# Cisco AMP Threat Grid Appliance 설정 및 컨피그레이션 가이드

버전 2.1.6

**최종 업데이트:** 2017년 1월 5일

Cisco Systems, Inc. www.cisco.com

Cisco는 전 세계 200개가 넘는 지사를 운영하고 있습니다. 주소, 전화번호 및 팩스 번호는 Cisco 웹사이트 www.cisco.com/go/offices에 나와 있습니다.

# 목차

**그림 목록** ..... **IV**

**서론** ..... **1**

이 가이드의 대상 ..... 1
릴리스 노트 ..... 1
새로운 기능 ..... 1
*LDAP 인증* ..... *1*
*Cisco UCS C220 M4 Server* ..... *2*
*FireAMP Private Cloud 통합* ..... *2*
*버전 2.0* ..... *2*
지원 -- Threat Grid 문의 ..... 2
*지원 모드* ..... *3*
*지원 모드 시작 - 버전 1.4.4 이전의 라이선스 해결 방법* ..... *3*
*서버 지원* ..... *4*
*스냅샷 지원* ..... *4*

**계획** ..... **5**

사용자 설명서 및 온라인 도움말 ..... 5
환경 요구 사항 ..... 5
하드웨어 요구 사항 ..... 5
하드웨어 설명서 ..... 5
네트워크 요구 사항 ..... 6
*DNS 서버 액세스* ..... *6*
*NTP 서버 액세스* ..... *6*
통합 – ESA/WSA/FIRE AMP 등 ..... ***7***
DHCP ..... 7
라이선스 ..... ***7***
조직 및 사용자 ..... 7
업데이트 ..... ***7***
Threat Grid Appliance 사용자 인터페이스 ..... 7

*TGSH 대화 상자* ..... *7*
*OpAdmin 포털* ..... *8*
*AMP Threat Grid Portal* ..... *8*
*CIMC* ..... *8*
네트워크 인터페이스 ..... 8
*Admin 인터페이스* ..... *8*
*Clean 인터페이스* ..... *8*
*Dirty 인터페이스* ..... *9*
*CIMC 인터페이스* ..... *9*
*예약된 인터페이스* ..... *9*
로그인 이름 및 비밀번호 -- 기본값 ..... *9*
*웹 UI 관리자* ..... *9*
*OpAdmin 및 셸 사용자* ..... *9*
*CIMC(Cisco Integrated Management Controller)* ..... *10*
설정 및 컨피그레이션 단계 개요 ..... 10
설정 및 컨피그레이션에 필요한 시간 ..... 10

**서버 설정 ..... 11**

네트워크 인터페이스 연결 설정 ..... 11
*C220 M3 Rack Server 설정* ..... *11*
*C220 M4 Rack Server 설정* ..... *13*
네트워크 인터페이스 설정 다이어그램 ..... 15
방화벽 규칙 제안 사항 ..... 16
전원 켜기 및 부팅 ..... 17

**초기 네트워크 컨피그레이션 - TGSH 대화 상자 ..... 19**

**컨피그레이션 마법사 - OpAdmin 포털 ..... 24**

컨피그레이션 워크플로 ..... 25
OpAdmin 포털에 로그인 ..... 25
관리자 비밀번호 변경 ..... 27
최종 사용자 라이선스 계약 ..... 28
네트워크 컨피그레이션 설정 ..... 28
*네트워크 컨피그레이션 및 DHCP* ..... *28*
라이선스 설치 ..... 29
이메일 호스트 컨피그레이션 ..... 29

서버 알림 컨피그레이션 ..... 30
NTP 서버 컨피그레이션 ..... 31
컨피그레이션 설정 검토 및 설치 ..... 31
**Threat Grid Appliance 업데이트 설치 ..... 34**
어플라이언스 빌드 번호 ..... 34
*어플라이언스 빌드 번호/버전 조회표 ..... 35*
**어플라이언스 설정 테스트 - 샘플 제출 ..... 37**
**어플라이언스 관리 ..... 38**
**부록 A – CIMC 컨피그레이션(권장) ..... 39**

# 그림 목록

그림 1 - OpAdmin 에서 라이브 지원 세션 시작 ..... 4
그림 2 - Cisco 1000BASE-T 구리 SFP(GLC-T) ..... 5
그림 3 - Cisco UCS C220 M3 SFF Rack Server ..... 11
그림 4 - Cisco UCS C220 M3 후면 세부 정보 ..... 12
그림 5 - Cisco UCS C220 M4 SFF Rack Server ..... 13
그림 6 - Cisco UCS C220 M4 후면 세부 정보 ..... 13
그림 7 - 네트워크 인터페이스 설정 다이어그램 ..... 15
그림 8 - 부팅 중 Cisco 화면 ..... 17
그림 9 - TGSH 대화 상자 ..... 18
그림 10 - TGSH 대화 상자 - 네트워크 컨피그레이션 콘솔 ..... 19
그림 11 - 진행 중인 네트워크 컨피그레이션(Clean 및 Dirty) ..... 20
그림 12 - 진행 중인 네트워크 컨피그레이션(Admin) ..... 21
그림 13 - 네트워크 컨피그레이션 확인 ..... 22
그림 14 - 네트워크 컨피그레이션 - 변경 사항 목록 ..... 23
그림 15 - IP 주소 ..... 24
그림 16 - OpAdmin 로그인 ..... 26
그림 17 - OpAdmin 비밀번호 변경 ..... 27
그림 18 - 라이선스 페이지 ..... 28
그림 19 - 설치 후 라이선스 정보 ..... 29
그림 20 - 알림 컨피그레이션 ..... 30
그림 21 - 어플라이언스 설치 중 ..... 31
그림 22 - 어플라이언스 설치 완료 ..... 32
그림 23 - 어플라이언스 재부팅 중 ..... 33
그림 24 - 어플라이언스가 구성됨 ..... 33
그림 25 - 어플라이언스 빌드 번호 ..... 34
그림 26 - Threat Grid Portal 로그인 페이지 ..... 37
그림 27 - Cisco 화면 – F8 키로 컨피그레이션 유틸리티 시작 ..... 39
그림 28 - CIMC 컨피그레이션 유틸리티 ..... 40
그림 29 - CIMC(Cisco Integrated Management Controller) 인터페이스 ..... 41

# 서론

Cisco AMP Threat Grid Appliance는 심층 위협 분석 및 콘텐츠가 포함된 매우 안전한 온프레미스 지능형 악성코드 분석 기능을 제공합니다. Threat Grid Appliance는 완벽한 Threat Grid 악성코드 분석 플랫폼을 제공하며, 단일 UCS 서버(UCS C220-M3 또는 C220 M4)에 설치됩니다. 조직에서는 이 어플라이언스에 악성코드 샘플을 제출하여 다양한 규정 준수 및 정책 제한 사항에 따라 운영할 수 있습니다.

은행, 의료 서비스 등과 같이 민감한 데이터를 처리하는 많은 조직에서는 악성코드 아티팩트와 같은 특정 유형의 파일을 허용하지 않는 다양한 규정 및 가이드라인에 따라 악성코드를 네트워크 외부로 전송하여 분석을 수행해야 합니다. Cisco AMP Threat Grid Appliance를 온프레미스로 활용하면 의심스러운 문서 및 파일을 이 어플라이언스로 전송하여 네트워크를 벗어나지 않고도 분석할 수 있습니다.

보안 팀은 AMP Threat Grid Appliance를 사용해 강력한 보안을 갖춘 고정(static) 및 동적(dynamic) 분석 기술로 모든 샘플을 분석할 수 있습니다. 어플라이언스에서는 해당 분석 결과와 이전에 분석한 수억 개의 악성코드 아티팩트의 상관관계를 연구하여 악성코드 공격, 캠페인, 그 분포에 대한 종합적인 관점을 제시합니다. 관찰된 활동과 특성을 담은 단일 샘플과 수백만 개의 기타 샘플의 상관관계를 빠르게 분석하여 기록 내역과 전체적인 맥락을 바탕으로 해당 행동을 완전히 파악할 수 있습니다. 보안 팀에서는 이 기능을 사용하여 지능형 악성코드의 위협과 공격으로부터 조직을 효과적으로 방어할 수 있습니다.

# 이 가이드의 대상

새로운 어플라이언스를 조직의 네트워크에 맞게 설정 및 구성한 다음 사용해야 악성코드를 분석할 수 있습니다. 이 가이드는 새로운 Threat Grid Appliance의 설정 및 구성을 담당하는 보안 팀 IT 직원을 위한 것입니다.

이 문서에서는 악성코드 분석을 위한 샘플을 제출할 수 있는 지점까지 새로운 Threat Grid Appliance를 초기에 설정하고 컨피그레이션을 완료하는 방법을 설명합니다.

자세한 내용은 Cisco AMP *Threat Grid Appliance 관리자 가이드*를 참조하십시오. 이 가이드는 Cisco.com의 **Install and Upgrade(설치 및 업그레이드) 페이지**에서 확인할 수 있습니다.

# 릴리스 정보

자세한 업데이트 정보는 OpAdmin 포털의 다음 위치에 있는 *릴리스 노트*를 참조하십시오.

**Operations(운영)** 메뉴 > **Update Appliance(어플라이언스 업데이트)**

*Threat Grid Appliance 릴리스 노트*의 형식화된 PDF 버전도 **온라인에서 사용 가능**합니다.

버전 조회표: Threat Grid Appliance 릴리스 정보의 목록은 *Threat Grid Appliance 관리자 가이드*의 업데이트 설치 섹션을 참조하십시오.

**참고:** Threat Grid Portal UI에 대한 릴리스 노트를 보려면 UI 내비게이션 바의 **Help(도움말)**를 클릭합니다.

# 새로운 기능

새로운 기능에 대한 전체적인 설명은 항상 *릴리스 노트*를 확인하십시오. 주요 특징에 대한 내용이 여기에 나와 있습니다.

## LDAP 인증

고객이 동일한 로그인 및 비밀번호를 공유하는 것을 원하지 않는 여러 어플라이언스 관리자와 함께 고객을 지원할 목적으로 LDAP 인증이 2017년 1월 5일에 릴리스된 버전 2.1.6의 OpAdmin 및 TGSH 대화 상자 관리자 인터페이스에 추가되었습니다. 자세한 내용은 *Threat Grid 관리자 가이드*를 참조하십시오.

## Cisco UCS C220 M4 Server

2016년 11월 17일에 릴리스된 C220 M4 Server는 하드웨어 새로 고침뿐만 아니라 보안 부팅 기능도 포함합니다. 업그레이드에 대해 질문 사항을 의논하려는 경우 support@threatgrid.com으로 문의하십시오.

**참고:** Threat Grid는 계약된 수명 주기가 만료될 때까지 M3를 계속해서 지원할 예정입니다. M4의 모든 동일한 기능도 기존 M3의 유선을 통한 업데이트로 사용할 수 있습니다.

M5 서버 업그레이드가 현재 개발 중에 있습니다. Cisco는 기존의 M3 및 M4 고객이 고객의 요구사항에 가장 적합한 서버 업그레이드와 데이터 마이그레이션, 백업, 출시 전략 등에 대한 질문 사항을 의논하려는 경우 support@threatgrid.com으로 문의할 것을 강력하게 권장합니다. 현재 개발 중인 Threat Grid Appliance 소프트웨어의 버전 2.1.5로의 마이그레이션을 통해 추가적인 복잡성이 도입되었습니다. Cisco는 M5의 업그레이드 경로를 계획하기 위한 최고의 접근 방식은 고객의 요구 사항을 개별적으로 해결하는 것이라고 생각합니다.

## FireAMP Private Cloud 통합

2.0.3 릴리스는 Clean 및 Dirty 네트워크 인터페이스 간의 DNS를 분할하는 기능, CA 관리 및 FireAM Private Cloud 통합 컨피그레이션을 포함하여 Threat Grid Appliance와 Fire AMP Private Cloud의 통합을 지원하는 기능을 포함합니다.

생성한 SSL 인증서는 현재 subjectAltName으로 중복된 CN을 지닙니다. 이는 최소 1개 이상의 subjectAltName이 존재하는 경우 CN 필드를 무시하는 SSL 클라이언트와의 비호환성을 다룹니다. 이러한 툴을 사용하는 경우 이전의 어플라이언스 생성 인증서를 다시 생성해야 할 수 있습니다.

## 버전 2.0

버전 2.0은 업데이트된 운영 체제에 구축되는 주요 릴리스입니다. 이 릴리스는 향후 하드웨어 릴리스를 지원하는 개선 기능을 포함할 뿐만 아니라, 클라우드 버전에 더욱 적합한 Threat Grid Portal UI도 선보입니다. 여기에는 새롭게 업데이트된 여러 가지 행동 지표 및 기타 변경 사항이 포함됩니다.

자세한 내용은 릴리스 3.3.45로 시작하는 *Threat Grid Portal 릴리스 노트*를 참조하십시오. Portal UI 내비게이션 바에서 **Help**(도움말)를 선택한 다음 릴리스 정보 링크를 클릭합니다. 릴리스 노트는 누적되며 가장 최신 버전에 이전 정보가 모두 포함되어 있습니다.

# 지원 - Threat Grid 문의

다음과 같이 다양한 방법으로 Threat Grid 엔지니어의 지원을 요청할 수 있습니다.

**이메일:** 질문이 있는 경우 support@threatgrid.com으로 이메일을 보내주십시오.

**지원 사례 열기:** 지원 사례를 열려면 Cisco.com ID가 있어야 합니다(없을 경우 생성). 또한 주문 송장에 포함된 서비스 계약 번호가 있어야 합니다. https://tools.cisco.com/ServiceRequestTool/scm/mgmt/case에 지원 사례를 입력합니다.

**전화:** Cisco 전화 번호는 http://www.cisco.com/c/en/us/support/index.html을 참조하십시오.

Threat Grid에서 지원을 요청할 때 다음 정보를 함께 보내주시기 바랍니다.

- 어플라이언스 버전: **OpAdmin > Operations(운영) > Update Appliance(어플라이언스 업데이트)**
- 전체 서비스 상태(셸의 서비스 상태)
- 네트워크 다이어그램 또는 설명(해당하는 경우)
- 지원 모드(셸 또는 웹 인터페이스)
- 지원 요청 세부 정보

## 지원 모드

Threat Grid 엔지니어의 지원을 요청하는 경우 Threat Grid 지원 엔지니어가 어플라이언스에 원격으로 액세스할 수 있도록 라이브 지원 세션인 "지원 모드"를 활성화해 달라고 요청할 수 있습니다. 어플라이언스의 정상적인 작동에는 영향을 미치지 않습니다. 이 작업은 **OpAdmin Portal Support(OpAdmin 포털 지원)** 메뉴를 통해 수행될 수 있습니다. TGSH 대화 상자에서도 **SUPPORT MODE(지원 모드)**를 활성화할 수 있습니다.

**Threat Grid 기술 지원을 사용하여 라이브 지원 세션을 시작하려면 다음을 수행합니다.**

**OpAdmin**에서 **Support(지원) > Live Support Session(라이브 지원 세션)**을 선택하고 **Start Support Session(지원 세션 시작)**을 클릭합니다.

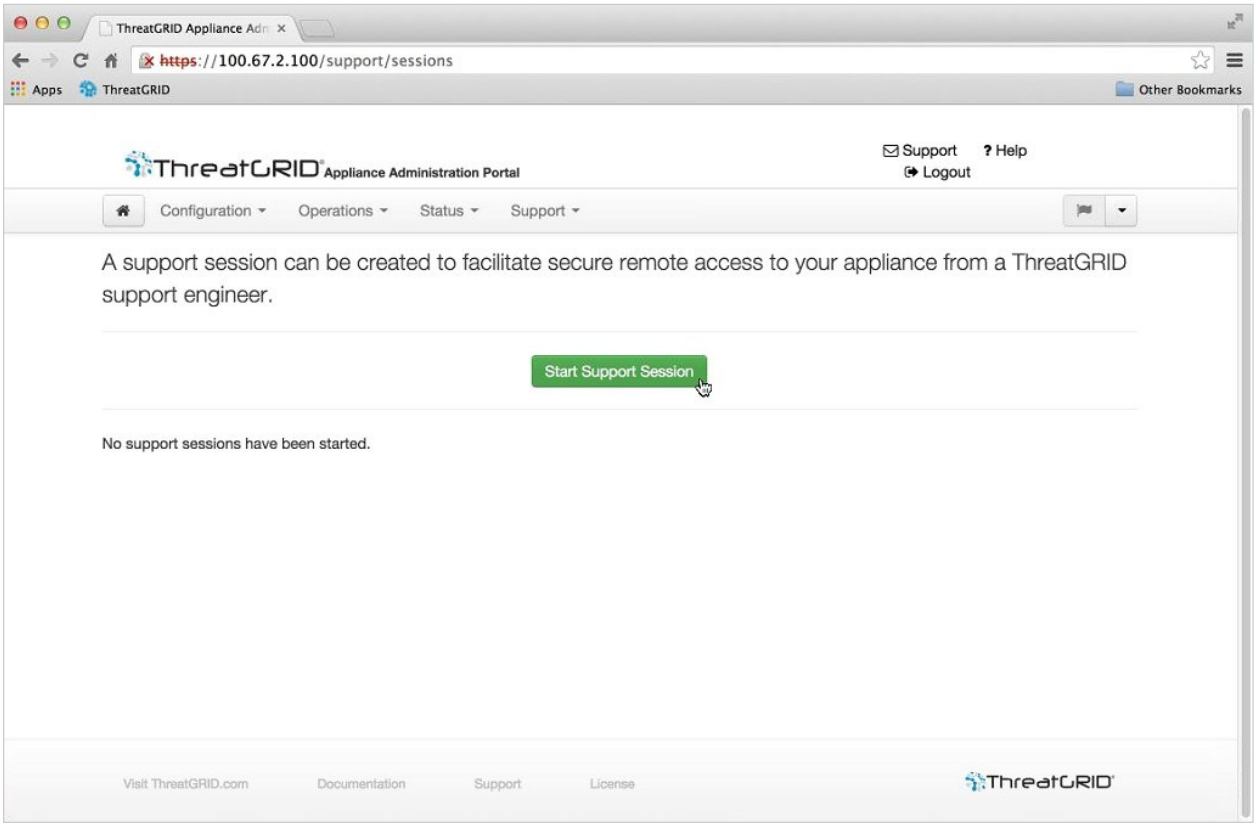
**참고:** 라이선싱 이전에 OpAdmin 마법사 작업 흐름을 중단하고 Support Mode(지원 모드)를 활성화할 수 있습니다.

## 지원 모드 시작 - 버전 1.4.4 이전의 라이선스 해결 방법

Threat Grid Appliance v 1.4.4에서 해결된 라이선스 문제가 있습니다. 소프트웨어 버전이 1.4.4 이전 버전인 경우, 라이선스를 허용하기 위해 *지원 모드* 서버에 최소한 한 번 이상(2015년 11월 14일 이후) 연결해야 합니다. 라이선스 검증 시점에 이러한 연결을 진행하고 있거나 활성화할 필요가 없습니다.

**필수:** 이 단계가 작동하려면 Dirty 네트워크를 가동해야 합니다.

**그림 1 - OpAdmin에서 라이브 지원 세션 시작**




## 서버 지원

지원 세션을 설정하려면 TG 어플라이언스에서 다음 서버에 연결해야 합니다.

- support-snapshots.threatgrid.com
- rash.threatgrid.com

두 서버 모두 활성 지원 세션 동안 방화벽에서 허용되어야 합니다.

## 스냅샷 지원

스냅샷 지원은 기본적으로 실행 중인 시스템의 스냅샷으로, 로그 및 ps 출력 등이 포함되어 있어 지원 담당자가 트러블슈팅하는 데 도움이 됩니다.

1. SSH가 지원 스냅샷 서비스를 위해 지정되어 있는지 확인합니다.
2. **Support(지원)** 메뉴에서 **Support Snapshots(스냅샷 지원)**를 선택합니다.
3. 스냅샷을 찍습니다.
4. 찍은 스냅샷을 직접 .tar .gz로 다운로드하거나 **Submit(제출)**을 눌러 Threat Grid 스냅샷 서버에 자동으로 업로드할 수 있습니다.

# 계획

Cisco AMP Threat Grid Appliance는 배송에 앞서 Cisco Manufacturing에서 Threat Grid 소프트웨어를 설치한 Linux 서버입니다. 새 어플라이언스를 수령하면 온프레미스 네트워크 환경에 맞게 설정 및 구성해야 합니다. 시작하기 전에 다양한 문제를 고려하고 계획해야 합니다. 아래에는 환경 요구 사항, 하드웨어 요구 사항, 네트워크 요구 사항이 설명되어 있습니다.

# 사용자 설명서 및 온라인 도움말

**Threat Grid Appliance -** Threat Grid Appliance 사용자 설명서(이 문서, *Threat Grid Appliance 관리자 가이드*, 릴리스 노트, 통합 가이드 등 포함)는 Cisco.com의 **Install and Upgrade(설치 및 업그레이드) 페이지**에서 확인할 수 있습니다.

**Threat Grid Portal UI 온라인 도움말** - 릴리스 노트, "Threat Grid 사용" 온라인 도움말, API 설명서를 포함하는 Threat Grid Portal 사용자 설명서 및 기타 정보는 사용자 인터페이스 상단에 있는 내비게이션 바에 위치한 **Help(도움말)** 메뉴에서 사용할 수 있습니다.

# 환경 요구 사항

Threat Grid Appliance는 UCS C220-M3 또는 C220-M4 Server에 구축됩니다. 어플라이언스를 설정 및 구성하기 전에 서버 사양에 따라 전원, 랙 공간, 냉각 및 기타 문제에 대한 필수 환경이 충족되는지 확인해야 합니다.

# 하드웨어 요구 사항

Admin 인터페이스의 폼 팩터는 SFP+입니다. 스위치에 사용 가능한 SFP+ 포트가 없거나 SFP+가 바람직하지 않은 경우 1000Base-T용 트렌시버를 사용하면 됩니다(예: Cisco 호환 기가비트 RJ 45 구리 SFP 트렌시버 모듈 미니 -GBIC - 10/100/1000 Base-T 구리 SFP 모듈).

**그림 2 - Cisco 1000BASE-T 구리 SFP(GLC-T)**

**모니터:** 서버에 모니터를 연결하거나 CIMC(Cisco Integrated Management Controller)를 구성한 경우, 원격 KVM을 사용할 수 있습니다.

# 하드웨어 설명서

**Cisco UCS C220 M4 Server 설치 및 서비스 가이드:**

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/C220M4/install/C220M4.pdf

**Cisco UCS C220 M3 Server 설치 및 서비스 가이드:**

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/C220/install/C220.html

**Cisco UCS C220 M3 High-Density Rack Server(소형 폼 팩터 디스크 드라이브 모델) 사양 시트:**

http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/C220M3_SFF_SpecSheet.pdf

**다음 사이트를 방문하면 Cisco에서 제공하는 유용한 전력/냉각 계산기를 사용할 수 있습니다.**

https://mainstayadvisor.com/Go/Cisco/Cisco-UCS-Power-Calculator.aspx

# 네트워크 요구 사항

Threat Grid Appliance에는 다음과 같이 3개의 네트워크가 필요합니다.

**Admin** - "*Admin*" 네트워크입니다. 이 네트워크를 구성해야 어플라이언스를 설정할 수 있습니다.

**Clean** - "*Clean*" 네트워크는 신뢰할 수 있는 트래픽을 어플라이언스로 보내는(요청) 데 사용됩니다. 여기에는 통합 어플라이언스가 포함됩니다. 예를 들어 Cisco ESA/WSA(Email Security Appliance/Web Security Appliance)에서는 Clean 인터페이스의 IP 주소에 연결합니다.

**참고:** 네트워크 트래픽에서 다음과 같이 특정한 제한된 유형은 Clean에서 아웃바운드될 수 있습니다.

- 원격 syslog 연결
- Threat Grid Appliance 자체에서 전송된 이메일 메시지
- FireAMP Private Cloud 디바이스에 대한 Disposition Update Service 연결
- 위의 모든 내용과 관련된 DNS 요청

**Dirty** - "*Dirty*" 네트워크는 어플라이언스의 아웃바운드 트래픽(악성코드 트래픽 포함)에 사용됩니다.

**참고:** 내부 네트워크 자산을 보호하려면 회사 IP와 다른 전용 외부 IP 주소(즉, "*Dirty*" 인터페이스)를 사용하는 것이 좋습니다.

네트워크 인터페이스 설정 정보 및 그림의 경우, 아래에서 네트워크 인터페이스 및 네트워크 인터페이스 연결 설정 섹션을 참조하십시오.

## DNS 서버 액세스

Disposition Update Service 조회 이외의 목적에 사용된 DNS 서버는 원격 syslog 연결을 분석하고 Threat Grid 소프트웨어 자체의 알림에 사용된 메일 서버를 분석하며 Dirty 네트워크를 통해 액세스 가능해야 합니다.

기본적으로 DNS는 Dirty 인터페이스를 사용합니다. Clean 인터페이스는 FireAMP Private Cloud 통합에 사용됩니다. FireAMP Private Cloud 호스트 이름을 Dirty 인터페이스를 통해 해석할 수 없는 경우, Clean 인터페이스를 사용하는 개별 DNS 서버를 OpAdmin 인터페이스에서 구성할 수 있습니다.

추가 정보는 *Threat Grid Appliance 관리 가이드*를 참조하십시오.

## NTP 서버 액세스

Dirty 네트워크를 통해 NTP 서버에 액세스할 수 있어야 합니다.

# 통합 – ESA/WSA/FireAMP 등

Threat Grid Appliance를 ESA/WSA 어플라이언스, FireAMP Private Cloud 등 다른 Cisco 제품과 함께 사용하려는 경우 추가 계획이 필요할 수 있습니다.

# DHCP

DHCP를 사용하도록 구성된 네트워크에 연결된 경우 **Using DHCP(DHCP 사용)** 섹션에 있는 지침을 따르십시오(*Threat Grid Appliance 관리자 가이드).*

# 라이선스

Cisco AMP Threat Grid에서 라이선스 및 비밀번호가 제공됩니다.

라이선스에 대한 질문의 경우, support@threatgrid.com으로 문의하십시오.

# 조직 및 사용자

어플라이언스 설정 및 네트워크 컨피그레이션을 완료한 경우, 사용자가 로그인하여 분석용 악성코드 샘플을 제출할 수 있으려면 초기 Threat Grid 조직 및 사용자 어카운트를 만들어야 합니다. 이 작업에서는 요구 사항에 따라 다양한 조직 및 사용자와 팀을 계획하고 조정해야 합니다.

Threat Grid 조직 및 사용자 관리는 *Threat Grid Appliance 관리자 가이드*에 나와 있습니다.

# 업데이트

Threat Grid Appliance 업데이트를 설치하기에 앞서 초기 어플라이언스 설정 및 컨피그레이션 단계를 **완료해야 합니다**.

이 가이드에 설명된 초기 컨피그레이션을 완료한 후 즉시 업데이트를 확인하는 것이 좋습니다.

업데이트는 순차적으로 수행해야 합니다. 라이선스를 설치한 후 Threat Grid Appliance 업데이트를 다운로드할 수 있으며, 업데이트 프로세스에서 초기 어플라이언스 컨피그레이션을 완료해야 합니다. 어플라이언스 업데이트 지침은 *Threat Grid Appliance 관리자 가이드*에 있습니다.

**참고:** SSH가 업데이트를 위해 지정되어 있는지 확인합니다.

# Threat Grid Appliance 사용자 인터페이스

서버가 네트워크에 제대로 연결되어 전원이 켜지면 다양한 사용자 인터페이스를 사용하여 Threat Grid Appliance를 구성할 수 있습니다. LDAP 인증은 버전 2.1.6의 TGSH 대화 상자 및 OpAdmin에 사용할 수 있습니다.

## TGSH 대화 상자

첫 번째 인터페이스는 **TGSH Dialog(TGSH 대화 상자)**로, 네트워크 인터페이스를 구성하는 데 사용됩니다. TGSH Dialog(TGSH 대화 상자)는 어플라이언스가 부팅될 때 표시됩니다.

### TGSH Dialog(TGSH 대화 상자)에 다시 연결

TGSH 대화 상자가 콘솔에 계속 열려 있으므로 어플라이언스에 모니터를 연결하거나, CIMC가 구성된 경우 원격 KVM을 통해 액세스할 수 있습니다.

TGSH 대화 상자에 다시 연결하려면 사용자 '**threatgrid**'로 관리 IP 주소에 SSH 액세스합니다.

필수 비밀번호는 임의로 생성되어 초기에 TGSH 대화 상자에 표시되는 초기 비밀번호 또는 다음 섹션에 설명된 대로 OpAdmin 포털 컨피그레이션의 첫 단계에서 만드는 새 관리자 비밀번호입니다.

## OpAdmin 포털

기본 Threat Grid GUI 컨피그레이션 툴입니다. 라이선스, 이메일 호스트, SSL 인증서 등을 포함한 대부분의 어플라이언스 컨피그레이션은 OpAdmin을 통해서만 수행할 수 있습니다.

## AMP Threat Grid 포털

Threat Grid 사용자 인터페이스 애플리케이션을 클라우드 서비스로 사용할 수 있으며, Threat Grid Appliance에 설치할 수도 있습니다. Threat Grid Cloud 서비스 및 Threat Grid Appliance에 포함된 Threat Grid Portal 간에는 통신하지 않습니다.

## CIMC

또 다른 사용자 인터페이스로는 서버 관리에 사용하는 "CIMC"(Cisco Integrated Management Controller)가 있습니다.

# 네트워크 인터페이스

## Admin 인터페이스

- Admin 네트워크에 연결합니다. Admin 네트워크의 **인바운드 전용**입니다.
- OpAdmin UI 트래픽
- tgsh-dialog의 SSH(인바운드)

**참고:** Admin 인터페이스의 폼 팩터는 SFP+입니다. 그림 2 - Cisco 1000BASE-T 구리 SFP(GLC-T)를 참조하십시오.

## Clean 인터페이스

- Clean 네트워크에 연결합니다. Clean은 기업 네트워크에서 액세스할 수 있어야 하지만 복구 모드를 제외하고 인터넷에 대한 아웃바운드 액세스가 필요하지 않습니다.
- UI 및 API 트래픽(인바운드)
- 샘플 제출
- SMTP(구성된 메일 서버에 대한 아웃바운드 연결)
- 복구 모드 지원 세션(아웃바운드)
- SSH(TGSH 대화 상자용 인바운드)

- 시스템 로그(구성된 시스템 로그 서버에 대한 아웃바운드)
- ESA/WSA – CSA 통합
- FireAMP Private Cloud 통합
- DNS – 선택 사항

### Dirty 인터페이스

- Dirty 네트워크에 연결합니다. 인터넷 액세스가 필요합니다. **아웃바운드 전용입니다.**
- DNS

  **참고:** FireAMP Private Cloud와의 통합을 설정 중인 경우, FireAMP 어플라이언스 호스트 이름은 Dirty 인터페이스를 통해 분석될 수 없으며 Clean 인터페이스를 사용하는 개별 DNS 서버는 OpAdmin에서 구성될 수 있습니다.
- NTP
- 업데이트
- 정상 작동 모드의 지원 세션
- 스냅샷 지원
- 악성코드 샘플 개시 트래픽

### CIMC 인터페이스

권장. CIMC(Cisco Integrated Management Controller) 인터페이스가 구성된 경우, 서버 관리 및 유지 보수에 사용될 수 있습니다. 자세한 내용은 부록 A – CIMC 컨피그레이션(권장)을 참조하십시오.

### 예약된 인터페이스

비관리 SFP+ 포트는 나중에 사용하기 위해 예약되어 있습니다.

## 로그인 이름 및 비밀번호 - 기본값

### 웹 UI 관리자

**로그인:** admin

**비밀번호:** "changeme"

### OpAdmin 및 셸 사용자

초기에는 Threat Grid/TGSH 대화 상자 임의 생성 비밀번호를 사용한 다음 OpAdmin 컨피그레이션 창의 첫 단계에서 입력한 새 비밀번호를 사용합니다.

비밀번호를 분실한 경우 **분실한 비밀번호** 지침(**지원** 섹션, *Threat Grid Appliance 관리자 가이드* 참조)을 따르십시오.

### CIMC(Cisco Integrated Management Controller)

**로그인:** admin

**비밀번호:** "password"

## 설정 및 컨피그레이션 단계 개요

이 문서에는 다음과 같은 설정 및 초기 컨피그레이션 단계가 설명되어 있습니다.

서버 설정

네트워크 인터페이스 연결 설정:

- Admin
- Clean
- Dirty

초기 네트워크 컨피그레이션 - TGSH 대화 상자

기본 컨피그레이션 – OpAdmin 포털

업데이트 설치

어플라이언스 설정 테스트: 분석용 샘플 제출

관리 컨피그레이션 – *Threat Grid Appliance 관리자 가이드*에 설명된 대로 OpAdmin 포털에서 나머지 관리 컨피그레이션 작업(라이선스 설치, 이메일 서버, SSL 인증서 등)을 완료합니다.

## 설정 및 컨피그레이션에 필요한 시간

서버 설정 및 초기 컨피그레이션 단계를 완료하는 데 1시간 정도 걸릴 수 있습니다.

**참고:** 초기 어플라이언스 컨피그레이션 설치 단계에서 TGSH 대화 상자의 "적용" 섹션을 수행하는 동안 기다려 주십시오.

해당 단계를 완료하는 데 10분 이상 걸릴 수 있습니다.

# 서버 설정

시작하려면 아래 그림과 같이 어플라이언스 후면의 두 전원 공급 장치를 연결하고, 포함된 KVM 어댑터를 외부 모니터 및 키보드에 연결한 후 서버 전면에 있는 KVM 포트에 꽂습니다.

CIMC를 구성한 경우 원격 KVM을 사용할 수 있습니다. CIMC 컨피그레이션에 대해서는 **CIMC 구성(선택 사항)**을 *부록*에서 참조하십시오.

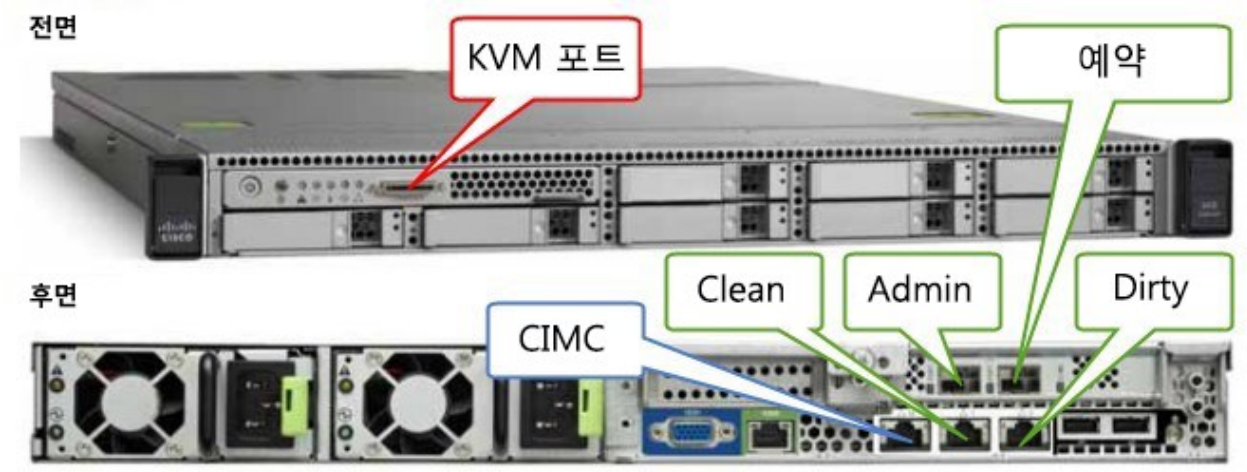
자세한 하드웨어 및 환경 설정 정보는 서버 제품의 설명서를 참조하십시오. 제품 설명서에 대한 링크는 위의 하드웨어 설명서 섹션에 있습니다.

# 네트워크 인터페이스 연결 설정

아래 그림과 같이 어플라이언스 후면에서 SFP+ 포트(2개) 및 3개의 Ethernet 포트를 찾아 네트워크 케이블을 연결합니다.

## C220 M3 Rack Server 설정

**그림 3 - Cisco UCS C220 M3 SFF Rack Server**



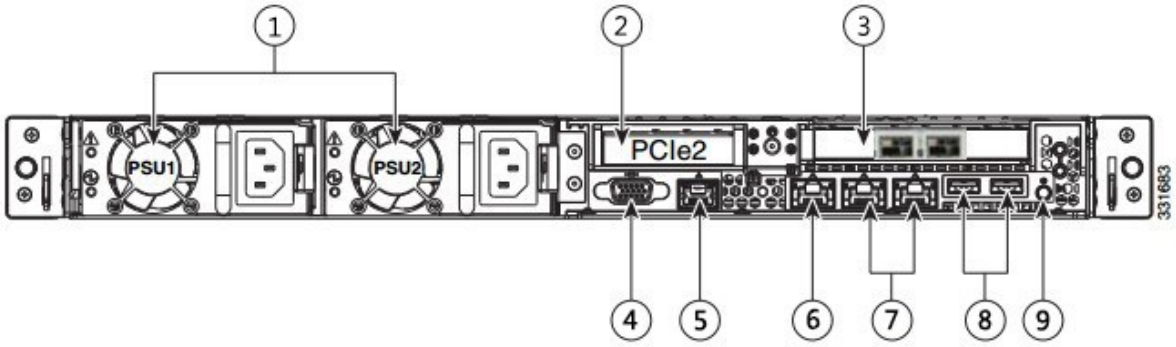

어플라이언스에 인터페이스를 올바르게 연결하고 구성해야 작동합니다.

**참고:** 어플라이언스의 세부 정보는 위의 이미지와 다를 수 있습니다. 질문이 있는 경우 **support@threatgrid.com**으로 문의하십시오.

**참고:** "Reserved"는 비관리 SFP+ 포트로, 나중에 사용하기 위해 예약되어 있습니다.

C220 M3 서버에 대한 자세한 내용은 아래 그림을 참조하십시오.

**그림 4 - Cisco UCS C220 M3 후면 세부 정보**

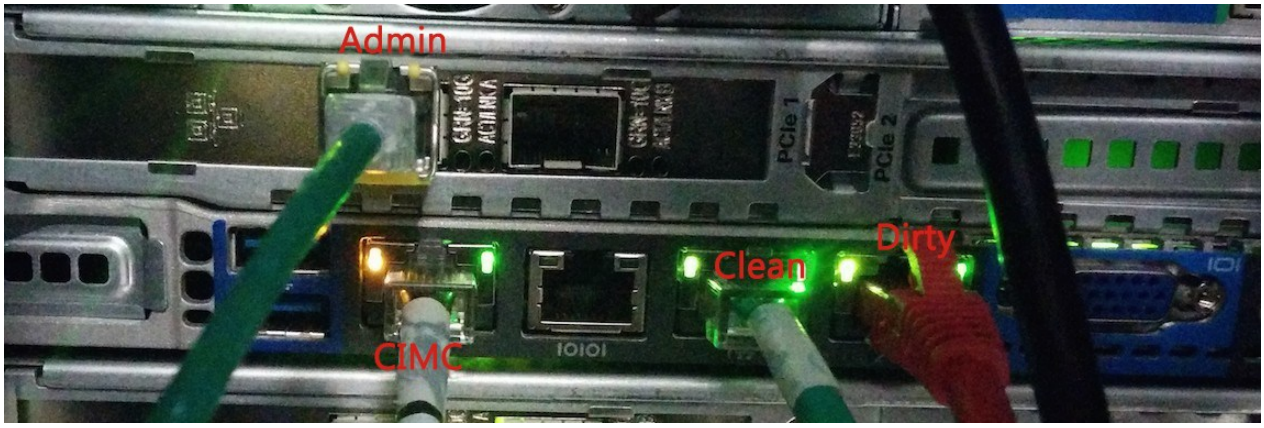



| | | | |
|---|---|---|---|
| 1 | 전원 공급 장치(최대 2개) | 6 | 10/100/1000 Ethernet 전용 관리 포트 1개 |
| 2 | 슬롯 2: 라이저의 로우 프로필 PCIe 슬롯:<br>(절반 높이, 절반 길이, x16 커넥터, x8 레인 폭) | 7 | 듀얼 1GbE 포트<br>(LAN1 및 LAN2) |
| 3 | 두 개의 SFP+ 포트<br>슬롯 1: 관리<br>슬롯 2: 백업 및 스토리지 지원용 예비 | 8 | USB 포트 |
| 4 | VGA 비디오 커넥터 | 9 | 후면 식별 버튼/LED |
| 5 | 시리얼 포트(RJ-45 커넥터)1 | – | – |

**참고:** 릴리스 1.0~1.2에서는 부팅 시 인터페이스가 연결되지 않은 경우 재부팅해야 할 수 있습니다. 이러한 문제는 1.3 이전에서 나타나는 것으로, 1.3 이후에서는 부팅 시점에 SFP가 계속 연결되어 있어야 하는 인터페이스에서만 발생합니다. SFP에 연결된 네트워크 케이블은 안전하게 핫 플러그 연결할 수 있습니다.

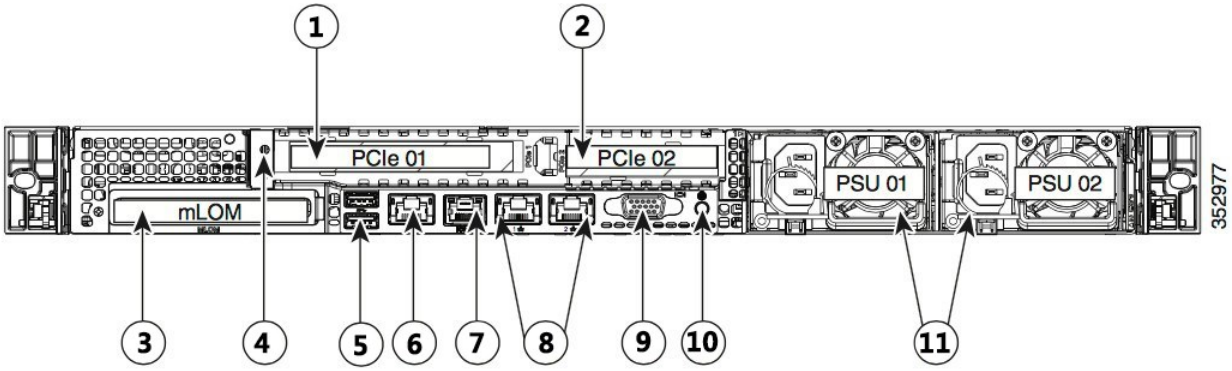
# C220 M4 Rack Server 설정

**그림 5 - Cisco UCS C220 M4 SFF Rack Server**




**참고:** 어플라이언스의 세부 정보는 위의 이미지와 다를 수 있습니다. 질문이 있는 경우 **support@threatgrid.com**으로 문의하십시오.

**그림 6 - Cisco UCS C220 M4 후면 세부 정보**




| | | | |
|---|---|---|---|
| **1** | PCIe 라이저 1/슬롯 1 | **7** | 시리얼 포트(RJ-45 커넥터) |
| **2** | PCIe 라이저 2/슬롯 2 | **8** | 이중 1Gb 이더넷 포트(LAN1 및 LAN2) |
| **3** | mLOM(Modular LAN-on-motherboard) 카드 슬롯 | **9** | VGA 비디오 포트(DB-15) |
| **4** | 접지 러그 홀(DC 전원 공급 장치) | **10** | 후면 장치 식별 버튼/LED |
| **5** | USB 3.0 포트 2개 | **11** | 전원 공급 장치(최대 2개, 1+1 이중화) |
| **6** | 1-Gb 이더넷 전용 관리 포트 | | |

**연결:**

**1 Admin**

**8 (왼쪽) Clean**

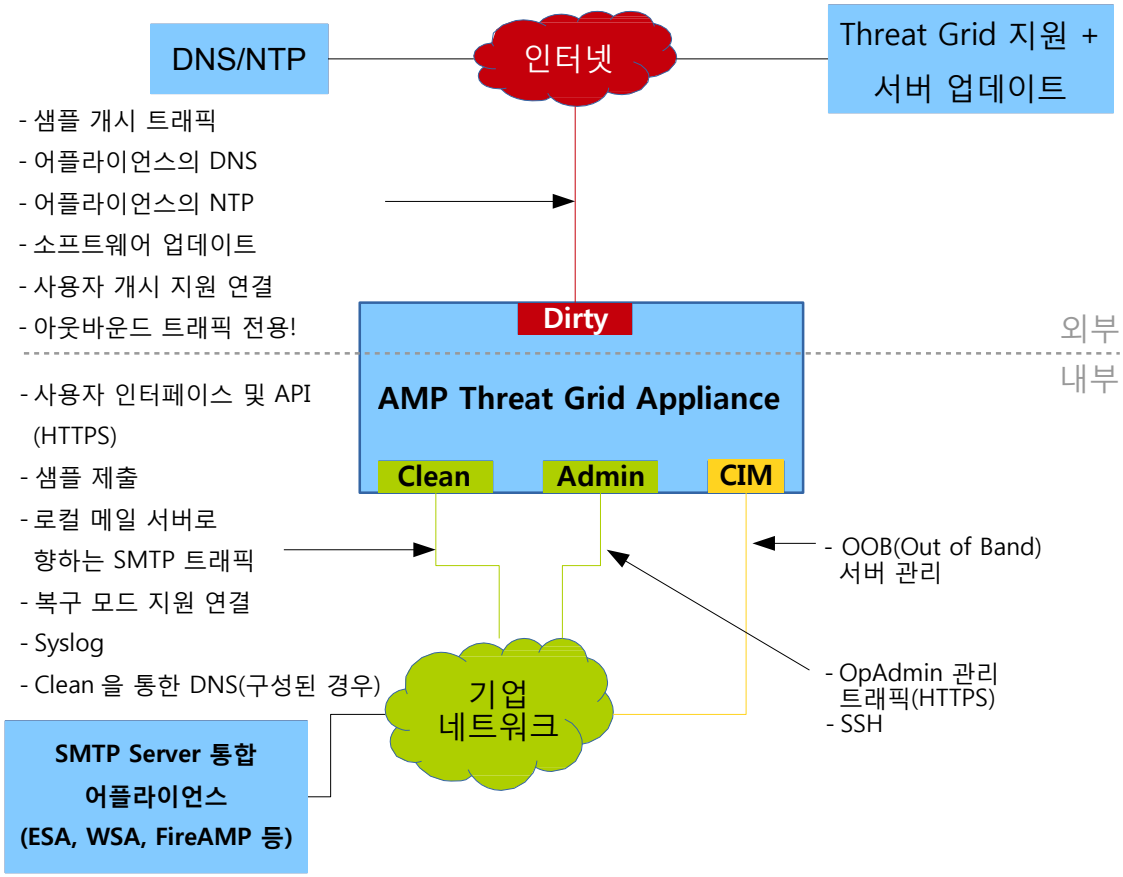
**8 (오른쪽) Dirty**

**6 CIMC**

# 네트워크 인터페이스 설정 다이어그램

이 섹션에서는 가장 논리적이고 권장되는 AMP Threat Grid Appliance 설정을 설명합니다. 그러나 각 고객의 인터페이스 설정은 다릅니다. 예를 들어 네트워크 요구 사항에 따라 적절한 네트워크 보안 조치를 취해 Dirty 인터페이스를 내부에 연결하거나 Clean 인터페이스를 외부에 연결하도록 결정할 수 있습니다.

**그림 7 - 네트워크 인터페이스 설정 다이어그램**



# 방화벽 규칙 제안 사항

| 변경 전 | 변경 후 | 프로토콜/포트 | 조치 | 이유 |
|---|---|---|---|---|
| Dirty 인터페이스 | 인터넷 | SMTP | 거부 | 스팸을 통한 악성코드 방지 |
| Dirty 인터페이스 | 인터넷 | TCP/19791 | 허용 | Threat Grid 지원에 대한 연결 허용 |
| Dirty 인터페이스 | 인터넷 | TCP/22 | 허용 | 스냅샷 서비스 업데이트 및 지원 |
| Dirty 인터페이스 | 인터넷 | IP/ANY | 허용 | 악성코드 샘플의 아웃바운드 트래픽 허용<br><br>정확한 결과를 얻으려면 악성코드를 해당 명령 및 제어 서버에 연결할 수 있어야 합니다. |
| Dirty 인터페이스 | 인터넷 | DNS | 허용 | 아웃바운드 DNS 허용 |
| Dirty 인터페이스 | 인터넷 | NTP<br><br>(UDP/123) | 허용 | 아웃바운드 트래픽에서 NTP에 액세스할 수 있도록 허용 |
| Clean 인터페이스 | SMTP 서버 | SMTP | 허용 | 어플라이언스에서 Clean 인터페이스를 사용하여 구성된 메일 서버에 SMTP 연결을 시작합니다. Clean 인터페이스에서는 "인터넷에 대한" 아웃바운드 연결이 필요하지 않습니다. |
| Clean 인터페이스 | 인터넷 | TCP/19791 | 허용 | Thread Grid 복구 모드 지원에 대한 연결 허용 |
| 사용자 네트워크 | Clean 인터페이스 | TCP/80<br>TCP/443 | 허용 | 어플라이언스 API 및 사용자 인터페이스 |
| Clean 인터페이스 | 사용자 네트워크 | 시스템 로그/구성 가능 | 허용 | 지정된 서버에 연결하여 시스템 로그 메시지 및 Threat Grid 알림을 수신하도록 허용 |
| 관리 네트워크 | Admin 인터페이스 | TCP/22<br>TCP/80<br>TCP/443 | 허용 | SSH<br><br>OpAdmin 포털 인터페이스 |
| 사용자 네트워크 | Clean 인터페이스 | TCP/9443 | 허용 | Threat Grid UI Glovebox 연결 허용 |

| 변경 전 | 변경 후 | 프로토콜/포트 | 조치 | 이유 |
|---|---|---|---|---|
| Clean 인터페이스 | 기업 DNS 서버 | UDP/53 및 TCP/53 | 허용 | 선택 사항이며 Clean DNS가 구성된 경우에만 필수 |
| Clean 인터페이스 | FireAMP Private Cloud | TCP/443 | 허용 | 선택 사항이며 FireAMP Private Cloud 통합을 사용하는 경우에만 필수 |

# 전원 켜기 및 부팅

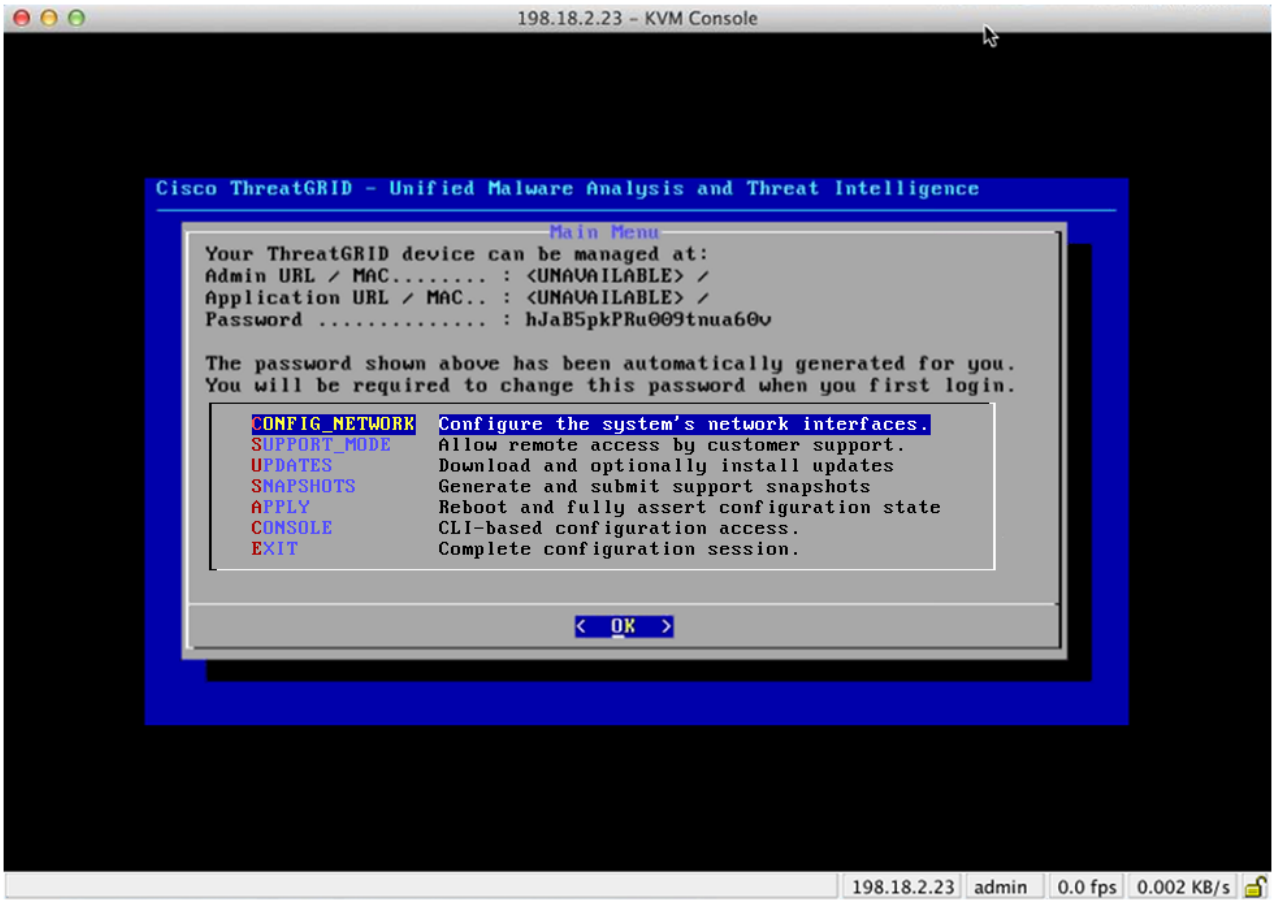
서버 주변 장치 및 네트워크 인터페이스를 연결한 후에는 어플라이언스를 켜고 부팅될 때까지 기다립니다. 다음과 같은 Cisco 화면이 잠시 표시됩니다.

**그림 8 - 부팅 중 Cisco 화면**


**참고:** 이 인터페이스를 구성하려면 메모리 검사가 완료된 후 **F8** 키를 누른 다음 *CONFIGURING CIMC 구성(선택 사항)* 섹션에 있는 지침을 따르십시오.

서버의 부팅 및 연결이 완료되면 콘솔에 **TGSH 대화 상자**가 표시됩니다.

**그림 9 - TGSH 대화 상자**




관리 URL이 사용할 수 없음으로 표시됩니다. 네트워크 인터페이스 연결이 아직 구성되지 않았으며 이 작업을 수행하기 위해 OpAdmin 포털에 연결할 수 없습니다.

**참고:** 편의를 위해 OpAdmin 포털 컨피그레이션 단계에서 관리자 비밀번호를 별도의 텍스트 파일에 기록(복사-붙여넣기)하십시오.

**중요:** 나중에 컨피그레이션 워크플로 단계에서 OpAdmin 포털 인터페이스에 액세스하고 해당 인터페이스를 구성하는 데 필요한 초기 관리자 비밀번호가 **TGSH 대화 상자**에 표시됩니다.

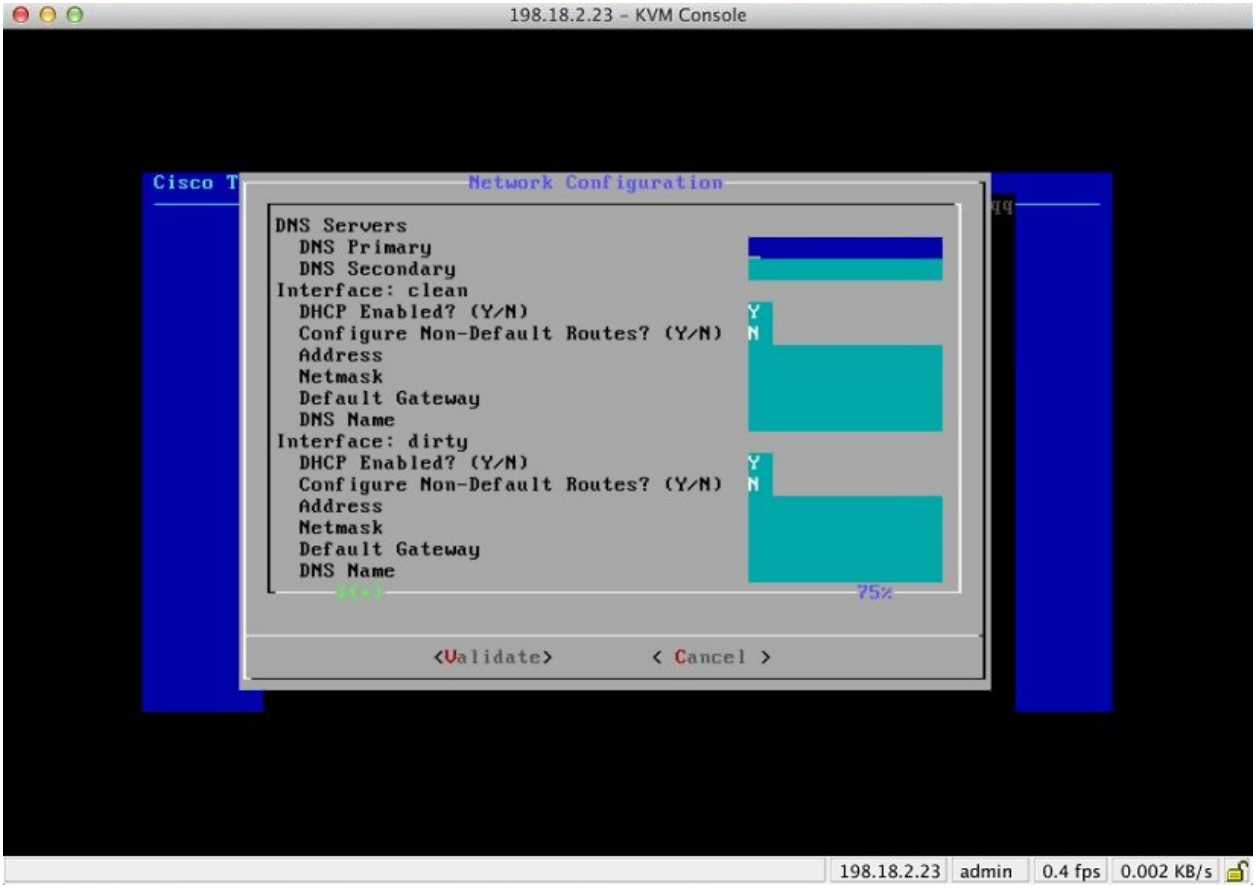
# 초기 네트워크 컨피그레이션 - TGSH 대화 상자

초기 네트워크 컨피그레이션은 TGSH 대화 상자에서 수행됩니다. 이 작업의 목표는 OpAdmin 인터페이스 툴에 대한 액세스를 허용하는 기본 컨피그레이션을 완료하여 라이선스, 이메일 호스트, SSL 인증서 등을 포함하는 나머지 컨피그레이션을 완료하는 것입니다.

**DHCP 사용자:** 다음 단계에서는 고정 IP 주소를 사용한다고 가정합니다. DHCP를 사용하여 IP 얻기에 대한 자세한 내용은 *Threat Grid Appliance 관리자 가이드*를 참조하십시오.

1. TGSH 대화 상자 인터페이스에서 **CONFIG_NETWORK**를 선택합니다. 네트워크 컨피그레이션 콘솔이 열립니다.

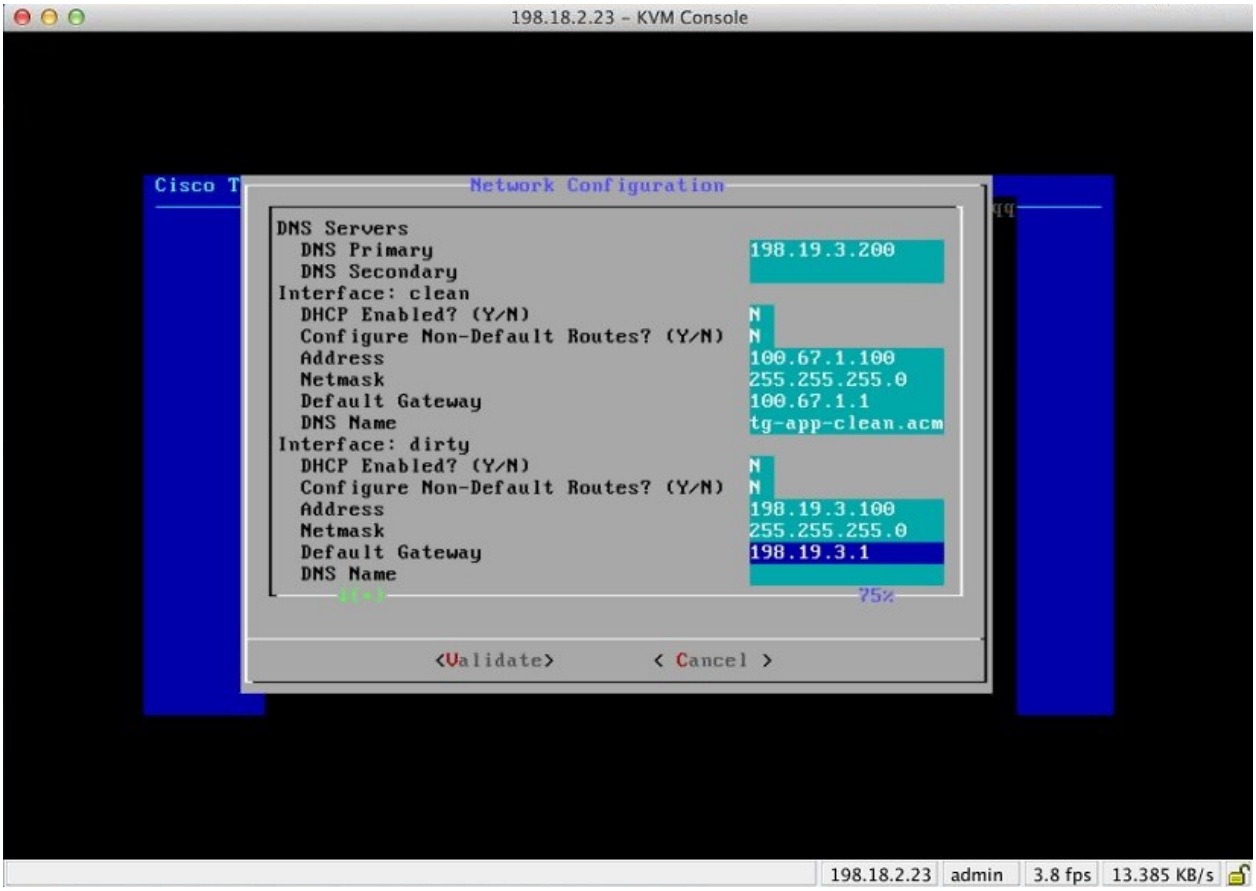
**그림 10 - TGSH 대화 상자 - 네트워크 컨피그레이션 콘솔**




2. 네트워크 관리자가 제공한 설정에 따라 Clean 인터페이스, Dirty 인터페이스, Admin 인터페이스의 빈 필드를 작성합니다.
3. **DHCP Enabled(DHCP 활성화됨)**를 **Y**에서 **N**으로 변경합니다.

   **참고:** 기존 문자에서 **백스페이스** 키를 눌러야 새 문자를 입력할 수 있습니다.
4. **DNS 이름.** 네트워크에서 Clean 네트워크에 DNS 이름을 사용하는 경우 여기에 이름을 입력합니다.
5. **Configure Non-Default Routes?(기본값이 아닌 경로를 구성하시겠습니까?)** 설정을 기본값인 **N**으로 유지합니다(추가 경로가 필요하지 않은 경우).

**그림 11 - 진행 중인 네트워크 컨피그레이션(Clean 및 Dirty)**




6. Dirty 네트워크의 **DNS 이름**을 공백으로 둡니다.

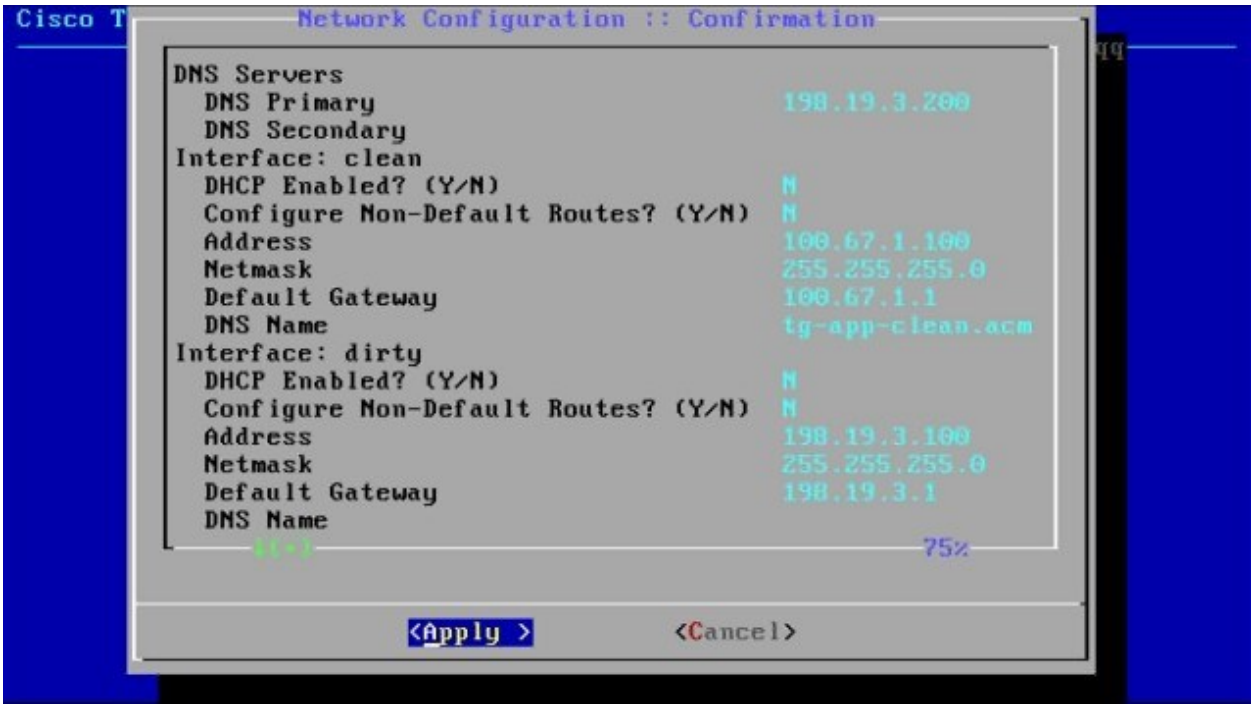
**그림 12 - 진행 중인 네트워크 컨피그레이션(Admin)**


7. 네트워크 설정을 입력한 후 아래쪽 탭에서 **Validate(검증)**를 선택하여 항목을 검증합니다.

   잘못된 값을 입력한 경우 오류가 표시될 수 있습니다. 이 경우 오류를 수정하고 다시 검증합니다.

   검증이 완료되면 Network Configuration Confirmation(네트워크 컨피그레이션 확인)에 입력한 값이 표시됩니다.

**그림 13 - 네트워크 컨피그레이션 확인**

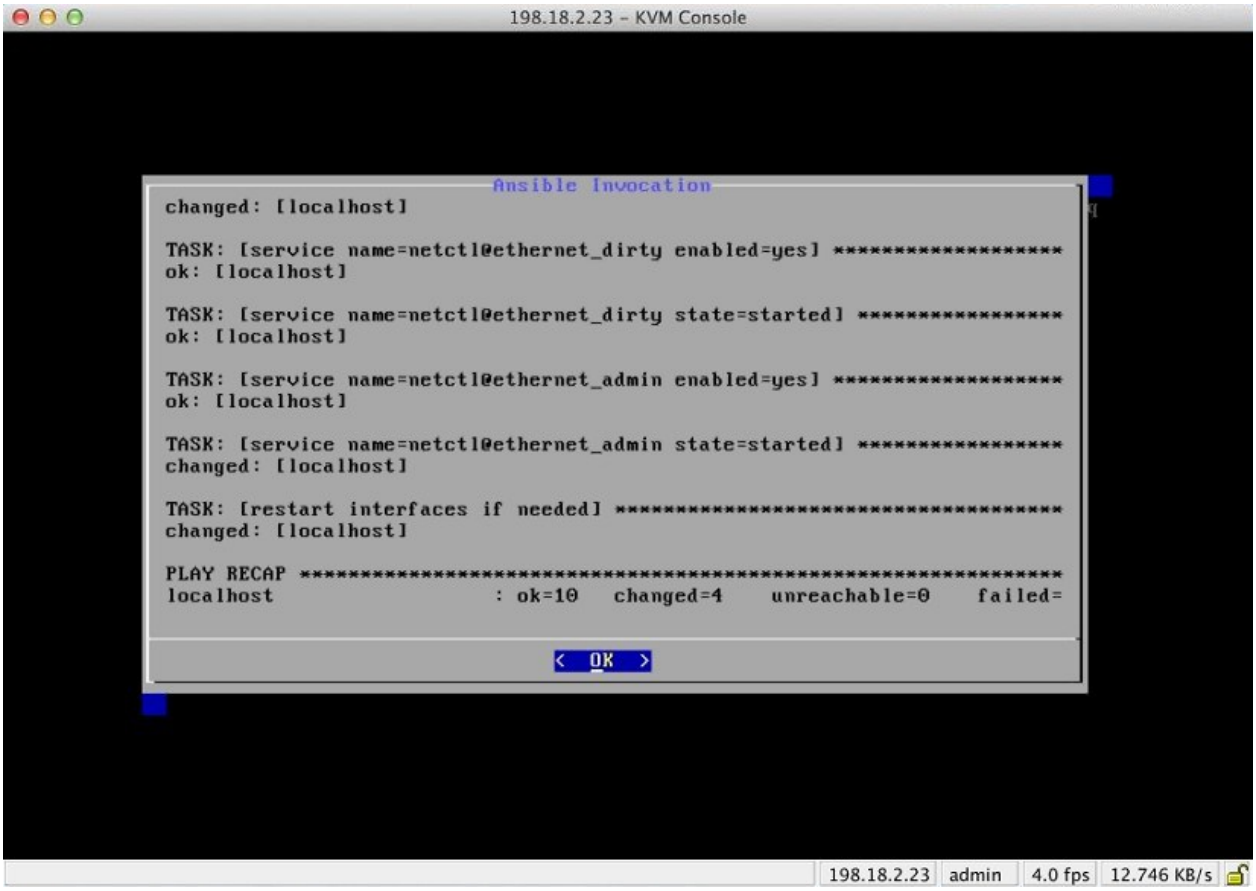



8. **Apply(적용)**를 선택하여 컨피그레이션 설정을 적용합니다.

   잠시 기다립니다. 이 단계를 완료하는 데 10분 이상 소요될 수 있습니다.

   설정이 적용되면 콘솔이 빈 회색 상자로 변하고 화면에 스크롤되는 컨피그레이션 정보가 표시될 수 있습니다. 그런 다음 완료된 컨피그레이션 변경에 대한 세부 정보가 나열됩니다.

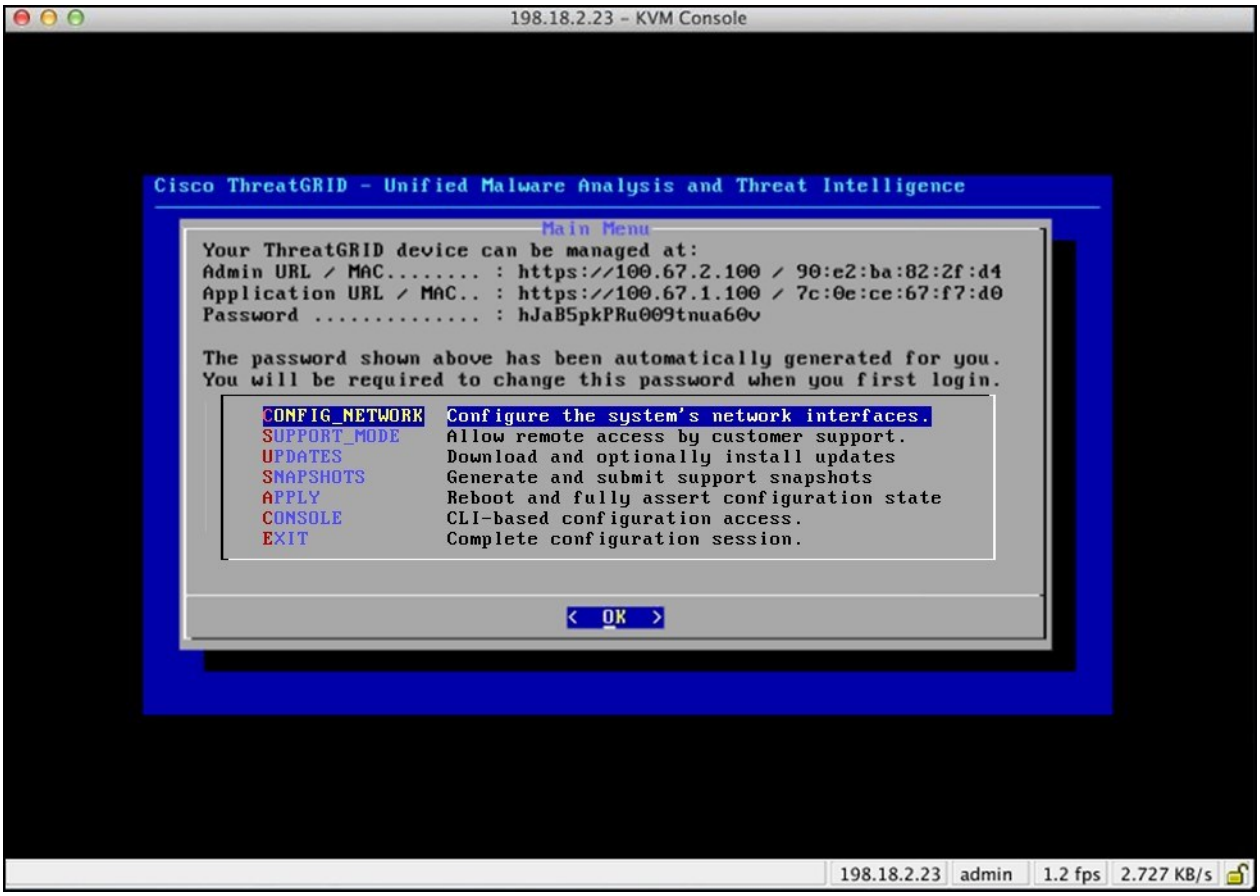
**그림 14 - 네트워크 컨피그레이션 - 변경 사항 목록**




9. **OK(확인)**를 선택합니다.

   다음과 같이 네트워크 컨피그레이션 콘솔을 다시 새로 고치고 입력한 IP 주소를 표시합니다.

**그림 15 - IP 주소**




어플라이언스의 네트워크 컨피그레이션을 완료했습니다.

**참고:** Clean 인터페이스 URL은 OpAdmin 포털 컨피그레이션을 완료해야 작동합니다.

**다음 설정 단계:**

어플라이언스 설정의 다음 단계는 다음 섹션 OpAdmin 포털 컨피그레이션 마법사에 설명된 대로 OpAdmin 포털의 워크플로를 사용하여 나머지 컨피그레이션 작업을 완료하는 것입니다.

# 컨피그레이션 마법사 - OpAdmin 포털

OpAdmin 포털은 어플라이언스의 Threat Grid 관리자 포털에 해당합니다. Admin 인터페이스에 IP 주소를 구성하면 사용할 수 있는 웹 사용자 인터페이스입니다.

OpAdmin 포털은 어플라이언스 구성에 권장되는 툴이며, 실제로 다음을 포함한 대부분의 어플라이언스 컨피그레이션은 OpAdmin 포털 인터페이스를 통해서만 수행할 수 있습니다.

- OpAdmin 포털 관리자의 비밀번호
- 이메일 서버
- DNS 서버
- NTP 서버
- SSL 인증서
- 기타 서버 설정
- https://<adminIP>/ 또는 https://<adminHostname>/

**참고:** 이러한 설정 중 일부는 초기 OpAdmin 포털 컨피그레이션 마법사 워크플로에서 완료되지 않습니다. 일부(예: SSL 인증서)는 *Threat Grid Appliance 관리자 가이드*에 설명된 대로 여러 단계에서 구성됩니다.

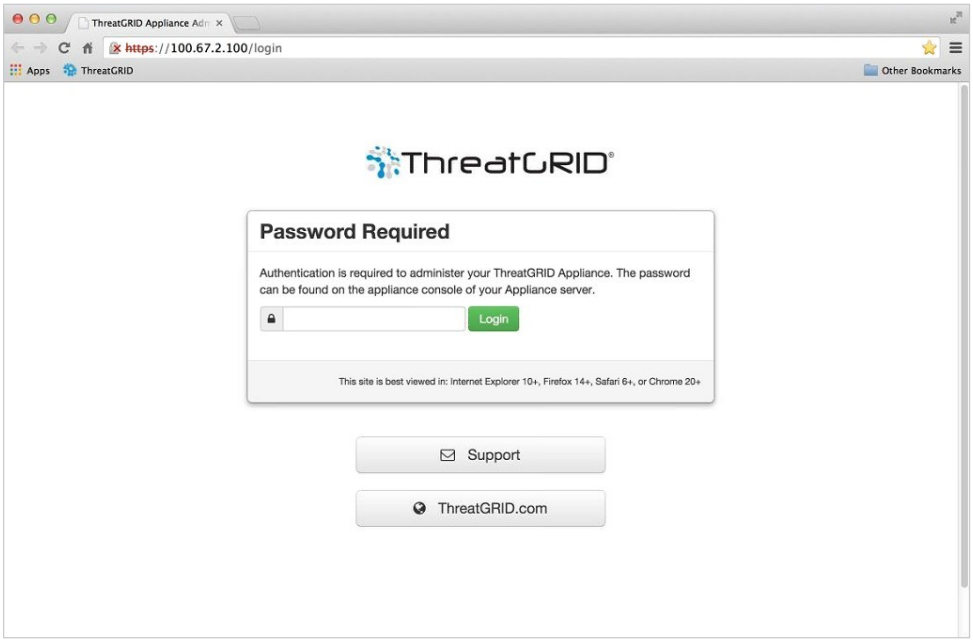
# 컨피그레이션 워크플로

다음 섹션에 있는 단계는 컨피그레이션 중 IP 주소에 장애가 발생할 가능성을 줄이기 위해 하나의 세션에서 완료해야 합니다.

# OpAdmin 포털에 로그인

1. OpAdmin 포털 인터페이스("Https"를 사용하는 관리 URL)에서 사용자의 브라우저를 가리킵니다. 다음과 같이 Threat Grid OpAdmin 로그인 화면이 열립니다.

**그림 16 - OpAdmin 로그인**



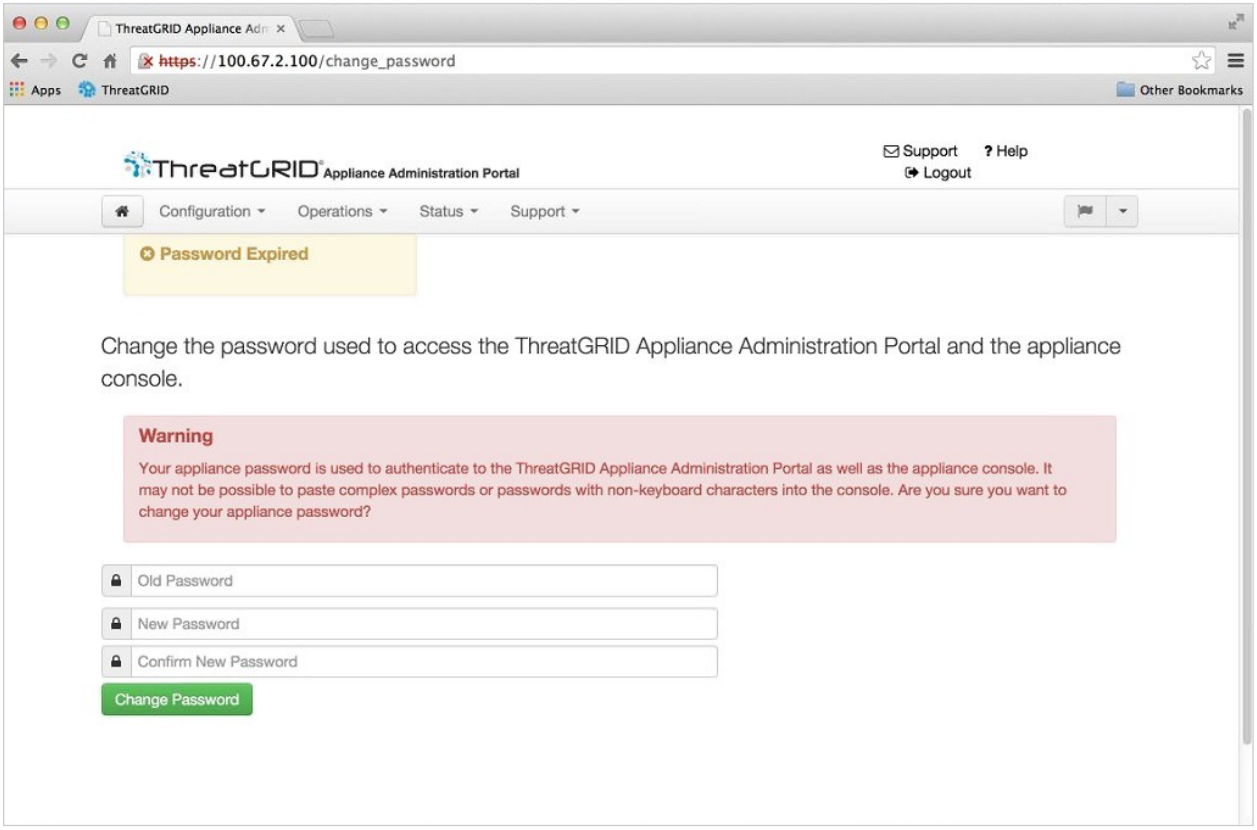

2. TGSH 대화 상자에서 복사한 기본 관리자 비밀번호를 입력하고 **Login(로그인)**을 클릭합니다. *Change Password(비밀번호 변경)* 페이지가 열립니다.

다음 섹션을 계속 진행합니다.

# 관리자 비밀번호 변경

초기 관리자 비밀번호는 배송 전 Threat Grid 설치 과정에서 임의로 생성되어 TGSH 대화 상자에 일반 텍스트로 표시됩니다. 초기 관리자 비밀번호를 변경해야 컨피그레이션 워크플로를 계속 진행할 수 있습니다.

**그림 17 - OpAdmin 비밀번호 변경**




1. TGSH 대화 상자의 비밀번호를 **Old Password(이전 비밀번호)** 필드에 입력합니다. 이때 사용할 수 있도록 비밀번호를 텍스트 파일로 가지고 있어야 합니다.
2. 새 비밀번호를 입력하고 확인합니다.
3. **Change Password(비밀번호 변경)**를 클릭합니다.

   비밀번호가 업데이트됩니다. *End User License Agreement(최종 사용자 라이선스 계약)* 페이지가 열립니다.

   **참고:** 새 비밀번호는 TGSH 대화 상자에서 눈에 보이는 텍스트로 표시되지 않으므로 따로 기록해 두어야 합니다.

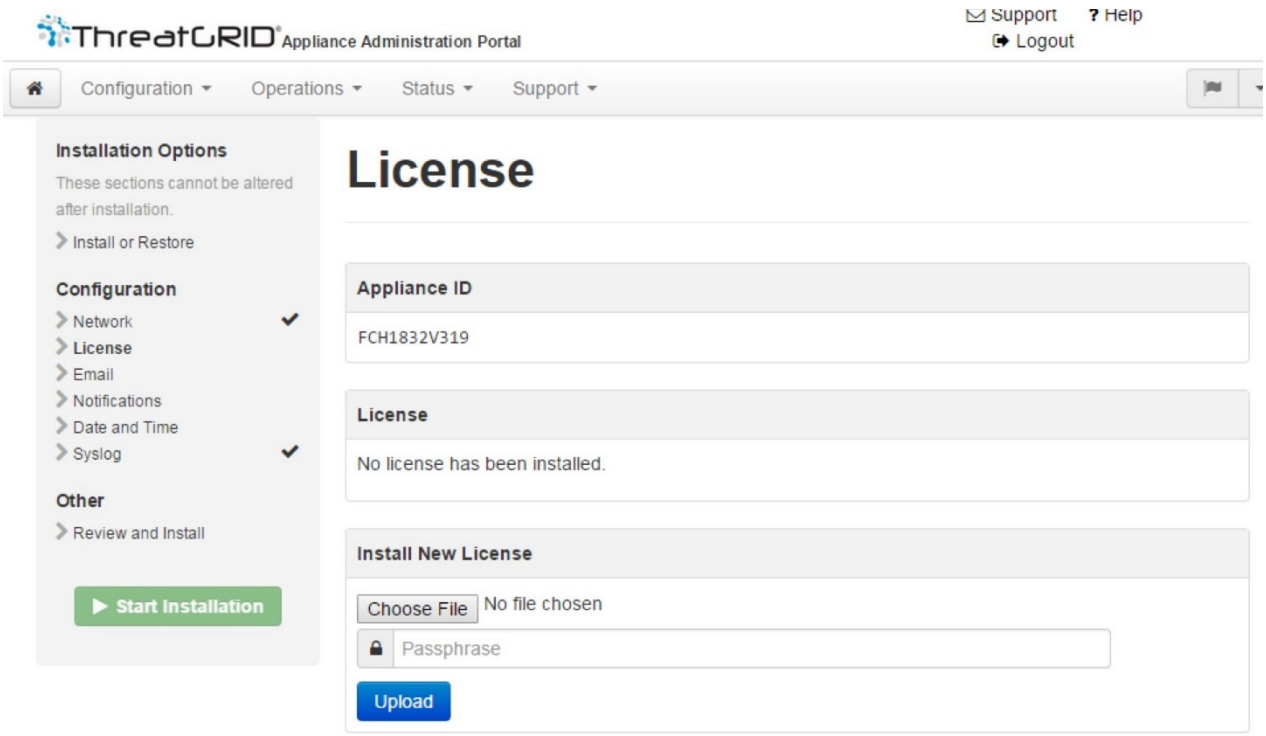
   비밀번호를 분실한 경우 **분실한 비밀번호** 지침(*지원* 섹션, *Threat Grid Appliance 관리자 가이드* 참조)을 따르십시오.

다음 섹션을 계속 진행합니다.

# 최종 사용자 라이선스 계약

1. 최종 사용자 라이선스 계약을 검토합니다.
2. 아래로 끝까지 스크롤한 후 **I HAVE READ AND AGREE(계약을 읽었으며 동의함)**를 클릭합니다. 다음과 같이 *License(라이선스)* 페이지가 열립니다.

**그림 18 - 라이선스 페이지**




다음 섹션인 네트워크 컨피그레이션 설정에 설명된 대로 컨피그레이션 워크플로를 따라 *라이선스를 설치하기 전에 네트워크를 구성*하는 것이 좋습니다.

# 네트워크 컨피그레이션 설정

TGSH 대화 상자에서 정적 네트워크 설정을 구성한 경우, 어플라이언스 네트워크 컨피그레이션 중 TGSH 대화 상자에 입력한 값이 네트워크 컨피그레이션 페이지에 표시되는 IP 주소에 반영됩니다.

## 네트워크 컨피그레이션 및 DHCP

초기 연결에 DHCP를 사용하여 Clean 및 Dirty IP 네트워크를 고정 IP 주소로 변경해야 하는 경우 *Threat Grid Appliance 관리자 가이드*의 ***Networking(네트워킹) > Using DHCP(DHCP 사용)*** 섹션에 있는 단계를 수행합니다.

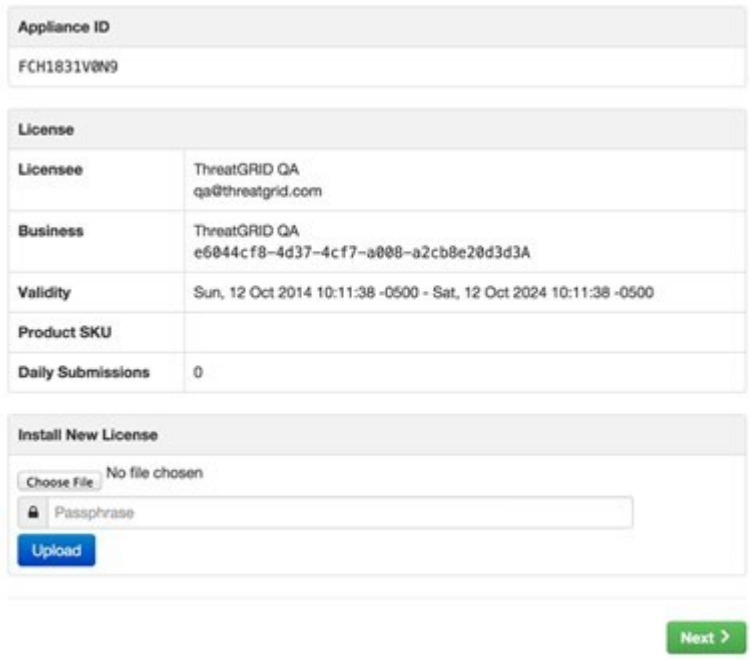
다음 섹션을 계속 진행합니다.

# 라이선스 설치

네트워크를 구성한 후에 Threat Grid 라이선스를 설치할 수 있습니다. v1.4.4 이전 버전에서 사용자의 라이선스를 수락하려면 지원 모드를 시작해야 합니다. 자세한 내용은 지원 모드 시작 - 버전 1.4.4 이전의 라이선스 해결 방법을 참조하십시오.

1. 왼쪽 열에서 **License(라이선스)**를 클릭합니다. *License(라이선스)* 페이지가 열립니다. 라이선스가 설치되지 않았습니다.
2. **Install New License(새 라이선스 설치)**에서 **Browse(찾아보기)**를 클릭하고 파일 관리자에서 라이선스 파일을 선택합니다.
3. Passphrase(패스프레이즈) 필드에 입력한 라이선스 비밀번호를 입력합니다.
4. **Upload(업로드)**를 클릭하여 설치합니다. 페이지가 새로 고쳐지고 라이선스 정보가 표시됩니다.

**그림 19 - 설치 후 라이선스 정보**




5. **Next(다음)**를 클릭하여 계속합니다. ***Email(이메일)*** 페이지가 열립니다.

다음 섹션을 계속 진행합니다.

# 이메일 호스트 컨피그레이션

워크플로의 다음 단계는 이메일 호스트를 구성하는 것입니다.

1. 왼쪽 열에서 **Email(이메일)**을 클릭합니다. *Email(이메일)* 페이지가 열립니다.
2. **업스트림 호스트**(이메일 호스트) 이름을 입력합니다.
3. 포트를 587에서 **25**로 변경합니다.

4. 기타 설정을 기본값으로 둡니다.
5. **Next(다음)**를 클릭합니다. *Notifications(알림)* 페이지가 열립니다.

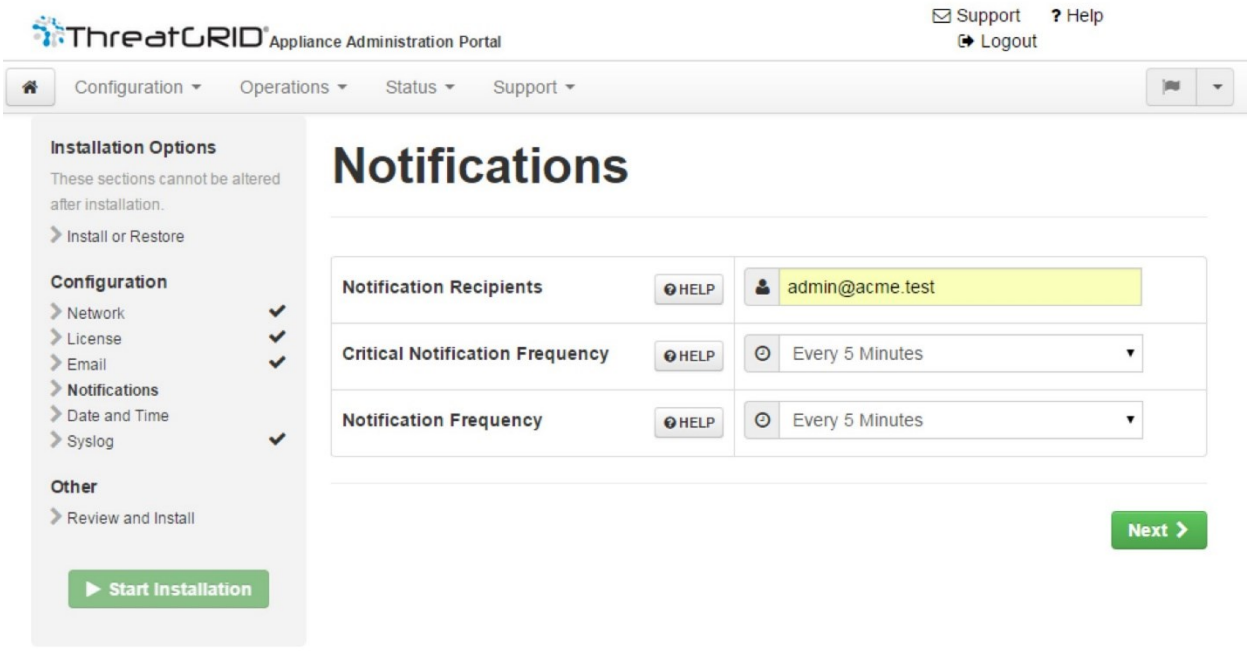
다음 섹션을 계속 진행합니다.

# 서버 알림 컨피그레이션

워크플로의 다음 단계는 하나 이상의 이메일 주소에 주기적으로 전달할 수 있는 알림을 구성하는 것입니다. 시스템 알림은 Threat Grid 포털 인터페이스에 표시되지만 이 페이지에서도 이메일을 통해 보낼 수 있는 알림을 설정할 수 있습니다.

**참고:** 업데이트 v1.3에는 시스템 로그 메시지 및 Thread Grid 알림을 수신할 수 있는 시스템 로그 서버를 구성하는 페이지가 포함되어 있습니다. 자세한 내용은 *Threat Grid Appliance 관리 가이드*를 참조하십시오.

**그림20 - 알림 컨피그레이션**




1. 먼저 드롭다운 목록에서 **Critical Notification Frequency(중요 알림 빈도)** 및 **Notification Frequency(알림 빈도)**를 선택하여 설정합니다.
2. 그런 다음 **Notification Recipients(알림 받는 사람)**에 하나 이상의 이메일 주소를 쉼표로 구분하여 입력합니다.
3. **Next(다음)**를 클릭합니다. *Date and Time(날짜 및 시간)* 페이지가 열립니다.

다음 섹션을 계속 진행합니다.

# NTP 서버 컨피그레이션

NTP("Network Time Protocol") 서버를 식별하는 단계입니다.

1. **NTP 서버** IP 또는 NTP 이름을 입력합니다.

   NTP 서버가 여러 개인 경우 공백 또는 쉼표를 사용하여 구분합니다.

2. 현재 시스템 시간을 무시하고 브라우저와 동기화합니다.

3. **Next(다음)**를 클릭합니다.

   모든 컨피그레이션 단계 옆에 체크 박스가 있는 *Review and Install(검토 및 설치)* 페이지가 열립니다.

다음 섹션을 계속 진행합니다.

# 컨피그레이션 설정 검토 및 설치

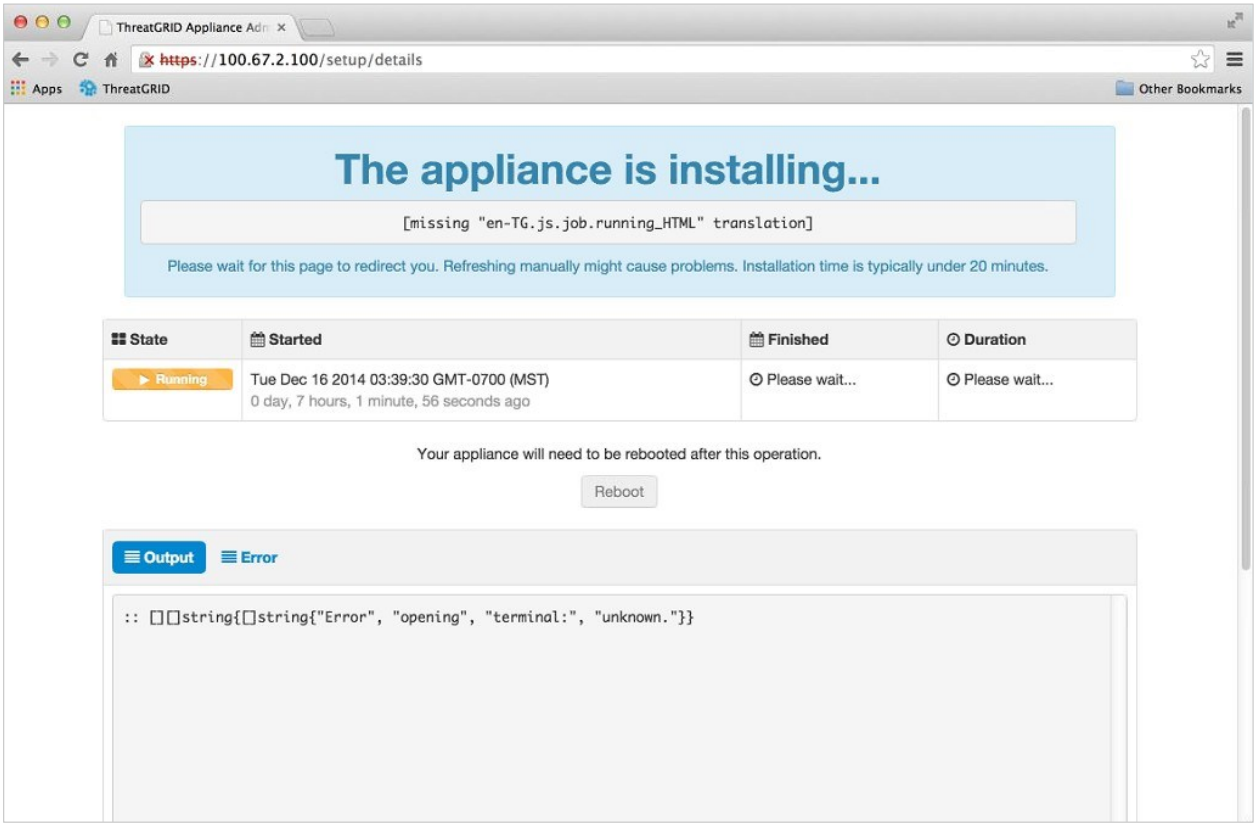
네트워크 컨피그레이션 설정을 입력했으므로 아래 설명된 대로 해당 설정을 설치해야 합니다.

1. *Review and Install(검토 및 설치)* 페이지에서 **Start Installation(설치 시작)**을 클릭합니다.

   컨피그레이션 스크립트를 설치하면 "*The appliance is installing...*(어플라이언스를 설치하고 있습니다...)"과 같은 메시지가 표시됩니다.

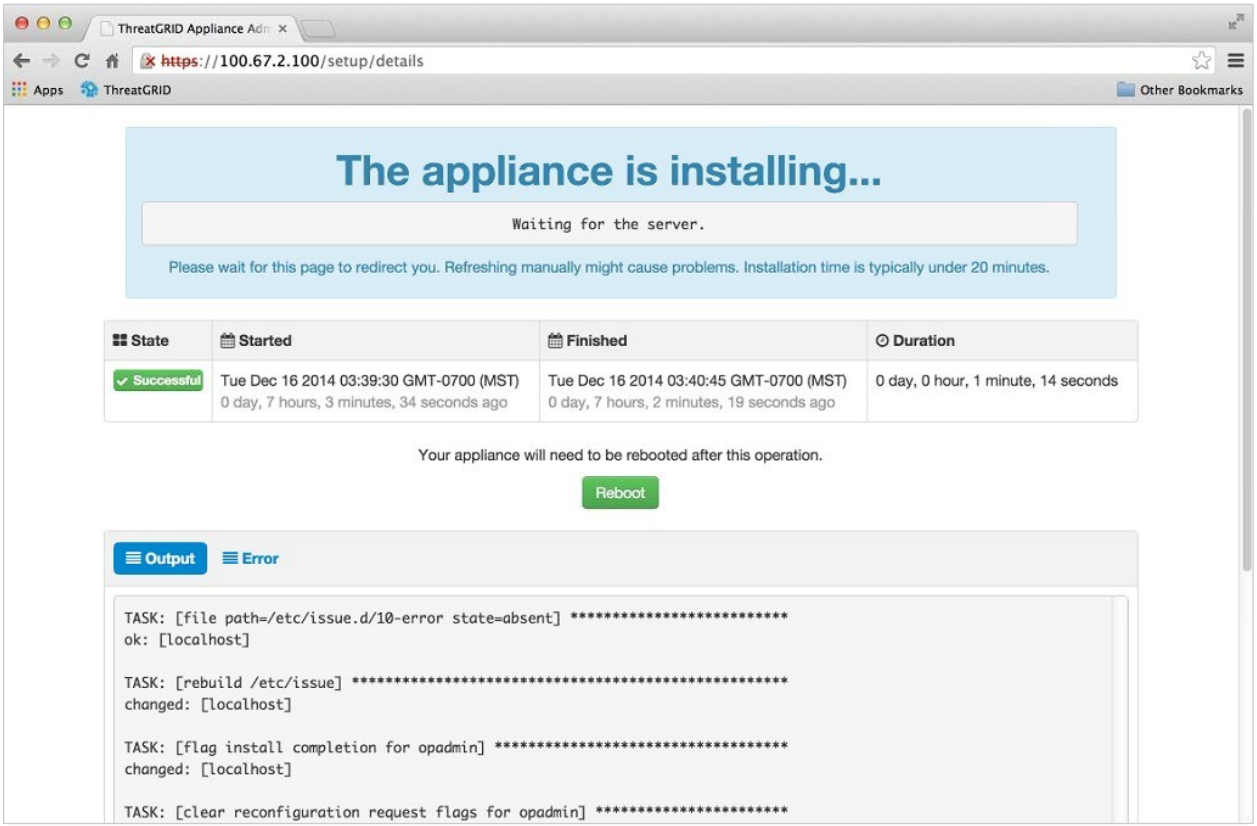
**참고:** 대기합니다. 이 단계를 완료하는 데 10분 이상 걸릴 수 있습니다. 화면에 컨피그레이션이 적용되면서 해당 정보가 표시됩니다.

**그림 21 - 어플라이언스 설치 중**



2. 설치가 완료되면 상태가 주황색의 **Running(실행 중)**에서 성공을 나타내는 녹색의 **Successful(완료)** 메시지로 변경됩니다. **Reboot(재부팅)** 단추가 녹색으로 변경되고 컨피그레이션 출력이 표시됩니다.

**그림 22 - 어플라이언스 설치 완료**

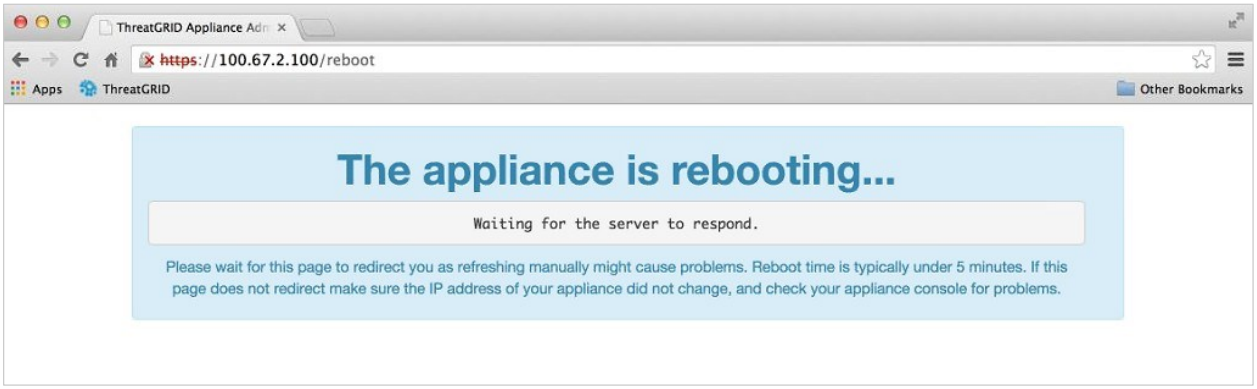



3. 설치가 완료되면 **Reboot(재부팅)**를 클릭합니다. "*The appliance is rebooting.*(어플라이언스를 재부팅하고 있습니다.)"이라는 메시지가 표시됩니다.

   재부팅하는 데 최대 5분이 걸릴 수 있습니다.

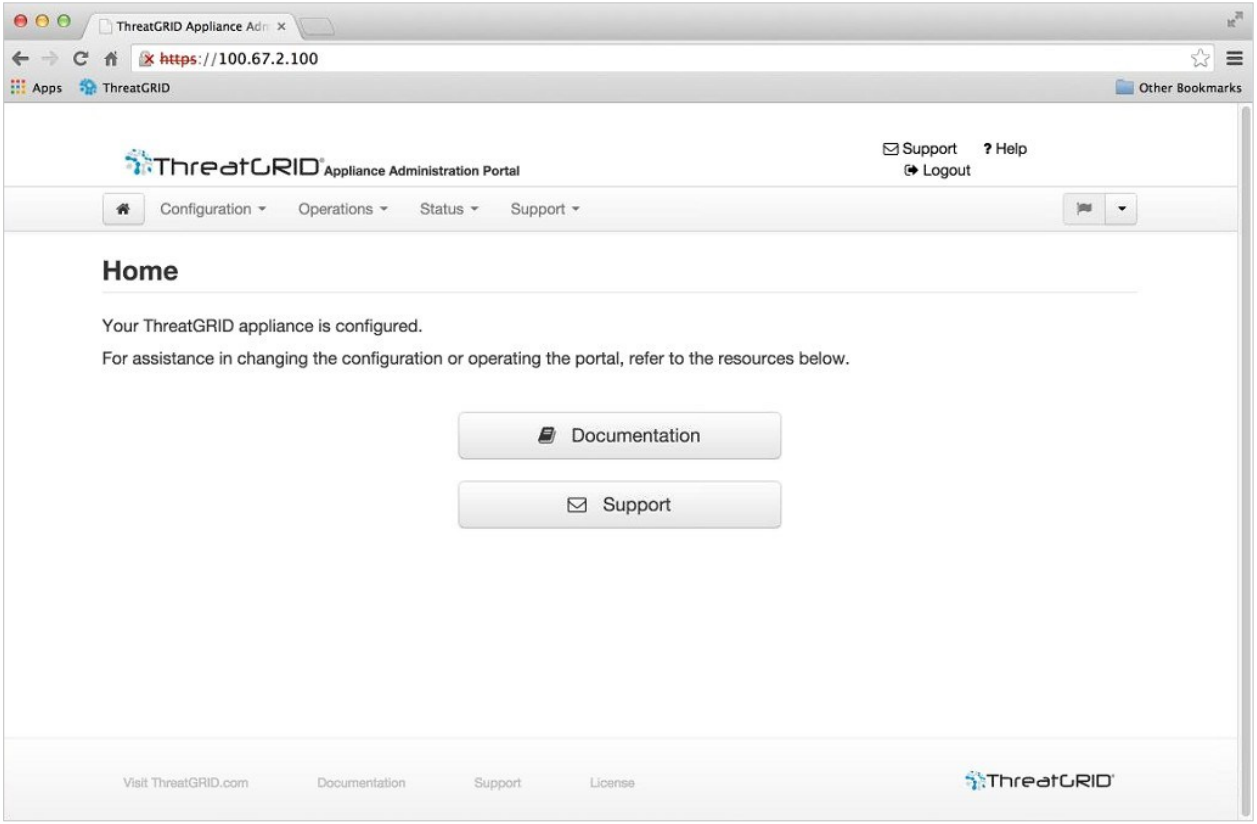
어플라이언스를 재부팅하는 동안에는 아무것도 변경하지 마십시오.

**그림 23 - 어플라이언스 재부팅 중**




어플라이언스를 재부팅하면 다음과 같이 어플라이언스가 구성되었다는 확인 메시지가 표시됩니다.

**그림 24 - 어플라이언스가 구성됨**




어플라이언스가 설정되고 초기 컨피그레이션이 완료됩니다.

# Threat Grid Appliance 업데이트 설치

초기 Threat Grid Appliance 설정을 완료한 후 사용 가능한 업데이트를 설치하고 계속하는 것이 좋습니다.

Threat Grid Appliance 업데이트는 **OpAdmin** 포털을 통해 적용됩니다.

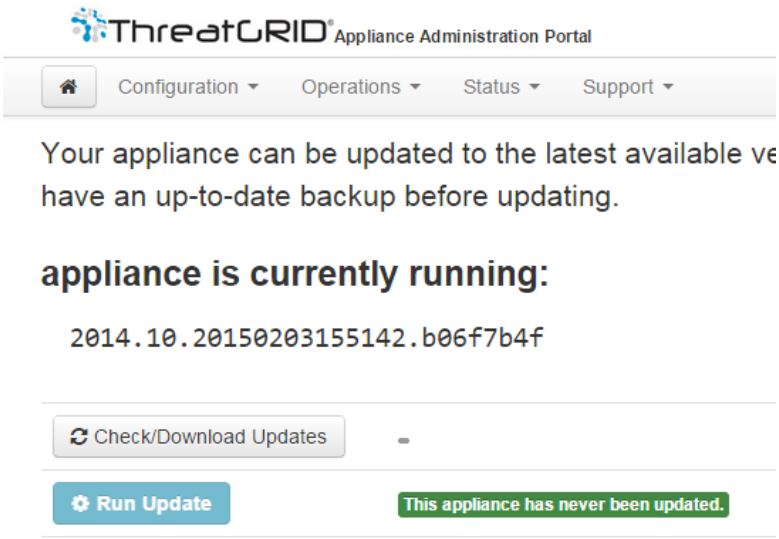
1. **Operations(운영)** 메뉴에서 **Update Appliance(어플라이언스 업데이트)**를 선택합니다. 업데이트 페이지가 열리고 어플라이언스의 현재 빌드가 표시됩니다.
2. **Check/Download Updates(업데이트 확인/다운로드)**를 클릭합니다. 소프트웨어에서 Threat Grid Appliance 소프트웨어의 최신 업데이트/버전이 있는지 확인하고, 있을 경우 다운로드합니다. 시간이 걸릴 수 있습니다.
3. 업데이트가 다운로드되면 **Run Update(업데이트 실행)**를 클릭하여 설치합니다.

업데이트 설치에 대한 자세한 내용은 *Threat Grid Appliance 관리자 가이드*를 참조하십시오.

# 어플라이언스 빌드 번호

어플라이언스의 빌드 번호는 업데이트 페이지인 OpAdmin **Operations(운영)** > **Update Appliance(어플라이언스 업데이트)**에서 확인할 수 있습니다.

**그림 25 - 어플라이언스 빌드 번호**



## 어플라이언스 빌드 번호/버전 조회표

어플라이언스의 빌드 번호는 위에서 설명한 대로 업데이트 페이지인 OpAdmin **Operations(운영)** > **Update Appliance(어플라이언스 업데이트)**에서 확인할 수 있습니다. 어플라이언스 빌드 번호는 다음 버전 번호에 해당합니다.

| 빌드 번호 | 릴리스 버전 | 릴리스 날짜 | 참고 |
|---|---|---|---|
| 2016.05.20170105200233.32f70432.rel | 2.1.6 | 2017-01-07 | OpAdmin/tgsh-dialog를 위한 LDAP 인증 지원 |
| 2016.05.20161121134140.489f130d.rel | 2.1.5 | 2016-11-21 | ElasticSearch5, CSA 성능 수정 |
| 2016.05.20160905202824.f7792890.rel | 2.1.4 | 2016-09-05 | 제조업 관련 주요 사항 |
| 2016.05.20160811044721.6af0fa61.rel | 2.1.3 | 2016-08-11 | 오프라인 업데이트 지원 키, M4 초기화 지원 |
| 2016.05.20160715165510.baed88a3.rel | 2.1.2 | 2016-07-15 | |
| 2016.05.20160706015125.b1fc50e5.rel-1 | 2.1.1 | 2016-07-06 | |
| 2016.05.20160621044600.092b23fc | 2.1 | 2016-06-21 | |
| 2015.08.20160501161850.56631ccd | 2.0.4 | 2016-05-01 | 2.1 업데이트를 위한 시작점. 2.1로 업데이트하기 전에 2.0.4가 있어야 합니다. |
| 2015.08.20160315165529.599f2056 | 2.0.3 | 2016-03-15 | AMP 통합, CA mgmt. 및 스플릿 DNS 도입 |
| 2015.08.20160217173404.ec264f73 | 2.0.2 | 2016-02-18 | |
| 2015.08.20160211192648.7e3d2e3a | 2.0.1 | 2016-02-12 | |
| 2015.08.20160131061029.8b6bc1d6 | 2.0 | 2016-02-11 | 이 버전에서 2.0.1로 강제 업데이트 |
| 2014.10.20160115122111.1f09cb5f | 1.4.6 | 2016-01-27 | 2.0.4 업데이트를 위한 시작점 |
| 2014.10.20151123133427.898f70c2 | v1.4.5 | 2015-11-25 | |
| 2014.10.20151116154826.9af96403 | v1.4.4 | | |
| 2014.10.20151020111307.3f124cd2 | v1.4.3 | | |

| 빌드 번호 | 릴리스 버전 | 릴리스 날짜 | 참고 |
|---|---|---|---|
| 2014.10.20150904134201.ef4843e7 | v1.4.2 | | |
| 2014.10.20150824161909.4ba773cb | v1.4.1 | | |
| 2014.10.20150822201138.8934fa1d | v1.4 | | |
| 2014.10.20150805134744.4ce05d84 | v1.3 | | |
| 2014.10.20150709144003.b4d4171c | v1.2.1 | | |
| 2014.10.20150326161410.44cd33f3 | v1.2 | | |
| 2014.10.20150203155143+hotfix1.b06f7b4f | v1.1+hotfix1 | | |
| 2014.10.20150203155142.b06f7b4f | v1.1 | | |
| 2014.10.20141125162160+hotfix2.8afc5e2f | v1.0+hotfix2<br>**참고:**<br>1.0+hotfix2는 대용량 파일을 중단 없이 처리할 수 있도록 업데이트 시스템 자체를 수정하는 필수 업데이트입니다. | | |
| 2014.10.20141125162158.8afc5e2f | v1.0 | | |

**참고:** 릴리스 버전 1.0-1.2 a에서는 부팅 시 인터페이스가 연결되지 않은 경우 재부팅해야 할 수 있습니다. 이러한 문제는 v1.3 이전에서 나타나는 것으로, v1.3 이후에서는 부팅 시점에 SFP가 계속 연결되어 있어야 하는 인터페이스에서만 발생합니다. SFP에 연결된 네트워크 케이블은 안전하게 핫 플러그 연결할 수 있습니다.

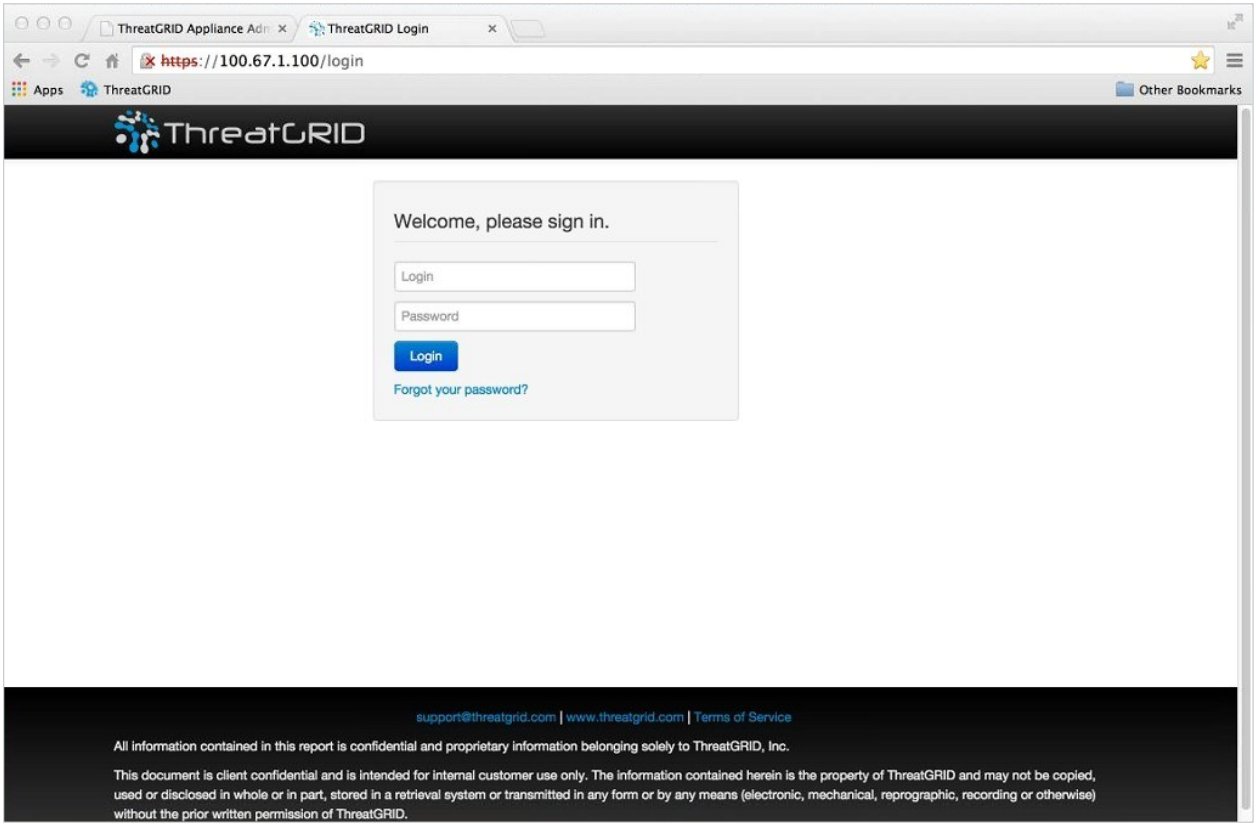
**참고:** 1.0에서 1.0+hotfix2로 업데이트하는 데는 약 15분이 걸립니다. 1.0에서 1.3으로 전체 업데이트를 적용하는 데는 데이터 마이그레이션을 제외하고 약 30분이 걸립니다.

# 어플라이언스 설정 테스트 - 샘플 제출

Threat Grid Appliance를 최신 버전으로 업데이트한 후에는 Threat Grid 소프트웨어를 사용하여 악성코드 샘플을 제출함으로써 어플라이언스를 올바르게 구성했는지 최종적으로 테스트합니다.

1. Clean 인터페이스로 구성한 주소를 방문하여 AMP Threat Grid Portal에 로그인합니다. Threat Grid 로그인 페이지가 열립니다.

**그림 26 - Threat Grid Portal 로그인 페이지**




2. 기본 로그인 및 비밀번호인 **admin/changeme**를 입력합니다.
3. **Login(로그인)**을 클릭합니다. 기본 Threat Grid *Sample Analysis*(샘플 분석) 페이지가 열립니다.
4. 오른쪽 상단 모서리에 있는 **Submit a Sample(샘플 제출)** 상자에서 샘플 파일을 선택하거나 *URL*을 입력하여 악성코드 분석을 제출합니다.
5. **Upload Sample(샘플 업로드)**을 클릭합니다. Threat Grid 샘플 분석 프로세스가 시작됩니다.

   샘플이 여러 분석 단계를 거치는 것을 볼 수 있습니다. 분석하는 동안 샘플이 *Submissions*(제출) 섹션에 나열됩니다. 분석이 완료되면 *Samples*(샘플) 섹션에서 결과를 확인할 수 있으며 분석 보고서에 세부 사항이 표시됩니다.

# 어플라이언스 관리

Threat Grid Appliance를 설정하고 초기 컨피그레이션을 완료하면 어플라이언스 관리자가 사용할 수 있습니다.

릴리스 노트, 업데이트, SSL 인증서, 사용자 추가, 기타 관리자 작업 및 항목은 *Threat Grid Appliance 관리자 가이드*에 설명되어 있습니다.

# 부록 A – CIMC 컨피그레이션(권장)

서버가 부팅될 때 표시되는 첫 번째 창은 Cisco 창으로, 여기에서 "CIMC"(Cisco Integrated Management Controller) 컨피그레이션 유틸리티를 시작할 수 있습니다. CIMC 인터페이스를 원격 서버 관리에 사용할 수 있습니다.

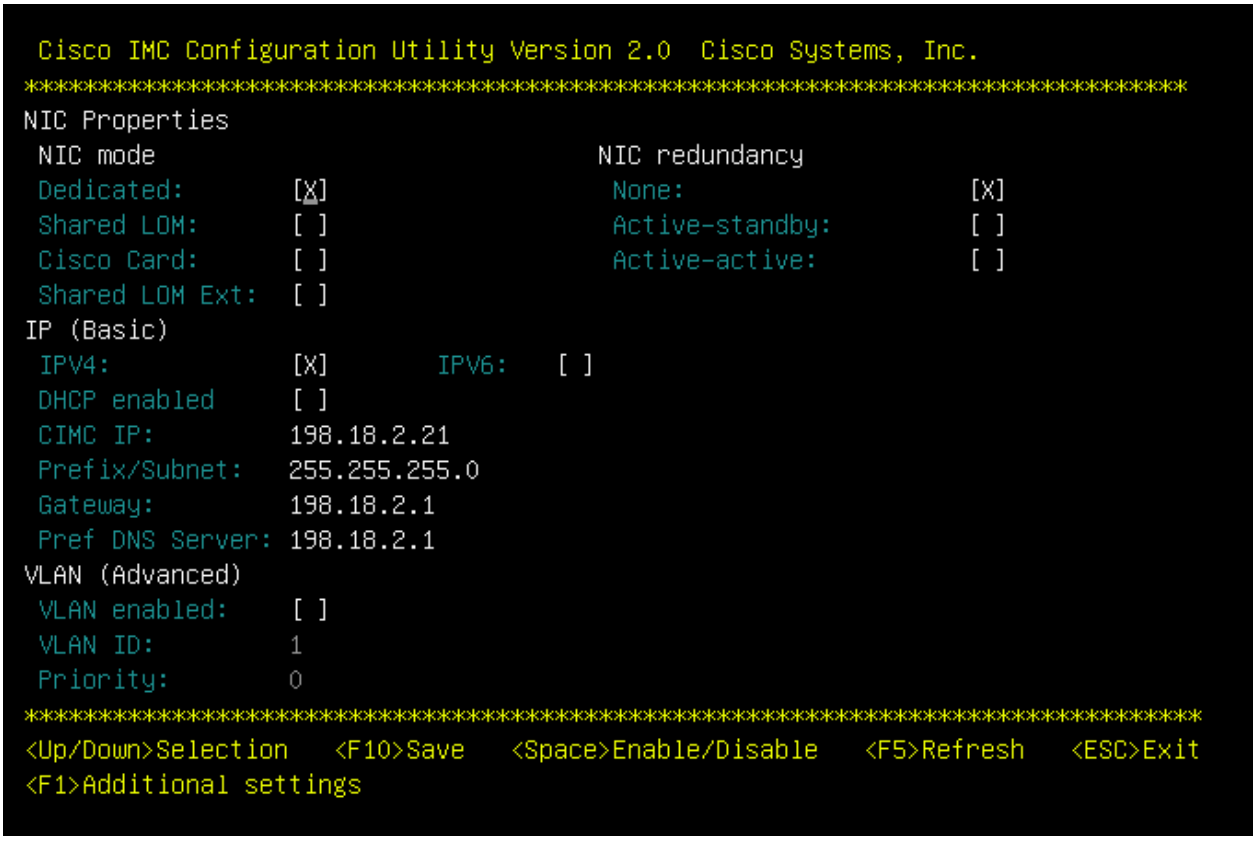
어플라이언스에 직접 연결된 모니터 및 키보드가 있어야 합니다.

1. 서버 전원을 켭니다. 다음과 같은 Cisco 화면이 열립니다.

**그림 27 - Cisco 화면 – F8 키로 컨피그레이션 유틸리티 시작**

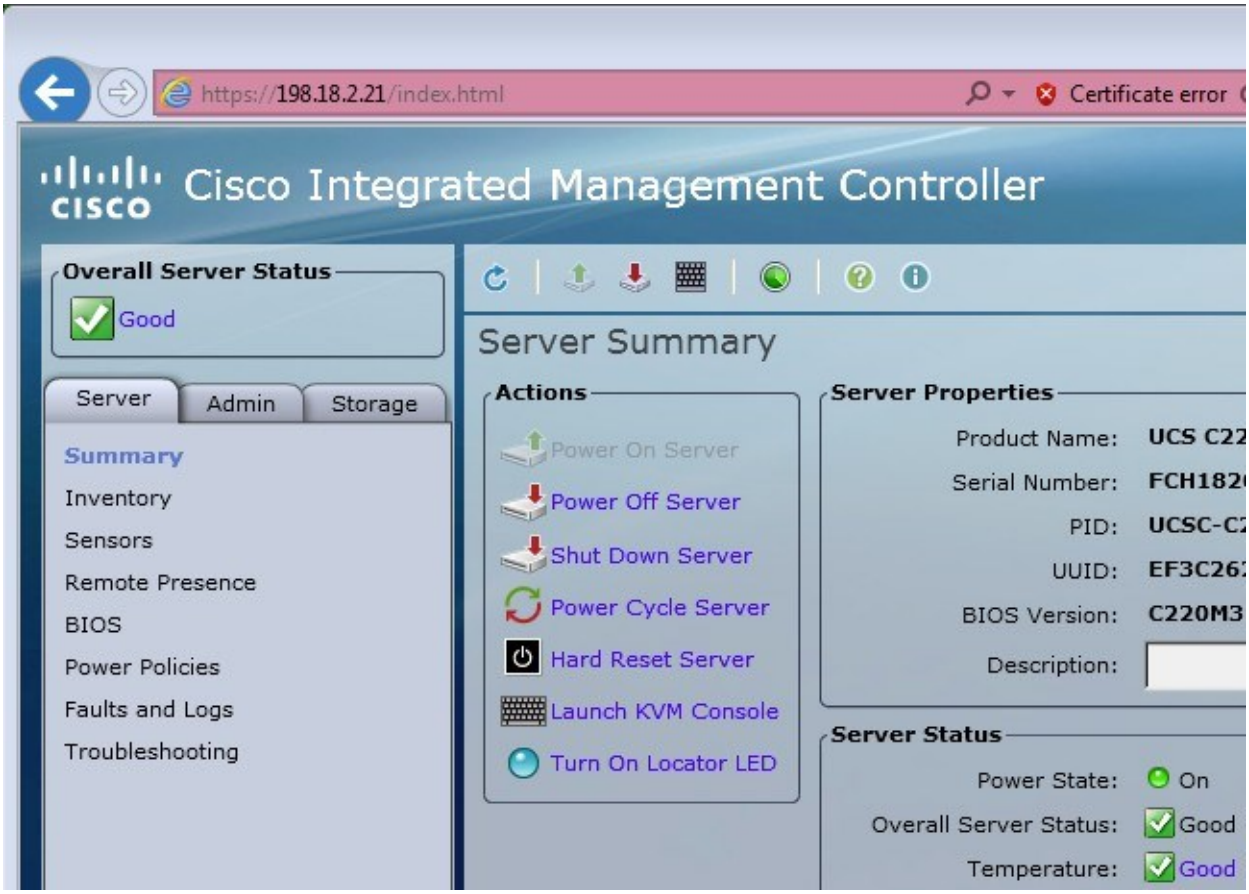

2. 메모리 검사가 완료되면 **F8** 키를 눌러 다음과 같이 CIMC 컨피그레이션 유틸리티를 시작합니다.

그림 28 - CIMC 컨피그레이션 유틸리티




3. CIMC 컨피그레이션 유틸리티에서 원격 서버 관리에 사용할 IP 주소를 설정합니다.
4. 작업 완료 시 Save(저장)한 다음 Exit(종료)합니다.
   이제 웹 브라우저에서 https:// *<CIMC-IP address>*/를 사용하여 서버를 원격으로 관리할 수 있습니다.
5. 초기 사용자 이름은 "**admin**", 비밀번호는 "**password**"입니다.

그림 29 - CIMC(Cisco Integrated Management Controller) 인터페이스




이제 CIMC 인터페이스를 사용하여 서버 상태를 확인하거나 KVM을 열어 나머지 설정 단계를 원격으로 완료할 수 있습니다.