Installing and Configuring Windows Server 2012

Create Group Policy Objects

- **Introduction**
- **Create a GPO Central Store**
- **Manage Starter GPOs**
- **Configure GPO links**
- **Configure Multiple Local Group Policies**
- **GPO Security Filtering**
- **Summary**

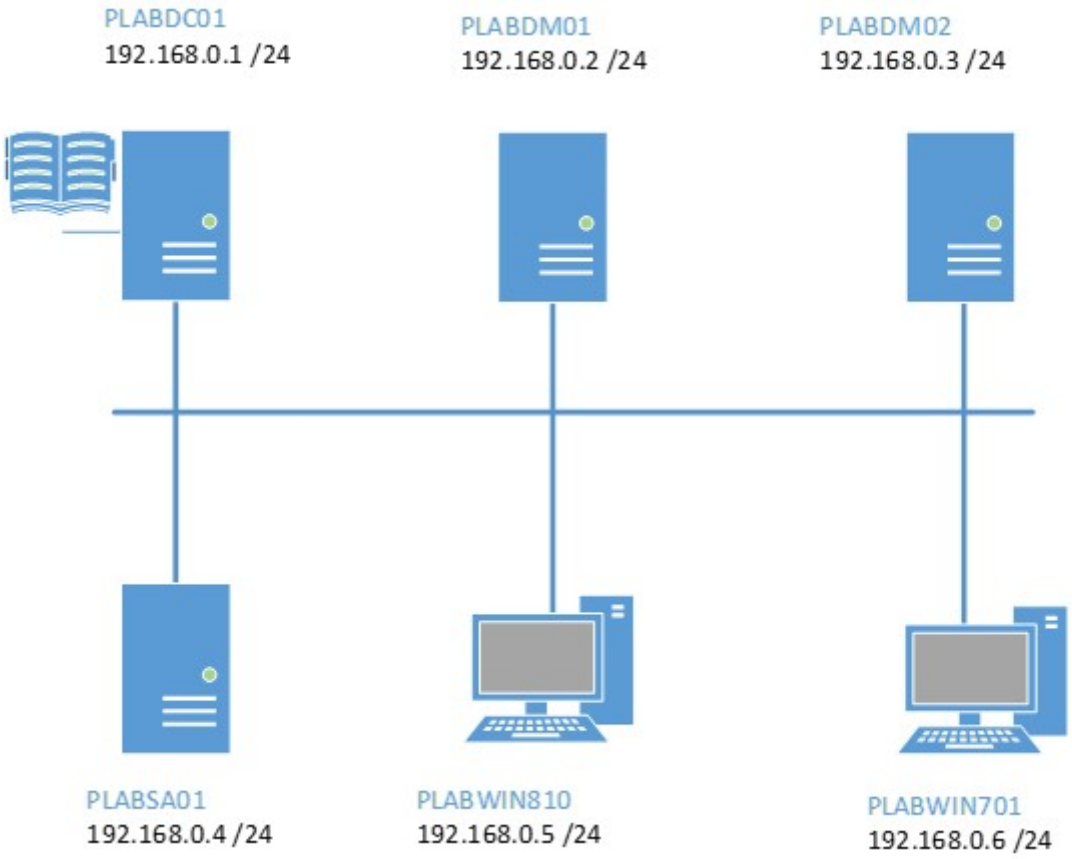
Introduction

The **Create Group Policy Objects** module provides you with the instruction and server hardware to develop your hands on skills in the defined topics. This module includes the following exercises:

- Create a GPO Central Store
- Manage Starter GPOs
- Configure GPO Links
- Configure Multiple Local Group Policy Objects
- GPO Security Filtering

Lab Diagram

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



Connecting to your Lab

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

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

Each exercise will detail which console you are required to work on to carry out the steps.

To start simply click on the named Server from the device list (located on the left hand side of the screen) and click the **Power on** from the in tools bar. In some cases the devices may power on automatically.

During the boot up process an activity indicator will be displayed in the name tab:

- Black - Powered Off
- Blue - Working on your request
- Green - Ready to access

> *If the remote console is not displayed automatically in the main window (or popup) click the **Connect** icon located in the tools bar to start your session.*

If the remote console does not appear please try the following option:

- Switch between the HTML 5 and Java client versions in the tools bar.

In the event this does not resolve your connectivity problems please visit our Help / Support pages for additional resolution options.

Copyright Notice
This document and its content is copyright of Practice-IT - © Practice-IT 2014. All rights reserved. Any redistribution or reproduction of part or all of the contents in any form is prohibited other than the following:
1. You may print or download to a local hard disk extracts for your personal and non-commercial use only.
2. You may copy the content to individual third parties for their personal use, but only if you acknowledge the website as the source of the material. You may not, except with our express written permission, distribute or commercially exploit the content. Nor may you transmit it or store it in any other website or other form of electronic retrieval system.

Exercise 1 - Create a GPO Central Store

In this exercise, you will perform the tasks required to create Group Policy Objects (GPOs).

Please refer to your course material or use your favourite search engine to research for more information about this topic.

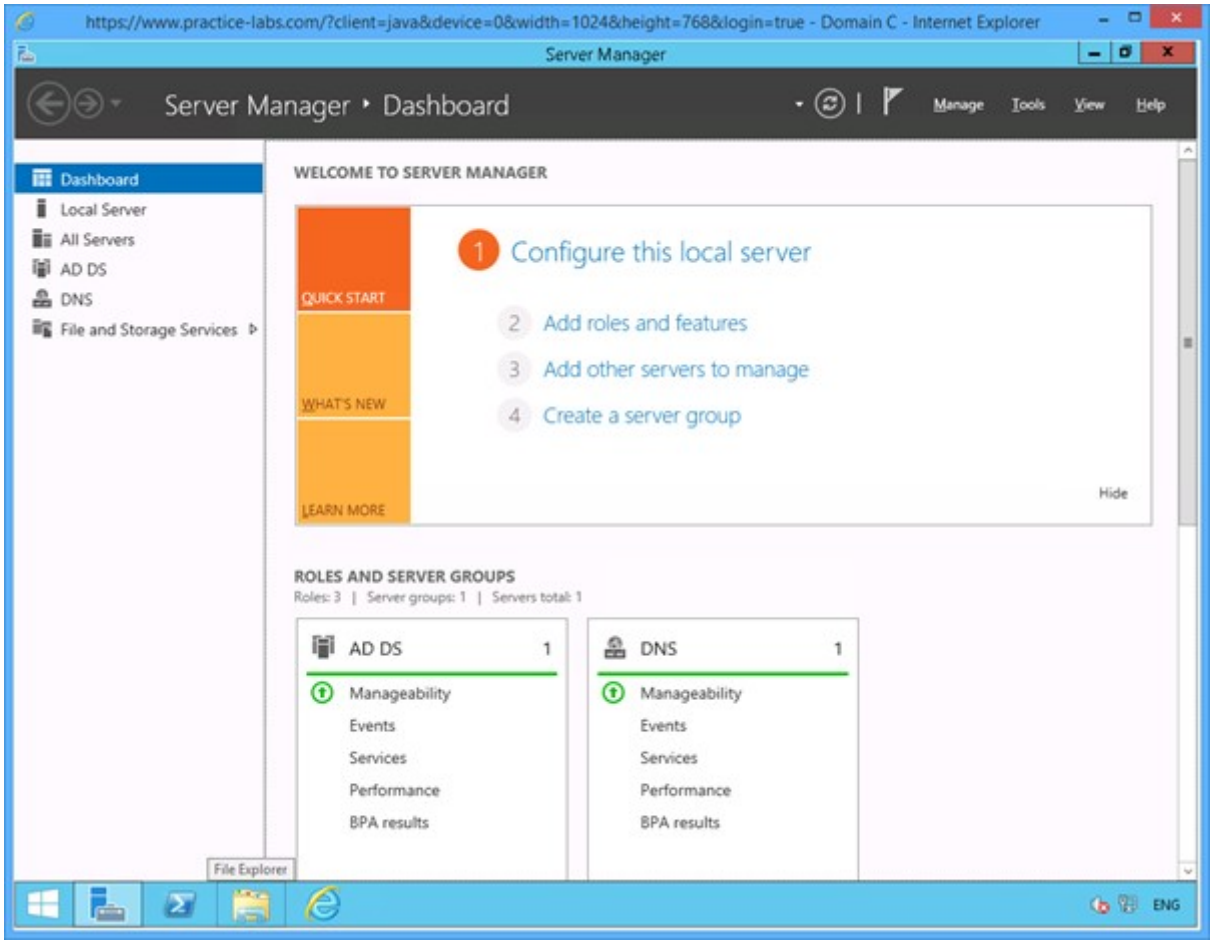
Task 1 - Create a GPO Central Store

In the Windows environment, the Administrative Template files are saved as the .admx files that the Group Policy administrators can use. As a Group Policy Administrator, you can create a Central Store in the SYSVOL folder on a domain controller to centrally store all the .admx files. The Group Policy tools use the .admx files stored in the Central Store. The .admx files, which are stored in the Central Store, are later replicated to all domain controllers in a domain.♂To create a GPO Central Store, perform the following steps:

Step 1

Ensure you have powered on the required devices and connect to **PLABDC01.**

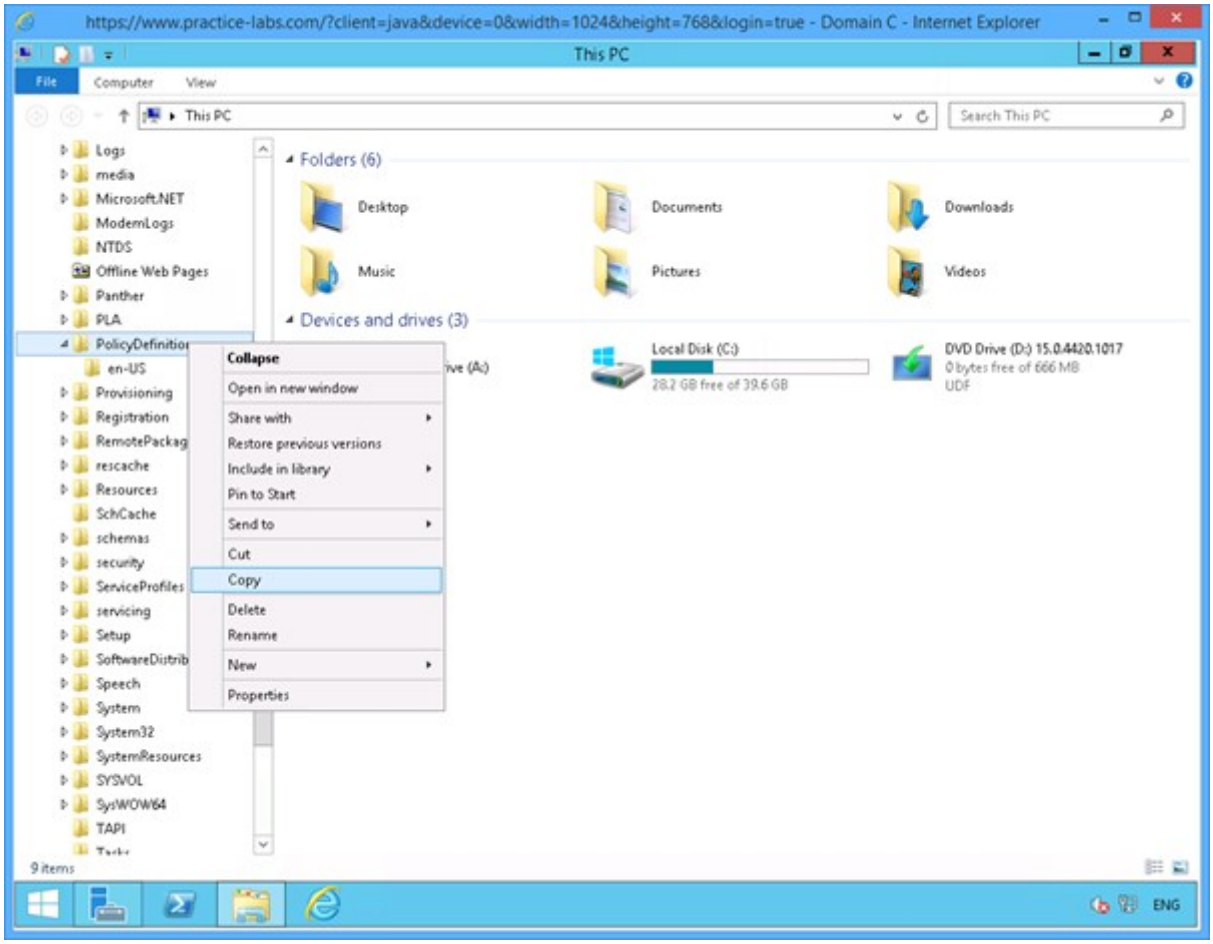
In the taskbar, click the **File Explorer** icon.



Step 2

Expand **Local Disk C** drive, navigate to the **Windows > PolicyDefintions** folder.

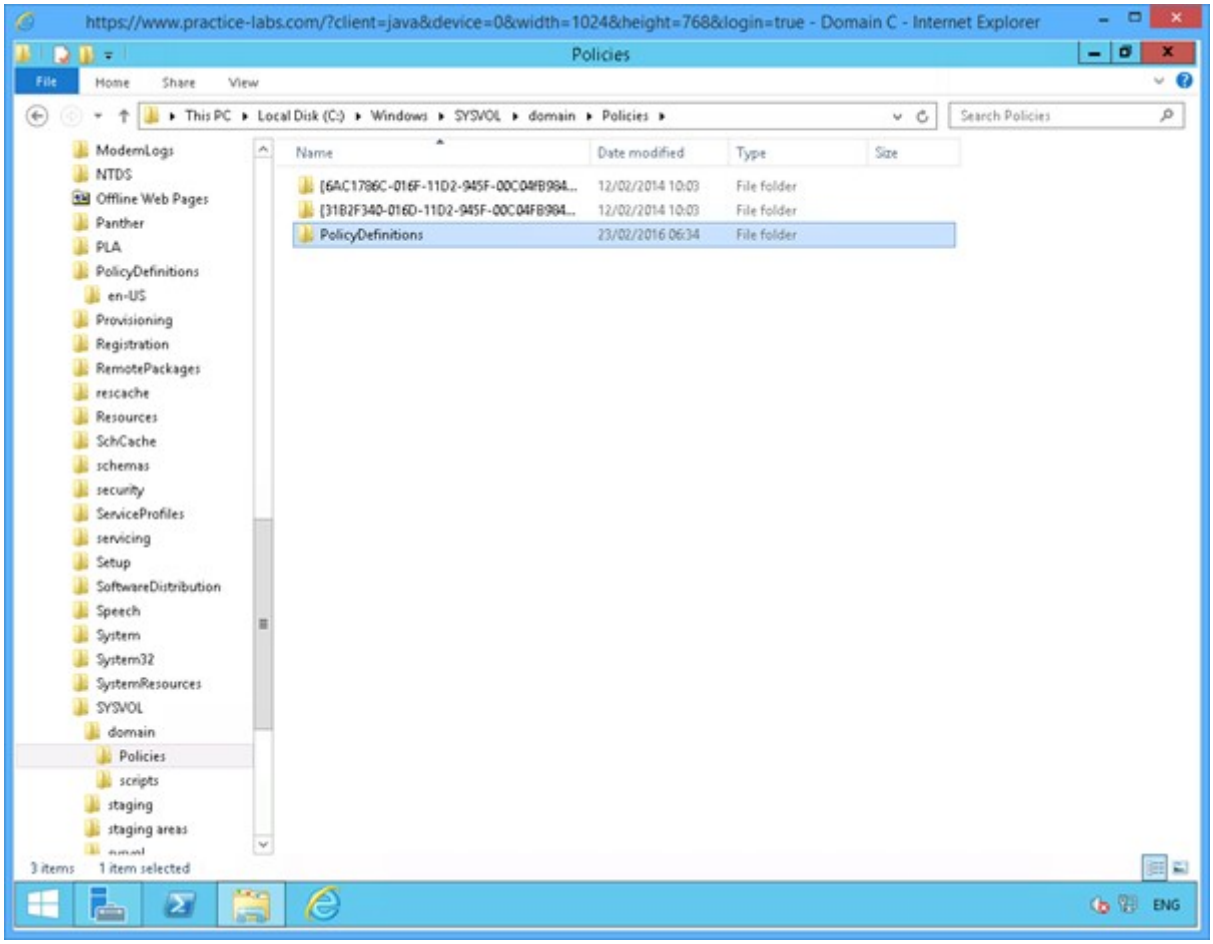
Right-click **PolicyDefinitions** then select **Copy**.



Step 3

Navigate to the **C:Windows > SYSVOL > domain** and click **Policies** folder.

On the details pane on the right, paste the **PolicyDefinitions** folder.

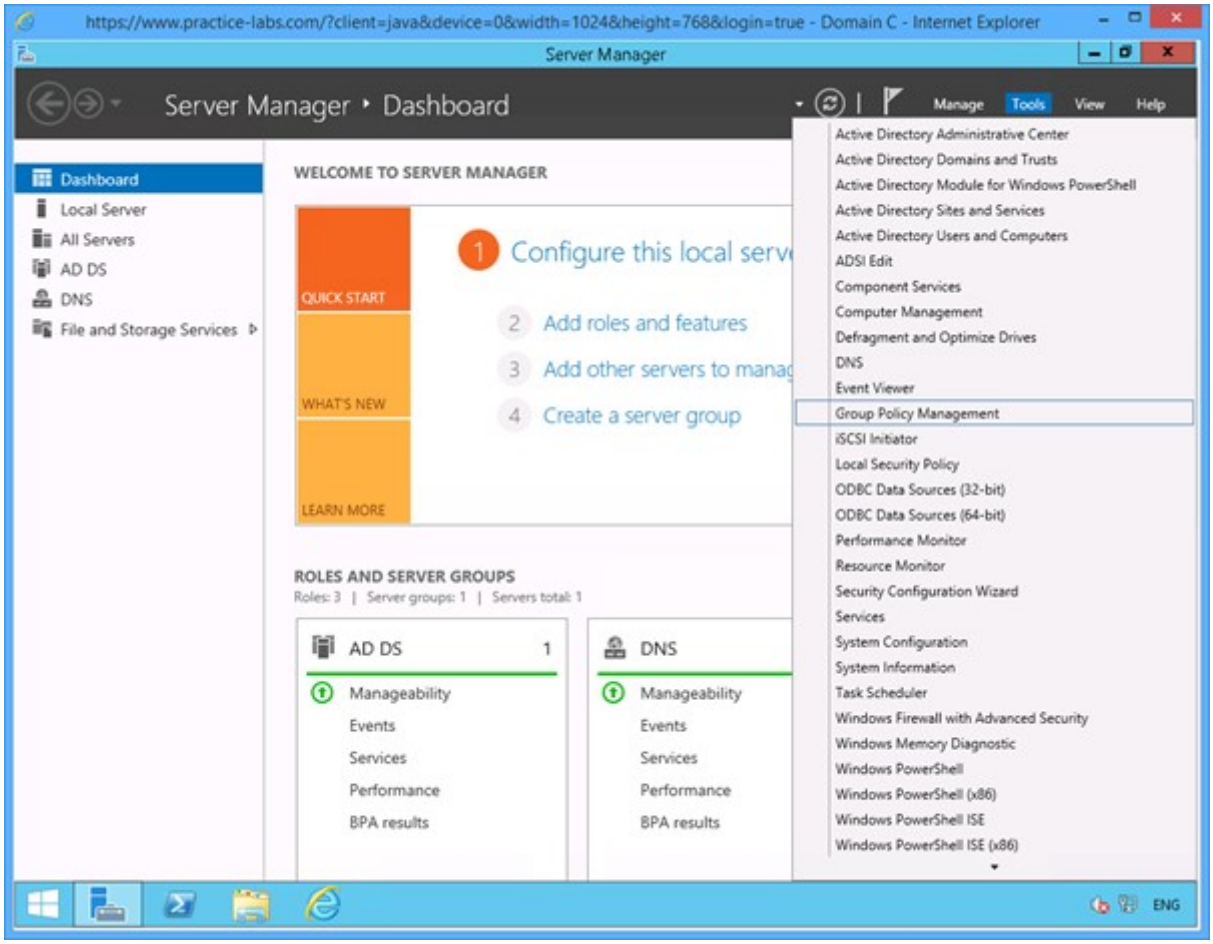


Step 4

Close the **Policies** window. You should have the **Desktop** displayed.

The **Server Manager** Dashboard window is open.

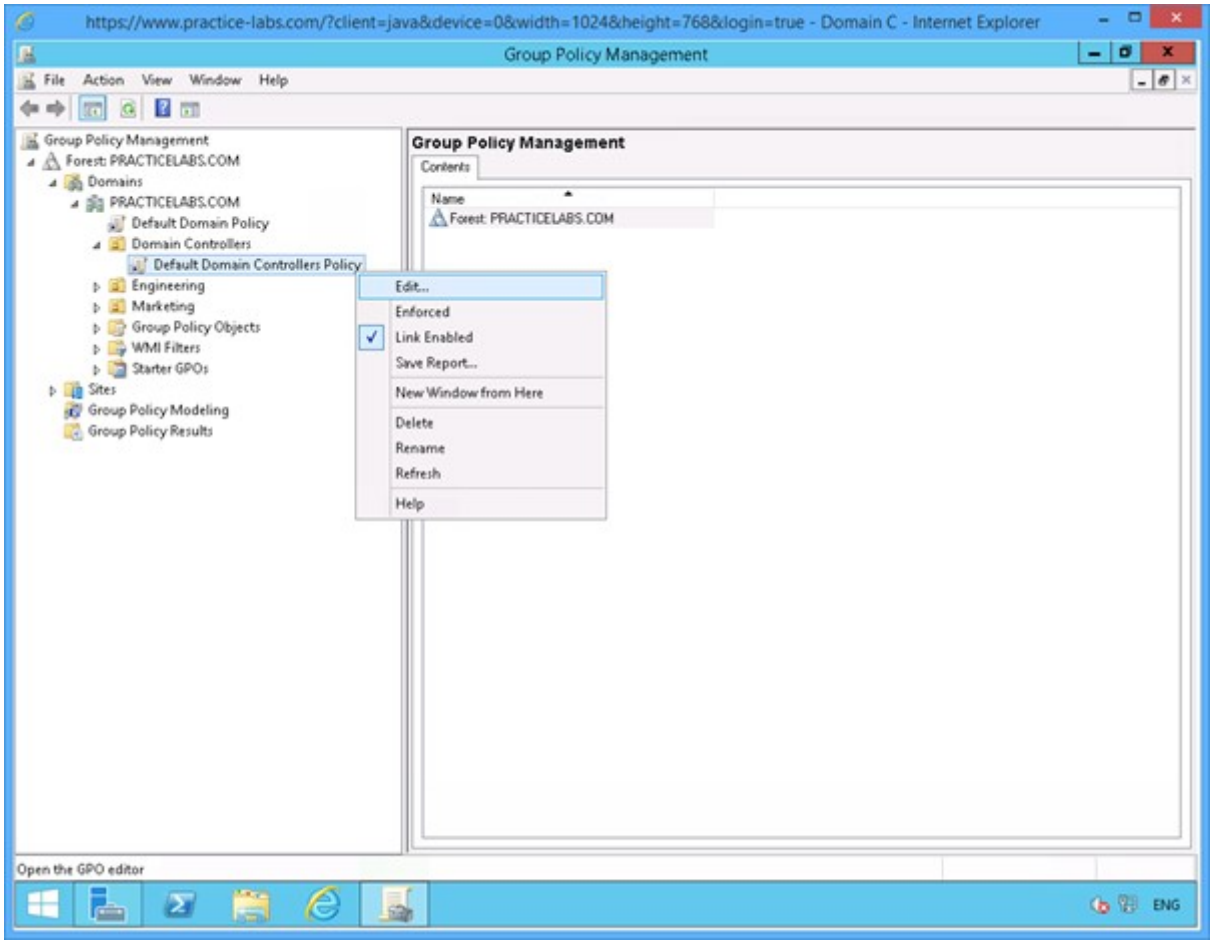
In the upper right hand corner, click **Tools**, and then select **Group Policy Management**.



Step 5

On Group Policy Management console, expand **Forest: PRACTICELABS.COM,** go to **Domains > PRACTICELABS.COM** > **Domain Controllers** OU.

Right-click on **Default Domain Controllers Policy** and select **Edit**...



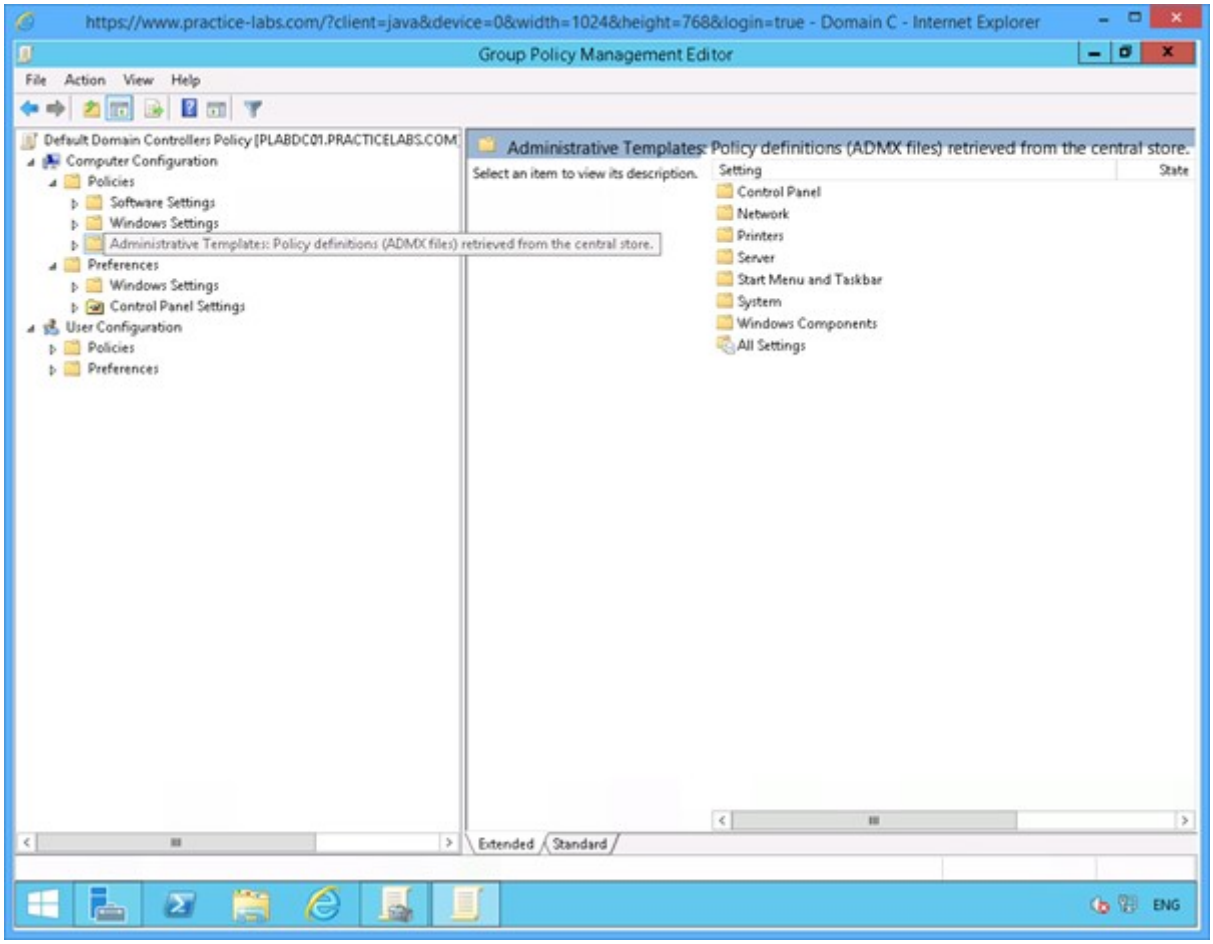
Step 6

The **Group Policy Management Editor** snap-in is displayed.

Expand **Computer Configuration** then **Policies** and **select Administrative Template: Policy definitions**.

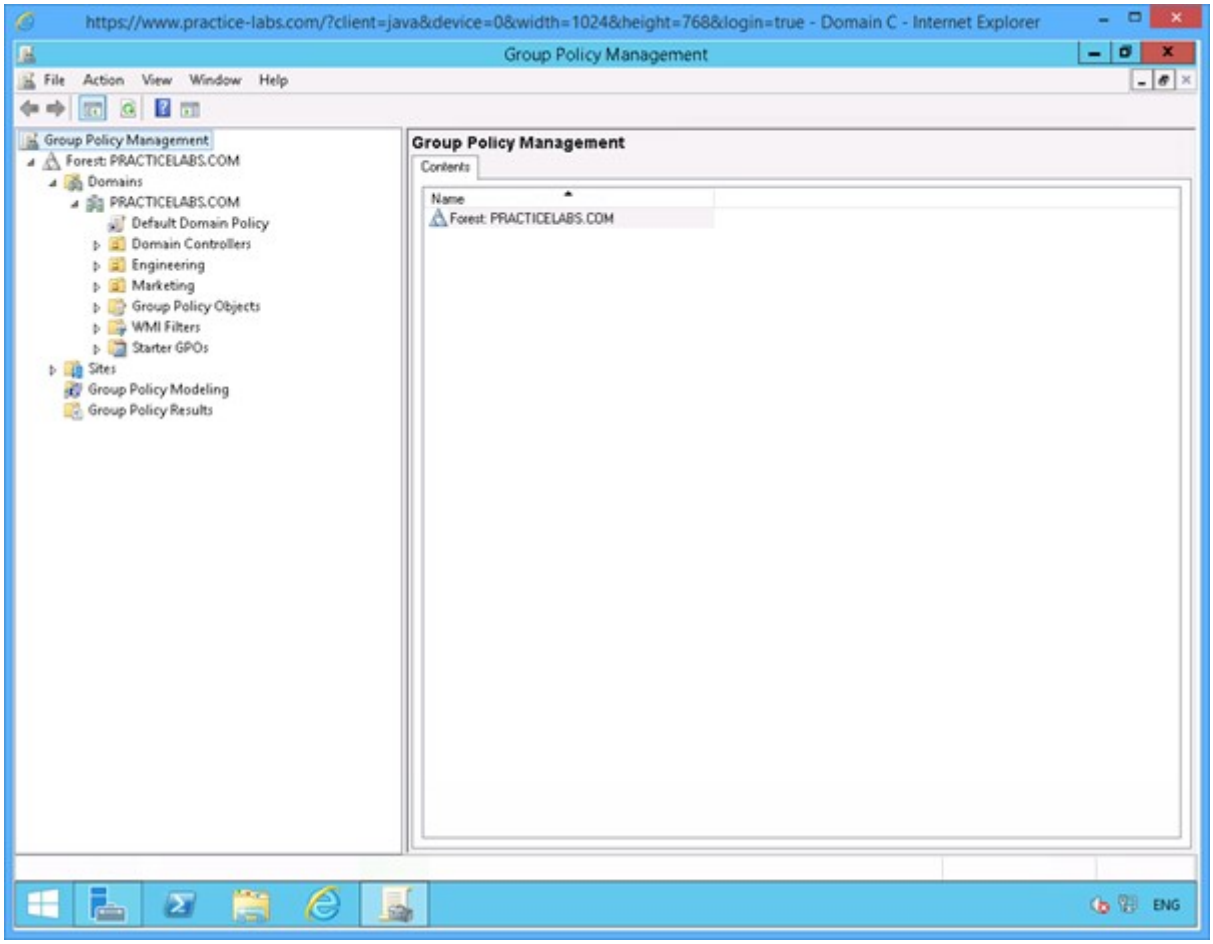
Note that you will get a tooltip stating that policy definitions are retrieved from **Central Store**.

Close **Group Policy Management Editor** window.



Step 7

Keep **Group Policy Management** console window open for the next activity.



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

Exercise 2 - Manage Starter GPOs

A Starter GPO contains the Administrative Template policy settings in a single object. You can import and export the Starter GPO. The shared sysvol contains a sub-folder named Starter GPOs, which contains all the Starter GPOs, when you create this type of GPOs.

Please refer to your course material or use your favourite search engine to research for more information about this topic.

Task 1 - Create Starter GPOs

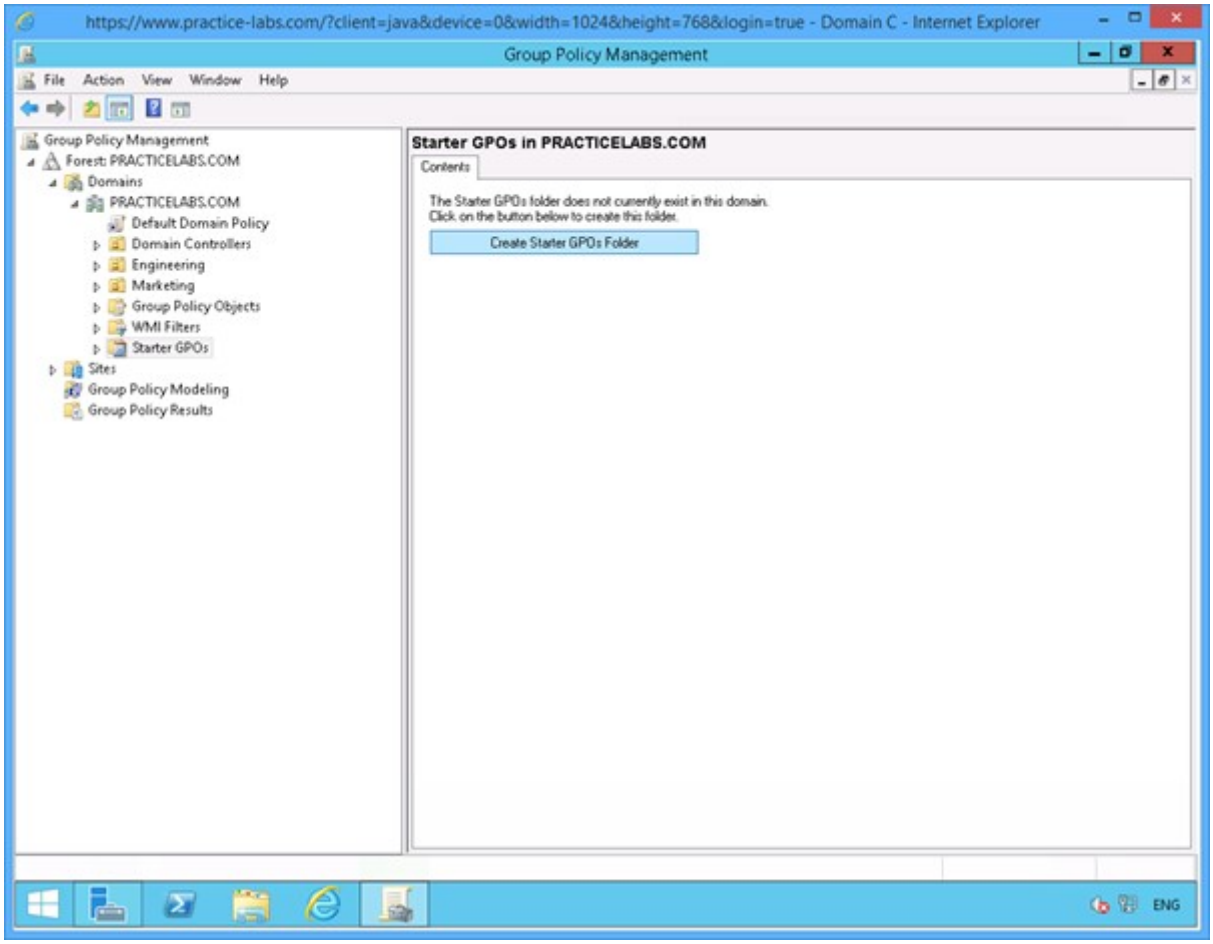
To manage Starter GPOs, perform the following steps:

Step 1

On **PLABDC01,** the **Group Policy Management** console is open.

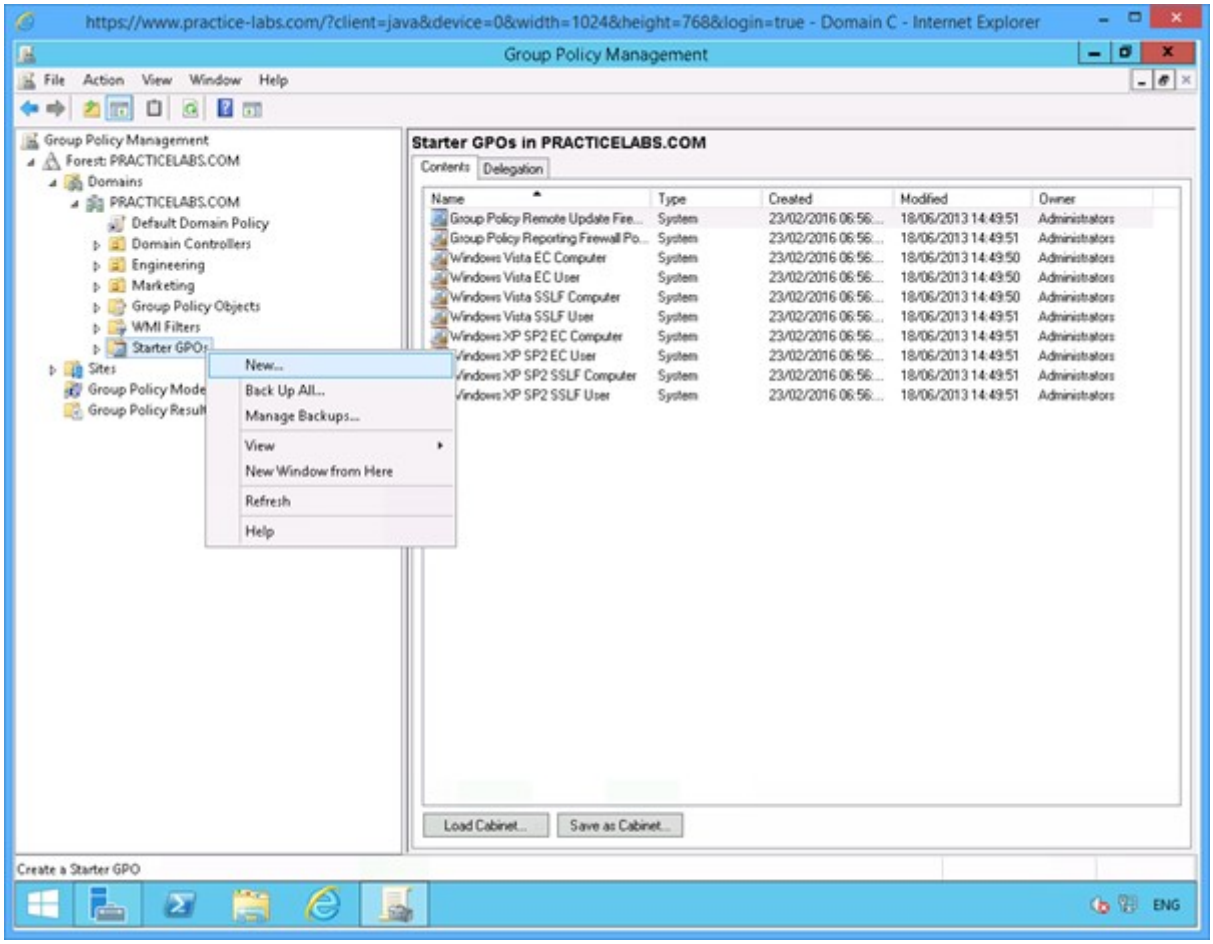
Navigate to **Domains** > **PRACTICELABS.COM** and click on **Starter GPOs** folder.

Click **Create Starter GPOs Folder** button.



Step 2

Right-click **Starter GPOs** in the left pane and select **New**...

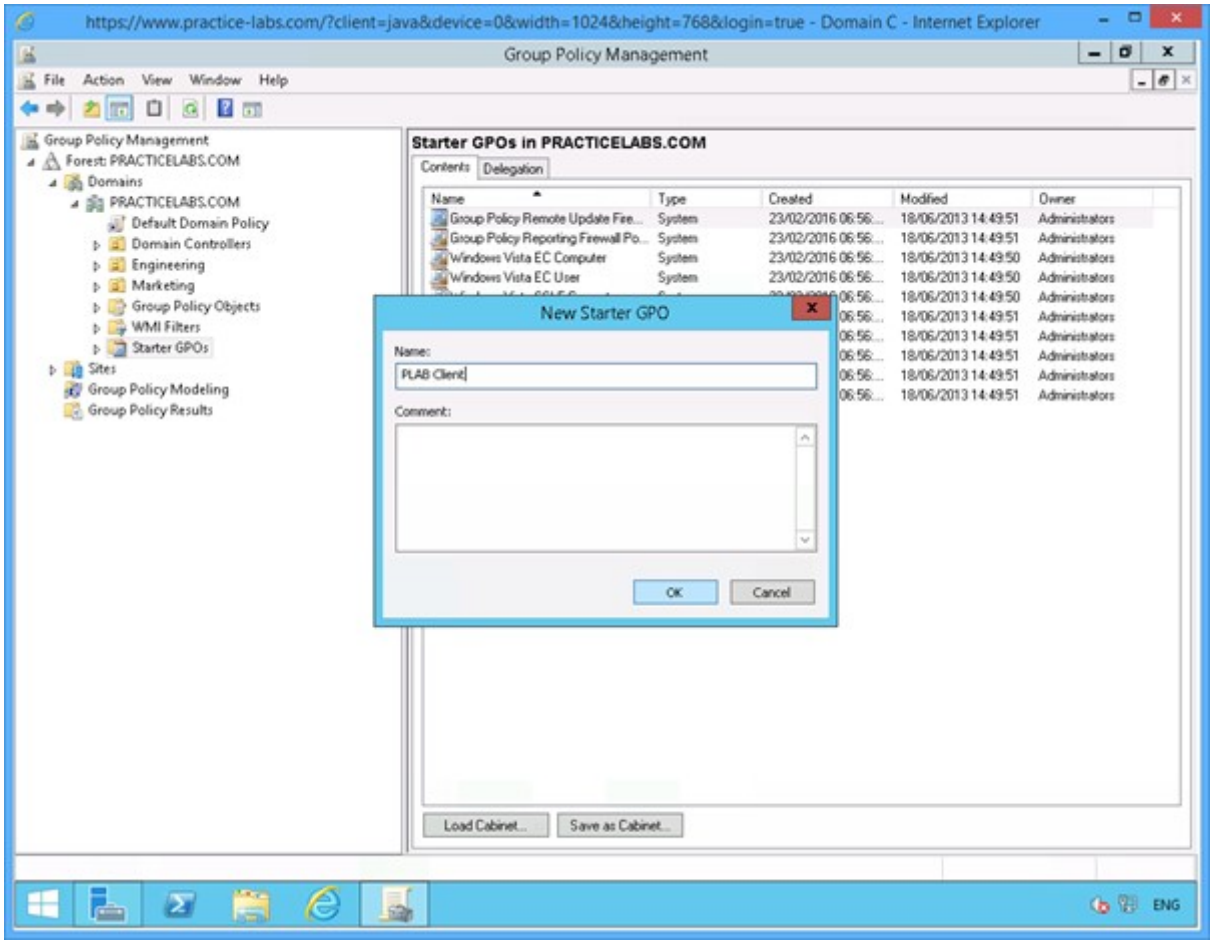


Step 3

From the **New Starter GPO** dialog box, click in the **Name** text box, type:

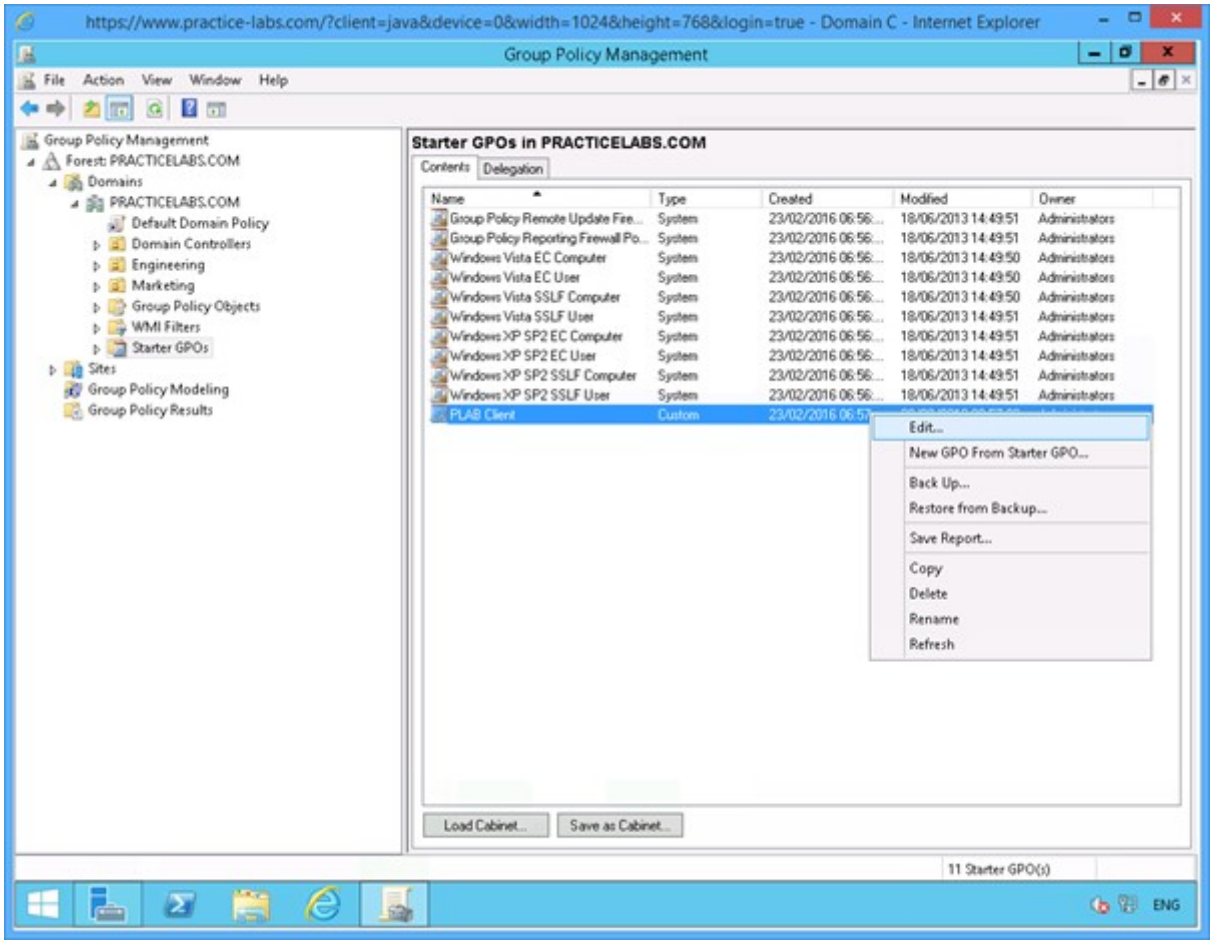
```
PLAB Client
```

Click **OK**.



Step 4

Right-click **PLAB Client** and select **Edit**...

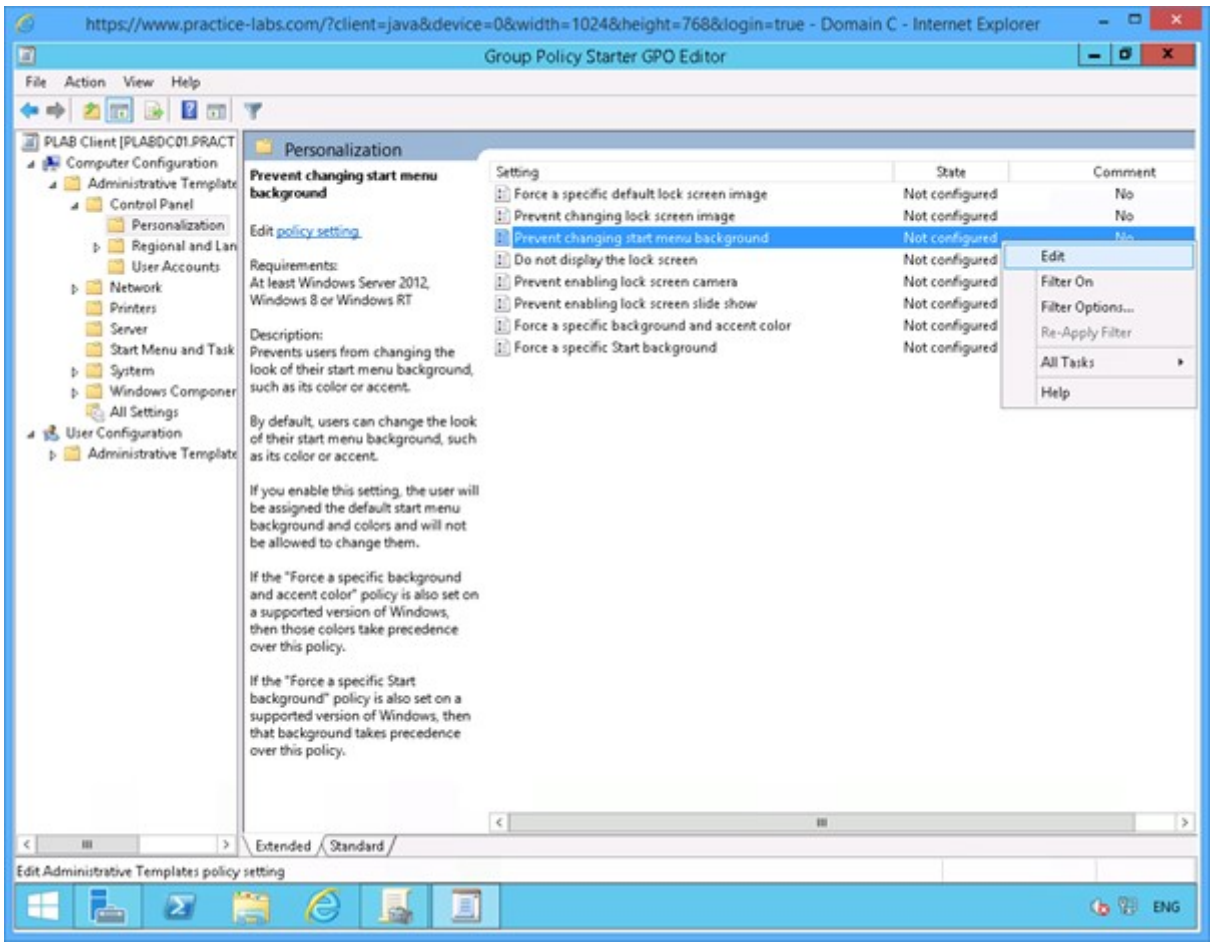


Step 5

The **Group Policy Starter GPO Editor** window is displayed.

Expand **Computer Configuration** > **Administrative Templates** > **Control Panel** and click **Personalization** folder.

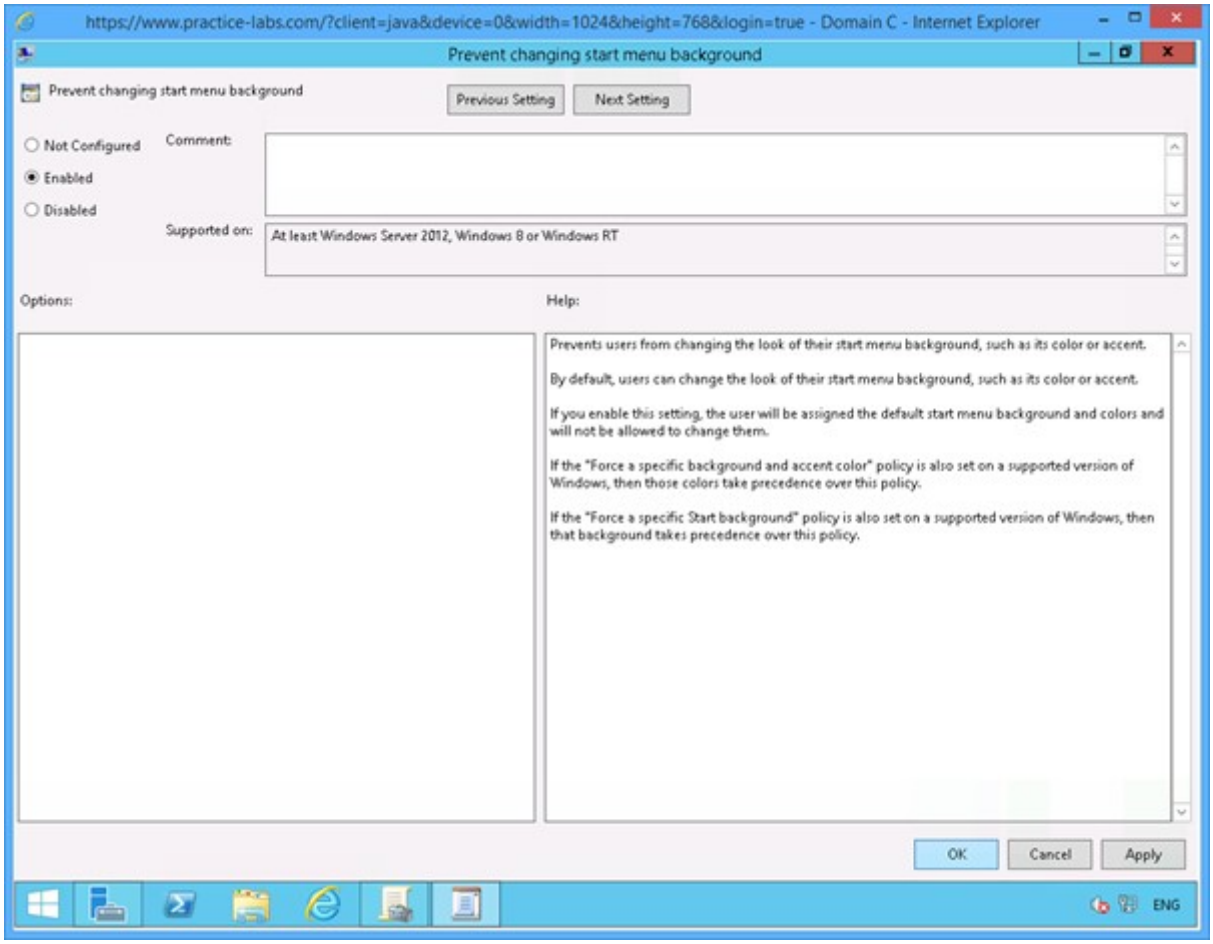
On the details pane, right-click **Prevent changing start menu background** and select **Edit**.



Step 6

On the **Prevent changing start menu background** dialog box, select **Enabled**.

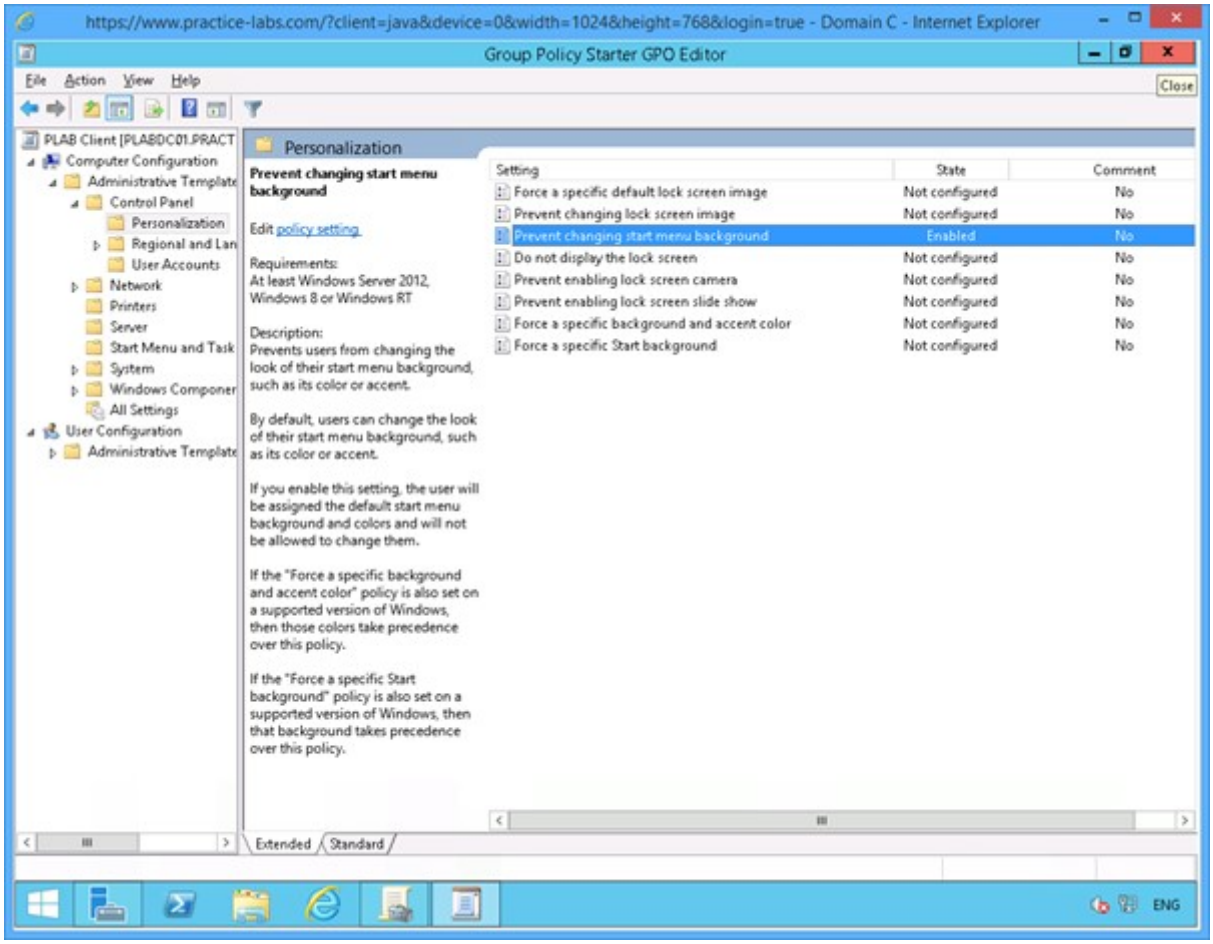
Click **OK**.



Step 7

Note that in the right pane, the policy is now shown as **Enabled**.

Close the **Group Policy Starter GPO Editor** window.

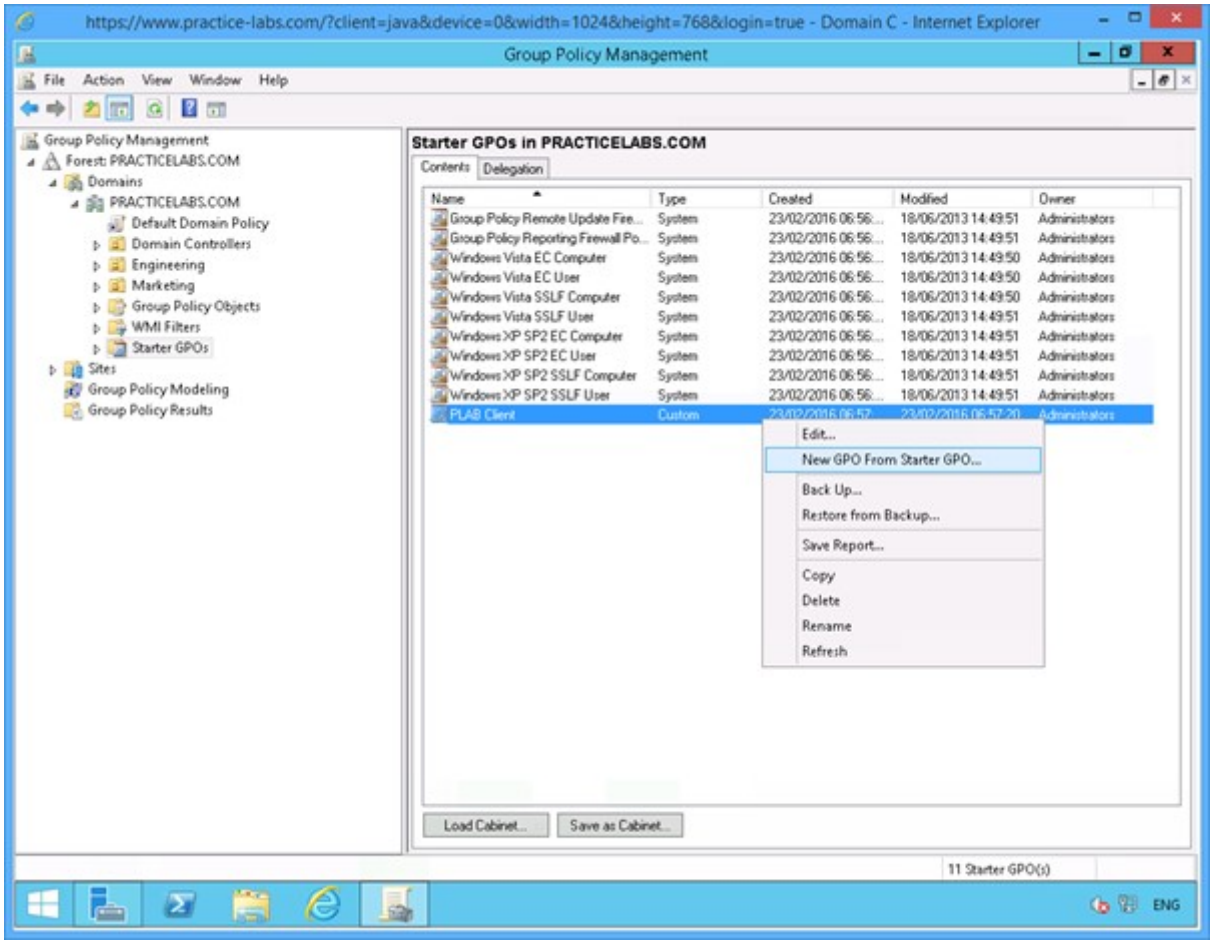


Step 8

The **Group Policy Management** snap-in should be displayed.

You will now create a GPO from the **PLAB Client Starter** GPO.

Right-click **PLAB Client** and select **New GPO from Starter GPO**.



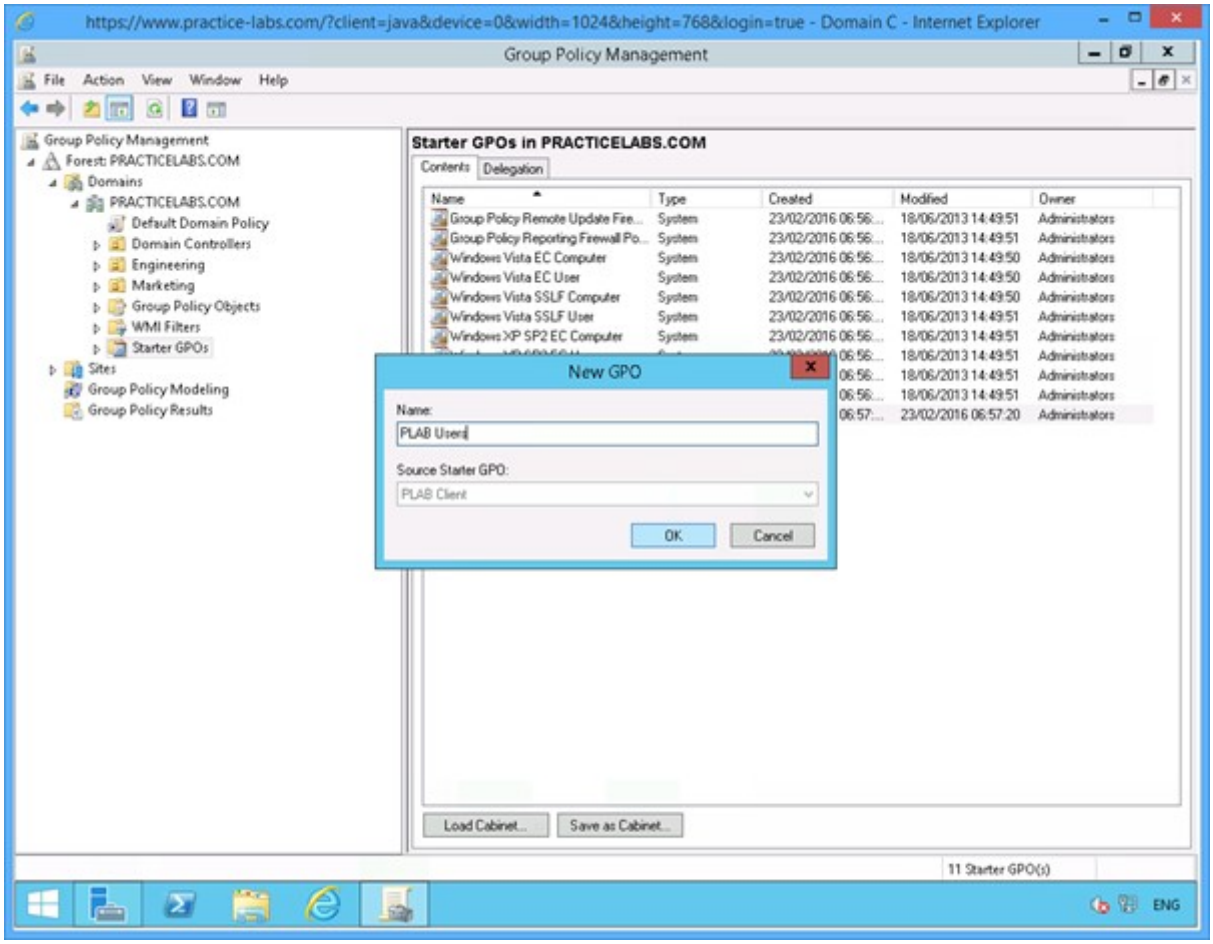
Step 9

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

```
PLAB Users
```

Click **OK**.

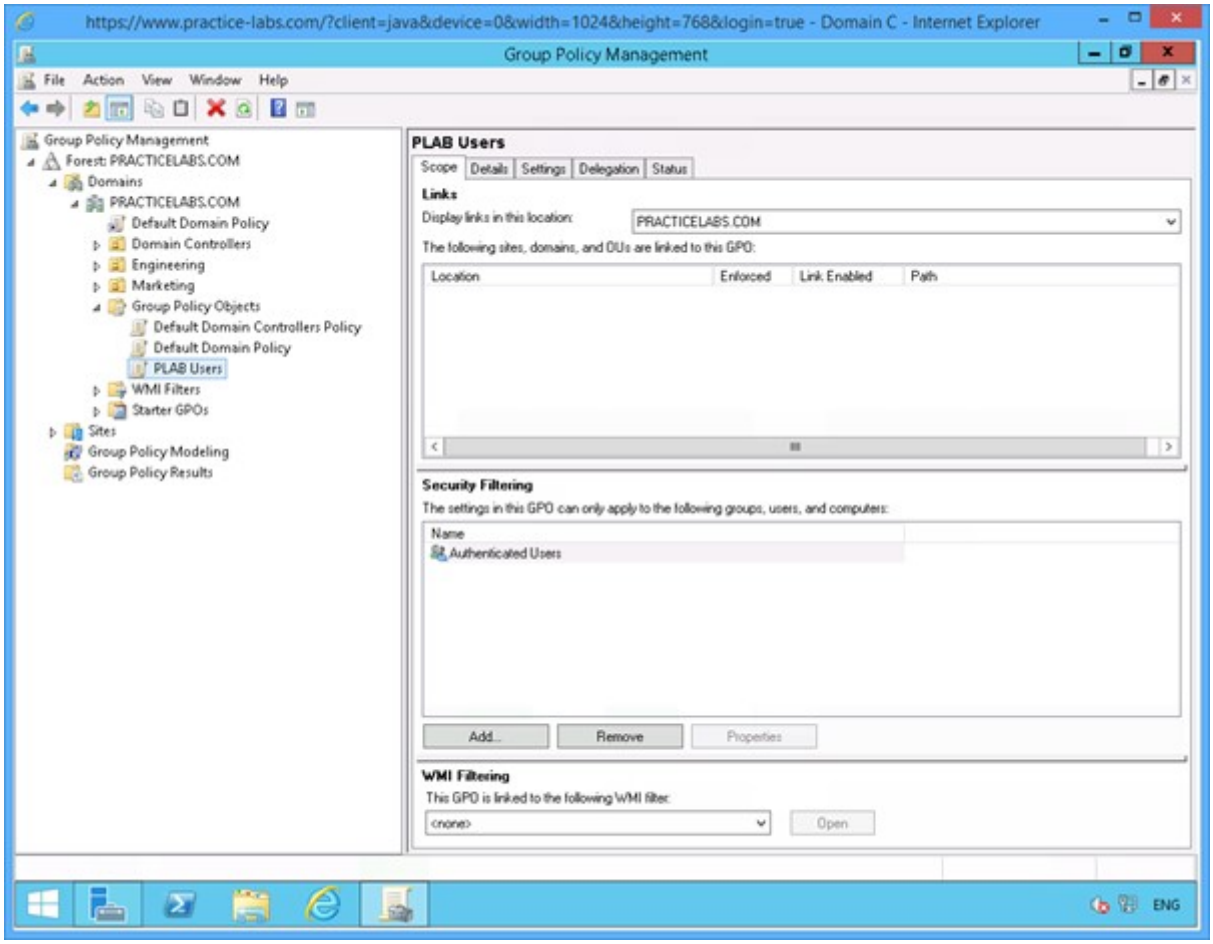
Note that the **Source Starter GPO** is set as **PLAB Client**.



Step 10

Navigate to the **Group Policy Object** node and expand it.

Note that **PLAB Users** GPO is created.



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

Task 2 - Copying Starter GPOs

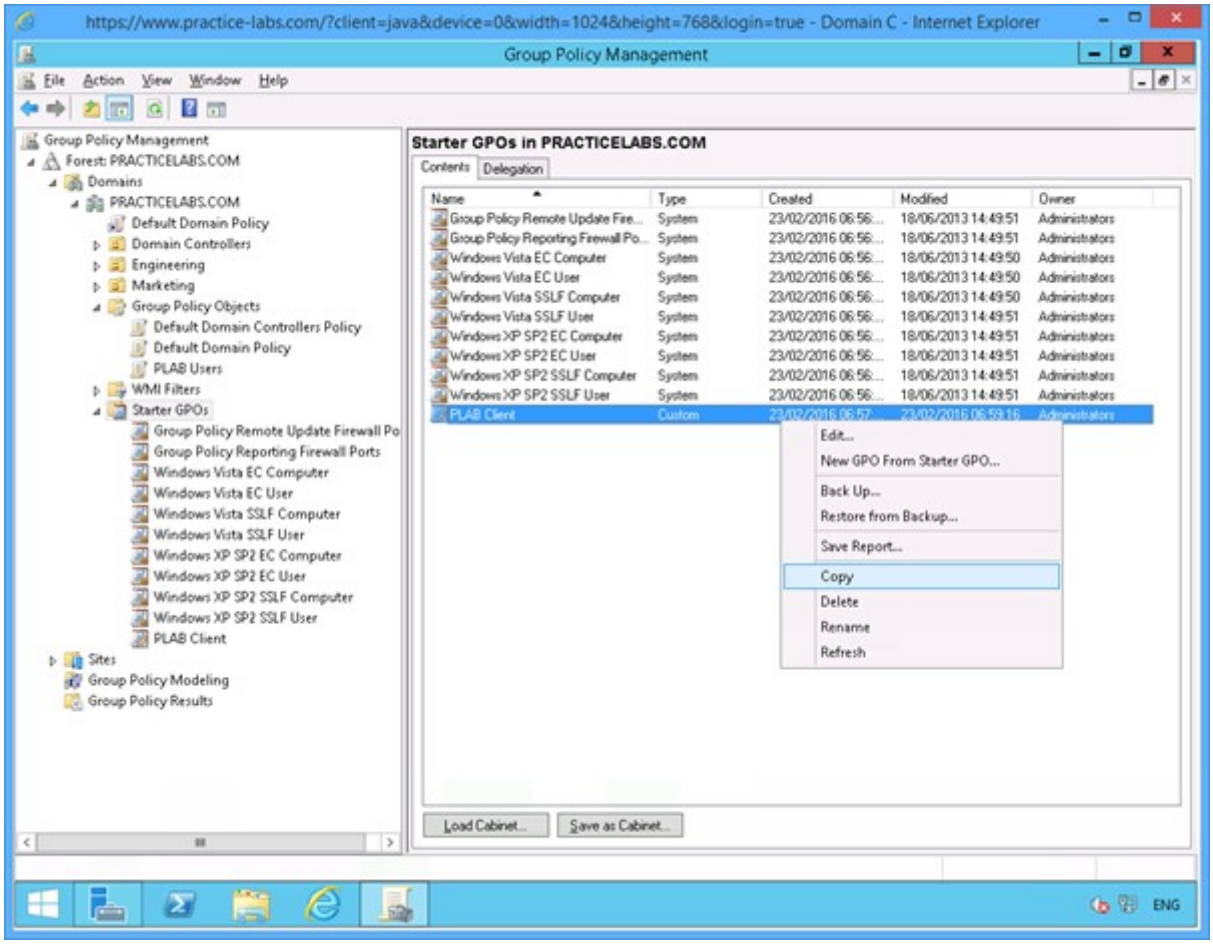
If you need to replicate the settings of one Starter GPO to another, you can make a copy of the Starter GPO rather than creating a new Starter GPO.

To copy a starter GPO, perform the accompanying steps:

Step 1

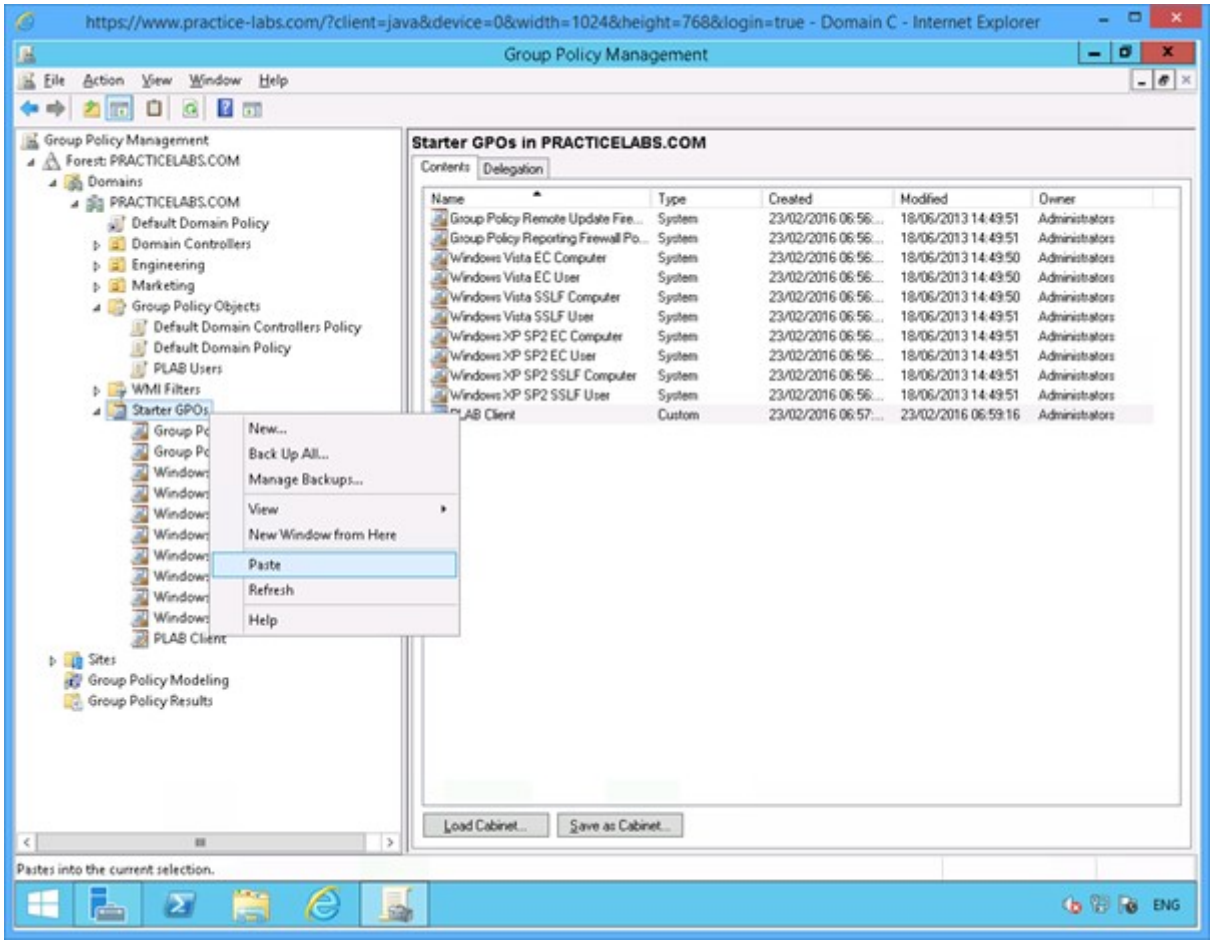
On **PLABDC01** device, the **Group Policy Management** console is open.

Click **Starter GPOs** node, right-click the **PLAB Client** Starter GPO and select **Copy**.



Step 2

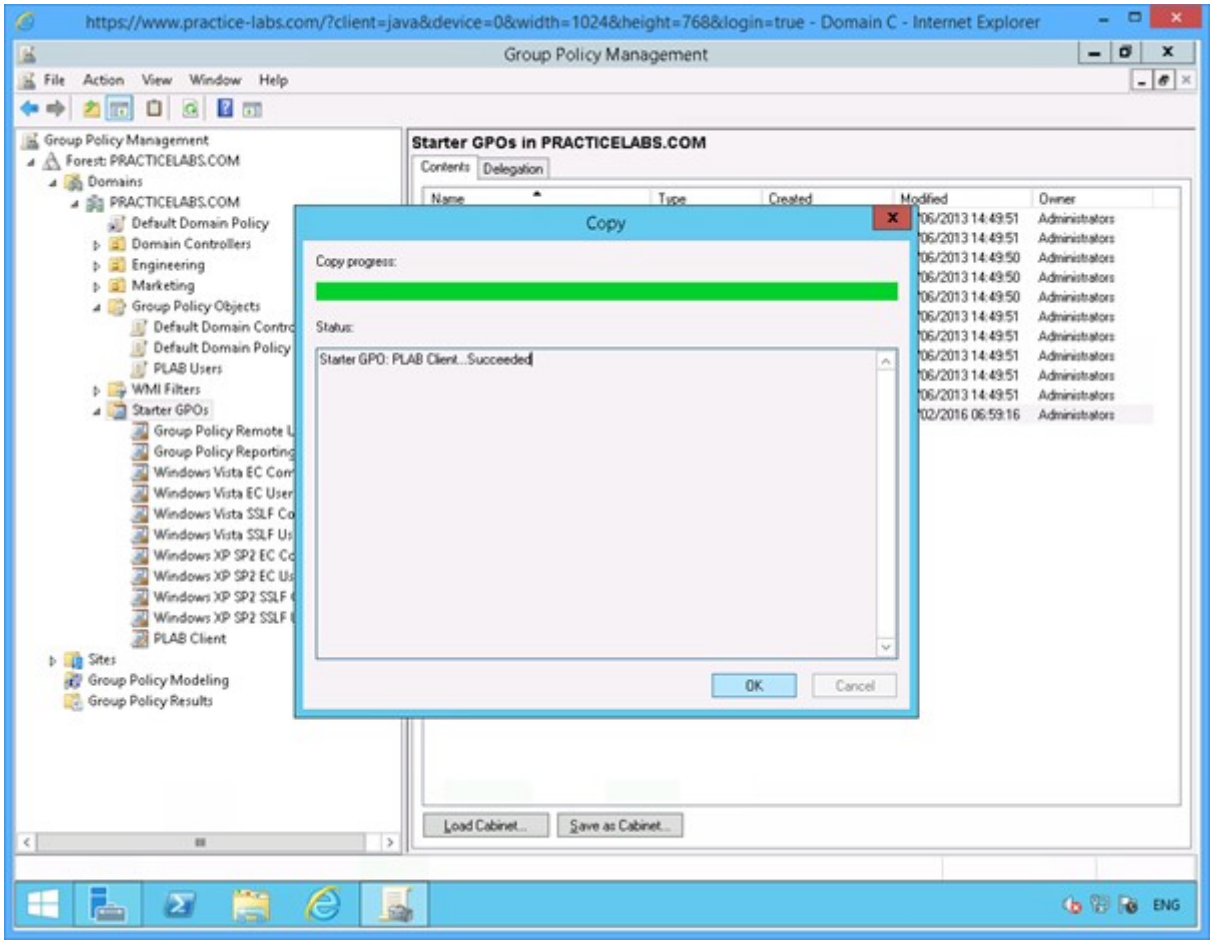
In the left pane, right-click the **Starter GPOs** node and select **Paste**.



Step 3

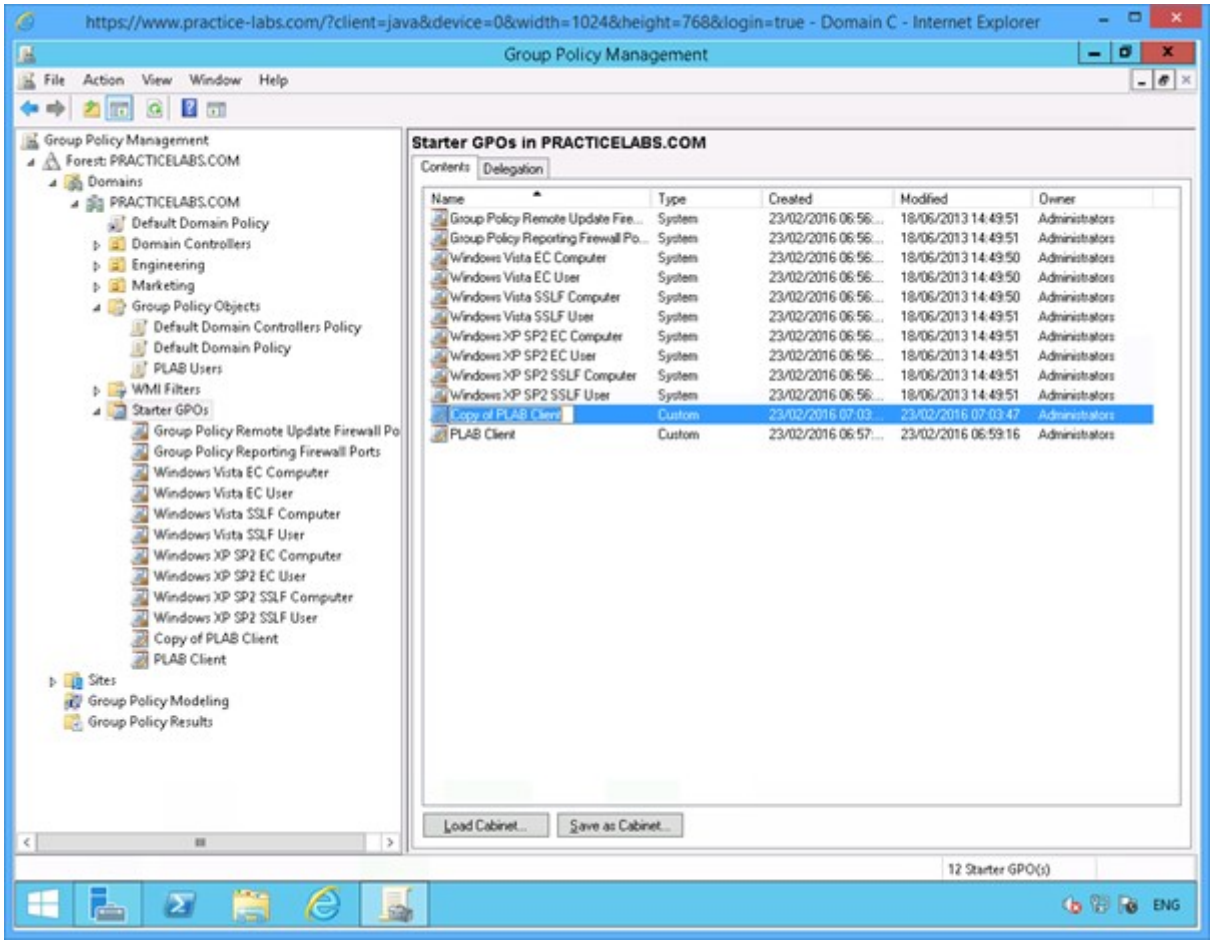
The **Copy** dialog box is displayed. It shows the copy progress of the Starter GPO.

Click **OK** to close the **Copy** dialog box.



Step 4

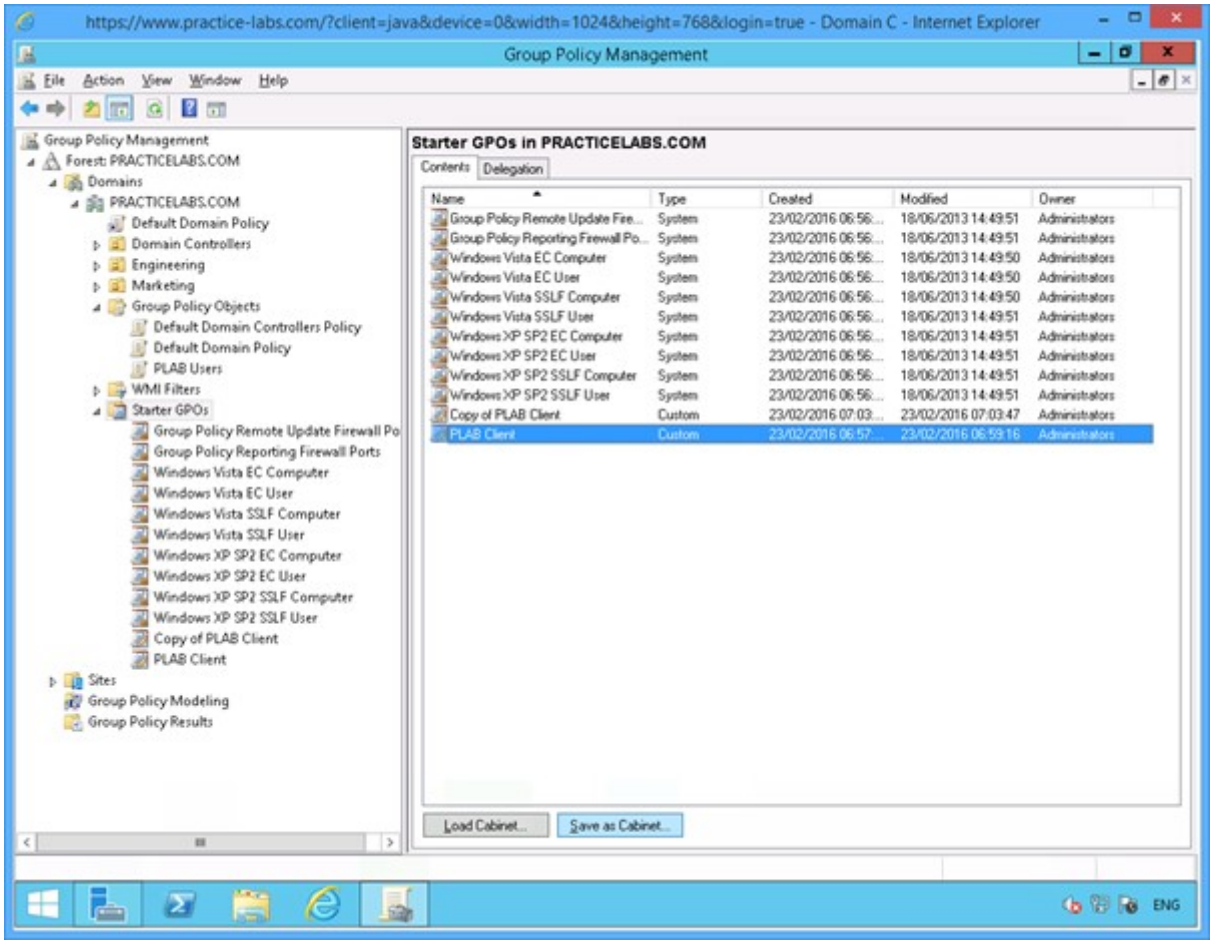
Note that in the right pane, a new Starter GPO with the name **Copy of PLAB Client** appears.



Step 5

You can also export and import the Starter GPO.

Select **PLAB Client** and click **Save as Cabinet** button at the bottom of the right pane.

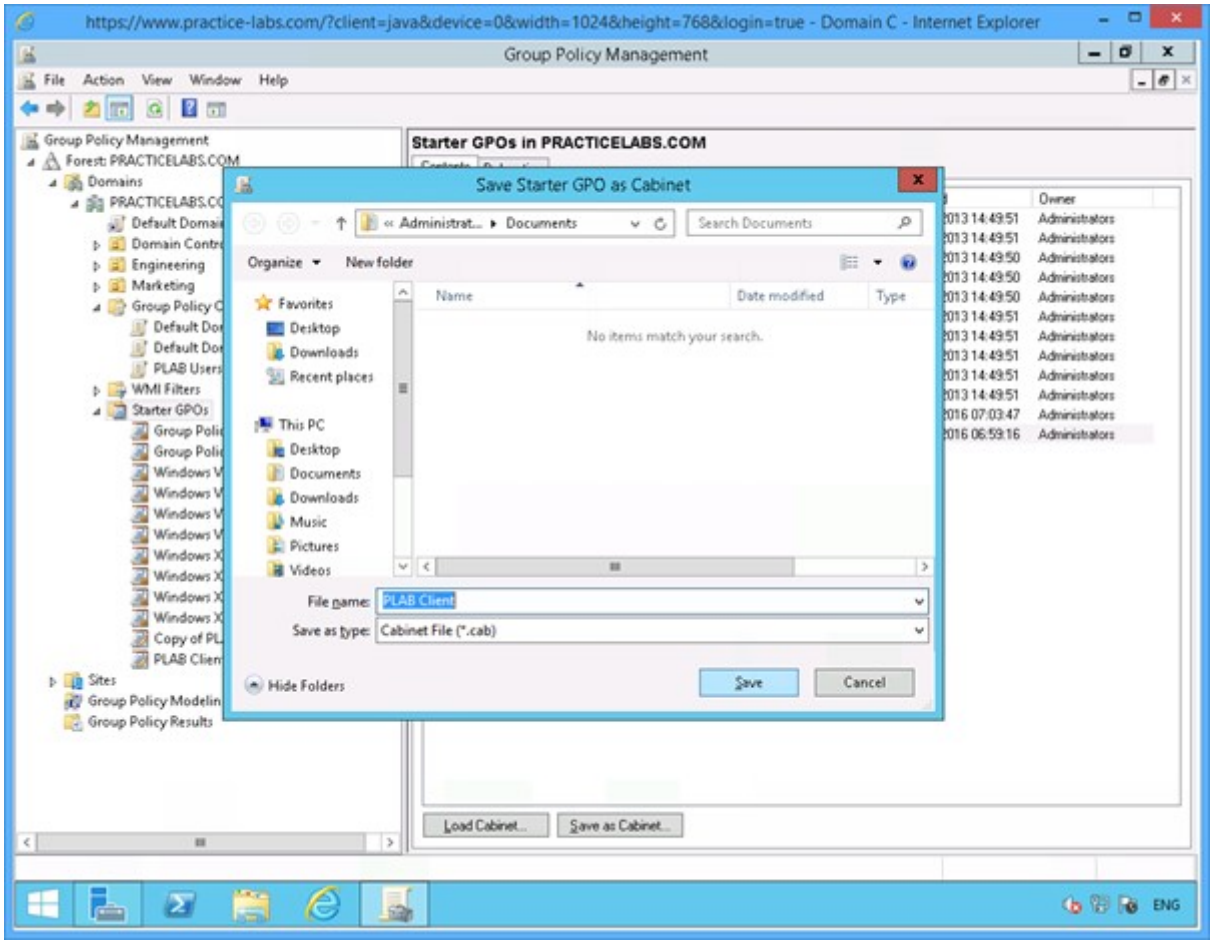


Step 6

The **Save Starter GPO as Cabinet** dialog box is displayed.

The default name **PLAB Client** is entered in the **File name** text box.

Click **Save** and remember the folder where you are saving the cabinet file.

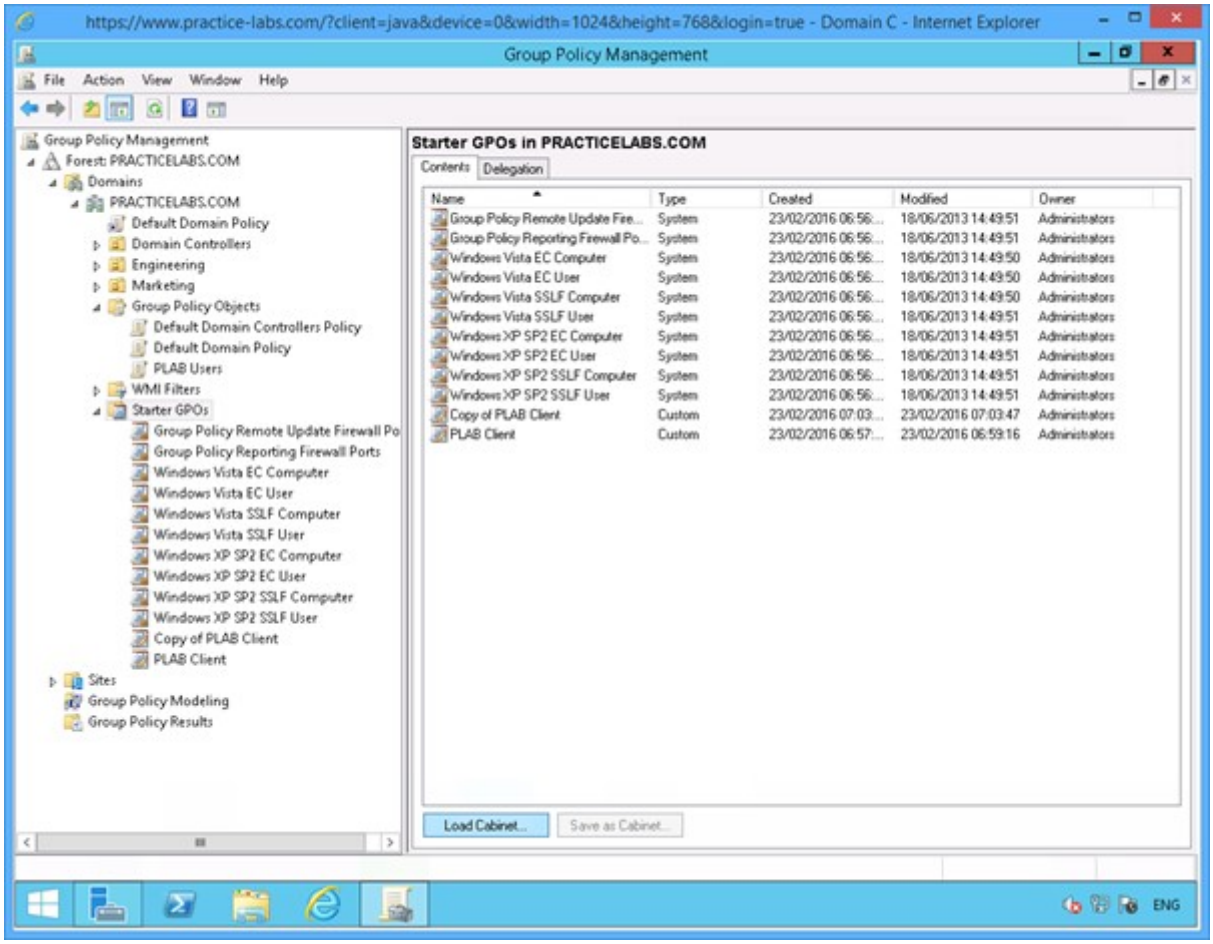


Step 7

Now, you will import the Starter GPO that you exported as the cabinet file.

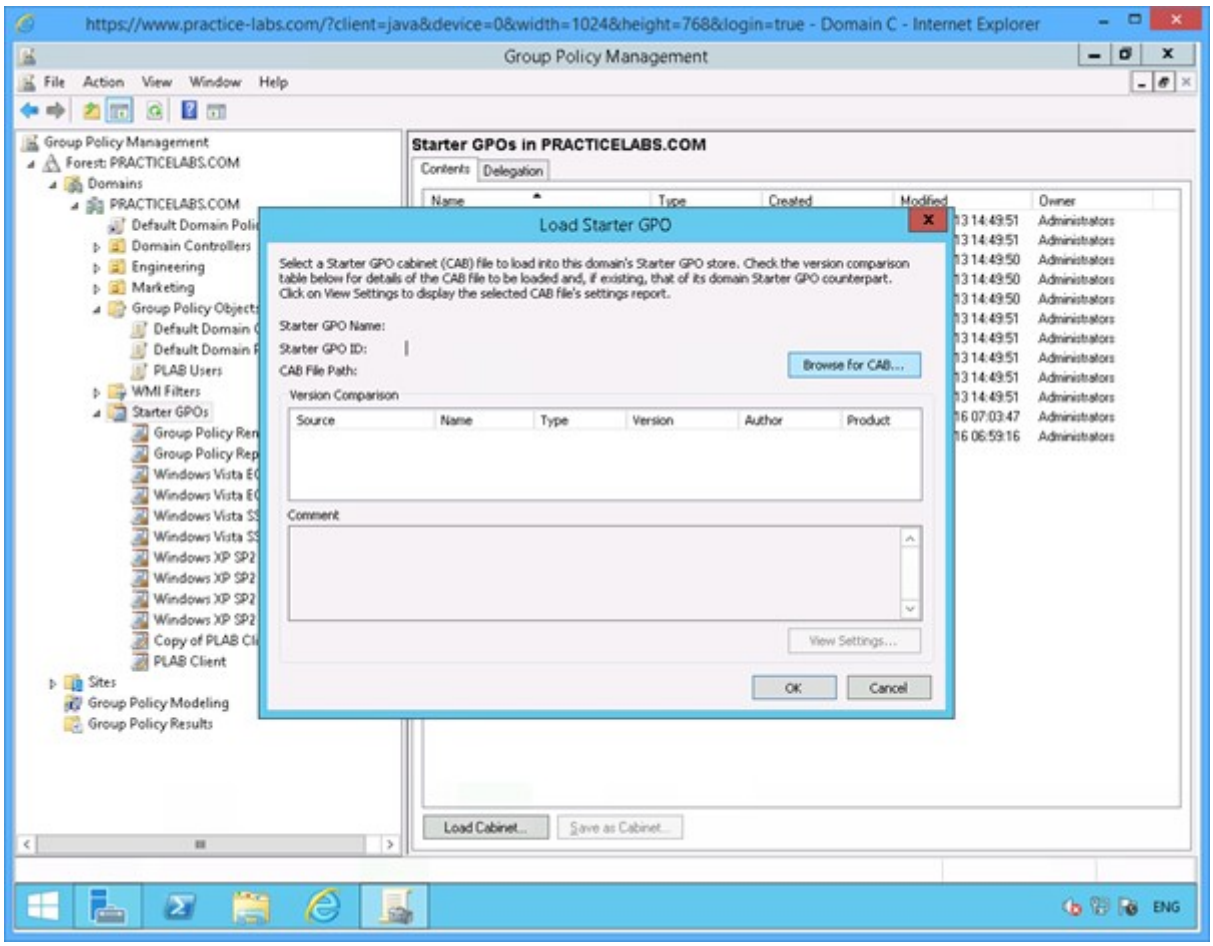
Select the **Starter GPOs** node in the left pane if already not selected.

In the right pane, click **Load Cabinet** at the bottom.



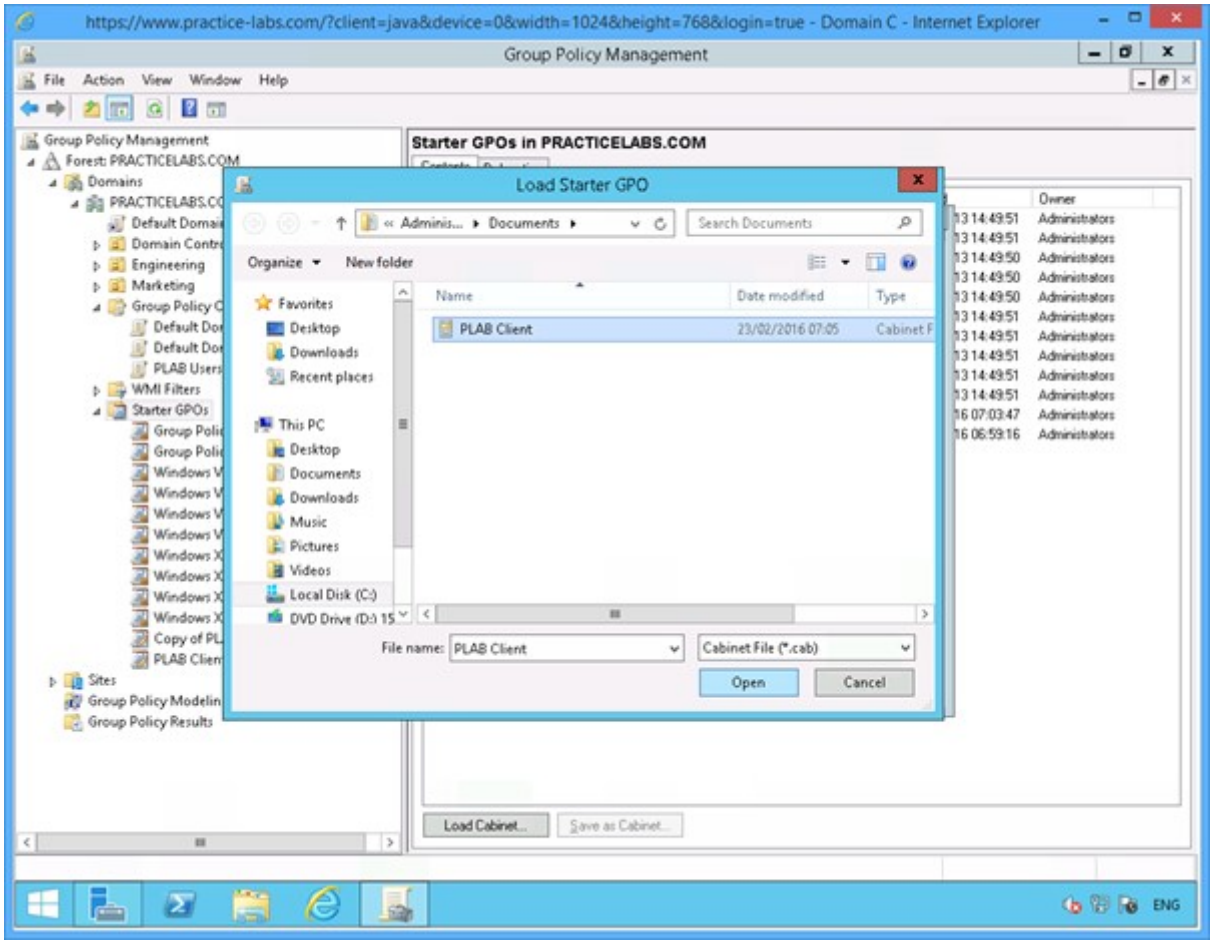
Step 8

The **Load Starter GPO** dialog box, click **Browse for CAB**...



Step 9

On the **Load Starter GPO** dialog box, select **PLAB Client** and click **Open**.

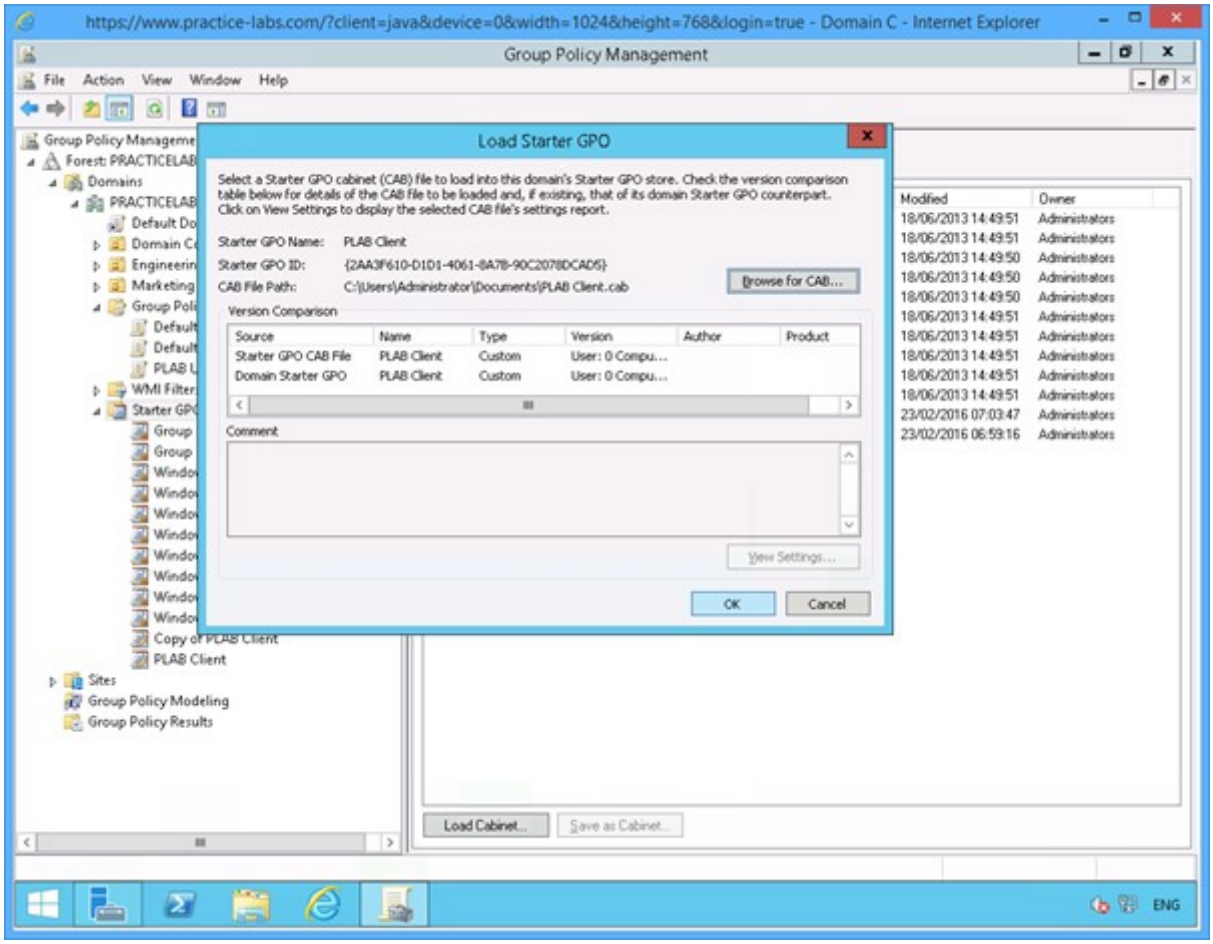


Step 10

Note that the cabinet file is now loaded in the **Load Starter GPO** dialog box.

A version comparison is displayed.

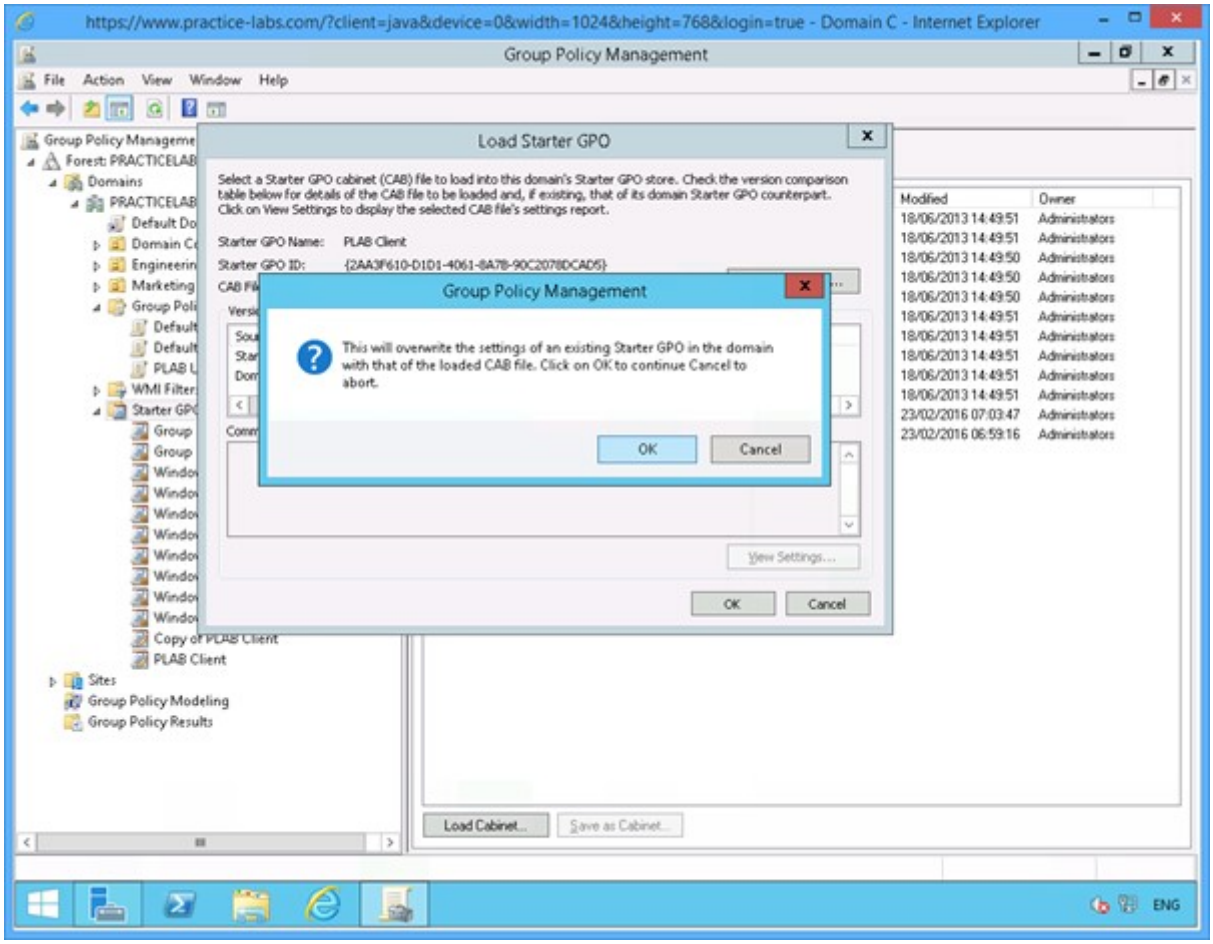
Click **OK**.



Step 11

Since you are importing the Starter GPO on the same domain controller, you will be prompted with a message that you are about to overwrite the existing Starter GPO.

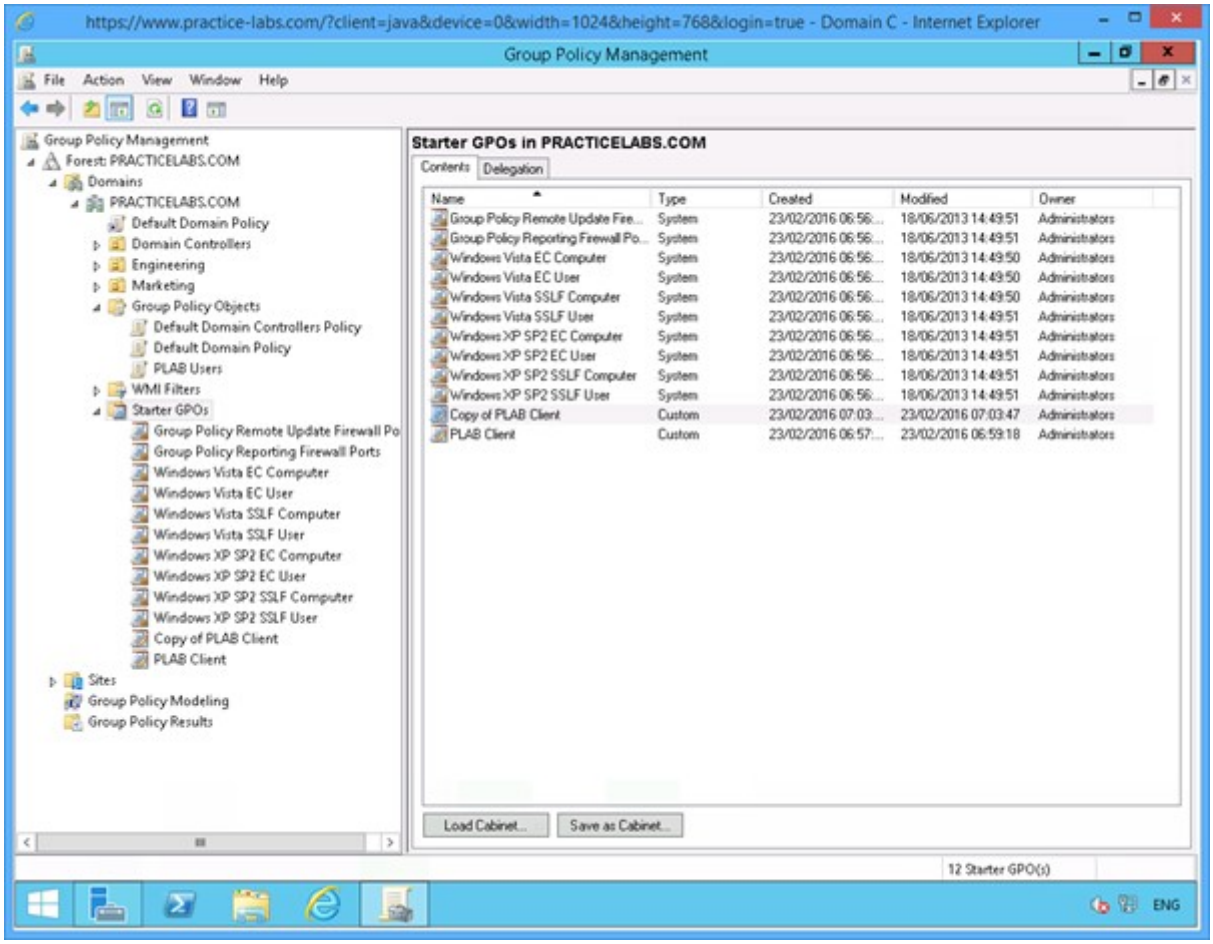
Click **OK**.



Step 12

The Starter GPO, **PLAB Client**, is now imported.

Keep **Group Policy Management** console open for the next activity.



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

---

Exercise 3 - Configure GPO links

In this exercise, you will configure group policy object links for organizational units and the Windows domain.

Please refer to your course material or use your favourite search engine to research for more information about this topic.

> ***Note:*** *Before starting this task, ensure you have a GPO created with the name PLAB Users. If you have completed the previous tasks in this exercise, then you should have PLAB Users created.*

Task 1 - Configuring Group Policy Links

You can link a GPO to the following objects in Active Directory like Domain, Site and Organizational Units OUs.

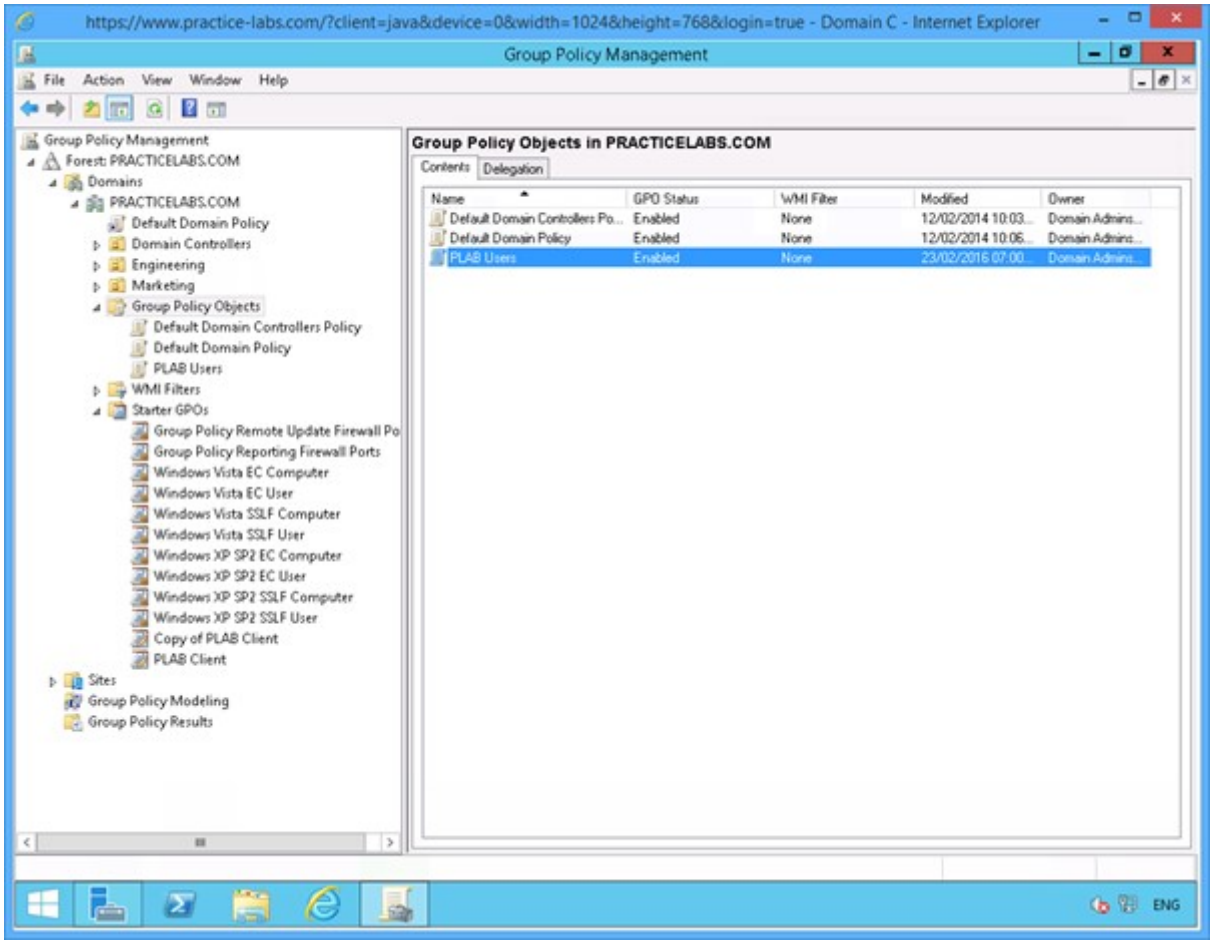
To link a GPO, perform the following steps:

Step 1

On **PLABDC01** device, the **Group Policy Management** console is open.

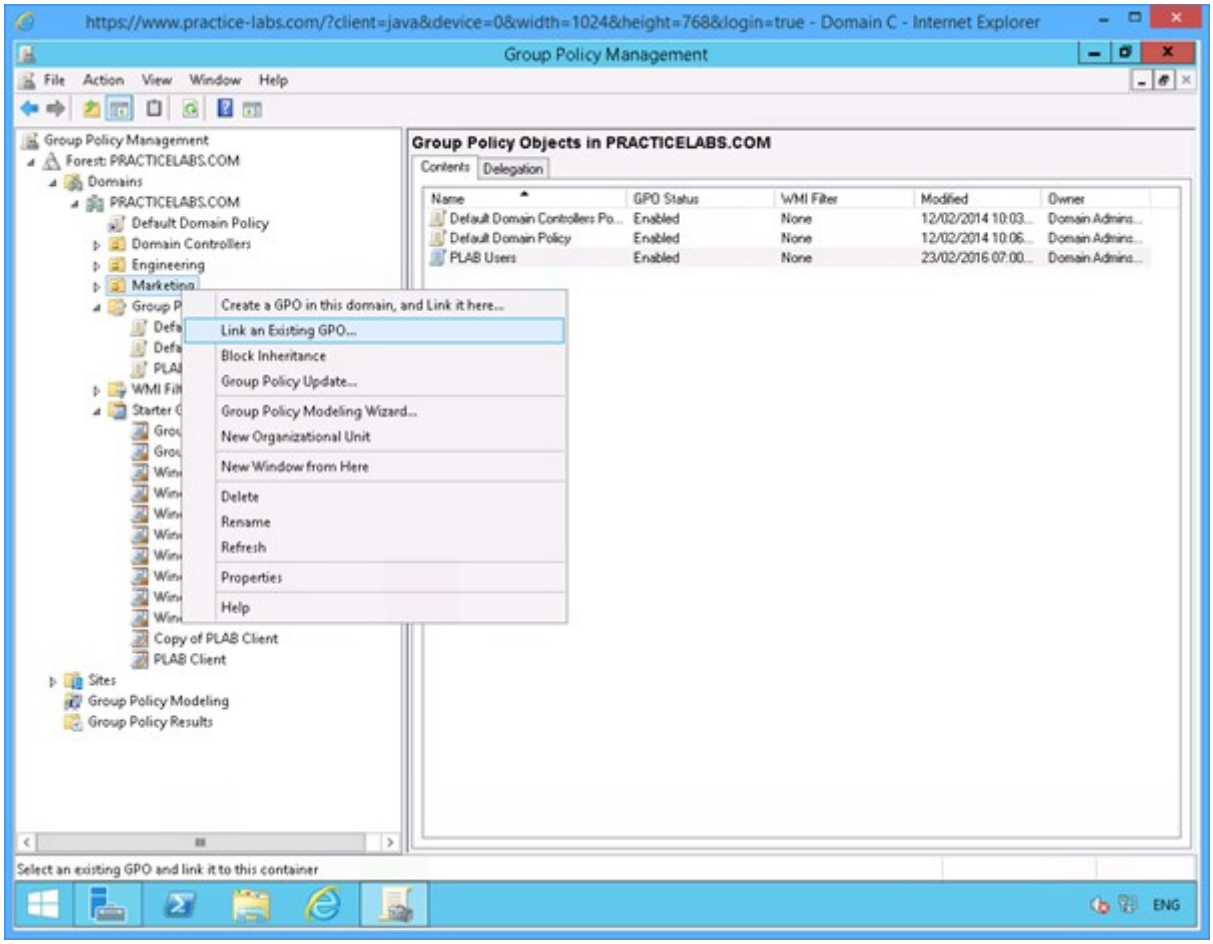
In the left pane, expand **Forest: PRACTICELABS.COM**, expand **Domains**, expand **PRACTICELABS.COM**, and select **Group Policy Objects**.

Note that you have **PLAB Users** GPO created.



Step 2

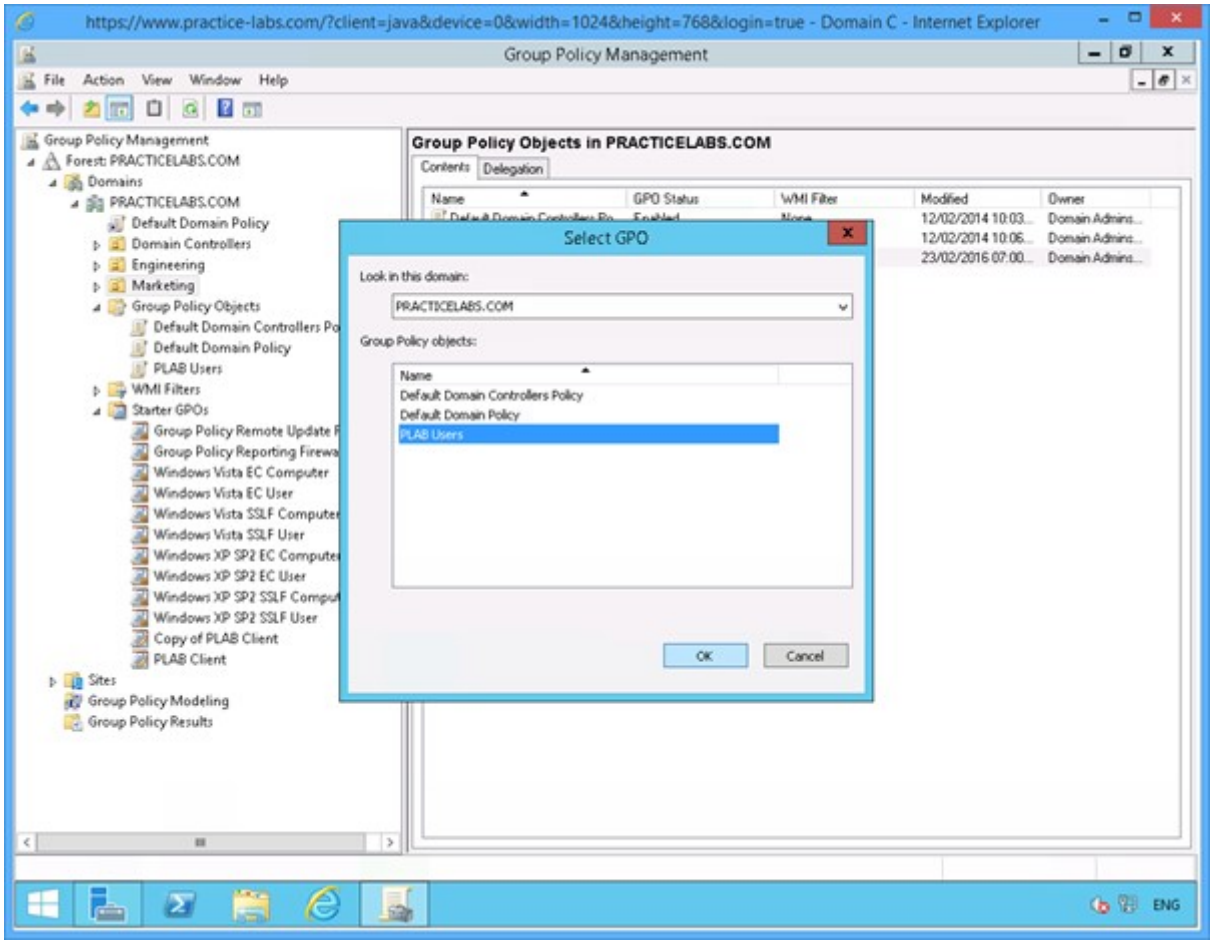
On the left pane, right-click **Marketing** and select **Link an Existing GPO**...



Step 3

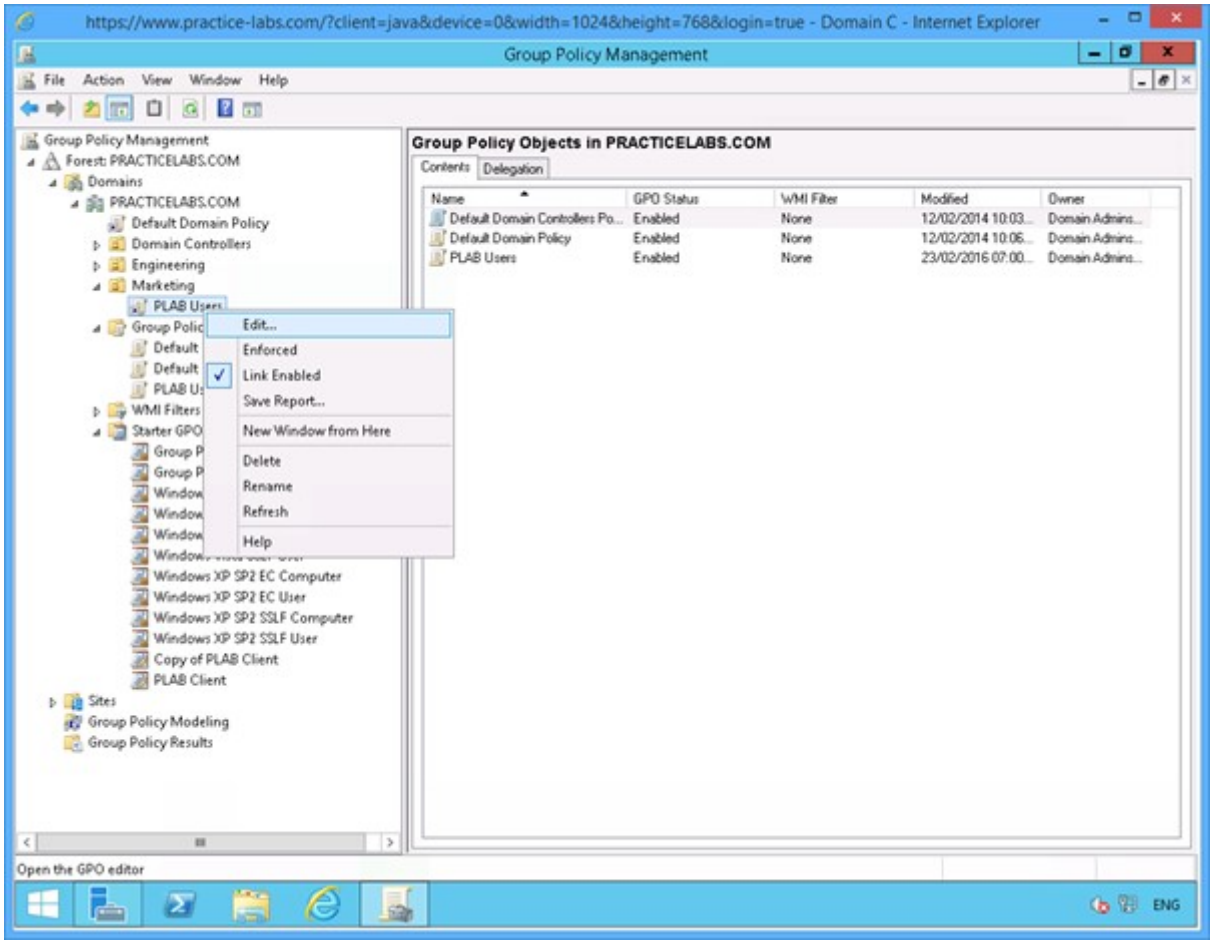
On the **Select GPO** dialog box, click on **PLAB Users.**

Click **OK**.



Step 4

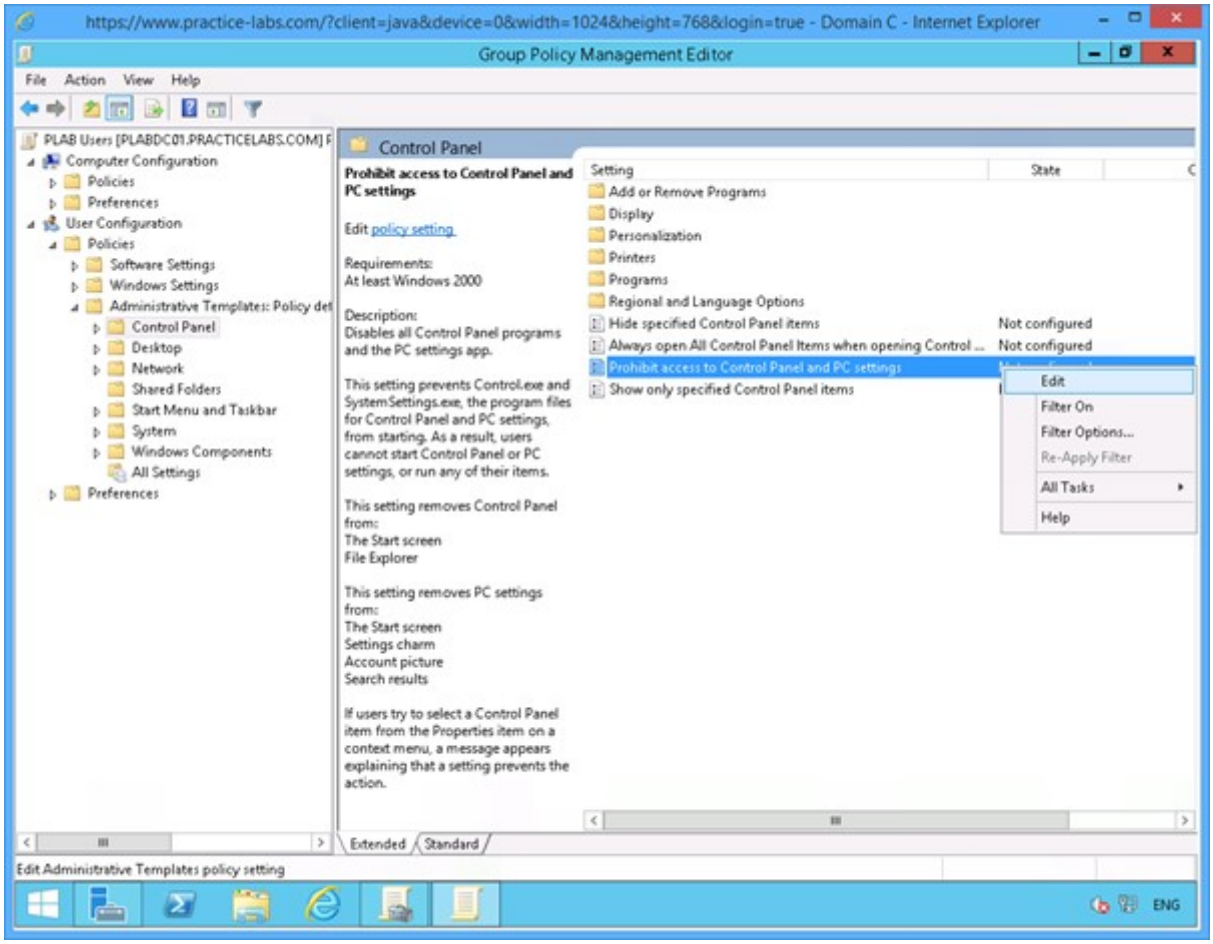
Expand **Marketing** organizational unit and right-click on **PLAB Users** and select **Edit**...



Step 5

On the Group Policy Management Editor window, expand **User Configuration** > **Policies** > **Administrative Templates: Policy Definitions** and click **Control Panel**.

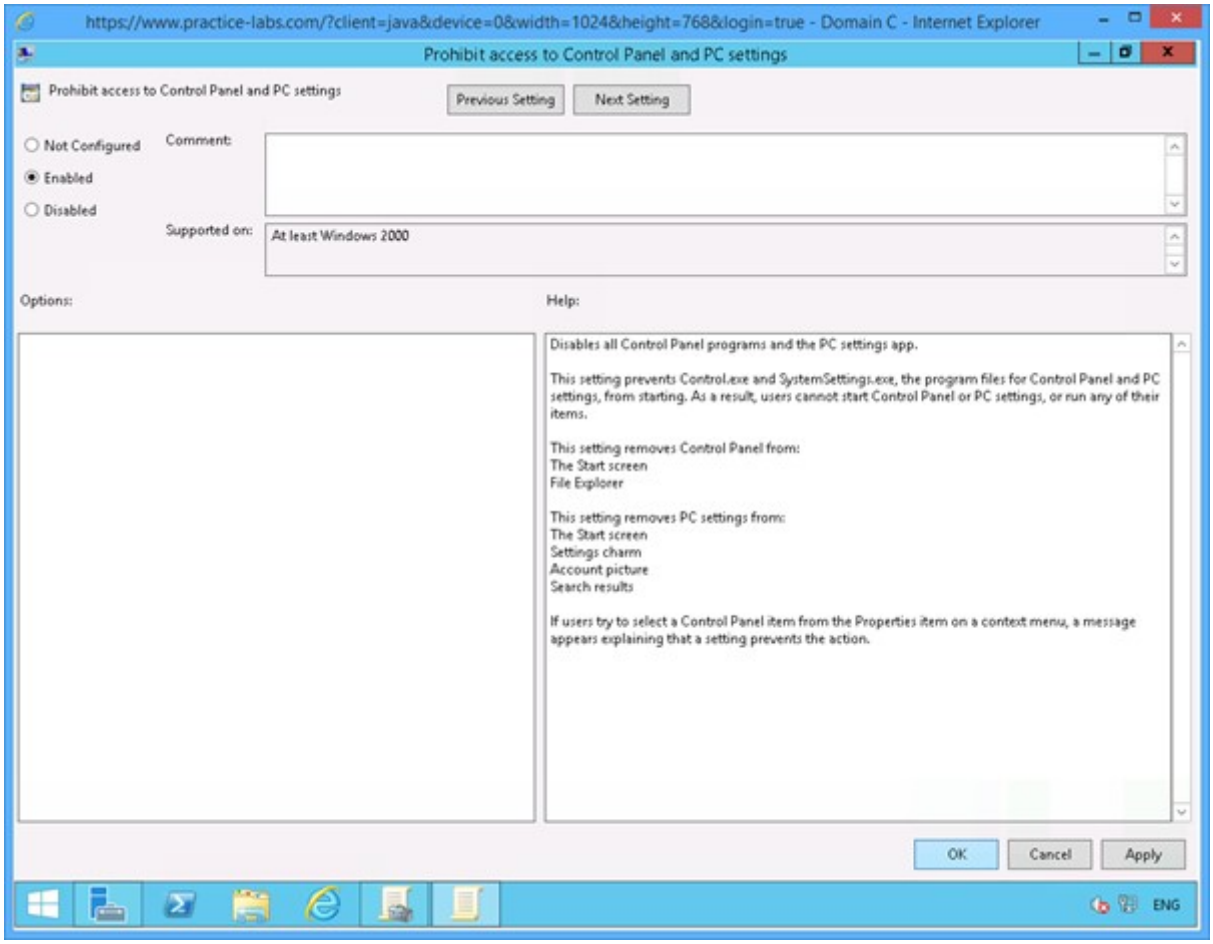
Right-click on **Prohibit access to Control Panel and PC settings** and select **Edit**...



Step 6

On the **Prohibit access to Control Panel and PC settings** dialog box, select **Enabled**.

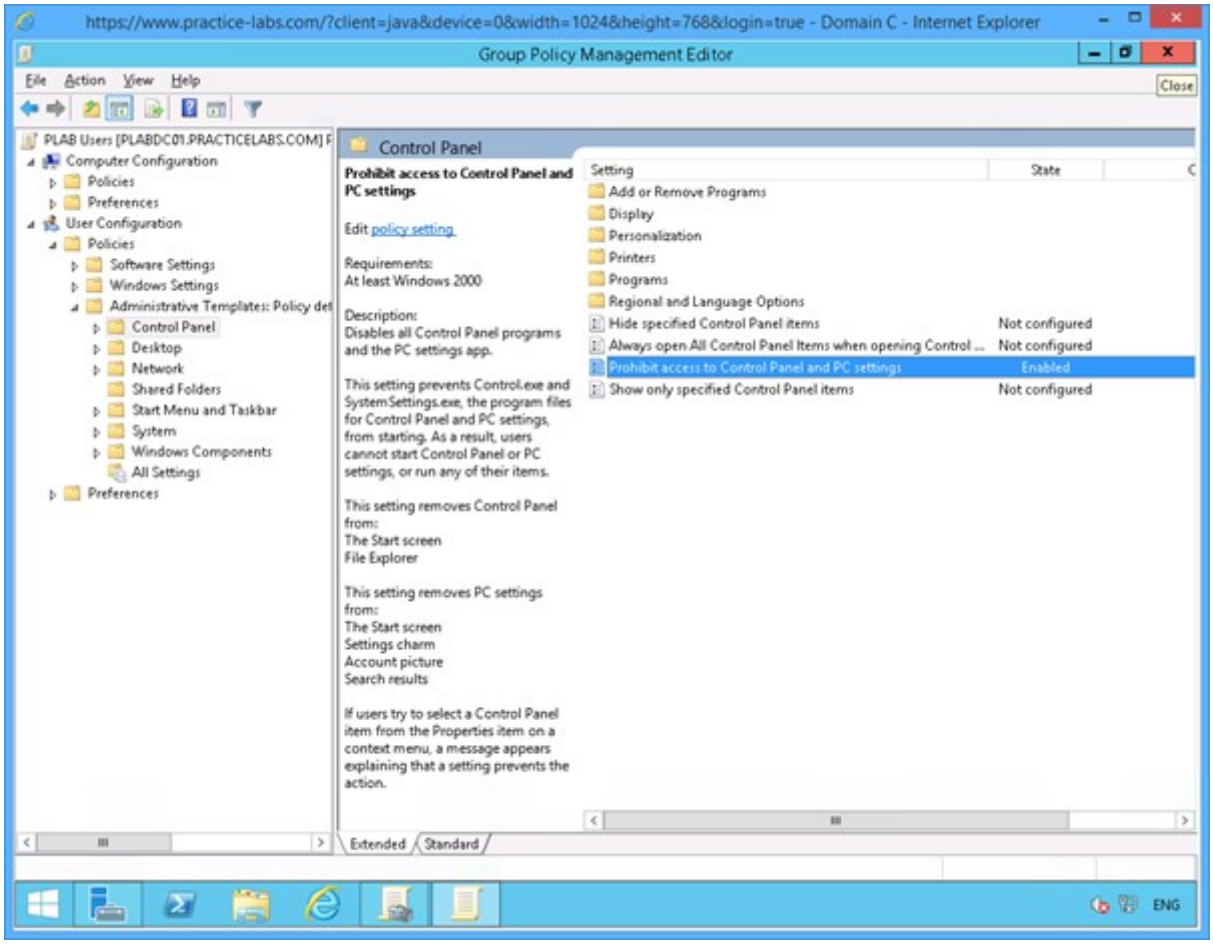
Click **OK**.



Step 7

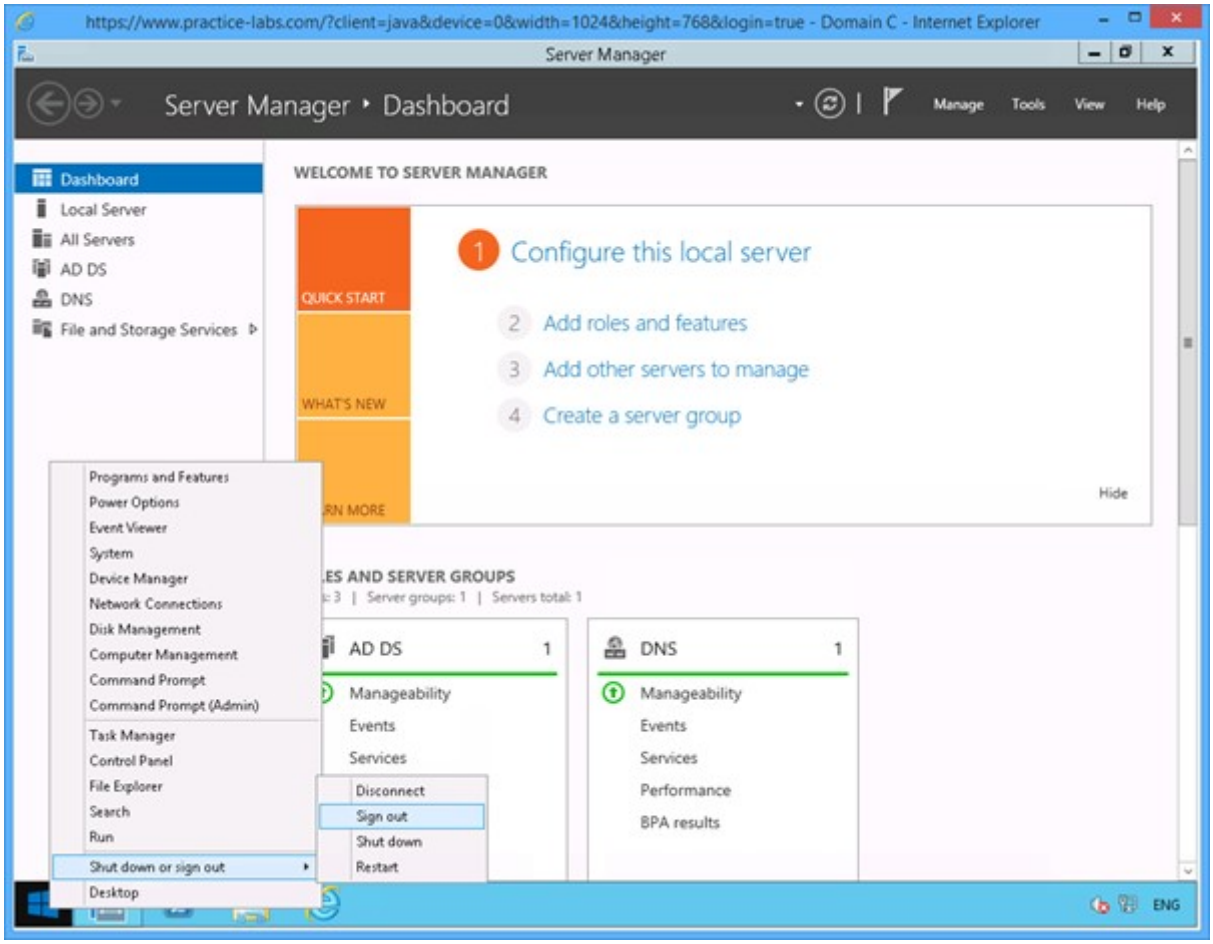
Close **Group Policy Management Editor** window.

Similarly, close **Group Policy Management Console** window.



Step 8

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



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

Task 2 - Verify GPOs Restrictions Client

You will now verify that the control panel restrictions will apply to users located in the Marketing OU.

First, you will need to disable automatic login to the devices in the lab, so that you can sign on to the device using a re

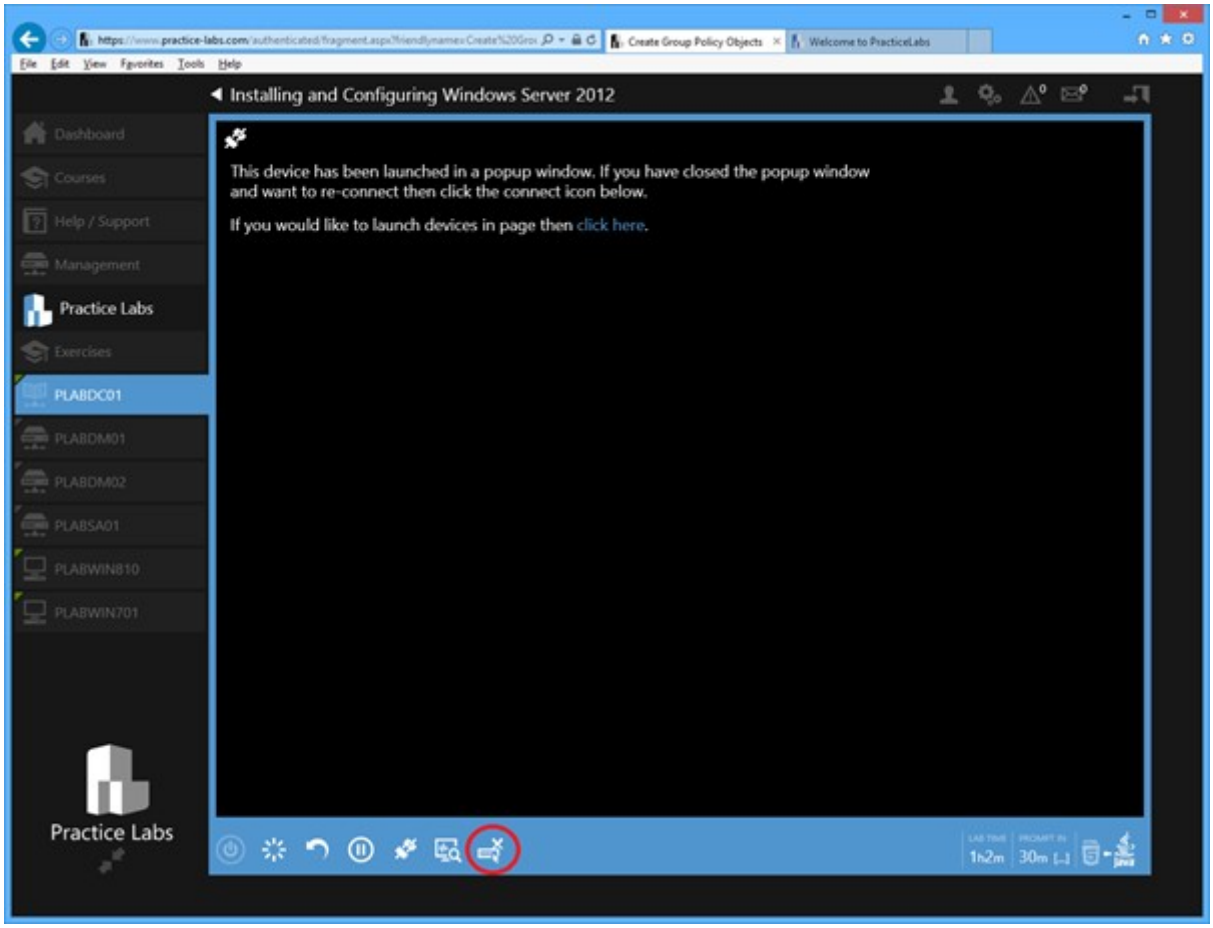
To verify if the GPO settings are applied to a user, perform the following steps:

Step 1

Access the **Practice Labs** web application.

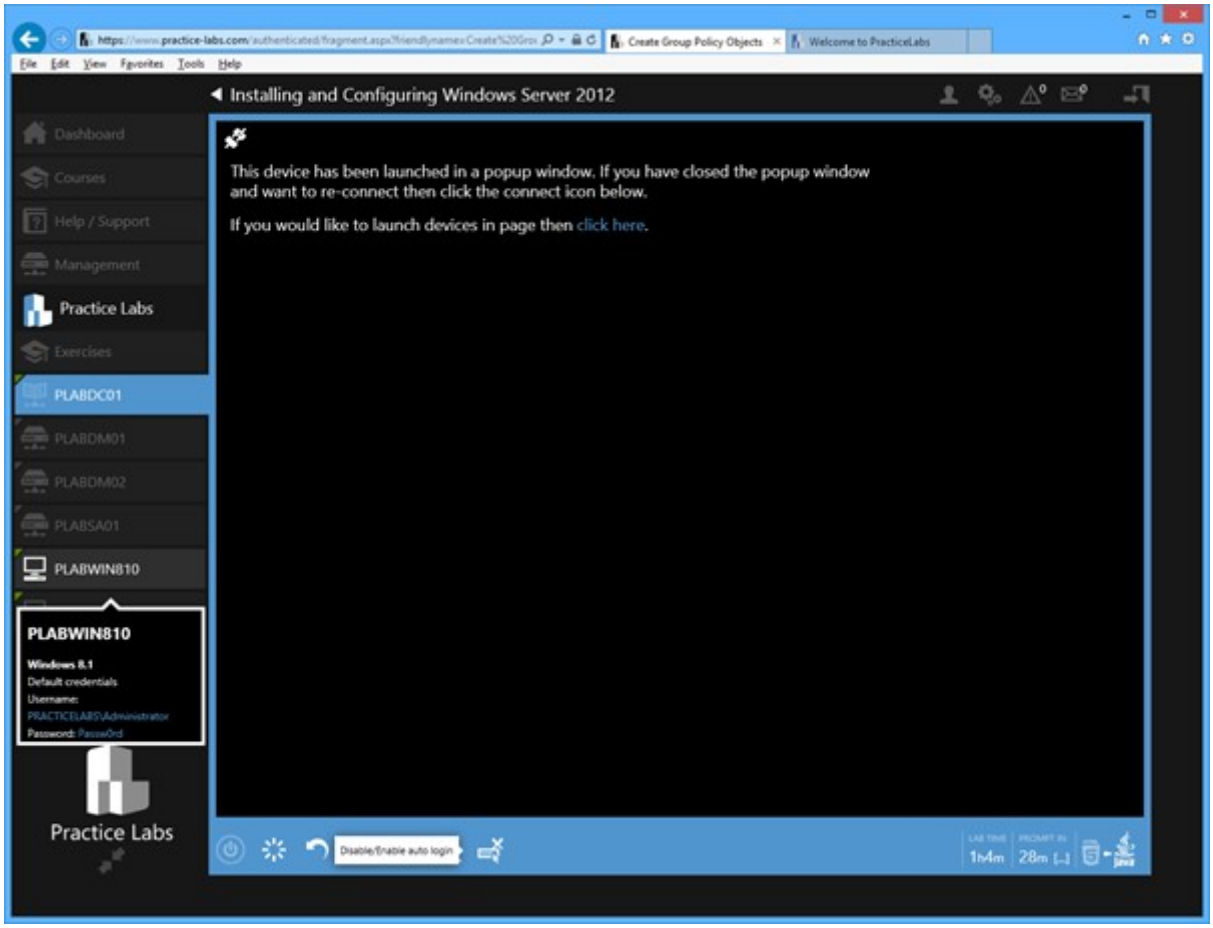
Click **Disable/Enable Auto Login** button.

Verify that **X** (cross) icon is displayed.



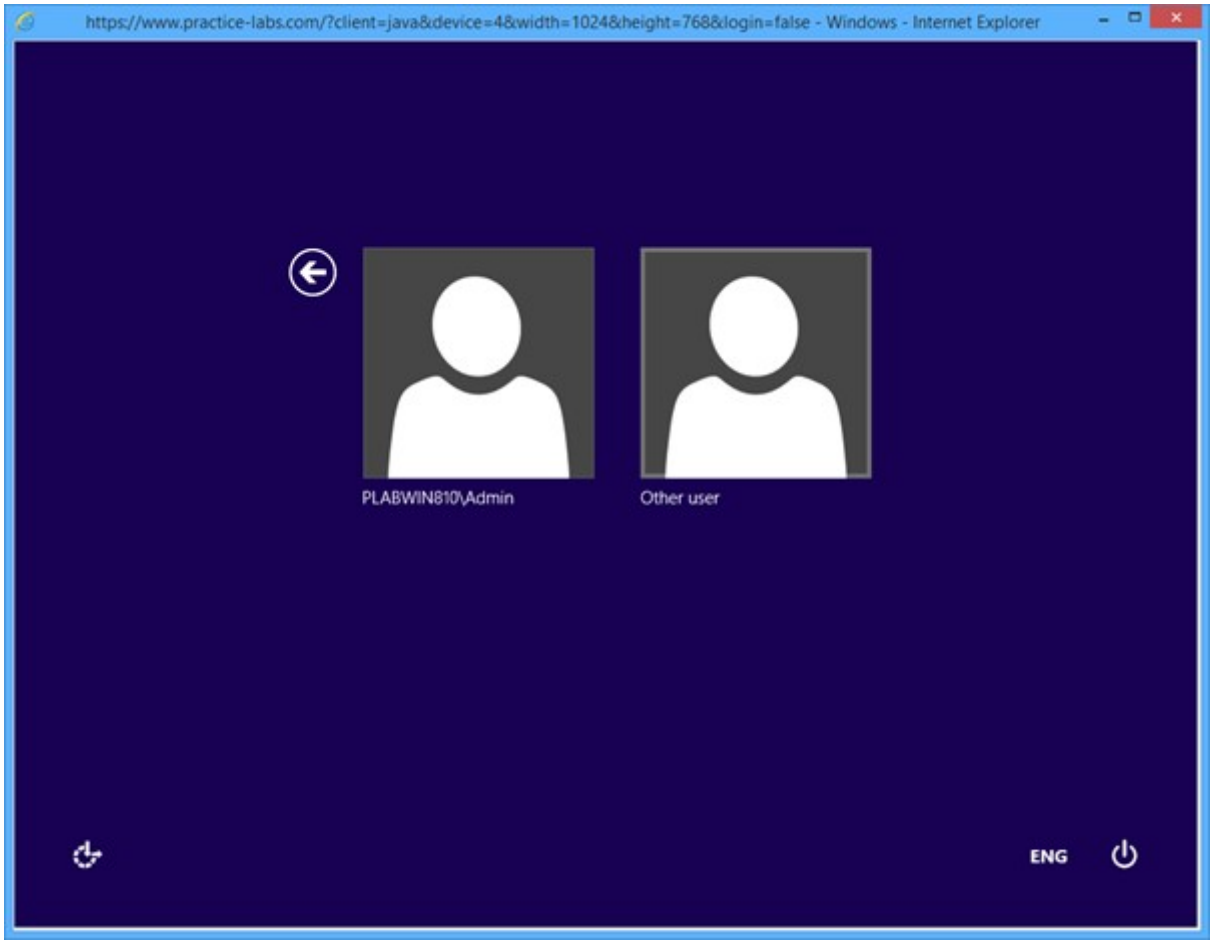
Step 2

Connect to **PLABWIN810** device.



Step 3

On the sign on page, click **Other user**.



Step 4

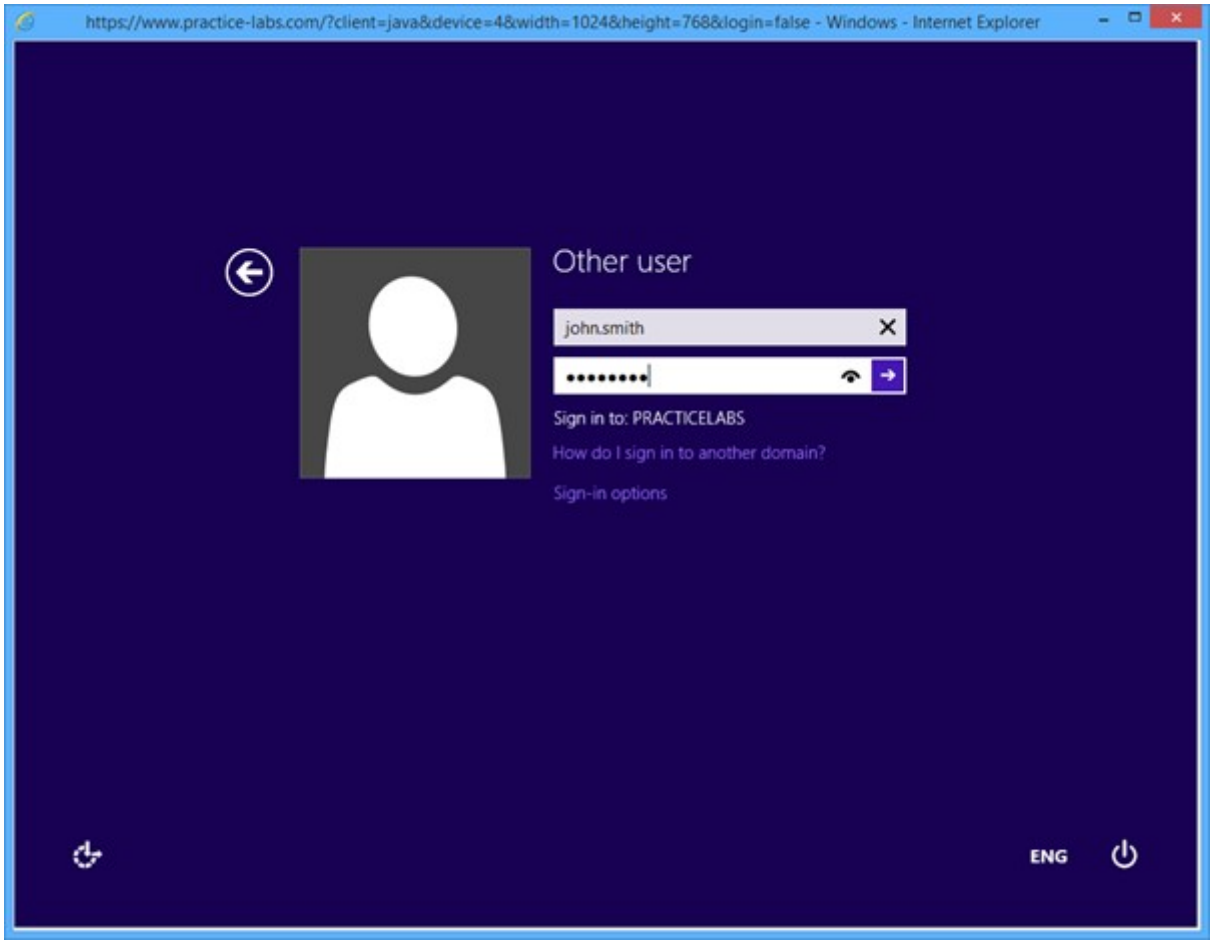
On the **User name** box, type:

```
john.smith
```

On the **Password** text box, type:

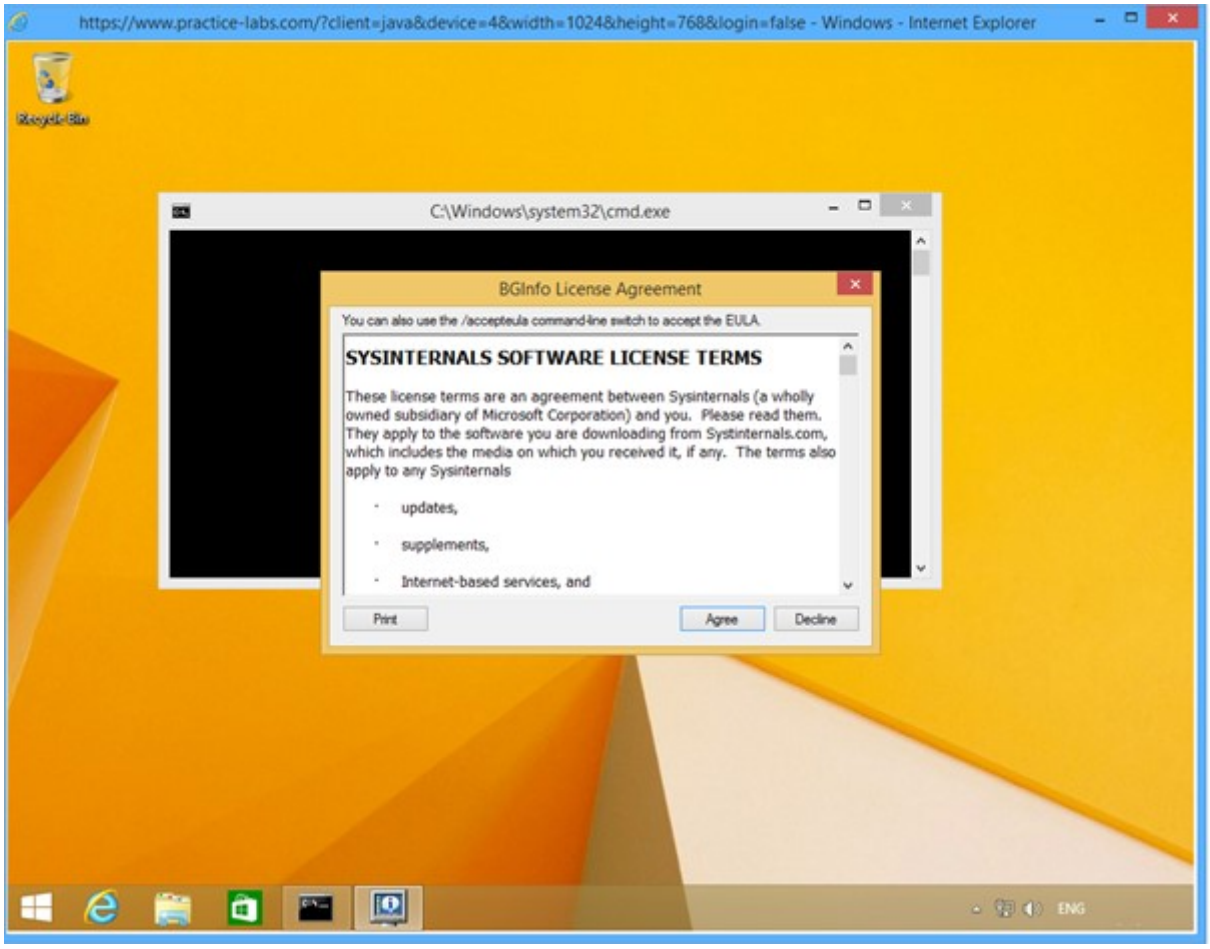
```
Passw0rd
```

Press **Enter**.



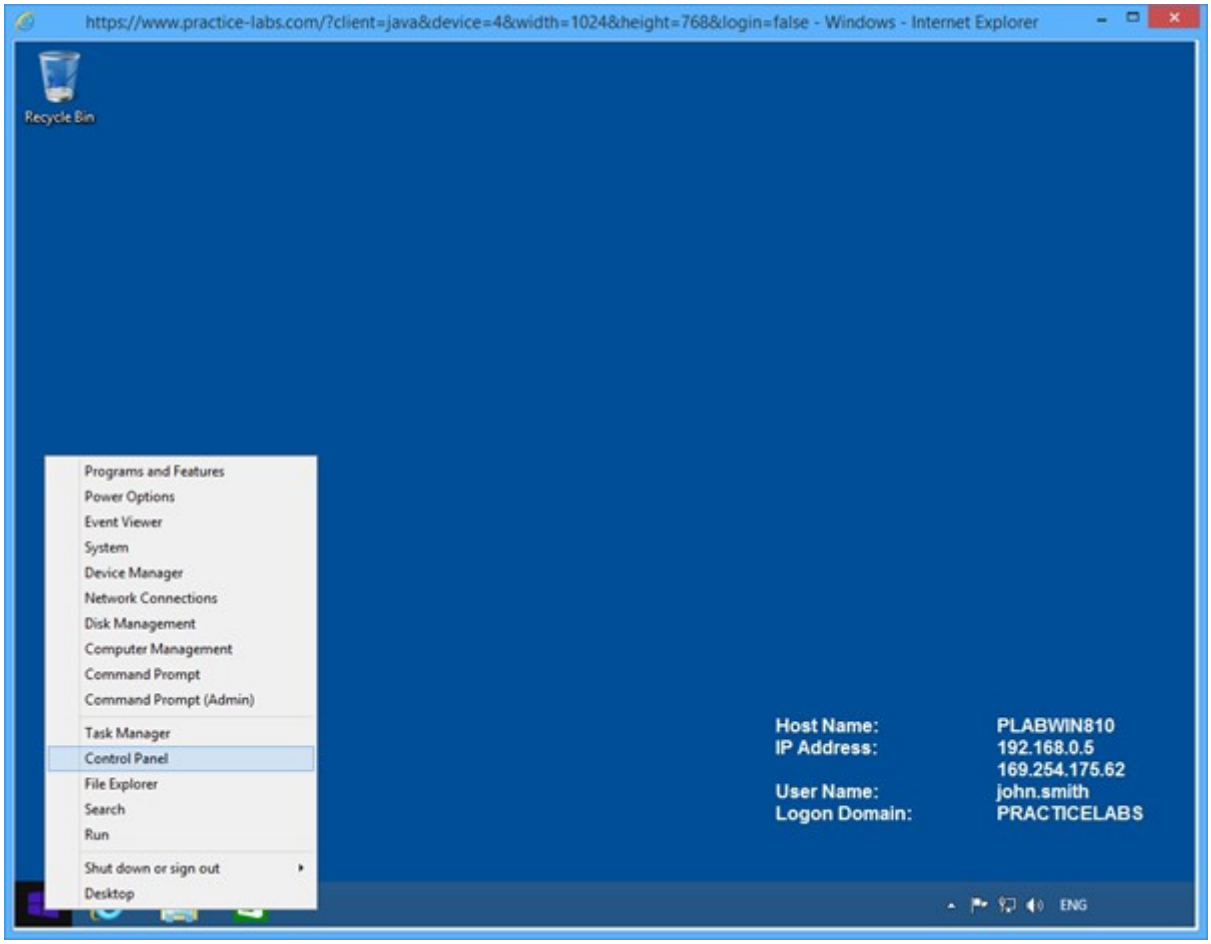
Step 5

If the **BGInfo License Agreement** dialog box is presented to you, click **Agree**.



Step 6

Right-click **Start** charm and select **Control Panel**.

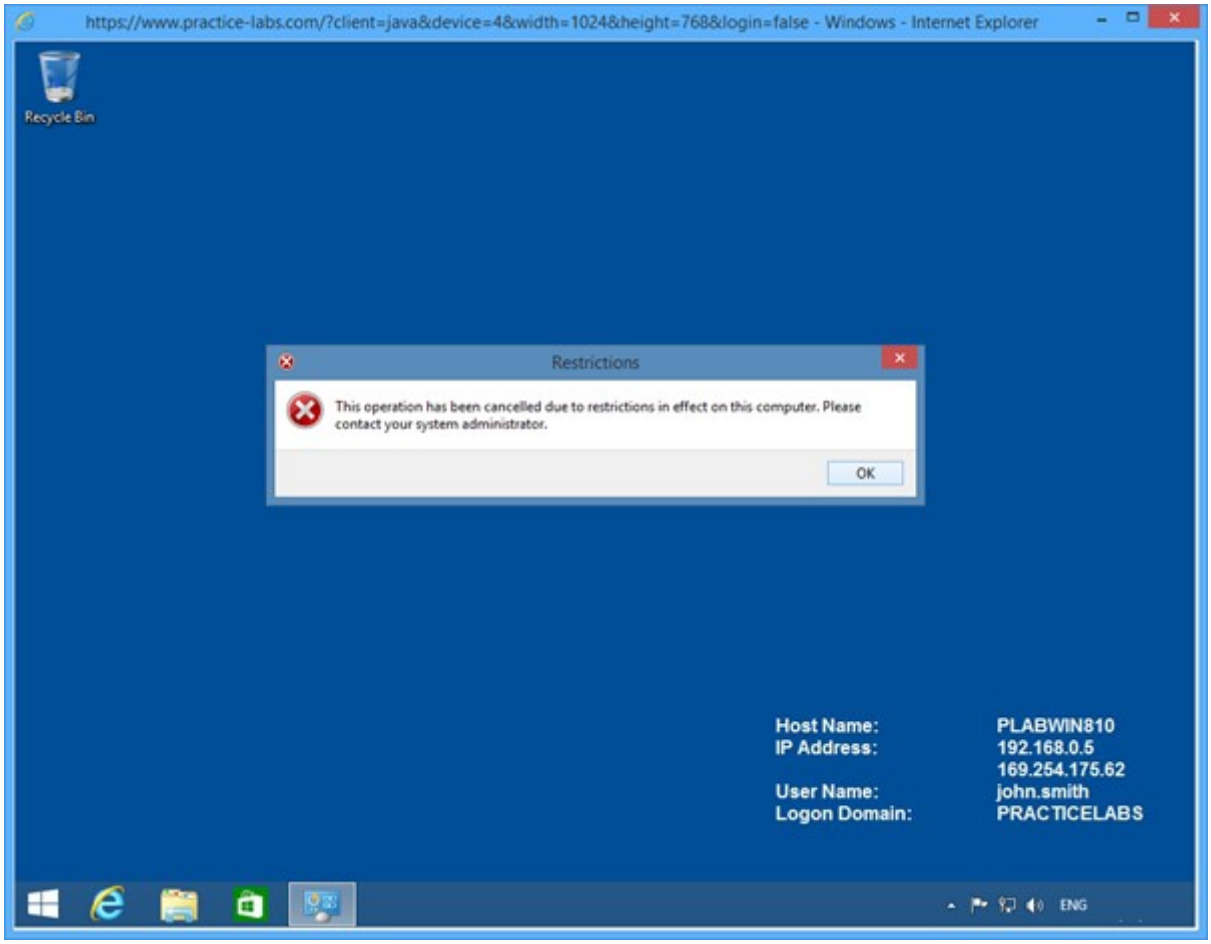


Step 7

John Smith will get a Restrictions dialogue box saying about restrictions enforced in this computer.

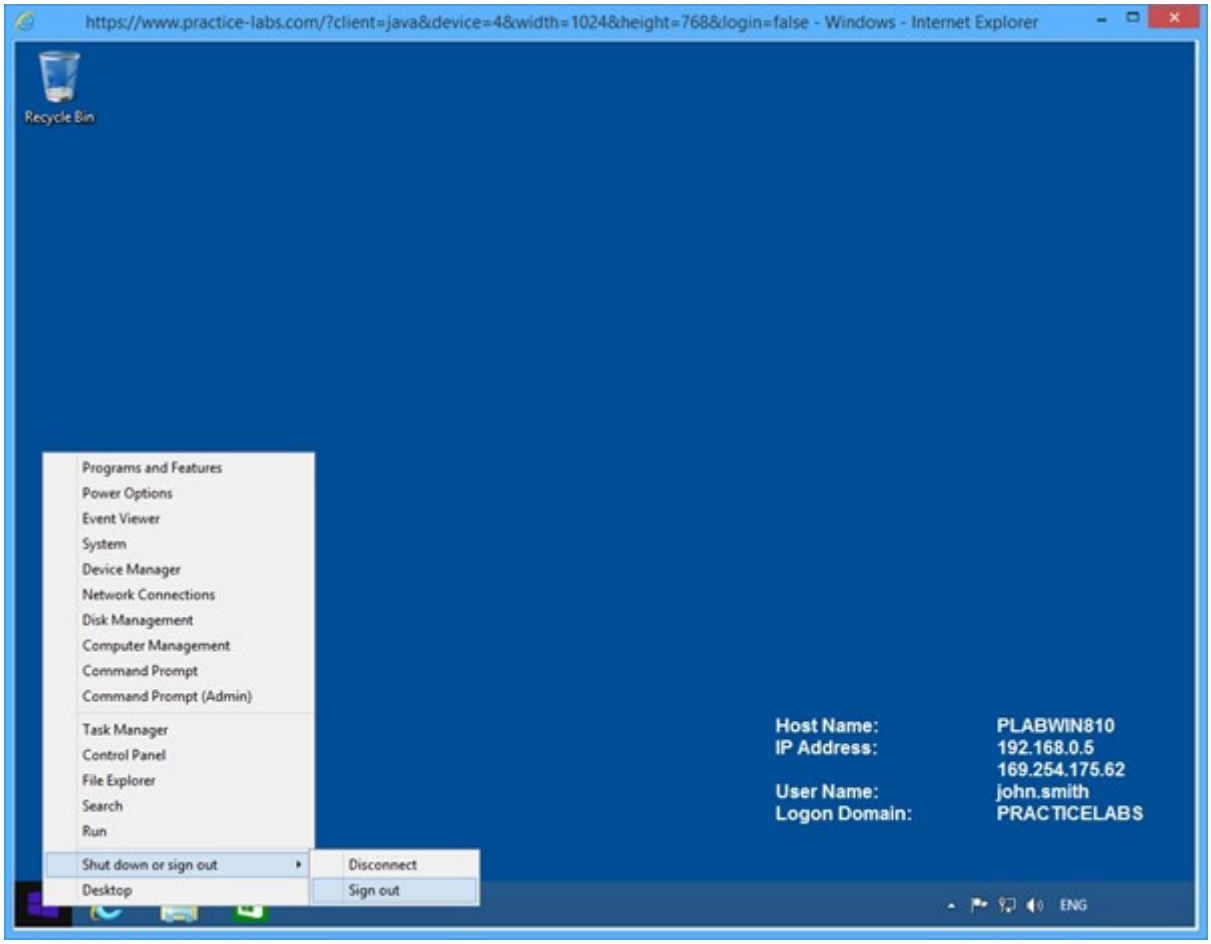
Click **OK**.

This means that the policy is enforced for John Smith because this user is located inside the Marketing OU.



Step 8

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



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

Exercise 4 - Configure Multiple Local Group Policies

Windows 8.1 provides the ability to create multiple local Group Policies. You can configure different settings for different users.

Please refer to your course material or use your favourite search engine to research for more information about this topic.

Task 1 - Creating User Accounts

In this task, you will create local user accounts that will be used for demonstrating the function of Local Group Policy Objects (GPO) on a Windows 8.1 computer.

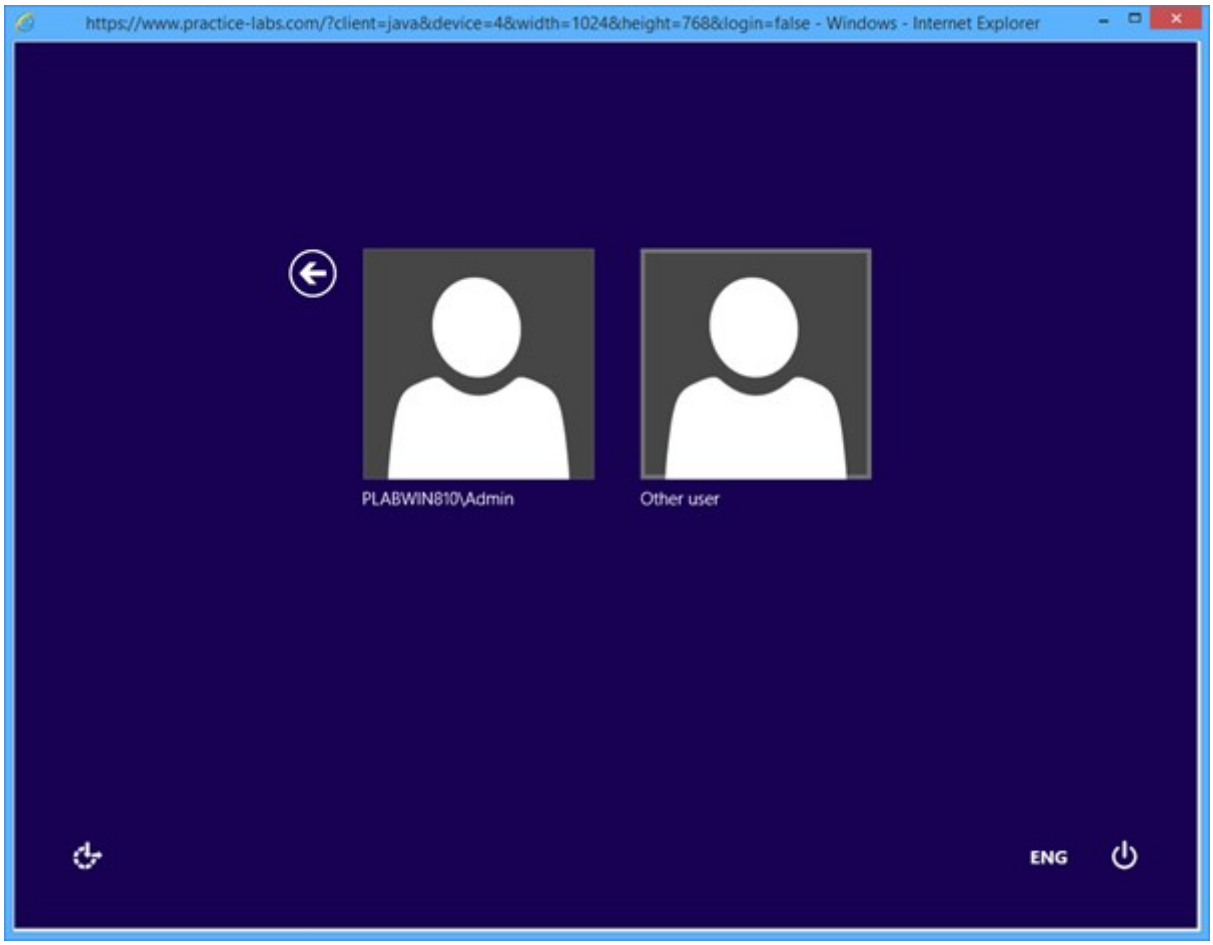
The user accounts will be created using the command line utility called NET.

To create the user accounts, perform the accompanying steps:

Step 1

Access the **Practice Labs** web application and connect to **PLABWIN810** device.

On the sign on screen, click **Other user**.



Step 2

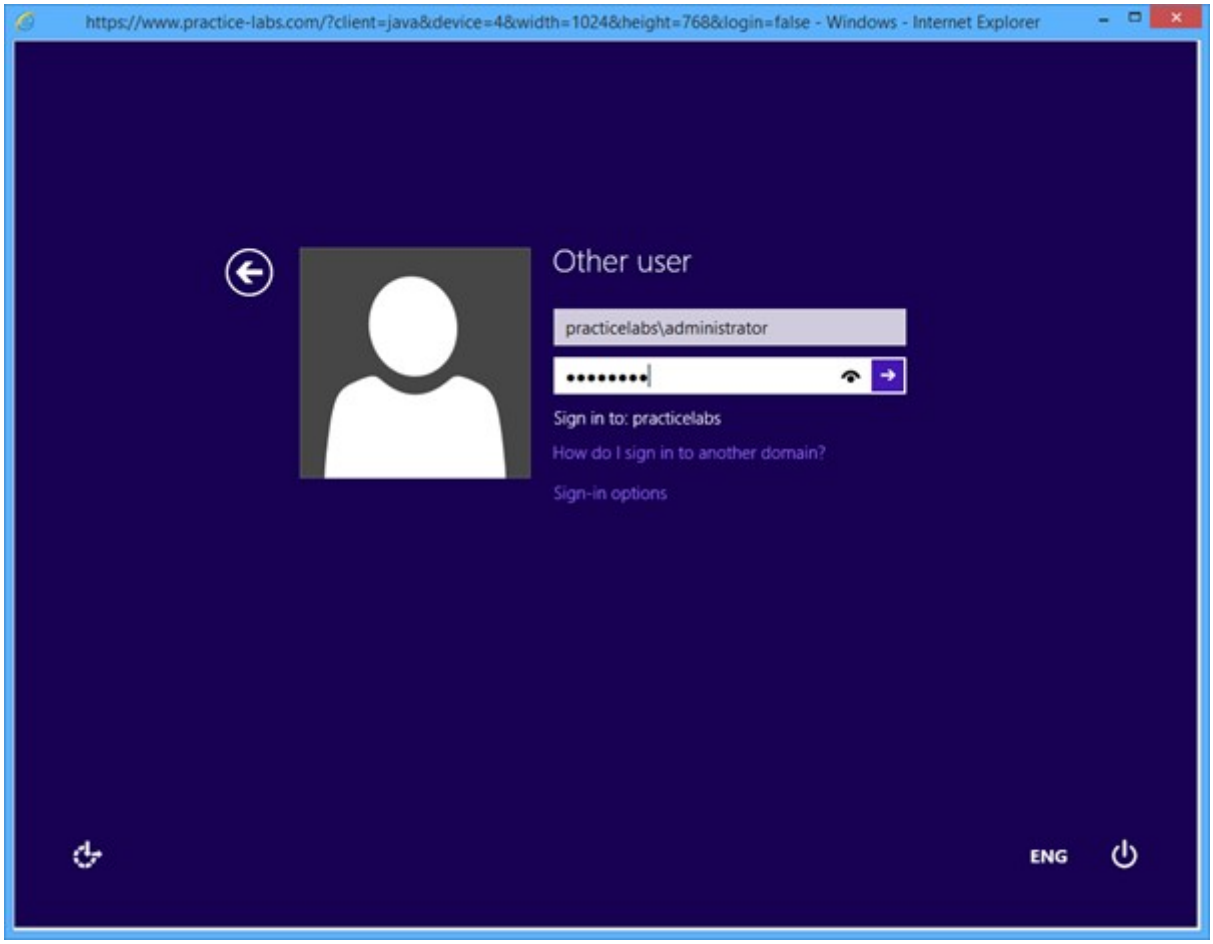
On the User name box, type:

```
practicelabs\administrator
```

On the Password box, type:

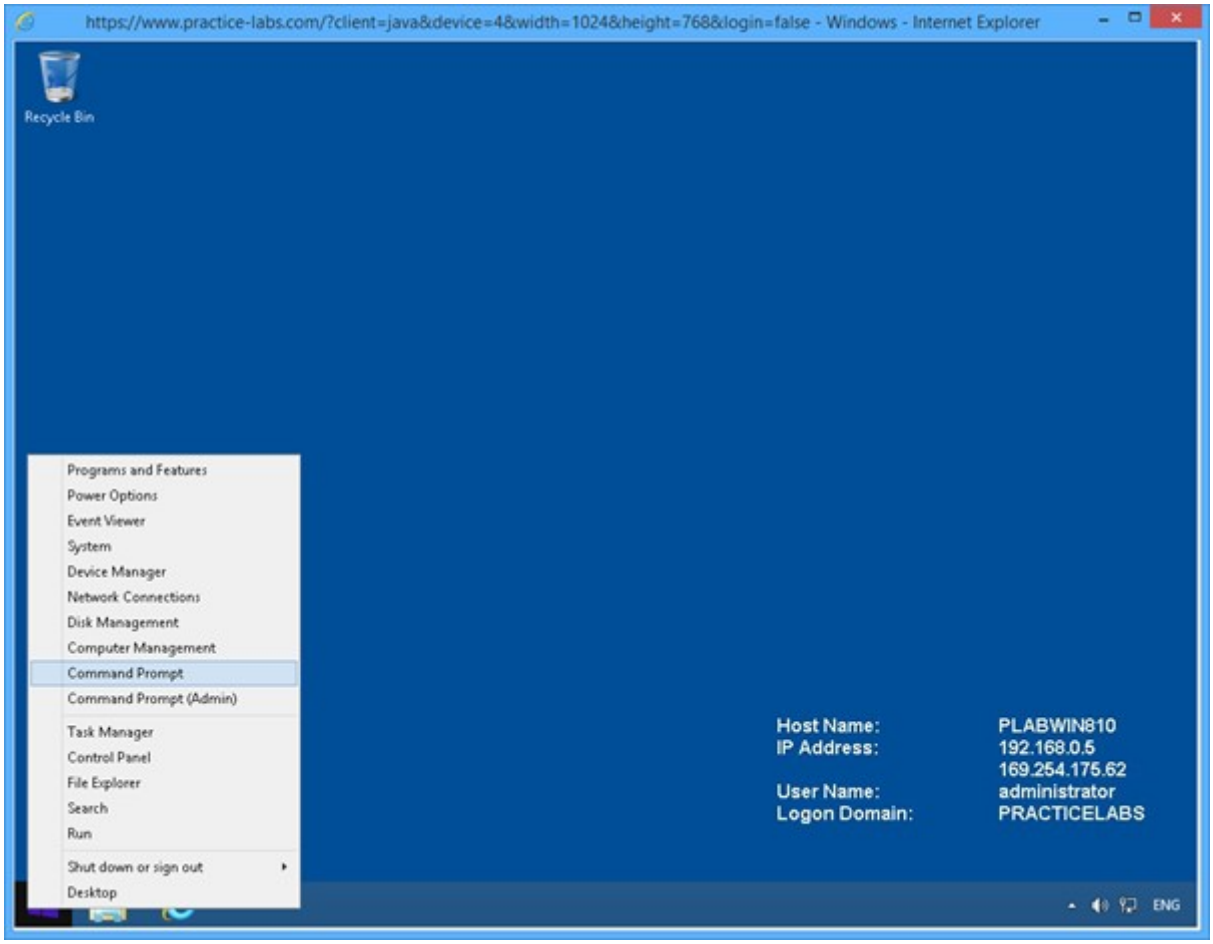
```
Passw0rd
```

Press **Enter**.



Step 3

When signed on to **PLABWIN810**, right-click **Start** charm and select **Command Prompt**.



Step 4

On the command prompt you will create two user accounts using the NET command.

To create the first user, type:

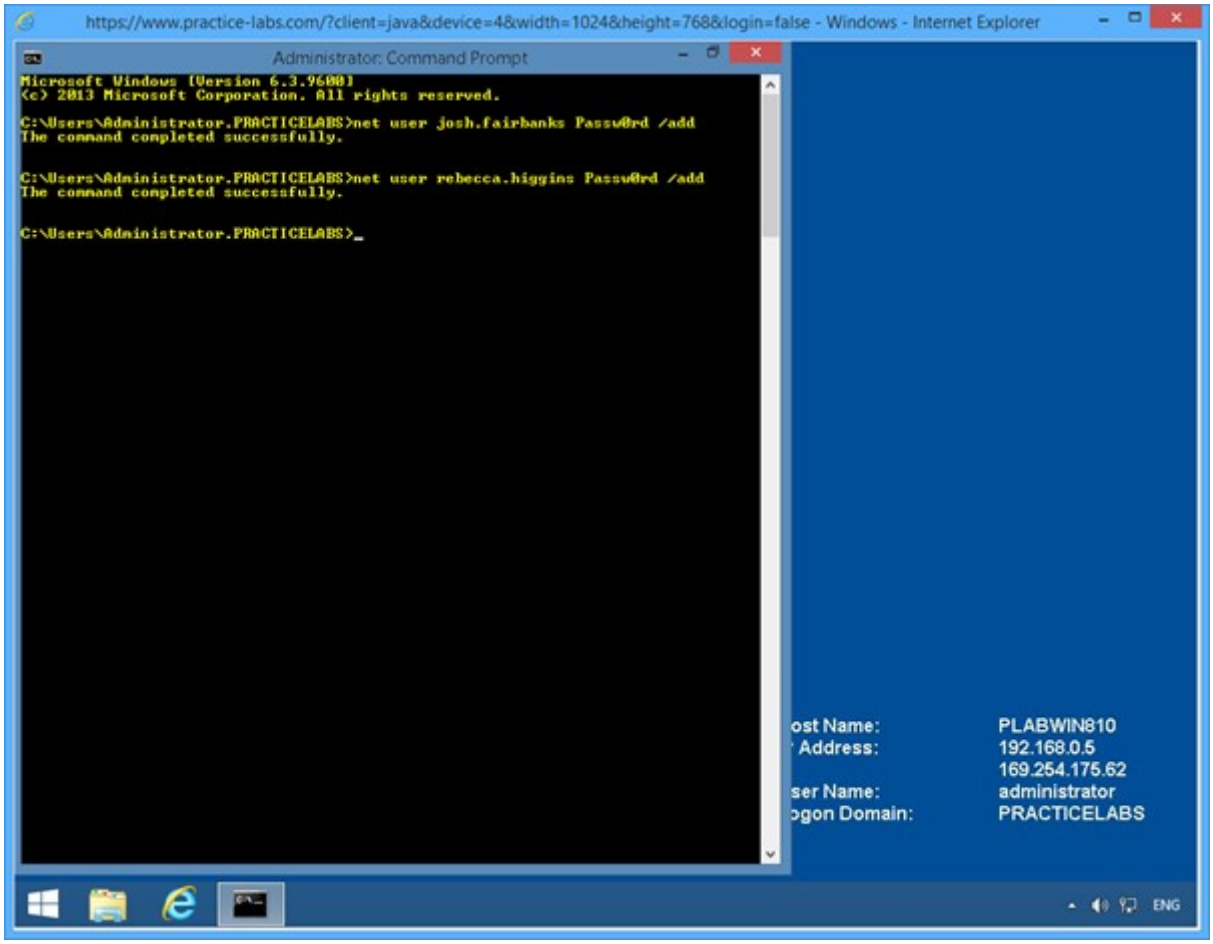
```
net user josh.fairbanks Passw0rd /add
```

Press **Enter**.

On the next prompt, to create another user, type:

```
net user Rebecca.higgins Passw0rd /add
```

Press **Enter**.

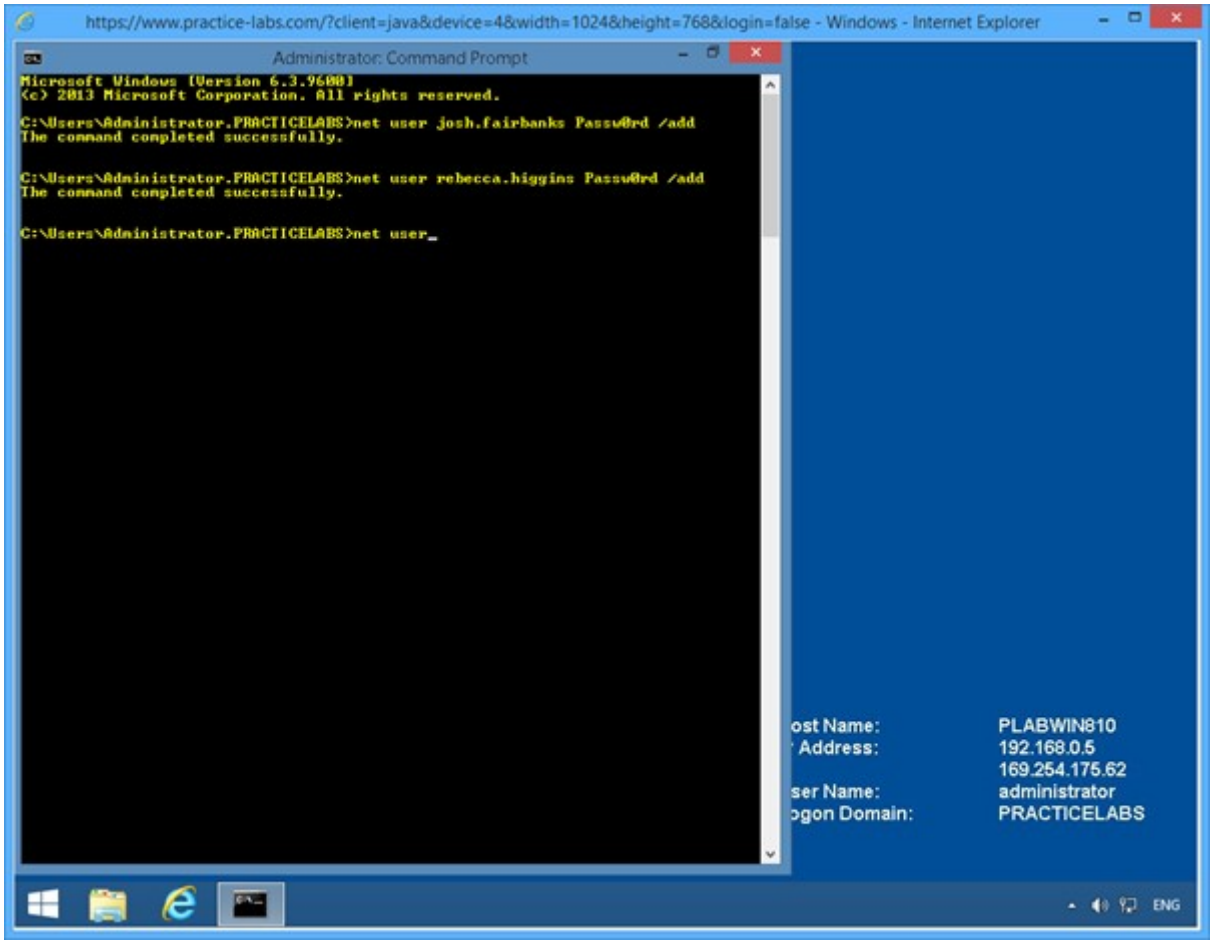


Step 5

To verify that the new user accounts are present in the local computer, type:

```
net user
```

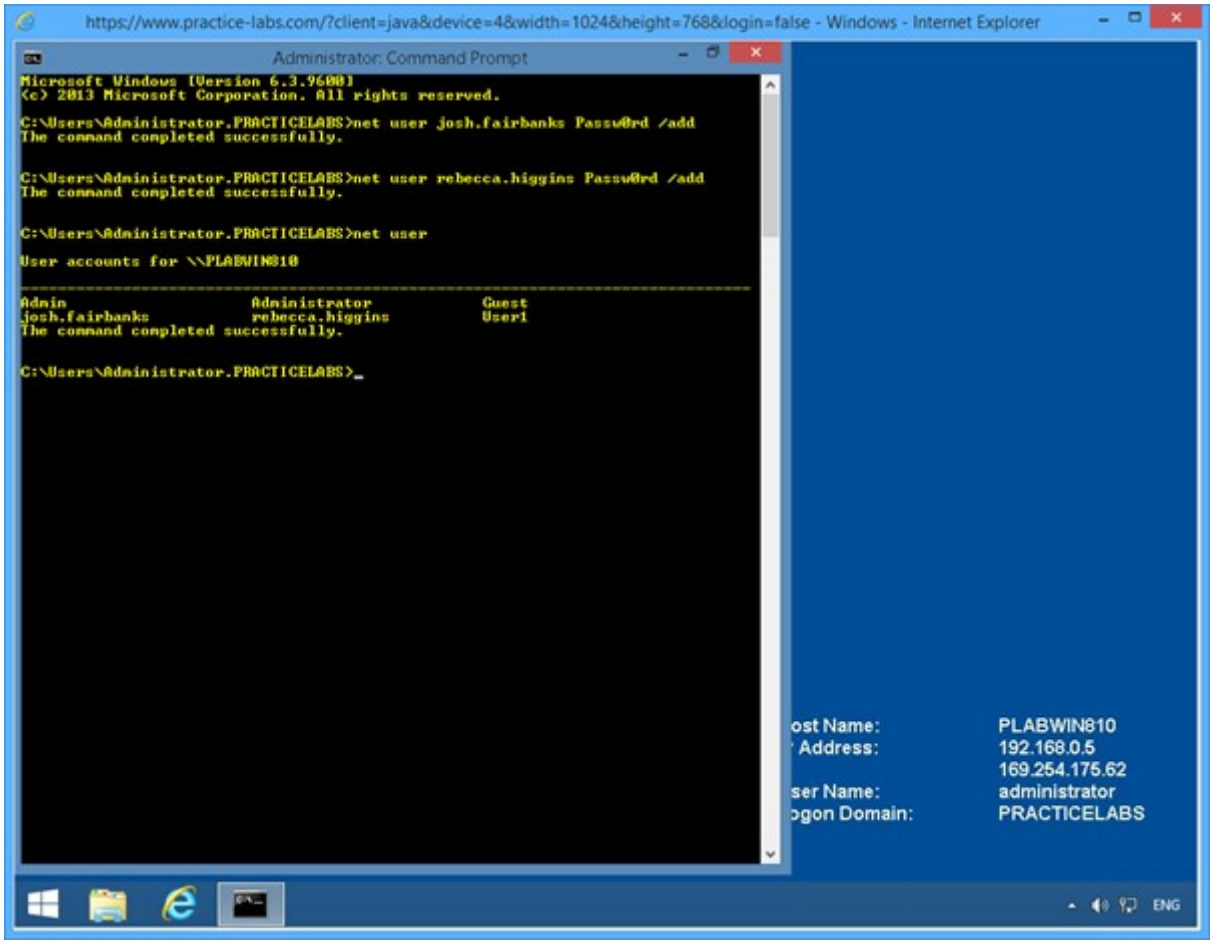
Press **Enter**.



Step 6

Notice the two local user accounts named **josh.fairbanks** and **rebecca.higgins** are registered users in the PLABWIN810 computer.

Keep the command prompt open for the next activity.



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

Task 2 - Creating Local Group Policy

A Local Group Policy is a scaled down version of the Domain Group Policy Object (GPO) applied in Active Directory domains. The Local GPO do not have the features of software deployment and folder redirection. Nonetheless, you can use the local GPO for imposing restrictions on a local computer.

A local Group Policy Object (GPO) can be created even for Windows computers that are members of an Active Directory domain.

When a local GPO is enforced on a Windows device, this will affect all users who sign on to the computer.

To create a local group policy for a device, perform the following steps:

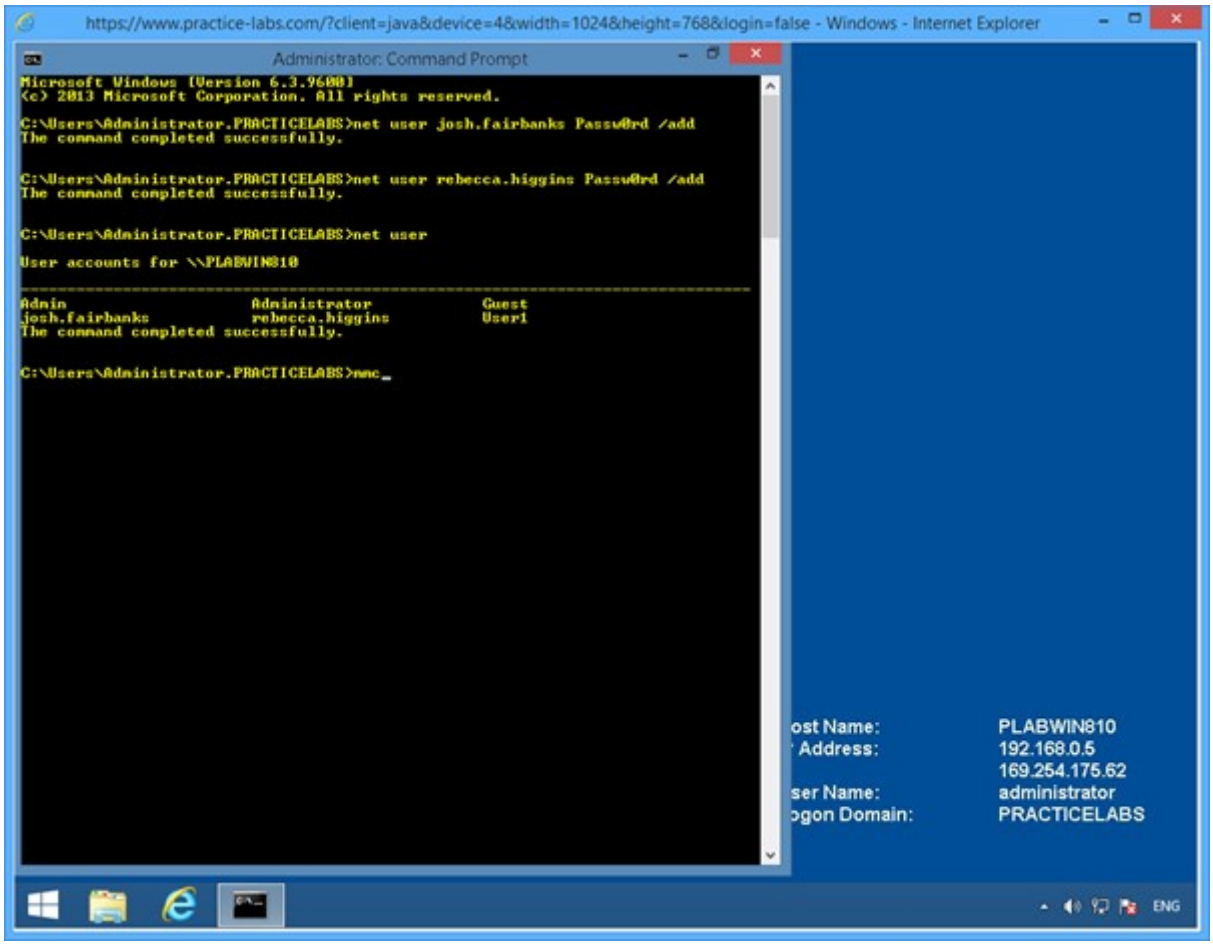
Step 1

On **PLABWIN810**, the command prompt window is currently open.

To open a blank **Microsoft Management Console,** type:

```
mmc
```

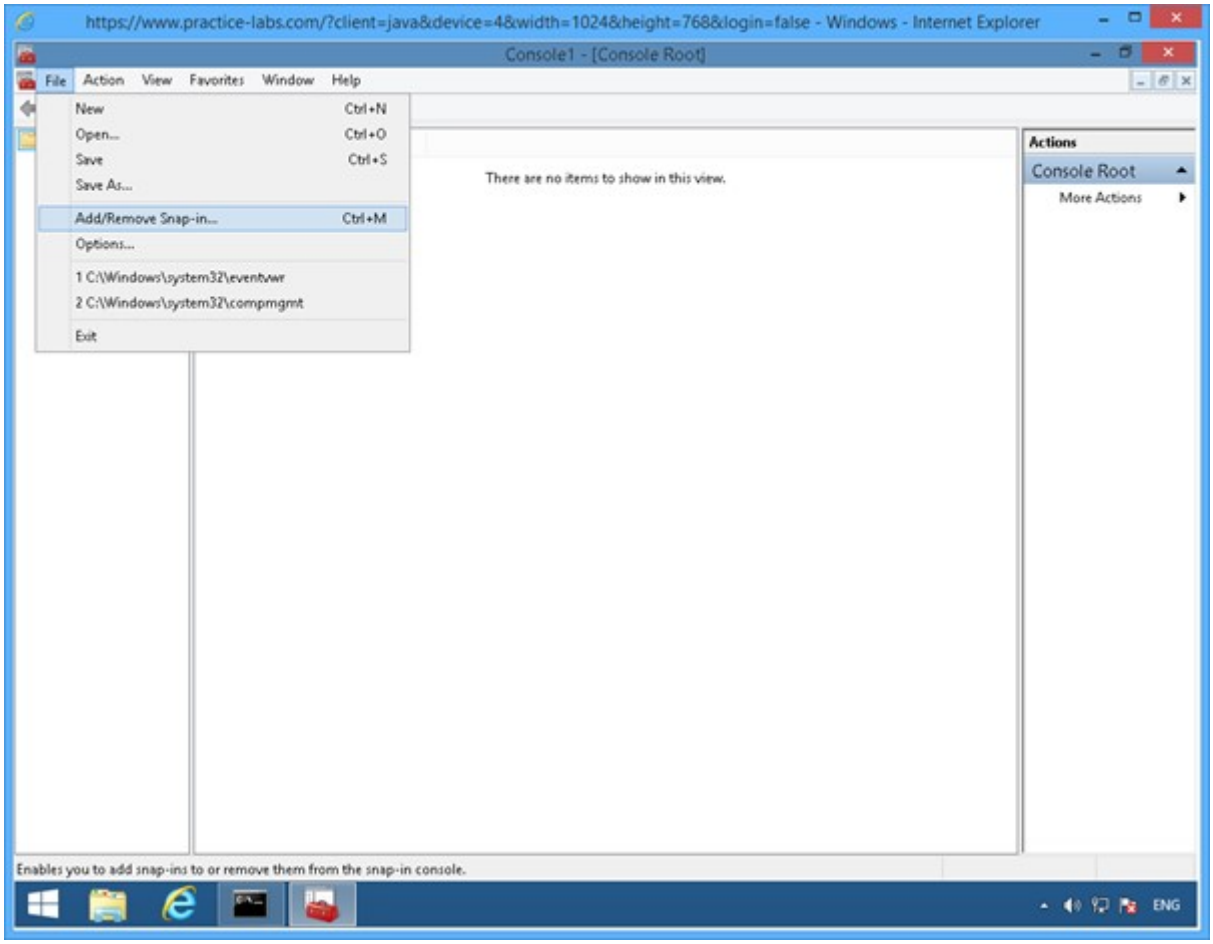
Press **Enter.**



Step 2

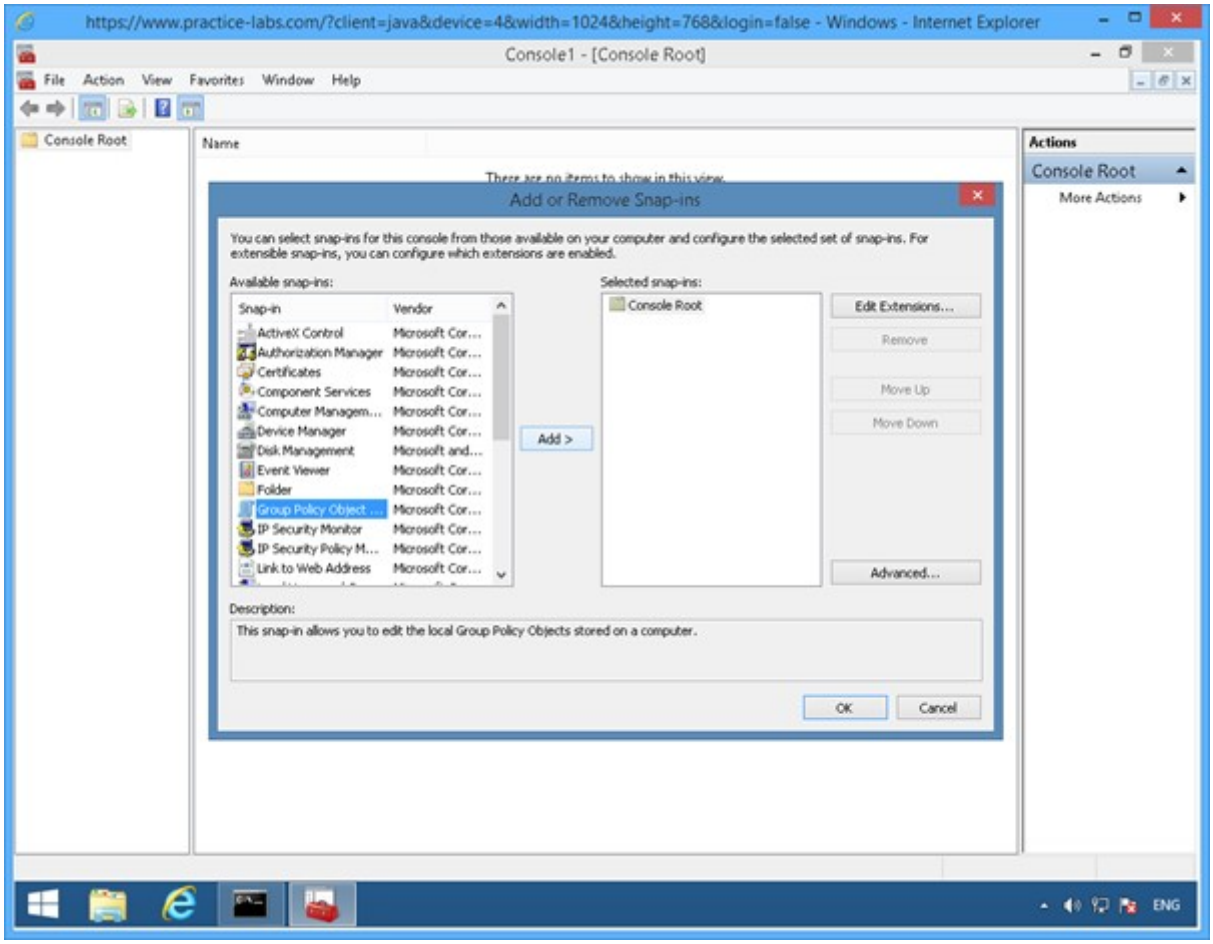
The **Console1** window opens.

Click **File** menu and select **Add/Remove Snap-in**...



Step 3

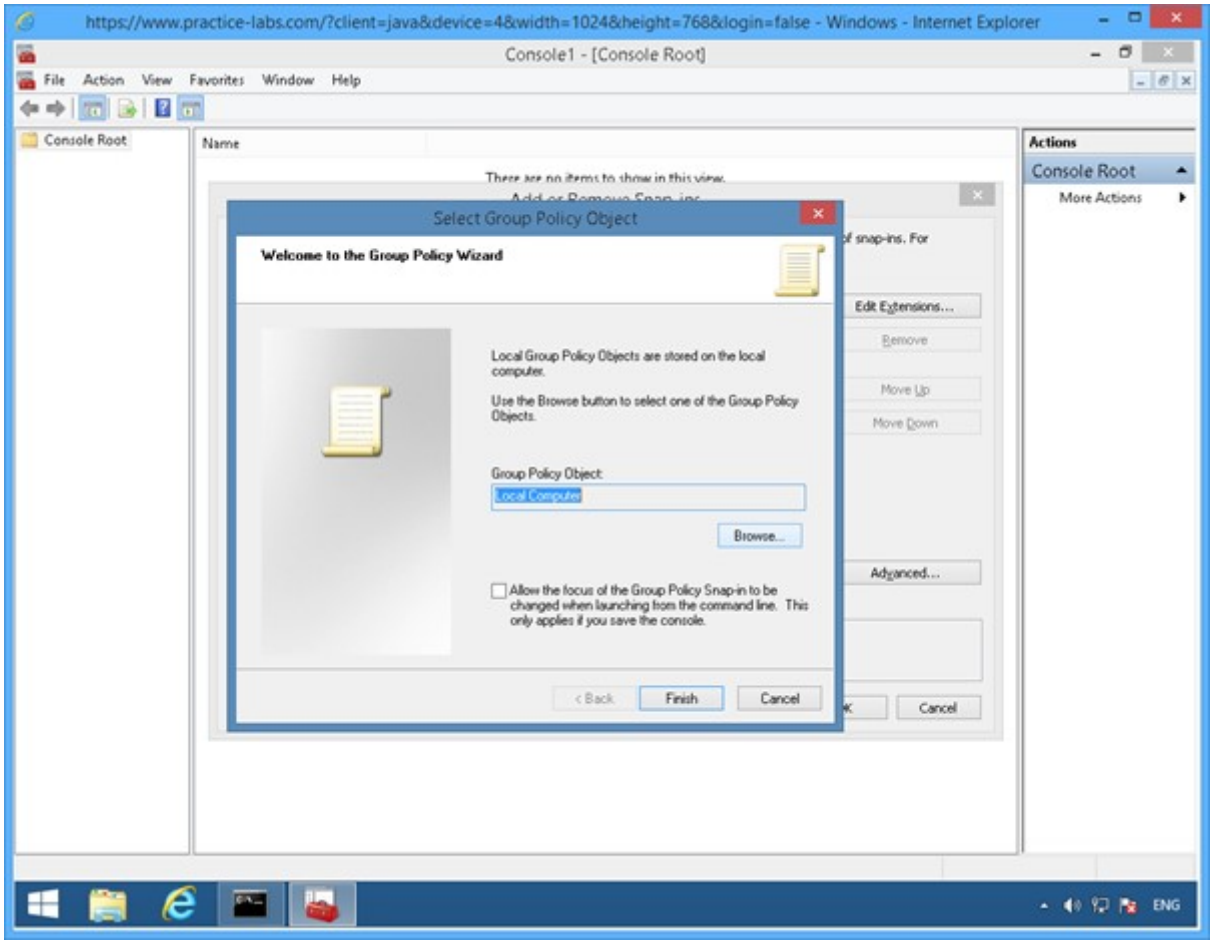
On the **Add or Remove Snap-ins** dialog box, under **Available snap-ins** column, select **Group Policy Object**... and click **Add**.



Step 4

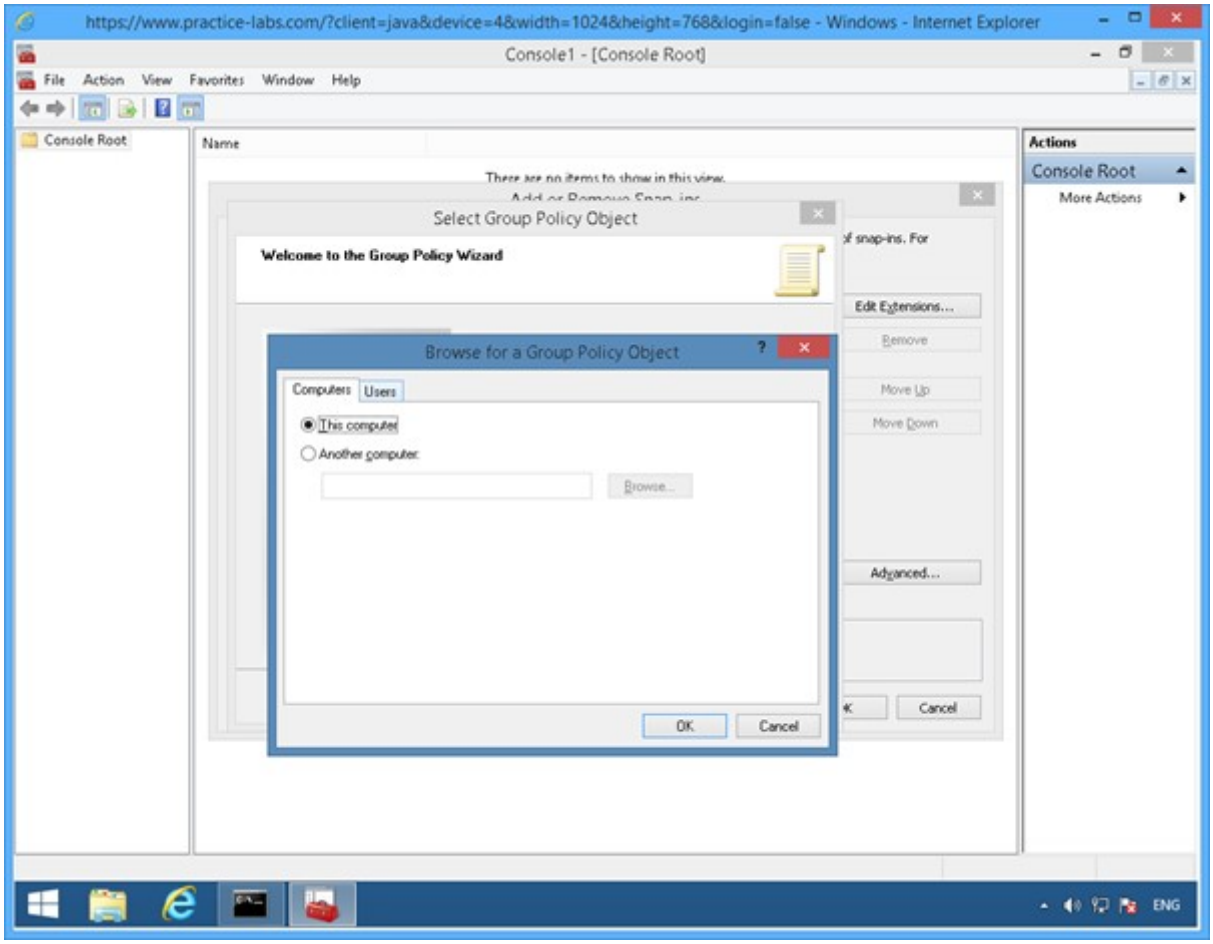
The **Select Group Policy Object** is displayed.

On the **Welcome to the Group Policy Wizard** page click **Browse**...



Step 5

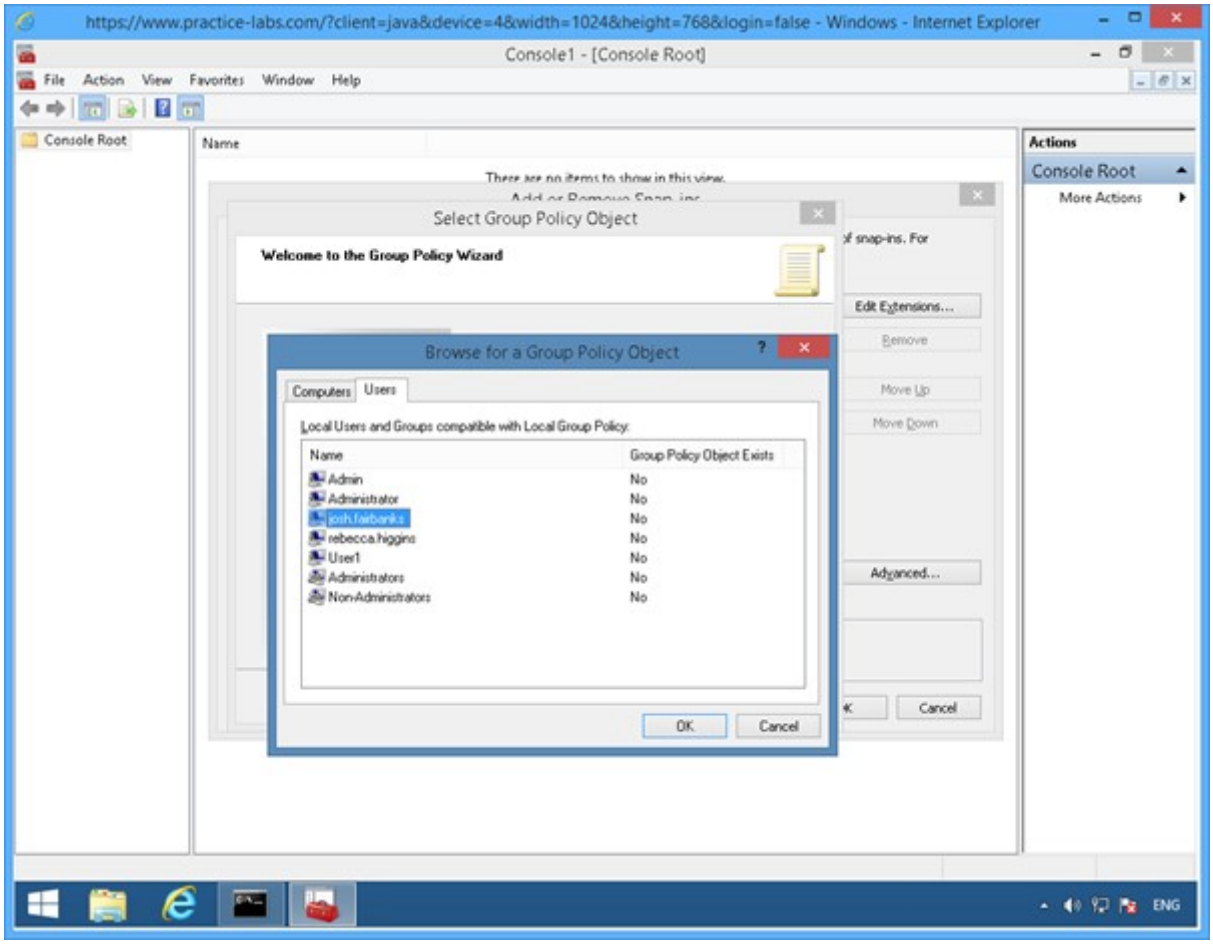
On the **Browse for a Group Policy Object** dialog box, click **Users** tab.



Step 6

On the **Users** tab, select **josh.fairbanks**.

Click **OK**.

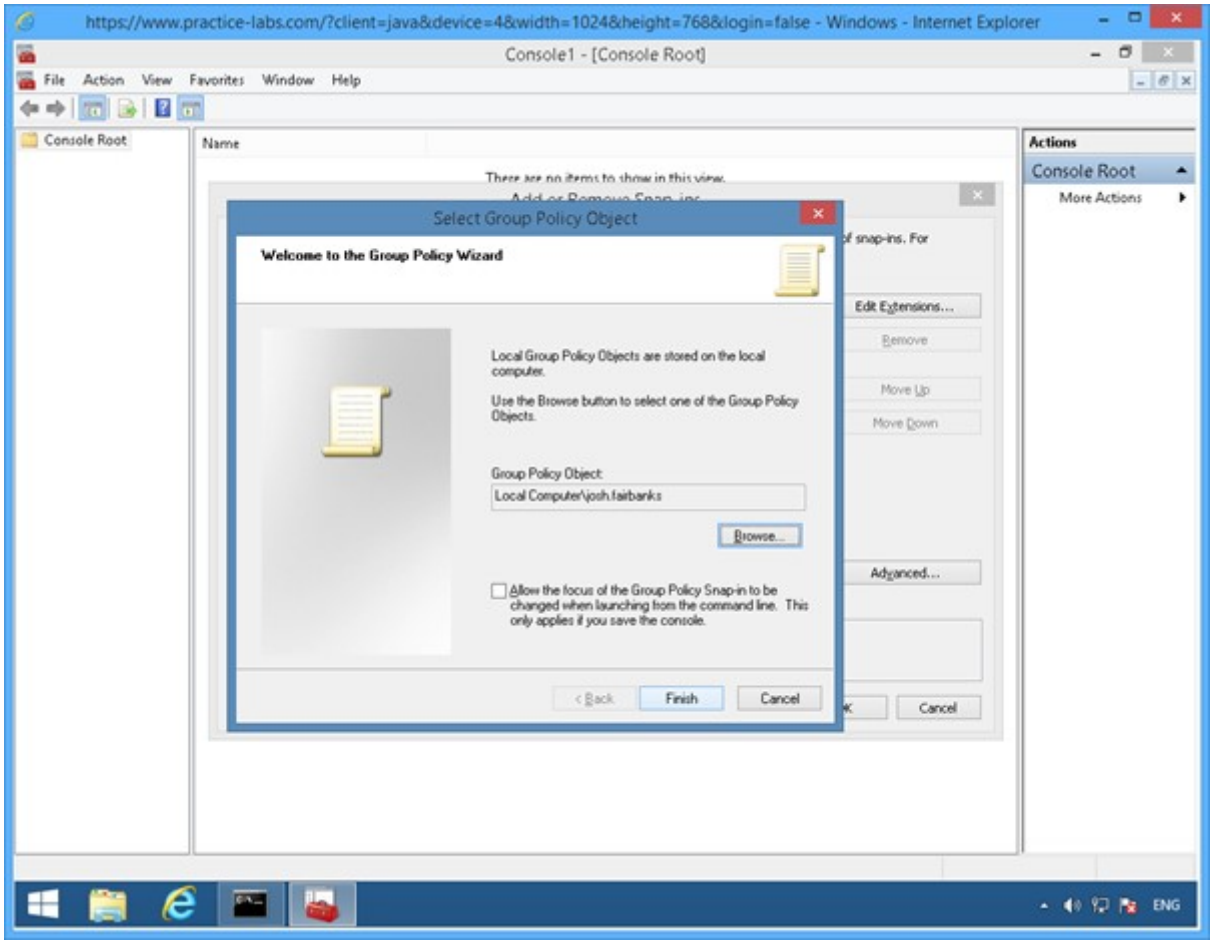


Step 7

Back in the **Welcome to the Group Policy Wizard** dialog box, click **Finish**.

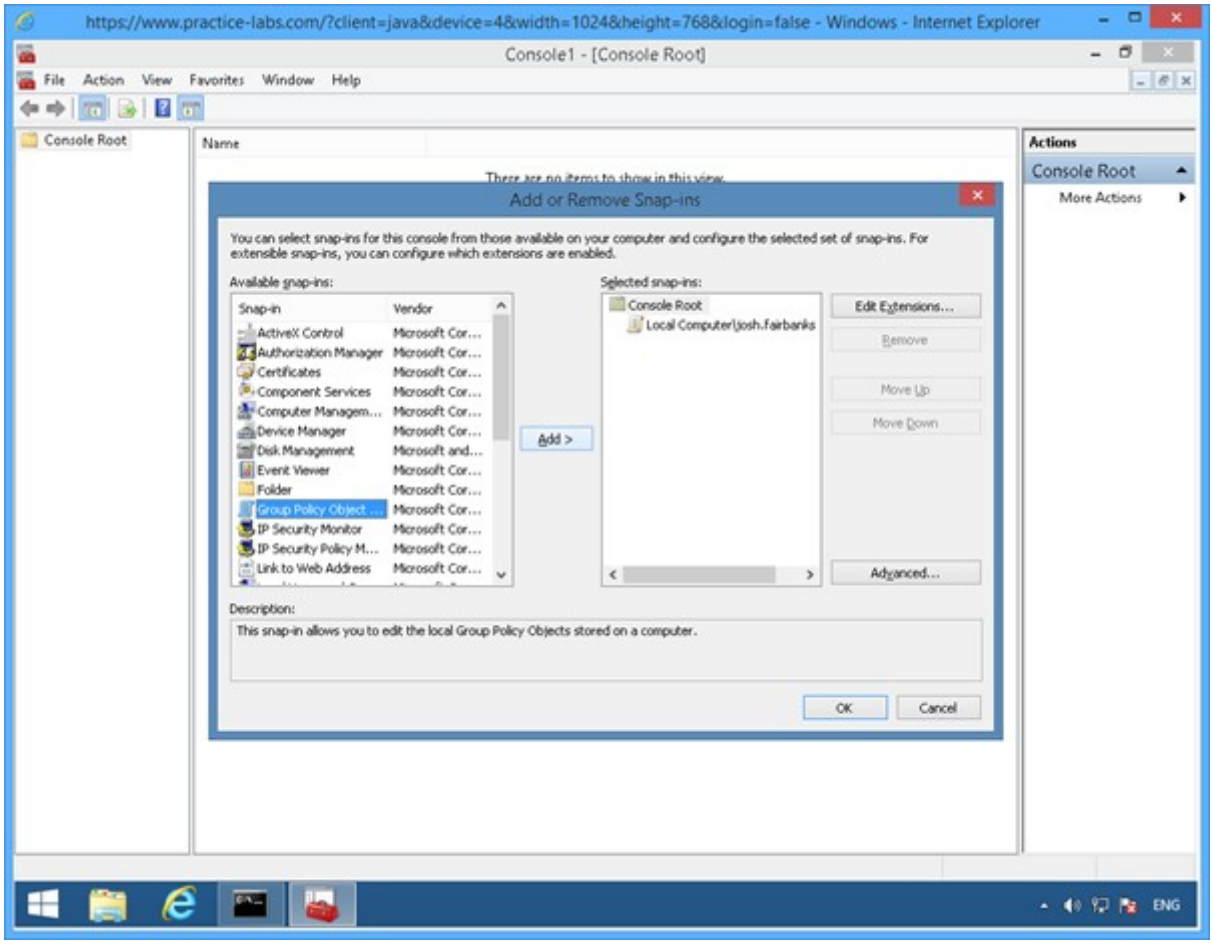
Notice that you have a **Local Computer\josh.fairbanks** added.

You will repeat these steps this time for a user named **rebecca.higgins.**



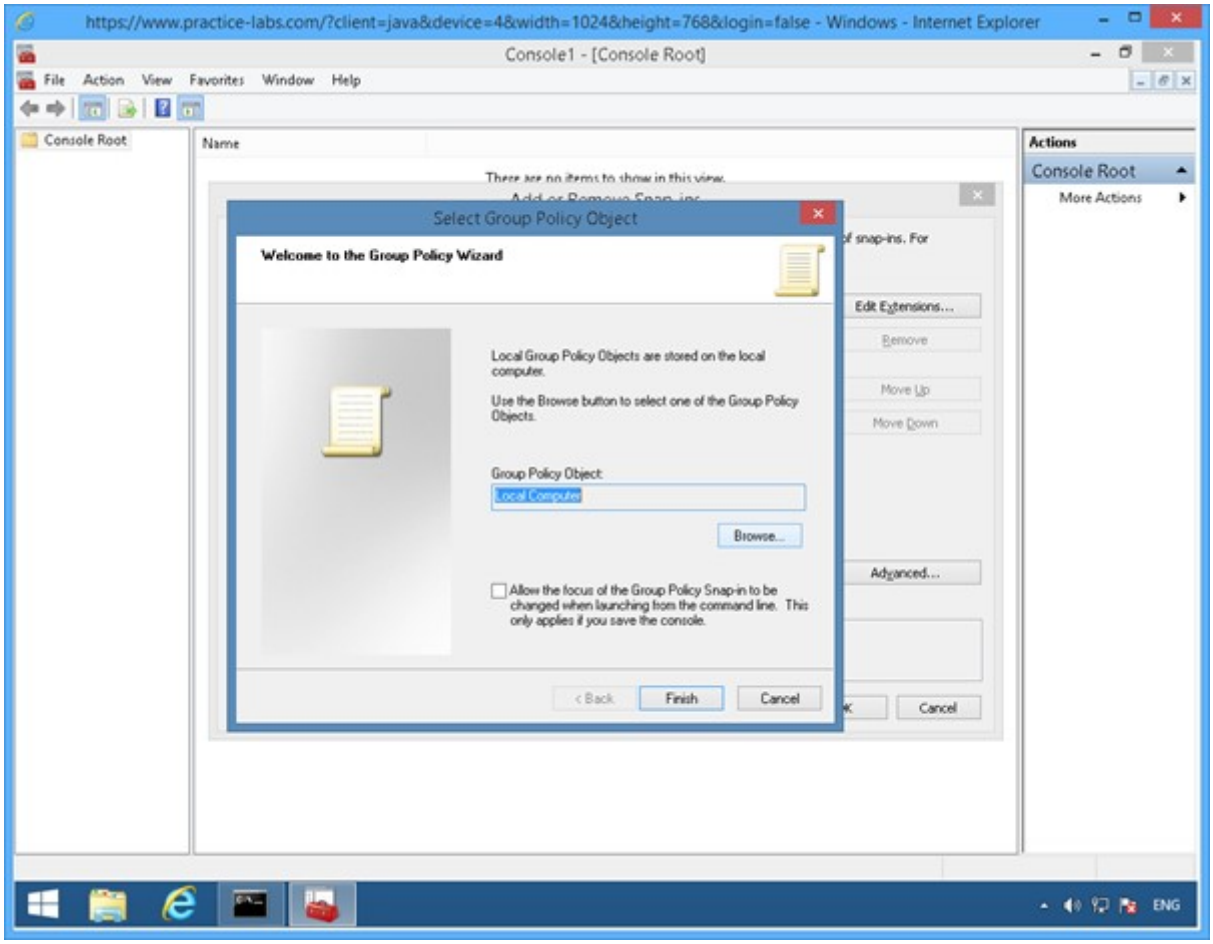
Step 8

Back on the **Add or Remove Snap-ins** dialog box, select **Group Policy Object**... and click **Add>**



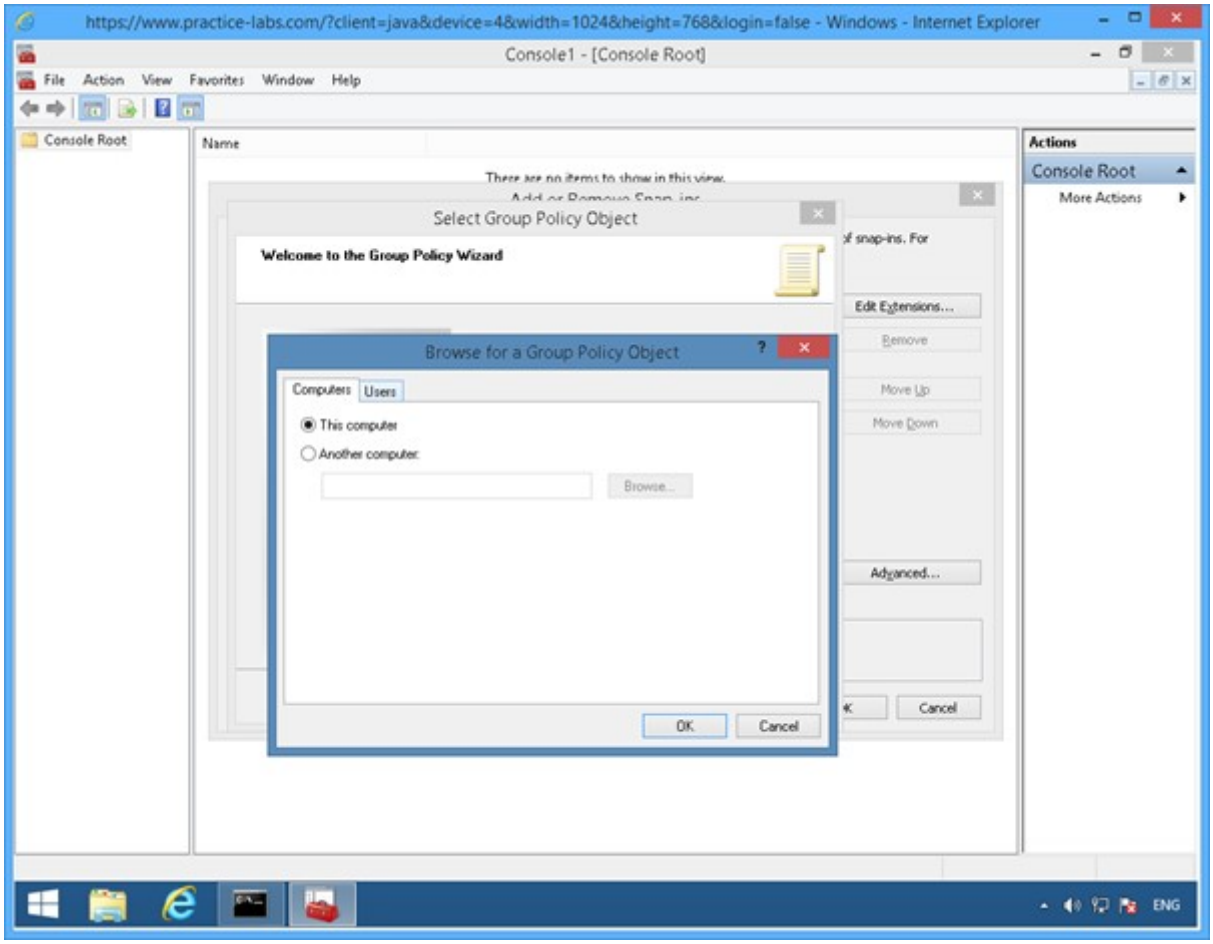
Step 9

Again on the **Welcome to the Group Policy Wizard** page, click **Browse**...



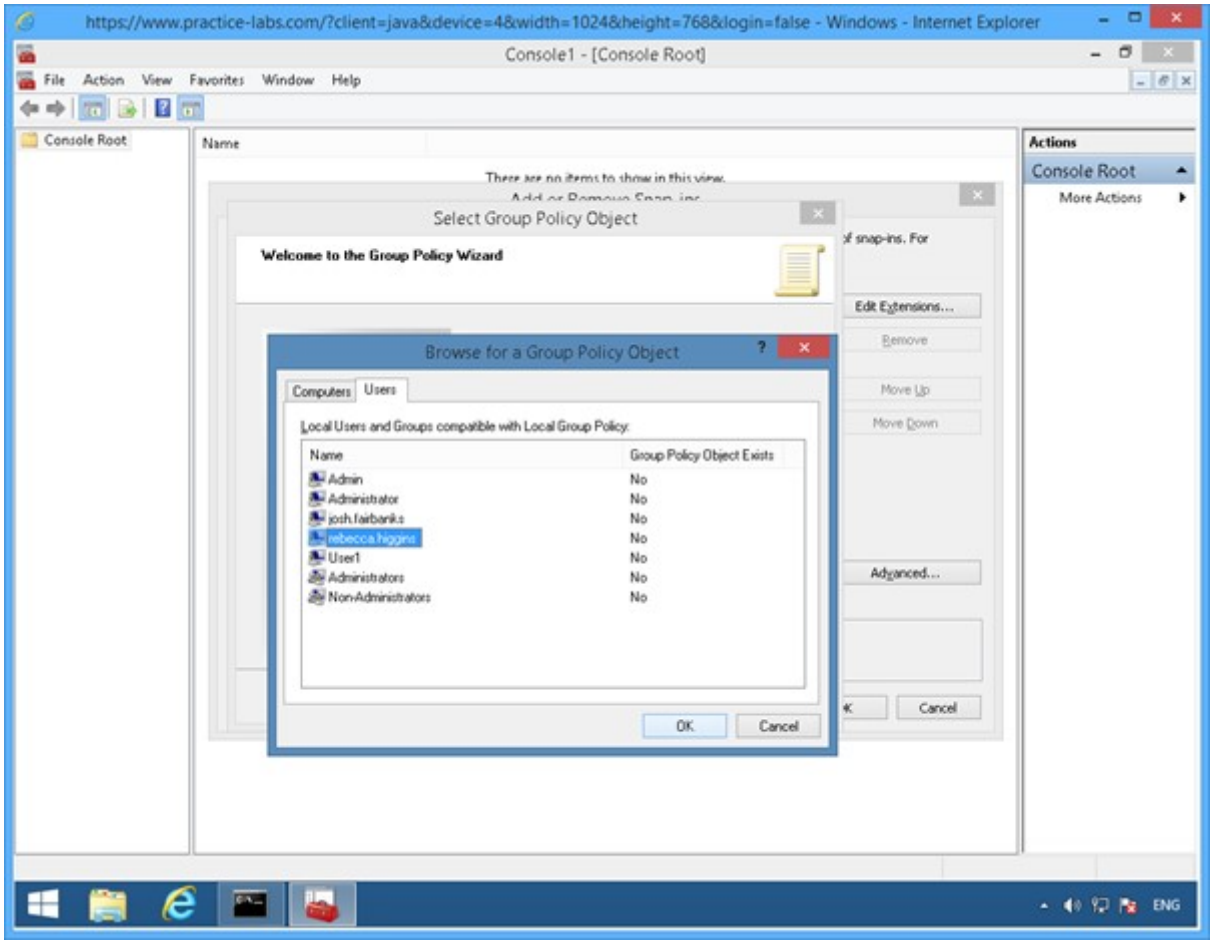
Step 10

On the **Browse for a Group Policy Object** dialog box, click **Users** tab.



Step 11

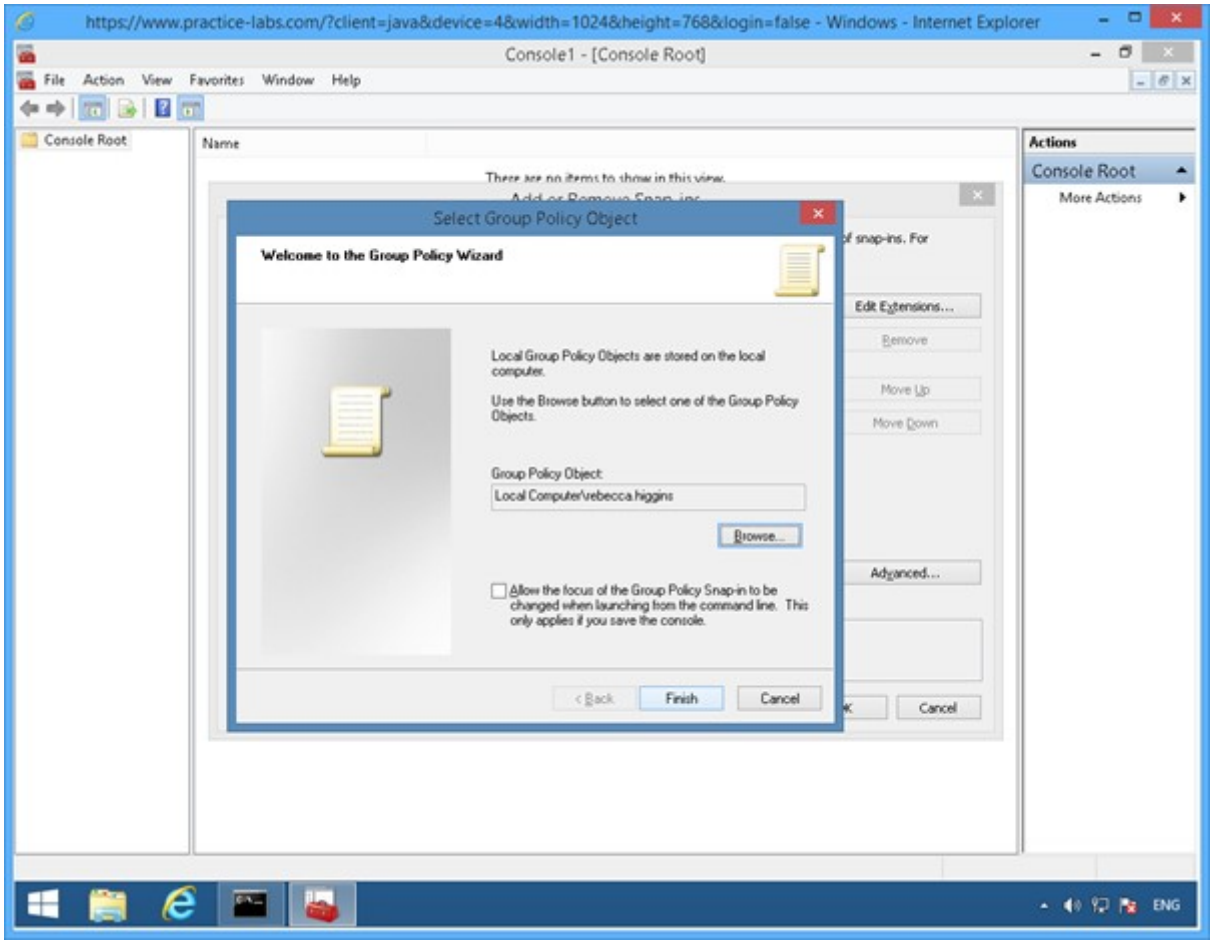
On the **Users** tab, select **rebecca.higgins** and click **OK**.



Step 12

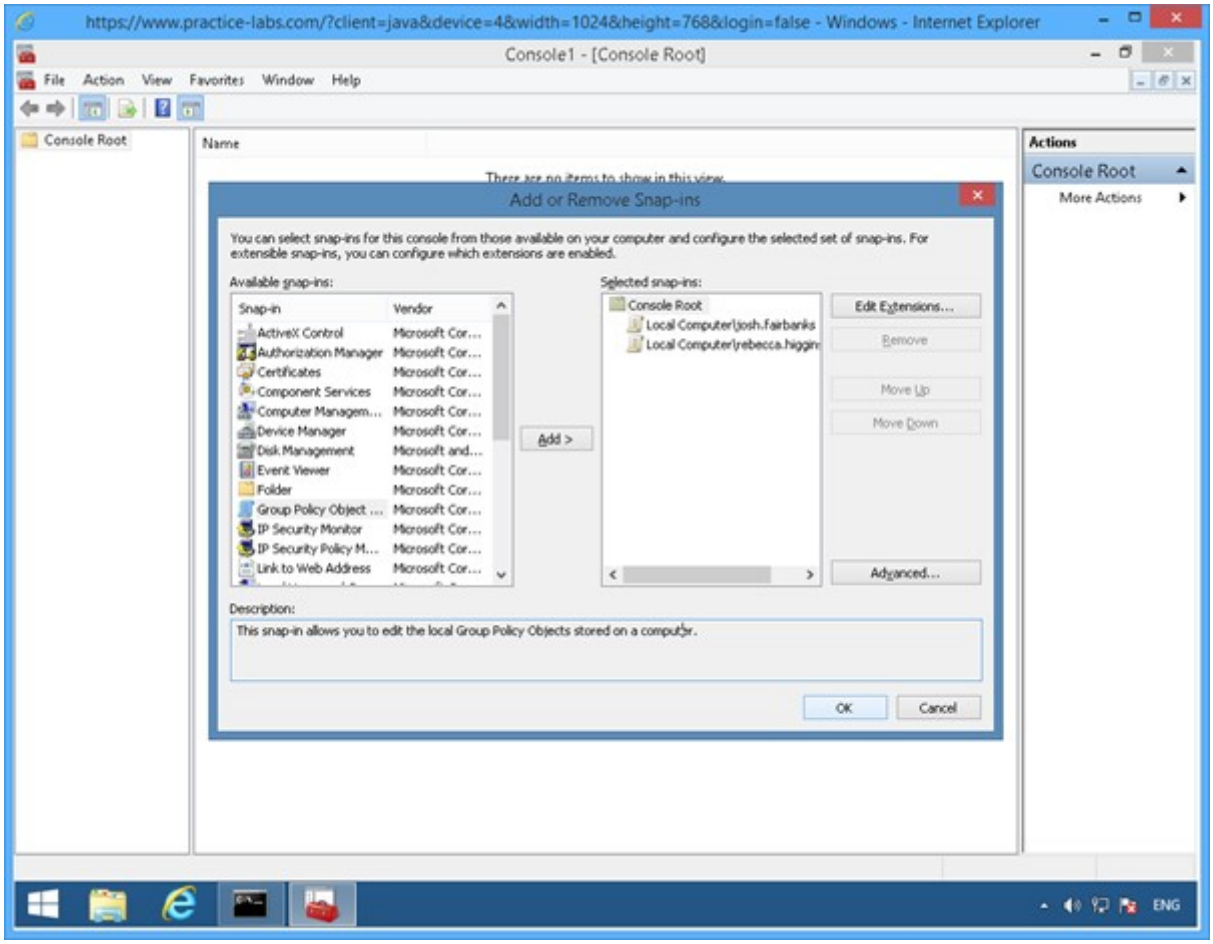
Back on the **Welcome to the Group Policy Wizard** page, you have **added Local Computer\rebecca.higgins**.

Click **Finish**.



Step 13

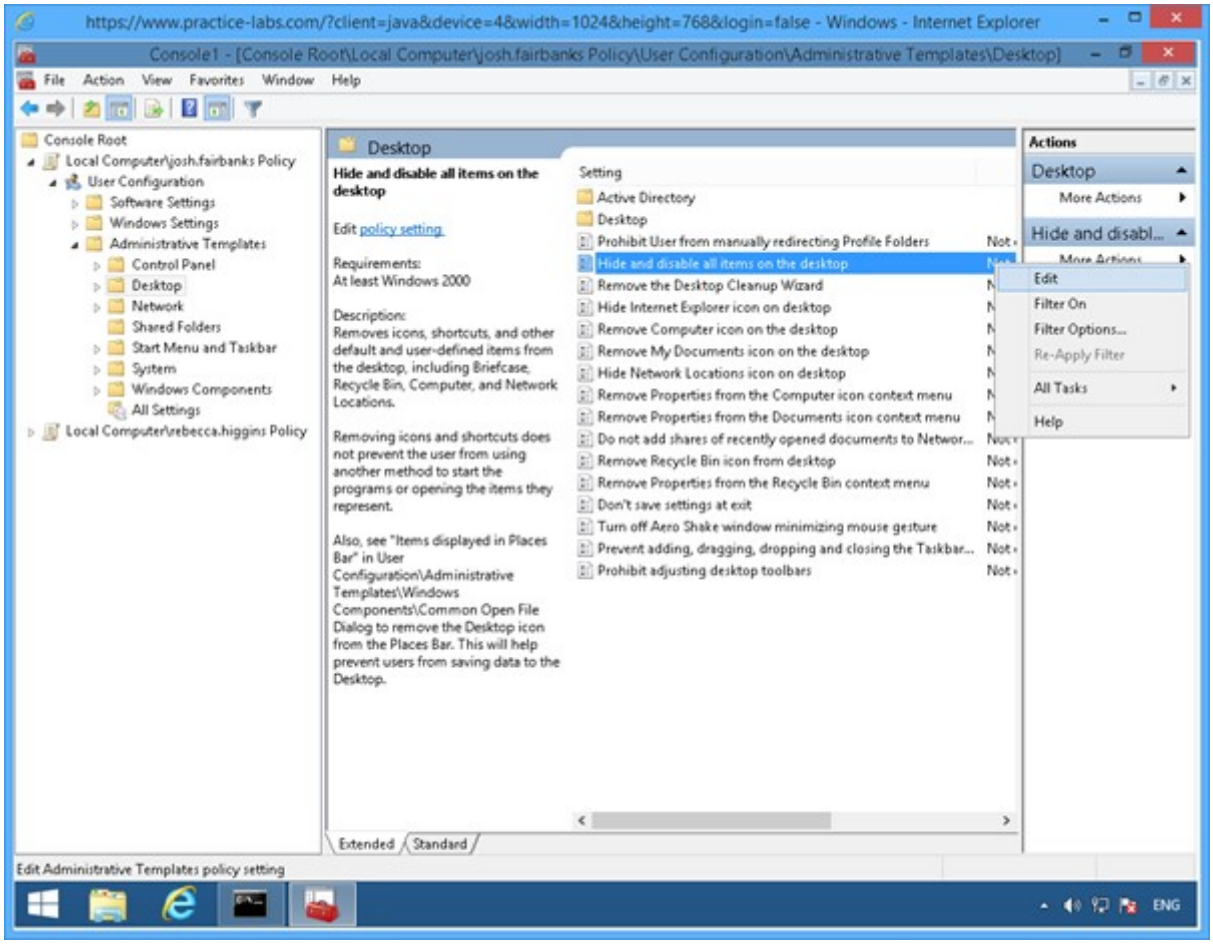
Click **OK** to close **Add Remove Snap-in** dialog box.



Step 14

From **Console1**, expand **Local Computer\josh.fairbanks Policy** > **User Configuration** > **Administrative Templates** and click **Desktop** folder.

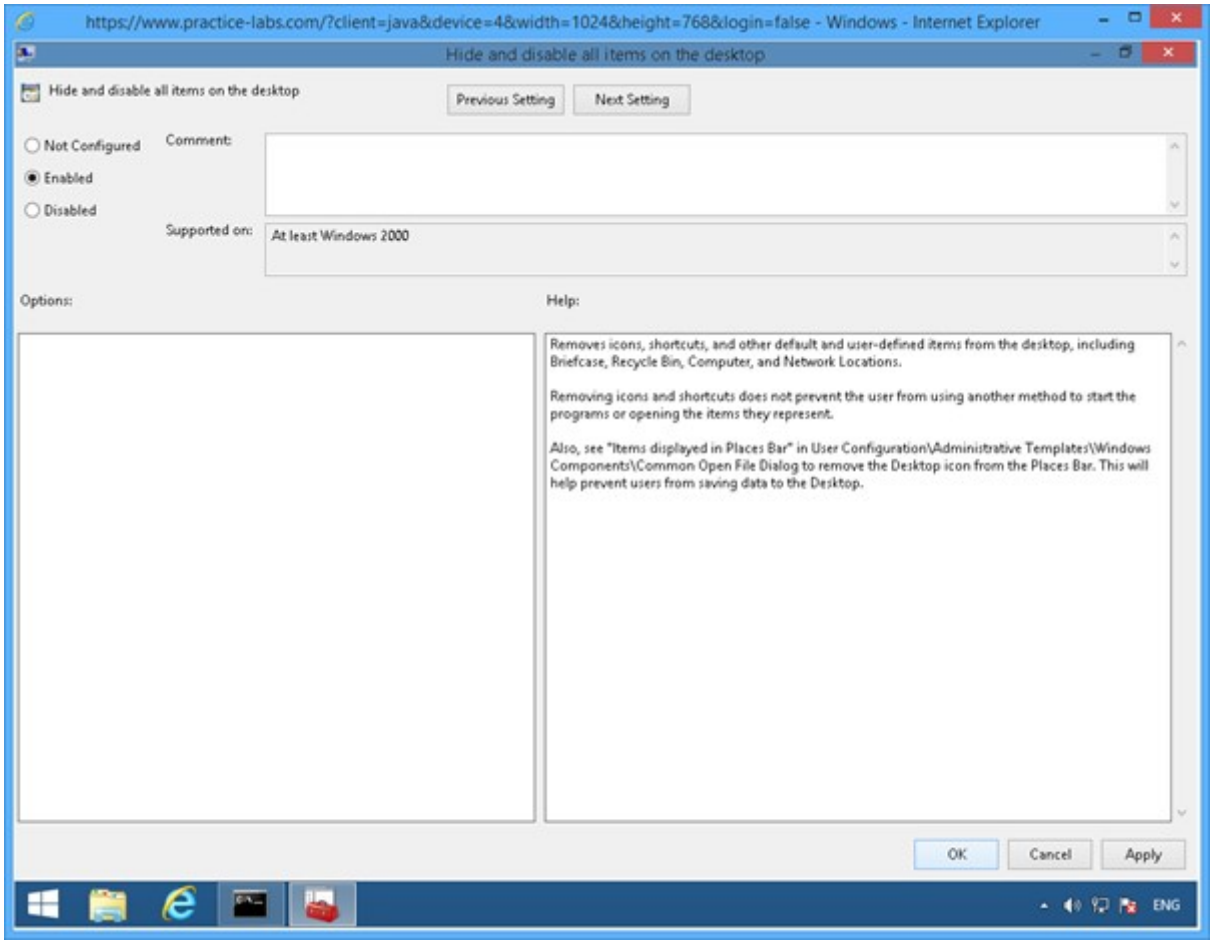
On the details pane, right-click on **Hide and disable all items on the desktop** and select **Edit**.



Step 15

On **Hide and disable all items on desktop** dialog box, select **Enabled** option.

Click **OK**.

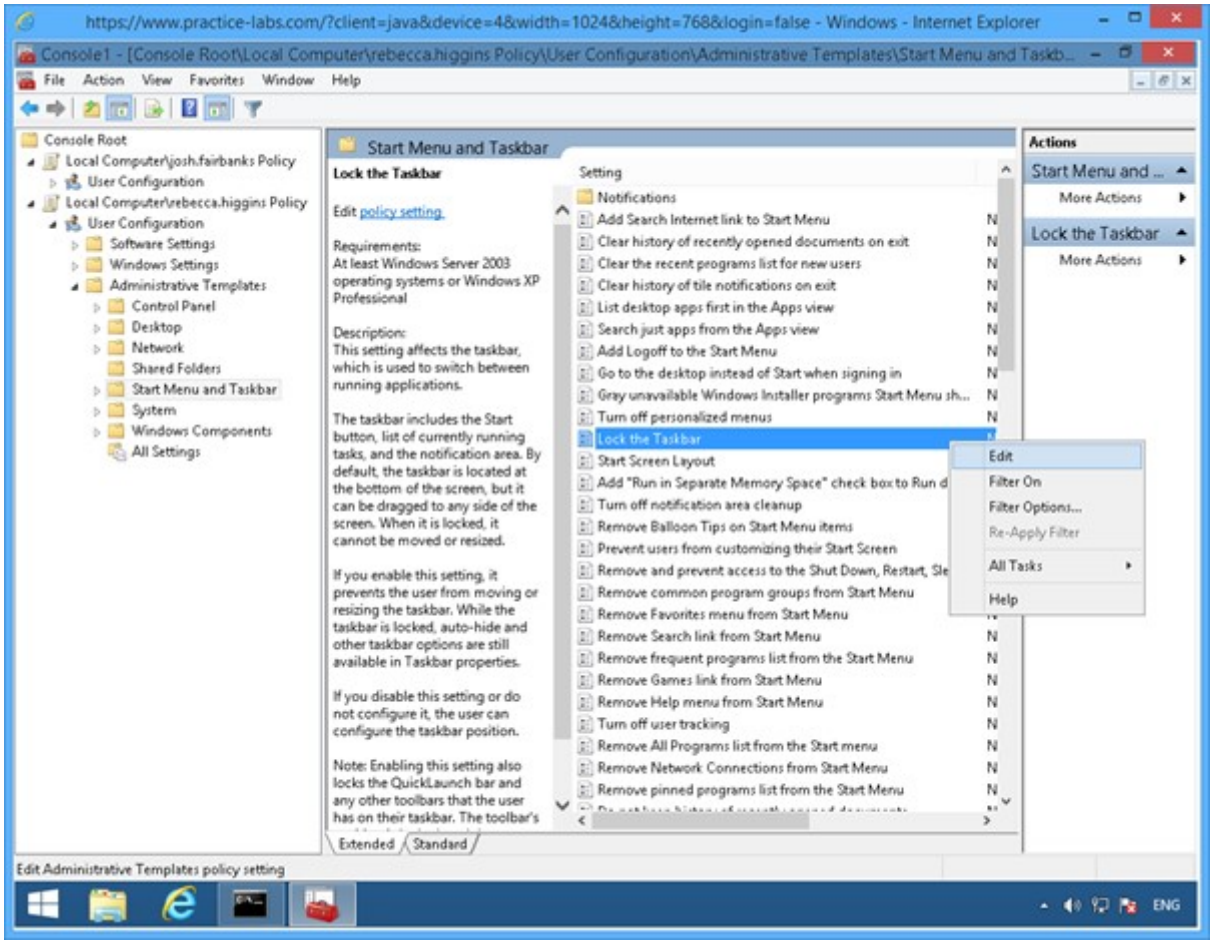


Step 16

You are redirected back to the **Console1** window.

Now expand **Local Computer\Rebecca.Higgins Policy** > **User Configuration** > **Administrative Templates** and click **Start Menu and Taskbar** folder.

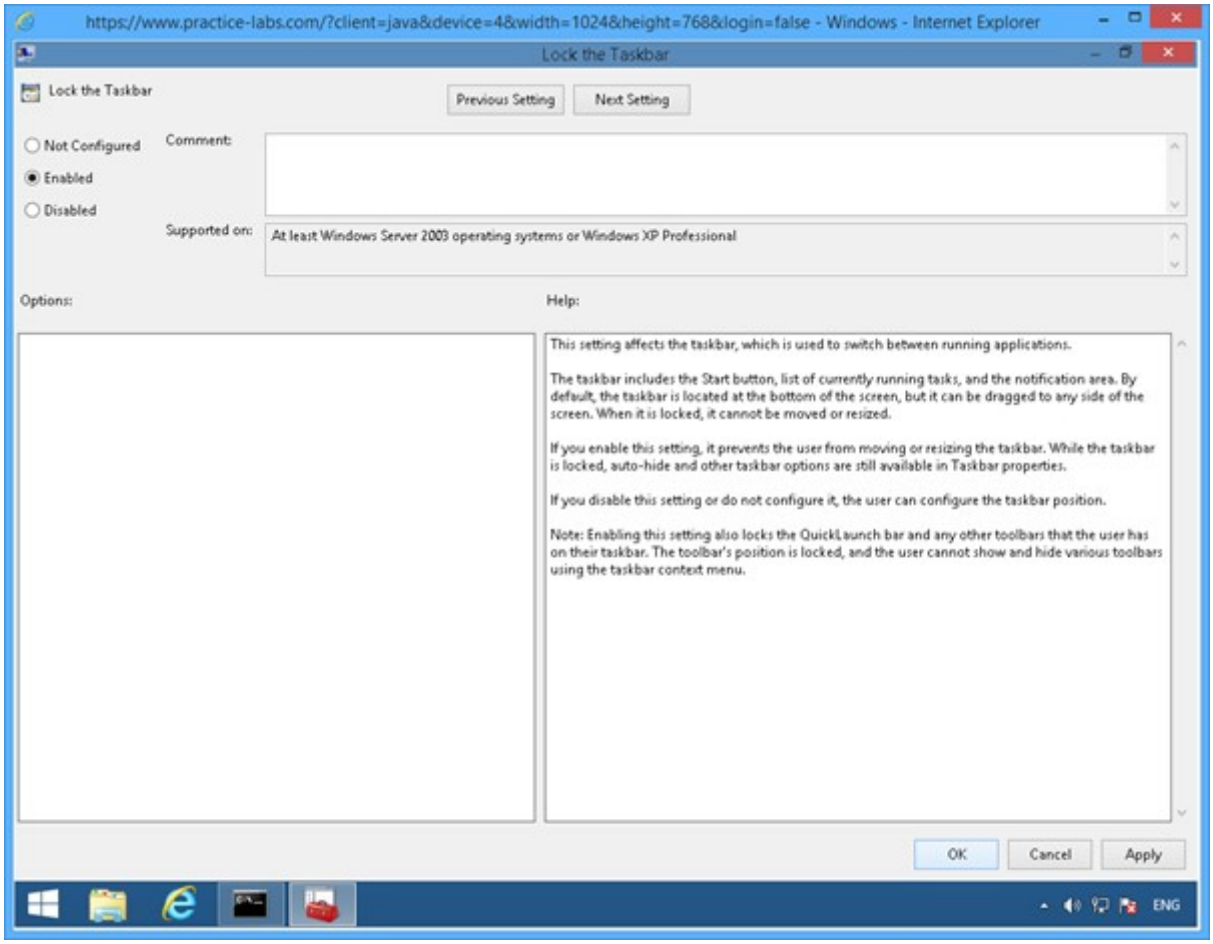
On the details pane, right-click on **Lock the Taskbar** and choose **Edit**.



Step 17

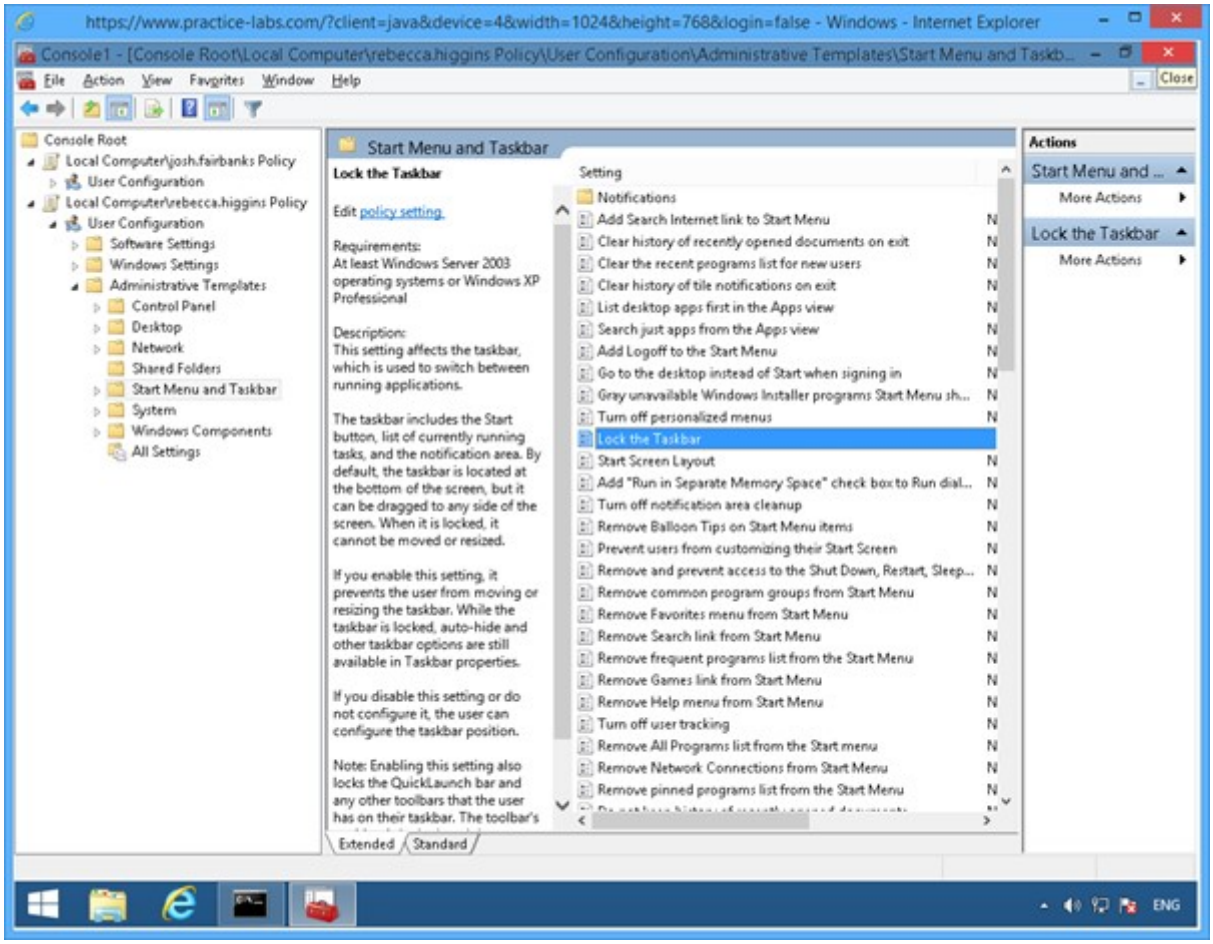
On the **Lock the Taskbar** dialog box, click **Enabled** option.

Click **OK**.



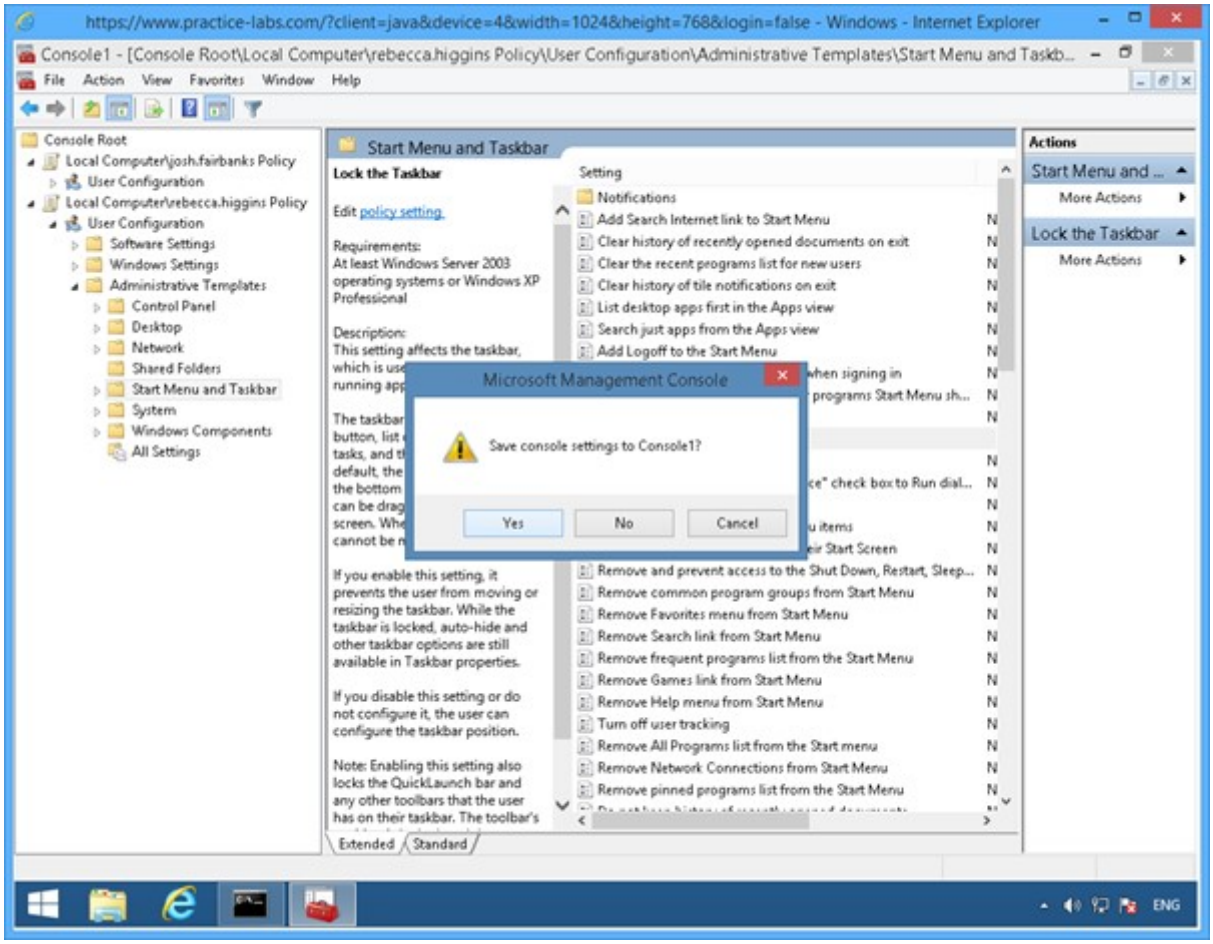
Step 18

After creating the local group policy for the two users, close **Console1** window.



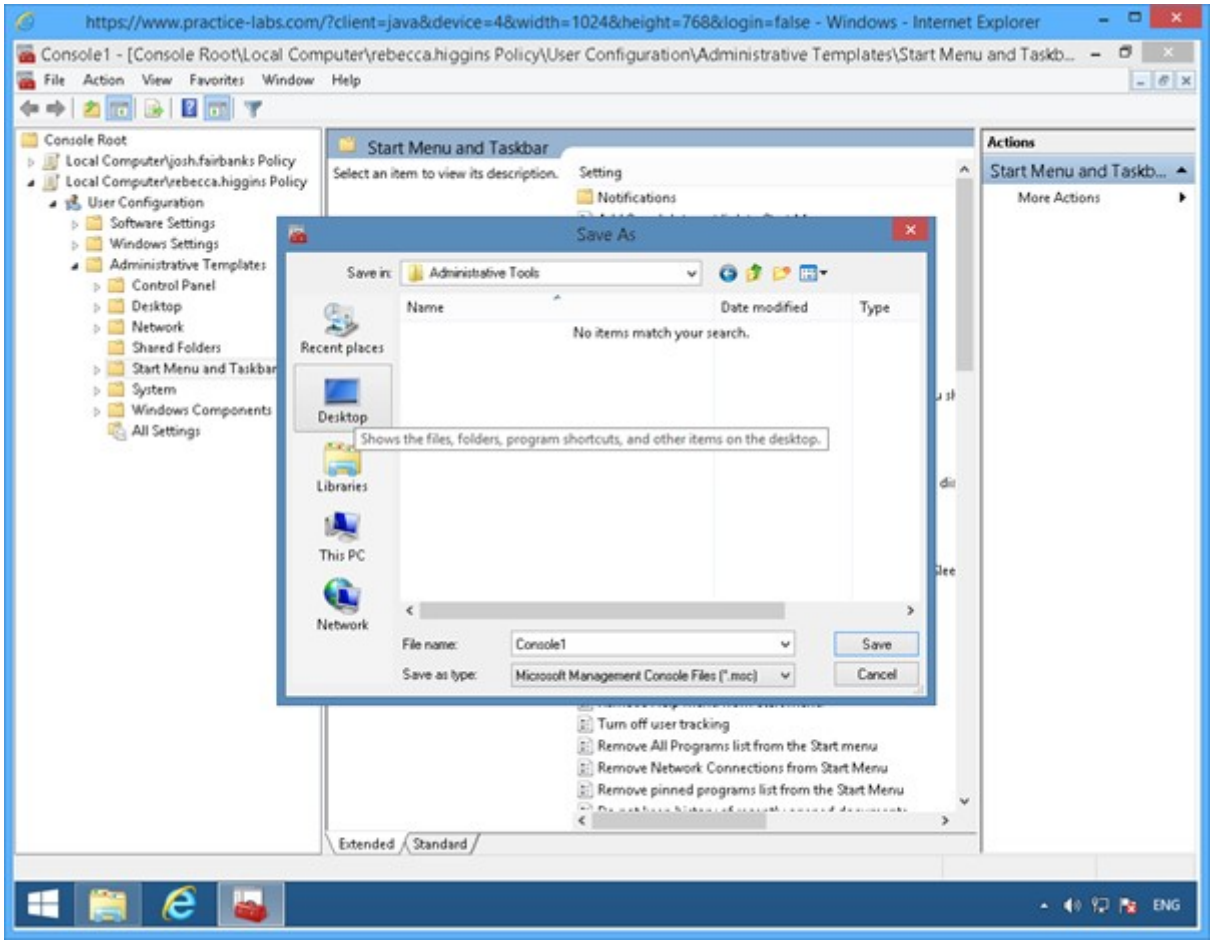
Step 19

When asked to save console settings to Console1, click **Yes**.



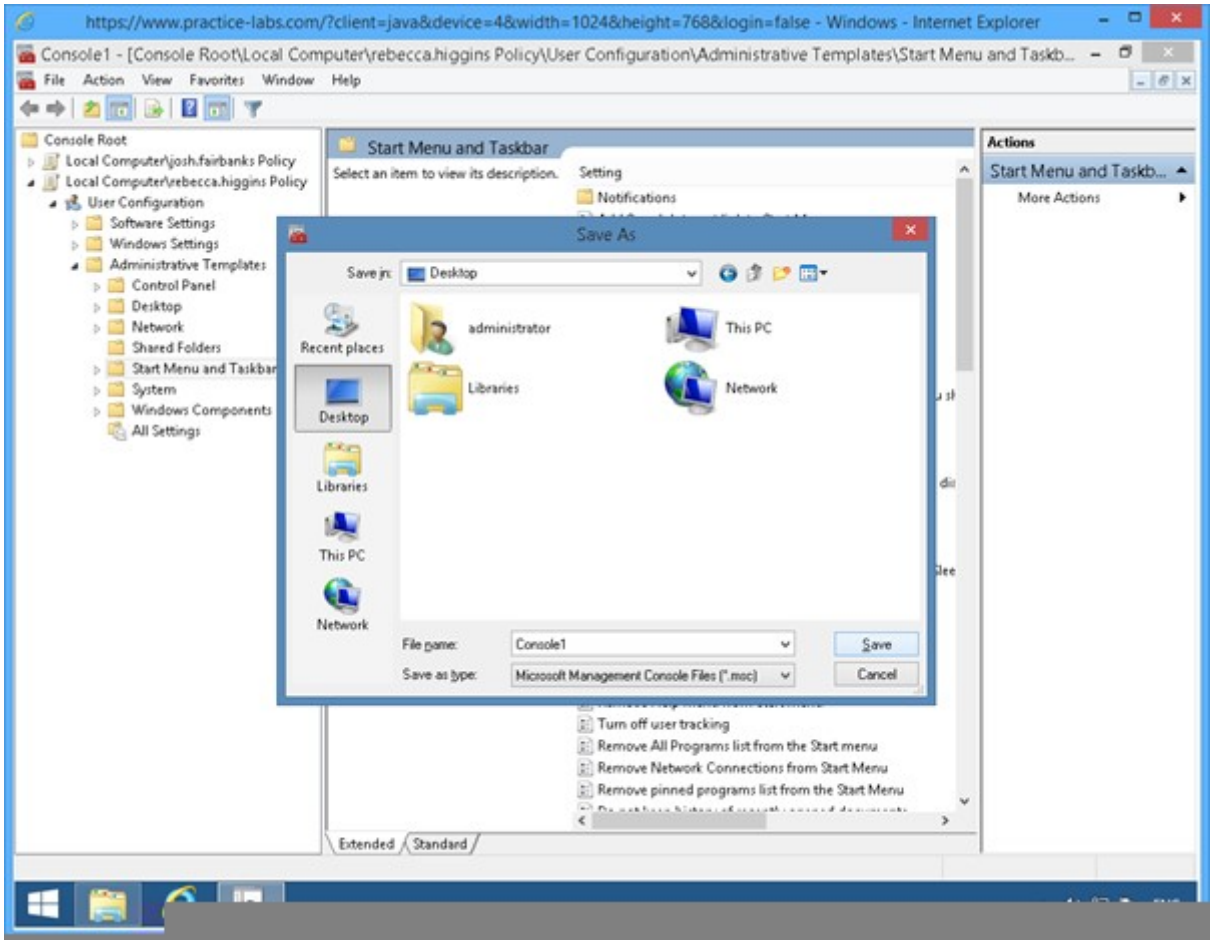
Step 20

On the **Save As** dialog box, click **Desktop** on the left panel.



Step 21

When Desktop is selected, keep the default file name and click **Save**.



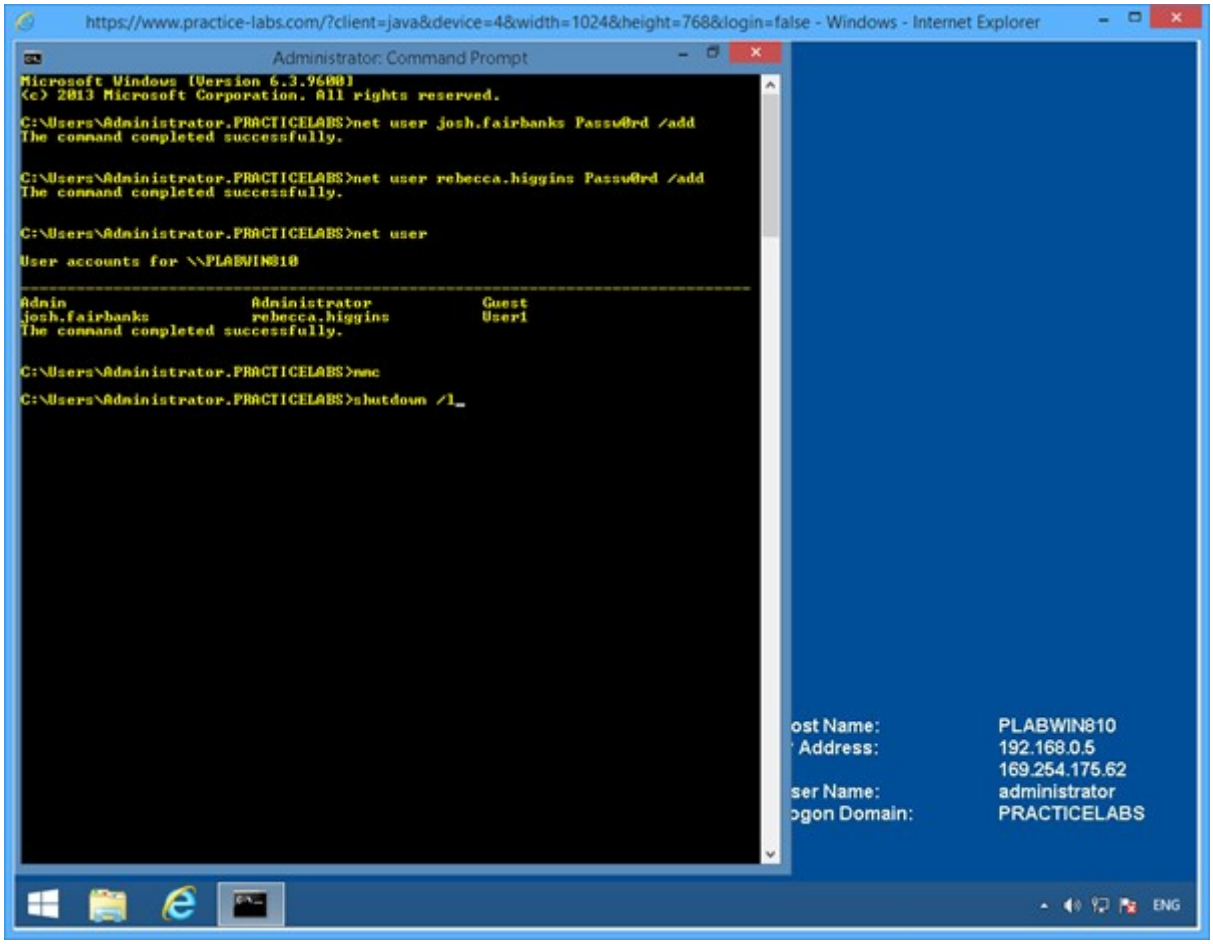
Step 22

Back on the command prompt window, you will sign out the currently signed on user to test the local group policy that were created for Josh and Rebecca.

To sign out, type:

```
shutdown /l
```

Press **Enter**.



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

Task 3 - Verify Local GPO

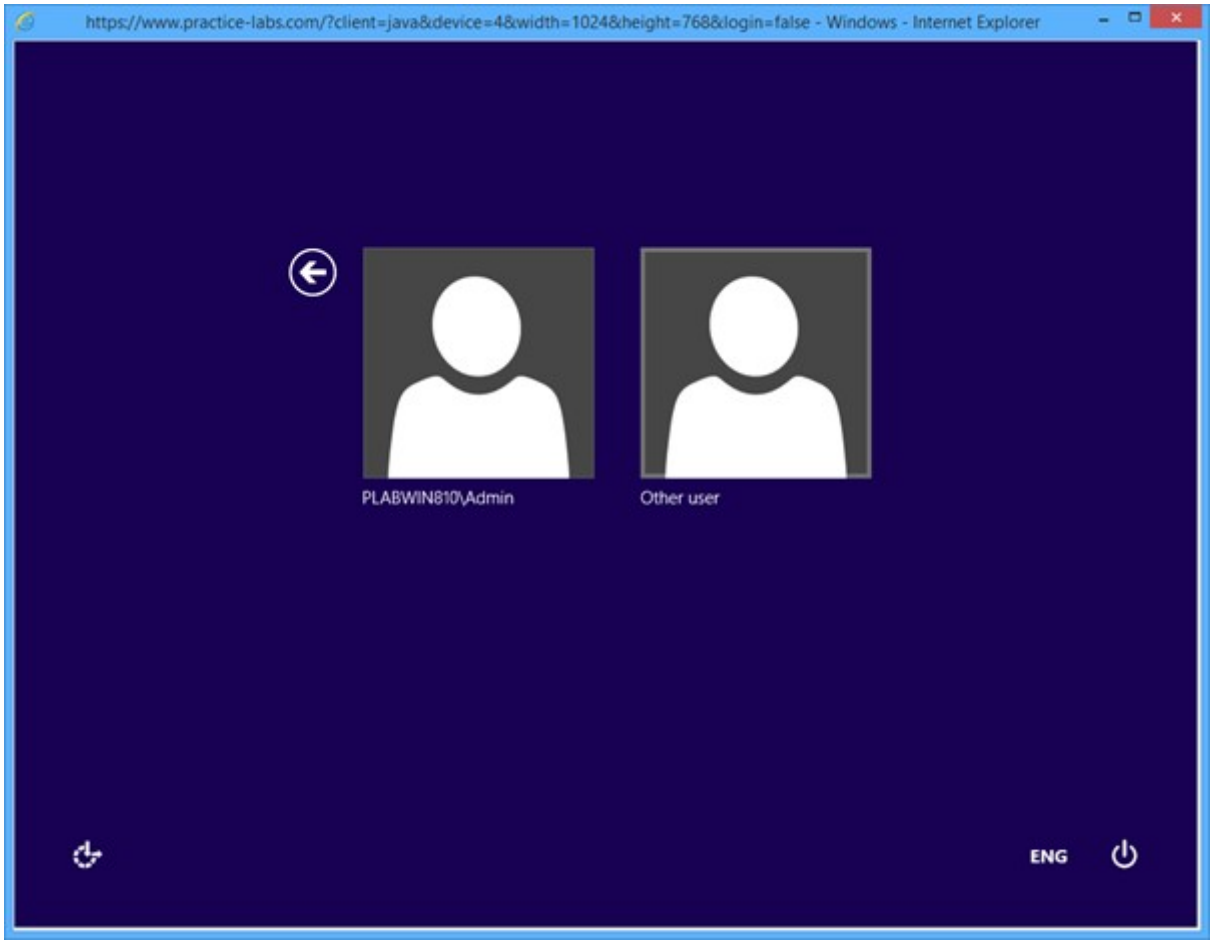
In this task, you will sign on as josh.fairbanks to verify if the local GPO is applied.

To verify the application of the local GPO, perform the following steps:

Step 1

Connect to **PLABWIN810** device using the Practice Labs web application.

On the sign-on page, click **Other user**.



Step 2

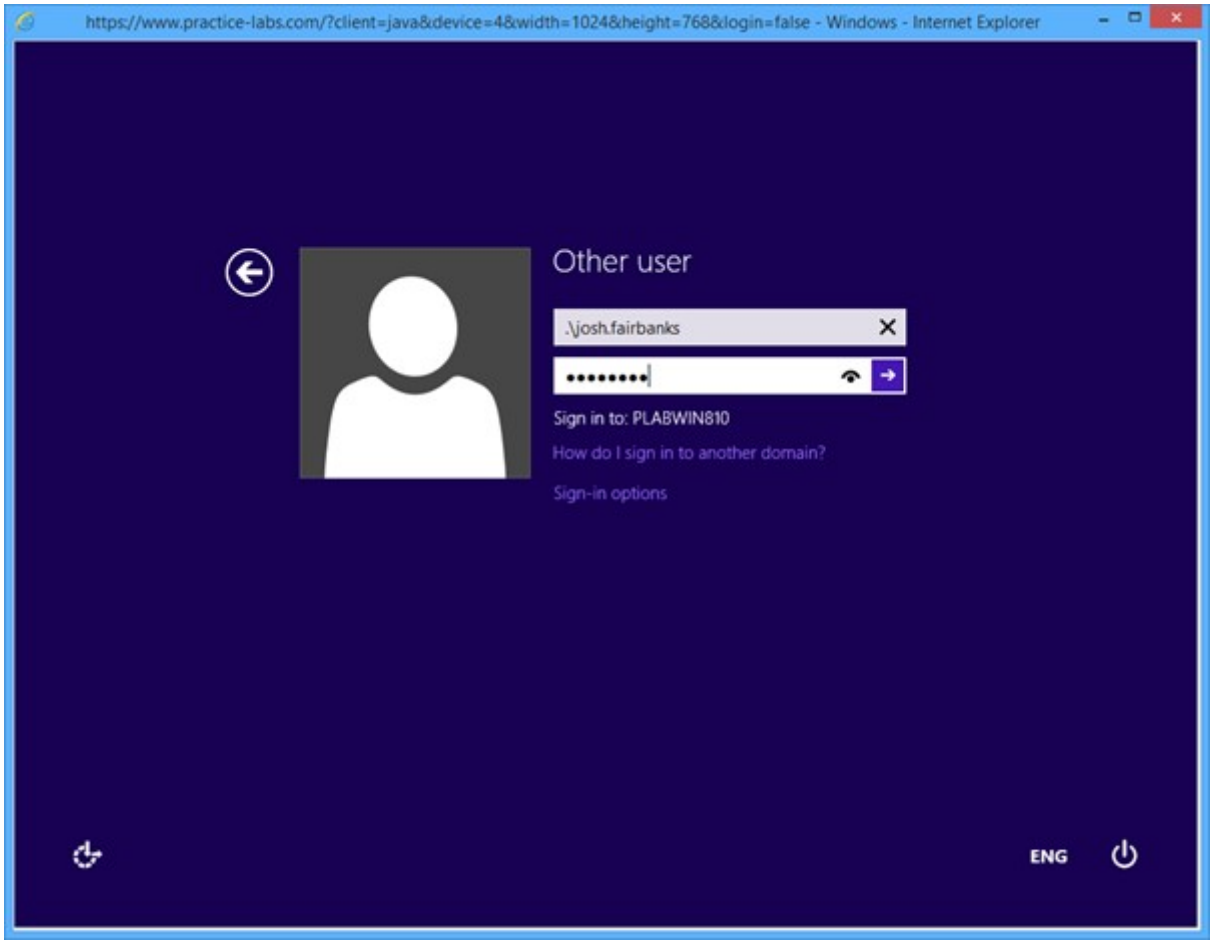
On the User name box, type

```
.\josh.fairbanks
```

On the Password box, type

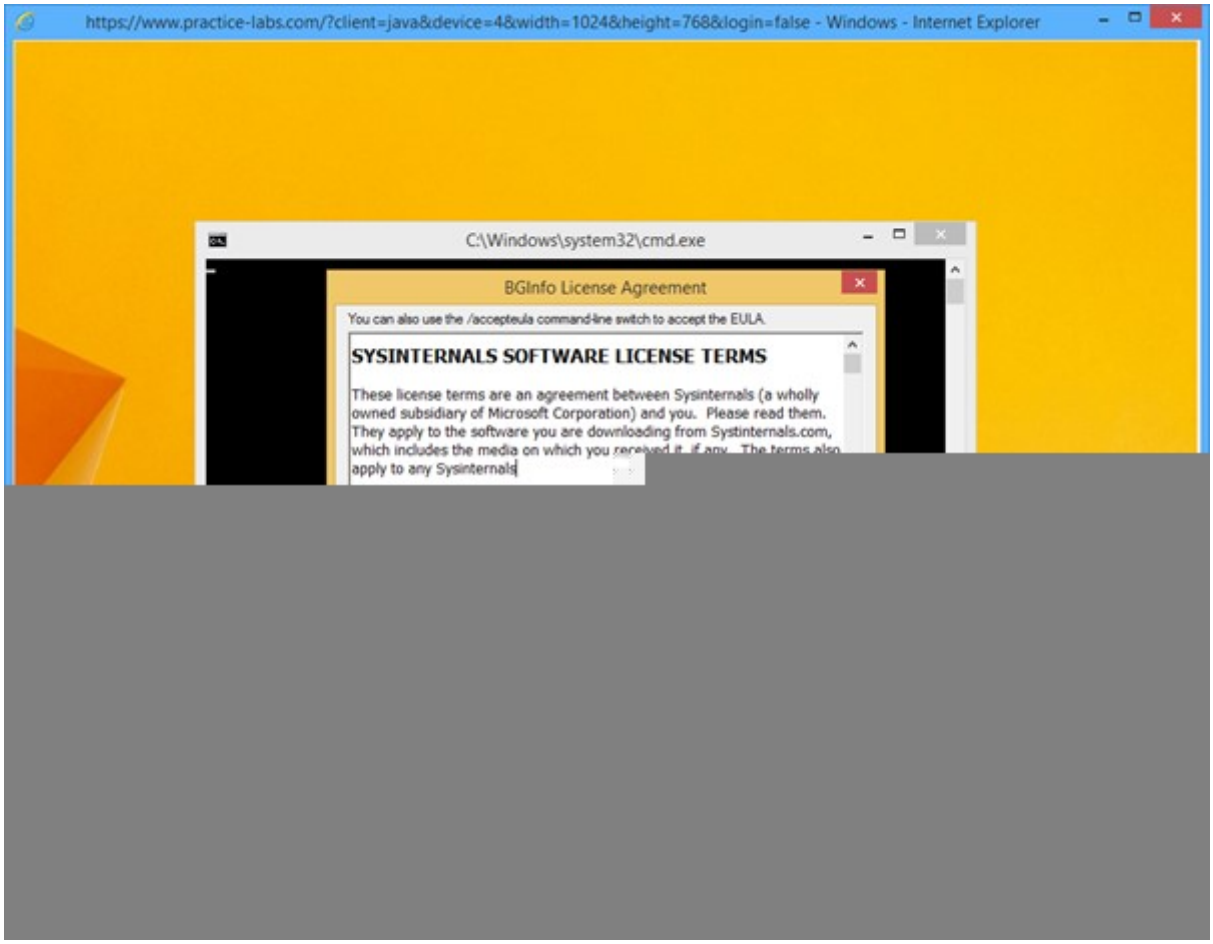
```
Passw0rd
```

Press **Enter**.



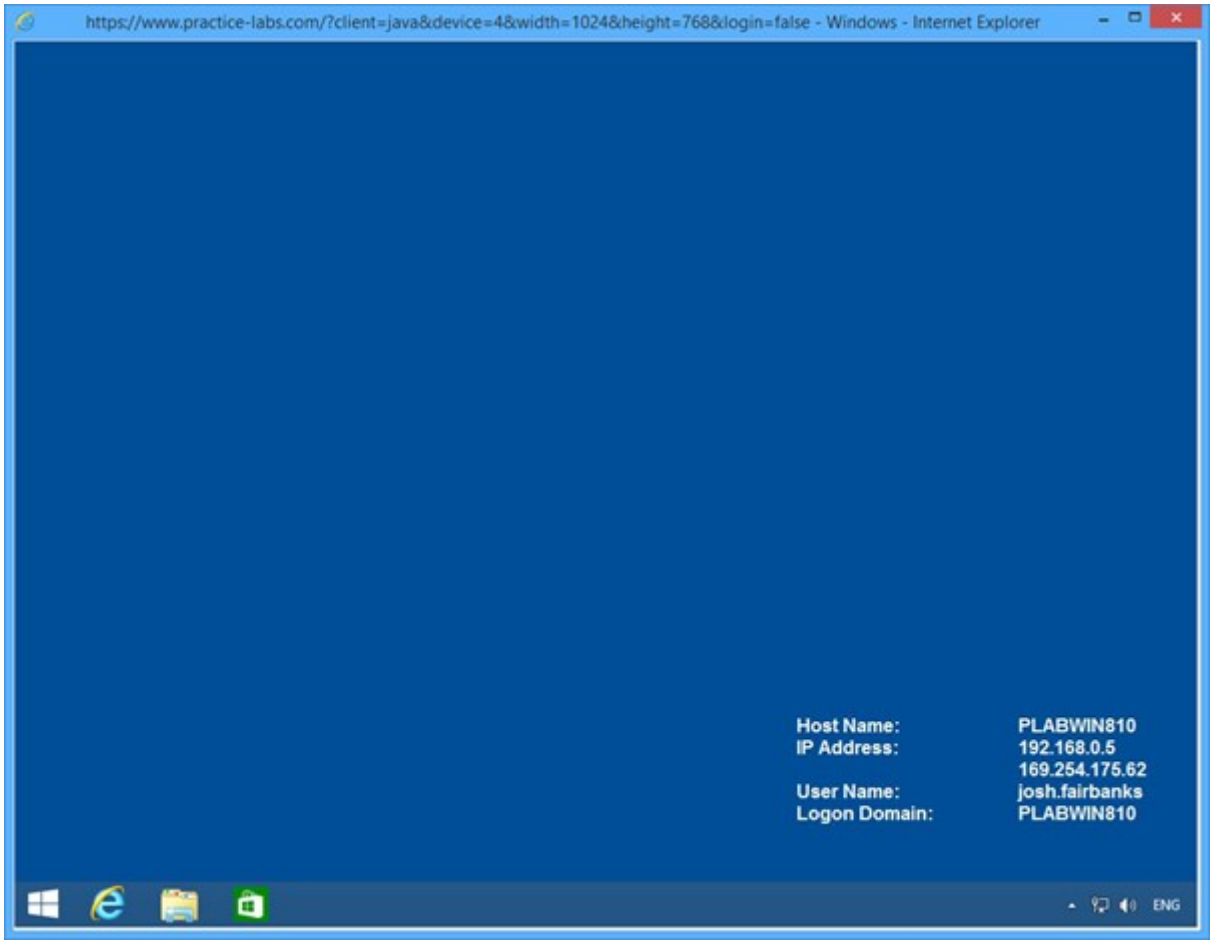
Step 3

When presented with the **BGInfo License Agreement** dialog box, click **Agree**.



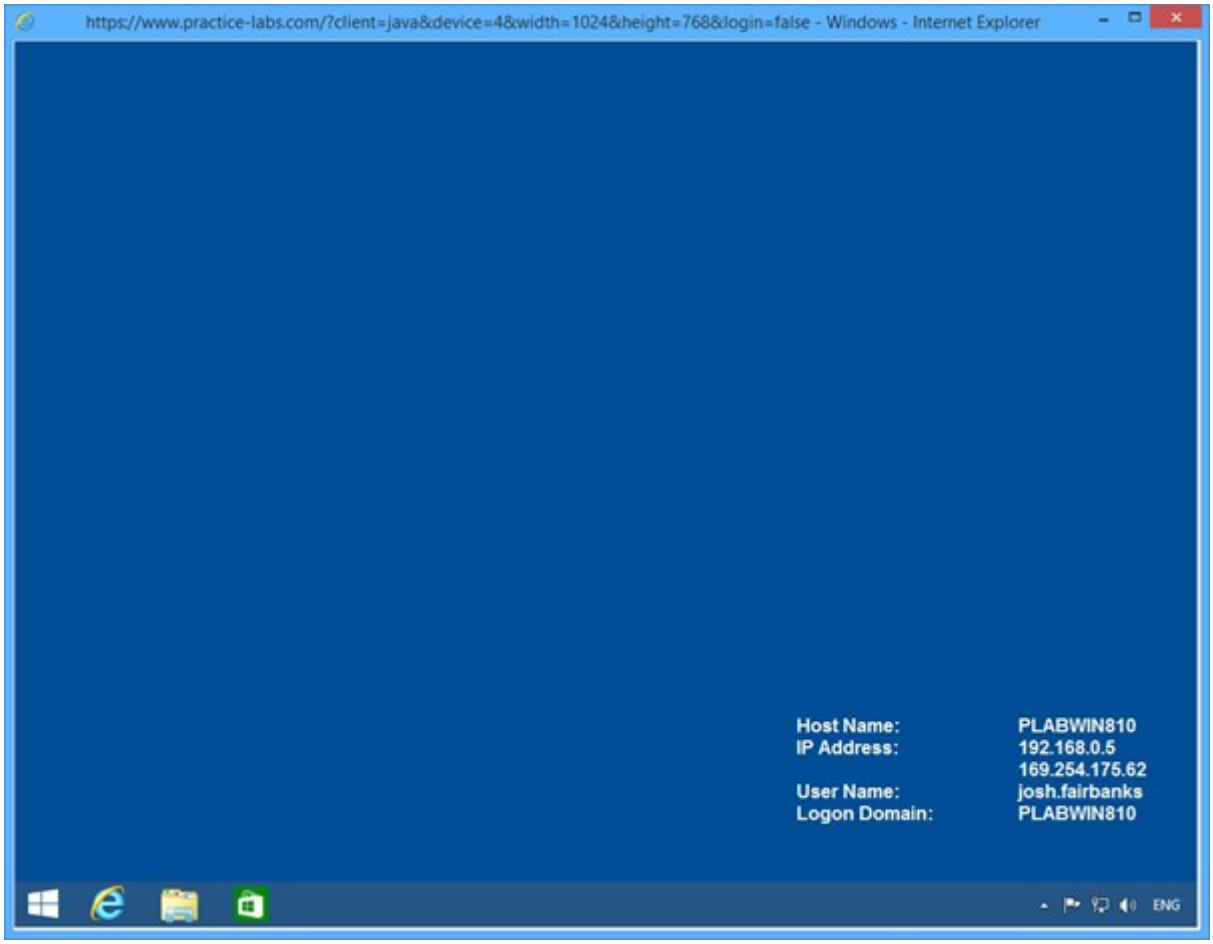
Step 4

Verify that no icons are visible on desktop.



Step 5

Right-click on desktop and notice that no shortcut menus appear.



Step 6

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

Step 7

Connect to **PLABWIN810** device using the Practice Labs web application.

On the sign-on page, click **Other user**.

Step 8

On the User name box, type

```
.\rebecca.higgins
```

On the Password box, type

```
Passw0rd
```

Press **Enter**.

Step 9

When presented with the **BGInfo License Agreement** dialog box, click **Agree**.

Step 10

Right-click the taskbar and notice that the option "**Lock the taskbar**" is greyed out.

This means that the local group policy for Rebecca Higgins is applied.

Step 11

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

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

Task 4 - Remove PLAB Users Starter GPO

You will remove the PLAB Users GPO that was linked earlier to Marketing OU to avoid conflicts in the next exercise about security filtering.

To remove the starter GPO, perform the following steps:

Step 1

Connect to **PLABDC01**.

On the sign on screen, click **PRACTICELABS\Administrator**.

Step 2

On the Password field, type:

```
Passw0rd
```

Press **Enter**.

Step 3

On **Server Manager - Dashboard**, click **Tools** and select **Group Policy Management**.

Step 4

On **Group Policy Management** console, expand to **Forest: PRACTICELABS.COM > Domains > PRACTICELABS.COM > Marketing** if you are not in the group policy path.

Under **Marketing** OU, right-click **PLAB Users** and select **Delete**.

Step 5

Click **OK** to delete the group policy object link with **Marketing** OU.

Step 6

Keep **Group Policy Management** console window open for the next activity.

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

Exercise 5 - GPO Security Filtering

Security filtering feature in Group Policy Objects is a powerful feature that allows you limit the application of group policy objects to selected users or security groups in an Active Directory domain.

In this exercise, you will exempt a security group from inheriting a group policy object rule that is linked on the domain level of a Active Directory,

Please refer to your course material or use your favourite search engine to research for more information about this topic.

Task 1 - Configure Security Filtering

In this lab, some organizational units have been pre-created to meet the requirements of implementing Group Policy Objects in the domain.

To set up security filtering in GPO, perform the accompanying steps:

Step 1

On the **PLABDC01** device, the **Group Policy Management** console is open.

On the **Group Policy Management** console, right-click **PRACTICELABS.COM** node and select **Create a GPO in this domain and link it here**...

Step 2

On **New GPO** box, type:

```
Screen Saver disabled
```

Click **OK**.

Step 3

Under the **PRACTICELABS.COM** domain node, click on **Screen saver disabled.**

Important: This policy about **Screen saver disabled** will apply, by default, to all users in the **PRACTICELABS.COM** domain. Later, you will configure Security Filtering so that the policy will apply only to a selected group in the domain.

If reminder about group policy object links appears, click **Do not show this message again** check box.

Click **OK**.

Step 4

Under the **PRACTICELABS.COM** domain node, right-click on **Screen Saver disabled** and select **Edit**.

Step 5

On the **Group Policy Management Editor** window, expand to **User Configuration** > **Policies** > **Administrative Templates** > **Control Panel** and click **Personalization** folder.

On the details pane on the right, right-click on **Enable screen saver** and select **Edit**.

Step 6

On the **Enable screen saver** dialog box, click **Disabled** option.

Click **OK**.

Step 7

You will be redirected back to the **Group Policy Management Editor** window.

The policy is now enabled.

Close **Group Policy Management Editor** window.

Step 8

You will directed back in Group Policy Management console.

Under **PRACTICELABS.COM** node and select **Screen saver disabled.**

On the right details pane, locate **Security Filtering** section.

Step 9

Under **Security Filtering** section, select **Authenticated Users** and click **Remove** button.

Step 10

On the **Group Policy Management** dialog box, click **OK** to remove this delegation privilege.

Step 11

Go back in **Security Filtering** section and click **Add**...

Step 12

On **Select User, Computer or Group** dialog box, type:

```
gengineering
```

Click **Check Names**.

Step 13

When the **GEngineering** group is underlined, click **OK**.

Step 14

The Security Filtering now contains only **GEngineering** group.

This means that the policy **Screen saver disabled** will apply to members of the **GEngineering** security group.

Close **Group Policy Management** Editor.

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

Task 2 - Verify Security Filtering

In this task, you will sign on to Windows 8.1 device using an account which is a member of the **GEngineering** group. You will verify that the policy Screen saver

disabled is applied to the members of the said group.

To verify security filtering for a group, perform the following steps:

Step 1

Connect to **PLABWIN810** using the Practice Labs web application.

On the sign-on page, click **Other User**.

Step 2

On the User name box, type:

```
jan.regus
```

On the Password field type:

```
Passw0rd
```

Press **Enter**.

Step 3

When the user is successfully signed on, right-click on desktop and select **Personalize**.

Step 4

On the **Personalization** page, locate **Screen Saver** section.

Notice that there is an icon indicating that Screen saver is unavailable for this user.

Nonetheless, click **Screen Saver** web link.

Step 5

On **Screen Saver Settings** dialog box, verify that the controls are unavailable.

Because of the GPO assigned to the domain but filtered to apply to **GEngineering** group, a user named **Jan Regus** will have no option to change the Screen saver settings.

Click **OK**.

Step 6

Right-click **Start** charm and select **Command prompt**.

Step 7

You will now verify the policies that are applied to the user named Jan Regus.

On the command prompt, type:

```
gpresult /z > results.txt
```

Press **Enter**

The above command will collect the group policy objects applicable to the user in verbose mode and save them in results.txt file.

Step 8

You will not receive a confirmation whether the command was successful. This is the default system behaviour.

On the next prompt to view the results.txt, type:

```
notepad results.txt
```

Press **Enter**.

Step 9

On the **results-Notepad** window, locate **USER SETTINGS > Applied Group Policy Objects** section.

Notice that **Screen saver disabled** is listed.

Step 10

To try other user accounts who are not members of the **GEngineering** group, you will sign out the current user.

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

Step 11

Connect again to **PLABWIN810** and click **Other User** from the sign on screen.

Step 12

On the **User name** box, type:

```
john.smith
```

On the Password field type:

```
Passw0rd
```

Press **Enter**.

Step 13

Click **Agree** if the **BGInfo License Agreement** appears.

Step 14

Right-click on desktop and choose **Personalize**.

Step 15

On the **Personalization** window, click **Screen Saver**.

Step 16

On the **Screen Saver Settings** dialog box, verify that the controls are available.

Click **OK**.

This means that Security Filtering works as John Smith who is not a member of the **GEngineering** group can change the screen saver settings.

Shut down all the virtual machines to revert these devices to their default state using Practice Labs web application.

Summary

In this exercise, you learnt to configure the following:

- Create a GPO Central Store
- Manage Starter GPOs
- Configure GPO links
- Configure multiple local group policies
- Configure security filtering