ليمعلل نمآلا NAM فيرعت فلم نيوكت Windows ىلع ISE 3.3 لالخ نم ەرشنو

تايوتحملا

<u>ةمدقملا</u> <u>قيساسأ تامولعم</u> <u>قيساسألاا تابلطتملا</u> <u>تابلطتملا</u> <u>ةمدختسملا تانوكملا</u> <u>نى وك ت ل ا</u> <u>ةكېشلل يطيطختلا مسرلا</u> <u>تانايٻلا قفدت</u> <u>لوحملا نېوكت</u> <u>Secure Client ةمزح ليزنت</u> ISE نىوكت ISE يالع قمزجانا ليمجت 1. قوطخانا <u>فيرعتالا فالم ررحم ةادأ نم NAM فيرعت فالم ءاشنا. 2 ةوطخارا</u> <u>ISE ىلع NAM فيرعت فلم ليمحت .3 ةوطخلا</u> <u>عضولاً فيرعت فلم ءاشناً .4 ةوطخلاً</u> <u>ليكولا نيوكت ءاشنا .5 ةوطخلا</u> <u>لېمعلا رېفوت چەن .6 قوطخلا</u> <u>عضولا جەن .7 ةوطخلا</u> <u>قكبش زاهج ةفاض| .8 ةوطخلا</u> <u>ليوختايا فيرعت فالم .9 ةوطخايا</u> <u>اەب جومسمالا تالوكوتورىلا. 10 قوطخارا</u> طش نلا لي لدلا. 11 قوطخلا <u>چەنلا تاغومچم .12 قوطخلا</u> <u>قحص ل انم ق ق حت ل ا</u> اهتى المتكانية ا <u>2. EAP-FAST ةوطخلا</u> <u>يعضو حسم .3 ةوطخلا</u> <u>اهحالصاو ءاطخألا فاشكتسا</u> <u>NAM فيرعت فلم .1 ةوطخلا</u> <u>عسومالا NAM ليجست .2 ةوطخاا</u> <u>لوحملا يلع ءاطخألا جيجصت.3 ةوطخلا</u> ISE <u>يلع ءاطخألا جي حصت 4 قوطخلا</u> <u>ةلص تاذ تامولعم</u>

ةمدقملا

نمآلا ليمعلا ةكبش ىلإ لوصولا ريدم فيرعت فلم رشن ةيفيك دنتسملا اذه حضوي (NAM) تيوهلا تامدخ كرحم لالخ نم Cisco نم (NAM)

ةيساسأ تامولعم

ةحفاصم EAP-FAST مدختسي ،ىلوألاا ةلحرملاا يف .نيتلحرم يف EAP-FAST ةقداصم ثدحت (TLV) لوطلا عونلا ميق تانئاك مادختساب حيتافملا تالدابم ةقداصمو ريفوتل TLS ةقداصملاب ةقلعتملا تانايبلا لقنل هذه TLV تانئاك مادختسا متي .يمحم قفن ءاشنإل ليمعلا ةدقع طارخناب ةيناثلا ةلحرملا أدبت ،قفنلا ءاشنا درجمبو .مداخلاو ليمعلا نيب ضيوفتلاو ةقداصملا تاسايس ءاشنإل تاثداحملا نم ديزم يف (ISE) ةيوهلا تامدخ دهعمو المحيول

رفوتيو ةقداصم ةقيرطك EAP-FAST مادختسال NAM نيوكت فيرعت فلم دادعإ متي ايرادإ ةفرعملا تاكبشلل.

فلم نمض مدختسملاو زاهجلا لاصتا عاوناً نم الك نيوكت نكمي ،كلذ ىلإ ةفاضإلابو نيوكت فيرعت NAM.

عم NAM مادختساب ةكرشلا ىلإ لماك لوصو ىلع ةكرشلاب صاخلا Windows زاهج لصحي صحف Posture.

نيوكت سفن مادختساب ةديقم ةكبش ىلإ لوصولا قح يصخشلا Windows زاهج بستكي NAM.

فيرعت فلم رشنل تاميلعت دنتسملا اذه مدقي Cisco Secure Client Network Access Manager (NAM) ةيوهلا تامدخ كرحم ةيعضو لخدم ربع (ISE) قيوهلا تامدخ كرحم قيعضو لخدم ربع (JSE) . عضولا قفاوت نم ققحتلا يلإ.

ةيساسألا تابلطتملا

تابلطتملا

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- (ISE) ةيوەلا تامدخ كرحم •
- AnyConnect NAM و فيرعتالا فالم ررحم •
- عضولا جەن •
- تامدخل Cisco Catalyst نيوكت 802.1x

ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملاو جماربلا تارادصإ ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست

- Cisco ISE، اثدحألا تارادصإلاو 3.3 رادصإلا
- Windows 10 عم Cisco Secure Mobility Client 5.1.4.74 ثدحألا تارادصإلاو
- ثدحألاا تارادصإلاو Cisco IOS® XE 17.6.5 جمانربب Cisco Catalyst 9200 switch لوحملا
- Active Directory 2016

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا عاشنإ مت. تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألاا عيمج تأدب رمأ يأل لمتحملا ريثأتلل كمەف نم دكأتف ،ليغشتلا ديق كتكبش.

نيوكتلا

ةكبشلل يطيطختلا مسرلا



تانايبلا قفدت

لخدم ىلٍ ەيجوتلا ةداعإل ليوختلا جەن ISE رفوي ،ةكبشلاب رتويبمك زاەج لصتي امدنع عضولا

ليمع دادمإ ةحفص ىلإ يصخشلا رتويبمكلا ىلع HTTP تانايب رورم ةكرح هيجوت ةداعإ متت ISE، نم NSA قيبطت ليزنت متي ثيح ،ISE

رتويبمكلا ىلع ليغشتلا ةداعإ ليغشت ىلإ NAM ةدحو تيبثت يدؤي.

فيرعت فلم ىلإ ادانتسا EAP-FAST ةقداصم ذيفنتب NAM ةدحو موقت ،ليغشتلا ةداعإ دعب NAM.

نم ققحتلا متيو ((ISE) ةيوهلا تامدخ كرحم ةيعضو) Posture صحف ليغشت كلذ دعب متي ISE. عضو جهن ىلإ ادانتسا قفاوتلا

لوحملا نيوكت

.هيجوتلا ةداعإو dot1x ةقداصمل لوصولا لوحم نيوكتب مق

```
ديدج AAA جذومن
ةيضارتفالاا ةعومجملا رطق فصن AAA1x ةقداصم ةطقن
AAA ضيوفت ةكبشل ةيضارتفالاا ةعومجملا رطق فصن
منارتفا فاقيإ-ءدب ةعومجم رطق فصنل xAA1x قبساحم ةطقن
AAA مداخ رطق فصنل يكيمانيدلاا فلؤملا
client 10.127.197.53 server-key qwerty123
Any عونلا-ةقداصملا
```

كرتشم id-ةسلج AAA

ip radius source-interface vlan1000 مداخ ةمس RADIUS 6 on-for-login-auth مداخ ةمس ADIUS 8 مراخ قمس 25 لوصولا بلط نمضتي radius مداخ قمس 25 لوصولا بلط نمضتي mac ietf مداخ قمس ايلعلاا ةلاحلا نم mac ietf قيسنت 31 رطقلا فصن مداخ قمس RADIUS RAD1 قيسنت 31 دفنملا RADIUS RAD1 ناونع secret-key>

dot1x system-auth-control

لخدم ىلإ ەەيجوت ةداعإ دارملا مدختسملل ەيجوتلا ةداعإل لوصولا يف مكحتلا ةمئاق نيوكت اليمع دادمإ ISE.

ن تو مول ا لوصول ا يف مكحتل ا قمئاق ip access-list 10 لجم يأ UDP ضفر 20 لوم 20 لجم يأ TCP ضفر 30 ليغشت ديەمت قمظنا يأل EQ BOOTPC ليغشت ديەمت ماظن يأل UDP لوكوتورب ضفر 30 ب قصاخ 40 ب قصاغ ISE Server IP> 50 الوكوتورب يأ مادختساب حامسل EQ mww 60 حيرصت TCP ي eq 443

لوحملا ىلع HTTP ەيجوت ةداعإو زاەجلا بقعت نيكمتب مق.

حةزمجألاا بقعت جەن مسا> ةزمجألاا بقعت جەن بقعتلا نيكمت نراق<interface name> زامجلا جەن قافراب صاخلا <زامجلا بقعت جەن مسا>

ip http server ip http secure-server

Secure Client ةمزح ليزنت

ايودي Profile Editor و Secure Client Windows و Compliance Module Webdeploy Files ايودي <u>software.cisco.com</u> نم

5. نمآلا ليمعلا جتنملا مسا نع ثحبلا طيرش عون يف

كلذ يف امب) نمآلا ليمعلا < ةياهنلا ةطقن نامأ < نامألا < تاليزنتلل ةيسيئرلا ةحفصلا AnyConnect VPN ليمع جمانرب < 5 نمآلا ليمعلا < (AnyConnect VPN

Cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg

- · Cisco-secure-client-win-4.3.4164.8192-isecompliance-webdeploy-k9.pkg
- tools-Cisco-secure-client-win-5.1.4.74-profileeditor-k9.msi

ISE نيوكت

ISE ىلع ةمزحلا ليمحت .1 ةوطخلا

زكرم ىلإ لقتنا ،ISE ةدجو لالخ نم قفاوتلاو نمآلا ليمعلاب ةصاخلا بيولا رشن مزح ليمحتل يلحملا صرقلا نم ليكولا دراوم < ةفاضإ < دراوملا < ليمعلا دادمإ < Posture < لمعلا

Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
Client Provis Resources Client Provis	iloning Policy iloning Portal	Agent Resources From Local Agent Resources Fr	Disk > Agent Resources Fro	om Local Disk				
		Category	Cisco Provided Pacl	kages ✓	()			
			 Agent Uploaded Name 	Resources	јуре	١	/ersion I	Description
			CiscoSecureClientDes	ctopWindows 5.1	CiscoSecureClientDe	esktopWindows	5.1.4.74	Cisco Secure Client for
		Submit						

Overview	Network Devices	Client Pr	ovisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings		
Client Provisi	oning Policy	Pos									
Resources		Rest	Juices								
Client Provisi	oning Portal	🖉 Edit		🖒 Duplicate 🔋 Deid	ote						
			Name			Туре	Version	Last Upda	te 🗸	Description	
			Lab Profile			AgentProfile	Not Applicable	2024/07/2	26 17:23:41		
			Agent Configu	ration		AgentConfig	Not Applicable	2024/07/2	26 16:00:49		
			NAM Profile			AgentProfile	Not Applicable	2024/07/2	26 16:00:00		
			CiscoSecureC	lientComplianceModul	eWindows 4.3.4164	CiscoSecureClientCo	o 4.3.4164.8192	2024/07/2	26 15:58:44	Cisco Secure Client Win	
			CiscoSecureC	lientDesktopWindows	5.1.4.074	CiscoSecureClientDe	a 5.1.4.74	2024/07/2	26 15:56:27	Cisco Secure Client for	
			Cisco-ISE-NSI	P		Native Supplicant Pro	o Not Applicable	2023/07/0	04 05:25:16	Pre-configured Native S	
			CiscoAgentles	sOSX 5.0.03061		CiscoAgentlessOSX	5.0.3061.0	2023/07/	04 04:24:14	With CM: 4.3.3045.6400	

فيرعتلا فلم ررحم ةادأ نم NAM فيرعت فلم ءاشنإ .2 ةوطخلا

<u>ىنيوكت</u> ليلدلا اذه ىلإ عجرا ،NAM فيرعت فلم نيوكت ةيفيك لوح تامولعم ىلع لوصحلل

. <u>ليمعلل نمآلا NAM فيرعت فلم</u>

ISE ىلع NAM فيرعت فلم ليمحت .3 ةوطخلا

دادمإ ىلإ لقتنا ،ليكو فيرعت فلمك ISE ىلع "NAM "configuration.xml فيرعت فلم ليمحتل يلحملا صرقلا نم ليكولا دراوم < دراوملا < ليمعلا

Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
Client Provision Resources	oning Policy oning Portal	Agent Resources From Local Agent Resources From	Disk > Agent Resources Fro	om Local Disk				
		Category	Customer Created F	Packa: Y				
		Туре	Agent Profile	~				
		* Name	New Profile					
		Description						
			Choose File configu	uration.xml				
		Submit						

عضولا فيرعت فلم ءاشنإ .4 ةوطخلا

Overview Network Devi	ces Client Pro	visioning	Policy Elem	ents	Posture Policy	Policy	Set
Client Provisioning Policy							
Resources	Reso	urces					
Client Provisioning Portal	🖉 Edit	$+$ Add \wedge	Duplicate	🗊 Dele	ete		
		Agent reso	urces from Cisco si	ite		Version	La
		Agent reso	urces from local dis	sk	oSecureClientCo	4.3.4164	20
		Native Sup	plicant Profile		ıtConfig	Not Applic	20
		Agent Cont	investion		e Supplicant Pro	Not Applic	20
		Agent Post	ure Profile		oAgentlessWind	5.0.3061.0	20
		AMP Enable	er Profile		DsXSPWizard	2.7.0.1	20
		NAM Profile		Ager	ntProfile	Not Applic	20

Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets T
Client Provis	ioning Policy		tings > Lab Profile		
Client Provis	ioning Portal	Agent Posture Profil Name * Posture Profile Description: Agent Behavior	e		
		Parameter		Value	
		Enable debug log		Yes	~
		Operate on non-802.	1X wireless	No	~
		Enable signature cheo	* (i)	No	~

مداوخلا عيمجب لاصتالاب ليكولل حامسلل * ةفاضإ سنت ال ،عضولا لوكوتورب مسق نم.

ليكولا نيوكت ءاشنإ .5 ةوطخلا

Overview	Network Devices	Client Prov	/isioning	Policy E	lements	Posture Policy	/
Client Provision	oning Policy	D					
Resources		Reso	urces	;			
Client Provision	oning Portal	🖉 Edit	+ Add	Duplicate	n 🗊 Dele	te	
			Agent re	esources from Cis	sco site		Ver
			Agent re	esources from loc	al disk	oSecureClientCo	4.3
			Native S	Supplicant Profile		ntConfig	Not
			Agent C	onfiguration		e Supplicant Pro	Not
			Agent P	osture Profile	•	oAgentlessWind	5.0
			AMP En	abler Profile		DsXSPWizard	2.7
			NAM Profi	e	Ager	tProfile	Not

ةدحولا ديدحت نمض اهليمحت مت يتلاا نمآلا ليمعلاو قفاوتلل ةيطمنلا ةدحولا ةمزح ددح DART تادحوو NAM ةكرحو (ISE) ةيوهلا تامدخ كرحم ةيعضو ددح ،ةيطمنلا

Engine			Work	Centers / P	Posture	
Overview	Network Devices	Client Provisioning	Policy I	Elements	Posture Policy	Policy Sets
Client Pro	ovisioning Policy	Agent Configuration > New Ag	jent Config	uration		
Resource	s					
Client Pro	ovisioning Portal					
		* Select Agent Package:		CiscoSecure	ClientDesktopWindo	ws 5.1 🗸
		* Configuration Name:		Agent Config	guration	
		Description:				
		Description Value Not	tes			
		* Compliance Module	с —	iscoSecureClie	entComplianceModul	e₩~
		Cisco Secure Client N	lodule	Selection		
		ISE Posture				
		VPN				
		Zero Trust Access				
		Secure Firewall Posture				
		Network Visibility				

لاسرا قوف رقناو NAM فيرعت فلمو عضولا رتخأ ،ديدحت فيرعت فلم تحت.

Overview	Network Devices	Client Provis	ioning	Policy Elements	Posture	Policy
Client Provisi	oning Policy	Umbrella Start Before				
Resources		Logon				
Client Provision	oning Portal	Diagnostic and Reporting Tool				
		Profile Sele	ction			
		* ISE Posture	Posture Pr	ofile	~	
		VPN			~	
		Network Access Manager	NAM Profil	le	~	
		Network Visibility			~	
		Umbrella			~	
		Customer Feedback			~	

ليمعلا ريفوت جەن .6 ةوطخلا

مت يذلا ليكولا نيوكت ددحو Windows ليغشتلا ماظنل ليمع ريفوت جەن ءاشنإب مق ةقباسلا ةوطخلا يف ەؤاشنإ.

Overview	Network Devices	Client Provi	isioning Pol	icy Elements	Posture Po	licy	Policy Sets	Troublesh	oot Rep	orts Settings				
Client Provisi Nesources Client Provis	ioning Policy	Client Define the Cli For Agent Co For Native Su Windows Age Intel architect For Windows Mac ARM64 µ If you configu without an Af	Provisioning P Infiguration: version pplicant Configura Int, Mac Agent, Ma Urues. Mac policies Agent ARM64 poli osolicies require no re an ARM64 clien XM64 condition. Th	bing Policy olicy to determine of agent, agent ticen: wizard profile with the same par- cies, configure St Other Conditions to provisioning pol- is is because an o	what users will profile, agent co e and/or wizard. Ac Agentless po kage for both an ession: OS-Archi arm64 configura cy for an OS, en endpoint is matc	receive u mpliance Drag and blicies su rchitecture E trions. asure that hed sequ	upon login and us module, and/or a d drop rules to ch pport ARM64. Wi res. :QUALS arm64 in t the ARM64 polic ientially with the j	er session initia agent customizz lange the order, indows policies the Other Conc cy is at the top o policies listed in	tion: tion package. run separate p lítions column. of the condition this window.	ackages for ARM4 ar	nd			
			Rule Name		Identity Group	•	Operating Sys	items	Other Con	ditions		Results		
		8 🖬	IOS		Any	and	Apple IOS All		d Condition(s)		ther	Cisco-ISE-NSP		A
		: .	Android	r	Δinv	and	Android	ar	d Condition(s)		ther	Cisco-ISE-NSP	Edit of	
		8 😖	Windows		Any	and	Windows All		d Condition(s)		ther	Agent Configuration	Edit 🗸	1
		∷ ☑	MAC OS	ц	Any	and	Mac OSX	ar	d Condition(s)		then	CiscoTemporalAgentOSX 5.0.03061 And MacOsXSPWizard 2.7.0.1 And Cisco-ISE- NSP	Edit 🜱	Ľ.
		8 💌	Chromebook		Any	and	Chrome OS All		d Condition(s)		then	Cisco-ISE-Chrome-NSP		•
													Save	Reset

عضولا جەن .7 ةوطخلا

ر<u>شنال ليالد</u> ىلإ عجرا ،ەطورشو عضولا ةسايس ءاشنإ ةيفيك لوح تامولعم ىلع لوصحلل <u>ال ا</u>ذه <u>يعضول ISE Posture</u> .

ةكبش زاهج ةفاضإ .8 ةوطخلا

.ةكبشلا دراوم < ةرادإ ىلإ لقتنا ،كرتشملا RADIUS رس حاتفمو لوحملل IP ناونع ةفاضإل

Engine		Administr	ation / Network Resou	irces
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Serve	rs RADIUS Server Se
Network Devices Default Device Device Security Settings	Network Devices	List > aaa evices		
	Name Description			
	IP Address	• ✓ ^{* ⊮} 10.197.213.22	2 [/] 32 🕸	
	Device Profil	e 🏄 Cisco	✓ ①	
	Model Name		~	

Engine			Administr	ration / Network Resource	S
Network Devices	Network Dev	vice Groups Ne	twork Device Profiles	External RADIUS Servers	RADIUS Server Sequences
Network Devices		Device Type	All Device Types	Set To D	Default
Default Device Device Security Settings		🗹 🗸 Radiu	IS Authentication Settin	ngs	
		RADIUS	UDP Settings		
		Protocol	RADIUS		
		Shared Se	ecret	Show	
		Use S	Second Shared Secret 🕦		
			Second Shared Secret		
		CoA Port	1700		Default

ليوختلا فيرعت فلم .9 ةوطخلا

< ةسايسلا رصانع < ةسايسلا ىل لوتنا ،ةيعضولل ەيجوت ةداعإ صيصخت فلم ءاشنإل جئاتنلا.

Engine				Policy / Policy Elements
Dictionaries Conditions	Result	ts		
Authentication Authorization Authorization Profiles Downloadable ACLS	> ~	Stan For Policy	Export go to Administration > Sys	tion Profiles stem > Backup & Restore > Policy Export Page Delete
Profiling	>		Name	Profile
Posture	>			🏙 Cisco 🥡
Client Provisioning	>		Cisco_IP_Phones	🏙 Cisco 🥡
			Cisco_Temporal_Onboard	🏭 Cisco i

ةداعإل (ACL) لوصولا يف مكحتلا ةمئاق عم ليمعلا ديوزت لخدم ددح ،رماوألا ةمەم تحت ميجوتلا.

Dictionaries Conditions	Results
Authentication >	Authorization Profiles > Redirection
Authorization V	* Name Redirection
Downloadable ACLs	Description
Profiling > Posture >	* Access Type ACCESS_ACCEPT ~
Cilent Provisioning >	Network Device Profile 🗮 Cisco 🗸 🕀
	Service Template
	Passive Identity Tracking 🔲 🕤
	✓ Common Tasks ✓ Web Redirection (CWA, MDM, NSP, CPP) O Client Provisioning (Posture) ✓ ACL redirect-acl ✓ Value Client Provisioning Portal (defi
	Static IP/Host name/FQDN Suppress Profiler CoA for endpoints in Logical Profile

اەب حومسملا تالوكوتوربلا. 10 ةوطخلا

حومسملا تالوكوتوربلا < ةقداصملا < جئاتنلا < ةسايسلا رصانع < ةسايسلا ىل لقتنا لسلست تادادعإ ددح ،اهب EAP،

Dictionaries	Conditions		Results
Authentication		~	Allowed Protocols Services List > Default Network Access
Allowed Proto	cols		Allowed Protocols
Authorization		>	Name Default Network Access
Profiling		>	Description Default Allowed Protocol Service
Posture		>	



طشنلا ليلدلا. 11 ةوطخلا

اذإ تالاجملا تاعومجم ديدحت متو Active Directory لاجم ىلا ISE قحص نم ققحتلا مامضنا مت ليوختلا طورشل رمألا مزل.

Active Directory < ةيجراخلا ةيوەلا رداصم < ةيوەلا ةرادإ < ةرادإ

Engine		Administration / Identity Management
Identities	Groups External Identity Sc	purces Identity Source Sequences Settings
	External Identity Sources	Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
	 Certificate Authenticat Active Directory PRAD LDAP 	* Join Point Name PRAD O * Active Directory Domain aaa.prad.com O
	ODBC RADIUS Token RSA SecuriD	ISE Node ∧ ISE Node R Status Domain Controller Site pk3-3.aaa.prad.com PRIMARY Z Operational CXLabs-WIN2022.aaa.pr Default-First-Site-Na
	 SAML Id Providers Social Login 	

جەنلا تاعومجم .12 ةوطخلا

تاعومجم < ةسايسلا ىلإ لقتنا .dot1x بلط ةقداصمل ISE ىلع جەن ةعومجم ءاشنإب مق . تاسايسلا

Engi	ne				Policy / Policy Sets	🔺 Evoluntic	m Mode 87 Days	Q	۵	0	Q X
	Policy	/ Sets]			Reset					Save
		Status	Policy Set Name	Description	Conditions	Allowed Protocols /	Server Seque	ice	Hits	Actions	View
	C	Search									
			Dot1x Policy		Wired_802.1X	Default Network Acc	xess /			¢	
			Default	Default policy set						ŵ	

ةقداصملا جەنل ةيوە ردصمك Active Directory ددح.

~Authenticatio	n Policy(1)							
🔶 Status	Rule Name	Conditions			Use		Hits	Actions
Q Searc								
					PRAD	<u> </u>		
	Default			-	> Options			ŝ

ةقڧاوتم ريغو ةڧورعم ريغ عضولا ةلاح ىلإ ادانتسا ةڧلتخم ليوخت دعاوق نيوكتب مق ةقڧاوتمو.

ەذە مادختسالا ةلاح يف.

- فلمو نمآ ليمع تيبثتل ISE ليمع دادمإ ةباوب ىلإ هيجوتلا ةداعإ :يلوألا لوصولا فيرعت NAM
- ةداعإ ىلإ دنتسملا عضولا فاشتكال ليمعلا دادمإ لخدم ىلإ لوصولا :فورعم ريغ لوصو هيجوتلا
- ، قكبشلا ىل إلماكلا لوصول :قفاوتم لوصو
- لوصولا ضفر :قفاوتم ريغ •

∼Auth	norization	Policy(5)						
					Results			
÷	Status	Rule Name	Cond	litions	Profiles	Security Groups	Hits	Actions
C) Search							
		Non-compliant Access	AND	E Session-PostureStatus EQUALS NonCompliant Session-PostureStatus EQUALS User and machine both succeeded				ŝ
		Unknown Access	AND	Equals Unknown Network Access EapChainingResult EQUALS User and machine both succeeded	Redirection			¢
		Compliant Access		L: Session-PostureStatus EQUALS Compliant Q: Network Access-EapChainingResult EQUALS User and machine both succeeded				¢
		Initial Access		PRAD-ExternalGroups EQUALS aaa.prad.com/Users/Domain Computers	Redirection			¢
		Default						¢
						Reset		Save

ةحصلا نم ققحتلا

اهتيبثتو ISE نم Secure Client Posture/NAM ةدحو ليزنت .1 ةوطخلا

ليوخت ةدعاق ىلع طغضلا عم ،dot1x لالخ نم اهتقداصم تمت يتلا ةياهنلا ةطقن ددح ةرشابملا تالجسلا < RADIUS < تايلمعلا ىل لقتنا ."يلوألا لوصولا

Ø	Seset Repeat Counts	🖒 Export To	~						Filter 🗸 🤞
	Time	Status	Details	Endpoint ID	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
				B4:96:91:F9:56:8B					
	Jul 27, 2024 12:10:17	•	6			Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending
	Jul 27, 2024 12:10:17	2	lõ			Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending
	Jul 27, 2024 12:09:31		là -			Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending

اەقيبطت متي يتلا لوصولا يف مكحتلا ةمئاقو ەيجوتلا ةداعإل URL ناونع ددح ،لوحملا ىلع .قياەنلا ةطقن ىلع

ليصافت Switch#show Authentication Session Interface te1/0/24 i TenGigabitEthernet1/0/24 i IIF: 0x19262768 i MAC: x4x6.xxxx.xxx فورعم ريغ :Pv6: خيم ريغ :IPv6: حاين i Pv4: <client-IP> i مدختسمل ا مس i host/DESKTOP-xxxxx.aaa.prad.com ن من عمن ا مس i امهال : الياجمل ا coper Control dir: ن امهال يداحأ i امهال : المعل ا قسل جام رفوتم ريغ : المعل ا قسل جل ا فرعم رمام ا قسل جل ا فرعم ن مرما ا المعل ا الالحيا ا المراح ا رشۇملا: 0x7a00017 ةيلاحلا ةسايسلا: POLICY_TE1/0/24

ةيلحملا تاسايسلا: قمدخلا بلاق: default_linksec_policy_should_secure (priority 150) نيمأت بجي :نامألا جەن طابترالا نيمأت متي مل :نامألا قلاح

مداخلاا جەن: جوتلا ةداعإل (ACL) لوصولا يف مكحتلا ةمئاق :URL ەيجوت ةداعإل (ACL) لوصولا يف مكحتلا ةمئاق URL: <u>https://ise33.aaa.prad.com:8443/portal/gateway?sessionId=16D5C50A0000002CF067366A&portal=ee39</u> <u>7180-4995-8aa2-9fb282645a8f&action=cpp&token=518f857900a37f9afc6d2da8b6fe3bc2</u> ل لوصولا يف مكحتلا ةمئاق

بولسألا ةلاح ةمئاق: بولسألا ةلاح dot1x Authc حاجن

Switch#sh1/0/24 زاەجلا بقعت تانايب ةدعاق ةەجاو

راسيلاا ىلإ ةلاحلا رمع vlan ن نراق ناونع ةقبط طبر ةكبشلا ناونع ةقبط 0 لواحي ARP X.X.X b496.91f9.568b TE1/0/24 1000 005 4mn Reachable 39 S

ةيعضو) ISE Posture ىلإ اەەيجوت ةداعإ تمت يتلا رورملا ةكرح نم ققحت ،ةياەنلا ةطقن ىلع .ةياەنلا ةطقن ىلع ةكبشلا دادعإ دعاسم ليزنتل ءدب قوف رقناو ((ISE) ةيوەلا تامدخ كرحم





.NSA قيبطت تيبثتل ليغشت ىلع رقنا



(عضولا) Posture تبثيو ISE نم "نمآلا ليمعلا ليمع" ليزنت ءاعدتساب NSA موقي ،نآلاو

. NAM.xml فيرعت فلم نيوكتو NAM.xml ةدحوو



معن ةقطقط .NAM تيبثت دعب ليغشتلا ةداعإ ةبلاطم ليغشت مت.



2. EAP-FAST ةوطخلا

نم لك ةقداصمب NAM موقت ،مدختسملا لوخد ليجستو رتويبمكلا ليغشت ةداعإ درجمب لالخ نم زاهجلاو مدختسملا EAP-FAST.

ةدحولاا نأو ةلصتم اەنأ ضرعي NAM نإف ،حيحص لكشب ةياەنلا ةطقن ةقداصم تمت اذإ ةيعضولل يئوضلا حسملا ليغشتب موقت عضولل ةيطمنلا.

() Cisco Secur	re Client		3 - 3		×
	AnyConnect VPN: Ready to connect.	~] (Connect	
	Network: Connected (wired	· · · · · · · · · · · · · · · · · · ·	2	& ~	
	ISE Posture: Scanning system	10%	Sc	an Again	
\$ (1)					4 14 15

.فورعملا ريغ لوصولا ةدعاق ىلإ لوصولاب نآلا ةياەنلا ةطقن موقت ،ISE Live تالجس ىلع



جئاتنو NAM فيرعت فلم نيوكت ىلإ دنتسي EAP-FAST ةقداصملا لوكوتورب نآلا جئاتنو NAM فيرعت فلم نيوكت يل دنتسي EAP تقداصمل

AcsSessionID	pk3-3/511201330/230
NACRadiusUserName	user1
NACRadiusUserName	host/DESKTOP-QSCE4P3
SelectedAuthenticationIden	PRAD
AuthenticationStatus	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatched	Unknown Access
IssuedPacInfo	Issued PAC type=Machine Authorization with expiration time: Sat Jul 27 01:29:06 2024
EndPointMACAddress	
EndPointMACAddress EapChainingResult	User and machine both succeeded
EndPointMACAddress EapChainingResult ISEPolicySetName	User and machine both succeeded Dot1x Policy
EndPointMACAddress EapChainingResult ISEPolicySetName IdentitySelectionMatchedRule	User and machine both succeeded Dot1x Policy Default
EndPointMACAddress EapChainingResult ISEPolicySetName IdentitySelectionMatchedRule AD-User-Resolved-Identities	User and machine both succeeded Dot1x Policy Default user1@aaa.prad.com
EndPointMACAddress EapChainingResult ISEPolicySetName IdentitySelectionMatchedRule AD-User-Resolved-Identities AD-User-Candidate- Identities	User and machine both succeeded Dot1x Policy Default user1@aaa.prad.com
EndPointMACAddress EapChainingResult ISEPolicySetName IdentitySelectionMatchedRule AD-User-Resolved-Identities AD-User-Candidate- Identities AD-Host-Resolved-Identities	User and machine both succeeded Dot1x Policy Default user1@aaa.prad.com User1@aaa.prad.com

يعضو حسم .3 ةوطخلا

صحفلا ليغشتب (ةنمآلا ليمعلا ةيعضو) Secure Client Posture ةيطمنلا ةدحولا موقت ISE. ةيعضو جەن ىلإ ادانتسا ىوكشك ةمالع عضو متيو (ليمعلا ةيعضو)

Sisco Secure Client	- 🗆 X
AnyConnect VPN: Use a browser to gain access.	✓ Connect
Web Authentication Required	
Network: Connected () wired	ैक्र ∽ ः≡
ISE Posture: Compliant. Network access allowed.	Scan Again
Ö (1)	apap
m U	CISCO

جەن ىلٍ لوصولاب ةياەنلا ةطقن موقت نآلاو يئوضلا Posture حسم دعب CoA ليغشت متي ىوكشلا ىلٍ لوصولا.

ø										٩
	Time	Status	Details	Endpoint ID	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status	
×				84:96:91:F9:56:88						
	Jul 27, 2024 12:29:32	•	18			Dot1x Policy >> Default	Dot1x Policy >> Compliant Access	PermitAccess	Compliant	
	Jul 27, 2024 12:29:32	۵	ъ			Dot1x Policy >> Default	Dot1x Policy >> Compliant Access	PermitAccess	Compliant	÷
	Jul 27, 2024 12:29:31	٠	18						Compliant	÷
	Jul 27, 2024 12:29:06		16			Dot1x Policy >> Default	Dot1x Policy >> Unknown Access	Redirection		÷
	Jul 27, 2024 12:28:48	2	lò.		host/DESKTOP-QSCE4P3	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending	÷

اهحالصإو ءاطخألا فاشكتسا

NAM فيرعت فلم .1 ةوطخلا

يصخشلا رتويبمكلا ىلع راسملا اذه يف NAM configuration.xml فيرعت فلم دوجو نم ققحت ةيطمنلا NAM ةدحو تيبثت دعب.

C:\ProgramData\Cisco\CiscoSecure Client\Network Access Manager\System

> Th	is PC > Local Disk (C:) > ProgramData > Cisc	o > Cisco Secure Clien	t > Network Access	Manager > system
	Name	Date modified	Туре	Size
	configuration	7/26/2024 4:53 PM	XML Document	7 KB
ж	internalConfiguration	7/27/2024 12:27 AM	XML Document	3 KB
A	userConfiguration	7/27/2024 12:27 AM	XML Document	1 KB
*				
*				

عسوملا NAM ليجست .2 ةوطخلا

"تادادعإلا" زمر ددحو ماهملا طيرش نم نمآلا ليمعلا زمر ىلع رقنا".

Cisco Secur	e Client	2-2		\times
	AnyConnect VPN: Ready to connect.		Connect	
	Network: Connected () wired		X ~	
	ISE Posture: Compliant. Network access allowed.	-	Scan Again	
☆ ①				-ili.ili. cisco

ليجستلا نيكمت رايتخالا ةناخ ددح .لجسلا تادادعإ بيوبتلا ةمالع < ةكبشلا ىلإ لقتنا عسوملا

تياباغيم 100 ىلإ ةمزحلا طاقتلا فلم مجح نييعت.

.ةياەنلا ةطقن ىلع DART ةمزح ءاشنإل صيخشتلا قوف رقنا ،رادصإلا جاتنإ دعب

cisco Secure	Client
Status Overview	Network Access Manager
AnyConnect VPN	Configuration Log Settings Statistics Message History
Network :	
ISE Posture	IHV: Off ~
	Filter Driver: Off Credential Provider Packet Capture Maximum Packet Capture File Size (MB):
Collect diagnostic information for all installed components.	

اهذيفنتب NAM تماق ةوطخ لك ليصافت لئاسرلا تاظوفحم مسق ضرعي.

لوحملا ىلع ءاطخألا حيحصت .3 ةوطخلا

.قفدت redirection و dot1x ىرحتي نأ حاتفملا ىلع طبضي اذه تنكم

debug ip http all

debug ip http تاكرح

debug ip http url

set platform software trace smd switch active R0 aaa debug set platform software trace smd عطشن جاتفم R0 dot1x-all debug set platform software trace smd switch active R0 radius debug set platform software trace smd switch active R0 auth-mgr-all debug set platform software trace smd switch active R0 eap-all debug set platform software trace smd switch active R0 eap-all debug set platform software trace smd switch active R0 epm-all debug

R0 EPM طشن يساسألا ماظنلا جمانرب عبتتل SMD هيجوت ةداعإ ءاطخأ حيحصت طبض

set platform software trace smd switch active R0 webauth-aaa debug

set platform software trace smd switch active R0 webauth-httpd debug

تالجسلا ضرعل

show logging

show logging process smd يلخاد

ISE ىلع ءاطخألا حيحصت .4 ةوطخلا

عاطخألاا حيحصت ىوتسم ىلع اەنييعت متيس يتلا ةزەجألا ەذە عم ISE معد ةمزح عمجت:

- ةيعضو •
- ةباوب •
- دادمإ •
- Runtime-AAA
- فإ سإ نإ •
- ة MSF-ة ا
- يرسيوس •
- VebApp-ليم

ةلص تاذ تامولعم

<u>نمآلا ليمعلا NAM نيوكت</u>

<u>ISE Posture ل يعضولا رشنالا ليالد</u>

<u>Catalyst 9000 Series Switches تالوحم ىلع امحالصاو Dot1x ءاطخأ فاشكتسأ</u>

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما