

نام أة وومجم تامالع نني عتل ISE 3.2 ني وكت لمع تاسلج ل PassiveID

تايوت حمل

[ةمدقم](#)

[ةيساس أال تابلطت](#)

[تابلطت](#)

[ةمدختسم ل تانوك](#)

[ةيساس أ تامولعم](#)

[ني وكت](#)

[فدت ل ليطي طخت ل مسر](#)

[تان وكت](#)

[ةحصلا نم ققحت](#)

[ISE نم ققحت](#)

[PxGrid كرتشم نم ققحت](#)

[TrustSec SXP ريطن نم ققحت](#)

[اهجالص او عاخذ أال فاشك](#)

[ISE ل عاخذ أال حيحصت ني كمت](#)

[تالچس ل تاص اصق](#)

ةمدقم

لمع تاسلج ل اهصي صخت و (SGTs) نام أة وومجم تامالع ني وكت ةي فيك دن تسم ل اذ فصي ISE 3.2 في ل وخت ل تاسايس ل ل خ نم ل مال فرعم

ةيساس أال تابلطت

تابلطت

ةيلات ل عيضاوم ل ابة فرعم كيدل نوكت نأ Cisco ي صوت

- Cisco ISE 3.2
- Passive ID و TrustSec و PxGrid

ةمدختسم ل تانوك

ةيلات ل ةي دام ل تانوك ل او جم ارب ل تارادص ل دن تسم ل اذ في ةراول تامولعم ل دن تست

- Cisco ISE 3.2
- FMC 7.0.1
- WS-C3850-24P رادص ل لغشت ل 16.12.1

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجالا نم دنتسملا اذه يف ةدراوللا تامولعمل عاشنإ مت تناك اذا. (يضا رتفا) حوسمم نيوكت ب دنتسملا اذه يف ةمدختسملا ةزهجالا عيمج تأدب رمأ يأل لمحتحمل ريثأتلل كمهف نم دكأتف ،لغيغشتلا ديقتك تبش

ةيساسأ تامولعم

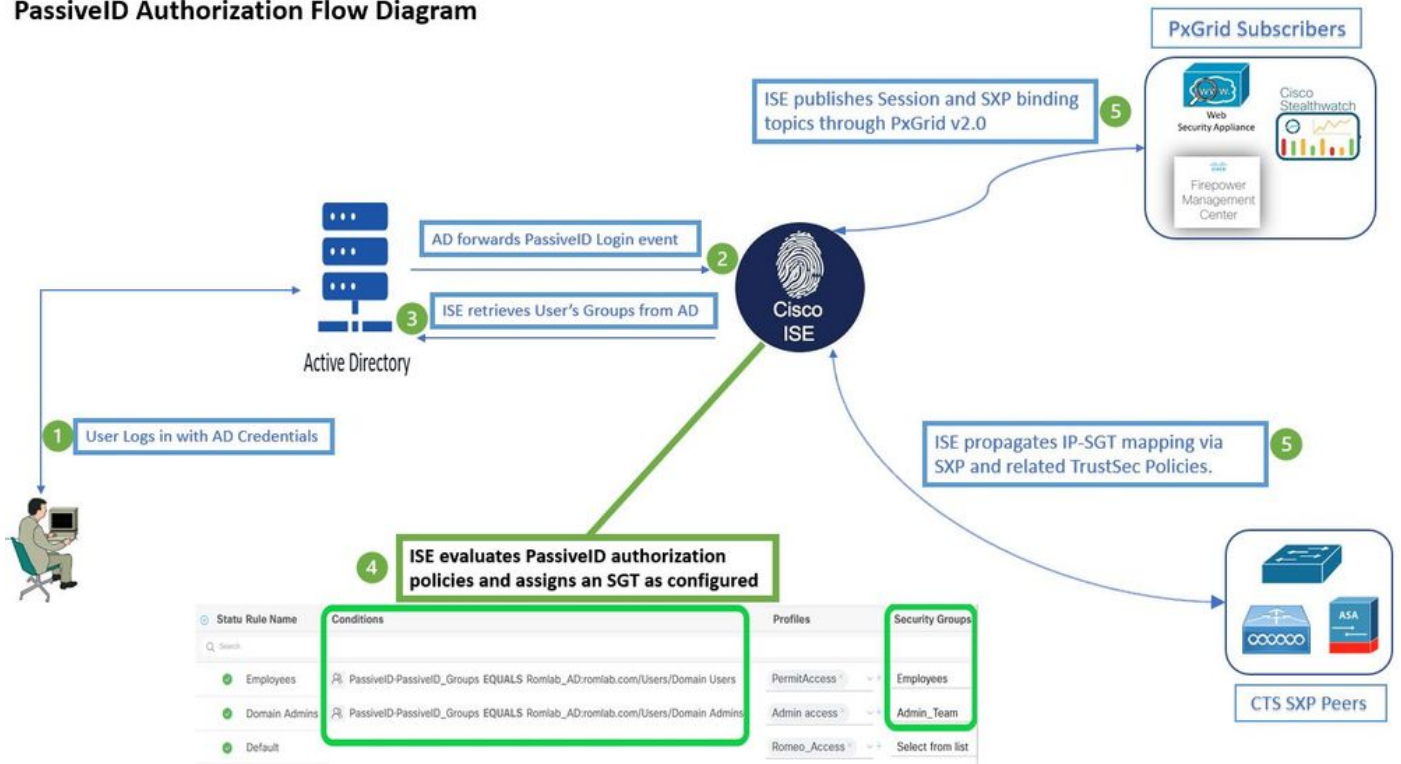
اذه يطيغي ال .ةردقلا هذه معددي يذلا ىندألا رادصإلا وه Cisco Identity Services Engine (ISE) 3.2 [ليدل](#) عجار ،ةلص تاذا تامولعم ىلع لوصحلل SXP و PxGrid و PassivID نيوكت دنتسملا [ةرادلا](#).

ةسلجل طقف (SGT) نامأ ةعومجم مقرر نييعت نكمي ،مدقألا تارادصإلا وأ ISE 3.1 تارادصإلا يف تاسايس نيوكت اننكمي ،ISE 3.2 عم MAB و 802.1x لثم ةطشنلا ةقداصملا وأ RADIUS لمع Identity Services Engine (ISE) لبقتسي امدنع هنا ثيحب PassivID لمع تاسلجل ليوختلا WMI Active Directory Domain Controllers (AD DC) لثم رفوم نم مدختسملا لوخذ ليحست ثادحأ ةيوضع ىلا اذانتسا PassivID لمع ةسلجل (SGT) نامأ ةعومجم ةمالع نيوعي هناف ،AD ليكوا وأ ةعومجم و IP-Sgt نييعت ليصافت رشن نكمي .مدختسملا (AD) ةعومجم ىلا وأ/و (SXP) بيقرلا لدابت لوكتورب ربع TrustSec لاجم ىلا PassivID ب ةصاخلا تانالعالا نم (FMC) ةيرانلا ةقاطلا ةرادا زكرم لثم (Pxgrid) ياساسألا ماظنلا لدابت ةكبش يكرتشم Cisco نم (Stealthwatch) ةنمآلا ةكبشلا تاليلحتو Cisco.

نيوكتلا

قفدتلل يطيختلا مسرلا

PassivID Authorization Flow Diagram



قفدتلل يطيختلا مسرلا

تانويكتلا

ليوختال قفدت ني كمت:

ةناخ Authorization Flow نم ققحت و Active Directory > Advanced Settings > PassiveID Settings لي لقتنا راياخ اذه PassiveID. لي لوخدلا لي جست يم دخت سمل ليوختال تاسايس ني وكتل رايتخال اياضارتفا تزجعا.

PassiveID Settings

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

History interval*

Domain Controller event inactivity time*
(monitored by Agent)

Latency interval of events from agent*

User session aging time*

Authorization Flow ⓘ

ليوختال قفدت ني كمت

ي ف SXP و PxGrid و PassiveID تامدخ لي غشت نم دكأت، ةزيمل ا هذه لمعت يكل: ةظالم Administration > System > Deployment نمض اذه نم ققحتال كنكمي. كب ةصاخال رشنال ةلمع

جهنل ةومجم ني وكت:

1. (ن سحتسم) PassiveID ل ةلصفنم جهن ةومجم ءاشن ا.
2. كب صاخال رفوملا عون ددحو PassiveID·PassiveID_Provider ةمسلال مدختسا، طورشلل.

Policy Sets

Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	PassiveID_Sessions		PassiveID·PassiveID_Provider EQUALS Agent	Default Network Access	5	⚙️	➔
✓	Default	Default policy set		Default Network Access	133	⚙️	➔

جهنل ةومجم

1. ةوطخلال ي ف اهؤاشنإ م ت يتاللا جهنلال ةعومجمل ضيوفتلال دعوق نيوكت 3.

- عامسأ وأ AD تاعومجم ىلع انب PassiveID سوماق مدختساو ةدعاق لكل طرش عاشناب مق امهيلك وأ ني مدختسملل.
- تانيوكتلال ظفحب مقو ةدعاق لكل نامأ ةعومجم ةمالع نيوكتب مق.

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
●	Employees	PassiveID:PassiveID_Groups EQUALS Lfc_AD:Lfc.lab/Users /Domain Users	PermitAccess x	Employees	3	⊗ ⊖ + ⚙
●	Domain Admins	PassiveID:PassiveID_Groups EQUALS Lfc_AD:Lfc.lab/Users /Domain Admins	Admin access x	Admin_Team	2	⊗ ⊖ + ⚙
●	Default		DenyAccess x	Select from list	0	⊗ ⊖ + ⚙

ليوختلال ةسايس

قفتدلال اذه ي ف مدختسم ريغ هنأل ةلص يذ ريغ ةقداصملا جهن: ةظحالم

عاشنإل تامس PassiveID_Provider، PassiveID_Groups، و PassiveID_Username مادختسإ كنكمي: ةظحالم ليوختلال دعوق.

4. Publish SXP bindings on pxGrid و Add RADIUS and PassiveID Mappings into SXP IP SGT Mapping Table يكرتشم عم PassiveID تانوييعة ةكراشم مل Work Centers > TrustSec > Settings > SXP Settings لىل لقتنا 4. ISE لىل SXP تانوييعة لودج ي ف مهنيمضتو PxGrid.

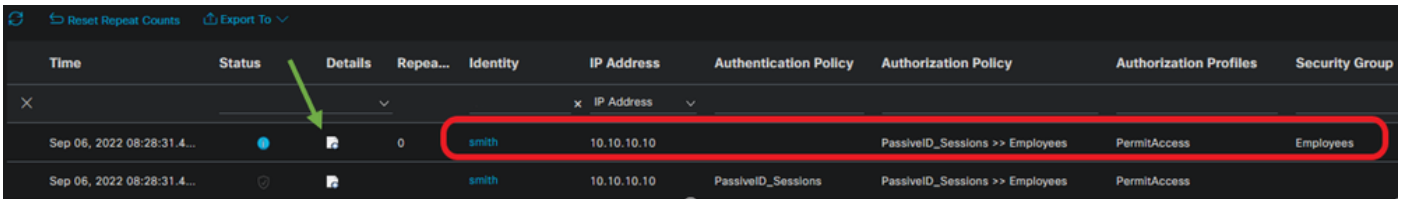
General TrustSec Settings	SXP Settings
TrustSec Matrix Settings	<input checked="" type="checkbox"/> Publish SXP bindings on pxGrid <input checked="" type="checkbox"/> Add Radius and PassiveID mappings into SXP IP SGT mapping table
Work Process Settings	Global Password
SXP Settings	Global Password ●●●●●●●●●● This global password will be overridden by the device specific password
ACI Settings	

ةحصلا نم ققحتلا

ححص لكشب نيوكتلا لمع ديكأتل مسقلا اذه مدختسا

ISE نم ققحتلا

تادحول AD لپكو و WMI لثم رفوم نم ISE ىلى مدختسملا لوخد لپجست تادحأ لاسرا درجمب
Operations > ىلى لقتنا Live تالجس صحف ىلى لقتنا، Active Directory (AD DC) ةمدخ لاجم مكحت
Radius > Live Logs.



Time	Status	Details	Repea...	Identity	IP Address	Authentication Policy	Authorization Policy	Authorization Profiles	Security Group
Sep 06, 2022 08:28:31.4...	●	ⓘ	0	smith	10.10.10.10	PassiveID_Sessions	PassiveID_Sessions >> Employees	PermitAccess	Employees
Sep 06, 2022 08:28:31.4...	○	ⓘ		smith	10.10.10.10	PassiveID_Sessions	PassiveID_Sessions >> Employees	PermitAccess	

ةرشابملا Radius تالجس

لائملا اذه يف، مدختسملا لصفم ريرقت ضرعل لپصافتلا دومع يف ربكملا زمرقوف رقنا
(Smith (Domain Users) انه حضوم وه امك

Overview

Event	5236 Authorize-Only succeeded
Username	smith
Endpoint Id	10.10.10.10
Endpoint Profile	
Authentication Policy	PassiveID_Sessions
Authorization Policy	PassiveID_Sessions >> Employees
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2022-09-06 20:28:31.393
Received Timestamp	2022-09-06 20:28:31.393
Policy Server	ise-3-2
Event	5236 Authorize-Only succeeded
Username	smith
Endpoint Id	10.10.10.10
Calling Station Id	10.10.10.10
IPv4 Address	10.10.10.10
Authorization Profile	PermitAccess


Other Attributes

ConfigVersionId	108
AuthorizationPolicyMatched_	Employees
ISEPolicySetName	PassiveID_Sessions
AD-User-Resolved-Identities	smith@Lfc.lab
AD-User-Resolved-DNs	CN=smith,CN=Users,DC=Lfc,DC=lab
AD-User-DNS-Domain	Lfc.lab
AD-Groups-Names	Lfc.lab/Builtin/Administrators
AD-Groups-Names	Lfc.lab/Builtin/Remote Desktop Users
AD-Groups-Names	Lfc.lab/Builtin/Remote Management Users
AD-Groups-Names	Lfc.lab/Builtin/Users
AD-Groups-Names	Lfc.lab/Users/Denied RODC Password Replication Group
AD-Groups-Names	Lfc.lab/Users/Domain Test
AD-Groups-Names	Lfc.lab/Users/NAD Admins
AD-Groups-Names	Lfc.lab/Users/Domain Users
AD-User-NetBios-Name	Lfc
AD-User-SamAccount-Name	smith
AD-User-Qualified-Name	smith@Lfc.lab
AuthorizationSGTName	Employees
ProviderIpAddress	10.10.10.132
SessionId	cf0d2acd-0d3d-413b-b2fb-6860df3f0d84
provider	Agent
UseCase	PassiveIDAuthZOnly

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 - Lfc\smith
24313	Search for matching accounts at join point - Lfc.lab
24315	Single matching account found in domain - Lfc.lab
24323	Identity resolution detected single matching account
24355	LDAP fetch succeeded - Lfc.lab
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 Agent
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15036	Evaluating Authorization Policy
90500	New Identity Mapping
5236	Authorize-Only succeeded

PassiveID	لم اوخ	رثأ	passiveid-*.log
PxGrid	pxgrid	رثأ	pxgrid-server.log
SXP	sxp	ءاطخألا حىحصت	sxp.log

 حىحصت نبيعت ةداع| ركذت ، اءال صء او ءاطخألا فاشك تسأ نم ءاهت نالا دنع : ةظءالم Reset to Default. قوف رقن او ةلصل اءاذ ةدقعل دىءت وءاطخألا

ءالءسل ءاصاصق

1. رءومل نم لوءءل لىءسء ءاءء ISE مءلسى .

Passiveid-*.log file:

```
2022-09-06 20:28:31,309 DEBUG [Grizzly-worker(27)][[]] com.cisco.idc.agent-probe- Received login event.
Identity Mapping.probe = Agent , dc-host = /10.10.10.132 , Identity Mapping.server = ise-3-2 , event-operation-
type = ADD ,

2022-09-06 20:28:31,309 DEBUG [Grizzly-worker(27)][[]] com.cisco.idc.agent-probe- Validating incoming logging
event...

2022-09-06 20:28:31,309 DEBUG [Grizzly-worker(27)][[]] com.cisco.idc.agent-probe- Building login event to be
published to session directory.
2022-09-06 20:28:31,309 DEBUG [Grizzly-worker(27)][[]] com.cisco.idc.agent-probe- retrieving user's additional
information from Active Directory.

2022-09-06 20:28:31,326 DEBUG [Grizzly-worker(26)][[]] com.cisco.idc.agent-probe- Forwarded login event to
session directory. Identity Mapping.id-src-first-port = -1 , Identity Mapping.dc-domainname = Lfc.lab , Identity
Mapping.id-src-port-start = -1 , Identity Mapping.probe = Agent , Identity Mapping.id-src-port-end = -1 , Identity
Mapping.event-user-name = smith , Identity Mapping.dc-host = /10.10.10.132 , Identity Mapping.agentId = ,
Identity Mapping.server = ise-3-2 , Identity Mapping.event-ip-address = 10.10.10.10 ,
```

فلم Passiveid-*.log

2. رءنء موقى واهن وءكء مءىءل لىءوءءل ةسءى سل اق فو بىقرل نبيءءب ISE موقى .
SXP ءارظن و PxGrid ءىءرءشم لىل PassiveID ءىءءءسءم ل IP-SGT ءاطءم

فلم sxp.log:

```
2022-09-06 20:28:31,587 DEBUG [sxp-service-http-96443] cisco.ise.sxp.rest.SxpGlueRestAPI:27 - Adding session binding tag=4, ip=10.10.10.10, vns=[], vpns=[null] nasIp=10.10.10.132
2022-09-06 20:28:31,587 DEBUG [sxp-service-http-96443] cisco.ise.sxp.rest.SxpGlueRestAPI:23 - session binding created for ip address : 10.10.10.10/32

2022-09-06 20:28:31,613 DEBUG [SxpNotification] cisco.cpm.sxp.engine.SxpEngine:23 - Adding 1 session bindings

2022-09-06 20:28:31,613 DEBUG [SxpNotificationSerializer-Thread] cisco.cpm.sxp.engine.SxpEngine:42 - Adding session binding RestSxpLocalBinding(tag=4, groupName=null, ipAddress=10.10.10.10/32, nasIp=10.10.10.132, sessionId=cf0d2acd-0d3d-413b-b2fb-6860df3f0d84, peerSequence=null, sxpBindingOpType=ADD, sessionExpiryTimelnMillis=-1, apic=false, routable=true, vns=[DEFAULT_VN]) to VPNs [default]
```

فلم sxp.log

pxgrid-server.log file:

```
2022-09-06 20:28:31,693 TRACE [Grizzly(1)][] cpm.pxgrid.ws.client.WsEndpoint -::: Send. session=[id=b0df936b-bfab-435f-80e6-aa836aa3b24c,client=~ise-fanout-ise-3-2,server=wss://ise-3-2.Lfc.lab:8910/pxgrid/ise/pubsub]
frame=[command=SEND,headers=[content-length=1859, destination=/topic/distributed, from=~ise-fanout-ise-3-2, via=~ise-fanout-ise-3-2],content-len=1859] content=MESSAGE
content-length:1/30
destination:/topic/com.cisco.ise.session
message-id:616
subscription:2
via::~ise-fanout-ise-3-2
{"sessions":[{"timestamp":"2022:09:06T20:28:31.41105:00","state":"AUTHENTICATED","userName":"smith","callingStationId":"10.10.10.10","auditSessionId":"ddda40ec-e557-4457-81db-a36af7b7d4ec",
"ipAddresses":["10.10.10.10"],"nasIpAddress":"10.10.10.132","ctsSecurityGroup":"Employees","adNormalizedUser":"smith",
"adUserDomainName":"Lfc.lab","adUserNetBiosName":"Lfc","adUserResolvedIdentities":"smith@Lfc.lab","selectedAuthzProfiles":["PermitAccess"]},"sequence":13}

2022-09-06 20:28:31,673 TRACE [Grizzly(1)][] cpm.pxgrid.ws.client.WsEndpoint -::: Send. session=[id=b0df936b-bfab-435f-80e6-aa836aa3b24c,client=~ise-fanout-ise-3-2,server=wss://ise-3-2.Lfc.lab:8910/pxgrid/ise/pubsub]
frame=[command=SEND,headers=[content-length=308, destination=/topic/distributed, from=~ise-fanout-ise-3-2, via::~ise-fanout-ise-3-2],content-len=308] content=MESSAGE
content-length:176
destination:/topic/com.cisco.ise.sxp.binding
message-id:612
subscription:2
via::~ise-fanout-ise-3-2
{"operation":"CREATE","binding":{"ipPrefix":"10.10.10.10/32","tag":4,"source":"10.10.10.132",
"peerSequence":["10.10.10.135,10.10.10.132"],"vpn":"default"},"sequence":17}
```

فلم pxgrid-server.log

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا 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 ة 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 (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا