

DTLS ربيع ThreatGrid RADIUS ةقداصم نيوكت OPadmin و مكحتلا ةدحو لخدم

تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[نيوكتلا](#)

[نيوكتلا](#)

[ةحصللا نم ققحتلا](#)

[اهحالص او عااطخألا فاشكتسا](#)

ةمدقملا

(RADIUS) ممدختسملا ةمدخي في دعب نع ةقداصملا ببلط ةقداصم ةزيم دنننسملا اذه فصلي ليجستب نيومدختسملا ل حمسي وهو. ThreatGrid (TG) نم 2.10 رادصإلا في اهميدقت مت يتلا ةقداصملا مداخل في ةننخمل دامتعالا تانايب عم مكحتلا ةدحو ةباوبو ةرادإلا لخدم يلا لوخدلا ةقداصملا (AAA) ةبساحملاو ضيوفتلاو.

ةزيملا نيوكتلا ةيرورضلا تاوطخل دجت، دنننسملا اذه في.

ةيساسألا تابلطتملا

تابلطتملا

- لعلأ وأ 2.10 رادصإلا ThreatGrid
- مداخل DTLS ربيع RADIUS ةقداصم معددي ذلأ AAA مداخل (draft-ietf-radext-dtls-04)

ةمدختسملا تانوكملا

- زايج ThreatGrid 2.10
- Identity Services Engine (ISE)، رادصإلا 2.7

ةصاخ ةيلمعم ةئيب في ةدوجوملا ةزهجالا نم دنننسملا اذه في ةدراولا تامولعملل ءاشنإ مت تناك اذإ. (يضا رتفا) حوسمم نيوكت دنننسملا اذه في ممدختسملا ةزهجالا عيمج تادب رما يال لمحتملا ريثاتلل كمهف نم دكأتف، ةرشابم كتكباش.

نيوكتلا

ةزيملا ISE و ThreatGrid زايج نيوكت ةيفيك لوح ةيليصفت تاداشرا مسقلا اذه مدقي RADIUS ةقداصم.

UDP 2083 ذفنملا يلع لاصتالاب حامسلا نم دكأت، ةقداصملا نيوكت لجا نم: **ةظالم**

ISE (PSN) ةسايس ةمدخ ةدقعو ةفيظنل ThreatGrid ةهجاو ني

نيوكتلا

ةقداصم لل ThreatGrid ةداهش دادع 1. ةوطخل

عجرملا ةداهش نأ ينعى امم ةلدابتملا تاداهش لل ةقداصم DTLS ربع RADIUS مدختسي CA نم ةعقووملا RADIUS DTLS ةداهش نم الوا ققحت . ةبولطم ISE نم (CA) قدصملا

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... #Certificate Services End point Sub CA - wccot-ise26-1#00002	pxGrid		wccot-ise26-1.lemo.com	Certificate Services End point Sub CA - wccot-ise26-1	Wed, 20 Feb 2019	Wed, 21 Feb 2029
CN=wccot-ise27-1.lemo... C=PL#LEMON CA #00003	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group (j)	wccot-ise27-1.lemo.com	LEMON CA	Tue, 19 Nov 2019	Thu, 19 Nov 2020
Default self-signed server certificate	Not in use		wccot-ise27-1.lemo.com	wccot-ise27-1.lemo.com	Mon, 18 Nov 2019	Sat, 16 Nov 2024
Default self-signed saml server certificate - CN=SAML_wccot-ise26-1.lemo.com	SAML		SAML_wccot-ise26-1.lemo.com	SAML_wccot-ise26-1.lemo.com	Thu, 21 Feb 2019	Fri, 21 Feb 2020
OU=ISE Messaging Service,CN=wccot-ise26-1.lemo.com#Certificate Services End point Sub CA - wccot-ise26-1#00001	ISE Messaging Service		wccot-ise26-1.lemo.com	Certificate Services End point Sub CA - wccot-ise26-1	Wed, 20 Feb 2019	Wed, 21 Feb 2029

ISE نم قدصملا عجرملا ةداهش ري دصت 2. ةوطخل

عجرملا ناكم دح ،اهب قووثوم تاداهش > تاداهش ةراد > تاداهش > ماظن > ةرادا يلى لقتنا : قجال تقول صرقلا يلع ةداهشال ظفح مث ،ةروصلال يف حضوم وه امك ري دصت دح ،قدصملا

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 2026
Cisco Root CA 2048	Disabled	Endpoints Infrastructure AdminAuth	5F 8B 7B 2B 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 2026
Cisco Root CA M2	Enabled	Endpoints Infrastructure AdminAuth	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2026
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.c...	wccot-ise26-1.lemo.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 4A DC 5C...	DigiCert SHA2 High Ass...	DigiCert High Assurance...	Tue, 22 Oct 2013	Sun, 22 Oct 2026
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 80 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 2026
LEMON CA	Enabled	Endpoints Infrastructure AdminAuth	12 34 56 78	LEMON CA	LEMON CA	Fri, 21 Jul 2017	Wed, 21 Jul 2026

ةكبشلال يلى لوصو زاهجك ThreatGrid ةفاض 3. ةوطخل

لخداؤو TG ل ديدج ل اخدا عاشن ا ل فاضا > ةك بشلا ةزهجا > ةك بشلا دراوم > ةرادا ا ل ل قتنا قوف رقنا . ةروصلا يف حضورم وه امك بولطملا DTLS دحو ةفيظنلا ةهجاو ل IP ناوع ، مسالا لفسالا يف "ظفح

The screenshot displays the configuration interface for a network device in Cisco ISE. The main configuration area is titled "Network Devices" and shows the following settings:

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

Other sections like TACACS Authentication Settings, SNMP Settings, and Advanced TrustSec Settings are collapsed.

ل. لي وختلا جهنل لي وخت في رعت فلم عاشن ا ل 4. ةوطخل

رقناو لي وختلا تافي صوت > لي وختلا > جئاتنلا > ةسايسلا رصانع > ةسايسلا ا ل ل قتنا رقناو ةروصلا يف حضورم وه امك ةمدقتملا صئاصللا تاداعا دحو مسالا ل خدا . ةفاض ا ل ل قتنا لفسالا يف "ظفح

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.

ةقداصم ةسايس ءاشنإ 5 ةوطخلإ

مقوجهنلإ ةعومجم مسا لخدأ "+ قوف رقناو ةسايسلا ءاعومجم > ةسايسلا إلإ لقتنا وه امك ظفح قوف رقنا، ةف يظنلإ TG ةهجاو إلإ نيعملا، NAD IP Address إلإ طرشلإ نيعت ب ةروصلإ يف حضورم:

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 Policy Sets. 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.

ل يوقت ةسايس ءاشنإ 6 ةوطخلإ

مق مٹ "+ قوف رقناو، ل يوقتلا جهن عيسوتب مقو، ل يوقتلا جهن إلإ لاقنلإ > قوف رقنا

ظفح قوف رقنا ءاهت نال دعب ، ءروصلال يف حضوم وه امك نيوكت لال

Authorization Policy (3)				Results	Security Groups	Hits	Actions
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	⚙️	

الك قباطت نيذال ني مدخت سمل ءفاكل ءءاو ضيوفت ءءاق ءاشن انك نمي : حيملت
مدخت سمل ءءاو لوؤس مل او نيطرش لال

ThreatGrid ل ءوه ءءاهش ءاشن ان 7. ءوطلال


يواضي بلل ينحن مل اءات فم لال ThreatGrid ليم ءءاهش دن تست نأ بءي

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

داري تسلا نم ققحت . ISE اءب قءي يءالا ءءازنلا ءئيءه لبق نم اءيل ءي ققوت لال مءي نأ بءي
لوح تامول ءمل نم ءي زم لعل لوصء لال [ءب قوءوم لال ءءاهش لال نءءم](#) ءءفص [للال رءءلال ءءاهش لال](#)
ءب قوءوم لال ISE ءءاهش نءءم لال قءصم ءءرم ءءاهش ءفاضا ءي ءي

RADIUS مءءءءال ThreatGrid نيوكت 8. ءوطلال

RADIUS ءءاهش يف . RADIUS > نيوكت لال لال لقتنا ، لوؤس مل لءءم لال لوءءل لءءسءب مق
ءصءال PEM ءقس نم لال ءءاهش لال يف ، ISE نم ءءي مءءءم ءي ءءال PEM فلم يءءءم قصل لال CA
فلم ب صءال لءم ءءال ءءاءءم قصل يءءءم يف و CA نم ءم لءءم لال ءءاهش قصل ب
ظفح ءقءقء . ءروصلال يف حضوم وه امك ءقءقءال ءوطلال نم private-ec-key.pem



[Support](#) [? Help](#)
[Logout](#)

Configuration ▾
Operations ▾
Status ▾
Support ▾

RADIUS DTLS Configuration

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

RADIUS تادادع| ظفح دعب TG زاھج نيوكت اداع| بجي: ةظحالم

مكحتللا ةدحويمدختسمل RADIUS مدختسم مسا ةفاضل. 9 ةوطخلل

لل RADIUS مدختسم مسا ةفاضل بجي، مكحتللا ةدحو لخدم لىل لوخدلل ليجستل
ةروصلل يف حضوم وه امك صاخلل مدختسمل

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

طقف RADIUS ةقداصم نيكمتم. 10 ةوطخلل

ماظنلل ةقداصم لطي يذلاو، ديدج راخي رهظي، لوؤسمل لخدم لىل حجائل لوخدلل ليجست دعب
لل RADIUS لىل ةدنتسم ةقداصم طقف كرتي و امامت لىل حمل

Threat Grid Appliance Administration Portal

Support Help Logout

Configuration Operations Status Support

RADIUS DTLS Configuration

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

ةحصلل نم ققحتلل

وه امك تاحفصلل لىل لوخدلل ليجست ودبي نآلاو، جورخلل ليجستب مق، TG نيوكت اداع| دعب

يلاوتلا لىل ع مكحتلا ةدحوو لوؤس مل او روصلا لخدم يف لاجلا



Authentication Required

Authenticate using RADIUS:

RADIUS Login

RADIUS Password

Authenticate

or

Authenticate using System Password:

System Password

Authenticate

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



Threat Grid

Use your RADIUS username and password.

RADIUS username

RADIUS password

Log In

[Forgot password?](#)

اهحال صإو عاطخأل فاشكتسا

ThreatGrid و ةكبشلا لاصتاتاو ISE: لكاشم ببست نأ نكمي تانوكم ةثالث كانه

- ThreatGrid ةقداصم تابلط لىإ ServiceType=Administrative عجرت اهنأ نم دكأت، ISE يف لىإ صافاتلا ددحو ISE لىع ةرشابملا تالچسلا >RADIUS> تايلمعلا لىإ لقتنا

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

- إلى لوقتنا. ISE إلى عمزح طاقنتلا كيلي عف، تا بل لطلال هذه ىرت نكت مل اذا في IP ل قح رفوو، TCP غيرفت >صخيشتلا تاودأ >اهاحالصإو اءاطخأل فاشكتسأ >اىلعملال ليحست لواحو وءب قوف رقنا، TG ب ءصاخال فيظنتلا ءهءاب صاخال ءيفصتلا لماع

ThreatGrid لوجن

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

لوصل ل Wireshark في PCAP فلم حت فا. اهتدايز تمت تي تال تي ابال تادحو ددع ىرت نأ بجي تامولعمل نم ديزم ىلع.

- حت فصل او "ThreatGrid" في ظفح" قوف رقن ل ادعب "ام أطخ شح نكلو، فسأن" أطخل تي أر اذا ىلى امك ودبت

 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](#).

حات فم مادختس! بجي. ليمعلا ةداهشل RSA حات فم تم دختسأ دق حجراأل ىلع كنأ ينعي اذهو 7. ةوطخلال في ةدحمل تاملعمل عم ECC

ةمچرتل هذه لوح

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تمچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبلاو
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل مهتغب
Cisco يلخت. فرتم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىلإ أمئاد ةوچرلاب يصوت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارل) يلصلأل يزي لچنل دن تسمل