# Windows에서 ISE 3.3을 통해 보안 클라이언트 NAM 프로파일 구성 및 구축

# 목차

<u>소개</u>

<u>배경 정보</u>

<u>사전 요구 사항</u> <u>요구 사항</u>

사용되는 구성 요소

#### 설정

<u>네트워크 다이어그램</u>

<u>데이터 흐름</u>

<u>스위치 구성</u>

<u>보안 클라이언트 패키지 다운로드</u>

#### <u>ISE 구성</u>

<u>1단계. ISE에 패키지 업로드</u>

<u>2단계. 프로파일 편집기 도구에서 NAM 프로파일 만들기</u>

<u> 3단계. ISE에 NAM 프로필 업로드</u>

<u>4단계. Posture 프로파일 생성</u>

<u>5단계. 에이전트 구성 생성</u>

<u>6단계. 클라이언트 프로비저닝 정책</u>

<u>7단계. 상태 정책</u>

<u>8단계. 네트워크 디바이스 추가</u>

<u>9단계. 권한 부여 프로파일</u>

<u>10단계. 허용되는 프로토콜</u>

<u>11단계. 액티브 디렉토리</u>

<u>12단계. 정책 집합</u>

#### <u>다음을 확인합니다.</u>

<u>1단계. ISE에서 Secure Client Posture/NAM 모듈 다운로드 및 설치</u>

<u>2단계. EAP-FAST</u>

<u>3단계. 상태 검사</u>

#### <u>문제 해결</u>

<u>1단계. NAM 프로필</u>

<u>2단계. NAM 확장 로깅</u>

<u>3단계. 스위치의 디버깅</u>

<u>4단계. ISE에서 디버깅</u>

<u>관련 정보</u>

소개

이 문서에서는 ISE(Identity Services Engine)를 통해 Cisco Secure Client NAM(Network Access Manager) 프로파일을 구축하는 방법에 대해 설명합니다.

# 배경 정보

EAP-FAST 인증은 두 단계로 이루어집니다. 첫 번째 단계에서 EAP-FAST는 TLS 핸드셰이크를 사 용하여 TLV(Type-Length-Values) 객체를 사용하여 키 교환을 제공하고 인증하여 보호된 터널을 설 정합니다. 이러한 TLV 객체는 클라이언트와 서버 간에 인증 관련 데이터를 전달하는 데 사용됩니다 . 터널이 설정되면 두 번째 단계는 필요한 인증 및 권한 부여 정책을 설정하기 위해 클라이언트 및 ISE 노드가 추가 대화에 참여하는 것으로 시작합니다.

NAM 컨피그레이션 프로필은 EAP-FAST를 인증 방법으로 사용하도록 설정되며, 관리자가 정의한 네트워크에 사용할 수 있습니다.

또한 NAM 컨피그레이션 프로필 내에서 머신 및 사용자 연결 유형을 모두 구성할 수 있습니다. 회사 Windows 장치는 NAM with Posture 검사를 사용하여 완전한 회사 액세스 권한을 얻습니다. 개인 Windows 장치는 동일한 NAM 구성을 사용하여 제한된 네트워크에 액세스할 수 있습니다.

이 문서에서는 웹 배포를 사용하여 ISE(Identity Services Engine) Posture Portal을 통해 Cisco Secure Client NAM(Network Access Manager) 프로필을 배포하는 방법과 함께 Posture Compliance Check를 제공합니다.

# 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Identity Services Engine(ISE)
- AnyConnect NAM 및 프로파일 편집기
- 상태 정책
- 802.1x 서비스를 위한 Cisco Catalyst 구성

# 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE, 릴리스 3.3 이상
- Windows 10(Cisco Secure Mobility Client 5.1.4.74 이상)
- Cisco Catalyst 9200 스위치(소프트웨어 Cisco IOS® XE 17.6.5 이상)
- Active Directory 2016

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

### 네트워크 다이어그램



#### 데이터 흐름

PC가 네트워크에 연결되면 ISE는 포스처 포털로 리디렉션하기 위한 권한 부여 정책을 제공합니다.

PC의 http 트래픽은 ISE 클라이언트 프로비저닝 페이지로 리디렉션되며, 여기서 NSA 애플리케이 션이 ISE에서 다운로드됩니다.

그런 다음 NSA는 PC에 보안 클라이언트 에이전트 모듈을 설치합니다.

에이전트 설치가 완료되면 에이전트는 ISE에 구성된 Posture 프로파일 및 NAM 프로파일을 다운로 드합니다.

NAM 모듈을 설치하면 PC에서 재시작이 트리거됩니다.

다시 시작한 후 NAM 모듈은 NAM 프로필을 기반으로 EAP-FAST 인증을 수행합니다.

그런 다음 Posture 스캔이 트리거되고 ISE Posture Policy에 따라 컴플라이언스가 점검됩니다.

# 스위치 구성

dot1x 인증 및 리디렉션을 위한 액세스 스위치를 구성합니다.

aaa 새 모델

aaa 인증 dot1x 기본 그룹 반경 aaa 인증 네트워크 기본 그룹 radius aaa accounting dot1x default start-stop group radius aaa 서버 radius 동적 작성자 클라이언트 10.127.197.53 서버 키 Qwerty123 인증 유형 any

aaa session-id common ip radius 소스 인터페이스 Vlan1000 radius-server 특성 6 on-for-login-auth radius-server 특성 8 include-in-access-req radius-server 특성 25 access-request 포함 radius-server 특성 31 mac 형식 ietf 대문자 radius 서버 RAD1 주소 ipv4 <ISE 서버 IP> auth-port 1812 acct-port 1813 키 <비밀 키>

dot1x 시스템 인증 제어

사용자가 ISE 클라이언트 프로비저닝 포털로 리디렉션되도록 리디렉션 ACL을 구성합니다.

ip access-list extended redirect-acl 10 deny udp any any eq domain 20 deny tcp any any eq domain 30 deny udp any eq bootpc any eq bootps 40 deny ip any host <ISE server IP> 50 허용 tcp any eq www 60 permit tcp any eq 443

스위치에서 디바이스 추적 및 http 리디렉션을 활성화합니다.

device-tracking policy <device tracking policy name> 추적 사용 인터페이스 <인터페이스 이름> device-tracking attach-policy <device tracking policy name>

ip http 서버 ip http 보안 서버

보안 클라이언트 패키지 다운로드

프로파일 편집기, Secure Client 창 및 Compliance Module webdeploy 파일을 software.cisco.com에서 수동으로 <u>다운로드</u>

제품 이름 검색 표시줄에 Secure Client 5를 입력합니다.

Downloads Home(홈) > Security(보안) > Endpoint Security(엔드포인트 보안) > Secure Client(AnyConnect 포함) > Secure Client 5(보안 클라이언트 5) > AnyConnect VPN Client Software(AnyConnect VPN 클라이언트 소프트웨어)

- cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg
- cisco secure-client-win-4.3.4164.8192-isecompliance-webdeploy-k9.pkg
- ・ 도구-cisco-secure-client-win-5.1.4.74-profileeditor-k9.msi

# ISE 구성

1단계. ISE에 패키지 업로드

ISE에서 Secure Client and Compliance Module webdeploy 패키지를 업로드하려면 Workcenter > Posture > Client Provisioning > Resources > Add > Agent Resources from Local Disk로 이동합니 다.

Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
Client Provisio Resources Client Provisio	oning Policy oning Portal	Agent Resources From Local Agent Resources Fr	Disk > Agent Resources Fr	rom Local Disk				
		Category	Cisco Provided Pac	kages	() 9			
			<ul> <li>Agent Uploaded</li> </ul>	Resources	6		landan f	
			CiscoSecureClientDes	ktopWindows 5.1	ype CiscoSecureClientDe	v esktopWindows 5	5.1.4.74	Cisco Secure Client for
		Sidemi						
		Submit						

Overview	Network Devices	Client Pr	ovisioning	Policy Elem	ents Posture Poli	icy Policy Set	s Troubleshoot	Reports	Settings	
Client Provisi	oning Policy	D								
Resources		Reso	ources							
Client Provisi	oning Portal									
		🖉 Edit		Duplicate	🔋 Delete					
			Name			Туре	Version	Last Upd	ate 🗸	Description
			Lab Profile			AgentProfile	Not Applica	ble 2024/07/	26 17:23:41	
			Agent Config	guration		AgentConfig	Not Applica	ble 2024/07/	26 16:00:49	
			NAM Profile			AgentProfile	Not Applica	ble 2024/07/	26 16:00:00	
			CiscoSecure	ClientCompliance	eModuleWindows 4.3.41	64 CiscoSecure	ClientCo 4.3.4164.81	92 2024/07	26 15:58:44	Cisco Secure Client Win
			CiscoSecure	ClientDesktopWi	indows 5.1.4.074	CiscoSecure	ClientDe 5.1.4.74	2024/07/	26 15:56:27	Cisco Secure Client for
			Cisco-ISE-N	SP		Native Suppli	cant Pro Not Applica	ble 2023/07/	04 05:25:16	Pre-configured Native S
			CiscoAgentl	essOSX 5.0.0306	51	CiscoAgentle	ssOSX 5.0.3061.0	2023/07	04 04:24:14	With CM: 4.3.3045.6400

### 2단계. 프로파일 편집기 도구에서 NAM 프로파일 만들기

NAM 프로필을 구성하는 방법에 대한 자세한 내용은 이 안내서인 <u>보안 클라이언트 NAM 프로필 구</u> 성을 참조하십시오.

3단계. ISE에 NAM 프로필 업로드

ISE의 NAM 프로필 "Configuration.xml"을 에이전트 프로필로 업로드하려면 Client Provisioning(클 라이언트 프로비저닝) > Resources(리소스) > Agent Resources From Local Disk(로컬 디스크의 에

# 이전트 리소스)로 이동합니다.

Overview Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
Client Provisioning Policy Resources Client Provisioning Portal	Agent Resources From Local	Disk > Agent Resources Fr	rom Local Disk				
	Category	Customer Created	Packa, ~				
	Туре	Agent Profile	~				
	* Name	New Profile					
	Description						
		Choose File config	uration.xml				
	Submit						

# 4단계. Posture 프로파일 생성

Overview Network Devices	Client Provisioning	Policy Elemen	ts Posture Polic	y Policy Set
Client Provisioning Policy				
Resources	Resources			
Client Provisioning Portal	🖉 Edit 🕂 Add 🔿	🗂 Duplicate 🍵	Delete	
	Agent res	sources from Cisco site		Version La
	Agent res	sources from local disk	oSecureClientCo	4.3.4164 20
	Native Su	upplicant Profile	ntConfig	Not Applic 20
		ofiguration	e Supplicant Pro	. Not Applic 20
	Agent Po	sture Profile	oAgentlessWind	5.0.3061.0 20
	AMP Ena	bler Profile	DsXSPWizard	2.7.0.1 20
	NAM Profile	;	AgentProfile	Not Applic 20

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

Posture Protocol 섹션에서 에이전트가 모든 서버에 연결할 수 있도록 \*를 추가하는 것을 잊지 마십 시오.

# 5단계. 에이전트 구성 생성

Overview	Network Devices	Client Prov	isioning	Policy El	ements	Posture Policy	′
Client Provisi	oning Policy	_					
Resources		Reso	urces	\$			
Client Provisi	oning Portal	_					
		🖉 Edit	+ Add	Duplicate	🗍 Dele	te	
			Agent re	esources from Cis	co site		Ver
			Agent re	esources from loca	al disk 🛛	SecureClientCo	4.3
			Native S	Supplicant Profile	1	tConfig	Not
			Agent C	Configuration	,	e Supplicant Pro	Not
			Agent P	osture Profile		AgentlessWind	5.0
			AMP En	abler Profile		DsXSPWizard	2.7
		$\square$	NAM Profi	le	Agen	tProfile	Not

#### 업로드된 보안 클라이언트 및 규정 준수 모듈 패키지를 선택하고 모듈 선택 아래에서 ISE Posture, NAM 및 DART 모듈을 선택합니다

Er	ngine			Work	Centers / P	Posture	
(	Overview	Network Devices	Client Provisioning	Policy I	Elements	Posture Policy	Policy Sets
	Client Provisio	ning Policy	Agent Configuration > New Ag	ent Config	uration		
	Resources		Agent Configuration / New Ag	ent ooning			
	Client Provisio	ning Portal					
			* Select Agent Package:		CiscoSecure	ClientDesktopWindow	vs 5.1 🗸
			* Configuration Name:		Agent Config	guration	
			Description:				
			Description Value Not	es			
			* Compliance Module	c	iscoSecureClie	entComplianceModule	ew ~
			Cisco Secure Client N	lodule	Selection		
			ISE Posture				
			VPN				
			Zero Trust Access				
			Network Access Manager				
			Network Visibility				

Profile(프로파일) 아래에서 Posture(포스처) 및 NAM Profile(NAM 프로파일)을 선택하고 Submit(제 출)을 클릭합니다.

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

# 6단계. 클라이언트 프로비저닝 정책

Windows 운영 체제용 클라이언트 프로비저닝 정책을 생성하고 이전 단계에서 생성한 에이전트 컨 피그레이션을 선택합니다.

Overview	Network Devices	Client Prov	Isloning Policy Ele	ments	Posture Policy		Policy Sets Tr	oubleshoo	ot Reports	Settings					
Client Provisi Resources Client Provisi	loning Policy	Client Define the Cl For Agent Co For Native St Windows Ag Intel architec For Windows Mac ARM64 If you configu without an Af	Client Provisioning Policy to determine what users will receive upon login and user session initiation: For Agent Configuration: version of agent, agent profile and/or wizard profile and/or gent coustomization package. For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order. Windows Agent, Mac Agent, Mac Temporal and Mac Agentless policies support ARM64. Windows policies run separate packages for ARM4 and Intel architectures. Mac policies run the same package for both architectures. For Windows Agent, AMM64 policies, configure Session: OS-Architecture EQUALS arm64 in the Other Conditions column. Mac ARM64 policies require no Other Condifigurations. If you configure an ARM64 client provisioning policy for an OS, ensure that the ARM64 policy is at the top of the conditions list, ahead of policies without an ARM64 condition. This is because an endpoint is matched sequentially with the policies listed in this window.												
			Rule Name	ŀ	dentity Groups		Operating Systems		Other Conditions		Results				
		8 🖬	IOS	IF A	Any	and	Apple IOS All	and	Condition(s)	ther	Cisco-ISE-NSP		Edit 👻	^	
		: 🗩	Android	H A	Inv	and	Android	and	Condition(s)	the	Cisco-ISE-NSP		Calle 🗸		
		8 🖬	Windows	If A	Any	and	Windows All	and	Condition(s)	ther	Agent Configuration		Edit 🗸		
		8	MAC OS	IF A	Any	and	Mac OSX	and	Condition(s)	ther	CiscoTemporalAgent 5.0.03061 And MacOsXSPWizard 2.7.0.1 And Cisco-IS NSP	osx 6e-	Edit 🗠	Γ	
		8 🖬	Chromebook	If A	Any		Chrome OS All		Condition(s)	ther	Cisco-ISE-Chrome-N	NSP			
												Sav	ve	Reset	

7단계. 상태 정책

포스처 정책 및 조건을 생성하는 방법에 대한 자세한 내용은 이 설명서 <u>ISE 포스처 규범적 구축 설</u> 명서를 참조하십시오.

8단계. 네트워크 디바이스 추가

스위치 IP 주소 및 radius 공유 비밀 키를 추가하려면 Administration(관리) > Network Resources(네 트워크 리소스)로 이동합니다.

Engine		Administr	ration / Network Reso	urces
Network Devices Network Devices Default Device	Network Device Groups	Network Device Profiles	External RADIUS Serve	ers RADIUS Server Se
Device Security Settings	Network De Name Description	vices 		
	IP Address Device Profile Model Name	✓ * IP : 10.197.213.23 e	2 / <u>32</u> 🕸	

Engine			Administr	ation / Network Resources	
Network Devices	Network Dev	vice Groups Net	work Device Profiles	External RADIUS Servers	RADIUS Server Sequences
Network Devices		Device Type	All Device Types	Set To De	əfault
Default Device Device Security Settings		🗹 🗸 Radius	S Authentication Settir	ngs	
		RADIUS U	DP Settings		
		Protocol	RADIUS		
		Shared Sec	cret	Show	
		Use Se	econd Shared Secret 🕕		
			Second Shared Secret		
		CoA Port	1700	Set To D	

# 9단계. 권한 부여 프로파일

포스처 리디렉션 프로필을 생성하려면 Policy(정책) > Policy Elements(정책 요소) > Results(결과)로 이동합니다.



명령 작업 아래에서 리디렉션 ACL이 있는 클라이언트 프로비저닝 포털을 선택합니다.

Dictionaries Conditions	Results
Authentication	Authorization Profiles > Redirection
Authorization ~	Authorization Profile
Authorization Profiles	* Name Redirection
Downloadable ACLs	Description
Profiling )	* Access Type
Posture	ACCESS_ACCEPT ~
Client Provisioning	Network Device Profile 🏙 Cisco 🗸 🕀
	Service Template
	Track Movement
	Agentless Posture
	Passive Identity Tracking 🔲 🕕
	✓ Common Tasks
	✓ Web Redirection (CWA, MDM, NSP, CPP) ①
	Client Provisioning (Posture) V ACL redirect-acl V Value Client Provisioning Portal (defi V
	Static IP/Host name/FQDN Suppress Profiler CoA for endpoints in Logical Profile

# 10단계. 허용되는 프로토콜

Policy(정책) > Policy elements(정책 요소) > Results(결과) > Authentication(인증) > Allowed Protocols(허용되는 프로토콜)로 이동하고 EAP Chaining(EAP 체인) 설정을 선택합니다.

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		>						



### 11단계. 액티브 디렉토리

ISE가 Active Directory 도메인과 조인되고 인증 조건에 필요한 경우 도메인 그룹이 선택되었는지 확인합니다.

관리 >	신원	관리 >	· 외부	ID 소스	>	Active	Directory	/
------	----	------	------	-------	---	--------	-----------	---

Engine		Administration / Identity Management
Identities	Groups External Identity So	urces Identity Source Sequences Settings
	External Identity Sources	Connection Allowed Domains PassivelD Groups Attributes Advanced Settings
	<ul> <li>Certificate Authenticat</li> <li>Active Directory</li> <li>PRAD</li> <li>LDAP</li> </ul>	* Join Point Name PRAD ① * Active Directory asa.prad.com ① + Join + Leave ② Test User ☆ Diagnostic Tool ♂ Refresh Table
	<ul> <li>ODBC</li> <li>RADIUS Token</li> </ul>	ISE Node A ISE Node R Status Domain Controller Site
	<ul> <li>RSA SecurID</li> <li>SAML Id Providers</li> <li>Social Login</li> </ul>	pk3-3.aaa.prad.com PRIMARY Operational CXLabs-WIN2022.aaa.pr Default-First-Site-Na

12단계. 정책 집합

dot1x 요청을 인증하기 위해 ISE에 정책 집합을 생성합니다. Policy(정책) > Policy sets(정책 집합)로 이동합니다.

Engi	Ingine				Policy / Policy Sets	🔺 Evaluati	on Mode 87 Days	Q	۵	0	Q   2
	Policy	Policy Sets				Reset					Save
		Status	Policy Set Name	Description	Conditions	Allowed Protocols	/ Server Seque	nce	Hits	Actions	View
	C	Search									
			Dot1x Policy		E Wired_802.1X	Default Network Ac	cess 🧷	-		¢	
			Default	Default policy set						¢	

Active Directory를 인증 정책의 ID 소스로 선택합니다.

VAuthentication Policy(1)							
Status Rule Name	Conditions			Use		Hits	Actions
Q Search							
				PRAD	<u> </u>		
🥏 Default	Default			 > Options			ŝ

상태 알 수 없음, 비 규격 및 규정 준수를 기반으로 다른 권한 부여 규칙을 구성 합니다.

이 활용 사례에서는

- 초기 액세스: ISE 클라이언트 프로비저닝 포털로 리디렉션하여 보안 클라이언트 에이전트 및 NAM 프로필 설치
- 알 수 없는 액세스: 리디렉션 기반 포스처 검색을 위한 클라이언트 프로비저닝 포털에 액세스
- 규정 준수 액세스: 전체 네트워크 액세스
- Non-Compliant: 액세스 거부

~Authorization	n Policy(5)									
					Results	Results				
+ Status	s Rule Name		Cond	tions	Profiles		Security Groups		Hits	Actions
Q Search										
	Non-compliant	Access	AND	L         Session PostureStatus EQUALS NonCompilant           Q         Network Access-EapChainingResult EQUALS User and machine both succeeded						ŝ
	Unknown Acce		AND	E Session-PostureStatus EQUALS Unknown     Network Access-EapChainingResult EQUALS User and machine both succeeded	Redirection					ŵ
	Compliant Acc	055	AND	E Session-PostureStatus EQUALS Compliant     Network Access-EapChainingResult EQUALS User and machine both succeeded	PermitAccess					¢
	Initial Access			PRAD-ExternalGroups EQUALS aaa.prad.com/Users/Domain Computers	Redirection					¢
	Default									ŵ
								Reset		Save

# 다음을 확인합니다.

### 1단계. ISE에서 Secure Client Posture/NAM 모듈 다운로드 및 설치

dot1x를 통해 인증 된 엔드 포인트를 선택 하고 "초기 액세스" 권한 부여 규칙을 적중 합니다. Operations(운영) > Radius > Live Logs(라이브 로그)로 이동합니다.

Ø												
	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				
	Jul 27, 2024 12:10:17	2	G			Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection				
	Jul 27, 2024 12:09:31		là -	B4:96:91:F9:56:8B	host/DESKTOP-QSCE4P3.a	Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection	Pending			

스위치에서 엔드포인트에 적용되는 리디렉션 URL 및 ACL을 지정합니다.

Switch#show authentication session interface te1/0/24 details 인터페이스: TenGigabitEthernet1/0/24 IIF-ID: 0x19262768 MAC 주소: x4x6.xxxx.xxxx IPv6 주소: 알 수 없음 IPv4 주소: <client-IP> 사용자 이름: host/DESKTOP-xxxxxx.aaa.prad.com 상태: 권한 부여됨 도메인: 데이터 Oper host mode(작동 호스트 모드): single-host 작업 제어 디렉토리: 둘 다 세션 시간 초과: 해당 없음 공통 세션 ID: 16D5C50A0000002CF067366B 계정 세션 ID: 0x0000001f 핸들: 0x7a000017 현재 정책: POLICY Te1/0/24 로컬 정책: 서비스 템플릿: DEFAULT\_LINKSEC\_POLICY\_SHOULD\_SECURE(우선순위 150) 보안 정책: 보안 유지 보안 상태: 링크 보안되지 않음 서버 정책: URL 리디렉션 ACL: redirect-acl URL 리디렉션: https://ise33.aaa.prad.com:8443/portal/gateway?sessionId=16D5C50A0000002CF067366A&portal=ee39 7180-4995-8aa2-9fb282645a8f&action=cpp&token=518f857900a37f9afc6d2da8b6fe3bc2 ACS ACL: xACSACLx-IP-PERMIT\_ALL\_IPV4\_TRAFFIC-57f6b0d3

메서드 상태 목록: 메서드 상태 dot1x 인증 성공

Switch#sh 디바이스 추적 데이터베이스 인터페이스 te1/0/24

네트워크 레이어 주소 링크 레이어 주소 인터페이스 vlan privi 기간 상태 시간 남음 ARP X.X.X.X b496.91f9.568b Te1/0/24 1000 005 4mn 연결 가능 39초 시도 0

엔드포인트에서 ISE Posture Posture로 리디렉션된 트래픽을 확인하고 Start(시작)를 클릭하여 엔 드포인트에서 Network Setup Assistant를 다운로드합니다.

Google Chrome isn't your default browser Set as default	
Client Provisioning Portal	
Device Security Check Your computer requires security software to be installed before you can connect to the ne	łwork.
Client Provisioning Portal  Device Security Check  Your computer requires security software to be installed before you can connect to the network	Recent download history cisco-secure-client-ise-network- assistant- win-5.1.4.74_pk3-3.aaa.prad.com_8443_ WPTsDtD0R0SunsnMYBlglg.exe 3.0 MB + Done
Unable to detect Posture Agent  This is my first time here  1. You must install Agent to check your device before accessing the network  Click here to download and install Agent  2. After installation, Agent will automatically scan your device before allowing you access to the network.  3. You have 4 minutes to install and for the system scan to complete.  Tip: Leave Agent running so it will automatically scan your device and connect you faster next time you access this network.  You have 4 minutes to install and for the compliance check to complete	Full download history
+ Remind me what to do next	

NSA 애플리케이션을 설치하려면 실행을 클릭합니다.



이제 NSA는 ISE에서 Secure Client Agent 다운로드를 호출하고 Posture, NAM 모듈 및 NAM Profile configuration.xml을 설치합니다.



NAM 설치 후 재시작 프롬프트가 트리거되었습니다. Yes(예)를 클릭합니다.



2단계. EAP-FAST

PC가 다시 시작되고 사용자가 로그인하면 NAM은 EAP-FAST를 통해 사용자와 머신 모두를 인증합 니다.

엔드포인트가 올바르게 인증되면 NAM은 엔드포인트가 연결되었음을 표시하고 포스처 모듈은 포 스처 스캔을 트리거합니다.

🕲 Cisco Secu	re Client		-2		×
	AnyConnect VPN: Ready to connect.	~	Co	onnect	
	Network: Connected ( ) wired	]	Ĩ		
	ISE Posture: Scanning system 10%	6	Sca	n Again	
		_			

ISE Live Logs(라이브 로그)에서 엔드포인트가 이제 Unknown Access Rule(알 수 없는 액세스 규칙 )에 도달합니다.

 Jul 27, 2024 12:29:06...
 Image: Control of the con

이제 인증 프로토콜은 NAM 프로필 컨피그레이션을 기반으로 EAP-FAST이며 EAP-Chaining 결과 는 "성공"입니다.

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

3단계. 상태 검사

Secure Client Posture Module은 Posture Scan을 트리거하며 ISE Posture Policy에 따라 Complaint로 표시됩니다.

🕲 Cisco Secur	e Client	-	
A AN			
	AnyConnect VPN: Use a browser to gain access.		
	~		Connect
Web Authent	ication Required		
	Network: Connected (		
	wired		🍇 ∨ 📰
	ISE Posture:		
	Compliant.		
	Network access allowed.		Scan Again
<b>\$</b> (1)			cisco

CoA는 포스처 스캔 후 트리거되며 이제 엔드포인트가 Complaint Access Policy에 도달합니다.

ø	D Reset Repeat Counts	🖒 Export To	~						Filter $$	۰
	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	•	là -			Dot1x Policy >> Default	Dot1x Policy >> Compliant Access	PermitAccess	Compliant	:
	Jul 27, 2024 12:29:32	۰	ъ			Dot1x Policy >> Default	Dot1x Policy >> Compliant Access	PermitAccess	Compliant	÷
	Jul 27, 2024 12:29:31		а						Compliant	÷
	Jul 27, 2024 12:29:06	2	18			Dot1x Policy >> Default	Dot1x Policy >> Unknown Access	Redirection		÷
	Jul 27, 2024 12:28:48	v.	là.			Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection		÷



### 1단계. NAM 프로필

NAM 모듈 설치 후 PC의 이 경로에 NAM 프로파일 configuration.xml이 있는지 확인합니다.

C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system

> This PC > Local Disk (C:) > ProgramData > Cisco > Cisco Secure Client > Network Access Manager > system								
	Name	Date modified	Туре	Size				
*	configuration	7/26/2024 4:53 PM	XML Document	7 KB				
	internalConfiguration	7/27/2024 12:27 AM	XML Document	3 KB				
Ŕ	userConfiguration	7/27/2024 12:27 AM	XML Document	1 KB				
*								
1								

# 2단계. NAM 확장 로깅

작업 표시줄에서 보안 클라이언트 아이콘을 클릭하고 "설정" 아이콘을 선택합니다.

🕲 Cisco Secu	re Client	-		$\times$
	AnyConnect VPN: Ready to connect.		Connect	
	Network: Connected ( )		<b>X</b>	:=
	ISE Posture: Compliant. Network access allowed.		Scan Again	
\$ ①				altalta cisco

Network(네트워크) > Log Settings(로그 설정) 탭으로 이동합니다. Enable Extended Logging(확장 로깅 활성화) 확인란을 선택합니다.

패킷 캡처 파일 크기를 100MB로 설정합니다.

문제를 재현한 후 Diagnostics(진단)를 클릭하여 엔드포인트에서 DART 번들을 생성합니다.

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

Message History(메시지 기록) 섹션에는 NAM이 수행한 모든 단계의 세부 정보가 표시됩니다.

3단계. 스위치의 디버그

스위치에서 이러한 디버그를 활성화하여 dot1x 및 리디렉션 흐름의 문제를 해결합니다.

ip http all 디버그

ip http 트랜잭션 디버그

디버그 ip http url

플랫폼 소프트웨어 추적 smd 스위치 활성 R0 aaa 디버그 설정 set platform software trace smd switch active R0 dot1x-all 디버그 플랫폼 소프트웨어 추적 smd 스위치 활성 R0 radius 디버그 설정 플랫폼 소프트웨어 추적 smd 스위치 활성 R0 auth-mgr-all 디버그 설정 플랫폼 소프트웨어 추적 smd 스위치 활성 R0 eap-all 디버그 설정 플랫폼 소프트웨어 추적 smd 스위치 활성 R0 epm-all 디버그 설정

set platform software trace smd switch active R0 epm-redirect  $\Box H \Box$ 

플랫폼 소프트웨어 추적 smd 스위치 활성 R0 webauth-aaa 디버그 설정

플랫폼 소프트웨어 추적 smd 스위치 활성 R0 webauth-httpd 디버그 설정

로그를 보려면

로깅 표시

로깅 프로세스 smd 내부 표시

4단계. ISE에서 디버깅

다음 속성을 사용하여 디버그 레벨에서 설정할 ISE 지원 번들을 수집합니다.

- 상태
- 포털
- 프로비저닝
- 런타임 AAA
- nsf
- nsf 세션
- 스위스인
- 클라이언트-웹앱

# 관련 정보

<u>보안 클라이언트 NAM 구성</u>

<u>ISE 포스처 규범적 구축 설명서</u>

<u>Catalyst 9000 Series 스위치의 Dot1x 문제 해결</u>

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.