

Secure Endpoint Virtual Private Cloud 설치 및 구성

목차

[소개](#)

[사전 요구 사항](#)

[VPC 구축](#)

[VM 설치](#)

[초기 관리 인터페이스 설정](#)

[웹 GUI를 통한 vPC의 초기 컨피그레이션](#)

[설정](#)

[Services](#)

[AirGap 업데이트 패키지](#)

[문제 #1 - 데이터 저장소의 공간 소진](#)

[문제 #2 - 이전 업데이트](#)

[기본 문제 해결](#)

[문제 #1 - FQDN 및 DNS 서버](#)

[문제 #2 - 루트 CA 문제](#)

소개

이 문서에서는 ESXi 환경의 서버에 VPC(Virtual Private Cloud)를 성공적으로 구축하는 방법을 설명하고 중점적으로 살펴봅니다. Quick Start Guide, Deployment Strategy, Entitlement Guide, Console and Administrator User Guide와 같은 다른 문서는 이 사이트 설명서를 참조하십시오.

기고자: Roman Valenta, Cisco TAC 엔지니어

사전 요구 사항

요건:

VMware ESX 5 이상

- 클라우드 프록시 모드(전용): 128GB RAM, CPU 코어 8개(각각 4개 코어의 CPU 2개 권장), VMware 데이터 저장소의 최소 여유 디스크 공간 1TB
- 드라이브 유형: 에어 갭 모드에 필요한 SSD이며 프록시에 권장됨
- RAID 유형: 1개의 RAID 10 그룹(스트라이프 미러)
- 최소 VMware 데이터 저장소 크기: 2TB
- RAID 10 그룹의 최소 데이터 저장소 랜덤 읽기(4K): 60K IOPS
- RAID 10 그룹의 최소 데이터 저장소 랜덤 쓰기(4K): 30K IOPS

Cisco에서는 다음 항목에 대해 알고 있는 것이 좋습니다.

- 인증서 작업 방법에 대한 기본 지식
- DNS 서버(Windows 또는 Linux)에서 DNS를 설정하는 방법에 대한 기본 지식
- VMWare ESXi에 OVA(Open Virtual Appliance) 템플릿 설치

이 LAB에서 사용:


VMware ESX 6.5

- 클라우드 프록시 모드(전용): 48GB RAM, 8개의 CPU 코어(각각 4개의 코어로 구성된 2개의 CPU 권장), VMware 데이터 저장소의 최소 여유 디스크 공간 1TB
- 드라이브 유형: SATA
- RAID 유형: RAID 1 1개
- 최소 VMware 데이터 저장소 크기: 1TB
- MobaXterm 20.2(PuTTY와 유사한 다중 터미널 프로그램)
- Cygwin64(AirGap 업데이트 다운로드에 사용)


추가로

- openssl 또는 XCA를 사용하여 생성하는 인증서
- DNS 서버(Linux 또는 Windows) 실습에서 Windows Server 2016 및 CentOS-8을 사용했습니다.
- 테스트 엔드포인트용 Windows VM
- 라이선스

메모리가 48GB RAM 미만인 경우 버전 3.2+ VPC를 사용할 수 없게 됩니다.

 참고: Private Cloud OVA는 VMWare에서 드라이브 파티션을 지정할 필요가 없도록 드라이브 파티션을 생성합니다. 이 서버는 정상 인터페이스 호스트 이름을 확인합니다.

버전별 하드웨어 [요구 사항](#)에 대한 자세한 내용은 VPC 어플라이언스 데이터 시트를 참조하십시오.

 참고: 이 문서의 정보는 특정 랩 환경의 디바이스에서 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

VPC 구축

eDelivery 또는 엔타이틀먼트 이메일에 제공된 URL을 선택합니다. OVA 파일을 다운로드하고 설치를 진행합니다.

VM 설치

1단계:

그림과 같이 File(파일) > Deploy OVF Template(OVF 템플릿 구축)으로 이동하여 Deploy OVF Template(OVF 템플릿 구축) 마법사를 엽니다.

- 1 Select creation type
- 2 Select OVF and VMDK files**
- 3 Select storage
- 4 License agreements
- 5 Deployment options
- 6 Additional settings
- 7 Ready to complete

Select OVF and VMDK files

Select the OVF and VMDK files or OVA for the VM you would like to deploy

Enter a name for the virtual machine.

AMP-vPC

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

x vm PrivateCloud-Latest.ova



Back Next Finish Cancel

- 1 Select creation type**
- 2 Select OVF and VMDK files
- 3 Select storage
- 4 License agreements
- 5 Deployment options
- 6 Additional settings
- 7 Ready to complete

Select creation type

How would you like to create a Virtual Machine?

Create a new virtual machine

Deploy a virtual machine from an OVF or OVA file

Register an existing virtual machine

This option guides you through the process of creating a virtual machine from an OVF and VMDK files.



Back Next Finish Cancel

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- 4 License agreements
- 5 Deployment options
- 6 Additional settings
- 7 Ready to complete

Select storage

Select the datastore in which to store the configuration and disk files.

The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
vDisk-70_12	922.75 GB	921.8 GB	VMFS5	Supported	Single
vDisk-70_34	930.25 GB	929.3 GB	VMFS5	Supported	Single
vDisk-70_56	930.25 GB	929.3 GB	VMFS5	Supported	Single
vDisk-70_78	930.25 GB	929.3 GB	VMFS5	Supported	Single


4 items

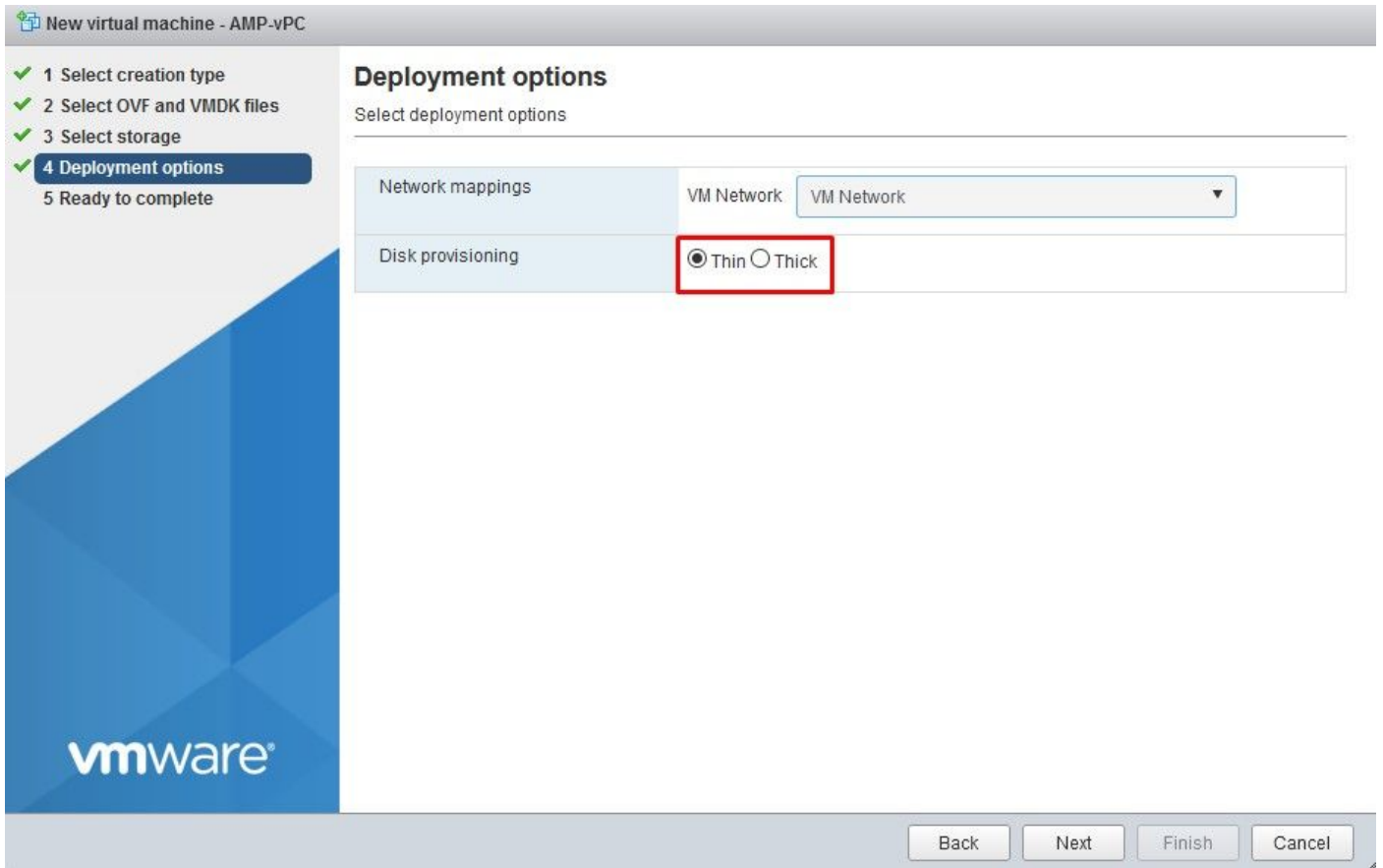
Back

Next

Finish

Cancel

 참고: Thick Provisioning(썩 프로비저닝)은 디스크가 생성될 때 공간을 예약합니다. 이 옵션을 선택하면 Thin Provisioned(씬 프로비저닝)보다 성능이 향상될 수 있습니다. 그러나 이는 필수 사항이 아닙니다. 이제 이미지에 표시된 대로 Next(다음)를 선택합니다.



2단계:

찾아보기...를 선택하여 OVA 파일을 선택한 후 다음을 선택합니다. 이미지에 표시된 대로 OVF 템플릿 상세내역 페이지에서 기본 OVA 매개변수를 확인합니다. 다음 페이지에서 선택합니다.


New virtual machine - AMP-vPC

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- ✓ 5 Ready to complete

Ready to complete

Review your settings selection before finishing the wizard

Product	FireAMP PrivateCloud x86_64
VM Name	AMP-vPC
Disks	PrivateCloud_3.2.0_202010082118_v6.5_signed-disk1.vmdk,PrivateCloud_3.2.0_202010082118_v6.5_signed-disk2.vmdk,PrivateCloud_3.2.0_202010082118_v6.5_signed-disk3.vmdk,PrivateCloud_3.2.0_202010082118_v6.5_signed-disk4.vmdk
Datastore	vDisk-70_12
Provisioning type	Thin
Network mappings	VM Network: VM Network
Guest OS Name	Unknown

 Do not refresh your browser while this VM is being deployed.

vmware

Back Next Finish Cancel

초기 관리 인터페이스 설정


New virtual machine - AMP-vPC

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- ✓ 5 Ready to complete

Ready to complete

Review your settings selection before finishing the wizard

Product	FireAMP PrivateCloud x86_64
VM Name	AMP-vPC
Disks	PrivateCloud_3.2.0_202010082118_v6.5_signed-disk1.vmdk,PrivateCloud_3.2.0_202010082118_v6.5_signed-disk2.vmdk,PrivateCloud_3.2.0_202010082118_v6.5_signed-disk3.vmdk,PrivateCloud_3.2.0_202010082118_v6.5_signed-disk4.vmdk
Datastore	vDisk-70_12
Provisioning type	Thin
Network mappings	VM Network: VM Network
Guest OS Name	Unknown

 Do not refresh your browser while this VM is being deployed.

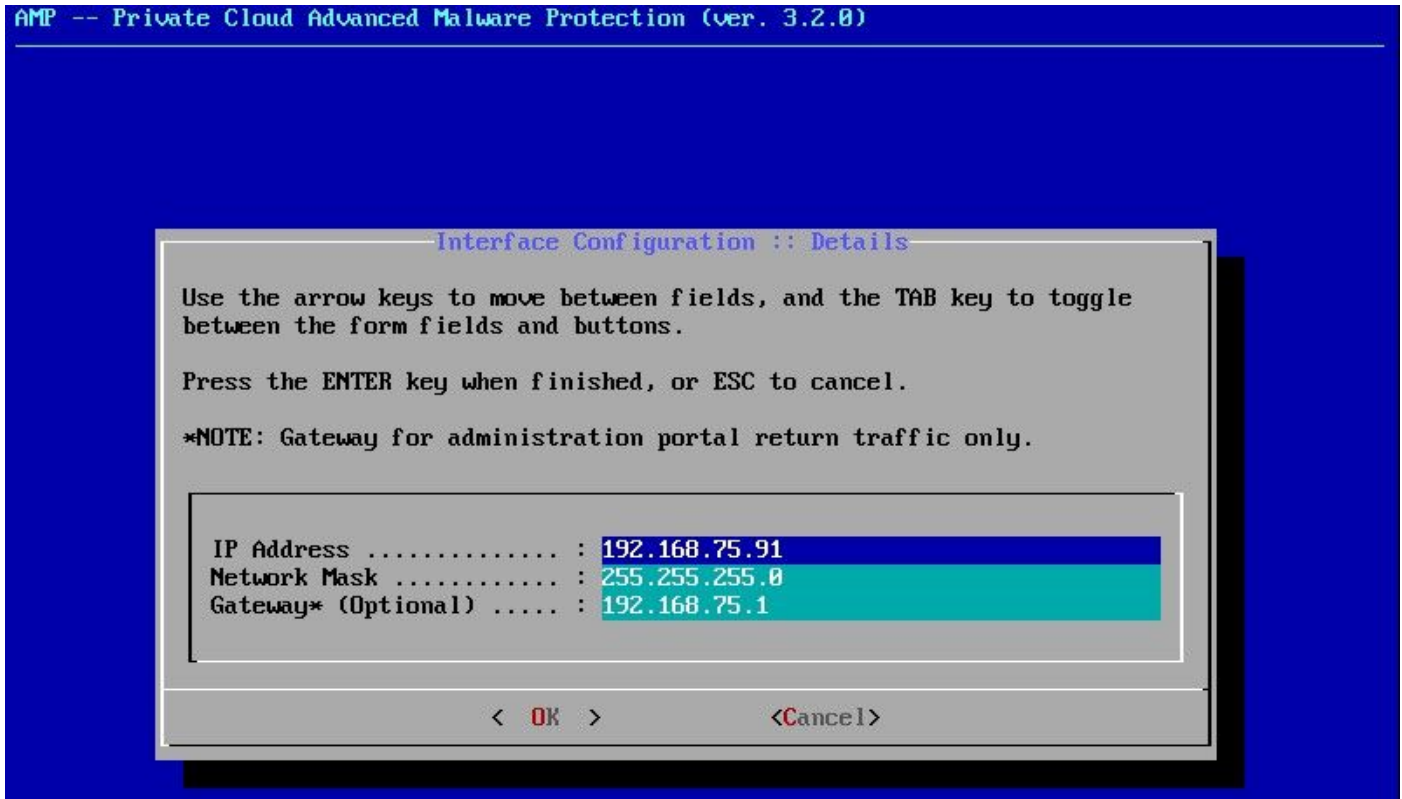
vmware

Back Next Finish Cancel

VM이 부팅되면 VM 콘솔을 통해 초기 컨피그레이션을 수행합니다.

1단계:

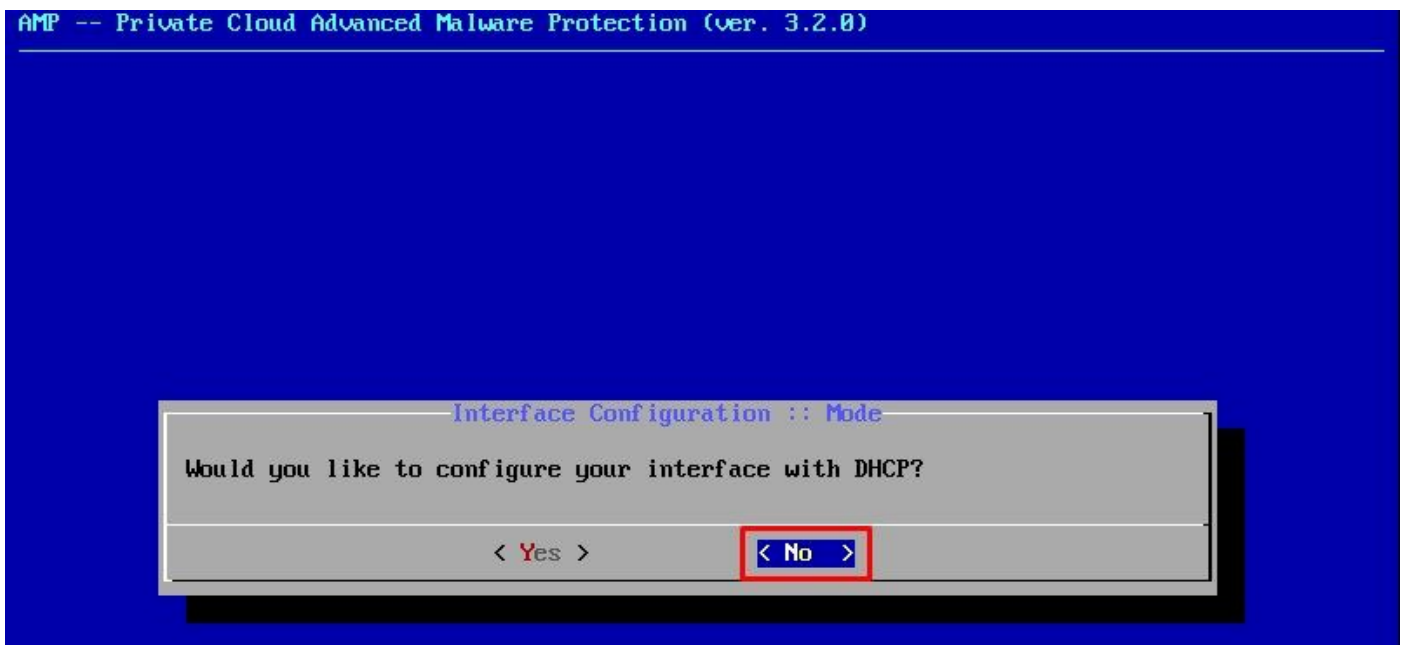
인터페이스가 DHCP 서버에서 IP 주소를 받지 못한 경우 URL에 [UNCONFIGURED]가 표시될 수 있습니다. 이 인터페이스는 관리 인터페이스입니다. 이것은 프로덕션 인터페이스가 아닙니다.



2단계:

Tab, Enter 및 화살표 키를 탐색할 수 있습니다.

CONFIG_NETWORK로 이동하고 키보드에서 Enter 키를 선택하여 Secure Endpoint Private Cloud의 관리 IP 주소 컨피그레이션을 시작합니다. DHCP를 사용하지 않으려면 No(아니요)를 선택하고 Enter(키 입력)를 선택합니다.





표시된 창에서 Yes(예)를 선택하고 Enter key(키 입력)를 선택합니다.



IP가 이미 사용 중인 경우 이 오류 로그를 사용하여 처리합니다. 그냥 돌아가서 사용하지 않고 독특한 것을 고르세요.

Restarting eth0...

```
ERROR : [/etc/sysconfig/network-scripts/ifup-eth] Error, some other host (00:0C:29:41:74:E3) already uses address 192.168.75.91.  
ERROR : [/etc/sysconfig/network-scripts/ifup-eth] Error, some other host (00:0C:29:41:74:E3) already uses address 192.168.75.91.  
ERROR : [/etc/sysconfig/network-scripts/ifup-eth] Error, some other host (00:0C:29:41:74:E3) already uses address 192.168.75.91.
```

```
=====  
ERROR: The interface failed to reconfigure.  
=====
```

Press ENTER key to continue...

AMP -- Private Cloud Advanced Malware Protection (ver. 3.2.0)

Interface Configuration :: Details

Use the arrow keys to move between fields, and the TAB key to toggle between the form fields and buttons.

Press the ENTER key when finished, or ESC to cancel.

*NOTE: Gateway for administration portal return traffic only.

IP Address	:	192.168.75.92
Network Mask	:	255.255.255.0
Gateway* (Optional)	:	192.168.75.1

< OK >

<Cancel>

모든 것이 잘 되면 다음과 같은 출력이 표시됩니다

```

- execute semanage fcontext --add --type var_log_t "/data/log(/.*)?"
* execute[ConfigurePokedLogs] action run
- execute semanage fcontext --add --type var_log_t "/data/poked(/.*)?"
* execute[ConfigureCloudLogs] action run
- execute semanage fcontext --add --type var_log_t "/data/cloud/log(/.*)?"
* execute[ConfigureEventLogs] action run
- execute semanage fcontext --add --type var_log_t "/data/event_log_store(/.*)?"
* execute[RestoreSELinuxFileContextData] action run
- execute restorecon -R /data
Recipe: base::ssh
* template[etc/ssh/sshd_config] action create
- update content in file /etc/ssh/sshd_config from c85f41 to badlab
--- /etc/ssh/sshd_config 2021-04-09 13:25:01.969995024 +0000
+++ /etc/ssh/.chef-sshd_config20210410-8506-1ry0qx2 2021-04-10 06:13:11.889389544 +0000
@@ -18,7 +18,7 @@
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
-ListenAddress 192.168.75.208
+ListenAddress 192.168.75.92

# The default requires explicit activation of protocol 1
Protocol 2
- restore selinux security context
* template[etc/ssh/sshd_config] action create (up to date)
* service[ssh_server] action enable (up to date)
* service[ssh_server] action start (up to date)
Recipe: base::grub-conf
* cookbook_file[etc/default/grub] action create (up to date)
* execute[Update grub if new kernel installed] action run (skipped due to only_if)
* execute[Ensure grub menu displays Cisco not CentOS] action run (skipped due to only_if)
Recipe: base::transparent-hugepages
* execute[disable transparent hugepage] action run
- execute echo never > /sys/kernel/mm/transparent_hugepage/enabled
* execute[disable transparent hugepage defrag] action run
- execute echo never > /sys/kernel/mm/transparent_hugepage/defrag
* execute[disable transparent hugepage for default kernel] action run

```

Restarting eth0...

Reconfiguring...

```

[2021-04-10T06:12:42+00:00] WARN: Ohai::Config[:disabled_plugins] is set. Ohai::Config[:disabled_plugins] is deprecated and will be removed in future releases of ohai. Use ohai.disabled_plugins in your configuration file to configure :disabled_plugins for ohai.
[2021-04-10T06:12:42+00:00] WARN: Ohai::Config[:disabled_plugins] is set. Ohai::Config[:disabled_plugins] is deprecated and will be removed in future releases of ohai. Use ohai.disabled_plugins in your configuration file to configure :disabled_plugins for ohai.
Starting Chef Client, version 12.14.89

```

3단계:

새 고정 IP를 사용하여 블루 스크린이 다시 팝업될 때까지 기다립니다. 또한 일회용 비밀번호를 기록해 두시기 바랍니다. 메모를 하고 브라우저를 엽시다.

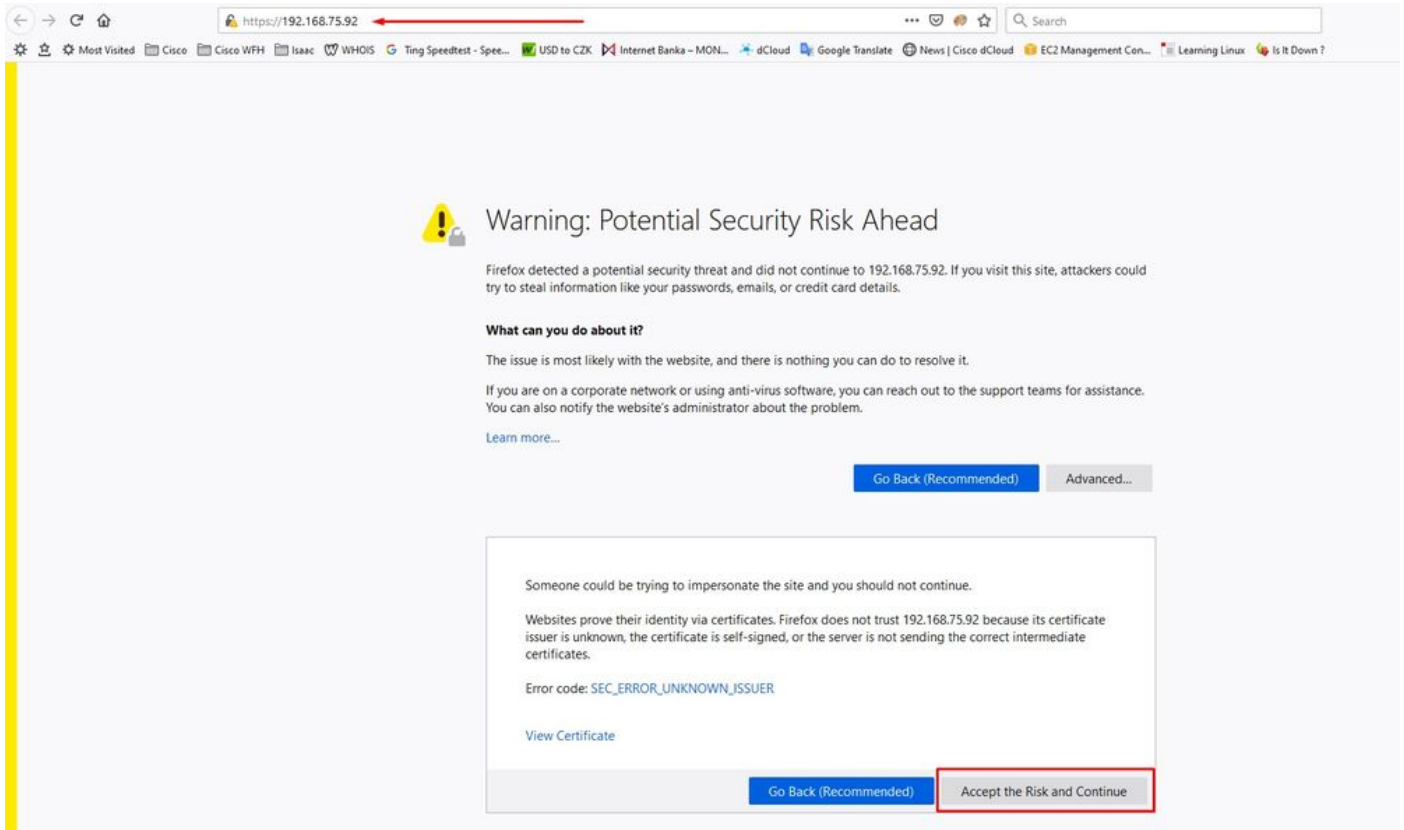


웹 GUI를 통한 vPC의 초기 컨피그레이션

1단계:

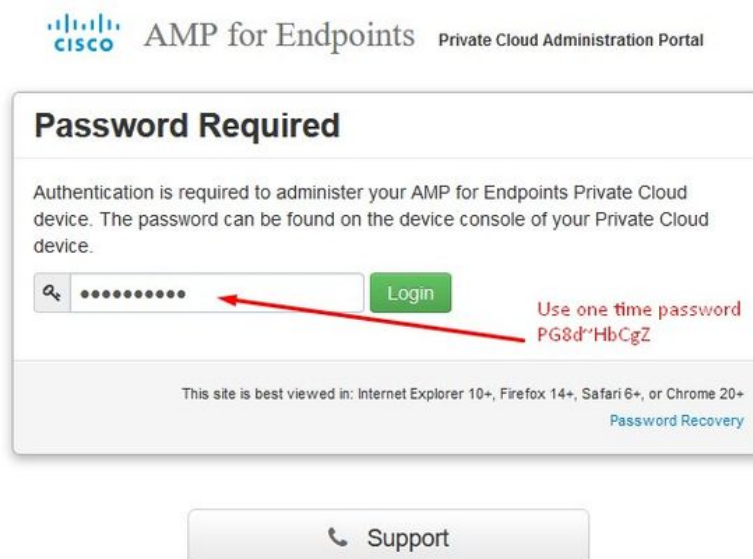
웹 브라우저를 열고 어플라이언스의 관리 IP 주소로 이동합니다. 이미지에 표시된 대로 Secure Endpoint Private Cloud에서 자체 HTTPS 인증서를 처음 생성할 때 인증서 오류를 수신할 수 있습니다. Secure Endpoint Private Cloud의 자체 서명 HTTPS 인증서를 신뢰하도록 브라우저를 구성합니다.

브라우저에서 이전에 구성한 STATIC IP를 입력합니다.



2단계:

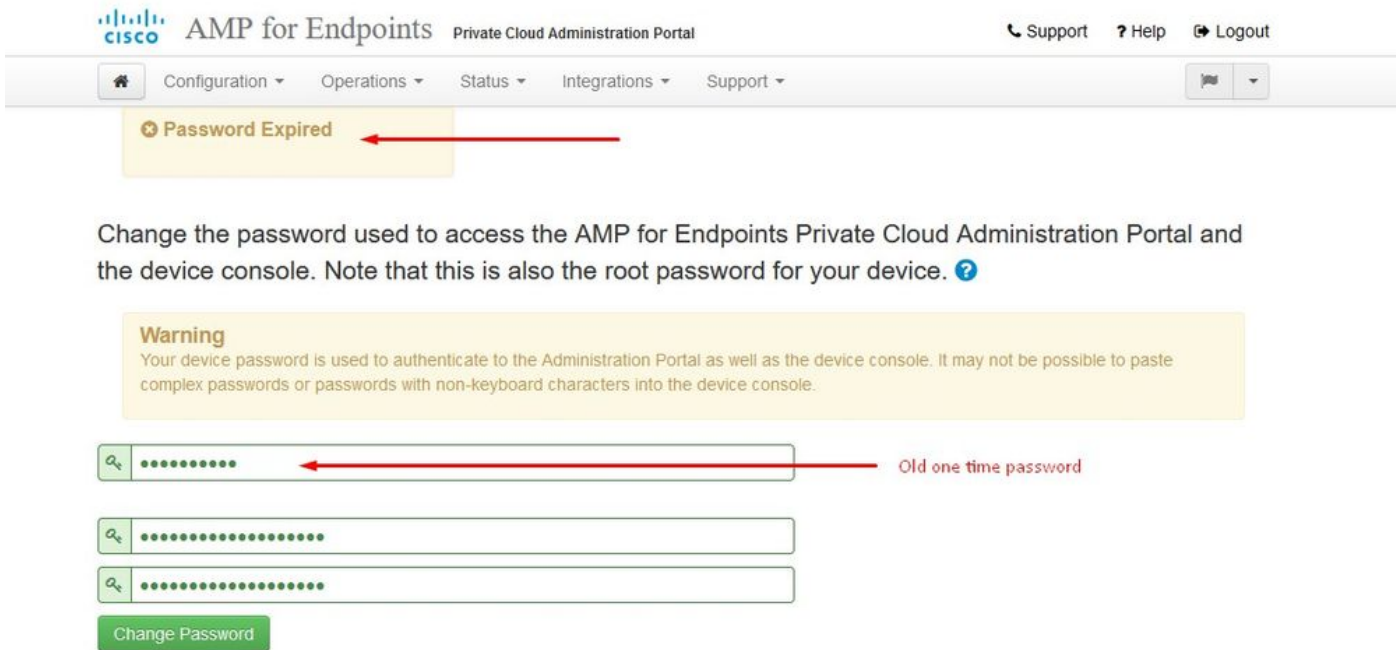
로그인한 후 비밀번호를 재설정해야 합니다. Old Password(이전 비밀번호) 필드에 콘솔의 초기 비밀번호를 사용합니다. New Password(새 비밀번호) 필드에서 새 비밀번호를 사용합니다. 새 암호 필드에 새 암호를 다시 입력합니다. 암호 변경을 선택합니다.



3단계:

로그인한 후 비밀번호를 재설정해야 합니다. Old Password(이전 비밀번호) 필드에 콘솔의 초기 비

밀번호를 사용합니다. New Password(새 비밀번호) 필드에서 새 비밀번호를 사용합니다. 새 암호 필드에 새 암호를 다시 입력합니다. 암호 변경을 선택합니다.



4단계:

라이선스 계약서에 동의하려면 다음 페이지에서 아래쪽으로 스크롤합니다. I have read and agree를 선택하십시오.



5단계:

계약에 동의하면 그림과 같은 설치 화면이 나타납니다. 백업에서 복원하려는 경우 여기에서 복원할 수 있습니다. 그러나 이 설명서에서는 Clean Installation 옵션을 진행합니다. Clean Installation(클린 설치) 섹션에서 Start(시작)를 선택합니다.

Installation Options

Only the License section can be altered after installation.

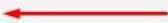
- > Install or Restore
- > License

Install or Restore

Either perform a clean installation or select a location to restore your device from. When restoring you will have the option to edit your configuration before restore proceeds.

Clean Installation

Start >



Restore

Local Remote Upload

Restore a recovery file using your browser. Note that this method is only recommended for small recovery files (less than 20MB).

+ Choose Restore File

/data

Start >

6단계:

가장 먼저 필요한 것은 앞으로 나아갈 수 있는 허가증입니다. 제품 구매 시 라이선스 및 패스프레이즈를 받게 됩니다. on+Upload License File을 선택합니다. 라이선스 파일을 선택하고 암호를 입력합니다. Upload License(라이선스 업로드)에서 선택합니다. 업로드가 실패하면 암호가 정확한지 확인하십시오. 업로드에 성공하면 유효한 라이선스 정보가 있는 화면이 표시됩니다. Next(다음)를 선택합니다. 여전히 라이선스를 설치할 수 없는 경우 Cisco 기술 지원에 문의하십시오.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore
- > License

License

Device ID

EG[REDACTED]V5

License

No license has been installed.

Install New License

license + Upload License File

.....

Upload License

License was successfully uploaded

Installation Options

Only the License section can be altered after installation.

- Install or Restore ✓
- License ✓
- Welcome
- Deployment Mode
- AMP for Endpoints Console
- Account
- Hardware Requirements

Configuration

- Network
- Date and Time
- Certificate Authorities
- Upstream Proxy Server
- Email ✓
- Notifications ✓
- Backup ✓
- SSH ✓
- Syslog ✓
- Updates ✓

Services

- Authentication
- AMP for Endpoints Console
- Disposition Server
- Disposition Server

License

Device ID
E60[redacted]/5

License	
Licensee	Roman Valenta rva[redacted].com
Business	Cisco - rvalenta 395a6444[redacted]-7a86fb49b7a5
Validity	2021-04-01 - 2025-12-31
Product SKU	FP-AMP-CLOUD=
Seats	50

Replace License [\(click to expand\)](#)

Next >

7단계:

이미지에 표시된 대로 시작 페이지를 수신합니다. 이 페이지는 프라이빗 클라우드를 구성하기 전에 보유해야 하는 정보를 보여줍니다. 요구 사항을 주의 깊게 읽습니다. 사전 설치 구성을 시작하려면 다음을 선택하십시오.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > **Welcome**
- > Deployment Mode
- > AMP for Endpoints Console
- > Account
- > Hardware Requirements

Configuration

- > Network
- > Date and Time
- > Certificate Authorities
- > Upstream Proxy Server ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication
- > AMP for Endpoints Console
- > Disposition Server
- > Disposition Server
- > Extended Protocol
- > Disposition Update
- > Service
- > Firepower Management Center

Other

- > Recovery
- > Review and Install

[▶ Start Installation](#)

Welcome to Private Cloud

Before you begin

AMP for Endpoints Private Cloud needs certain network and infrastructure resources in place.



You will be asked to provide this information as you proceed through the installation. For more information and examples, please refer to the Private Cloud Deployment Strategy guide.

**Two Static IP Addresses**

One for administrative use, and the other for enterprise-facing services.

**DNS Server**

Provides hostname resolution to the Private Cloud device.

**Hostnames and Trusted Certificates**

One hostname and trusted certificate for each of the following services:

- Authentication.
- AMP for Endpoints Console.
- Disposition Server.
- Disposition Server - Extended Protocol.
- Disposition Update Service.
- Firepower Management Center Link.

Note: Hostnames can not be changed once the device has finished installation.

**SMTP Server**

Used for emails, alerts, and notifications.

**NTP Server**

Provides time synchronization across your Private Cloud device and endpoints.

**External Internet connection (Proxy Mode only)**

Proxy Mode devices perform anonymized disposition queries against the Cisco Cloud.

[Next >](#)

설정

1단계:

참고: 다음 슬라이드 세트에는 이미지에 표시된 것처럼 AIR GAP 모드에만 고유한 일부 제외 항목이 포함되어 있습니다. 이는 AIRGAP ONLY로 묶어서 표시되어야 합니다



Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode
- > AMP for Endpoints Console
- > Account
- > Hardware Requirements

Configuration

- > Network
- > Date and Time
- > Certificate Authorities
- > Upstream Proxy Server ✓
- > Email ✓
- > Notifications
- > Backup ✓
- > SSH
- > Syslog ✓
- > Updates ✓

Deployment Mode

Cloud proxy mode performs disposition lookups against Cisco Cloud disposition servers. Standalone mode disables upstream communication with Cisco Cloud disposition servers and performs disposition lookups against a local database.

Cloud Proxy

- Requires an Internet connection and communication with AMP for Endpoints Connectors managed by this device.
- Disposition queries are proxied to the Cisco Cloud.
- Content updates contain TETRA definitions.
- Content and software updates can be retrieved and applied automatically.

Standalone

- May require an Internet connection
- Communication with AMP for Endpoints Connectors managed by this device are needed.
- Disposition queries are handled by the Private Cloud device.
- Content updates contain TETRA definitions as well as file disposition information.
- Updates may be downloaded separately or automatically on this device.

≡ ≡ AIRGAP ONLY ≡ ≡



Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode
- > Standalone Operation
- > AMP for Endpoints Console
- > Account
- > Hardware Requirements

Configuration

- > Network
- > Date and Time
- > Certificate Authorities
- > Upstream Proxy Server ✓
- > Email ✓
- > Notifications
- > Backup ✓
- > SSH
- > Syslog ✓
- > Updates ✓

Deployment Mode

Cloud proxy mode performs disposition lookups against Cisco Cloud disposition servers. Standalone mode disables upstream communication with Cisco Cloud disposition servers and performs disposition lookups against a local database.

Cloud Proxy

- Requires an Internet connection and communication with AMP for Endpoints Connectors managed by this device.
- Disposition queries are proxied to the Cisco Cloud.
- Content updates contain TETRA definitions.
- Content and software updates can be retrieved and applied automatically.

Standalone

- May require an Internet connection
- Communication with AMP for Endpoints Connectors managed by this device are needed.
- Disposition queries are handled by the Private Cloud device.
- Content updates contain TETRA definitions as well as file disposition information.
- Updates may be downloaded separately or automatically on this device.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > Standalone Operation
- > AMP for Endpoints Console
- > Account
- > Hardware Requirements

Configuration

- > Network
- > Date and Time
- > Certificate Authorities
- > Upstream Proxy Server ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Standalone Operation

Air Gap mode requires updates to be downloaded separately from this Private Cloud device, and applied via an ISO file attached to the device.

[Air Gap](#)

- Does not require an Internet Connection
- Updates must be downloaded separately and applied to this Private Cloud device.

AIRGAP ≡ ≡ 전용 ≡ ≡

2단계:

Secure Endpoint Console Account(보안 엔드포인트 콘솔 계정) 페이지로 이동합니다. 관리 사용자는 콘솔에서 정책, 컴퓨터 그룹을 만들고 사용자를 추가하는 데 사용됩니다. 콘솔 어카운트의 이름, 이메일 주소 및 비밀번호를 입력합니다. Next(다음)에서 선택합니다.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints Console Account
- > Hardware Requirements

Configuration

- > Network
- > Date and Time
- > Certificate Authorities
- > Upstream Proxy Server ✓
- > Cisco Cloud
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

AMP for Endpoints Console Account

Configure the initial account for the AMP for Endpoints Console. The AMP for Endpoints Console is the main interface for your AMP for Endpoints Private Cloud.

Name	Roman	Valenta
Business Name	Cisco - rvalenta	
Email Address	rval[REDACTED].com	
	rval[REDACTED].com	
Password	
	

Next >

OVA 파일에서 구축할 때 이 문제를 실행하면 두 가지 선택 사항 중 하나를 선택할 수 있습니다. 이 문제를 계속 진행하여 해결하거나 나중에 종료한 다음 구축된 VM에 연결하여 적절히 조정합니다. 다시 시작한 후에는 나간 위치를 계속 진행합니다.

참고: 128GB RAM 및 8CPU 코어로 올바르게 로드된 버전 3.5.2의 OVA 파일에서 수정되었습니다.

Hardware Requirements

Hardware Requirements Not Met
Your current configuration does not meet the hardware requirements.

It is recommended that you shutdown this device and adjust its hardware allocation to meet or exceed the minimum requirements. If you proceed, you may experience system instability.

	Installed	Minimum Required
CPU Cores	4	8
Memory	125 GB	128 GB

Shutdown [I understand the risks >](#)

참고: 실습 용도가 아닌 경우 권장 값만 사용하십시오.

Edit settings - AMP-vPC (ESXi 5.0 virtual machine)

Virtual Hardware | VM Options

Add hard disk | Add network adapter | Add other device

CPU	8		
Memory	131072	MB	It will work with 48Gb as well
Hard disk 1	376.52343	MB	
Hard disk 2	17.272949	GB	
Hard disk 3	1.7216082	TB	
Hard disk 4	4.765625	GB	
SCSI Controller 0	LSI Logic Parallel		
Network Adapter 1	VM Network		<input checked="" type="checkbox"/> Connect
Network Adapter 2	VM Network		<input checked="" type="checkbox"/> Connect
CD/DVD Drive 1	Host device		<input type="checkbox"/> Connect
Video Card	Specify custom settings		

Save | Cancel

리부팅한 후에는 출발한 곳으로 계속 이동합니다.



Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints Console ✓
- > Account ✓
- > Hardware Requirements

Configuration

- > Network
- > Date and Time
- > Certificate Authorities
- > Upstream Proxy Server ✓
- > Cisco Cloud
- > Email ✓
- > Notifications
- > Backup ✓
- > SSH
- > Syslog ✓
- > Updates ✓

Hardware Requirements

✓ Hardware Requirements Met


Your current configuration meets or exceeds the hardware requirements.

Hardware Configuration

	Installed	Minimum Required
CPU Cores	8	8
Memory	125 GB	128 GB

Next >

고정 IP로 ETH1도 구성해야 합니다.

 참고: 인터페이스에 대한 MAC 주소 예약을 생성하지 않은 경우 DHCP를 사용하도록 디바이스를 구성하지 않아야 합니다. 인터페이스의 IP 주소가 변경되면 구축된 Secure Endpoint Connector에 심각한 문제가 발생할 수 있습니다. DNS 서버를 구성하지 않은 경우 공용 DNS 임시를 사용하여 설치를 완료할 수 있습니다.

3단계:

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints Console Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time
- > Certificate Authorities
- > Upstream Proxy Server ✓
- > Cisco Cloud
- > Email ✓
- > Notifications
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication
- > AMP for Endpoints Console
- > Disposition Server
- > Disposition Server
- > Extended Protocol
- > Disposition Update
- > Service
- > Firepower Management Center

Other

- > Recovery
- > Review and Install

▶ Start Installation

Network Configuration

Clicking Next will apply your interface configuration before validating your settings. If using DHCP, a release/renew will be performed to obtain the reserved DHCP lease.

Administration Portal eth0 / 00:0C:29:A6:4A:11

IP Assignment 192.168.75.92 [More details](#)

Interface Configuration eth1 / 00:0C:29:A6:4A:1B

IP Assignment 192.168.75.209 [More details](#)

IP Assignment Static ←

IP Address 192.168.75.93

Check for IP Address conflicts

Subnet Mask 255.255.255.0

Gateway 192.168.75.1

DNS

Primary DNS Server 8.8.8.8 ← Use public DNS temporary.

Secondary DNS Server

Next (Applies Configuration) ▶

4단계:

Date and Time 페이지가 나타납니다. 날짜 및 시간 동기화에 사용할 하나 이상의 NTP 서버의 주소를 입력합니다. 내부 또는 외부 NTP 서버를 사용할 수 있으며 심표 또는 공백으로 구분된 목록을 통해 둘 이상을 지정할 수 있습니다. 시간을 브라우저와 동기화하거나 디바이스 콘솔에서 amp-ctl ntpdate를 실행하여 NTP 서버와의 즉각적인 시간 동기화를 강제합니다. Next(다음)를 선택합니다.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints Console ✓
- > Account ✓
- > Hardware Requirements ✓
- Configuration**
- > Network ✓
- > **Date and Time**
- > Certificate Authorities
- > Upstream Proxy Server ✓
- > Cisco Cloud
- > Email ✓
- > Notifications
- > Backup ✓
- > SSH ✓

Date and Time

NTP Servers HELP

192.168.75.254 Optional Verify hostname resolution

Current System Time

2021 / 4 / 10

8 : 17 . 24 UTC

Set by NTP

Next >

≡ ≡ AIRGAP ONLY ≡ ≡

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > Standalone Operation ✓
- > AMP for Endpoints Console ✓
- > Account ✓
- > Hardware Requirements ✓
- Configuration**
- > Network ✓
- > Date and Time ✓
- > Certificate Authorities
- > Upstream Proxy Server ✓
- > **Prepare amp-sync**
- > Email ✓
- > Notifications
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Prepare amp-sync

You will need to load a snapshot of the Protect DB and retrieve the latest AMP updates from Cisco after your device has finished installing in air gap mode. Cisco provides a shell script called amp-sync that will retrieve the updates and build an ISO file that you can then mount on your AMP device.

It is suggested that you begin the download process now since the initial update is very large.

Download amp-sync Next >

AIRGAP ≡ ≡ 전용 ≡ ≡

5단계:

이미지에 표시된 대로 Certificate Authorities(인증 기관) 페이지가 나타납니다. 루트 인증서를 추가하려면 Add Certificate Authority(인증 기관 추가)에서 선택합니다.

Installation Options

- Only the License section can be altered after installation.
- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints Console ✓
- > Account ✓
- > Hardware Requirements ✓

Certificate Authorities

Add Certificate Authority

No certificate authorities have been uploaded to this device.

Next >

Installation Options

- Only the License section can be altered after installation.
- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints Console ✓
- > Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication ✓
- > AMP for Endpoints Console ✓
- > Disposition Server ✓

Add Certificate Authority

Certificate Root (PEM .crt) Disable Strict TLS Check

- Certificate file has been uploaded.
- Certificate is in a readable format.
- Certificate start and end dates are valid.
- Certificate end date is later than 20 months from today.
- Certificate file only contains one certificate.
- Certificate does not use sha-1 signature algorithm.
- Certificate using RSA keys must use a key size of 2048 or more.

AMP-vPC-Root-CA.pem + Add Certificate Root

Cancel Upload

Installation Options

- Only the License section can be altered after installation.
- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints Console ✓
- > Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓

Certificate Authorities

Add Certificate Authority

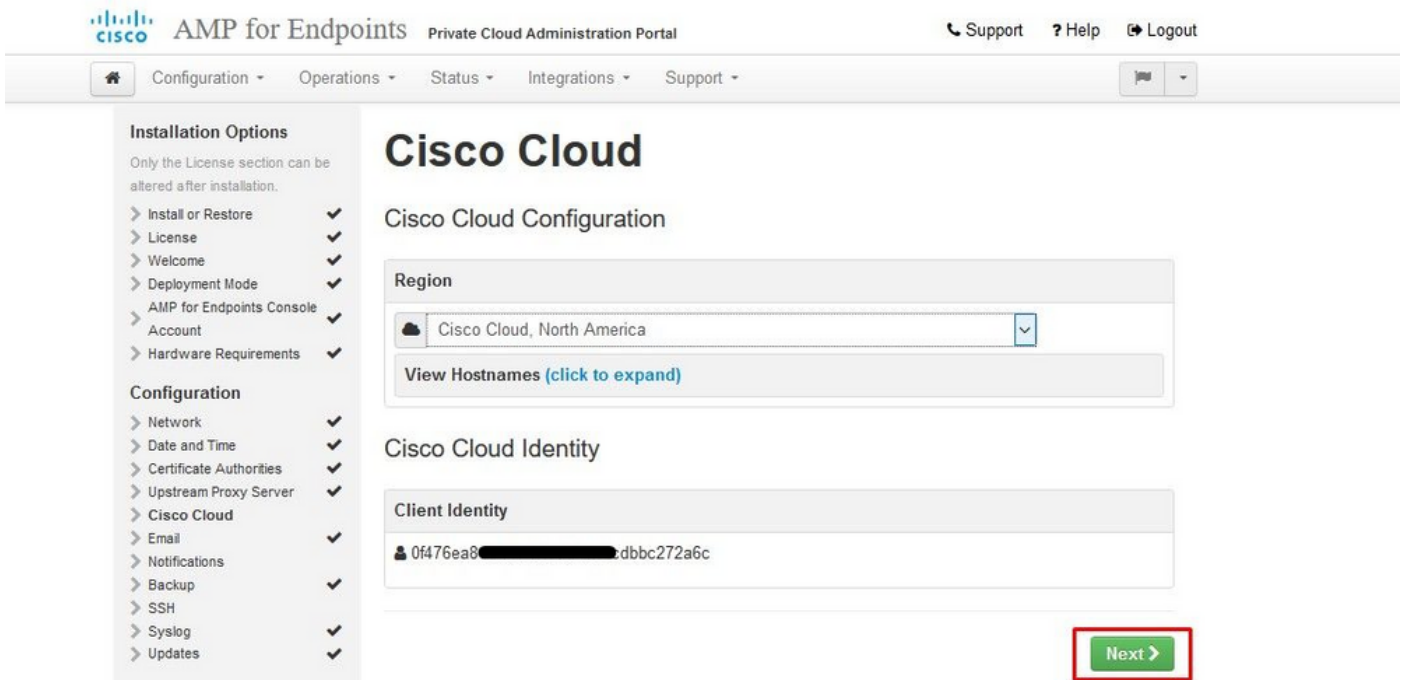
Certificate		(click to collapse)
Issuer	AMP-vPC	Download
Subject	AMP-vPC	
Validity	2021-04-09 16:28:00 UTC - 2031-04-09 16:28:00 UTC	Delete

Next >

6단계:

다음 단계는 그림과 같이 Cisco Cloud 페이지를 구성하는 것입니다. 적절한 Cisco 클라우드 지역을 선택합니다. Secure Endpoint Private Cloud 디바이스가 파일 조회 및 디바이스 업데이트를 위해

Cisco Cloud와 통신하기 위해 방화벽 예외를 생성해야 하는 경우 View Hostnames(호스트 이름 보기)를 확장합니다. Next(다음)에서 선택합니다.



7단계:

이미지에 표시된 대로 알림 페이지로 이동합니다. Critical(중요) 및 Regular Notifications(일반 알림)의 빈도를 선택합니다. 보안 엔드포인트 장치에 대한 알림 알림을 수신할 이메일 주소를 입력합니다. 이메일 별칭을 사용하거나 쉼표로 구분된 목록을 통해 여러 주소를 지정할 수 있습니다. 디바이스에서 사용하는 발신자 이름 및 이메일 주소를 지정할 수도 있습니다. 이러한 알림은 Secure Endpoint Console 서브스크립션과 동일하지 않습니다. 여러 Secure Endpoint Private Cloud 디바이스가 있는 경우 고유한 디바이스 이름을 지정할 수도 있습니다. Next(다음)를 선택합니다.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints Console ✓
- > Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication
- > AMP for Endpoints Console
- > Disposition Server
- > Disposition Server
- > Extended Protocol

Notifications

Notification Frequency

Critical Notification Frequency	HELP	Every 5 Minutes
Notification Frequency	HELP	Every Week

Notification Addresses

Notification Recipients	HELP	rv[REDACTED]om
Notification Sender Address	HELP	donotreply@cisco.com
Notification Sender Name	HELP	AMP for Endpoints Device

Device Name

Device Name	HELP	CyberNet vPC 2
-------------	------	----------------

Next >

8단계:

그런 다음 그림과 같이 SSH Keys 페이지로 이동합니다. Add SSH Key(SSH 키 추가)에서 선택하여 디바이스에 추가할 공개 키를 입력합니다. SSH 키를 사용하면 루트 권한이 있는 원격 셸을 통해 디바이스에 액세스할 수 있습니다. 신뢰할 수 있는 사용자만 액세스 권한을 부여해야 합니다. 프라이빗 클라우드 디바이스에는 OpenSSH 형식의 RSA 키가 필요합니다. 나중에 관리 포털의 Configuration(컨피그레이션) > SSH를 통해 SSH 키를 더 추가할 수 있습니다. Next(다음)에서 선택합니다.

Maintenance Mode

Sanity Check Failing

This page allows you to add and remove SSH keys on your Cisco AMP for Endpoints Private Cloud device. SSH keys allow administrators remote root authentication to the device. Only trusted users should be granted access.

Add SSH Key

Windows PuTTY

2021-11-17 23:01:01 +0000
created 20 days ago

2021-11-17 23:01:01 +0000
20 days since last update

Edit

```
ecdsa-sha2-nistp256 AAAAE2K...oeCAvfEzyIea9PbgwnlB9DjTeJgFXtR7Q6fd0g4vT9eD5XOXZd
I4DKhrTNBv8/77T0d/Jagx7Przxs=
```

다음은 서비스 섹션입니다. 다음 페이지에서 호스트 이름을 지정하고 이러한 디바이스 서비스에 적합한 인증서 및 키 쌍을 업로드해야 합니다. 다음 몇 슬라이드에서는 6개 인증서 중 하나의 컨피그레이션을 볼 수 있습니다.

Services

1단계:

컨피그레이션 프로세스 중에 이러한 오류가 발생할 수 있습니다.

첫 번째 "오류"가 3개의 화살표로 강조 표시됩니다. 이를 우회하려면 "Disable Strict TLS Check(엄격한 TLS 확인 비활성화)"를 선택 취소하면 됩니다.

Installation Options
Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints ✓
- > Console Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > **Authentication**
- > AMP for Endpoints
- > Console
- > Disposition Server
- > Disposition Server
- > Extended Protocol
- > Disposition Update
- > Service
- > Firepower Management Center

Other

- > Recovery
- > Review and Install

[▶ Start Installation](#)

Authentication Configuration

Authentication Hostname HELP

vPC2-Authentication.cyberworld.local Validate DNS Name

Authentication Certificate Disable Strict TLS Check Undo Replace Certificate

Certificate (PEM .crt)	Key (PEM .key)
<input checked="" type="checkbox"/> Certificate file has been uploaded.	<input checked="" type="checkbox"/> Key file has been uploaded.
<input checked="" type="checkbox"/> Certificate is in a readable format.	<input checked="" type="checkbox"/> Key contains a supported key type.
<input checked="" type="checkbox"/> Certificate start and end dates are valid.	<input checked="" type="checkbox"/> Key contains public key material.
<input checked="" type="checkbox"/> Certificate contains a subject.	<input checked="" type="checkbox"/> Key contains private key material.
<input checked="" type="checkbox"/> Certificate contains a common name.	<input checked="" type="checkbox"/> Key contains a public key matching the uploaded certificate.
<input checked="" type="checkbox"/> Certificate contains a public key matching the uploaded key.	
<input checked="" type="checkbox"/> Certificate matches hostname.	
<input checked="" type="checkbox"/> Certificate is signed by a trusted root authority.	
<input checked="" type="checkbox"/> Certificate issued after 07/01/2019 must have a validity period of 825 days or less.	
<input checked="" type="checkbox"/> Certificate issued after 09/01/2020 must have a validity period of 398 days or less.	
<input checked="" type="checkbox"/> Certificate does not use sha-1 signature algorithm.	
<input checked="" type="checkbox"/> Certificate using RSA keys must use a key size of 2048 or more.	
<input checked="" type="checkbox"/> Certificate must specify server certificate in Extended Key Usage extension.	

vPC2-Authenticator + Choose Key

vPC2-Authenticator + Choose Certificate

[Next >](#)

엄격한 TLS 확인 안 함

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints Console ✓
- > Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > **Authentication** ←
- > AMP for Endpoints Console
- > Disposition Server
- > Disposition Server
- > Extended Protocol
- > Disposition Update
- > Service
- > Firepower Management Center

Other

- > Recovery
- > Review and install

▶ Start Installation

Authentication Configuration

Authentication Hostname

vPC2-Authentication.cyberworld.local Validate DNS Name

Authentication Certificate

Disable Strict TLS Check Undo Replace Certificate

Certificate (PEM .crt)	Key (PEM .key)
<input checked="" type="checkbox"/> Certificate file has been uploaded.	<input checked="" type="checkbox"/> Key file has been uploaded.
<input checked="" type="checkbox"/> Certificate is in a readable format.	<input checked="" type="checkbox"/> Key contains a supported key type.
<input checked="" type="checkbox"/> Certificate start and end dates are valid.	<input checked="" type="checkbox"/> Key contains public key material.
<input checked="" type="checkbox"/> Certificate contains a subject.	<input checked="" type="checkbox"/> Key contains private key material.
<input checked="" type="checkbox"/> Certificate contains a common name.	<input checked="" type="checkbox"/> Key contains a public key matching the uploaded certificate.
<input checked="" type="checkbox"/> Certificate contains a public key matching the uploaded key.	vPC2-Authenticac + Choose Key
<input checked="" type="checkbox"/> Certificate matches hostname.	vPC2-Authentication.cyberworld.local.pem
<input checked="" type="checkbox"/> Certificate is signed by a trusted root authority.	
vPC2-Authenticac + Choose Certificate	vPC2-Authentication.cyberworld.local.crt

Next >

2단계:

"DNS 이름 검증"을 선택한 상태로 두면 다음 오류가 발생합니다. 여기 두 가지 선택이 있습니다.

#1: Validate DNS(DNS 검증) 확인 표시를 선택 취소합니다.

#2: DNS 서버로 돌아가 나머지 호스트 레코드를 구성합니다.

An error occurred while processing your request.

- Hostname does not resolve

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints ✓
- > Console Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication
- > AMP for Endpoints
- > Console
- > Disposition Server
- > Disposition Server
- > Extended Protocol
- > Disposition Update
- > Service
- > Firepower Management Center

Other

- > Recovery
- > Review and Install

▶ Start Installation

Authentication Configuration

Authentication Hostname HELP

vPC2-Authentication.cyberworld.local Validate DNS Name

Authentication Certificate Disable Strict TLS Check Undo Replace Certificate

Certificate (PEM .crt)	Key (PEM .key)
<input checked="" type="checkbox"/> Certificate file has been uploaded.	<input checked="" type="checkbox"/> Key file has been uploaded.
<input checked="" type="checkbox"/> Certificate is in a readable format.	<input checked="" type="checkbox"/> Key contains a supported key type.
<input checked="" type="checkbox"/> Certificate start and end dates are valid.	<input checked="" type="checkbox"/> Key contains public key material.
<input checked="" type="checkbox"/> Certificate contains a subject.	<input checked="" type="checkbox"/> Key contains private key material.
<input checked="" type="checkbox"/> Certificate contains a common name.	<input checked="" type="checkbox"/> Key contains a public key matching the uploaded certificate.
<input checked="" type="checkbox"/> Certificate contains a public key matching the uploaded key.	<input type="text"/> + Choose Key
<input checked="" type="checkbox"/> Certificate matches hostname.	
<input checked="" type="checkbox"/> Certificate is signed by a trusted root authority.	
<input type="text"/> + Choose Certificate	

Next >

이제 나머지 인증서에 대해 동일한 프로세스를 5번 더 반복합니다.

인증

- 인증 서비스는 향후 버전의 Private Cloud에서 사용자 인증을 처리하는 데 사용할 수 있습니다.

보안 엔드포인트 콘솔

- Console은 보안 엔드포인트 관리자가 보안 엔드포인트 콘솔에 액세스하고 보안 엔드포인트 커넥터가 새 정책 및 업데이트를 받을 수 있는 DNS 이름입니다.

서버 분류

- Disposition Server는 Secure Endpoint Connector에서 클라우드 조회 정보를 보내고 검색하는 DNS 이름입니다.

Disposition Server - 확장 프로토콜


- Disposition Server - Extended Protocol은 새로운 Secure Endpoint Connector가 클라우드 조회 정보를 보내고 검색하는 DNS 이름입니다.

속성 업데이트 서비스

- Disposition Update Service는 Cisco Threat Grid 어플라이언스를 프라이빗 클라우드 디바이스에 연결할 때 사용합니다. Threat Grid 어플라이언스는 Secure Endpoint Console에서 분석할 파일을 전송하는 데 사용되며, Threat Grid에서는 분석된 파일의 성향(정상 또는 악성)을 업데이트하는 데 성향 업데이트 서비스를 사용합니다.

Firepower 관리 센터

-Firepower Management Center 링크를 사용하면 Cisco FMC(Firepower Management Center) 디바이스를 프라이빗 클라우드 디바이스에 연결할 수 있습니다. 이렇게 하면 FMC 대시보드에 보안 엔드포인트 데이터를 표시할 수 있습니다. FMC와 Secure Endpoint의 통합에 대한 자세한 내용은 FMC 설명서를 참조하십시오.

 주의: 디바이스가 설치를 완료한 후에는 호스트 이름을 변경할 수 없습니다.

필요한 호스트 이름을 기록해 둡니다. Secure Endpoint Private Cloud에 대해 6개의 고유한 DNS A 레코드를 생성해야 합니다. 각 레코드는 Virtual Private Cloud Console 인터페이스(eth1)의 동일한 IP 주소를 가리키며 Private Cloud 및 Secure Endpoint에서 모두 확인해야 합니다.

3단계:

다음 페이지에서 복구 파일을 다운로드한 다음 확인합니다.

이미지에 표시된 대로 복구 페이지가 나타납니다. 설치를 시작하기 전에 컨피그레이션의 백업을 다운로드하고 확인해야 합니다. 복구 파일에는 모든 컨피그레이션과 서버 키가 포함되어 있습니다. 복구 파일이 손실되면 컨피그레이션을 복원할 수 없으며 모든 Secure Endpoint 커넥터를 다시 설치해야 합니다. 원래 키가 없으면 전체 프라이빗 클라우드 인프라를 새 키로 재구성해야 합니다. 복구 파일에는 opadmin 포털과 관련된 모든 컨피그레이션이 포함되어 있습니다. 백업 파일에는 복구 파일의 내용은 물론 이벤트, 커넥터 기록 등과 같은 대시보드 포털 데이터가 포함됩니다. 이벤트 데이터 및 모두 없이 opadmin만 복원하려는 경우 복구 파일을 사용할 수 있습니다. 백업 파일에서 복원하는 경우 opadmin 및 대시보드 포털 데이터가 복원됩니다.

로컬 컴퓨터에 백업을 저장하려면 Download(다운로드)를 선택합니다. 파일이 다운로드되면 Choose File(파일 선택)을 선택하여 백업 파일을 업로드하고 손상되지 않았는지 확인합니다. 다음을 선택하여 파일을 확인하고 진행합니다.

- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓
- Services**
- > Authentication ✓
- > AMP for Endpoints ✓
- > Console ✓
- > Disposition Server ✓
- > Disposition Server ✓
- > Extended Protocol ✓
- > Disposition Update ✓
- > Service ✓
- > Firepower Management Center ✓

1. Download Recovery File

Please keep a copy of this file in a safe place.

[Download](#)

2. Verify Recovery File

After downloading your backup, upload it to the device to verify that you have a matching copy.

[Browse...](#) pre-install-backup.bak

Recovery File Ready for Download
created less than a minute ago

[Next >](#)



Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints ✓
- > Console Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication ✓
- > AMP for Endpoints ✓
- > Console ✓
- > Disposition Server ✓
- > Disposition Server ✓
- > Extended Protocol ✓
- > Disposition Update ✓
- > Service ✓
- > Firepower Management Center ✓

Other

- > Recovery ✓
- > Review and Install ✓

[▶ Start Installation](#)

Review and Install

Review the following information and, once you are satisfied with your configuration settings, begin the installation. Note that the configuration shown below cannot be altered after installation.

Clean Installation

A clean installation will be performed.

Installation Type

[Edit](#)

Cloud Proxy

- Requires an Internet connection and communication with AMP for Endpoints Connectors managed by this device.
- Disposition queries are proxied to the Cisco Cloud.
- Content updates contain TETRA definitions.
- Content and software updates can be retrieved and applied automatically.

AMP for Endpoints Console Account

[Edit](#)

Name	Roman Valenta
Email Address	rva[REDACTED].com
Business Name	Cisco - rvalenta

Recovery

[Edit](#)

Uploaded Recovery File Matches Current Settings

[▶ Start Installation](#)

≡ ≡ AIRGAP ONLY ≡ ≡

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > Standalone Operation ✓
- > AMP for Endpoints Console Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Prepare amp-sync ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication ✓
- > AMP for Endpoints Console ✓
- > Disposition Server ✓
- > Disposition Server ✓
- > Extended Protocol ✓
- > Disposition Update ✓
- > Service ✓
- > Firepower Management Center ✓

Other

- > Recovery ✓
- > Review and Install ✓

▶ Start Installation

Review and Install

Review the following information and, once you are satisfied with your configuration settings, begin the installation. Note that the configuration shown below cannot be altered after installation.

Clean Installation

A clean installation will be performed.

Installation Type Edit

Standalone Air Gap ←

- Does not require an Internet Connection
- Communication with AMP for Endpoints Connectors managed by this device are needed.
- Disposition queries are handled by the Private Cloud device.
- Content updates contain TETRA definitions as well as file disposition information.
- Updates must be downloaded separately and applied to this Private Cloud device.

AMP for Endpoints Console Account Edit

Name	Roman Valenta
Email Address	rvalenta@...m
Business Name	Cisco vamrodia PC v2

Recovery Edit

Uploaded Recovery File Matches Current Settings

▶ Start Installation

AIRGAP ≪ ≪ 전용 ≪ ≪

이와 비슷한 입력이 보입니다.

주의: 이 페이지에서는 문제가 발생할 수 있으므로 새로 고치지 마십시오.

The device is installing...

Please wait for this page to redirect you. Refreshing manually might cause problems. Installation time is typically under 20 minutes.

State	Started	Finished	Duration
▶ Running	Sat Apr 10 2021 13:36:08 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 0 minute, 14 seconds ago	⌚ Please wait...	⌚ Please wait...

Your device will need to be rebooted after this operation.

Reboot

☰ Output

```
le_chunk
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP::StreamHandler calling Chef::HTTP::Decompressor::NoopInflater#handle_chunk
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::Decompressor#handle_request
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::Authenticator#handle_request
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::RemoteRequestID#handle_request
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::ValidateContentLength#handle_request
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::ValidateContentLength#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: HTTP server did not include a Content-Length header in response, cannot identify truncated downloads.
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::RemoteRequestID#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::Authenticator#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::Decompressor#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::CookieManager#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::JSONOutput#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::JSONInput#handle_stream_complete
[2021-04-10T17:36:20+00:00] INFO: Storing updated cookbooks/rabbitmq/recipes/default.rb in the cache.
[2021-04-10T17:36:20+00:00] DEBUG: Creating directory /var/run/cookbooks/rabbitmq/recipes
```

⬇ Download Output

설치가 완료되면 재부팅 버튼을 누릅니다

The device is installing...

Please wait for this page to redirect you. Refreshing manually might cause problems. Installation time is typically under 20 minutes.

State	Started	Finished	Duration
✓ Successful	Sat Apr 10 2021 13:36:08 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 24 minutes, 14 seconds ago	Sat Apr 10 2021 13:57:05 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 3 minutes, 17 seconds ago	0 day, 0 hour, 20 minutes, 57 seconds

Your device will need to be rebooted after this operation.

Reboot

Output

```
[2021-04-10T17:57:04+00:00] INFO: Running report handlers
[2021-04-10T17:57:04+00:00] INFO: Report handlers complete
[2021-04-10T17:57:04+00:00] DEBUG: Server doesn't support resource history, skipping resource report.
[2021-04-10T17:57:04+00:00] DEBUG: Audit Reports are disabled. Skipping sending reports.
[2021-04-10T17:57:04+00:00] DEBUG: Forked instance successfully reaped (pid: 2552)
[2021-04-10T17:57:04+00:00] DEBUG: Exiting
Sending system notification (this may take some time).
Running retryable command, 40 retries remaining.
=====
Chef run finished successfully
=====
Registration against the AMP for Endpoints Disposition Server has previously succeeded.

=====
Installation has finished successfully! Please reboot!
=====
```

Download Output

≡ ≡ AIRGAP ONLY ≡ ≡

The device is installing...

Please wait for this page to redirect you. Refreshing manually might cause problems. Installation time is typically under 20 minutes.

State	Started	Finished	Duration
✓ Successful	Tue Nov 02 2021 14:46:30 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 21 minutes, 21 seconds ago	Tue Nov 02 2021 15:07:02 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 0 minute, 49 seconds ago	0 day, 0 hour, 20 minutes, 32 seconds

Your device will need to be rebooted after this operation.

Reboot

Output

```
[2021-11-02T19:07:01+00:00] INFO: Running report handlers
[2021-11-02T19:07:01+00:00] INFO: Report handlers complete
[2021-11-02T19:07:01+00:00] DEBUG: Server doesn't support resource history, skipping resource report.
[2021-11-02T19:07:01+00:00] DEBUG: Audit Reports are disabled. Skipping sending reports.
[2021-11-02T19:07:01+00:00] DEBUG: Forked instance successfully reaped (pid: 29292)
[2021-11-02T19:07:01+00:00] DEBUG: Exiting
Sending system notification (this may take some time).
Running retryable command, 40 retries remaining.
=====
Chef run finished successfully
=====
Registration is not possible in air gap mode.
=====
Installation has finished successfully! Please reboot!
=====
```

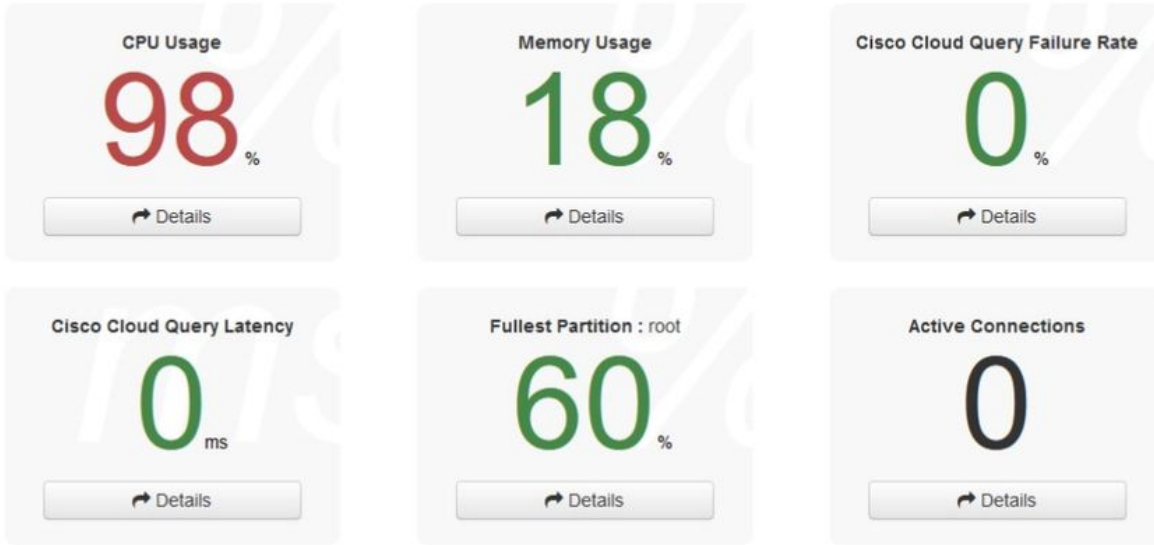
Download Output

AIRGAP ≪ ≪ 전용 ≫ ≫

어플라이언스가 완전히 부팅되면 다음에 관리자 인터페이스로 로그인하면 이 대시보드가 표시됩니다. 처음에는 CPU가 높지만 몇 분 정도 기다리면 안정됩니다.



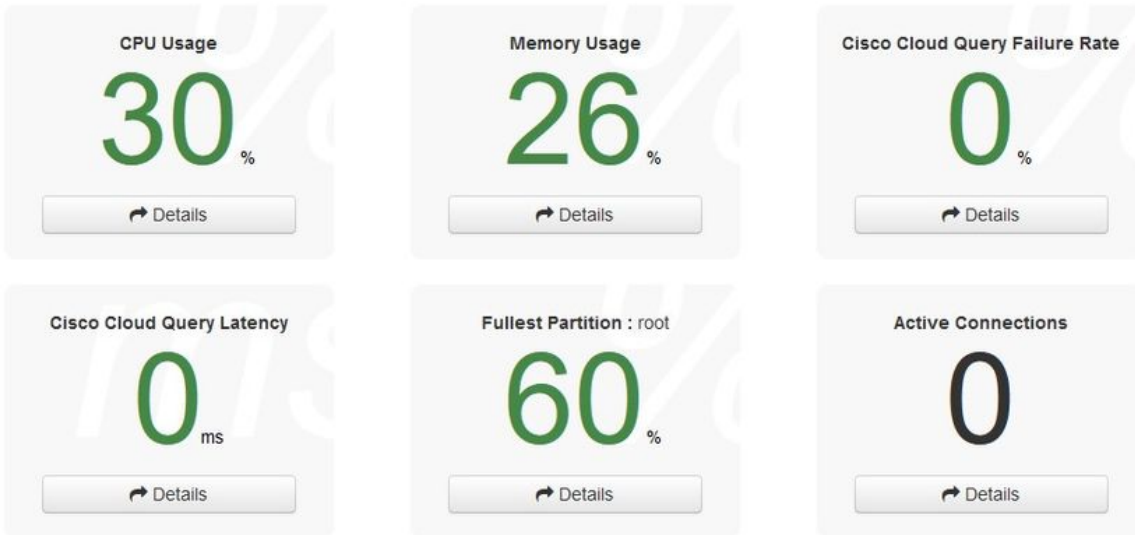
Key Metrics



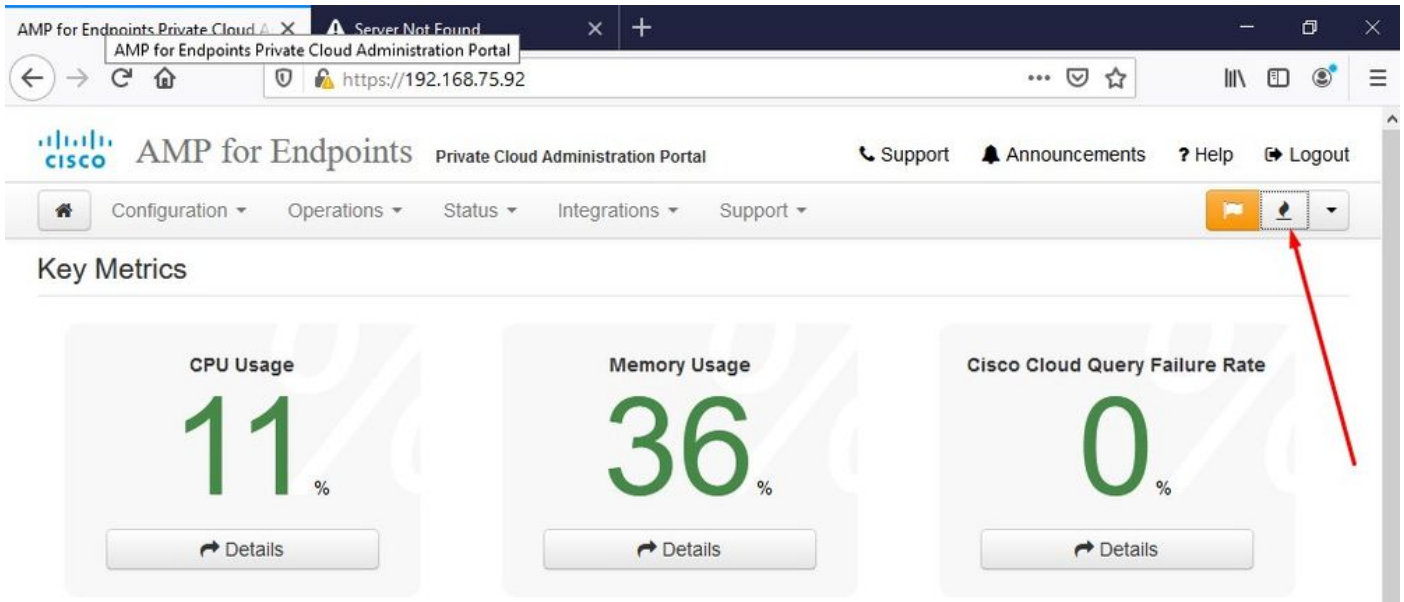
몇 분 후...



Key Metrics



여기에서 Secure Endpoint(보안 엔드포인트) 콘솔로 이동합니다. 깃발 옆에 있는 오른쪽 구석에 볼 처럼 보이는 작은 아이콘을 클릭합니다.



≡ ≡ AIRGAP ONLY ≡ ≡

보시다시피, DB 보호 스냅샷, 클라이언트 정의, DFC 및 Tetra로 인해 온전성 검사에 실패했습니다. 이는 이전에 amp-sync를 통해 준비되고 VM에 업로드되거나 NFS 위치에 저장된 다운로드된 ISO 파일을 통한 오프라인 업데이트를 통해 수행해야 합니다.



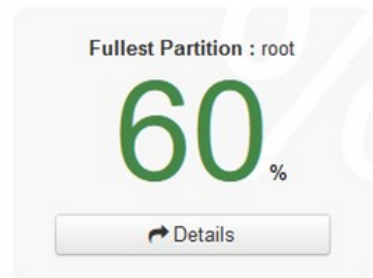
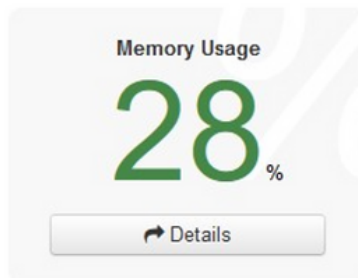
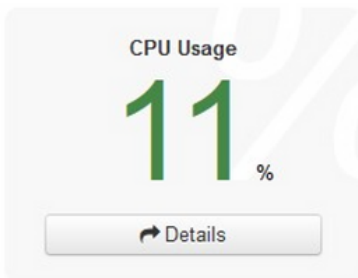
Sanity Check Failing

The device `sanity_check` is failing; your device might not function properly until corrective measures are taken.

Details

FAIL: A Protect DB snapshot has not been loaded. Devices configured in standalone mode should have a Protect DB snapshot loaded. Protect DB snapshots contain threat intelligence about known clean and known malicious files.

Key Metrics





Sanity Check Failing

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

There is no ISO loaded. Load an ISO and try again.

Content

3.2.0_202010081917

Client Definitions, DFC, Tetra Content Version

Update Content

Import Protect DB

ABSENT

Protect DB Version

Import a Protect DB snapshot to your standalone device.

Checked 1 minute ago; the update check failed.

Software

3.2.0_202010082118

Private Cloud Software Version

Update Software

Checked 1 minute ago; the update check failed.

AirGap 업데이트 패키지

처음으로 보호 DB를 받으려면 이 명령을 사용해야 합니다

```
./amp-sync all
```

참고: 이 명령을 통해 모든 패키지를 다운로드한 다음 확인하면 24시간 이상 걸릴 수 있습니다. 속도와 링크 품질에 따라 다릅니다. 1Gig 파이버의 경우 완료하는 데 거의 25시간이 소요됩니다. 부분적으로는 이 다운로드가 AWS에서 직접 다운로드되어 제한되기 때문이기도 합니다. 마지막으로, 이 다운로드는 상당히 큼니다. 제 경우에는 다운로드한 파일이 323GB였습니다.

이 예에서는 CygWin64를 사용했습니다.

1. Cygwin x64 버전을 다운로드하여 설치합니다.
2. setup-x86_64.exe를 실행하고 설치 프로세스를 통해 모든 기본값을 선택합니다.
3. 다운로드 미러를 선택합니다.
4. 설치할 패키지 선택:
모두 -> 네트 -> 컬

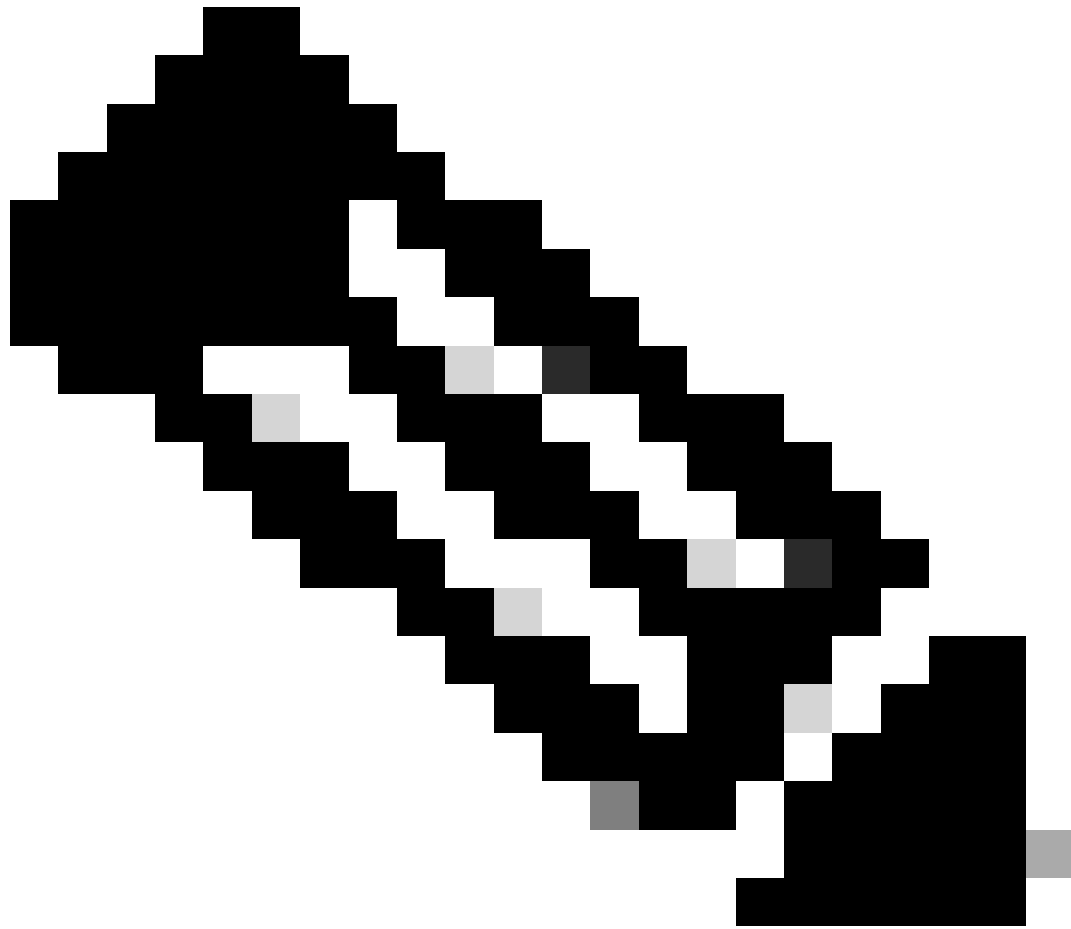
모두 -> 유틸리티 -> genisoimage

모두 -> 유틸리티 -> xmlstarlet

* VPC 3.8.x up -> xorriso

```
User@VMStation-1 ~
$ ./amp-sync all
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/MOTD
No MOTD for today, nothing to download. Continuing...
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/MOTD-AmpSync-1.0.7
No MOTD for today, nothing to download. Continuing...
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/MOTD-AmpSync-1.0.7-prod
No MOTD for today, nothing to download. Continuing...
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/repomd.xml
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 2991 100 2991 0 0 15991 0 --:--:-- --:--:-- --:--:-- 16167
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/0813e87ac364885e8a82aa3b568226cdfdff10d0bb1cb240875ee43a89240ea0-other.sqlite.bz2
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 11331 100 11331 0 0 98544 0 --:--:-- --:--:-- --:--:-- 97k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/0813e87ac364885e8a82aa3b568226cdfdff10d0bb1cb240875ee43a89240ea0-other.sqlite.bz2
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/22f49a7fe81b71ee153be870c7f6d20c9238a89c7d7e277956bbccb2c2f41d8-filelists.xml.gz
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 915k 100 915k 0 0 3324k 0 --:--:-- --:--:-- --:--:-- 3342k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/22f49a7fe81b71ee153be870c7f6d20c9238a89c7d7e277956bbccb2c2f41d8-filelists.xml.gz
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/691eabb8ceb5473093376c1a6312ed1e3cd6593fd1df2af1e3b3dbe472d84ff9-filelists.sqlite.bz2
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 1094k 100 1094k 0 0 3302k 0 --:--:~ --:--:~ --:--:~ 3317k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/691eabb8ceb5473093376c1a6312ed1e3cd6593fd1df2af1e3b3dbe472d84ff9-filelists.sqlite.bz2
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/e4e3c4029829b3a3b02751f61af15f36561a8aac1ea7b1af66101d0eab569014-primary.sqlite.bz2
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 135k 100 135k 0 0 747k 0 --:--:~ --:--:~ --:--:~ 756k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/e4e3c4029829b3a3b02751f61af15f36561a8aac1ea7b1af66101d0eab569014-primary.sqlite.bz2
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/e6f73d52fc5079064aff7178401579a8de6259f8ac91b1e5e913cdb47ff069-primary.xml.gz
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 54480 100 54480 0 0 383k 0 --:--:~ --:--:~ --:--:~ 383k
```

```
User@VMStation-1 ~
99.91% done, estimate finish Thu Nov 4 08:39:50 2021
99.91% done, estimate finish Thu Nov 4 08:39:51 2021
99.92% done, estimate finish Thu Nov 4 08:39:50 2021
99.92% done, estimate finish Thu Nov 4 08:39:50 2021
99.92% done, estimate finish Thu Nov 4 08:39:51 2021
99.93% done, estimate finish Thu Nov 4 08:39:50 2021
99.93% done, estimate finish Thu Nov 4 08:39:50 2021
99.93% done, estimate finish Thu Nov 4 08:39:51 2021
99.93% done, estimate finish Thu Nov 4 08:39:50 2021
99.94% done, estimate finish Thu Nov 4 08:39:50 2021
99.94% done, estimate finish Thu Nov 4 08:39:51 2021
99.94% done, estimate finish Thu Nov 4 08:39:50 2021
99.95% done, estimate finish Thu Nov 4 08:39:50 2021
99.95% done, estimate finish Thu Nov 4 08:39:51 2021
99.95% done, estimate finish Thu Nov 4 08:39:50 2021
99.96% done, estimate finish Thu Nov 4 08:39:50 2021
99.96% done, estimate finish Thu Nov 4 08:39:51 2021
99.96% done, estimate finish Thu Nov 4 08:39:51 2021
99.97% done, estimate finish Thu Nov 4 08:39:51 2021
99.97% done, estimate finish Thu Nov 4 08:39:52 2021
99.97% done, estimate finish Thu Nov 4 08:39:51 2021
99.98% done, estimate finish Thu Nov 4 08:39:51 2021
99.98% done, estimate finish Thu Nov 4 08:39:52 2021
99.98% done, estimate finish Thu Nov 4 08:39:52 2021
99.99% done, estimate finish Thu Nov 4 08:39:52 2021
99.99% done, estimate finish Thu Nov 4 08:39:52 2021
99.99% done, estimate finish Thu Nov 4 08:39:52 2021
99.99% done, estimate finish Thu Nov 4 08:39:52 2021
100.00% done, estimate finish Thu Nov 4 08:39:52 2021
Total translation table size: 0
Total rockridge attributes bytes: 345811
Total directory bytes: 512364
Path table size(bytes): 148
Max brk space used 2f0000
157803265 extents written (308209 MB)
Package successful: PrivateCloud-3.2.0-Updates-2021-11-03-prod.iso
User@VMStation-1 ~
$
```



참고: CygWin64를 기본 다운로드 도구로 사용하는 최신 업데이트 VPC 3.8.x에서는 아래에 설명된 이 문제가 발생할 수 있습니다.

```
User@VMStation-1 ~
$ ./amp-sync all

=====
Prerequisite Program(s) Missing
=====

A prerequisite tool was not found in your PATH, or is not an appropriate
version. You must have the following tools installed in order for the AMP for En
dpoints
Air-Gap Update Tool to function:

    awk
    base64
    basename
    cat
    comm
    curl
    dirname
    mv
MISSING -> xorriso
            sha256 / sha256sum / shasum
            sort
            tr
            xmlstarlet

These tools should be available in both Windows Subsystem for Linux and most
Unix-like operating systems.
```

[릴리스 정보](#) 페이지 #58. 보시다시피 "xorriso"가 필요합니다. ISO의 형식을 ISO 9660으로 변경했으며, 이 종속성은 이미지를 적절한 형식으로 변환하여 업데이트를 완료할 수 있도록 하는 것입니다. 안타깝게도 CygWin64는 내장된 저장소에는 xorriso를 제공하지 않습니다. 그러나 여전히 CygWin64를 사용하려는 사용자에게는 이 문제를 극복할 수 있는 방법이 있습니다.

Installing dependencies

CentOS

To run amp-sync you will first have to install EPEL, xorriso, and xmlstarlet.

1. Enable the EPEL repo.
 - > `sudo yum install epel-release`
2. Install dependencies via yum.
 - > `sudo yum install xorriso`
 - > `sudo yum install xmlstarlet`

Ubuntu

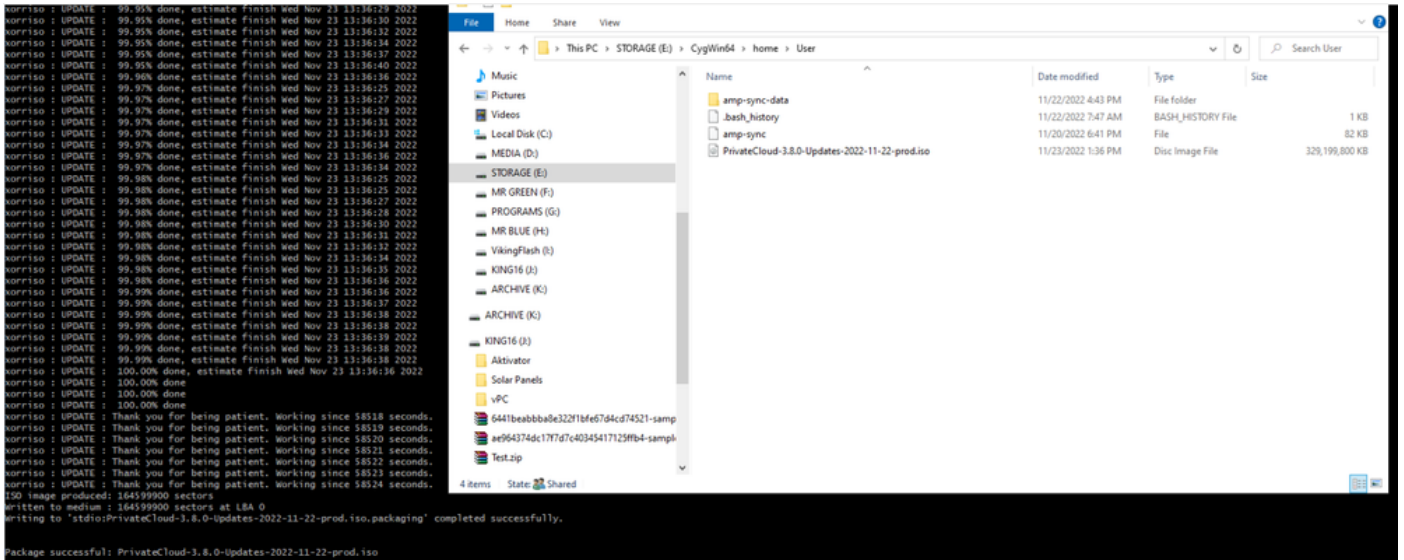
To run amp-sync you will first have to install xorriso and xmlstarlet.

- Install dependencies via apt.
 - > `sudo apt install xorriso`
 - > `sudo apt install xmlstarlet`

Windows

1. Set up Windows Subsystem for Linux (WSL) with the Ubuntu distribution. See the [Microsoft documentation](#) for details.
2. Expand the WSL virtual hard disk size to comply with minimum free disk space. See the [Microsoft documentation](#) for details.
3. Install xorriso and xmlstarlet dependencies via apt.
 - > `sudo apt install xorriso`
 - > `sudo apt install xmlstarlet`

CygWin을 다시 사용하려면 GitHub 리포지토리에서 xorriso를 수동으로 다운로드해야 합니다. 브라우저 열고 <Latest xorriso.exe 1.5.2 pre-build for Windows>를 입력하면 <PeyTy/xorriso-exe-for-windows - GitHub>라는 이름의 첫 번째 링크가 나타나며 해당 GitHub 페이지로 이동하여 <xorriso-exe-for-windows-master.zip> 파일을 zip 파일 내에 다운로드합니다. <xorriso.exe-for-windows-master.zip>이라는 다른 파일 중에서 이 파일을 <CygWin64\bin>에 복사하고 붙여넣습니다. <amp-sync> 명령을 다시 실행하십시오. 그림과 같이 더 이상 오류 메시지가 표시되지 않고 시작 및 완료 다운로드를 다운로드해야 합니다.



Airgap Mode에서 현재(이 경우) 3.2.0 VPC의 백업을 수행합니다.

CLI에서 이 명령을 사용할 수 있습니다

```
rpm -qa | grep Pri
```

또는 이미지에 표시된 대로 Operations(작업) > Backups(백업)로 이동하고 Perform Backup(백업 수행)으로 이동할 수도 있습니다.



Sanity Check Failing

Backups create a copy of your configuration and databases.

Manual Backup

Perform Backup

Last Backup Successful

Transferring Backups To External Storage Is Recommended

To facilitate disaster recovery, you are strongly encouraged to transfer backup archives to a secure external backup location. Transfer of backup archives can be performed via download, sftp, or rsync.

Backup Job Details

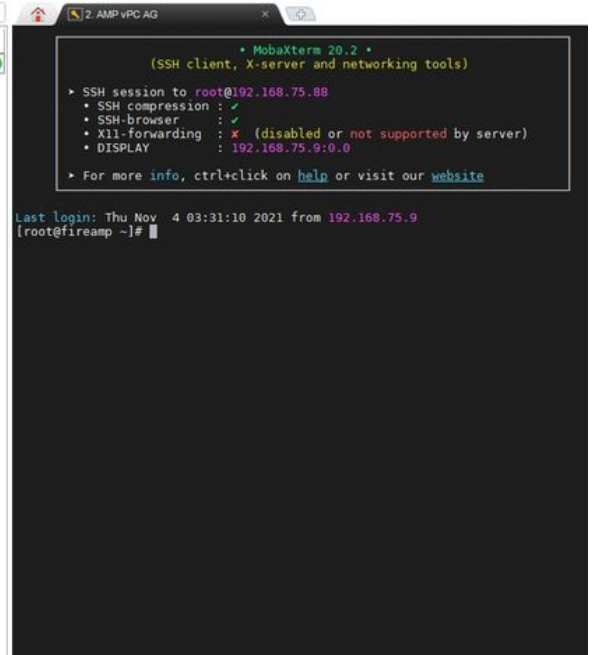
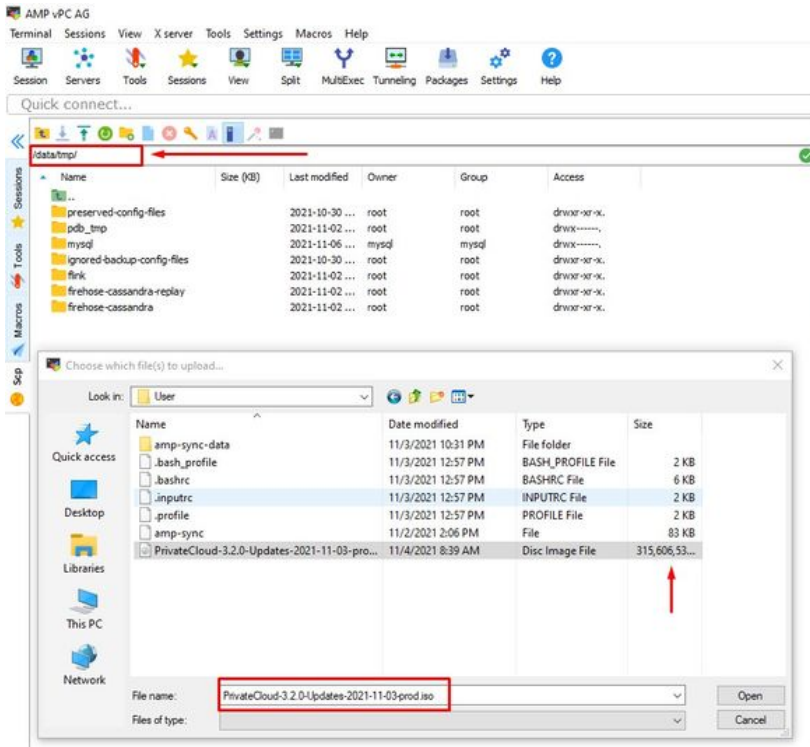
Previous Backups

The number of backups that will be stored on disk is: 1.

Name	Size	Timestamp	Operations
/data/backups/amp-backup-20211106-0000.18.bak	738 MB	2021-11-06 00:03:43 +0000 about 17 hours ago	

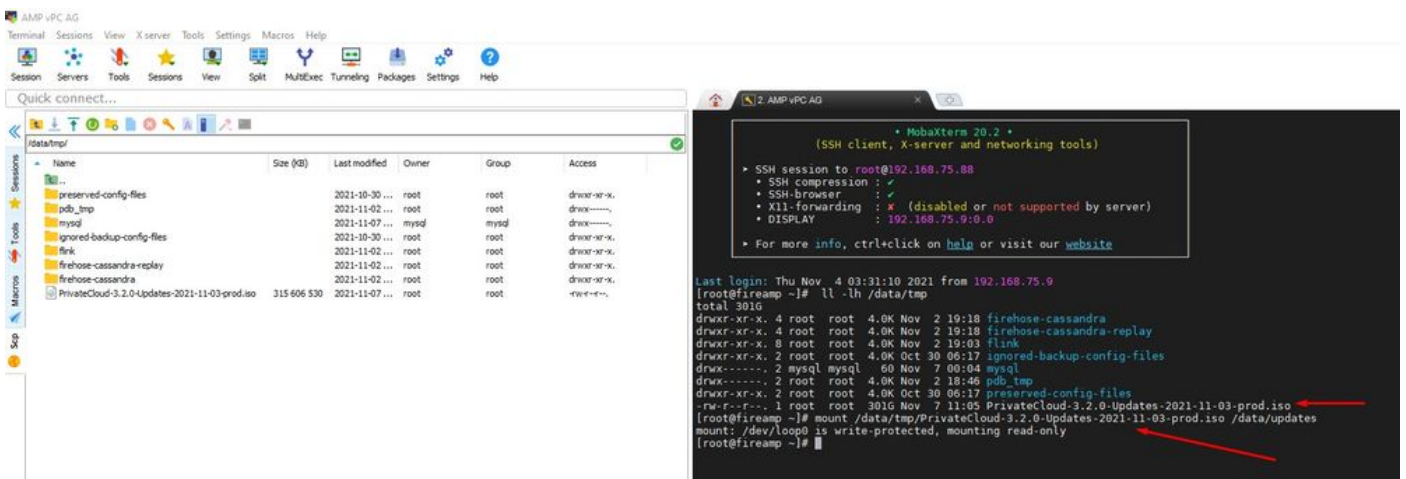
amp-sync로 생성된 최신 ISO를 VPC에 전송합니다. 이 작업에는 사용자의 속도에 따라 최대 몇 시간이 걸릴 수도 있습니다. 이 경우 16시간이 넘게 전송되었습니다.

/data/tmp



업로드가 완료되면 ISO를 마운트합니다.

`mount /data/tmp/PrivateCloud-3.2.0-Updates-2021-11-03-prod.iso /data/updates/`



업데이트를 수행하려면 `opdamin` UI로 이동합니다. Operations(운영) > Update Device(디바이스 업

데이트) > Check update ISO(ISO 업데이트 확인)를 선택합니다.

The screenshot displays the Cisco AMP for Endpoints Private Cloud Administration Portal. At the top, there is a navigation bar with the Cisco logo, 'AMP for Endpoints', and 'Private Cloud Administration Portal'. On the right, there are links for 'Announcements', 'Help', and 'Logout'. Below the navigation bar, there are tabs for 'Configuration', 'Operations', 'Status', 'Integrations', and 'Support'. A 'Sanity Check Failing' notification is visible in a red box. The main content area features a 'Check Update ISO' button, which is highlighted with a red arrow. Below this, there is a 'Checking ISO for updates...' status indicator. The 'Content' section shows a version '3.2.0_202010081917' with a status of 'ABSENT' and a message 'Import a Protect DB snapshot to your standalone device.' There are buttons for 'Update Content' and 'Import Protect DB'. The 'Software' section shows a version '3.2.0_202010082118' with a message 'A software update is available.' and a button for 'Update Software'.

이 예제에서는 먼저 콘텐츠 업데이트를 진행합니다.

Sanity Check Failing

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

Content

3.2.0_202010081917
Client Definitions, DFC, Tetra Content Version

Update Content

Import Protect DB

ABSENT
Protect DB Version

A content update is available.

ISO contains Protect DB snapshot version 20210531-0613.
Import a Protect DB snapshot to your standalone device.

Software

3.2.0_202010082118
Private Cloud Software Version

Update Software

A software update is available.

그런 다음 Import Protect DB(보호 DB 가져오기)를 선택합니다.

Sanity Check Failing

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

Content

20211102210054
Client Definitions, DFC, Tetra Content Version

Update Content
Import Protect DB

ABSENT
Protect DB Version

Import a Protect DB snapshot to your standalone device.

Checked less than a minute ago; content is up to date.

Software

3.2.0_202010082118
Private Cloud Software Version

Update Software

A software update is available.

보시다시피 이 과정은 완료하는 데 시간이 오래 걸릴 수 있는 매우 긴 프로세스입니다.

Protect DB importing

The device is currently importing a Protect DB snapshot. This process can take several hours.

State	Started	Finished	Duration
Running	2021-11-07 18:48:44 +0000 less than a minute ago	Please wait...	Please wait...

Output

```
Attempting to mount an ISO, if one is present.
mount: special device /dev/cdrom does not exist
Starting update.
Stopping apply-cloud-deltas...
Stopping authentication_web...
Stopping authentication_worker...
```

Download Output

⚙️ Protect DB importing

The device is currently importing a Protect DB snapshot. This process can take several hours.

State	Started	Finished	Duration
▶ Running	2021-11-07 18:48:44 +0000 42 minutes ago	⌚ Please wait...	⌚ Please wait...

☰ Output

```

Extraction 14.9GB at 6.6MB/s eta: 9:28:03 6% [== ]
Extraction 14.9GB at 6.6MB/s eta: 9:28:21 6% [== ]
Extraction 14.9GB at 6.6MB/s eta: 9:28:27 6% [== ]
Extraction 14.9GB at 6.5MB/s eta: 9:28:40 6% [== ]
Extraction 14.9GB at 6.5MB/s eta: 9:28:46 6% [== ]
Extraction 14.9GB at 6.5MB/s eta: 9:28:58 6% [== ]
Extraction 14.9GB at 6.5MB/s eta: 9:29:12 6% [== ]
Extraction 14.9GB at 6.5MB/s eta: 9:29:26 6% [== ]
Extraction 15.0GB at 6.5MB/s eta: 9:28:56 6% [== ]
Extraction 15.0GB at 6.6MB/s eta: 9:28:20 6% [== ]
Extraction 15.0GB at 6.6MB/s eta: 9:28:28 6% [== ]
Extraction 15.0GB at 6.5MB/s eta: 9:28:44 6% [== ]
Extraction 15.0GB at 6.5MB/s eta: 9:28:51 6% [== ]
Extraction 15.0GB at 6.5MB/s eta: 9:28:48 6% [== ]
Extraction 15.0GB at 6.5MB/s eta: 9:28:56 6% [== ]
Extraction 15.0GB at 6.5MB/s eta: 9:29:10 6% [== ]
Extraction 15.0GB at 6.5MB/s eta: 9:29:23 6% [== ]
                    
```

[Download Output](#)

⚙️ Protect DB importing

The device is currently importing a Protect DB snapshot. This process can take several hours.

State	Started	Finished	Duration
▶ Running	2021-11-19 17:04:05 +0000 about 20 hours ago	⌚ Please wait...	⌚ Please wait...

☰ Output

```

Extraction 233.2GB at 4.2MB/s eta: 0:00:02 99% [=====]
Extraction 233.2GB at 4.2MB/s eta: 0:00:00 99% [=====]
Extraction 233.2GB at 4.2MB/s eta: 0:00:00 100% [=====]
Snapshot Version 3
Going to drop disposition tables.
Dropping detections table.
Dropping binaries table.
Dropping binaries_detections table.
Dropping samples table.
Dropping publishers table.
Dropping cas table.
Dropping certificates table.
Dropping cert_fingerprints table.
Recreating Protect DB tables from the schema in the snapshot.
Importing Protect DB data (this may take some time).
Importing detections table (this may take some time).
Importing binaries table (this may take some time).
                    
```

문제 #1 - 데이터 저장소의 공간 소진

여기에서 두 가지 문제를 해결할 수 있습니다. 3.5.2 이전의 vPC는 외부 NFS 스토리지를 마운트할 수 없으므로 업데이트 ISO 파일을 /data/temp 디렉토리에 업로드해야 합니다. 제 경우에는 데이터 저장소가 1TB밖에 되지 않아서 VM이 다운되었습니다. 즉, 3.5.2 이하 버전의 AirGap VPC를 성공적으로 구축하려면 데이터 스토어에 2TB 이상의 공간이 필요합니다

아래 이미지는 ESXi 서버에서 가져온 것으로, VM을 부팅하려고 할 때 HDD에 사용 가능한 공간이 더 이상 없다는 오류를 표시합니다. 128GB RAM을 64GB로 임시 전환하여 이 오류를 복구할 수 있었습니다. 그리고 나서 다시 부팅할 수 있었다. 또한 이 VM을 싼 클라이언트로 프로비저닝할 경우, 싼 클라이언트 구축의 단점은 디스크 크기가 증가할 수 있다는 것이지만, 공간을 확보하더라도 축소되지 않는다는 것입니다. 즉, 300GB 파일을 vPC의 디렉토리에 업로드한 다음 삭제했다고 가정해 보겠습니다. ESXi의 디스크는 여전히 HDD에서 300GB 더 적은 공간을 보여줍니다



문제 #2 - 이전 업데이트

두 번째 문제는 소프트웨어 업데이트를 처음 실행하는 경우의 2차 평가판에서와 마찬가지로 3.2.0에서 3.5.2로 업그레이드하기 위해 VPC를 사용했기 때문에 3.2.0은 더 이상 원래 3.2.0 버전에 있지 않기 때문에 새로운 ISO 업데이트 파일을 다운로드해야 했습니다.

Maintenance Mode
The device is in maintenance mode.
External services are unavailable.

Sanity Check Failing

Disabling TLS 1.0/1.1

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

There is no ISO loaded. Load an ISO and try again.

Content

3.2.0_202010081917
Client Definitions, DFC, Tetra Content Version

Update Content

Import Protect DB

ABSENT
Protect DB Version

Import a Protect DB snapshot to your standalone device.
The previous Protect DB import failed.

Checked 24 minutes ago; the update check failed.

Software

3.5.3_202111080345
Private Cloud Software Version

Update Software

Checked 24 minutes ago; the update check failed.

ISO 업데이트 파일을 다시 마운트하면 표시되는 오류입니다.



Maintenance Mode

Sanity Check Failing

Disabling TLS 1.0/1.1

Home / Operations - Update Device / Update Check Details

The update check failed

Something went wrong while checking for updates.

State	Started	Finished	Duration
Failed	2021-11-16 16:29:23 +0000 less than a minute ago	2021-11-16 16:29:30 +0000 less than a minute ago	less than a minute

Output

```

Attempting to mount an ISO, if one is present.
Starting update check.
http://127.0.0.1:8080/PrivateCloud/3.5.3/prod/repodata/repomd.xml: [Errno 14] HTTP Error 404 - Not Found
Trying other mirror.
To address this issue please refer to the below wiki article

https://wiki.centos.org/yum-errors

If above article doesn't help to resolve this issue please use https://bugs.centos.org/.

One of the configured repositories failed (FireAMP PrivateCloud Repository),
and yum doesn't have enough cached data to continue. At this point the only
safe thing yum can do is fail. There are a few ways to work "fix" this:

1. Contact the upstream for the repository and get them to fix the problem

```

Download Output

이 그림에서는 업데이트 이미지를 VPC에 마운트하는 다른 방법을 보여 줍니다. 버전 3.5.x에서는 NFS 스토리지와 같은 원격 위치를 사용하여 VPC와 업데이트 파일을 공유할 수 있습니다.



Maintenance Mode

Sanity Check Failing

Disabling TLS 1.0/1.1

Mount an Update ISO

ISO Configuration

HELP

Mount Type

- ISO
- ISO
- NFS4
- NFS3

Mount Status

No ISO mounted



Sanity Check Failing

Disabling TLS 1.0/1.1

Configuration saved.

Mount an Update ISO

ISO Configuration

HELP

Mount Type

NFS3

Remote Share

192.168.75.4:/AMPAG

Remote ISO File

PrivateCloud-3.5.3-Updates-2021-11-16-prod.iso

Mount

Mount Status

Mounted ISO

nfs 192.168.75.4:/AMPAG PrivateCloud-3.5.3-Updates-2021-11-16-prod.iso

Unmount

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

Content

3.5.2_202110122340

Client Definitions, DFC, Tetra Content Version

Update Content

Import Protect DB

ABSENT

Protect DB Version

ISO contains Protect DB snapshot version 20210531-0613.

Import a Protect DB snapshot to your standalone device.

A content update is available.

Software

3.5.2_202110130433

Private Cloud Software Version

Update Software

A software update is available.

온전성 확인 실패는 현재 VPC에서 사용할 수 없는 보호 DB와 관련이 있습니다



AMP for Endpoints

Private Cloud Administration Portal

Announcements

Help

Logout



Configuration

Operations

Status

Integrations

Support

Standalone



Sanity Check Failing

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

Content

3.5.2_202110122340

Client Definitions, DFC, Tetra Content Version

Update Content

Import Protect DB

ABSENT

Protect DB Version

ISO contains Protect DB snapshot version 20210531-0613.

Import a Protect DB snapshot to your standalone device.

A content update is available.

Software

3.5.2_202110130433

Private Cloud Software Version

Update Software

A software update is available.

⚙️ Protect DB importing

The device is currently importing a Protect DB snapshot. This process can take several hours.

☰ State	📅 Started	📅 Finished	🕒 Duration
▶ Running	2021-11-19 17:04:05 +0000 about 20 hours ago	⌚ Please wait...	⌚ Please wait...

☰ Output

```
Extraction 233.2GB at 4.2MB/s eta: 0:00:02 99% [=====]
Extraction 233.2GB at 4.2MB/s eta: 0:00:00 99% [=====]
Extraction 233.2GB at 4.2MB/s eta: 0:00:00 100% [=====]
Snapshot Version 3
Going to drop disposition tables.
Dropping detections table.
Dropping binaries table.
Dropping binaries_detections table.
Dropping samples table.
Dropping publishers table.
Dropping cas table.
Dropping certificates table.
Dropping cert_fingerprints table.
Recreating Protect DB tables from the schema in the snapshot.
Importing Protect DB data (this may take some time).
Importing detections table (this may take some time).
Importing binaries table (this may take some time).
```

[Download Output](#)

✔ Protect DB imported successfully

A Protect DB snapshot was successfully imported.

State	Started	Finished	Duration
✔ Successful	2021-11-19 17:04:05 +0000 about 1 month ago	2021-12-21 01:08:11 +0000 less than a minute ago	about 1 month

Output

```
Starting firehose_cassandra...
Starting firehose_cassandra_replay...
Starting firehose_publisher...
Starting firehose_publisher_replay...
Starting install-token-api...
Starting mgmt_unicorn...
Starting mongo_event_consumer...
Starting portal_unicorn...
Starting redis...
Starting retro-dipper...
Starting retrohose...
Starting retrohose-replay...
Starting tevent_listener...
Starting crond...
Starting flight...
Starting docker...
Sending notification (this may take some time).
```

Download Output

다음 업데이트가 자동으로 시작됩니다.



⚙ Importing Protect DB deltas.

Your Protect DB is being updated with threat intelligence that was queued during a previous content update. Each delta can take several hours to import, and system performance might be impacted during this time.

You should run content updates at the end of the business day or week to ensure updates are applied outside of peak use.

Queued Updates

20211116-2135

Queued Protect DB Update Version



Protect DB

20210531-0613

0.80%

Update Progress

Protect DB Database 가져오기의 매우 긴 프로세스가 끝난 후 클라이언트 정의 및 소프트웨어를 이동하고 업데이트할 수 있습니다. 이 작업은 약 3시간 이상 걸릴 수 있습니다.

✔ Content updated successfully

The device successfully performed a content update.

State	Started	Finished	Duration
✔ Successful	2021-12-21 03:10:11 +0000 28 minutes ago	2021-12-21 03:37:53 +0000 less than a minute ago	28 minutes

Output

```

Attempting to mount an ISO, if one is present.
PASS: The mount point / has sufficient space available: 23273033728 >= 1000000000
PASS: The mount point / has sufficient inodes available: 2018323 >= 100000
All checks succeeded!
Repdata is over 2 weeks old. Install yum-cron? Or run: yum makecache fast
Error: No matching Packages to list
Resolving Dependencies
--> Running transaction check
--> Package AMP-PrivateCloud-content.x86_64 0:3.5.2_202110122340-0 will be updated
--> Package AMP-PrivateCloud-content.x86_64 0:20211117234515-0 will be an update
--> Package fireamp-amp-exprev-classifier.x86_64 0:3.4.0-0.1a64 will be updated
--> Package fireamp-amp-exprev-classifier.x86_64 0:3.4.0-0.1a76 will be an update
--> Package fireamp-apde-signatures.x86_64 0:935-1 will be updated
--> Package fireamp-apde-signatures.x86_64 0:1052-1 will be an update
--> Package fireamp-clamav-definitions.x86_64 0:1634076372-7 will be updated
--> Package fireamp-clamav-definitions.x86_64 0:1637186573-7 will be an update
--> Package fireamp-clamav-definitions.x86_64 0:1634076372-7 will be updated
    
```

Download Output

마지막으로, 이 프로세스는 시간이 매우 오래 걸릴 것입니다.

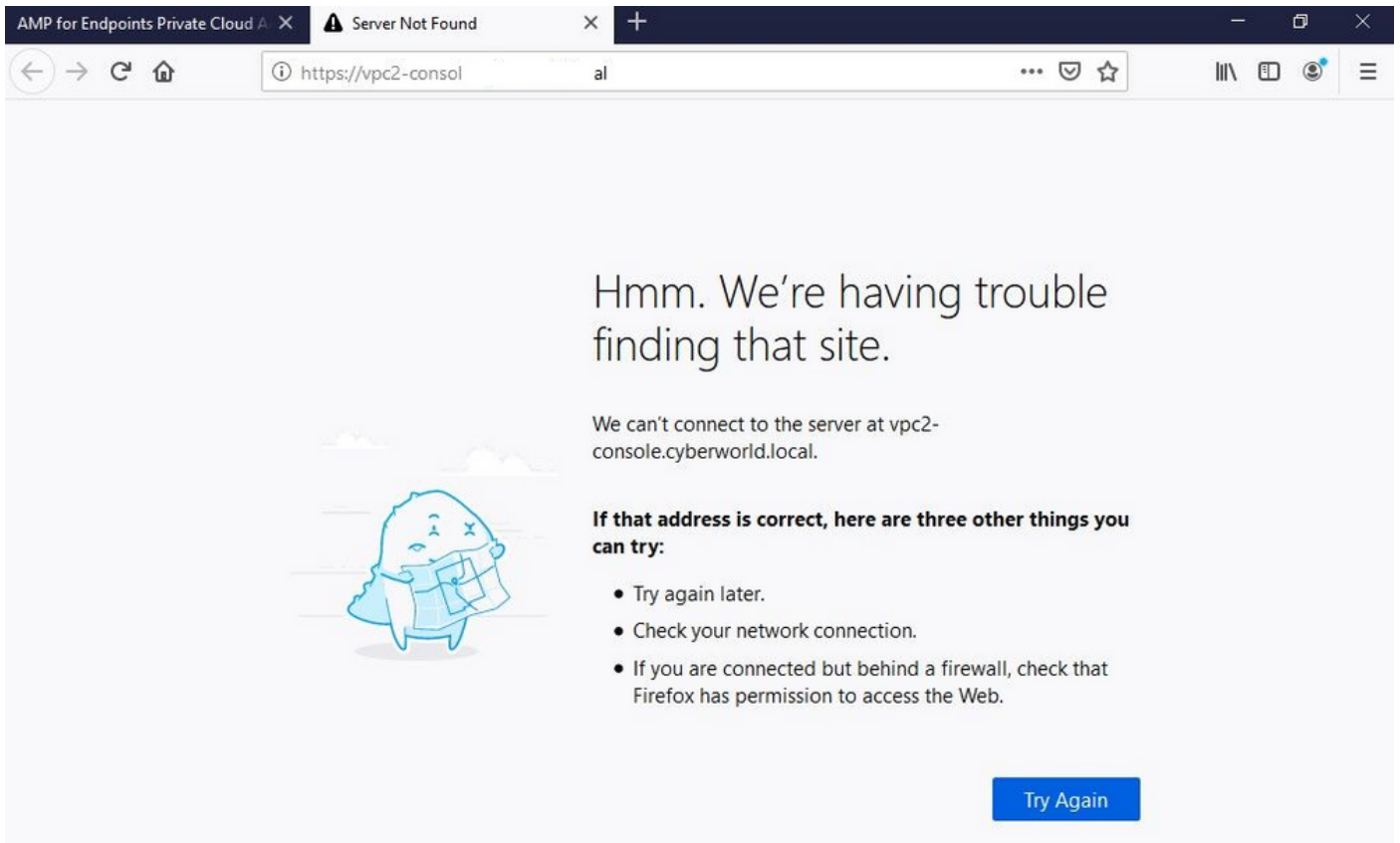
VPC 어플라이언스의 경우 HW 어플라이언스를 업데이트하고, ISO 파일을 마운트하고, USB에서 부팅하는 다른 방법이 포함된 이 TZ를 방문하십시오.

<https://www.cisco.com/c/en/us/support/docs/security/amp-virtual-private-cloud-appliance/217134-upgrade-procedure-for-airgapped-amp-priv.html#anc5>

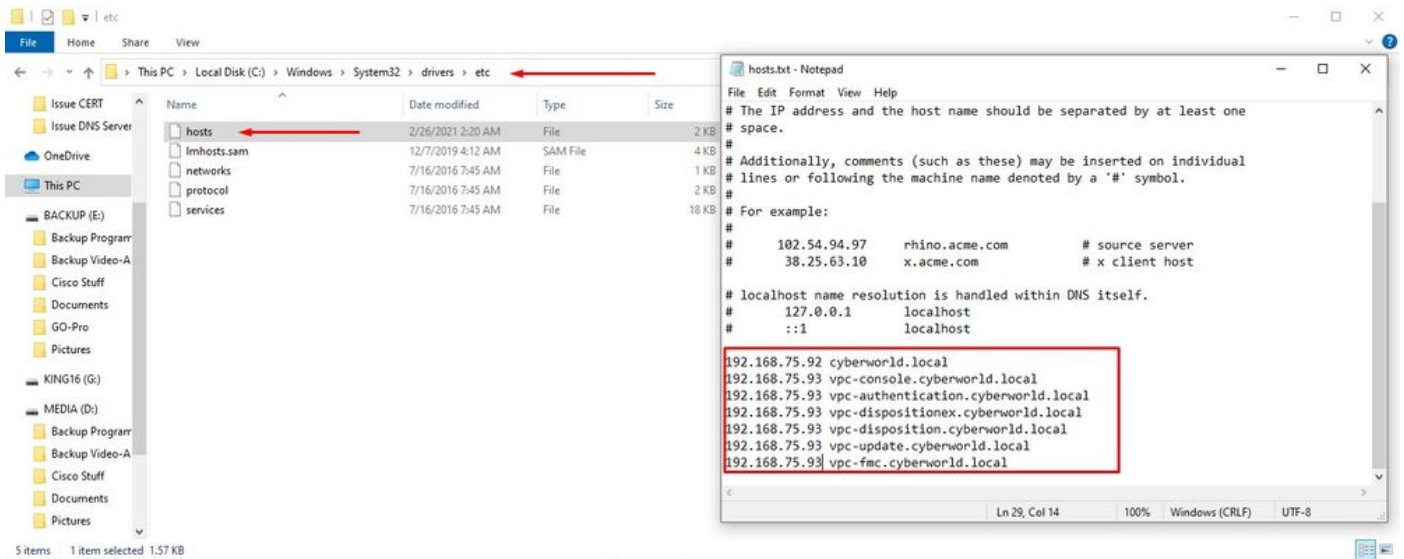
기본 문제 해결

문제 #1 - FQDN 및 DNS 서버

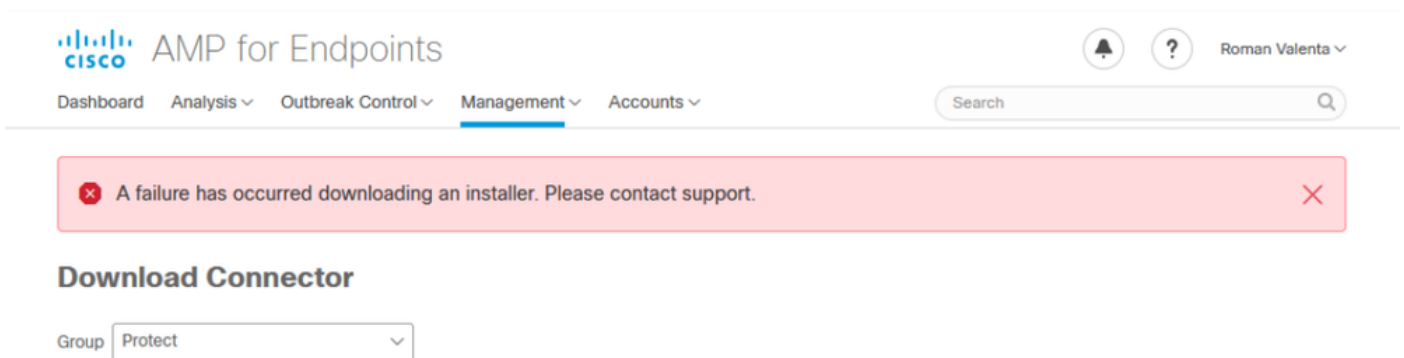
DNS 서버가 설정되지 않고 모든 FQDN이 제대로 기록되고 해결되지 않을 경우 발생할 수 있는 첫 번째 문제입니다. Secure Endpoint "fire" 아이콘을 통해 Secure Endpoint 콘솔로 이동하려고 하면 문제가 이렇게 나타날 수 있습니다. IP 주소만 사용하는 경우 정상적으로 작동하지만 커넥터를 다운로드할 수 없습니다. 아래 3번째 그림에서 볼 수 있듯이.



이미지에 표시된 것처럼 로컬 시스템에서 HOSTS 파일을 수정하면 문제가 해결되고 오류가 발생합니다.



Secure Endpoint 커넥터 설치 프로그램을 다운로드하는 동안 이 오류가 발생합니다.



몇 가지 트러블슈팅 후 올바른 해결책은 DNS 서버를 설치하는 것뿐이었습니다.

DNS Resolution Console: nslookup vPC-Console.cyberworld.local (Returned 1, start 2021-03-02 15:43:00 +0

```

=====
Server:      8.8.8.x
Address:     8.8.8.x#53

```

```

** server can't find vPC-Console.cyberworld.local: NXDOMAIN

```

DNS 서버에 모든 FQDN을 기록하고 Virtual Private Cloud의 레코드를 퍼블릭 DNS에서 DNS 서버로 변경하면 모든 작업이 정상적으로 시작됩니다.



Configure network settings.

- Device Summary
- Change Password
- Cisco Cloud
- Network**
- Date and Time
- Certificate Authorities
- Proxy
- Notifications
- License
- Email
- Backup
- SSH
- Syslog
- Updates
- Services

Admin	eth0 / 00:0C:29:A6:4A:11
	IP Assignment 192.168.75.92 More details
Interface	eth1 / 00:0C:29:A6:4A:1B
	IP Assignment 192.168.75.93 More details
	IP Assignment <input type="text" value="Static"/>
	IP Address <input type="text" value="192.168.75.93"/>
	<input checked="" type="checkbox"/> Check for IP Address conflicts
	Subnet Mask <input type="text" value="255.255.255.0"/>
	Gateway <input type="text" value="192.168.75.1"/>

Warning: Address and Hostname Changes

If you change the IP address of the interface you must also update the DNS records for each of your configured hostnames to point to the new address. AMP for Endpoints Connectors will expect services to be available at the original DNS names assigned to them.

[View the Configuration help page for a list of affected services.](#)

DNS
Primary DNS Server <input type="text" value="192.168.75.4"/>



Configuration Changed

Configuration changes do not take effect until reconfiguration is performed.

[Reconfigure Now](#)

[Reconfiguration](#)

Configuration saved.



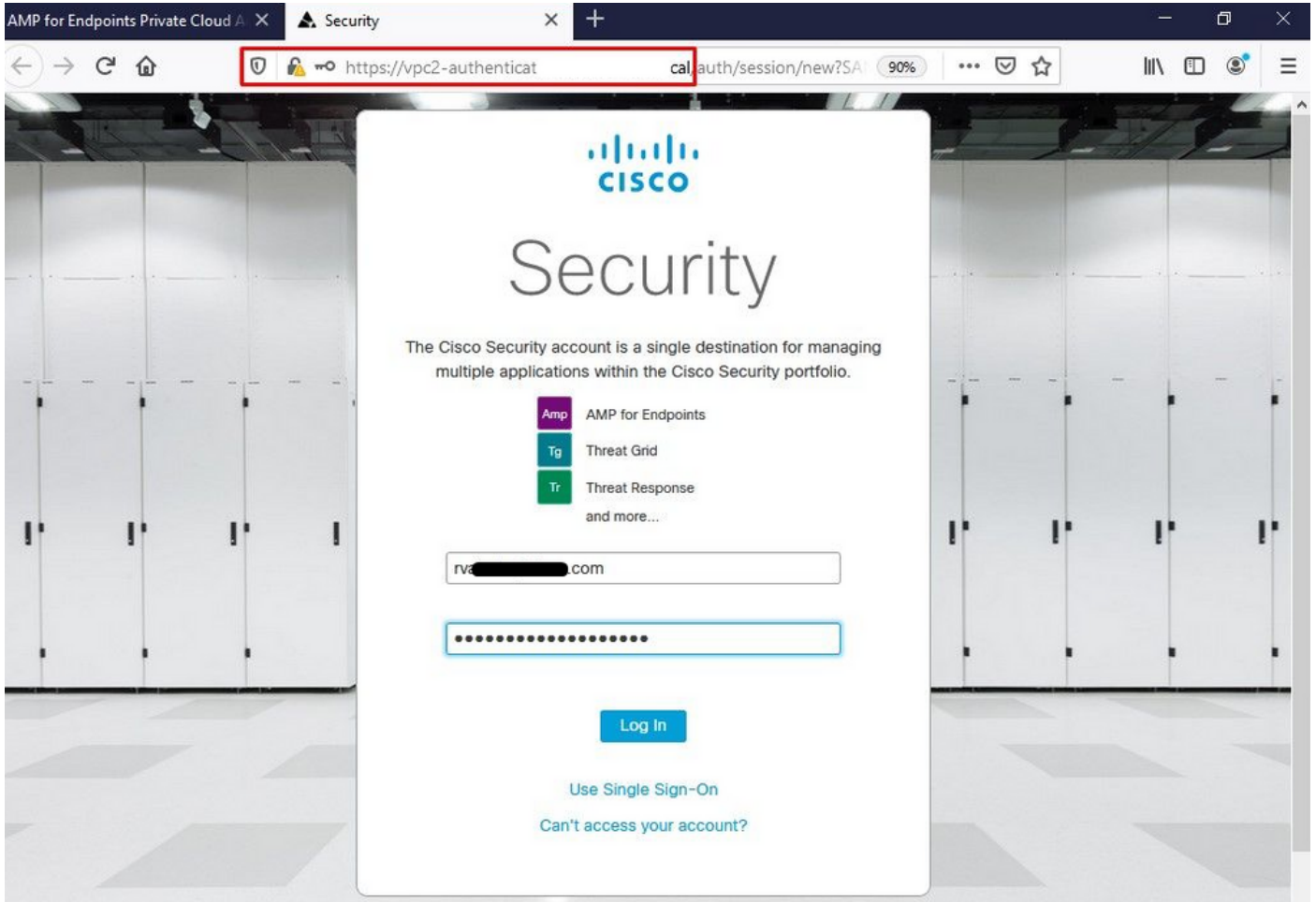
State	Started	Finished	Duration
	Sun Apr 11 2021 20:19:00 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 1 minute, 45 seconds ago	Please wait...	Please wait...

Output

```
[2021-04-12T00:20:43+00:00] DEBUG: Found current_uid == nil, so we are creating a new file, updating owner
[2021-04-12T00:20:43+00:00] INFO: file[/tmp/cqlsh_check_superuser_password.cql] owner changed to 4015
[2021-04-12T00:20:43+00:00] DEBUG: Found current_gid == nil, so we are creating a new file, updating group
[2021-04-12T00:20:43+00:00] INFO: file[/tmp/cqlsh_check_superuser_password.cql] group changed to 4015
[2021-04-12T00:20:43+00:00] DEBUG: Found current_mode == nil, so we are creating a new file, updating mode
[2021-04-12T00:20:43+00:00] INFO: file[/tmp/cqlsh_check_superuser_password.cql] mode changed to 600
[2021-04-12T00:20:43+00:00] DEBUG: Restoring selinux security content with /sbin/restorecon -R "/tmp/cqlsh_check_superuser_passwo
rd.cql"
[2021-04-12T00:20:43+00:00] INFO: Processing execute[cqlsh_check_superuser_password] action run (/var/run/cookbooks/cassandra/pro
viders/cqlsh.rb line 16)
[2021-04-12T00:20:43+00:00] DEBUG: Providers for generic execute resource enabled on node include: [Chef::Provider::Execute]
[2021-04-12T00:20:43+00:00] DEBUG: Provider for action run on resource execute[cqlsh_check_superuser_password] is Chef::Provide
r::Execute
[2021-04-12T00:20:43+00:00] INFO: Retrying execution of execute[cqlsh_check_superuser_password], 19 attempt(s) left
[2021-04-12T00:20:45+00:00] DEBUG: Providers for generic execute resource enabled on node include: [Chef::Provider::Execute]
[2021-04-12T00:20:45+00:00] DEBUG: Provider for action run on resource execute[cqlsh_check_superuser_password] is Chef::Provide
r::Execute
```

Download Output

이 시점에서 로그인하고 커넥터를 다운로드할 수 있습니다



환경에 대한 초기 보안 엔드포인트 정책 마법사를 가져옵니다. 사용하는 안티바이러스 제품(있는 경우), 프록시 및 구축할 정책의 유형을 안내합니다. 커넥터의 운영 체제에 따라 적절한 설정... 버튼을 선택합니다.

그림과 같이 Existing Security Products 페이지가 나타납니다. 사용하는 보안 제품을 선택합니다. 엔드포인트에서 성능 문제를 방지하기 위해 적용 가능한 제외를 자동으로 생성합니다. Next(다음)를 선택합니다.

AMP for Endpoints Private Cloud X Dashboard X +

← → ↻ 🏠 🔒 https://vpc2-consol 'dashboard/fresh' 📄 ⋮ 📌 ⭐ 🏠 📄 👤

CISCO AMP for Endpoints 🔔 ? Roman Valenta ▾

Dashboard Analysis ▾ Outbreak Control ▾ Management ▾ Accounts ▾ Search 🔍

Dashboard

Cisco - rvalenta

Dashboard Inbox Overview Events

Getting Started

- [View Online Help](#)
- [Download Cisco AMP for Endpoints User Guide](#)
- [Download Cisco AMP for Endpoints Deployment Strategy](#)

Deploy AMP for Endpoints Connectors

- [Set Up Windows Connector](#)
- [Set Up Mac Connector](#)
- [Set Up Linux Connector](#)

Demo Data

Demo Data allows you to see how Cisco AMP for Endpoints works by populating your Console with replayed data from actual malware infections. Enabling Demo Data will add computers and events to your Cisco AMP for Endpoints Console so you can see how the Dashboard, File Trajectory, Device Trajectory, Threat Root Cause, and Detections and Events displays behave when malware is detected. Demo Data can coexist with live data from your Cisco AMP for Endpoints deployment, however, because of the severity of some of the Demo Data

Demo Computers

WannaCry [Click here to view PDF](#)
The WannaCry attack involves a remote compromise through the Windows SMB (Server Message Block) service using the ETERNALBLUE exploit. Upon system compromise, the attacker drops the WannaCry ransomware variant that is initially identified by AMP for Endpoints using ransomware indicators of compromise, and later by AMP Cloud signatures.

SFEicar [Click here to view PDF](#)
Learn how Indications of Compromise can alert you to potential malware problems and how to determine their effects in Device Trajectory.

ZAccess [Click here to view PDF](#)
Use Device Trajectory to watch a rootkit exploit privilege escalation on a computer, and use File Trajectory to discover which other endpoints have been compromised.

ZBot [Click here to view PDF](#)
See how a vulnerable version of Internet Explorer can expose you to malware. Use Device Trajectory to learn what happened and use application blocking lists to stop the future execution of vulnerable programs.

CozyDuke [Click here to view PDF](#)
Trace a detection back to an abused DLL search path, block any communications to its upstream CnC, and deploy an Endpoint IOC to contain further attacks.

커넥터 다운로드.

Step 1: Existing Security Products

Step 2: Set Up Proxy

Step 3: Download Connector

Audit Only	Protect	Triage	Server	Windows Domain Controllers
Used when you're still learning about the product and want to install it without any impact to your existing systems.	Used during normal operations and you want Cisco AMP for Endpoints to quarantine a file.	Used when you have a known or suspected infected machine.	Used when you're installing a connector on standard Windows servers.	installing a connector on Windows Domain Controllers.
Policy Details	Policy Details	Policy Details	Requirements	Requirements
Files Audited	Files Quarantined	Files Quarantined	Files Audited	Files Audited
Network Blocked	Network Blocked	Network Blocked	Network Off	Network Off
Offline Engine TETRA	Offline Engine TETRA	Offline Engine TETRA	Offline Engine TETRA	Offline Engine TETRA
Download	Download	Download	Download	Download

[Back](#) [Next](#)

Step 4: Verify, Contain, and Protect

Opening amp_Protect.exe

You have chosen to open:

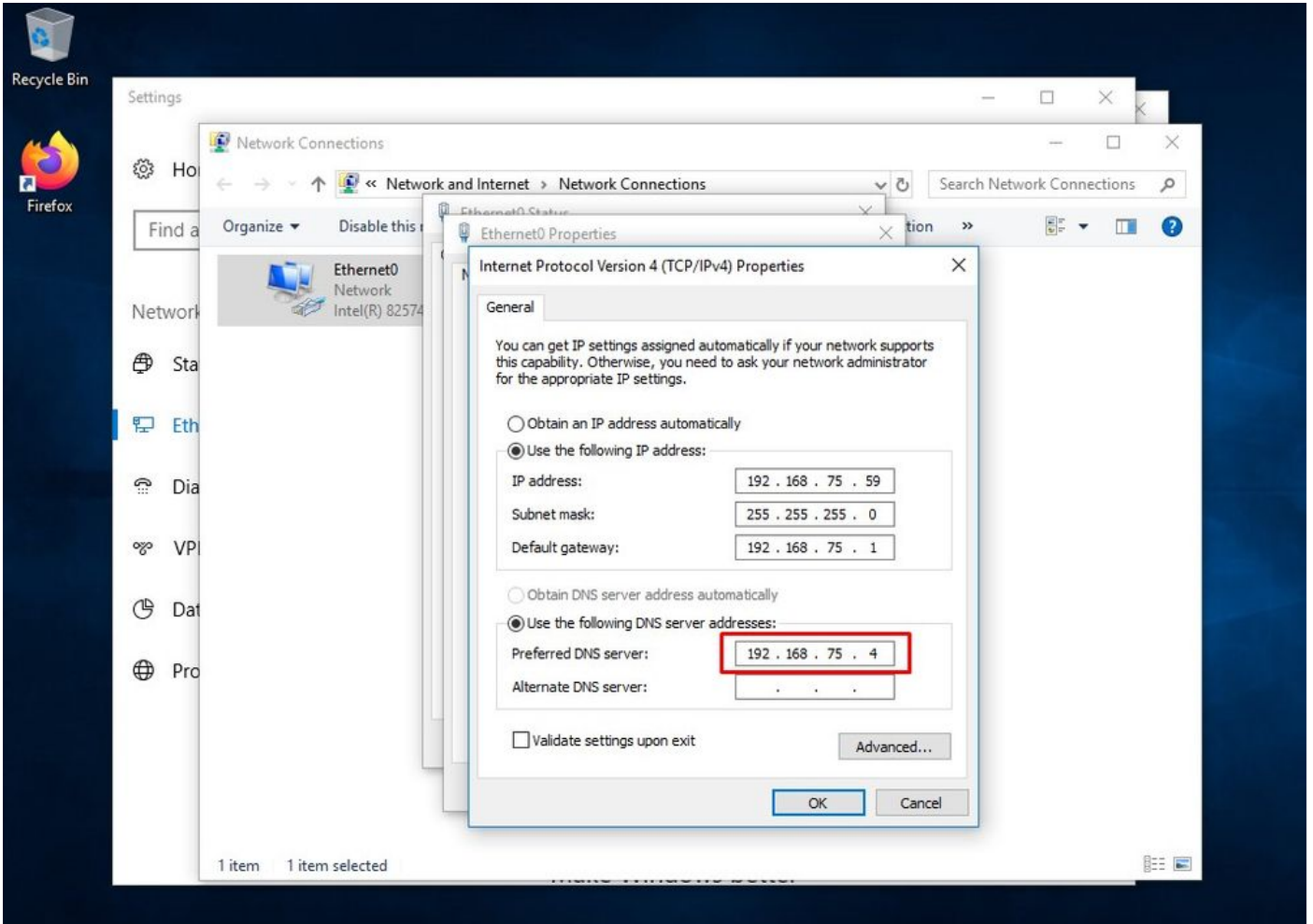
amp_Protect.exe
which is: exe File
from: https://vpc-console.cyberworld.local

Would you like to save this file?

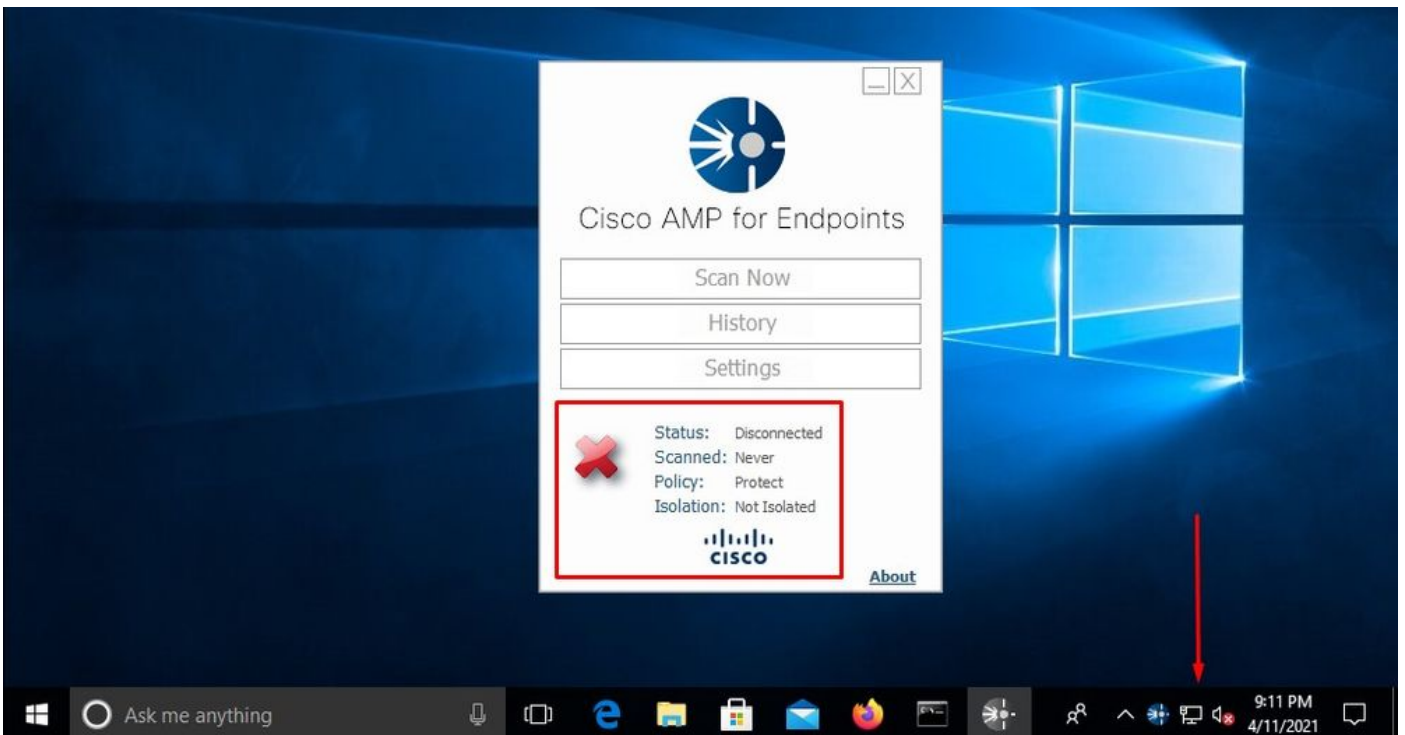
[Save File](#) [Cancel](#)

문제 #2 - 루트 CA 문제

자체 내부 인증서를 사용하는 경우 발생할 수 있는 다음 문제는 초기 설치 후 커넥터가 연결 해제된 것으로 표시될 수 있다는 것입니다.



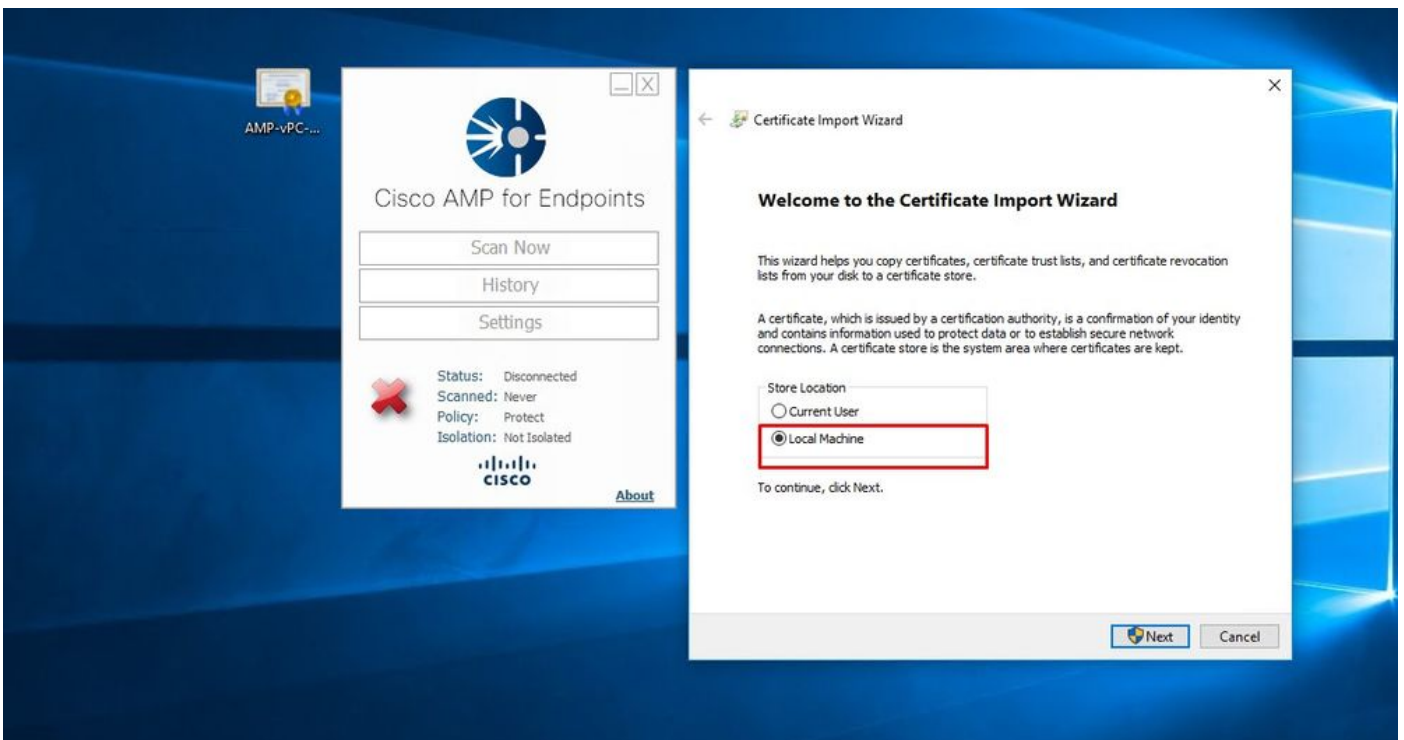
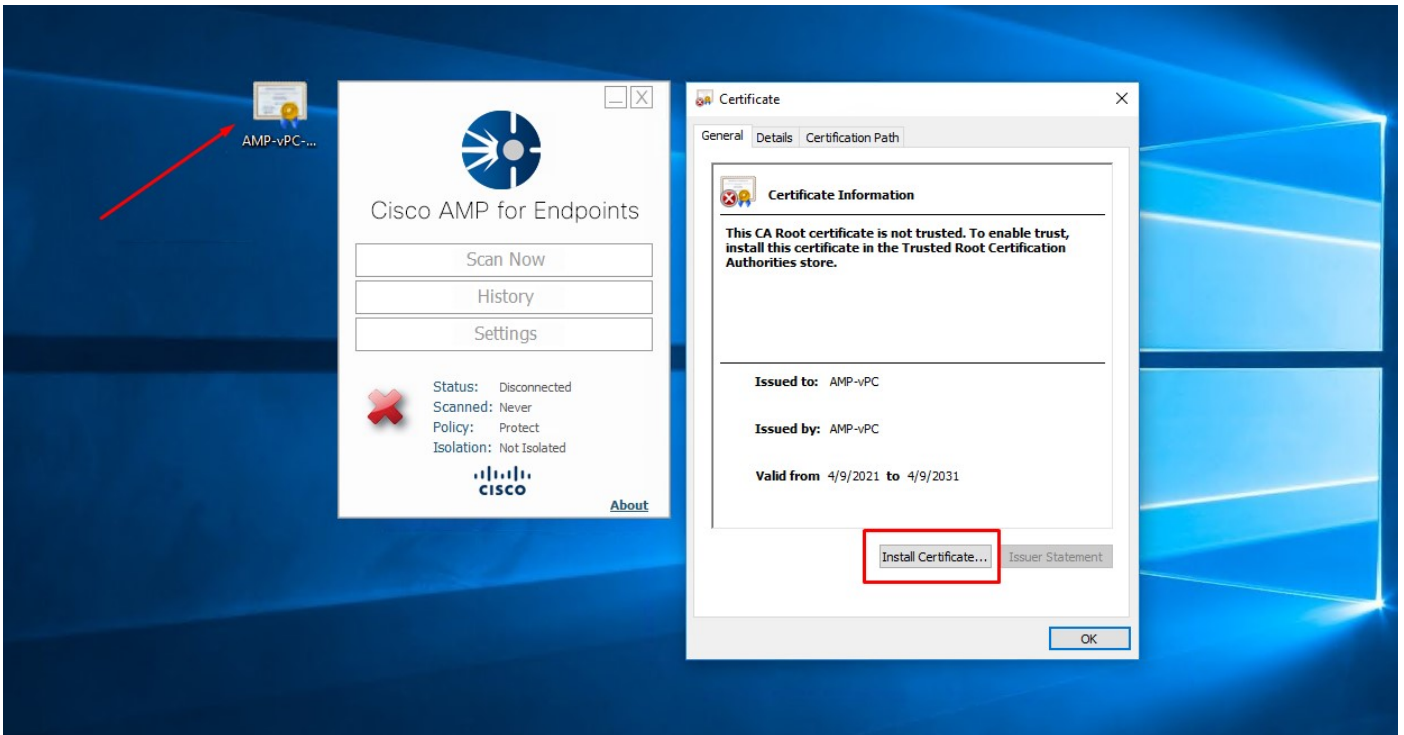
커넥터를 설치하면 Secure Endpoint(보안 엔드포인트)가 Disconnected(연결 끊김)로 표시될 수 있습니다. 진단 번들을 실행하고 로그를 통해 문제를 확인할 수 있습니다.

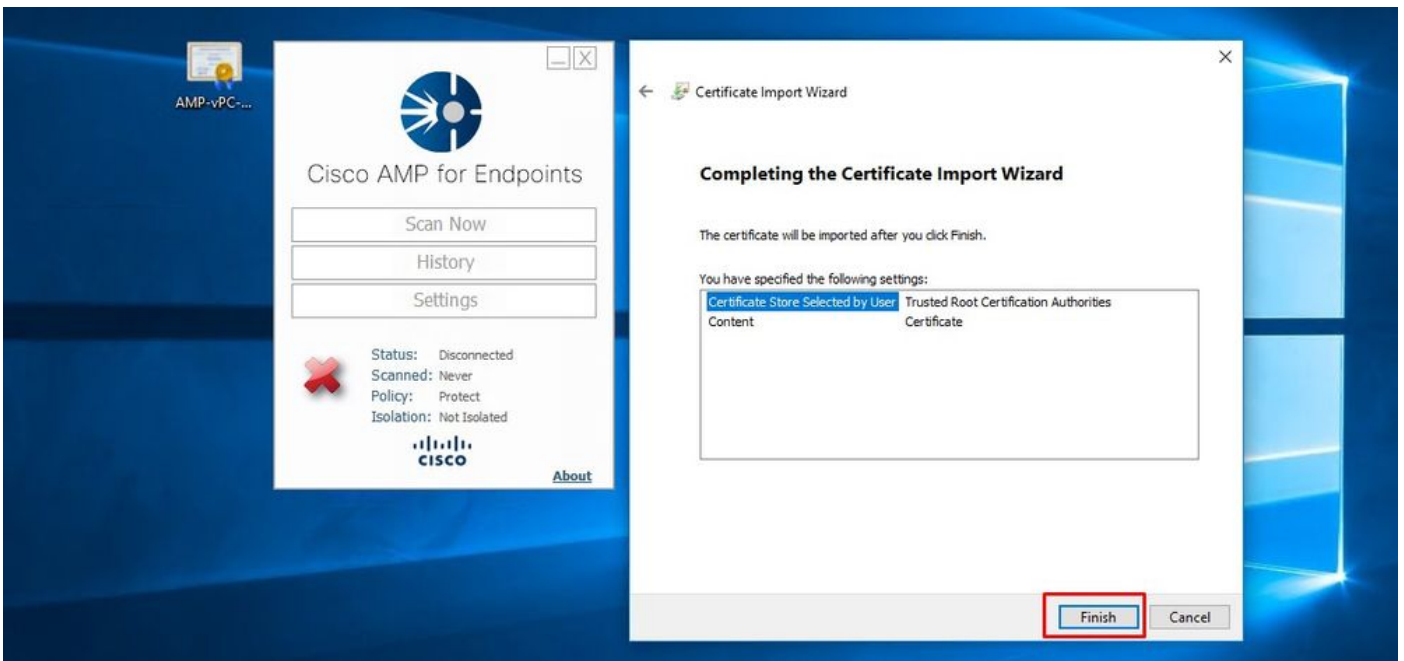
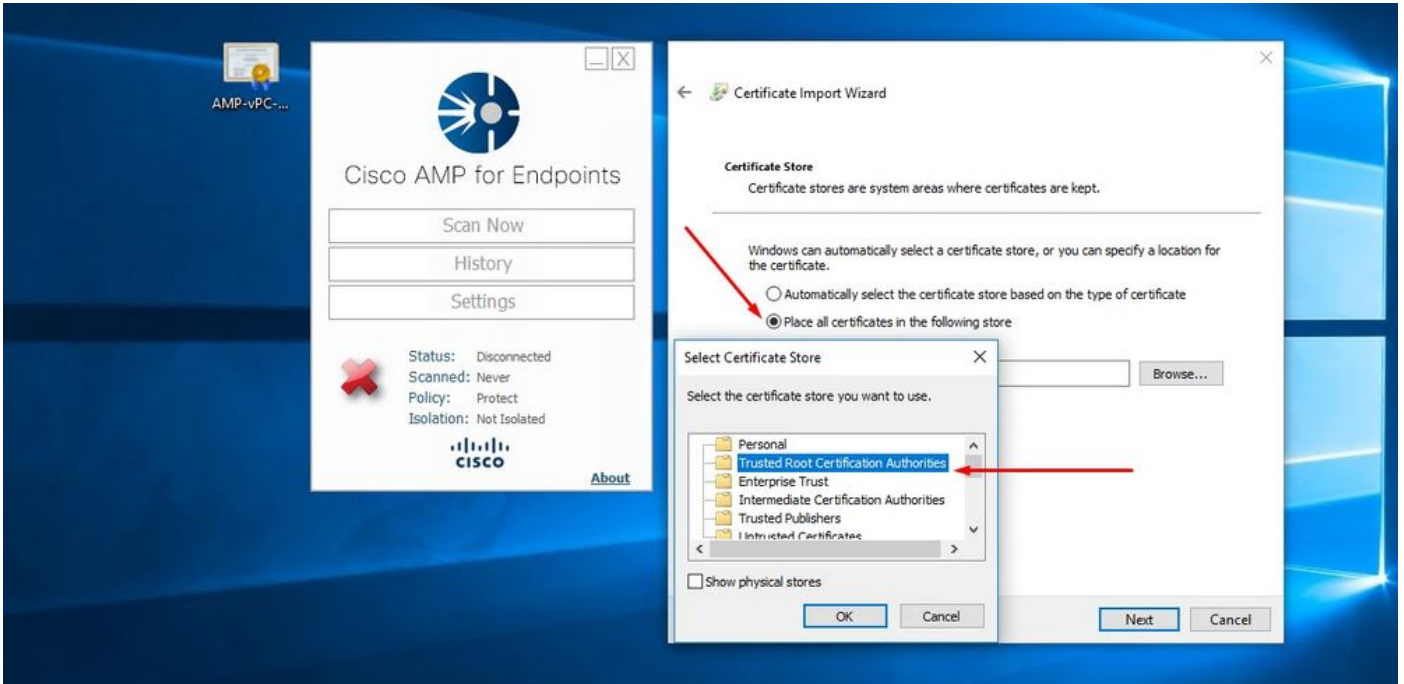


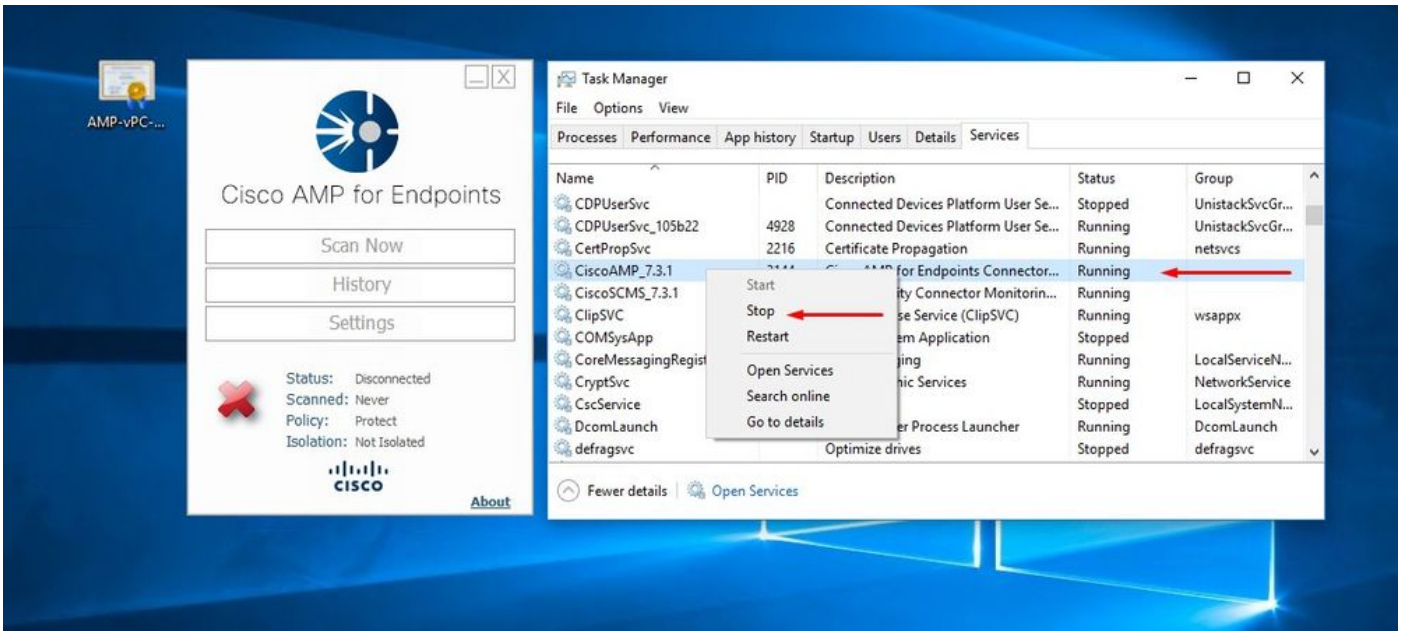
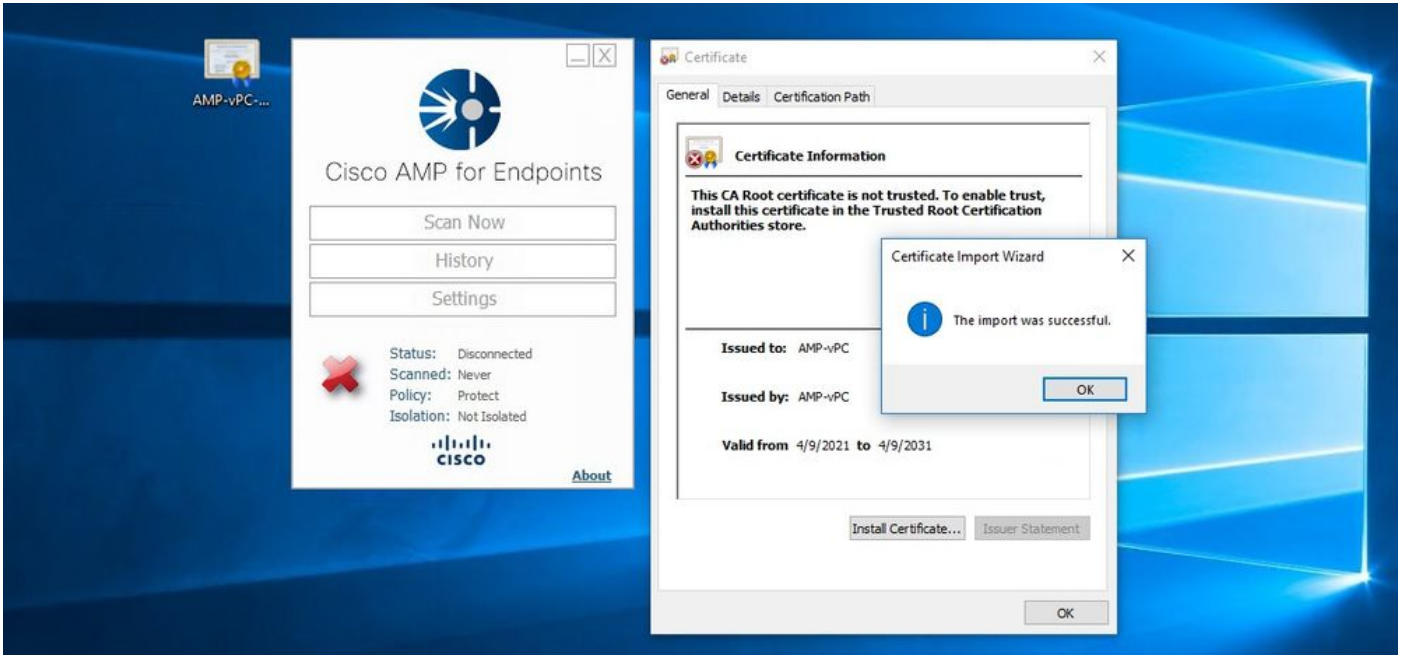
진단 번들에서 수집된 이 출력을 기반으로 Root CA(루트 CA) 오류를 확인할 수 있습니다

(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1011]: GET request https://vPC-Console.cyberworl
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1051]: async request failed (SSL peer certificat
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1074]: response failed with code 60

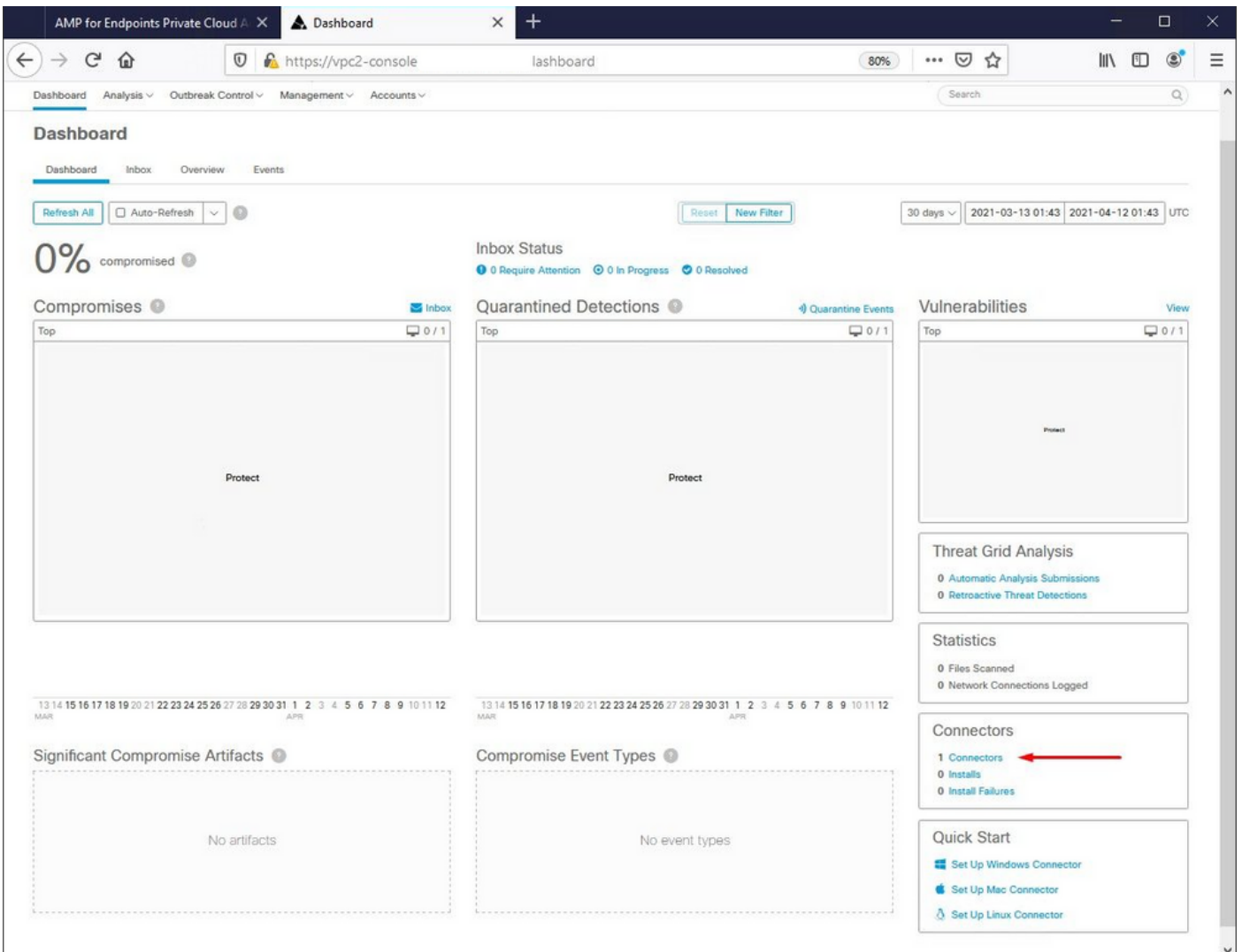
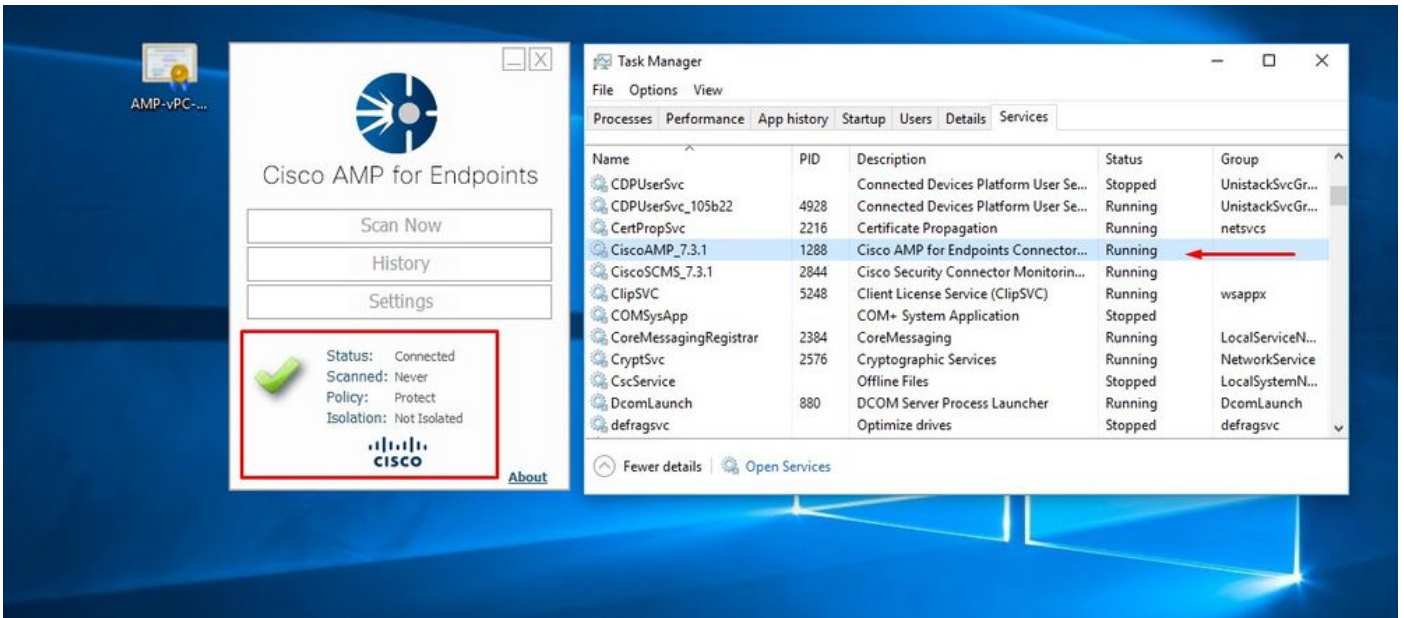
루트 CA를 신뢰할 수 있는 루트 CA 저장소에 업로드한 다음 보안 엔드포인트 서비스를 다시 시작합니다. 모든 것이 예상대로 작동하기 시작한다.







바운스되면 Secure Endpoint 서비스 커넥터가 예상대로 온라인 상태가 됩니다.



악의적인 활동 테스트

Dashboard

Dashboard **Inbox** Overview Events

Refresh All Auto-Refresh

Reset New Filter

30 days 2021-03-13 01:56 2021-04-12 01:56 UTC

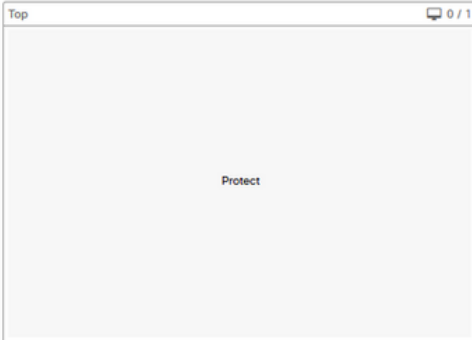
0% compromised

Inbox Status

0 Require Attention 0 In Progress 0 Resolved

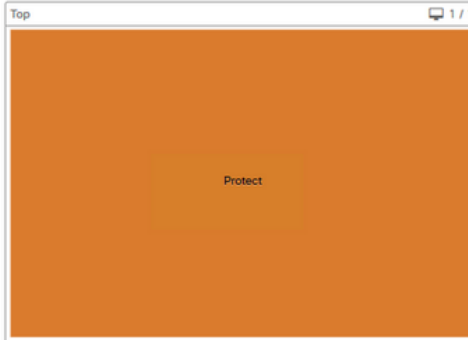
Compromises

Inbox 0 / 1



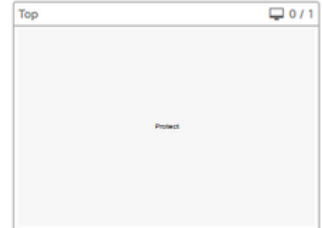
Quarantined Detections

Quarantine Events 1 / 1



Vulnerabilities

View 0 / 1



Threat Grid Analysis

0 Automatic Analysis Submissions
0 Retroactive Threat Detections

Statistics

0 Files Scanned
0 Network Connections Logged

Connectors

1 Connectors
0 Installs
0 Install Failures

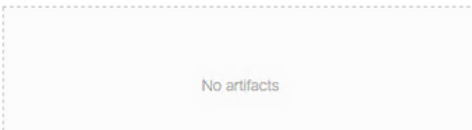
Quick Start

Set Up Windows Connector

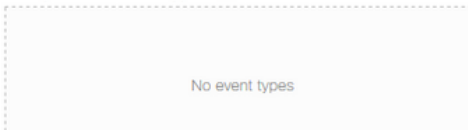
13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12
MAR APR

13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12
MAR APR

Significant Compromise Artifacts



Compromise Event Types



이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.