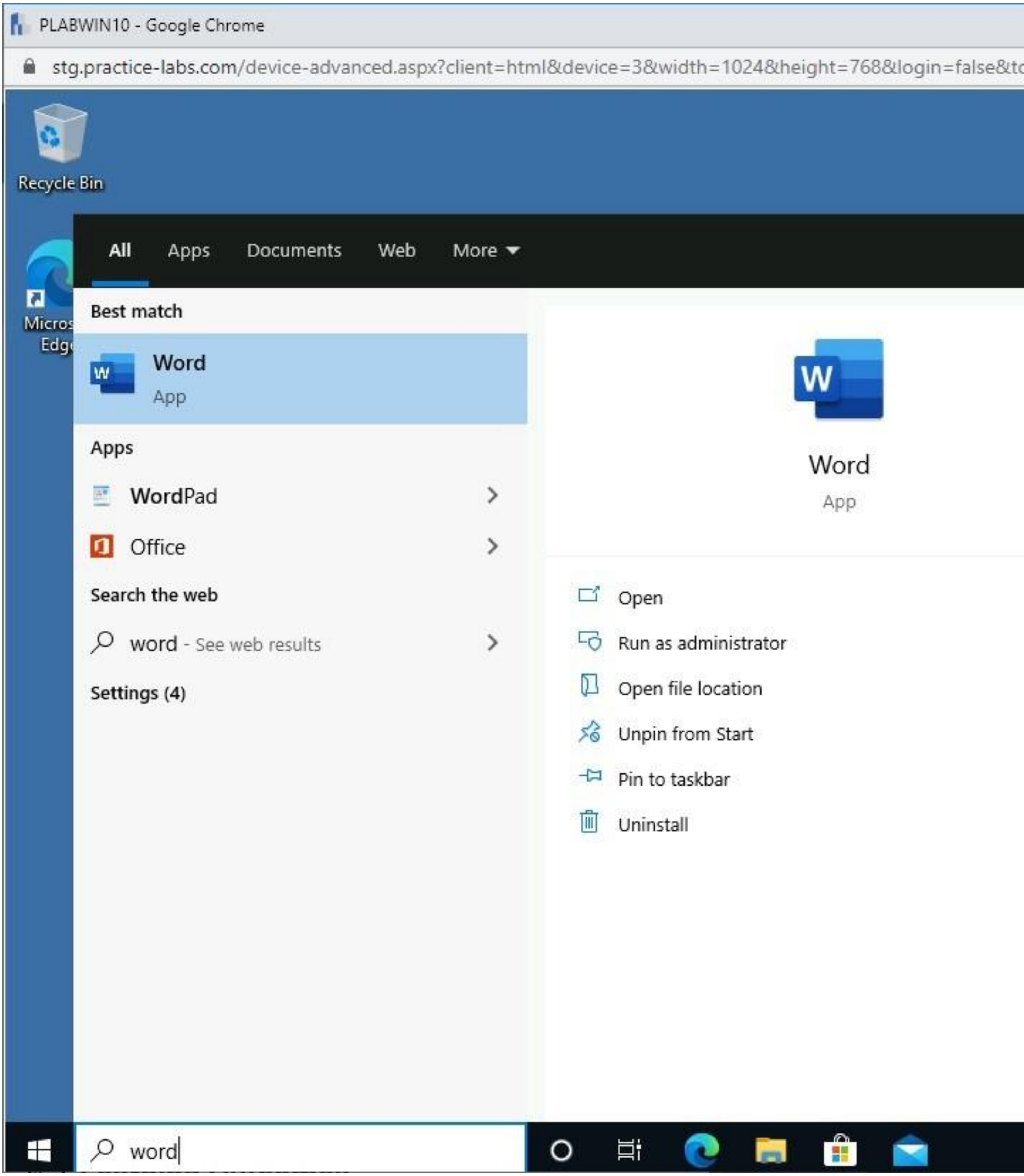
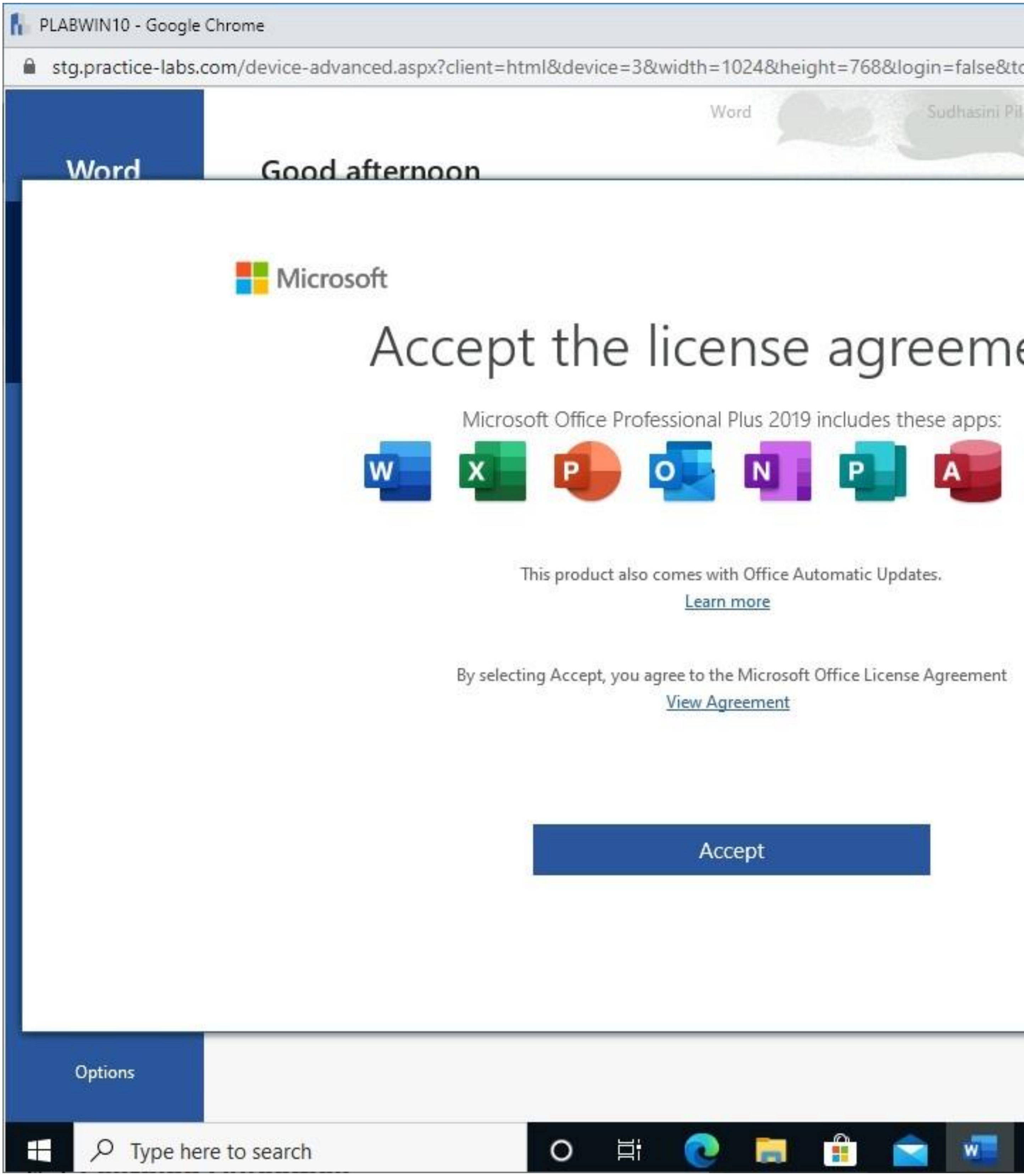


Figure 2.96 Screenshot of PLABWIN10 desktop: Required option on the

Best match popup menu is selected.

Step 2

Select **Accept** from **Accept the license agreement** message box.



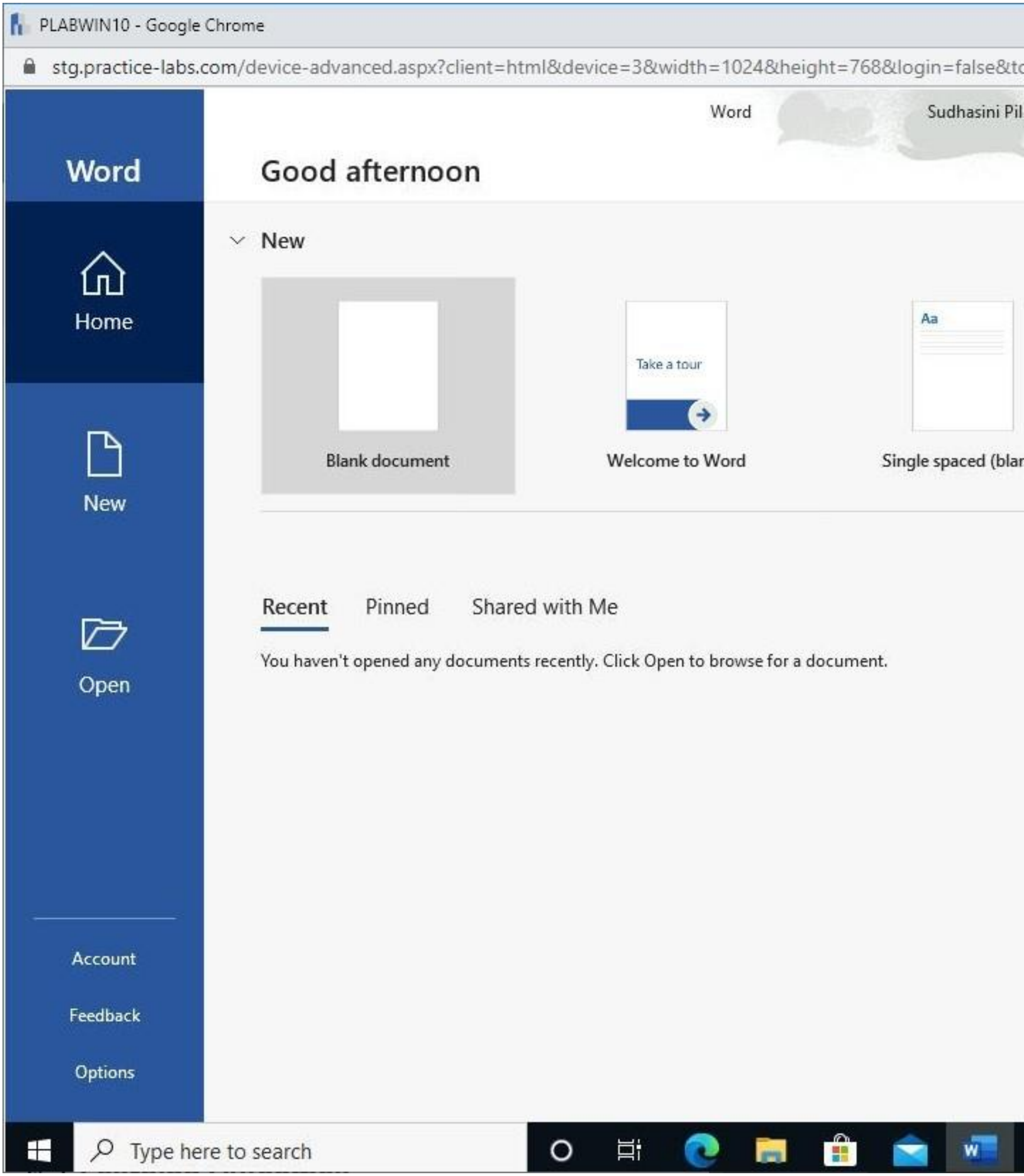
PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&to
Word
Sudhasini Pil
Word
Good afternoon
Microsoft
Accept the license agreeme
Microsoft Office Professional Plus 2019 includes these apps:
W
X
P
O
N
P
A
This product also comes with Office Automatic Updates.
Learn more
By selecting Accept, you agree to the Microsoft Office License Agreement
View Agreement
Accept
Options
Type here to search

Figure 2.97 Screenshot of PLABWIN10 desktop: Accept button on the

Microsoft Accept the license agreement screen is highlighted.

Step 3

Select **Blank document** from the backstage view of **Word**.



PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc
Word
Sudhasini Pil
Word
Good afternoon
Home
New
Open
Account
Feedback
Options
New
Blank document
Take a tour
Welcome to Word
Aa
Single spaced (blar
Recent
Pinned
Shared with Me
You haven't opened any documents recently. Click Open to browse for a document.
Type here to search

Figure 2.98 Screenshot of PLABWIN10 desktop: Blank document option on

the backstage view of the Microsoft Word app is highlighted.

Step 4

Click **Sensitivity** on the Ribbon.

Notice it displays the labels that were created earlier.

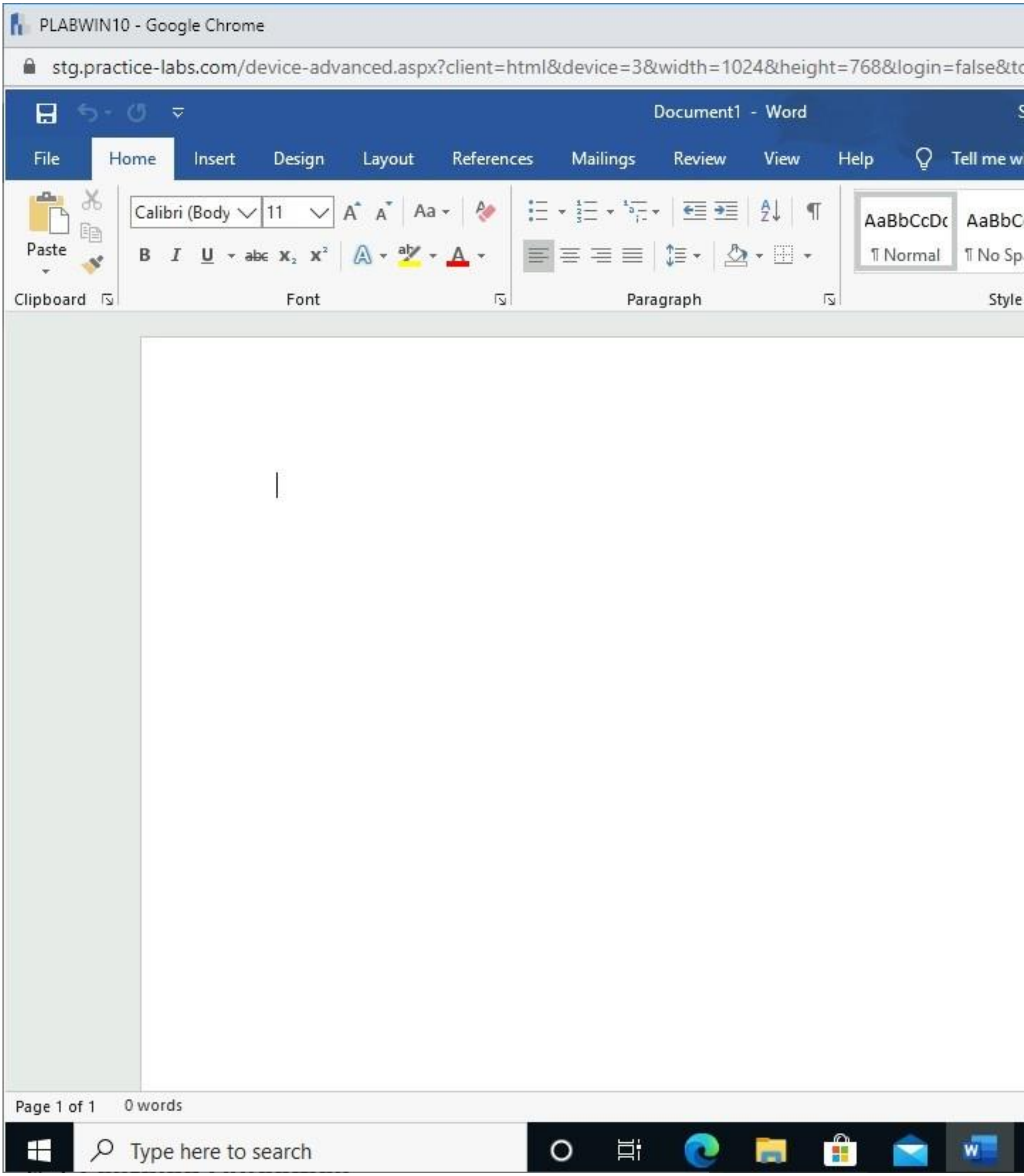


Figure 2.99 Screenshot of PLABWIN10 desktop: Sensitivity option on the

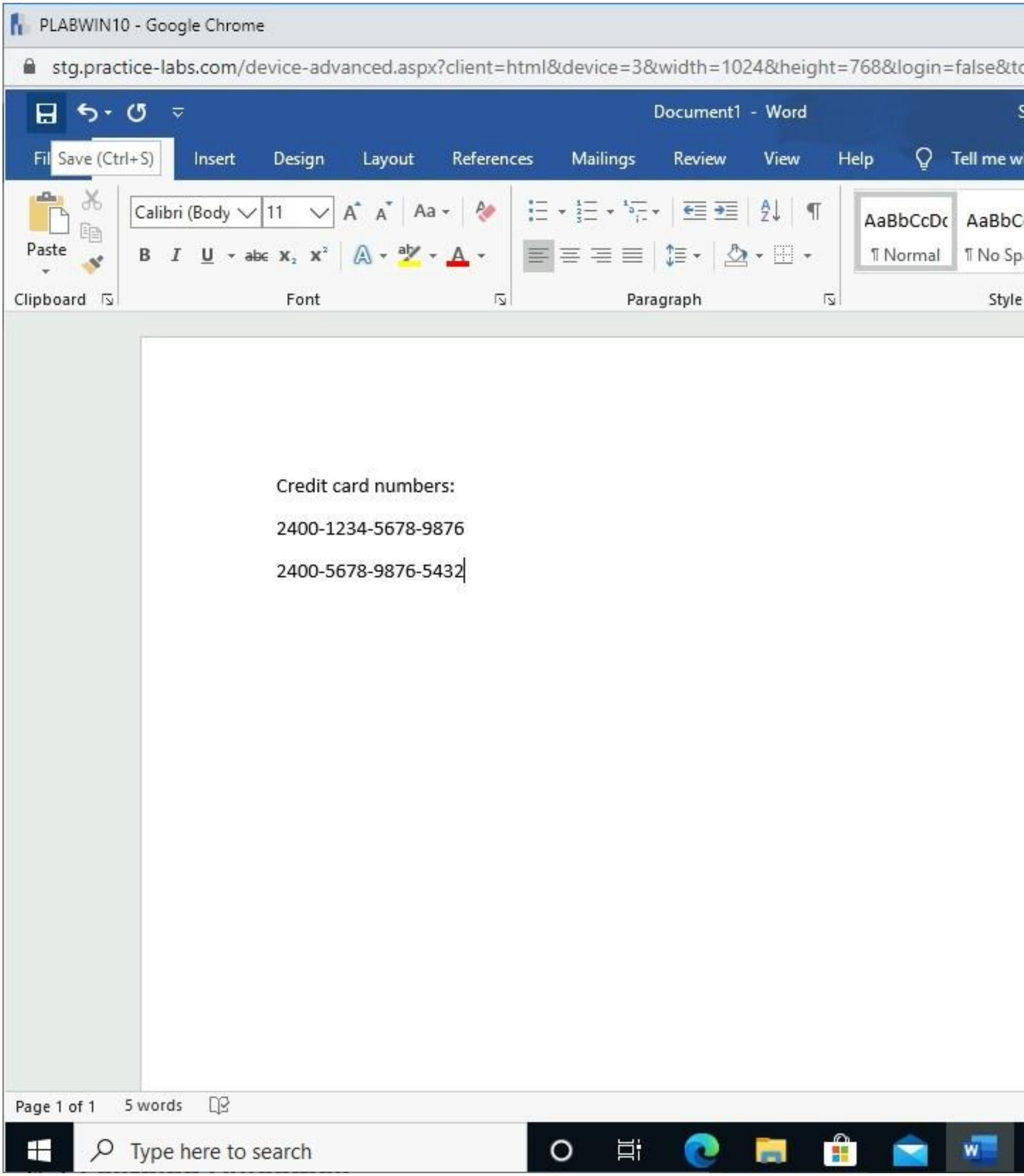
Home menu ribbon of the Word interface is selected listing the labels created earlier.

Step 5

On the **Document1** window, type the following:

```
Credit card numbers:
2400-1234-5678-9876
2400-5678-9876-5432
```

Click the **Save** icon.



Credit card numbers:

2400-1234-5678-9876

2400-5678-9876-5432

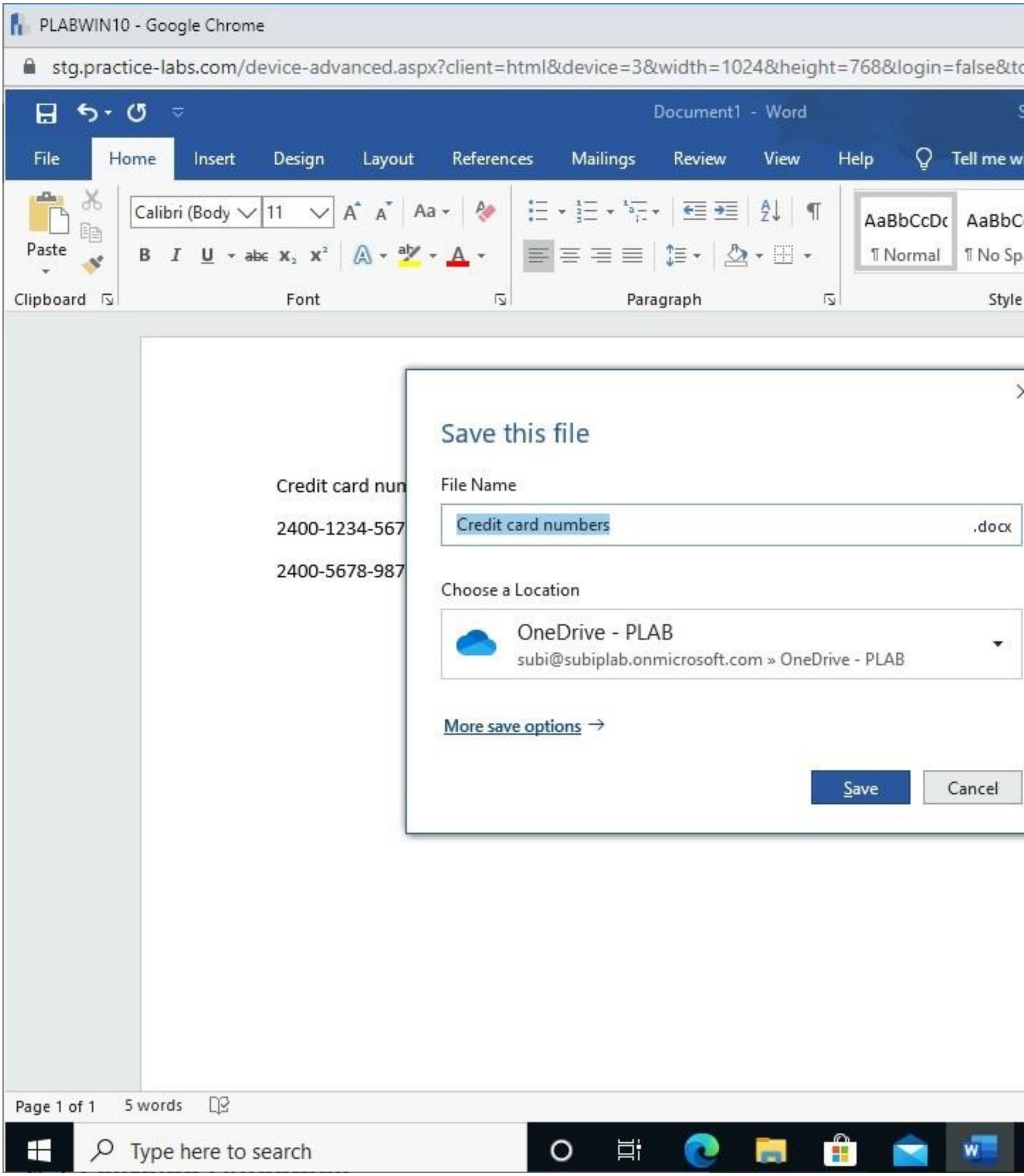
Figure 2.100 Screenshot of PLABWIN10 desktop: Microsoft Word

document is displayed showing the required text typed in, and the Save icon highlighted.

Step 6

Click **Got it** on the **Choose a location** message box.

On the **Save this file** dialog box, select **More save options**.



Credit card nun

2400-1234-567

2400-5678-987

Save this file

File Name

Credit card numbers .docx

Choose a Location

OneDrive - PLAB
subi@subiplab.onmicrosoft.com » OneDrive - PLAB

More save options →

Save Cancel

Figure 2.101 Screenshot of PLABWIN10 desktop: Save this file dialog box is

displayed showing the required settings performed and the More save options link selected.

Step 7

On the **Save As** page in the backstage view, select **Browse**.

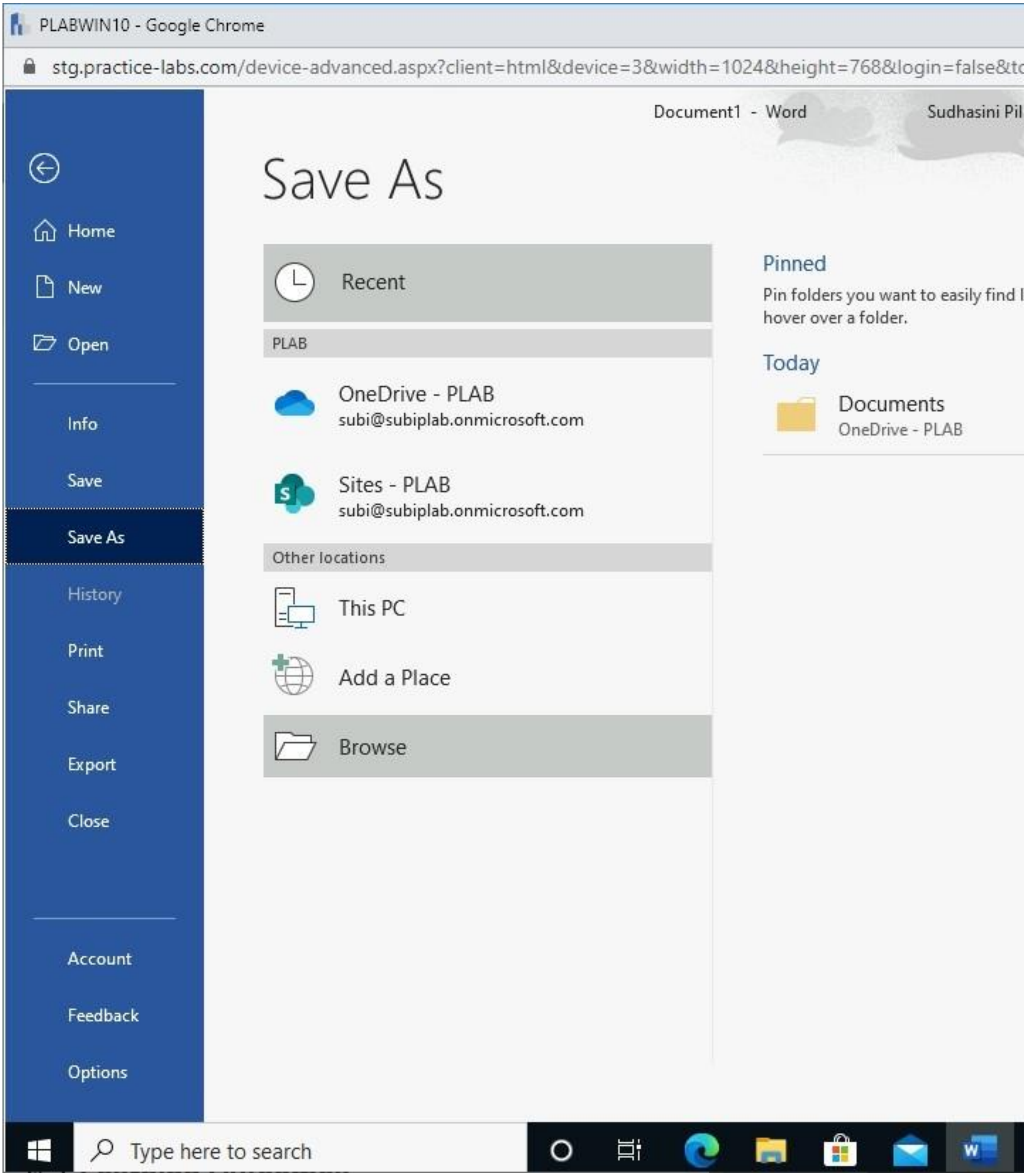


Figure 2.102 Screenshot of PLABWIN10 desktop: Browse option on the

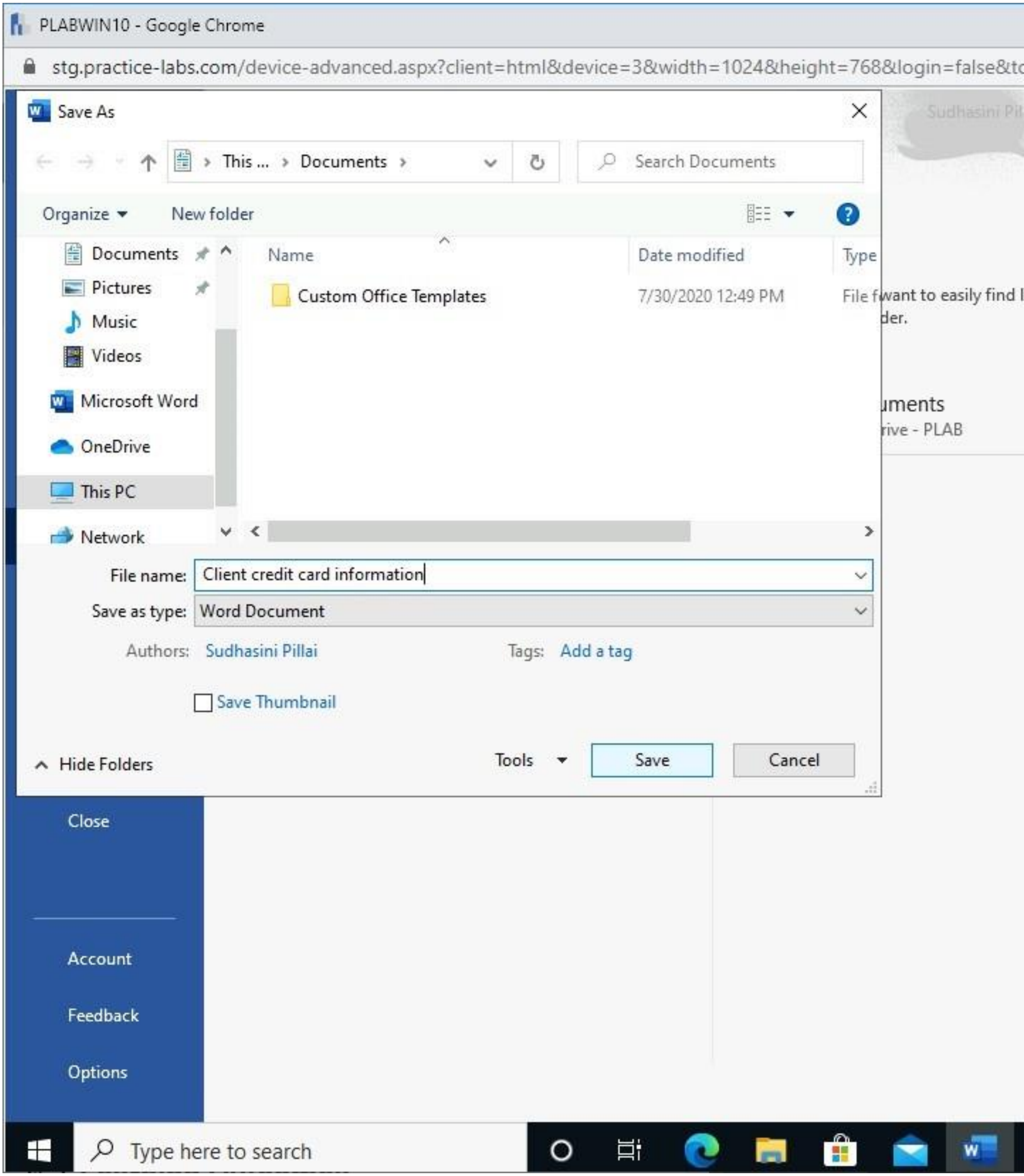
Save As backstage menu is selected.

Step 8

From the **Save As** dialog box, use the following filename:

```
Client credit card information
```

Click **Save**.



PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=false&tc

Save As

This ... › Documents ›

Name	Date modified	Type
Custom Office Templates	7/30/2020 12:49 PM	File f

File name: Client credit card information

Save as type: Word Document

Authors: Sudhasini Pillai

Tags: Add a tag

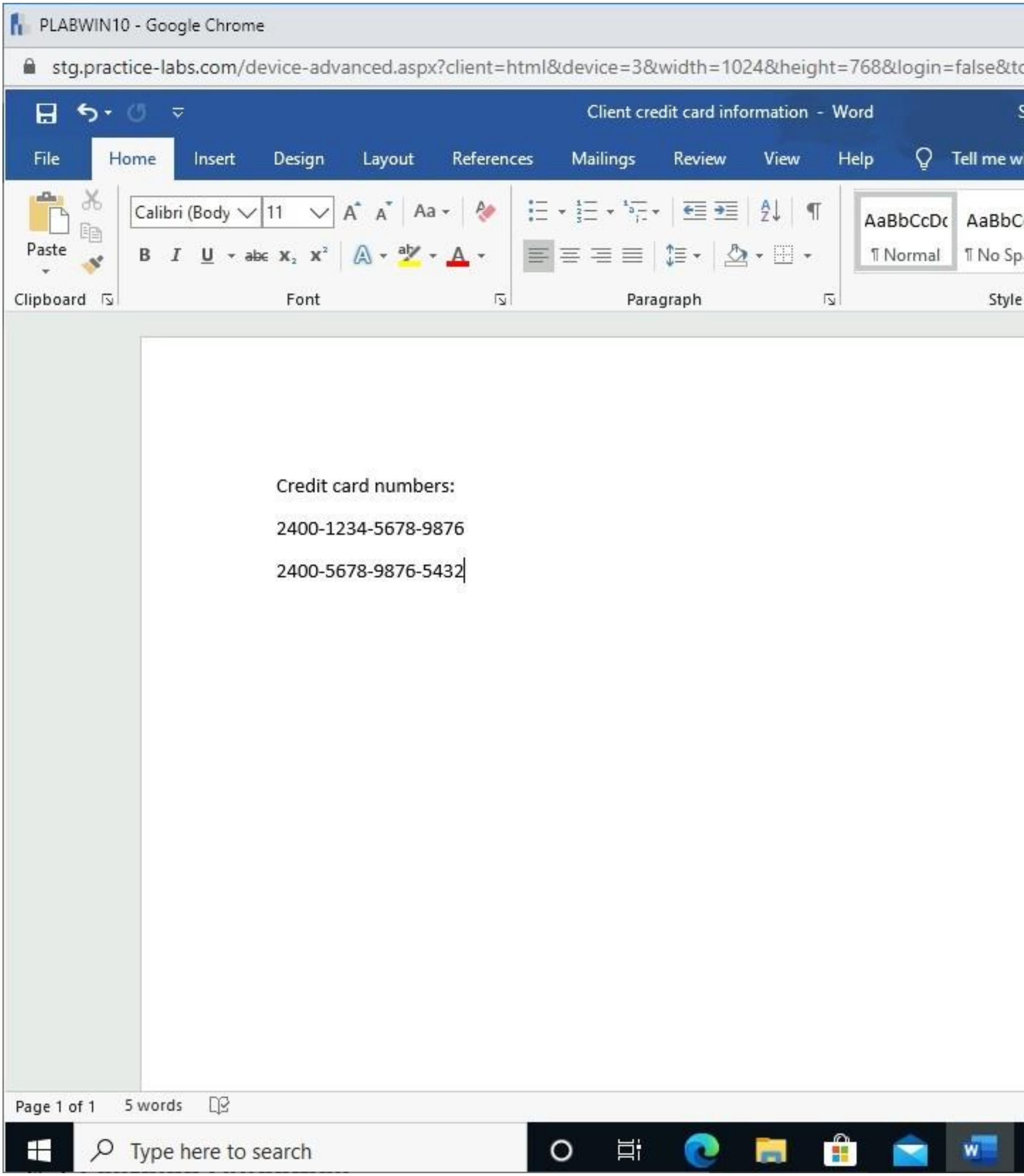
□ Save Thumbnail

Figure 2.103 Screenshot of PLABWIN10 desktop: Save As dialog box is

displayed showing the required filename typed in and the Save button highlighted.

Step 9

Back in the **Client credit card information** document window, click **Sensitivity,** and select **Secret.**



Credit card numbers:

2400-1234-5678-9876

2400-5678-9876-5432

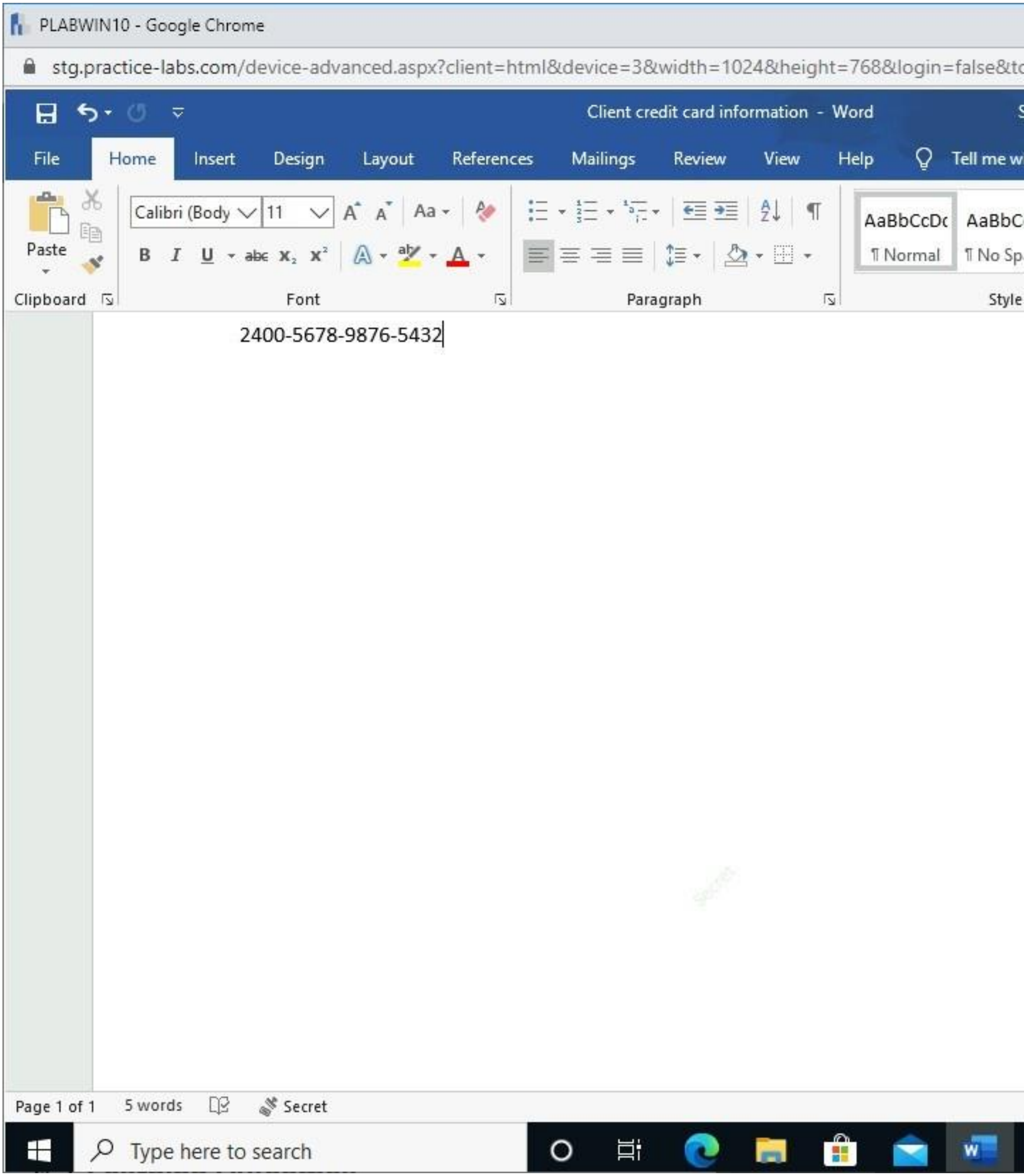
Figure 2.104 Screenshot of PLABWIN10 desktop: Sensitivity > Secret

menu-options on the Home menu ribbon of the Word interface is selected.

Step 10

The **Client credit card information** document window now indicates a “**Secret**” label.

Observe the green watermark at the center of the document page.



2400-5678-9876-5432

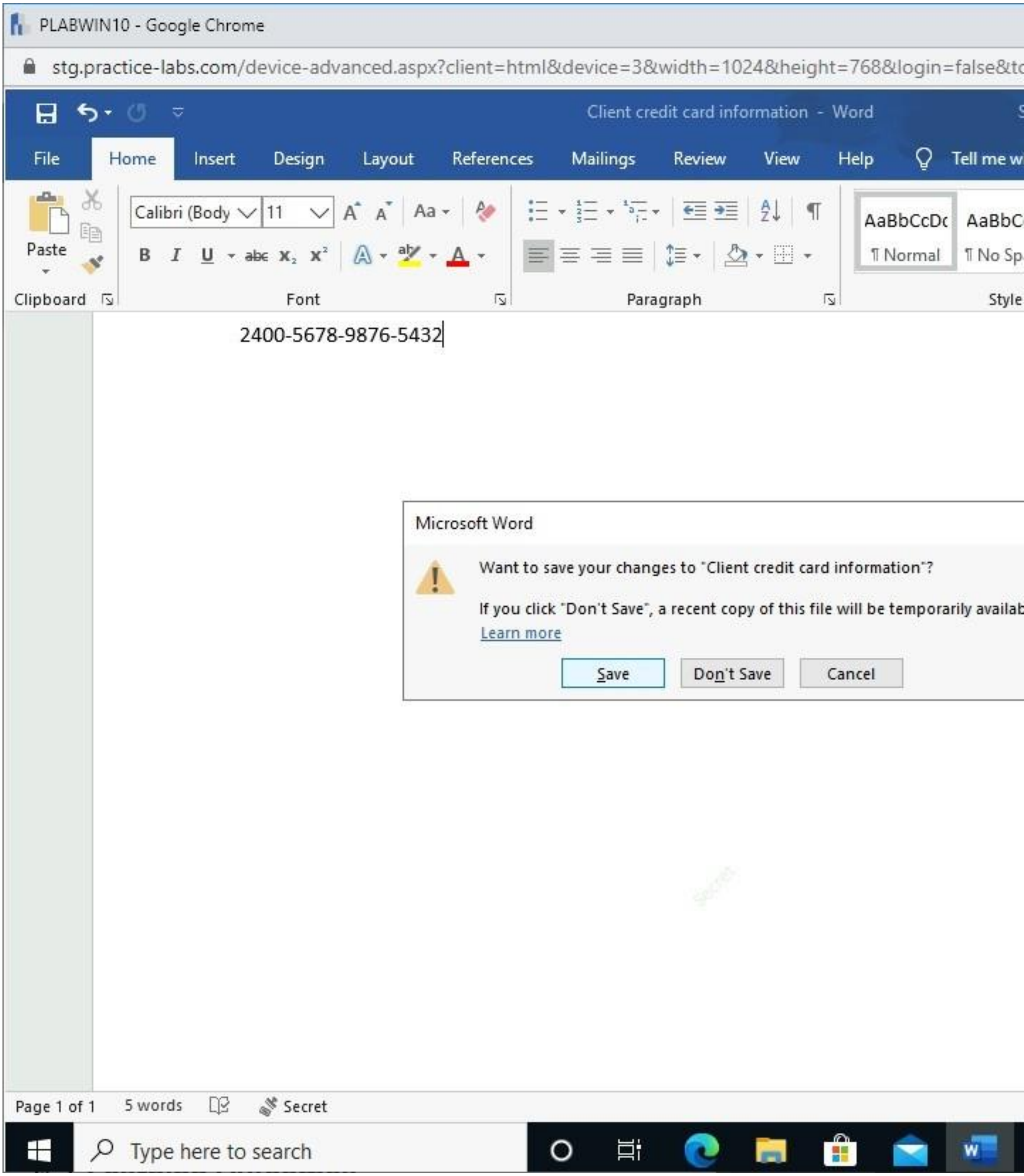
Figure 2.105 Screenshot of PLABWIN10 desktop: Specified label is now

applied to the document displayed.

Step 11

Close the document window.

Click **Save** in the **Microsoft Word** message box.



2400-5678-9876-5432

Microsoft Word

Want to save your changes to "Client credit card information"?

If you click "Don't Save", a recent copy of this file will be temporarily availab

Learn more

Figure 2.106 Screenshot of PLABWIN10 desktop: Microsoft Word

information box is displayed prompting to save changes to the file and showing the Save button highlighted.

Step 12

Right-click **Start**, point to **Shut down or sign out** and click **Sign out**.

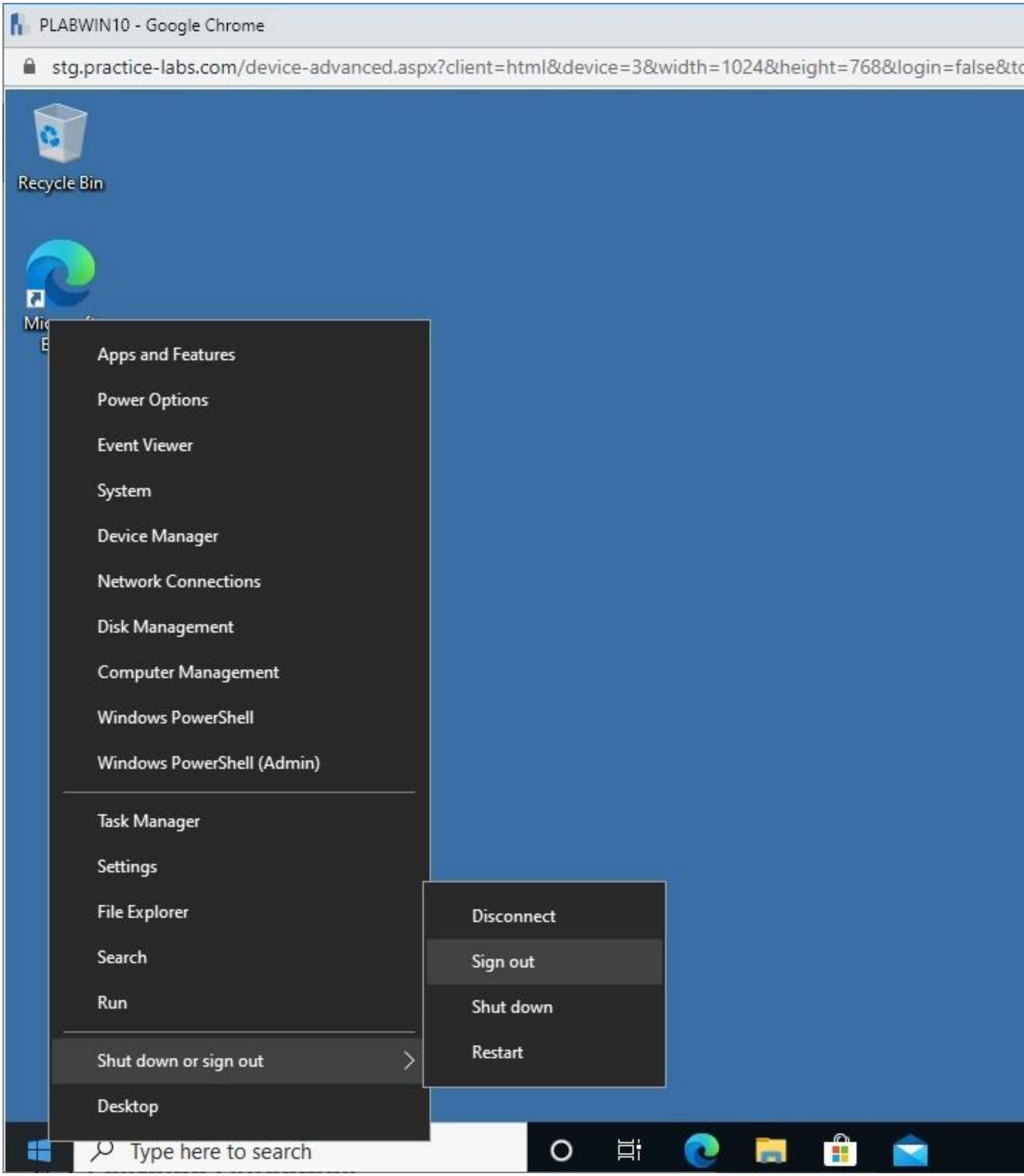


Figure 2.107 Screenshot of PLABWIN10 desktop: Context menu (that

appears on right-clicking the Start charm) > Shut down or sign out > Sign out menu-options are selected.

Keep all devices that you have powered on in their current state and proceed to the review section.

Review

Well done, you have completed the **Implement Azure Information Protection** Practice Lab.

Summary

You completed the following exercises:

- Exercise 1 - Configure Prerequisites for Azure Information Protection
- Exercise 2 - Implement Azure Information Protection Labels

You should now be able to:

- Remove Device from Azure AD
- Remove Domain Computer from Active Directory
- Join the Computer to Azure AD
- Generate Default Policies and Labels
- Migrate AIP Labels to Office 365 Security and Compliance Center
- Create a Custom Label
- Edit the Confidential Label
- Publish the Labels
- Install Azure Information Protection Client Unified Labeling
- Enable Remote Desktop
- Configure Proxy Server Settings for a New User
- Verify AIP Policy