Configure and Deploy Secure Client NAM Profile through ISE 3.3 on Windows

Contents

Introduction
Background Information
Prerequisites
Requirements
Components Used
Configuration
Network Diagram
Data Flow
Configure Switch
Download the Secure client Package
ISE Configuration
Step 1. Upload the Package on ISE
Step 2. Create a NAM Profile from Profile editor tool
Step 3. Upload the NAM Profile on ISE
Step 4. Create a Posture Profile
Step 5. Create Agent Configuration
Step 6. Client Provisioning Policy
Step 7. Posture Policy
Step 8. Add Network device
Step 9. Authorization Profile
Step 10. Allowed Protocals
Step 11. Active Directory
Step 12. Policy sets
Verify
Step 1. Download and Install Secure Client Posture/NAM module from ISE
Step 2. EAP-FAST
Step 3. Posture Scan
Troubleshoot
Step 1. NAM Profile
Step 2. NAM Extended Logging
Step 3.Debugs on Switch
Step 4. Debugs on ISE
Related Information

Introduction

This document describes how to deploy the Cisco Secure Client Network Access Manager (NAM) profile

through Identity Services Engine (ISE).

Background Information

EAP-FAST authentication occurs in two phases. In the first phase, EAP-FAST employs a TLS handshake to provide and authenticate key exchanges using Type-Length-Values (TLV) objects to establish a protected tunnel. These TLV objects are used to convey authentication-related data between the client and server. Once the tunnel is established, the second phase begins with the client and ISE node engaging in further conversations to establish the required authentication and authorization policies.

The NAM configuration profile is set up to use EAP-FAST as the authentication method and is available for administratively defined networks.

In addition, both machine and user connection types can be configured within the NAM configuration profile.

The corporate Windows device gain full corporate access using the NAM with Posture check. The personal Windows device gain access to a restricted network using the same NAM configuration.

This document provides instructions for deploying the Cisco Secure Client Network Access Manager (NAM) profile via the Identity Services Engine (ISE) Posture Portal using web deployment, along with Posture Compliance Check.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Identity Services Engine (ISE)
- AnyConnect NAM and Profile Editor
- Posture Policy
- Cisco Catalyst configuration for 802.1x services

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ISE, Release 3.3 and later
- Windows 10 with Cisco Secure Mobility Client 5.1.4.74 and later
- Cisco Catalyst 9200 switch with software Cisco IOS® XE 17.6.5 and later
- Active Directory 2016

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configuration

Network Diagram



Data Flow

When a PC connects to the network, the ISE provides the authorization policy for redirection to the Posture Portal.

The http traffic on the PC is redirected to the ISE Client Provisioning Page, where the NSA application is downloaded from ISE.

The NSA then installs the Secure Client agent modules on the PC.

After the agent installation is completed, the agent downloads the Posture profile and NAM profile configured on ISE.

The installation of the NAM module triggers a restart on the PC.

After the restart, NAM module performs EAP-FAST authentication based on the NAM profile. The Posture scan is then triggered and compliance is checked based on the ISE Posture Policy.

Configure Switch

Configure the access switch for dot1x authentication and redirection.

aaa new-model aaa authentication dot1x default group radius aaa authorization network default group radius aaa accounting dot1x default start-stop group radius aaa server radius dynamic-author client 10.127.197.53 server-key Qwerty123 auth-type any aaa session-id common ip radius source-interface Vlan1000 radius-server attribute 6 on-for-login-auth radius-server attribute 8 include-in-access-req radius-server attribute 25 access-request include radius-server attribute 31 mac format ietf upper-case radius server RAD1 address ipv4 <ISE server IP> auth-port 1812 acct-port 1813 key <secret-key> dot1x system-auth-control

Configure Redirect ACL for user to be redirected to ISE Client Provisioning Portal.

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 permit tcp any any eq www 60 permit tcp any any eq 443

Enable device tracking and http redirection on the switch.

device-tracking policy <device tracking policy name> tracking enable interface <interface name> device-tracking attach-policy <device tracking policy name> ip http server

ip http secure-server

Download the Secure client Package

Download the Profile Editor, Secure Client windows and Compliance Module webdeploy files manually from <u>software.cisco.com</u>

On the product name search bar type Secure Client 5.

Downloads Home > Security > Endpoint Security > Secure Client (including AnyConnect) > Secure Client 5 > AnyConnect VPN Client Software

- 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 Configuration

Step 1. Upload the Package on ISE

To upload the Secure Client and Compliance Module webdeploy packages on ISE, Navigate to **Workcenter** > **Posture** > **Client Provisioning** > **Resources** > **Add** > **Agent Resources from Local Disk**.

Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
Client Provisio Resources Client Provisio	uning Policy	Agent Resources From Local Agent Resources Fro	Disk → Agent Resources Fro	om Local Disk				
		Category	Cisco Provided Pac	kages	() 9			
			 Agent Uploaded 	Resources				
			Name		Гуре		Version	Description
			CiscoSecureClientDes	ktopWindows 5.1	CiscoSecureClientDe	esktopWindows	5.1.4.74	Cisco Secure Client for
		Submit	ancel					

Overview	Network Devices	Client Pro	ovisioning	Policy Eleme	nts Posture Policy	Policy Sets	Troubleshoot	Reports	Settings		
Client Provisio	oning Policy	Reso	ources								
Client Provisio	oning Portal	/ Edit		Duplicate	Delete						
			Name		.	Туре	Version	Last Upda	ite 🗸	Description	
			Lab Profile			AgentProfile	Not Applicable	2024/07/	26 17:23:41		
			Agent Config	guration		AgentConfig	Not Applicable	2024/07/	26 16:00:49		
			NAM Profile			AgentProfile	Not Applicable	2024/07/	26 16:00:00		
			CiscoSecure	ClientCompliance	ModuleWindows 4.3.4164	CiscoSecureClientCo	4.3.4164.8192	2024/07/	26 15:58:44	Cisco Secure Client Win	
			CiscoSecure	ClientDesktopWind	dows 5.1.4.074	CiscoSecureClientDe	5.1.4.74	2024/07/	26 15:56:27	Cisco Secure Client for	
			Cisco-ISE-N	SP		Native Supplicant Pro	Not Applicable	2023/07/	04 05:25:16	Pre-configured Native S	
			CiscoAgentle	essOSX 5.0.03061		CiscoAgentlessOSX	5.0.3061.0	2023/07/	04 04:24:14	With CM: 4.3.3045.6400	

Step 2. Create a NAM Profile from Profile editor tool

For information on how to configure a NAM profile refer this guide <u>Configure Secure Client NAM Profile</u>.

Step 3. Upload the NAM Profile on ISE

To upload the NAM Profile "Configuration.xml" on ISE as Agent Profile, navigate to **Client Provisioning** > **Resources** > **Agent Resources From Local Disk**.

Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
Client Provisio Resources Client Provisio	ning Policy ning Portal	Agent Resources From Local Agent Resources Fro	Disk ≻ Agent Resources Fr om Local Disk	om Local Disk				
		Category	Customer Created	Packa: V	Ū			
		Type * Name	Agent Profile New Profile	~				
		Description	Choose File configu	uration.xml				
		Submit						

•

Step 4. Create a Posture Profile

Overview Network Devices	Client Provisioning	Policy Elemen	nts Posture P	Policy Policy Se
Client Provisioning Policy	5			
Resources	Resources			
Client Provisioning Portal	🖉 Edit 🔶 Add 🔿	Duplicate	Delete	
	Agent re	sources from Cisco site		Version L
	Agent re	sources from local disk	oSecureClient	Co 4.3.4164 2
	Native S	upplicant Profile	ntConfig	Not Applic 2
		onfiguration	e Supplicant	Pro Not Applic 2
	Agent Po	osture Profile	oAgentlessWi	nd 5.0.3061.0 2
	AMP Ena	abler Profile	DsXSPWizard	2.7.0.1 2
	NAM Profil	e	AgentProfile	Not Applic 2

Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Т		
Client Provis	sioning Policy							
Client Provis	sioning 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 che	ck (1)	No	~			

From the Posture Protocol section, do not forget to add * in order to allow the Agent to connect to all servers.

Step 5. Create Agent Configuration

Overview	Network Devices	Client Prov	visioning	Policy E	lements	Posture Policy	′
Client Provisio	oning Policy	Deee		_			
Resources		Reso	urces	6			
Client Provisio	oning Portal	/ Edit	+ Add	ت Duplicate	e 👔 Dele	ete	
			Agent r	esources from Cis	sco site		Ver
			Agent r	esources from loc	al disk	oSecureClientCo	4.3
			Native	Supplicant Profile		ıtConfig	Not
			Agent (Configuration		e Supplicant Pro	Not
			Agent F	Posture Profile		oAgentlessWind	5.0
			AMP Er	abler Profile		DsXSPWizard	2.7
			NAM Profi	le	Ager	ntProfile	Not

Select the uploaded secure client and compliance module package and under the Module selection, select the ISE Posture, NAM and DART modules

Er	ngine			Work	Centers /	Posture	
(Overview	Network Devices	Client Provisioning	Policy	Elements	Posture Policy	Policy Sets
	Client Provisio	oning Policy	Agent Configuration > New 4	Agent Confid	ouration		
	Resources		Agent comgutation / Ren /	igont ooning	Janation		
	Client Provisio	oning Portal					
			* Select Agent Package:		CiscoSecur	eClientDesktopWindov	ws 5.1. 🗸
			* Configuration Name:		Agent Conf	iguration	
			Description:				
			Description Value No	otes			
			* Compliance Module		CiscoSecureCl	ientComplianceModul	eW ~
			Cisco Secure Client	Module	Selection		
			ISE Posture		1		
			VPN		J		
			Zero Trust Access				
			Network Access Manager				
			Secure Firewall Posture]		

Under Profile select, choose the **Posture** and **NAM** Profile and click **Submit**.

Overview Network Devices Client Provisioning Policy Ele	ements Posture Policy
Client Provisioning Policy Start Before	
Resources Logon	
Client Provisioning Portal Diagnostic and Reporting Tool	
Profile Selection	
* ISE Posture Posture Profile	~
VPN	~
Network Access NAM Profile Manager	~
Network Visibility	~
Umbrella	~
Customer Feedback	~

Step 6. Client Provisioning Policy

Create a client Provisioning Policy for Windows operating system and select the **Agent Configuration** created in the previous step.

Overview	Network Devices	Client Prov	isioning Po	licy Elements	Posture Poli	cy	Policy Sets	Troublest	hoot	t Reports	Settings					
Cilent Provisi Résources Cilent Provisi	oning 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: versio pipicant Configura Int, Mac Agent, Mi tures. Mac policies Agent ARM64 clier M64 condition. Th	olicy to determin n of agent, agent tion: wizard profi ac Temporal and I run the same pa cicles, configure S Other Conditions the provisioning po his is because an	cy a what users will re profile, agent comp e and/or wizard. Di dea Agentless politi cksape for both arch ession: OS-Archite arm64 configuratio licy for an OS, ensu endpoint is matche	ceive u oliance rag and cies sup itecture cture E ons, ire that d sequ	pon login and us module, and/or I drop rules to cl oport ARM64. W es. QUALS arm64 in the ARM64 poli entially with the	ser session initi agent customiz hange the order findows policies n the Other Con icy is at the top policies listed i	ation ration r. dition of th n this	r: package. separate packages ns column. he conditions list, at s window.	for ARM4 and read of policies					
			Rule Name		Identity Groups		Operating Sys	stems		Other Conditions			Results			
		8 🛛	IOS		Any	and	Apple IOS All	a	ind	Condition(s)		then	Cisco-ISE-NSP		Â	
		: 🗖	Android	н	Δnv	and	Android	a	nd	Condition(s)		then	Cisco-ISF-NSP	Edit v		
		8 🖬	Windows		Any		Windows All	a	ind	Condition(s)		then	Agent Configuration	Edit 🛩		
		8	MAC OS	H	Any	and	Mac OSX	a	ind	Condition(s)		then	CiscoTemporalAgentOSX 5.0.03061 And MacOsXSPWizard 2.7.0.1 And Cisco-ISE- NSP	Edit ~	I	
		# 💌	Chromebook		Any	and	Chrome OS All		ind	Condition(s)		then	Cisco-ISE-Chrome-NSP		•	
														Save		Reset

Step 7. Posture Policy

For information on how to create the Posture Policy and conditions, refer this guide <u>ISE Posture Prescriptive</u> <u>Deployment Guide</u>.

Step 8. Add Network device

To add the switch IP address and the radius shared secret key, navigate to **Administration > Network Resources**.

Engine		Administra	ation / Network Reso	ources
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Serv	vers RADIUS Server Se
Network Devices Detault Device Device Security Settings	Network Devices	List > aaa evices		
	Name Description	aaa 		
	IP Address	* I ^{P :} 10.197.213.22	/ <u>32</u> 🗇	
	Device Profile	e 🎎 Cisco	~ ①	
	Model Name		~	

Engine	Administration / Network Resources								
Network Devices	Network Dev	ice Groups Net	twork Device Profiles	External RADIUS Ser	vers RADIU	S Server Sequences			
Network Devices		Device Type	All Device Types	<u> </u>	Set To Default				
Default Device Device Security Settings		🗹 🗸 Radiu	S Authentication Settir	ngs					
	RADIUS UDP Settings								
		Protocol	RADIUS						
		Shared Se	cret						
		📃 Use S	econd Shared Secret 🕕						
			Second Shared Secret						
		CoA Port	1700		Set To Default				

Step 9. Authorization Profile

To create a Posture redirection profile, navigate to **Policy > Policy Elemets > Results**.

Engine			Policy / Policy Elements		
Dictionaries Conditions	Results				
Authentication > Authorization > Authorization Profiles	Stan For Policy	tandard Authorization Profiles Policy Export go to Administration > System > Backup & Restore > Policy Export Page			
Downloadable AGLS	🧷 Edit	+ Add 🗂 Duplicate	Delete		
Profiling >		Name	Profile		
Posture >			🔠 Cisco 👔		
Client Provisioning >		Cisco_IP_Phones	競 Cisco 👔		
		Cisco_Temporal_Onboard	🇱 Cisco 🕠		

Under command task, select the client Provisioning Portal with redirect ACL.

Dictionaries Conditions	Results
Authentication	Authorization Profiles > Redirection Authorization Profile
Authorization Profiles Downloadable ACLs	* Name Redirection
Profiling	Description
Posture	* Access Type ACCESS_ACCEPT ~
Client Provisioning	>> Network Device Profile the Cisco the Hermitian termination terminatination terminati
	Service Template Track Movement Agentless Posture Passive Identity Tracking
	 Common Tasks Web Redirection (CWA, MDM, NSP, CPP) () Client Provisioning (Posture) \sigma ACL redirect-acl \sigma Value Client Provisioning Portal (defi \sigma Lienter Portal (defi \sigma Lienter Portal (defi \sigma Lienter Portal (defi \sigma

Step 10. Allowed Protocals

Navigate to **Policy > Policy elements > Results > Authentication > Allowed Protocols**, Selsct the **EAP Chaining** settings,

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		>	



Step 11. Active Directory

Validate ISE is joined with Active directory domain and the domain groups are selected if needed for the authorization conditions.

	T 1 (14) T			a	D! (
Administration >	- Identity Man	agement > Ex	xternal Identity	Sources > Active	Directory
	Identity Initian		neer nan Laenerey	Sources / meente	Directory

Engine	Administration / Identity Management
Identities Groups External Identit	y Sources Identity Source Sequences Settings
External Identity Sources	Connection Allowed Domains PassivelD Groups Attributes Advanced Settings
<	* Join Point Name PRAD ① * Active Directory aaa.prad.com ① + Join + Leave Q Test User % Diagnostic Tool € Refresh Table
CODBC RADIUS Token RADIUS Token	ISE Node ISE Node R Status Domain Controller Site pk3-3.aaa.prad.com PRIMARY Øperational CXLabs-WIN2022.aaa.pr Default-First-Site-Na
SAML Id Providers	

Step 12. Policy sets

Create a Policy set on ISE to authenticate the dot1x request. Navigate to **Policy > Policy sets** .

Engi	ne			Policy / Policy Sets	🔺 Evaluati	on Mode 87 Days	a ¢	0	Q X
	Policy Sets				Reset				Save
	📀 Statu	s Policy Set Name	Description	Conditions	Allowed Protocols	Server Sequence	e Hits	Actions	View
	Q Sear								
		Dot1x Policy		Wired_802.1X	Default Network Ac	cess 🧷		ŵ	
		Default	Default policy set					ŵ	

Select the Active directory as identity source for Authentication Policy.

Status Rule Name Conditions Use	Hits	Actions
Q Search		
+		
PRAD I V		
Default	86	ŝ

Configure different Authorization rules based on posture status unknown, non-compliant and compliant.

In this use case.

- Initial Access : Redirection to ISE Client Provisioning Portal to install Secure client agent and NAM Profile
- Unknown Access: Access to Client Provisioning Portal for redirection based Posture discovery
- Compliant Access: Full network access
- Non-Compliant: Deny Access

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

Verify

Step 1. Download and Install Secure Client Posture/NAM module from ISE

Select the endpoint authenticated through dot1x, hitting "**Initial Access**" Authorization rule. Navigate to **Operations > Radius > Live Logs**



On Switch, specify the redirection URL and ACL getting applied for the Endpoint.

Switch#show authentication session interface te1/0/24 details Interface: TenGigabitEthernet1/0/24 IIF-ID: 0x19262768 MAC Address: x4x6.xxxx.xxxx IPv6 Address: Unknown IPv4 Address: <client-IP> User-Name: host/DESKTOP-xxxxx.aaa.prad.com Status: Authorized Domain: DATA Oper host mode: single-host Oper control dir: both Session timeout: N/A Common Session ID: 16D5C50A0000002CF067366B Acct Session ID: 0x000001f Handle: 0x7a000017 Current Policy: POLICY_Te1/0/24 Local Policies: Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150) Security Policy: Should Secure Security Status: Link Unsecured Server Policies: URL Redirect ACL: redirect-acl URL Redirect: https://ise33.aaa.prad.com:8443/portal/gateway?sessionId=16D5C50A0000002CF067366A&portal=ee39fd08-7180-4995-8aa2-9fb282645a8f&action=cpp&token=518f857900a37f9afc6d2da8b6fe3bc2 ACS ACL: xACSACLx-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3 Method status list: Method State dot1x Authc Success Switch#sh device-tracking database interface te1/0/24 Network Layer Address Link Layer Address Interface vlan prlvl age state Time left ARP X.X.X.X b496.91f9.568b Te1/0/24 1000 0005 4mn REACHABLE 39 s try 0

On the Endpoint, verify the traffic redirected to ISE Posture Posture and click **Start** to download the Network Setup Assistant on the Endpoint.

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 net Start	twork.
Client Provisioning Portal Device Security Check Your computer requires security software to be installed before you can connect to the network. Unable to detect Posture Agent + This is my first time here	Recent download history cisco-secure-client-ise-network- assistant- win-5.1.4.74_pk3-3.aaa.prad.com_8443_ WPTsDtDDROSunsnMYBIgIg.exe 3.0 MB + Done Full download history
 You must install Agent to check your device before accessing the network <u>Click here to download and install Agent</u> After installation, Agent will automatically scan your device before allowing you access to the network. 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 	
+ Remind me what to do next	

Click **Run** to install the NSA application.



Now, the NSA invokes the Secure Client Agent download from ISE and installs the Posture, NAM module, and NAM Profile **configuration.xml**.



A restart prompt triggered after NAM installation. Click Yes.



Step 2. EAP-FAST

Once the PC restarted and the user logged in, the NAM authenticates both user and machine through EAP-FAST.

If the endpoint authenticates correctly, NAM displays that it is connected and the Posture Module triggers the Posture Scan.

🕑 Cisco Secu	re Client		3 — 3		×
	AnyConnect VPN: Ready to connect.	~]	Connect	
	Network: Connected (wired	•	8	& ~ :	
	ISE Posture: Scanning system	10%	Sc	an Again	
\$ (1)					4114114

On ISE Live Logs, the Endpoint is now hitting the Unknown Access Rule.



Now the Authentication Protocol is EAP-FAST based on the NAM Profile configuration and EAP-Chaining result is "Success".

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

Step 3. Posture Scan

The Secure Client Posture Module triggers the Posture Scan and is marked as Complaint based on the ISE Posture Policy.

S Cisco Secur	e Client	_	
	AnyConnect VPN: Use a browser to gain access.	~	Connect
Web Authent	cation Required		
	Network: Connected () wired		°& ∽ ≔
	ISE Posture: Compliant. Network access allowed.		Scan Again
* 0			alu

The CoA is triggered after the Posture Scan and now the Endpoint hits the Complaint Access Policy.

ø									۲	
	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	۵	là.			Dot1x Policy >> Default	Dot1x Policy >> Compliant Access	PermitAccess	Compliant	÷
	Jul 27, 2024 12:29:31		a.						Compliant	÷
	Jul 27, 2024 12:29:06	2	là.			Dot1x Policy >> Default	Dot1x Policy >> Unknown Access	Redirection		
	Jul 27, 2024 12:28:48		6			Dot1x Policy >> Default	Dot1x Policy >> Initial Access	Redirection		

Troubleshoot

Step 1. NAM Profile

Verify the NAM Profile **configuration.xml** is present in this path on the PC after the NAM module installation.

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

This PC → Local Disk (C:) → ProgramData	> Cisco > Cisco Secure Clien	t > Network Access	s 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
userConfiguration	7/27/2024 12:27 AM	XML Document	1 KB
P			
P			

Step 2. NAM Extended Logging

Click on the Secure Client Icon from task bar and select "settings" icon.

Cisco Secur	re Client	7-3		\times
	AnyConnect VPN: Ready to connect.		Connect	
	Network: Connected () wired		8	
	ISE Posture: Compliant. Network access allowed.		Scan Again	
\$ ①	~ (3)			disala. cisco

Navigate to the **Network > Log Settings** tab. Check the **Enable Extended Logging** checkbox. Set the Packet Capture File Size to 100 MB.

After reproducing the issue, click on **Diagnostics** to create the DART Bundle on the Endpoint.

cisco	Secure (Client				
Status Overvi	ew	Network Access Manager Configuration Log Settings Statistics Message History				
AnyConnect \	/PN					
Network	>	Use extended logging to collect additional information about product operations.				
ISE Posture		IHV: Off ~				
		Filter Driver: Off Credential Provider Packet Capture Maximum Packet Capture File Size (MB): 100				
Collect diagnost installed Diag	ic information for all components. gnostics					

The Message History section displays the details of every step that NAM performed.

Step 3. Debugs on Switch

Enable these debugs on the switch to troubleshoot dot1x and redirection flow.

debug ip http all

debug ip http transactions

debug ip http url

set platform software trace smd switch active R0 aaa debug set platform software trace smd switch active 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 epm-all debug

set platform software trace smd switch active R0 epm-redirect debug

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

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

To view the logs

show logging

show logging process smd internal

Step 4. Debugs on ISE

Collect the ISE support bundle with these atributes to be set at the debug level:

- posture
- portal
- provisioning
- runtime-AAA
- nsf
- nsf-session
- swiss
- client-webapp

Related Information

Configure Secure Client NAM

ISE Posture Prescriptive Deployment Guide

Troubleshoot Dot1x on Catalyst 9000 Series Switches