

콘솔 및 OPadmin 포털에 대한 DTLS 인증을 통한 ThreatGrid RADIUS 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

소개

이 문서에서는 TG(ThreatGrid) 버전 2.10에 도입된 원격 인증 전화 접속 사용자 서비스(RADIUS) 인증 기능에 대해 설명합니다. 사용자는 관리 포털뿐만 아니라 AAA(Authentication, Authorization and Accounting) 서버에 저장된 자격 증명을 사용하여 콘솔 포털에 로그인할 수 있습니다.

이 문서에서는 기능을 구성하는 데 필요한 단계를 찾습니다.

사전 요구 사항

요구 사항

- ThreatGrid 버전 2.10 이상
- DTLS 인증을 통한 RADIUS를 지원하는 AAA 서버(draft-ietf-radext-dtls-04)

사용되는 구성 요소

- ThreatGrid Appliance 2.10
- ISE(Identity Services Engine) 2.7

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

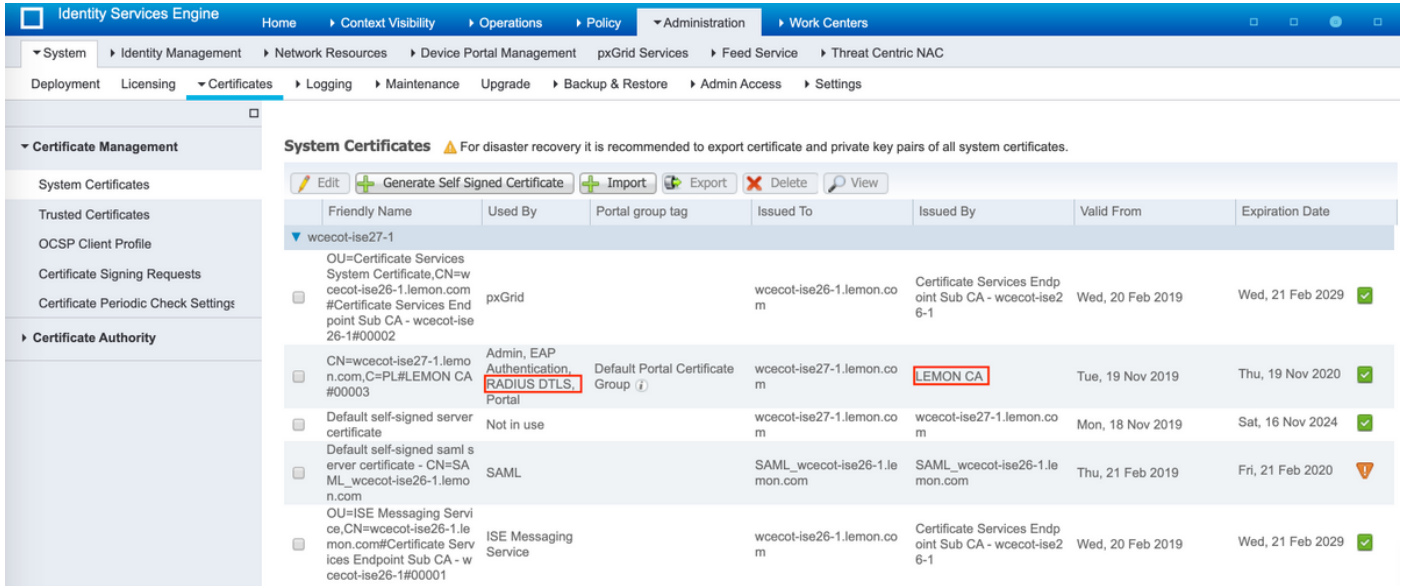
이 섹션에서는 RADIUS 인증 기능을 위해 ThreatGrid Appliance 및 ISE를 구성하는 방법에 대한 자세한 지침을 제공합니다.

참고: 인증을 구성하려면 ThreatGrid Clean 인터페이스와 ISE PSN(Policy Service Node) 간에 포트 UDP 2083의 통신이 허용되는지 확인합니다.

구성

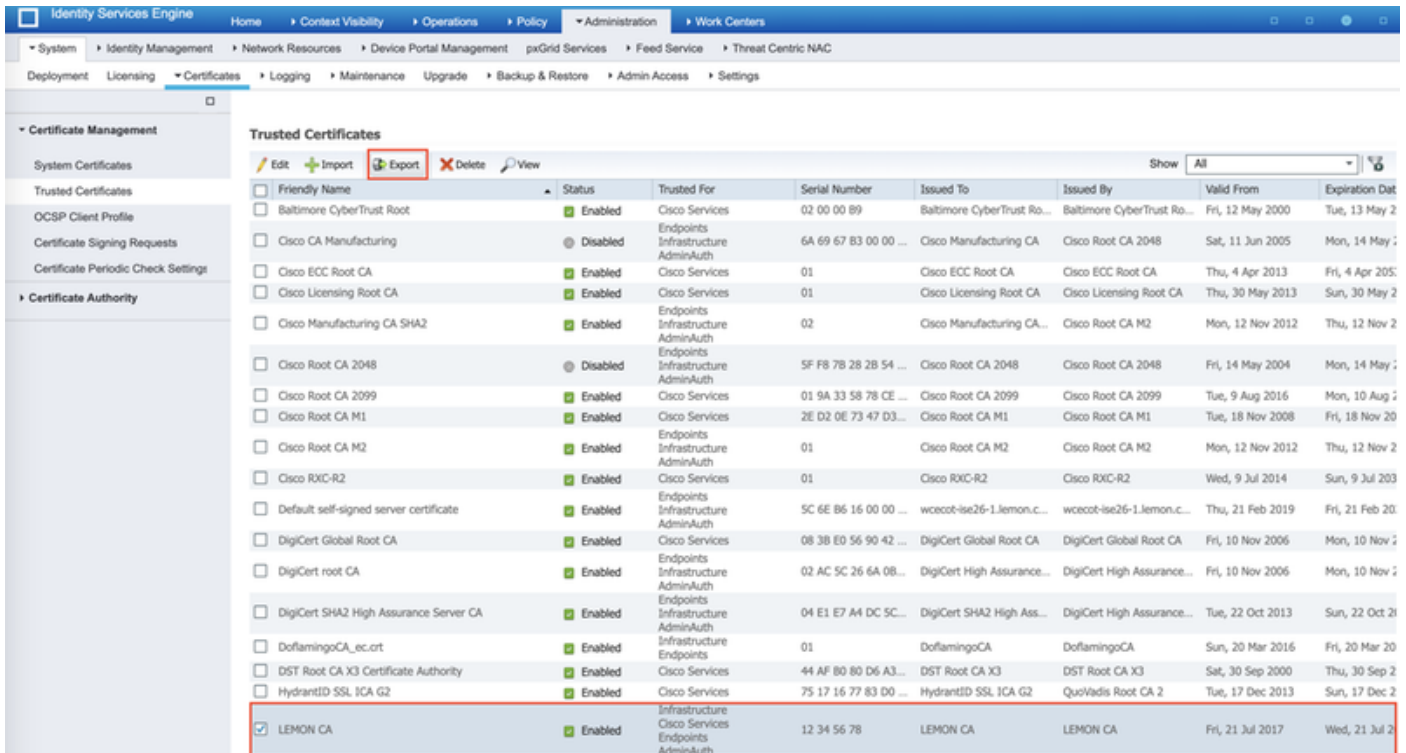
1단계. 인증을 위해 ThreatGrid 인증서를 준비합니다.

DTLS를 통한 RADIUS는 상호 인증서 인증을 사용하므로 ISE의 CA(Certificate Authority) 인증서가 필요합니다. 먼저 CA 서명 RADIUS DTLS 인증서를 확인합니다.



2단계. ISE에서 CA 인증서를 내보냅니다.

Administration(관리) > System(시스템) > Certificates(인증서) > Certificate Management(인증서 관리) > Trusted Certificates(신뢰할 수 있는 인증서)로 이동하여 CA를 찾은 다음 이미지에 표시된 대로 Export(내보내기)를 선택하고 나중에 사용할 수 있도록 인증서를 디스크에 저장합니다.



3단계. ThreatGrid를 네트워크 액세스 디바이스로 추가합니다.

Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이)

스) > Add(추가)로 이동하여 TG에 대한 새 항목을 생성하고 Clean(정상) 인터페이스의 Name, IP 주소
 소를 입력하고 이미지에 표시된 대로 DTLS Required(DTLS 필요)를 선택합니다.아래쪽에서
 Save를 클릭합니다.

The screenshot displays the configuration interface for a Network Device in Cisco ISE. The configuration includes:

- Name:** ksec-threatgrid02-clear
- Description:** (empty)
- IP Address:** 10.62.148.171 / 32
- Device Profile:** Cisco
- Model Name:** (empty)
- Software Version:** (empty)
- Network Device Group:**
 - Location: All Locations
 - IPSEC: No
 - Device Type: All Device Types
- RADIUS Authentication Settings:**
 - RADIUS UDP Settings:** Protocol: RADIUS, Shared Secret: (empty), CoA Port: 1700
 - RADIUS DTLS Settings:** DTLS Required: , Shared Secret: radius/dtls, CoA Port: 2083, Issuer CA of ISE Certificates for CoA: LEMON CA, DNS Name: ksec-threatgrid02-clear.cisco
 - General Settings:** Enable KeyWrap: , Key Encryption Key: (empty), Message Authenticator Code Key: (empty), Key Input Format: ASCII

Buttons for 'Save' and 'Reset' are located at the bottom of the configuration area.

4단계. 권한 부여 정책에 대한 권한 부여 프로파일을 생성합니다.

Policy(정책) > Policy elements(정책 요소) > Results(결과) > Authorization(권한 부여) >
 Authorization Profiles(권한 부여 프로파일)로 이동하고 Add(추가)를 클릭합니다.이름을 입력하고
 이미지에 표시된 대로 고급 속성 설정을 선택하고 저장을 클릭합니다.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > TG opadmin

Authorization Profile

* Name ThreatGrid

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

Advanced Attributes Settings

Radius:Service-Type = Administrative

Attributes Details

Access Type = ACCESS_ACCEPT
Service-Type = 6

Save Reset

5단계. 인증 정책을 생성합니다.

Policy(정책) > Policy Sets(정책 세트)로 이동하고 "+"를 클릭합니다. Policy Set Name을 입력하고 조건을 TG의 정상 인터페이스에 할당된 NAD IP Address로 설정하고 이미지에 표시된 대로 Save(저장)를 클릭합니다.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets

Reset Policyset Hitcounts Reset Save

	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	OK	ThreatGrid		Network Access: Device IP Address EQUALS 10.62.148.171	Default Network Access			
	OK	Default	Default policy set		Default Network Access	59		

6단계. 권한 부여 정책을 생성합니다.

">"을 클릭하여 권한 부여 정책으로 이동하고 권한 부여 정책을 확장한 다음 "+"를 클릭하고 이미지

에 표시된 대로 구성을 클릭한 다음 저장:

Authorization Policy (3)			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✔	ThreatGrid Admin	Radius-NAS-Identifier EQUALS Threat Grid Admin	ThreatGrid	Select from list	1	⚙️
✔	ThreatGrid Console	Radius-NAS-Identifier EQUALS Threat Grid UI	ThreatGrid	Select from list	1	⚙️
✔	Default		DenyAccess	Select from list	17	⚙️

팁: Admin 및 UI 조건과 일치하는 모든 사용자에게 대해 하나의 권한 부여 규칙을 생성할 수 있습니다.

7단계. ThreatGrid용 ID 인증서를 만듭니다.

ThreatGrid의 클라이언트 인증서는 Elliptic Curve 키를 기반으로 해야 합니다.

```
openssl ecparam -name secp521r1 -genkey -out private-ec-key.pem
```

ISE가 신뢰하는 CA에서 서명해야 합니다. ISE [Trusted Certificate Store](#)에 CA 인증서를 추가하는 방법에 대한 자세한 내용은 [Import the Root Certificates to the Trusted Certificate Store](#) 페이지를 참조하십시오.

8단계. RADIUS를 사용하도록 ThreatGrid를 구성합니다.

관리 포털에 로그인하고 Configuration(컨피그레이션) > **RADIUS로 이동합니다**. RADIUS CA Certificate(RADIUS CA 인증서)에서 ISE에서 수집한 PEM 파일의 내용을 Client Certificate paste PEM 형식 인증서(CA에서 받은 인증서 붙여넣기) 및 Client Key paste content of private-ec-key.pem 파일(이전 단계에서 받은 내용 붙여넣기)에 이미지에 표시된 대로 붙여넣습니다. Save(저장):

RADIUS DTLS Configuration

Authentication Mode		Either System Or RADIUS Authentication
RADIUS Host		10.48.17.135
RADIUS DTLS Port	HELP	2083
RADIUS CA Certificate	HELP	rVOxvUhoHai7g+B -----END CERTIFICATE-----
RADIUS Client Certificate	HELP	QFrtRNBHrKa -----END CERTIFICATE-----
RADIUS Client Key	HELP	2TOKEY4waktmOluw== -----END EC PRIVATE KEY-----
Initial Application Admin Username	HELP	radek

참고:RADIUS 설정을 저장한 후 TG 어플라이언스를 재구성해야 합니다.

9단계. 콘솔 사용자에게 RADIUS 사용자 이름을 추가합니다.

콘솔 포털에 로그인하려면 이미지에 표시된 대로 각 사용자에게 RADIUS 사용자 이름 특성을 추가해야 합니다.

Details

Login	radek
Name	radek /
Title	Add... /
Email	rolszowy@cisco.com /
Integration	<input type="text" value="none"/>
Role	admin
Status	<input checked="" type="radio"/> Active <input type="radio"/> Inactive
RADIUS Username	<input type="text" value="radek"/>
Default UI Submission Privacy	<input type="radio"/> Private <input type="radio"/> Public <input checked="" type="radio"/> Unset
EULA Accepted	No
CSA Auto-Submit Types	Add... /
Can Flag Entities	<input type="radio"/> True <input type="radio"/> False <input checked="" type="radio"/> Unset
Enable Direct SSO Setup	<input type="radio"/> True <input type="radio"/> False <input checked="" type="radio"/> Unset

10단계. RADIUS 전용 인증을 활성화합니다.

관리 포털에 성공적으로 로그인하면 로컬 시스템 인증을 완전히 비활성화하고 RADIUS 기반 인증만 남겨두는 새 옵션이 나타납니다.

Threat Grid Appliance Administration Portal

Support Help Logout

Configuration Operations Status Support

RADIUS DTLS Configuration

Authentication Mode	<input type="text" value="Only RADIUS Authentication Permitted"/>
RADIUS Host	<input type="text" value="10.48.17.135"/>

다음을 확인합니다.

TG가 다시 구성되면 로그오프하고 이제 로그인 페이지는 각각 이미지, 관리자 및 콘솔 포털과 같습니다.



Authentication Required

Authenticate using RADIUS:



Authenticate

or

Authenticate using System Password:



Authenticate

This site is best viewed in: Internet Explorer 10+, Firefox 14+, Safari 6+, or Chrome 20+



Threat Grid

i Use your RADIUS username and password.

RADIUS username

RADIUS password

Log In

[Forgot password?](#)

문제 해결

문제를 일으킬 수 있는 구성 요소는 다음과 같습니다. ISE, 네트워크 연결 및 ThreatGrid.

- ISE에서 ServiceType=Administrative를 ThreatGrid의 인증 요청으로 반환하는지 확인합니다 .Operations(운영) >RADIUS>Live Logs on ISE(ISE의 라이브 로그)로 이동하고 세부 정보를 확인합니다.

Time	Status	Details	Repeat ...	Identity	Authentication Policy	Authorization Policy	Authorizati...	Network Device	
x				Identity	ThreatGrid	x	Authorization Policy	Authorization	Network Device
Feb 20, 2020 09:40:38.753 AM	✓			radek	ThreatGrid >> Default	ThreatGrid >> ThreatGrid Admin	TG opadmin	ksec-threatgrid02-clean	
Feb 20, 2020 09:40:18.260 AM	✓			radek	ThreatGrid >> Default	ThreatGrid >> ThreatGrid Console	TG console	ksec-threatgrid02-clean	

Authentication Details


Source Timestamp	2020-02-20 09:40:38.753
Received Timestamp	2020-02-20 09:40:38.753
Policy Server	wcecot-ise27-1
Event	5200 Authentication succeeded
Username	radek
User Type	User
Authentication Identity Store	Internal Users
Authentication Method	PAP_ASCII
Authentication Protocol	PAP_ASCII
Service Type	Administrative
Network Device	ksec-threatgrid02-clean
Device Type	All Device Types
Location	All Locations
Authorization Profile	TG opadmin
Response Time	13 milliseconds

- 이러한 요청이 표시되지 않으면 ISE에서 패킷 캡처를 수행합니다. Operations(운영)>Troubleshoot(문제 해결)>Diagnostic Tools(진단 도구)>TCP Dump(TCP 덤프)로 이동하여 TG 정상 인터페이스의 Filter(필터)에 IP를 제공하고 Start(시작)를 클릭한 후 ThreatGrid에 로그

인을 시도합니다.

TCP Dump

Monitor the packet headers on the network and save to a file (up to 5 Minutes)

Status  Monitoring... (approximate file size: 8192 bytes) [Stop](#)

Host Name

Network Interface

Promiscuous Mode On Off

Filter
Example: 'ip host helios and not iceberg'

Format

Dump File

[Download](#)

[Delete](#)

바이트 수가 증가했음을 확인해야 합니다. 자세한 내용을 보려면 Wireshark에서 pcap 파일을 여십시오.

- ThreatGrid에서 저장을 클릭한 후 "We're sorry but something was wrong"이라는 오류 메시지가 표시되고 페이지가 다음과 같이 표시됩니다.



We're sorry, but something went wrong.

The server experienced an error while processing your request. Please retry your request later.

If this problem persists, [contact support](#).

즉, 클라이언트 인증서에 RSA 키를 가장 많이 사용했을 것입니다. 7단계에서 지정한 매개변수와 함께 ECC 키를 사용해야 합니다.