# AD および NAM プロファイルのバイナリ証明書 比較を行う 802.1x EAP-TLS のコンフィギュレ ーション例

## 内容

概要 前提条件 要件 使用するコンポーネント 表記法 設定 トポロジ トポロジの詳細 70-スイッチの設定 証明書の準備 <u>ドメイン コントローラのコンフィギュレーション</u> サプリカントのコンフィギュレーション ACS 設定 確認 トラブルシュート ACS での無効な時間設定 証明書が AD DC で設定およびバインドされない NAM プロファイルのカスタマイズ 関連情報

## 概要

このドキュメントでは、サプリカントにより提供されるクライアント証明書および Microsoft Active Directory (AD) で保持された同じ証明書のバイナリ証明書比較を行う、Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) および Access Control System (ACS) での 802.1x コンフィギュレーションについて説明します。 AnyConnect Network Access Manager (NAM) プロファイルは、カスタマイズに使用されます。このドキュ メントでは、すべてのコンポーネントのコンフィギュレーション、およびコンフィギュレーショ ンをトラブルシューティングする状況について説明します。

前提条件

#### 要件

このドキュメントに特有の要件はありません。

#### 使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるもの ではありません。

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、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

#### 表記法

ドキュメント表記の詳細については、『<u>シスコ テクニカル ティップスの表記法</u>』を参照してくだ さい。

### 設定

#### トポロジ

- ・802.1x サプリカント:Cisco AnyConnect Secure Mobility Client Release 3.1.01065(NAM モ ジュール)を使用した Windows 7
- 802.1x オーセンティケータ: 2960 スイッチ
- 802.1x 認証サーバ:ACS リリース 5.4
- Microsoft AD 統合 ACS:ドメイン コントローラ: Windows 2008 Server

#### トポロジの詳細

- ACS : 192.168.10.152
- •2960:192.168.10.10(e0/0:サプリカント接続)
- DC 192.168.10.101
- Windows 7 : DHCP

### フロー

Windows 7 ステーションには、EAP-TLS メソッドで ACS サーバを認証するサプリカントとして 使用される、AnyConnect NAM がインストールされています。802.1x にスイッチは、オーセンテ ィケータとして機能します。ユーザ証明書は、ACS により検証されます。ポリシー認証は、証明 書の Common Name (CN)に基づいたポリシーを適用します。また、ACS は、AD からユーザ 証明書をフェッチし、サプリカントにより提供される証明書とのバイナリ比較を行います。

#### スイッチの設定

#### スイッチには、基本コンフィギュレーションがあります。デフォルトでは、ポートは隔離VLAN 666にあります。このVLANにはアクセスが制限されています。ユーザが承認されると、ポート VLAN が再設定されます。

aaa authentication login default group radius local aaa authentication dotlx default group radius aaa authorization network default group radius dotlx system-auth-control

interface Ethernet0/0
switchport access vlan 666
switchport mode access
ip device tracking maximum 10
duplex auto
authentication event fail action next-method
authentication order dot1x mab
authentication port-control auto
dot1x pae authenticator
end

radius-server host 192.168.10.152 auth-port 1645 acct-port 1646 key cisco

#### 証明書の準備

EAP-TLS では、証明書は、サプリカントおよび認証サーバの両方で必要です。この例は、 OpenSSL により生成された証明書に基づいています。Microsoft 認証局(CA)は、企業ネットワ ークでの導入を簡素化できます。

CA を生成するには、次のコマンドを入力します。
 openssl genrsa -des3 -out ca.key 1024
 openssl req -new -key ca.key -out ca.csr
 cp ca.key ca.key.org
 openssl rsa -in ca.key.org -out ca.key
 openssl x509 -req -days 365 -in ca.csr -signkey ca.key -out ca.crt
 CA 証明書は、ca.crt ファイルに保存されます。秘密(保護されない)キーは、ca.key ファ
 イルに保存されます。

次の3つのユーザ証明書およびACSの証明書を生成します。これらはすべてCAにより署名されます。CN=test1CN=test2CN=test3CN=acs54次に、CiscoのCAにより署名された1つの証明書の生成スクリプトを示します。

openssl genrsa -des3 -out server.key 1024 openssl req -new -key server.key -out server.csr

cp server.key server.key.org
openssl rsa -in server.key.org -out server.key

openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt -days 365 openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt -certfile ca.crt

秘密キーは server.key ファイルに保存され、証明書は server.crt ファイルに保存されます。 pkcs12 バージョンは、server.pfx ファイルに保存されます。

3. 各証明書(.pfx ファイル)をダブルクリックして、ドメイン コントローラにインポートしま す。ドメイン コントローラで、3 つすべての証明書は、信頼できる証明書でなければなりま

#### せん。

🚟 certingr - [Certificates - Current I	User\Personal\Certificates]				
File Action View Help					
🗢 ə> 🖄 📰 🔏 💺 🔀	🔒 🔽 🗊		Certificate	X	<sup>m</sup>
Certificates - Current User	Issued To A	Issued By	General Details Certification Path		E
Certificates	Egladministrator	Administrator	- Certification path		L
🗉 🚞 Trusted Root Certification Autho	Eltest1	TAC	TAC		
🗉 🚞 Enterprise Trust	test2	TAC	tests		
Intermediate Certification Authority	test3	TAC			
Active Directory User Object					
Intrusted Publishers     Intrusted Certificates					
Third-Party Root Certification A					
🗉 🚞 Trusted People					
🗉 🛄 Certificate Enrolment Requests					
Smart Card Trusted Roots					L
					Г
				View Certificate	
				[/	
			Certificate status:		
<u> </u>	•		This certificate is OK.		
			1		F
Add rokes	Roles:	Active Direc	Learn more about certification paths		
international and a second	NOICH	10110 210			
Add features	Feature	s: Group Polic		ak	for
	- Cottare				

同じプロセスが、Windows 7(サプリカント)で実行されるか、Active Directory によりユーザ証 明書にプッシュされます。

## ドメイン コントローラのコンフィギュレーション

特定の証明書を AD の特定のユーザにマッピングする必要があります。

- 1. Active Directory ユーザおよびコンピュータから、[Users] フォルダに移動します。
- 2. [View] メニューから、[Advanced Features] を選択します。

Active Directory Users and Computers	
File Action View Help	
(= in Add/Remove Columns	🝸 🔁 🕱
Active Direc Large Icons	Description   Wbudowane konto do ad
	. Wyznaczeni administrator . Wyznaczeni administrator
E Con     Users, Contacts, Groups, and Computers as containe     For     ✓ Advanced Features     E Con     Los     Filter Options	ers . Wyznaczeni administrator Grupa administratorów DNS . Klienci DNS, którzy są upo
	Wbudowane konto do dos Group Członkowie tej grupy nie
NTDS Quotas Image: Security of the	Group Członkowie tej grupy mog Group Wszystkie stacje robocze i Group Wszystkie kontrolery dom Group Elementy członkowskie tej Group Elementy członkowskie tej Konto usługi centrum dyst Group Serwery w grupie mogą z
Twórcy-właś Security ( Użytkownicy Security ( Wydawcy ce Security (	Group Członkowie tej grupy mog Group Wszyscy użytkownicy do Group Członkowie tej grupy maj

- 3. 次のユーザを追加します。 test1test2test3注:パスワードは重要ではありません。
- 4. [Properties] ウィンドウから、[Published Certificates] タブを選択します。テスト用の証明書 を選択します。たとえば、test1 の場合、ユーザ CN は test1 です。注:名前マッピング(ユ 一ザ名を右クリック)は使用しないでください。これは、別のサービスで使用されます。

Active Directory Users and Com	puters	test2 Properties				
File Action View Help			Security Environment Sessions Remote control			
🍊 🔿 🔊 🚟 🔏 🗎 🗶 🖻	a 🗟 🛃 🔽 📷 🔍 🗽 🕾 🤋	r 🖂 🖗	Terminal Services Profile COM+ Attribute Editor			
Active Directory Users and Comput	Name Type	Description	General   Address   Account   Profile   Telephones   Organization   Published Certificates   Member Of   Password Replication   Dial-in   Object			
E Statio	Administrator Security Group	Wyznaczeni ac	List of X509 certificates published for the user account			
Computers     Domain Controllers     ForeignSecurityPrincipals	Administrator Security Group Administrator Security Group DosAdmins Security Group	Wyznaczeni ac Wyznaczeni ac Grupa administ	Issued To Issued By Intended Purposes Expiration Lightest2 TAC Server Authentication 2014-03-			
LostAndFound     Pogram Data     Southern	Image: Security Group         Image: Security Group           Goscie domeny         Security Group           Socie         User	Klienci DNS, kti Wszyscy gości Wbudowane ki				
Users TDS Quotas	Grupa bez re Security Group Grupa z repi Security Group	Członkowie tej Członkowie tej				
	Kontrolery d Security Group Kontrolery d Security Group	Wszystkie kon Elementy człor				
	& Kontrolery d Security Group krbtgt User	Elementy człor Konto usługi ce	View Derthoste			
	Serwery RAS Security Group	Serwery w gru				
	Lest2 User	Członkowie tej				
	Wydawcy ce Security Group	Członkowie tej	Add from Store Add from File Remove Copy to File			
	1		OK Cancel Apply Hsip			

この段階では、証明書は、AD の特定のユーザにバインドされます。これは、Idapsearch で検証 できます。

ldapsearch -h 192.168.10.101 -D "CN=Administrator,CN=Users,DC=cisco-test,DC=com" -w Adminpass -b "DC=cisco-test,DC=com"

#### 次に、test2の結果の例を示します。

# test2, Users, cisco-test.com
dn: CN=test2,CN=Users,DC=cisco-test,DC=com

#### . . . . . . . . . . . . . . . . . .

userCertificate:: MIICuDCCAiGgAwIBAgIJAP6cPWHhMc2yMA0GCSqGSIb3DQEBBQUAMFYxCzAJ BgNVBAYTA1BMMQwwCgYDVQQIDANNYXoxDzANBgNVBAcMBldhcnNhdzEMMAoGA1UECgwDVEFDMQwwC gYDVQQLDANSQUMxDDAKBgNVBAMMA1RBQzAeFw0xMzAzMDYxMjUzMjdaFw0xNDAzMDYxMjUzMjdaMF oxCzAJBgNVBAYTA1BMMQswCQYDVQQIDAJQTDEPMA0GA1UEBwwGS3Jha293MQ4wDAYDVQQKDAVDaXN jbzENMAsGA1UECwwEQ29yZTEOMAwGA1UEAwwFdGVzdDIwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ AoGBAMFQZywrGTQKL+LeI19ovNavCFSG2zt2HGs8qGPrf/h3o4IIvU+nN6aZPdkTdsjiuCeav8HYD aRznaK1LURt1PeGtHlcTgcGZ1MwIGptimzG+h234GmPU59k4XSVQixARCDpMH8IBR9zOSWQLXe+kR iZpXC444eKOh6wO/+yWb4bAgMBAAGjgYkwgYYwCwYDVR0PBAQDAgTwMHcGA1UdJQRwMG4GCCsGAQU FBwMBBggrBgEFBQcDAgYKKwYBBAGCNwoDBAYLKwYBBAGCNwoDBAEGCCsGAQUFBwMBBggrBgEFBQgC FQYKKwYBBAGCNwoDAQYKKwYBBAGCNxQCAQYJKwYBBAGCNxUGBggrBgEFBQcDAjANBgkqhkiG9w0BA QUFAAOBgQCuXwAgcYqLNm6gEDTWm/OWmTFjPyA5KSDB76yVqZwr11ch7eZiNSmCtH7Pn+VILagf9o tiF15ttk9KX6tIvbeEC4X/mQVgAB3HuJH5sL1n/k2H10XCXKfMqMGrtsZrA64tMCcCeZRoxfAO94n PulwF4nkcnu1x0/B7x+LpcjxjhQ==

## サプリカントのコンフィギュレーション

- 1. このプロファイル エディタ、anyconnect-profileeditor-win-3.1.00495-k9.exe をインストール します。
- 2. Network Access Manager Profile Editor を開き、特定のプロファイルを設定します。
- 3. 特定の有線ネットワークを作成します。

File Help	Networks Profile: C:\1	Networks Profile: C:\1\prof1.xml										
Networks	Network	Network										
35	Name	Name Media Type Group*										
	my configured 802	2.1x profile Wired	Local networks									
				Add								
				Edit								
				Delete								

この段階で、各認証で証明書を使用する選択肢をユーザに与えることは非常に重要です。こ の選択はキャッシュされません。また、保護されていないIDとして「username」を使用し ます。ACSが証明書のADを照会するために使用するIDと同じではないことに注意してくだ さい。この ID は、ACS で設定されます。

Network Access Manager	Networks Profile: C:\1\prof1.xml									
Network Groups	User Identity Unprotected Identity Pattern:	[username]	Media Type Security Leve Connection Ty User Auth Credentials							
	User Credentials Use Single Sign On Credentials Prompt for Credentials Remember Forever Remember while User is L Never Remember	(Requires Smart Card) .ogged On								
	Certificate Sources     Smart Card or OS certificates     Smart Card certificates only	Remember Smart Card Pin <ul> <li>Remember Forever</li> <li>Remember while User is Logged On</li> <li>Never Remember</li> </ul>								

- 4. .xml ファイルを c:\Users\All Users\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml として保存します。
- 5. Cisco AnyConnect NAM サービスを再起動します。

この例では、手動によるプロファイル導入を示します。AD を使用して、このファイルをすべて のユーザに導入できます。また、VPN と統合される場合、ASA を使用してプロファイルをプロ ビジョニングできます。

## ACS 設定

1.	AD ドメインに都	参加します。	)								
	» ⊕ MyWorkspace	Users and identity Stores > Ext	ernal kilerality Stores > Active Dire	ctory							
	By Network Resources     Boundary Stores     Menthy Groups	General Directory Groups Directory Atributes Machine Access Restrictions Connection Datails									
	<ul> <li>Internal Identity Stores</li> <li>Users</li> </ul>	Node	Nade Role	Status	Domain Name	Domain Controller Name					
	Hosts	ats54	Primary	Joined and Connected	cisco-test.com	win-grag7bwtime.cisco-test.com					
	<ul> <li>External Identity Stores</li> <li>LDAP</li> </ul>	Join/Test Connection	Leave	•							
	RSA SecuriD Token Servers RSA SecuriD Token Servers RADIUS Identity Servers	Click on Sine Changes's to save AD configuration. Once you have successfully connected to the Domain, you can select Directory Omups and Directory Athlotso to be available through index in policy rules. Pressing on Class Configuration will sense the AD configuration and envoue ACE machine from the Domain.									
	Certificate Authorities	End User Authenticatio	n Settings								
	Certificate Authentication Profile	Enable passwor	d changa								
	Policy Elements     Access Policies	Enable machine	Enable mathine authentication     Enable dial-in check								
	· · · Hunitating and Reports	Enable caliback	check for dial-in clients								
	· _ summoning and respons	Required fields									
	<ul> <li>System Administration</li> </ul>										

ACS は、サプリカントから受信した証明書の CN フィールドを使用して、AD ユーザ名をマ ッチングします(この例では、test1、test2 または test3 です)。 バイナリ比較もイネーブ ルにされます。これにより、ACS は、AD からユーザ証明書を取得して、サプリカントによ り受信した同じ証明書と比較します。これが一致しない場合、認証は失敗します。

🕨 🎲 My Workspace	Users and Identity Stores > Certificate Authentication Profile > Edit "cert profile 2"
Internal Identity Stores	General  O Name: Cert profile 2  Description:
Histina Identity Stores     Hosts     External Identity Stores     LDAP     Active Directory     RSA SecurID Token Servers     DMU0 Model Directory	Certificate Definition Principal Username X509 Attribute: Common Name Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory Name: AD1 Select Perform fields
Certificate Authorities Certificate Authonities Identity Store Sequences	
E. Access Policies      Monitoring and Reports      System Administration	

2. Identity Store Sequence を設定します。これは、証明書ベースの認証および証明書プロファ イルで AD を使用します。

My Workspace	Users and identity Stores > identity Store Sequences > Edit: "seq"
In the second	General
🔹 🎒 Users and Identity Stores	o Name: Iseq
Identity Groups  Internal Identity Stores Users Hosts External Identity Stores LDAP Active Directory RSA SecurID Token Servers RADIUS Identity Servers Certificate Authorities Certificate Authorities Certificate Sequences Policy Elements	Description:         Authentication Method List         Certificate Authentication Profile         Certificate Based         Certificate Based         Certificate Based         Password Based         Additional Attribute Retrieval Search List         An optional set of additional identity stores from which attributes will be retrieved         Available         Selected         Internal Hosts         NAC Profiler         win2k3
Locess Policies     Monitoring and Reports     System Administration	
	Advanced Options o = Required fields

これは、RADIUS Identity ポリシーの Identity Source として使用されます。

🕨 😚 My Workspace	Access Policies > Access Services > Default Network Access > Identity
Network Resources	Single result selection O Rule based result selection
B Users and Identity Stores	Identity Source: seq Select
Policy Elements	Advanced Options
👻 🎭 Access Policies	
Access Services     Service Selection Pulse	
O Default Device Admin	
Identity	
Authorization     O Default Network Access	
Identity	
Authorization	
Max Session User Settings	
Max Session Group Settings	
<ul> <li>Monitoring and Reports</li> </ul>	
System Administration	

3.2 つの認証ポリシーを設定します。最初のポリシーは、test1 に使用され、そのユーザのア クセスを拒否します。もう一方のポリシーは、test 2 に使用され、VLAN2 プロファイルでの アクセスを許可します。

	0. 1	0										
<ul> <li>MyWorkspace</li> </ul>	Access	control Policies & Access Services Service & Detroit Melawark Access & Authoritarian										
Network Resources	Standa	Standard Policy Exception Policy										
Users and Identity Stores	Netw	And a start of the second start of the										
Policy Elements												
<ul> <li>Access Policies</li> </ul>	FIDS	Filter Status 💌 Match it Equals 🔻 Enabled 💌 Clear Filter Go 🔻										
<ul> <li>Access Services</li> <li>Service Selection Rules</li> </ul>			Status	Name	NDB:Location	Time And Date	Conditions Compound Condition	Results Authorization Profiles	Hit Count			
👻 \Theta Default Device Admin	5		Θ	<u>ONtesti</u>	ANY	-ANY	Certificate Dictionary:Common Name equals test1	DenyAccess	6			
Identity Automication	8			CNtest2	-ANY-	-ANS	Certificate Dictionary.Common Name equals test2	vtan2	7			
Wax Bession Group Searngs     Nontoring and Reports     System Administration												

VLAN2 は、ユーザとスイッチの VLAN2 をバインドする RADIUS 属性を返す認証プロファ イルです。

<ul> <li>My Workspace</li> </ul>	Policy Ele	ments	> Authorization and P	Permissions > N	etwork	Access > Authorization Profiles > Edit: "\
In the second						_
B Users and Identity Stores	Gei	neral .S	Common Tasks	RADIUS Attr	ibutes	
👻 🎭 Policy Elements	Do	vnloa	dable ACL Name:	Not in Use	-	
<ul> <li>Session Conditions         <ul> <li>Date and Time</li> <li>Custom</li> <li>Network Conditions</li> <li>End Station Filters</li> <li>Device Filters</li> <li>Device Port Filters</li> <li>Authorization and Permissions</li> <li>Network Access</li> <li>Authorization Profiles</li> </ul> </li> </ul>	Filt Pro Voi Per VL/ Rea Rea	er-ID / xy AC ce VL missi N N ID/ uther auther	ACL: L: AN ion to Join: Name: ntication ntication Timer:	Not in Use Not in Use Not in Use Static Not in Use		Value 2
<ul> <li>✓ Device Administration</li> <li>Shell Profiles</li> <li>Command Sets</li> <li>✓ Named Permission Objects</li> <li>Downloadable ACLs</li> </ul>	Ma Re: QO Inp Out	ntain authei S ut Poli put P(	icy Map: olicy Map:	Not in Use Not in Use	<b>▼</b>	
Access Policies	802	.1X-R	EV			
Monitoring and Reports	Lin	(Sec ) Redi	Security Policy: irect	Not in Use		
🕨 🍓 System Administration	Wh	en a l	URL is defined for F	edirect an ACL	. must	also be defined
	UR	L for F	Redirect:	Not in Use	-	
	UR	LRed	direct ACL:	Not in Use		
	🔅 = i	Requi	ired fields			

### 4. ACS に CA 証明書をインストールします。

+ 6	🚯 My Workspace	Users and identity Stores > Certificate Authorities									
+ (	Network Resources	Cer	Certificate Authorities								
÷ á	B Users and Identity Stores	Filt	er:		💌 Ma	tch if:	💌 Go 🗢				
⊥ ≖ I	Identity Groups nternal Identity Stores			Friendly Name	•	Expiration	Issued To	Issued By	Description		
₹ E	Users Hosts External Identity Stores LDAP Active Directory BSA Security Taken Secure			TAC		08:11 16.11.2013	TAC	TAC			
	RADIUS Identity Servers Certificate Authonities Certificate Authonities Identity Store Sequences										

5. ACS の Cisco の CA により署名される証明書(拡張認証プロトコルで使用)を生成および インストールします。

<ul> <li>Isola Network Resources</li> <li>Users and Identify Stores</li> <li>Policy Elements</li> <li>Access Policies</li> <li>Access Policies</li> <li>Montoring and Reports</li> <li>System Administration</li> <li>Authorit Calloh</li> <li>Authorit Calloh</li> <li>Authorit Calloh</li> <li>Authorit Calloh</li> <li>Operations</li> <li>Operations</li> <li>Configuration</li> <li>Generations</li> <li>Configuration</li> <li>Access Policies</li> <li>Experiment Inter</li> <li>Issued By</li> <li>Valid From</li> <li>Valid Trop Valid Trop</li></ul>	► 🖓 MyWorkspace	System Administration > Co	nfiguration > Local Server 0	ertificates > Local Cert	ificates		
<ul> <li>Wers and identity Stores</li> <li>Policy Elements</li> <li>Access Policies</li> <li>Access Policies</li></ul>	By Network Resources	Local Certificates					
<ul> <li>Policy Elements</li> <li>Access Policies</li> <li>Monitoring and Reports</li> <li>Weintoring and Reports</li> <li>System Administration</li> <li>Autorication</li> <li>Autorization</li> <li>Autorization</li> <li>Users</li> <li>Autoritation Settings</li> <li>Max User Session Global Settings</li> <li>Purge User Sessions</li> <li>Operations</li> <li>Configuration</li> <li>Global System Options</li> <li>TACCS's Settings</li> <li>EAP-FAST</li> <li>Battings</li> <li>EAP-FAST</li> <li>Battings</li> </ul>	Users and Identity Stores	Fitter	💌 Match if:		Ga 🛛 👻		
<ul> <li>Access Policies</li> <li>Montoring and Reports</li> <li>System Administration</li> <li>Aumorization</li> <li>Aumorization</li> <li>Aumorization</li> <li>Aumorization</li> <li>Users</li> <li>Authoritication Settings</li> <li>Max User Session Blobal Settings</li> <li>Purge User Sessions</li> <li>Operations</li> <li>Configuration</li> <li>Global System Colores</li> <li>Configuration</li> <li>Global System Colores</li> <li>Configuration</li> <li>Global System Colores</li> <li>FAP. Settings</li> <li>EAP.FAST</li> <li>Battings</li> <li>Generate PAC</li> </ul>	Policy Elements						
<ul> <li>Montoring and Reports</li> <li>action</li> <li>Authorization</li> <li>Operations</li> <li>Distributed System Management</li> <li>Scheduel Backups</li> <li>Local Operations</li> <li>Configuration</li> <li>Colobal System Opions</li> <li>TACACS+ Settings</li> <li>FEAP-FAST</li> <li>Bettings</li> <li>Generate PAD</li> </ul>	Access Policies	Friendly Name	<ul> <li>Issued to</li> </ul>	Issued By	Valid From	valid to (expiration)	Protocol
36554       36554       36554       172118.02.2013       172118.05.2013       NA         Authorization       Authorization       Authorization       NA         Authorization       Authorization       NA         Authorization       Authorization       NA         Authorization       NA         Authorization       NA         Authorization       NA         Authorization       NA         Operations       Distributed System Management         Scheuled Backups       NA         Local Operations       NA         Configuration       Colobal System Opions         TACACS+ Settings       FEAP-FAST         Battings       Generate PAD	Monitoring and Reports	<u>acso4</u>	acso4	DAG	09:23 22.02.2013	09:23 22:02:2014	EAP, Management Interface
R8A SecurID Prompts	<ul> <li>Montoring and Reports</li> <li>System Administration         <ul> <li>Authorization</li> <li>Users</li> <li>Authorization</li> <li>Users</li> <li>Authorization Settings</li> <li>Max User Session Blobal Settings</li> <li>Purge User Sessions</li> </ul> </li> <li>Operations         <ul> <li>Distributed System Management</li> <li>Scheduled Backups</li> <li>Local Operations</li> <li>Configuration</li> <li>Global System Options</li> <li>TACACS+ Settings</li> <li>EAP-FLS Settings</li> <li>EAP-FLS Settings</li> <li>Benerate PAC</li> <li>RSA SecuriD Prompts</li> <li>Dictionaries</li> <li>Protocols</li> <li>Identity</li> <li>Local Server Certificates</li> <li>Local Cenficates</li> </ul> </li> </ul>	acs54	acs64	ac554	17:21 19.02.2013	17:21 18.85.2013	ΝΛ Α

## 確認

AnyConnect NAM が使用されるまで、Windows 7 サプリカントでネイティブ 802.1x サービスを ディセーブルにすることをお勧めします。設定済みプロファイルにより、クライアントは特定の 証明書の選択が許可されます。

Cisco AnyConnect		
Choose certificate for the connection my configured	Cisco AnyConnect Secure Mobility Client	23
test3@  test3@ test2@	VPN: Verify your network connection.	1
test1@ Issued By: TAC	No Network Connectivity	,
Serial Number: FE9C3D61E131CD83	Network: Authenticating	1
OK Cancel	my configured 802.1x profile 🔍 👻 😑	J
	¢ ()	а)н. со

test2 証明書が使用される場合、スイッチは、成功応答と RADIUS 属性を受信します。

00:02:51: %DOT1X-5-SUCCESS: Authentication successful for client	
(0800.277f.5f64) on Interface Et0/0	
00:02:51: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dotly	: '
for client (0800.277f.5f64) on Interface Et0/0	
switch#	

00:02:51: %EPM-6-POLICY\_REQ: IP=0.0.0.0| MAC=0800.277f.5f64| AUDITSESID=C0A80A0A00000001000215F0| AUTHTYPE=DOT1X| EVENT=APPLY

switch#show authentication sessions interface e0/0

```
Interface: Ethernet0/0

MAC Address: 0800.277f.5f64

IP Address: Unknown

User-Name: test2

Status: Authz Success

Domain: DATA

Oper host mode: single-host

Oper control dir: both

Authorized By: Authentication Server

Vlan Policy: 2

Session timeout: N/A

Idle timeout: N/A

Common Session ID: COA80A0A0000001000215F0

Acct Session ID: 0x0000005

Handle: 0xE8000002
```

Runnable methods list: Method State dotlx Authc Succes

VLAN 2 は割り当てられます。 他の RADIUS 属性を ACS の認証プロファイルに追加できます (Advanced Access Control List または再認証タイマーなど)。

次に、ACS のログを示します。

I	12813	Extracted TLS CertificateVerify message.
	12804	Extracted TLS Finished message.
	12801	Prepared TLS ChangeCipherSpec message.
	12802	Prepared TLS Finished message.
	12816	TLS handshake succeeded.
	12509	EAP-TLS full handshake finished successfully
	12505	Prepared EAP-Request with another EAP-TLS challenge
	11006	Returned RADIUS Access-Challenge
	11001	Received RADIUS Access-Request
	11018	RADIUS is re-using an existing session
	12504	Extracted EAP-Response containing EAP-TLS challenge-response
	<u>Evaluat</u>	ting Identity Policy
	15006	Matched Default Rule
	24432	Looking up user in Active Directory - test2
	24416	User's Groups retrieval from Active Directory succeeded
	24469	The user certificate was retrieved from Active Directory successfully.
	22054	Binary comparison of certificates succeeded.
	22037	Authentication Passed
	22023	Proceed to attribute retrieval
	22038	Skipping the next IDStore for attribute retrieval because it is the one we authenticated against
	22016	Identity sequence completed iterating the IDStores
	<u>Evaluat</u>	ting Group Mapping Policy
	12506	EAP-TLS authentication succeeded
	11503	Prepared EAP-Success
	<u>Evaluat</u>	ting Exception Authorization Policy
	15042	No rule was matched
	<u>Evaluat</u>	ting Authorization Policy
	15004	Matched rule
	15016	Selected Authorization Profile - vlan2
	22065	Max sessions policy passed
	22064	New accounting session created in Session cache
l	11002	Returned RADIUS Access-Accept

## トラブルシュート

## ACS での無効な時間設定

発生する可能性のあるエラー:ACS Active Directory の内部エラー

12504 Extracted EAP-Response containing EAP-TLS challenge-response 12571 ACS will continue to CRL verification if it is configured for specific CA 12571 ACS will continue to CRL verification if it is configured for specific CA 12811 Extracted TLS Certificate message containing client certificate. 12812 Extracted TLS ClientKeyExchange message. 12813 Extracted TLS CertificateVerify message. 12804 Extracted TLS Finished message. 12801 Prepared TLS ChangeCipherSpec message. 12802 Prepared TLS Finished message. 12816 TLS handshake succeeded. 12509 EAP-TLS full handshake finished successfully 12505 Prepared EAP-Request with another EAP-TLS challenge 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request 11018 RADIUS is re-using an existing session 12504 Extracted EAP-Response containing EAP-TLS challenge-response Evaluating Identity Policy 15006 Matched Default Rule 24432 Looking up user in Active Directory - test1 24416 User's Groups retrieval from Active Directory succeeded 24463 Internal error in the ACS Active Directory 22059 The advanced option that is configured for process failure is used. 22062 The 'Drop' advanced option is configured in case of a failed authentication request.

## 証明書が AD DC で設定およびバインドされない

発生する可能性のあるエラー: Active Directory からユーザ証明書を受信できませんでした。

<ul> <li>12571 ACS will continue to CRL verification if it is configured for specific CA</li> <li>12811 Extracted TLS Certificate message containing client certificate.</li> <li>12812 Extracted TLS CertificateVenfy message.</li> <li>12804 Extracted TLS CertificateVenfy message.</li> <li>12804 Extracted TLS CintKeyExchange message.</li> <li>12804 Extracted TLS Finished message.</li> <li>12805 Prepared TLS Finished message.</li> <li>12806 Prepared TLS Finished message.</li> <li>12807 Prepared TLS Finished message.</li> <li>12808 EXP-TLS full handshake finished successfully</li> <li>12509 EAP-TLS full handshake finished successfully</li> <li>12509 Extracted EAP-Request with another EAP-TLS challenge</li> <li>11001 Received PADIUS Access-Request</li> <li>11018 RADIUS is re-using an existing session</li> <li>12504 Extracted EAP-Response containing EAP-TLS challenge-response</li> <li>Evaluating identity Policy</li> <li>12504 Extracted EAP-Response containing EAP-TLS challenge-response</li> <li>Evaluating identity Policy</li> <li>12504 Extracted EaP-Response containing EAP-TLS challenge-response</li> <li>Evaluating identity Policy</li> <li>12504 Extracted EAP-Response containing EAP-TLS challenge-response</li> <li>Evaluating identity Policy</li> <li>12504 Extracted EAP-Response containing EAP-TLS challenge-response</li> <li>224432 Looking up user in Active Directory succeeded</li> <li>224432 Looking up user in Active Directory succeeded</li> <li>224434 User's Groups retrieval from Active</li></ul>		
12811       Extracted TLS Certificate message containing client certificate.         12812       Extracted TLS ClientKeyExchange message.         12813       Extracted TLS CertificateVenfy message.         12804       Extracted TLS Chinished message.         12805       Prepared TLS ChangeCipherSpec message.         12806       Prepared TLS Finished message.         12807       Prepared TLS Finished message.         12808       EAP-TLS full handshake succeeded.         12809       EAP-TLS full handshake finished successfully         12809       EAP-REQuest with another EAP-TLS challenge         11000       Received RADIUS Access-Challenge         11001       Received RADIUS Access-Request         12804       Extracted EAP-Response containing EAP-TLS challenge-response         Evaluating Identity Policy       Isoland and and and and and and and and and	12571	ACS will continue to CRL verification if it is configured for specific CA
12812       Extracted TLS ClientKeyExchange message.         12813       Extracted TLS CertificateVerify message.         12804       Extracted TLS Finished message.         12805       Prepared TLS Finished message.         12806       Prepared TLS Finished message.         12807       Prepared TLS Finished message.         12808       Prepared TLS Finished message.         12809       EAP-TLS full handshake succeeded.         12509       EAP-TLS full handshake finished successfully         12509       Fepared EAP-Request with another EAP-TLS challenge         11001       Received RADIUS Access-Challenge         11001       Received RADIUS Access-Request         11012       RADIUS is re-using an existing session         12504       Extracted EAP-Response containing EAP-TLS challenge-response         Evaluating Identity Policy       1         12606       Matched Default Rule         22416       Useris Groups retrieval from Active Directory succeeded         22419       Useris Groups retrieval from Active Directory.         22429       Bilany comparison of certificate failed         22057       The advanced option that is configured in case of a failed authentication request is used.         22058       EAP-TLS authentication failed         22059 <td< th=""><th>12811</th><th>Extracted TLS Certificate message containing client certificate.</th></td<>	12811	Extracted TLS Certificate message containing client certificate.
12813       Extracted TLS CertificateVenfy message.         12804       Extracted TLS Finished message.         12805       Prepared TLS ChangeCipherSpec message.         12806       JEster TLS Finished message.         12807       Prepared TLS Finished message.         12808       TLS handshake succeeded.         12809       EAP-TLS full handshake finished successfully         12509       EAP-TLS full handshake finished successfully         12505       Prepared EAP-Request with another EAP-TLS challenge         11001       Received RADIUS Access-Challenge         11001       Received RADIUS Access-Request         11018       RADIUS is re-using an existing session         12504       Extracted EAP-Response containing EAP-TLS challenge-response         Evaluating Identity Policy       Isolon Matched Default Rule         24432       Looking up user in Active Directory - test2         24448       Failed to retrieve the user certificate from Active Directory.         24448       Failed to retrieve the user certificate from Active Directory.         22049       Binary comparison of certificates failed         22057       The advanced option that is configured for a failed authentication request is used.         22051       The Preject' advanced option is configured in case of a failed authentication request.	12812	Extracted TLS ClientKeyExchange message.
12804Extracted TLS Finished message.12801Prepared TLS ChangeCipherSpec message.12802Prepared TLS Finished message.12803Prepared TLS Finished message.12804TLS handshake succeeded.12805FAP-TLS full handshake finished successfully12806EAP-TLS full handshake finished successfully12807EAP-TLS full handshake finished successfully12808EAP-TLS full handshake finished successfully12809EAP-TLS full handshake finished successfully12809Extracted EAP-Request with another EAP-TLS challenge11011RADIUS is re-using an existing session12804Extracted EAP-Response containing EAP-TLS challenge-responseEvaluating Identity Policy12804Extracted EAP-Response containing EAP-TLS challenge-response24432Looking up user in Active Directory - test224432Looking up user in Active Directory - test224443Looking up user in Active Directory succeeded24400Some of the expected attributes are not found on the subject record. The default values, if configured, will be used for these attributes.24448Failed to retrieve the user certificate from Active Directory.22499Binary comparison of certificates failed22057The advanced option that is configured for a failed authentication request	12813	Extracted TLS CertificateVerify message.
12801Prepared TLS ChangeCipherSpec message.12802Prepared TLS Finished message.12816TLS handshake succeeded.12816TLS handshake succeeded.12805PAP-TLS full handshake finished successfully12806EAP-TLS full handshake finished successfully12807Prepared EAP-Request with another EAP-TLS challenge11008Received RADIUS Access-Challenge11001Received RADIUS Access-Request11012Received RADIUS access-Request11013RADIUS is re-using an existing session12804Extracted EAP-Response containing EAP-TLS challenge-responseEvaluating Identity Policy1806Matched Default Rule24432Looking up user in Active Directory - test224446User's Groups retrieval from Active Directory succeeded24100Some of the expected attributes are not found on the subject record. The default values, if configured, will be used for these attributes.24468Failed to retrieve the user certificate from Active Directory.22049Binary comparison of certificates failed22057The advanced option that is configured in case of a failed authentication request is used.22057EAP-TLS authentication failed22057EAP-TLS authentication failed21507EAP-TLS authentication failed21507EAP-TLS authentication failed21507EAP-TLS authentication failed21507EAP-TLS authentication failed21509EAP-TLS authentication failed21509EAP-TLS authentication failed <t< th=""><th>12804</th><th>Extracted TLS Finished message.</th></t<>	12804	Extracted TLS Finished message.
12802       Prepared TLS Finished message.         12816       TLS handshake succeeded.         12509       EAP-TLS full handshake finished successfully         12505       Prepared EAP-Request with another EAP-TLS challenge         11006       Returned PADIUS Access-Challenge         11001       Received RADIUS Access-Request         11018       RADIUS is re-using an existing session         12504       Extracted EAP-Response containing EAP-TLS challenge-response         Evaluating Identity Policy       Isoo         15006       Matched Default Rule         24432       Looking up user in Active Directory - test2         24446       User's Groups retrieval from Active Directory succeeded         24100       Some of the expected attributes are not found on the subject record. The default values, if configured, will be used for these attributes.         24458       Failed to retrieve the user certificate from Active Directory.         22049       Binary comparison of certificates failed         22057       The advanced option that is configured for a failed authentication request is used.         22051       The 'Reject' advanced option is configured in case of a failed authentication request.         12507       EAP-TLS authentication failed         11500       Prepared EAP-Failure         11500       Prepared EAP-Failure	12801	Prepared TLS ChangeCipherSpec message.
12816 TLS handshake succeeded.         12509 EAP-TLS full handshake finished successfully         12505 Prepared EAP-Request with another EAP-TLS challenge         11006 Returned RADIUS Access-Challenge         11001 Received RADIUS Access-Challenge         11001 Received RADIUS Access-Request         11018 RADIUS is re-using an existing session         12504 Extracted EAP-Response containing EAP-TLS challenge-response         Evaluating Identity Policy         15006 Matched Default Rule         24432 Looking up user in Active Directory - test2         24416 User's Groups retrieval from Active Directory succeeded         24410 Some of the expected attributes are not found on the subject record. The default values, if configured, will be used for these attributes.         24488 Failed to retrieve the user certificate from Active Directory.         22049 Binary comparison of certificates failed         22057 The advanced option that is configured in case of a failed authentication request.         22050 The Reject' advanced option is configured in case of a failed authentication request.         22051 The Reject' advanced option is configured in case of a failed authentication request.         12507 EAP-TLS authentication failed         11504 Prepared EAP-Failure         11003 Returned RADIUS Access-Reject	12802	Prepared TLS Finished message.
12509EAP-TLS full handshake finished successfully12505Prepared EAP-Request with another EAP-TLS challenge11006Returned RADIUS Access-Challenge11001Received RADIUS Access-Request11018RADIUS is re-using an existing session12504Extracted EAP-Response containing EAP-TLS challenge-responseEvaluating Identity Policy15006Matched Default Rule24421Looking up user in Active Directory - test224416User's Groups retrieval from Active Directory succeeded24409Some of the expected attributes are not found on the subject record. The default values, if configured, will be used for these attributes.24468Failed to retrieve the user certificate from Active Directory.22049Binary comparison of certificates failed22057The advanced option that is configured for a failed authentication request is used.22061The 'Reject' advanced option is configured in case of a failed authentication request.12507EAP-TLS authentication failed11504Prepared EAP-Failure11003Returned RADIUS Access-Reject	12816	TLS handshake succeeded.
12505       Prepared EAP-Request with another EAP-TLS challenge         11006       Returned RADIUS Access-Challenge         11001       Received RADIUS Access-Request         11018       RADIUS is re-using an existing session         12504       Extracted EAP-Response containing EAP-TLS challenge-response         Evaluating Identity Policy	12509	EAP-TLS full handshake finished successfully
11006Returned PADIUS Access-Challenge11001Received RADIUS Access-Request11018RADIUS is re-using an existing session12504Extracted EAP-Response containing EAP-TLS challenge-responseEvaluating Identity Policy15006Matched Default Rule24432Looking up user in Active Directory - test224416User's Groups retrieval from Active Directory succeeded24100Some of the expected attributes are not found on the subject record. The default values, if configured, will be used for these attributes.24468Failed to retrieve the user certificate from Active Directory.22049Binary comparison of certificates failed22057The advanced option that is configured for a failed authentication request is used.22061The 'Reject' advanced option is configured in case of a failed authentication request.12507EAP-TLS authentication failed11504Prepared EAP-Failure11003Returned RADIUS Access-Reject	12505	Prepared EAP-Request with another EAP-TLS challenge
<ul> <li>11001 Received RADIUS Access-Request</li> <li>11018 RADIUS is re-using an existing session</li> <li>12504 Extracted EAP-Response containing EAP-TLS challenge-response</li> <li>Evaluating Identity Policy</li> <li>15006 Matched Default Rule</li> <li>24432 Looking up user in Active Directory - test2</li> <li>24416 User's Groups retrieval from Active Directory succeeded</li> <li>24100 Some of the expected attributes are not found on the subject record. The default values, if configured, will be used for these attributes.</li> <li>24468 Failed to retrieve the user certificate from Active Directory.</li> <li>22049 Binary comparison of certificates failed</li> <li>22057 The advanced option that is configured for a failed authentication request is used.</li> <li>22061 The 'Reject' advanced option is configured in case of a failed authentication request.</li> <li>12507 EAP-TLS authentication failed</li> <li>11504 Prepared EAP-Failure</li> <li>11003 Returned RADIUS Access-Reject</li> </ul>	11006	Returned RADIUS Access-Challenge
<ul> <li>11018 RADIUS is re-using an existing session</li> <li>12504 Extracted EAP-Response containing EAP-TLS challenge-response</li> <li>Evaluating Identity Policy</li> <li>15006 Matched Default Rule</li> <li>24432 Looking up user in Active Directory - test2</li> <li>24416 User's Groups retrieval from Active Directory succeeded</li> <li>24100 Some of the expected attributes are not found on the subject record. The default values, if configured, will be used for these attributes.</li> <li>24468 Failed to retrieve the user certificate from Active Directory.</li> <li>22049 Binary comparison of certificates failed</li> <li>22057 The advanced option that is configured for a failed authentication request is used.</li> <li>22061 The 'Reject' advanced option is configured in case of a failed authentication request.</li> <li>12507 EAP-TLS authentication failed</li> <li>11504 Prepared EAP-Failure</li> <li>11003 Returned RADIUS Access-Reject</li> </ul>	11001	Received RADIUS Access-Request
12504 Extracted EAP-Response containing EAP-TLS challenge-response         Evaluating Identity Policy         15006 Matched Default Rule         24432 Looking up user in Active Directory - test2         24416 User's Groups retrieval from Active Directory succeeded         24100 Some of the expected attributes are not found on the subject record. The default values, if configured, will be used for these attributes.         24468 Failed to retrieve the user certificate from Active Directory.         22049 Binary comparison of certificates failed         22057 The advanced option that is configured for a failed authentication request is used.         22061 The 'Reject' advanced option is configured in case of a failed authentication request.         12507 EAP-TLS authentication failed         11504 Prepared EAP-Failure         11003 Returned PADIUS Access-Reject	11018	RADIUS is re-using an existing session
Evaluating Identity Policy 15006 Matched Default Rule 24432 Looking up user in Active Directory - test2 24416 User's Groups retrieval from Active Directory succeeded 24100 Some of the expected attributes are not found on the subject record. The default values, if configured, will be used for these attributes. 24468 Failed to retrieve the user certificate from Active Directory. 22049 Binary comparison of certificates failed 22057 The advanced option that is configured for a failed authentication request is used. 22061 The 'Reject' advanced option is configured in case of a failed authentication request. 12507 EAP-TLS authentication failed 11504 Prepared EAP-Failure 11003 Returned PADIUS Access-Reject	12504	Extracted EAP-Response containing EAP-TLS challenge-response
<ul> <li>15006 Matched Default Rule</li> <li>24432 Looking up user in Active Directory - test2</li> <li>24416 User's Groups retrieval from Active Directory succeeded</li> <li>24100 Some of the expected attributes are not found on the subject record. The default values, if configured, will be used for these attributes.</li> <li>24468 Failed to retrieve the user certificate from Active Directory.</li> <li>22049 Binary comparison of certificates failed</li> <li>22057 The advanced option that is configured for a failed authentication request is used.</li> <li>22061 The 'Reject' advanced option is configured in case of a failed authentication request.</li> <li>12507 EAP-TLS authentication failed</li> <li>11504 Prepared EAP-Failure</li> <li>11003 Returned PADIUS Access-Reject</li> </ul>	Evaluat	ting Identity Policy
<ul> <li>24432 Looking up user in Active Directory - test2</li> <li>24416 User's Groups retrieval from Active Directory succeeded</li> <li>24100 Some of the expected attributes are not found on the subject record. The default values, if configured, will be used for these attributes.</li> <li>24468 Failed to retrieve the user certificate from Active Directory.</li> <li>22049 Binary comparison of certificates failed</li> <li>22057 The advanced option that is configured for a failed authentication request is used.</li> <li>22061 The 'Reject' advanced option is configured in case of a failed authentication request.</li> <li>12507 EAP-TLS authentication failed</li> <li>11504 Prepared EAP-Failure</li> <li>11003 Returned PADIUS Access-Reject</li> </ul>	15006	Matched Default Rule
<ul> <li>24416 User's Groups retrieval from Active Directory succeeded</li> <li>24100 Some of the expected attributes are not found on the subject record. The default values, if configured, will be used for these attributes.</li> <li>24468 Failed to retrieve the user certificate from Active Directory.</li> <li>22049 Binary comparison of certificates failed</li> <li>22057 The advanced option that is configured for a failed authentication request is used.</li> <li>22061 The 'Reject' advanced option is configured in case of a failed authentication request.</li> <li>12507 EAP-TLS authentication failed</li> <li>11504 Prepared EAP-Failure</li> <li>11003 Returned PADIUS Access-Reject</li> </ul>	24432	Looking up user in Active Directory - test2
<ul> <li>24100 Some of the expected attributes are not found on the subject record. The default values, if configured, will be used for these attributes.</li> <li>24468 Failed to retrieve the user certificate from Active Directory.</li> <li>22049 Binary comparison of certificates failed</li> <li>22057 The advanced option that is configured for a failed authentication request is used.</li> <li>22061 The 'Reject' advanced option is configured in case of a failed authentication request.</li> <li>12507 EAP-TLS authentication failed</li> <li>11504 Prepared EAP-Failure</li> <li>11003 Returned RADIUS Access-Reject</li> </ul>	24416	User's Groups retrieval from Active Directory succeeded
<ul> <li>24468 Failed to retrieve the user certificate from Active Directory.</li> <li>22049 Binary comparison of certificates failed</li> <li>22057 The advanced option that is configured for a failed authentication request is used.</li> <li>22061 The 'Reject' advanced option is configured in case of a failed authentication request.</li> <li>12507 EAP-TLS authentication failed</li> <li>11504 Prepared EAP-Failure</li> <li>11003 Returned RADIUS Access-Reject</li> </ul>	24100	Some of the expected attributes are not found on the subject record. The default values, if configured, will be used for these attributes.
<ul> <li>22049 Binary comparison of certificates failed</li> <li>22057 The advanced option that is configured for a failed authentication request is used.</li> <li>22061 The 'Reject' advanced option is configured in case of a failed authentication request.</li> <li>12507 EAP-TLS authentication failed</li> <li>11504 Prepared EAP-Failure</li> <li>11003 Returned RADIUS Access-Reject</li> </ul>	24468	Failed to retrieve the user certificate from Active Directory.
<ul> <li>22057 The advanced option that is configured for a failed authentication request is used.</li> <li>22061 The 'Reject' advanced option is configured in case of a failed authentication request.</li> <li>12507 EAP-TLS authentication failed</li> <li>11504 Prepared EAP-Failure</li> <li>11003 Returned RADIUS Access-Reject</li> </ul>	22049	Binary comparison of certificates failed
22061 The 'Reject' advanced option is configured in case of a failed authentication request. 12507 EAP-TLS authentication failed 11504 Prepared EAP-Failure 11003 Returned RADIUS Access-Reject	22057	The advanced option that is configured for a failed authentication request is used.
12507 EAP-TLS authentication failed 11504 Prepared EAP-Failure 11003 Returned RADIUS Access-Reject	22061	The 'Reject' advanced option is configured in case of a failed authentication request.
11504 Prepared EAP-Failure 11003 Returned RADIUS Access-Reject	12507	EAP-TLS authentication failed
11003 Returned RADIUS Access-Reject	11504	Prepared EAP-Failure
	11003	Returned RADIUS Access-Reject

## NAM プロファイルのカスタマイズ

企業ネットワークでは、マシンとユーザの両方の証明書を使用して認証を行うことをお勧めしま す。このような場合、制限付き VLAN のスイッチでオープン 802.1x モードを使用することをお 勧めします。802.1x でマシンを再起動する場合、最初の認証セッションが開始し、AD マシン証 明書を使用して認証が行われます。次に、ユーザが証明書を提供し、ドメインにログインすると 、ユーザ証明書で次の認証セッションが開始されます。ユーザは、正しい(信頼できる)VLAN に接続され、フル ネットワーク アクセスが提供されます。これは、Identity Services Engine (ISE) で統合されます。



[Machine Authentication] および [User Authentication] タブから個別の認証を設定できます。

オープン 802.1x モードがスイッチで許容されない場合、ログオン機能がクライアント ポリシー で設定される前に、802.1x モードを使用できます。

## 関連情報

- <u>Cisco Secure Access Control System 5.3 ユーザ ガイド</u>
- <u>Cisco AnyConnect Secure Mobility Client 管理者ガイド リリース 3.0</u>
- <u>AnyConnect セキュア モビリティ クライアント 3.0:Windows 上での Network Access</u> <u>Manager& Profile Editor</u>
- <u>テクニカル サポートとドキュメント Cisco Systems</u>