WindowsおよびISE 3.2を使用したDot1x用のセ キュアなクライアントNAMの設定

内容
<u>前提条件</u>
<u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
設定
ネットワーク図
コンフィギュレーション
<u>1. セキュアクライアントNAM(Network Access Manager)のダウンロードとインストール</u>
<u>2. セキュアクライアントNAMプロファイルエディタをダウンロードしてインストールします</u>
<u>.</u>
<u>3. 一般的なデフォルト設定</u>
<u>4. シナリオ1:PEAP(MS-CHAPv2)ユーザ認証のためのセキュアなクライアントNAMサプリカ</u> <u>ントの設定</u>
<u>5. シナリオ2:EAP-FAST同時ユーザ認証とマシン認証のためのセキュアなクライアント</u> <u>NAMサプリカントの設定</u>
<u>6. シナリオ3:EAP TLSユーザ証明書認証のためのセキュアなクライアントNAMサプリカント</u> の設定
ーーー <u>7. シナリオ1 PEAP MSCHAPv2に基づく認証を許可するためのISR 1100およびISEの設定</u>
<u>確認</u>
トラブルシュート
問題:セキュアクライアントでNAMプロファイルが使用されていません。
問題2:さらなる分析のためにログを収集する必要があります <u>。</u>
ー <u>1. NAM拡張ロギングの有効化</u>
<u>2. 問題を再現します。</u>
<u>3. セキュアクライアントDARTバンドルを収集します。</u>
<u>関連情報</u>

はじめに

このドキュメントでは、Windowsでセキュアクライアントネットワーク解析モジュール(NAM)を 設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- RADIUSサプリカントとは何かについての基本的な知識
- Dot1x
- PEAP
- PKI

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Windows 10 Proバージョン22H2ビルド19045.3930
- ISE 3.2
- Cisco C1117 Cisco IOS® XEソフトウェア、バージョン17.12.02
- Active Directory 2016

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景説明

このドキュメントでは、WindowsでセキュアなクライアントNAMを設定する方法について説明し ます。事前展開オプションと、dot1x認証を実行するプロファイルエディタが使用されます。また 、これを実現する方法の例をいくつか示します。

ネットワーキングにおいて、サプリカントとは、ポイントツーポイントLANセグメントの一方の 端にあるエンティティで、そのリンクの他方の端に接続されたオーセンティケータによる認証を 求めるものです。IEEE 802.1X標準では、「サプリカント」という用語はハードウェアまたはソ フトウェアを指します。実際には、サプリカントはエンドユーザコンピュータにインストールさ れるソフトウェアアプリケーションです。ユーザはサプリカントを呼び出し、クレデンシャルを 送信して、コンピュータをセキュアネットワークに接続します。認証に成功すると、通常、オー センティケータはコンピュータがネットワークに接続することを許可します。

ネットワークアクセスマネージャについて

Network Access Managerは、ポリシーに従ってセキュアなレイヤ2ネットワークを提供するクラ イアントソフトウェアです。最適なレイヤ2アクセスネットワークを検出して選択し、有線ネット ワークとワイヤレスネットワークの両方にアクセスするためのデバイス認証を実行します。 Network Access Managerは、セキュアなアクセスに必要なユーザとデバイスのIDおよびネットワ ークアクセスプロトコルを管理します。インテリジェントに機能し、管理者が定義したポリシー に違反する接続をエンドユーザが行わないようにします。

Network Access Managerはシングルホーム設計になっており、一度に1つのネットワーク接続だ けを許可します。また、有線接続は無線よりも優先順位が高いため、有線接続を使用してネット ワークに接続している場合、ワイヤレスアダプタはIPアドレスなしで無効になります。

設定

ネットワーク図

dot1x認証では、dot1xを実行できるサプリカント、RADIUS内でdot1xトラフィックをカプセル化 するプロキシとして機能するNAS/NADとも呼ばれるオーセンティケータ、および認証サーバの 3つの部分が必要であることを理解することが重要です。

この例では、サプリカントはさまざまな方法でインストールおよび設定されます。後で、ネット ワークデバイスの設定と認証サーバのシナリオを示します。



ネットワーク図

コンフィギュレーション

- 1. セキュアクライアントNAM(Network Access Manager)をダウンロードしてインストールします。
- 2. Secure Client NAMプロファイルエディタをダウンロードしてインストールします。
- 3. 一般的なデフォルト設定
- 4. シナリオ1:PEAP(MS-CHAPv2)ユーザ認証用のセキュアクライアントNAMサプリカントの設定。
- 5. シナリオ2:ユーザ認証とマシン認証の設定と同時に、EAP-FAST用のセキュアなクライア ントNAMサプリカントを設定します。
- 6. シナリオ3パート1:EAP-TLS用のセキュアなクライアントNAMサプリカントの設定
- 7. シナリオ3パート2:NADとISEのデモンストレーションを設定します。
- 1. セキュアクライアントNAM(Network Access Manager)のダウンロードとインストール

Cisco Software のダウンロード

製品名の検索バーで、「Secure Client 5」と入力します。

Downloads Home > Security > VPN and Endpoint Security Clients > Secure Client (AnyConnectを含む) > Secure Client 5 > AnyConnect VPN Client Softwareの順に選択します。

この設定例では、バージョン5.1.2.42が使用されています。

Secure ClientをWindowsデバイスに導入する方法は、SCCM、アイデンティティサービスエンジン、およびVPNヘッドエンドから複数あります。ただし、この記事で使用するインストール方法は、導入前の方法です。

ページで、Cisco Secure Client Headend Deployment Package(Windows)ファイルを検索します

```
Cisco Secure Client Pre-Deployment 06-Feb-2024 108.30 MB \stackrel{\bullet}{\longrightarrow} Package (Windows) - includes individual MSI files 
cisco-secure-client-win-5.1.2.42-predeploy-k9.zip Advisories
```

Msi zipファイル

o

ダウンロードして解凍したら、Setupをクリックします。

Profiles	4/4/2024 7:16 PM
🧵 Setup	4/4/2024 7:16 PM
ժ cisco-secure-client-win-1.182.3-thousandeyes-predeploy-k9	4/4/2024 7:16 PM
🕵 cisco-secure-client-win-5.1.2.42-core-vpn-predeploy-k9	4/4/2024 7:16 PM
ժ cisco-secure-client-win-5.1.2.42-dart-predeploy-k9	4/4/2024 7:16 PM
ժ cisco-secure-client-win-5.1.2.42-iseposture-predeploy-k9	4/4/2024 7:16 PM
ժ cisco-secure-client-win-5.1.2.42-nam-predeploy-k9	4/4/2024 7:16 PM
ժ cisco-secure-client-win-5.1.2.42-nvm-predeploy-k9	4/4/2024 7:16 PM
ժ cisco-secure-client-win-5.1.2.42-posture-predeploy-k9	4/4/2024 7:16 PM
ժ cisco-secure-client-win-5.1.2.42-sbl-predeploy-k9	4/4/2024 7:16 PM
ժ cisco-secure-client-win-5.1.2.42-umbrella-predeploy-k9	4/4/2024 7:16 PM
d cisco-secure-client-win-5.1.2.5191-zta-predeploy-k9	4/4/2024 7:16 PM
🛞 Setup	4/4/2024 7:16 PM
setup	4/4/2024 7:16 PM

クライアント・ファイルの保護

Network Access ManagerとDiagnostics and Reporting Toolモジュールをインストールします。



警告:Cisco Secure Client Wizardを使用する場合、VPNモジュールは自動的にインストー ルされ、GUIでは表示されません。VPNモジュールがインストールされていない場合、 NAMは機能しません。個々のMSIファイルを使用する場合、または別のインストール方 法を使用する場合は、VPNモジュールをインストールしてください。



[選択項目のインストール(Install Selected)] をクリックします。

EULAに同意します。

Supplemental End User License Agreement IMPORTANT: READ CAREFULLY By clicking accept or using the Cisco Technology, you agree that such use is governed by the Cisco End User License Agreement and the applicable Product Specific Terms (collectively, the "EULA"). You also acknowledge and agree that you have read the Cisco Privacy Statement. If you do not have authority to bind your company and its affiliates, or if you do not agree with the terms of the EULA, do not click 'accept' and do not use the Cisco Technology. If you are a Cisco channel partner accepting on behalf of an end customer ("customer"), you must inform the customer that the EULA applies to customer's use of the Cisco Technology and provide the customer with access to all relevant terms. The latest version of documents can be found at the following locations. Cisco End User License Agreement https://www.cisco.com/c/en/us/about/legal/cloud-andsoftware/end user license agreement.html Applicable Product Specific Terms: https://www.cisco.com/c/en/us/about/legal/cloudand-software/software-terms.html Cisco Privacy Statement: https://www.cisco.com/c/en/us/about/legal/privacy-full.html Accept Decline

EULAウィンドウ

NAMのインストール後に再起動が必要です。

Cisco Secure Client Install Selector

You must reboot your system for the installed changes to take effect.



リブート要件ウィンドウ

インストールが完了すると、Windowsの検索バーからファイルを検索して開くことができます。



X

2. セキュアクライアントNAMプロファイルエディタをダウンロードしてインストールする。

Dot1xの設定には、Cisco Network Access Manager Profile Editorが必要です。

セキュアクライアントをダウンロードした同じページに、Profile Editorオプションがあります。

この例では、バージョン5.1.2.42のオプションを使用しています。

Profile Editor (Windows) tools-cisco-secure-client-win-5.1.2.42-profileeditor-k9.msi Advisories 06-Feb-2024 15.71 MB



プロファイルエディタ

ダウンロードが完了したら、インストールに進みます。

msiファイルを実行します。

🚽 Cisco Secure Client Profile Editor Setup





Welcome to the Cisco Secure Client Profile Editor Setup Wizard

The Setup Wizard will install Cisco Secure Client Profile Editor on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

Next >

Cancel

< Back

プロファイルエディタの設定ウィンドウ





Choose the setup type that best suits your needs



	< Back	Next >	Cancel
--	--------	--------	--------

プロファイルエディタの設定



d Cisco Secure Client Profile Editor Setup	×
Ready to Install	
The Setup Wizard is ready to begin the Cisco Secure Client Profile Editor installation	
Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.	
Advanced Installer	
< Back Sinstal Cancel	

インストールウィンドウ

[Finish] をクリックします。



プロファイルエディタの設定の終了

インストールが完了したら、検索バーからNetwork Access Managerプロファイルエディタを開き ます。



検索バーのNAMプロファイルエディタ

Network Access Managerとプロファイルエディタのインストールが完了しました。

3. 一般的なデフォルト設定

この記事で説明するすべてのシナリオには、次の設定が含まれています。

- クライアントポリシー
- 認証ポリシー
- ネットワークグループ

Policy Notication Policy	Profile: Untitled			
ks	Connection Settings			
rk Groups	Default Connection Timeout (sec.)	40		
	Connection Attempt:			
	O Before user logon			
	Time to wait before allowing user to logon (sec.)	40		
	After user logon			
	Media			
	Manage Wi-Fi (wireless) Media			
	Enable validation of WPA/WPA2/WPA3 handshake	e		
	Enable Randomized MAC Address			
	Default Association Timeout (sec.)	5		
	Manage Wired (802.3) Media			
	Manage Mobile Broadband (36) Media			
	Enable Data Roaming			
	End-user Control			
	Allow end-user to:			
	Disable Client	Select machine	connection type	
		Enable by de	fan de	
		C chance by de	iour	
	Specify a script or application to run when connected	d		
	Auto-connect			
	Administrative Status			
	Service Operation FIPS Mode		Captive Portal Detection	
	Enable Disable Disable Enable	Disable	O Enable	

NAMプロファイルエディタクライアントポリシー

File Help			
Network Access Manager	Authentication Policy Profile: Untitled		
- Networks	Allow Association Modes	Allowed Authentication Modes	
	Select All (Personal)	Select All Outer	
	Open (no encryption)	⊡ EAP-FAST	
	Open (Static WEP)	EAP-GTC EAP-MSCHAPv2	
	Shared (WEP)	EAP-TLS	
	WPA Personal TKIP	EAP-TLS	
	WPA Personal AES	EAP-TTLS	
	WPA2 Personal TKIP	EAP-MD5 EAP-MSCHAPv2	
	WPA2 Personal AES	MSCHAP (legacy)	
	WPA3 Open (OWE)	MSCHAPv2 (legacy)	
	WPA3 Personal AES (SAE)	∐ LEAP	
	Select All (Enterprise)	✓ PEAP ✓ EAP-GTC	
	Open (Dynamic (802.1X) WEP)	EAP-MSCHAPv2	
	WPA Enterprise TKIP	EAP-TLS Allowed Wired Security	
	WPA Enterprise AES	Select All	
	WPA2 Enterprise TKIP	Open (no encryption)	
	WPA2 Enterprise AES	802. 1x only	
	CCKM Enterprise TKIP	802. 1x with MacSec	
	CCKM Enterprise AES	AES-GCM-128	
	WPA3 Enterprise AES	M W W W W W W W W W W W W W W W W W W W	
	WPA3 Enterprise AES		

NAMプロファイルエディタの認証ポリシー

File Help		
Network Access Manager	Network Groups Profile: Untitled	
Networks	Group:	
3 Network Groups	Local networks v Delete New	
	Allow end-user to: Create Networks Create Networks See scan list Network Order	
	Global Networks	
	Wind-	
	wired	
	Up	
	Down	
	Wireless:	
	Up	
	Down	
	Down	
	Other Hetworks in Level estimates	
	Other Networks in Local networks Available Networks	
	wired:	
	Up Name Cur	rrent Group
	Down	
	Wirelaser	
	Wreess: Wreess:	
	Up Name Cur	rrent Group
	Dava	
	Down	

Network Groupsタブ

4. シナリオ1:PEAP(MS-CHAPv2)ユーザ認証のためのセキュアなクライアントNAMサプリカントの設定

Networksセクションに移動します。

デフォルトのNetworkプロファイルは削除できます。

[Add] をクリックします。

Networks Profile: Untitled

Network

lame	Media Type	Group*	
			Add
			Edit
			Delete
A network in an	oup 'Global' is a member of <i>all</i> gro	ups.	

ネットワークプロファイルの作成

Networkプロファイルに名前を付けます。

Group MembershipにGlobalを選択します。Wired Network Mediaを選択します。

Networks

Name:	PEAP MSCHAPv2			Media Ty
Group Membership				Security Le
O In group:	Local networks	~	e	
In all groups (Global)				
Choose Your Network Media			-	
Wired (802.3) Network				
Select a wired network if	the endstations will be connect	ng to the network		
with a traditional etherne	t cable.			
O Wi-Fi (wireless) Network				
Select a WiFi network if th	ne endstations will be connectin	g to the network		
via a wireless radio conne	ction to an Access Point.			
SSID (max 32 chars):				
	Hidden Network			
	Corporate Network			
Association Timeout	5	seconds		
Common Settings				
Script or application on each use	er's machine to run when conne	cted.		
		Browse Local Machine		
Connection Timeout	40	seconds		
	Canad			

Network Profile Media Typeセクション

[Next] をクリックします。

Authenticating Networkを選択し、Security Levelセクションのその他のオプションにはデフォルトを使用します。

rks Security Level	no security, and ar	e open to anybody within range.	This is	Media Type Security Level Connection Type
Authenticating Network Authenticating network enterprise level network other network infrast	or records. orks provide the high orks. Authenticatio tructure.	nest level of security and are perf n networks require radius servers	fect for s, and	
802. 1X Settings authPeriod (sec.)	30	startPeriod (sec.)	3	
heldPeriod (sec.)	60	maxStart	2	
	Port Authe	ntication Exception Policy e port exceptions w data traffic before authenticati	on	
Security Key Management None Encryption		w data traffic after authentication AP fails	n even if	

-

```
ネットワークプロファイルのセキュリティレベル
```

Nextをクリックして、Connection Typeセクションを続けます。

File Help

Network Access Manager	Networks Profile: Untitled	
Network Groups	Network Connection Machine Connection This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and ather undates from the network before the user has access. User Connection The user connection should be used when a machine connection is not needed. A user connection will make the network available after the user has logged on. Machine and User Connection This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in. 	Media Type Security Level Connection Type User Auth Credentials
	Next Cancel	

ネットワークプロファイル接続タイプ

User Connection接続タイプを選択します。

Nextをクリックして、利用可能になったUser Authセクションを続けます。

一般的なEAP MethodとしてPEAPを選択します。

Network Access Manager	, Networks Profile: Untitled	
Networks Network Groups	EAP Methods EAP-MD5 EAP-MSCHAPV2 EAP-TTLS EAP-TTLS EAP-TTLS EAP-TTLS EAP-FAST EAP-FEAP EAP-FAST Validate Server Identity Enable Fast Reconnect Disable when using a Smart Card Inner Methods based on Credentials Source Authenticate using a Password EAP-MSCHAPV2 EAP-GTC EAP-TLS, using a Certificate Authenticate using a Token and EAP-GTC	Media Type Security Level Connection Typ User Auth Certificates Credentials

ネットワークプロファイルユーザ認証

EAP-PEAP Settingsでデフォルト値を変更しないでください。

「クレデンシャルソースに基づく内部メソッド」セクションに進みます。

EAP PEAPに対して存在する複数の内部方式から、Authenticate using a Passwordを選択し、 EAP-MSCHAPv2を選択します。

Nextをクリックして、Certificateセクションに進みます。



注:[Certificate]セクションが表示されるのは、[EAP-PEAP Settings]で[Validate Server Identity]オプションが選択されているためです。EAP PEAPでは、サーバ証明書を使用し てカプセル化を行います。

CertificatesセクションのCertificate Trusted Server Rulesで、Common Name end with c.com ルー ルが使用されます。 設定のこのセクションでは、EAP PEAPフロー中にサーバが使用する証明書 について説明します。ご使用の環境でIdentity Service Engine(ISE)を使用している場合は、ポリシ ーサーバノードEAP証明書の共通名を使用できます。

Cisco Secure Client Profile	Editor - Network Access Manager	
Cisco Secure Client Profile File Help Client Policy Client Policy Authentication Policy Network Groups	Editor - Network Access Manager Networks Profile: Untitled Certificate Trusted Server Rules Common Name ends with c.com Certificate Field Match Value Subject Alt. Name Add Save	Media Type Security Level Connection Type User Auth Certificates Credentials
	Include Root Certificate Authority (CA) Installed on the OS Include Root Certificate Authority (CA) Certificates Add Remove	

Network Profile Certificateセクション

Certificate Trusted Authorityでは、2つのオプションを選択できます。 このシナリオでは、 RADIUS EAP証明書に署名した特定のCA証明書を追加する代わりに、オプションTrust any Root Certificate Authority (CA) Installed on the OSを使用します。

このオプションを使用すると、Windowsデバイスは、Manage User Certsプログラムの Certificates — Current User > Trusted Root Certification Authorities > Certificatesに含まれている 証明書によって署名されたすべてのEAP証明書を信頼します。

[Next] をクリックします。

Profile: Untitled		
User Identity		Media Type
Unprotected Identity Pattern:	anonymous	Security Level
		Connection Type
Protected Identity Pattern:	[username]	User Auth
		Certificates
. Liser Credentials		Credentials
Prompt for Credentials Remember Forever Remember while User Never Remember Use Static Credentials Password:	is Logged On	

Network Profile Credentialセクション

Credentialsセクションでは、User Credentialsセクションのみが変更されます。

Prompt for Credentials > Never Rememberオプションが選択されているため、認証を行うユーザ は認証ごとにクレデンシャルを入力する必要があります。

[Done] をクリックします。

File > Save Asオプションを使用して、Secure Client Network Access Manager(SCA)プロファイ ルをconfiguration.xmlとして保存します。

作成したばかりのプロファイルをセキュアクライアントネットワークアクセスマネージャで使用 するには、次のディレクトリにあるconfiguration.xmlファイルを新しいファイルで置き換えます。

C:\ProgramData\Cisco\Ciscoセキュアクライアント\Network Access Manager\system



注:ファイルはconfiguration.xmlという名前である必要があります。そうでない場合は機 能しません。



ファイルセクションの置換

5. シナリオ2:EAP-FASTユーザとマシンの同時認証のためのセキュアなクライアントNAMサプリ カントの設定

NAMプロファイルエディタを開き、Networksセクションに移動します。

[Add] をクリックします。

Networks Profile: Untitled

Network

Name	Media Type	Group*	
			Add
			Edit
			Delete
			Delete
* A network in gro	up 'Global' is a member of <i>all</i> /gro	ups.	

NAMプロファイルエディタネットワークタブ

ネットワークプロファイルに名前を入力します。

Group MembershipにGlobalを選択します。WiredNetwork Mediaを選択します。

Help Network Access Manager Or Client Policy Authentication Policy	Networks Profile: Untitled			
Authentication Policy	Name: Group Membership In group: In all groups (Global) Choose Your Network Media Wired (802.3) Network Select a wired network if	EAP-FAST Local networks	onnecting to the network	Media Type Security Level
	with a traditional ethernet Wi-Fi (wireless) Network Select a WiFi network if th via a wireless radio conne SSID (max 32 chars): Association Timeout	e endstations will be co ction to an Access Point Hidden Networ Corporate Net	nnecting to the network	
	Common Settings Script or application on each use	r's machine to run when	a connected. Browse Local Machine	
	Connection Timeout	40	seconds	
	N	Canc	el	

– 🗆 🗆

Media Typeセクション

[Next] をクリックします。

Authenticating Networkを選択し、このセクションの残りのオプションではデフォルト値を変更し ないでください。



Cancel

Security Level Profile Editorセクション

Nextをクリックして、Connection Typeセクションを続けます。

Next





Connection Typeセクション

3番目のオプションを選択して、ユーザとマシンの認証を同時に設定します。

[Next] をクリックします。



Machine Authセクション

Machine Authセクションで、EAP方式としてEAP-FASTを選択します。EAP FAST設定のデフォ ルト値は変更しないでください。Inner methods based on Credentials Sourceセクションで、方式 としてAuthenticate using a PasswordとEAP-MSCHAPv2を選択します。次にUse PACsオプショ ンを選択します。

[Next] をクリックします。

CertificatesセクションのCertificate Trusted Server Rulesで、ルールの共通名はc.comで終わって います。このセクションでは、EAP PEAPフロー中にサーバが使用する証明書について説明しま す。ご使用の環境でIdentity Service Engine(ISE)を使用している場合は、ポリシーサーバノード EAP証明書の共通名を使用できます。

Networks Profile: Untitled

					Security Leve
ode with c	c. com				Connection Typ
nus vitur c	c.com				Machine Auth
					Certificates
					Credentials
					User Auth
					Certificates
Match	h		Value		Credentials
exac	ctly matches		/		
Add			Save		
			Sure		
ate Author	rity (CA) Ins y (CA) Certif	talled on t	he OS		
ate Author	rity (CA) Ins	stalled on t	he OS		
Authority Add	rity (CA) Ins	talled on t	he OS Remove		
Add	rity (CA) Ins	talled on t	he OS Remove		

Machine Auth Server Certificate Trustセクション

Certificate Trusted Authorityでは、2つのオプションを選択できます。 このシナリオでは、 RADIUS EAP証明書に署名した特定のCA証明書を追加する代わりに、オプションTrust any Root Certificate Authority (CA) Installed on the OSを使用します。

このオプションを使用すると、ユーザ証明書の管理プログラム(Current User > Trusted Root Certification Authorities > Certificates)に含まれている証明書によって署名されたすべてのEAP証 明書がWindowsによって信頼されます。

[Next] をクリックします。

Client Policy Authentication Policy	Networks Profile: Untitled		
Networks	Machine Identity		Media Type
Network Groups	Unprotected Identity Pattern:	host/anonymous	Security Level
		······	Connection Type
	Protected Identity Pattern:	host/[username]	Machine Auth
			Certificates
	Machina Cradaptials		Credentials
	Had the credendals		User Auth
	 Use Machine Credentials 		Credentials
	O Use Static Credentials		
	0		
	Password:		

マシン認証クレデンシャルセクション

Machine CredentialsセクションでUse Machine Credentialsを選択します。

[Next] をクリックします。

File Help

Authentication Policy Networks	EAP Methods		Media Type
	C FAR-MDS	O FAP-TI S	Security Level
	O EAD MECHADUS	OFAD THE	Connection Type
	O EAP 475CHAPV2	O BAP-ITES	Machine Auth
	O EAP-GTC	OPEAP	Certificates
	a concernance of the second	EAP-FAST	Credentials
	Extend user connection beyon	nd log off	User Auth
			Certificates
	EAP-FAST Settings		Credentials
	Validate Server Identity		
	Enable Fast Reconnect		
	Disable when using a Sma	rt Card	
	Inner Methods based on Credentials S	iource	
	Authenticate using a Password	d	
		EAD CTC	
	Authenticate using a Certificat	te	
	 When requested send the 	e client certificate in the clear	
	 Only send client certificate 	es inside the tunnel	
	 Send client certificate using 	ng EAP-TLS in the tunnel	
	 Authenticate using a Token and 	nd EAP-GTC	
	Use PACs		

User Authentication セクション

User Authでは、EAP MethodとしてEAP-FASTを選択します。

EAP-FAST設定セクションでデフォルト値を変更しないでください。

Inner Method based on credentials sourceセクションでは、方式としてAuthenticate using a PasswordとEAP-MSCHAPv2を選択します。

Use PACsを選択します。

[Next] をクリックします。

CertificatesセクションのCertificate Trusted Server Rulesで、このルールはCommon Name ends with c.comです。次の設定は、EAP PEAPフロー中にサーバが使用する証明書用です。ご使用の 環境でISEを使用している場合は、ポリシーサーバノードEAP証明書の共通名を使用できます。

Networks Profile: C:\Users\LAB 5\Desktop\EAP FAST\configuration.xml

ertificate Trusted Server Ru	lec		
- Concerte Husted Server R	neo		Security Level
Common Name ande with	C 500		Connection Type
Common Warne enus with	C.COIII		Machine Auth
			Certificates
			Credentials
			User Auth
			Certificates
Certificate Field	Match	Value	Credentials
Common Name	\sim ends with	✓ c.com	
	Remove	Save	
Trust any Root Certi Include Root Certific	ficate Authority (CA) Installe ate Authority (CA) Certificate	d on the OS es	
Trust any Root Certi Include Root Certific	ficate Authority (CA) Installe	d on the OS es	
Trust any Root Certi Include Root Certific	ficate Authority (CA) Installe	d on the OS es	
ertificate Trusted Authority Trust any Root Certi Include Root Certific	ficate Authority (CA) Installe ate Authority (CA) Certificate	d on the OS es Remove	
ertificate Trusted Authority Trust any Root Certi Include Root Certific	ficate Authority (CA) Installe ate Authority (CA) Certificate	d on the OS es Remove	

User Auth Server Certificate Trustセクション

Certificate Trusted Authorityでは、2つのオプションを選択できます。このシナリオでは、 RADIUS EAP証明書に署名した特定のCA証明書を追加する代わりに、オプションTrust any Root Certificate Authority (CA) Installed on the OSを使用します。

[Next] をクリックします。

Networks

Profile: Untitled

Jser Identity		Media Type
Unprotected Identity Pattern:	anonymous	Security Level
		Connection Typ
Protected Identity Pattern:	[username]	Machine Auth
		Certificates
Jser Credentials		Credentials
	_	User Auth
O Use Single Sign On Credential	S	Certificates
Prompt for Credentials		Credentials
Remember Forever		
Remember while User	r is Logged On	
Never Remember		
O Use Static Credentials		
Password:		

ユーザ認証クレデンシャル

Credentialsセクションでは、User Credentialsセクションだけが変更されます。

オプションPrompt for Credentials > Never Rememberが選択されています。したがって、認証の たびに、認証するユーザは自分のクレデンシャルを入力する必要があります。

Doneボタンをクリックします。

File > Save asの順に選択し、Secure Client Network Access Manager(SCA)プロファイルを configuration.xmlとして保存します。

作成したばかりのプロファイルをSecure Client Network Access Managerで使用するには、次の ディレクトリにあるconfiguration.xmlファイルを新しいファイルで置き換えます。

C:\ProgramData\Cisco\Ciscoセキュアクライアント\Network Access Manager\system



注:ファイルはconfiguration.xmlという名前である必要があります。そうでない場合は機能しません。

6. シナリオ3:EAP TLSユーザ証明書認証のためのセキュアなクライアントNAMサプリカントの設定

NAMプロファイルエディタを開き、Networksセクションに移動します。

[Add] をクリックします。

Networks Profile: Untitled

Network

lame	Media Type	Group*	
			Add
			Edit
			Delete
	www.Volaballia.a.manhar.af.allan		
* A network in g	oup Global is a member of all gro	Joha .	

Network Creationセクション

ネットワークプロファイルに名前を付けます。この例では、名前付きはこのシナリオで使用され るEAPプロトコルと一致します。

Group MembershipにGlobalを選択します。有線ネットワークメディアです

Er Cisco Secure Client Profile Editor - Network Access Manager

- 22 Client Policy - 22 Authentication Policy	Profile: Untitled	_		
Networks	Name: Group Membership In group: In group: In al groups (Global) Choose Your Network Media Wired (802.3) Network Select a wired network if the with a traditional ethernet With Ethericational ethernet	EAP-TLS Local networks the endstations will be contracted by the c	onnecting to the network	Media Type Security Leve
	Select a WFi network if th	e endstations will be con	necting to the network	
	via a wireless radio conne	ction to an Access Point.		
	SSID (max 32 chars):			
		Hidden Network	c voric	
	Association Timeout	5	seconds	
	Common Settings			
	Script or application on each use	r's machine to run when	connected.	
			Browse Local Machine	
	Connection Timeout	40	seconds	

Media Typeセクション

[Next] をクリックします。

Authenticating Networkを選択し、Security Levelセクションの残りのオプションではデフォルト値 を変更しないでください。

File Help Network Access Manager Networks Client Policy **Profile: Untitled** Networks Security Level Media Type Security Level Open Network Connection Type Open networks have no security, and are open to anybody within range. This is the least secure type of net Authenticating Network Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure. 802. IX Settings authPeriod (sec.) 30 startPeriod (sec.) 3 heldPeriod (sec.) 60 maxStart 2 Port Authentication Exception Policy Enable port exceptions Allow data traffic before authentication Security Key Management (i) Allow data traffic after authentication even if None v EAP fails Encryption EAP succeeds but key management fails AES GCM 128 AES GCM 256 Cancel Next

セキュリティレベル

File Help

このシナリオは、証明書を使用したユーザ認証を対象としています。このため、オプションUser Connectionが使用されます。

111

P Cisco Secure Client Profile Editor - Network Access Manager

Authentication Policy	Network Connection Type	Mada Tura
		Security Level
20 ·····	O Machine Connection	Connection Type
	This should be used if the end station should log onto the network before the	Liser Auth
	user logs in. This is typically used for connecting to domains, to get GPO's and	Credentials
	other updates from the network before the user has access.	
	 User Connection The user connection should be used when a machine connection is not needed. A user connection will make the network available after the user has logged on. 	
	Machine and User Connection This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.	

```
接続タイプ
```

EAP方式としてEAP-TLSを設定します。EAP-TLS設定セクションでデフォルト値を変更しないで ください。

E Cisco Secure Client Profile Editor - Network Access Manager

Network Access Manager Orect Client Policy Authentication Policy Authentication Policy Networks	Networks Profile: Untitled	
	EAP Methods	Media Type
- A Network Groups	○ EAP-MD5	Security Level
	C EAP-MSCHAPV2 C EAP-TTLS	Connection Type
	O EAP-GTC O PEAP	User Auth
	OFAP-FAST	Certificates
	0.000	Credentials
	 ✓ Validate Server Certificate ✓ Enable Fast Reconnect ☐ Disable when using a Smart Card 	

User Authセクション

Certificatesセクションで、AAA EAP-TLS証明書と一致するルールを作成します。ISEを使用している場合は、Administration > System > Certificatesセクションでこのルールを確認します。

Certificate Trusted Authorityセクションで、Trust any Root Certificate Authority (CA) installed on the OSを選択します。

P Cisco Secure Client Profile Editor - Network Access Manager

Networks F Network Groups	Certificate Trusted Server Rules Common Name ends with c.com	Media Type Security Level Connection Type Liter Auth
	Certificate Field Match Value Subject Alt. Name Add Save Certificate Trusted Authority Certificate Trusted Authority Installed on the OS Include Root Certificate Authority (CA) Installed on the OS Include Root Certificate Authority (CA) Certificates	Credentials
	Add Remove	

ユーザ認証サーバ証明書の信頼設定

[Next] をクリックします。

User Credentialsセクションでは、最初の部分のデフォルト値を変更しないでください。

Networks Profile: Untitled

ser Identity		Media Type
Unprotected Identity Pattern:	[username]@[domain]	Security Level
		Connection Type
		User Auth
		Certificates
User Credentials		Credentials
Use Single Sign On Credential	s (Requires Smart Card)	
O Prompt for Credentials		
Remember Forever		
Remember while User	is Logged On	
O Never Remember		
Certificate Source	Remember Smart Card Pin	
Smart Card or OS certificates	Remember Forever	
 Smart Card certificates only 	 Remember while User is Logged On 	
	Never Remember	
Smart Card Removal Policy		
Disconnect from Network		
Use Certificate Matching Dule (M	av 10)	
	ax 10)	
Rule Logic OR OAND		
Field Oper-	ator Value	
		^
		·
	Add Edit Delete	
Done	Cancel	

User Auth Credentialsセクション

EAP TLSプロセス中にユーザが送信するID証明書と一致するルールを設定することが重要です。 これを行うには、Use Certificate Maching Rule (Max 10)の横にあるチェックボックスをクリック します。

[Add] をクリックします。

Certificate Matching Rule Entry × Certificate Field Match Ssuer.CN Equals Value My Internal OR 3rd Party CA.com OK Cancel OK Cancel C								
Certificate Field Match Issuer.CN Equals Value My Internal OR 3rd Party CA.com OK Cancel OK Cancel OBJOR AND d Operator Value Image: Concel	🖆 Certificate Matchi	ng Rule Entry						\times
Issuer.CN Value My Internal OR 3rd Party CA.com OK OK Cancel OK Cancel OK OK OK OK OK OK OK Cancel OK OK OK OK Cancel OK Cancel OK OK <	Certificate Field		Ν	Match				
Value My Internal OR 3rd Party CA.com OK Cancel OK Cancel	Issuer.CN		~	Equals				\sim
My Internal OR 3rd Party CA.com OK Cancel OK Cancel	Value							
OK Cancel	My Internal OR 3rd Par	ty CA.com						_
e Logic OR AND d Operator Value Add Edit Delete	O	<			Cano	el 🛛		
e Logic OR AND d Operator Value Add Edit Delete								
e Logic OR AND d Operator Value	ose cerunicate materiing it	uic (max 10)						
d Operator Value	Logic OR OAN	D						
Add Edit Delete	d	Operator		١	Value			
Add Edit Delete								^
Add Edit Delete								~
				Add		Edit	Delete	2

My Internal OR 3rd Party CA.comという文字列を、ユーザ証明書のCNに置き換えます。

Certificate Matching Ruleウィンドウ

Client Policy	Profile: Untitled		
Networks Network Groups	User Identity Unprotected Identity Pattern:	[username]@[domain]	Media Type Security Level Connection Type User Auth Certificates
	User Credentials User Single Sign On Credentials Prompt for Credentials Remember Forew Remember while Never Remember Certificate Source Smart Card or OS certificat Smart Card certificates on	ntials (Requires Smart Card) er User is Logged On tes y Remember Smart Card Pin Remember Forever Remember Forever Remember while User is Logged On	Credentials
	Smart Card Removal Policy Disconnect from Network Use Certificate Matching Rule Rule Logic OR AND	(Max 10)	
	Field C Issuer.CN EC	Add Edit Delete	

User Auth Certificate Credentialsセクション

Doneをクリックして、設定を終了します。

File > Save asの順に選択して、Secure Client Network Access Managerプロファイルを configuration.xmlとして保存します。

作成したばかりのプロファイルをSecure Client Network Access Managerで使用するには、次の ディレクトリにあるconfiguration.xmlファイルを新しいファイルで置き換えます。

C:\ProgramData\Cisco\Ciscoセキュアクライアント\Network Access Manager\system



注:ファイルはconfiguration.xmlという名前である必要があります。そうでない場合は機能しません。

7. シナリオ1 PEAP MSCHAPv2に基づく認証を許可するためのISR 1100およびISEの設定

ISR 1100ルータを設定します。

このセクションでは、dot1xを機能させるためにNADが必要とする基本設定について説明します。



注:マルチノードISE導入の場合は、ポリシーサーバノード(PSN)ペルソナが有効になっ ている任意のノードをポイントします。これを確認するには、Administration > System > DeploymentタブでISEに移動します。

aaa new-model aaa session-id common ! aaa authentication dot1x default group ISE-CLUSTER aaa authorization network default group ISE-CLUSTER aaa accounting system default start-stop group ISE-CLUSTER aaa accounting dot1x default start-stop group ISE-CLUSTER 1 aaa server radius dynamic-author client A.B.C.D server-key <Your shared secret> l ļ radius server ISE-PSN-1 address ipv4 A.B.C.D auth-port 1645 acct-port 1646 timeout 15 key <Your shared secret>

```
!
!
aaa group server radius ISE-CLUSTER
server name ISE-PSN-1
!
interface GigabitEthernet0/1/0
description "Endpoint that supports dot1x"
switchport access vlan 15
switchport mode access
authentication host-mode multi-auth
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast
```

Identity Service Engine 3.2を設定します。

ネットワークデバイスを設定します。

ISE Administration > Network Resources > Network DevicesにISR NADを追加します。

[Add] をクリックします。

Net	work Devices			
				Selected 0
🖉 Edit	+ Add 🗍 Duplicate	山 Import 🏠 Export 🗸	🔒 Generate PAC	🍵 Delete 🗸
	Name 🔿 IP/Mask	Profile Name	Location	Туре

Network Deviceセクション

作成するNADに名前を割り当てます。ネットワークデバイスのIPを追加します。

≡ Cisco ISE	Admi	nistration · Network Reso	urces	A Evaluation Mode 29 Days	Q @	Q	٩
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	More \vee			
Network Devices Default Device	Network Devices List	> ISR1100					
Device Security Settings	Name	ISR1100					
	Description						
	< IP Address	✓ * IP :A.B.C.D	′ <u>32</u> 🖗				
	Device Profile	Cisco					
	Model Name						
	Software Versio	n					

ネットワークデバイスの作成

同じページの下部に、ネットワークデバイス設定で使用したものと同じ共有秘密を追加します。

 RADIUS Authentication Settings 							
RADIUS UDP Set	tings						
Protocol	RADIUS						
Shared Secret			Show				
Use Second Sha	ared Secret 🕕						
S	econd Shared						
S	ecret	Show					
CoA Port	1700		Set To Default				



変更を保存します。

エンドポイントの認証に使用されるIDを設定します。

ISEローカル認証が使用されます。外部ISE認証については、この記事では説明しません。

Administration > Identity Management > Groupsタブに移動し、ユーザが属するグループを作成します。このデモンストレーション用に作成したIDグループはiseUsersです。

≡	С	isc	o ISE			Adminis	tration · Ide	entity Man	nagemen	t		🛦 Eva	luation Mo	de 29 Days	Q	0	Q	٩
lde	ntitie	es	Group	ps	External I	dentity Sources	Identity	/ Source Se	equences	s Settings								
,	denti ≣Q < >	ity G	roups Endpoint User Idea	t Identity	v groups	User Identity Gr Identity Gr * Name Description	oups > New U Dup iseUsers	Jser Identity G	roup	Submit	Cancel							
,	denti EQ < >	ity G	roups Endpoint User Ider	: Identity ntity Gro	Ç y Groups Doups	User Identity Gr Identity Gr * Name Description	oups > New U Dup iseUsers	lser Identity G	roup	Submit	Cancel							

IDグループの作成

[Submit] をクリックします。

Administration > Identity Management > Identity タブに移動します。

[Add] をクリックします。



Network Access Usersセクション

必須フィールドの一部として、ユーザの名前で始まります。この例では、ユーザ名iseiscoolを使 用しています。

Network Access Users List	New Network Access User		
✓ Network Access	User		
* Username	iseiscool		
Status	🗹 Enabled 🗸		
Account Name Alias		© _	
Email		-	

ユーザにパスワードを割り当てます。 VainillaISE97が使用されます。

✓ Passwords				
Password Type:	Internal Users 🗸 🗸			
Password Lifetime				
 With Expiration Password will ex Never Expires 	pire in 60 days			
	Password	Re-Enter Password		
* Login Password			Generate Password	0
Enable Password			Generate Password	0

User Creation Passwordセクション

ユーザをグループiseUsersに割り当てます。

∼ Use	er Groups		
I	iseUsers	~	1

ネットワークアクセスユーザの作成

ポリシーセットを設定します。

ISEメニュー>ポリシー>ポリシーセットに移動します。

デフォルトのポリシーセットを使用できます。ただし、この例では「Wired」という名前のAPが 作成されます。



注:ポリシーセットの分類と区別は、トラブルシューティングに役立ちます。



注:追加アイコンまたはプラスアイコンが表示されていない場合は、任意のポリシーセットの歯車アイコンをクリックし、[上に新しい行を挿入]を選択できます。

0	Default	Default policy set	Default Network Access	0 +	63	ŝ	>
				Insert ne	w row a	above	

歯車アイコンのオプション

使用されている条件は有線8021xです。これをドラッグして、Useをクリックします。



認証ポリシー条件スタジオ

Allowed ProtocolsセクションでDefault Network Accessを選択します。

	SE	Policy · Poli	cy Sets		A Evaluation Mode 2	9 Days	Q Ø	60 ¢
Policy Sets				Reset	Reset Policyset H			Save
🕂 Status	Policy Set Name	Description	Conditions	Allowed Protocols	/ Server Sequence	Hits	Actions	View
Q Search								
۲	Wired		Wired_802.1X	Default Network A	\sim +		ŝ	>
۲	Default	Default policy set		Default Network A			ŵ	>
						Reset		Save

ポリシーセットの概要

[Save] をクリックします。

2.d.認証ポリシーと認可ポリシーを設定します。

>アイコンをクリックします。

Authentication Policyセクションを展開します。

+アイコンをクリックします。

✓ Authentication	Policy (1)					
🕂 Status	Rule Name	Conditions		Use	Hits	Actions
Q Search						
			+			
⊘	Default			All_User_ID_Stores /		ŝ

認証ポリシー

認証ポリシーに名前を割り当てます。 この例では、「Internal Authentication」を使用しています。

この新しい認証ポリシーの条件列で+アイコンをクリックします。

事前に設定された条件Wired Dot1xが使用されます。

最後に、Use列でInternal Usersを選択します。

\vee Authentication Policy (1)			
Status Rule Name	Conditions	Use	Hits Actions
Q Search			
		Internal Users 🛛 🗸 🗸	
		✓ Options If Auth fail	
Internal Authentication	Wired_802.1X	REJECT /	ති
		If User not found REJECT	153
		If Process fail	

認証ポリシー

認可ポリシー.

Authorization Policyセクションは、ページの下部にあります。これを展開して、+アイコンをクリックします。

	Cis	co ISE		Policy · I	Policy Sets	A Evaluation Mode 29 Days	Q	0	9	٥
						 Options 				
> 4	Author	ization F	Policy - Local Exceptions							
> 4	Author	ization F	Policy - Global Exceptions							
$\sim I$	Author	ization F	Policy (1)							
					Results					
	} s	itatus	Rule Name	Conditions	Profiles	Security Groups	Hit	:s /	Actions	8
	Q									
					+					
		0	Default		DenyAccess	Select from list 🖉 +			ŝ	
						Rese			Save	

認可ポリシー

最近作成した許可ポリシーに名前を付けます。 この設定例では、名前Internal ISE Usersを使用し ます。

この許可ポリシーの条件を作成するには、Conditions列の+アイコンをクリックします。

グループIseUsersが使用されます。

Attributeセクションをクリックします。

IdentityGroupアイコンを選択します。

ディクショナリから、IdentityGroup属性に付属するInternalUserディクショナリを選択します。

Library	E	ditor										,	_
Search by Name			InternalUser·l	dentityGrou	p							-	8)
	• ₽ ₹	Selec	ct attribute for	conditio									
∷ 🗐 5G		•	🕸 O 坐	⊜₽	٩	8		©	1	ø	Ŀ	ę	
: BYOD_is_Registered			Dictionary		A	ttribu	te		ID	·	nfo		
Catalyst_Switch_Local_Web_A			All Dictionaries		A	Attribut	e		ID				
: E Compliance_Unknown_Devices		-	CWA		CW/	A_Exte	rnalGroups						
: Compliant_Devices		*	IdentityGroup		Des	cription	n						
EAP-MSCHAPv2		*	IdentityGroup		Nam	ne				0			
🗄 📄 EAP-TLS		*	InternalUser		lden	ntityGro	oup			0			
		*	PassiveID		Pass	siveID_	Groups						

条件の作成

Equals演算子を選択します。

User Identity Groupsで、グループIseUsersを選択します。

Library	Editor	
Search by Name		InternalUser-IdentityGroup
	P *	Equals Viser Identity Groups:iseUsers ×
∷ 🗐 5G 🕕 🕕		Set to 'Is not' Duplicate Save
BYOD_is_Registered		NEW AND OR
:: Catalyst_Switch_Local_Web_A uthentication		
: E Compliance_Unknown_Devices		
: Compliant_Devices		
EAP-MSCHAPv2		
EAP-TLS		
		Close

Useをクリックします。

Result認可プロファイルを追加します。

事前に設定されたプロファイルPermit Accessが使用されます。



注:この有線Dot1xポリシーセットに一致する、ユーザIDグループISEUsersに属さない ISEへの認証は、デフォルトの認可ポリシーに一致し、結果はDenyAccessになることに 注意してください。

\sim Auth	V Authorization Policy (1)										
					Results						
Ŧ	Status	Rule Name		Conditions	Profiles		Security Groups		Hits	Actions	
Q											
	0	Internal ISE Users	*	InternalUser-IdentityGroup EQUALS User Identity Groups:iseUsers	PermitAccess ×	~+	Select from list			ŝ	
	0	Default			DenyAccess		Select from list			ŝ	
								Reset		Save	

認可ポリシー

[Save] をクリックします。

確認

設定が完了すると、Secure Clientによってクレデンシャルの入力を求めるプロンプトが表示され、PEAP MSCHAPv2プロファイルの使用が指定されます。

以前に作成したクレデンシャルが入力されます。

🕲 Cisco Secur	e Client	-		×		
	Network:				Cisco Secure Client PEAP MSCHAPv2	×
	Authenticating				Please enter your username and password network: PEAP MSCHAPv2	for the
	PEAP MSCHAPv2	¹ X	x ~	≔	Username: iseiscool	
					Password: VainilaISE97	
•				cisco	Show Password	
					OK Ca	ancel

セキュアクライアントNAM

エンドポイントの認証が正しく行われているかどうかを確認します。 NAMが接続されていること を表示します。

Scisco Secure	e Client	_		\times
	Network: Connected (192.168.15.2) PEAP MSCHAPv2		X ~	
- X				
\$ ()				cisco

情報アイコンをクリックし、メッセージ履歴セクションに移動すると、NAMが実行したすべての 手順の詳細が表示されます。



クライアントのメッセージ履歴の保護

7:06:01 PM PEAP MSCHAPv2 : Authenticating 7:06:21 PM PEAP MSCHAPv2 : Acquiring IP Address 7:06:21 PM PEAP MSCHAPv2 : Connected

クライアントのメッセージ履歴の保護

ISEから、Operations > Radius LiveLogsの順に移動して、認証の詳細を確認します。次の図に示 すように、使用されたユーザ名が表示されます。

また、次のような詳細情報もあります。

- ・ タイムスタンプ.
- MAC アドレス.
- ポリシーセットが使用されました。
- 認証ポリシー。

セキュアクライアントNAM

- 認可ポリシー.
- ・その他関連情報

=	E Cisco ISE						ADIUS			🛦 Ev	A Evaluation Mode 7 Days Q			
Live L	ogs Live Sessions													
Misco	nfigured Supplicants 🕕		, i	Misconfigur	ed Network Devices		RADI	US Drops 🕕	Client Stopped Respon	ding 🕕		Repeat Co	ounter 🕕	
	0				0			25	0			0)	
									Refres Neve	h rr →	Show Latest 20 records	Within Last 5 m Filter V	inutes 🗸	
	Time	Status	Details	Repea	Identity	Endpoint ID	Endpoint	Authentication Policy	Authorization Policy	Authoriz	IP Address	Networ	k De	
					Identity	Endpoint ID	Endpoint Pr	Authentication Policy	Authorization Policy	Authorizatio	IP Address	Network	Devic	
	Apr 23, 2024 05:38:07.0	٠	2					Wired >> Internal Authentication	Wired >> Internal ISE Users	PermitAcc				
	Apr 23, 2024 06:38:06.8		R				Unknown	Wired >> Internal Authentication	Wired >> Internal ISE Users	PermitAcc		ISR1100		
Last	Updated: Tue Apr 23 202	4 13:02:14 GMT	-0600 (Cent	ral Standard	i Time)							Records S	hown: 2	

ISE RADIUSライブログ

正しいポリシーにヒットすることが確認でき、結果として認証ステータスの成功となるので、設 定は正しいと結論付けられます。

トラブルシュート

問題:セキュアクライアントでNAMプロファイルが使用されていません。

プロファイルエディタで作成した新しいプロファイルがNAMで使用されていない場合は、Secure ClientのNetwork Repairオプションを使用します。

このオプションは、Windowsバー> Circumflexアイコンのクリック> Secure Clientアイコンの右ク リック> Network Repairの順に選択すると表示されます。



Network Repairセクション

問題2:さらなる分析のためにログを収集する必要があります。

1. NAM拡張ロギングの有効化

NAMを開き、歯車アイコンをクリックします。



NAMインターフェイス

Log Settingsタブに移動します。Enable Extended Loggingチェックボックスにチェックマークを 付けます。

S Cisco Secure Client	- 🗆	×
Secure Client		0
Network Access Manager	Diagnostics	
Configuration Log Settings Statistics Message History		
Use extended logging to collect additional information about product operations.		
Enable Extended Logging		
IHV: Off ~		
Filter Driver: Off ~		
Credential Provider		
Packet Capture		
Maximum Packet Capture File Size (MB): 100		

クライアントNAMログのセキュリティ設定

2. 問題を再現します。

拡張ロギングを有効にすると、ログが生成されてトラフィックがキャプチャされたことを確認す るために、問題が複数回再現されます。

3. セキュアクライアントDARTバンドルを収集します。

Windowsから検索バーに移動し、Cisco Secure Client Diagnostics and Reporting Toolと入力します。



DARTモジュール

インストールプロセス中に、このモジュールもインストールしました。これは、ログと関連する dot1xセッション情報を収集することで、トラブルシューティングプロセスを支援するツールです 。

X

a la la

CISCO

Cancel

Next

最初のウィンドウでNextをクリックします。

Cisco Secure Client - DART

Diagnostic and Reporting Tool (DART)

DART is a tool that helps to bundle the appropriate log files and diagnostic information that can be used for analyzing and debugging the Cisco Secure Client.

This wizard will guide you through the steps required to create the diagnostic bundle. To continue, click Next.

DARTモジュール

再度Nextをクリックして、ログバンドルをデスクトップに保存できるようにします。

Cisco Secure Client - DART	×
Bundle Creation Option	uluilu cisco
Select "Default" to include the typical log files and diagnostic informatio bundle. Select "Custom" to choose the list of log files and diagnostic in to be included in the bundle.	n in the formation
 Default - Bundle will be saved to Desktop Custom 	
DART requires administrative privileges to clear Cisco Secure Clier Clear	n t logs. All Logs
Back Next	Cancel

DARTモジュール

必要に応じて、Enable Bundle Encryptionチェックボックスにチェックマークを付けます。

Cisco	Secure Client - DART			×
Bun	dle Encryption Option			uluulu cisco
	Enable Bundle Encryption			
	🗹 Mask Password			
	Encryption Password			
	Confirm Password			
		Back	Next	Cancel

DARTモジュール

DARTログ収集が開始されます。

Cisco Secure Client - DART

Bundle Creation Progress	uļuiļu cisco
Processing Application logs	
Finish	Cancel

DARTログの収集

プロセスが完了するまで10分以上かかる場合があります。

×

Cisco Secure Client - DART

Bundle Creation Result		uluilu cisco
The bundle was created successfully in C: 5\Desktop\DARTBundle_0423_1538.zip.	:\Users\LAB	
		KÇ
THE		
	Email Bundle	Finish

DARTバンドルの作成結果

DART結果ファイルは、デスクトップディレクトリにあります。

Name

Date modified

Туре

DARTBundle_0423_1538

4/24/2024 1:14 PM

Compressed (zipped) Folder

DART結果ファイル



シスコのテクニカルサポートとダウンロード

×

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。