

AMP Private Cloud PC3000 이미지 재생성 및 백업 복원

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

소개

이 문서에서는 AMP(Advanced Malware Protection) Private Cloud 하드웨어 어플라이언스를 출하시 상태로 재이미지화한 다음 백업을 복원하는 방법에 대해 설명합니다. 어플라이언스를 공장 상태로 되돌리려면 8단계를 건너뛰고 일반 설치를 따릅니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco AMP Private Cloud PC3000
- Cisco CIMC(Integrated Management Controller)를 통한 KVM(Kernel-based Virtual Machine) 액세스

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco AMP Private Cloud PC3000 3.1.1
- KVM 콘솔에 액세스하기 위한 Chrome 브라우저

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

구성

1단계. CIMC에 로그인합니다. KVM 콘솔을 엽니다.

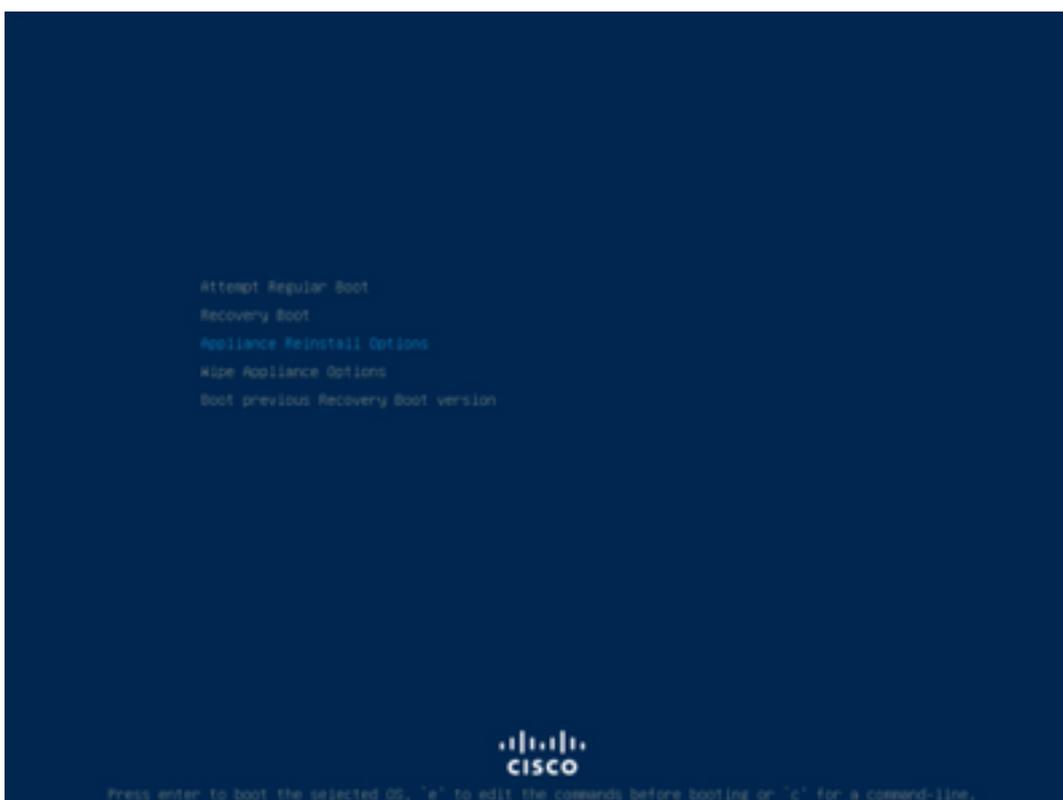
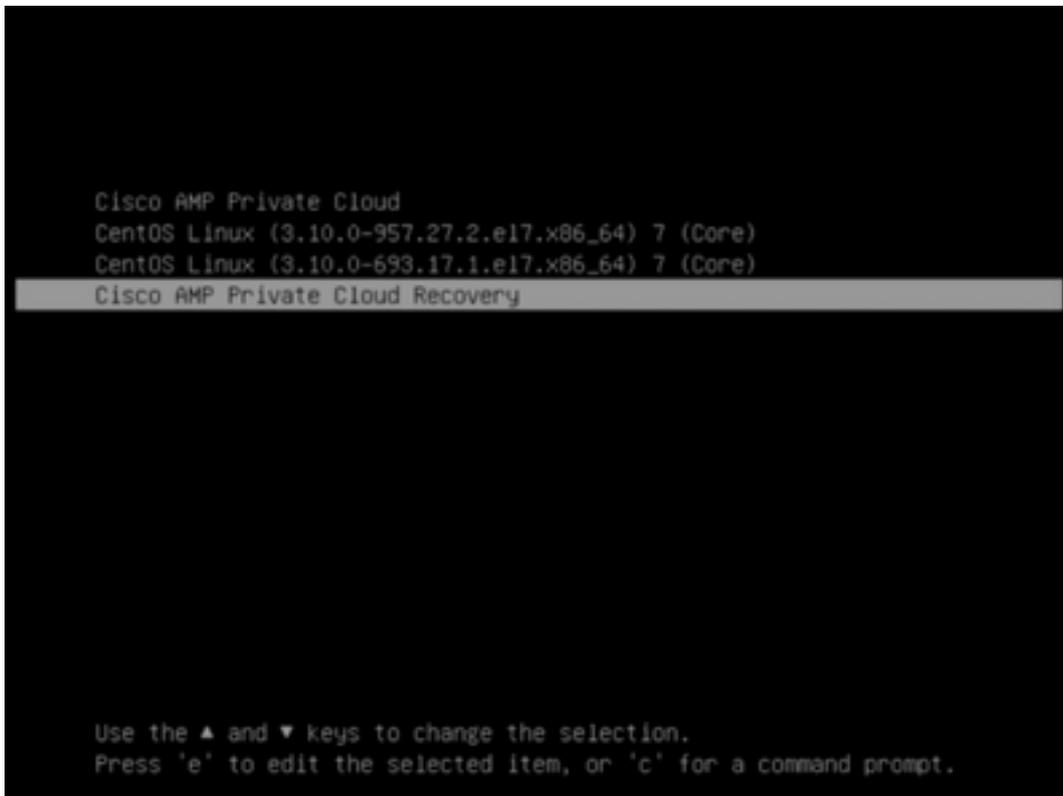
브라우저에서 해당 페이지에 대한 팝업이 활성화되었는지 확인합니다.

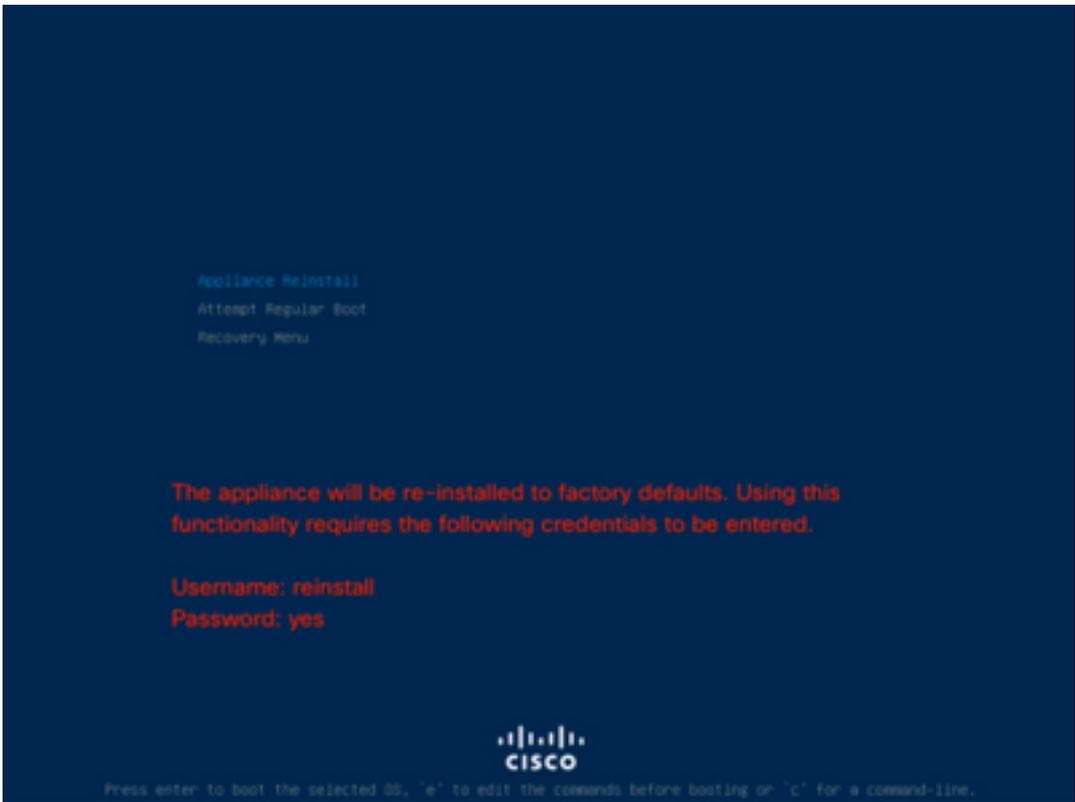
2단계. 어플라이언스를 다시 로드합니다.

관리 포털, SSH(Secure Shell) 또는 CIMC KVM을 통해 어플라이언스를 재부팅할 수 있습니다.

3단계. BIOS(Basic Input Output System) POST(Power-on self-test)가 완료되면 GNU GRand Unified Bootloader (GRUB) 메뉴가 나타납니다.

Cisco AMP Private Cloud Recovery > Appliance Reinstall Options > Appliance Reinstall을 선택합니다.

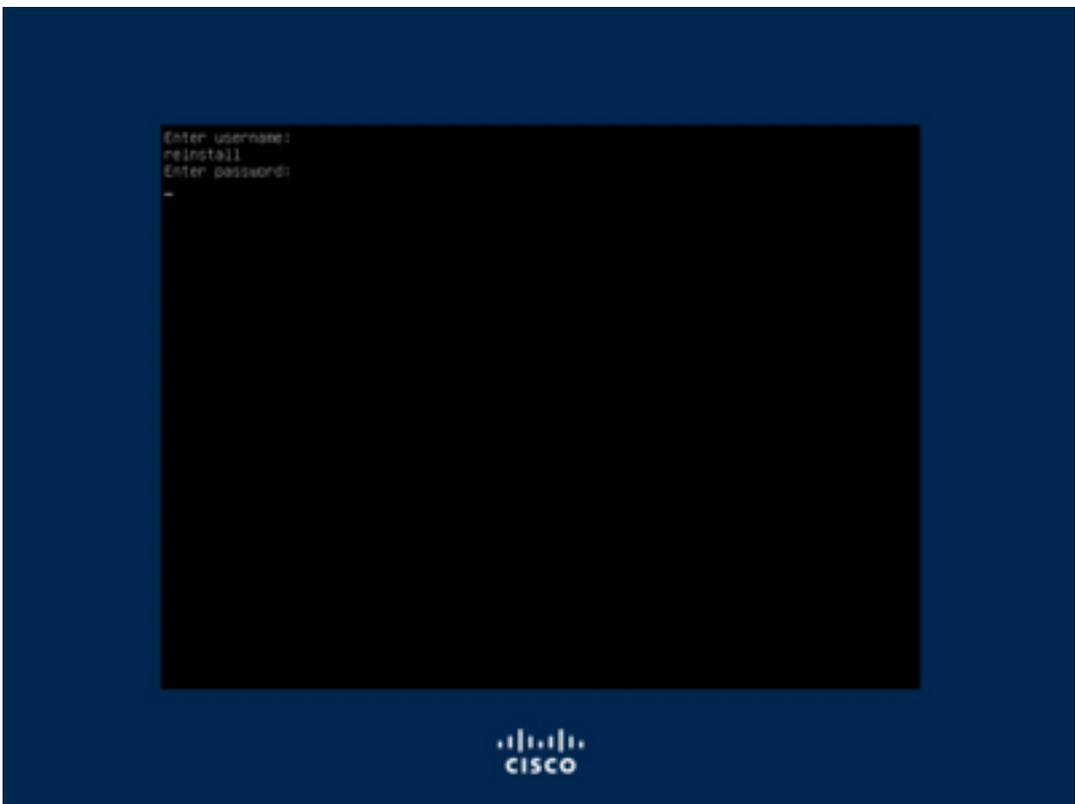




4단계. 사용자 이름과 비밀번호를 입력합니다.

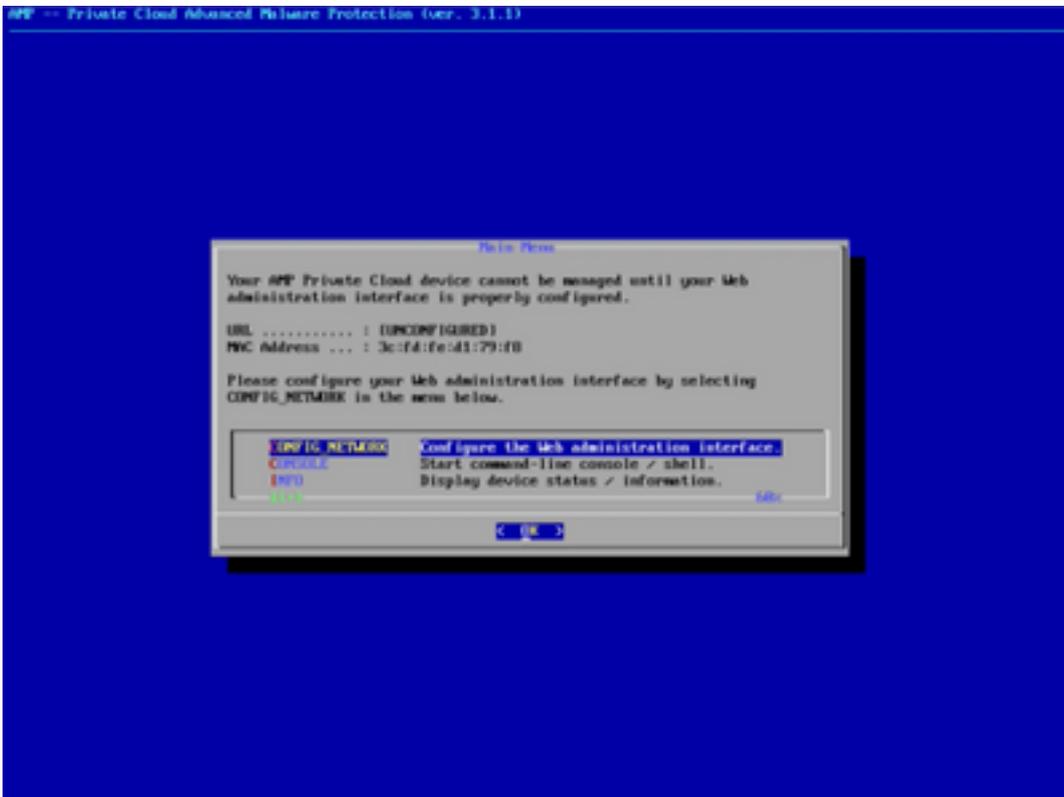
사용자 이름: 재설치

암호: 예

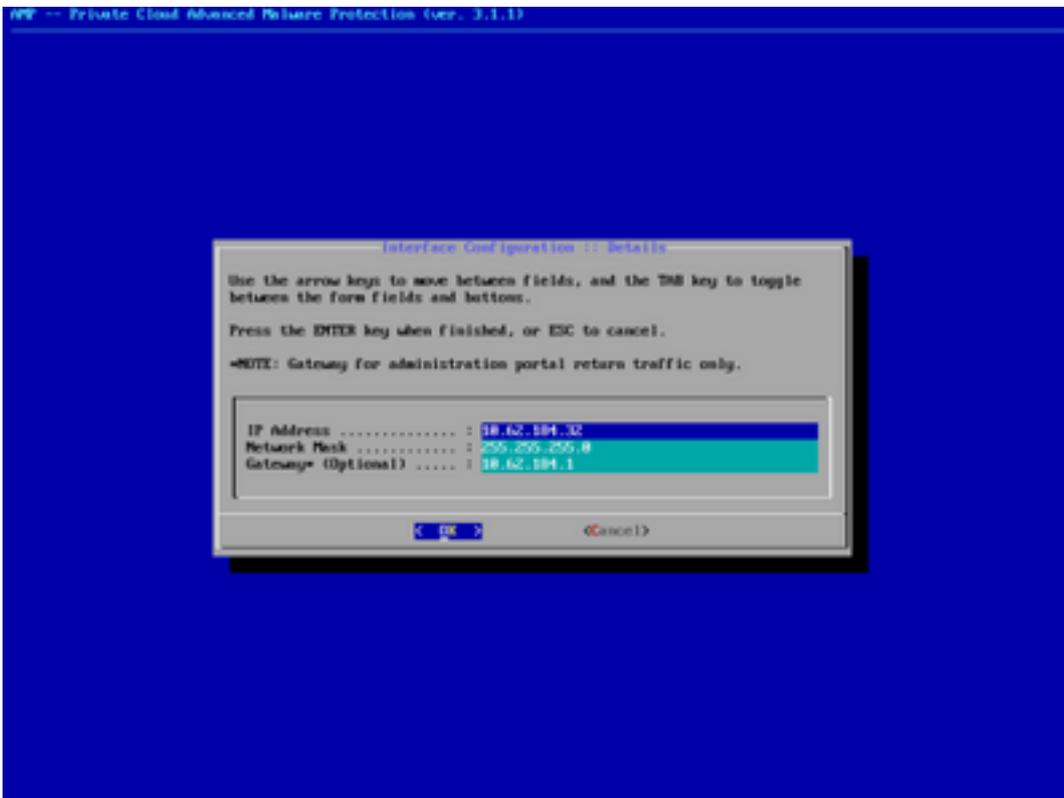


5단계. 리이미징이 시작되고 다시 로드되면 초기 메뉴가 표시됩니다.

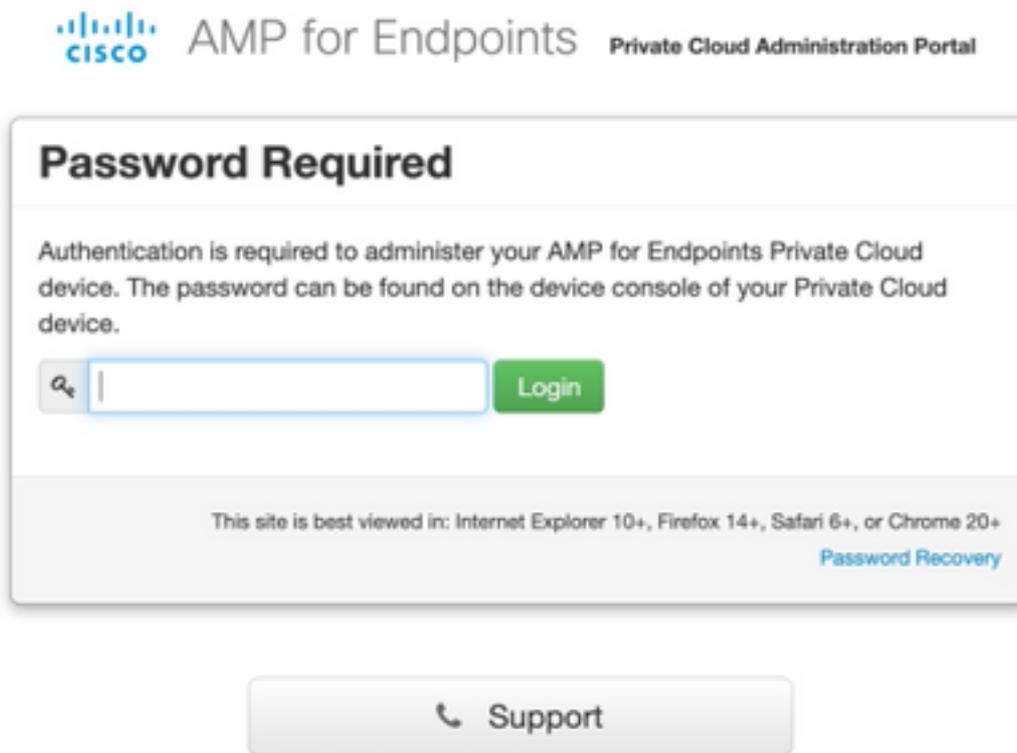
```
l 11.7176383 sdhci: registered new interface driver sdhci-platf-generic
l 11.7448181 sdhci-platf: USB Serial support registered for generic
l 11.7538991 HUSB2T1P: No PS/2 controller found. Probing ports directly.
l 11.7932271 usb 1-6: new high-speed USB device number 2 using xhci_hcd
l 12.1082041 usb 1-6: New USB device found, idVendor=0a1b, idProduct=9400
l 12.1231031 usb 1-6: New USB device strings: Mfr=1, Product=2, SerialNumber=3
l 12.1305360 usb 1-6: Product: Emulex Fibre4 HighSpeed HB
l 12.1365131 usb 1-6: Manufacturer: Emulex Communications
l 12.1409121 usb 1-6: SerialNumber: 0x00000000
l 12.1461331 hub 1-6:1.0: USB hub found
l 12.1506580 hub 1-6:1.0: 7 ports detected
l 12.2675321 usb 1-7: new high-speed USB device number 3 using xhci_hcd
l 12.2775351 HUSB2T1P: Can't read CR while initializing 0042
l 12.3656221 HUSB2T1P: probe of 0042 failed with error -5
l 12.3969051 xhci_hcd: PS/2 mouse device comes for all mice
l 12.3910640 rtc_cmos 00:00: RTC can wake from S4
l 12.3964271 rtc_cmos 00:00: rtc core: registered rtc_cmos as rtc0
l 12.3980100 rtc_cmos 00:00: alarms up to one month, y1k, 114 bytes wrms, 16pt irq
l 12.3254351 intel_pstate: Intel P-state driver initializing
l 12.3322251 intel_pstate: HWP enabled
l 12.3792980 cpuidle: using governor menu
l 12.3948271 EFI Variables Facility v0.01 2004-Aug-17
l 12.3982851 tsc: Refined TSC clocksource calibration: 2593.766 MHz
l 12.3991321 Switched to clocksource tsc
l 12.4017921 hidraw: raw HID events driver (C) Jiri Kosina...
l 12.4096241 usbhid: USB HID core driver
l 12.4119481 usb 1-7: New USB device found, idVendor=0914, idProduct=6578
l 12.4119521 usb 1-7: New USB device strings: Mfr=0, Product=1, SerialNumber=0
l 12.4119551 usb 1-7: Product: USB2.0 Hub
l 12.4132041 hub 1-7:1.0: USB hub found
l 12.4139421 hub 1-7:1.0: 4 ports detected
l 12.4452241 Detected 1 PCI Subspaces
l 12.4454231 Registering PCI driver as Mellox controller
l 12.4519080 drop_monitor: Initializing network drop monitor service
l 12.4562761 TUN: tunctl registered
l 12.4620581 Initializing RDRD netlink socket
l 12.4666521 NET: Registered protocol family 18
l 12.4726251 NET: Registered protocol family 17
l 12.4728481 usb 1-6:1: new high-speed USB device number 4 using xhci_hcd
l 12.4818881 nls_gcc: NLS GDB support
l 12.4917751 intel_rdt: Intel RDT RR allocation detected
l 12.5056261 microcode: sig=0x00054, pf=0x00, revision=0x200004d
l 12.5134881 microcode: Microcode Update Binary: 02_01_01/microcode.bin (cc-0). Peter Oruba
```



6단계. CONFIG_NETWORK 하위 메뉴에서 네트워크를 구성합니다.



7단계. 5단계의 비밀번호로 AMP OPadmin 포털에 로그인합니다.



8단계. SFTP 또는 SCP를 사용하여 원격 서버에서 /data/로 백업을 다운로드합니다.

- 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 Configuration ✓
- 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 ✓
 - > Firewall Management Center ✓
- Other**
- > Review and Install
- [▶ Start Installation](#)

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.

Preparing Restore

Your restore file is being processed, please wait.

- + Adding mongo_event_consumer account.
- + Running startup script to generate new password.
Generating a random password for mongo_event_consumer
- + Removing the .rpmnew file
- + Removing event_mongo_store service
- + Adding firehose_cassandra account.
- + Running startup script to generate new password.
Generating a random password for firehose_cassandra
- Checking for bios and lmc updates. This may take some time.
- If an update is available and the update is successful, you will be asked to reboot the box.

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 ▶](#)

Restore

Local Remote [Upload](#)

Restore from a backup file present on the device. Files will be extracted to the directory your backup is located in during the restore process; for this reason, it is recommended that the file be located in the /data directory.

📁 /data/amp.bak

9단계. Hardware Configuration(하드웨어 컨피그레이션)을 확인하고 Next(다음) > Start Installation(설치 시작)을 클릭합니다.

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 Configuration**

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 ✓
- > Finpower Management Center ✓

Other

- > Review and Install

▶ Start Installation

Hardware Configuration

	Installed	Minimum Required
CPU Cores	48	8
Memory	1510 GB	128 GB

Next >

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 Configuration ✓

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 ✓
- > Firewall Management Center ✓

Other

- > 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.

Restore Ready

Your configuration has been restored, and your data will be restored during installation. You may review and edit some parts of your configuration before proceeding with installation.

Installation Type ✎ Edit

Standalone Connected

- Requires 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.

AMP for Endpoints Console Account ✎ Edit

Name	Wojciech Cecot
Email Address	wcecot@cisco.com
Business Name	Cisco - wcecot

Recovery

When restoring from a backup, a recovery image is not required.

Start Installation

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
▶ Pending	Tue May 12 2020 10:05:17 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 0 minute, 46 seconds ago	⊙ Please wait...	⊙ Please wait...

Your device will need to be rebooted after this operation.

Reboot

Output

```

[2020-05-12T08:05:18+00:00] DEBUG: Loading plugin at /opt/chef/embedded/lib/ruby/gems/2.3.0/gems/shai-8.20.0/lib/shai/plugins/ruby.rb
[2020-05-12T08:05:18+00:00] DEBUG: Loading plugin at /opt/chef/embedded/lib/ruby/gems/2.3.0/gems/shai-8.20.0/lib/shai/plugins/network.rb
[2020-05-12T08:05:18+00:00] DEBUG: Loading plugin at /opt/chef/embedded/lib/ruby/gems/2.3.0/gems/shai-8.20.0/lib/shai/plugins/powershell.rb
[2020-05-12T08:05:18+00:00] DEBUG: Loading plugin at /opt/chef/embedded/lib/ruby/gems/2.3.0/gems/shai-8.20.0/lib/shai/plugins/os.rb
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -s' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -r' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -v' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -m' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -p' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -o' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'env lscod' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin LSB: ran 'lsb_release -a' and returned 0
    
```

Download Output

10단계. 복원 성공 후 다시 부팅해야 합니다.

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 May 12 2020 10:05:17 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 34 minutes, 19 seconds ago	Tue May 12 2020 10:22:17 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 17 minutes, 19 seconds ago	0 day, 0 hour, 16 minutes, 59 seconds

Your device will need to be rebooted after this operation.

[Reboot](#)

Output

```
[2020-05-12T00:22:15+00:00] INFO: Mapping folders to ensure that they are valid
[2020-05-12T00:22:15+00:00] INFO: Running report handlers
[2020-05-12T00:22:15+00:00] INFO: Report handlers complete
[2020-05-12T00:22:15+00:00] DEBUG: Server doesn't support resource history, skipping resource report.
[2020-05-12T00:22:15+00:00] DEBUG: Audit Reports are disabled. Skipping sending reports.
[2020-05-12T00:22:15+00:00] DEBUG: Forked instance successfully reaped (pid: 97568)
[2020-05-12T00:22:15+00:00] DEBUG: Exiting
Sending system notification (this may take some time).
Running retryable command, 40 retries remaining.

-----
Chef run finished successfully
-----

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

[Download Output](#)

다음을 확인합니다.

어플라이언스를 재부팅한 후 두 포털이 모두 제대로 작동하는지 확인합니다. 웹 브라우저에서 OAdmin 및 콘솔 포털을 열어 보십시오. 두 포털에 모두 액세스하는 데 몇 분 정도 걸립니다.

문제 해결

백업 복원 프로세스의 경우 OAdmin 및 콘솔 포털의 비밀번호는 이전과 동일합니다. 그렇지 않으면 마법사에서 설정한 내용을 사용해야 합니다.