

ThreatGrid RADIUS via DTLS-verificatie configureren voor console en OPAdmin-portal

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Configuratie](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

In dit document wordt de verificatie van externe verificatie (RADIUS) door gebruiker in Service (RADIUS) beschreven, die in ThreatGrid (TG) versie 2.10 is geïntroduceerd. Hiermee kunnen gebruikers zich aanmelden bij het Admin-portal en een portal voor console met aanmeldingsgegevens die zijn opgeslagen in de AAA-server.

In dit document vindt u de gewenste stappen om de functie te configureren.

Voorwaarden

Vereisten

- ThreatGrid versie 2.10 of hoger
- AAA-server die RADIUS via DTLS-verificatie ondersteunt (concept-ietf-radext-dts-04)

Gebruikte componenten

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

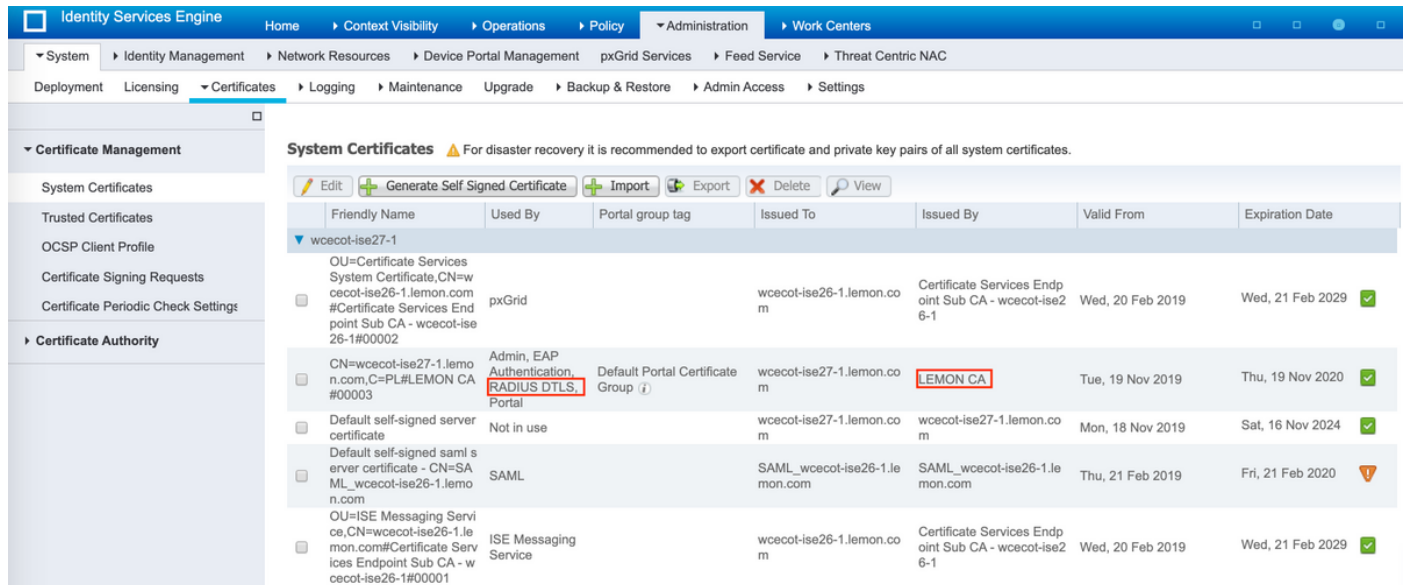
Deze sectie verschaft uitgebreide instructies over het configureren van ThreatGrid-applicatie en ISE voor RADIUS-verificatie functie.

Opmerking: Om de authenticatie te configureren dient u ervoor te zorgen dat communicatie over poort-UDP 2083 is toegestaan tussen ThreatGrid Clean interface en ISE Policy Service Node (PSN).

Configuratie

Stap 1. Bereid het ThreatGrid-certificaat voor op verificatie.

RADIUS over DTLS maakt gebruik van wederzijdse certificatie, wat betekent dat het certificaat van de certificaatinstantie (CA) van ISE vereist is. Controleer eerst wat een CA-ondertekend RADIUS DTLS-certificaat is:



System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date
OU=Certificate Services System Certificate,CN=wccot-ise26-1.lemon.com#Certificate Services Endpoint Sub CA - wccot-ise26-1#00002	pxGrid		wccot-ise26-1.lemon.com	Certificate Services Endpoint Sub CA - wccot-ise26-1	Wed, 20 Feb 2019	Wed, 21 Feb 2029
CN=wccot-ise27-1.lemon.com,C=PL#LEMON CA#00003	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group (j)	wccot-ise27-1.lemon.com	LEMON CA	Tue, 19 Nov 2019	Thu, 19 Nov 2020
Default self-signed server certificate	Not in use		wccot-ise27-1.lemon.com	wccot-ise27-1.lemon.com	Mon, 18 Nov 2019	Sat, 16 Nov 2024
Default self-signed saml server certificate - CN=SAML_wccot-ise26-1.lemon.com	SAML		SAML_wccot-ise26-1.lemon.com	SAML_wccot-ise26-1.lemon.com	Thu, 21 Feb 2019	Fri, 21 Feb 2020
OU=ISE Messaging Service,CN=wccot-ise26-1.lemon.com#Certificate Services Endpoint Sub CA - wccot-ise26-1#00001	ISE Messaging Service		wccot-ise26-1.lemon.com	Certificate Services Endpoint Sub CA - wccot-ise26-1	Wed, 20 Feb 2019	Wed, 21 Feb 2029

Stap 2. Exporteren van het CA-certificaat uit ISE.

navigeren naar **Beheer > Systeem > Certificaten > certificaatbeheer > Vertrouwde certificaten**, plaats de CA, selecteer **Exporteren** zoals in de afbeelding, en sla het certificaat voor later op de schijf op:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Certificate Management

System Certificates

Trusted Certificates

OCSP Client Profile

Certificate Signing Requests

Certificate Periodic Check Settings

Certificate Authority

Trusted Certificates

Edt Import Export Delete View Show All

Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date
Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 89	Baltimore CyberTrust Ro...	Baltimore CyberTrust Ro...	Fri, 12 May 2000	Tue, 13 May 20...
Cisco CA Manufacturing	Disabled	Endpoints Infrastructure AdminAuth	6A 69 67 83 00 00 ...	Cisco Manufacturing CA	Cisco Root CA 2048	Sat, 11 Jun 2005	Mon, 14 May 20...
Cisco ECC Root CA	Enabled	Cisco Services	01	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Fri, 4 Apr 2025
Cisco Licensing Root CA	Enabled	Cisco Services	01	Cisco Licensing Root CA	Cisco Licensing Root CA	Thu, 30 May 2013	Sun, 30 May 20...
Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure AdminAuth	02	Cisco Manufacturing CA...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 20...
Cisco Root CA 2048	Disabled	Endpoints Infrastructure AdminAuth	5F F8 7B 28 2B 54 ...	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May 2004	Mon, 14 May 20...
Cisco Root CA 2099	Enabled	Cisco Services	01 9A 33 58 78 CE ...	Cisco Root CA 2099	Cisco Root CA 2099	Tue, 9 Aug 2016	Mon, 10 Aug 20...
Cisco Root CA M1	Enabled	Cisco Services	2E D2 0E 73 47 D3...	Cisco Root CA M1	Cisco Root CA M1	Tue, 18 Nov 2008	Fri, 18 Nov 20...
Cisco Root CA M2	Enabled	Endpoints Infrastructure AdminAuth	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 20...
Cisco RXIC-R2	Enabled	Cisco Services	01	Cisco RXIC-R2	Cisco RXIC-R2	Wed, 9 Jul 2014	Sun, 9 Jul 2023
Default self-signed server certificate	Enabled	Endpoints Infrastructure AdminAuth	5C 6E B6 16 00 00 ...	wccot-ise26-1.lemo...	wccot-ise26-1.lemo...	Thu, 21 Feb 2019	Fri, 21 Feb 20...
DigiCert Global Root CA	Enabled	Cisco Services	08 3B E0 56 90 42 ...	DigiCert Global Root CA	DigiCert Global Root CA	Fri, 10 Nov 2006	Mon, 10 Nov 20...
DigiCert root CA	Enabled	Endpoints Infrastructure AdminAuth	02 AC SC 26 6A 0B...	DigiCert High Assurance...	DigiCert High Assurance...	Fri, 10 Nov 2006	Mon, 10 Nov 20...
DigiCert SHA2 High Assurance Server CA	Enabled	Endpoints Infrastructure AdminAuth	04 E1 E7 A4 DC 5C...	DigiCert SHA2 High Ass...	DigiCert High Assurance...	Tue, 22 Oct 2013	Sun, 22 Oct 20...
DoflamingoCA_ec.crt	Enabled	Endpoints Infrastructure AdminAuth	01	DoflamingoCA	DoflamingoCA	Sun, 20 Mar 2016	Fri, 20 Mar 20...
DST Root CA X3 Certificate Authority	Enabled	Cisco Services	44 AF 80 80 D6 A3...	DST Root CA X3	DST Root CA X3	Sat, 30 Sep 2000	Thu, 30 Sep 20...
HydrantID SSL ICA G2	Enabled	Cisco Services	75 17 16 77 83 D0 ...	HydrantID SSL ICA G2	QuoVadis Root CA 2	Tue, 17 Dec 2013	Sun, 17 Dec 20...
LEMON CA	Enabled	Infrastructure Cisco Services Endpoints AdminAuth	12 34 56 78	LEMON CA	LEMON CA	Fri, 21 Jul 2017	Wed, 21 Jul 20...

Stap 3. Voeg ThreatGrid toe als toegangsapparaat voor het netwerk.

Navigeer aan **Beheer > Netwerkbronnen > Netwerkapparaten > Toevoegen** om een nieuwe ingang voor TG te maken en voer het **Naam**, **IP-adres** van de interface Schoonmaken in en selecteer **DTLS vereist** zoals in de afbeelding. Klik onder op **Opslaan**:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network Devices

Default Device

Device Security Settings

Network Devices List > ksec-threatgrid02-clean

Network Devices

* Name

Description

IP Address * IP: /

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

Use Second Shared Secret

CoA Port

RADIUS DTLS Settings

DTLS Required

Shared Secret

CoA Port

Issuer CA of ISE Certificates for CoA

DNS Name

General Settings

Enable KeyWrap

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

TACACS Authentication Settings

SNMP Settings

Advanced TrustSec Settings

Stap 4. Maak een vergunningsprofiel voor het vergunningsbeleid.

Navigeer in **Policy > Policy elementen > Resultaten > autorisatie > autorisatieprofielen** en klik op **Add**. Voer een **naam** in en selecteer **Geavanceerde kenmerken** zoals in de afbeelding weergegeven en klik op **Opslaan**:

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The left sidebar shows a tree view with 'Authentication', 'Authorization', 'Profiling', 'Posture', and 'Client Provisioning'. The main content area is titled 'Authorization Profiles > TG opadmin' and 'Authorization Profile'. The configuration form includes:

- Name:** ThreatGrid (highlighted with a red box)
- Description:** (empty field)
- Access Type:** ACCESS_ACCEPT
- Network Device Profile:** Cisco
- Service Template:**
- Track Movement:**
- Passive Identity Tracking:**

 Below the form is a 'Common Tasks' section and an 'Advanced Attributes Settings' section where a rule is defined: 'Radius:Service-Type = Administrative' (highlighted with a red box). The 'Attributes Details' section shows 'Access Type = ACCESS_ACCEPT' and 'Service-Type = 6'. At the bottom are 'Save' and 'Reset' buttons.

Stap 5. Maak een authenticatiebeleid.

Navigeren in op **beleid > Stappen beleid** en klik op "+". Voer een **naam** in voor de beleidsinstelling en stel de voorwaarde in op **NAD IP-adres**, toegewezen aan de schone interface van TG, klik op **Opslaan** zoals in de afbeelding:

The screenshot shows the 'Policy Sets' section of the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The left sidebar shows a tree view with 'Policy Sets', 'Profiling', 'Posture', 'Client Provisioning', and 'Policy Elements'. The main content area shows a table of Policy Sets with columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, Hits, Actions, and View. The table contains two rows:

- ThreatGrid:** Status: ✔, Policy Set Name: ThreatGrid, Description: Network Access: Device IP Address EQUALS 10.62.148.171, Allowed Protocols / Server Sequence: Default Network Access, Hits: (empty), Actions: (gear icon), View: (> icon). This row is highlighted with a red box.
- Default:** Status: ✔, Policy Set Name: Default, Description: Default policy set, Allowed Protocols / Server Sequence: Default Network Access, Hits: 59, Actions: (gear icon), View: (> icon).

 At the top right of the table are buttons for 'Reset Policyset Hitcounts', 'Reset', and 'Save'.

Stap 6. Maak een vergunningenbeleid.

Klik op ">" om naar het machtigingsbeleid te gaan, breid het machtigingsbeleid uit, klik op "+" en

configureren zoals in de afbeelding, nadat u op **Opslaan** hebt geklikt:



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

Tip: U kunt één autorisatieregel maken voor al uw gebruikers die aan beide voorwaarden voldoen, Admin en UI.

Stap 7. Maak een identiteitsbewijs voor ThreatGrid.

ThreatGrid's client-certificaat moet zijn gebaseerd op de Elliptic Curve-toets:

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

Het moet worden ondertekend door de CA die de ISE vertrouwt. Controleer of [de basiscertificaten naar de pagina Trusted certificaatwinkel](#) zijn [geïmporteerd](#) voor meer informatie over het toevoegen van een CA-certificaat aan ISE Trusted certificaatwinkel.

Stap 8. Configuratie van ThreatGrid om RADIUS te gebruiken.

Meld u aan bij het beheerportal, navigeer naar **Configuration>RADIUS**. In RADIUS CA certificaatpasta de inhoud van het PEM-bestand dat van ISE is verzameld, in een client-certificaatpasta PEM-geformatteerd certificaat dat van CA is ontvangen en in een client-Key goedinhoud van een `privaat-ec-key.pem`-bestand dat is verkregen uit de vorige stap zoals in de afbeelding wordt getoond. Klik op **Opslaan**:

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

Opmerking: U moet het TG-apparaat opnieuw configureren nadat u de RADIUS-instellingen hebt opgeslagen.

Stap 9. Voeg RADIUS-gebruikersnaam toe aan console-gebruikers.

Als u wilt inloggen op een portal, moet u de RADIUS-gebruikersnaam aan de betreffende gebruiker toevoegen, zoals in de afbeelding:

Details

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

Stap 10. Laat alleen RADIUS-verificatie in.

Na het succesvol inloggen in het admin portal verschijnt er een nieuwe optie, die lokale systeemverificatie volledig uitschakelt en de enige op RADIUS gebaseerde optie achterlaat.

Threat Grid Appliance Administration Portal

Support ? Help
Logout

Configuration Operations Status Support

RADIUS DTLS Configuration

Authentication Mode	<input type="button" value="RADIUS Authentication Not Enabled"/> <input checked="" type="button" value="Either System Or RADIUS Authentication Permitted"/> <input checked="" type="button" value="Only RADIUS Authentication Permitted"/>
RADIUS Host	<input type="text" value="10.48.17.135"/>

Verifiëren

Nadat TG opnieuw is ingesteld, logt u uit en nu ziet het loggen in pagina's er zo uit in de afbeeldingen, admin en console portal:



Authentication Required

Authenticate using RADIUS:



or

Authenticate using System Password:



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?](#)

Problemen oplossen

Er zijn drie componenten die problemen kunnen veroorzaken: ISE, netwerkconnectiviteit en ThreatGrid.

- In ISE, zorg ervoor dat het ServiceType=Administration teruggeeft aan de authenticatieverzoeken van ThreatGrid. Navigatie in naar **bewerkingen>RADIUS>Live-logbestanden** op ISE en controleer details:

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

- Als u deze aanvragen niet ziet, voert u een pakketvastlegging op ISE uit. Navigatie naar Operations>Troubleshoot>Diagnostische Gereedschappen>TCP-pomp, specificeer IP in het veld Filter van de schone interface van de TG, klik op Start en probeer in te loggen op

ThreatGrid:

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](#)

U moet zien dat het aantal bytes is verhoogd. Open het PDF-bestand in Wireshark voor meer informatie.

- Als je de fout ziet "Het spijt ons, maar er is iets fout gegaan" nadat je op Save in ThreatGrid klikt en de pagina er zo uitziet:



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](#).

Dat betekent dat je waarschijnlijk de RSA-toets voor het client certificaat gebruikte. U moet de ECC-toets gebruiken met de parameters die in stap 7 zijn gespecificeerd.