為控制檯和OPadmin門戶配置ThreatGrid RADIUS over DTLS身份驗證

目錄

簡介

本檔案介紹ThreatGrid(TG)版本2.10中引入的遠端驗證撥入使用者服務(RADIUS)驗證功能。此功能允許使用者使用儲存在驗證、授權及記帳(AAA)伺服器中的憑證登入管理員入口和主控台入口。

在本檔案中，您會找到配置該功能所需的步驟。

必要條件

需求

- ThreatGrid 2.10或更高版本
- 支援RADIUS over DTLS身份驗證的AAA伺服器(draft-ietf-radext-dtls-04)

採用元件

- ThreatGrid裝置2.10
- 身分識別服務引擎(ISE)2.7

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

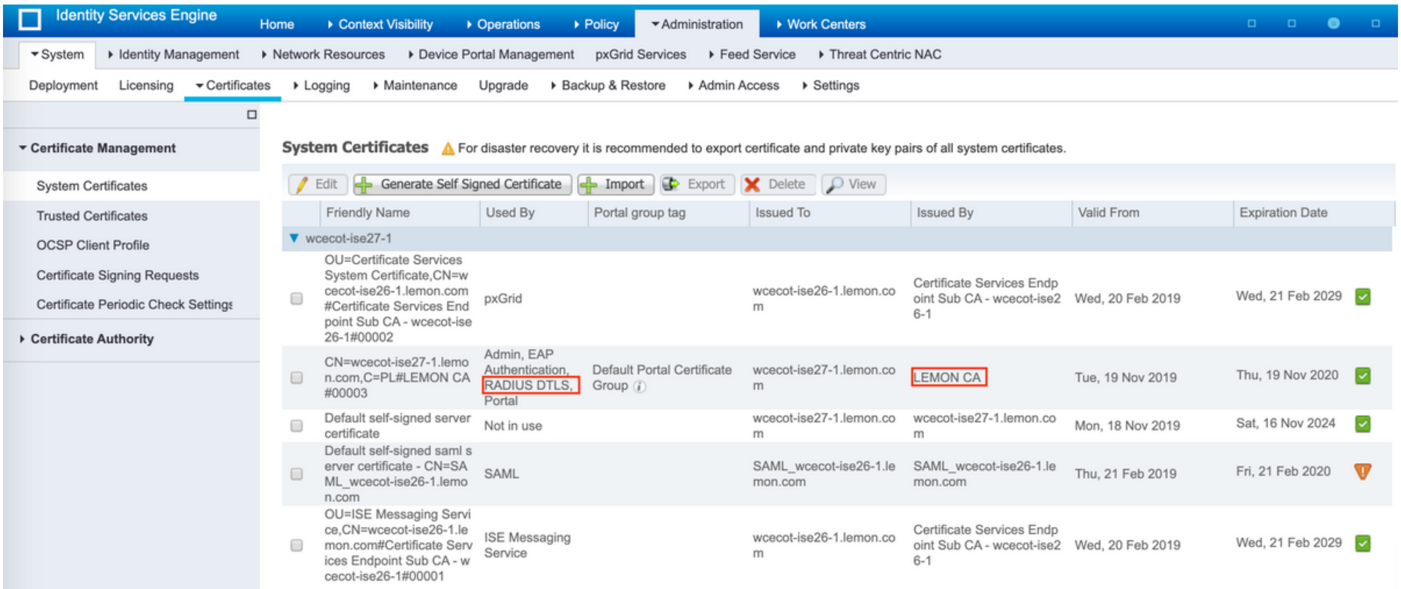
本節提供有關如何為RADIUS身份驗證功能配置ThreatGrid裝置和ISE的詳細說明。

> **附註**：為了配置身份驗證，請確保允許ThreatGrid Clean介面和ISE策略服務節點(PSN)之間的埠UDP 2083上的通訊。

組態

步驟1.準備ThreatGrid證書以進行身份驗證。

RADIUS over DTLS使用相互憑證驗證，這表示需要來自ISE的憑證授權單位(CA)憑證。首先檢查哪個CA簽名的RADIUS DTLS證書：

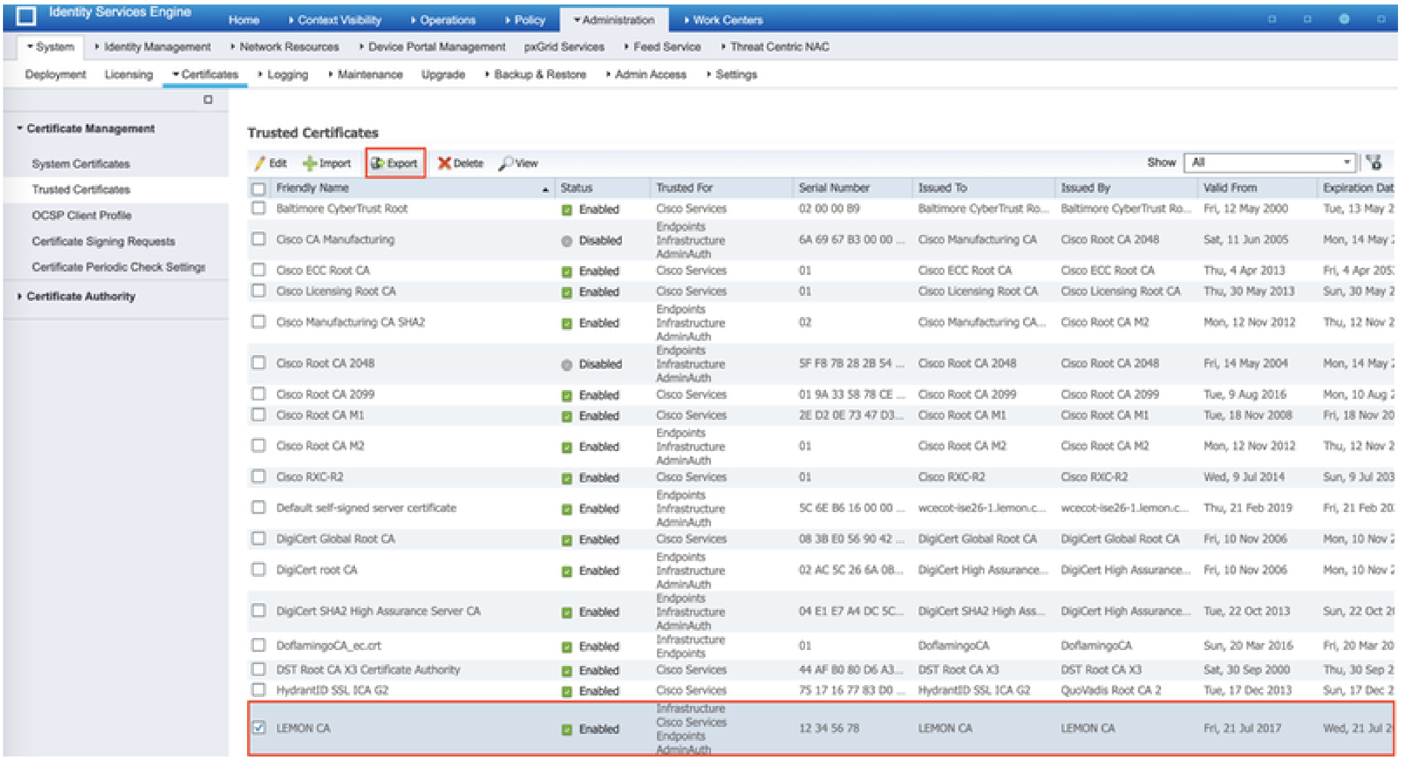


System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

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

步驟2.從ISE匯出CA證書。

導覽至**Administration > System > Certificates > Certificate Management > Trusted Certificates**，找到CA，選擇**Export**（如圖所示），然後將憑證儲存到磁碟上以備後用：

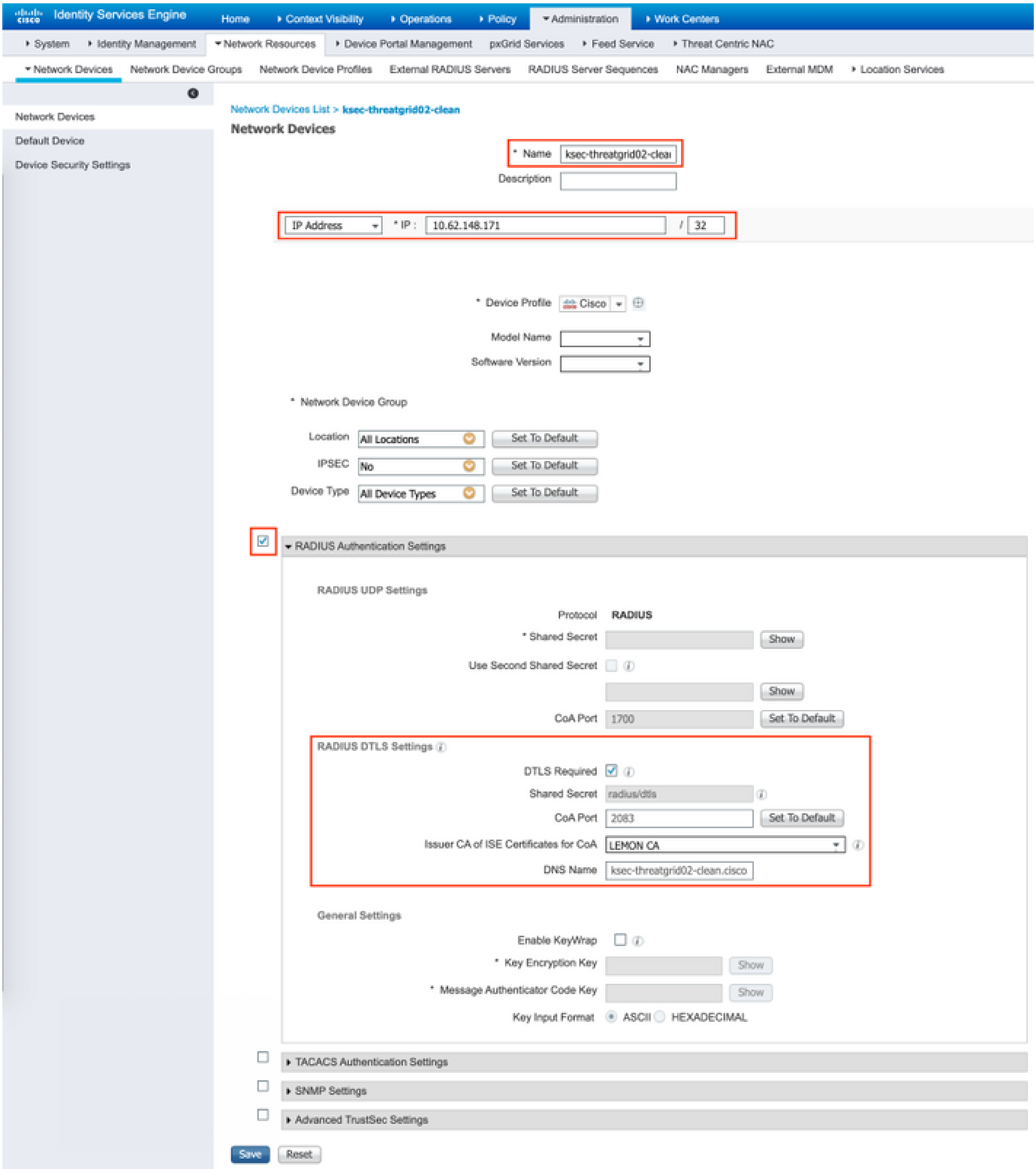


Trusted Certificates

□	Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Dat
□	Baltimore CyberTrust Root	✓ Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust Ro...	Baltimore CyberTrust Ro...	Fri, 12 May 2000	Tue, 13 May 2
□	Cisco CA Manufacturing	● Disabled	Endpoints Infrastructure AdminAuth	6A 69 67 B3 00 00 ...	Cisco Manufacturing CA	Cisco Root CA 2048	Sat, 11 Jun 2005	Mon, 14 May 2
□	Cisco ECC Root CA	✓ Enabled	Cisco Services	01	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Fri, 4 Apr 205
□	Cisco Licensing Root CA	✓ Enabled	Cisco Services	01	Cisco Licensing Root CA	Cisco Licensing Root CA	Thu, 30 May 2013	Sun, 30 May 2
□	Cisco Manufacturing CA SHA2	✓ Enabled	Endpoints Infrastructure AdminAuth	02	Cisco Manufacturing CA...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2
□	Cisco Root CA 2048	● Disabled	Endpoints Infrastructure AdminAuth	5F F8 78 28 28 54 ...	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May 2004	Mon, 14 May 2
□	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 2
□	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 2
□	Cisco RXC-R2	✓ Enabled	Cisco Services	01	Cisco RXC-R2	Cisco RXC-R2	Wed, 9 Jul 2014	Sun, 9 Jul 203
□	Default self-signed server certificate	✓ Enabled	Endpoints Infrastructure AdminAuth	5C 6E B6 16 00 00 ...	wcecot-ise26-1.lemon.c...	wcecot-ise26-1.lemon.c...	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 2
□	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 2
□	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 2
□	DoflamingoCA_ec.crt	✓ Enabled	Infrastructure Endpoints	01	DoflamingoCA	DoflamingoCA	Sun, 20 Mar 2016	Fri, 20 Mar 20
□	DST Root CA X3 Certificate Authority	✓ Enabled	Cisco Services	44 AF B0 80 D6 A3...	DST Root CA X3	DST Root CA X3	Sat, 30 Sep 2000	Thu, 30 Sep 2
□	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 2
☑	LEMON CA	✓ Enabled	Infrastructure Cisco Services Endpoints AdminAuth	12 34 56 78	LEMON CA	LEMON CA	Fri, 21 Jul 2017	Wed, 21 Jul 2

步驟3.將ThreatGrid新增為網路訪問裝置。

導覽至**Administration > Network Resources > Network Devices > Add**，為TG建立新條目，並輸入Clean介面的**Name**、**IP address**，然後選擇**DTLS Required**，如下圖所示。按一下底部的**Save**:



Network Devices List > ksec-threatgrid02-clean

Network Devices

* Name: ksec-threatgrid02-clea

Description:

IP Address * IP : 10.62.148.171 / 32

* Device Profile: Cisco

Model Name:

Software Version:

* Network Device Group

Location: All Locations (Set To Default)

IPSEC: No (Set To Default)

Device Type: All Device Types (Set To Default)

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

* Shared Secret: (Show)

Use Second Shared Secret: □

(Show)

CoA Port: 1700 (Set To Default)

RADIUS DTLS Settings

DTLS Required: ☑

Shared Secret: radius/dtls

CoA Port: 2083 (Set To Default)

Issuer CA of ISE Certificates for CoA: LEMON CA

DNS Name: ksec-threatgrid02-clean.cisco

General Settings

Enable KeyWrap: □

* Key Encryption Key: (Show)

* Message Authenticator Code Key: (Show)

Key Input Format: ● ASCII ○ HEXADECIMAL

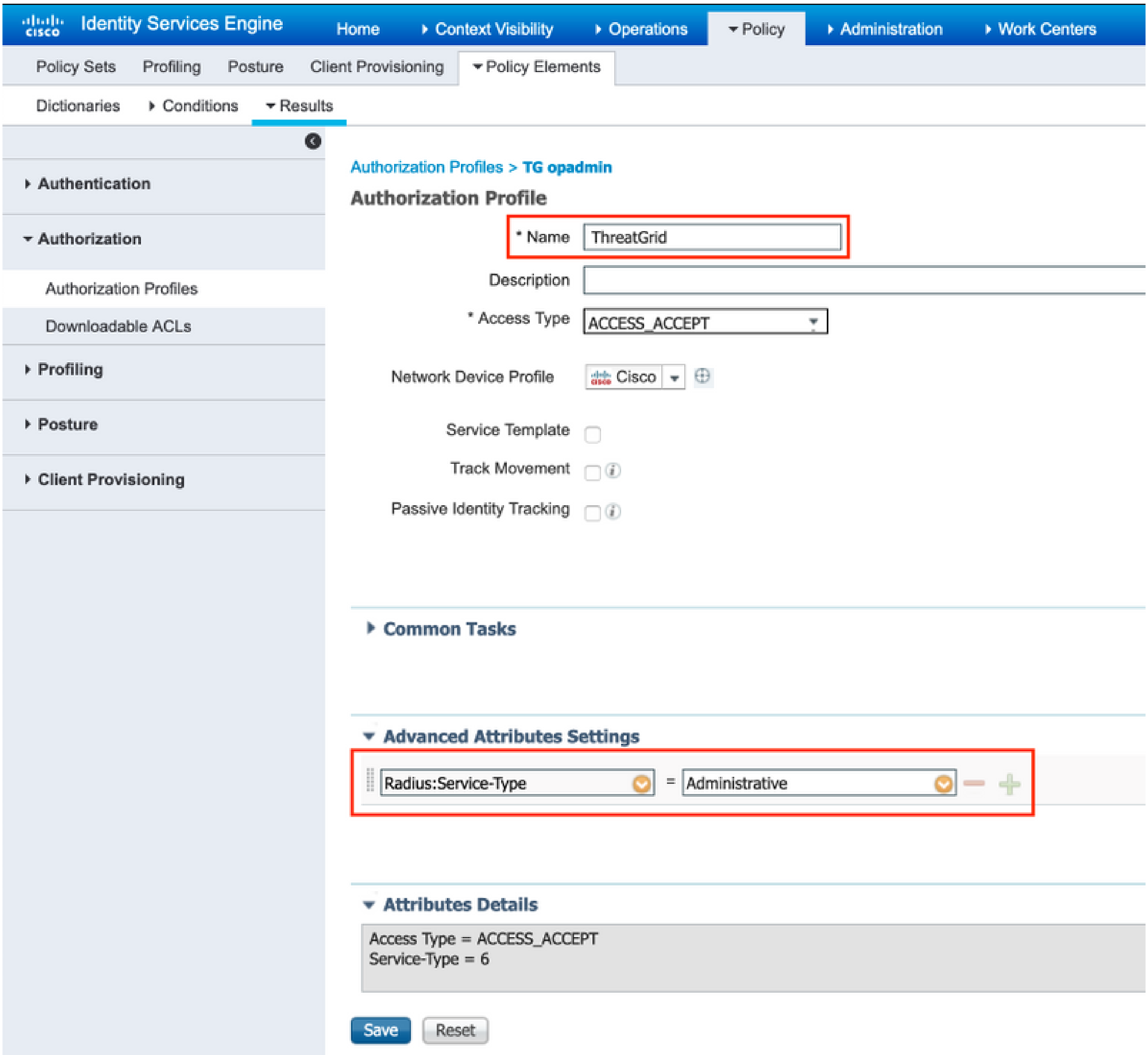
□ TACACS Authentication Settings

□ SNMP Settings

□ Advanced TrustSec Settings

步驟4.為授權策略建立授權配置檔案。

導航到**Policy > Policy elements > Results > Authorization > Authorization Profiles**，然後點選**Add**。輸入**Name**並選擇**Advanced Attributes Settings**，如下圖所示，然後按一下**Save**:



Authorization Profiles > TG opadmin

Authorization Profile

* Name: ThreatGrid

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

Advanced Attributes Settings

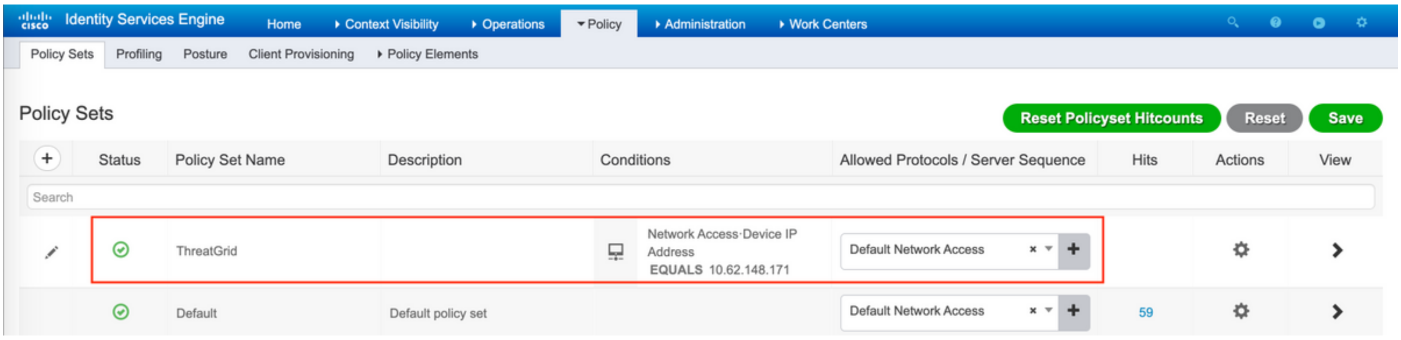
Radius:Service-Type = Administrative

Attributes Details

Access Type = ACCESS_ACCEPT
Service-Type = 6

步驟5.建立身份驗證策略。

導航到**Policy > Policy Sets**，然後點選「**+**」。 輸入策略集**名稱**，並將條件設定為**NAD IP地址**（分配給TG的乾淨介面），然後點選**Save**，如下圖所示：

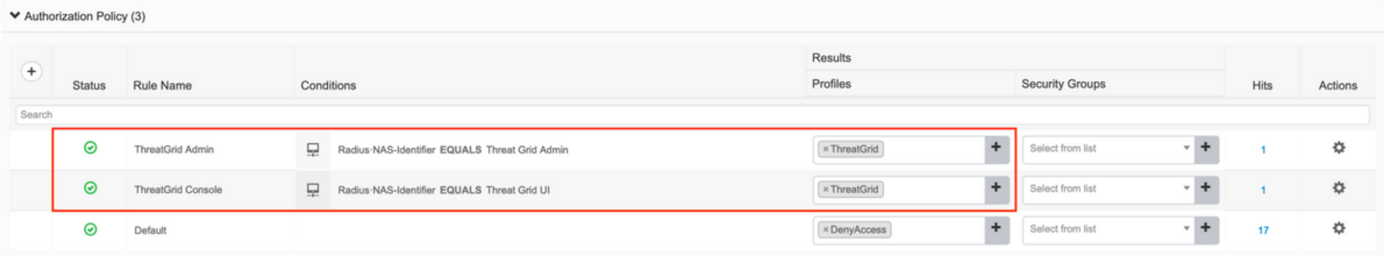


Policy Sets

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

步驟6.建立授權策略。

按一下「>」轉到授權策略，展開授權策略，按一下「+」**並配置，如下圖所示，完成後按一下Save**:



Authorization Policy (3)

Status	Rule Name	Conditions	Results 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	⚙

提示：您可以為所有同時符合管理員和UI條件的使用者建立一個授權規則。

步驟7.為ThreatGrid建立身份證書。

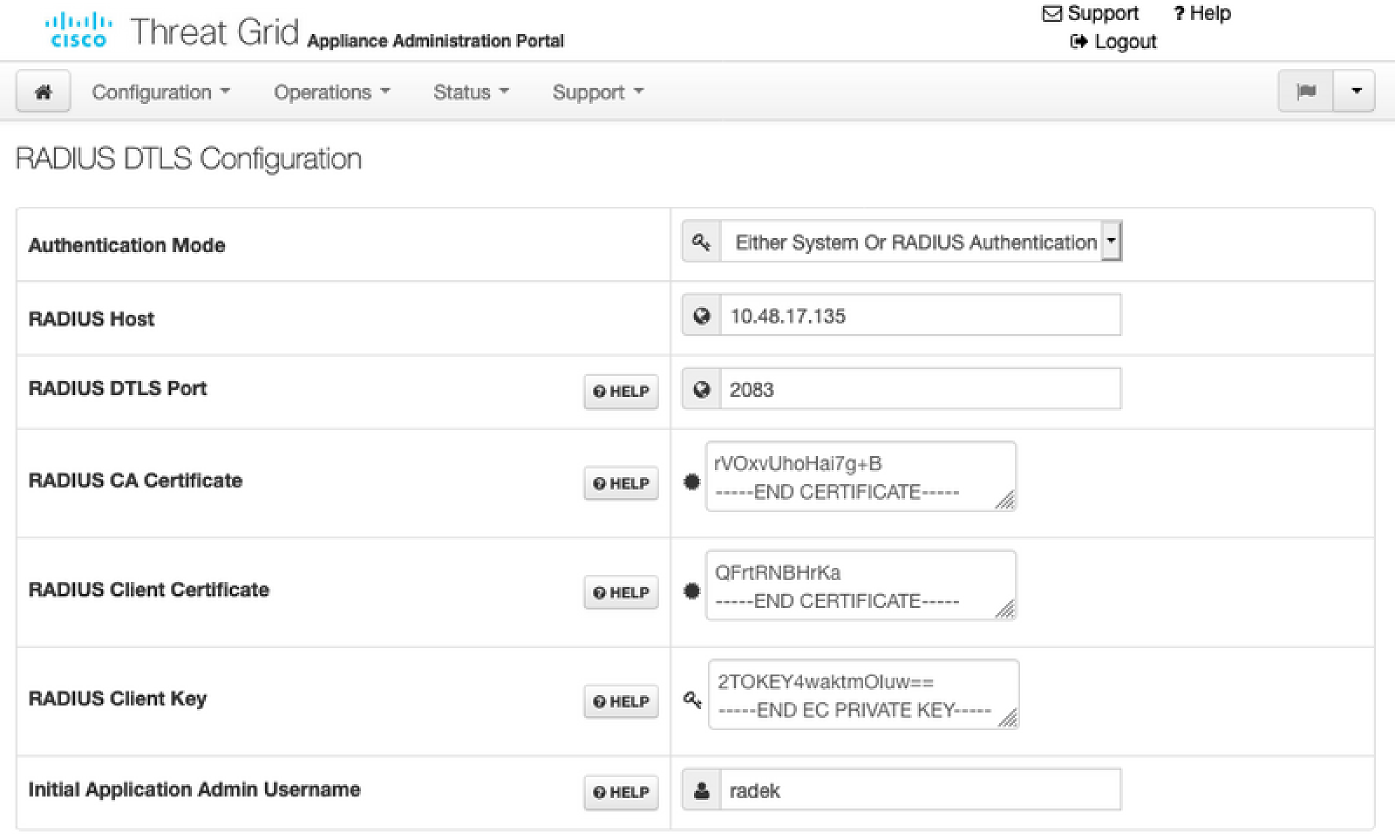
ThreatGrid的客戶端證書必須基於橢圓曲線金鑰：

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

必須由ISE信任的CA簽署。選中*Import the Root Certificates to the Trusted Certificate Store*頁面，獲取有關如何將CA證書新增到ISE受信任證書儲存區的詳細資訊。

步驟8.將ThreatGrid配置為使用RADIUS。

登入管理員入口網站，導覽至**Configuration>RADIUS**。在RADIUS CA證書中，貼上從ISE收集的PEM檔案的內容；在客戶端證書中，貼上從CA接收的PEM格式的證書；在客戶端金鑰中，貼上來自上一步的private-ec-key.pem檔案的內容，如圖所示。按一下「**Save**」：



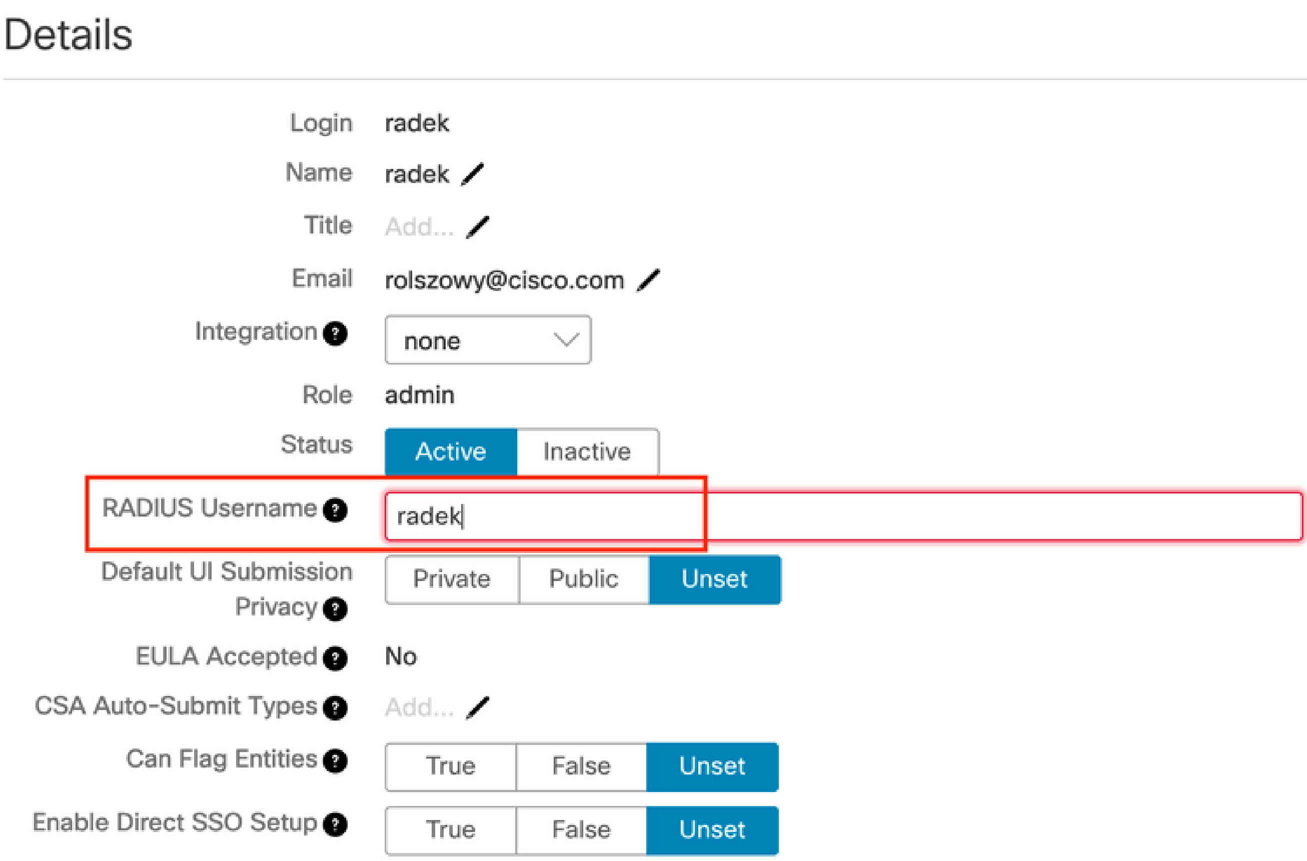
RADIUS DTLS Configuration

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

附註：儲存RADIUS設定後，必須重新配置TG裝置。

步驟9.將RADIUS使用者名稱新增到控制檯使用者。

若要登入主控台入口網站，您必須將RADIUS Username屬性新增到各自的使用者，如下圖所示：

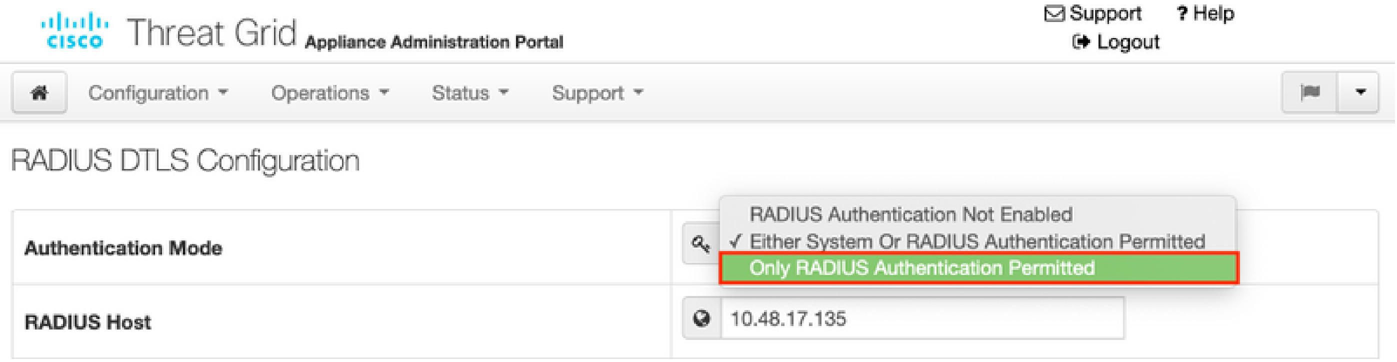


Details

Login	radek
Name	radek
Title	Add...
Email	rolszowy@cisco.com
Integration	none
Role	admin
Status	[✓ Active] Inactive
RADIUS Username	radek
Default UI Submission Privacy	Private Public [✓ Unset]
EULA Accepted	No
CSA Auto-Submit Types	Add...
Can Flag Entities	True False [✓ Unset]
Enable Direct SSO Setup	True False [✓ Unset]

步驟10.啟用僅RADIUS身份驗證。

成功登入到管理員門戶後，會出現一個新選項，該選項將完全禁用本地系統身份驗證，並保留唯一的基於RADIUS的身份驗證。

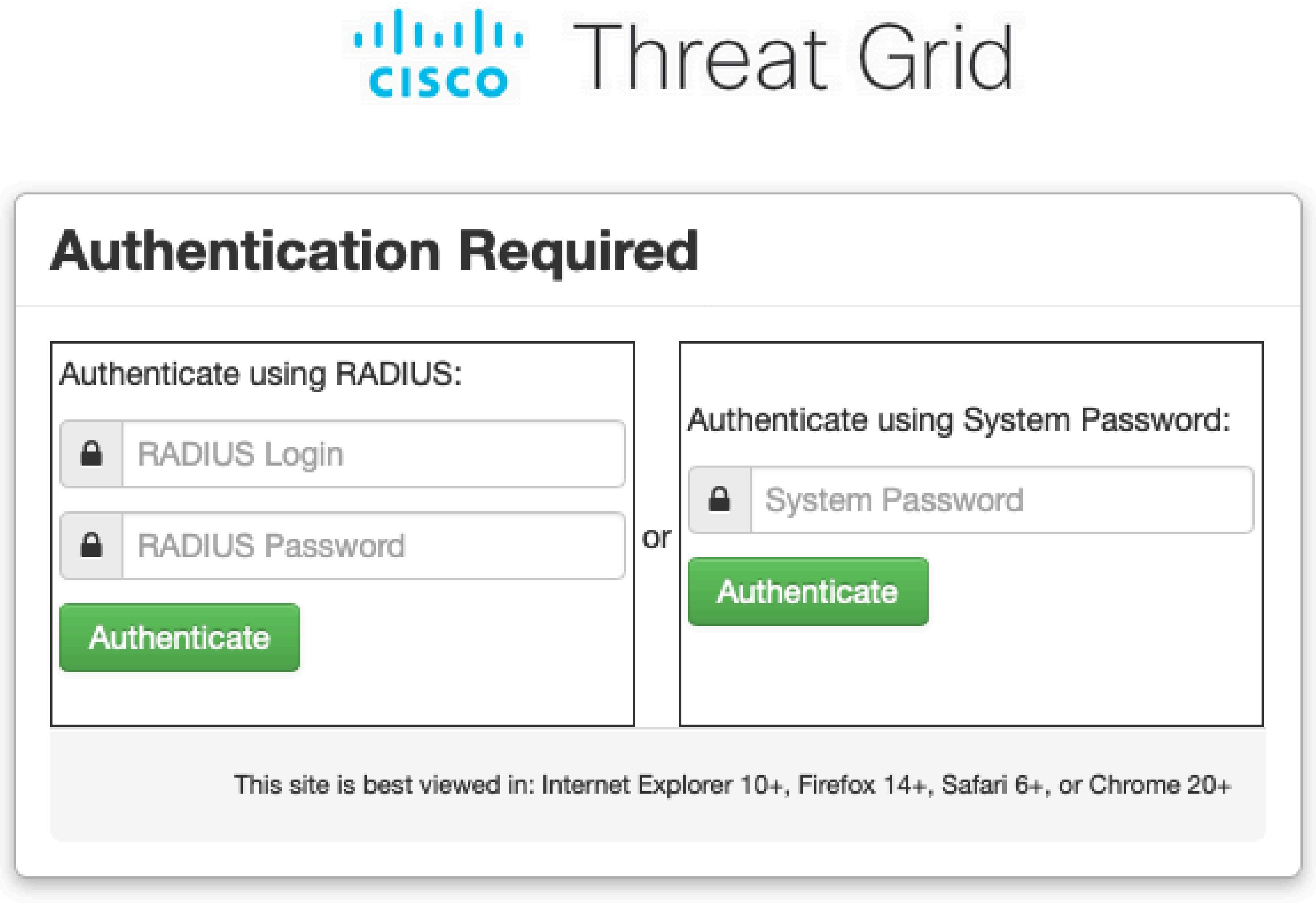


RADIUS DTLS Configuration

Authentication Mode	RADIUS Authentication Not Enabled ✓ Either System Or RADIUS Authentication Permitted Only RADIUS Authentication Permitted
RADIUS Host	10.48.17.135

驗證

重新配置TG後，註銷登入頁面，現在登入頁面在映像、管理門戶和控制檯門戶中看起來與此類似：



Threat Grid

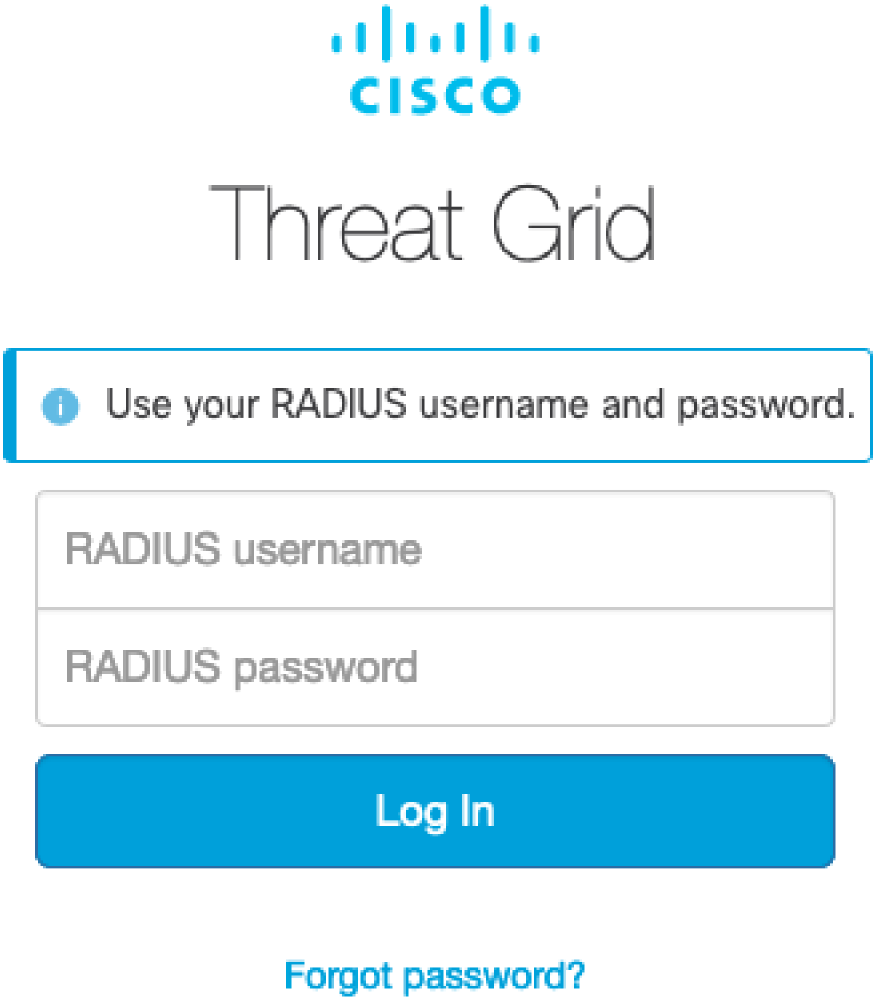
Authentication Required

Authenticate using RADIUS:

or

Authenticate using System Password:

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



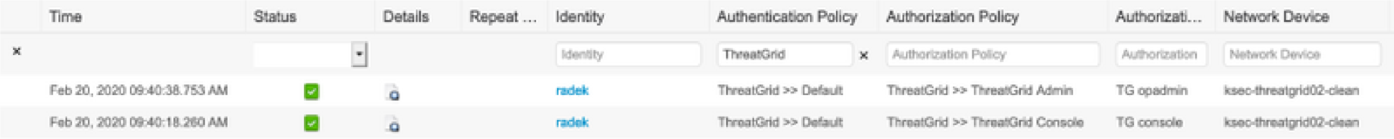
Threat Grid

Use your RADIUS username and password.

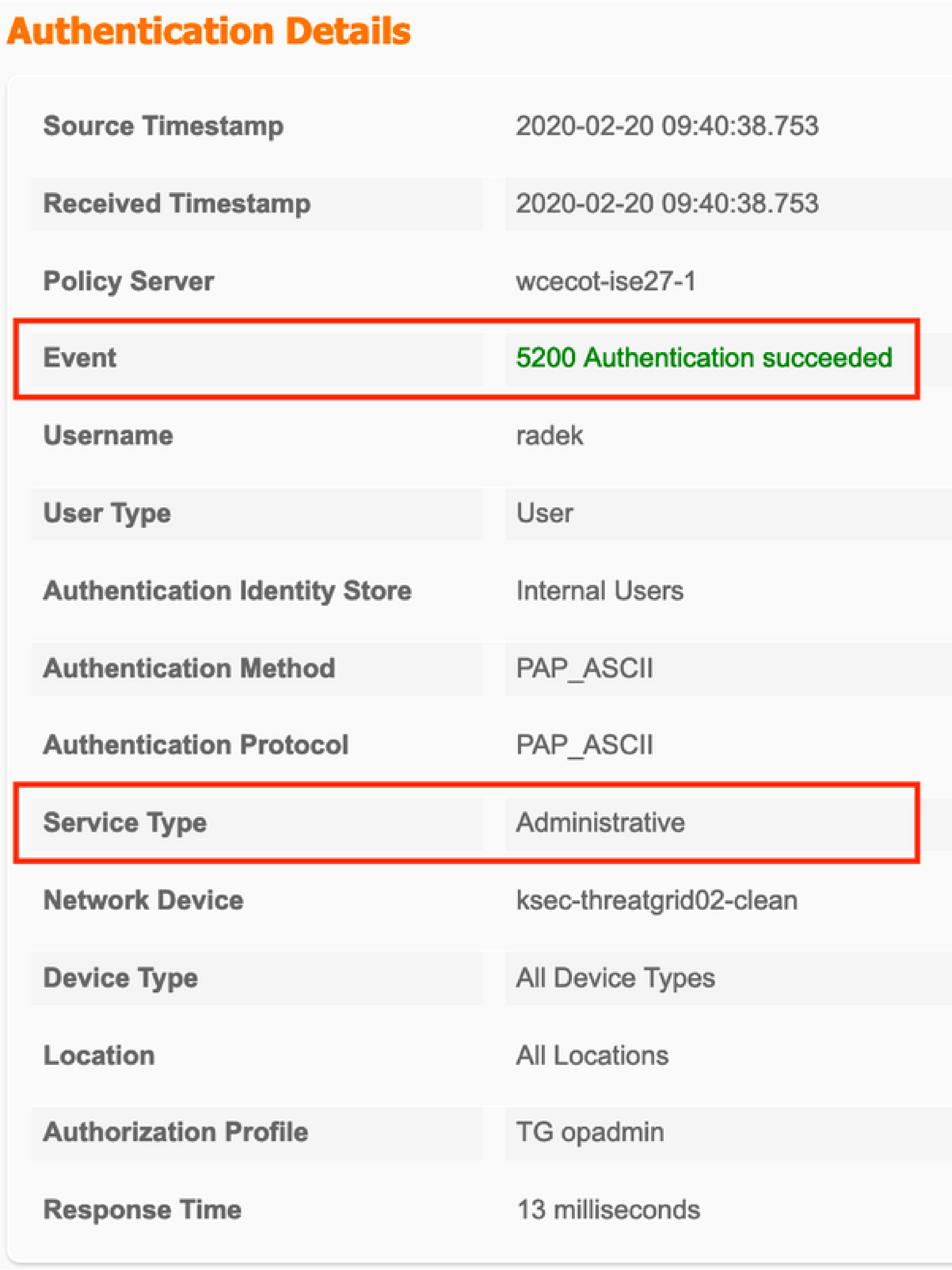
疑難排解

以下三個元件可能會導致問題：ISE、網路連線和ThreatGrid。

- 在ISE中，確保它將ServiceType=Administrative返回ThreatGrid的身份驗證請求。導覽至**Operations>RADIUS>ISE上的Live Logs**，並檢查詳細資訊：



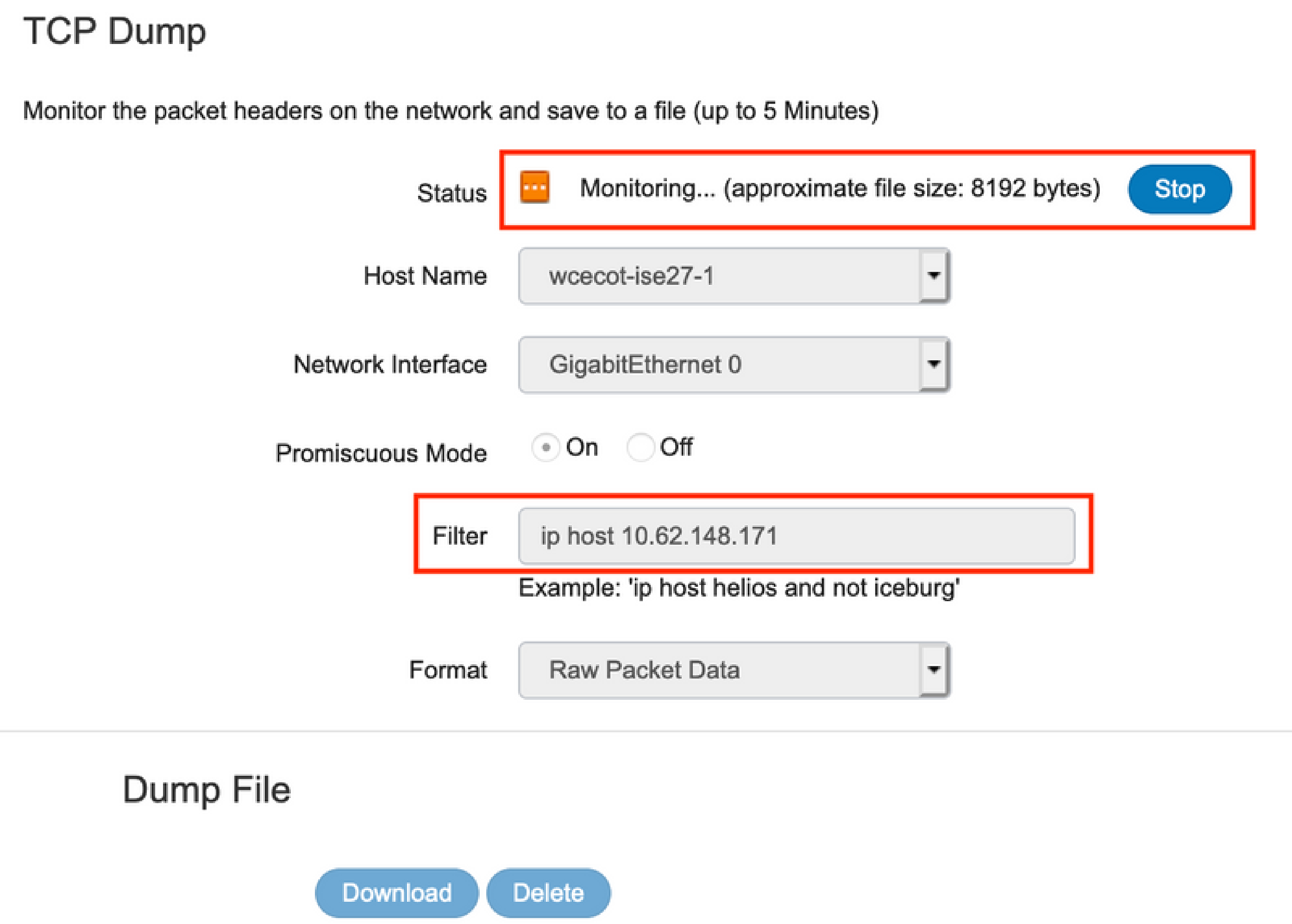
	Time	Status	Details	Repeat ...	Identity	Authentication Policy	Authorization Policy	Authorizati...	Network Device
×						ThreatGrid ×			
	Feb 20, 2020 09:40:38.753 AM	✓			radek	ThreatGrid >> Default	ThreatGrid >> ThreatGrid Admin	TG opadmin	ksec-threatgrid02-clean
	Feb 20, 2020 09:40:18.260 AM	✓			radek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

- 如果您沒有看到這些請求，請在ISE上執行資料包捕獲。導航到Operations> Troubleshoot> Diagnostic **Tools> TCP Dump**，在TG的**clean interface的Filter欄位中提供IP，按一下Start**並嘗試登入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: wcecot-ise27-1

Network Interface: GigabitEthernet 0

Promiscuous Mode: ● On ○ Off

Filter: ip host 10.62.148.171

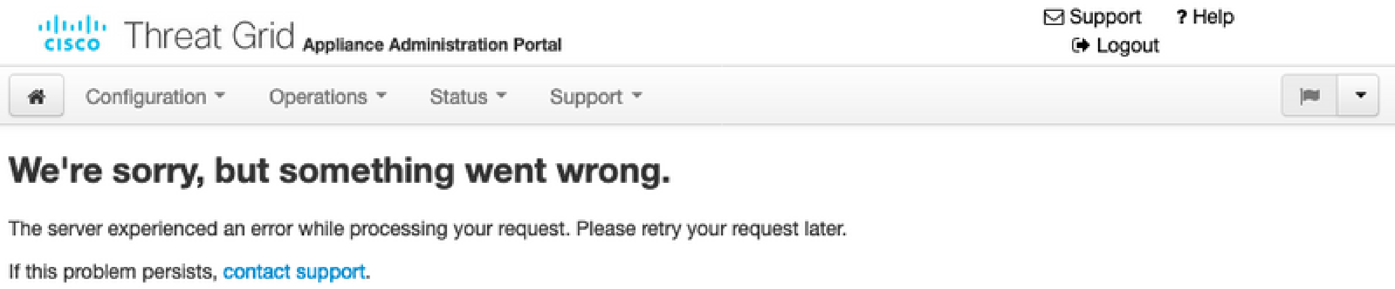
Example: 'ip host helios and not iceburg'

Format: Raw Packet Data

Dump File

您必須看到該位元組數增加。在Wireshark中開啟pcap檔案以瞭解詳細資訊。

- 如果您在ThreatGrid中按一下「儲存」後看到錯誤「很抱歉，但出現了問題」，則頁面如下所示：



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.

這表示您很可能對客戶端證書使用了RSA金鑰。必須使用具有步驟7中指定的引數的ECC金鑰。