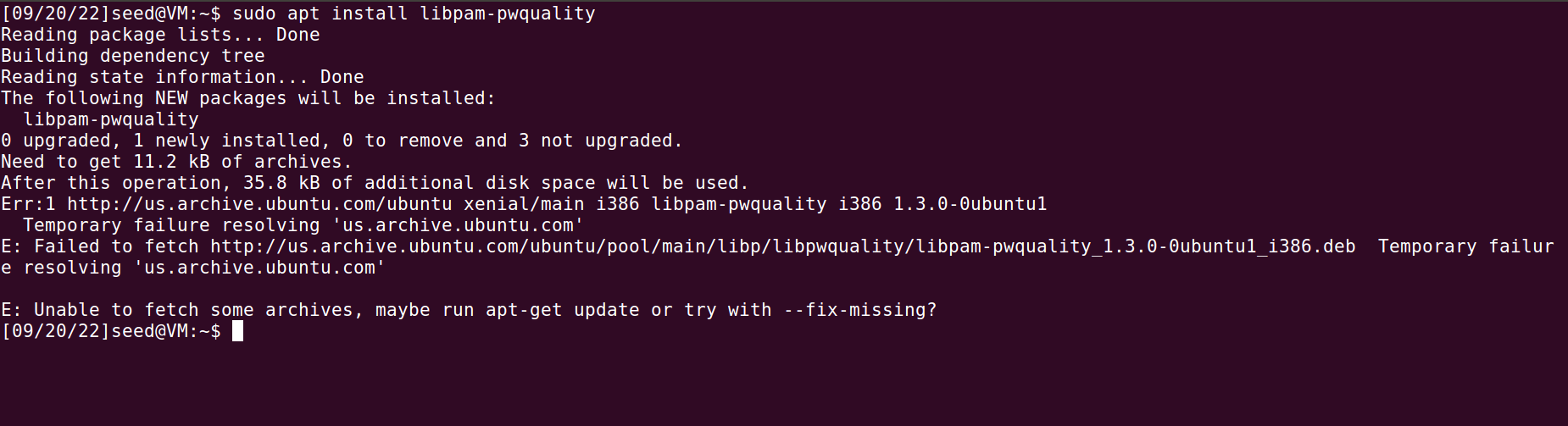
**Lab 03. Authentication**

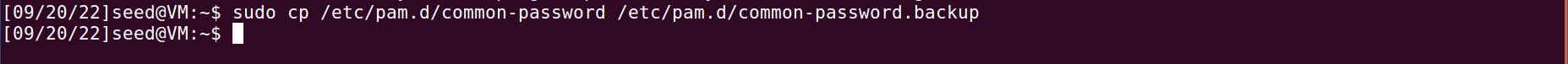
1. **Password policies**
2. **Linux:Ubuntu**

**Step 1. Install package: PAM (lib-pamquality)**

$ sudo apt install libpam-pwquality



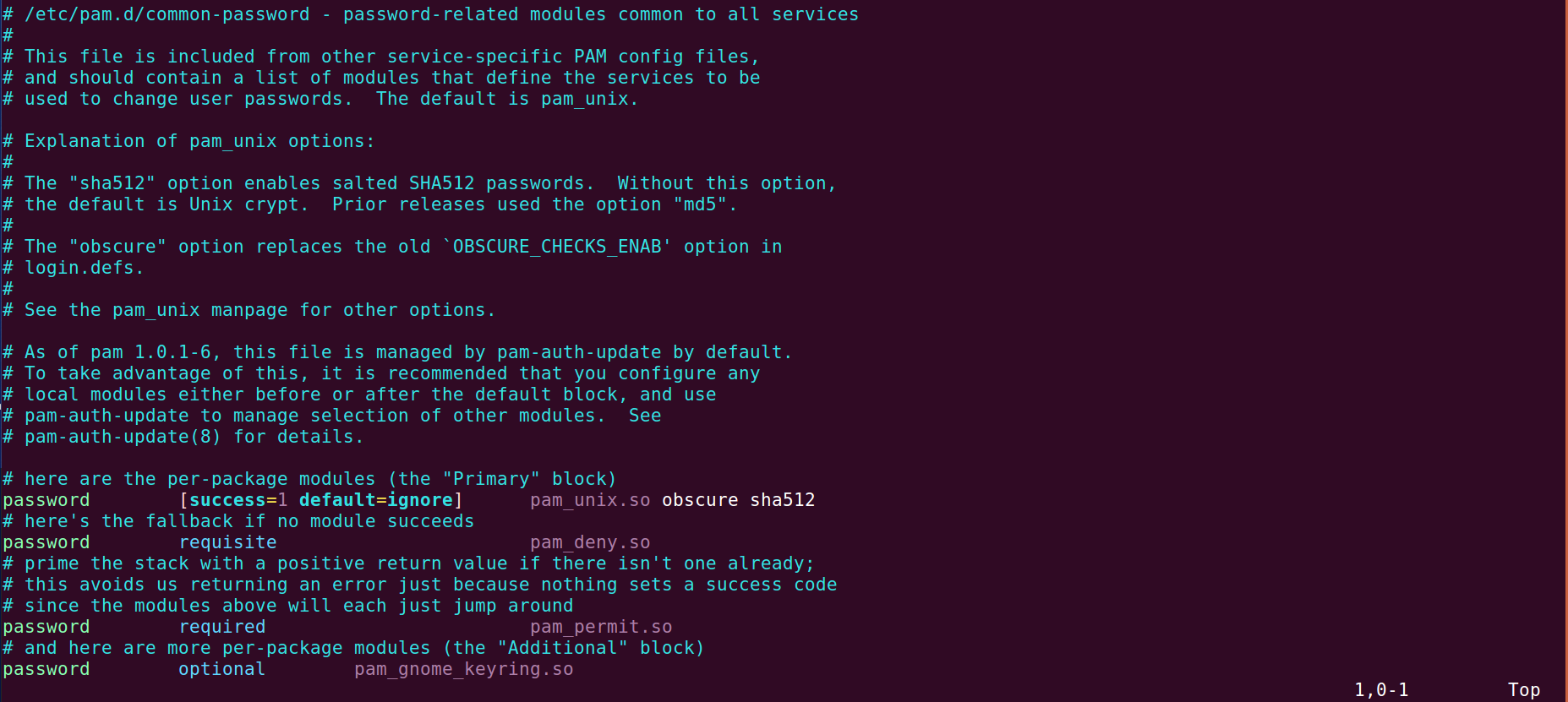
**Step 2. Edit the configuration:**

* Trước khi chúng ta tiến hành configuration thì nên chạy dòng lệnh bên dưới:

$sudo cp /etc/pam.d/common-password /etc/pam.d/common-password.backup

Chúng ta thực hiện lệnh trên nhằm tạo ra file backup để phòng ngừa mình configuration sai hay bị hư hỏng gì đó thì chúng ta vẫn có thể khôi phục lại.

* Khi chạy xong, chúng ta sẽ tiến hành chỉnh sửa các thông số trong file/etc/pam.d/ common-password.

$sudo vi /etc/pam.d/common-password

Options:

**retry:** *Số lần liên tiếp người dùng có thể nhập sai mật khẩu*.

**minlen:***Độ dài tối thiểu của mật khẩu*

**difok:***Ký tự có thể tương tự như mật khẩu cũ*

**lcredit:***Số chữ cái viết thường tối thiểu*

**ucredit:** *Số chữ hoa tối thi*

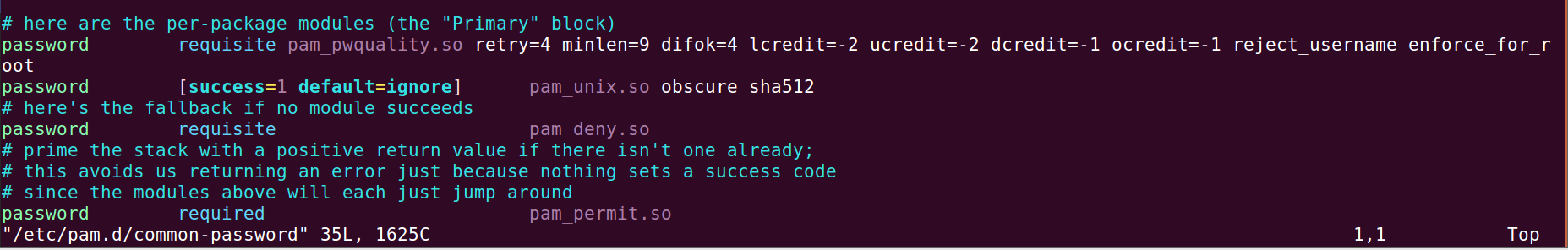
**dcredit:***Số chữ số tối thiểu*

**ocredit:***Số kí tự đặt biệt tối thiểu*

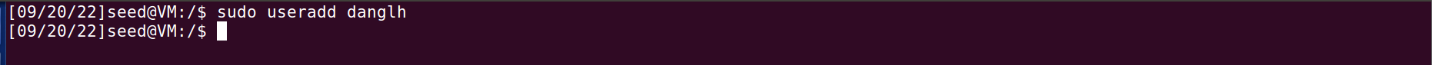
**reject\_username:***Từ chối mật khẩu có chứa tên người dùng*

**enforce\_for\_root:***Đồng thời thực thi chính sách cho người dùng gốc*

**Example:**

password        requisite pam\_pwquality.so retry=4 minlen=9 difok=4 lcredit=-2 ucredit=-2 dcredit=-1 ocredit=-1 reject\_username enforce\_for\_root

***Verify the configuration:***

* Sau khi điều chỉnh các thông số, chúng ta sẽ tiến hành tạo một tài khoản:

$sudo useradd danglh

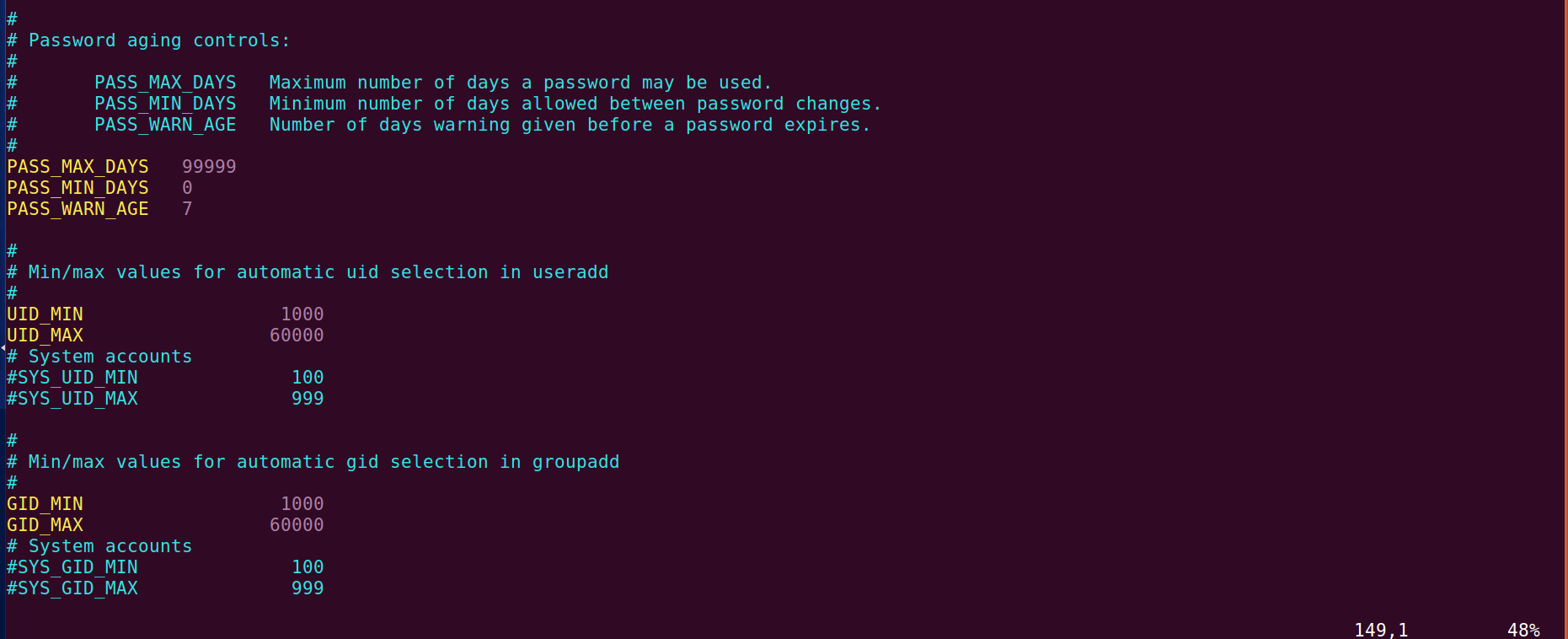
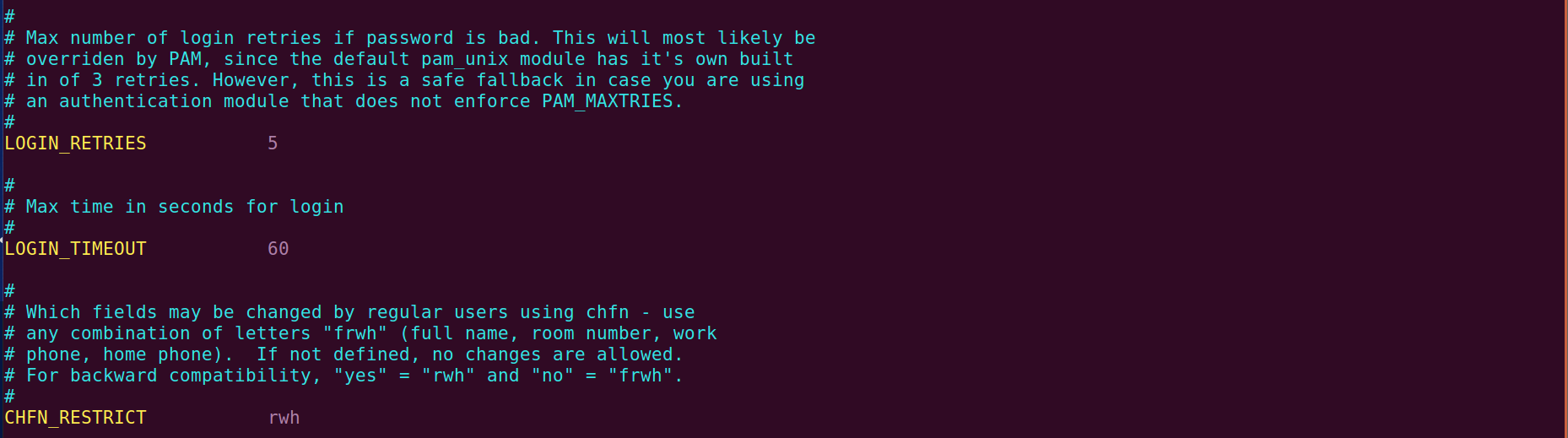
$s$sudo passwd danglh



Ở đây em đã đặt mật khẩu là: ***Haidang1607@*** -> Thoả các yêu cầu khi nãy config nên là hệ thống đã thông báo ‘Password update successfully’.

**Step 3. Edit the configuration:**

$sudo vi /etc/login.defs



Sau khi nhập lệnh trên ta sẽ được như hình, chúng ta có thể thấy được các thông số như:

+ PASS\_MAX\_DAYS: Số ngày tối đa một mật khẩu có thể được sử dụng.

+ PASS\_MIN\_DAYS: Số ngày tối thiểu được phép giữa các lần thay đổi mật khẩu.

+ PASS\_WARN\_AGE: Số ngày cảnh báo được đưa ra trước khi mật khẩu hết hạn.

+ LOGIN\_TIMEOUT: Thời gian tối đa tính bằng giây để đăng nhập.

**Verify the configuration**

Ví dụ, em sẽ thay đổi LOGIN\_TIMEOUT là 10 để test thử mình có config thành công hay không.

Như vậy, nếu sau 10s em không gõ gì thì hệ thống sẽ không cho nhập, mình phải nhấn Enter thì mới có thể nhập lại.

1. **MS Windows:**

Create an account and test some functionalities:

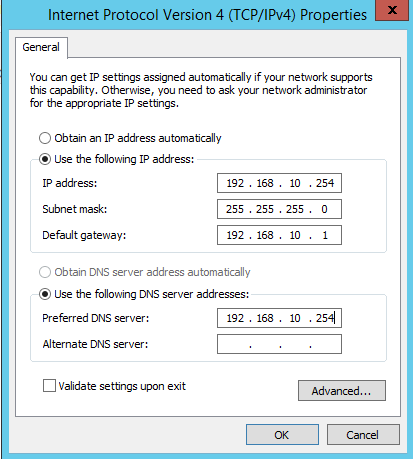
* Minimum the password length
* Strong password
* Account lockout threshold

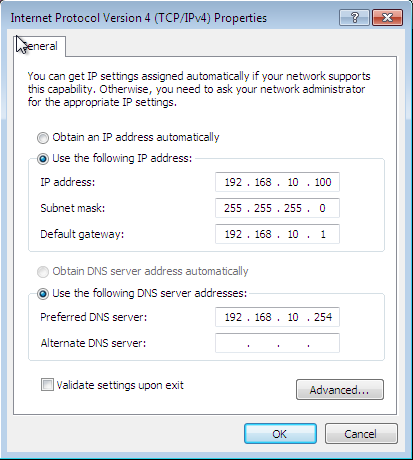


**Step 1. Set up the network topology**

* Trong bước này ta sử dụng 2 máy windows Windows 7 và : Windows Server 2012 R2
* Tiến hành set IP cho 2 máy:

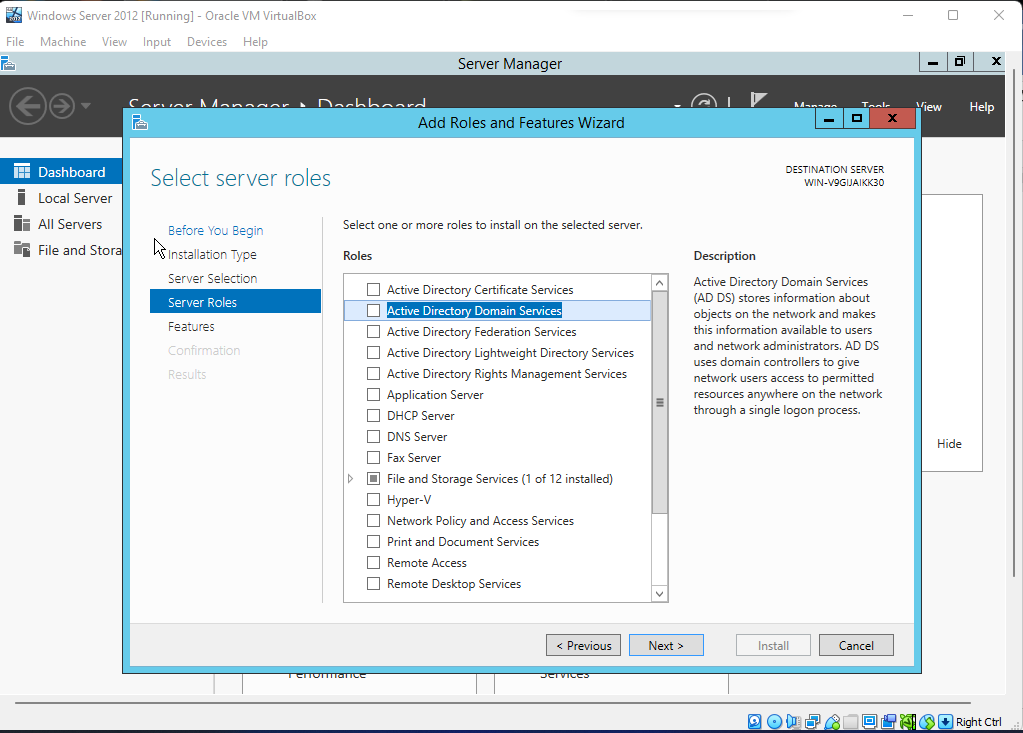
+ Máy server (Window Server 2012 R2) có địa chỉ IP - 192.168.10.254



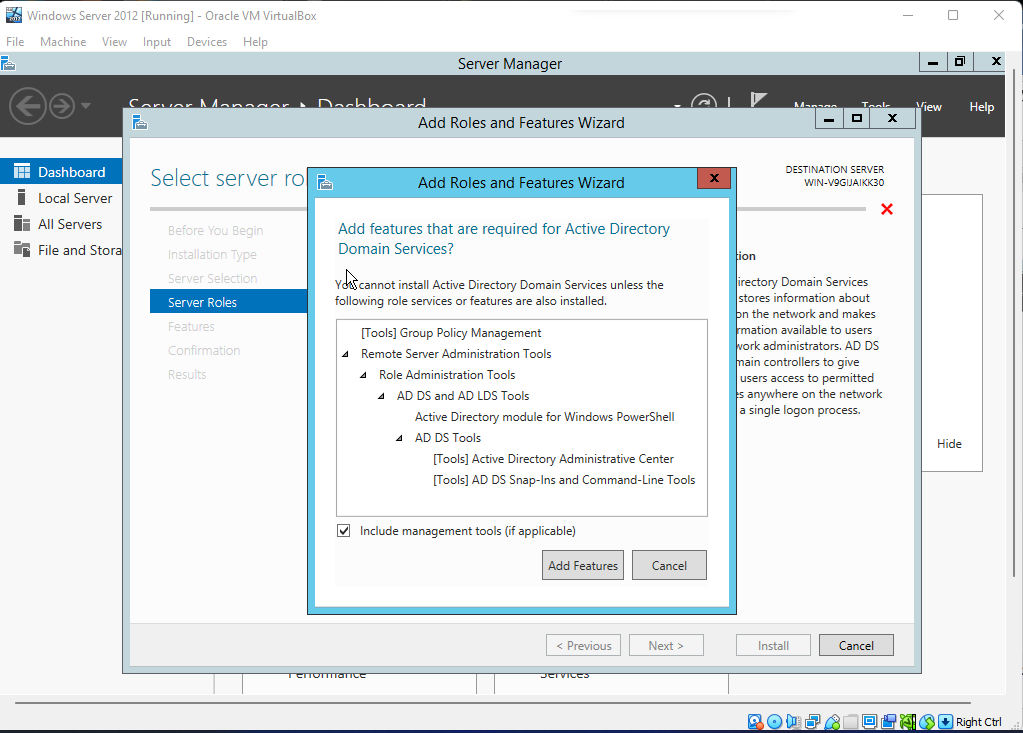
+ Máy client (Window 7) có địa chỉ IP - 192.168.10.100

**Step 2. Upgrade Server to domain controller (HCMUTE.VN) & create an account (testuser)**

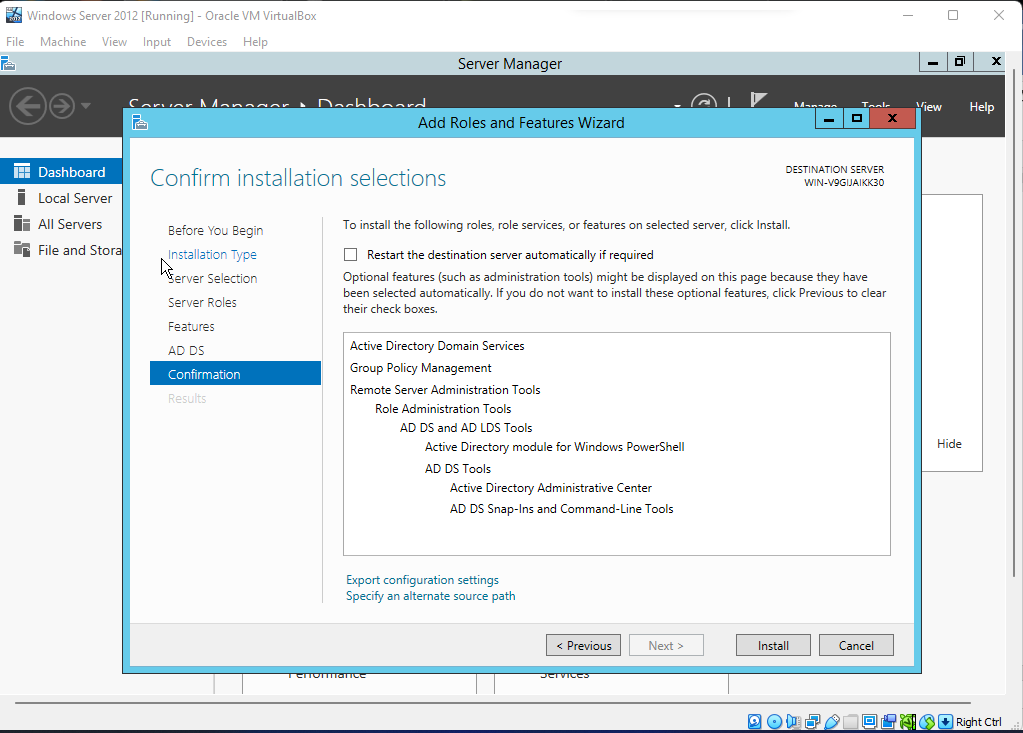
* Add Roles Active Directory Domain Services cho máy chủ

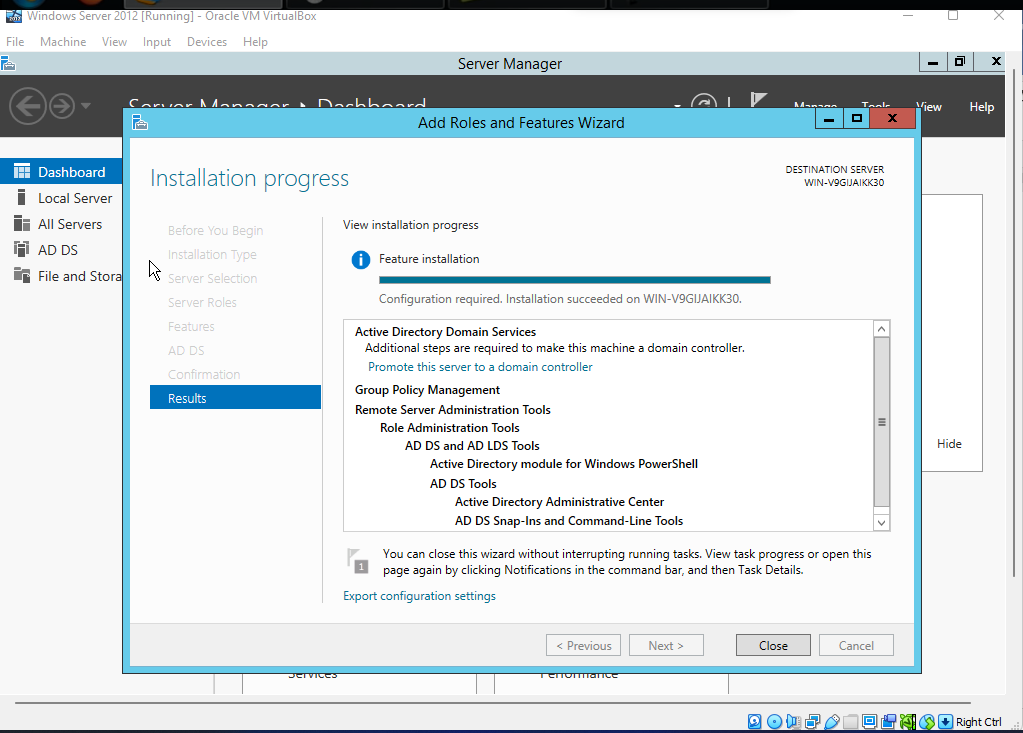
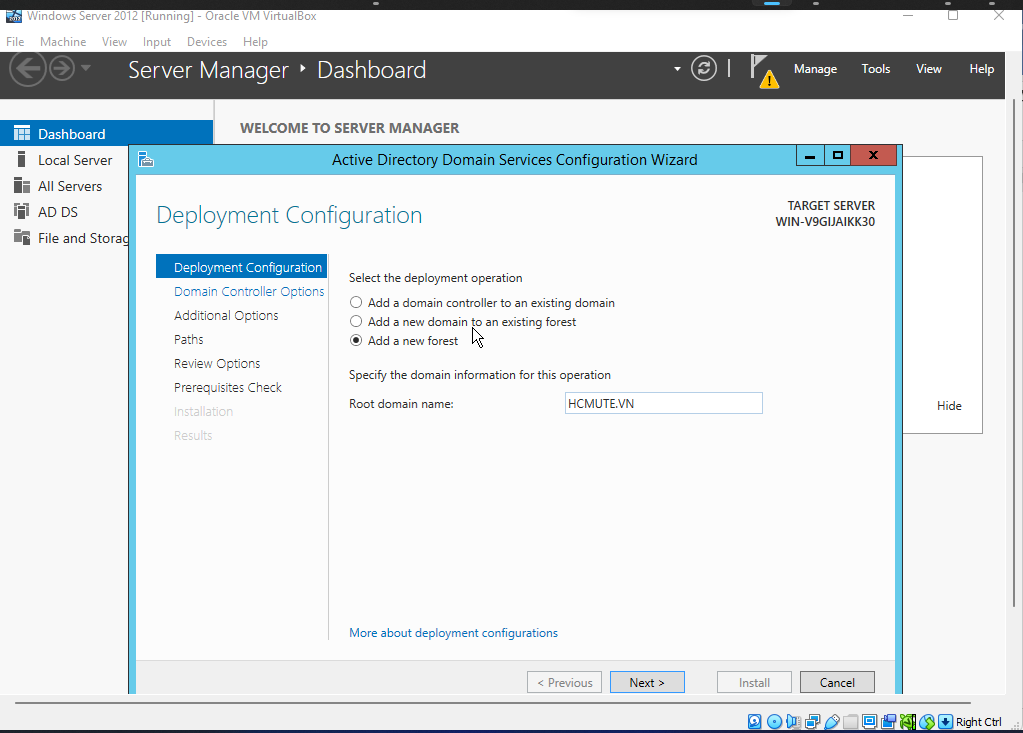
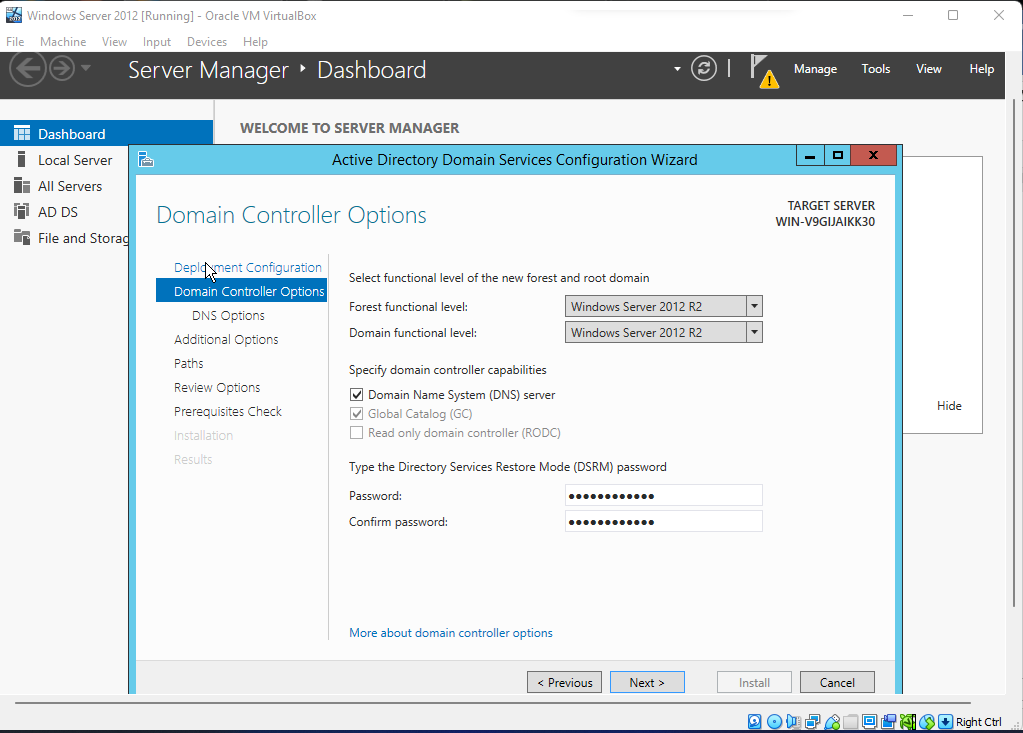
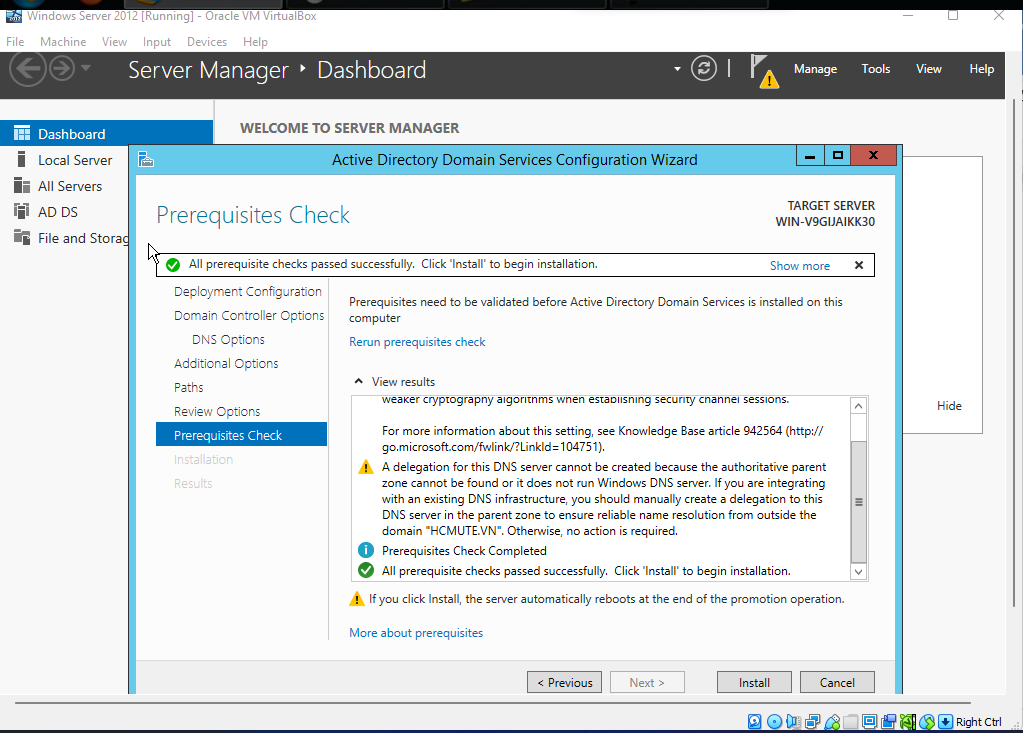
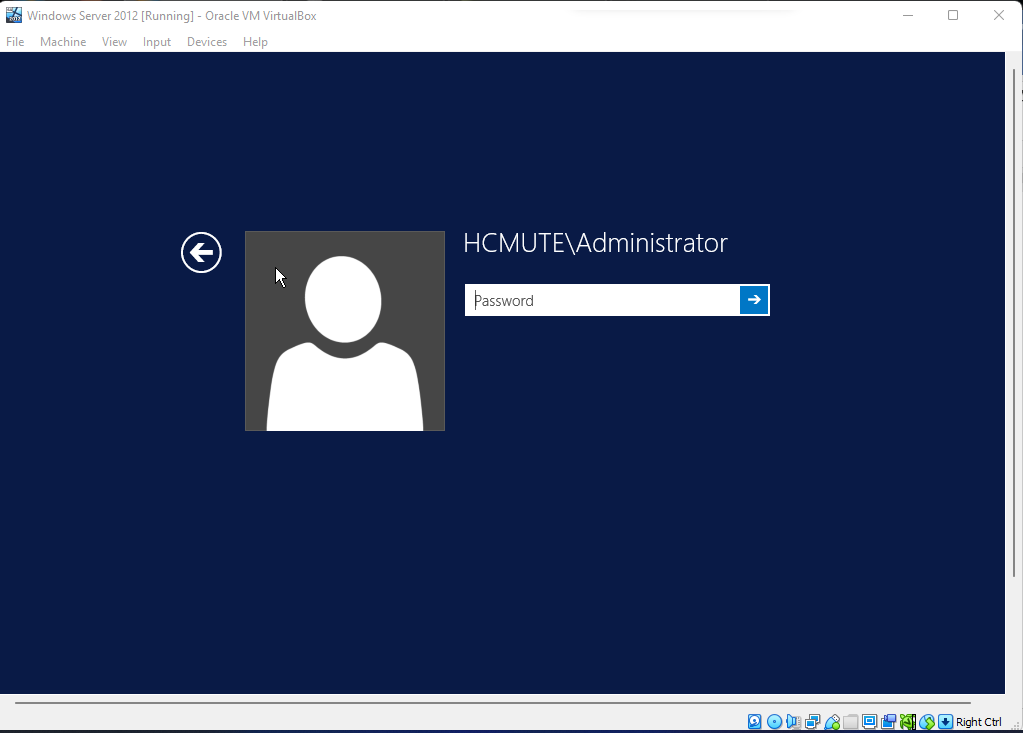
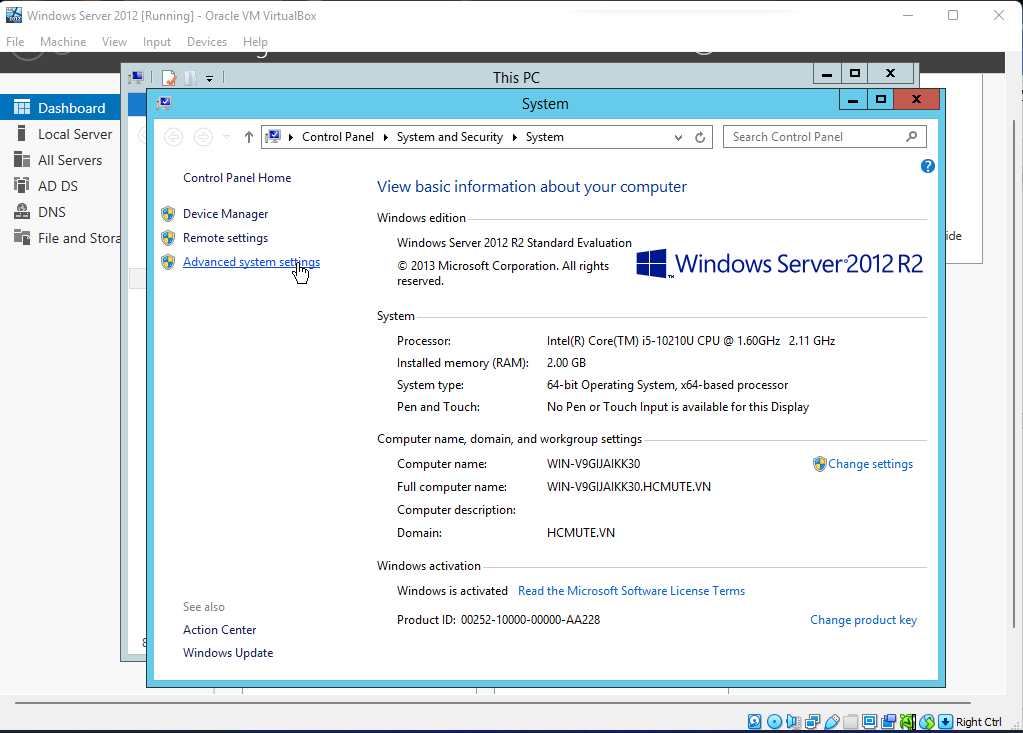


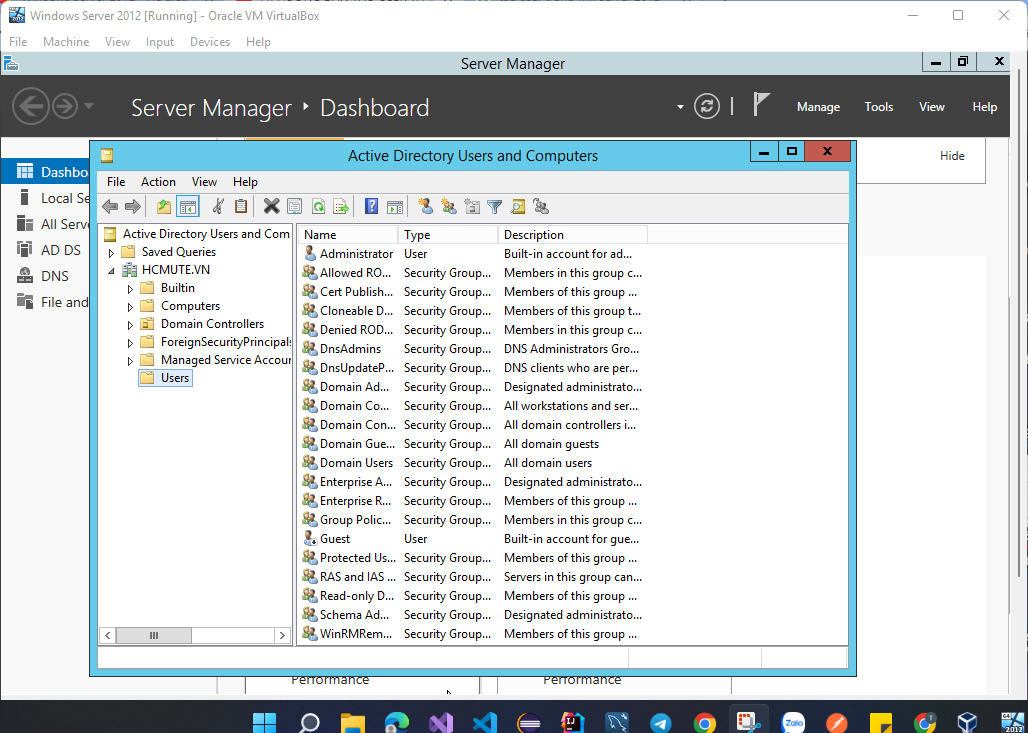
* Chọn Add Features



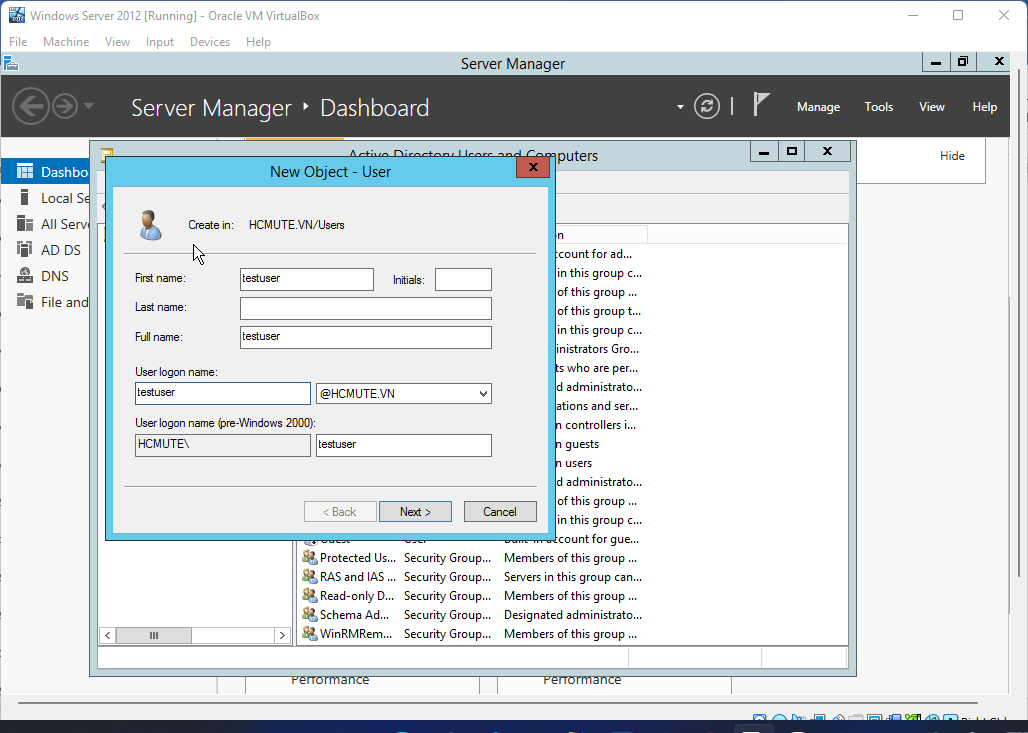
* Sau đó chọn Next đến khi có giao diện này thì ấn Install

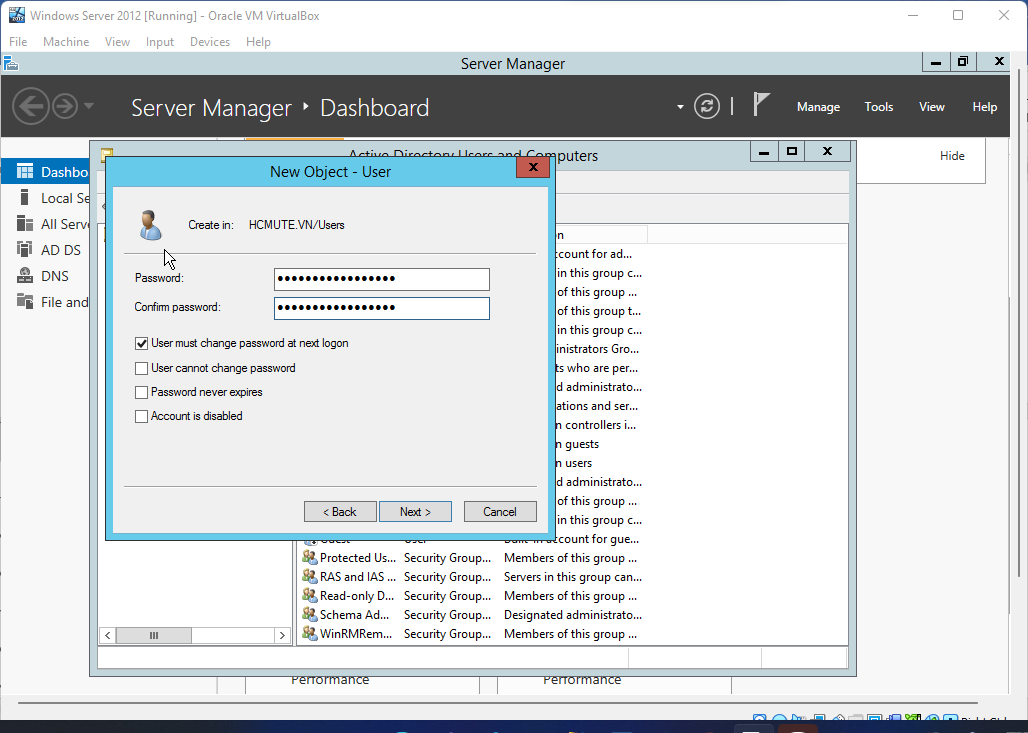
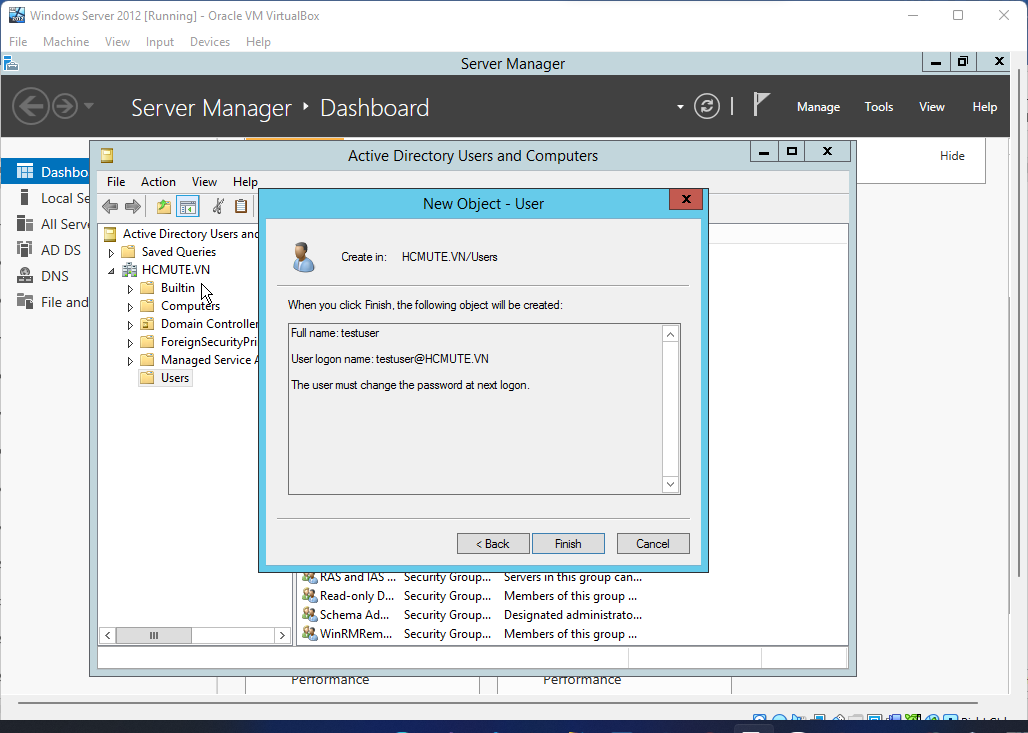


* Install đã hoàn thành
* Ta tiến hành tạo một domain có tên HCMUTE.VN trên máy server
* Ta đặt password 
* Hệ thống tiến hành kiểm tra khi thỏa các yêu cầu chúng ta tiến hành install
* Sau khi install thành công hệ thống sẽ buộc chúng ta sign out và khởi động lại
* Sau khi đã tạo domain thành công ta tiến hành kiểm tra thông tin của máy server
* Lúc này tên máy server có thêm đuôi HCMUTE.VN đây là domain chúng ta vừa tạo
* Tiếp theo chúng ta tạo tài khoản **testuser** thực hiện theo các bước sau: **Server Manager -> Tool -> Active Directory User and Computer**

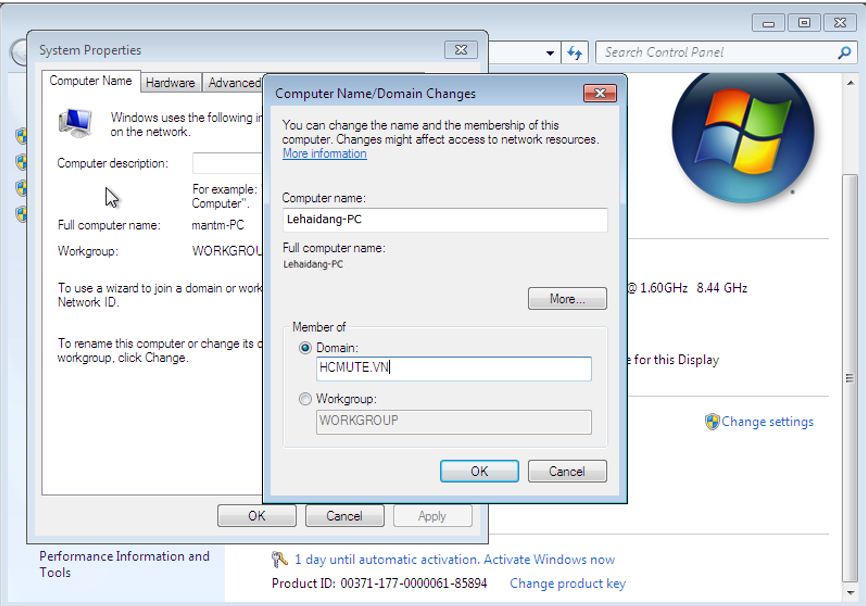


* **Click phải User -> New -> User** ta tiến hành tạo User

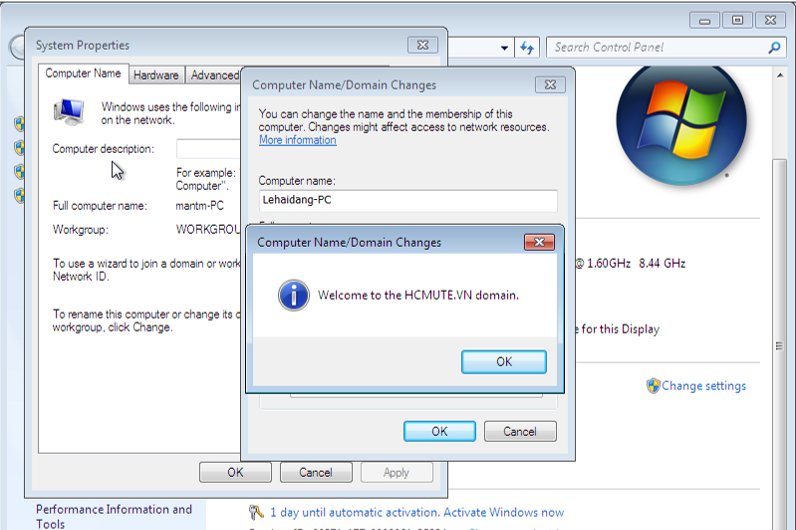


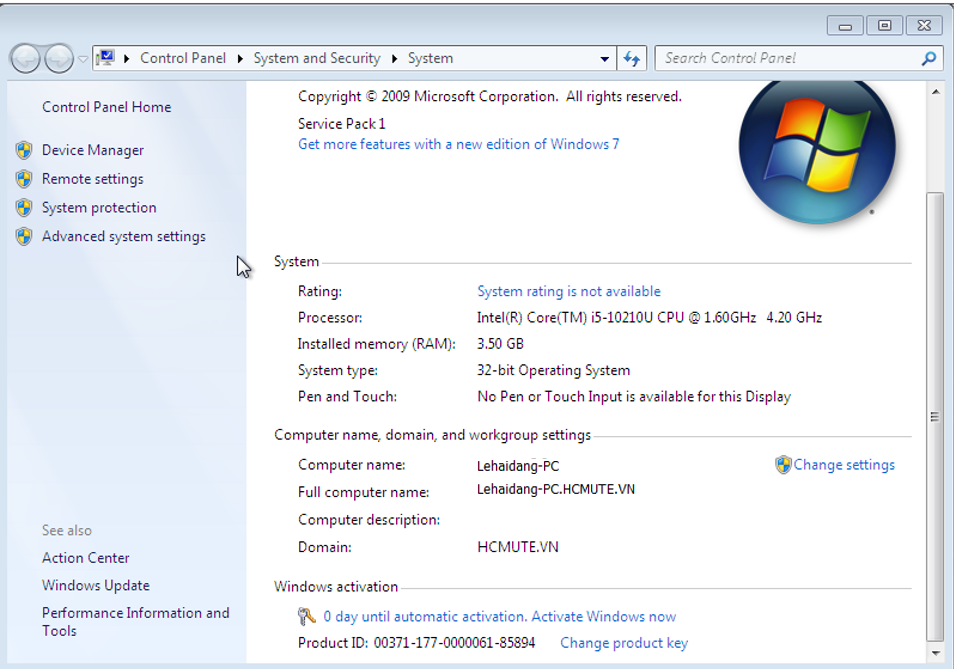
* Ta tạo account theo yêu cầu có tên là **testuser,** sau đó xác nhận mật khẩu “LeHaiDang050902@”
* Hoàn thành quá trình tạo User

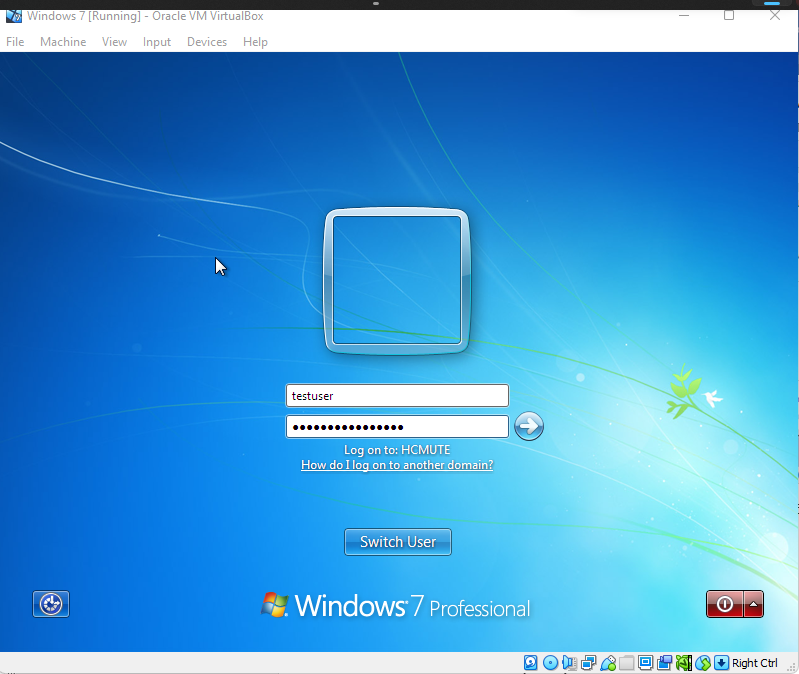
**Step 3. Join PC to Domain Controller (account: testuser)**

* Đầu tiên, ta vào máy client (Windows 7) và thay đổi domain của máy thành domain vừa tạo là HCMUTE.VN

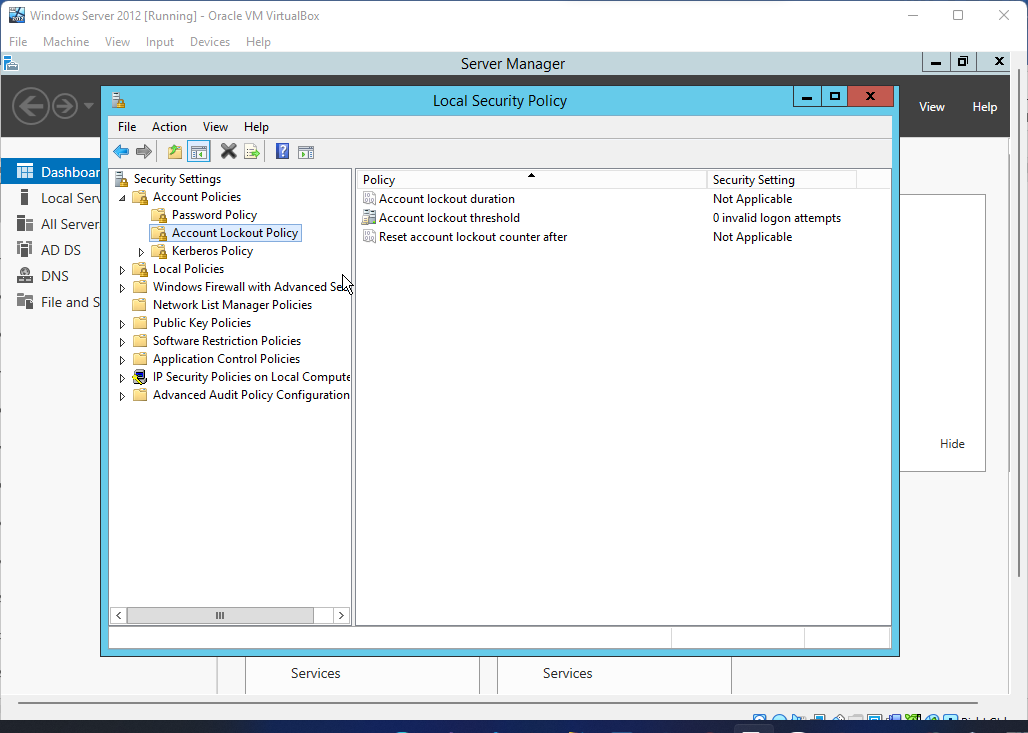
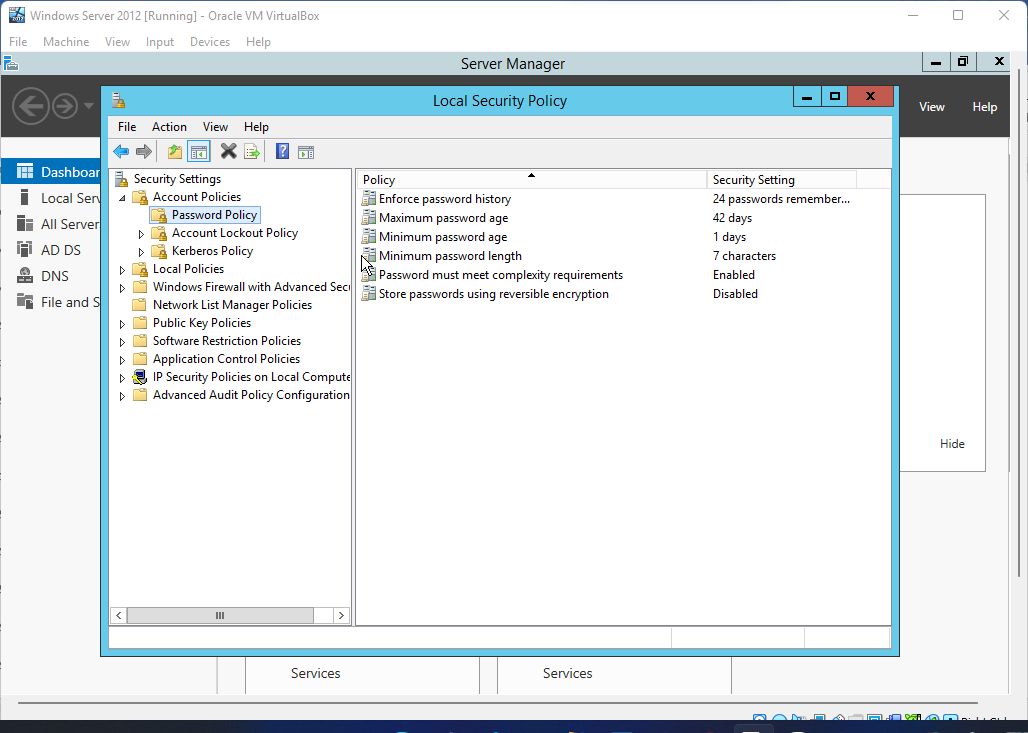


* Khi chúng ta ấn OK thì hệ thống sẽ kêu chúng ta đăng nhập 1 tài khoản mà ta đã tạo ở phía Server: (account **testuser** với password: **LeHaiDang050902@**)
* Khi ta login thành công thì giao diện hiển thị như trên, ta tiến hành kiểm tra lại thông tin của máy Client



* Lúc này máy Client thuộc domain do máy server tạo, có đuôi là HCMUTE.VN
* Cuối cùng ta đăng nhập vào máy Client để kiểm tra
* Quá trình login diễn ra thành công

**Step 4. Configure the password policy in Domain Controller**

* Trong Domain, ta có thể thay đổi các quy định về mật khẩu của các user để phù hợp với các mục đích nào đó trong Password Policy.
* Ý nghĩa của các thông tin trong Password Policy:

+ Enforce password history (Mật khẩu không thể trùng lặp 24 lần đầu tiên).

+ Maximum password age (Mật khẩu chỉ được sử dụng trong vòng 42 ngày)

+ Minimum password age (Số ngày đưa ra cảnh báo trước khi mật khẩu hết hạn)

+ Minnimum password length (Số lượng kí tự tối thiểu: 7)

+ Password must meet complexity requirements (Yêu cầu độ phức tạp phải có kí tự thường, in hoa, số, kí tự đặt biệt : Enable)

+ Store passwords using reversible encryption (Mã hóa mật khẩu: Disable)

* Ý nghĩa của các thông tin trong Acount Policy:

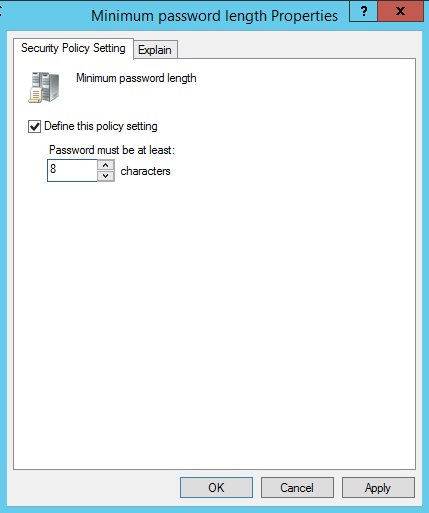
+ Account lookout duration (thời hạn khóa tài khoản)

+ Account lookout threshold (Số lần được đăng nhập sai, nếu nhập sai nhiều hơn account sẽ bị khóa)

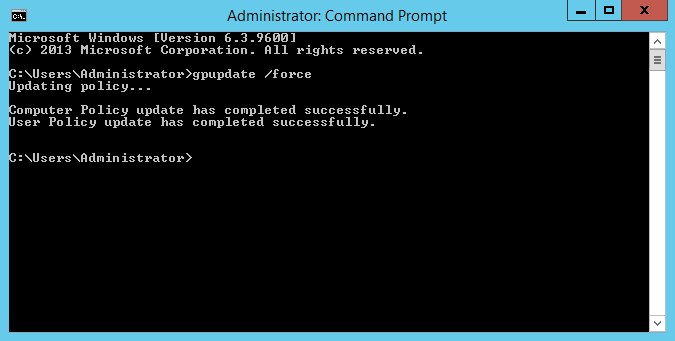
+ Reset account lookout counter after (sau bao lâu thì account reset lại)

* Ta thử thay đổi yếu tố Minnimum password length của Password Policy thành 8 và sau đó update policy xuống toàn bộ miền và các user

+ Thay đổi Minnimum password length: 7 thành 8

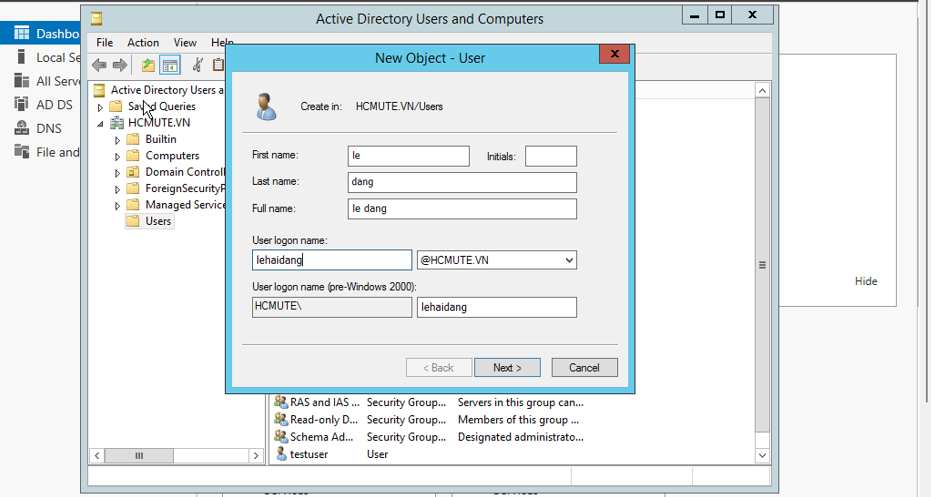


+ Update xuống toàn bộ miền và các user bằng lệnh gpupdate /force trong cmd của máy server



**Step 5. Verify the configuration on the PC client**

* Tạo một user mới:



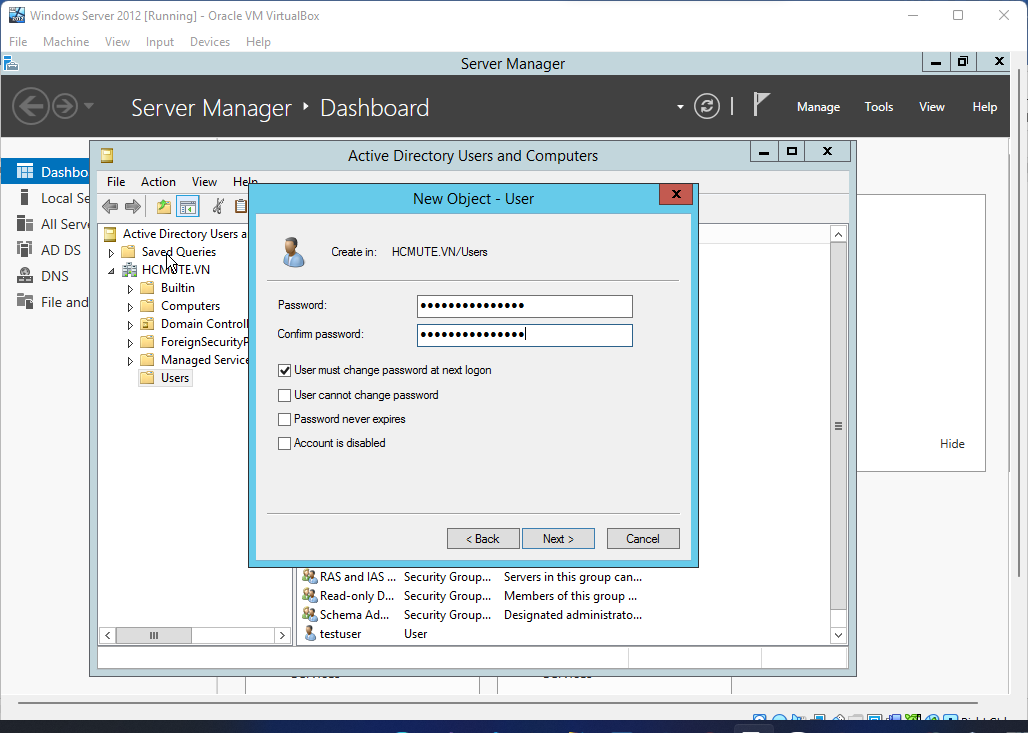
Các tick chọn lần lượt là:

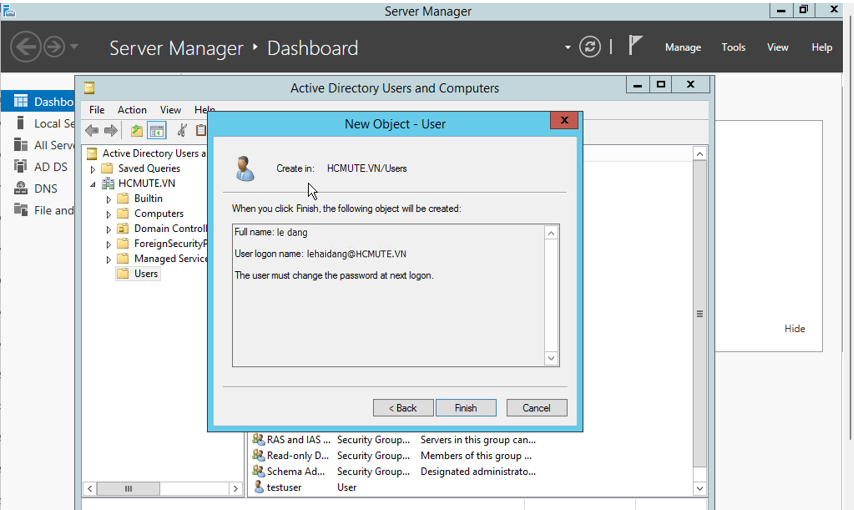
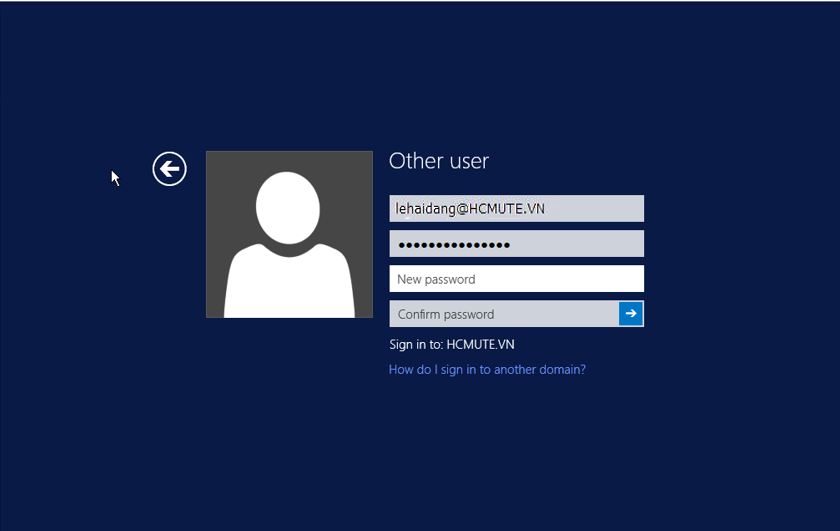
+ User must change password at next logon: Bắt buộc người dùng phải đổi mật khẩu ở lần đăng nhập (lần đăng nhập đầu tiên kể từ khi đặt mật khẩu) kế tiếp.

+ User cannot change password: Người dùng không thể thay đổi mật khẩu.

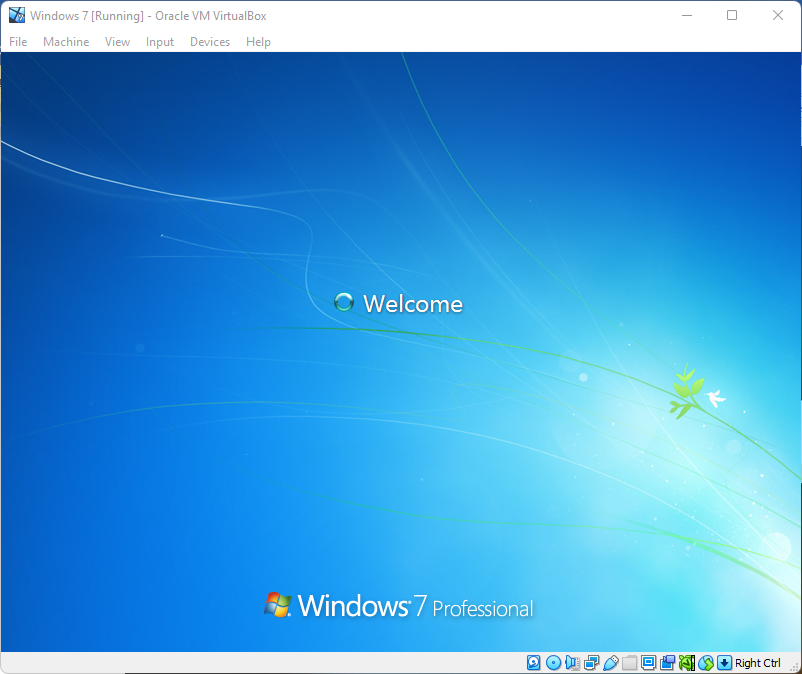
+ Password never expired: Mật khẩu không bao giờ hết hạn.

+ Account is disable: Bạn chỉ chọn dòng này khi muốn khóa tài khoản người dùng (thường sử dụng khi muốn vô hiệu hóa một tài khoản trong hệ thống).



* Tạo user thành công:
* Khi mật khẩu không vi phạm các Policy thì sẽ thoát ra và không có bất kỳ thông báo nào
* Ta tiến hành đăng nhập lần đầu để thay đổi Password

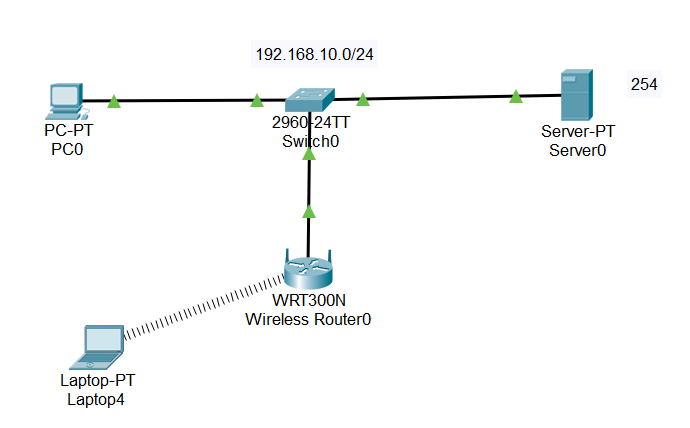


* Mật khẩu mới: Haidang1607@@, mật khẩu đúng với policy nên được chấp thuận
* Ta trở về máy Client và thử đăng nhập sai 5 lần thì màng hình sẽ treo ở trạng thái load 30s sau đó mới cho đăng nhập tiếp

1. **WiFi authentication (WPA2)**

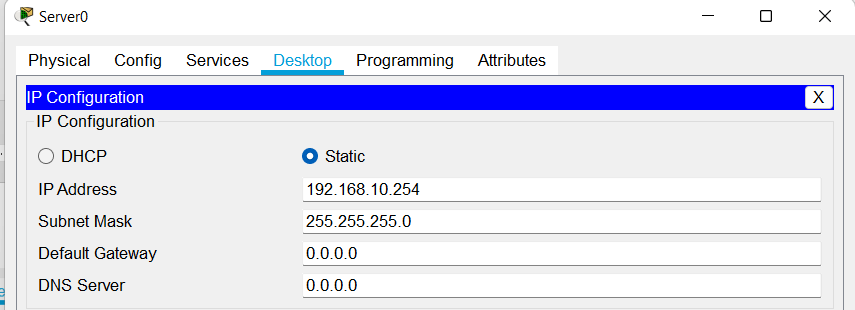
Network topology

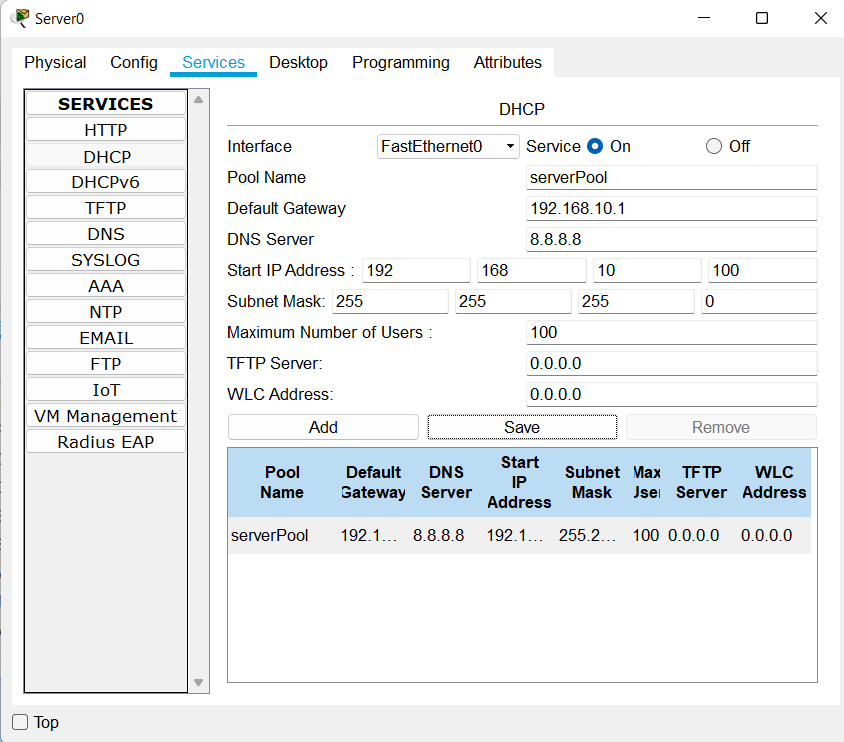




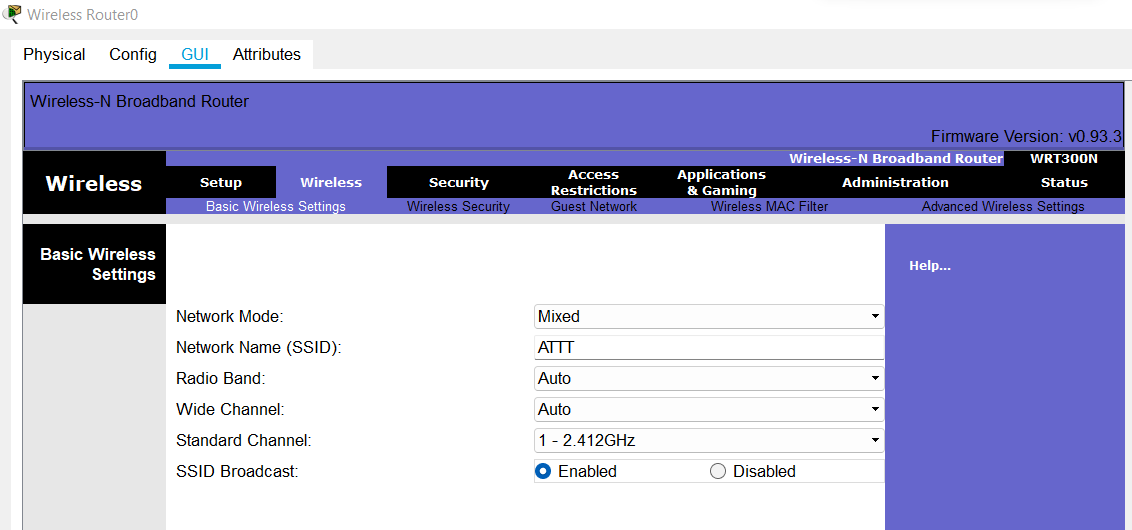
Step 1. Configure DHCP server

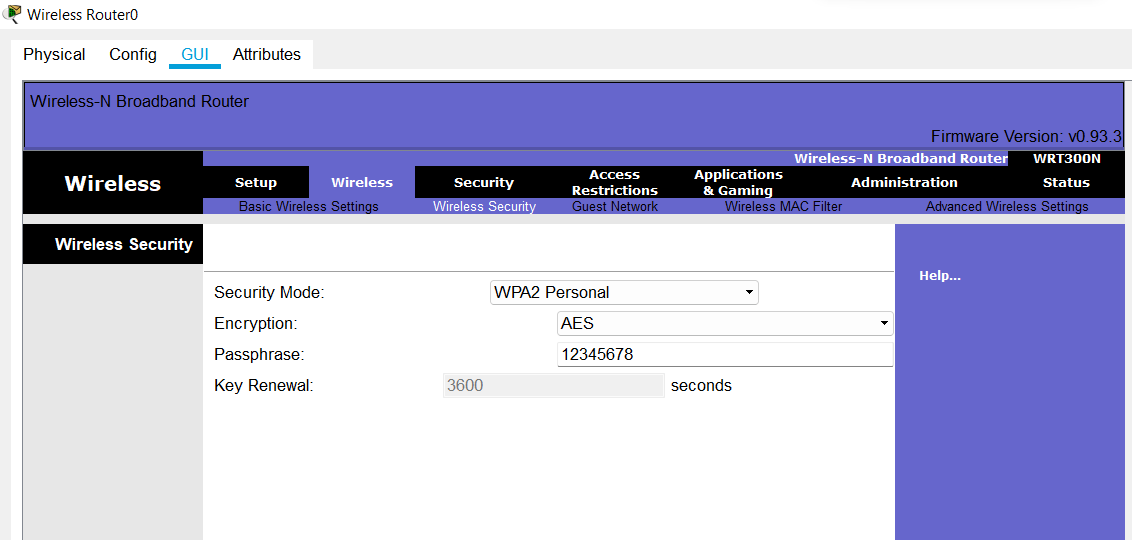
* IP address: 192.168.10.254



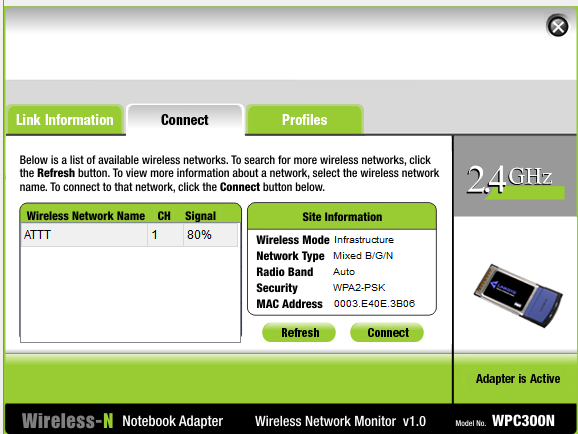
* DHCP server:
  + Network: 192.168.10.0/24
  + IP range: 192.168.10.100 – 192.168.10.200
  + Default gateway: 192.168.10.1
  + DNS: 8.8.8.8

Step 2. Configure AP

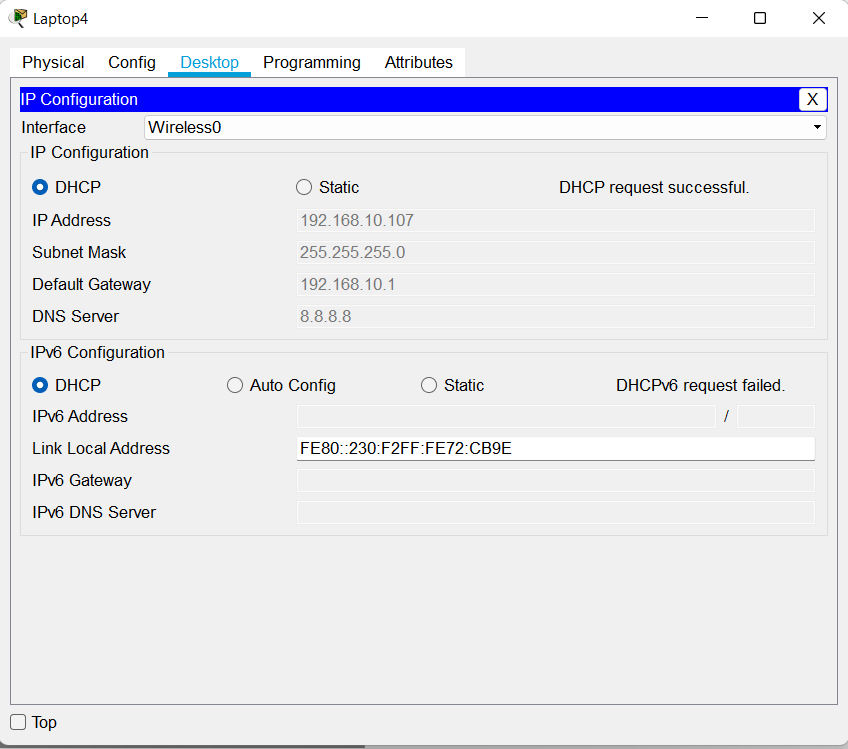
* SSID: ATTT
* Authentication: WPA2 – Personal
* Password: 12345678



Step 3. Verify the configuration

Lúc này, laptop muốn join vào thì phải mở card wifi để join:

Sau khi connect thành công, chúc ta sẽ tiến hành kiểm tra IP có đúng như chúng ta muốn không (lấy IP từ DHCP server):



Như vậy, chúng ta đã thấy Laptop đã lấy được IP từ Server.

1. **Authentication with Radius server (802.1X)**

Network topology:



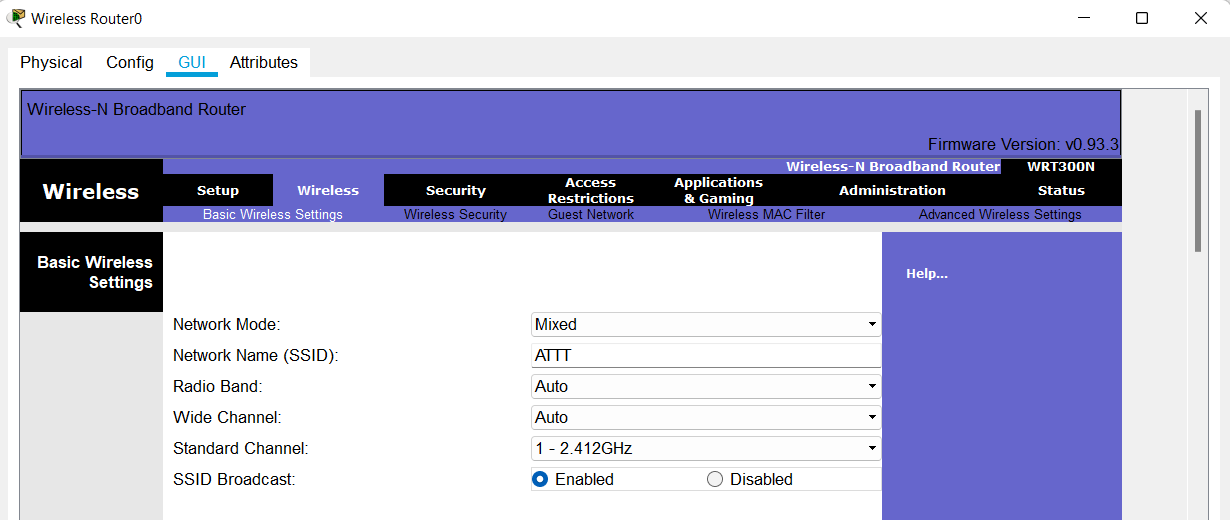
Lab environment: **Cisco Packet Tracer**

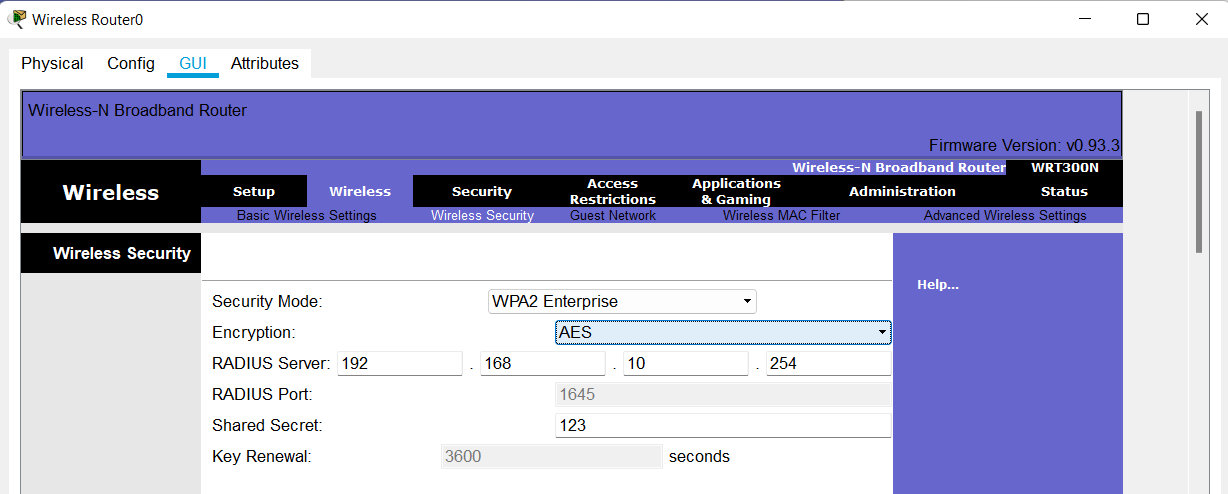
Step 1. Configure IP address & DHCP server

* DHCP server: 192.168.10.254/24
* Configure DHCP server
  + Network: 192.168.10.0/24
  + IP range: 192.168.10.100 – 192.168.10.200
  + Default gateway: 192.168.10.1
  + DNS: 8.8.8.8

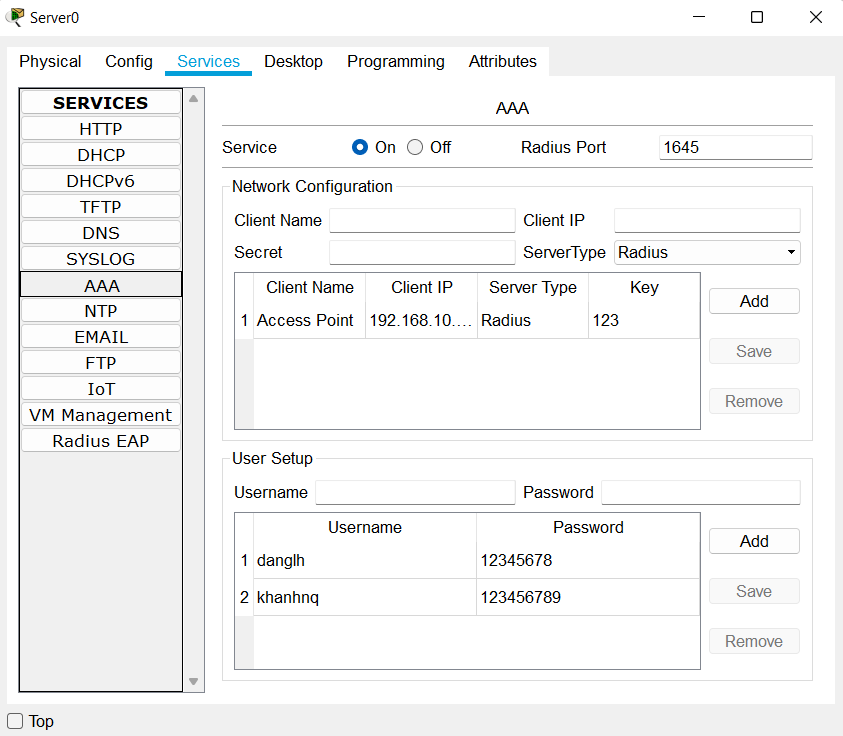
Step 2. Configure AP’s IP address

* AP’s IP address: 192.168.10.100/24
* SSID: ATTT
* Authentication (radius server): WPA2 – Enterprise



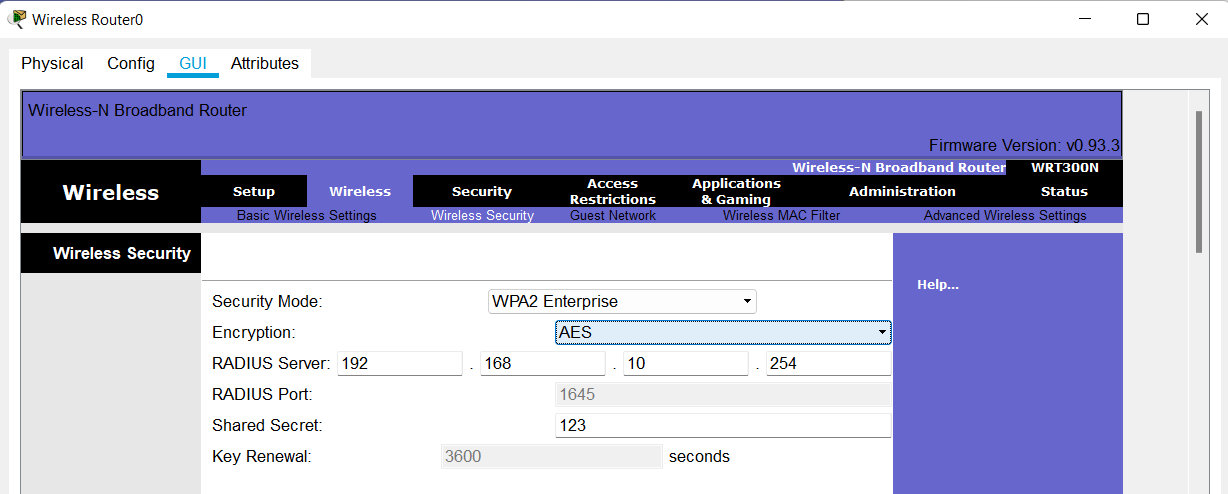


Step 3. Configure RADIUS server

* Set the IP address of the Radius client (the authenticator – AP’s IP address)
* Set the key-ID
* Create accounts

Step 4. Configure RADIUS client ( authenticator) on the AP

* Set the IP address of the Radius server
* Set the key-ID (the same as Key-ID on the Radius server)



Step 5. Verify the configuration - test on the supplicant

* Mình sẽ tiến hành kết nối Laptop thử. Trình tự các bước:
  + Nhấp vào Laptop
  + Chọn Profiles
  + Edit
  + Advanced setup
  + Next -> Next
  + Chọn như hình bên dưới và next

\

* + Nhập username và password rồi next



* + Save và Connect, nếu ra như hình dưới là thành công.

\



* + Chúng ta làm tương tự với laptop còn lại.

