

ISE و ISE مادختساب ةزهجال ةرادال APIC نيوكت TACACS+

تايوتحمل

[ةمدقمل](#)

[ةيساسال تابلطتمل](#)

[تابلطتمل](#)

[ةمدختسمل تانوكمل](#)

[نيوكتل](#)

[ةكبشلال ليطيطختل مسرل](#)

[ةقداصمل اعاج](#)

[APIC نيوكت](#)

[ISE نيوكت](#)

[ةحصلل نم ققحتل](#)

[اهجالص او اعاطخال فاشكتسا](#)

ةمدقمل

لوكوتورب عم لوؤسمل ايمدختسم ةقداصمل ISE عم APIC جم د اعاج دن تسمل اذه فصلي TACACS+.

ةيساسال تابلطتمل

تابلطتمل

ةيلاتل عيضاوملاب ةفرعم كيدل نوكت ناب Cisco ي صوت:

- (APIC) ةيساسال ةينبال ةسايس قيبطتب ةصاخال مكحتل ةدحو
- (ISE) ةيوهال فشك تامدخ كرم
- Tacacs لوكوتورب

ةمدختسمل تانوكمل

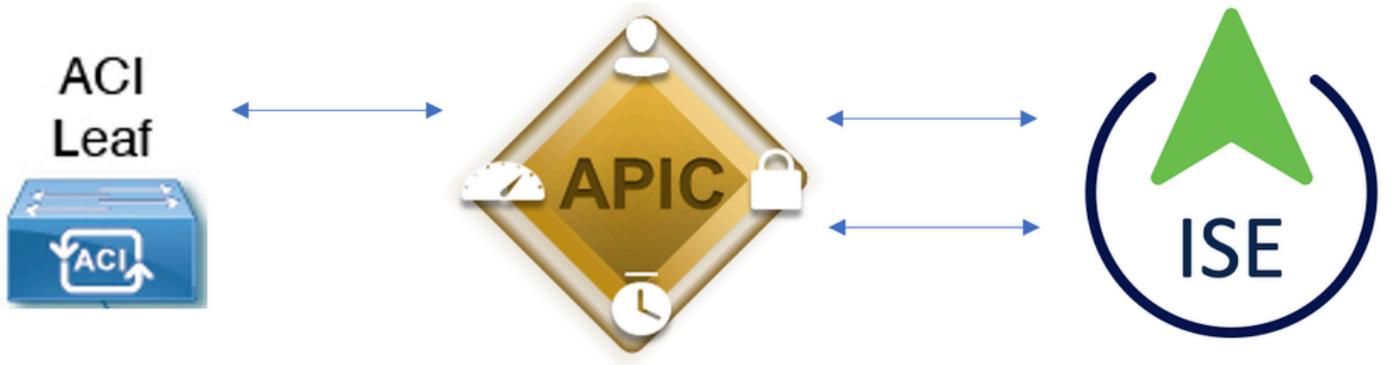
ةيلاتل ةيدامل تانوكمل او جم اربال تارادصل ل دن تسمل اذه يف ةدراول تامولعمل دن تست:

- APIC رادصلال 4.2(7u)
- 1 ححصت 3.2 رادصلال ISE

ةصاخ ةيلمعم ةئيبي يف ةدوومل ةزهجال نم دن تسمل اذه يف ةدراول تامولعمل عاشن اتم تناك اذا. (يضارتفا) حوسمم نيوكتب دن تسمل اذه يف ةمدختسمل ةزهجال عيمج تادب رمايال لم تحملل ريثاتلل كمهف نم دكأتف، ليغشتللا ديق كتكبش

نيوكتلا

ةكبش لل يطي طختلا مسرلا



لمكتلل يطي طختلا مسرلا

ةقداصملا ءارحإ

ل. لوؤسملا مدختسملا تاغوسم مادختساب APIC قي بطت ىلإ لوخدلا ل.جس. 1 ةوطخلا

وأ اي لحم اهتحص نم ققحتلا او دامتعالا تانايب ليغشتب ةقداصملا ةي لمع موقت. 2 ةوطخلا
م Active Directory ةمدخ لالخنم

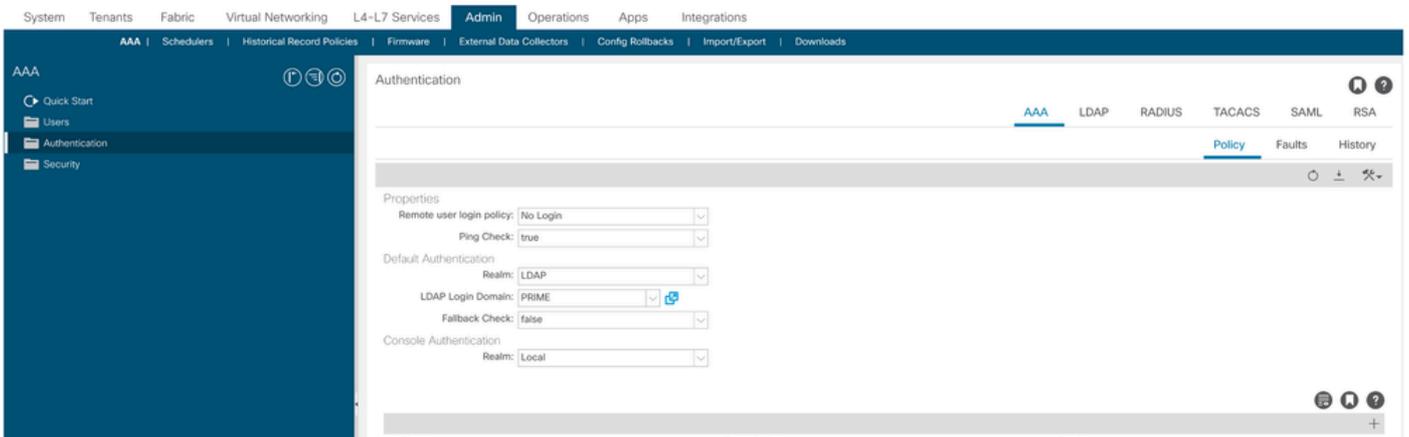
APIC ىلإ لوصولي لوختل حامس ةمزح ISE لسري، ةقداصملا حاجن درجمب. 3 ةوطخلا

احجان ةقداصملا ارشابم ال.جس ISE ضرعي. 4 ةوطخلا

نم عزج يه يتلا ةيفرطال تالوحملا ىلإ TACACS+ نيوكت خسنب APIC موقت: ةظالم
ةينبل.

نيوكت APIC

لوخد ليحست لاجم ءاشنال ةنوقيأ رتخا وAAA > Authentication > AAA ىلإ لقتنا. 1 ةوطخلا
ديج.



APIC لوخد ليحست لوؤسم نيوكت

ءاشنإل نڤرفوم قوف+رقن او دڤدل لؤخدلا لڤجست ل اءم ل ملاءو مسا دڤدءت ب مق 2 ةوطءلا دڤءرفوم.

Create Login Domain



Name:

Realm:

Description:

Providers:

Name	Priority	Description
------	----------	-------------

Cancel

Submit

APIC لؤءد لڤجست لوؤسم

Providers:

Name	Priority	Description
<input type="text" value="select an option"/>	<input type="text"/>	<input type="text"/>

Create TACACS+ Provider

Update Cancel

APIC TACACS رفوم

ءهن ةومءم رءءاو، كرتشم رس فڤرءت ب مقو، فڤضم ل مسا و IP ISE ناوع دء 3 ةوطءلا لؤخدلا لڤجست لوؤسم ىلإ TACACS+ رفوم ةفاضل Submit رءن ا (EPG) ةرادلل ةڤاهنل ةطقن.

Create TACACS+ Provider



Host Name (or IP Address):

Description:

Port:

Authorization Protocol: CHAP MS-CHAP PAP

Key:

Confirm Key:

Timeout (sec):

Retries:

Management EPG:

Server Monitoring: Disabled Enabled

Cancel

Submit

APIC TACACS رقوم تادادع

Create Login Domain



Name:

Realm:

Description:

Providers:

Name	Priority	Description
52.13.89	1	

Cancel

Submit

Host Name	Description	Port	Timeout (sec)	Retries
52.13.89		49	5	1

Tacacs رفوم ضرع ةقيرط

ISE نيوكت

ةزهجأةومجمءاشنإ. ةكبشلا ةزهجأةومجم > ةكبشلا دراوم > ةرادإ > إلقتنا 1. ةوطخلا ةزهجالا ءاونأ ءيمج نمض ةكبش.

☰ Cisco ISE

Network Devices **Network Device Groups** Network Device Profiles External

Network Device Groups

All Groups

Choose group ▾

↻ **Add** Duplicate Edit 🗑️ Trash 👁️ Show group members 📥 Import 📤 Export ▾ ☰

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	✓ All Device Types	All Device Types
<input type="checkbox"/>	APIC	

ISE ةكبش ةزهجأةومجم

ناونعو APIC م سا فيرعتAddرتخأ. Administration > Network Resources > Network Devices. ةوطخلا 2. ةوطخلا IP، ءلعةمدختسمل رورملا ءملك ددحو، TACACS+ رايخإ طخو زاهجالا عون تحت APIC رتخاو، Submit. رقنا. APIC TACACS+ دوزم نيوكت

Network Devices

Default Device

Device Security Settings

[Network Devices List](#) > APIC-LAB

Network Devices

Name Description IP Address * IP : Device Profile Cisco Model Name Software Version

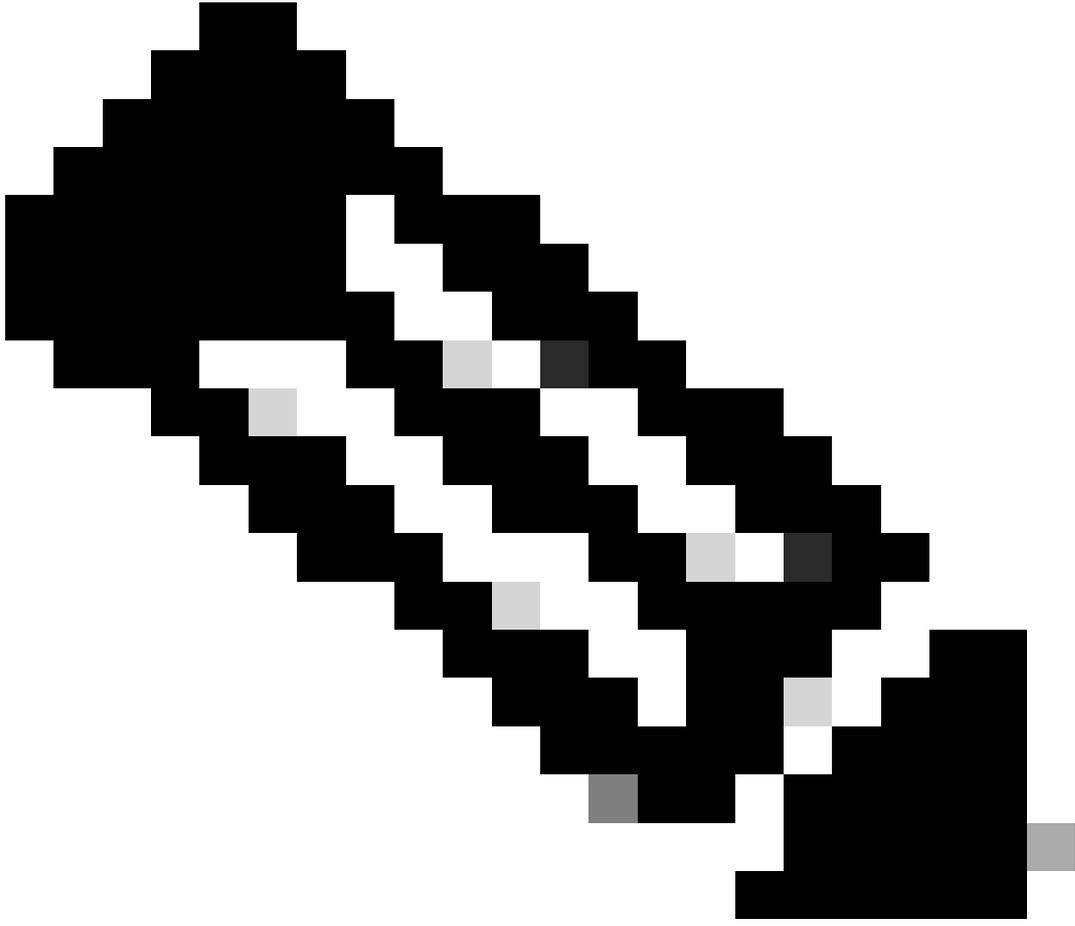
Network Device Group

Location [Set To Default](#)IPSEC [Set To Default](#)Device Type [Set To Default](#) RADIUS Authentication Settings TACACS Authentication SettingsShared Secret [Show](#)[Retire](#)

ةيفرطالالالوحملل 2. ةوطخالاو 1. ةوطخالاررك

Active Directory عم ISE حمد لجأ نم طابترالال اذه يلع ةدوجومال تاداشرالال مدختسأ 3. ةوطخالال

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/217351-ad-integration-for-cisco-ise-gui-and-cli.html>.

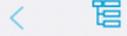


AD لوؤسم تاعومجم ونيلخادلا نيمدختسملا نملك دننستسملا اذه نمضتي: ةظحالم
نيمدختسملا ةيوه ردصم مادختساب رابتخال اءارجإ متي، كلذ عمو، ةيوه رداصمك
AD تاعومجملا اهسفن يه ةجيتنلا. نيلخادلا

رقن او User Identity Groups رتخأ >Administration > Identity Management > Groups. ةللقنتنا (يرايتخا). 4. ةوطخال
طقف ةءارق لل Admin يمدختسمو Admin يمدختسملا ةءحاو ةعومجم ءاشنإب مق Add. قوف

Identity Groups

EQ



> Endpoint Identity Groups

> User Identity Groups

User Identity Groups

[Edit](#) [+ Add](#) [Delete](#) [Import](#) [Export](#)

Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_
<input type="checkbox"/> APIC_RO	i
<input type="checkbox"/> APIC_RW	

ةي وه لة ع وم جم

4. ة و ط خ ل ا ي ف ا ه و ا ش ن ا م ت ة ع و م ج م ل ك ل م د خ ت س م ل ك ن ي ي ع ت ب م ق . م د خ ت س م و A d m i n م د خ ت س م A d m i n > Administration > Identity Management > Identity. ا د د ر ق ن ا (ي ر ا ي ت خ ا) . 5. ة و ط خ ل ا >

Users

Latest Manual Network Scan Res...

Network Access Users

[Edit](#) [+ Add](#) [Change Status](#) [Import](#) [Export](#) [Delete](#) [Duplicate](#)

Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups
<input type="checkbox"/> Enabled	APIC_ROUser					APIC_RO
<input type="checkbox"/> Enabled	APIC_RWUser					APIC_RW

6. ة و ط خ ل ا > Administration > Identity Management > Identity Source Sequence. ا د د ر ق ن ا (ي ر ا ي ت خ ا) . 6. ة و ط خ ل ا ف ي ر ع ت ب م ق و ، ا د د ر ق ن ا . ة م ا ق ل ا ن م ة ي و ه ر د ص م I n t e r n a l U s e r s A D J o i n P o i n t s ا د د ر ق ن ا ، م س ا n e x t s t o r e i n t h e s e q u e n c e ا و ا ر ق ن ا ا و A d v a n c e d S e a r c h L i s t S e t t i n g s ا ه ا ن د ا .

∨ Identity Source Sequence

* Name **APIC_ISS**

Description

∨ Certificate Based Authentication

Select Certificate Authentication Profile ∨

∨ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available		Selected
Internal Endpoints		iselab
Guest Users		Internal Users
All_AD_Join_Points		
	<input type="button" value=">"/> <input type="button" value="<"/> <input type="button" value=">>"/> <input type="button" value="<<"/>	<input type="button" value="↑"/> <input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="↓"/>

∨ Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

- Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"
- Treat as if the user was not found and proceed to the next store in the sequence

ةوهلا ردصم لسلسلت

7. ةفاضل ددح ☰ > Work Centers > Device Administration > Policy Elements > Results > Allowed Protocols.

لوكونورب ةمئاق نم MS-CHAPv1 ب حامسلا او CHAP ب حامسلا دي دحت يغلأو، امسا فرعو ظفح ددح. ةقداصملا

☰ Cisco ISE

Overview Identities User Identity Groups Ext Id Sources Network Resources

Conditions >

Network Conditions >

Results ▾

Allowed Protocols

TACACS Command Sets

TACACS Profiles

[Allowed Protocols Services List](#) > TACACS Protocol

Allowed Protocols

Name TACACS Protocol

Description

▾ Allowed Protocols

Authentication Protocols

Only Authentication Protocols relevant to TACACS are displayed.

Allow PAP/ASCII

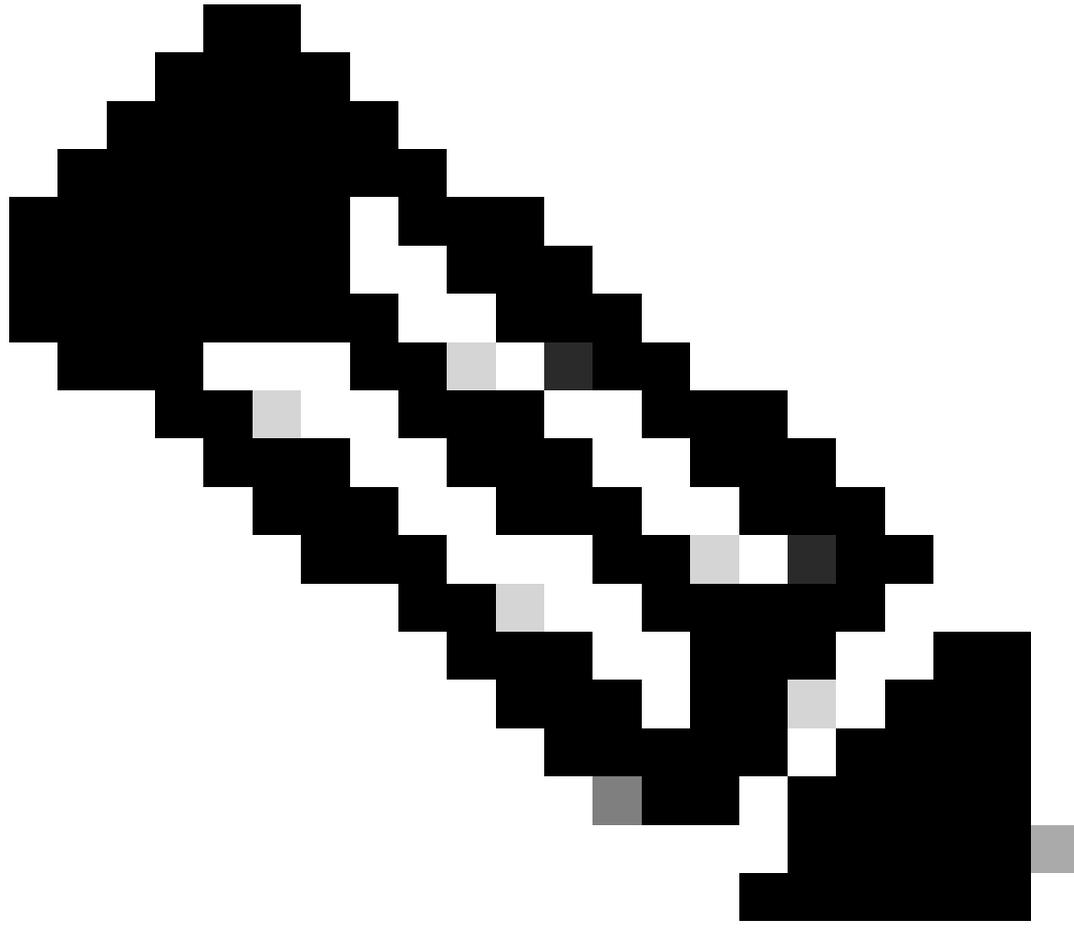
Allow CHAP

Allow MS-CHAPv1

Tacacs ل حامسلا لوكونورب

رقنا. Save. Raw View. تحت ةمئاقلا يف ةدوجوملا تامسلا لىل ع اءان ب نيفي صوت add ئشنأو
8. رقنا > Work Centers > Device Administration > Policy Elements > Results > TACACS Profile. لىل لقتنا.

- لوؤسملا مدختسم: cisco-av-pair=shell:domains=all/admin/
- طقف لوؤسم مدختسم ةءارق: cisco-av-pair=shell:domains=all/read-all



ليوختلا ةلحرم لشفت ،ةيفاضا فورح وأ ةفاسم ةلاح يف :ةظحالم

Overview Identities User Identity Groups Ext Id Sources Network Resources **Policy Elements** Device Administration

Conditions > TACACS Profiles > APIC ReadWrite Profile

TACACS Profile

Name
APIC ReadWrite Profile

Description

Task Attribute View **Raw View**

Profile Attributes

cisco-av-pair=shell:domains=all/admin/

Cancel Save

TACACS فيرعت فلم

Overview Identities User Identity Groups Ext Id Sources Network Resources

TACACS Profiles

Refresh Add Duplicate Trash Edit

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	APIC ReadOnly Profile	Shell	
<input type="checkbox"/>	APIC ReadWrite Profile	Shell	

TACACS و ReadOnly لوؤسم فيرعت تافلم

جهن ةومجم ءاشن اب مق >Work Centers > Device Administration > Device Admin Policy Set. الى لقتنا 9 ةوطخلا TACACS رتخا 1 ةوطخلا في هؤاشن ا مت APIC ذل زا هلا عون رتخاو ،مسا ديحتب مقو ،ةديج Save. رقتناو ،ه حومسم لوكوتوربك 7 ةوطخلا في هؤاشن ا مت يذلا Protocol

ةقداصم طرشك ىرخأل تامسلا وأ عقوملا مادختسا نكمي :ةظحالم

مسا فيرعتب مقو ،لوؤسم مدختسم عون لكل لىوخت فيرعت فلم عاشناب مق 11. ةوطخلال لثم ةيفاضا طورش مادختسا نكمي .طرشك AD مدختسم ةعومجم وأ/أو لىلخاد مدختسم رتخاو Save.رقن او لىوخت جهن لك يف بسانملا Shell فيرعت فلم رتخأ APIC.

Authorization Policy (3)

Status	Rule Name	Conditions	Command Sets	Shell Profiles	Hits	Actions
ON	APIC Admin RO	AND Network Access Device IP Address EQUALS 188.21 IdentityGroup-Name EQUALS User Identity Groups:APIC_RO		APIC ReadOnly Profile	34	
ON	APIC Admin User	AND Network Access Device IP Address EQUALS 188.21 OR IdentityGroup-Name EQUALS User Identity Groups:APIC_RW Iselab-ExternalGroups EQUALS ciscoise.lab/Bulltin/Administrators		APIC ReadWrite Profile	18	
ON	Default		DenyAllCommands	Deny All Shell Profile	0	

TACACS ضيوفت فيرعت فلم

ةحصلال نم ققحتلا

رتخأ .مدختسملا لوؤسم تاغوسم مادختساب APIC مدختسم ةهجاو ىلى لوخدلا لاجس 1. ةوطخلال ةمئاقلا نم TACACS راىخ

APIC
Version 4.2(7u)
CISCO

User ID
APIC_ROUser

Password
.....

Domain
S_TACACS

Login

APIC لوخد لىجست

ةبسانملا تاسايسلا قىببطت متىو APIC مدختسم ةهجاو ىلى لوصولا نم ققحت 2. ةوطخلال TACACS Live تالاجس ىلع

Welcome to APIC

What's new in version 4.2(7u)



New Features

- Floating L3out
 - Docker EE (Kubernetes) container integration
 - L4-L7 Services support in vPod
 - Backup PBR destination
 - Support for 64 Remote Leaf pairs
- UI Enhancements:
 - User-defined UI banner
 - First Time Setup wizard
 - Simplified L3Out creation
 - EPG to leafs deployment view

[View Release Notes](#)

Getting Started

[What's New in v4.2\(7u\)](#)

[Online Videos \(YouTube™\)](#)

[View All Tutorial Videos](#)

Explore

[Configuration Guides](#)

[Knowledge Base Articles](#)

[APIC Communities](#)

Support

[Online Help](#)

[Troubleshooting](#)

[Documentation](#)

Do not show on login

[Review First Time Setup](#)

[Get Started](#)

APIC بيحرت ةلاسر

طقف ةارقلا ةرادا يم دختس مل 2 و 1 تا و طخل ررك

☰ Cisco ISE

Operations · TACACS

Live Logs

🔄 Export To

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Devic...
×	⌵		Identity	⌵	Authentication Policy	Authorization Policy	Ise Node	Network Device N...
Apr 20, 2023 10:14:42.4...	✓	🔒	APIC_ROUser	Authorizat...		APIC >> APIC Admin RO	PAN32	APIC-LAB
Apr 20, 2023 10:14:42.2...	✓	🔒	APIC_ROUser	Authentic...	APIC >> APIC Authentication Po...		PAN32	APIC-LAB

Last Updated: Fri Apr 21 2023 00:14:53 GMT+0200 (Central European Summer Time)

ةرشابملا TACACS+ تالجس

اهحال صا و اءاطخال فاشك ت سا

Debug Nodes قوف رقن او TACACS رتخأ. >Operations > Troubleshoot > Debug Wizard ☰ يلا لقتنا 1. ةوطخل

Debug Profile Configuration

Debug Wizard contains predefined debug templates with the help of which you can troubleshoot issues on ISI

 Add  Edit  Remove  Debug Nodes

<input type="checkbox"/>	Name	Description	Status
<input type="checkbox"/>	802.1X/MAB	802.1X/MAB	DISABLED
<input type="checkbox"/>	Active Directory	Active Directory	DISABLED
<input type="checkbox"/>	Application Server Issues	Application Server Issues	DISABLED
<input type="checkbox"/>	BYOD portal/Onboarding	BYOD portal/Onboarding	DISABLED
<input type="checkbox"/>	Context Visibility	Context Visibility	DISABLED
<input type="checkbox"/>	Guest portal	Guest portal	DISABLED
<input type="checkbox"/>	Licensing	Licensing	DISABLED
<input type="checkbox"/>	MnT	MnT	DISABLED
<input type="checkbox"/>	Posture	Posture	DISABLED
<input type="checkbox"/>	Profiling	Profiling	DISABLED
<input type="checkbox"/>	Replication	Replication	DISABLED
<input checked="" type="checkbox"/>	TACACS	TACACS	DISABLED

حیح صت ال فی رع ت فلم نی وک ت

Save. ررق ناو رورم ال ة کرح ملتست ی تل ال ة دق ال رتخأ 2. ة وطلخ ال

Debug Profile Configuration

Debug Log Configuration

Debug Profile Configuration > Debug Nodes

Debug Nodes

Selected profile **TACACS**

Choose on which ISE nodes you want to enable this profile.

↻
Filter ▼
⚙️

<input type="checkbox"/> Host Name	Persona	Role
<input checked="" type="checkbox"/> PAN32.ciscoise.lab	Administration, Monitoring, Policy Service	PRI(A), PRI(M)
<input type="checkbox"/> SPAN32.ciscoise.lab	Administration, Monitoring, Policy Service, ...	SEC(A), SEC(M)

Cancel
Save

ءاطخألا حىحصت دقع دىدت

Operations > Troubleshoot > Download
logs
ءاطخألا حىحصت دقع دىدت

AcsLogs, 2023-04-20 22:17:16, 866, DEBUG, 0x7f93cab7700, cntx=0004699242, sesn=PAN32/469596415/70, CPMSession

ام ةحص نم ققحتلاب مق، ضيوفتلاو ةقداصملا تامولعم ءاطخألا حىحصت راهظا مدع ةلاح يف
ىلى:

1. ISE ةدقع ىلع "ةزهجالا ةرادا" ةمدخ نىكمت متي.
2. APIIC نىوكت ىلى حىحصلا ISE ناونع ةفاضا تمت.
3. حومسم (TACACS) 49 ذفنملا نأ نم ققحتف، فصتنملا يف ةيامح راج دوجو ةلاح يف
ه.

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء ن أ عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة ي رش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ي ل أ ة مچرت ل ض ف أ ن أ ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (رف و ت م ط بار ل ا) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا