

Configurer ThreatGrid RADIUS sur l'authentification DTLS pour la console et le portail OAdmin

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Configuration](#)

[Vérification](#)

[Dépannage](#)

Introduction

Ce document décrit la fonctionnalité d'authentification RADIUS (Remote Authentication Dial In User Service) introduite dans ThreatGrid (TG) version 2.10. Il permet aux utilisateurs de se connecter au portail Admin ainsi qu'au portail Console avec des informations d'identification stockées dans le serveur AAA (Authentication, Authorization and Accounting).

Dans ce document, vous trouverez les étapes nécessaires pour configurer la fonctionnalité.

Conditions préalables

Conditions requises

- ThreatGrid version 2.10 ou ultérieure
- Serveur AAA prenant en charge l'authentification RADIUS sur DTLS (draft-ietf-radext-dtls-04)

Components Used

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

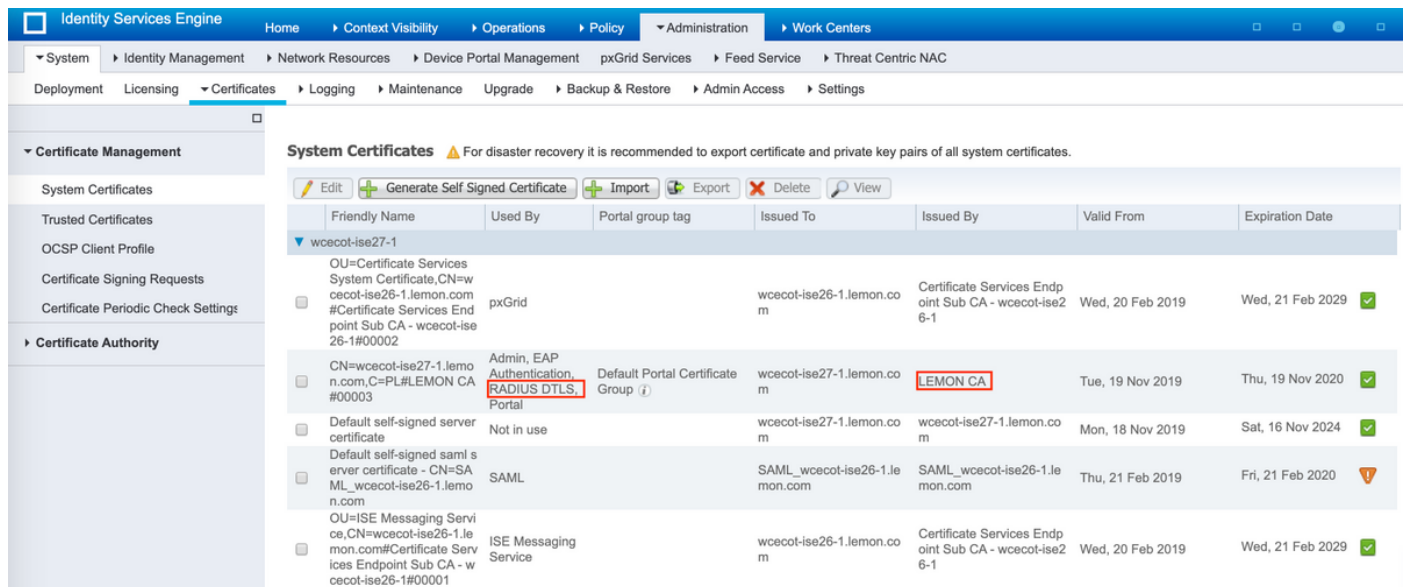
Cette section fournit des instructions détaillées sur la façon de configurer la fonctionnalité ThreatGrid Appliance et ISE pour l'authentification RADIUS.

Note: Afin de configurer l'authentification, assurez-vous que la communication sur le port UDP 2083 est autorisée entre l'interface ThreatGrid Clean et le noeud de service de stratégie ISE (PSN).

Configuration

Étape 1. Préparez le certificat ThreatGrid pour l'authentification.

RADIUS sur DTLS utilise l'authentification mutuelle des certificats, ce qui signifie que le certificat d'autorité de certification (CA) d'ISE est nécessaire. Vérifiez d'abord quel certificat RADIUS DTLS CA a signé :



The screenshot shows the 'System Certificates' page in the ISE Administration console. The page includes a navigation menu on the left and a main content area with a table of certificates. The table has the following columns: Friendly Name, Used By, Portal group tag, Issued To, Issued By, Valid From, and Expiration Date. The 'LEMON CA' certificate is highlighted, and its 'Used By' field is marked with a red box, indicating it is used for RADIUS DTLS authentication.

	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	
▼	wcecot-ise27-1							
<input type="checkbox"/>	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	✓
<input type="checkbox"/>	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	✓
<input type="checkbox"/>	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	✓
<input type="checkbox"/>	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	⚠
<input type="checkbox"/>	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	✓

Étape 2. Exporter le certificat CA à partir d'ISE.

Accédez à **Administration > System > Certificates > Certificate Management > Trusted Certificates**, localisez l'autorité de certification, sélectionnez **Export** comme indiqué dans l'image et enregistrez le certificat sur le disque pour plus tard :

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

Edit
 Import
 Export
 Delete
 View
 Show All

Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date
<input type="checkbox"/> Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 89	Baltimore CyberTrust Ro...	Baltimore CyberTrust Ro...	Fri, 12 May 2000	Tue, 13 May 20...
<input type="checkbox"/> 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...
<input type="checkbox"/> Cisco ECC Root CA	Enabled	Cisco Services	01	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Fri, 4 Apr 2025
<input type="checkbox"/> Cisco Licensing Root CA	Enabled	Cisco Services	01	Cisco Licensing Root CA	Cisco Licensing Root CA	Thu, 30 May 2013	Sun, 30 May 20...
<input type="checkbox"/> Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure AdminAuth	02	Cisco Manufacturing CA...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 20...
<input type="checkbox"/> 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...
<input type="checkbox"/> 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...
<input type="checkbox"/> 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...
<input type="checkbox"/> 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...
<input type="checkbox"/> Cisco RXIC-R2	Enabled	Cisco Services	01	Cisco RXIC-R2	Cisco RXIC-R2	Wed, 9 Jul 2014	Sun, 9 Jul 2023
<input type="checkbox"/> 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...
<input type="checkbox"/> 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...
<input type="checkbox"/> 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...
<input type="checkbox"/> 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...
<input type="checkbox"/> DoflamingoCA_ec.crt	Enabled	Endpoints Infrastructure AdminAuth	01	DoflamingoCA	DoflamingoCA	Sun, 20 Mar 2016	Fri, 20 Mar 20...
<input type="checkbox"/> 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...
<input type="checkbox"/> 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...
<input checked="" type="checkbox"/> LEMON CA	Enabled	Infrastructure Cisco Services Endpoints AdminAuth	12 34 56 78	LEMON CA	LEMON CA	Fri, 21 Jul 2017	Wed, 21 Jul 20...

Étape 3. Ajoutez ThreatGrid en tant que périphérique d'accès au réseau.

Accédez à **Administration > Network Resources > Network Devices > Add** pour créer une nouvelle entrée pour TG et entrez le **Name**, **IP address** de l'interface Clean et sélectionnez **DTLS Required** comme indiqué dans l'image. Cliquez sur **Enregistrer** en bas :

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

Network Devices > Network Device Groups > Network Device Profiles > External RADIUS Servers > RADIUS Server Sequences > NAC Managers > External MDM > Location Services

Network Devices

Default Device

Device Security Settings

Network Devices List > ksec-threatgrid02-clean

Network Devices

* Name ksec-threatgrid02-clean

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 (i)

CoA Port 1700 Set To Default

RADIUS DTLS Settings (i)

DTLS Required (i)

Shared Secret radius/dtls (i)

CoA Port 2083 Set To Default

Issuer CA of ISE Certificates for CoA LEMON CA (i)

DNS Name ksec-threatgrid02-clean.cisco

General Settings

Enable KeyWrap (i)

* Key Encryption Key Show

* Message Authenticator Code Key Show

Key Input Format ASCII HEXADECIMAL

TACACS Authentication Settings

SNMP Settings

Advanced TrustSec Settings

Save Reset

Étape 4. Créez un profil d'autorisation pour la stratégie d'autorisation.

Accédez à **Stratégie > Éléments de stratégie > Résultats > Autorisation > Profils d'autorisation** et cliquez sur **Ajouter**. Entrez **Name** et sélectionnez **Advanced Attributes Settings** comme indiqué dans l'image, puis cliquez sur **Save** :

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main menu includes Policy Sets, Profiling, Posture, Client Provisioning, and Policy Elements. The left sidebar shows a tree view with Authentication, Authorization, Profiling, Posture, and Client Provisioning. The main content area is titled 'Authorization Profiles > TG opadmin' and 'Authorization Profile'. The configuration fields are:

- Name: ThreatGrid (highlighted with a red box)
- Description: (empty)
- Access Type: ACCESS_ACCEPT
- Network Device Profile: Cisco
- Service Template: (checkbox)
- Track Movement: (checkbox)
- Passive Identity Tracking: (checkbox)

 Below the configuration fields is a 'Common Tasks' section and an 'Advanced Attributes Settings' section. In the 'Advanced Attributes Settings' section, a rule is defined: 'Radius:Service-Type' = 'Administrative' (highlighted with a red box). Below this is the 'Attributes Details' section showing 'Access Type = ACCESS_ACCEPT' and 'Service-Type = 6'. At the bottom are 'Save' and 'Reset' buttons.

Étape 5. Créez une stratégie d'authentification.

Naviguez jusqu'à **Policy > Policy Sets** et cliquez sur "+« . Entrez **Nom** du jeu de stratégies et définissez la condition sur **Adresse IP NAD**, attribuée à l'interface propre de TG, cliquez sur **Enregistrer** comme indiqué dans l'image :

The screenshot shows the Cisco Identity Services Engine (ISE) Policy Sets configuration page. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main menu includes Policy Sets, Profiling, Posture, Client Provisioning, and Policy Elements. The left sidebar shows a tree view with Authentication, Authorization, Profiling, Posture, and Client Provisioning. The main content area is titled 'Policy Sets' and has buttons for 'Reset Policyset Hitcounts', 'Reset', and 'Save'. Below the buttons is a table with columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, Hits, Actions, and View. The table contains two rows:

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 x +		⚙️	➔
✓	Default	Default policy set		Default Network Access x +	59	⚙️	➔

 The 'ThreatGrid' row is highlighted with a red box.

Étape 6. Créez une stratégie d'autorisation.

Cliquez sur ">" pour accéder à la stratégie d'autorisation, développez la stratégie d'autorisation,

cliquez sur "+" et configurez comme indiqué dans l'image, une fois que vous avez terminé, cliquez sur **Enregistrer** :

Authorization Policy (3)				Results		Hits	Actions
Status	Rule Name	Conditions	Profiles	Security Groups			
✔	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	⚙️

Conseil : vous pouvez créer une règle d'autorisation pour tous vos utilisateurs qui correspondent aux deux conditions, Admin et UI.

Étape 7. Créez un certificat d'identité pour ThreatGrid.

Le certificat client de ThreatGrid doit être basé sur la clé Elliptic Curve :

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

Il doit être signé par l'autorité de certification en qui ISE fait confiance. Consultez [la page Importer les certificats racines dans le magasin de certificats de confiance](#) pour plus d'informations sur la façon d'ajouter un certificat d'autorité de certification au magasin de certificats de confiance ISE.

Étape 8. Configurez ThreatGrid pour utiliser RADIUS.

Connectez-vous au portail admin, accédez à **Configuration >RADIUS**. Dans RADIUS CA Certificate, collez le contenu du fichier PEM collecté à partir d'ISE, dans Client Certificate, collez le certificat au format PEM reçu de CA et dans Client Key, collez le contenu du fichier private-ec-key.pem à partir de l'étape précédente, comme illustré dans l'image. Cliquez sur **Enregistrer** :

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

Note: Vous devez reconfigurer l'appliance TG après avoir enregistré les paramètres RADIUS.

Étape 9. Ajoutez le nom d'utilisateur RADIUS aux utilisateurs de la console.

Pour vous connecter au portail de la console, vous devez ajouter l'attribut Nom d'utilisateur RADIUS à l'utilisateur respectif, comme indiqué dans l'image :

Details

Login	radek
Name	radek /
Title	Add... /
Email	rolszowy@cisco.com /
Integration	<input type="text" value="none"/>
Role	admin
Status	<input checked="" type="button" value="Active"/> <input type="button" value="Inactive"/>
RADIUS Username	<input type="text" value="radek"/>
Default UI Submission Privacy	<input type="button" value="Private"/> <input type="button" value="Public"/> <input checked="" type="button" value="Unset"/>
EULA Accepted	No
CSA Auto-Submit Types	Add... /
Can Flag Entities	<input type="button" value="True"/> <input type="button" value="False"/> <input checked="" type="button" value="Unset"/>
Enable Direct SSO Setup	<input type="button" value="True"/> <input type="button" value="False"/> <input checked="" type="button" value="Unset"/>

Étape 10. Activez l'authentification RADIUS uniquement.

Une fois la connexion au portail d'administration terminée, une nouvelle option apparaît, qui désactive complètement l'authentification du système local et laisse le seul système 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"/>

Vérification

Une fois que TG a été reconfiguré, déconnectez-vous et maintenant les pages de connexion ressemblent respectivement aux images, à l'administrateur et au portail de console :



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?](#)

Dépannage

Trois composants peuvent poser des problèmes : ISE, connectivité réseau et ThreatGrid.

- Dans ISE, assurez-vous qu'il renvoie ServiceType=Administrative aux demandes d'authentification de ThreatGrid. Accédez à **Operations>RADIUS>Live Logs** sur ISE et vérifiez les détails :

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

- Si ces requêtes ne s'affichent pas, effectuez une capture de paquets sur ISE. Accédez à **Operations>Troubleshoot>Diagnostic Tools>TCP Dump**, fournissez l'adresse IP dans le champ Filter de l'interface **propre du TG**, cliquez sur **Start** et essayez de vous connecter à

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](#)

Vous devez voir augmenter le nombre d'octets. Ouvrez le fichier pcap dans Wireshark pour plus d'informations.

- Si vous voyez l'erreur « Désolé, mais un problème est survenu » après avoir cliqué sur Enregistrer dans ThreatGrid et que la page ressemble à ceci :

 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](#).

Cela signifie que vous avez probablement utilisé la clé RSA pour le certificat client. Vous devez utiliser la clé ECC avec les paramètres spécifiés à l'étape 7.