コンソールおよびOPadminポータルのThreatGrid RADIUS over DTLS認証の設定

内容

概要

このドキュメントでは、ThreatGrid(TG)バージョン2.10で導入されたRemote Authentication Dial In User Service(RADIUS)認証機能について説明します。ユーザは、認証、許可、アカウンティング(AAA)サーバに保存されたクレデンシャルを使用して、AdminポータルおよびConsoleポータルにログインできます。

このドキュメントでは、この機能を設定するために必要な手順について説明します。

前提条件

要件

- ThreatGridバージョン2.10以降
- RADIUS over DTLS認証をサポートするAAAサーバ(draft-ietf-raid-dtls-04)

使用するコンポーネント

- ThreatGridアプライアンス2.10
- Identity Services Engine(ISE)2.7

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

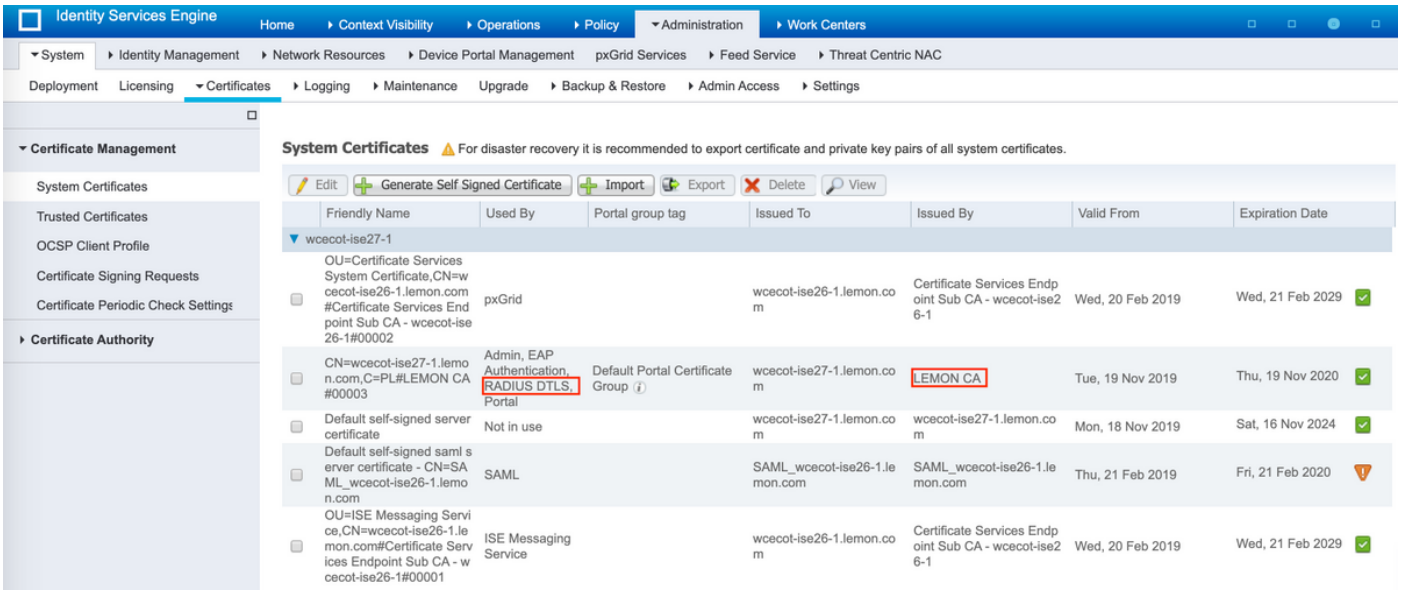
このセクションでは、RADIUS認証機能のThreatGridアプライアンスおよびISEの設定方法について詳しく説明します。

注：認証を設定するには、ポートUDP 2083での通信がThreatGrid Cleanインターフェイスとと ISE Policy Service Node(PSN)間で許可されていることを確認します。

コンフィギュレーション

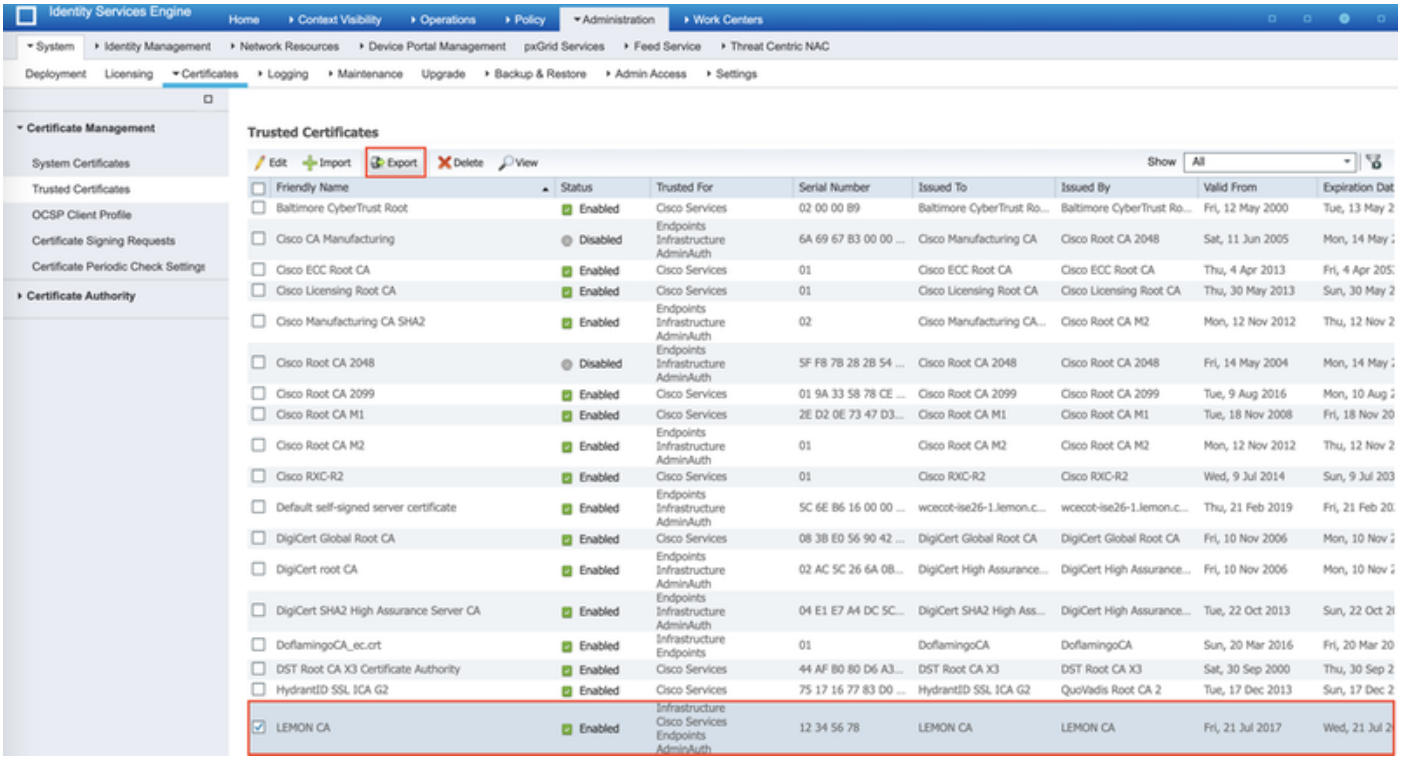
ステップ1：認証用のThreatGrid証明書を準備します。

RADIUS over DTLSは相互証明書認証を使用します。つまり、ISEからの認証局(CA)証明書が必要になります。まず、どのCA署名付きRADIUS DTLS証明書を確認します。



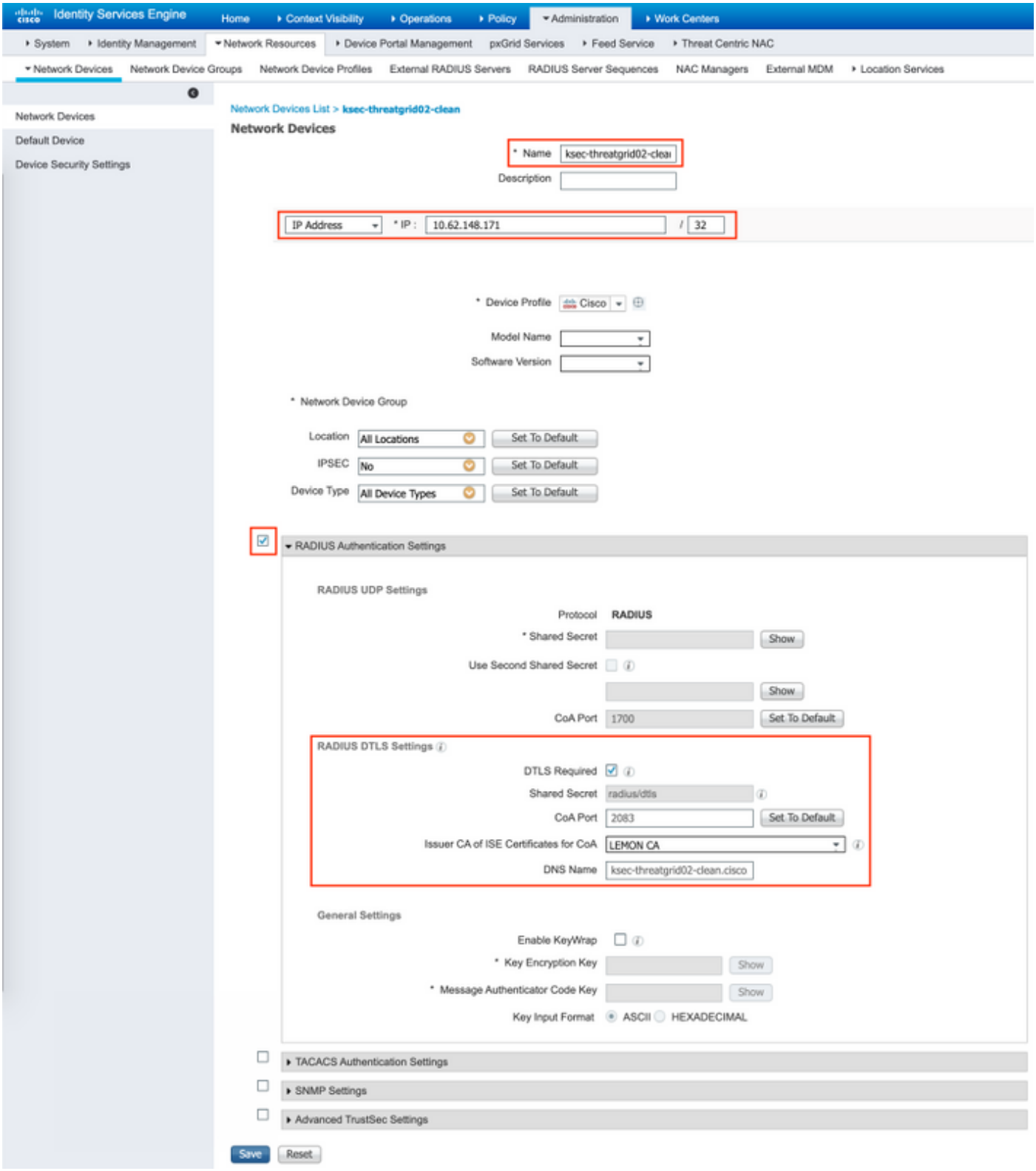
ステップ2:ISEからCA証明書をエクスポートします。

[Administration] > [System] > [Certificates] > [Certificate Management] > [Trusted Certificates]に移動して、CAを見つけ、図に示すように[Export]を選択し、証明書を後でディスクに保存します。



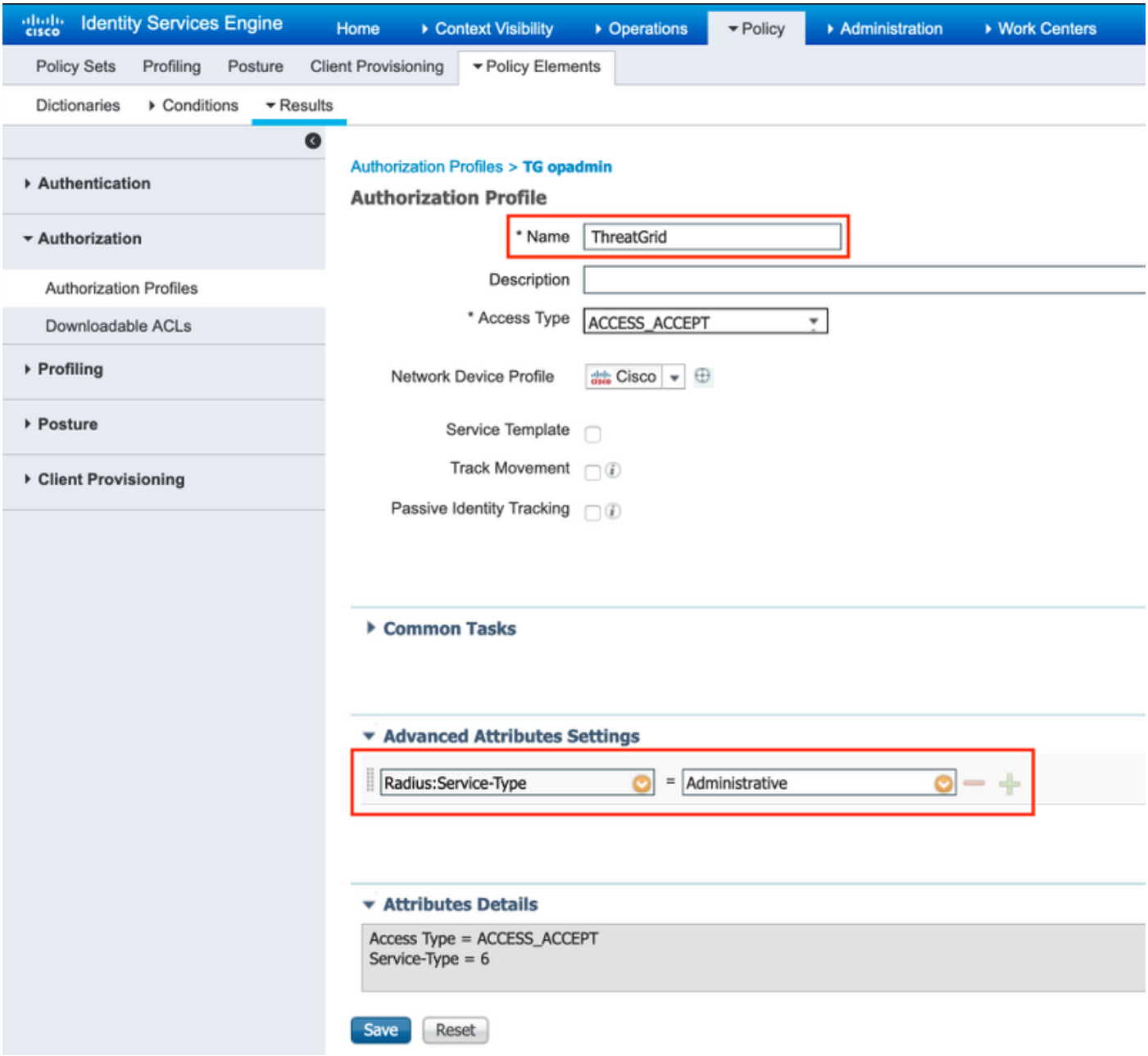
ステップ3：ネットワークアクセスデバイスとしてThreatGridを追加します。

[Administration] > [Network Resources] > [Network Devices] > [Add]に移動して、TGの新しいエントリを作成し、Cleanインターフェイスの**Name**、**IP address**を入力し、図に示すように[DTLS Required]を選択します。下部の**[保存]**をクリックします。



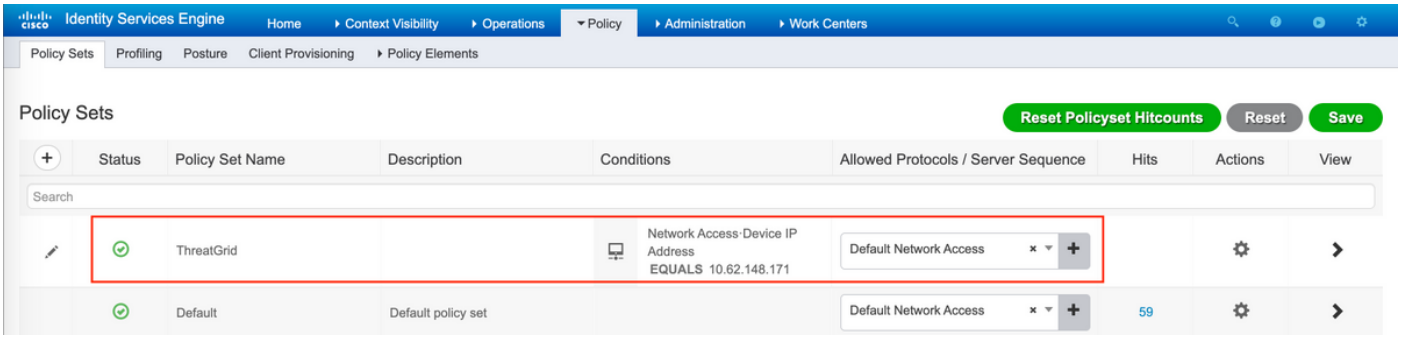
ステップ4：認可ポリシーの認可プロファイルを作成します。

[Policy] > **[Policy elements] > [Results] > [Authorization] > [Authorization Profiles]に移動し、[Add]をクリックします。**名前を入力し、図に示すように**[Advanced Attributes Settings]**を選択し、**[Save]**をクリックします。



ステップ5：認証ポリシーを作成します。

[Policy] > [Policy **Sets]に移動し**、[+]をクリックします。 [Policy Set **Name**]を入力し、条件を[**NAD IP Address**]に設定し、TGのクリーンインターフェイスに割り当て、図に示すように[**Save**]をクリックします。



ステップ6：許可ポリシーを作成します。

[**>**]をクリックして承認ポリシーに移動し、[Authorization Policy]を展開し、[**+**]をクリックして図

に示すように設定します。完了したら、[Save]をクリックします。

ヒント:AdminとUIの両方の条件に一致するすべてのユーザに対して1つの認可ルールを作成できます。

ステップ7:ThreatGridのID証明書を作成します。

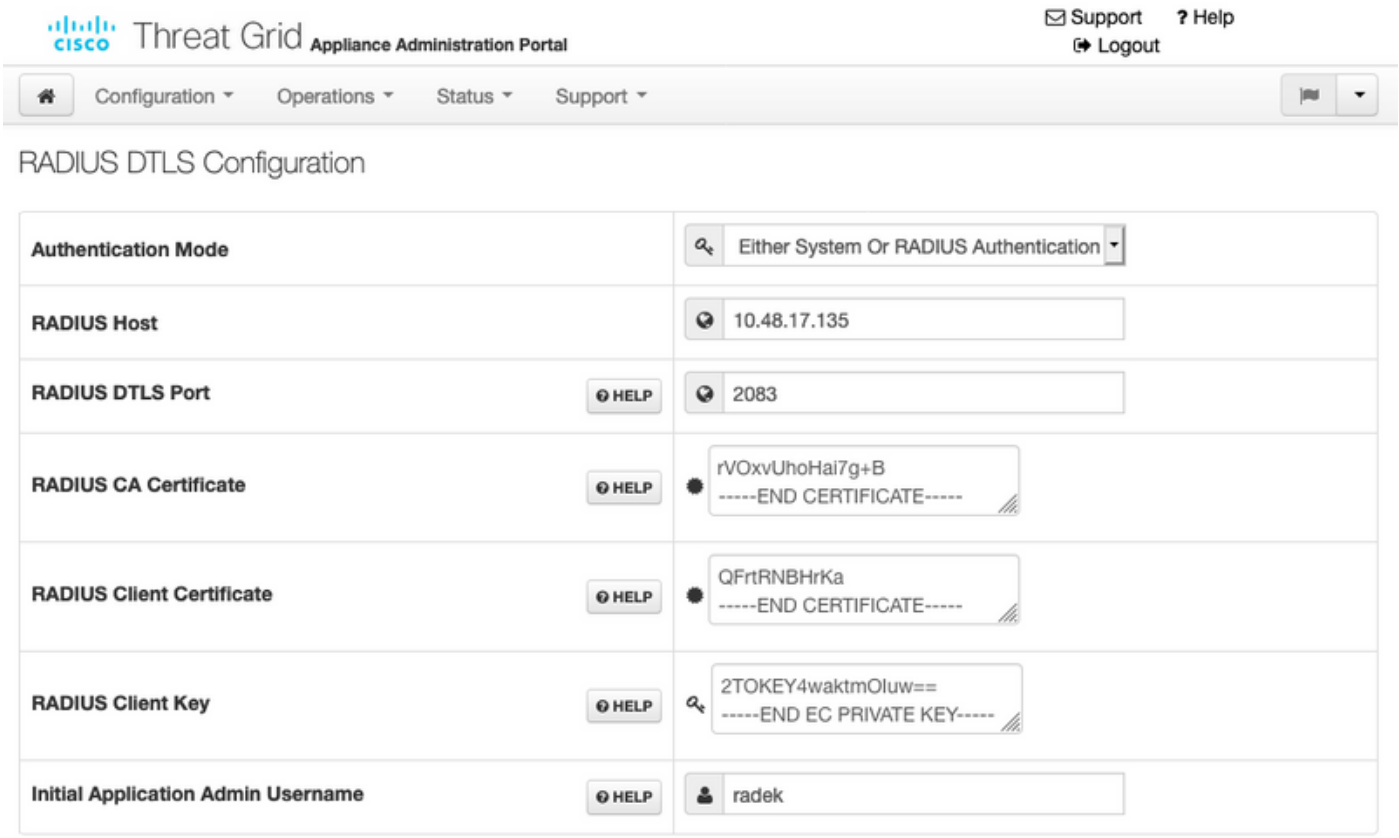
ThreatGridのクライアント証明書は、楕円曲線キーに基づいている必要があります。

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

ISEが信頼するCAによって署名される必要があります。ISE信頼*証明書ストアにCA証明書を追加する方法の詳細について*は、[Import the Root Certificates to the Trusted Certificate Store]ページを確認してください。

ステップ8:RADIUSを使用するようにThreatGridを設定します。

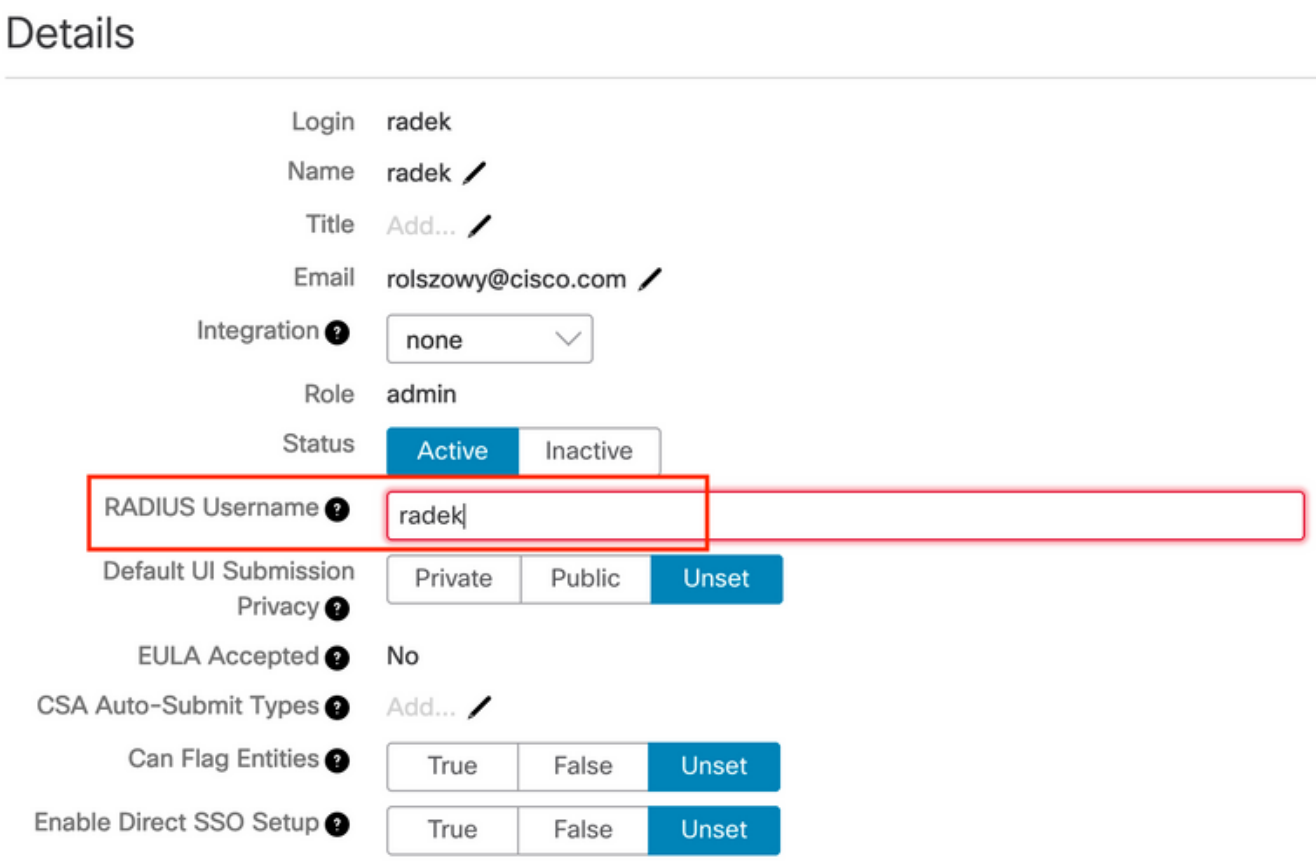
管理ポータルにログインし、[Configuration] > [RADIUS] に移動します。RADIUS CA Certificateに、ISEから収集したPEMファイルの内容を貼り付け、CAから受信したPEM形式の証明書をクライアント証明書に貼り付け、前の手順のprivate-ec-key.pemファイルの内容をに貼貼貼付付にけます。[Save]をクリックします。



注：RADIUS設定を保存した後は、TGアプライアンスを再設定する必要があります。

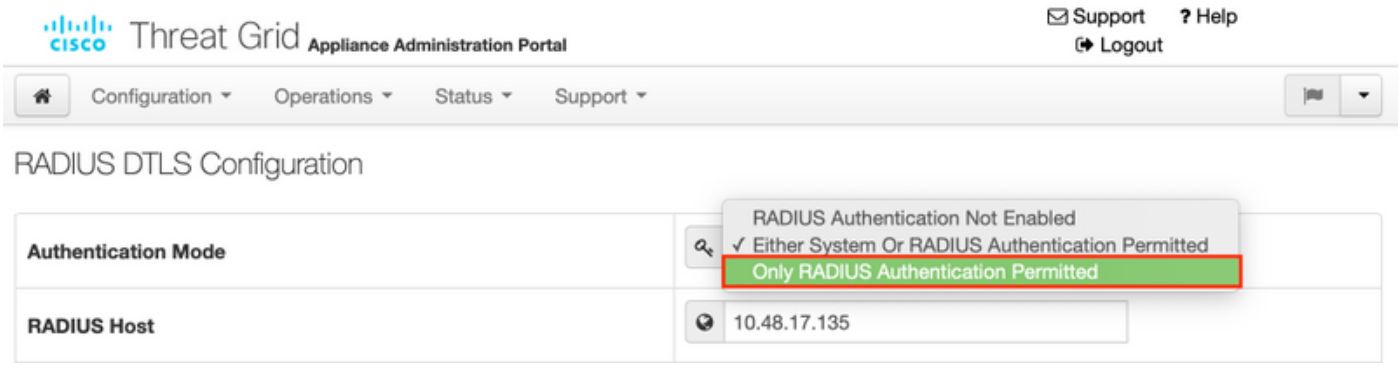
ステップ9：コンソールユーザにRADIUSユーザ名を追加します。

コンソールポータルにログインするには、図に示すように、RADIUSユーザ名属性を各ユーザに追加する必要があります。



ステップ10:RADIUSのみの認証を有効にします。

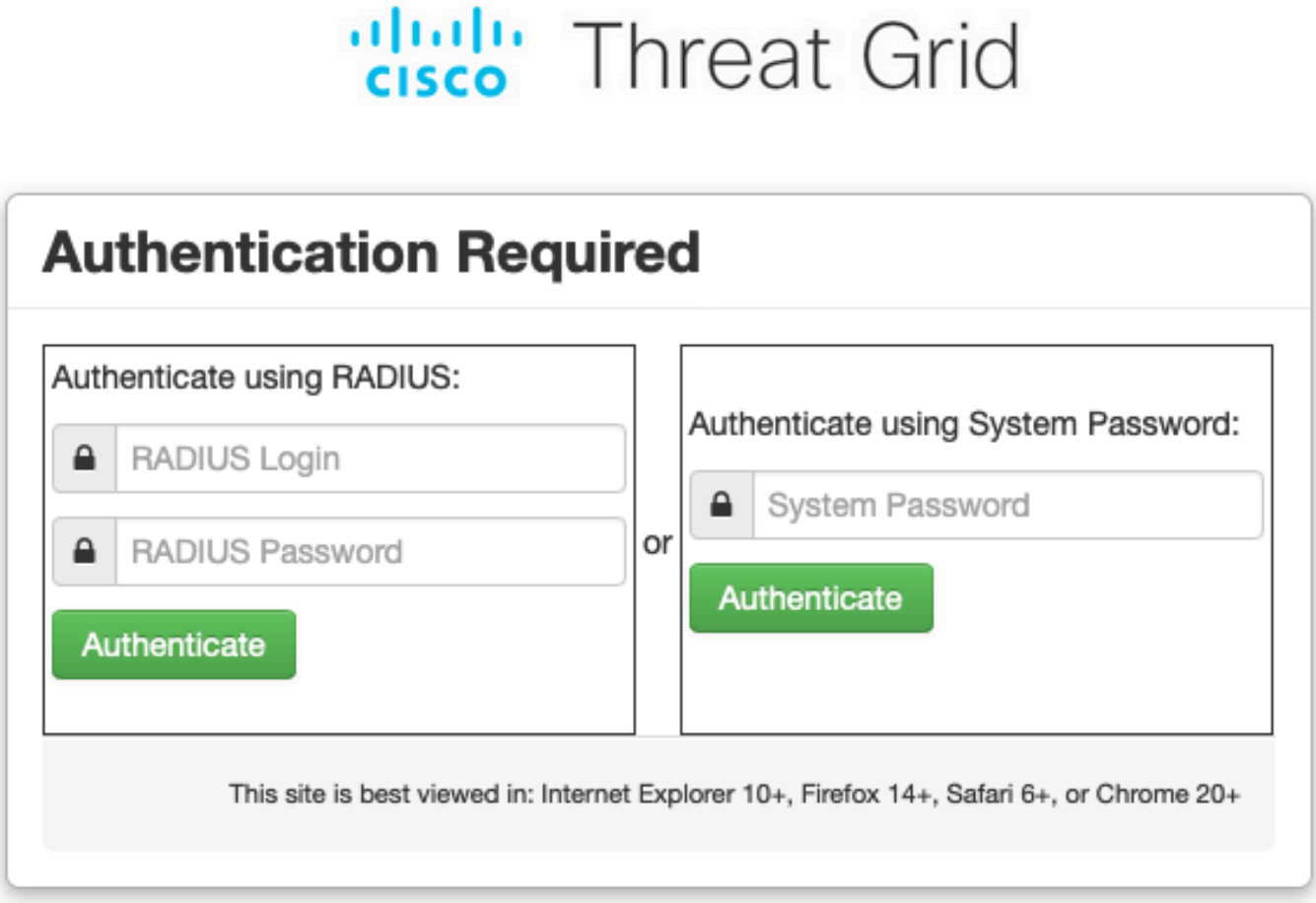
管理ポータルへのログインが成功すると、新しいオプションが表示されます。このオプションは、ローカルシステム認証を完全に無効にし、RADIUSベースの認証だけを残します。

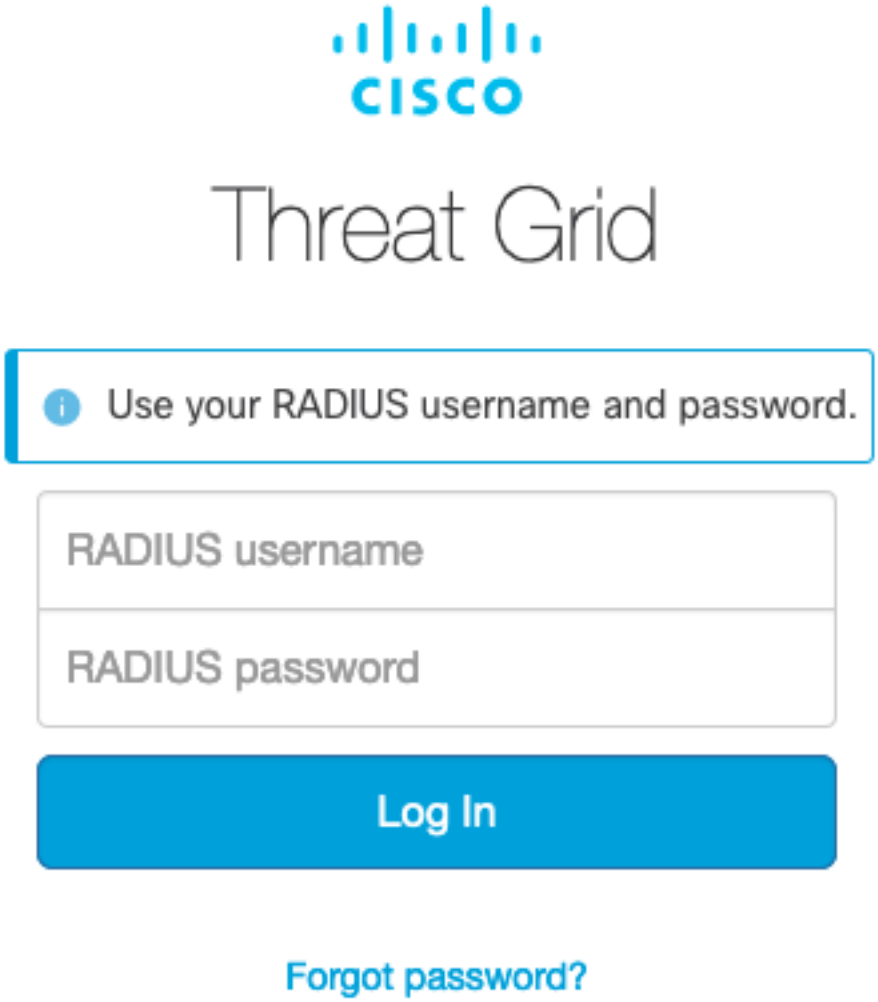


確認

TGを再設定した後、ログオフすると、ログインページはイメージ、管理ポータル、およびコンソ

ールポータルでそれぞれ次のようになります。

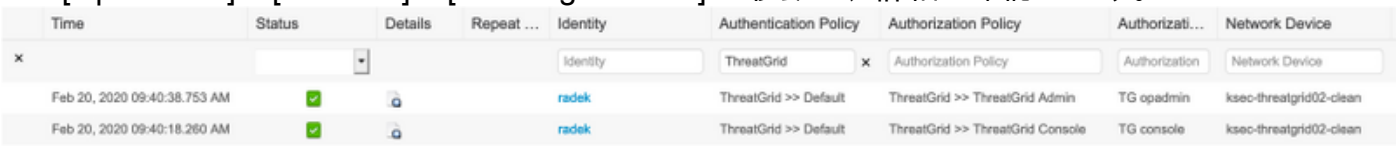




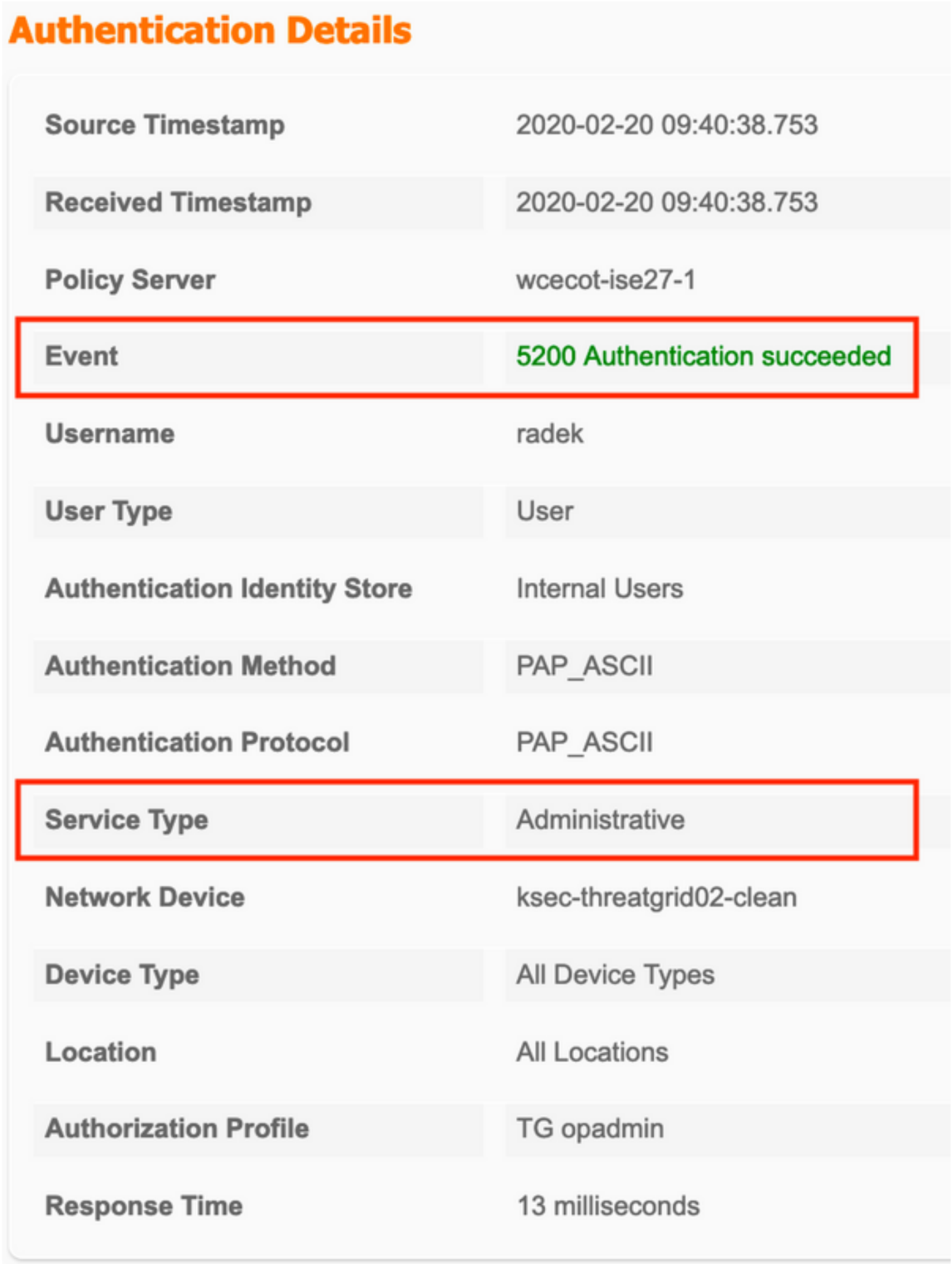
トラブルシュート

問題を引き起こす可能性のあるコンポーネントは3つあります。ISE、ネットワーク接続、およびThreatGrid。

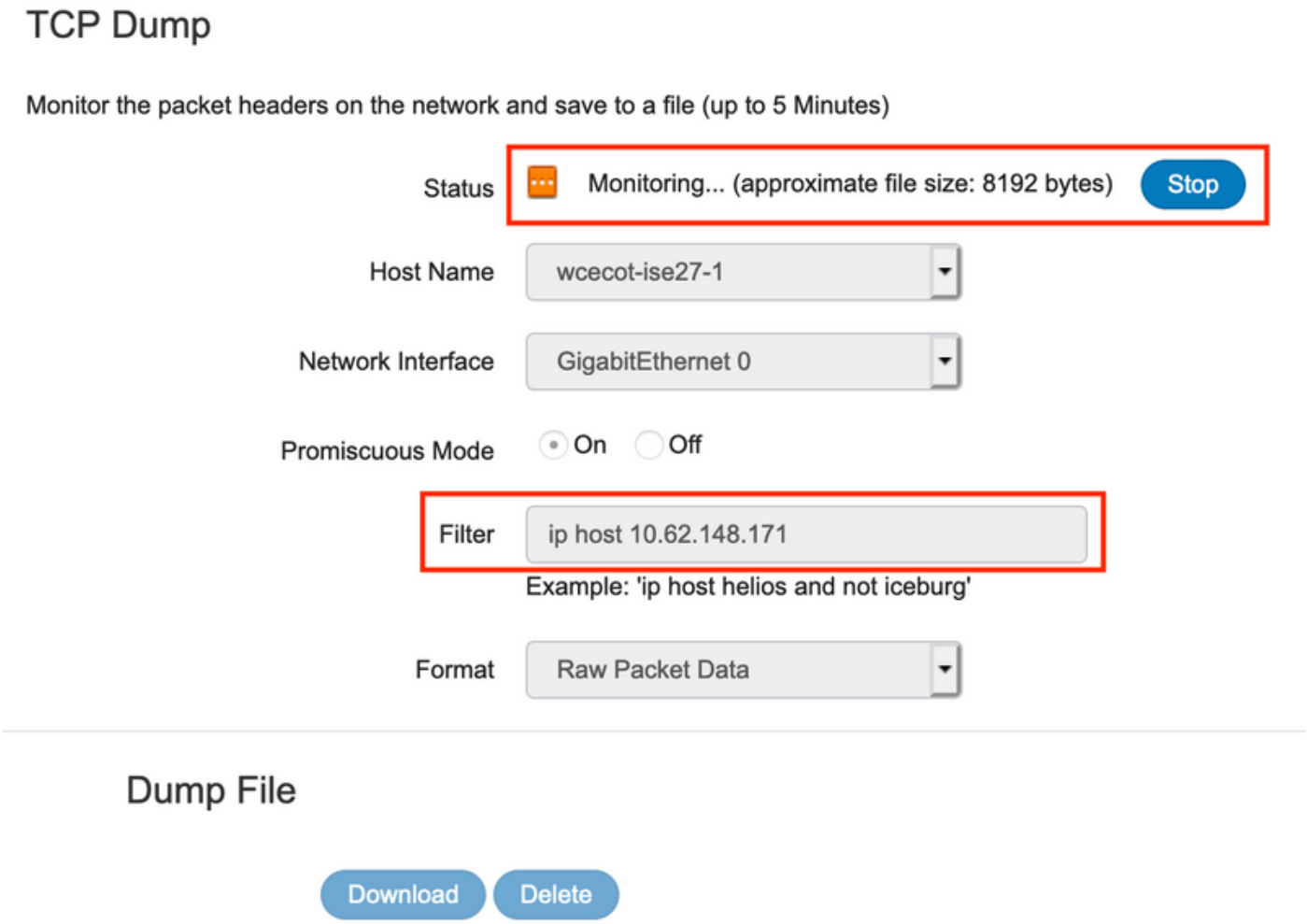
- ISEで、ThreatGridの認証要求にServiceType=Administrativeが返されることを確認します。[Operations] > [RADIUS] > [Live Logs on ISE] に移動し、詳細を確認します。



Time	Status	Details	Repeat ...	Identity	Authentication Policy	Authorization Policy	Authorizati...	Network Device
×				Identity	ThreatGrid ×	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

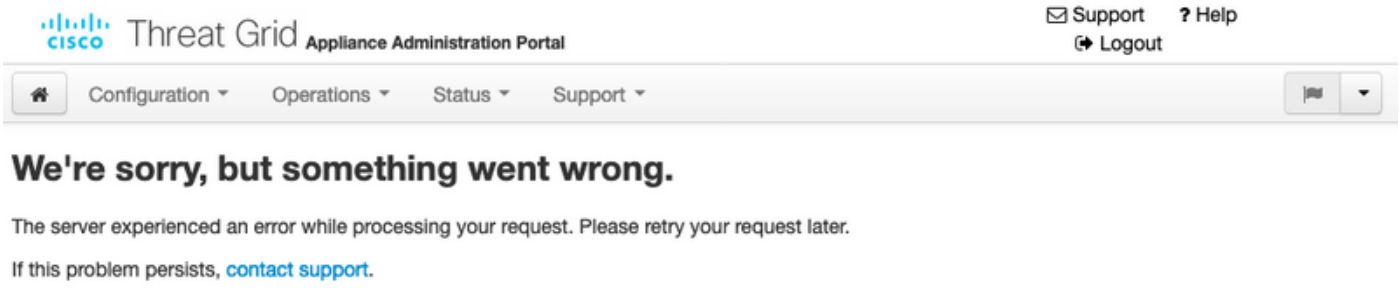


- これらの要求が表示されない場合は、ISEでパケットキャプチャを実行します。[Operations] > [Troubleshoot] > [TCP Dump]に移動し、TGのクリーンなインターフェイスの[Filter]フィールドにIPを入力し、[Start] をクリックして、ThreatGridにログインします。



このバイト数が増加していることが確認できます。詳細については、Wiresharkでpcapファイルを開きます。

- [ThreatGridで保存(Save in ThreatGrid)]をクリックした後に「We're sorry, but things wrong」というエラーが表示され、ページは次のようになります。



つまり、クライアント証明書にRSAキーを最も使用している可能性が高いということです。手順7で指定したパラメータでECCキーを使用する必要があります。