

Configurazione di ThreatGrid RADIUS su autenticazione DTLS per console e portale OAdmin

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritta la funzionalità di autenticazione RADIUS (Remote Authentication Dial In User Service) introdotta nella versione 2.10 di ThreatGrid (TG). Consente agli utenti di accedere al portale di amministrazione e al portale della console con le credenziali archiviate nel server di autenticazione, autorizzazione e accounting (AAA).

In questo documento vengono illustrati i passaggi necessari per configurare la funzionalità.

Prerequisiti

Requisiti

- ThreatGrid versione 2.10 o superiore
- Server AAA che supporta l'autenticazione RADIUS su DTLS (draft-ietf-radext-dtls-04)

Componenti usati

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

In questa sezione vengono fornite istruzioni dettagliate su come configurare l'appliance ThreatGrid

e ISE per la funzionalità di autenticazione RADIUS.

Nota: Per configurare l'autenticazione, verificare che la comunicazione sulla porta UDP 2083 sia consentita tra l'interfaccia ThreatGrid Clean e ISE Policy Service Node (PSN).

Configurazione

Passaggio 1. Preparare il certificato ThreatGrid per l'autenticazione.

RADIUS over DTLS utilizza l'autenticazione reciproca dei certificati, il che significa che è necessario il certificato CA (Certification Authority) ISE. Verificare innanzitutto quale certificato DTLS RADIUS firmato dalla CA:

Identity Services Engine Administration > Work Centers > Certificates > System Certificates

System Certificates

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

Generate Self Signed Certificate Import Export Delete View

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

Passaggio 2. Esportare il certificato CA da ISE.

Passare a **Amministrazione > Sistema > Certificati > Gestione certificati > Certificati attendibili**, individuare la CA, selezionare **Esporta** come mostrato nell'immagine e salvare il certificato sul disco per utilizzarlo in seguito:

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 RXC-R2	Enabled	Cisco Services	01	Cisco RXC-R2	Cisco RXC-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 5C 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...

Passaggio 3. Aggiungere ThreatGrid come dispositivo di accesso alla rete.

Selezionare **Amministrazione > Risorse di rete > Dispositivi di rete > Aggiungi** per creare una nuova voce per TG e immettere **Nome**, **indirizzo IP** dell'interfaccia Pulisci e selezionare **DTLS Required** come mostrato nell'immagine. Fare clic su **Save** (Salva) in basso:

Identity Services Engine 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 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

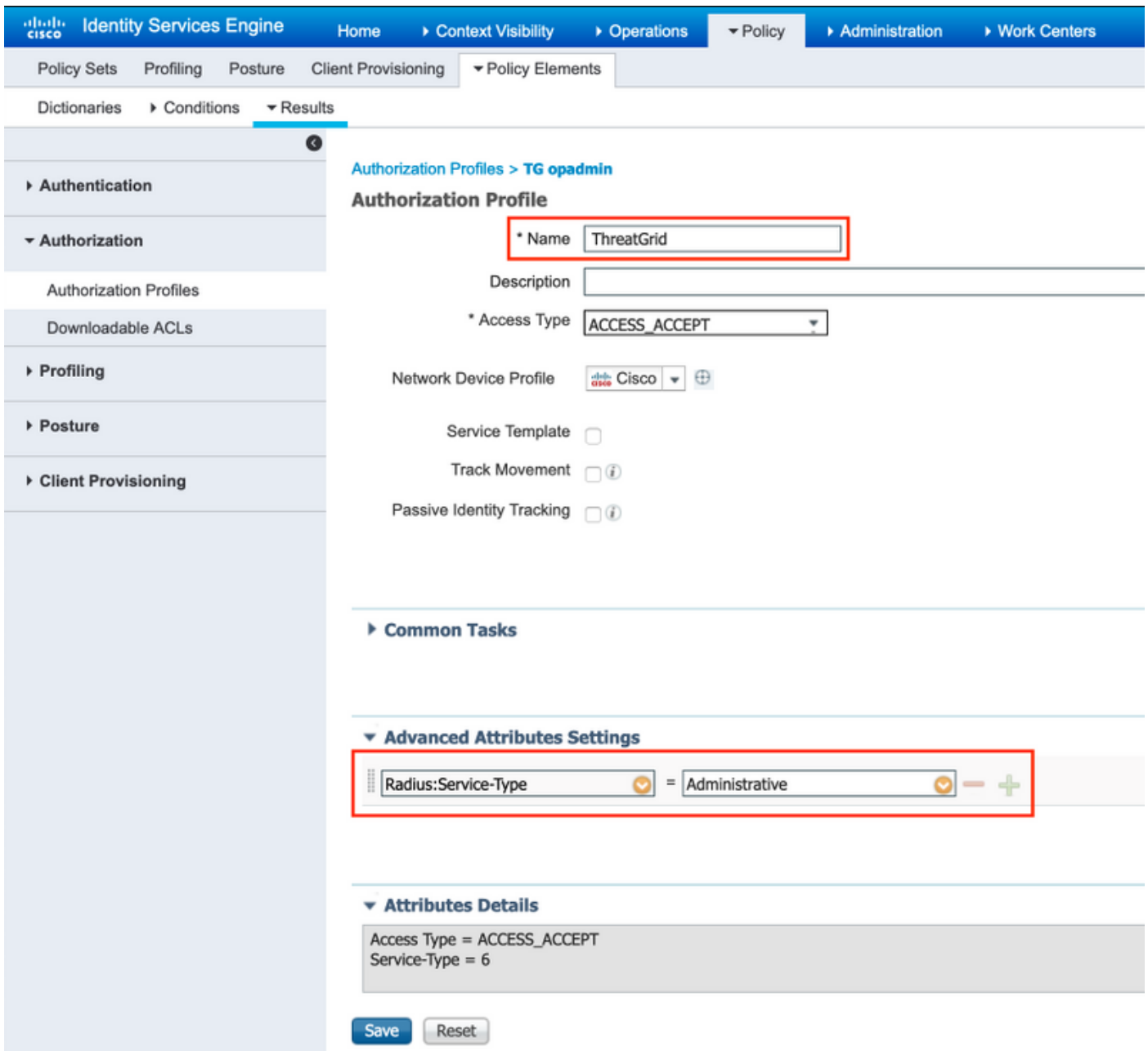
TACACS Authentication Settings

SNMP Settings

Advanced TrustSec Settings

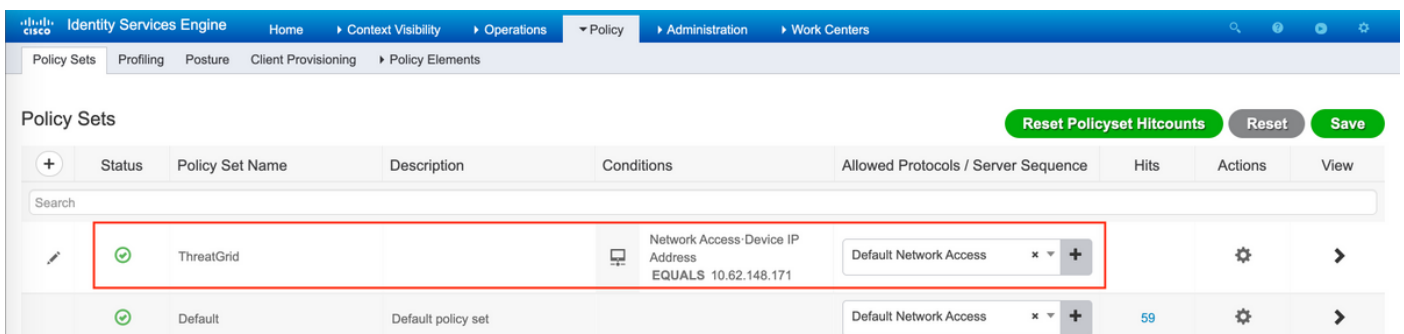
Passaggio 4. Creare un profilo di autorizzazione per i criteri di autorizzazione.

Passare a **Criterio > Elementi criteri > Risultati > Autorizzazione > Profili di autorizzazione** e fare clic su **Aggiungi**. Immettere **Name**, selezionare **Advanced Attributes Settings** come mostrato nell'immagine e fare clic su **Save**:



Passaggio 5. Creare un criterio di autenticazione.

Selezionare **Policy > Policy Sets** e fare clic su "+". Immettere Policy Set **Name** e impostare la condizione su **NAD IP Address**, assegnato all'interfaccia pulita di TG, fare clic su **Save** come mostrato nell'immagine:



Passaggio 6. Creare un criterio di autorizzazione.

Fare clic su ">" per accedere al criterio di autorizzazione, espandere il criterio di autorizzazione,

fare clic su "+" e configurare come mostrato nell'immagine, dopo aver terminato di fare clic su **Salva**:



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	⚙️	

Suggerimento: è possibile creare una sola regola di autorizzazione per tutti gli utenti che soddisfano entrambe le condizioni, Ammin e UI.

Passaggio 7. Creare un certificato di identità per ThreatGrid.

Il certificato client di ThreatGrid deve essere basato sulla chiave a curva ellittica:

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

Deve essere firmata dall'autorità di certificazione (CA) di cui ISE si fida. Per ulteriori informazioni su come aggiungere [il](#) certificato CA [all'](#)archivio certificati attendibile ISE, vedere [Importazione](#) dei certificati [radice](#) nella pagina [Archivio certificati attendibili](#).

Passaggio 8. Configurare ThreatGrid per l'utilizzo di RADIUS.

Accedere al portale di amministrazione e selezionare **Configuration>RADIUS**. In Certificato CA RADIUS incollare il contenuto del file PEM raccolto da ISE, in Certificato client incollare il certificato formattato PEM ricevuto da CA e in Chiave client incollare il contenuto del file private-ec-key.pem del passaggio precedente, come mostrato nell'immagine. Fare clic su **Salva**:

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

Nota: È necessario riconfigurare l'accessorio TG dopo aver salvato le impostazioni RADIUS.

Passaggio 9. Aggiungere il nome utente RADIUS agli utenti della console.

Per accedere al portale della console, è necessario aggiungere l'attributo Username RADIUS all'utente corrispondente, come mostrato nell'immagine:

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	<input type="radio"/> Private <input type="radio"/> Public <input checked="" type="radio"/> Unset
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

Passaggio 10. Abilitare l'autenticazione solo RADIUS.

Dopo aver eseguito correttamente l'accesso al portale di amministrazione, viene visualizzata una nuova opzione che disabilita completamente l'autenticazione del sistema locale e lascia l'unica basata su RADIUS.

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"/>

RADIUS Authentication Not Enabled
✓ Either System Or RADIUS Authentication Permitted
Only RADIUS Authentication Permitted

Verifica

Dopo la riconfigurazione di TG, disconnettersi e le pagine di accesso saranno visualizzate rispettivamente nelle immagini, nel portale di amministrazione e nel portale della console:



Threat Grid

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?](#)

Risoluzione dei problemi

I problemi possono essere causati da tre componenti: ISE, connettività di rete e ThreatGrid.

- In ISE verificare che restituisca ServiceType=Administrative alle richieste di autenticazione di ThreatGrid. Passare a **Operations>RADIUS>Live Logs** on ISE e controllare i dettagli:

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

- Se queste richieste non vengono visualizzate, eseguire un'acquisizione pacchetto su ISE. Selezionare Operations (Operazioni)>Troubleshoot>Diagnostic Tools (Strumenti di diagnostica) TCP Dump, fornire l'indirizzo IP nel campo Filter (Filtro IP in) dell'interfaccia clean

(Pulita) del TG, fare clic su **Start** e provare ad accedere a 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](#)

È necessario verificare che il numero di byte sia aumentato. Per ulteriori informazioni, aprite il file pcap in Wireshark.

- Se viene visualizzato l'errore "Si è verificato un errore" dopo aver fatto clic su Salva in ThreatGrid e la pagina avrà il seguente aspetto:

 Threat Grid Appliance Administration Portal [Support](#) [Help](#)
[Logout](#)

[Home](#) [Configuration](#) [Operations](#) [Status](#) [Support](#)

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](#).

Ciò significa che molto probabilmente è stata utilizzata la chiave RSA per il certificato client. È necessario utilizzare la chiave ECC con i parametri specificati nel passaggio 7.