

Lab 2 Window Security Hardening

1. User Management

1.1 ใช้คำสั่ง net user CorpAdmin ใช้รหัส P@ssw0rd

```
PS C:\Windows\system32> net user CorpAdmin P@ssw0rd1234 /add
The command completed successfully.
```

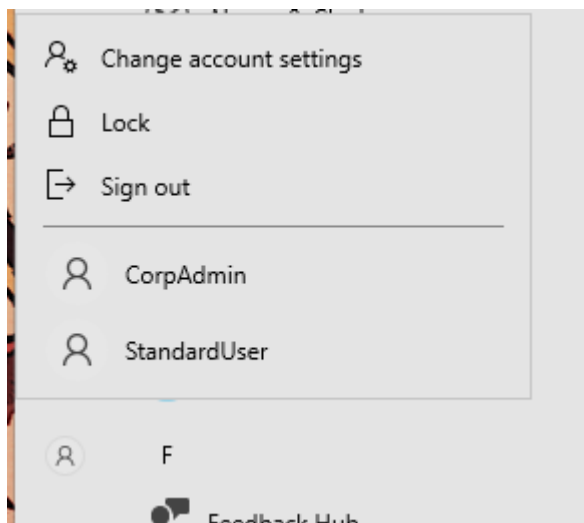
1.2 ใช้คำสั่ง net localgroup Administrators CorpAdmin

```
PS C:\Windows\system32> net localgroup Administrators CorpAdmin /add
The command completed successfully.
```

1.3 ใช้คำสั่ง net user StandardUser ใช้รหัส Password1234

```
PS C:\Windows\system32> net user StandardUser Password1234 /add
The command completed successfully.
```

Account ของทั้ง 2



2. Local Security Policy

2.1 ใช้คำสั่ง net account เพื่อ กำหนดความยาวขั้นต่ำ 12 ตัวอักษร

```
PS C:\Windows\system32> net accounts /minpwlen:12
The command completed successfully.
```

2.2 . ใช้คำสั่ง reg add เพื่อบังคับให้ใช้ complexity (ตัวพิมพ์ใหญ่/เล็ก/ตัวเลข/สัญลักษณ์)

```
PS C:\Windows\system32> reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v LimitBlankPasswordUse /t REG_DWORD /d 1 /f
The operation completed successfully.
```

2.3 ตั้ง Account Lockout Policy โดยจะมี (ล็อกหลังจากใส่รหัสผิด 5 ครั้ง, ระยะเวลาล็อก 30 นาที, Reset counter หลัง 30 นาที)

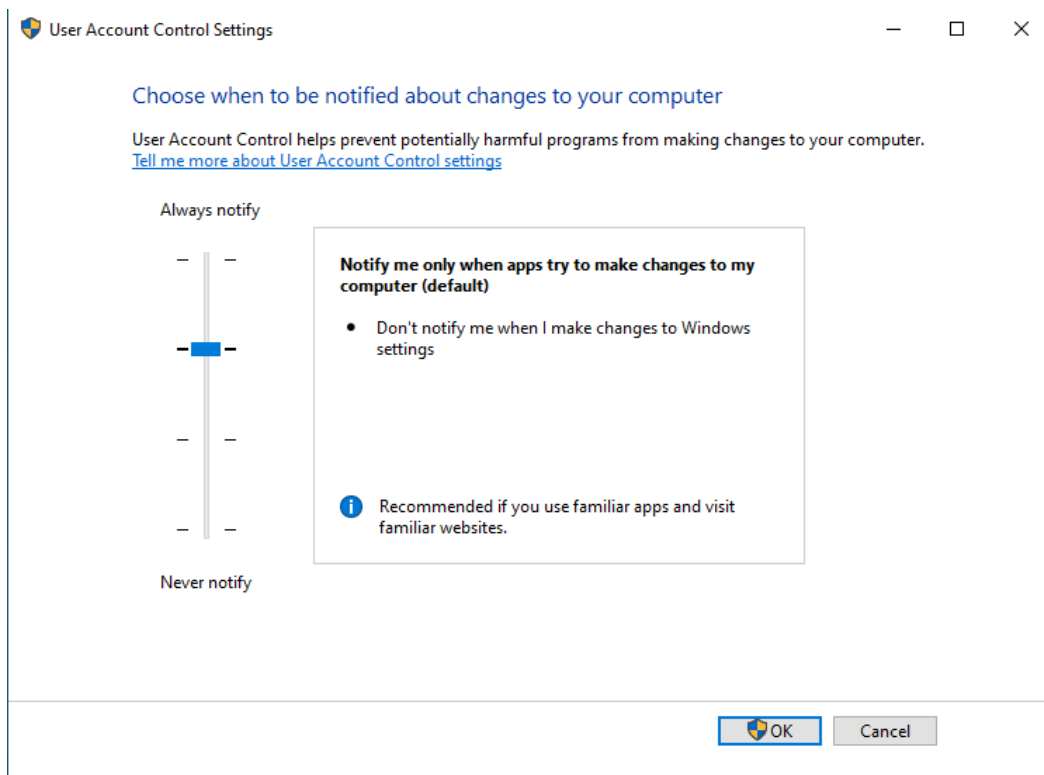
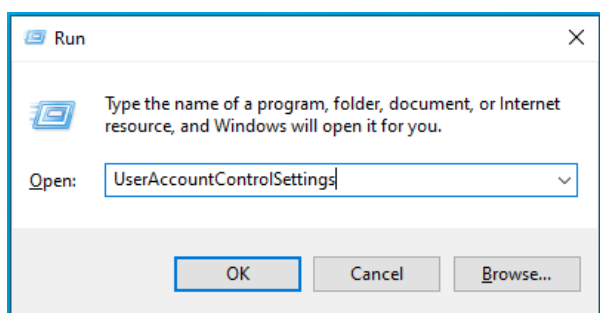
```
PS C:\Windows\system32> net accounts /lockoutthreshold:5
The command completed successfully.
```

```
PS C:\Windows\system32> net accounts /lockoutduration:30
The command completed successfully.
```

```
PS C:\Windows\system32> net accounts /lockoutwindow:30
The command completed successfully.
```

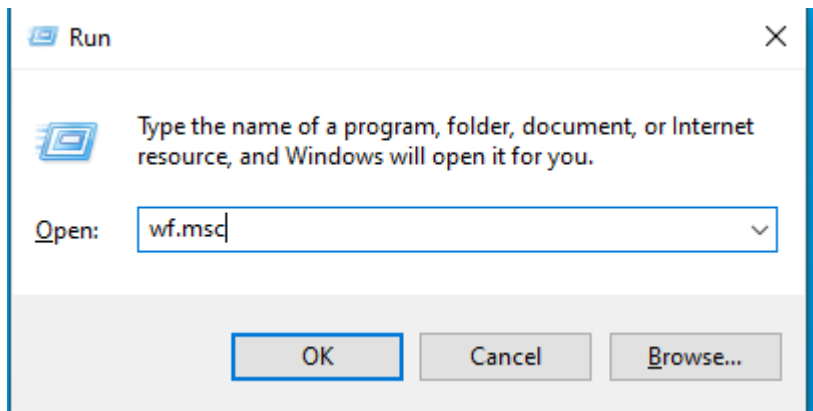
3. UAC (User Account Control)

3.1 กด Win + R แล้ว พิมพ์ UserAccountControlSettings กด Enter แล้วตรวจสอบว่า slider อยู่ที่ Default (Notify me only when apps try to make changes to my computer)

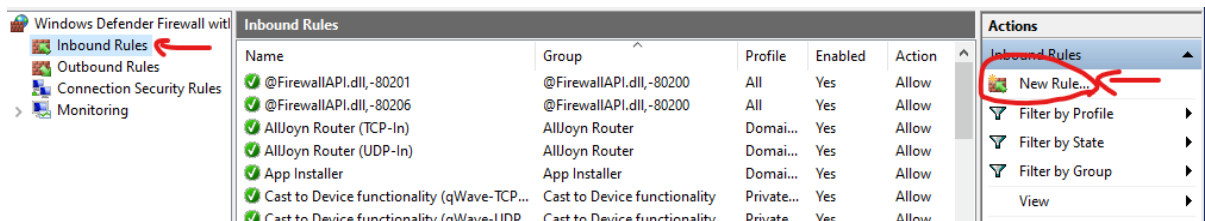


4. Windows Defender Firewall

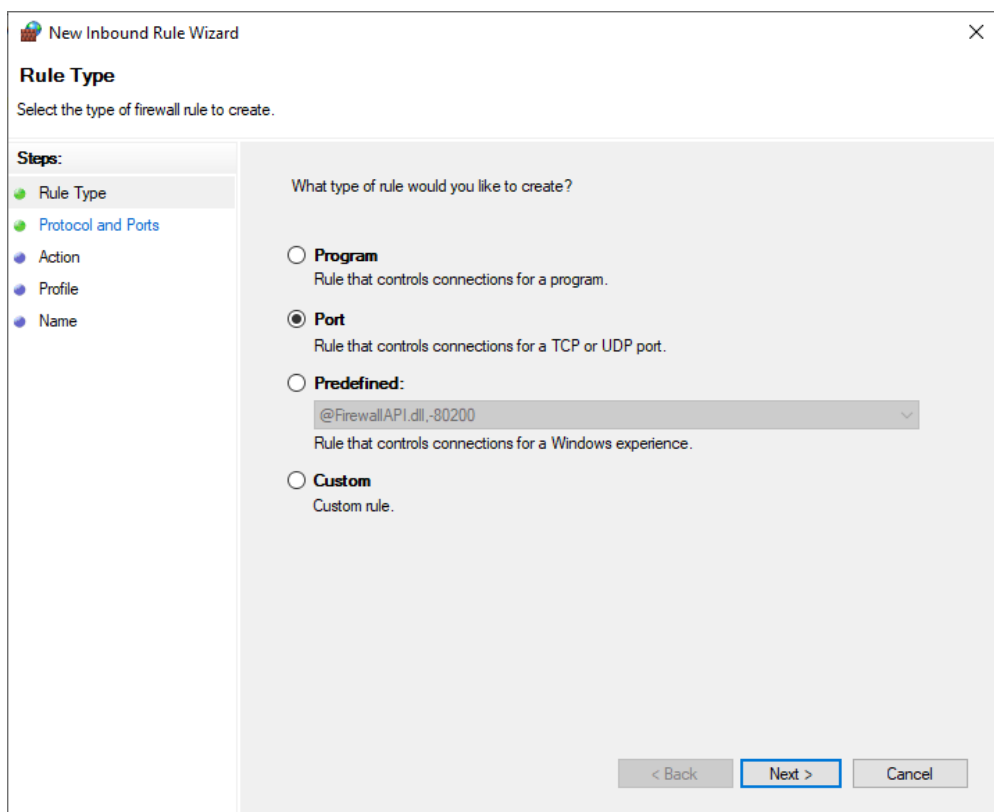
4.1 กด Win + R พิมพ์ wf.msc แล้วกด Enter



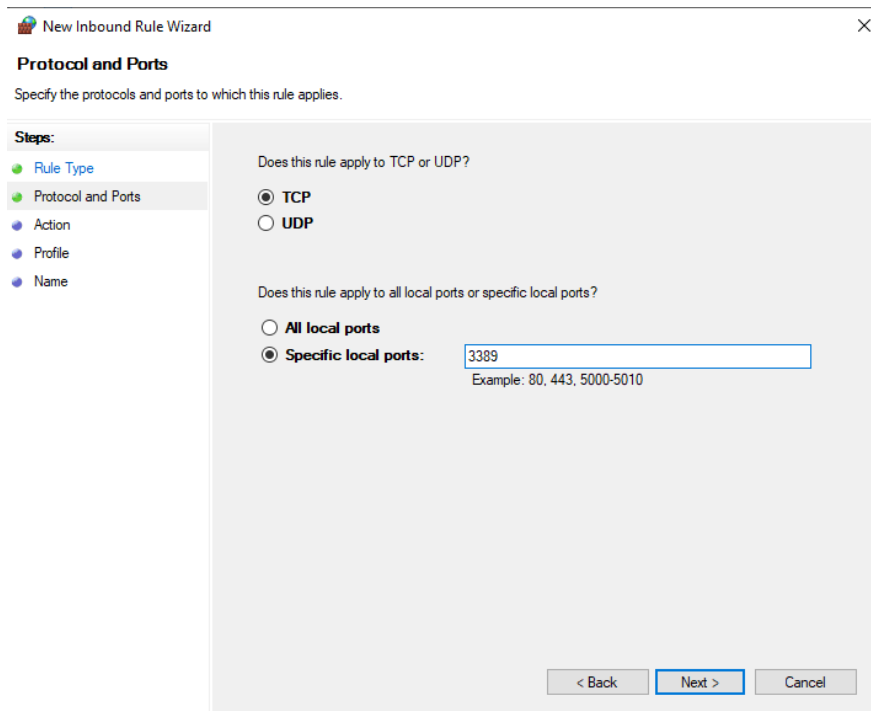
4.2 เลือกไปที่ Inbound Rules แล้วกดไปที่ New Rules



4.3 เลือกไปที่ port แล้วกด Next



กดไปที่ Tcp แล้วเลือก specific local port แล้วกรอก 3389



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

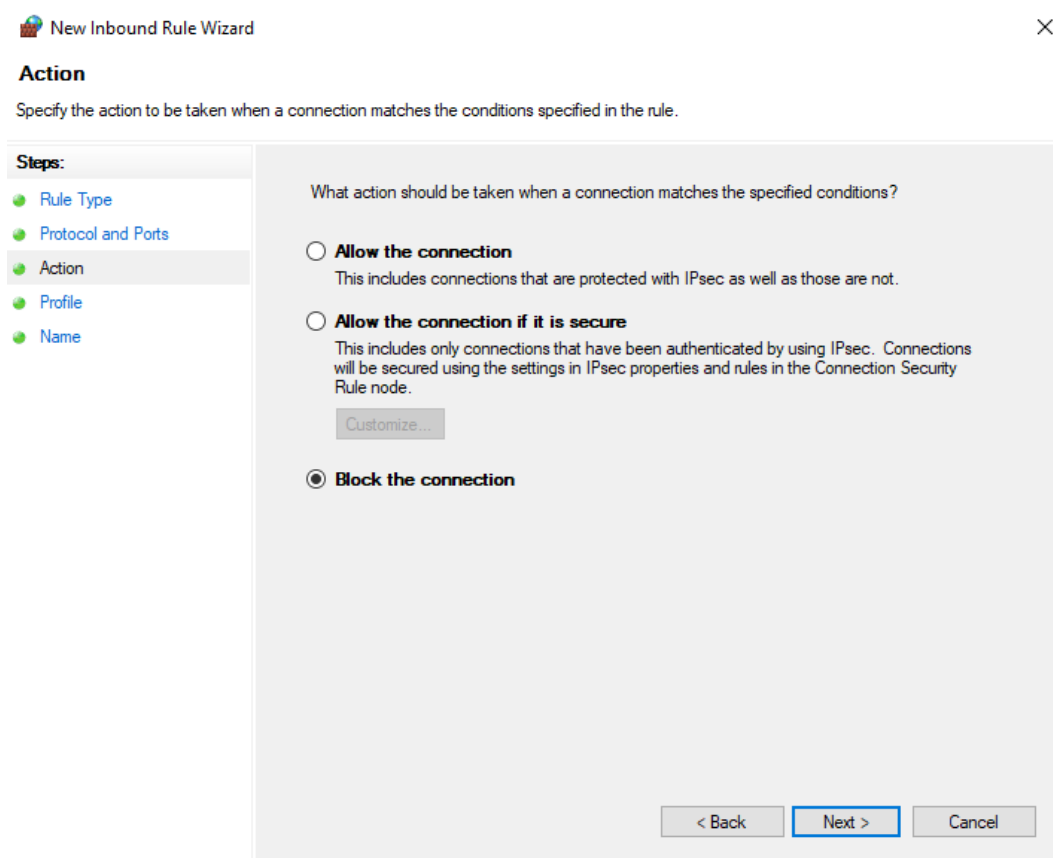
☒ TCP
☐ UDP

Does this rule apply to all local ports or specific local ports?

☐ All local ports
☒ Specific local ports:
Example: 80, 443, 5000-5010

< Back Next > Cancel

4.4 เลือก Block the connection แล้วกด Next



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

☐ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

☐ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

☒ **Block the connection**

< Back Next > Cancel

4.5 เลือกทั้งหมด แล้ว กด Next

New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile**
- Name

When does this rule apply?

☒ **Domain**
Applies when a computer is connected to its corporate domain.

☒ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☒ **Public**
Applies when a computer is connected to a public network location.

< Back **Next >** Cancel

4.6 ตั้งชื่อ Rule เป็น Block DRP แล้วกด Finish

New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name**

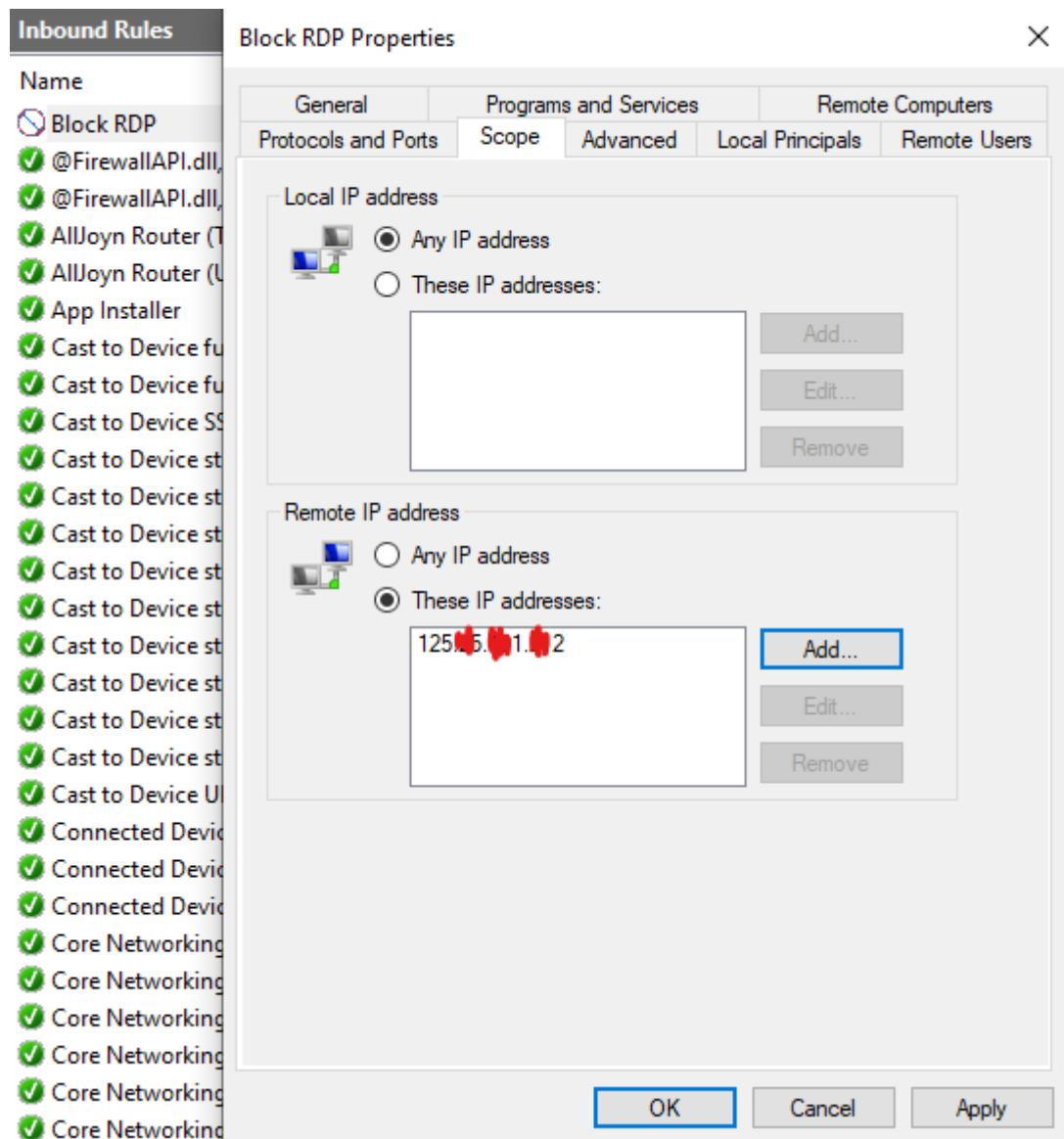
Name:
Block RDP

Description (optional):

< Back **Finish** Cancel

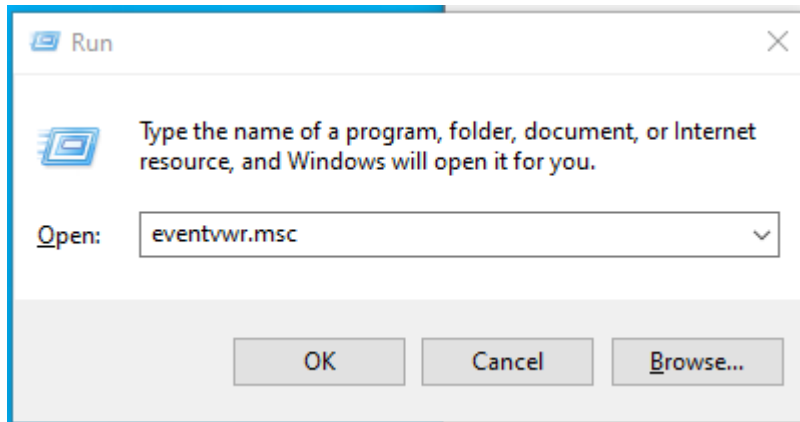
4.7 กดแก้ไข Rule Block DRP แล้วเลือกไปที่ Scope เลือกไปที่ Remote ip Address

เลือก These ip Address กด add แล้วใส่ ip เครื่องตัวเองและกด Allow connection
ที่เหลือก็บล็อกทั้งหมด



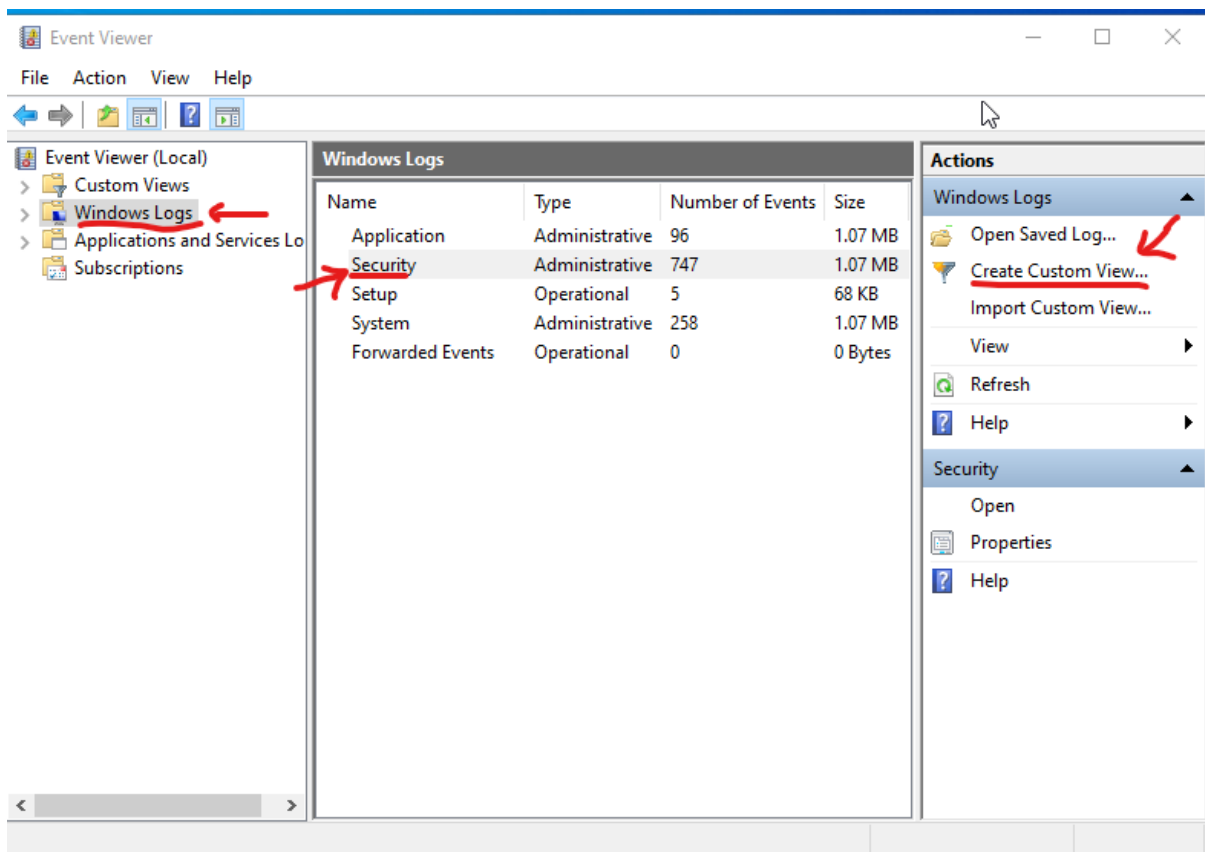
5. Event Viewer

5.1 กด Window + R พิมพ์ eventvwr.msc แล้วกด Enter

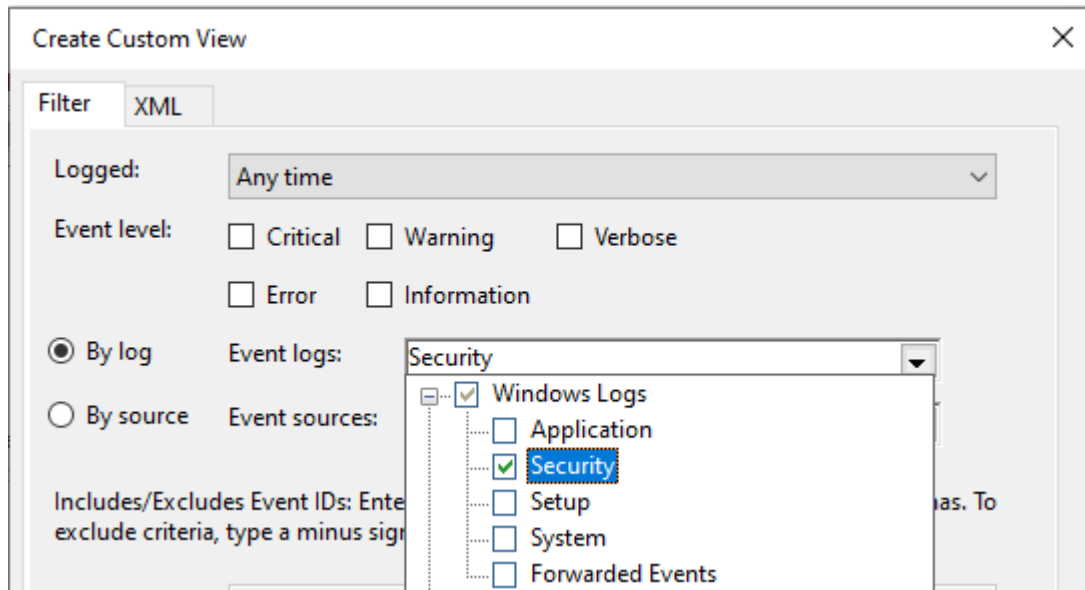


5.2 ไปที่ window Logs แล้วกด Security แล้วกดคลิกขวาที่ Custom Views แล้วกดไปที่

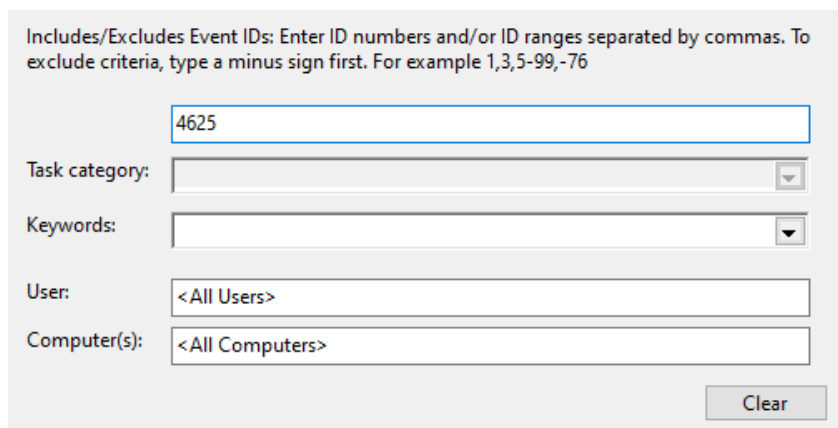
Create Custome Views



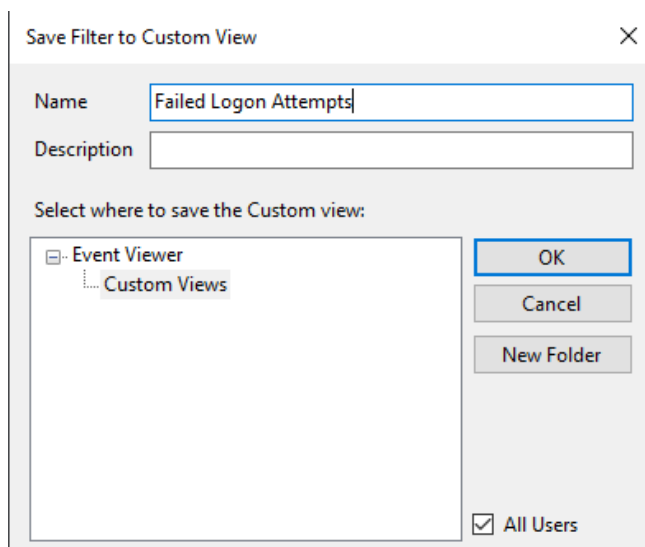
5.3 เลือกไปที่ Filter แล้วกด By log เลือกไปที่ Security



5.4 ใส่ Event id เป็น 4625



5.5 ตั้งชื่อไฟล์ เป็น Failed Logon Attempts แล้วกด OK



ปัญหาที่พบและข้อเสนอแนะ

ปัญหาที่พบ

Windows 10 Home ไม่มี Local Users and Groups (lusrmgr.msc)

→ ไม่สามารถสร้างผู้ใช้ผ่าน compmgmt.msc ได้ ต้องใช้ Settings หรือ net user command แทน

Windows 10 Home ไม่มี Local Security Policy (secpol.msc)

→ ต้องตั้ง Password Policy และ Lockout Policy ผ่าน Command (net accounts) หรือ Registry แทน

ข้อเสนอแนะเพิ่มเติม

ควร Upgrade เป็น Windows 10 Pro เพื่อให้เข้าถึงเครื่องมือ Security เช่น Local Security Policy ได้โดยตรง