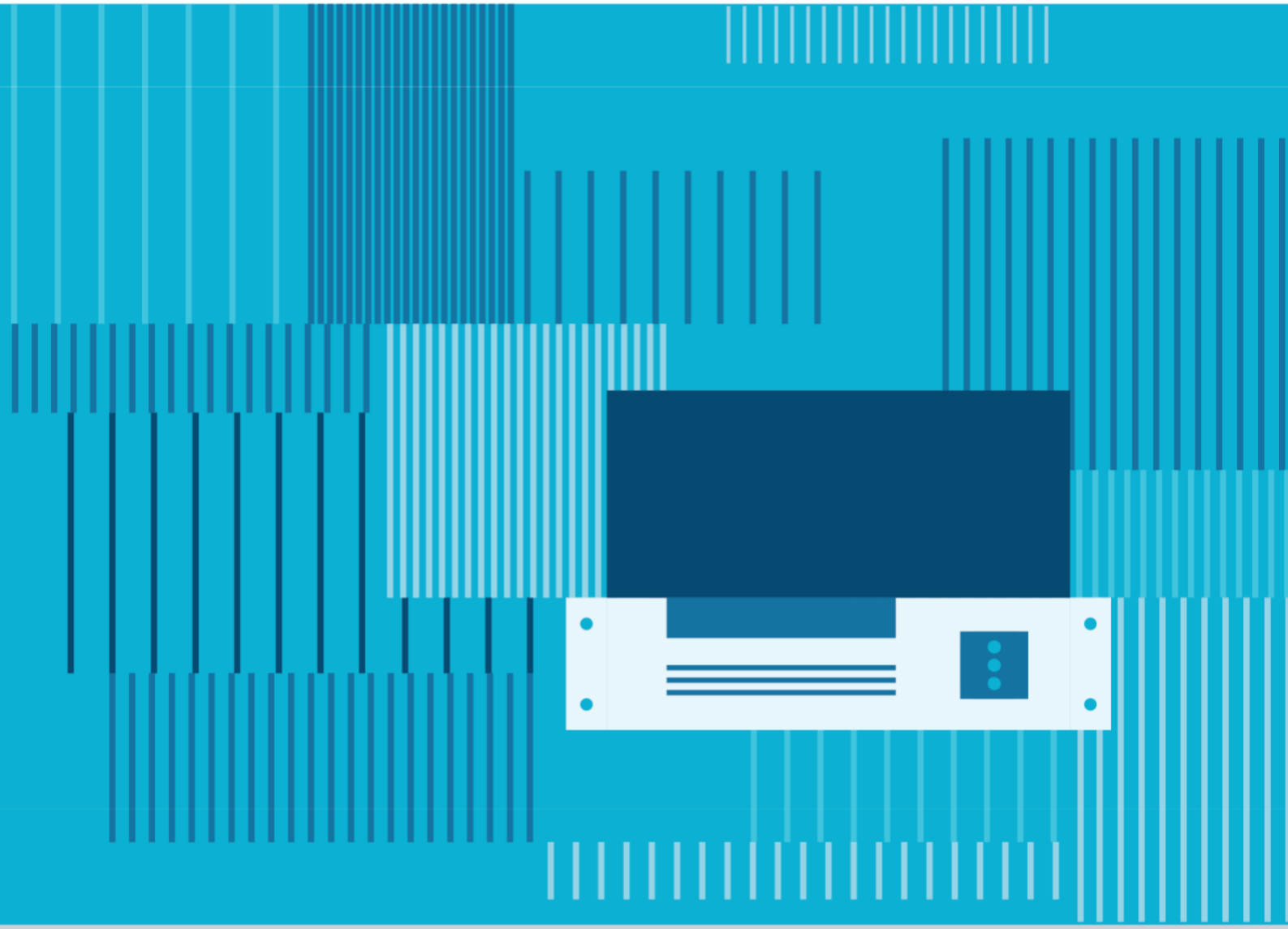
ENDPOINT PROTECTOR | by CoSoSys

가상 및 하드웨어 어플라이언스 사용자 매뉴얼



버전: 4.0

날짜: 2022 년 11 월 11 일

목 차

변경 내역

버전	날짜	비고
1.0	2020	문서 만들어짐
2.0	2022.05.16	문서가 현재 템플릿으로 업데이트됨
3.0	2022.07.10	Endpoint Protector 구성, 서버 정보, 유지 관리, 지원 챕터 이미지가 업데이트됨
4.0	2022.11.11	브라우저에서 루트 인증서 설치 챕터가 제거됨

1. Endpoint Protector 가상 어플라이언스 포맷

Endpoint Protector 가상 어플라이언스는 다른 포맷과 다양한 플랫폼에서 사용할 수 있습니다. 아래 테이블은 지원하는 가장 환경, 버전, 주요 포맷 목록을 제공합니다.

1.1. 테이블

Endpoint Protector 가상 어플라이언스는 이전 버전의 가상화 소프트웨어에서도 구동할 수 있습니다. 이는 가능한 쉽게 테스팅과 구현을 하도록 만듭니다. 추가적인 정보는 다음 챕터에서 찾을 수 있습니다.

Supported Virtual Environments	Version	.OVF	.OVA	.VMX	.VHD	.PVM	.XVA
VMware Player	7.1.0	•	•	•			
VMware Workstation	11.1.0	•	•	•			
Oracle VM VirtualBox	5.0.28	•	•				
VMware vSphere (ESXi)	6.0.0	•	•				
VMware Fusion Professional	7.1.3	•	•				
Hyper-V Manager Windows Server 2016	10.0.14393.0				•		
Parallels Desktop	11.1.3					•	
Citrix XenCenter	6.2						•

참고: 가장 일반적으로 사용되는 포맷은 OVF (Open Virtualization Format)입니다. 주요 가상화 소프트웨어와 호환되기 때문입니다.

1.2. 가상화 소프트웨어로 지원되는 포맷

위의 테이블 목록에 있는 가상화 소프트웨어에 추가하여 언급된 포맷은 또한 아래의 소프트웨어에서도 지원합니다.

1. **OVF and OVA**
    - VMware Workstation 11.1
    - VMware Player 5.0 (or higher)
    - VMware Fusion 7.1.2
    - VMware ESXi 5.1 (or higher)
    - Oracle VM VirtualBox
    - Citrix XenCenter 6.2
2. **VHD**
    - Microsoft Hyper-V 6.1.7601.17514
    - Microsoft Hyper-V 6.3.9600.16384
3. **PVM**
    - Parallels Desktop 10.2.1
4. **XVA**
    - Citrix XenServer 5.5
    - Citrix XenServer 6.0
5. **VMX**
    - VMware Player 5.0 (or higher)
    - VMware Workstation 9.0 (or higher)

참고: .VMX 가상 어플라이언스는 최신 VMware Workstation 버전 (v11.x.x)와 최신 VMware Player 버전 (v7.x.x)에서 구동되도록 설정됩니다.

이전 버전의 VMware Workstation / VMware Player 에서 가상 어플라이언스가 구동하기 위해서는 아래 단계를 따르시기 바랍니다:

1. .zip 파일 압축을 풀고 압축이 풀린 위치로 이동;
2. 텍스트 편집기를 사용하여 .VMX 파일 편집을 클릭;
3. "virtualHW.version" 필드 검색;
4. 기본 버전 (default = 11)을 새로운 버전으로 대체
    - VMware Workstation v9.x.x 또는 VMware Player v5.x.x 에서 .VMX 가상 어플라이언스를 구동하기를 원하면 virtualHW.version = "9" 으로 편집
    - VMware Workstation v10.x.x 또는 VMware Player v6.x.x 에서 .VMX 가상 어플라이언스를 구동하기를 원하면 virtualHW.version = "10" 으로 편집
5. 변경 내용 저장 후 텍스트 편집기 닫기;
6. 가상 이미지 가져오기;
7. 가상 머신 시작

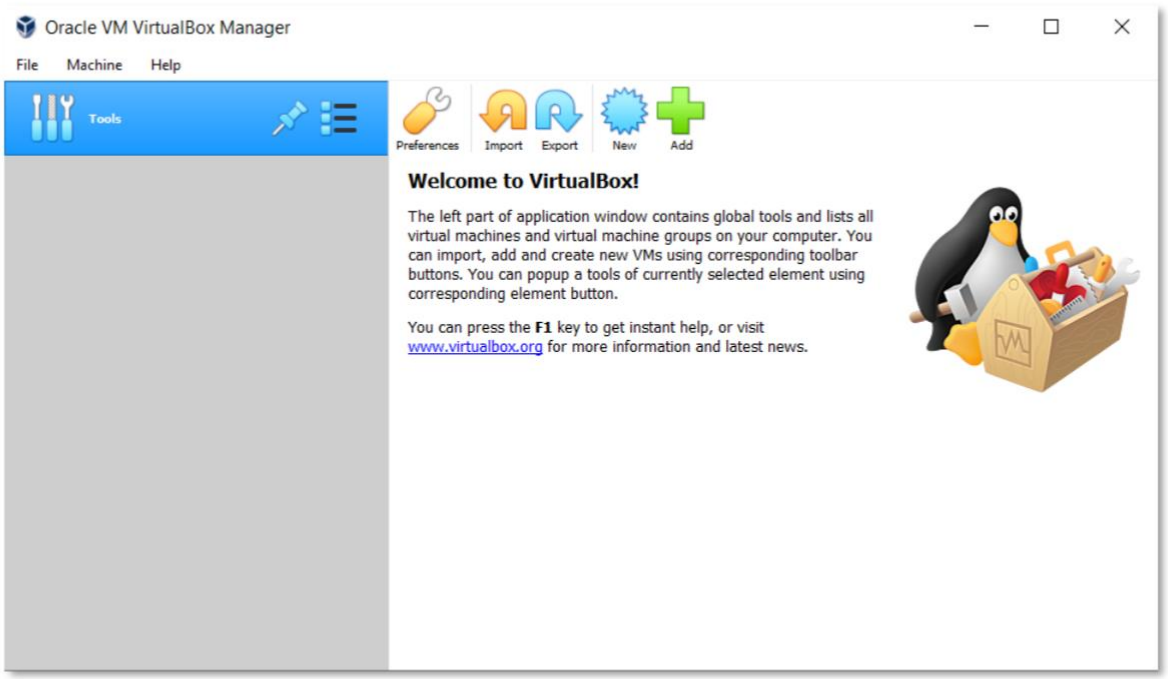
2. OVF 포맷을 사용하여 구현

OVF 포맷을 사용하여 Endpoint Protector 가상 어플라이언스를 구현하는 여러 옵션이 있습니다.

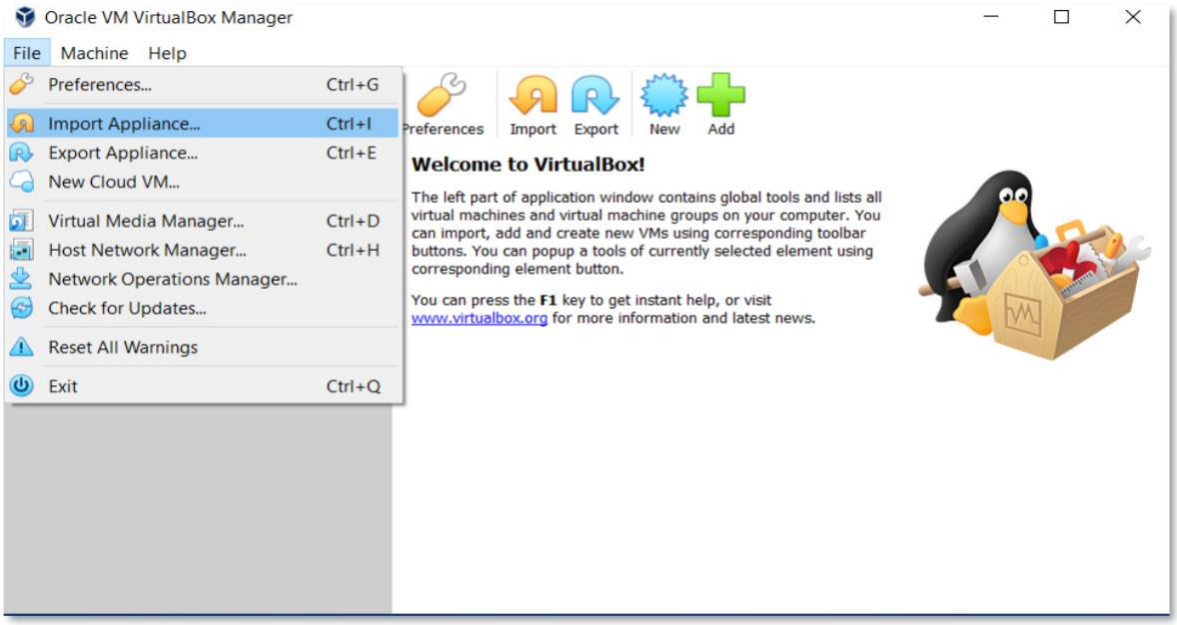
2.1. Oracle VM VirtualBox

Oracle VM VirtualBox 사용하여 구현하기 위해서는 아래 단계를 따르시기 바랍니다:

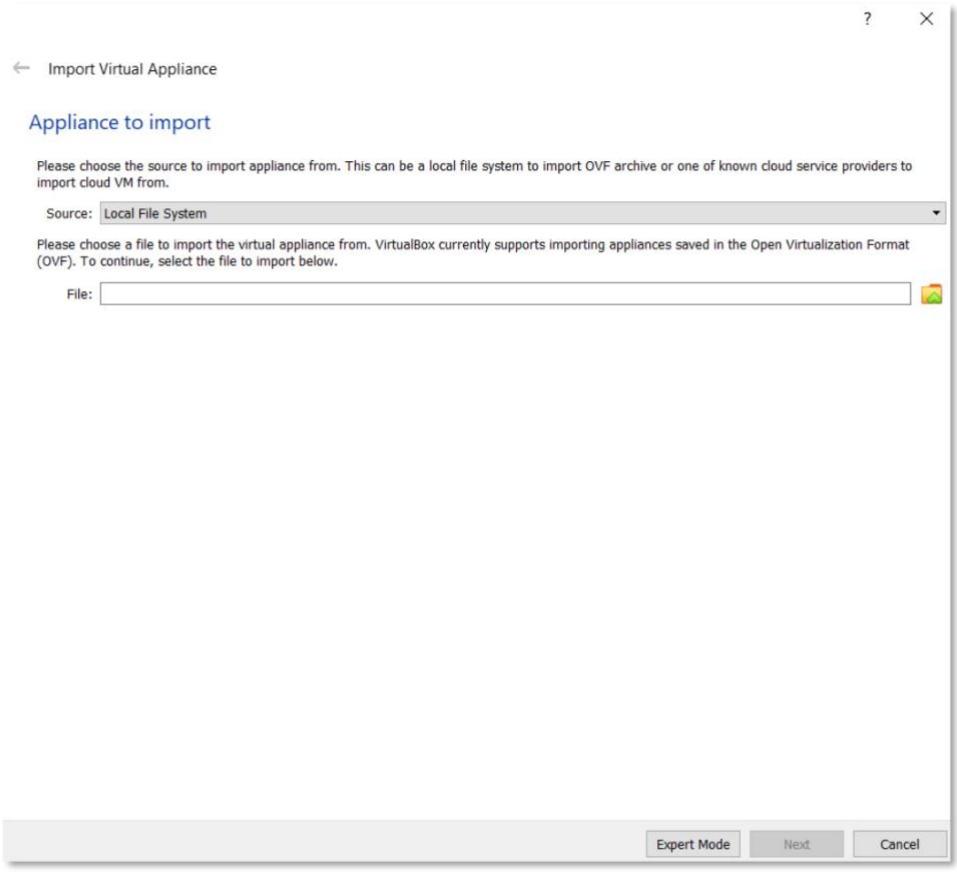
1. 다운로드한 패키지를 Unzip;
2. **VirtualBox** 열기;



3. **File** 이동 후 **Import Appliance** 선택;

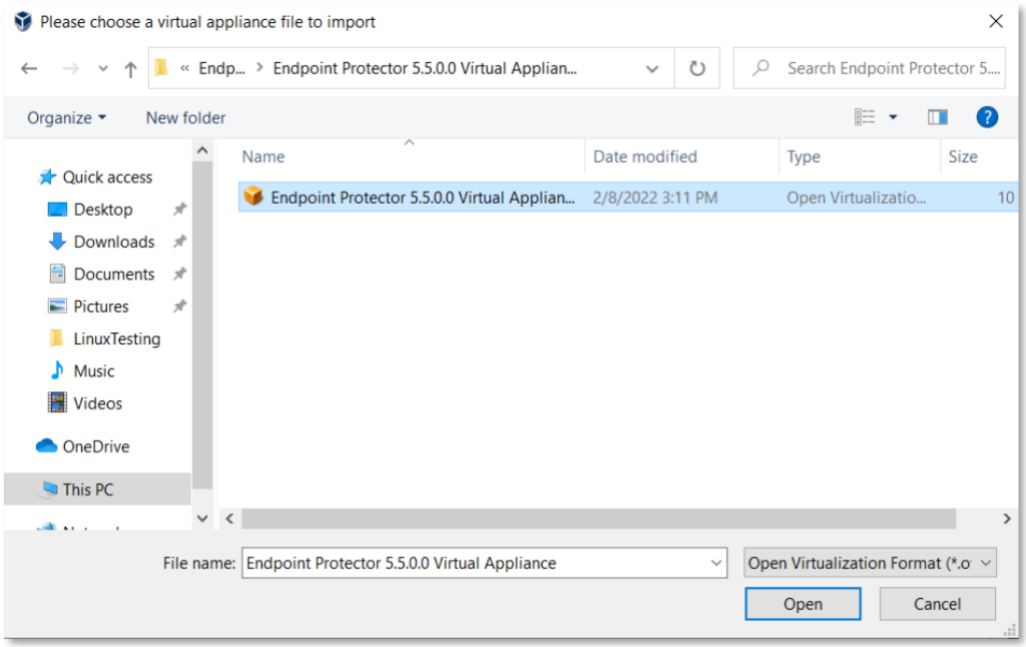


4. **Appliance to import** 페이지에서 **File icon** 클릭 후 압축이 풀린 OVF 파일을 찾아서 선택;

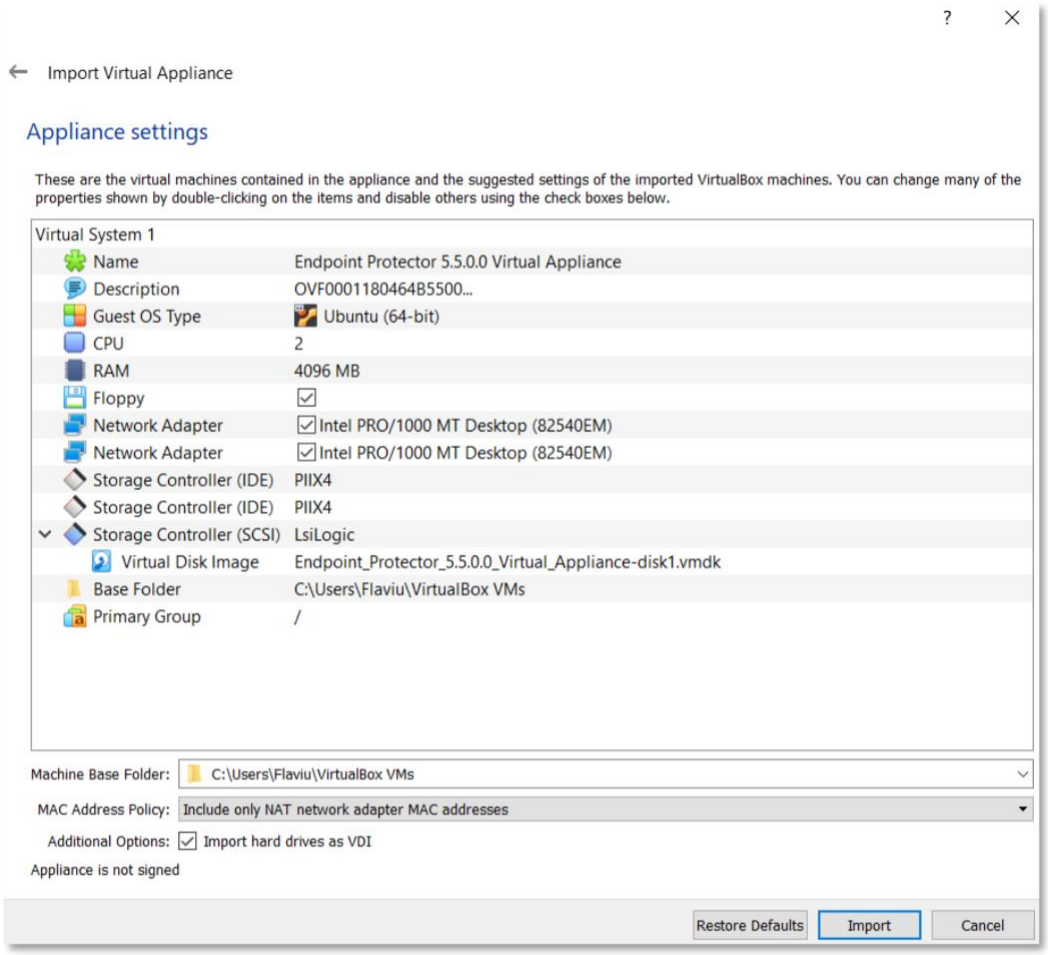


-

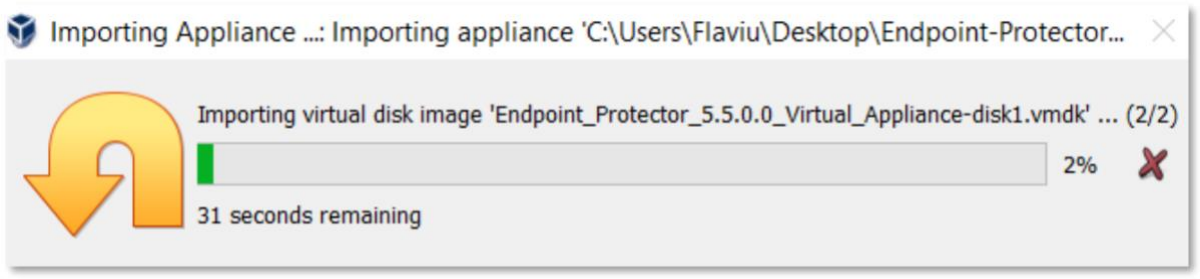
5. **Open** 클릭;



6. **Import** 클릭;

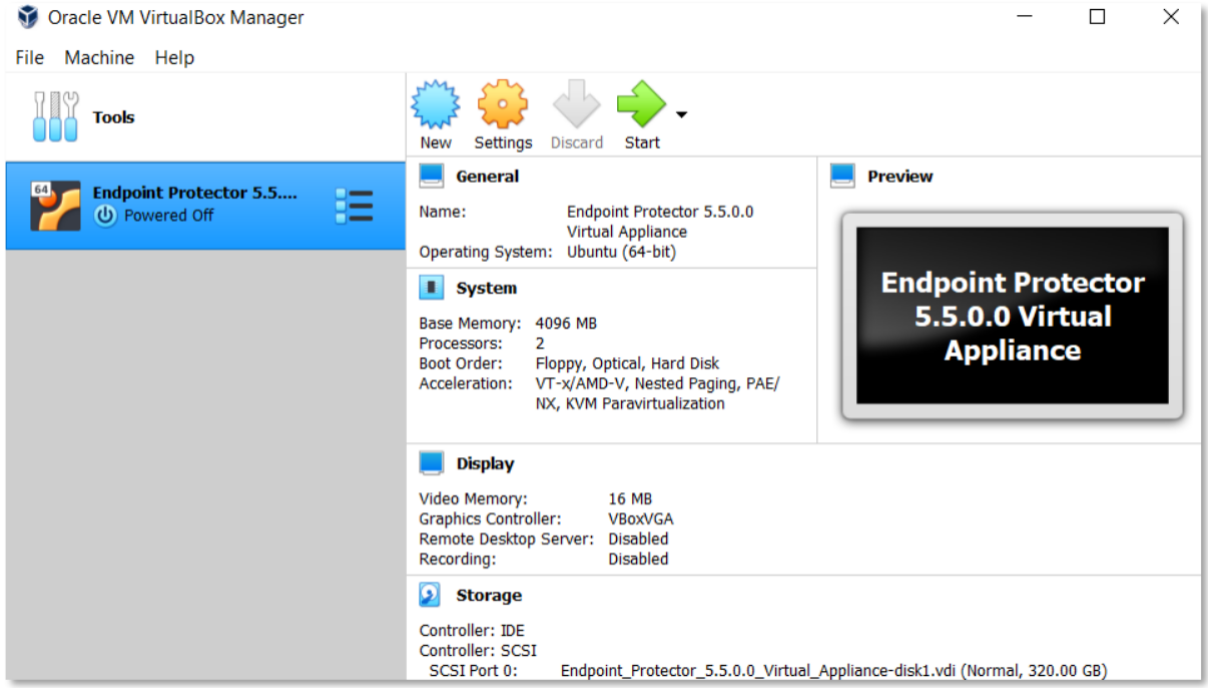


7. 진행 상태가 표시되며 가져오기 기다리기;



이제 가상 머신은 사용 준비가 되었습니다.

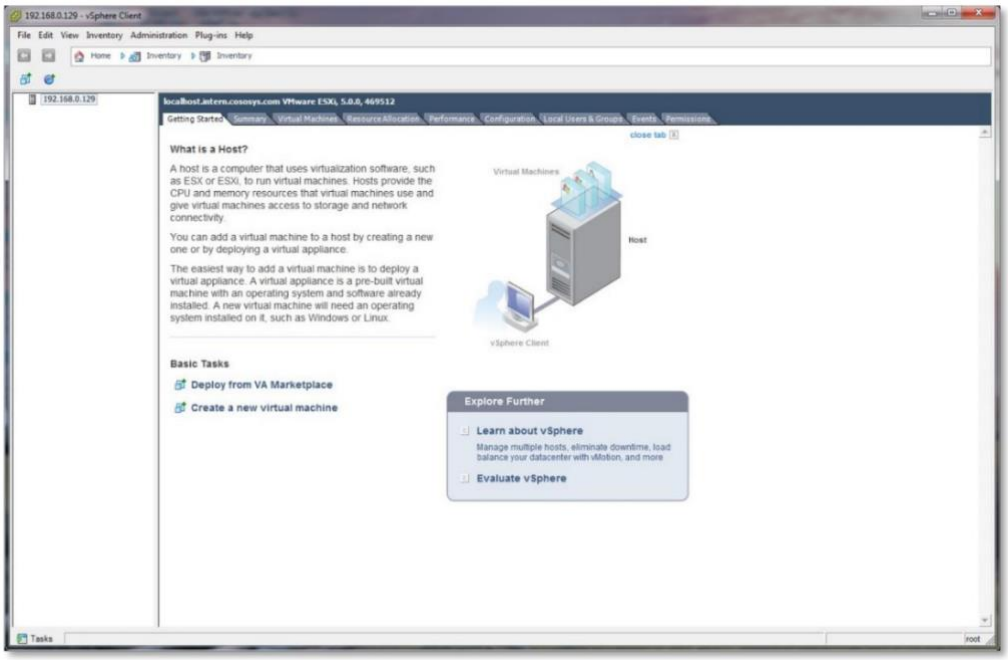
Endpoint Protector 사용자 매뉴얼을 참조하시기 바랍니다.



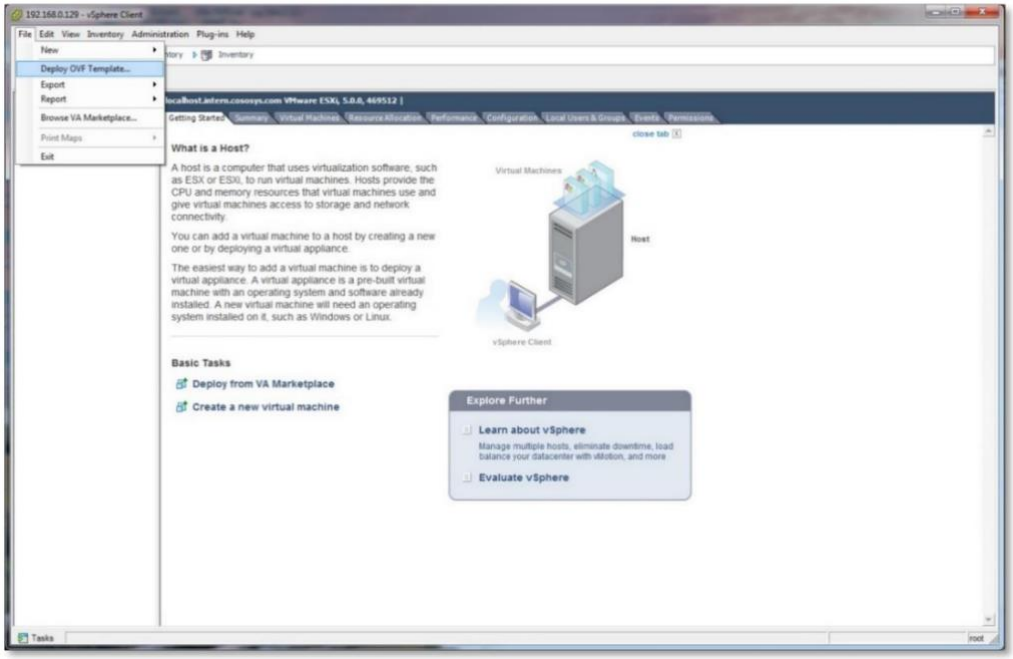
2.2. VMware vSphere

VMware vShpere 구현하려면 아래 단계를 따르시기 바랍니다:

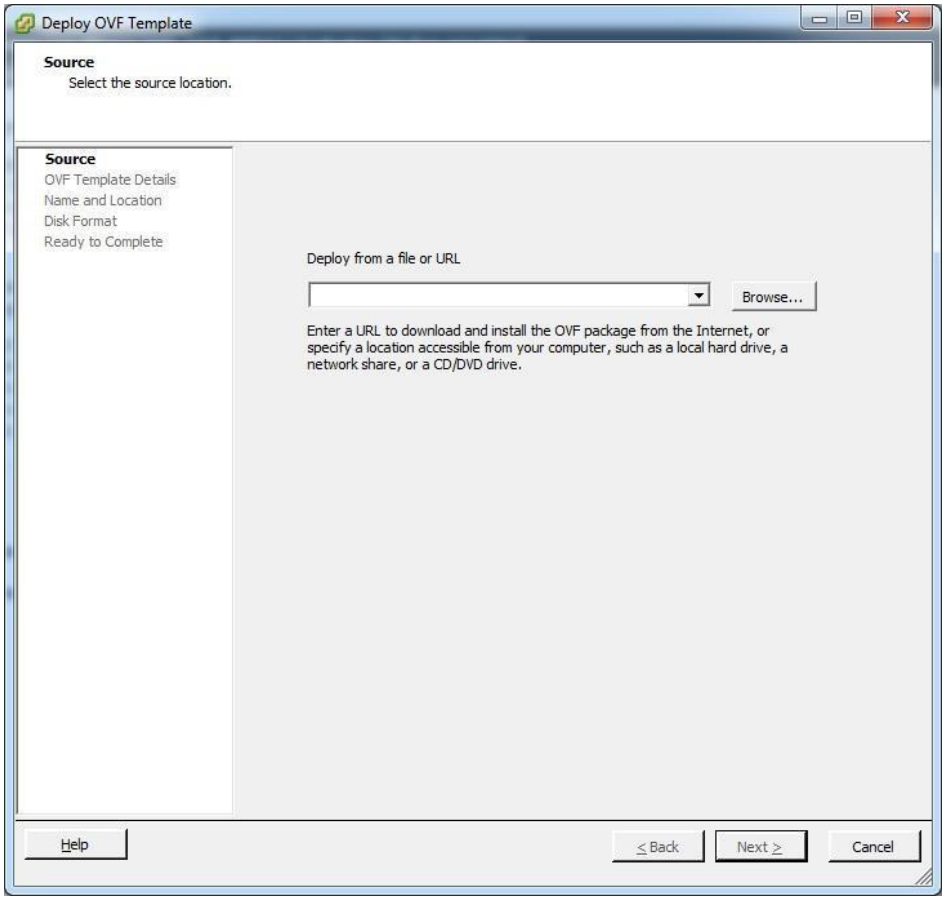
1. 다운로드 패키지 Unzip;
2. **vSphere** 시작;



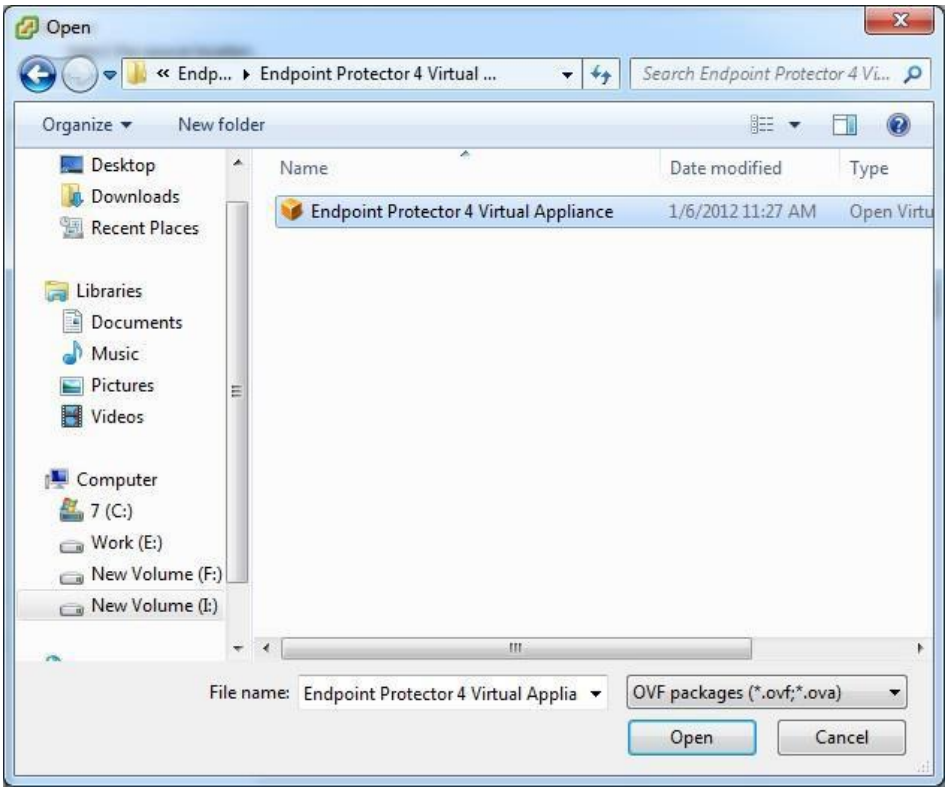
3. **File** 이동 후 **Deploy OVF Template** 선택;



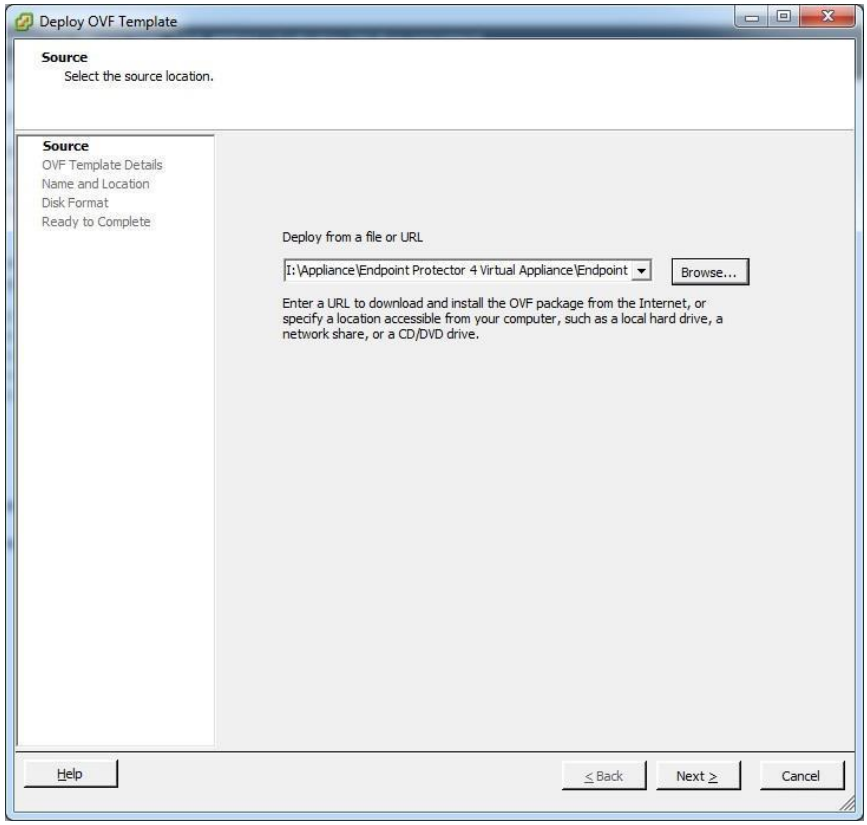
4. **Browse** 클릭;



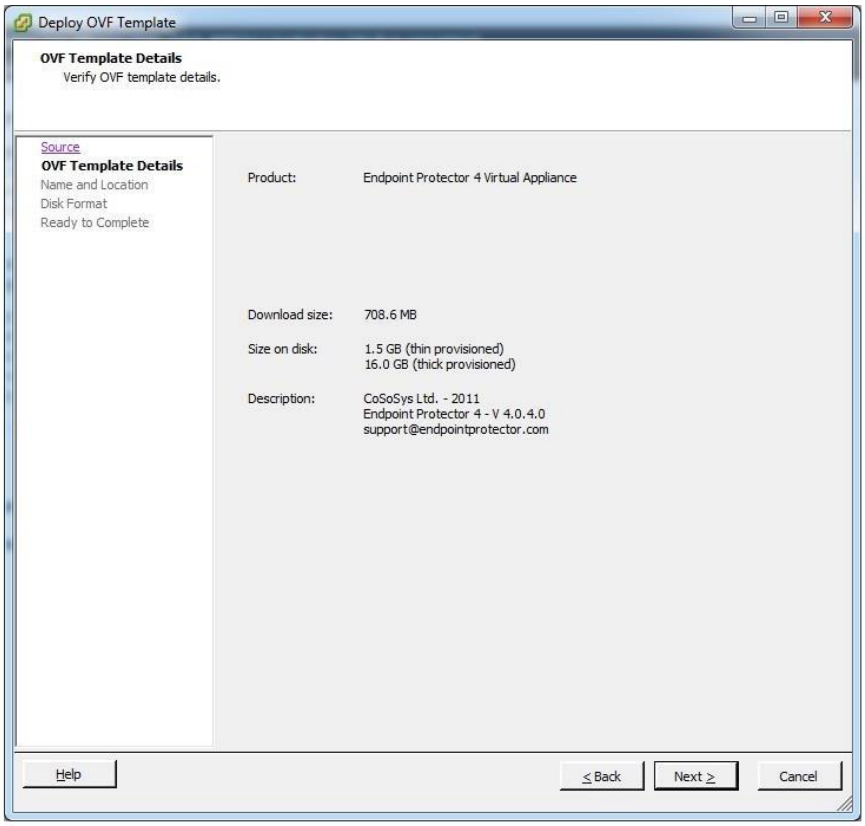
5. 압축이 풀린 파일에서 OVF 파일 선택;



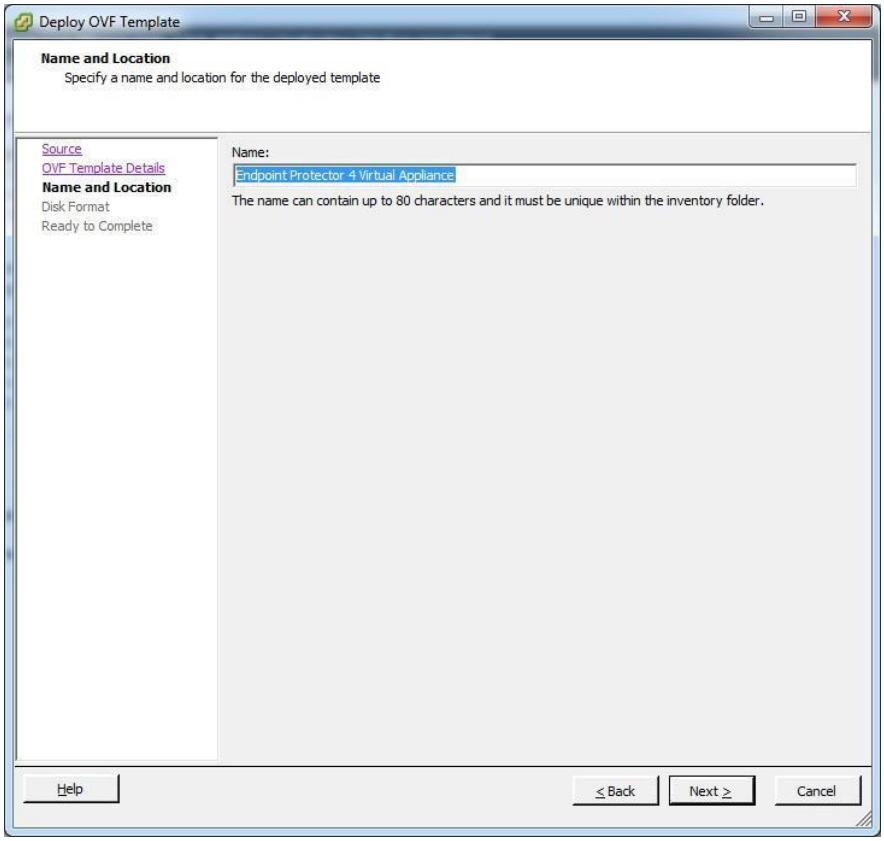
6. **Next** 클릭;



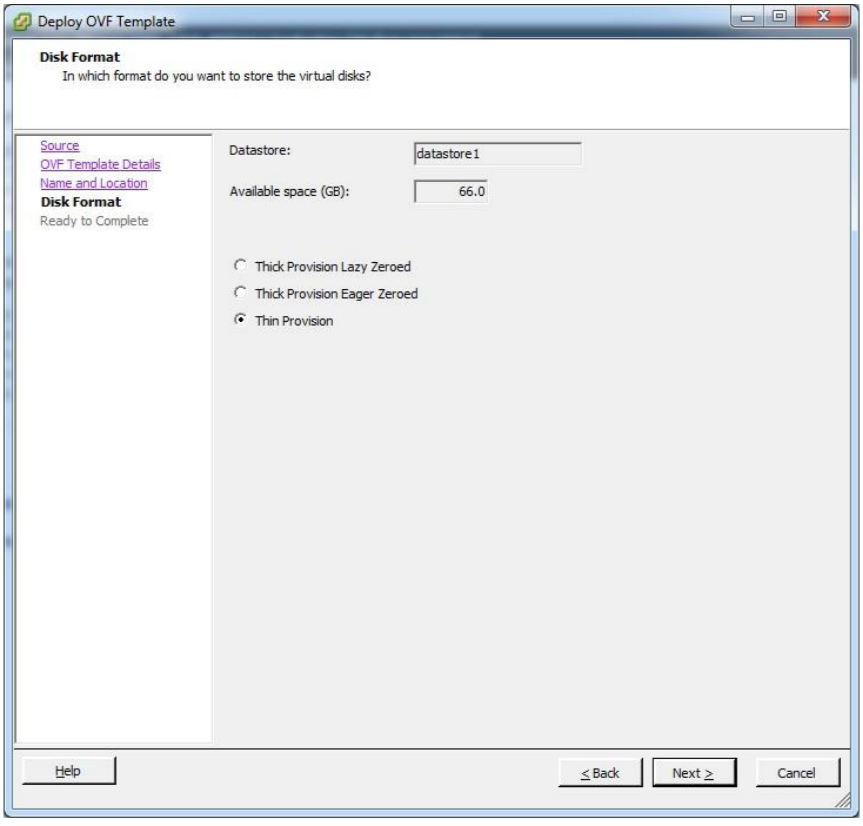
7. 템플릿 상세 정보 확인 후 **Next**;



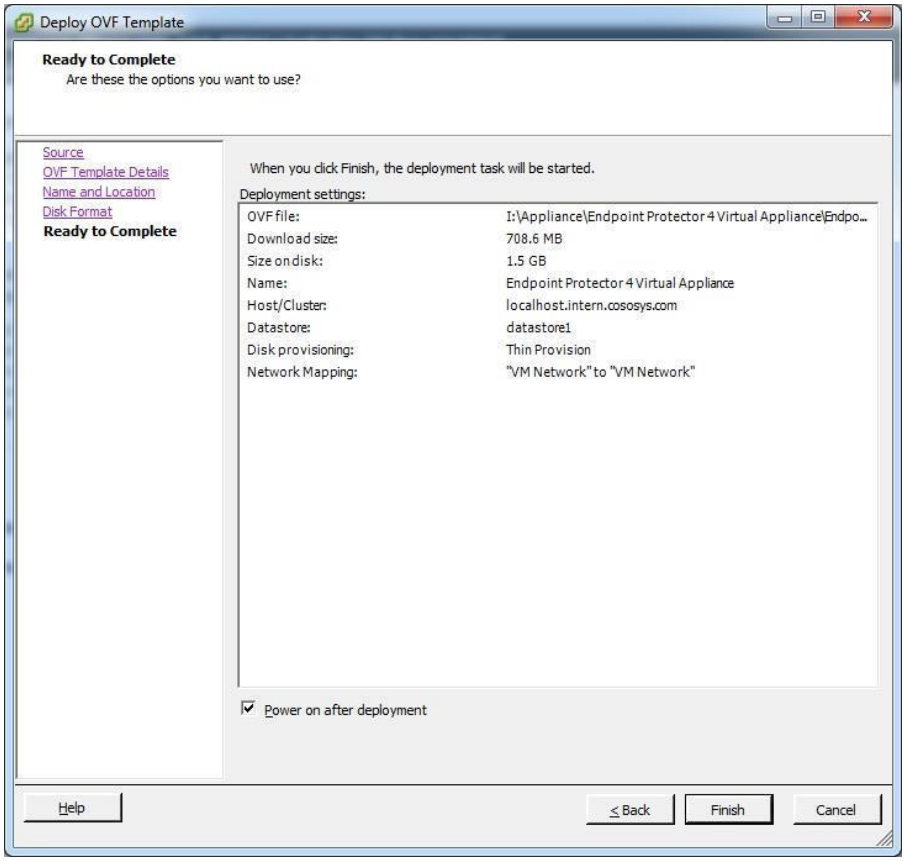
8. OVF 템플릿 이름을 입력 후 **Next** 클릭;



9. **Thin provision** 디스크 포맷 옵션 선택 후 **Next** 클릭;



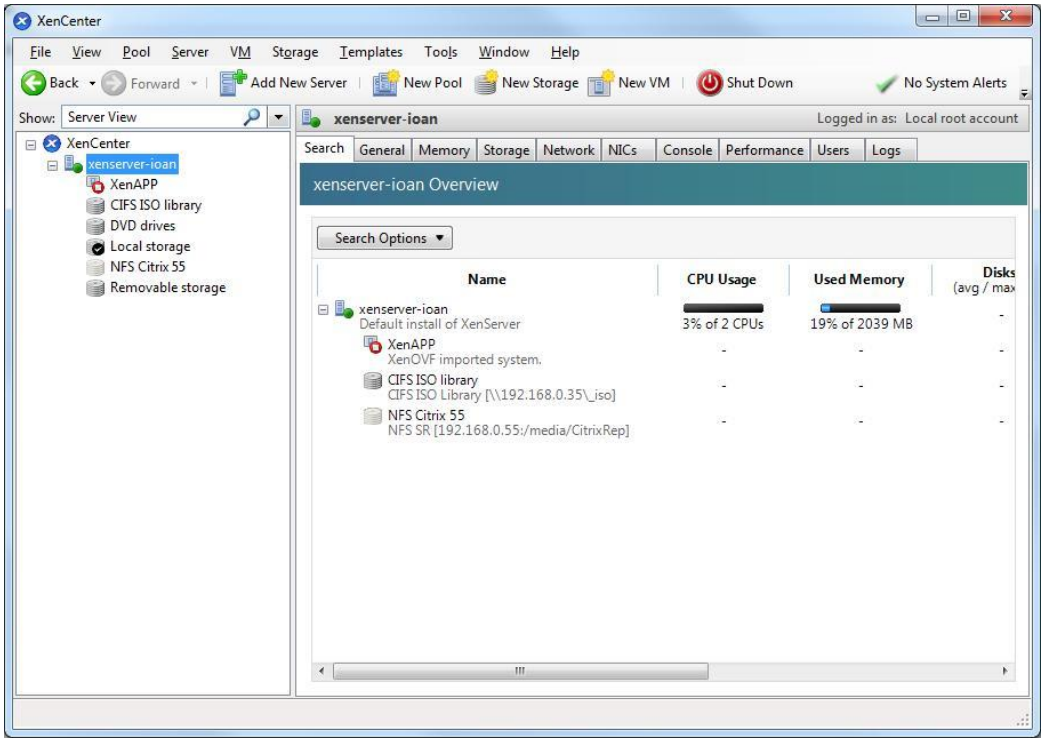
10. 설치 완료를 위해 **Finish** 클릭



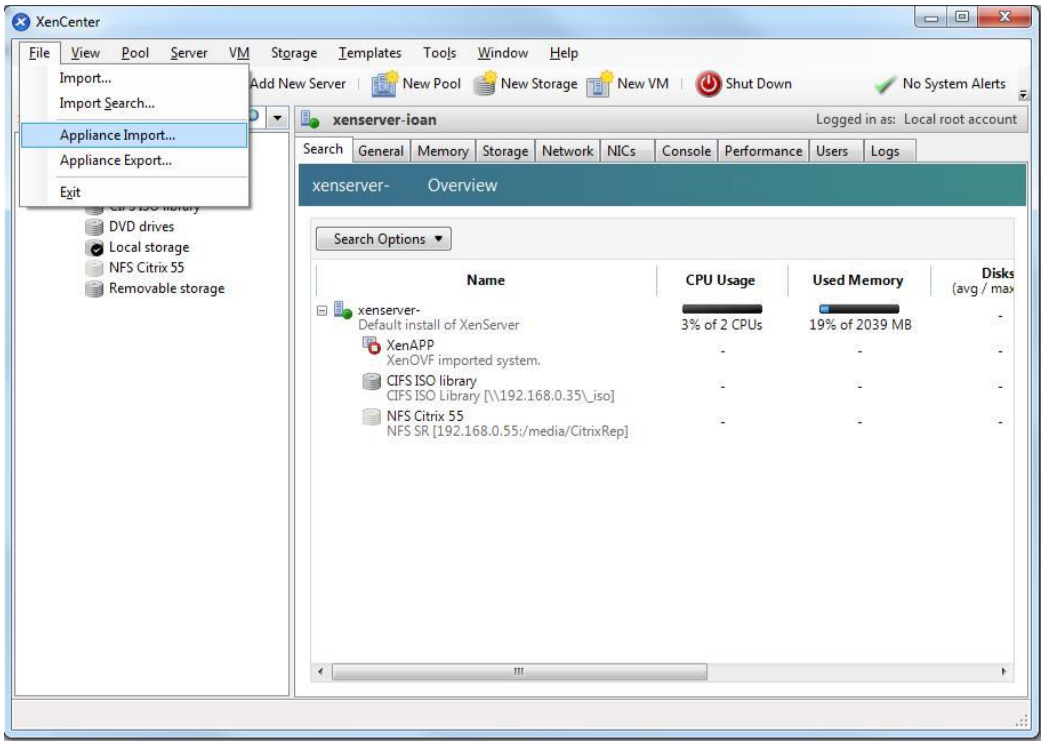
2.3. Citrix XenServer 5.6

1. 다운로드 패키지 압출 풀기;

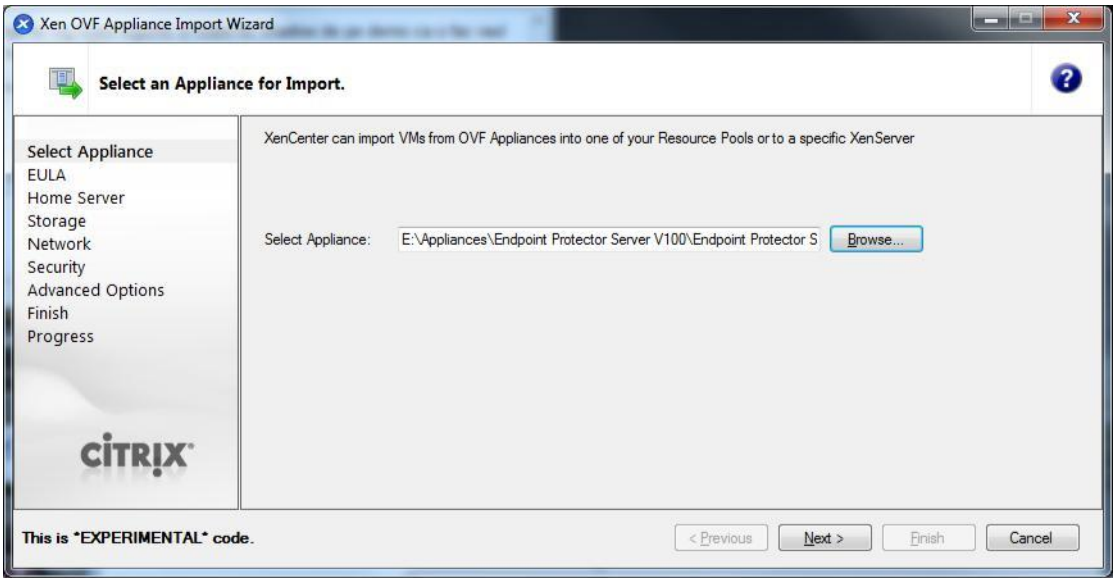
2. **XenCenter** 시작;



3. **File** 이동 후 **Appliance Import** 선택;

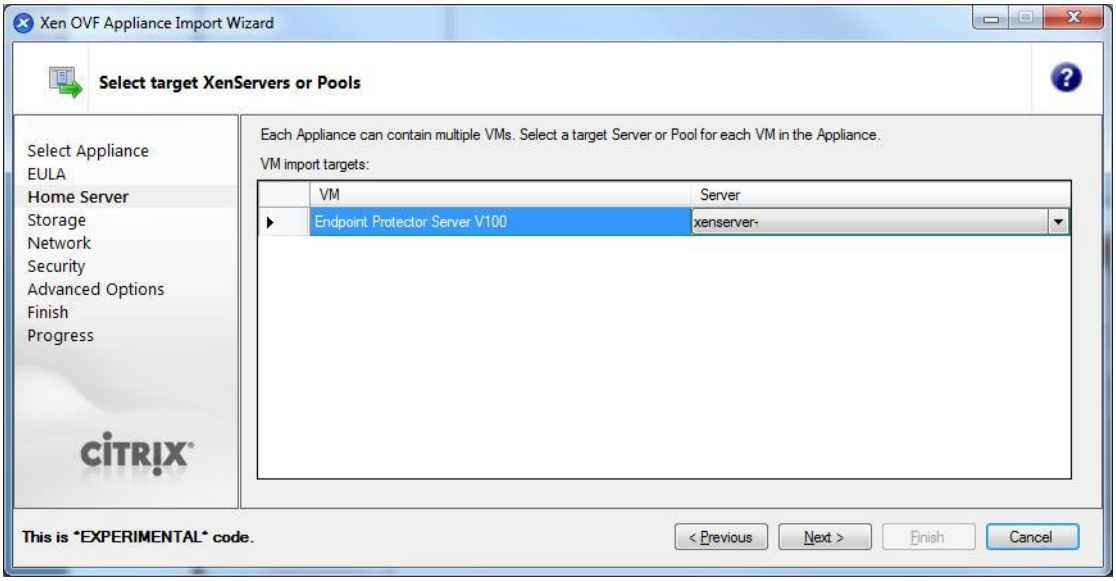


4. OVF 파일 선택 후 **Next** 클릭;

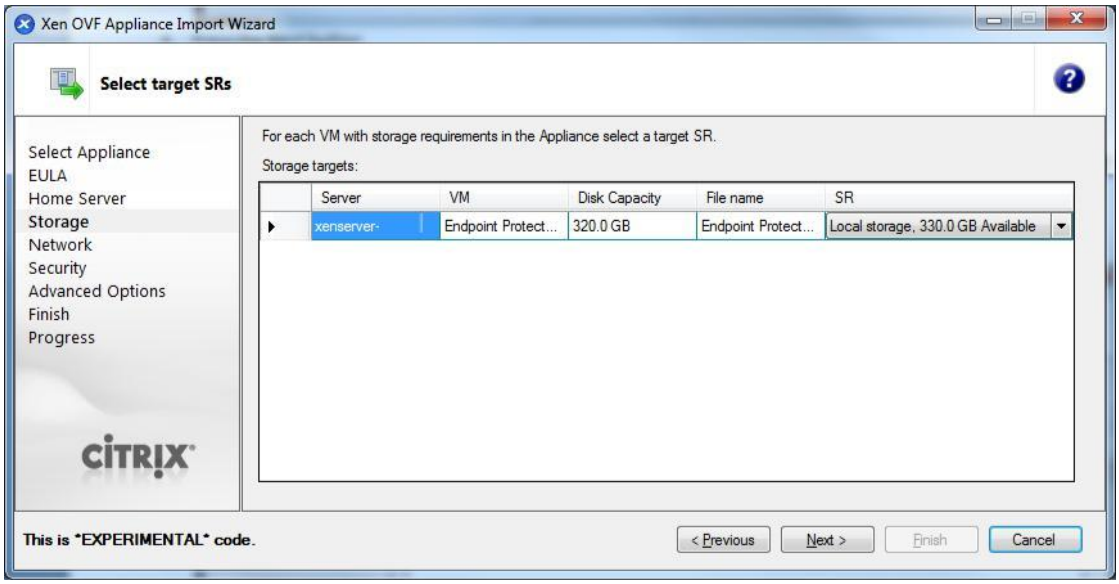


5. EULA 읽고 동의 후 **Next** 클릭;

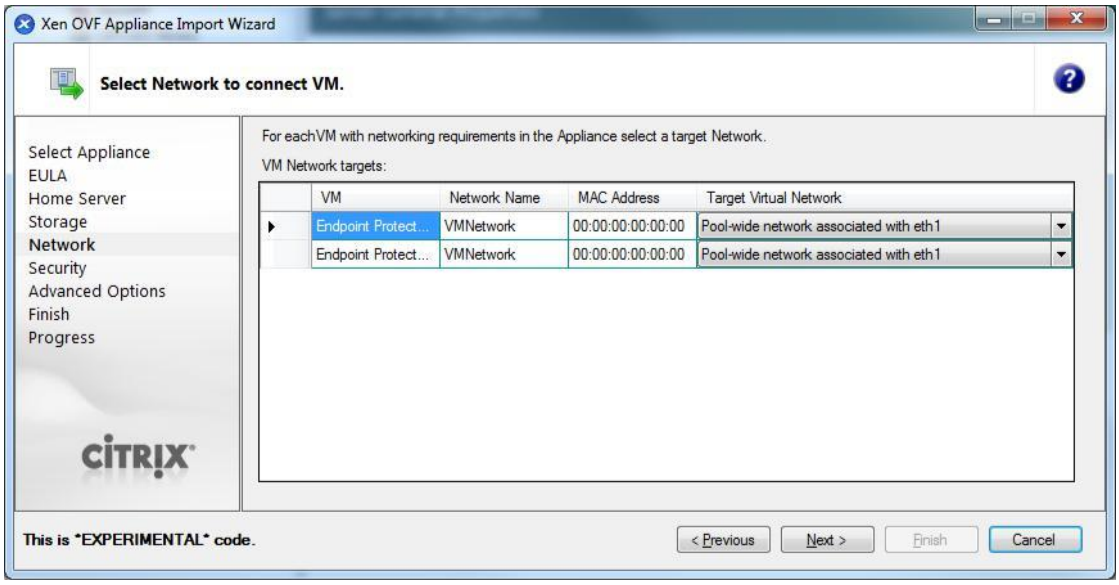
6. 가상 어플라이언스 선택;



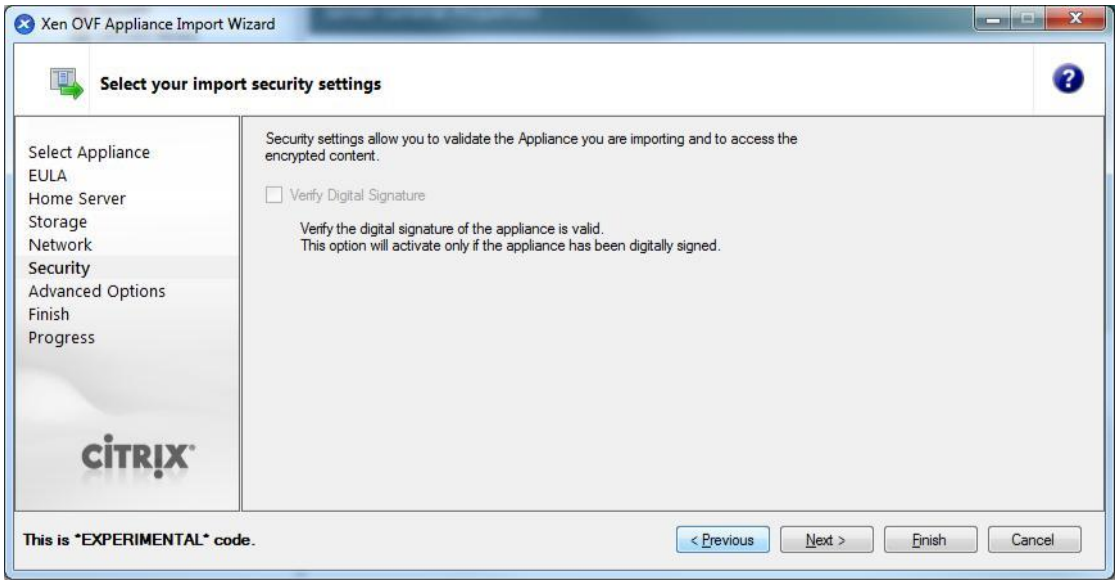
7. 스토리지 위치 선택;



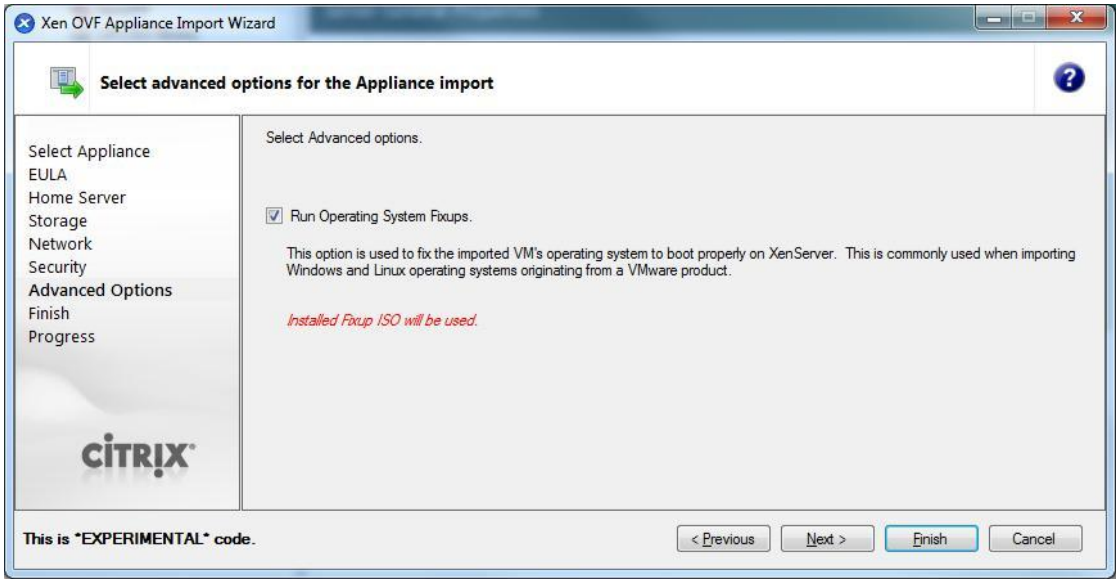
8. 네트워크 선택 (기본 값 유지);



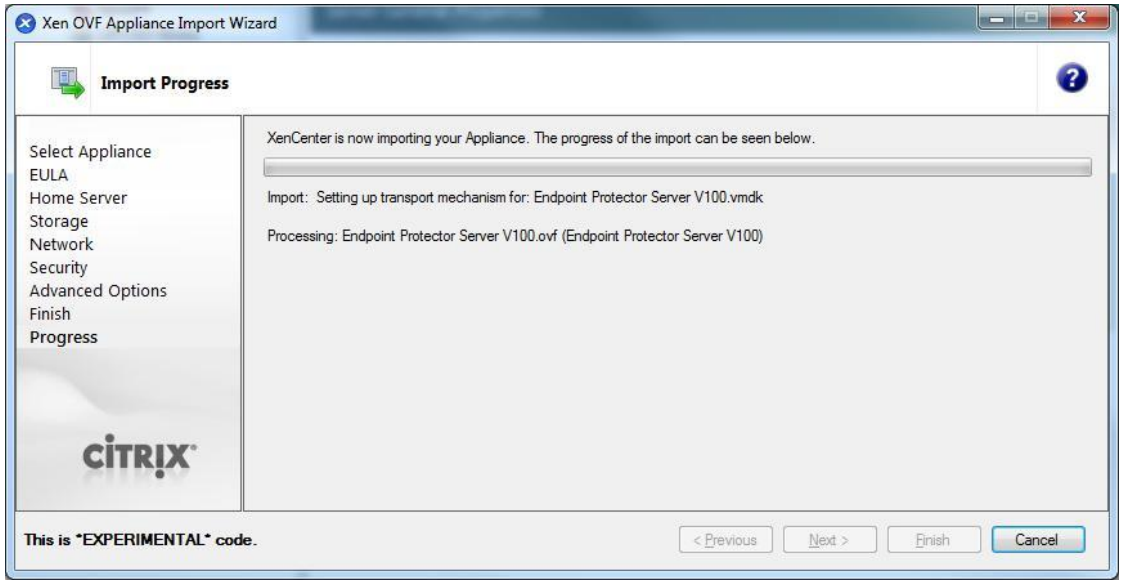
9. 보안 화면에서 **Next** 클릭;



10. 고급 옵션 화면에서 **Next** 클릭;



11. **Finish** 스크린에서 구성을 리뷰하고 **Finish** 클릭 그리고 가져오기 완료를 기다림.



이 지점에서 가상 머신은 시작 준비가 됩니다.

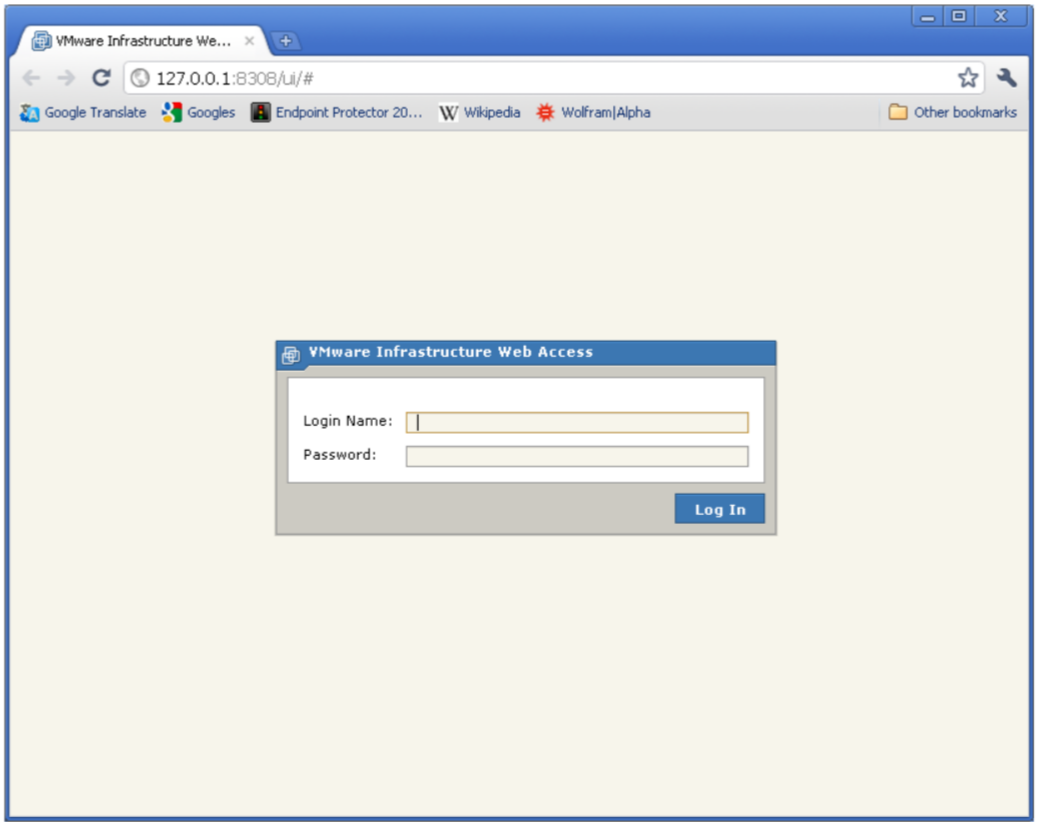
Endpoint Protector 사용자 매뉴얼을 참조하시기 바랍니다.

3. VMX 포맷 사용하여 구현하기

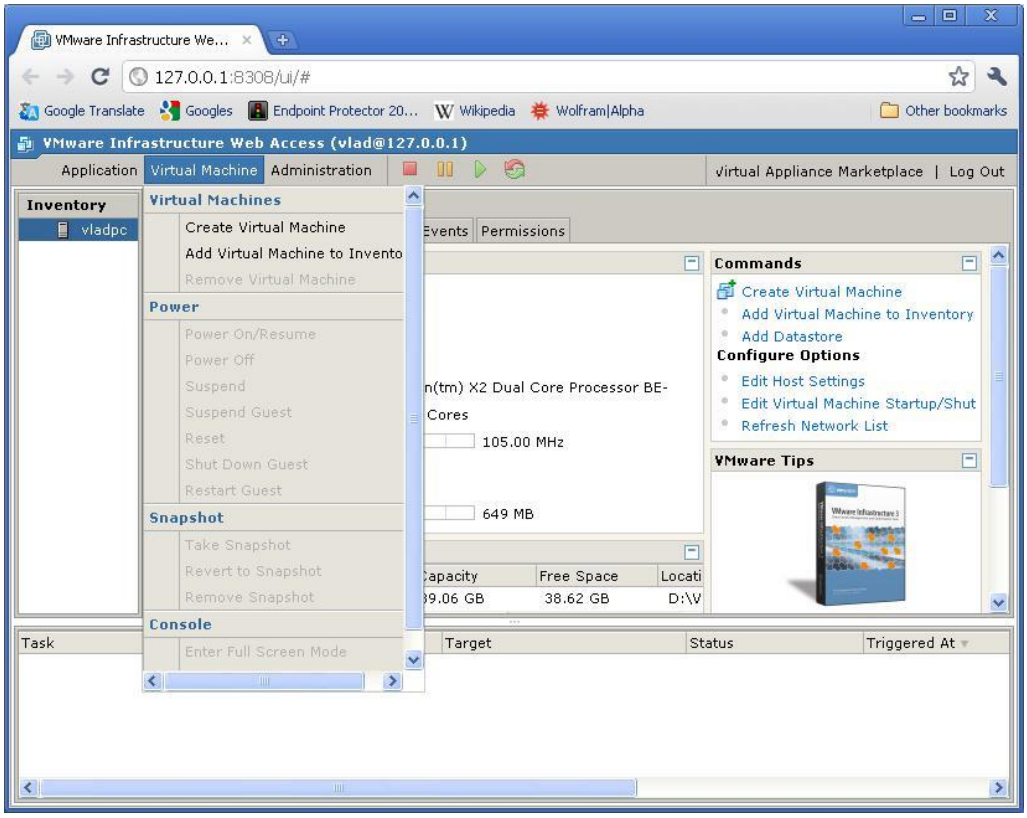
VMX 포맷을 사용하여 Endpoint Protector 가상 어플라이언스를 구현하는 여러 옵션이 있습니다.

3.1. VMware 서버 사용하여 구현하기

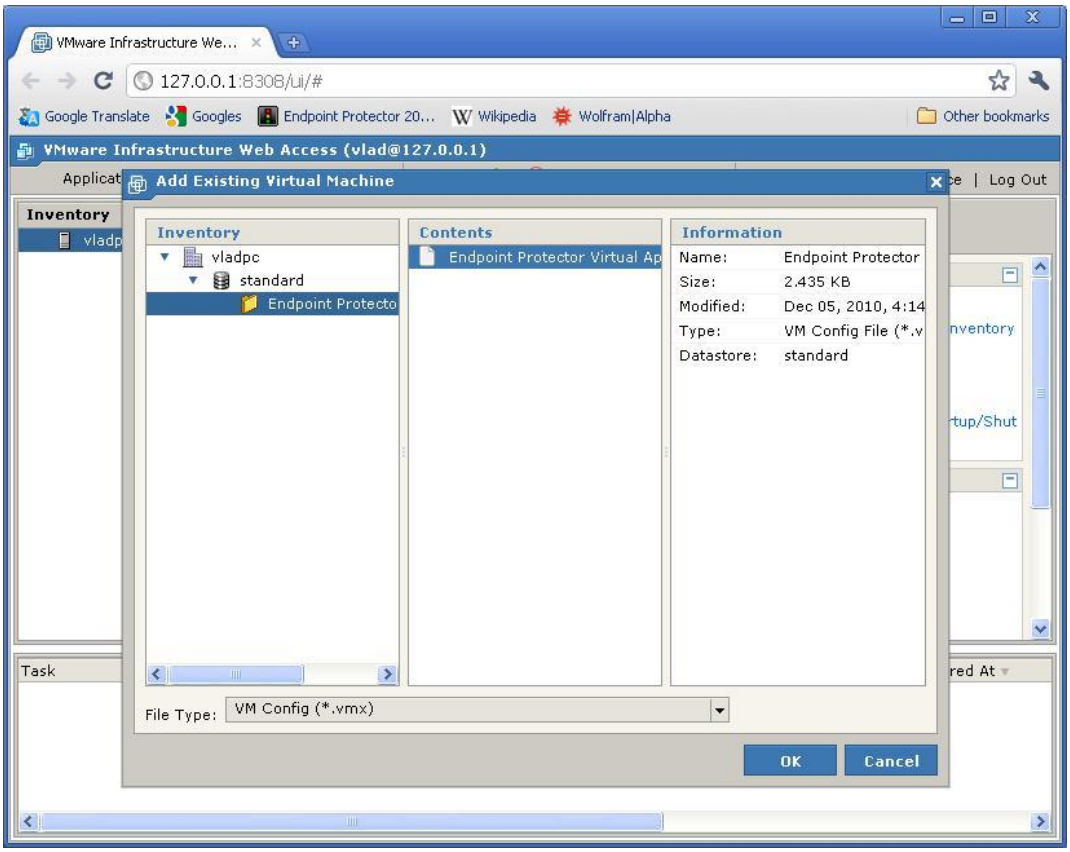
1. 다운로드한 Endpoint Protector 가상 어플라이어스 패키지 압축 해제 후 가장 머신을 저장하는 경로에 파일을 이동;
2. VMware 서버 웹 인터페이스 열고 로그인;



3. **Add Virtual Machine to inventory** 선택;



4. 인벤토리에서 Endpoint Protector 가상 어플라이언스 찾은 후 VMX 파일 선택하고 **OK** 클릭;



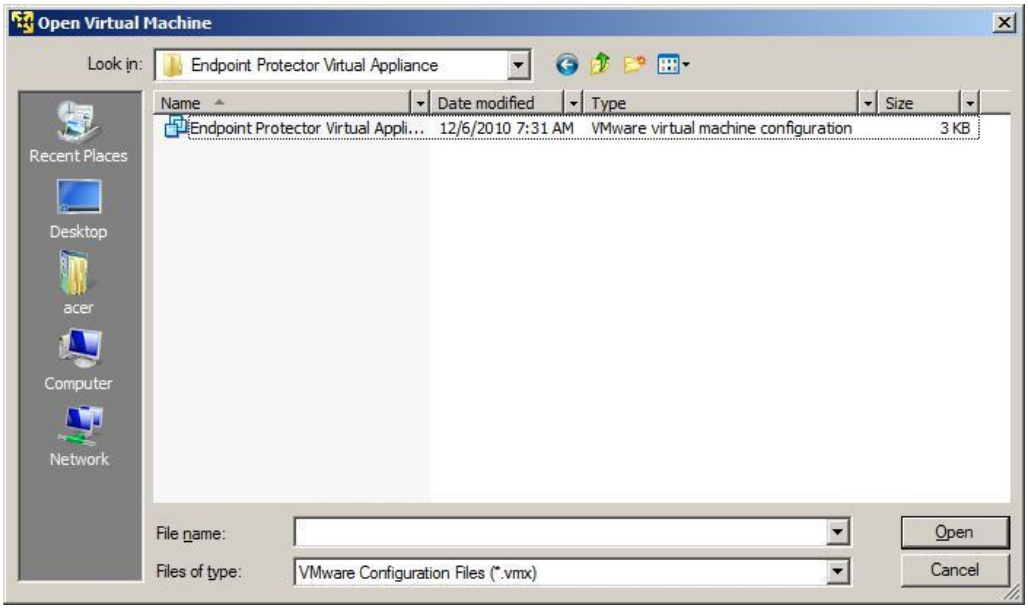
이 지점에서 가상 머신은 시작 준비가 됩니다.

Endpoint Protector 사용자 매뉴얼을 참조하시기 바랍니다.

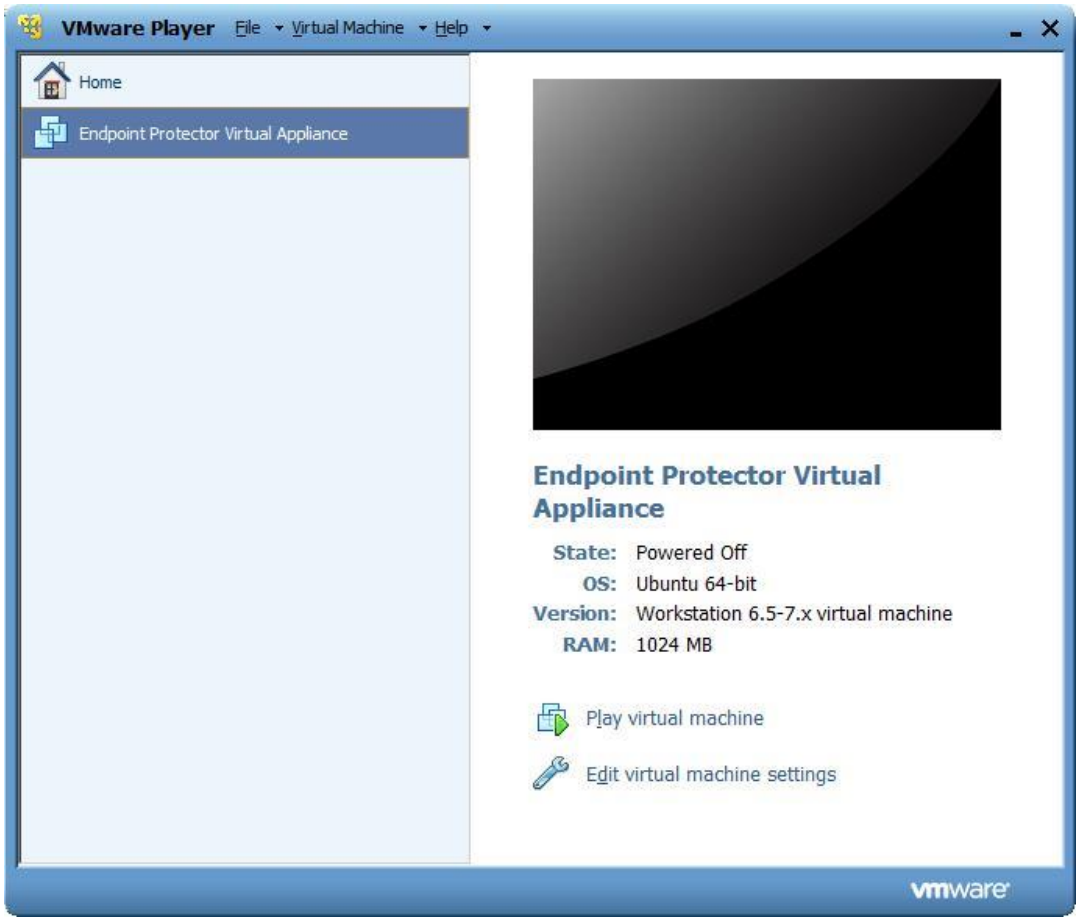
3.2. VMware Player 사용하여 구현

1. 다운로드한 Endpoint Protector 가상 어플라이언스 압축을 풀고 가상 머신이 저장된 경로에 파일을 이동;
2. VMware Player 열기;

3. **Open a Virtual Machine** 선택 후 압축 해제 한 위치의 VMX 파일 선택 그리고 **Open** 클릭;



4. 가상 머신이 인벤토리에 있으면 **Play Virtual Machine** 클릭;



5. 가상 머신이 복사되었거나 이동되었는지 물어보면 이동됨을 선택 (네트워크에 Endpoint Protector 만 있는 경우);

이 지점에서 가상 머신은 시작 준비가 됩니다.

Endpoint Protector 사용자 매뉴얼을 참조하시기 바랍니다.

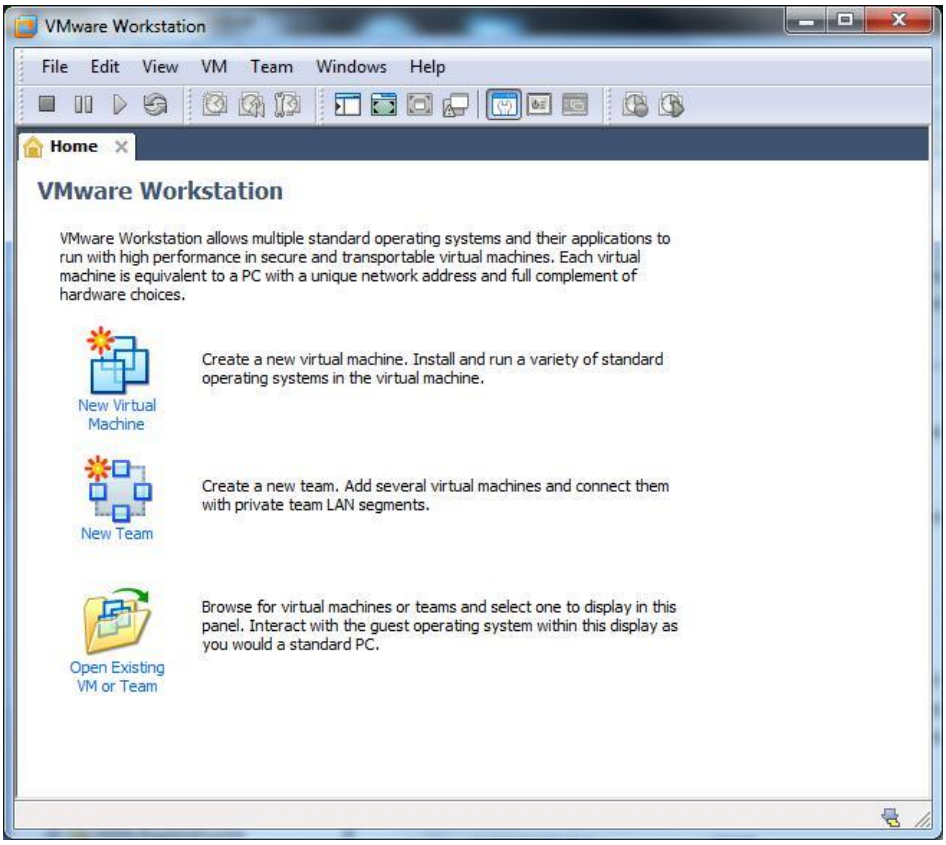
중요: Endpoint Protector 가상 어플라이언스가 구동 중일 때 VMware Player 를 중지하지 마십시오!

또한 VMware Player 가 구동 중일 때 컴퓨터 전원을 끄지 마십시오.

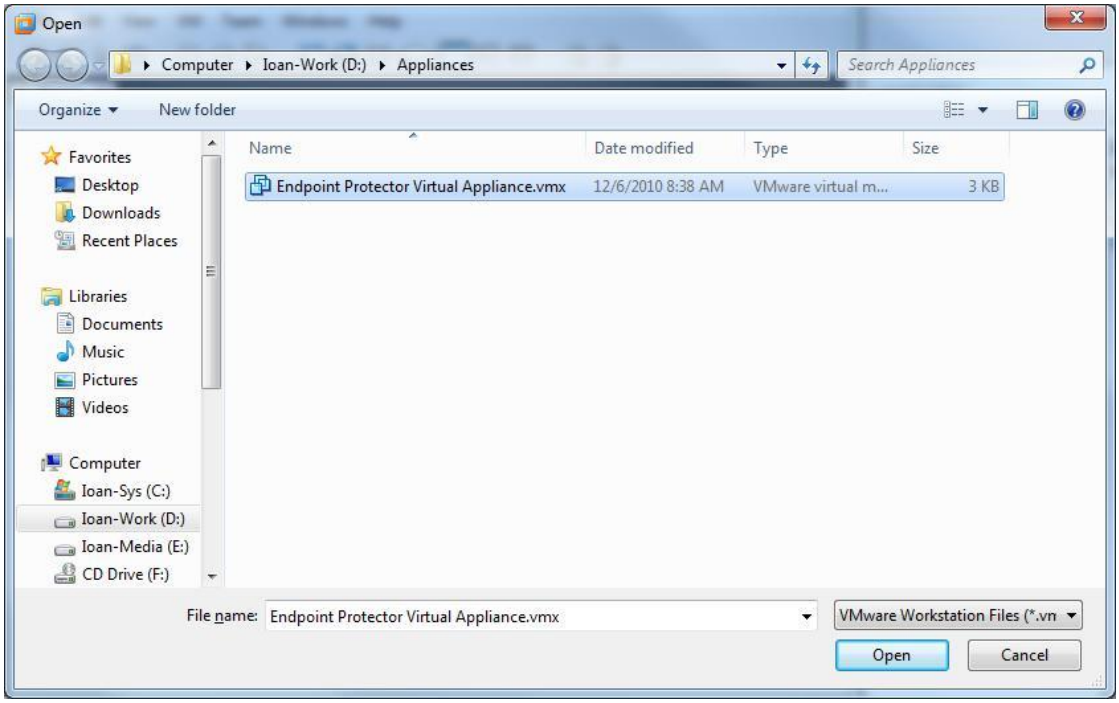
3.3. VMware Workstation 을 사용하여 구현하기

1. 다운로드한 Endpoint Protector 가상 어플라이언스의 압축을 풀고 가상 머신이 저장된 경로에 파일 이동;

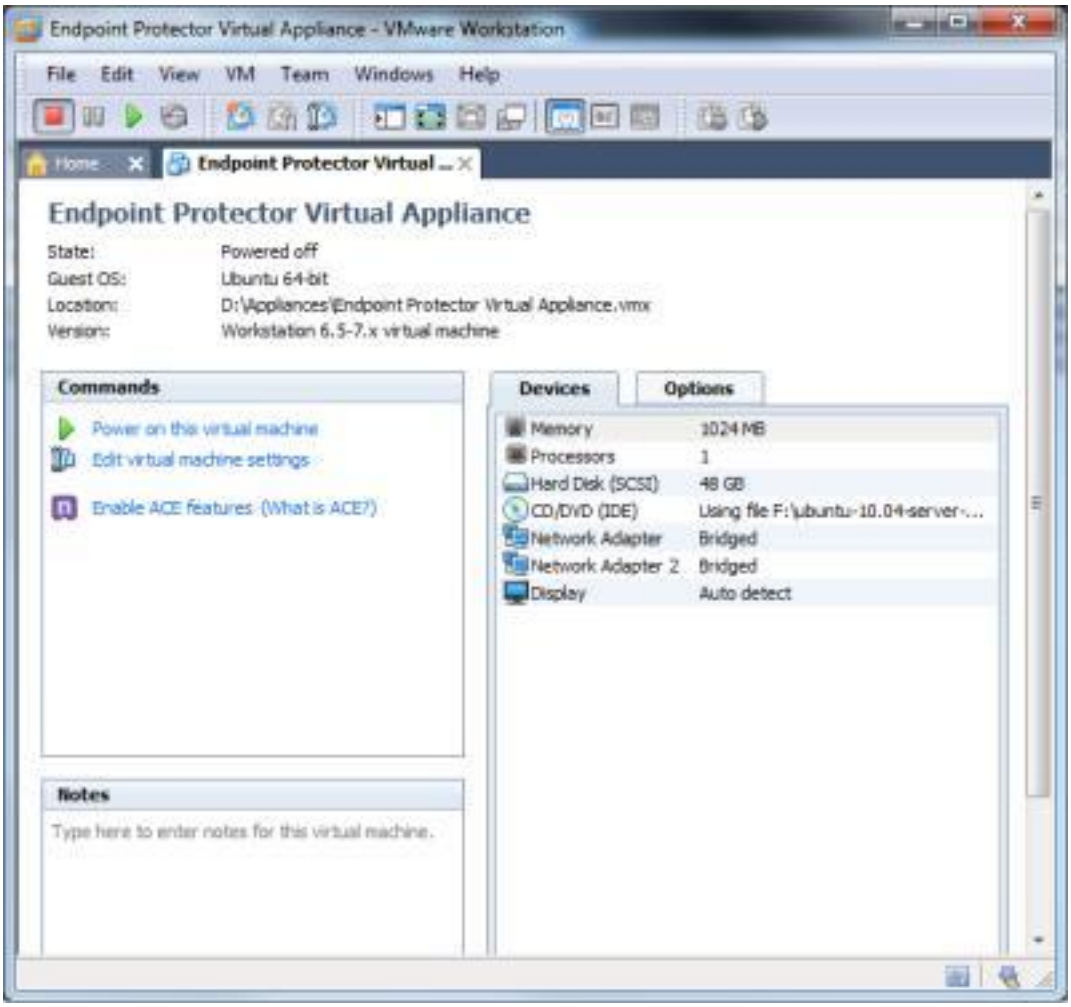
2. VMWare Workstation 열기;



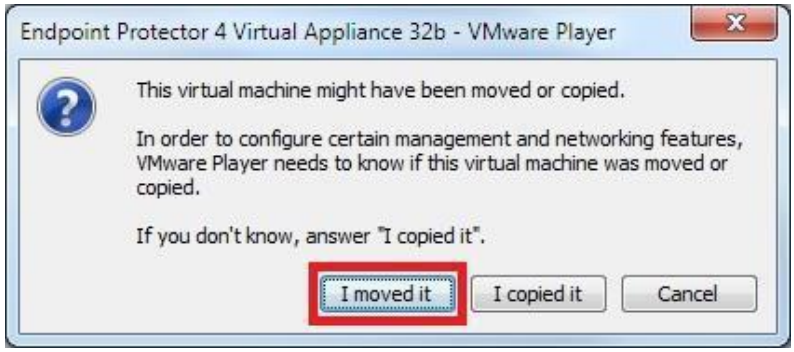
3. 존재하는 VM 또는 Team 선택하여 열기;



4. 가상 어플라이언스가 인벤토리에 있으면 가상 어플라이언스 전원 켜기;



5. 가상 머신이 복사되었거나 이동되었는지 물어보면 이동됨을 선택 (네트워크에 Endpoint Protector 만 있는 경우);



이 지점에서 가상 머신은 시작 준비가 됩니다.

Endpoint Protector 사용자 매뉴얼을 참조하시기 바랍니다.

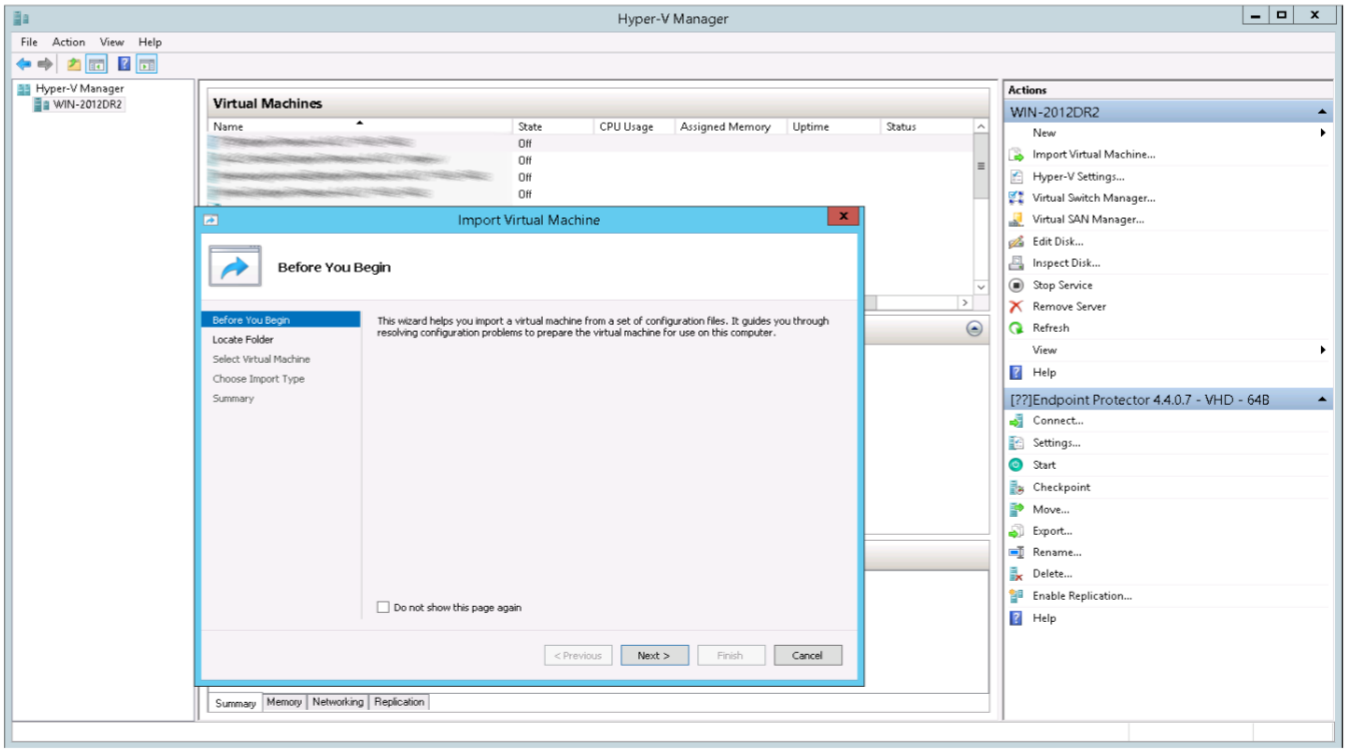
4. VHD 포맷 사용하기

VHD 포맷을 사용하여 Endpoint Protector 가상 어플라이언스를 구현하는 여러 옵션이 있습니다.

이 방법을 아래에서 설명하겠습니다.

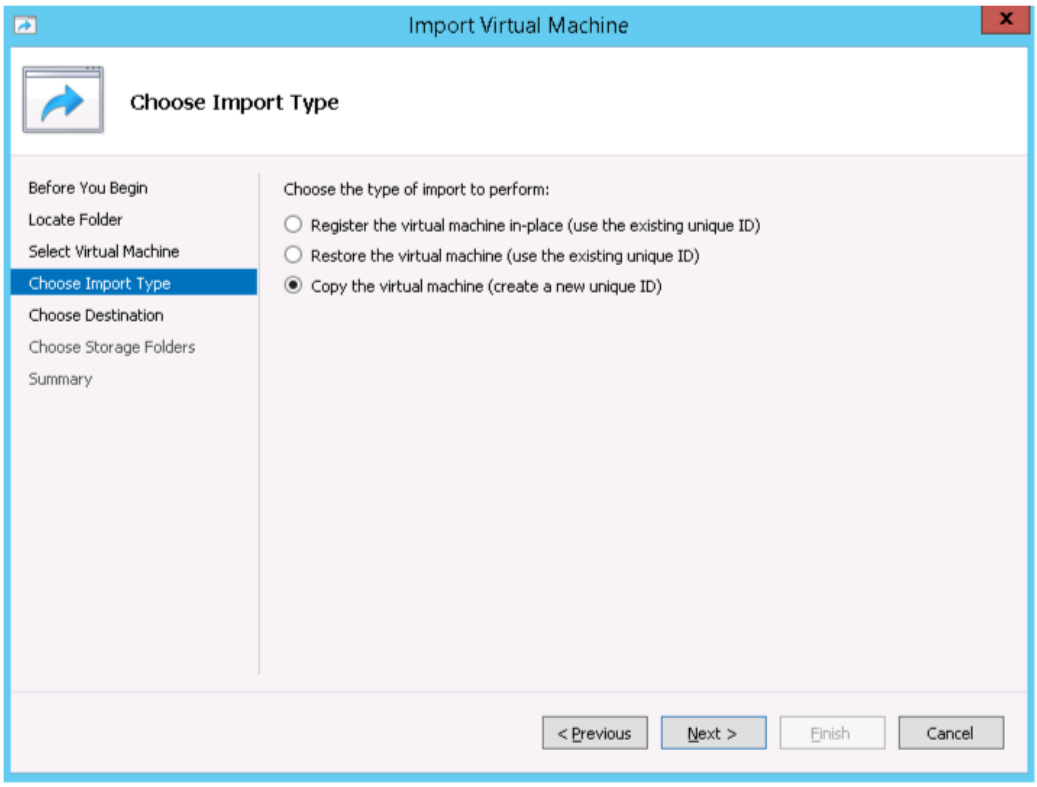
4.1. Microsoft Hyper-V 2012 사용하여 구현하기

1. 다운로드한 Endpoint Protector 가상 어플라이언스 .zip 패키지 압축 풀기;
2. Hyper-V Manager 시작;
3. 가상 머신을 가져오기 위해서 우측 박스 선택;

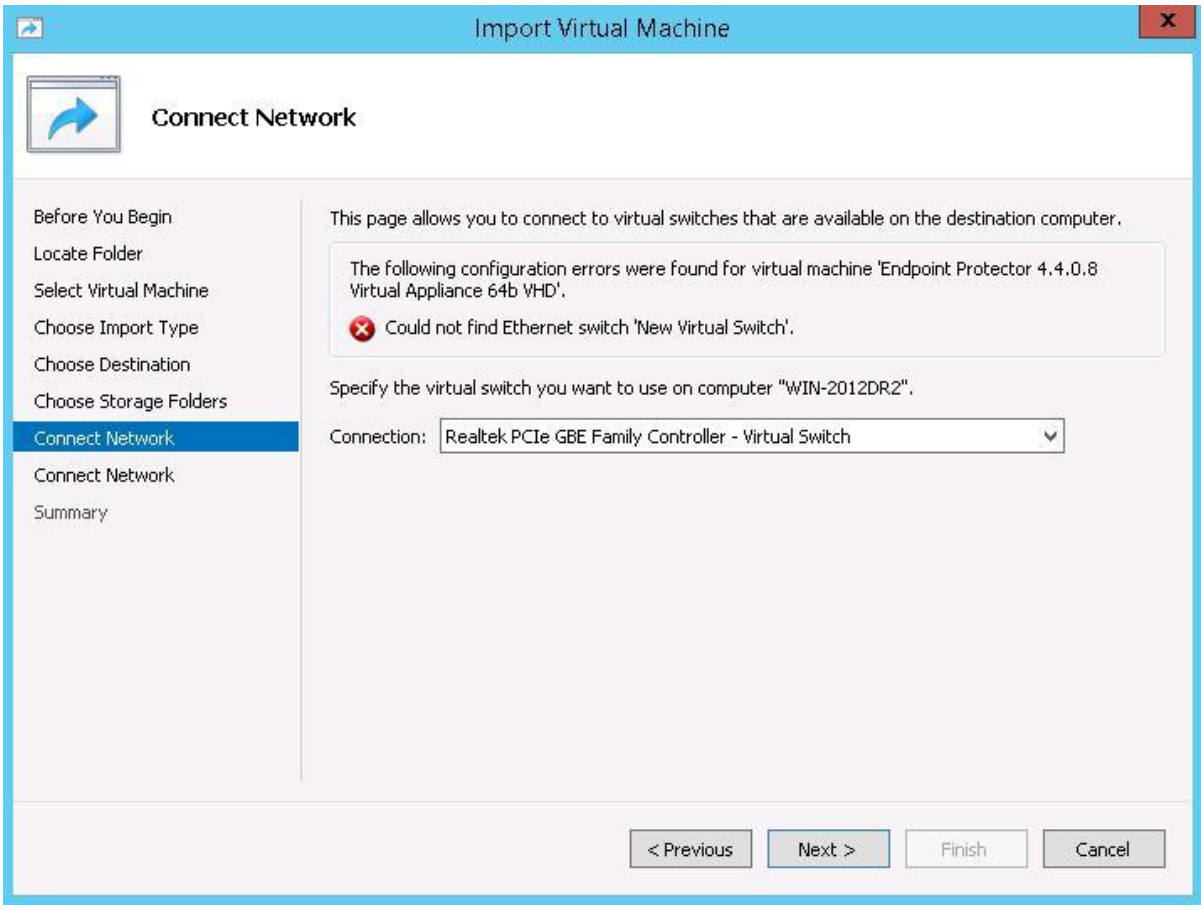


3.1 어플라이언스의 폴더와 파일이 포함된 폴더 선택;

3.2 **Choose Import Type** 섹션에서 **Copy the virtual machine (create a new unique ID)** 옵션 선택;



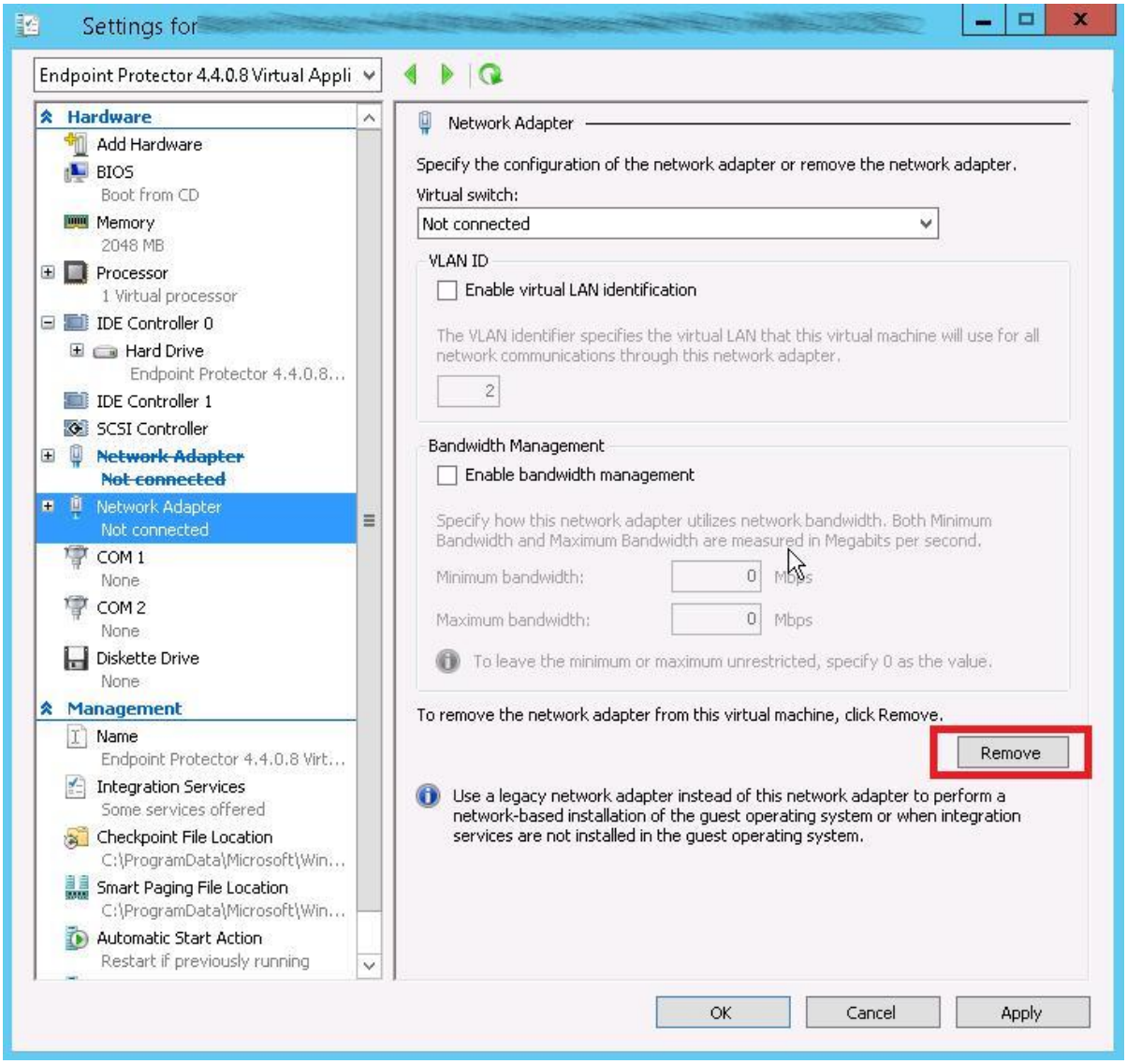
3.3. 네트워크 어댑터의 연결된 네트워크 에러를 무시하기 위해서 **Next**, **Next,** 클릭 후 **Finish**;



4. 가상 머신 목록에 새로운 가상 머신이 나타남;

5. 새로운 가상 머신 오른쪽 클릭 후 **Settings** 선택;

6. 좌측 박스에서 두 개의 존재하는 네트워크 어댑터 제거;



8. **Apply** 클릭 – 가장 머신을 지금 가져오고 구성이 준비됨.

Endpoint Protector 사용자 매뉴얼을 참조하시기 바랍니다.

5. 가상 어플라이언스 설정 마법사

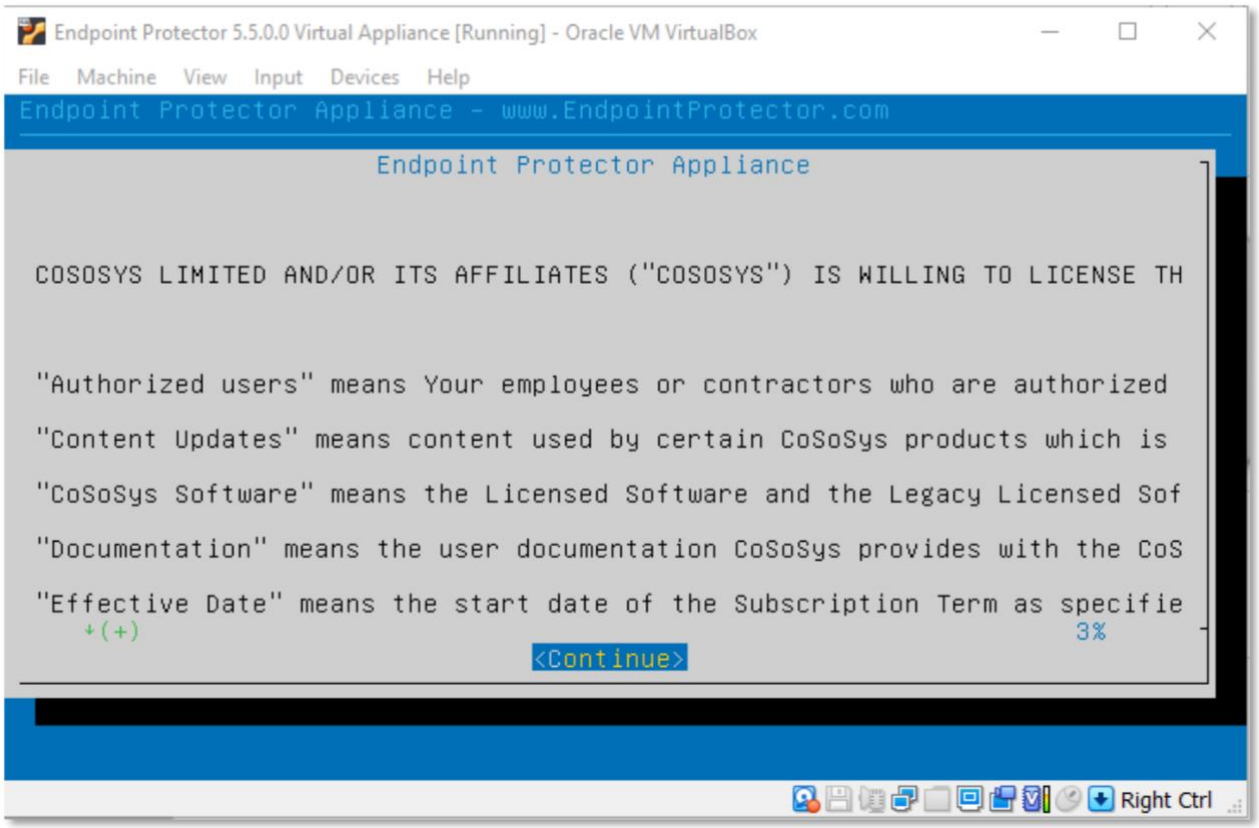
Endpoint Protector 어플라이언스 (가상 또는 하드웨어)는 방화벽 화이트리스트로 443 과 80 포트 인바운드 트래픽이 요구됩니다. 아래를 참조 하시기 바랍니다:

Endpoint Protector 서버 및 클라이언트 통신: 443

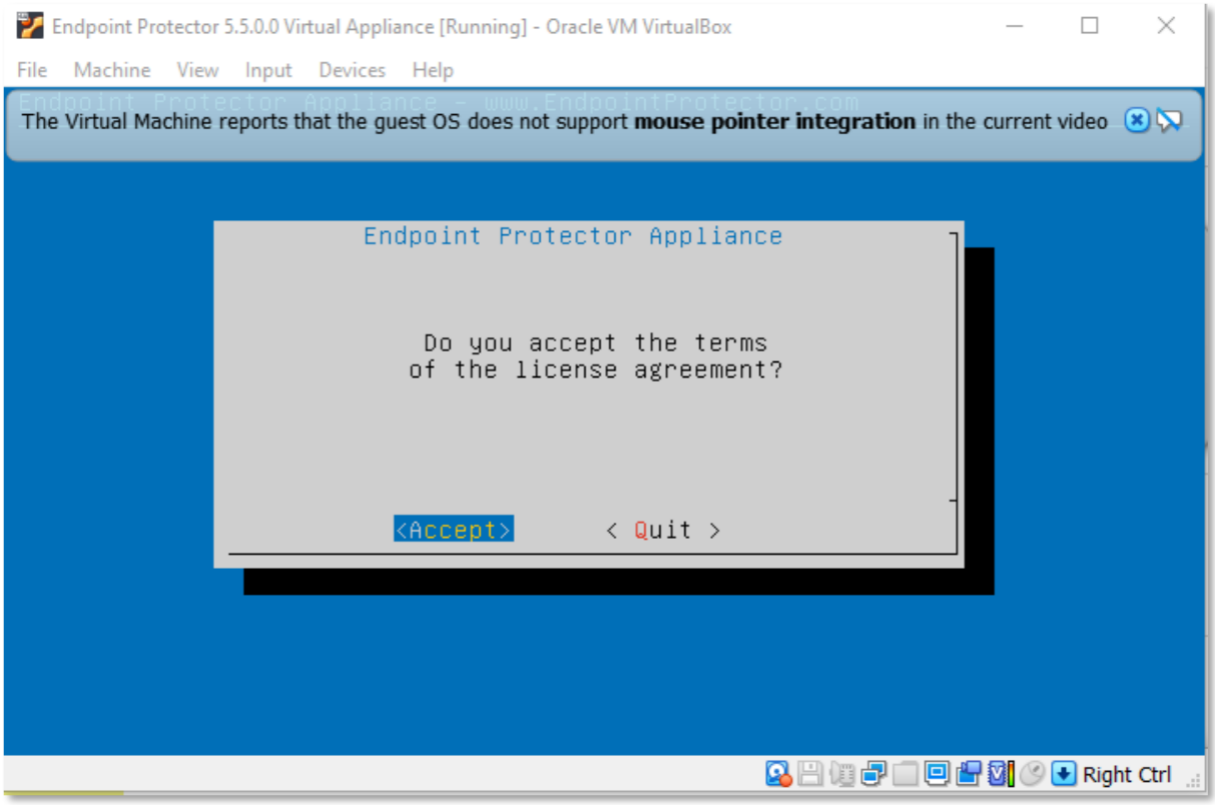
- Mobile Device Management 클라우드 (cloud.endpointprotector.com): 443
- Live Update (liveupdate.endpointprotector.com): 80 & 443

Endpoint Protector 어플라이언스를 처음 구성할 때 아래 단계를 따르시기 바랍니다:

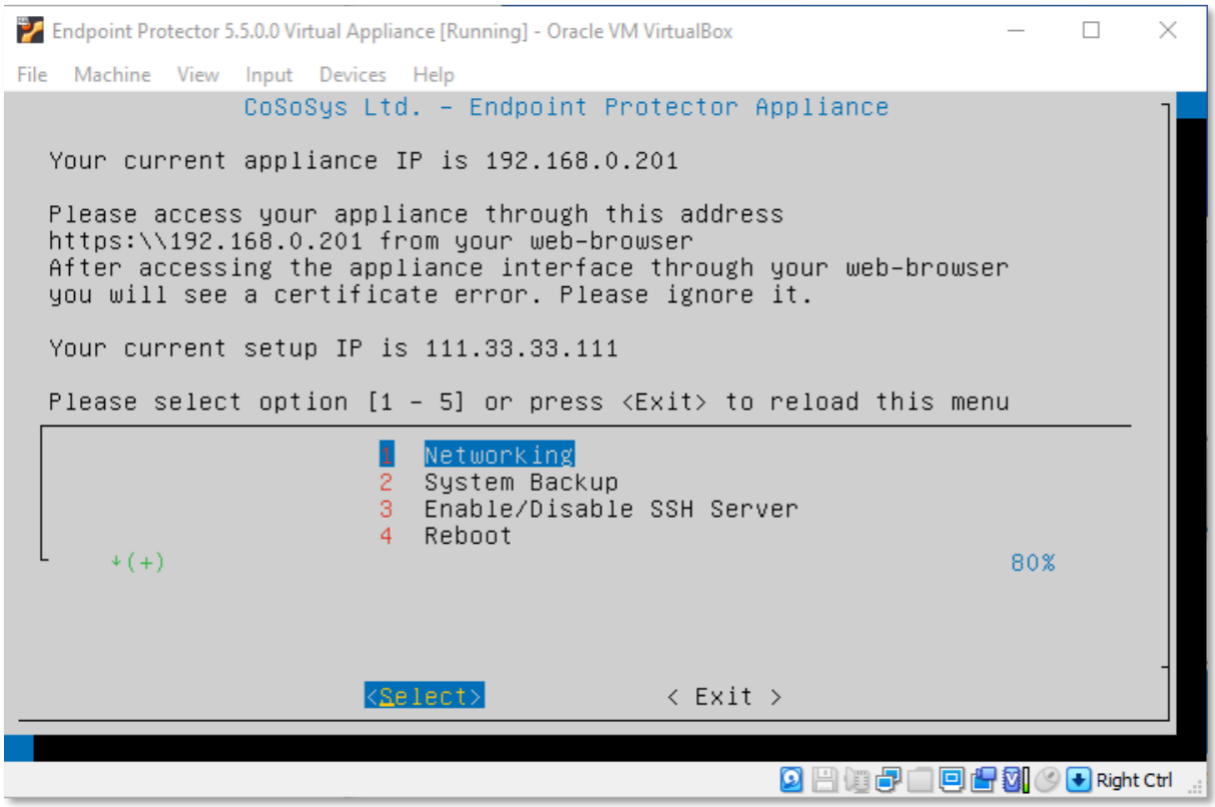
1. End User License Agreement 를 읽고 **Continue** 선택;



2. **Accept** 선택;

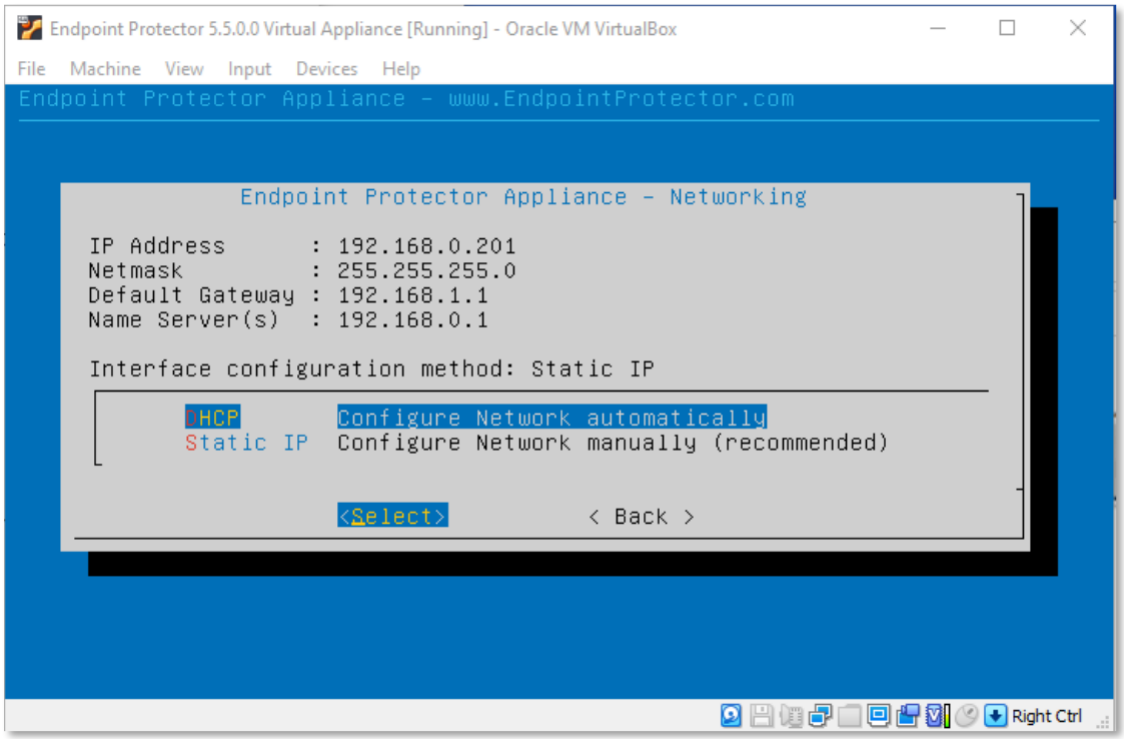


3. **Networking** 선택;



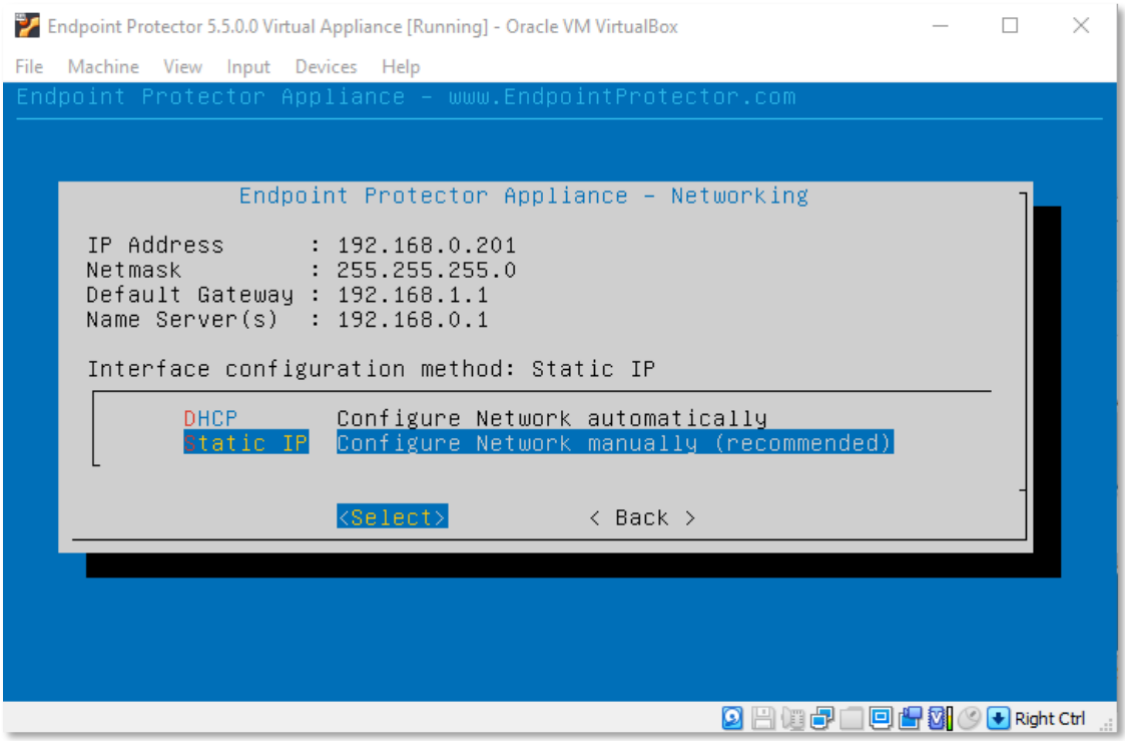
4. 구성 방법을 사용할 수 있음.

중요: 네트워크 설정은 수동 구성을 권장합니다.

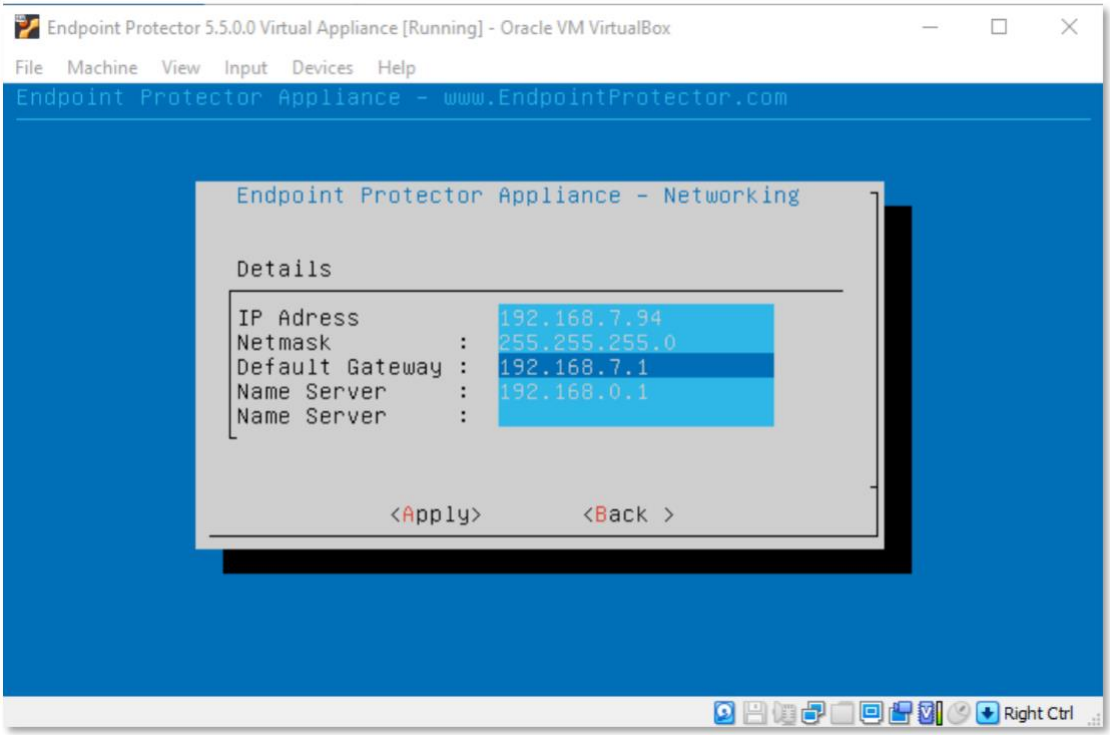


5.1. 수동 구성 (정적 IP 사용)

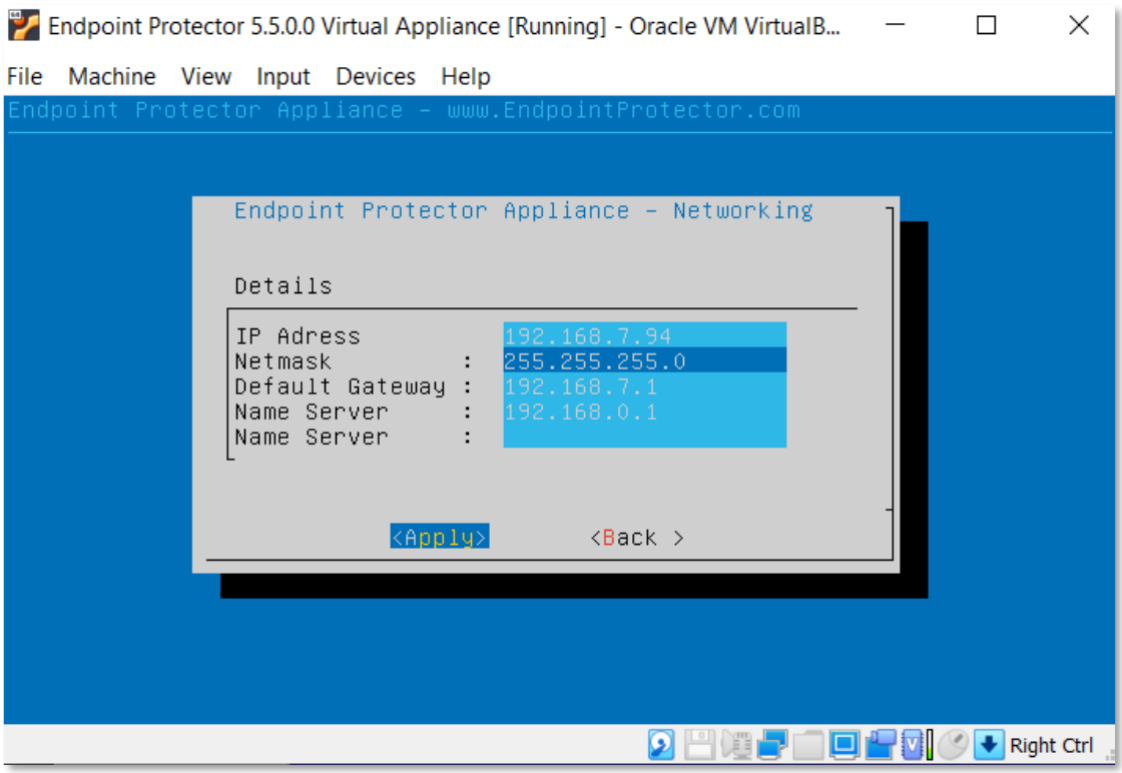
1. 네트워크 수동 **Configure** 선택 (권장);



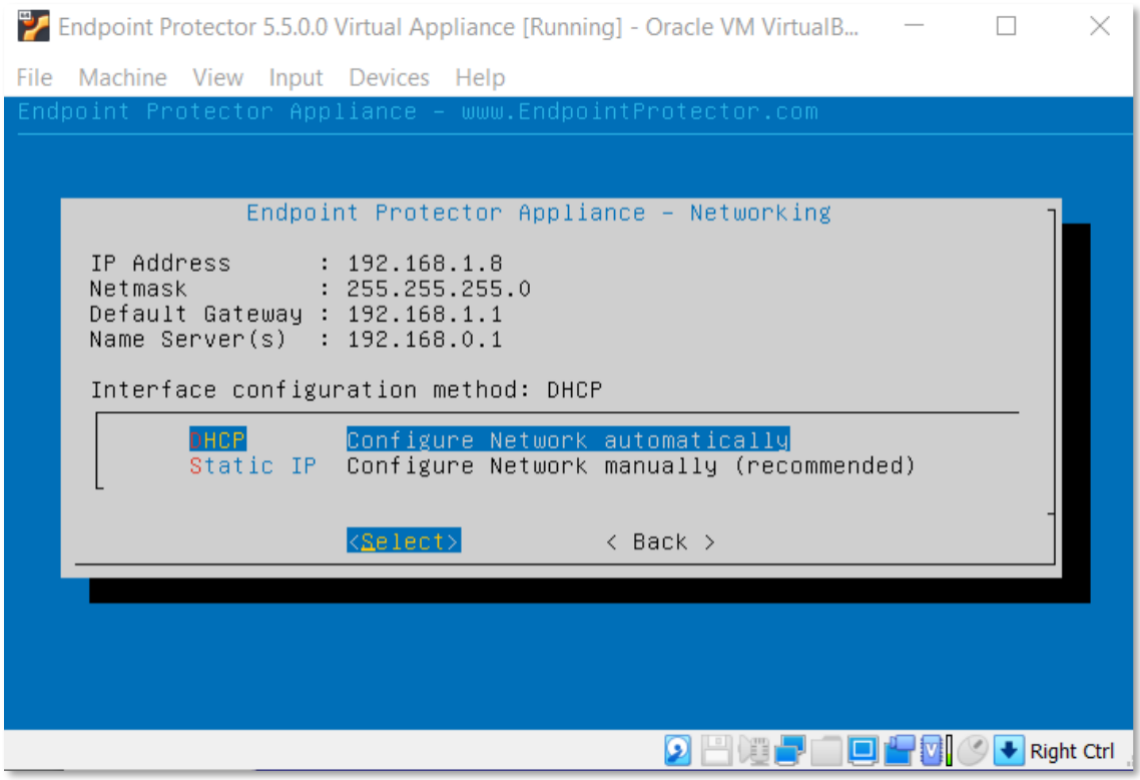
2. IP 주소 및 기본 게이트웨이 설정 (예: IP 주소는 192.168.7.94 로 게이트웨이는 192.168.7.1 로 설정);



3. **Tab** 키 누름;

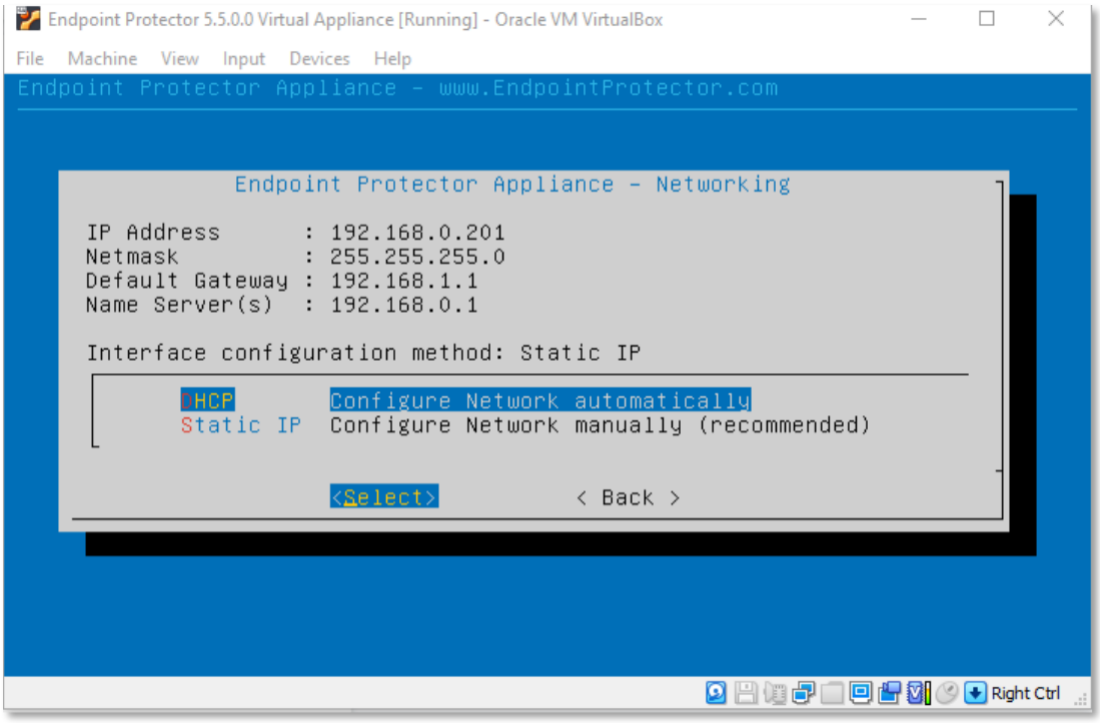


4. **Apply** 선택 – 가상 어플라이언스는 이제 구성된 IP 주소로 사용 가능합니다. (예: https://192.168.1.8)



5.2. 자동 구성 (동적 IP 사용)

자동으로 네트워크 구성을 선택 후 **Enter** 합니다. IP 주소와 게이트웨이는 자동으로 구성됩니다.

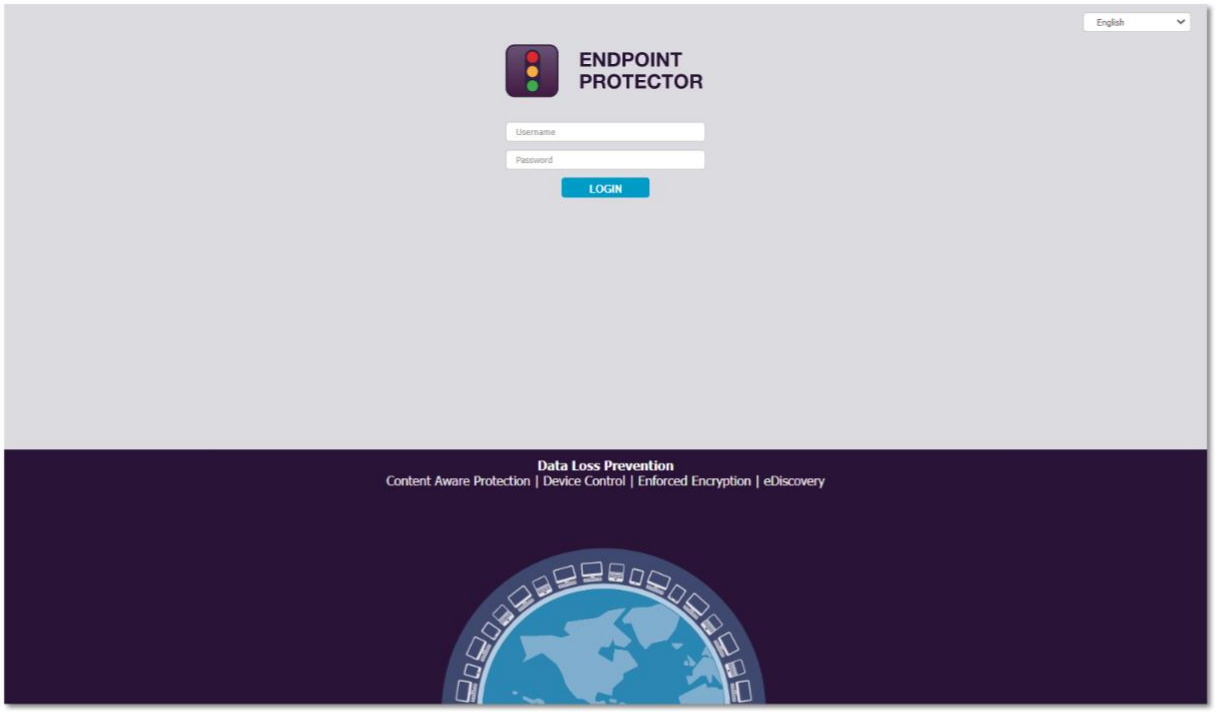


6. Endpoint Protector 구성

Endpoint Protector 설정 마법사에서 정적 IP 로 할당한 후에 네트워크로 어플라이언스로 통신할 수 있습니다. Endpoint Protector 사용자 인터페이스는 HTTPS 주소로 접근할 수 있습니다 (예: https://192.168.0.201).

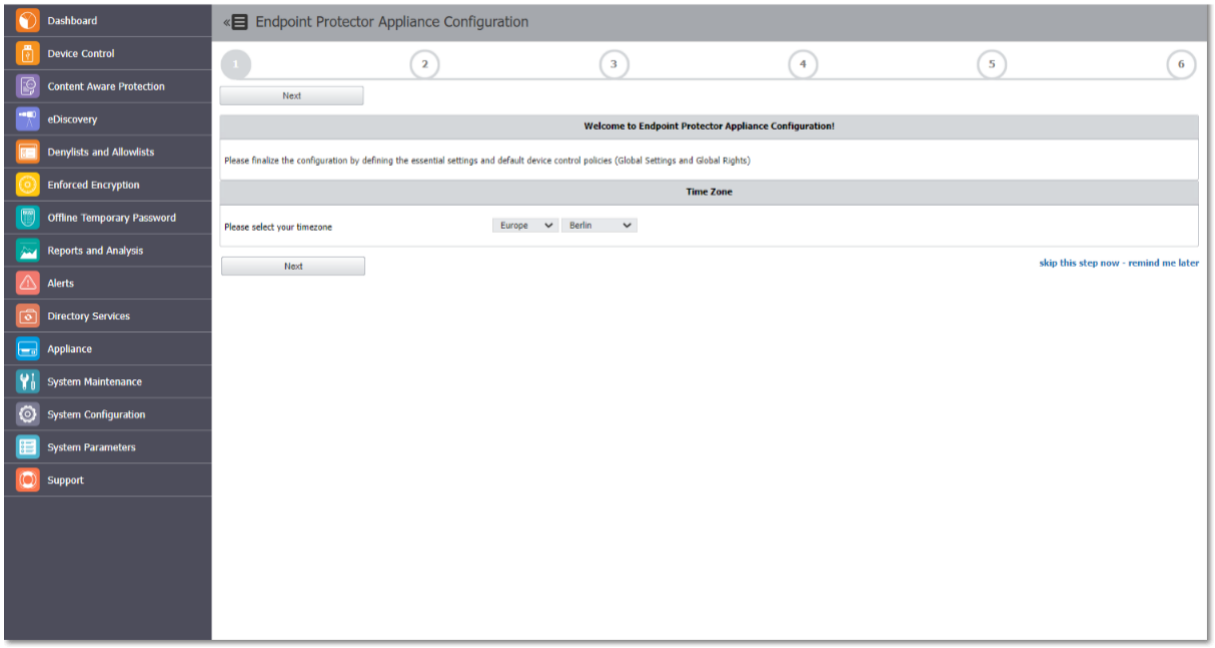
6.1. Endpoint Protector 로그인

Endpoint Protector 설정 마법사에 정의된 사용자 이름 및 암호를 입력합니다.
기본 Endpoint Protector 계정은 root 를 사용합니다.



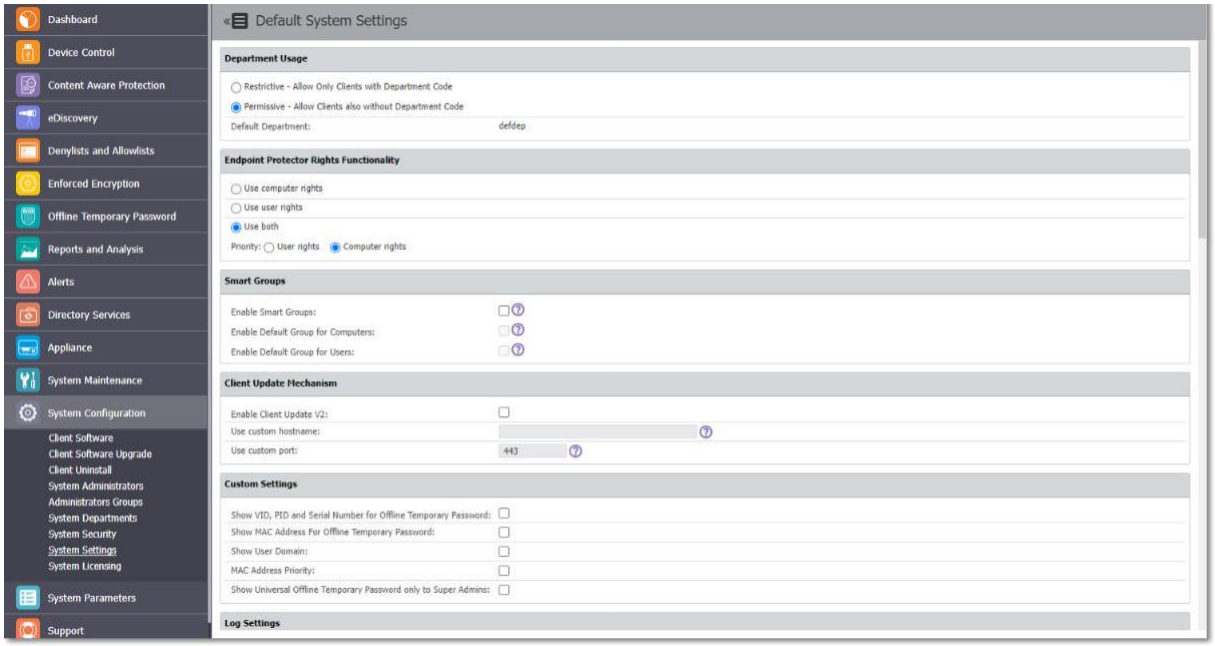
6.2. 구성 마법사

Endpoint Protector 구성을 마무리하기 위해서 일부 중요한 기본 설정과 기본 매체 제어 정책 (전체 설정)이 아래 단계에 따라서 정의되어야 합니다.



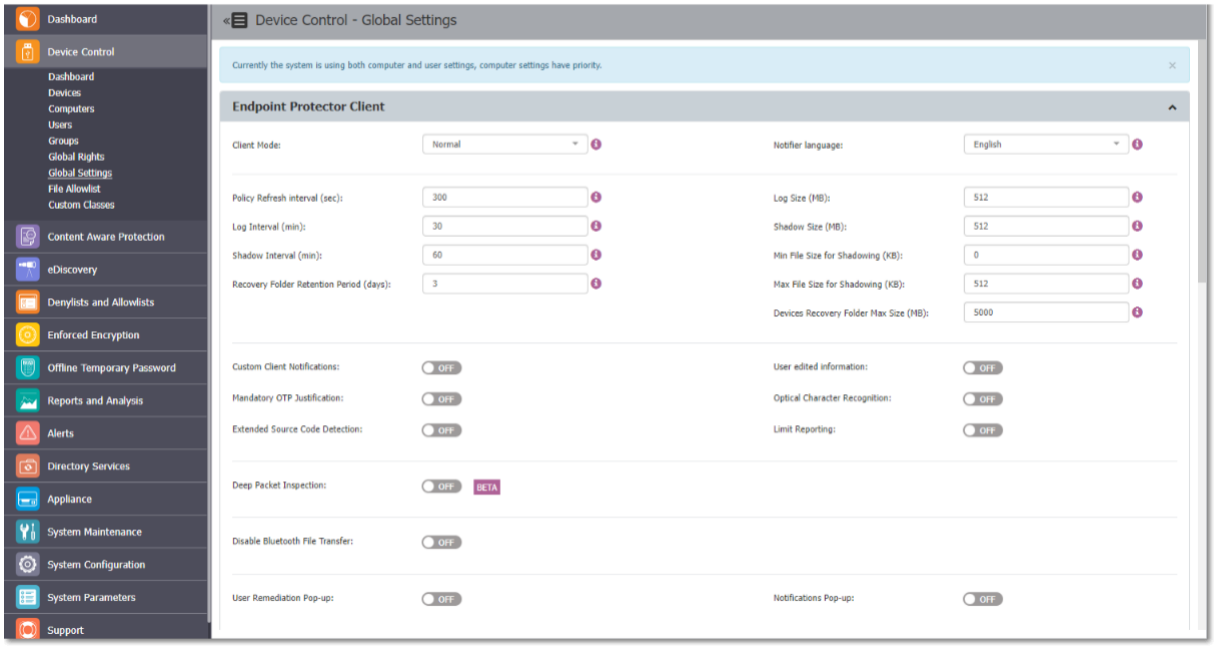
6.3. 시스템 설정

일부 기본 설정은 Endpoint Protector 의 적정한 기능을 수행하기 위해서 요구됩니다. 권한 우선순위, 경고를 받는 이메일, 주요 관리자 연락처, 프록시 서버 설정 등을 선택합니다.



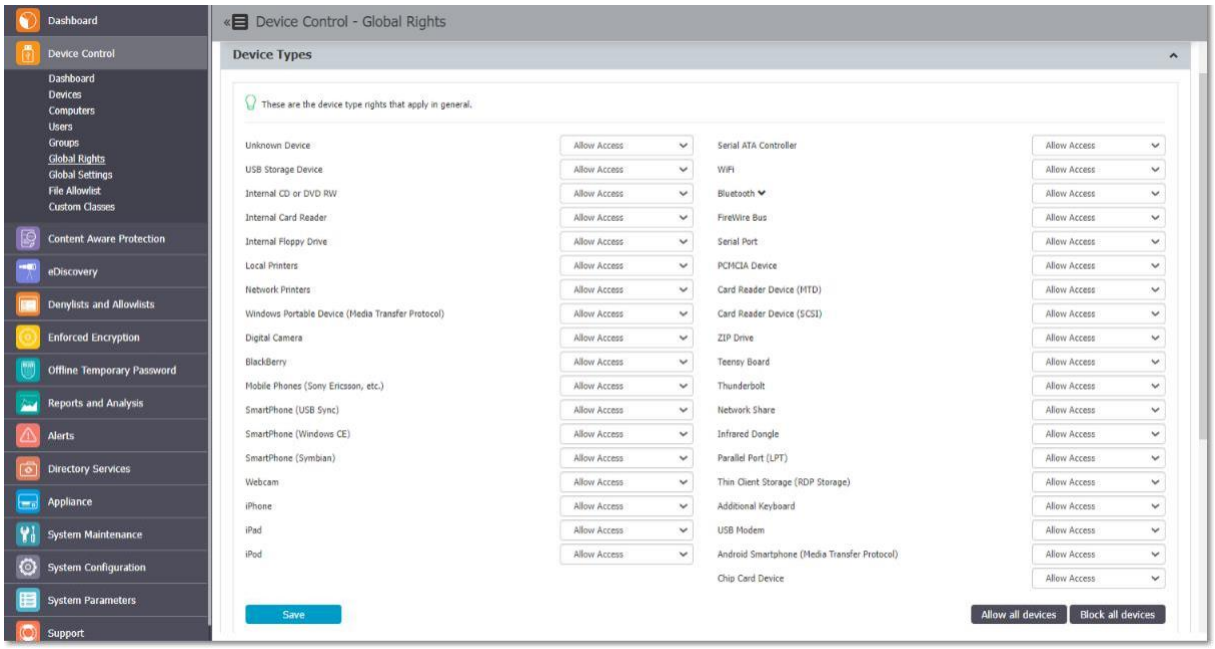
추가적으로 Endpoint Protector 새로고침 간격, 파일 추적 및 사본 보관과 같은 활성화 또는 비활성화 그리고 생성된 로그의 기본 매개변수를 구성할 수 있습니다.

기본으로 권장된 설정이 이미 구성되어 있고 전체 네트워크를 통해서 전체적으로 적용합니다.



6.4. Default Device Control Rights

Endpoint Protector 는 기본으로 매체 제어 모듈을 사용해서 USB 장치, 주변 포트가 전체 권한으로 미리 구성되어 있습니다. 이러한 구성은 후에 언제든지 변경이 가능하고 더 상세하게 적용할 수 있습니다 (장치, 컴퓨터, 사용자, 그룹).



6.5. Endpoint Protector 구성 마법사 끝내기

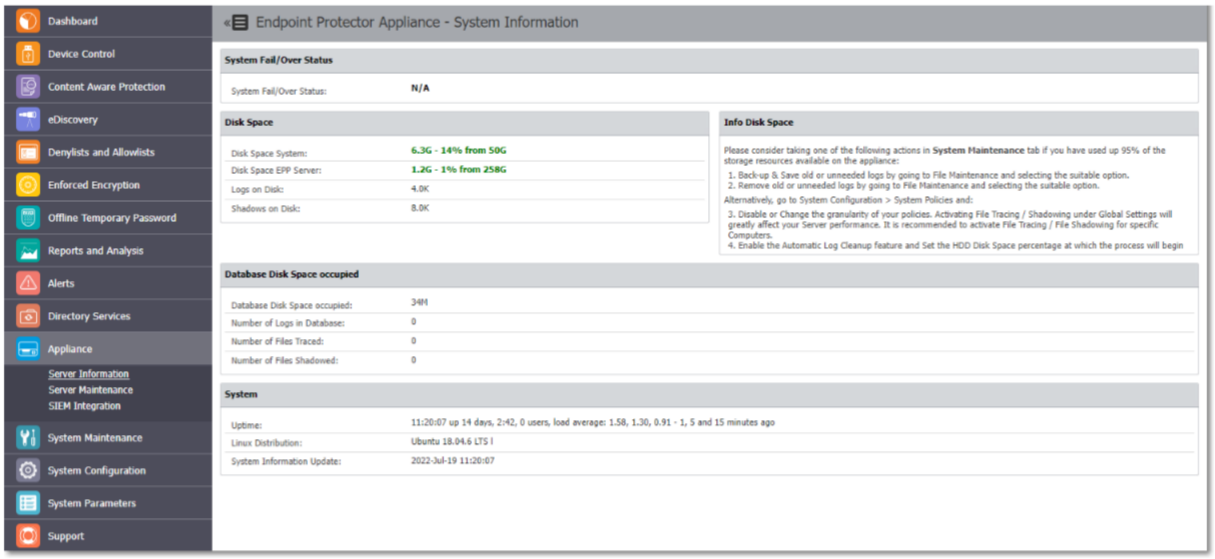
위의 단계를 따라서 Endpoint Protector 설정과 구성이 완료되었습니다. 다음 단계는 보호가 필요한 Windows, Mac, Linux 컴퓨터에 배포하는 것입니다.

7. 서버 정보 및 유지보수

Endpoint Protector 서버 정보 및 유지보수 설정은 메인 메뉴의 장비 섹션에서 가능합니다.

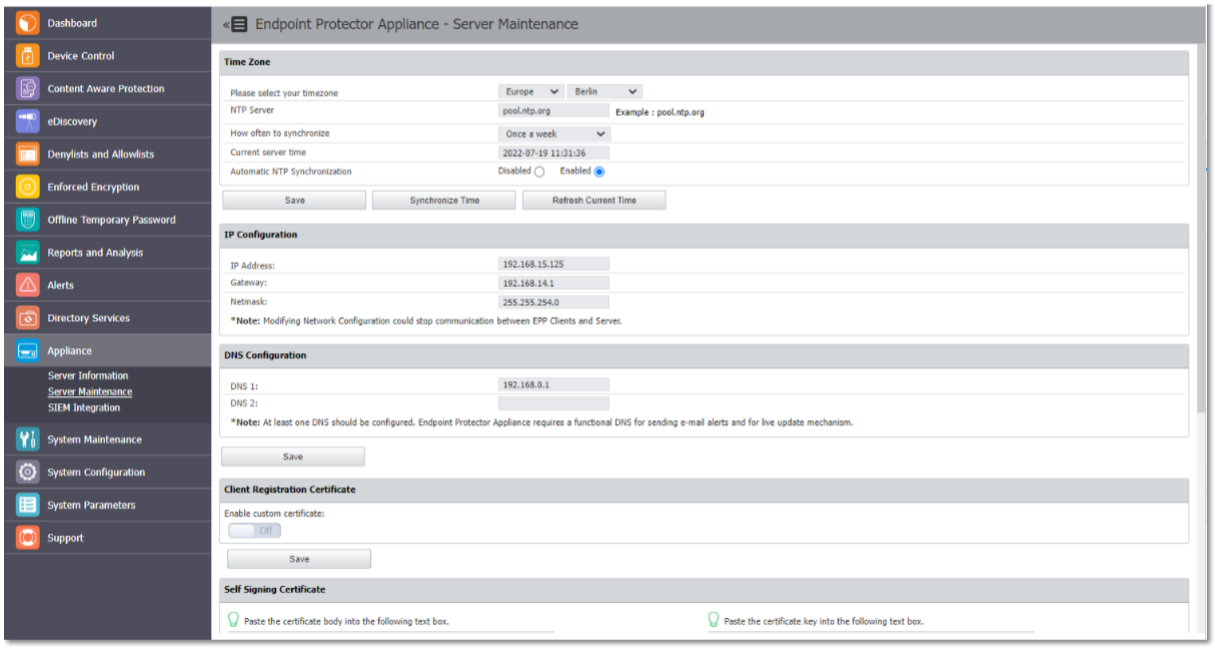
7.1. 서버 정보

이 섹션은 서버의 현재 상태에 대한 정보를 표시합니다.



7.2. 서버 유지보수

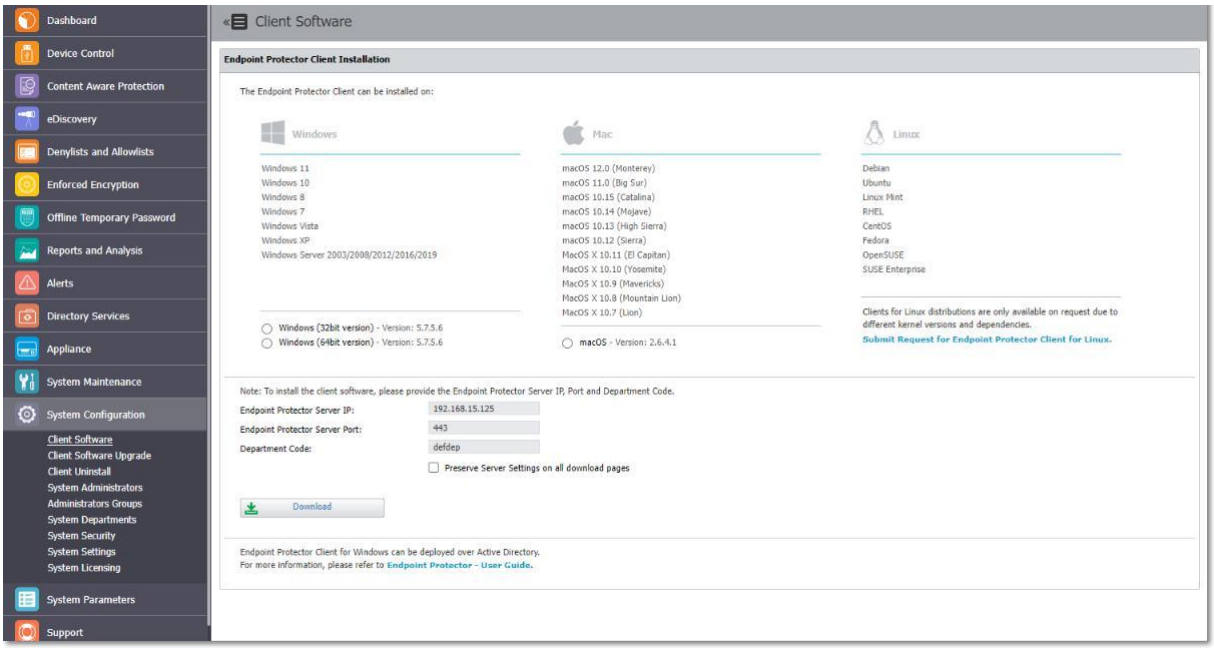
T 이 섹션은 장비 네트워크 설정, 재부팅 또는 전원 끄기 등의 옵션을 제공합니다.



7.3. Endpoint Protector 클라이언트 설치

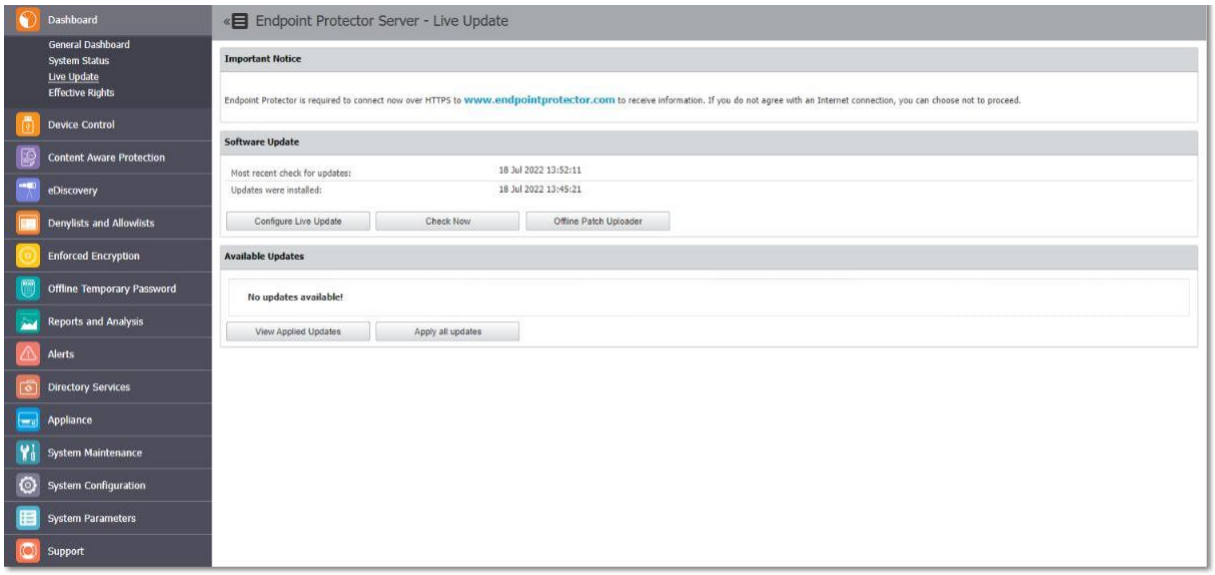
Endpoint Protector 클라이언트는 네트워크에 있는 컴퓨터에 배포되어야 합니다. 브라우저에서 정적 IP 주소로 접근해서 어플라이언스에서 직접 다운로드할 수 있습니다 (예: http://192.168.0.201). Endpoint Protector 다운로드 섹션은 HTTPS 및 HTTP 모두 접근할 수 있습니다. 이는 관리자가 아닌 사용자도 Endpoint Protector 클라이언트를 배포할 수 있도록 허용합니다.

Endpoint Protector 관리자가 네트워크에 있는 컴퓨터에 클라이언트를 배포하려면 위치 저장이 필요합니다. Active Directory 또는 Apple Remote Desktop 과 같은 솔루션은 배포를 더 쉽게 만들어 줍니다.



7.4. Endpoint Protector Live Update

Live Update 기능은 Endpoint Protector 업데이트 가능 여부를 온라인에서 확인할 수 있습니다. 이 프로세스는 수동으로 할 수 있고 옵션을 활성화하면 자동으로 가능합니다. 그러나 모든 가능한 업데이트의 설치는 Endpoint Protector 관리자가 승인을 해야합니다.



10. 면책

Endpoint Protector Appliance does not communicate outside of your network except with liveupdate.endpointprotector.com and cloud.endpointprotector.com.

Endpoint Protector does not contain malware software and does not send at any time any of your private information (if Automatic Live Update Reporting is DISABLED).

Each Endpoint Protector Server has the default SSH Protocol (22) open for Support Interventions and there is one (1) System Account enabled (epproot) protected with a password. The SSH Service can be disabled at customers' request.

Security safeguards, by their nature, are capable of circumvention. CoSoSys cannot, and does not, guarantee that data or devices will not be accessed by unauthorized persons, and CoSoSys disclaims any warranties to that effect to the fullest extent permitted by law.

EndpointProtector.com