



# PM PC 시스템 구축 보고서

RED 담당자	? 정조희
BLUE 담당자	민지 민지 백
진행 상태	완료
마감일	@2023년 8월 24일
최종 편집 일시	@2023년 8월 31일 오후 11:16
최종 편집자	예 예린 주
프로젝트	프로젝트 환경 구축

## PM PC 업무 파일

하나센터.zip

ESXi에 아래 사항 진행

### OS 설치

~~Windows 10 64x Home 버전~~

Windows 10 x64 22H2(OS build 19045.2965)

OS	Windows 10 Pro Version 1903 (OS Build 18362.356)
IP	172.30.40.251
USER	pm
PW	pm

### 애플리케이션 설치

UltraVNC(시나리오 변경으로 인한 취소)

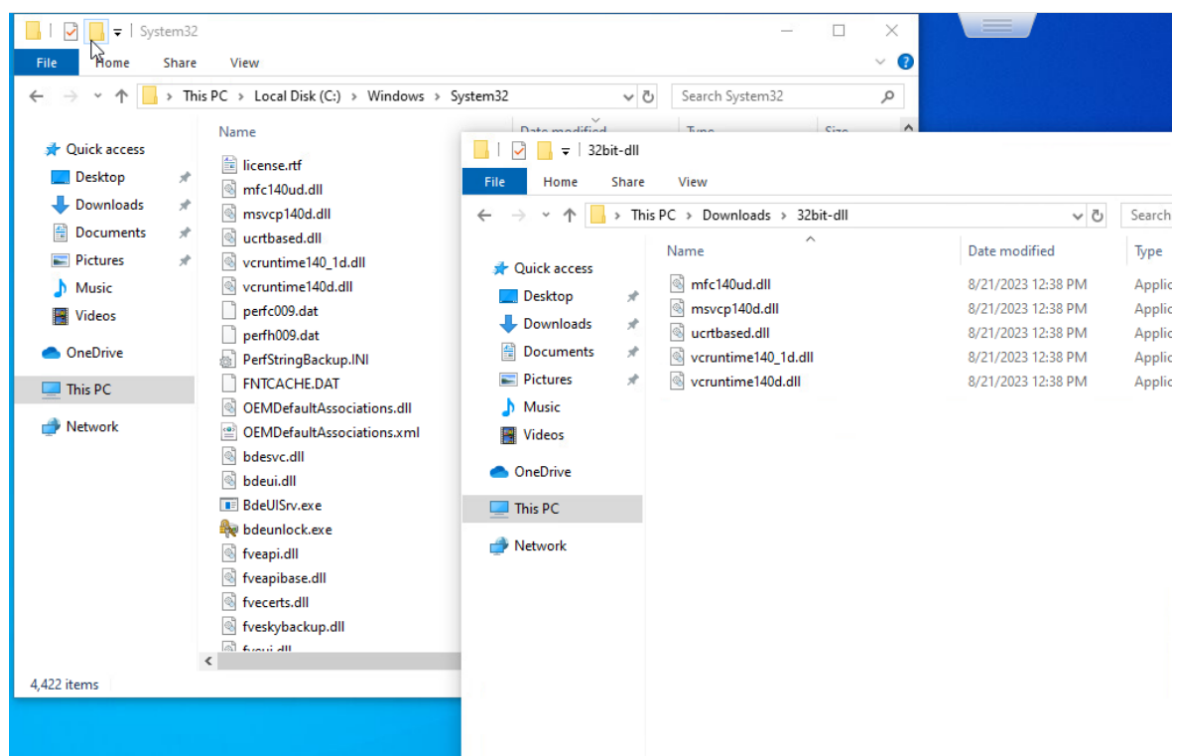
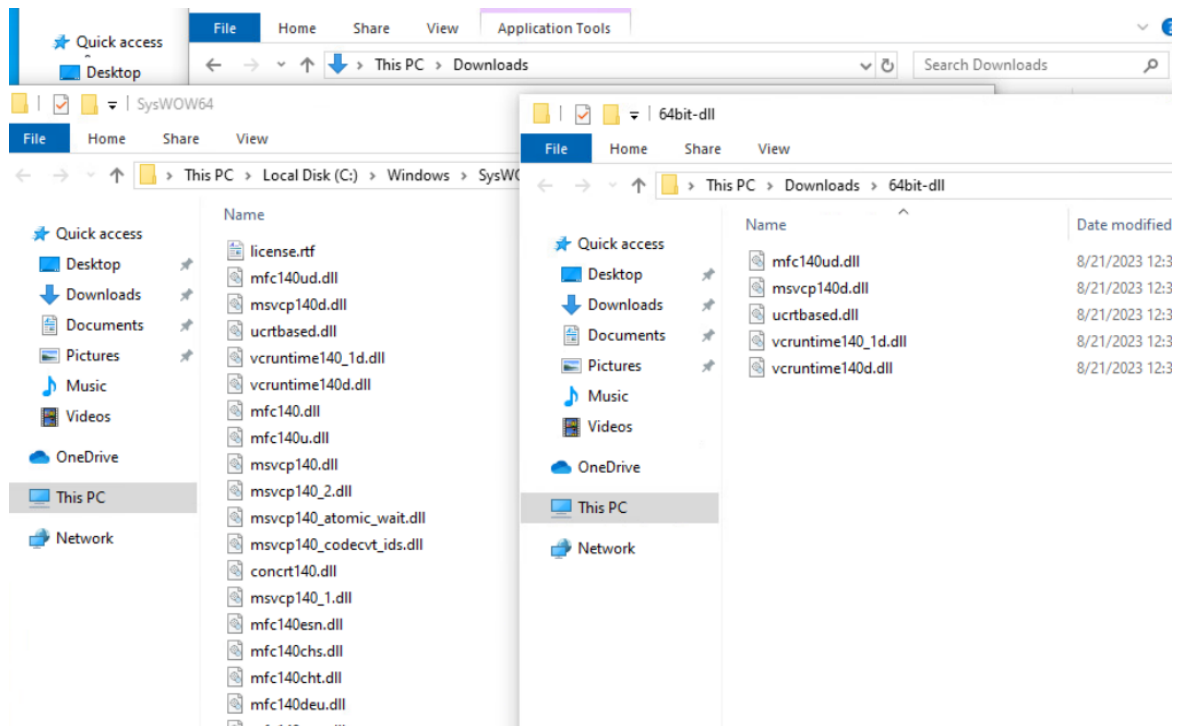
Visual Studio 2022

rdpwrapper.zip

Xshell(설치 후 db 접속 세션 만들어두기)

## 윈도우 환경 설정(취약점 부여)

### ▼ dll Error 해결

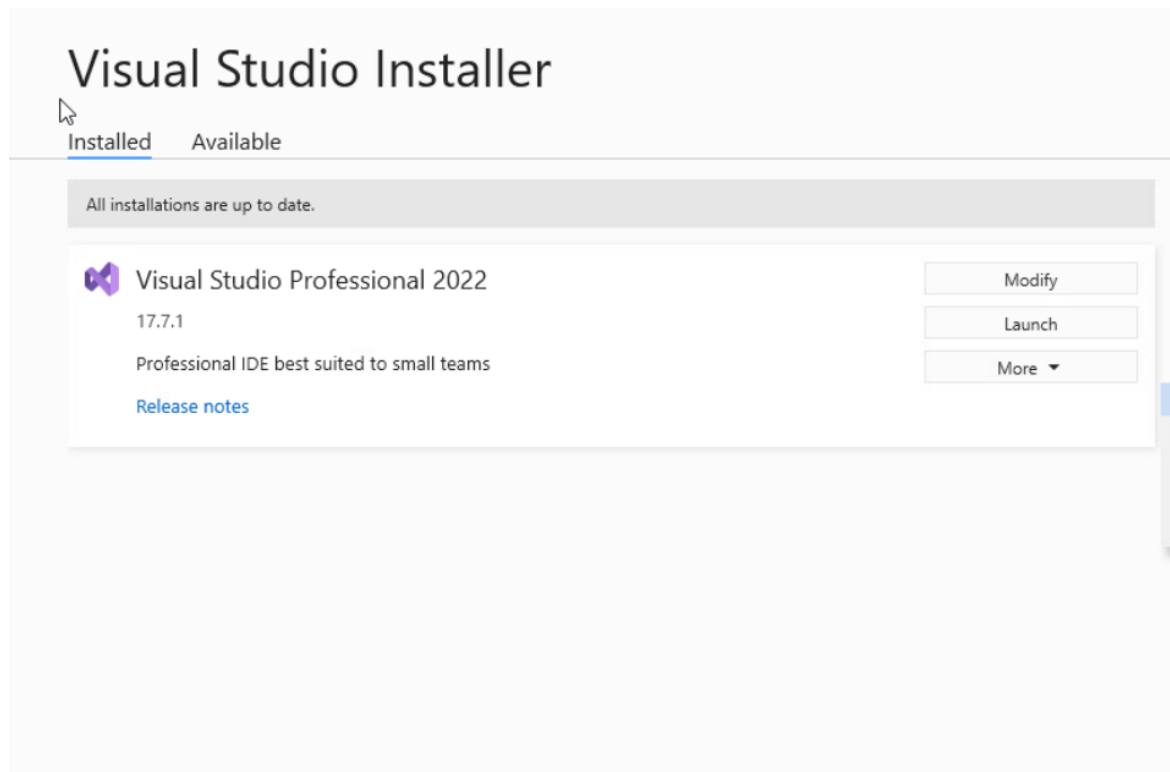


[32bit-dll.zip](#)

64bit-dll.zip

위 파일 각각 아래 경로에 복사

C:\Windows\System32\  
C:\Windows\SysWOW64\



Visual Studio 2022 Professional 설치

## ▼ 원격 접속 설정

로컬 그룹 정책 설정

로컬 그룹 정책 편집기 > 컴퓨터 구성 > 관리 템플릿 > Windows 구성 요소 > 터미널 서비스 > 원격 데스크톱 세션 호스트 > 연결

원격 데스크톱 서비스 사용자를 하나의 원격 데스크톱 서비스 세션으로 제한

원격 데스크톱 서비스 사용자를 하나의 원격 데스크톱 서비스 세션으로 제한
이전 설정(P)
다음 설정(N)

☐ 구성되지 않음(C)

☐ 사용(E)

☒ 사용 안 함(D)

설명:

지원:
Windows Server 2003 이상

옵션:

도움말:

이 정책 설정으로 사용자를 하나의 원격 데스크톱 서비스 세션으로 제한할 수 있습니다.

이 정책 설정을 사용하면 원격 데스크톱 서비스를 사용하여 원격으로 로그인하는 사용자가 해당 서버에서 하나의 세션(활성 또는 연결이 끊긴 상태)으로 제한됩니다. 사용자가 연결이 끊긴 상태에서 세션을 종료하면 다음 로그인할 때 사용자가 해당 세션에 자동으로 다시 연결됩니다.

이 정책 설정을 사용하지 않으면 사용자가 원격 데스크톱 서비스를 사용하여 원하는 수만큼 동시 원격 연결을 설정할 수 있습니다.

이 정책 설정을 구성하지 않으면 그룹 정책 수준에서 이 정책 설정이 지정되지 않습니다.

확인
취소
적용(A)

연결 개수 제한

이전 설정(P) 다음 설정(N)

☐ 구성되지 않음(C) 설명:   
☒ 사용(E)   
☐ 사용 안 함(D)

지원: Windows Server 2003 이상

옵션: 도움말:

TS 최대 허용 연결 999999

연결을 제한하지 않으려면 999999를 입력하십시오.

원격 데스크톱 서비스에서 서버에 대한 동시 연결 수를 제한할지 여부를 지정합니다.

이 설정을 사용하면 서버에서 활성화할 수 있는 원격 데스크톱 서비스 세션 수를 제한할 수 있습니다. 이 수가 초과되면 추가 사용자가 연결을 시도할 때 서버가 사용 중이므로 나중에 다시 시도하라는 오류 메시지가 사용자에게 표시됩니다. 세션 수를 제한하면 시스템 리소스를 사용하는 세션 수가 제한되므로 성능이 향상됩니다. 기본적으로 RD 세션 호스트 서버는 원격 데스크톱 서비스 세션 수를 제한하지 않으며 관리용 원격 데스크톱은 두 개의 원격 데스크톱 서비스 세션을 허용합니다.

이 설정을 사용하려면 서버에 대해 최대값으로 지정할 연결 수를 입력합니다. 연결 수를 제한하지 않으려면 999999를 입력합니다.

상태를 사용으로 설정하면 Windows 버전 및 서버에서 실행되는 원격 데스크톱 서비스 모드와 일치하는 지정된 수로 최대 연결 수가 제한됩니다.

상태를 사용 안 함 또는 구성되지 않음으로 설정하면 그룹 정책

확인 취소 적용(A)

위 설정은 관리자 권한으로 아래 커맨드 입력 시 동일 설정 가능

#### ▼ RDP Multi Session 정책 설정 커맨드

```
REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" /v fSingleSessionPerUser /t REG_DWORD /d 0 /f
// 싱글 세션 옵션 끄는 명령어

REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" /v MaxInstanceCount /t REG_DWORD /d 999999 /f
// 멀티 세션 개수 제한 없애는 명령어

gpupdate /force
// 정책 업데이트
```

#### ▼ UAC 보안 단계 설정

## 1단계로 조절

🛡️ 사용자 계정 컨트롤 설정

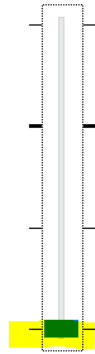
— □ ×

### 컴퓨터 변경 내용에 대한 알림 조건 선택

사용자 계정 컨트롤은 유해한 프로그램이 컴퓨터를 변경하는 것을 방지하는 데 도움을 줍니다.

[사용자 계정 컨트롤 설정에 대한 자세한 내용 보기](#)

항상 알림



알리지 않음

다음의 경우 항상 알리지 않음(사용자 계정 컨트롤 끄기)

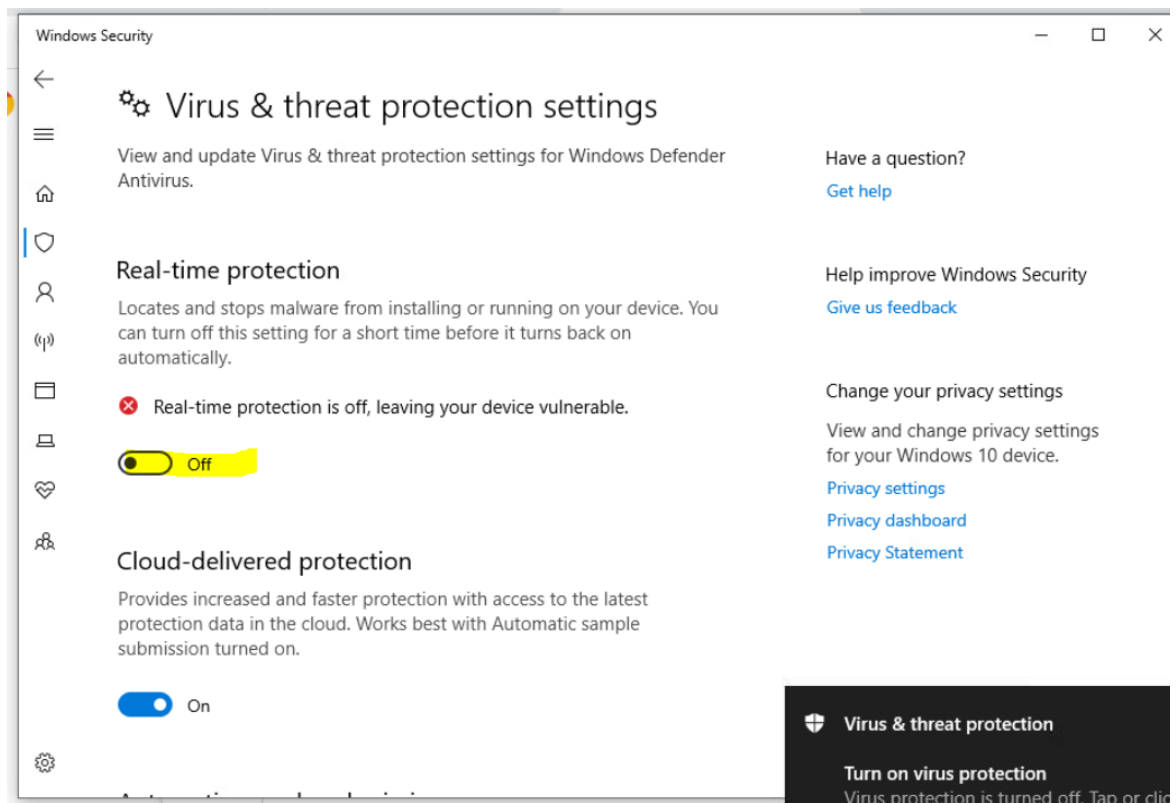
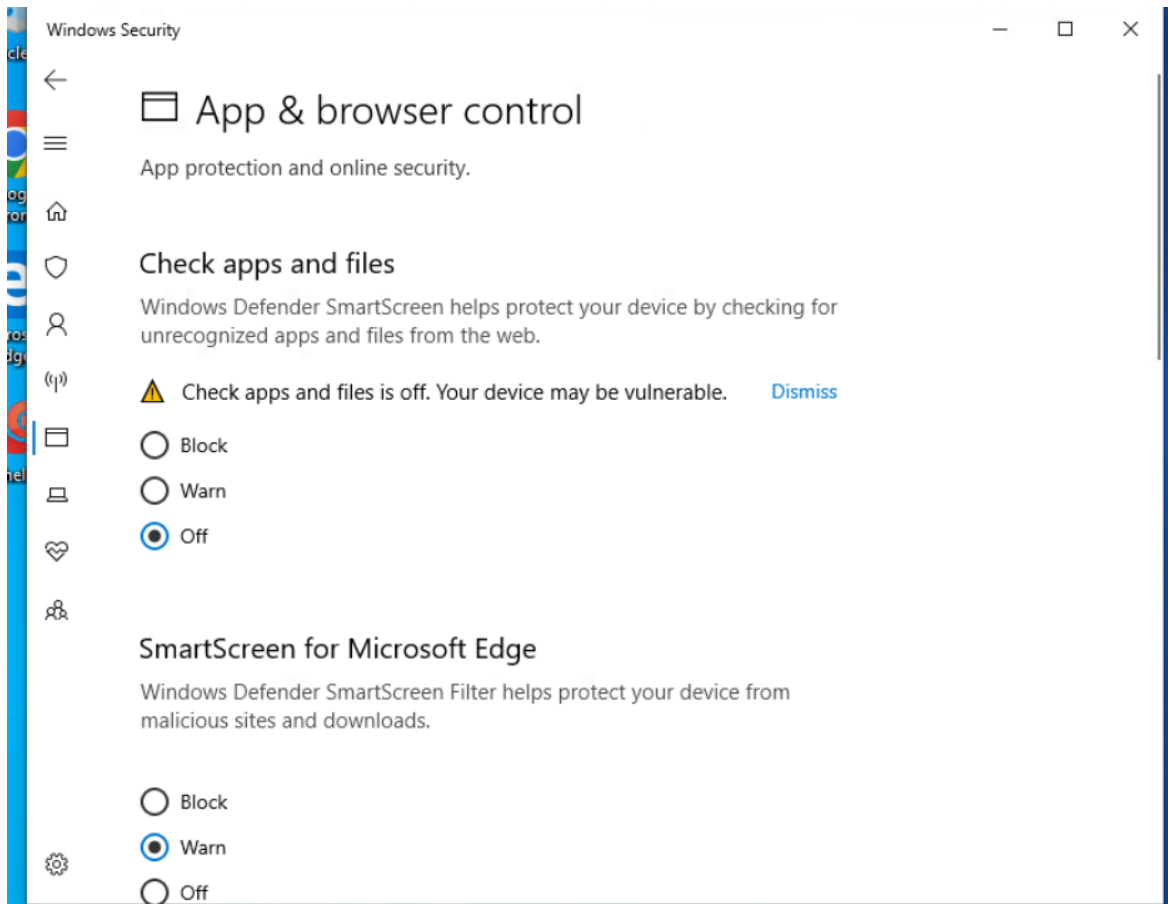
- 앱에서 사용자 모르게 소프트웨어를 설치하거나 컴퓨터를 변경하려는 경우
- 사용자가 직접 Windows 설정을 변경하는 경우

**i** 권장하지 않습니다.

🛡️ 확인

취소

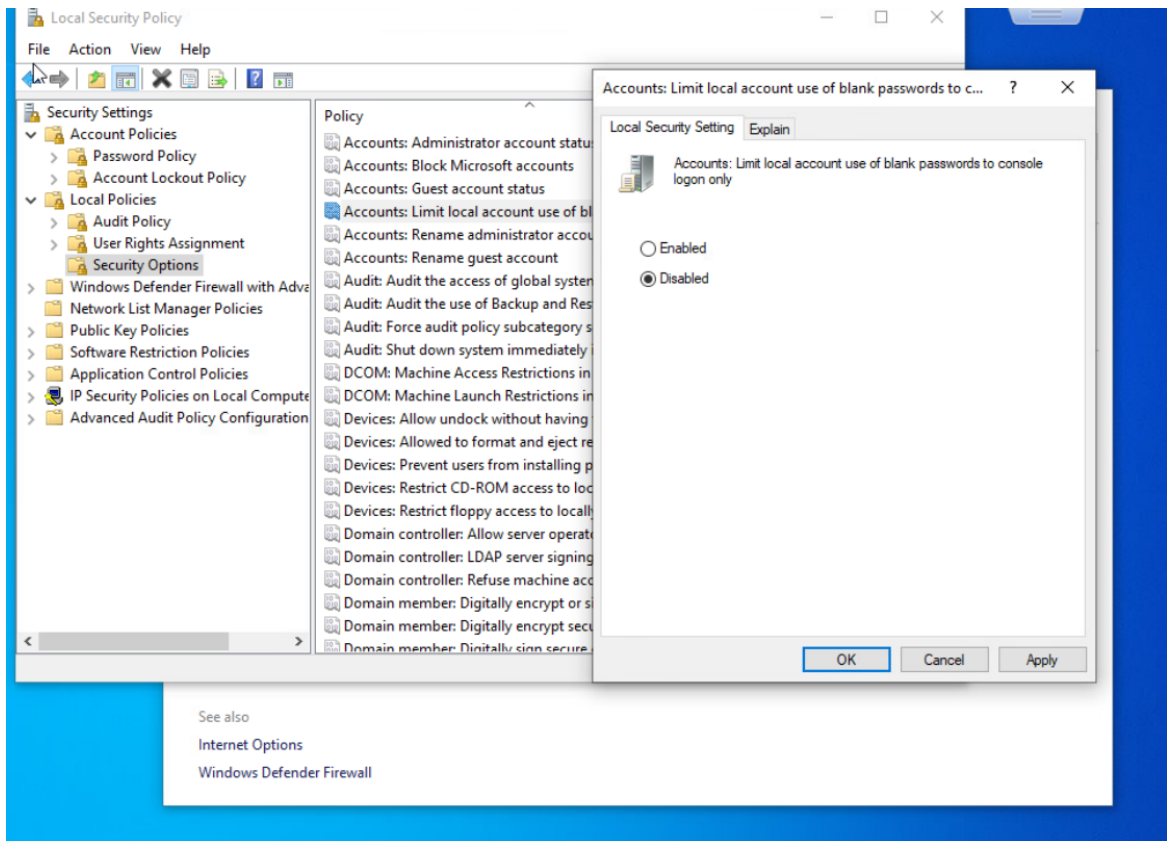
## ▼ Defender 설정



아래 설정 모두 OFF

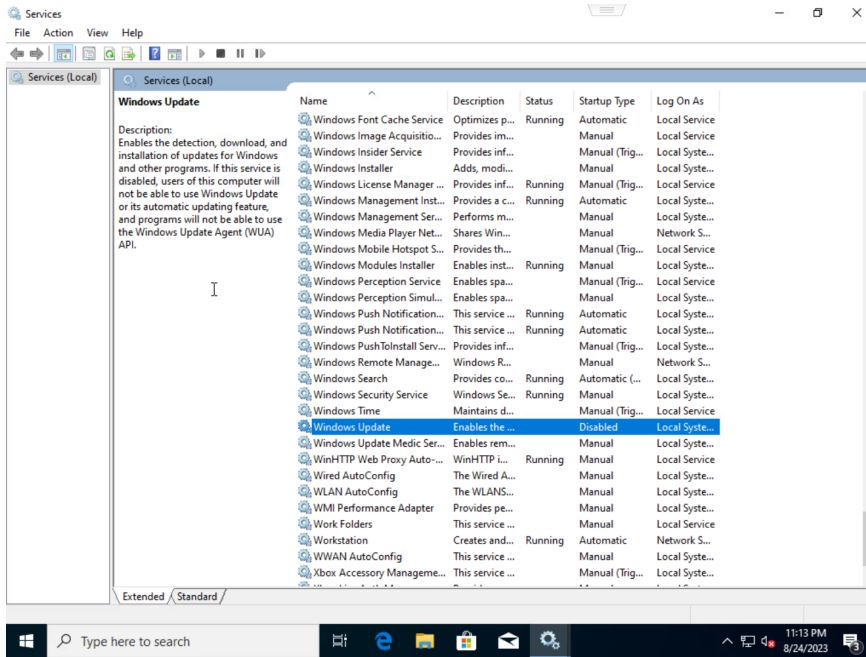
- Real-time protection
  - Cloud-delivered protection
  - Automatic sample submission
  - Tamper Protection
- 
- Check apps and files
  - SmartScreen for Microsoft Edge
  - SmartScreen for Microsoft Store apps

## ▼ 보안 정책 설정

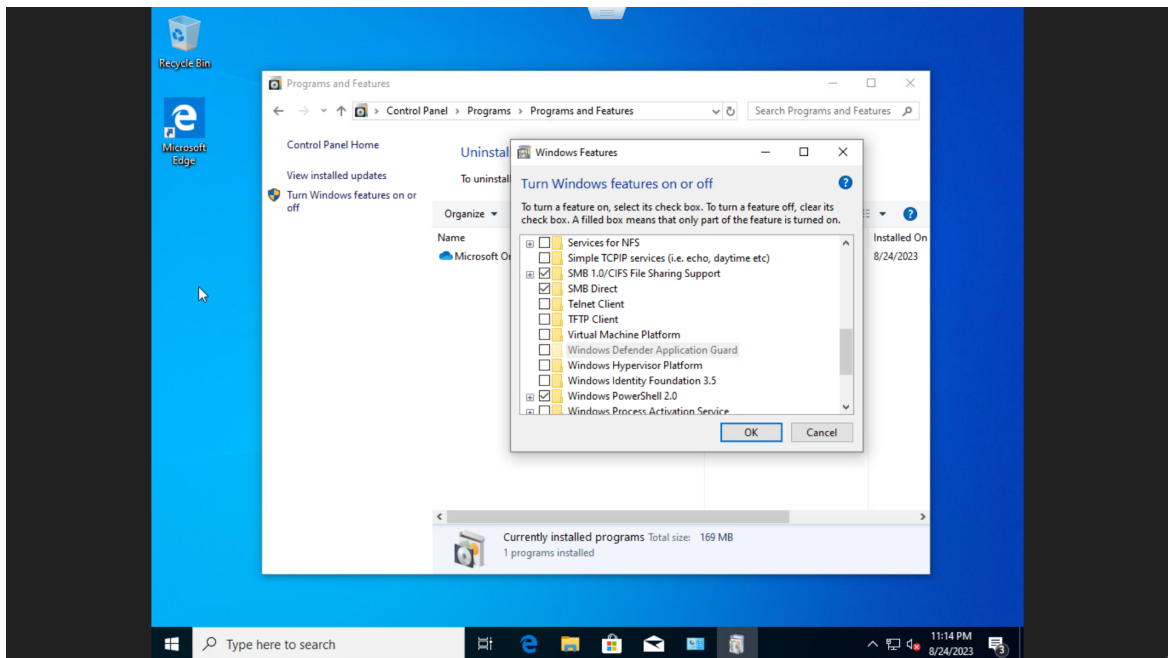


비어있는 비밀번호를 사용한 로그인 제한 설정 : Disabled

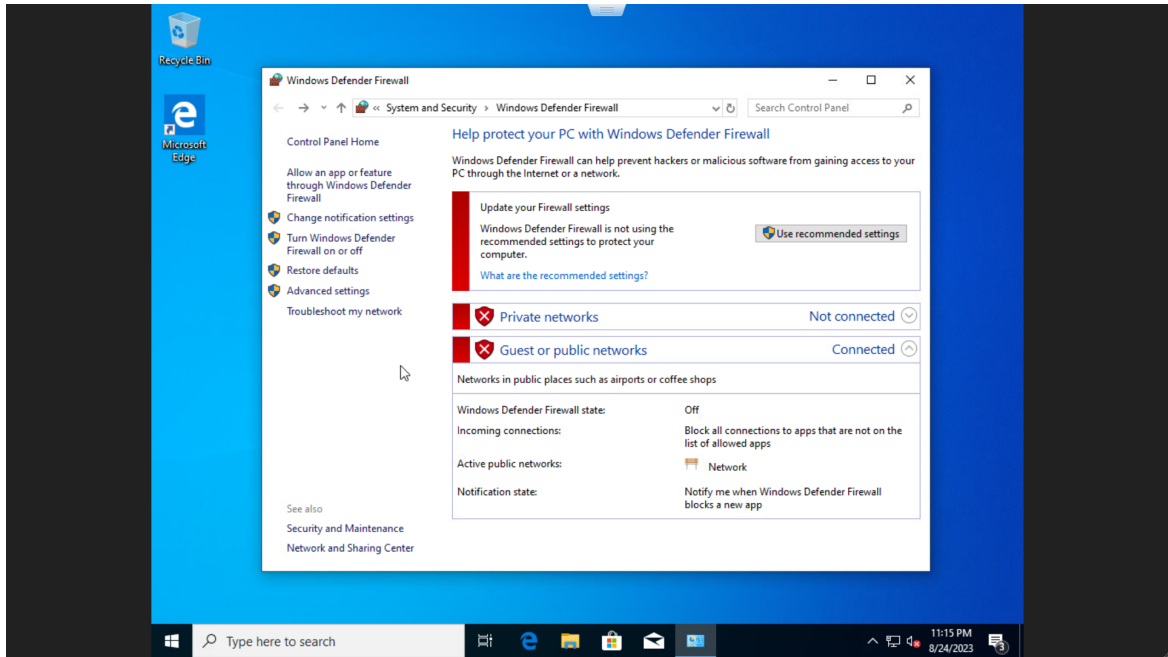




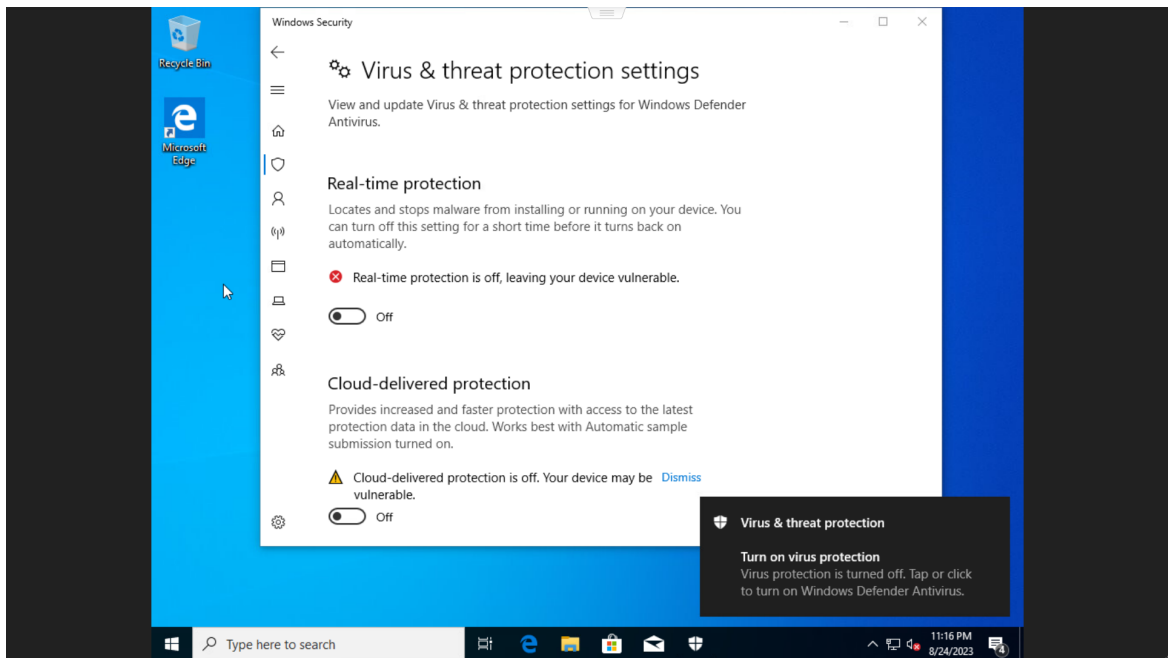
윈도우 업데이트 끄기



SMB 켜기



방화벽 끄기



실시간 감지끄기