

为控制台和OPadmin门户配置ThreatGrid RADIUS over DTLS身份验证

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[配置](#)

[验证](#)

[故障排除](#)

简介

本文档介绍在ThreatGrid(TG)版本2.10中引入的远程身份验证拨入用户服务(RADIUS)身份验证功能。它允许用户使用存储在身份验证、授权和记帐(AAA)服务器中的凭据登录管理员门户和控制台门户。

在本文档中，您找到配置该功能所需的步骤。

先决条件

要求

- ThreatGrid 2.10版或更高版本
- 支持RADIUS over DTLS身份验证的AAA服务器(draft-ietf-radext-dtls-04)

使用的组件

- ThreatGrid设备2.10
- 身份服务引擎(ISE)2.7

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始(默认)配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

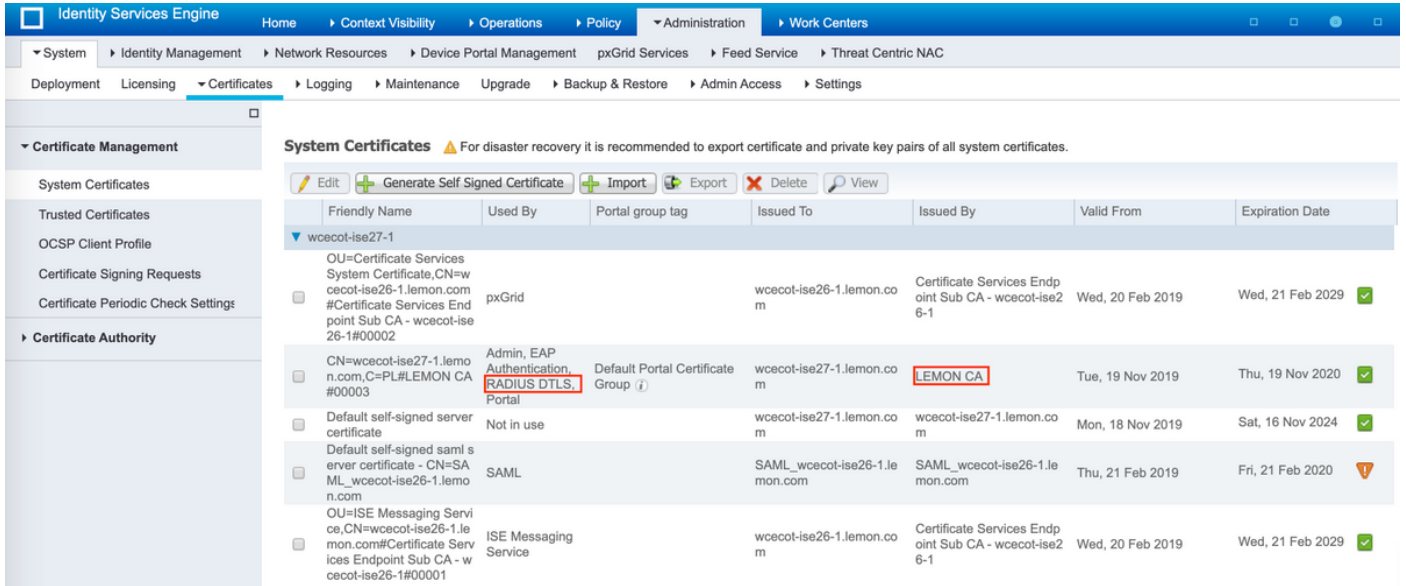
本节提供有关如何为RADIUS身份验证功能配置ThreatGrid设备和ISE的详细说明。

注意：要配置身份验证，请确保端口UDP 2083上的通信允许在ThreatGrid Clean接口和ISE策略服务节点(PSN)之间进行。

配置

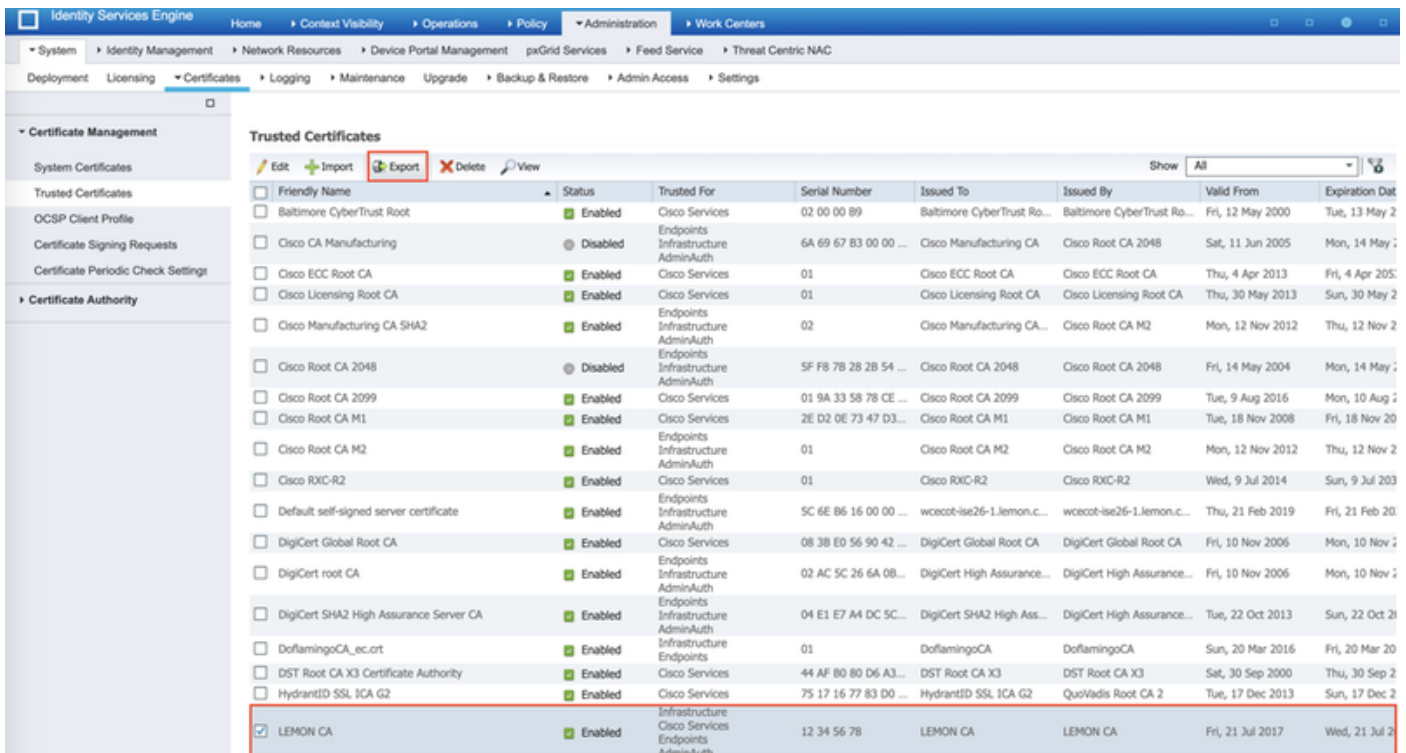
步骤1.准备ThreatGrid证书以进行身份验证。

RADIUS over DTLS使用相互证书身份验证，这意味着需要来自ISE的证书颁发机构(CA)证书。首先检查CA签名的RADIUS DTLS证书：



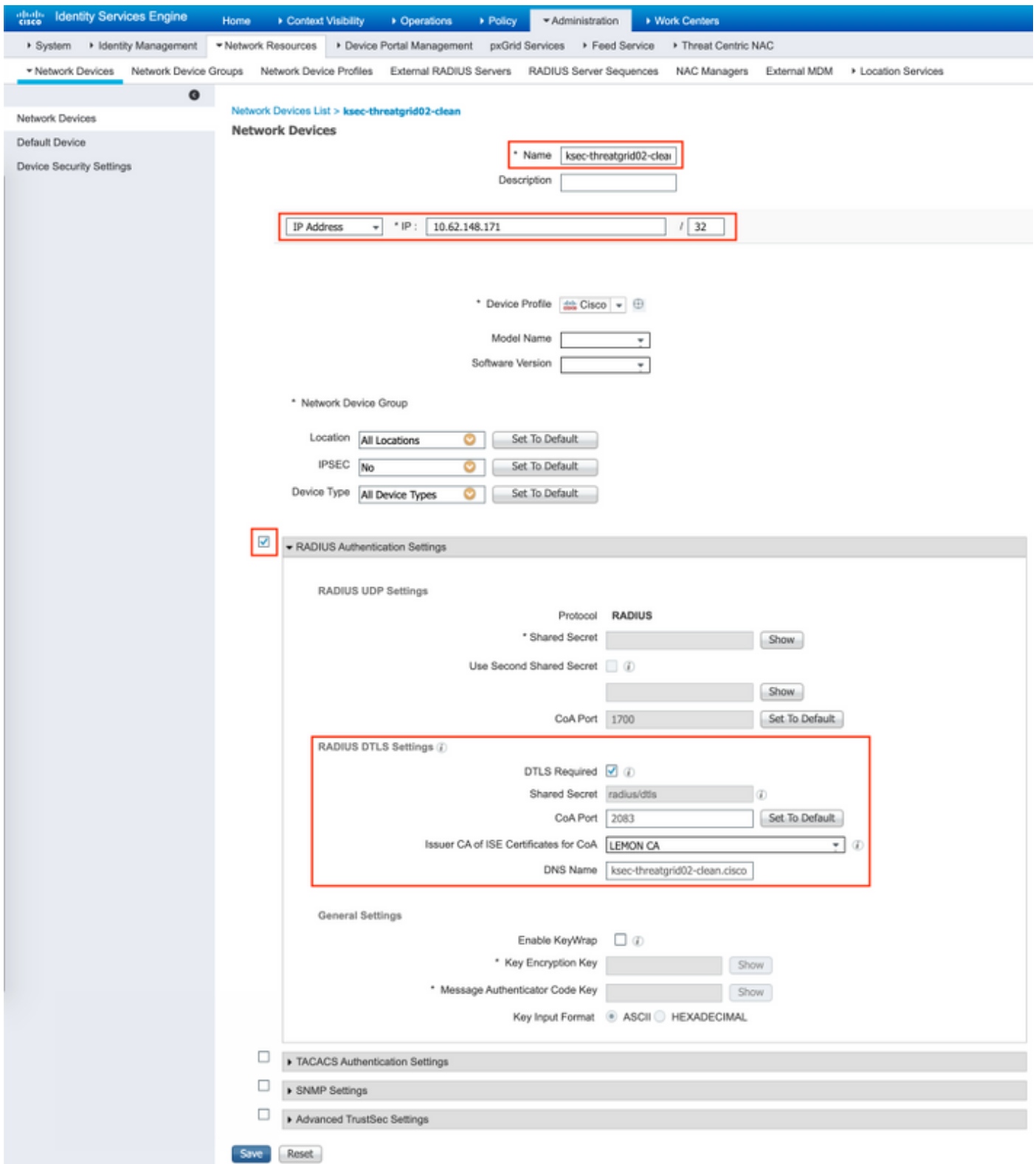
步骤2.从ISE导出CA证书。

导航至管理>System >证书>证书管理>受信任证书，找到CA，选择导出（如图所示），然后将证书保存到磁盘，以备以后使用：



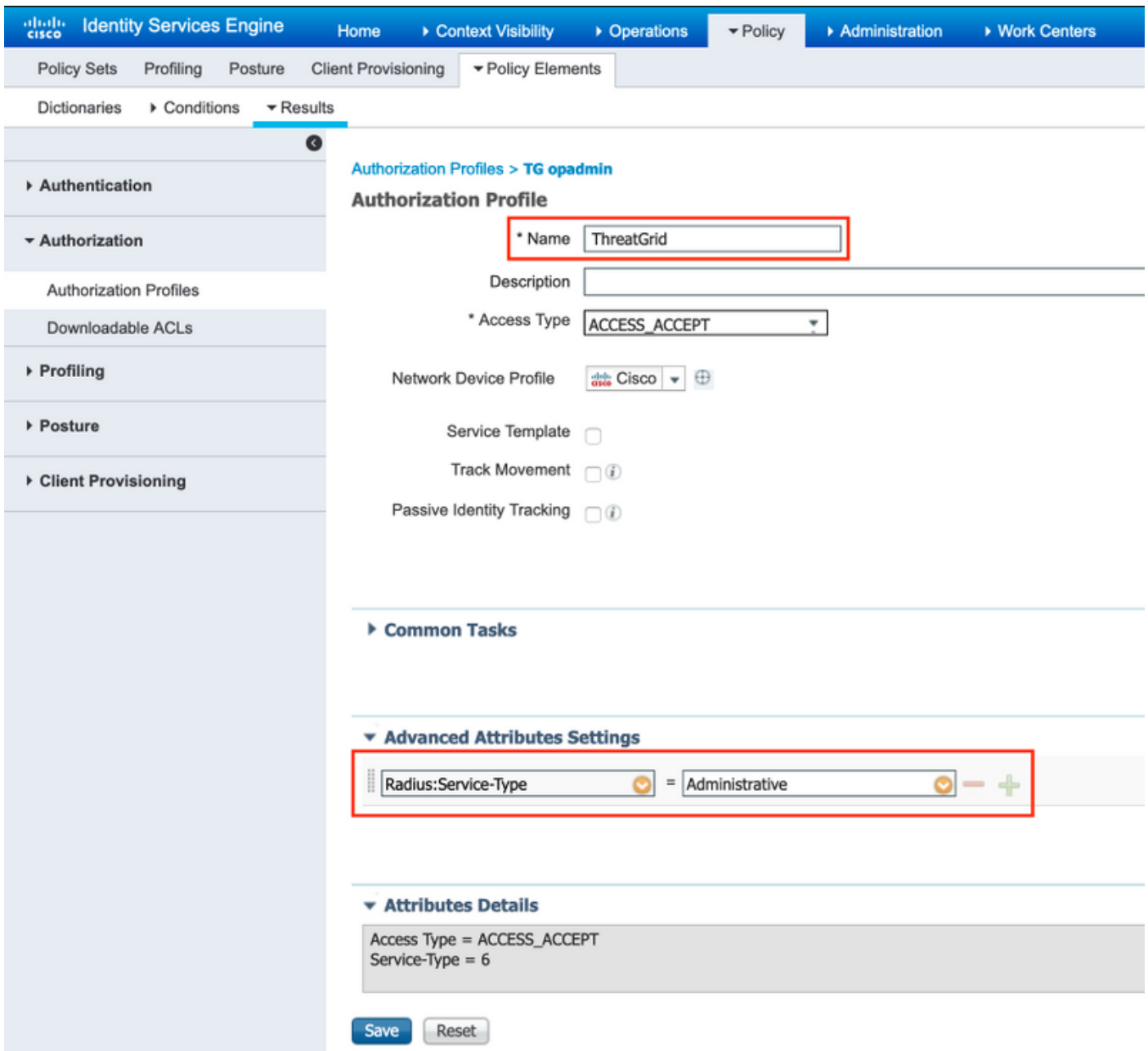
步骤3.将ThreatGrid添加为网络访问设备。

导航至管理>网络资源>网络设备>添加以为TG创建新条目，并输入Clean接口的名称、IP地址，然后选择DTLS Required（如图所示）。单击底部的“保存”：



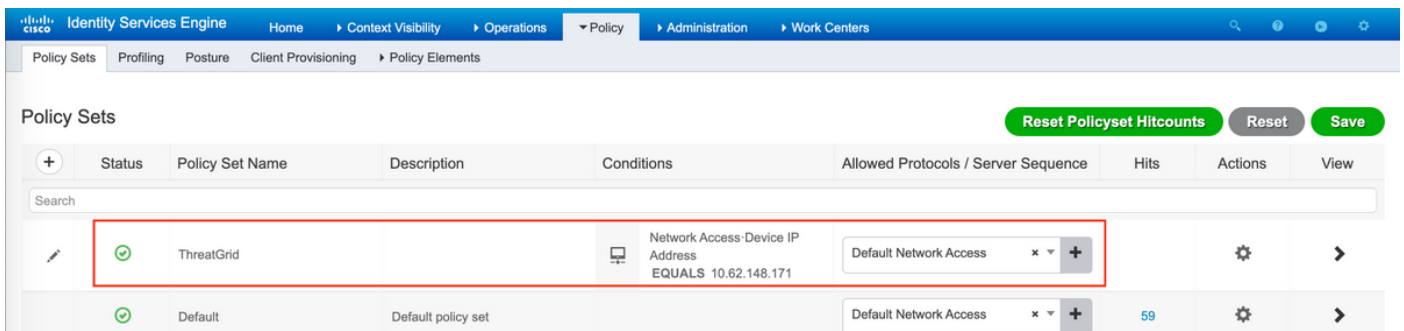
步骤4.为授权策略创建授权配置文件。

导航至策略>Policy元素>结果>授权>授权配置文件，然后单击添加。输入名称并选择高级属性设置（如图所示），然后单击保存：



步骤5.创建身份验证策略。

导航至策略>策略集，然后单击“+”。输入策略集名称，并将条件设置为NAD IP Address（分配给TG的干净接口），单击保存，如图所示：



步骤6.创建授权策略。

单击“>”转到授权策略，展开授权策略，单击“+”并配置如图所示，然后单击“保存”：

Authorization Policy (3)

+	Status	Rule Name	Conditions	Results		Hits	Actions
				Profiles	Security Groups		
	✓	ThreatGrid Admin	Radius-NAS-Identifier EQUALS Threat Grid Admin	xThreatGrid	+	1	⚙️
	✓	ThreatGrid Console	Radius-NAS-Identifier EQUALS Threat Grid UI	xThreatGrid	+	1	⚙️
	✓	Default		xDenyAccess	+	17	⚙️

提示：您可以为同时符合Admin和UI两种条件的所有用户创建一个授权规则。

步骤7.为ThreatGrid创建身份证书。

ThreatGrid的客户端证书必须基于椭圆曲线密钥：

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

它必须由ISE信任的CA签名。选中[将根证书导入受信任证书存储页](#)，了解有关如何将CA证书添加到ISE受信任证书存储的详细信息。

步骤8.将ThreatGrid配置为使用RADIUS。

登录管理员门户，导航至**Configuration > RADIUS**。在RADIUS CA证书中，粘贴从ISE收集的PEM文件的内容，在客户端证书中粘贴从CA接收的PEM格式的证书，在客户端密钥粘贴内容中粘贴从上一步的private-ec-key.pem文件，如图所示。单击**Save**：

Threat Grid Appliance Administration Portal

Support ? Help Logout

Configuration Operations Status Support

RADIUS DTLS Configuration

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

注意：保存RADIUS设置后，必须重新配置TG设备。

步骤9.向控制台用户添加RADIUS用户名。

要登录到控制台门户，必须将RADIUS用户名属性添加到相应用户，如图所示：

Details

Login	radek
Name	radek /
Title	Add... /
Email	rolszowy@cisco.com /
Integration ?	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

步骤10.仅启用RADIUS身份验证。

成功登录管理员门户后，将显示一个新选项，该选项将完全禁用本地系统身份验证并保留仅基于RADIUS的身份验证。

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"/>

验证

重新配置TG后，注销，现在登录页面在映像、管理员和控制台门户中分别显示为：



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?](#)

故障排除

有三个组件可能导致问题：ISE、网络连接和ThreatGrid。

- 在ISE中，确保它将ServiceType=Administrative返回到ThreatGrid的身份验证请求。导航至 **Operations > RADIUS > Live Logs** 并检查详细信息：

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

- 如果您没有看到这些请求，请在ISE上执行数据包捕获。导航至“操作”>“故障排除”>“诊断工具”>“TCP转储”，在TG的干净接口的“过滤器”字段中提供IP，然后单击“开始”并尝试登录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](#)

您必须看到字节数增加。在Wireshark中打开pcap文件以了解详细信息。

- 如果在您单击ThreatGrid中保存后看到错误“很抱歉，但出现了问题”，页面如下所示：



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](#).

这意味着您最可能将RSA密钥用于客户端证书。必须将ECC密钥与步骤7中指定的参数一起使用。