

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

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[コンフィギュレーション](#)

[確認](#)

[トラブルシューティング](#)

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、アカウントインテグ(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。

The screenshot shows the 'System Certificates' page in the Identity Services Engine Administration console. The page title is 'System Certificates' with a warning icon and text: 'For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.' Below the title are buttons for 'Edit', 'Generate Self Signed Certificate', 'Import', 'Export', 'Delete', and 'View'. A table lists certificates with columns: Friendly Name, Used By, Portal group tag, Issued To, Issued By, Valid From, and Expiration Date. The 'LEMON CA' certificate is highlighted in red. Its details are: Friendly Name: CN=wccot-ise27-1.lemo n.com,C=PL#LEMON CA #00003; Used By: Admin, EAP Authentication, RADIUS DTLS, Portal; Portal group tag: Default Portal Certificate Group (j); Issued To: wccot-ise27-1.lemo n.com; Issued By: LEMON CA; Valid From: Tue, 19 Nov 2019; Expiration Date: Thu, 19 Nov 2020.

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date
OU=Certificate Services System Certificate,CN=wccot-ise26-1.lemo n.com,C=PL#LEMON CA #Certificate Services End point Sub CA - wccot-ise 26-1#00002	pxGrid		wccot-ise26-1.lemo n.com	Certificate Services End point Sub CA - wccot-ise2 6-1	Wed, 20 Feb 2019	Wed, 21 Feb 2029
CN=wccot-ise27-1.lemo n.com,C=PL#LEMON CA #00003	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group (j)	wccot-ise27-1.lemo n.com	LEMON CA	Tue, 19 Nov 2019	Thu, 19 Nov 2020
Default self-signed server certificate	Not in use		wccot-ise27-1.lemo n.com	wccot-ise27-1.lemo n.com	Mon, 18 Nov 2019	Sat, 16 Nov 2024
Default self-signed saml s erver certificate - CN=SA ML_wccot-ise26-1.lemo n.com	SAML		SAML_wccot-ise26-1.lemo n.com	SAML_wccot-ise26-1.lemo n.com	Thu, 21 Feb 2019	Fri, 21 Feb 2020
OU=ISE Messaging Servi ce,CN=wccot-ise26-1.lemo n.com#Certificate Servi ces Endpoint Sub CA - wccot-ise26-1#00001	ISE Messaging Service		wccot-ise26-1.lemo n.com	Certificate Services End point Sub CA - wccot-ise2 6-1	Wed, 20 Feb 2019	Wed, 21 Feb 2029

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。

The screenshot shows the 'Trusted Certificates' page in the Identity Services Engine Administration console. The page title is 'Trusted Certificates' with buttons for 'Edit', 'Import', 'Export', 'Delete', and 'View'. A table lists certificates with columns: Friendly Name, Status, Trusted For, Serial Number, Issued To, Issued By, Valid From, and Expiration Date. The 'LEMON CA' certificate is highlighted in red. Its details are: Friendly Name: LEMON CA; Status: Enabled; Trusted For: Cisco Services Endpoints Infrastructure AdminAuth; Serial Number: 12 34 56 78; Issued To: LEMON CA; Issued By: LEMON CA; Valid From: Fri, 21 Jul 2017; Expiration Date: Wed, 21 Jul 2022.

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 2026
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 2026
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 2026
Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure AdminAuth	02	Cisco Manufacturing CA...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2022
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 2026
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 2026
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 2020
Cisco Root CA M2	Enabled	Endpoints Infrastructure AdminAuth	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2022
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 n.c...	wccot-ise26-1.lemo n.c...	Thu, 21 Feb 2019	Fri, 21 Feb 2020
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 2026
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 2026
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 2023
DoflamingoCA_ec.crt	Enabled	Endpoints Infrastructure AdminAuth	01	DoflamingoCA	DoflamingoCA	Sun, 20 Mar 2016	Fri, 20 Mar 2026
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 2026
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 2023
LEMON CA	Enabled	Infrastructure Cisco Services Endpoints AdminAuth	12 34 56 78	LEMON CA	LEMON CA	Fri, 21 Jul 2017	Wed, 21 Jul 2022

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。

The screenshot shows the Cisco Identity Services Engine (ISE) configuration page for a Network Device. The page is titled "Network Devices" and shows the configuration for a device named "ksec-threatgrid02-clean". The configuration includes the following fields:

- Name: ksec-threatgrid02-clean
- Description: (empty)
- IP Address: 10.62.148.171 / 32
- Device Profile: Cisco
- Model Name: (empty)
- Software Version: (empty)
- Network Device Group: (empty)
- Location: All Locations
- IPSEC: No
- Device Type: All Device Types
- RADIUS Authentication Settings (expanded):
 - RADIUS UDP Settings:
 - Protocol: RADIUS
 - Shared Secret: (empty)
 - Use Second Shared Secret: (empty)
 - CoA Port: 1700
 - RADIUS DTLS Settings (checked):
 - DTLS Required:
 - Shared Secret: radius/dtls
 - CoA Port: 2083
 - Issuer CA of ISE Certificates for CoA: LEMON CA
 - DNS Name: ksec-threatgrid02-clean.cisco
 - General Settings:
 - Enable KeyWrap:
 - Key Encryption Key: (empty)
 - Message Authenticator Code Key: (empty)
 - Key Input Format: ASCII
- TACACS Authentication Settings: (unchecked)
- SNMP Settings: (unchecked)
- Advanced TrustSec Settings: (unchecked)

Buttons: Save, Reset

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。

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Policy Sets Profiling Posture Client Provisioning > Policy Elements

Dictionarys > Conditions > Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > TG opadmin

Authorization Profile

* Name ThreatGrid

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

Advanced Attributes Settings

Radius:Service-Type = Administrative

Attributes Details

Access Type = ACCESS_ACCEPT
Service-Type = 6

Save Reset

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。

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Policy Sets Profiling Posture Client Provisioning > Policy Elements

Reset Policyset Hitcounts Reset Save

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

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。

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	⚙️

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ファイルの内容を貼貼貼付付にけます。[Save]をクリックします。

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：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。

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 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

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。

Threat Grid Appliance Administration Portal

Support Help Logout

Configuration Operations Status Support

RADIUS DTLS Configuration

Authentication Mode	<input type="text" value=""/> <input checked="" type="radio"/> Only RADIUS Authentication Permitted
RADIUS Host	<input type="text" value="10.48.17.135"/>

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。



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?](#)

トラブルシューティング

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	
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

- 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。

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](#)

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。

 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](#).

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。