Cisco AMP Threat Grid Appliance 관리자 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

서론

Cisco AMP TGA(Threat Grid Appliance)는 단일 Cisco UCS 서버에 설치된 완벽한 AMP Threat Grid 악성코드 분석 플랫폼을 제공합니다(UCS C220-M3 또는 UCS C220 M4). Threat Grid Appliance는 상세한 위협 분석 및 콘텐츠를 바탕으로 지능형 악성코드 분석을 수행하기 위해 안전하고 보안 수준이 높은 온프레미스 환경을 제공합니다.

은행, 보험사, 의료 서비스 등과 같이 민감한 데이터를 처리하는 많은 조직에서는 악성코드 아티팩트와 같은 특정 유형의 파일을 금지하는 다양한 규정 준수 규칙, 정책 제한 및 가이드라인에 따라 악성코드를 네트워크 외부로 전송하여 분석을 수행해야 합니다. 이러한 조직들은 Threat Grid Appliance를 온프레미스로 유지 보수함으로써 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

이 문서는 TGA 관리자 가이드입니다. 이 가이드는 새로운 Threat Grid Appliance를 시작하는 방법과 최적의 악성코드 분석을 위해 어플라이언스를 관리하는 방법을 설명합니다. 또한 Threat Grid Appliance를 기타 Cisco 제품 및 서비스(ESA 및 WSA 어플라이언스 및 FireAMP Private Cloud 디바이스 등)에 통합하는 관리자를 위한 정보를 제공합니다.

Threat Grid Appliance 설정 및 컨피그레이션에 대한 자세한 내용은 *Threat Grid Appliance 설정 및 컨피그레이션 가이드*(Threat Grid Appliance 제품 설명서 페이지에서 확인 가능)를 참조하십시오.

시작하기

Cisco AMP Threat Grid Appliance는 샘플을 분석하는 데 필요한 모든 구성 요소와 함께 배송하기 전에 설치된 Linux 서버입니다. 새 어플라이언스를 수령한 후 먼저 온프레미스 네트워크 환경에 맞게 설정 및 구성해야 합니다.

서버가 실행되면 Threat Grid Appliance 관리자는 조직 및 사용자의 Threat Grid 악성코드 분석 뿐만 아니라 어플라이언스 업데이트 및 백업을 관리하고 다른 서버 관리 작업을 담당합니다.

업데이트

Cisco는 사용하기 전에 모든 최신 기능 및 보안 업데이트가 설치되었는지 확인하기 위해 어플라이언스를 업데이트할 것을 권장합니다.

업데이트 설치 섹션에 설명된 대로 새 릴리스 업데이트를 확인하고 업데이트를 설치합니다.

설명서

Threat Grid Appliance 설명서(이 문서를 포함하여 *Threat Grid Appliance 설정 및 컨피그레이션 가이드*, 형식화된 릴리스 노트 버전, 통합 가이드 등)는 Cisco.com 웹 사이트의 *설치 및 업그레이드 가이드*에 있는 내부 리소스 페이지에서 확인할 수 있습니다. 이 페이지에는 현재 및 이전 어플라이언스 릴리스의 설명서에 대한 링크가 포함되어 있습니다.

Threat Grid Appliance 설정 및 컨피그레이션 가이드

*Threat Grid Appliance 설정 및 컨피그레이션 가이드*는 현재 문서와 함께 제공됩니다. 이 가이드에는 네트워크 인터페이스, 제안된 방화벽 규칙, 네트워크 다이어그램, 컨피그레이션 명령 및 기타 작업을 포함하는 자세한 설정 정보가 포함되어 있습니다.

Threat Grid Appliance 릴리스 노트

OpAdmin Portal(OpAdmin 포털) > Operations(운영) > Update Appliance(어플라이언스 업데이트) > Release Notes(릴리스 노트)

참고: Threat Grid Appliance 릴리스 노트의 형식화된 PDF 버전도 **설치 및 업그레이드 가이드** 페이지에서 확인할 수 있습니다(위의 링크 참조).

Threat Grid Portal 릴리스 노트

Portal UI Navigation bar(포털 UI 내비게이션 바) > Help(도움말) > Release Notes(릴리스 노트)

Threat Grid Portal 온라인 도움말 및 API 설명서

Threat Grid Portal의 *Threat Grid 사용* 온라인 도움말, API 설명서 및 기타 정보는 Threat Grid Portal 도움말 페이지에서 확인할 수 있습니다.

Threat Grid Portal user interface(Threat Grid Portal 사용자 인터페이스) >Navigation bar(내비게이션 바) > Help(도움말)

설명서에 대한 링크가 있는 **Help(도움말)** 홈 페이지가 열립니다.

ESA/WSA 어플라이언스 설명서

ESA 또는 WSA 어플라이언스와 Threat Grid Appliance의 연결에 대한 자세한 내용은 ESA/WSA 어플라이언스를 Threat Grid Appliance에 연결을 참조하십시오.

ESA/WSA의 온라인 도움말 또는 사용자 가이드의 *"Enabling and Configuring File Reputation and Analysis Services(파일 평판과 분석 서비스 사용 및 구성)"*에 대한 지침을 참조하십시오.

- ESA 사용자 가이드 위치:
  http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-user-guide-list.html
- WSA 사용자 가이드 위치:
  http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html

라이선싱

Threat Grid 라이선스는 *OpAdmin 컨피그레이션 라이선스* 페이지에서 관리됩니다.

Configuration(컨피그레이션) > License(라이선스)

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

속도 제한

API 속도 제한은 라이선스 계약의 조건이 적용되는 어플라이언스에 대한 전역 제한입니다. 이 제한은 API 제출에만 영향을 주며 수동 샘플 제출에는 영향을 주지 않습니다.

속도 제한은 역일이 아닌 롤링 타임의 24시간 창을 기준으로 합니다. 제출 제한을 모두 사용한 경우, 다음 API 제출에서 재시도하기 전 대기 시간에 대한 메시지와 함께 429 오류가 반환됩니다.

가정

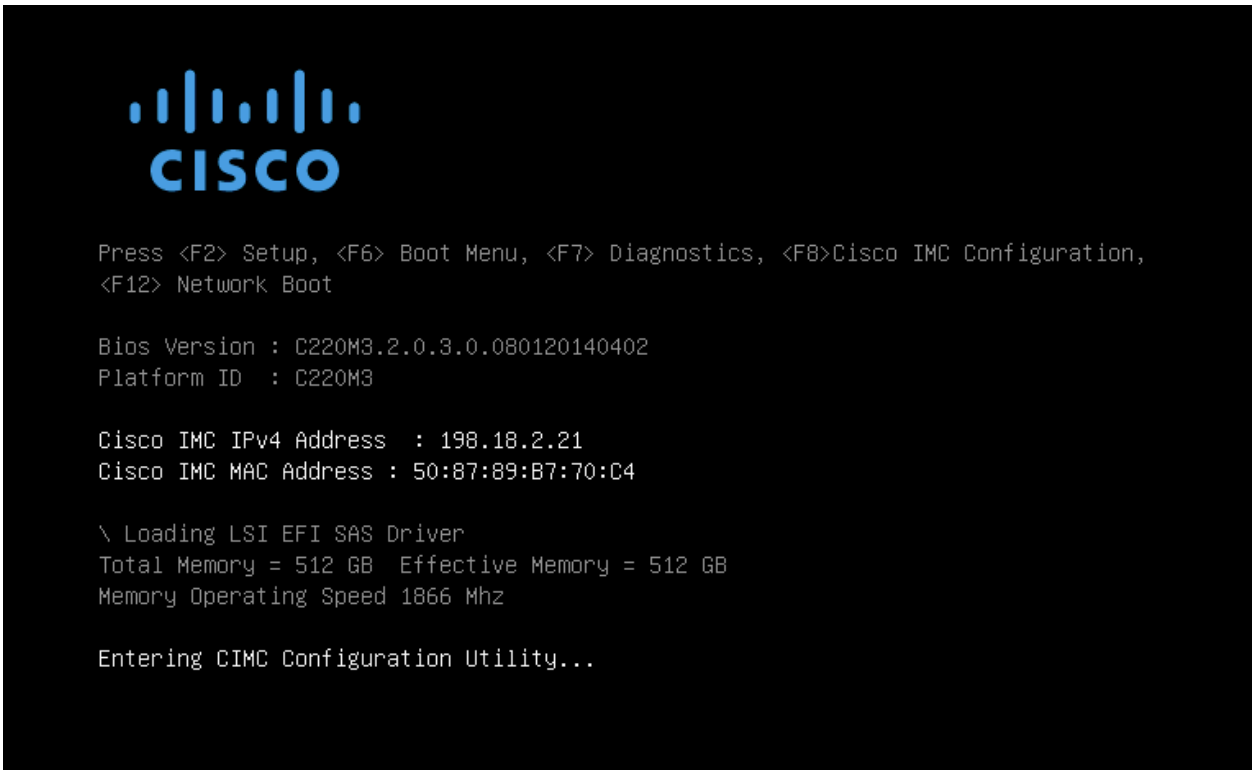
이 가이드에서는 초기 설정 및 컨피그레이션 단계가 *Threat Grid Appliance 설정 및 컨피그레이션 가이드*에 설명된 대로 완료되었으며 초기 테스트 악성코드 샘플이 성공적으로 제출 및 분석되었다고 가정합니다.

관리

전원 켜기

어플라이언스를 켜고 부팅될 때까지 기다립니다. 다음과 같은 Cisco 화면이 잠시 표시됩니다.

그림 1 - 부팅 중 Cisco 화면

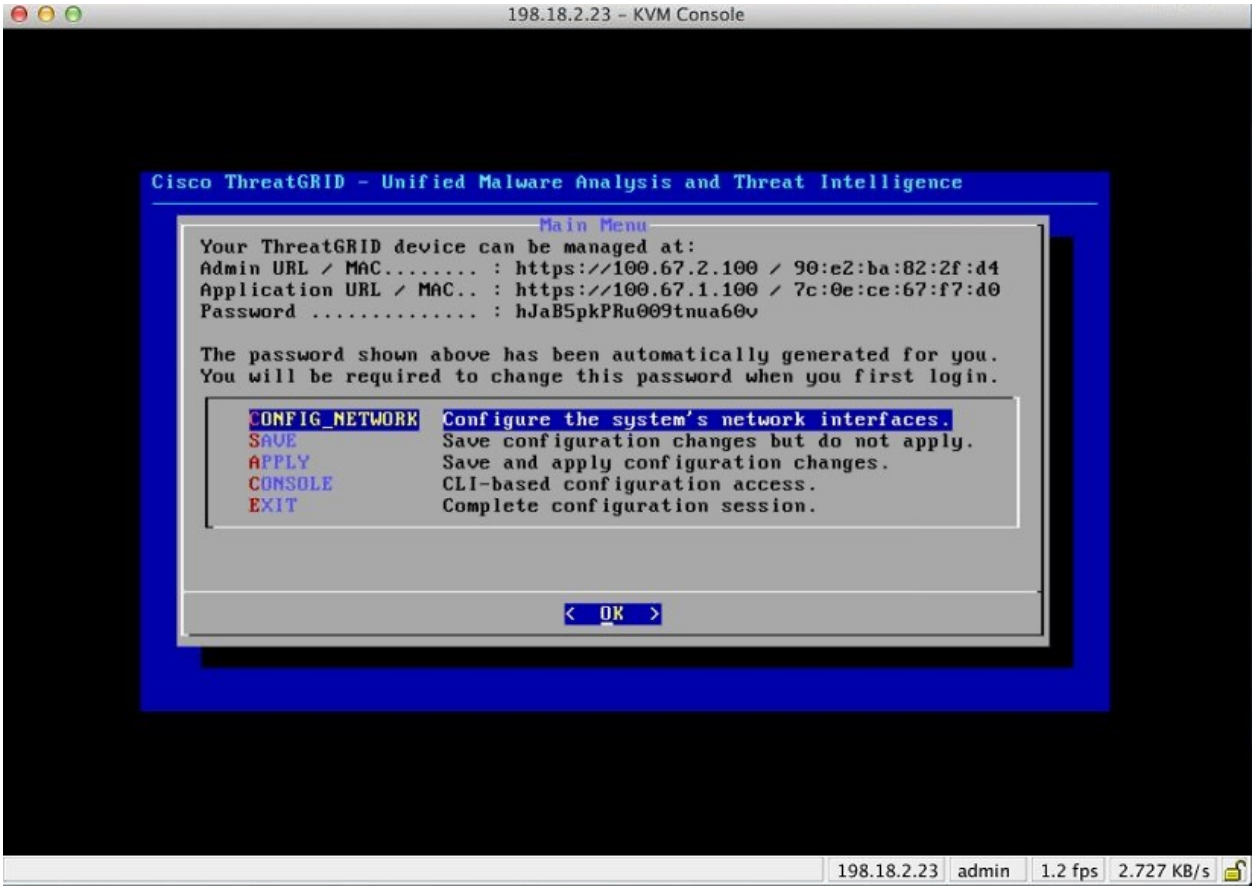


참고: CIMC 인터페이스를 구성하려는 경우, 메모리 검사가 완료된 후 **F8** 키를 누릅니다.

자세한 내용은 Threat Grid Appliance 설정 및 컨피그레이션 가이드의 *CIMC 구성* 섹션을 참조하십시오.

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

그림 2 - TGSH 대화 상자



참고: TG 어플라이언스를 설정 및 구성한 후, TGSH 대화 상자는 더 이상 OpAdmin 인터페이스에 액세스하고 구성하는 데 필요한 비밀번호를 표시하지 않습니다.

Lost Password(분실한 비밀번호): 나중에 비밀번호를 잊어버린 경우, 지침에 대해서는 분실한 비밀번호 복구를 참조하십시오.

로그인 이름 및 비밀번호 - 기본값

Threat Grid Portal UI 관리자

- **로그인:** "admin"
- **비밀번호:** "changeme"

TGA 관리자 - OpAdmin 및 threatgrid 사용자

OpAdmin 관리자 비밀번호는 "threatgrid" 사용자 비밀번호와 동일합니다. OpAdmin 인터페이스에서 유지 관리됩니다. 기본 관리자 비밀번호는 TGA 초기 설정 중에 변경되었으며 해당 단계가 일단 완료되면 확인 가능한 텍스트로 표시되지 않습니다. 비밀번호를 분실했으며 OpAdmin에 로그인할 수 없는 경우, 아래에서 **분실한 비밀번호 복구** 지침대로 수행하십시오.

CIMC(Cisco Integrated Management Controller)

- **로그인:** "admin"
- **비밀번호:** "password"

분실한 비밀번호 복구

기본 관리자 비밀번호는 초기 어플라이언스 설정 및 컨피그레이션 중에 TGSH 대화 상자에만 표시됩니다. 일단 초기 컨피그레이션이 완료되면 비밀번호가 표시 가능한 텍스트에 더 이상 표시되지 않습니다.

참고: 여러 관리자가 있을 경우 LDAP 인증을 TGSH 대화 상자 및 OpAdmin 로그인에 사용할 수 있습니다. 어플라이언스가 LDAP 인증 전용으로 구성된 경우, 복구 모드에서 비밀번호를 재설정하면 시스템 비밀번호를 사용하는 로그인을 허용하도록 인증 모드를 다시 구성합니다.

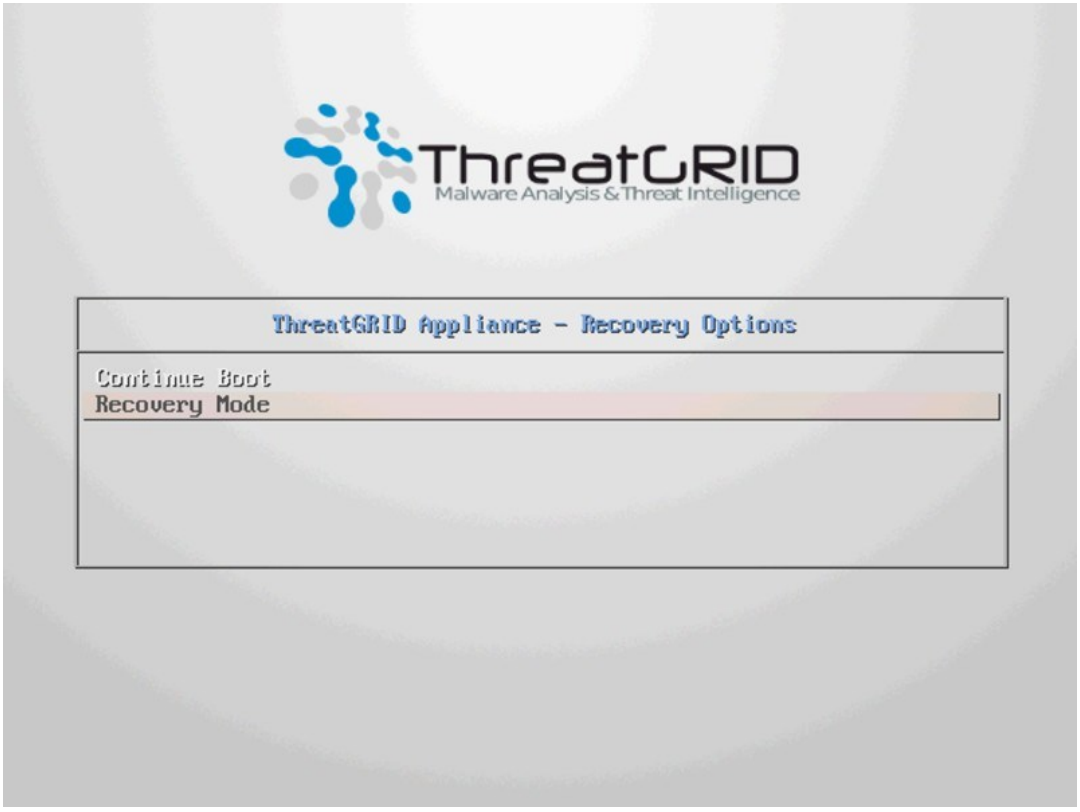
관리자 비밀번호를 분실하여 OpAdmin에 로그인할 수 없는 경우, 다음 단계를 완료하십시오.

분실한 관리자 비밀번호 재설정

1. 어플라이언스를 재부팅합니다.

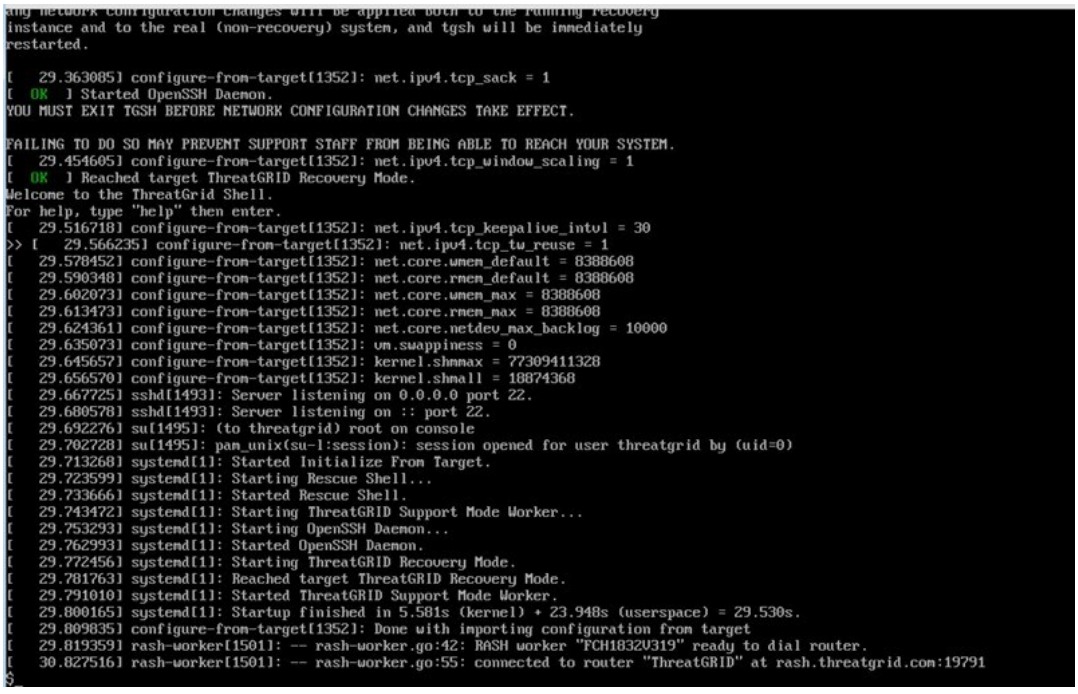
   부팅하는 동안 아래에 표시된 것과 같이 간단한 시간 창이 표시되어 **복구 모드**를 선택할 수 있습니다.

그림 3 - 부팅 메뉴 - 복구 모드



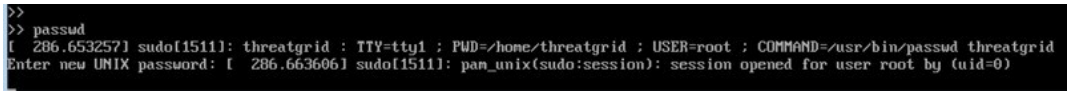
Threat Grid Shell이 열립니다.

그림 4 - 복구 모드의 Threat Grid Shell



2. Passwd를 실행하여 비밀번호를 변경합니다.

그림 5 - 새 비밀번호 입력



참고: 명령 프롬프트는 이 모드에서 항상 표시되지는 않으며 로깅 출력은 입력한 위치의 어느 지점에서나 표시될 수 있습니다. 이것은 입력에 영향을 주지는 않으며 "보이지 않게" 계속해서 입력할 수 있습니다.

3. 로깅 출력에서 2개의 줄을 무시합니다. 비밀번호를 보이지 않게 입력하고 Enter 키를 누른 다음 비밀번호를 다시 입력하고 다시 Enter 키를 누릅니다. 비밀번호는 표시되지 않습니다.
4. 새 비밀번호를 저장하기 위해 명령줄에서 exit를 **입력해야** 합니다.

   재부팅해도 새 비밀번호가 저장되지 않습니다. 모든 내용이 문제 없어 보이는 경우에도 exit를 입력하지 않는 경우 비밀번호 변경이 자동으로 삭제됩니다.
5. 그런 다음 reboot 명령을 입력하고 Enter 키를 눌러 일반 모드에서 어플라이언스를 시작합니다.

업데이트 설치

새 버전의 Threat Grid Appliance를 업데이트하기 전에, *Threat Grid Appliance 설정 및 컨피그레이션 가이드*에 설명되어 있는 초기 설정 및 컨피그레이션 단계를 완료해야 합니다.

새 어플라이언스: 이전 버전과 함께 제공된 새로운 어플라이언스가 있고 업데이트를 설치하려는 경우, 초기 컨피그레이션을 먼저 완료해야 합니다. 모든 어플라이언스 컨피그레이션을 완료할 때까지 업데이트를 적용하지 마십시오.

어플라이언스 업데이트는 라이선스가 설치되어야만 다운로드할 수 있으며 데이터베이스를 포함하여 어플라이언스가 완전히 구성되지 않은 경우에는 올바르게 적용되지 않을 수 있습니다.

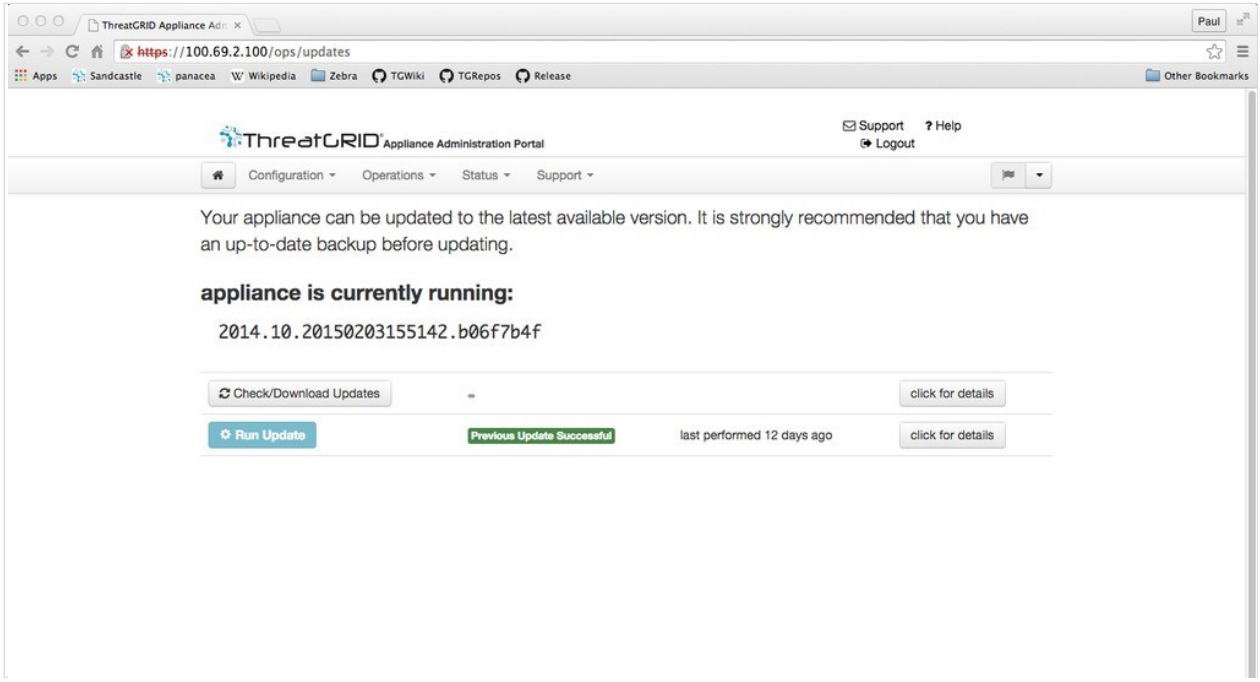
Threat Grid Appliance 업데이트는 OpAdmin 포털을 통해 적용됩니다.

업데이트는 한 방향으로 이루어지므로 더 최신 버전으로 업그레이드한 후에는 이전 버전으로 되돌릴 수 없습니다. 업데이트를 테스트하려면 분석을 위해 샘플을 제출합니다.

1. **Operations(운영)** 메뉴에서 **Update Appliance(어플라이언스 업데이트)**를 선택합니다.

   업데이트 페이지가 열리고 어플라이언스의 현재 빌드가 표시됩니다.

그림 6 - 어플라이언스 버전 번호



2. **Check/Download Updates(업데이트 확인/다운로드)**를 클릭합니다. 소프트웨어에서 Appliance 소프트웨어의 최신 업데이트/버전이 있는지 확인하고, 있을 경우 다운로드합니다.

   참고: 다운로드에 시간이 걸릴 수 있습니다.

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

3. 업데이트가 다운로드되면 **Run Update(업데이트 실행)**를 클릭하여 설치합니다.

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 릴리스 버전 번호에 해당합니다.

빌드 번호	릴리스 버전	릴리스 날짜	참고
2016.05.20170105200233.32f70432.rel	2.1.6	2017-01-05	LDAP 인증 추가
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	기본적으로 제조업의 관심 버전
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 **참고:** 이 버전이 2.0 업그레이드의 시작점입니다.	2016-01-27	2.0.4 업데이트를 위한 시작점

빌드 번호	릴리스 버전	릴리스 날짜	참고
2014.10.20151123133427.898f70c2	v1.4.5	2015-11-25	
2014.10.20151116154826.9af96403	v1.4.4		
2014.10.20151020111307.3f124cd2	v1.4.3		
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 **참고:** 1.0+hotfix2는 대용량 파일을 중단 없이 처리할 수 있도록 업데이트 시스템 자체를 수정하는 필수 업데이트입니다.		
2014.10.20141125162158.8afc5e2f	v1.0		

업데이트 포트

Threat Grid Appliance는 SSH, 포트 22를 통해 릴리스 업데이트를 다운로드합니다.

- 어플라이언스 버전 1.1부터 릴리스 업데이트는 아래에 설명된 것과 같이 웹 기반 관리 인터페이스(OpAdmin)가 아니라 텍스트(curses) 인터페이스에서 적용될 수 있습니다.
- 버전 1.3의 경우 DHCP를 사용하는 시스템은 명시적으로 DNS를 지정해야 합니다. 이전 버전의 경우에는 지정하지 않았습니다. 버전 1.3으로 명시적으로 지정된 DNS 서버가 없는 시스템의 업그레이드는 실패합니다.

업데이트 트러블슈팅

"*데이터베이스 업그레이드 실패*" 메시지는 새로운 어플라이언스가 예상한 버전보다 이전 버전의 PostgreSQL을 실행 중임을 의미합니다.

이것은 자동화된 데이터베이스 마이그레이션 프로세스가 성공하지 않았음을 의미하므로 2.0으로의 모든 업그레이드를 수행하기 전에 해결해야 할 중요한 사항입니다.

자세한 내용은 v2.0.1 릴리스 노트를 참조하십시오.

지원 - Threat Grid 문의

도움이 필요한 경우, 다음과 같이 여러 가지 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). 주문 송장에 포함된 서비스 계약 번호도 필요합니다.

  https://tools.cisco.com/ServiceRequestTool/scm/mgmt/case

- **전화:** 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

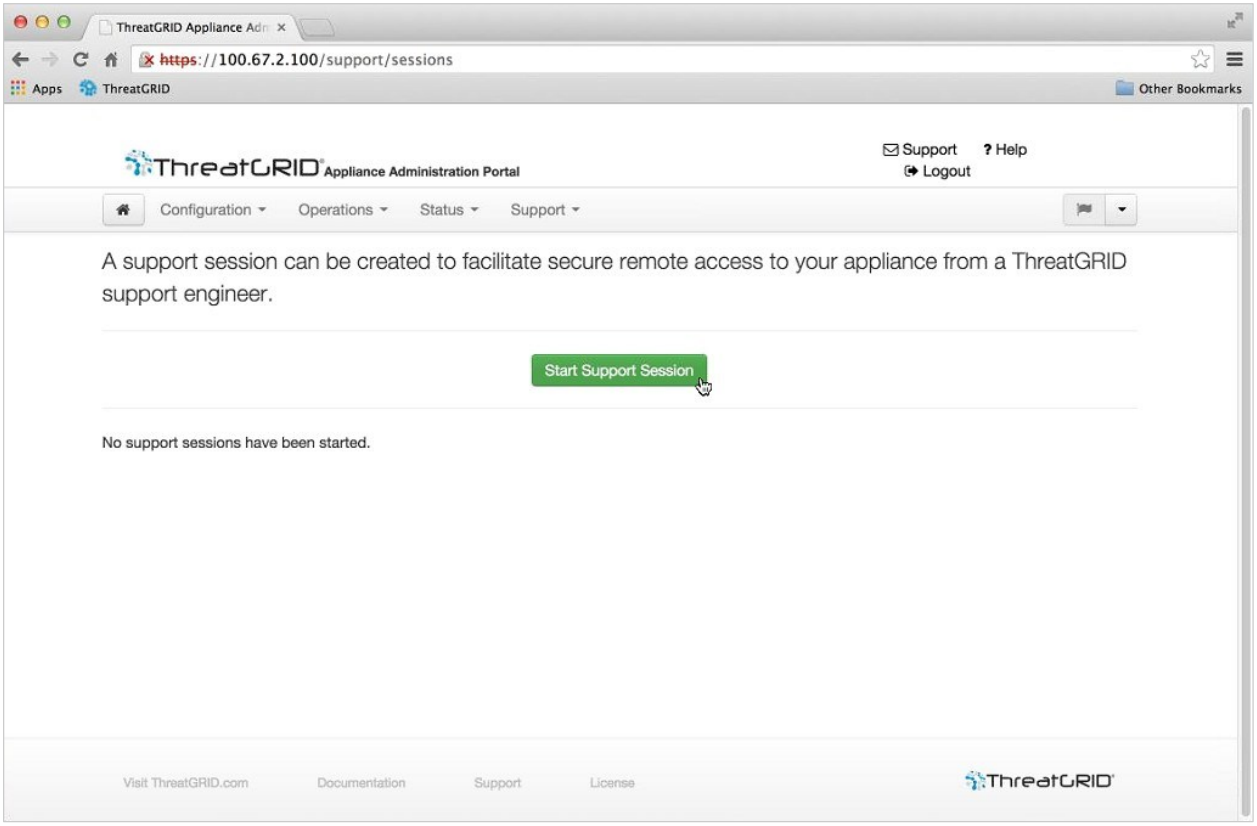
지원 모드

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.

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

그림 7 - 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. **Support(지원)** 메뉴에서 **Support Snapshots(스냅샷 지원)**를 선택합니다.
2. 스냅샷을 찍습니다.
3. 찍은 스냅샷을 직접 .tar .gz로 다운로드하거나 **Submit(제출)**을 눌러 Threat Grid 스냅샷 서버에 자동으로 업로드할 수 있습니다.

백업

OpAdmin의 Operations(운영) > Backups(백업)

백업은 설치된 SSL 인증서 및 네트워킹 컨피그레이션과 같이 어플라이언스에서 현재 활성 상태인 config 파일 집합을 포함합니다. 이 집합은 샘플, 사용자 또는 조직에 대한 데이터를 포함하지 않습니다.

여러 백업은 어플라이언스에서 생성되고 다운로드될 수 있습니다.

컨피그레이션 관리

초기의 Threat Grid Appliance 컨피그레이션은 *Threat Grid Appliance 설정 및 컨피그레이션 가이드*에 기록된 대로 어플라이언스 설정 중에 수행되었습니다.

Threat Grid Appliance 컨피그레이션은 **TGSH 대화 상자** 및 **OpAdmin 포털** 인터페이스에서 관리됩니다.

Threat Grid 조직 및 사용자 어카운트는 Threat Grid Portal UI를 통해 관리됩니다(내비게이션 바 오른쪽 상단 **Welcome(시작)** 메뉴).

TGSH 대화 상자 및 OpAdmin 컨피그레이션 작업에 대해서는 다음 섹션에 자세히 설명되어 있습니다.

네트워크 인터페이스 컨피그레이션 관리 – TGSH 대화 상자

TGSH 대화 상자 인터페이스는 주로 다음을 관리하기 위해 사용됩니다.

- 네트워크 인터페이스 컨피그레이션
- OpAdmin 관리자 비밀번호 확인
- 업데이트 설치
- 지원 모드 활성화
- 지원 스냅샷 생성 및 제출

참고: IP를 얻기 위해 DHCP를 사용 중인 경우, 아래의 *Networking(네트워킹)* 섹션으로 건너뛰십시오(*DHCP 사용).*

TGSH 대화 상자 인터페이스를 구성하는 방법

1. TGSH 대화 상자에 로그인합니다.

   참고: LDAP 전용 인증을 위해 구성된 경우 LDAP을 사용하여 TGSH 대화 상자에 로그인만 할 수 있습니다. 인증 모드가 시스템 비밀번호 또는 LDAP으로 설정된 경우, TGSH 대화 상자 로그인은 시스템 로그인만 허용합니다.

2. **TGSH 대화 상자** 인터페이스에서 **CONFIG_NETWORK**를 선택합니다.

   현재 네트워크 설정을 표시하는 네트워크 컨피그레이션 콘솔이 열립니다.

3. 필요에 따라 적절히 변경합니다.

   참고: 기존 문자에서 **백스페이스** 키를 눌러야 새 문자를 입력할 수 있습니다.

4. Dirty 네트워크의 **DNS 이름**을 공백으로 둡니다.

5. 네트워크 설정을 업데이트한 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.

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

   콘솔은 빈 회색 상자가 되고, 수행한 컨피그레이션 변경 사항에 대한 자세한 정보를 나열합니다.

7. **OK(확인)**를 선택합니다.

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

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 연결하는 한 가지 방법은 사용자 '**threatgrid**'로 관리 IP 주소에 SSH 액세스하는 것입니다. 필수 비밀번호는 임의로 생성되어 초기에 TGSH 대화 상자에 표시되는 초기 비밀번호 또는 OpAdmin 컨피그레이션의 첫 단계에서 만드는 새 관리자 비밀번호입니다.

비밀번호 업데이트

비밀번호를 잊어버리셨나요? *분실한 비밀번호 복구(*위의 *시작하기* 섹션)를 참조하십시오.

복구 모드에서 네트워킹 설정

1. 재부팅을 시작하고 짧은 기간 동안만 표시되는 부팅 메뉴를 기다립니다(위의 그림 3 - 부팅 메뉴 - 지원 모드 참조).
2. 복구 모드를 선택합니다. 시스템이 시작될 때까지 2분 정도 기다립니다.
3. 일단 시스템이 시작되면 clean 명령 프롬프트가 나타날 때까지 Enter 키를 여러 번 누릅니다.
4. **netctl clean**을 입력하고 다음과 같이 질문에 대답합니다.
    - 컨피그레이션 유형: 고정
    - IP 주소: <Clean IP 주소>/<넷마스크>
    - 게이트웨이 주소: <Clean 네트워크 게이트웨이>
    - 경로: <빈 칸으로 두기>
    - 마지막 질문에 **y**로 대답합니다.
5. **Exit**를 입력하여 컨피그레이션을 적용합니다.

이 시점에서 어플라이언스는 포트 19791/tcp에서 Clean 인터페이스의 아웃바운드 지원 연결 열기를 시도합니다.

기본 컨피그레이션 관리 – OpAdmin 포털

초기 설정 및 컨피그레이션 마법사는 *Threat Grid Appliance 설정 및 컨피그레이션 가이드*에 설명되어 있습니다. 새 어플라이언스에서는 관리자가 추가 컨피그레이션을 완료해야 하며 시간이 경과함에 따라 OpAdmin 설정을 업데이트해야 할 수 있습니다.

OpAdmin 포털은 Threat Grid Appliance 관리자의 기본 컨피그레이션 인터페이스입니다. 이 포털은 TGA의 **Admin** 인터페이스에 IP 주소를 구성하면 사용할 수 있는 웹 포털입니다.

OpAdmin은 어플라이언스 구성에 권장되는 툴이며, 실제로 대부분의 어플라이언스 컨피그레이션은 OpAdmin을 통해서만 수행할 수 있습니다. OpAdmin은 다음을 포함하여 여러 중요한 Threat Grid Appliance 컨피그레이션 설정을 구성하고 관리하는 데 사용됩니다.

- 관리자 비밀번호(OpAdmin 및 "threatgrid" 사용자의 경우)
- Threat Grid 라이선스
- 속도 제한
- SMTP
- SSH
- SSL 인증서
- DNS 서버(FireAMP Private Cloud 통합을 위한 DNS 컨피그레이션 포함)
- NTP 서버
- 서버 알림
- Syslog 메시지 및 Threat Grid 알림 원격 서버 설정
- CA 인증서 관리(FireAMP Private Cloud 통합용)
- LDAP 인증

참고: OpAdmin의 컨피그레이션 업데이트는 컨피그레이션 동안 IP 주소에 장애가 발생할 가능성을 줄이기 위해 하나의 세션에서 완료해야 합니다.

참고: OpAdmin은 게이트웨이 항목을 검증하지 않습니다. 잘못된 게이트웨이를 입력하고 저장하는 경우, OpAdmin 인터페이스에 액세스할 수 없습니다. 네트워킹 컨피그레이션이 Admin 인터페이스에서 수행된 경우 네트워킹 컨피그레이션을 수정하기 위해 콘솔을 사용해야 합니다. Admin이 계속 유효한 경우, OpAdmin에서 수정하고 재부팅할 수 있습니다.

미리 알림: OpAdmin은 HTTPS를 사용합니다. 관리 IP에서 브라우저를 가리키는 것으로는 충분하지 않고 https://adminIP/ 또는 https://adminHostname/를 가리켜야 합니다.

SSH 키

SSH 키를 설정하면 Threat Grid Appliance 관리자에게 SSH(threatgrid@<host>)를 통한 TGSH 대화 상자 액세스를 제공합니다.

루트 액세스 또는 명령 셸은 제공하지 않습니다. 여러 개의 키를 추가할 수 있습니다.

Configuration(컨피그레이션) > SSH

Syslog

이메일을 통해 시스템 알림을 전달하도록 설정(OpAdmin의 **Configuration(컨피그레이션)** > **Notifications(알림)**)할 수 있는 주기적인 알림 외에, syslog 메시지와 Threat Grid 알림을 수신하도록 원격 syslog 서버를 구성할 수 있습니다.

1. OpAdmin의 **Configuration(컨피그레이션)** > **Syslog**
2. 제공된 필드에 DNS 서버를 입력한 다음 드롭다운 목록에서 프로토콜을 선택합니다. TCP는 기본값이며 나머지는 UDP입니다.

3. DNS 조회를 수행하려면 **Verification(확인)** 상자를 선택합니다(**Save(저장)** 클릭 시). 호스트에서 이름을 해석할 수 없는 경우, 유효한 호스트 이름을 입력할 때까지 오류를 인쇄하고 저장하지 않습니다.

   Verification(확인) 상자를 선택하지 않은 경우, 어플라이언스는 DNS에서 유효한지 여부에 관계없이 모든 이름을 수락합니다.

4. **Save(저장)**를 클릭합니다.

편집 또는 삭제하는 방법: Syslog DNS를 업데이트해야 하는 경우, 간단하게 편집하거나 삭제하고 **Save(저장)**를 클릭합니다.

OpAdmin 및 TGSH 대화 상자의 LDAP 인증 구성

2.1.6 릴리스는 Threat Grid Appliance에 추가된 OpAdmin과 TGSH 대화 상자 로그인에 대한 LDAP 인증 및 권한 부여를 포함합니다. 이전에는 OpAdmin과 TGSH 대화 상자 인터페이스에 비밀번호가 1개만 있었으며 하나 이상의 어플라이언스 관리자를 지닌 경우, 관리자 간에 비밀번호를 공유해야 했습니다. 이는 잘못된 생각일 뿐만 아니라 많은 고객은 이러한 시나리오를 사용하지 않을 것을 요구하고 있습니다. Cisco는 해결책으로 LDAP 인증을 구현했습니다.

현재 도메인 컨트롤러 또는 LDAP 서버에서 관리되는 다양한 크리덴셜을 사용하여 여러 어플라이언스 관리자를 인증할 수 있습니다. LDAP 컨피그레이션은 중요하므로 설정하기 전에 세부 사항을 철저하게 이해하고 이 단계를 주의하여 수행하는 것이 좋습니다.

인증 모드는 시스템 비밀번호 전용 인증, 시스템 비밀번호 인증 또는 LDAP 및 LDAP 전용 인증을 포함합니다.

LDAP, LDAPS, STARTLS를 사용하는 LDAP의 3가지 LDAP 프로토콜 옵션이 있습니다.

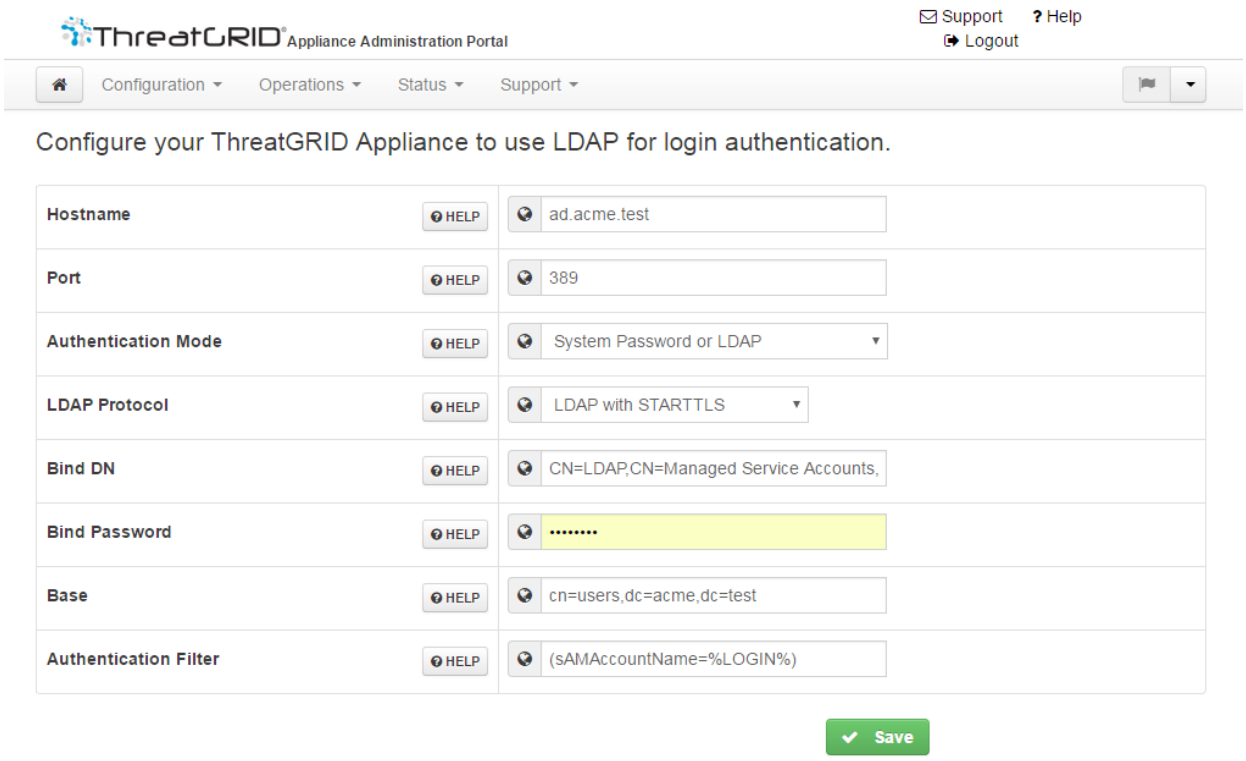
다음 사항에 유의하십시오.

- LDAP을 설정할 때 실수로 어플라이언스 외부에서 잠금이 설정되는 것을 방지하기 위해 "이중" 인증 모드(**시스템 비밀번호 또는 LDAP**)가 필수사항입니다. **LDAP 전용**은 초기에는 선택할 수 없습니다. 이 모드가 처음으로 작동하는지 확인하려면 이중 모드를 사용해야 합니다. **LDAP 전용**으로 전환하려면 초기 컨피그레이션 이후에 OpAdmin에서 로그아웃한 다음 LDAP 크리덴셜을 사용하여 다시 로그인해야 합니다.
- LDAP 전용 인증을 위해 구성된 경우 LDAP을 사용하여 TGSH 대화 상자에 로그인만 할 수 있습니다. 인증 모드가 시스템 비밀번호 또는 LDAP으로 설정된 경우, TGSH 대화 상자 로그인은 시스템 로그인만 허용합니다.
- 어플라이언스가 LDAP 인증 전용(**LDAP 전용**)으로 구성된 경우, 복구 모드에서 비밀번호를 재설정하면 시스템 비밀번호를 사용하는 로그인을 허용하도록 인증 모드를 다시 구성합니다.
- 멤버십을 제한하기 위해 인증 필터를 설정했는지 확인합니다.
- TGSH 대화 상자 및 OpAdmin은 **LDAP 전용** 모드에서만 LDAP 크리덴셜을 요청합니다. "LDAP 전용"이 구성된 경우, TGSH 대화 상자는 시스템 비밀번호를 요청하는 대신 LDAP 사용자/비밀번호를 요청합니다.
- 인증이 **시스템 비밀번호 또는 LDAP**에 대해 구성된 경우, TGSH 대화 상자는 계속해서 시스템 비밀번호만 요청하며 두 가지 모두를 요청하지는 않습니다.
- LDAP 트러블슈팅: 문제가 발생하면 복구 모드에서 비밀번호 재설정을 수행하여 이를 비활성화합니다.
- SSH를 통한 TGSH 대화 상자 액세스: LDAP 전용 모드일 때 ssh를 통한 tgsh-dialog 액세스용 LDAP 크리덴셜 **외**에 시스템 비밀번호 또는 구성된 SSH 키가 필요합니다.

LDAP 인증 구성 방법

1. OpAdmin에서 **Configuration(컨피그레이션)** > **LDAP**을 선택합니다. LDAP configuration(LDAP 컨피그레이션) 페이지가 열립니다.

그림 8 - LDAP 인증 컨피그레이션



2. 필드에 입력합니다.

   자세한 설명 및 추가 정보를 보려면 각 필드 옆에 있는 **?Help(?도움말)** 버튼을 클릭합니다.

   참고로, **LDAP 전용**을 구현하기 위해 설정을 변경하려면 LDAP 인증을 처음 구성할 때 시스템 비밀번호 또는 LDAP을 선택하고 OpAdmin에서 로그아웃한 다음 LDAP 크리덴셜을 사용하여 다시 로그인해야 합니다.

3. **Save(저장)**를 클릭합니다.

이제 사용자가 OpAdmin 또는 TGSH 대화 상자에 로그인할 때 다음 화면이 표시됩니다.

그림 9 - LDAP 전용

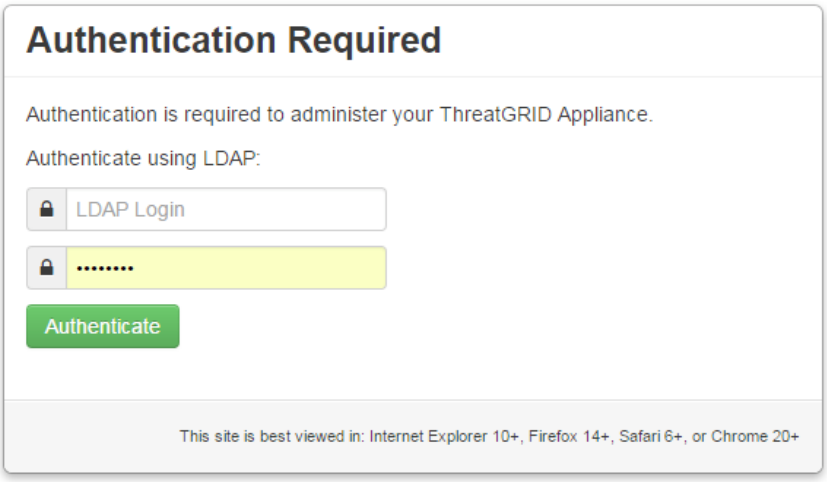
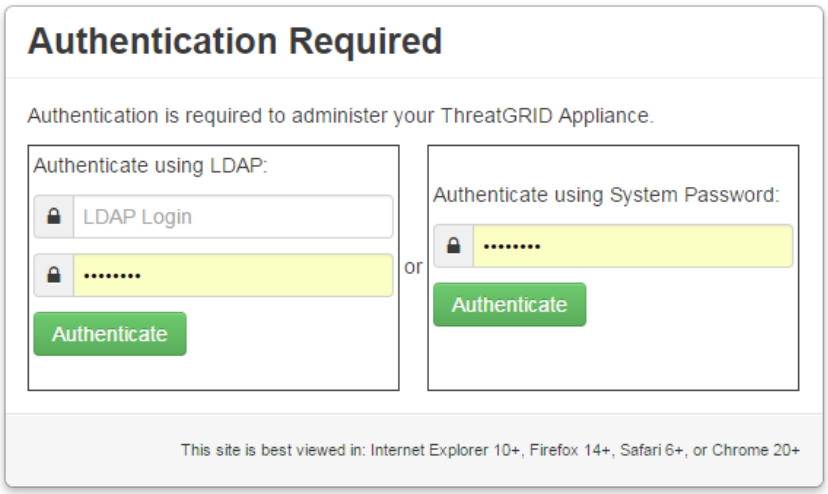


그림 10 - 시스템 비밀번호 또는 LDAP

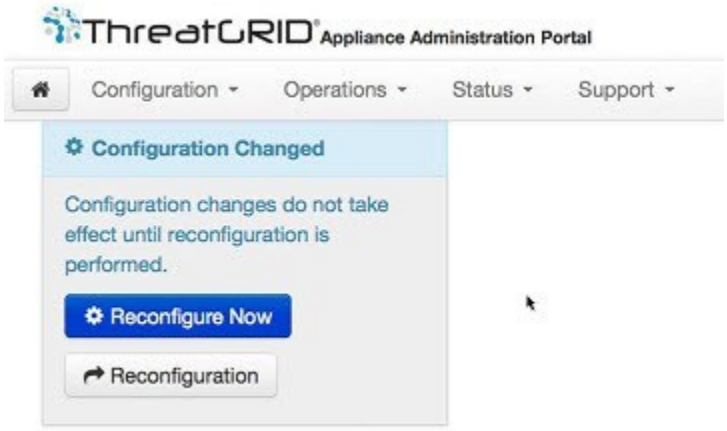


다시 컨피그레이션

컨피그레이션 설정을 변경할 경우, 하늘색 알림이 컨피그레이션 메뉴 아래에 표시됩니다. OpAdmin 컨피그레이션 설정 업데이트를 완료한 경우, 별도의 단계에서 다시 컨피그레이션을 저장해야 합니다.

1. **Configuration Changed(컨피그레이션 변경됨)**를 클릭합니다. **Reconfiguration(다시 컨피그레이션)** 대화 상자가 열립니다.

그림 11 - 지금 다시 구성



2. 어플라이언스에 변경 사항을 적용하려면 **Reconfigure(다시 구성)**를 클릭합니다.

DHCP 사용

대부분의 어플라이언스 사용자는 DHCP로 구성된 네트워크를 사용하지 않습니다. 그러나 DHCP를 사용하도록 구성된 네트워크에 연결된 경우, 이 섹션을 참고하십시오.

참고: 초기 어플라이언스 네트워크 컨피그레이션에서 DHCP를 사용했으며 이제 고정 IP 주소로 전환해야 하는 경우, 아래의 *네트워크 컨피그레이션 및 DHCP*를 참조하십시오.

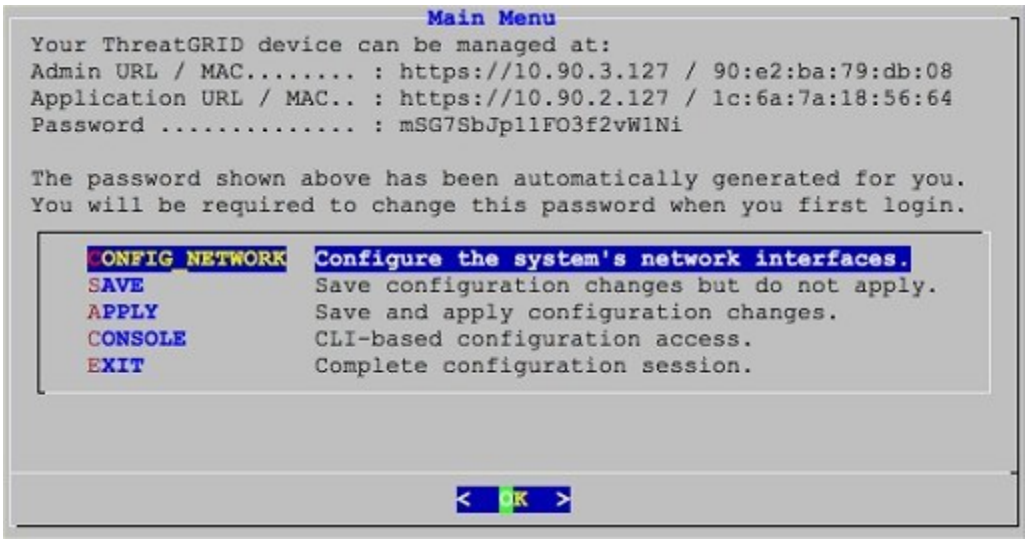
TGSH 대화 상자는 OpAdmin 포털 인터페이스에 액세스하고 구성하는 데 필요한 정보를 표시합니다.

DHCP의 IP 주소는 어플라이언스가 부팅된 직후에는 표시되지 않을 수 있습니다. 잠시만 기다려 주십시오.

DHCP의 명시적인 DNS

v1.3의 경우 DHCP를 사용하는 시스템은 명시적으로 DNS를 지정해야 합니다. 이전 버전의 경우에는 지정하지 않았습니다. 버전 1.3으로 명시적으로 지정된 DNS 서버가 없는 시스템의 업그레이드는 실패합니다.

그림 12 - TGSH 대화 상자(DHCP를 사용하도록 구성된 네트워크에 연결됨)



- **Admin URL(관리 URL):** Admin 네트워크. OpAdmin에서 나머지 컨피그레이션 작업을 계속 수행하려면 이 주소가 필요합니다.
- **Application URL(애플리케이션 URL):** Clean 네트워크

참고: 이것은 OpAdmin에서 컨피그레이션을 완료한 이후에 Threat Grid 애플리케이션에 액세스하는 데 사용할 주소입니다.

- Dirty 네트워크는 표시되지 않습니다.
- **Password(비밀번호)**는 어플라이언스 설치 중에 임의로 생성된 초기 관리자 비밀번호입니다. 초기 단계의 OpAdmin 컨피그레이션 프로세스이므로 이후에 이 비밀번호를 변경해야 합니다.

DHCP를 영구적으로 사용할 계획인 경우, 관리 IP 주소를 정적으로 변경해야 하는 경우가 아니면 추가 네트워크 컨피그레이션이 필요하지 않습니다.

네트워크 컨피그레이션 및 DHCP

- 초기 컨피그레이션에 DHCP를 사용했으며 지금 모든 3개의 네트워크에 대해 DHCP에서 영구 고정 IP 주소로 IP 할당을 조정해야 하는 경우, 아래 단계대로 수행하십시오.

참고: OpAdmin은 게이트웨이 항목을 검증하지 않습니다. 잘못된 게이트웨이를 입력하고 저장하는 경우, OpAdmin 인터페이스에 액세스할 수 없습니다. 네트워킹 컨피그레이션이 Admin 인터페이스에서 수행된 경우 네트워킹 컨피그레이션을 수정하기 위해 콘솔을 사용해야 합니다. Admin이 계속 유효한 경우, OpAdmin에서 수정하고 재부팅할 수 있습니다.

1. 왼쪽 열에서, **Network(네트워크)**를 클릭합니다. **Configuration(컨피그레이션) > Network(네트워크)**를 License(라이선스) 창에서 선택했지만 DHCP 네트워크 컨피그레이션이 아직 수행되지 않았습니다.

   Network Configuration(네트워크 컨피그레이션) 페이지가 표시됩니다.

Clean

2. **IP 할당.** 드롭다운 목록에서 **Static(고정)**을 선택합니다.
3. **IP 주소. Clean** 네트워크 인터페이스의 고정 IP 주소를 입력합니다.
4. **Subnet mask(서브넷 마스크)** 및 **Gateway(게이트웨이)**를 적절하게 입력합니다.
5. **Validate DNS Name(DNS 이름 검증)** 옆에 있는 상자를 선택하여 DNS가 입력한 IP 주소로 분석되는지 확인합니다.

Dirty

6. **IP 할당.** 드롭다운 목록에서 Static(고정)을 선택합니다.
7. **IP 주소. Dirty** 네트워크 인터페이스의 고정 IP 주소를 입력합니다.
8. **Subnet mask(서브넷 마스크)** 및 **Gateway(게이트웨이)**를 적절하게 입력합니다.

관리

Admin 네트워크 설정은 초기 어플라이언스 설정 및 컨피그레이션 동안 **TGSH 대화 상자**를 사용하여 구성되었습니다.

DNS

9. **Primary(기본)** 및 **Secondary DNS(보조 DNS)** 서버 필드를 입력합니다.

설정 저장

10. 작업이 완료되면 **Next(다음)(컨피그레이션 적용)**를 클릭하여 네트워크 컨피그레이션 설정을 저장합니다.

SMTP/이메일

이메일 컨피그레이션은 *Email(이메일)* 페이지에서 관리됩니다.

시간

NTP 서버는 *Date and Time(날짜 및 시간)* 페이지에서 관리됩니다.

DHCP 컨피그레이션 적용

DHCP 컨피그레이션 설정을 적용하려면 **Configuration Changed(컨피그레이션 변경됨)**를 클릭한 다음 **Reconfigure Now(지금 다시 구성)**를 클릭합니다.

SSL 인증서 및 Threat Grid Appliance

Threat Grid Appliance를 통해 들어오고 나가는 모든 네트워크 트래픽은 SSL을 사용하여 암호화됩니다. SSL 인증서를 관리하는 방법에 대한 전체 설명은 이 가이드의 범위를 벗어납니다. 그러나 SSL 인증서를 설정하여 Threat Grid Appliance와 ESA/WSA 어플라이언스, FireAMP Private Cloud와의 연결 및 기타 통합을 지원하는 단계를 안내하기 위해 다음과 같은 정보가 제공됩니다.

SSL을 사용하는 인터페이스

SSL을 사용하는 Threat Grid Appliance에는 2개의 인터페이스가 있습니다.

- **Clean** 인터페이스 - Threat Grid Portal UI 및 API, 통합(ESA/WSA 어플라이언스, FireAMP Private Cloud Disposition Update Service 등) 지원
- **Admin** 인터페이스 - **OpAdmin 포털** 지원

지원되는 SSL/TLS 버전

- TLSv1.0
- TLSv1.1
- TLSv1.2

고객 제공 CA 인증서 지원

2.0.3 릴리스에서는 고객이 고유한 신뢰할 수 있는 인증서 또는 CA 인증서를 가져올 수 있게 하여 고객이 제공하는 CA 인증서를 지원합니다.

SSL 인증서 - 자체 서명 기본값

Threat Grid Appliance는 자체 서명 SSL 인증서와 키 집합이 미리 설치된 상태로 제공됩니다. 한 집합은 **Clean** 인터페이스에 사용되고, 다른 집합은 **Admin** 인터페이스에 사용됩니다. 어플라이언스 SSL 인증서는 관리자가 교체할 수 있습니다.

기본 Threat Grid Appliance SSL 인증서 호스트 이름(공용 이름)은 "*pandem*"이며 유효 기간은 10년입니다. 컨피그레이션 동안 다른 호스트 이름이 Threat Grid Appliance에 할당된 경우, 인증서의 호스트 이름과 CN이 더 이상 일치하지 않습니다. 인증서의 호스트 이름은 연결 ESA 또는 WSA 어플라이언스 또는 기타 통합 Cisco 디바이스 또는 서비스에서 예상하는 호스트 이름과 일치해야 합니다. 인증서에 사용된 CN이 어플라이언스의 호스트 이름과 일치할 경우, 많은 클라이언트 애플리케이션은 SSL 인증서를 필요로 하기 때문입니다.

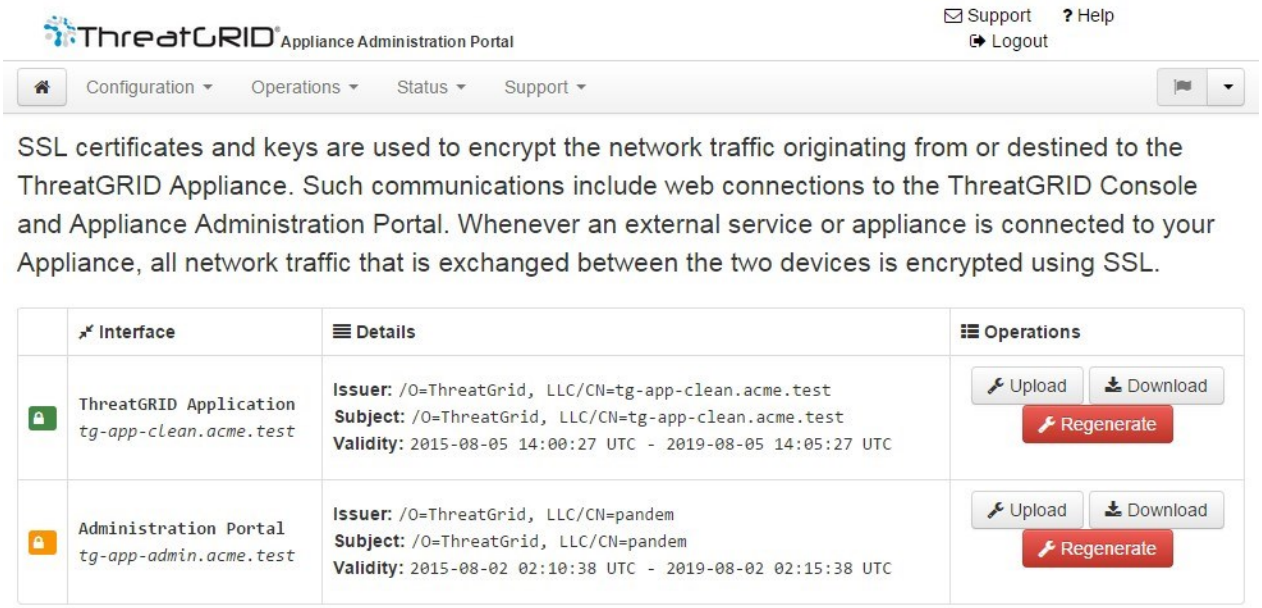
인바운드 연결을 위한 SSL 인증서 구성

ESA/WSA 어플라이언스 및 FireAMP Private Clouds 같은 다른 Cisco 제품의 경우, Threat Grid Appliance와 통합하고 여기에 샘플을 제출할 수 있습니다. 이러한 통합은 Threat Grid Appliance의 관점에서 *인바운드* 연결입니다. 통합 어플라이언스 또는 기타 디바이스는 Threat Grid Appliance의 SSL 인증서를 신뢰할 수 있어야 하므로, TGA에서 인증서를 내보낸 다음(우선 CN 필드에서 올바른 호스트 이름을 사용 중인지 확인하고 필요한 경우 이를 다시 생성하거나 교체), 해당 인증서를 통합 어플라이언스 또는 서비스로 가져와야 합니다.

인바운드 SSL 연결에 사용되는 Threat Grid Appliance에 대한 인증서는 **SSL Certificate Configuration(SSL 인증서 컨피그레이션)** 페이지에서 구성됩니다. **Clean** 및 **Admin** 인터페이스에 대한 SSL 인증서는 개별적으로 구성할 수 있습니다.

OpAdmin > Configuration(컨피그레이션) > SSL을 선택합니다. SSL Certificate configuration(SSL 인증서 컨피그레이션) 페이지가 열립니다.

그림 13 - SSL 인증서 컨피그레이션 페이지



위의 그림에는 2개의 SSL 인증서가 있습니다. "ThreatGRID Application(ThreatGRID 애플리케이션)"은 **Clean** 인터페이스이고, "Administration Portal(관리 포털)"은 **Admin** 인터페이스입니다.

CN 검증

SSL Certificate Configuration(SSL 인증서 컨피그레이션) 페이지에서 색상별 자물쇠 아이콘은 TG 어플라이언스에서 SSL 인증서의 상태를 나타냅니다. 호스트 이름은 SSL 인증서에 사용된 CN("Common Name")과 일치해야 합니다. 이 두 이름이 일치하지 않을 경우, 현재 호스트 이름에서 사용하는 인증서로 교체해야 합니다. 아래의 SSL 인증서 교체를 참조하십시오.

- 녹색 자물쇠 아이콘은 Clean 인터페이스 호스트 이름이 SSL 인증서에 사용된 CN과 일치함을 나타냅니다.
- 노란색 자물쇠 아이콘은 Admin 인터페이스 호스트 이름이 SSL 인증서의 CN과 일치하지 않음을 나타내는 경고입니다. 현재 호스트 이름을 사용하는 인증서로 교체해야 합니다.

SSL 인증서 교체

SSL 인증서는 일반적으로 다양한 이유에 따라 교체가 필요합니다. 예를 들어 인증서가 만료되거나 호스트 이름이 변경되는 경우가 있습니다. 또한 SSL 인증서는 Threat Grid Appliance와 기타 Cisco 디바이스 및 서비스 간의 통합을 지원하기 위해 추가하거나 교체해야 할 수 있습니다.

ESA/WSA 어플라이언스 및 기타 CSA Cisco 통합 디바이스는 Threat Grid Appliance 호스트 이름과 일치하는 CN이 있는 SSL 인증서를 요구할 수 있습니다. 이 경우, 기본 SSL 인증서를 교체하고 Threat Grid Appliance에서 액세스할 동일한 호스트 이름을 사용하여 새 인증서를 생성해야 합니다.

Threat Grid Appliance를 FireAMP Private Cloud와 통합하여 Disposition Update Service를 사용하려는 경우, FireAMP Private Cloud SSL 인증서를 설치하여 Threat Grid Appliance가 해당 연결을 신뢰할 수 있도록 해야 합니다.

다음과 같은 다양한 방법으로 Threat Grid Appliance의 SSL 인증서를 교체할 수 있습니다.

- 새 SSL 인증서 생성 - CN의 현재 호스트 이름 사용
- SSL 인증서 다운로드
- 새 SSL 인증서 업로드. 이는 커머셜 또는 엔터프라이즈 SSL이 될 수도 있고, OpenSSL을 사용하여 직접 만드는 인증서가 될 수도 있습니다.
- SSL 인증서 직접 생성 – OpenSSL 사용 예

다음 섹션에 설명되어 있습니다.

SSL 인증서 다시 생성

이 작업을 수행하면 v1.3 이전 Threat Grid Appliance에서처럼 OpenSSL 또는 기타 SSL 툴을 수동으로 사용하여 새 SSL 인증서를 생성해야 할 필요가 없습니다. 그러나, SSL 인증서 직접 생성 – OpenSSL 사용 예 섹션에 설명된 대로 이 방법은 계속해서 적용됩니다.

참고: 이 작업을 수행하기 전에 Threat Grid Appliance를 1.4.2 이상 버전으로 업그레이드해야 합니다.

OpAdmin SSL Certificate Configuration(OpAdmin SSL 인증서 컨피그레이션) 페이지에서 **Regenerate(다시 생성)**를 클릭합니다. 새로운 자체 서명 SSL 인증서는 인증서의 CN 필드에 있는 어플라이언스의 현재 호스트 이름을 사용하는 Threat Grid Appliance에서 생성됩니다. CN 검증 자물쇠 아이콘은 녹색입니다. 다시 생성된 인증서(.cert 파일)는 다음 섹션에 설명된 것처럼 다운로드 가능하며, 통합 어플라이언스에 설치할 수 있습니다.

SSL 인증서 다운로드

키가 아닌 Threat Grid SSL 인증서를 다운로드하고 통합 디바이스에 설치하여 TG 어플라이언스에서의 연결을 신뢰하도록 할 수 있습니다. 이 단계에는 .cert 파일만 필요합니다.

1. OpAdmin SSL Certificate Configuration(OpAdmin SSL 인증서 컨피그레이션) 페이지에서 가져오려는 인증서 옆의 **Download(다운로드)**를 클릭합니다**.** SSL 인증서가 다운로드됩니다.
2. 그 다음으로는 다른 SSL 인증서를 설치하는 방식과 마찬가지로, 다운로드한 SSL 인증서를 ESA/WSA 어플라이언스, FireAMP Public Cloud 또는 기타 통합 Cisco 제품에 설치합니다.

SSL 인증서 업로드

커머셜 또는 기업 SSL 인증서가 조직 내에 이미 있는 경우 이를 사용하여 TGA용 새 SSL 인증서를 생성하고, ESA/WSA 또는 기타 통합 디바이스에서 CA 인증서를 사용할 수 있습니다.

SSL 인증서 직접 생성 – OpenSSL 사용 예

또 다른 방법은 온프레미스에 SSL 인증서 인프라가 없고, 다른 방법으로는 인증서를 가져올 수 없을 경우 SSL 인증서를 수동으로 직접 만드는 것입니다. 이는 위에 설명된 방법대로 업로드할 수 있습니다.

이 예에서는 "Acme Company"의 새로운 자체 서명 SSL 인증서를 생성하는 명령에 대해 설명합니다. 이 예에서는 OpenSSL 인증서, 키, 기타 파일을 만들고 관리하는 표준 오픈 소스 SSL 툴인 OpenSSL을 사용합니다.

참고: OpenSSL은 Cisco 제품이 아니며, Cisco에서는 이에 대한 기술 지원을 제공하지 않습니다. OpenSSL 사용에 대한 자세한 내용은 웹을 검색하시기 바랍니다. Cisco에서는 SSL 인증서 생성을 위한 SSL 라이브러리인 *Cisco SSL*을 제공합니다.

```
openssl req -x509 -days 3650 -newkey rsa:4096 -keyout
tgapp.key -nodes -out tgapp.cert -subj "/C=US/ST=New
York/L=Brooklyn/O=Acme Co/CN=tgapp.acmeco.com"
```

- **openssl**: OpenSSL
- **req**: X.509 CSR(Certificate Signing Request) 관리를 사용하려는 경우를 지정합니다. "X.509"는 키 및 인증서 관리를 위해 SSL 및 TLS에서 사용하는 PKI(Public Key Infrastructure) 표준입니다. 새로운 X.509 인증서를 만들어야 하므로, 이 하위 명령을 사용합니다.
- **-X509:**: 이 옵션은 일반적으로 발생하는 인증서 서명 요청을 생성하는 대신 자체 서명 인증서를 만들겠다고 유틸리티에 명령함으로써 이전 하위 명령을 수정합니다.
- **-days 3650**: 이 옵션은 인증서가 유효한 것으로 간주되는 기간을 설정합니다. 여기에서는 10년으로 설정했습니다.
- **-newkey rsa:4096**: 이 옵션은 새 인증서와 새 키를 동시에 생성하려 한다고 지정합니다. 이전 단계에서 인증서에 서명하는 데 필요한 키를 만들지 않았으므로, 인증서와 함께 키를 만들어야 합니다. rsa:4096 부분은 길이가 4096비트인 RSA 키를 만들라는 의미입니다.
- **-keyout**: 이 라인은 사용자가 만들어 생성된 프라이빗 키 파일을 보관할 위치를 OpenSSL에 전달합니다.
- **-nodes**: 이 옵션은 인증서를 암호로 보호하는 옵션을 건너뛰라고 OpenSSL에 전달합니다. 서버가 구동되면 사용자 개입 없이 어플라이언스가 파일을 읽을 수 있어야 합니다. 암호가 있으면 재시작 이후마다 사용자가 이를 입력해야 하므로 이것이 불가능합니다.
- **-out**: 이 옵션은 사용자가 만드는 인증서를 보관할 위치를 OpenSSL에 전달합니다.
- **-subj:** 예:

  C=US: 국가

  ST=New York: 주

  L=Brooklyn: 위치

  O=Acme Co: 소유주 이름

  CN=tgapp.acmeco.com: Threat Grid Appliance FQDN("Fully Qualified Domain Name")을 입력하십시오. 여기에는 Threat Grid Appliance의 호스트 이름(예시의 "tgapp")과 끝에 추가되는 관련 도메인 이름("acmeco.com")이 함께 포함됩니다.

  중요: Threat Grid Appliance Clean 인터페이스의 FQDN과 일치시키기 위해 최소한 공용 이름을 변경해야 합니다.

새 SSL 인증서가 생성되면 SSL 페이지의 **Upload(업로드)** 버튼을 사용하여 인증서를 Threat Grid Appliance에 업로드하고, ESA/WSA 어플라이언스에도 업로드합니다(.cert 파일 전용).

아웃바운드 연결을 위한 SSL 인증서 구성

Threat Grid Appliance 릴리스 2.0.3에는 Disposition Update Service를 위해 FireAMP Private Cloud와의 통합을 지원하는 기능이 포함되어 있습니다.

DNS 구성

기본적으로 DNS는 Dirty 인터페이스를 사용합니다. Clean 인터페이스가 통합에 사용되어 FireAMP Private Cloud 같은 통합 어플라이언스 또는 서비스의 호스트 이름을 Dirty 인터페이스를 통해 해석할 수 없는 경우, Clean 인터페이스를 사용하는 개별 DNS 서버를 OpAdmin에서 구성할 수 있습니다.

OpAdmin에서 **Configuration(컨피그레이션) > Network(네트워크)**를 선택하고 Dirty 및 Clean 네트워크에 대한 DNS 필드를 작성한 다음 **Save(저장)**를 클릭합니다.

CA 인증서 관리

릴리스 2.0.3에 추가된 기능 중 하나는 *아웃바운드* SSL 연결을 지원하는 CA 인증서 관리 트러스트 저장소를 위한 새로운 페이지이므로, TGA는 FireAMP Private Cloud를 신뢰하여 악의적인 것으로 간주되는 분석된 샘플에 대해 알릴 수 있습니다.

OpAdmin에서 **Configuration(컨피그레이션) > CA Certificates(CA 인증서)**를 선택합니다. 다음을 선택합니다.

1. **Import from Host(호스트에서 가져오기).** 서버에서 인증서를 검색합니다. Retrieve certificates from server(서버에서 인증서 검색) 대화 상자가 열립니다.
2. FireAMP Private Cloud의 **Host(호스트)** 및 **Port(포트)**를 입력하고 **Retrieve(검색)**를 클릭합니다. 인증서가 검색됩니다.

또는

Import from Clipboard(클립보드에서 가져오기). 클립보드의 PEM을 붙여넣고 **Add Certificate(인증서 추가)**를 클릭합니다.

3. **Import(가져오기)**를 클릭합니다.

Disposition Update Service 관리

이 작업은 Threat Grid Portal UI 내에서 수행됩니다.

1. **My Account(내 어카운트)** 드롭다운 목록에서 **Manage FireAMP Integration(FireAMP 통합 관리)**을 선택합니다. Disposition Update Service 페이지가 열립니다.
2. FireAMP 컨피그레이션 포털에서 제공된 **FireAMP Private Cloud URL**, **admin user name(admin 사용자 이름)** 및 **password(비밀번호)**를 입력하고 **Config(구성)**를 클릭합니다.

FireAMP Private Cloud 어플라이언스 통합에 대한 자세한 내용은 아래에서 Threat Grid Appliance를 Cisco FireAMP Private Cloud에 연결을 참조하십시오.

ESA/WSA 어플라이언스를 Threat Grid Appliance에 연결

ESA/WSA 및 기타 어플라이언스, 디바이스, 서비스 등의 기타 Cisco 제품은 잠재적인 악성코드 샘플을 분석용으로 제출하기 위해 SSL로 암호화된 연결을 통해 Threat Grid Appliance와 통합될 수 있습니다.

"CSA 통합": ESA/WSA 어플라이언스와 Threat Grid Appliance 간의 통합은 "CSA 통합"이라고도 하는 "CSA API"(Cisco Sandbox API)에 의해 활성화됩니다.

분석을 위해 샘플을 제출하려면 우선 통합 ESA/WSA 어플라이언스를 Threat Grid Appliance에 등록해야 합니다. 통합 ESA/WSA 어플라이언스를 Threat Grid Appliance에 등록하려면, ESA/WSA 관리자가 우선 SSL 인증서 연결을 어플라이언스 및 네트워크 환경에 알맞게 설정해야 합니다.

이 섹션은 Threat Grid Appliance와 통신하기 위해 통합 ESA/WSA 어플라이언스와 기타 Cisco 제품 설정에 필요한 단계를 설명합니다.

ESA/WSA 설명서에 대한 링크

ESA/WSA의 온라인 도움말 또는 사용자 가이드의 *"Enabling and Configuring File Reputation and Analysis Services (파일 평판과 분석 서비스 사용 및 구성)"*에 대한 지침을 참조하십시오. Threat Grid Appliance는 본 가이드에서 자주 "분석 서비스" 또는 "프라이빗 클라우드 파일 분석 서버"라고도 합니다.

- ESA 사용자 가이드 위치:
  http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-user-guide-list.html
- WSA 사용자 가이드 위치:
  http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html

통합 프로세스 개요

시작하기 전에: 이 섹션은 Threat Grid Appliance와 ESA/WSA 어플라이언스 또는 기타 CSA 통합(인바운드) 간에 연결을 설정하는 단계에 대한 요약을 제공합니다.

각 단계에 대한 자세한 설명을 포함하는 표가 이 섹션 다음에 나옵니다.

Threat Grid Appliance SSL 인증서 SAN 또는 CN은 현재 호스트 이름 및 ESA/WSA 예상과 일치해야 합니다.

Threat Grid Appliance SSL 인증서 SAN("Subject Alternative Name" – 정의된 경우) 또는 CN("Common Name")은 통합 ESA/WSA 어플라이언스와의 성공적인 연결을 위해 호스트 이름 및 ESA/WSA 예상과 일치해야 하며 이것은 통합 ESA/WSA 어플라이언스가 Threat Grid Appliance를 식별할 때 사용하는 호스트 이름과 동일해야 합니다.

요건에 따라, Threat Grid Appliance에서 자체 서명 SSL 인증서를 다시 생성하여 해당 인증서가 SAN/CN 필드의 현재 호스트 이름을 사용하도록 해야 할 수 있습니다. 그런 다음 이 인증서를 업무 환경에 다운로드하고, 통합 ESA/WSA 어플라이언스에 업로드한 후 설치합니다.

또는 엔터프라이즈나 커머셜 SSL 인증서(또는 수동으로 생성된 인증서)를 업로드하여 현재 TGA SSL 인증서를 교체해야 할 수 있습니다.

자세한 지침은 위의 인바운드 연결을 위한 SSL 인증서 구성 섹션을 참조하십시오.

연결 확인:

SSL 인증서 설정이 완료되면, 그 다음 단계는 ESA/WSA 어플라이언스가 Threat Grid Appliance와 서로 통신할 수 있는지 확인하는 것입니다.

Cisco ESA/WSA 어플라이언스는 네트워크를 통해 Threat Grid Appliance의 **Clean** 인터페이스에 연결할 수 있어야 합니다.

TGA 및 ESA/WSA 어플라이언스가 서로 통신할 수 있는지 확인하려면 제품의 해당 가이드에서 지침을 참조하십시오. 위 링크를 참조하십시오.

ESA/WSA 파일 분석 컨피그레이션 완료:

파일 분석 보안 서비스를 활성화하고 고급 설정을 구성합니다.

Cisco ESA/WSA/기타 디바이스를 Threat Grid Appliance에 등록:

해당 제품의 설명서에 따라 구성된 ESA/WSA 어플라이언스는 Threat Grid Appliance에 자동으로 등록됩니다.

연결 디바이스를 등록하면 디바이스 ID를 로그인 ID로 사용하는 새로운 Threat Grid 사용자가 자동으로 생성되고, 동일한 ID에 기반한 이름을 사용하는 새로운 조직이 생성됩니다. 관리자는 다음 섹션에 설명된 대로, 새 디바이스 사용자 어카운트를 활성화해야 합니다.

Threat Grid Appliance에서 새 ESA/WSA 어카운트 활성화:

ESA/WSA 어플라이언스 또는 기타 통합 디바이스가 Threat Grid Appliance와 연결 및 등록될 경우, 새 Threat Grid 사용자 어카운트가 자동으로 생성됩니다. 이 사용자 어카운트의 초기 상태는 "비활성화"되어 있습니다. 다른 Threat Grid 사용자와 마찬가지로, 디바이스 사용자 어카운트는 분석을 위해 악성코드 샘플을 제출하는 데 사용하려면 우선 Threat Grid Appliance 관리자가 수동으로 활성화해야 합니다.

ESA/WSA 통합 프로세스 단계

이는 Threat Grid Appliance의 관점에서 *수신*되는 연결입니다.

이러한 통합은 CSA API를 사용합니다.

이 측면에서 수행해야 하는 작업에 대한 자세한 내용은 ESA 및 WSA 사용자 가이드를 참조하십시오.

단계	TGA(Threat Grid Appliance)	ESA/WSA/기타 CSA API 통합
1	TGA(Threat Grid Appliance)를 일반적으로 설정 및 구성합니다(즉, 통합은 아직 수행하지 않음). 업데이트를 확인하고 있는 경우 설치합니다.	
2		ESA/WSA 어플라이언스를 일반적으로 설정 및 구성합니다(즉, 통합은 아직 수행하지 않음).

단계	TGA(Threat Grid Appliance)	ESA/WSA/기타 CSA API 통합
3	**TGA SSL 인증서 SAN 또는 CN은 현재 호스트 이름 및 ESA/WSA 예상과 일치해야 합니다.** 자체 서명 SSL 인증서를 구축하려는 경우: 필요 시 기본값을 대체할 새 SSL 인증서("Threat Grid 애플리케이션" – Clean 인터페이스에 있음)를 생성하고 ESA/WSA 어플라이언스 디바이스에 설치하기 위해 다운로드합니다. TGA SSL 인증서는 위의 SSL 인증서 및 Threat Grid Appliance 섹션에 설명되어 있습니다. AMP Threat Grid Appliance의 호스트 이름이 SAN 또는 CN으로 지정된 인증서를 생성해야 합니다. AMP Threat Grid Appliance에서 제공하는 기본 인증서는 작동하지 않습니다. IP 주소가 아니라 호스트 이름을 사용합니다.	
4		**연결 확인** Cisco ESA/WSA 어플라이언스는 네트워크를 통해 Threat Grid Appliance의 **Clean** 인터페이스에 연결할 수 있어야 합니다.

단계	TGA(Threat Grid Appliance)	ESA/WSA/기타 CSA API 통합
5		**TG 어플라이언스 통합을 위한 ESA/WSA 어플라이언스 구성:** 전체 지침은 ESA/WSA 가이드를 참조하십시오. 다음 단계는 현재 가장 일반적인 유형의 통합이므로 ESA에만 해당합니다. 1. **Security Services(보안 서비스)** > **File Reputation and Analysis(파일 평판 및 분석)**를 선택합니다. 2. **Enable(활성화)**을 클릭합니다. 3. **Edit Global Settings(전역 설정 수정)**를 클릭합니다. 기본값으로 파일 분석은 활성화되어 있습니다. **Enable File Analysis(파일 분석 활성화)**을 선택 취소하지 않으면 다음 커밋 후에 파일 분석 기능 키가 활성화됩니다. 4. **File Analysis(파일 분석)** 섹션에서 분석을 위해 클라우드로 보낼 파일 유형을 선택합니다. 5. ESA 또는 WSA 가이드에 따라 필요한 대로 **Advanced Settings for File Analysis(파일 분석을 위한 고급 설정)**를 구성합니다. **파일 분석 서버 URL:** **Private Cloud(프라이빗 클라우드)**를 선택합니다. **서버:** 온프레미스 Cisco AMP Threat Grid Appliance의 **URL.** 이 값과 인증서에 IP 주소가 아니라 호스트 이름을 사용합니다. **SSL 인증서:** 온프레미스 Cisco AMP Threat Grid Appliance에서 생성한 자체 서명 인증서를 업로드합니다.

단계	TGA(Threat Grid Appliance)	ESA/WSA/기타 CSA API 통합
		가장 최근에 업로드된 자체 서명 인증서가 사용됩니다. 가장 최근 인증서 이전에 업로드된 인증서에 액세스할 수 없습니다. 필요한 경우 원하는 인증서를 다시 업로드합니다. 6. 변경 사항을 제출하고 커밋합니다. 참고로 **File Analysis Client ID(파일 분석 클라이언트 ID)**가 페이지의 하단에 표시됩니다. 이 ID는 7단계에서 활성화해야 하는 "사용자"를 식별합니다. **Threat Grid Appliance 자동 등록** 파일 분석용 컨피그레이션을 제출할 때 Email Security Appliance 또는 Web Security Appliance가 Threat Grid Appliance와 함께 자동으로 등록됩니다. 그러나 아래의 7단계에 설명된 대로 등록을 활성화해야 합니다.
6	**Threat Grid Appliance에서 새 디바이스 사용자 어카운트 활성화** 1. Threat Grid Portal UI에 Admin으로 로그인합니다. 2. 내비게이션 바의 **Welcome(시작)** 메뉴에서 **Manage Users(사용자 관리)**를 선택합니다. **Threat Grid Users(Threat Grid 사용자)** 페이지가 열립니다. 3. 디바이스 사용자 어카운트에 대한 **User Details(사용자 세부사항)** 페이지를 엽니다(Search(검색)를 사용하여 찾아야 할 수 있음). 사용자 상태가 현재 "비활성화"되어 있습니다. 4. **Re-Activate User(사용자 다시 활성화)**를 클릭합니다. 확인을 요청하는 대화 상자가 열립니다. 5. 대화 상자에서 **Re-Activate(다시 활성화)**를 클릭하여 확인합니다.	

이제 ESA/WSA 또는 기타 통합 어플라이언스 또는 디바이스가 Threat Grid Appliance와 연결을 시작할 수 있습니다.

Threat Grid Appliance를 Cisco FireAMP Private Cloud에 연결

Threat Grid Appliance Disposition Update Service 및 FireAMP Private Cloud 통합 설정 작업은 다음 순서에 따라 디바이스에서 수행해야 하며, 특히 새 어플라이언스를 설정하는 경우가 이에 해당합니다. 이미 설정 및 구성된 어플라이언스를 통합할 경우, 순서는 중요하지 않습니다.

이는 Threat Grid Appliance의 관점에서 나가는 연결입니다. 이러한 통합은 CSA API를 사용하지 않습니다.

이 측면에서 수행해야 하는 작업에 대한 자세한 내용은 FireAMP Private Cloud 설명서를 참조하십시오.

단계	TGA(Threat Grid Appliance)	FireAMP Private Cloud
1	TGA(Threat Grid Appliance)를 일반적으로 설정 및 구성합니다(즉, 통합은 아직 수행하지 않음). 업데이트를 확인하고 있는 경우 설치합니다.	
2		FireAMP Private Cloud를 일반적으로 설정 및 구성합니다(즉, 통합은 아직 수행하지 않음).
3		**TGA 통합을 위해 FireAMP Private Cloud 구성:** **Integrations(통합) > Threat Grid**를 선택하고 **Connection to Threat Grid(Threat Grid에 연결)** 섹션으로 이동합니다. Threat Grid Appliance와의 연결을 완료하려면 이를 신뢰해야 합니다. 해당하는 DNS 호스트 이름, SSL 인증서, API 키가 필요합니다. 이 정보를 찾으려면 TGA 열의 3.1단계로 이동합니다.

단계	TGA(Threat Grid Appliance)	FireAMP Private Cloud
3.1	**SSL 인증서: –** Threat Grid Appliance OpAdmin 인터페이스에서 **Configuration(컨피그레이션) > SSL**을 선택합니다. 필요 시 기본값을 대체할 새 SSL 인증서("Threat Grid 애플리케이션" – Clean 인터페이스에 있음)를 다시 생성하고 FireAMP Private Cloud 디바이스에 설치하기 위해 다운로드합니다. TGA SSL 인증서는 SSL 인증서 및 Threat Grid Appliance에 설명되어 있습니다. **호스트 이름** **Configuration(컨피그레이션) > Hostname(호스트 이름)**을 선택합니다. **API 키**: API 키는 Threat Grid Face Portal UI에서 통합에 사용할 어카운트의 **User Details(사용자 세부사항)** 페이지에서 찾을 수 있습니다. 1. **Threat Grid Portal UI**로 이동합니다. 2. 오른쪽 상단의 Welcome(시작) 메뉴(내비게이션 바의 오른쪽 상단 모서리에 위치)에서 **Manage Users(사용자 관리)**를 선택합니다. 3. 통합에 사용할 사용자 어카운트의 **User Details(사용자 세부사항)** 페이지로 이동하고(필요한 경우 Search(검색) 사용), **API Key(API 키)**를 복사합니다. 이 사용자가 꼭 "admin" 사용자일 필요는 없지만, Threat Grid Appliance에서 이 작업을 위해서만 생성한 다른 사용자가 해당될 수는 있습니다.	

단계	TGA(Threat Grid Appliance)	FireAMP Private Cloud
3.2		다음과 같이 **Connection to Threat Grid(Threat Grid에 연결)** 필드를 작성합니다. 1. TGA Hostname(TGA 호스트 이름)을 입력합니다. 2. 통합에 사용할 어카운트의 Threat Grid API Key(Threat Grid API 키)를 입력합니다. 3. TGA SSL Certificate(TGA SSL 인증서) 파일을 선택합니다. 4. Save Configuration(컨피그레이션 저장)을 클릭합니다. 5. Test Connection(테스트 연결)을 클릭합니다. 6. 연결 테스트를 통과하면, FireAMP Private Cloud에서 다시 컨피그레이션을 실행하여 변경 사항을 적용해야 합니다. 이렇게 하면 AMP가 Threat Grid Appliance와 통신할 수 있으며, 이 단계에서 샘플을 TG에 제출할 수 있습니다. 그러나 처리 결과를 TGA에 전달하려면 나머지 단계를 완료하여 Disposition Update Service를 설정해야 합니다. 자세한 내용은, FireAMP Private Cloud의 사용자 설명서를 참조하십시오.
4	**Disposition Update Service 설정** 다음 단계에서는 Disposition Update Service를 설정하는 방법을 설명합니다.	

단계	TGA(Threat Grid Appliance)	FireAMP Private Cloud
4.1	**DNS 구성(필요한 경우):** Clean 인터페이스는 FireAMP 통합에 사용됩니다. 그러나 기본적으로 DNS는 Dirty 인터페이스를 사용합니다. FireAMP Private Cloud 호스트 이름을 Dirty 인터페이스를 통해 해석할 수 없는 경우, Clean 인터페이스를 사용하는 개별 DNS 서버를 OpAdmin에서 구성할 수 있습니다. OpAdmin에서 **Configuration(컨피그레이션) > Network(네트워크)**를 선택하고 **Dirty** 및 **Clean** 네트워크에 대한 DNS 필드를 작성한 다음 **Save(저장)**를 클릭합니다.	
4.2	**CA 인증서 관리:** 다음 단계는 FireAMP Private Cloud SSL 인증서를 Threat Grid Appliance에 다운로드하거나 복사/붙여넣기하여 통합 디바이스를 신뢰할 수 있도록 하는 것입니다. 1. OpAdmin에서 **Configuration (컨피그레이션) > CA Certificates (CA 인증서)**를 선택합니다. FireAMP Private Cloud Host에서 가져올 SSL 인증서를 선택하거나, 클립보드에서 가져올 수 있습니다. 2. 가져올 인증서를 선택하고 **Import from Host(호스트에서 가져오기)**를 클릭합니다. **Retrieve certificates from server(서버에서 인증서 검색)** 대화 상자가 열립니다. FireAMP Appliance Disposition Service의 **Host(호스트)** 및 **Port(포트)**를 입력하고 **Retrieve(검색)**를 클릭합니다. 3. 인증서가 검색됩니다. 4. **Import(가져오기)**를 클릭합니다. 또는 **Import from Clipboard(클립보드에서 가져오기)**를 클릭합니다. 클립보드의 PEM을 붙여넣고 **Add Certificate(인증서 추가)**를 클릭합니다.	

단계	TGA(Threat Grid Appliance)	FireAMP Private Cloud
4.3	**FireAMP 통합 관리:** Threat Grid Face Portal UI의 오른쪽 상단 메뉴에서 **Manage FireAMP Integration(FireAMP 통합 관리)**을 선택합니다. Disposition Update Service 창이 열립니다. AMP Disposition Update Service URL을 입력합니다(FireAMP 어플라이언스에서 **Integrations(통합) > Threat Grid > FireAMP Private Cloud Details(FireAMP Private Cloud 세부사항)**를 선택하여 이 URL을 찾을 수 있음). **admin user name(admin 사용자 이름)** 및 **password(비밀번호)**를 입력하고 **Config(구성)**를 클릭합니다.	

Threat Grid 조직 및 사용자 관리

Threat Grid는 기본 조직 및 관리자를 포함하여 어플라이언스에 설치됩니다. 어플라이언스 설정 및 네트워크 컨피그레이션을 완료한 경우, 사용자가 로그인하여 분석용 악성코드 샘플을 제출할 수 있도록 추가 조직 및 사용자 어카운트를 생성할 수 있습니다.

조직, 사용자 및 관리자를 추가하려면 조직에 따라 다양한 사용자와 팀을 계획하고 조정해야 할 수 있습니다.

새 조직 생성

사용자는 항상 조직과 관련이 있으므로 사용자를 추가하려면 먼저 사용자를 추가할 대상 조직을 생성해야 합니다.

중요: 일단 조직이 생성되면 이 인터페이스에서 조직을 삭제할 수 없으므로 이 작업을 신중하게 계획하십시오.

1. Threat Grid Portal에 Admin으로 로그인합니다.
2. 왼쪽 상단 모서리에 있는 **Welcome(시작)** 드롭다운 링크를 클릭하고 **Manage Orgs(조직 관리)**를 선택합니다. Organizations(조직) 페이지가 열리고 어플라이언스에 있는 모든 조직이 나열됩니다.
3. 화면의 오른쪽 상단 모서리에 있는 **Add Organization(조직 추가)** 버튼을 클릭합니다. Properties(속성) 대화 상자가 열립니다.
4. 모두 필수 항목입니다.

   Name(이름): 조직의 이름을 추가합니다(현재는 이름에 크기 제한이 없음).

   Industry(업계): Industry(업계) 드롭다운에서 비즈니스 유형을 선택합니다. 목록에서 적용 가능한 업계가 없는 경우, 이를 Unknown(알 수 없음)으로 두고 Threat Grid 지원(support@threatgrid.com)에 문의하여 옵션 추가를 요청하십시오.

   다른 옵션을 입력합니다.

   속도 제한:

   API 속도 제한은 라이선스 계약의 조건이 적용되는 어플라이언스에 대한 전역 제한입니다. 이 제한은 API 제출에만 영향을 주며 수동 샘플 제출에는 영향을 주지 않습니다. 라이선스 속도 제한은 조직에 적용됩니다.

   기본 *사용자* 제출 속도 제한을 설정합니다. 또한 *Threat Grid 사용의* Threat Grid Portal 온라인 도움말(내비게이션 바에서 **Help(도움말) > Using Threat Grid Online Help(Threat Grid 사용 온라인 도움말)**에서)의 설명대로 샘플 제출 속도를 설정할 수 있습니다.

   속도 제한은 역일이 아닌 롤링 타임의 24시간 창을 기준으로 합니다. 제출 제한을 모두 사용한 경우, 다음 API 제출에서 재시도하기 전 대기 시간에 대한 메시지와 함께 429 오류가 반환됩니다.

   Priority(우선 순위) 필드는 없어지므로 지금은 "50"을 입력합니다.
5. **Create(생성)**를 클릭합니다. 새 조직이 생성되고 이제 조직 목록에 표시됩니다.

사용자 관리

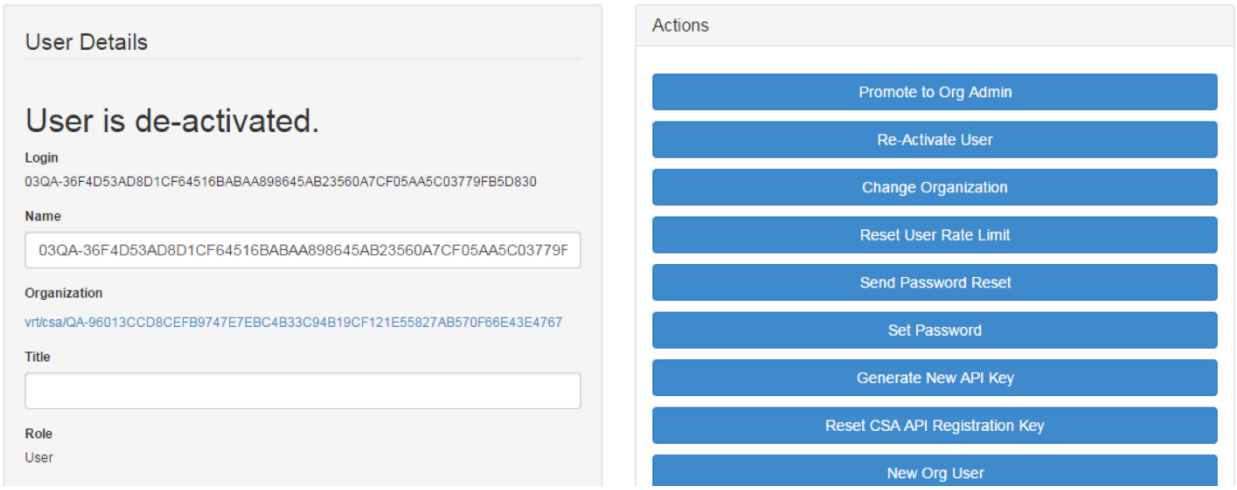
사용자 어카운트 관리(Cisco ESA/WSA 어플라이언스 및 기타 디바이스 통합을 위한 어카운트 포함)에 대한 지침 및 설명서는 Threat Grid Portal UI 온라인 도움말을 참조하십시오. 내비게이션 바에서 **Help(도움말) > Using Threat Grid Online Help(Threat Grid 온라인 도움말 사용) > Managing Users(사용자 관리)**를 선택합니다.

Threat Grid Appliance에서 새 디바이스 사용자 어카운트 활성화

ESA/WSA 어플라이언스 또는 기타 CSA("Cisco Sandbox API") 통합이 Threat Grid Appliance와 연결 및 등록될 경우, 새 Threat Grid 사용자 어카운트가 자동으로 생성됩니다. 이 사용자 어카운트의 초기 상태는 "비활성화"되어 있습니다. 다른 Threat Grid 사용자와 마찬가지로, 디바이스 사용자 어카운트는 분석을 위해 악성코드 샘플을 제출하는 데 사용하려면 우선 Threat Grid Appliance 관리자가 수동으로 활성화해야 합니다.

1. Threat Grid Portal UI에 Admin으로 로그인합니다.
2. 내비게이션 바의 **Welcome(시작)** 메뉴에서 **Manage Users(사용자 관리)**를 선택합니다. **Threat Grid Users(Threat Grid 사용자)** 페이지가 열립니다.
3. 디바이스 사용자 어카운트에 대한 **User Details(사용자 세부사항)** 페이지를 엽니다(Search(검색)를 사용하여 찾아야 할 수 있음). 사용자 상태가 현재 "비활성화"되어 있습니다.

그림 14 - 사용자 세부사항 페이지 > 사용자 다시 활성화



4. **Re-Activate User(사용자 다시 활성화)**를 클릭합니다. 확인을 요청하는 대화 상자가 열립니다.
5. 대화 상자에서 **Re-Activate(다시 활성화)**를 클릭하여 확인합니다.

이제 ESA/WSA 또는 기타 통합 어플라이언스 또는 디바이스가 Threat Grid Appliance와 통신할 수 있습니다.

프라이버시 및 샘플 가시성

분석을 위해 Threat Grid에 샘플을 제출할 때 중요한 고려 사항은 콘텐츠의 프라이버시입니다. 프라이버시는 Threat Grid 액세스 특히 검색 API를 사용하는 사용자가 민감한 자료를 찾는 일이 비교적 쉽기 때문에 분석을 위해 민감한 문서 또는 아카이브 유형을 제출한 경우 특히 중요한 고려 사항입니다.

프라이버시는 온프레미스 Threat Grid Appliance로 샘플을 제출할 때는 Threat Grid Cloud로 제출할 때보다 상대적으로 문제가 심각하지 않지만, TGA 관리자라면 반드시 프라이버시 및 샘플 가시성의 기본사항을 이해하고 있어야 합니다.

Threat Grid로 샘플을 제출하기 위한 프라이버시 및 샘플 가시성 모델은 비교적 간단합니다. 샘플이 프라이빗으로 지정되어 있지 않은 한, 제출자의 조직 외부에 있는 사용자가 볼 수 있습니다. 일반적으로 *프라이빗*으로 지정된 샘플은 샘플을 제출한 사용자와 같은 조직에 있는 Threat Grid 사용자만 볼 수 있습니다.

Threat Grid Appliance의 프라이버시 및 가시성

프라이버시 및 샘플 가시성 모델은 "CSA Integrations"에서 제출되는 샘플에 맞게 Threat Grid Appliance에서 수정됩니다. CSA Integrations는 CSA API를 통해 Threat Grid Appliance와 통합(등록)된 ESA/WSA 어플라이언스 및 기타 디바이스 또는 서비스와 같은 Cisco 제품입니다.

Threat Grid Appliance에서 수행되는 모든 샘플 제출의 기본값은 퍼블릭이며, 소속 조직과 관계없이 CSA Integrations를 비롯한 다른 모든 어플라이언스 사용자가 볼 수 있습니다.

모든 어플라이언스 사용자는 다른 모든 사용자가 제출한 샘플의 세부사항을 볼 수 있습니다.

비CSA Threat Grid 사용자는 Threat Grid Appliance로 프라이빗 샘플을 제출할 수 있으며, 이 경우 해당 샘플은 CSA Integrations를 비롯하여 제출자의 조직에 속한 다른 Threat Grid Appliance 사용자에게만 보입니다.

프라이버시 및 샘플 가시성 모델은 다음과 같은 용어를 사용하며 아래 표에 설명되어 있습니다.

CSA Integrations CSA Integrations는 CSA API를 통해 Threat Grid Appliance에 등록된 ESA/WSA 어플라이언스 및 기타 Cisco 디바이스 또는 서비스입니다. CSA Integrations에 의해 Threat Grid Appliance로 제출된 샘플의 기본값은 퍼블릭입니다.

Threat Grid 사용자 - 퍼블릭 정상적인 Threat Grid 사용자(즉, 비CSA Integrations)에 의해 Threat Grid Appliance로 제출되는 퍼블릭 샘플입니다.

예를 들어, Threat Grid Portal UI를 통해 또는 Threat Grid 네이티브 API를 사용하여 샘플을 제출하는 어플라이언스 관리자 또는 악성코드 분석가가 여기에 해당합니다.

Threat Grid 사용자 - 프라이빗 정상적인 Threat Grid 사용자가 Threat Grid Appliance에 제출하는 프라이빗 샘플입니다.

이 경우 프라이빗 샘플은 제출자의 조직 외부에 있는 다른 모든 어플라이언스 사용자에게는 보이지 않습니다. 샘플은 제출자와 같은 조직에 속한 CSA Integrations에만 보입니다.

그림 15 - Threat Grid Appliance의 프라이버시 및 가시성

	다음에서 액세스할 경우의 샘플 가시성:			
샘플 전송자:	같은 조직의 Threat Grid 사용자	다른 조직의 Threat Grid 사용자	같은 조직의 CSA Integration	다른 조직의 CSA Integration
Threat Grid 사용자 - 퍼블릭	풀패키지 구매	풀패키지 구매	풀패키지 구매	풀패키지 구매
Threat Grid 사용자 - 프라이빗	풀패키지 구매	없음	풀패키지 구매	없음
CSA Integrations(ESA/WSA 어플라이언스 등) Threat Grid Appliance에 제출되는 모든 CSA 기본값은 퍼블릭임	풀패키지 구매	풀패키지 구매	풀패키지 구매	풀패키지 구매

FireAMP Private Cloud와 Threat Grid Appliance 통합에도 동일한 기본 프라이버시 규칙이 적용됩니다.

어플라이언스 삭제

새 부팅 메뉴 옵션은 Threat Grid Appliance에서 디스크를 삭제할 수 있는 V1.4.4에서 사용 가능합니다.

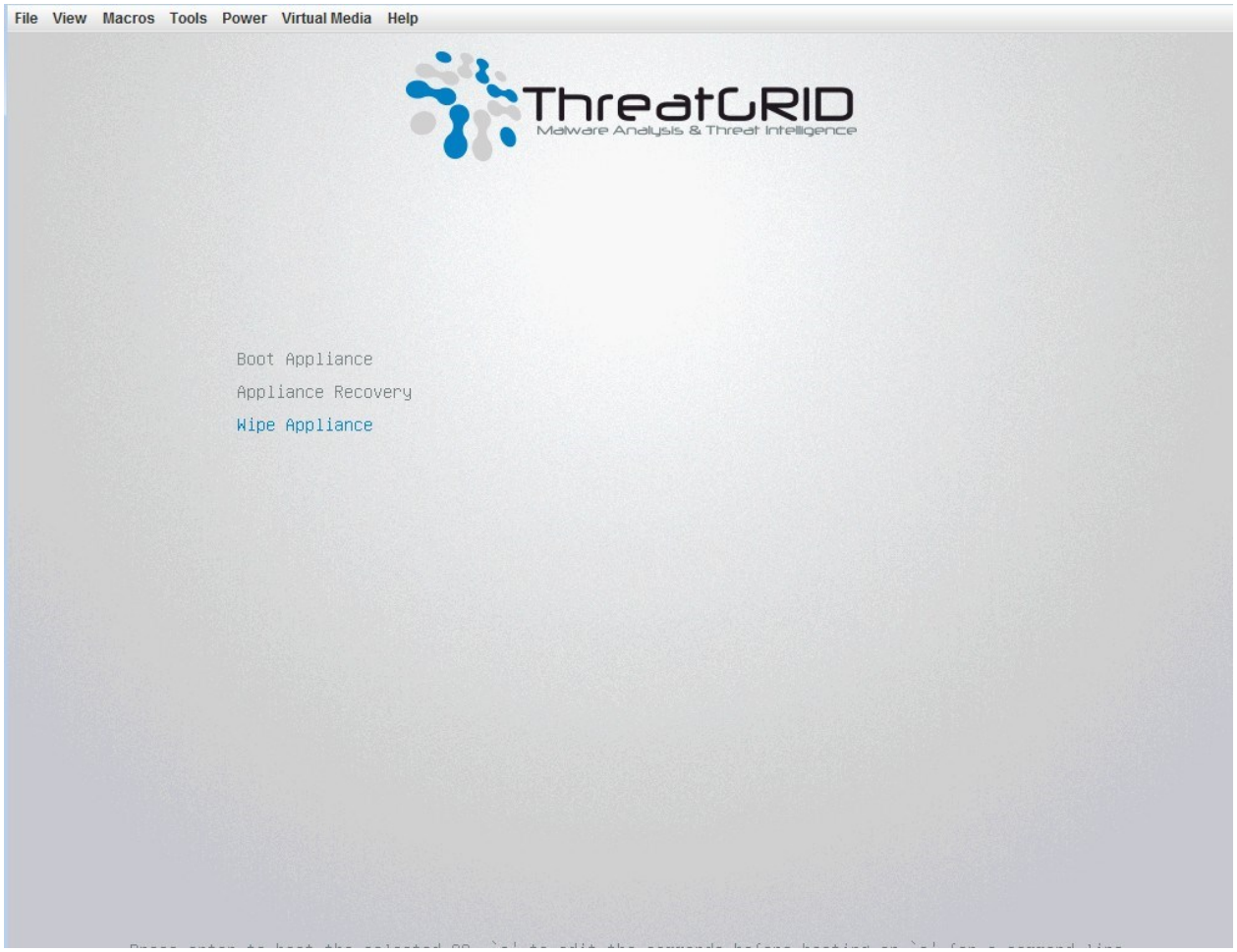
서비스를 해제하거나 Cisco Demo Loan 프로그램으로 반환하기 전에 어플라이언스 삭제 옵션을 사용하여 어플라이언스에서 모든 데이터를 제거합니다. 이 프로세스에서는 여러 가지 변수를 사용할 수 있는데 일부 옵션은 고급 기술을 사용하여 데이터 검색 시 안전하게 시도할 수 있도록 추가 단계를 수행합니다. 참고로, 이러한 기술이 최신 하드 드라이브 인코딩에서는 효과가 없는 것으로 생각되므로 가장 빠른 단일 단계의 삭제 옵션으로도 안전하고 충분한 것으로 간주됩니다.

중요: 이 작업을 수행한 다음에는 어플라이언스가 이미지로 다시 설치를 위해 Cisco에 반환되지 않은 경우 더 이상 작동하지 않을 수 있습니다.

1. 어플라이언스를 재부팅합니다.

   부팅 중에 **4초 창이 표시되며 이 창에서 Wipe Appliance(어플라이언스 삭제)**를 선택할 수 있습니다.

그림 16 - 어플라이언스 삭제



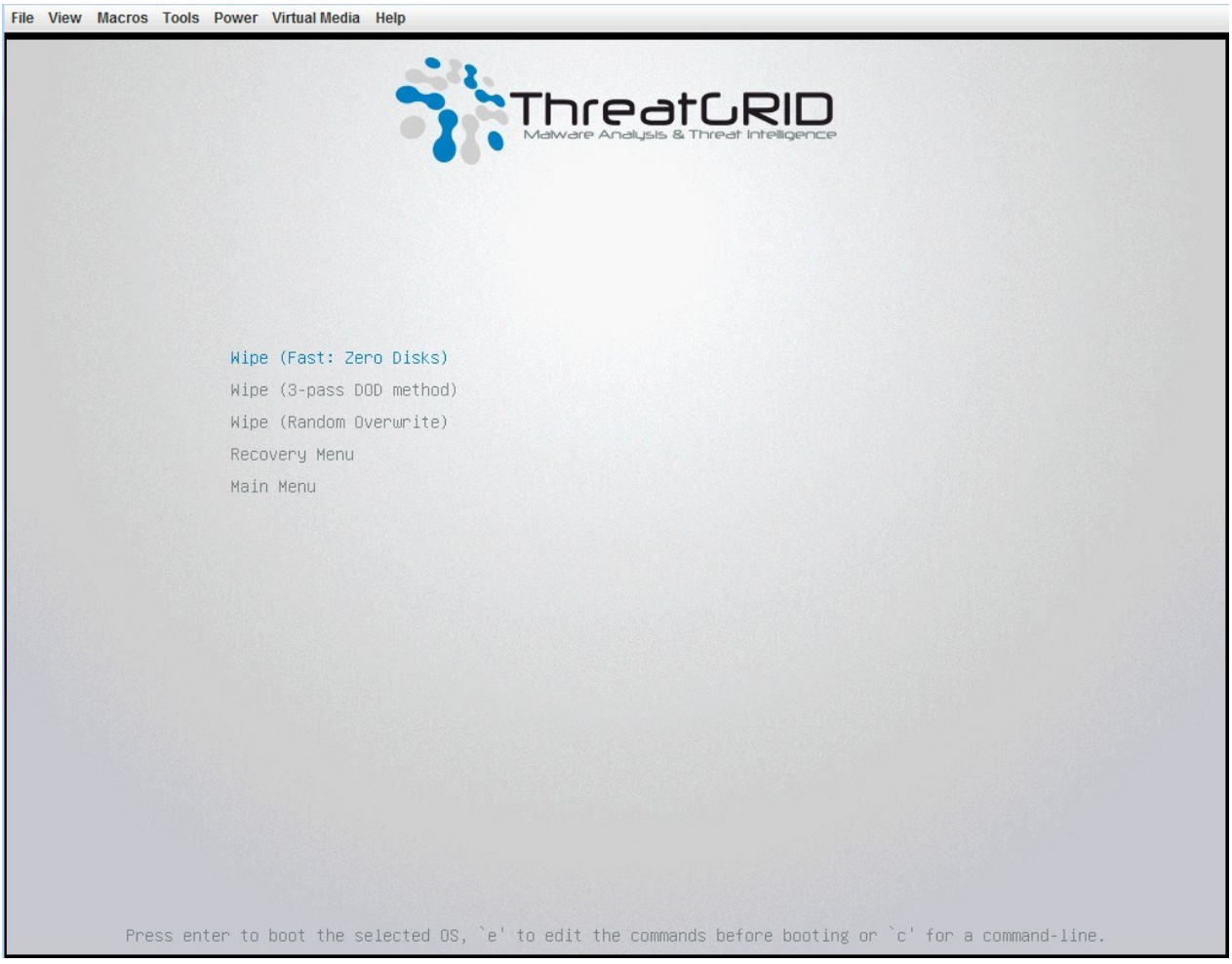
2. 이 옵션에서는 다음의 사용자 이름 및 비밀번호가 필요합니다.

   사용자 이름: "wipe(삭제)"

   비밀번호: "I ACCEPT ALL RESPONSIBILITY FOR THIS ACTION(이 작업에 대한 모든 책임을 수락합니다.)"

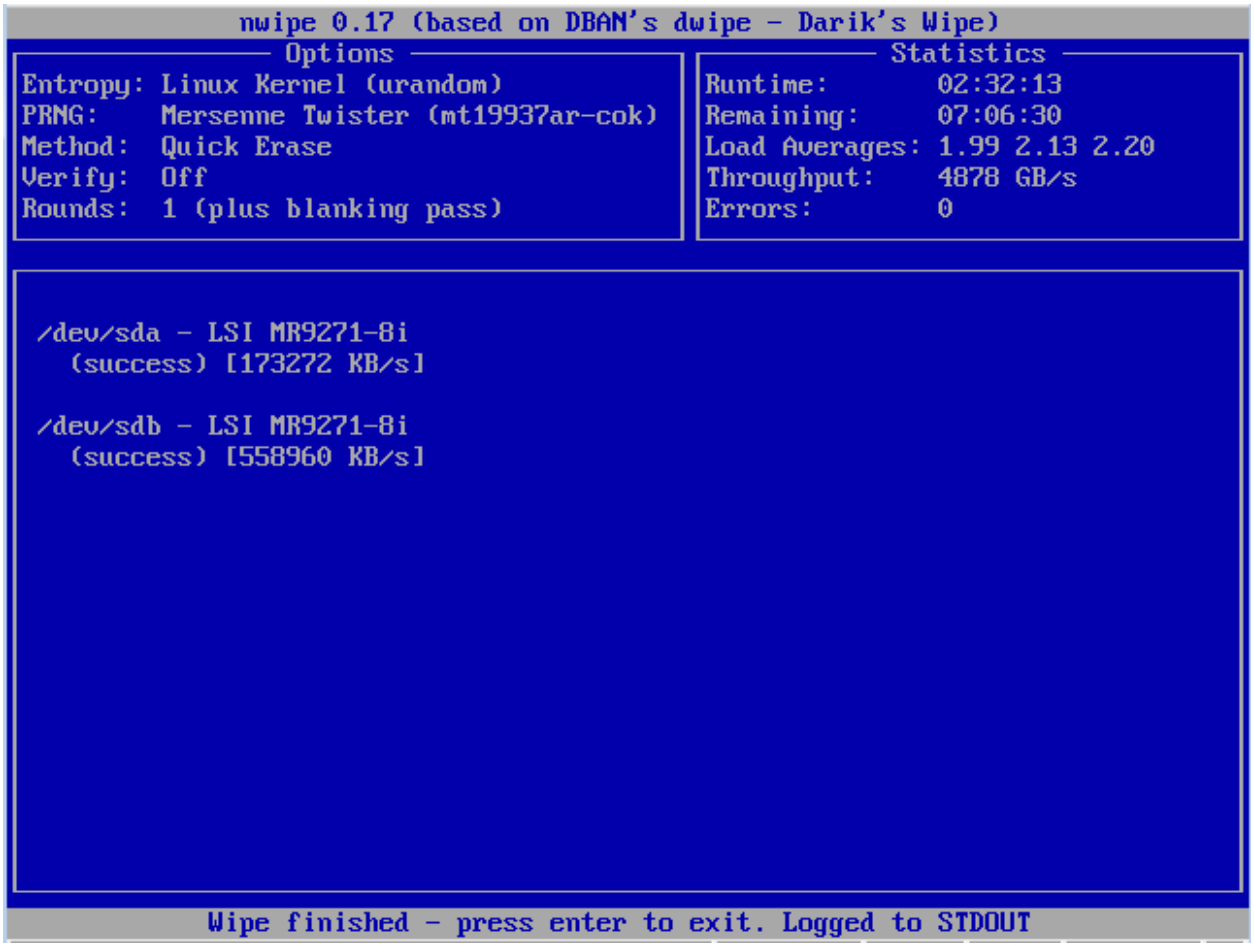
3. 다음으로, Wipe(삭제) 옵션을 선택합니다. 각 옵션의 대략적인 런타임 동안 삭제 옵션을 확인합니다.

그림 17 - 삭제 옵션



4. 다음과 같이 **Wipe Finished(삭제 완료됨)** 화면이 삭제 작업 완료 시 표시됩니다.

그림 18 - 삭제 완료됨



5. 종료하려면 **Enter** 키를 누릅니다.

삭제 옵션

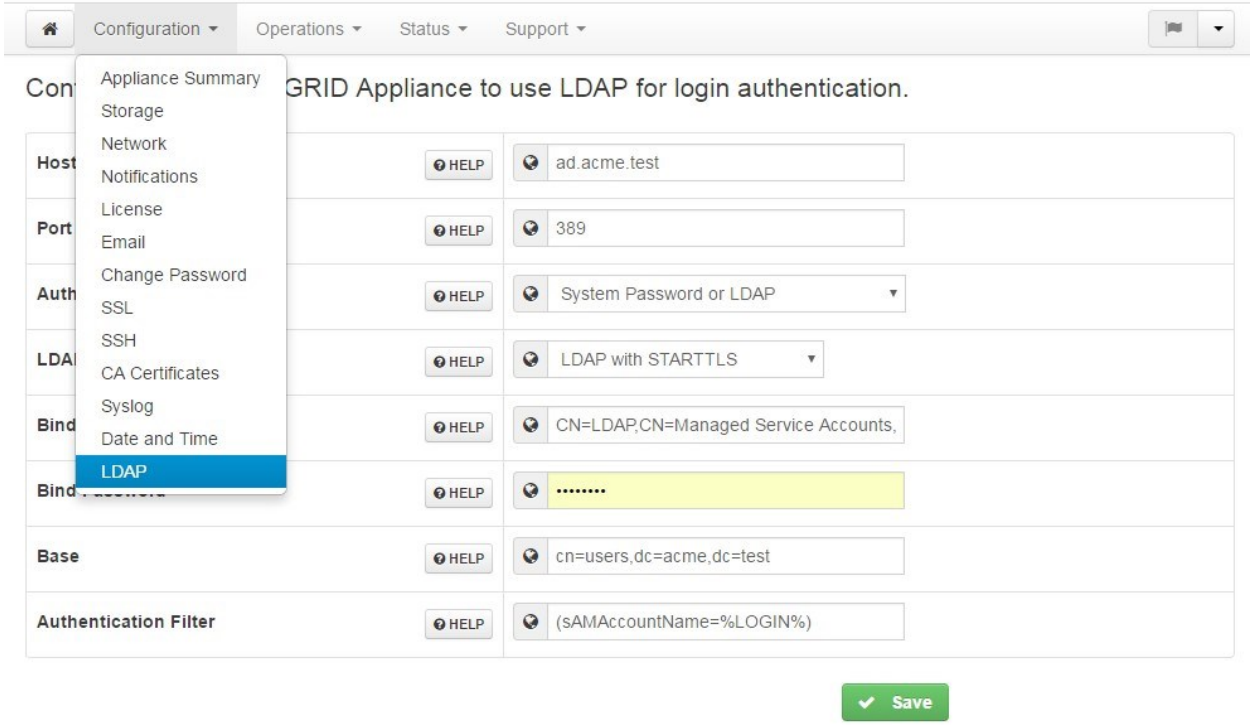
삭제 옵션	대략적인 런타임
삭제(신속: 제로 디스크)	2시간 30분
삭제(3단계 DOD 방법)	16시간
삭제(임의 덮어쓰기)	12시간

부록 - OpAdmin 메뉴

Cisco는 OpAdmin에서 여러 가지 작업을 수행하는 데 사용할 수 있는 다양한 메뉴 옵션을 자세히 보여주기 위해 다음과 같은 스크린 샷을 제공합니다.

컨피그레이션 메뉴

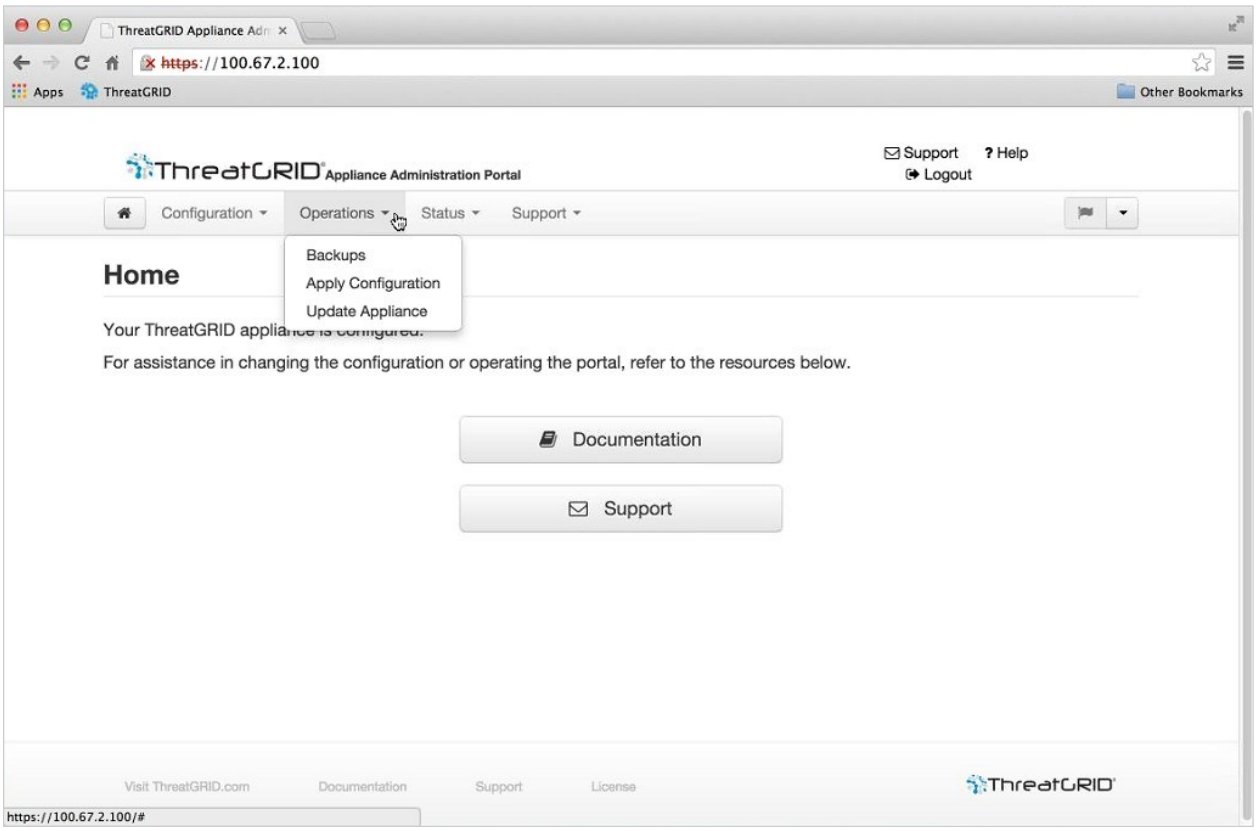
그림 19 - OpAdmin 컨피그레이션 메뉴



참고: 나중에 OpAdmin 컨피그레이션 설정을 변경해야 하는 경우, 편집 모드를 시작하려면 컨피그레이션 메뉴에서 액세스해야 합니다.

운영 메뉴

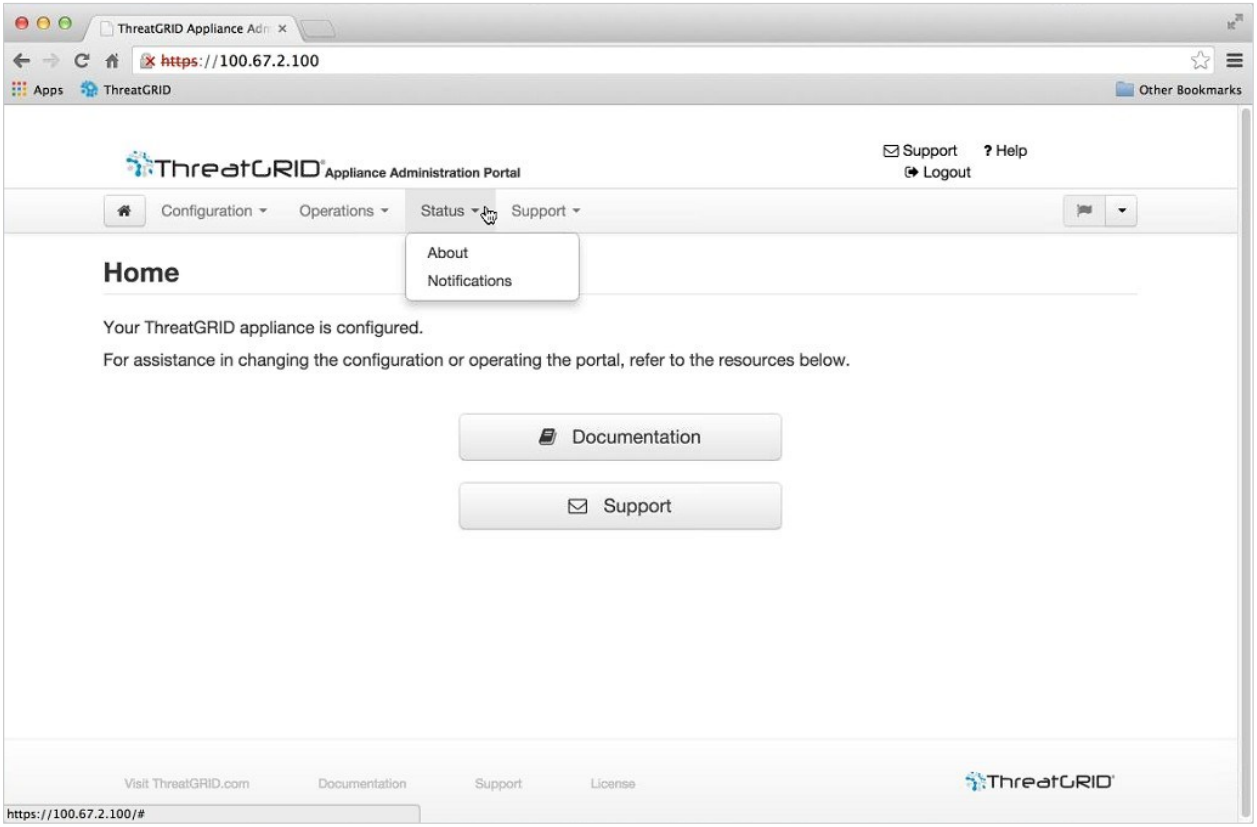
그림 20 - OpAdmin 운영 메뉴



참고: 릴리스 노트를 확인하려면 **Update Appliance(어플라이언스 업데이트)**를 선택합니다.

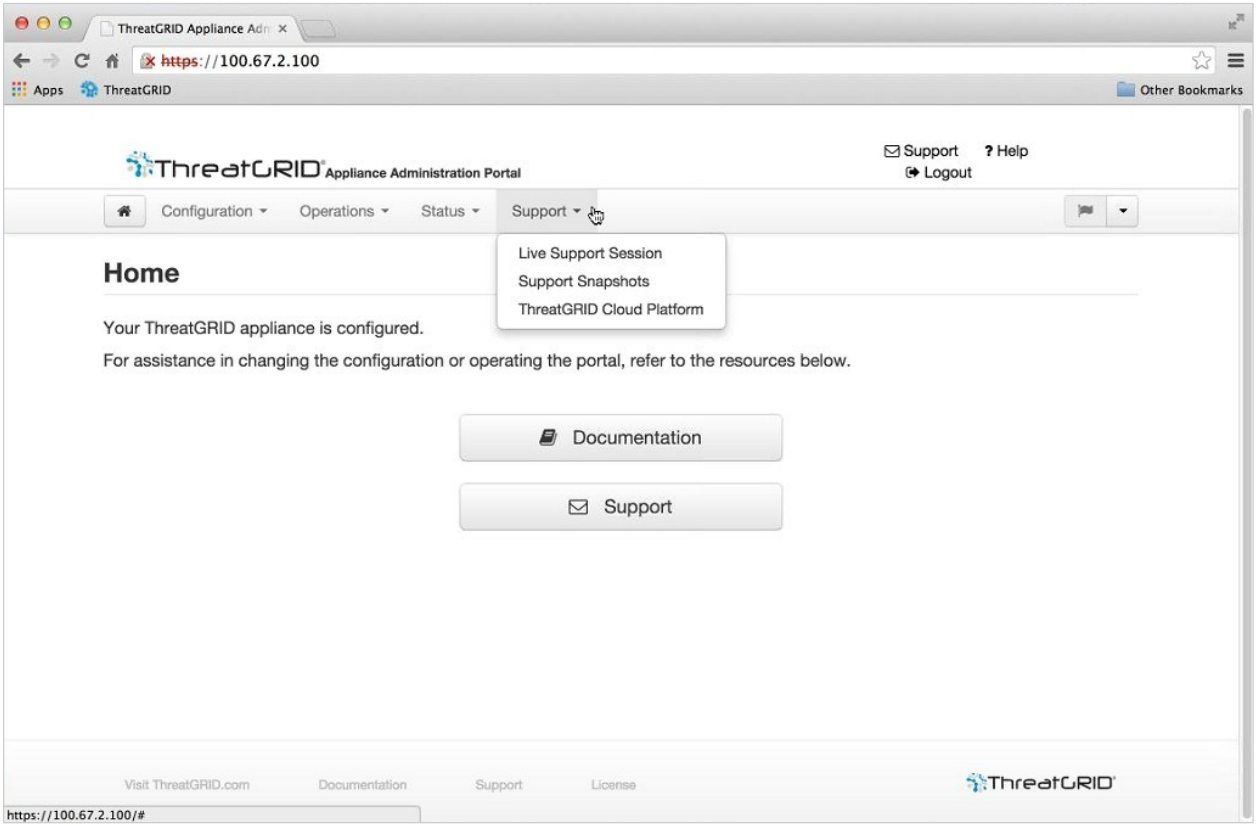
상태 메뉴

그림 21 - OpAdmin 상태 메뉴



지원 메뉴

그림 22 - OpAdmin 지원 메뉴



이 메뉴에서 라이브 지원 세션(지원 모드)에 액세스할 수 있습니다. 자세한 내용은 지원 섹션을 참조하십시오.