Threat Grid Appliance와 연결

버전 2.1.3

최종 업데이트: 2016년 8월 11일

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.

이 설명서의 제품 관련 사양 및 정보는 예고 없이 변경될 수 있습니다. 이 설명서의 모든 설명, 정보 및 권장 사항이 정확하다고 판단되더라도 어떠한 형태의 명시적이거나 묵시적인 보증도 하지 않습니다. 모든 제품의 해당 애플리케이션에 대한 사용은 전적으로 사용자에게 책임이 있습니다.

동봉한 제품의 소프트웨어 라이선스 및 제한된 보증은 제품과 함께 제공된 정보 패킷에 설명되어 있으며 본 문서에 참조를 통해 포함됩니다. 소프트웨어 라이선스 또는 제한된 보증을 찾을 수 없는 경우 CISCO 담당자에게 문의하여 복사본을 요청하십시오.

Cisco의 TCP 헤더 압축은 UNIX 운영 체제의 UCB 공개 도메인 버전의 일부로서 University of California, Berkeley (UCB)에서 개발된 프로그램을 적용하여 구현합니다. All rights reserved. Copyright © 1981, Regents of the University of California.

여기에 언급된 기타 모든 보증에도 불구하고 이러한 공급자의 모든 문서 및 소프트웨어는 모든 결함이 포함된 "있는 그대로" 제공됩니다. CISCO 및 위에 언급된 모든 공급자는 상품성, 특정 목적에의 적합성, 타인의 권리 비침해 또는 처리, 사용, 거래 행위로 발생하는 문제에 대한 묵시적 보증을 포함하여
(단, 이에 한하지 않음) 묵시적이든 명시적이든 모든 종류의 보증을 부인합니다.

CISCO 또는 그 공급자는 이 설명서의 사용 또는 사용할 수 없음으로 인한 모든 파생적, 부수적, 직접, 간접, 특별, 징벌적 또는 기타 모든 손해(영업 이익 손실, 영업 중단, 영업 정보 손실, 또는 그 밖의 금전적 손실로 인한 손해를 포함하되 이에 제한되지 않음)에 대하여 어떠한 경우에도 책임을 지지 않으며, 이는 CISCO 또는 그 공급자가 그와 같은 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

이 문서에서 사용된 모든 IP(인터넷 프로토콜) 주소와 전화 번호는 실제 주소와 전화 번호가 아닙니다. 이 문서에 포함된 예제, 명령 표시 출력, 네트워크 토폴로지 다이어그램 및 다른 그림은 이해를 돕기 위한 자료일 뿐이며, 실제 IP 주소나 전화 번호가 사용되었다면 이는 의도하지 않은 우연의 일치입니다.

Cisco 및 Cisco 로고는 미국 및 기타 국가에서 Cisco Systems, Inc. 및/또는 계열사의 상표 또는 등록 상표입니다. Cisco 상표 목록을 확인하려면 www.cisco.com/go/trademarks로 이동하십시오. 여기에 언급된 서드파티 상표는 해당 소유자의 자산입니다. 파트너라는 용어의 사용이 Cisco와 다른 업체 사이의 제휴 관계를 의미하는 것은 아닙니다.

표지 사진: 아치스 국립공원 안내소 위의 높은 산등성이에 피어 있는 구화 선인장입니다. 이 선인장은 거칠고 척박한 환경에서도 위험을 효과적으로 방어하고 자원을 최대한 활용하며 잘 자랍니다. Copyright © 2015 Mary C. Ecsedy. All rights reserved. 사전 허락 없이 사용할 수 없습니다.

*Threat Grid Appliance와 연결*은 Cisco AMP *Threat Grid Appliance 관리자 가이드*의 섹션으로 구성됩니다.

목차

그림 목록

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.

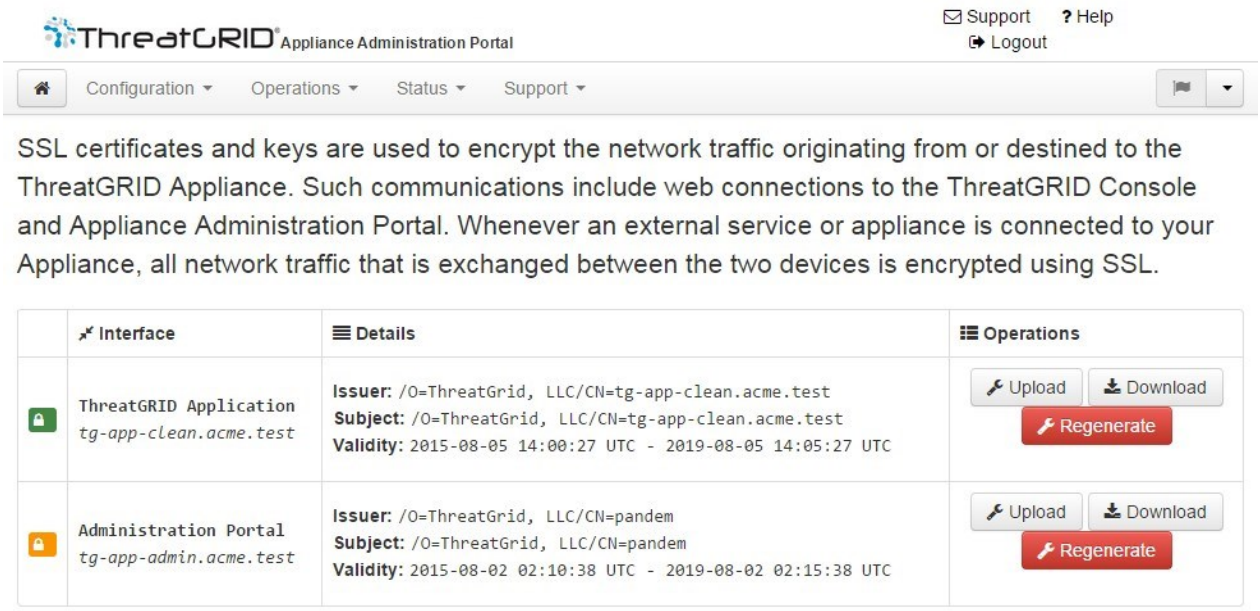
인바운드 연결을 위한 SSL 인증서 구성

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 1 - 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 Threat Grid Appliance를 Cisco FireAMP Private Cloud에 연결을 참조하십시오.

ESA/WSA 어플라이언스를 Threat Grid Appliance에 연결

ESA/WSA 및 기타 어플라이언스, 디바이스, 서비스 등의 Cisco 제품은 잠재적인 악성코드 샘플을 분석용으로 제출하기 위해 SSL로 암호화된 연결을 통해 Threat Grid Appliance와 통합될 수 있습니다. Threat Grid Appliance와 ESA/WSA 어플라이언스 간의 통합은 "CSA Integrations"라고도 하는 "CSA API"(Cisco Sandbox API)에 의해 활성화됩니다.

ESA/WSA 어플라이언스를 Threat Grid Appliance에 연결하려면 Threat Grid Appliance의 SSL 인증서 CN은 현재 호스트 이름과 일치해야 하며, 이러한 호스트 이름 또한 통합 ESA/WSA 어플라이언스에서 예상하는 호스트 이름과 일치해야 합니다.

분석을 위해 샘플을 제출하려면 우선 통합 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 섹션에서는 통합 ESA/WSA 어플라이언스 및 기타 Cisco 제품과 통신하기 위해 Threat Grid Appliance를 설정하는 데 필요한 단계를 설명합니다.

ESA/WSA 문서에 대한 링크

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

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

1. 호스트 이름은 CN 및 ESA/WSA 예상과 일치해야 합니다.

   Threat Grid Appliance SSL 인증서의 CN은 현재 호스트 이름과 일치해야 합니다. 통합 ESA/WSA 어플라이언스와 성공적으로 연결하려면, 이는 TGA를 확인하는 통합 ESA/WSA 어플라이언스에서도 동일한 호스트 이름이어야 합니다.

   요건에 따라, Threat Grid Appliance에서 자체 서명 SSL 인증서를 다시 생성하여 해당 인증서가 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 인바운드 연결을 위한 SSL 인증서 구성 섹션을 참조하십시오.

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

2. 연결을 확인합니다.

   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.

3. Cisco ESA/WSA 및 기타 디바이스를 Threat Grid Appliance에 등록합니다.

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

4. ESA/WSA 파일 분석 구성을 완료합니다.

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

Threat Grid Appliance에서 새 디바이스 사용자 어카운트 활성화

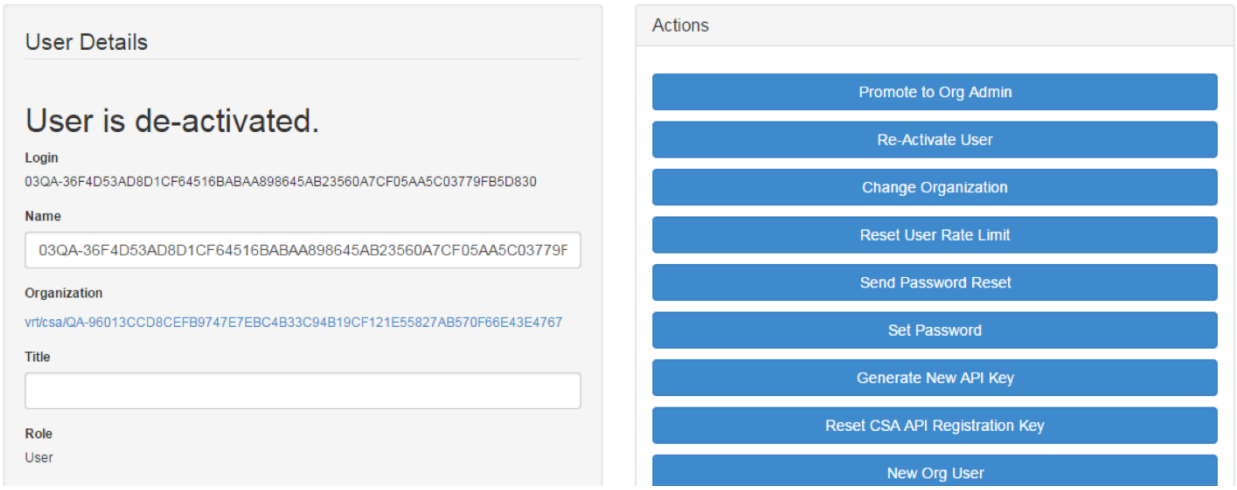
ESA/WSA 어플라이언스 또는 기타 통합 디바이스가 Threat Grid Appliance와 연결 및 등록될 경우, 새 Threat Grid 사용자 어카운트가 자동으로 생성됩니다. 이 사용자 어카운트의 초기 상태는 "비활성화"되어 있습니다.
다른 Threat Grid 사용자와 마찬가지로, 디바이스 사용자 어카운트는 분석을 위해 악성코드 샘플을 제출하는 데 사용하려면 우선 Threat Grid Appliance 관리자가 수동으로 활성화해야 합니다.

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 계정에 대한 **User Details(사용자 세부사항)** 페이지를 엽니다(Search(검색)를 사용하여 찾아야 할 수 있음). 사용자 상태가 현재 "비활성화"되어 있습니다.

그림 2 - 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.

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).	
2		FireAMP Private Cloud를 일반적으로 설정 및 구성합니다(즉, 통합은 아직 수행하지 않음).
3		**TGA 통합을 위해 다음과 같이 FireAMP Private Cloud를 구성합니다.** **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 있음). **호스트 이름** **Configuration(컨피그레이션) > Hostname(호스트 이름)**을 선택합니다. **API 키**: API 키는 Threat Grid Face Portal UI에서 통합에 사용할 계정의 **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 계정의 **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 구성을 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 구성을 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.

조직 관리에 대한 설명서는 *Threat Grid Appliance 관리자 가이드*를 참조하십시오. 이 가이드는 Cisco.com의 **Threat Grid Install and Upgrade(Threat Grid 설치 및 업그레이드)** 페이지에 있습니다.

사용자 어카운트 관리(Cisco ESA/WSA 어플라이언스 및 기타 디바이스 통합을 위한 어카운트 포함)에 대한 지침 및 문서는 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.

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 3 - 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.

자세한 내용은 cisco.com의 **Threat Grid Install and Upgrades(Threat Grid 설치 및 업그레이드)** 페이지에 있는 설명서를 참조하십시오.