

# فرعم لمع تاسلجل ليوختلا قفدت نيوكت ISE 3.2 في لمخال

## تايوتحمل

[عمدقمل](#)

[ةيساسأ تامولعم](#)

[ةيساسألا تابلطتمل](#)

[تابلطتمل](#)

[عمدختسمل تانوكمل](#)

[نيوكتلا](#)

[ةحصللا نم ققحتلا](#)

[اهخالصا وءاطخال فاشكتسا](#)

## عمدقمل

بيقرلا صي صيختل لمخال فرعم شادخال ليوختلا دعاوق نيوكت ةيفيك دننسملا اذه حضوي تاسلجل في.

## ةيساسأ تامولعم

عمجت اهنكلو، ةرشابم ني مدختسمل ةقداصمب (لمخال فرعم) ةيبلسلا ةيوهلا تامدخ موقت ال (AD) Active Directory لثم ةيجراخال ةقداصملا مداوخ نم IP نيوانعو ني مدختسمل تايوه نيكرتشملا عم تامولعمل كالت ةكراشمب موقت م، ني رفوملا مساب ةفورعمل.

نام ةومجم مقر ني عتل ضيوفت ةسايس نيوكتب كل حمست ةديج ةزيم ISE 3.2 مدقي (SGT) Active Directory ةومجم ةيوضع لادانتسا مدختسمل.

## ةيساسألا تابلطتمل

### تابلطتمل

ةيلاتل عيضاوملاب ةفرعم كي دل نوكت نأ Cisco ي صوت:

- Cisco نم ISE 3.x
- رفوم ي عم يبلسل فرعمل لمكت
- Active Directory (AD) ةرادا
- ميسقتلا (TrustSec)
- (ةيساسألا ةمظنألا لدابت ةكبش) PxGrid

### عمدختسمل تانوكمل

- 3.2 رادصإلا، (ISE) ةيوهلا عم دخ كرحم جم انرب
- Microsoft Active Directory
- Syslogs

ةصاخ ةي لمعم ةئي ب ي ف ةدوجوملا ةزهجالا نم دنتسملا اذه ي ف ةدراولما تامولعملما عاشنإ مت تناك اذا .(يضا رتفا) حوسمم نيوكتب دنتسملا اذه ي ف ةمدختسملا ةزهجالا عيمج تادب رما يال لمحتحملما ريثاتلل كمهف نم دكأتف ،ليغشتلا دي قكتكبش

## نيوكتلا

ISE تامدخ نيكمت 1. ةوطخل

1. ةمدخ نيكمتب مقو ،ريحت قوف رقناو ISE ةدقع رتخاو ،رشن > ةرادا يلى لقتنا ،ISE ي ف . ةي بلسل ةيوهلا ةمدخ نيكمت رتخاو ةسايسلا . ةس ل ل لال خ نم اهرشن متي نأ يلى ةجاحب لمخال فرعم تاسلج تناك اذا

PassiveID لوخد ليجست يمدختسمب ةصاخلا SGT ليصافت رشن نكمي ال :ريذحت عمو . SXP ي ف (API) تاقيبطتلا ةجمررب ةهجاو رفوم ةطساوب مهيلع قي دصتلا مت نيذلا يماظن لال خ نم نيمدختسملا ءالؤهب ةصاخلا ءابقرلا ليصافت رشن نكمي ،كلذ PXgrid و PXgrid.

The screenshot shows the configuration page for the Policy Service. The 'Policy Service' toggle is turned on. Under 'Enable Session Services', the 'Include Node in Node Group' dropdown is set to 'None'. 'Enable Profiling Service' is checked. 'Enable Threat Centric NAC Service' is unchecked. 'Enable SXP Service' is checked, and the 'Use Interface' dropdown is set to 'GigabitEthernet 0'. 'Enable Device Admin Service' is unchecked. 'Enable Passive Identity Service' is checked and highlighted with a red box.

ةنكمملا تامدخال

Active Directory نيوكتب مق 2. ةوطخل

1. رقنا مت Active Directory رتخاو ةي جراخلا ةيوهلا رداصم > ةيوهلا ةرادا > ةرادا يلى لقتنا . ةفاضل رزىل ع
2. لاسرا يلى رقنا . Active Directory لاجمو لاصتالا ةطقن مسال خدأ .

Identities   Groups   **External Identity Sources**   Identity Source Sequences

---

**External Identity Sources**

<    

> Certificate Authentication F

Active Directory

**Connection**

\* Join Point Name   **aaamexrub**

\* Active Directory Domain   **aaamexrub.com** Active Directory فاضا

3. رورملا ةم لك و مدختس مل مسا لخدأ .معن ةق طقط . AD لى ISE لى مضمني قش بنم نأ رهظي .3. OK قوف رقناو .

## Information

Would you like to Join all ISE Nodes to this Active Directory Domain?

No   **Yes**

لى مامضنالا ةعباتم

## Join Domain

Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

\* AD User Name **user**

\* Password \*\*\*\*\*

Specify Organizational Unit

Store Credentials

Cancel   **OK**

ISE  
Directory

Active لى مامضنالا

4. دادرتمسا قوف رقنا مث ، ةفاضل قوف رقناو ، تاعومجم لى لقتنا . تانالعال تاعومجم دادرتمسا .4. قفاوم قوف رقناو ةمتهمل تاعومجم لى عيمج رتخاو تاعومجم لى

## Select Directory Groups

This dialog is used to select groups from the Directory.

Domain: aaamexrub.com

Name Filter: \_\_\_\_\_ SID Filter: \_\_\_\_\_ Type Filter: All

Retrieve Groups... 53 Groups Retrieved.

<input type="checkbox"/>	aaamexrub.com/Users/Cloneable Domain Contro...	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Denied RODC Password ...	S-1-5-21-144182218-1144227253-205214604...	DOMAIN LOCAL
<input type="checkbox"/>	aaamexrub.com/Users/DnsAdmins	S-1-5-21-144182218-1144227253-205214604...	DOMAIN LOCAL
<input type="checkbox"/>	aaamexrub.com/Users/DnsUpdateProxy	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input checked="" type="checkbox"/>	aaamexrub.com/Users/Domain Admins	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Domain Computers	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Domain Controllers	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Domain Guests	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input checked="" type="checkbox"/>	aaamexrub.com/Users/Domain Users	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Enterprise Admins	S-1-5-21-144182218-1144227253-205214604...	UNIVERSAL
<input type="checkbox"/>	aaamexrub.com/Users/Enterprise Read-only De...	S-1-5-21-144182218-1144227253-205214604...	UNIVERSAL
<input type="checkbox"/>	aaamexrub.com/Users/Group Policy Creator Ow...	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Protected Users	S-1-5-21-144182218-1144227253-205214604...	GLOBAL

Cancel OK

تانالعالا تاعومجم دادرتسا

Connection Allowed Domains PassiveID **Groups**

Edit + Add Delete Group Update SID Values

<input type="checkbox"/>	Name	S
<input type="checkbox"/>	aaamexrub.com/Users/Domain Admins	S
<input type="checkbox"/>	aaamexrub.com/Users/Domain Users	S
<input type="checkbox"/>	aaamexrub.com/Users/sponsors	S

مت يتال تاعومجملا

اهدادرتسا

5. ةناخ ددح PassiveID تادادع| مسق يفو ةمدقتم تادادع| ل لقتنا .ليوختلا قفدت ني كمت .  
ظفحة ققط .ليوختلا قفدت رايختالا

## PassiveID Settings

The PassiveID settings that are configured in this section are applied to all the join points in Cisco ISE.

History interval*	10
Domain Controller event inactivity time* (monitored by Agent)	0
Latency interval of events from agent*	0
User session aging time*	24

Authorization Flow ⓘ

ليوختلا قفدت نيكم ت

syslog رفوم نيوك ت ب مق 3. ةوطخال

قوف رقناو، Syslog يرفوم رتخاو، نورفومال > PassiveID > لمعل زكارم لىل لقتنا 1. طافح ةق طقط. تامولعمل لمكأ م ث، ةفاضل

ال نكلو، ASA في حجان VPN لاصتا نم syslog ةلاس ر ISE ملتسي، ةلحال هذ في: ريذحت نيوك ت ل اذ دنتس مل اذ ةفصي.

## Syslog Providers

Name\*  
ASA

Description

Status\*  
Enabled


Host FQDN\*  
asa-rudelave.aaamexrub.com

Connection Type\*  
UDP - Port 40514

Template\*  
ASA VPN

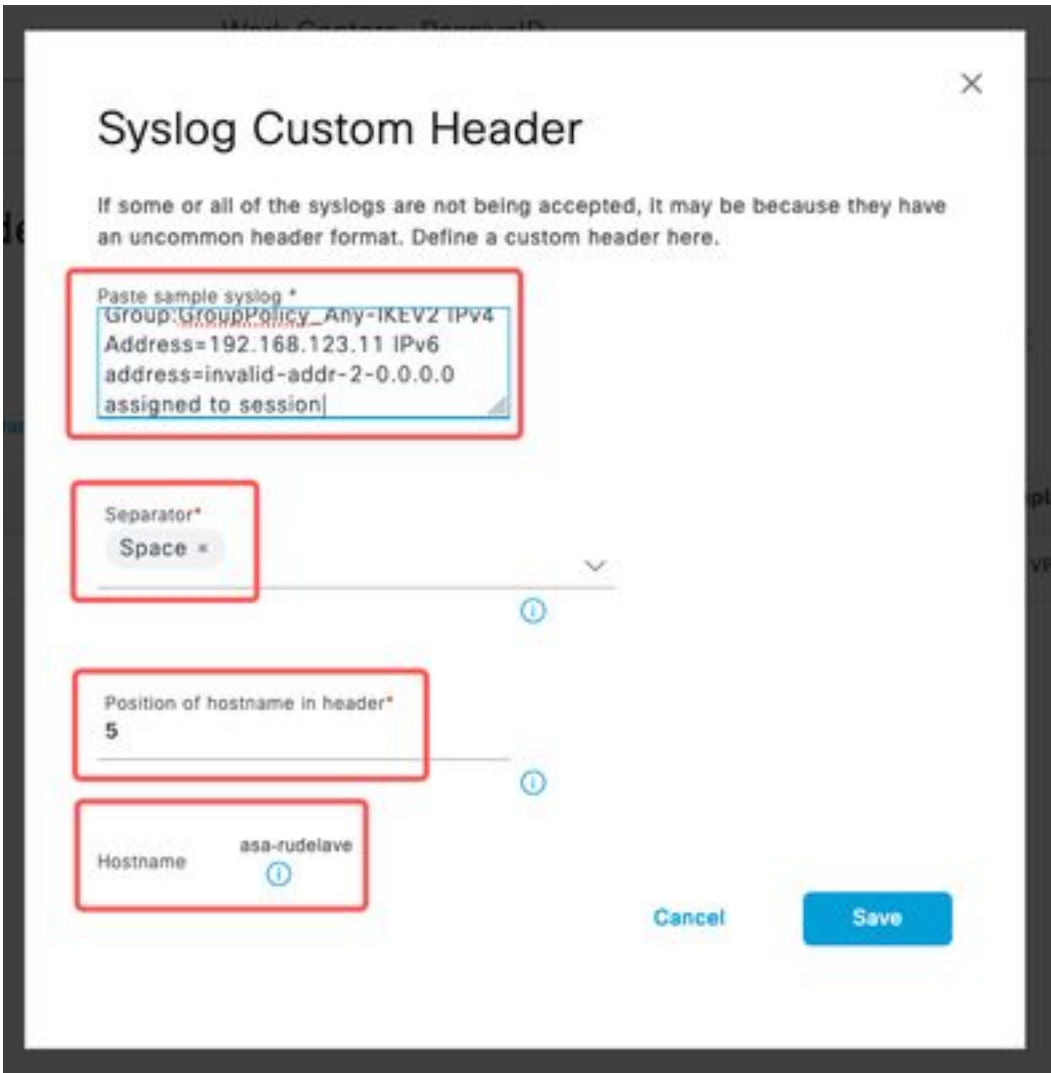
Default Domain  
aaamexrub.com

[View](#) [New](#)



syslog رفوم نيوكت

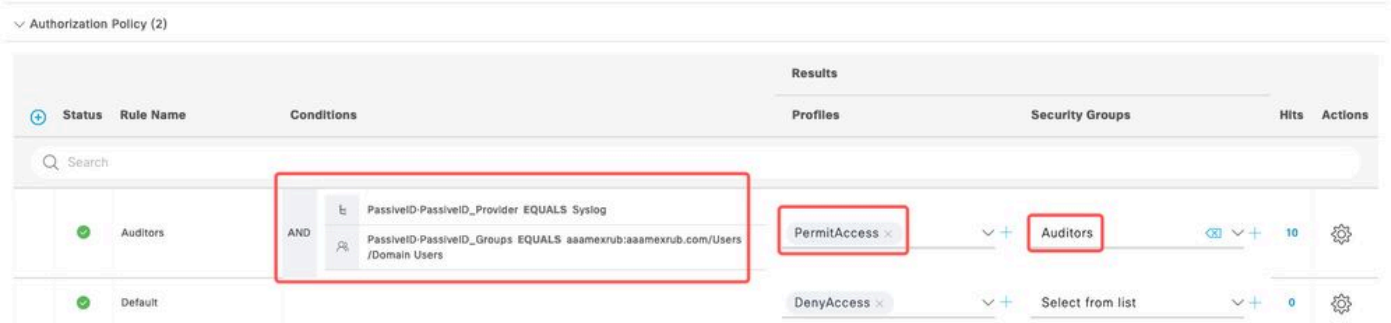
ىلع روثعلل بېوېت ەمالع واً لصاف مدختساو syslog جذومن قصلال. صصخم سآر رقنا 2. ظفح ەقطقط. فيضملا مسا رهظي، احيحص ناك اذا. زاهجالا فيضم مسا



صصخم سأسر نيوكت

#### ةقداصملا دعاوق نيوكت 4. ةوطخلما

1. جهنلا مدختسي هنإف، ةلجال هذولو. تاسايسلا تاعومجم > ةسايسلا ىلإ لقتنا. يف ةديج ةدعاق فضا، ليوختلا جهن يف. يضارتفالا جهنلا ىلع رقنا. يضارتفالا ةومجم عم اذه جمك كنكمي. نيروفوملا عيجم ىلع ISE يوتحي، Passiveld تاسايس ةلجال نامألا تاعومجم يف رتخاو، فيرت فلملك لوصولاب حامسلا رتخا. Passiveld. تامولعمل ةينقت طباضل



ةقداصملا دعاوق نيوكت

## ةحصلنا نم ققحتلا

قفدت ليوخت ىري نأ لچس يچ radius ل تصحف عي طتسي تنأ، syslog ل ISE ملتسي نإ ام. ةرشابملا تالچسلا > RADIUS > تايلمعلا ىلإ لقتنا.

جهنو مدختسمسا ىلع مقرلا اذه يوتحي. ضيوفتلا ثدح ةدهاشم كنكمي، تالجسلا ي هب ةنرتقملا نامألا ةومجم ةمالعولي وختلا

Time	Status	Details	Repea...	Identity	Endpoint ID	Authenticatio...	Authorization Policy	Authorization ...	Security ...	IP Address
Jan 31, ...	●	🔍	0	test	192.168.123.10	PassiveID provider	PassiveID provider >> Auditors	PermitAccess	Auditors	192.168.123.10
Jan 31, ...	🔍	🔍		test	192.168.123.10	PassiveID provider	PassiveID provider >> Auditors	PermitAccess		192.168.123.10

راديوس Radius Live

ةدهاشم كنكمي انه. ليصافتلا ريرقت قوف رقنا، ليصافتلا نم ديزملا نم ققحتلل بيقرلا صيصختلا تاسايسلا ميقي يذلا طقف حامسلا قفدت

#### Overview

Event	5236 Authorize-Only succeeded
Username	test
Endpoint Id	192.168.123.10
Endpoint Profile	
Authentication Policy	PassiveID provider
Authorization Policy	PassiveID provider >> Auditors
Authorization Result	PermitAccess

#### Steps

15041	Evaluating Identity Policy
15013	Selected Identity Source - All_AD_Join_Points
24432	Looking up user in Active Directory - All_AD_Join_Points
24325	Resolving identity - test@aaamexrub.com
24313	Search for matching accounts at join point - aaamexrub.com
24319	Single matching account found in forest - aaamexrub.com
24323	Identity resolution detected single matching account
24355	LDAP fetch succeeded - aaamexrub.com
24416	User's Groups retrieval from Active Directory succeeded - All_AD_Join_Points
22037	Authentication Passed
90506	Running Authorize Only Flow for Passive ID - Provider Syslog
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15036	Evaluating Authorization Policy
90500	New Identity Mapping
5236	Authorize-Only succeeded

#### Authentication Details

Source Timestamp	2023-01-31 16:15:04.507
Received Timestamp	2023-01-31 16:15:04.507
Policy Server	asc-ise32-726
Event	5236 Authorize-Only succeeded
Username	test
Endpoint Id	192.168.123.10
Calling Station Id	192.168.123.10
IPv4 Address	192.168.123.10
Authorization Profile	PermitAccess

RADIUS رشايملا لجال ريرقت

## اهالصا واطخالا فاشكتسا

Authoriatiون قفدتو PassiveID تاسلج، نيت عفت مدختسي هنإف، ةلجال هذهل ةبسنلاب جلام > اهالصا واطخالا فاشكتسا > تاي لمعلا للاقنا، ااطخالا حيحصت نيكم تل ISE. ةدقع رتخا م، ااطخالا حيحصت لجال نيوت > ااطخالا حيحصت

اطخالا حيحصت يوتسم نم ةيلاتلا تانوكملا نيكم تب مق، PassiveID ل ةبسنلاب

- PassiveID

اذه نم ققحتلا ديرت يذلا فلملا، لمال فرعملا روم لادانتسا، تالجسلا نم ققحتلل نينرخالا نيدوزم لل، passiveid-syslog.log فلملا ةعجارم كمزلي، ويارانيسلا

- passiveid.log لمي



- passiid-api.log
- passiid-endpoint.log
- passiid-span.log
- غولم و لم اوخ

ءاطخأل اءىءصء ءوءسم نم ءةءلءلء ءانوءكمءل ءنءكمءب مق ،لءووءءلء قءءءل

- ءاساءءسءلء ءءم
- ءنء ءررب

ءءءم:

Diagnostic Tools Download Logs **Debug Wizard**

Debug Profile Configuration  
Debug Log Configuration

Node List > asc-ise32-726.aamexrub.com

### Debug Level Configuration

Edit Reset to Default

Component Name	Log Level	Description	Log file Name
	debug		
<input type="radio"/> PassiveID	DEBUG	PassiveID events and messages	passiveid-wmi.log
<input type="radio"/> policy-engine	DEBUG	Policy Engine 2.0 related messages	ise-psc.log
<input type="radio"/> prrt-JNI	DEBUG	prrt policy decision request processing layer related ...	prrt-management.log

ءاطخأل اءىءصء ءنءكمءب ءمء

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او  
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل