* [Access your Practice Lab titles](https://uoplabs.practice-labs.com/authenticated/vNext/vn-content.aspx" \l "tabpanel-titlenavigation)
* [Access your exercise content](https://uoplabs.practice-labs.com/authenticated/vNext/vn-content.aspx#tabpanel-titlecontent)
* [Access your reports](https://uoplabs.practice-labs.com/authenticated/vNext/vn-content.aspx#tabpanel-reports)
* [Access your settings](https://uoplabs.practice-labs.com/authenticated/vNext/vn-content.aspx#tabpanel-settings)
* [Access help and support](https://uoplabs.practice-labs.com/authenticated/vNext/vn-content.aspx#tabpanel-help)

Infrastructure Admin

Week 3 - Access Control and PKI

Week 3

**Week 3**

**Access Control and PKI**

Ensuring that authorized users have access to needed files while protecting from unauthorized access is a large part of infrastructure administration.

For on-premise solutions, this can be supplemented by an Identity and Access Management service. For cloud based solutions, accessible by anyone with an internet connection, access control is much more important.

This lab will allow you to create some Windows Active Directory domain accounts and file shares. Then you will assign specific permissions and test them. Finally, you will get to experience encryption using public/private key pairs.

***Step 1 - Practice Labs Configuration Change***

Then click the “Off” switch in the “Device” section labelled “Server Auto Login”.

***Step 2 - Launch lab environment***

Connect to your **CYB205**practice lab and click the “Power on all devices” button. It may take several minutes for all of the devices to completely boot up.

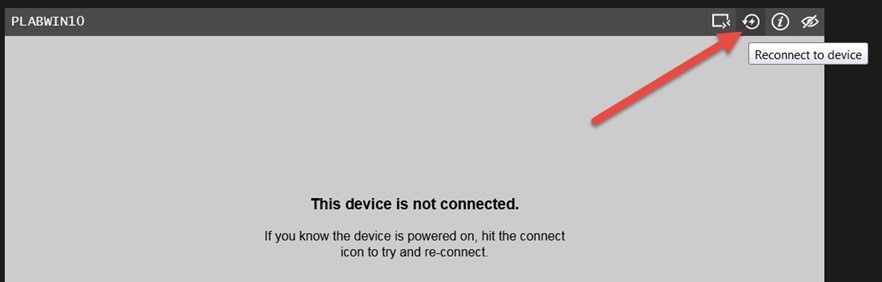
You will see three devices:

* **PLABDC01**- A Windows server functioning as the Active Directory domain controller.
* **PLABWIN10**- A Windows 10 client computer and member of the Active Directory domain.
* **PLABCENTOS**- A Centos Linux system on which we will be running Nessus.

***Step 3 - Login to PLABDC01 as Administrator***

One of the core components of an Active Directory system is a Domain Controller. Most Active Directory configurations will have multiple Domain Controllers for redundancy and load balancing. However, your environment is small and only has one.

Scroll down until you see the login screen for **PLABDC01**. If you see a grey screen which displays “Device is not Connected,” click on the “Reconnect to device” icon in the upper right corner.

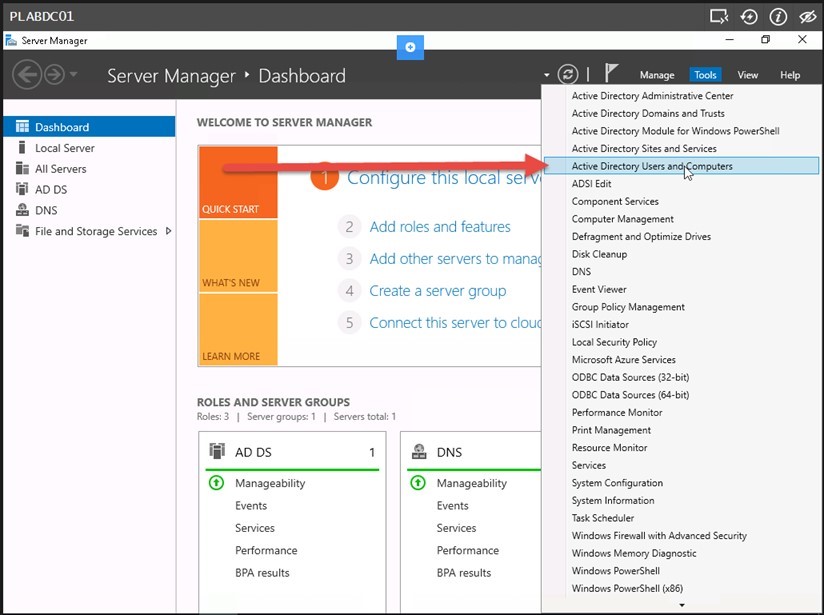


Enter **Passw0rd**in the Password field, then press Enter.

***Step 4 - Launch Active Directory User’s and Computers***

Active Directory Users and Computers is the primary means of administering user accounts, groups, organizational units, and computers within Microsoft’s Active Directory.

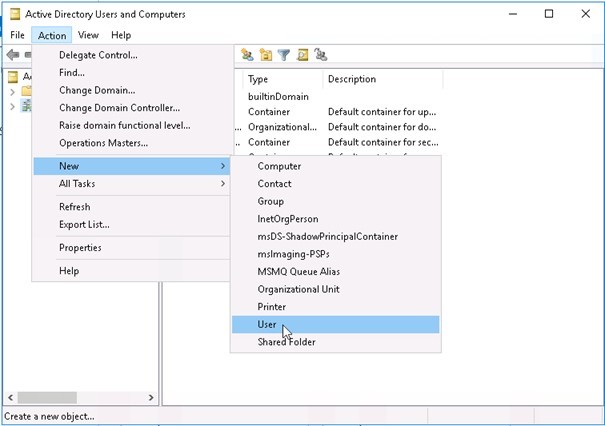
From the Server Manager Dashboard (Displayed by default after logging in), click the “Tools” pull-down menu, then click “Active Directory Users and Computers”.



The Active Directory Users and Computers console will load, and you should notice that this is the PRACTICELABS.COM domain.

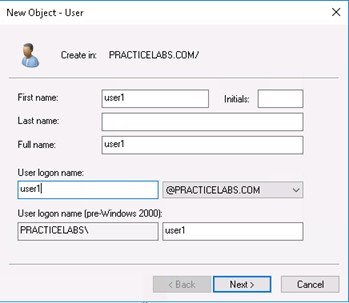
***Step 5 - Create users***

With the PRACTICELABS.COM domain highlighted in the left pane, select the “Users” container in the right pane. Next, click the “Action” pull-down menu, then click “New” and “User”.

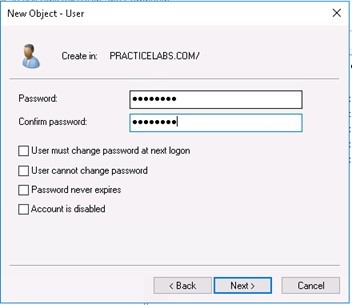


For this lab, we will create three users: user1, user2, and user3.

Begin by entering user1 in the “First Name” field. Notice this will automatically populate the “Full Name” field as well. Enter user1 again in the “User Logon Name” field, and click the “Next” button.



Enter **Passw0rd**in both the “Password” and “Confirm Password” fields, then be sure to **UNCHECK**the “User must change password at next logon” box. Click the “Next” button.



*Note: Passw0rd is an absolutely AWFUL password to ever use in the real world, but it is easy to remember for a lab environment such as this. In any production environment, make certain to use long passwords (10 characters or more), without dictionary words, which blend upper case letters, lower case letters, numbers, and symbols.*

Click the “Finish” button.

Now repeat this process to create entries for user2 and user3.

***Step 6 - Verify User Entries***

Double click on the “Users” object in the right pane of Active Directory Users and Computers. This will expand the PRACTICELABS.COM domain listing in the left pane and display a list of all domain users in the right pane.

Scroll down until you see your three newly created users.

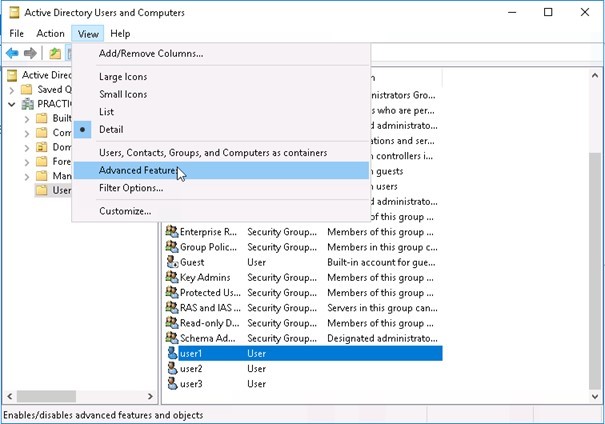
*ACTION: Capture a screenshot for your assignment. (On Windows use <ALT PrtSc> and then paste into Word. On Mac, use <SHIFT><COMMAND>4 and select the area you wish to capture. The .png image file will appear on your desktop)*

Double click on one of the users you created. This will open a new window showing the user properties.

*ACTION: Capture a screenshot for your assignment. (On Windows use <ALT PrtSc> and then paste into Word. On Mac, use <SHIFT><COMMAND>4 and select the area you wish to capture. The .png image file will appear on your desktop)*

Explore the different tabs of user properties. Then write a paragraph explaining many of the types of information which can be stored in an Active Directory user record. Click the “Cancel” button.

Click the “View” pull-down menu and click “Advanced Features”.



You will now see many additional options. Double click on the “Users” container in the right pane, find the users you created, and double click the same user you looked at in the previous step.

Do the tabs look the same?

*ACTION: Capture a screenshot for your assignment. (On Windows use <ALT PrtSc> and then paste into Word. On Mac, use <SHIFT><COMMAND>4 and select the area you wish to capture. The .png image file will appear on your desktop)*

Explore the tabs again and write a paragraph describing the additional tabs which are now available in “Advanced Features” mode.

Click the “Cancel” button. Close Active Directory Users and Computers.

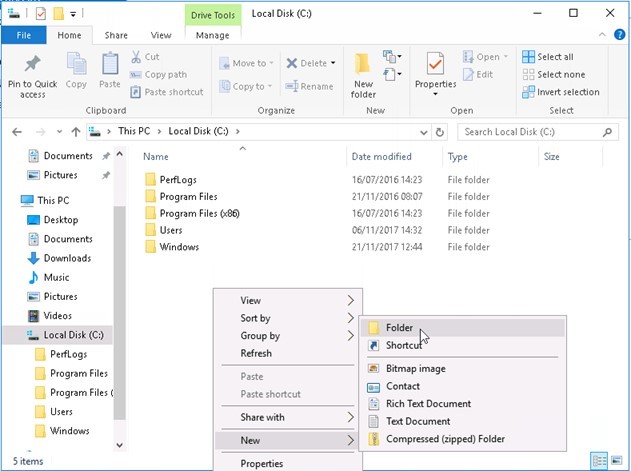
***Step 7 - Create a local shared folder and assign permissions***

Now we are going to make some files available to access over the network from this server.

*NOTE: Since this is the only server we have in your test environment, we will be using the Domain Controller as a file server, too. It is not usually a good idea to share resources from your Domain Controllers, as this could expose them to attack.*

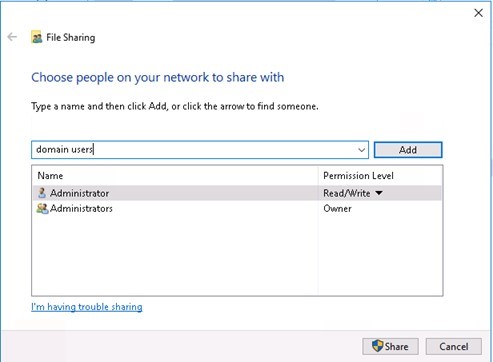
Click the yellow “File Explorer” icon in the task bar at the bottom of the console for **PLABDC01**. Double-Click “This PC” and “Local Disk (C:)”.

Right-click in the right pane (Below the “Windows” folder), then click “New” and “Folder”.



Rename your new folder Shared. Right click on the “Shared” folder and choose “Properties”. Click on the “Sharing” tab and then click the “Share” button. This will open a File Sharing dialog box.

We want to make sure that all users in the domain can access this file share, so type Domain users into the field and click the “Add” button.

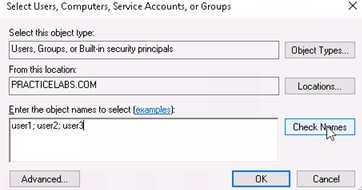


You will see the “Domain Users” group now has read permissions to the share. Click the down arrow to the right of this “Read” permission and change it to “Read/Write”, then click the “Share” button. You will see the folder is now shared. Click the “Done” button.

We have set the network share level permissions. Now it is time to set the filesystem permissions. Click the “Security” tab then click the “Edit” button.

In the “Group or user names” box, click “Domain Users” and then click the “Remove” button. Now, click the “Add” button. This will open a new dialog box.

In the “Enter the object names to select” box, enter user1; user2; user3 then click the “Check Names” button.

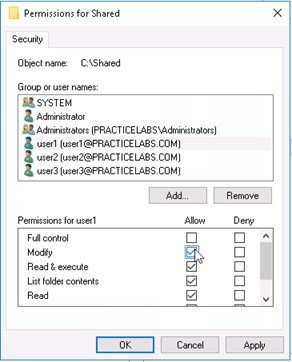


Notice what happens to your entries. This process allows you to quickly add multiple users.

*ACTION: Capture a screenshot for your assignment. (On Windows use <ALT PrtSc> and then paste into Word. On Mac, use <SHIFT><COMMAND>4 and select the area you wish to capture. The .png image file will appear on your desktop).*

Click the “OK” button. Your dialog box will close.

We want to assign very specific permissions to each of these users. Click on “user1” and then click the “Modify” check box under the “Allow” column.



This will give user1 the ability to read, write, and execute files in this folder.

Now, click on “user2” and verify that only the “Read & execute”, “List folder contents”, and “Read” checkboxes are checked.

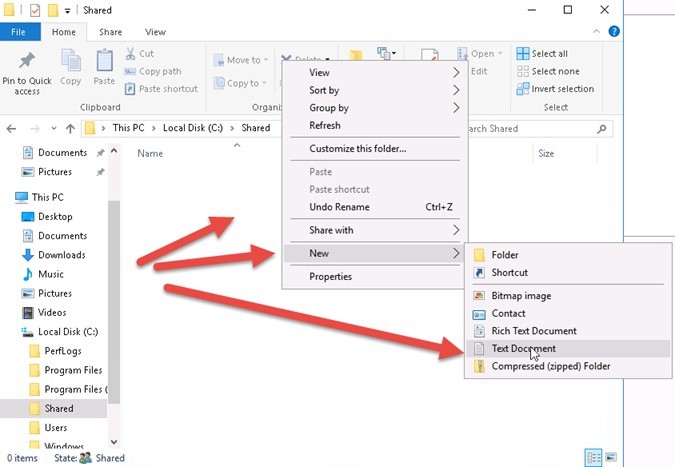
Finally, click on “User3” then click the checkbox for “Full Control” under the “Deny” column. Notice how this chances all options to “Deny” for this user.

Click the “OK” button. Carefully read the pop-up dialog about deny permissions.

*ACTION: Capture a screenshot for your assignment. (On Windows use <ALT PrtSc> and then paste into Word. On Mac, use <SHIFT><COMMAND>4 and select the area you wish to capture. The .png image file will appear on your desktop).*

Now click the “Close” button.

Finally, we need to put a file in the folder. Double click on the “Shared” folder. You will notice that the folder is completely empty. Right click anywhere in that empty space and choose “New” then “Text Document”.

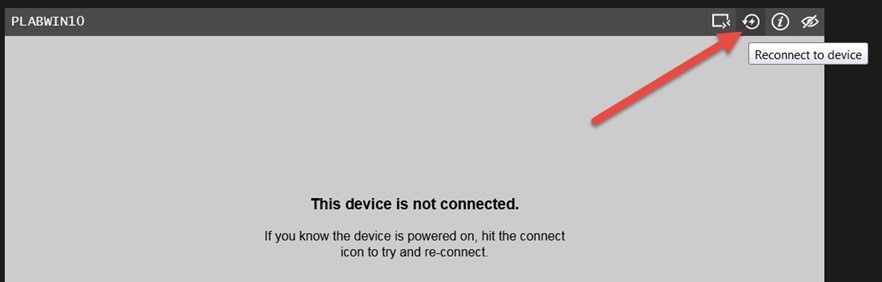


Rename the document “Test”. Now double click the “Test” document and type some text into it. Save the document and exit Notepad.

***Step 8 - Login to PLABWIN10 as Administrator***

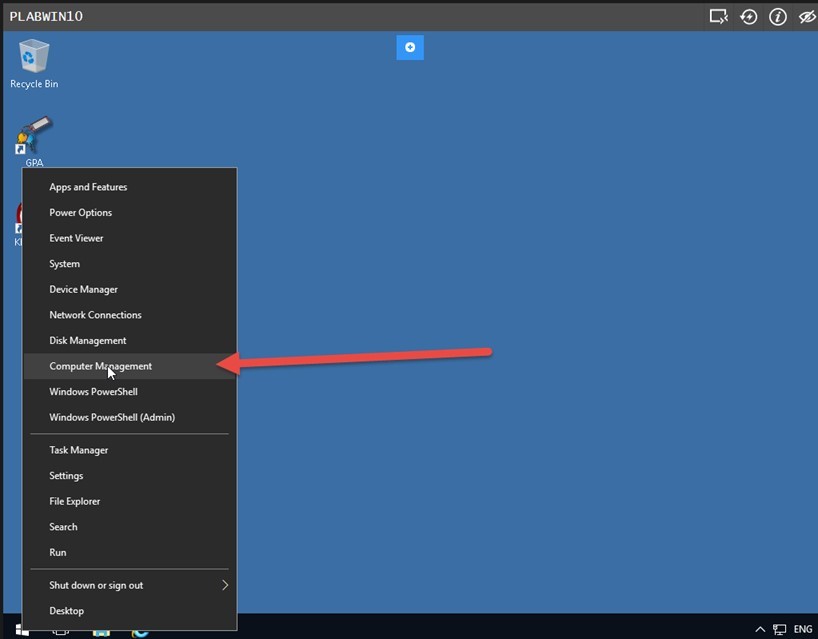
In order for your newly created domain users to login remotely to a system, they will need special permissions. We are going to make them local administrators on the Windows 10 system.

Scroll down until you see the login screen for **PLABWIN10**. If you see a grey screen which displays “Device is not Connected,” click on the “Reconnect to device” icon in the upper right corner.

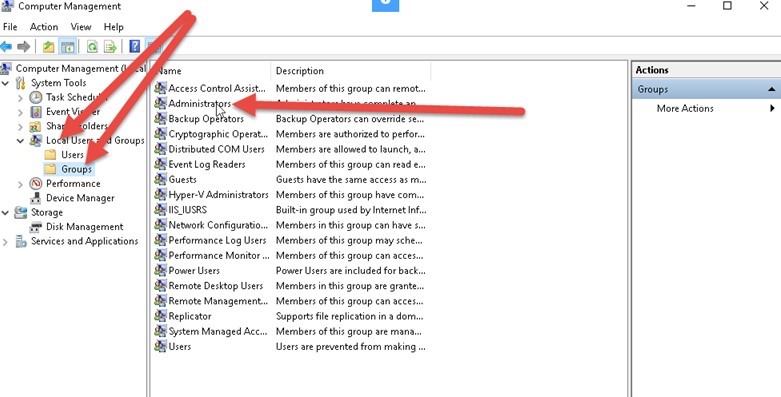


Enter **Passw0rd**in the Password field, then press Enter.

Right click the start button, then click on “Computer Management”.

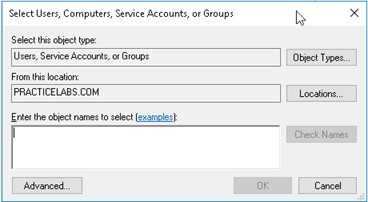


When the Computer Management console opens, expand “Local Users and Groups”, then click “Groups” and double click “Administrators” (Right Pane).



Click the “Add” button. Do you recognize this dialog box? It is the same as when we added our users to the filesystem permissions.

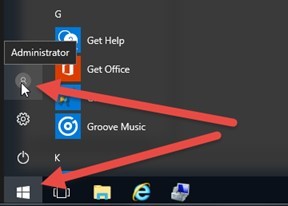
Enter them here the same way and click the “Check Names” button, then click the “OK” button.



*ACTION: Capture a screenshot for your assignment. (On Windows use <ALT PrtSc> and then paste into Word. On Mac, use <SHIFT><COMMAND>4 and select the area you wish to capture. The .png image file will appear on your desktop).*

Now click the “OK” button.

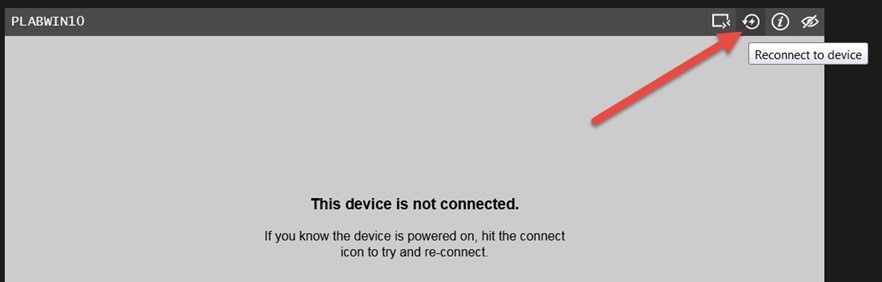
Now log out by clicking the start button and the user icon.



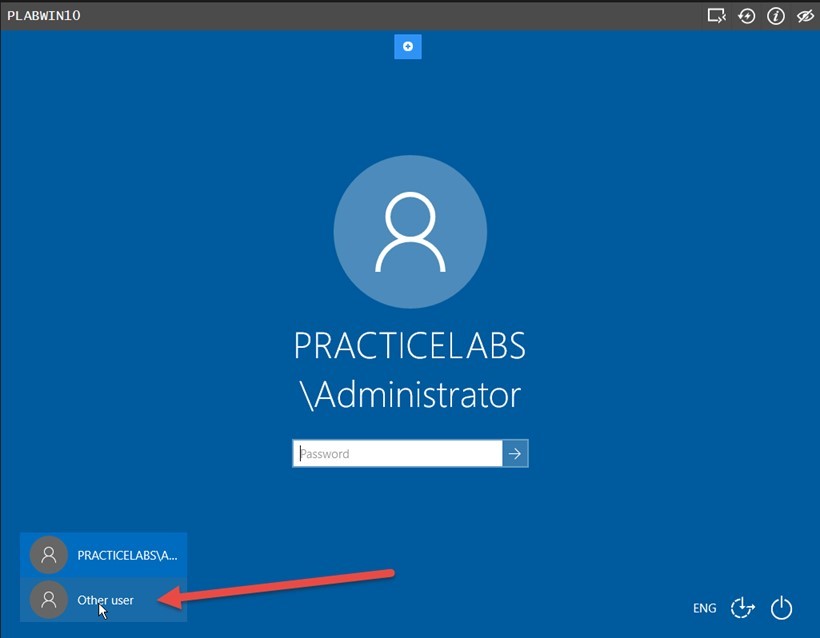
Then click “Sign Out”

***Step 9 - Login to PLABWIN10 as user1***

Scroll down until you see the login screen for **PLABWIN10**. If you see a grey screen which displays “Device is not Connected,” click on the “Reconnect to device” icon in the upper right corner.

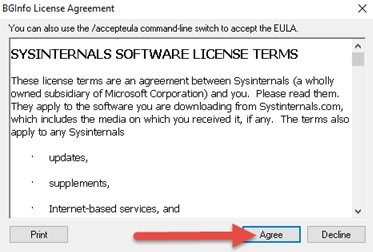


Click “Other user” in the lower left corner of the screen.



Enter user1 in the “User name” field and **Passw0rd**in the Password field, then press Enter.

You may see a “BGInfo License Agreement” page. Click “Agree”.



Now click the “Start” button and type **\\PLABDC01**and press enter.



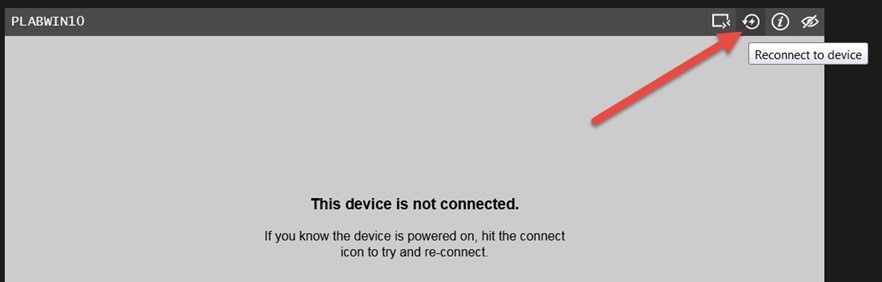
You will now see shared resources on the Domain Controller. Double click the “Shared” folder. The “Test” document should now be visible. Double click on the “Test” document to open it in Notepad. Add more text to the document, save it, and exit Notepad.

You have now verified that user1 can modify documents in the Shared folder.

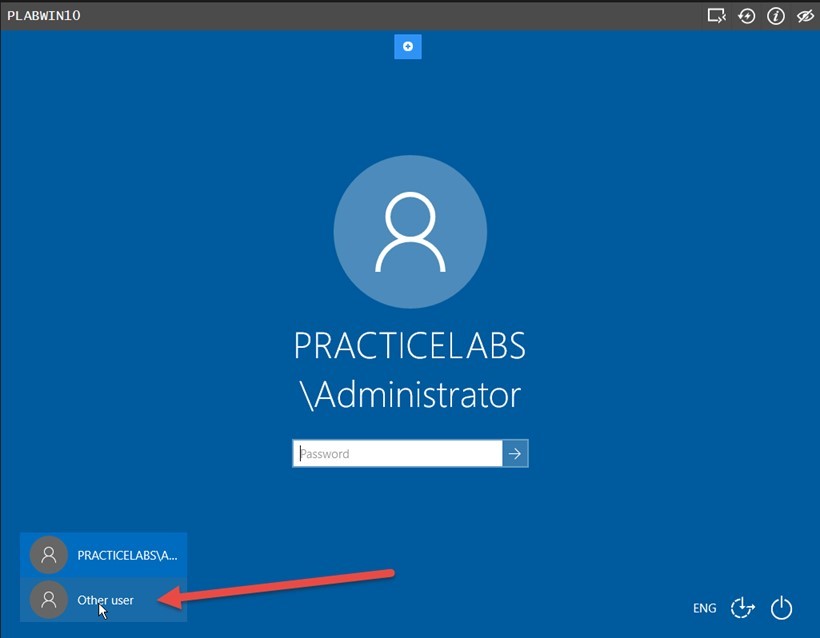
Click the “Start” button and logout as user1.

***Step 10 - Login to PLABWIN10 as user2***

Scroll down until you see the login screen for **PLABWIN10**. If you see a grey screen which displays “Device is not Connected,” click on the “Reconnect to device” icon in the upper right corner.

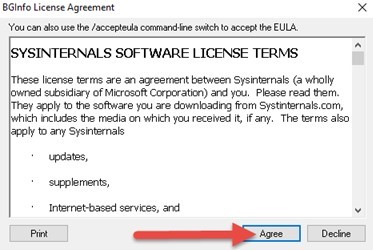


Click “Other user” in the lower left corner of the screen.



Enter user2 in the “User name” field and **Passw0rd**in the Password field, then press Enter.

You may see a “BGInfo License Agreement” page. Click “Agree”.



Now click the “Start” button and type **\\PLABDC01**and press enter.



You will now see shared resources on the Domain Controller. Double click the “Shared” folder. The “Test” document should now be visible.

Double click on the “Test” document to open it in Notepad. Add more text to the document, and try to save the document.

Did you receive any error messages?

*ACTION: Capture a screenshot for your assignment. (On Windows use <ALT PrtSc> and then paste into Word. On Mac, use <SHIFT><COMMAND>4 and select the area you wish to capture. The .png image file will appear on your desktop).*

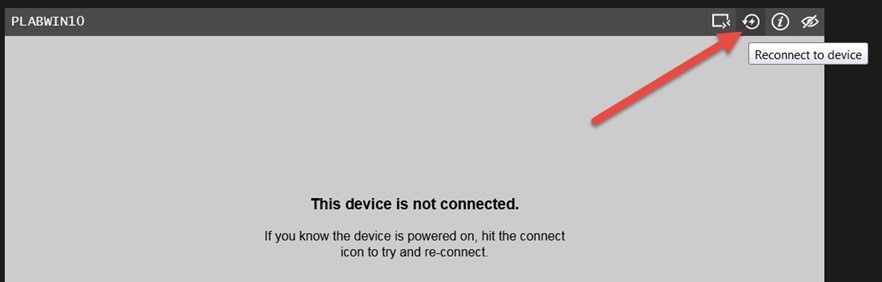
Close notepad without saving the document.

You have now verified that user2 can read, but not modify documents in the Shared folder.

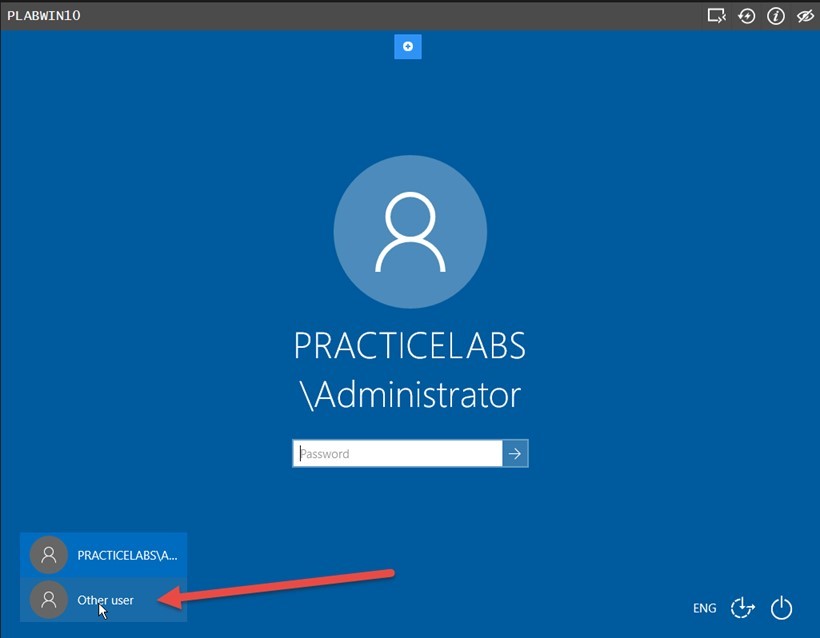
Click the “Start” button and logout as user2.

***Step 11 - Login to PLABWIN10 as user3***

Scroll down until you see the login screen for **PLABWIN10**. If you see a grey screen which displays “Device is not Connected,” click on the “Reconnect to device” icon in the upper right corner.

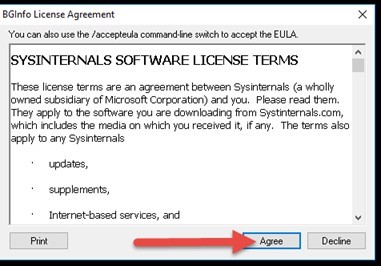


Click “Other user” in the lower left corner of the screen.



Enter user3 in the “User name” field and **Passw0rd**in the Password field, then press Enter.

You may see a “BGInfo License Agreement” page. Click “Agree”.



Now click the “Start” button and type \\PLABDC01 and press enter.



You will now see shared resources on the Domain Controller. Double click the “Shared” folder. The “Test” document should now be visible. Double click on the “Test” document to open it in Notepad.

Did you receive any error messages?

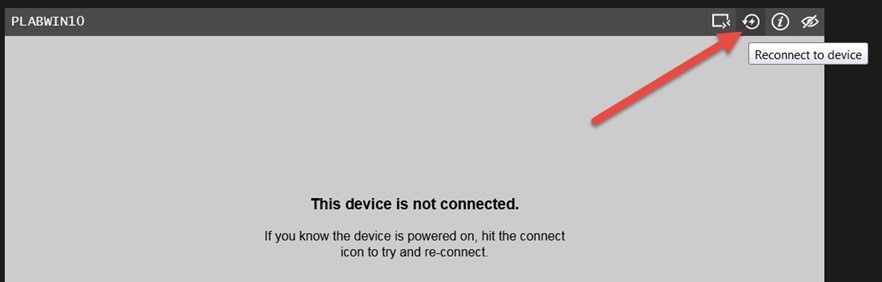
*ACTION: Capture a screenshot for your assignment. (On Windows use <ALT PrtSc> and then paste into Word. On Mac, use <SHIFT><COMMAND>4 and select the area you wish to capture. The .png image file will appear on your desktop)*

You have now verified that user3 has no access to documents in the Shared folder.

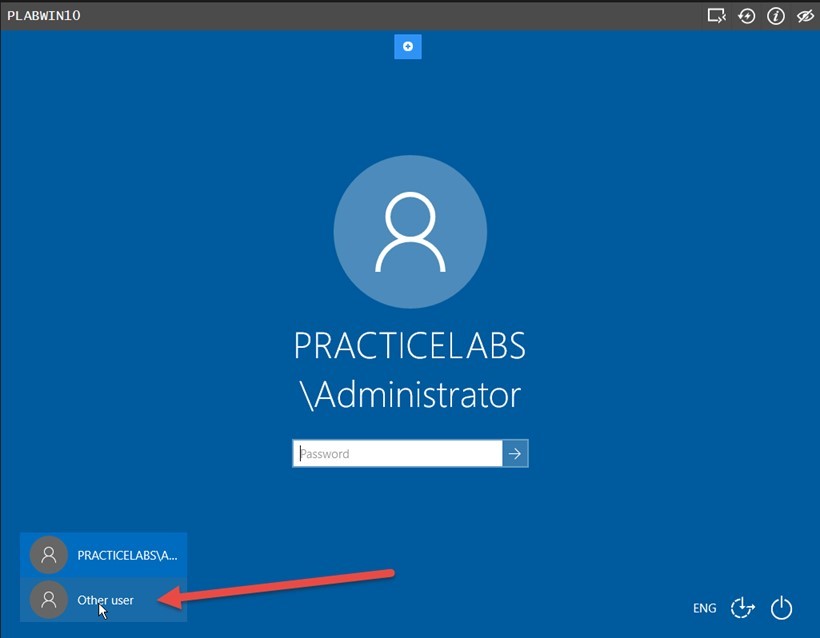
Click the “Start” button and logout as user3.

***Step 12 - Login to PLABWIN10 as user1 and create key pair***

Scroll down until you see the login screen for **PLABWIN10**. If you see a grey screen which displays “Device is not Connected,” click on the “Reconnect to device” icon in the upper right corner.



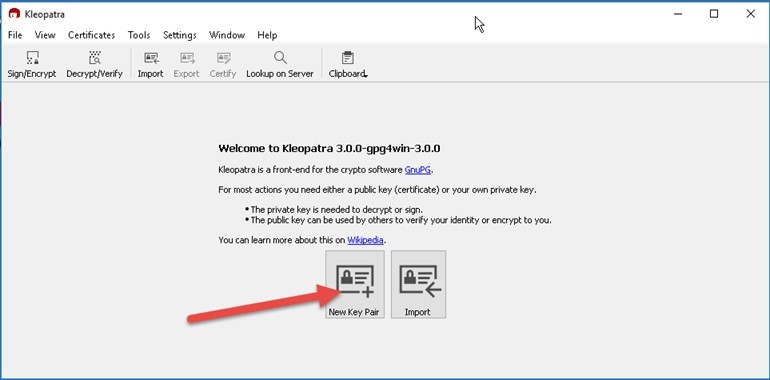
Click “Other user” in the lower left corner of the screen.



Enter user1 in the “User name” field and **Passw0rd**in the Password field, then press Enter.

When logged in, double click on the Kleopatra icon on the desktop. This is a key management system which interacts with the open source GnuPG encryption system. In order to use this system, you will need to generate a pair of keys: a public key and a private key.

Click on the “New Key Pair” icon.



In the “Name” field, enter user1 then click the “Next” button. After reviewing the key creation parameters, click the “Create” button.

You will be prompted to enter a passphrase. This is like a password to help to generate and protect your key pair. Enter user1passphrase in the “Pass phrase” and “Repeat” fields.

Your key pair will be generated, and this may take a couple minutes before you see the “Key Pair Successfully Created” message.

*ACTION: Capture a screenshot for your assignment. (On Windows use <ALT PrtSc> and then paste into Word. On Mac, use <SHIFT><COMMAND>4 and select the area you wish to capture. The .png image file will appear on your desktop)*

It is always critical to backup your keys and keep them in a safe backup location where only you can access them.

Click the “Make a Backup Of Your Key Pair…” button.

Click the folder icon to the right of the “Output file” field, click on the “Desktop” folder, then type user1-key-backup in the “File name” field and click “Save”.

Then click the “OK” button. You will be required to enter your passphrase again. Enter: user1passphrase and press the “OK” button.

Now click the “Finish” button.

You will see the backup of your keys on the desktop.

It is also important to share your public key with everyone so that they can interact with you. Click on “user1” within Kleopatra and click the “Export” icon. Navigate to the “Desktop” folder, then enter user1-public-key in the “File name” field. Then click the “Save” button.

You will now see the “user1-public-key” file on your desktop. To confirm the contents of that file, right click on it, choose “Open with” and then click “Choose another app”. Next, click “More apps”. Find and click “Notepad”, then click “OK”.

You can see that this file only contains your public key block. DO NOT EDIT THIS FILE. Close Notepad.

Now we will share your public key by copying it into the “Public Documents” folder. Click the “File Explorer” icon at the bottom of the screen (Yellow folder) and navigate to “This PC”, “Local Disk (C:)”, “Users”, “Public” and “Public Documents”.

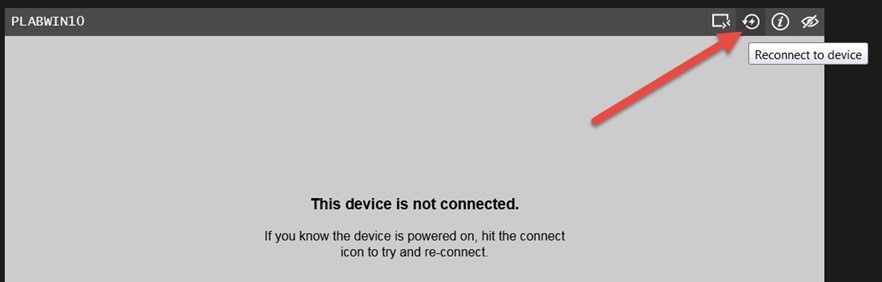
Copy the “user1-public-key” file from your desktop and paste it into the “Public Documents” folder.

Before we can do any more, we will need to login as a different user.

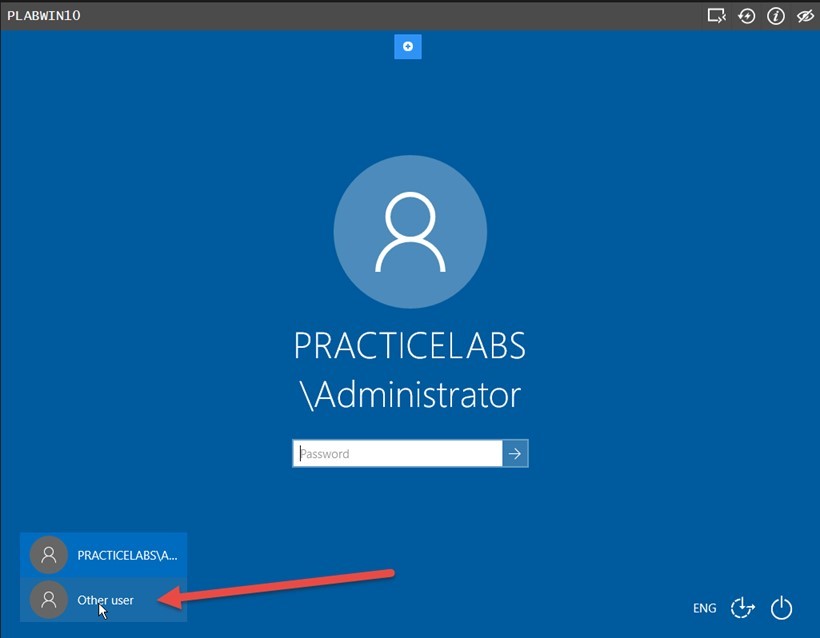
Click the “Start” button, then click the user1 account icon and sign out.

***Step 13 - Login to PLABWIN10 as user2 and create key pair***

Scroll down until you see the login screen for **PLABWIN10**. If you see a grey screen which displays “Device is not Connected,” click on the “Reconnect to device” icon in the upper right corner.



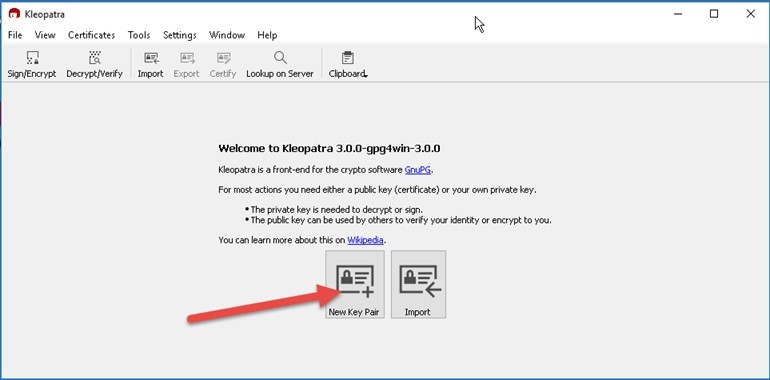
Click “Other user” in the lower left corner of the screen.



Enter user2 in the “User name” field and **Passw0rd**in the Password field, then press Enter.

When logged in, double click on the Kleopatra icon on the desktop.

Click on the “New Key Pair” icon.



In the “Name” field, enter user2 then click the “Next” button. After reviewing the key creation parameters, click the “Create” button.

You will be prompted to enter a passphrase. This is like a password to help to generate and protect your key pair. Enter user2passphrase in the “Pass phrase” and “Repeat” fields.

Your key pair will be generated, and this may take a couple minutes before you see the “Key Pair Successfully Created” message.

It is always critical to backup your keys and keep them in a safe backup location where only you can access them.

Click the “Make a Backup Of Your Key Pair…” button.

Click the folder icon to the right of the “Output file” field, click on the “Desktop” folder, then type user2-key-backup in the “File name” field and click “Save”.

Then click the “OK” button. You will be required to enter your passphrase again. Enter: user2passphrase and press the “OK” button.

Now click the “Finish” button.

You will see the backup of your keys on the desktop.

It is also important to share your public key with everyone so that they can interact with you. Click on “user2” within Kleopatra and click the “Export” icon. Navigate to the “Desktop” folder, then enter user2-public-key in the “File name” field.

Then click the “Save” button.

You will now see the “user2-public-key” file on your desktop.

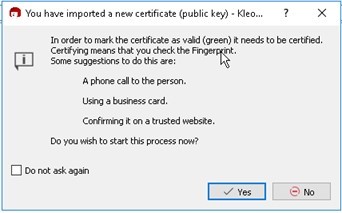
Now we will share your public key by copying it into the “Public Documents” folder. Click the “File Explorer” icon at the bottom of the screen (Yellow folder) and navigate to “This PC”, “Local Disk (C:)”, “Users”, “Public” and “Public Documents”.

Copy the “user2-public-key” file from your desktop and paste it into the “Public Documents” folder.

You will notice that the “user1-public-key” file is visible in this public folder. Let’s import it into Kleopatra. Within Kleopatra, click the “Import” button.

Navigate to “This PC”, “Local Disk (C:)”, “Users”, “Public” and “Public Documents”.

Then double click the “user1-public-key” file. You will receive a pop-up message asking you to verify the file. Click the “Yes” button.



In real life, you would verify this, or have it automatically verified by a public management system.

Check the “user1” checkbox and the “I have verified the fingerprint” checkbox, then click the “Next” button.



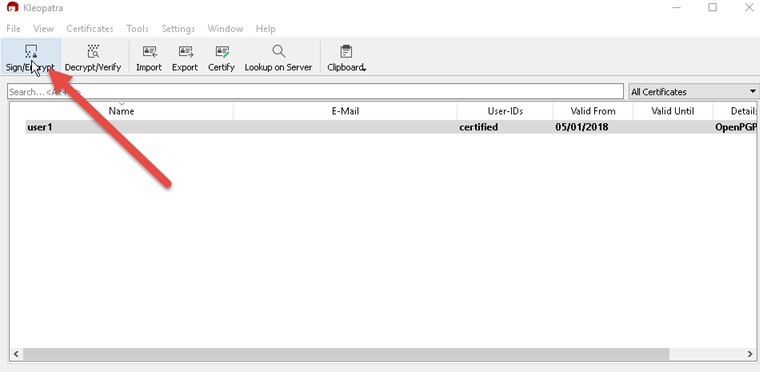
Finally, click the “Certify” button. You will be prompted to enter your passphrase. Enter user2passphrase and press “enter”. Then click the “Finish” button.

Now, let us create a message to encrypt. Right click on the desktop, then click “New” and “Text document”. Call this document user2-cleartext. Double click on the “user2-cleartext” file.

This will open the file in Notepad. In the document, type a few sentences of your choice.

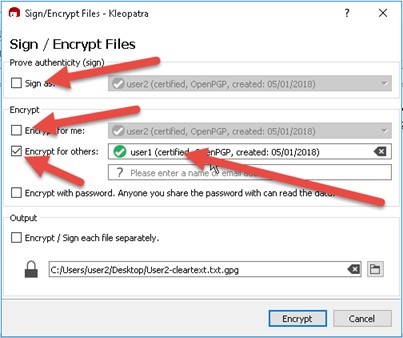
Save the file and exit Notepad.

Now, click the “Sign/Encrypt” icon in Klepoarta.

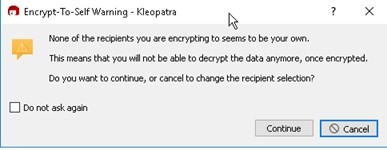


In the open file dialog box, navigate to the Desktop folder and click on the “user2-cleartext” file, then click the “Open” button.

Make sure that the “Sign as:” and “Encrypt for me” boxes are unchecked and “Encrypt for others” checkbox are checked. Enter user1 in the “Encrypt for others” field, and click on the “User1” entry there. Click the “Encrypt” button.



You will get a pop up message indicating that you will no longer be able to read the message. Click the “Continue” button.



Now click the “Finish” button.

This will create a new file on your desktop with a lock icon named “user2-cleartext.txt” (with a hidden extension of .gpg). To confirm the contents of that file, right click on it, choose “Open with” and then click “Choose another app”. Next, click “More apps”. Find and click “Notepad”, then click “OK”.

You can see that original message is unreadable. DO NOT EDIT THIS FILE. Close Notepad.

Rename the file to “user2-cyphertext.txt” and copy it into the “Public Documents” folder. This will remind us that this is the encrypted file.

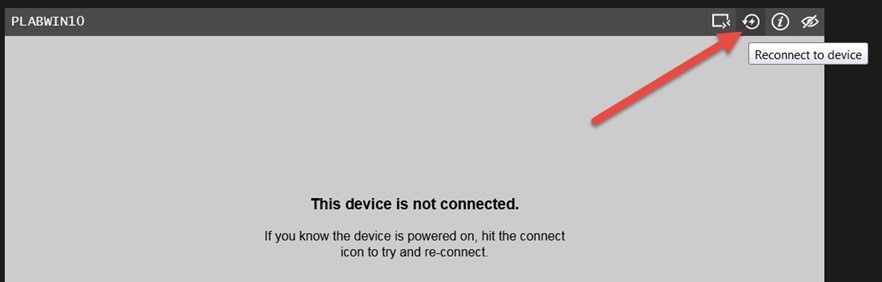
Think about what has happened. You encrypted this file for User1, so User1’s public key was used to encrypt the file. It can now only be decrypted using User1’s Private key. This is why User2 can no longer decrypt the file.

Now let’s see if User1 can read the file.

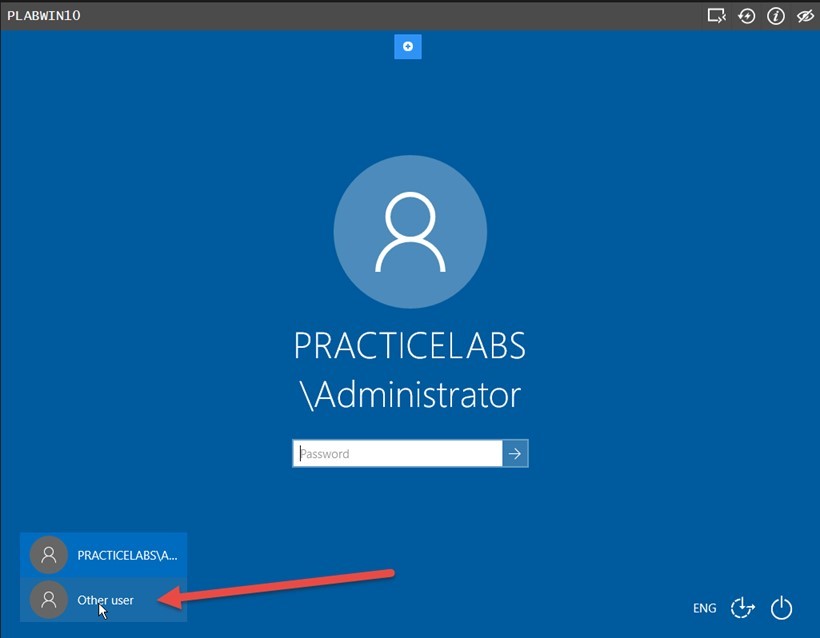
Click the “Start” button, then click the user2 account icon and sign out.

***Step 14 - Login to PLABWIN10 as user1 and read the encrypted message***

Scroll down until you see the login screen for **PLABWIN10**. If you see a grey screen which displays “Device is not Connected,” click on the “Reconnect to device” icon in the upper right corner.



Click “Other user” in the lower left corner of the screen.

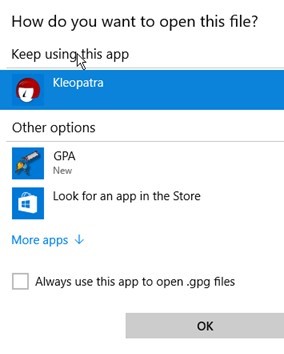


Enter user1 in the “User name” field and **Passw0rd**in the Password field, then press Enter.

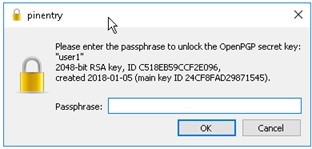
Click the “File Explorer” icon at the bottom of the screen (Yellow folder) and navigate to “This PC”, “Local Disk (C:)”, “Users”, “Public” and “Public Documents”.

Double click on the User2-cyphertext.txt file. You will receive a pop-up asking how you want to open the file.

Click Kleopatra and click the “OK” button.

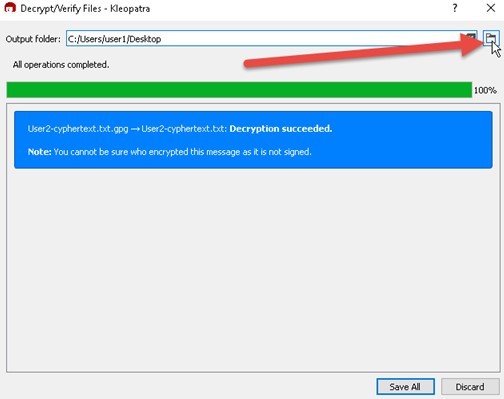


You will then be prompted to enter the user1 passphrase.



Enter user1passphrase and click the “OK” button.

When decryption completes, Click the folder icon to the right of the “Output folder” field and navigate to the Desktop. Click the “Select folder” button, then click the “Save All” button.



You should now have an unencrypted copy of the User2-cyphertext file on your desktop. Double click it to verify your original message.

*ACTION: Capture a screenshot for your assignment. (On Windows use <ALT PrtSc> and then paste into Word. On Mac, use <SHIFT><COMMAND>4 and select the area you wish to capture. The .png image file will appear on your desktop)*

Click the “Logout of Lab Platform” icon:

Practice Labs screenshot.

* Explain the types of information that can be stored in an Active Directory user record. The different types of information that can be stored on active directory user record is servers, computer accounts, volumes, printers, and the network user. Server is a computer, device or program that is dedicated to managing network resources. Computer account is an account that a computer is a part of windows domain. Volume or logical drive is a single accessible storage area with a single file system. Printer is device that makes a persistent representation of graphics or text on paper. Network Printer is a printer that accessed by network connection.
* **What are some of the additional tabs which are available in the Active Directory Users and Computers "Advanced Features" mode**? The additional tabs that are available in the active directory users and computers advanced features mode is the object and Attribute Editor tabs.
* **What are some of the specific challenges and risks associated with account management in a large infrastructure**?  Some challenges and risks associated with account management in a large infrastructure is lack of powerful computing platforms. The challenge is growing processing power of computers has been the lack of energy and space to power the computers. A solution is to employ multi-core platforms. Next, Data acquisition Problems is firewalls that protect emails, applications and web browsing will cause important packet losses in the TCP/IP networks. This will result in data loss and reduce the network speed. The solution is getting high-performance computing resources with a huge data set. IT managers need to employ better means to collect and store using high-speed networks. Another Challenge is compute management and Provisioning. This challenge has high-performance computing large data sets will require virtualization and automation to avoid adding more people to this process. The solution to this challenge is using distributive systems. Distributive system is a system whose components are located on different networked computers. They communicate and coordinate their actions by passing messages to one another. The components come together to achieve the same goal.
* **How can inadequate access controls or access management leave critical information vulnerable**? Inadequate access controls can expose the organization to unauthorized access of data or shutdown of computer services. This can also affect authorized users.
* **What protections does encryption offer, and how important is key management to keeping any encryption system secured**? Encryption protects your online privacy, complete security for all devices, receive data safely, and guarantee integrity. Key management is very important to meet compliance standards. Key management also secures data from risks posed by privileged users.
* **Consider a cloud-hosted Infrastructure as a Service (IaaS) environment with many users accessing these systems from all over the world. What advantages or challenges might there be managing these identities and associated keys?** The advantages managing identifies and associated keys are Allows easy access anywhere. People are increasingly using their social IDs to access services and resources, connect everyone to everything. improve employee productivity, enhance user experience, secure all aspects of your brand, and increase business agility.
* **Finally, conclude this week's assignment with a page explaining how the tools and processes demonstrated in the lab might be used by an infrastructure administrator to help secure an environment**.

An infrastructure administrator needs to take security and user access very seriously. By managing user access and activity through the exercises practiced in this week’s lab, the administrator can ensure that each user only has permission to access specific files and data. It is also the responsibility of the infrastructure Administrator that authorized users have access to needed files while protecting from unauthorized access. Administrators have to add roles and features, add other servers to manage, create a server group, and connect the server to cloud services. They must also verify user, create shared local folder and assign permissions. The administrator needs to create key pair. A key-value pair (KVP) is a set of two linked data items: a key, which is a unique identifier for some item of data, and the value, which is either the data that is identified or a pointer to the location of that data.