Configure Secure Client IKEv2/ASA in ASDM with AAA & Cert Auth

Contents

Introduction
Prerequisites
Requirements
Components Used
Network Diagram
Configurations
Configuration in ASDM
Step 1 Open VPN Wizards
Step 2. Connection Profile Identification
Step 3. VPN Protocols
Step 4. Client Images
Step 5. Authentication Methods
Step 6. SAML Configuration
Step 7. Client Address Assignme
Step 8. Network Name Resolution Servers
Step 9. NAT Exempt
Step 10. Secure Client Deployment
Step 11. Save Settings
Step 12. Confirm and Export Secure Client Profile
Step 13. Confirm Detail of Secure Client Profile
Step 14. Confirm Settings in ASA CLI
Step 15. Add Cryptographic Algorithm
Configuration in Windows Server
Configuration in ISE
Step 1. Add Device
Step 2. Add Active Directory
Step 3. Add Identity Source Sequesce
Step 4. Add Policy Set
Step 5. Add Authentication Policy
Step 6. Add Authorization Policy
Verify
Step 1. Copy Secure Client Profile to Win10 PC1
Step 2. Initiate VPN Connection
Step 3. Confirm Syslog on ASA
Step 4. Confirm IPsec Session on ASA
Step 5. Confirm Radius Live Log
Troubleshoot
Step 1. Initiate VPN Connection
Step 2. Confirm Syslog in CLI
Reference

Introduction

This document describes the steps necessary for configuring secure client over IKEv2 on ASA using ASDM with AAA and certificate authentication.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Configuration of Cisco Identity Services Engine (ISE)
- Configuration of CiscoAdaptive Security Virtual Appliance(ASAv)
- Configuration of Cisco Adaptive Security Device Manager (ASDM)
- VPN Authentication Flow

Components Used

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

- Identity Services Engine Virtual 3.3 patch 1
- Adaptive Security Virtual Appliance 9.20(2)21
- Adaptive Security Device Manager 7.20(2)
- Cisco Secure Client 5.1.3.62
- Windows Server 2016
- Windows 10

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.

Network Diagram

This image shows the topology that is used for the example of this document.

The domain name configured on Windows Server 2016 is ad.rem-system.com, which is used as an example in this document.



Network Diagram

Configurations

Configuration in ASDM

Step 1. Open VPN Wizards

Navigate to Wizards > VPN Wizards, click Secure Client VPN Wizard.



Click Next.



Click Next Button

Step 2. Connection Profile Identification

Input information for connection profile. Connection Profile Name : vpn-ipsec-tunnel-grp VPN Access Interface : outside

Secure Client VPN Conne	ection Setup Wizard	×
Steps	Connection Profile Identification	
 Introduction Connection Profile Identification VPN Protocols Client Images Authentication Methods SAML Configuration Client Address Assignme Network Name Resolutio Servers NAT Exempt Secure Client Deployme Summary 	This step allows you to configure a Connection Profile Name and the Interface the remote access users will access for VPN connections. Connection Profile Name: vpn-ipsec-tunnel-grp VPN Access Interface: outside v	
	< Back Next > It in Help	,

Connection Profile Identification

Step 3. VPN Protocols

Select IPsec, click Add button to add a new self-signed certificate.

Steps	VPN Protocols	Issued To Issued By Expiry Date Associated Trustpoints Usage Public Key Type Add
1. Introduction	Secure Client can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols you would like this connection profile to support.	Show Details
 Connection Profile Identification 		Delete
3. VPN Protocols	59.	
 Client Images 	IPsec	Export
5. Authentication Methods	Device Certificate	Install
6. SAML Configuration	Device certificate identifies the ASA to the remote access clients. Certain Secure	Re-Enroll
7. Clenc Address Assignme 8. Network Name Resolutio	available on the ASA.	
Servers	Participations - Hora	
9. NAT Exempt	Panage	
10. Secure Client Deployme		
 Summary 		
		End: 🔘 🔘 🗌 Match Case
		Certificate Expiration Alerts
		Send the first alert before : 60 (days) Set Default
	< Back Next > 現別 Help	Repeat Alert Interval : 7 (days)
		Weak Crypto Configurations
		Permit Weak key sizes and Hash Algorithms
		Public CA Enrolment Get your Cisco ASA security appliance up and running quickly with an SSL Advantage digital certificate from Entrust. Entrust
		offers Cisco customers a special promotional price for certificates and trial certificates for testing.
		Enroll ASA SSL certificate with Entrust
		Using a previously saved certificate signing request, enroll with Entrust.
		ASDM Identity Certificate Witard
		The Cisco ASIA floating certificate Wizard assists you in creating a self-signed certificate that is required for launching ASIA through launcher.
		Launch ASDM Identity Certificate Wizard
		ware or reserve set in a rest of the rest

VPN Protocols

Input information for self-signed certificate.

Trustpoint Name : vpn-ipsec-trustpoint

Key Pair : ipsec-kp

Ta Add Identity Certificate X	Ta Add Key Pair	×
Trustpoint Name: vpn-ipsec-trustpoint	Key Type: O RSA O ECDSA O EDDSA	
 Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key): 		
Decryption Passphrase:	Name: Use default key pair name	
File to Import From: Browse	O Enter new key pair name: ipsec-kp	
Add a new identity certificate:	Size: 4096 🗸	
Key Pair: ipsec-lp V Show New	Usage: O General purpose O Special	
Certificate Subject DN: CN=ciscoasa Select		
Generate self-signed certificate Act as local certificate authority and issue dynamic certificates to TLS-Proxy	Generate Now Cancel Help	
Advanced		
Add Certificate Cancel Help		

Detail of Self-Signed Certificate

Confirm the settings of VPN protocols, click Next button.

Secure Client VPN Conne	ection Setup Wizard	×
Steps 1. Introduction 2. Connection Profile Identification 3. VPN Protocols 4. Client Images 5. Authentication Methods 6. SAML Configuration 7. Client Address Assignme 8. Network Name Resolutio Servers 9. NAT Exempt 10. Secure Client Deployme 11. Summary	VPN Protocols Secure Client can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols yo would like this connection profile to support. SSL Pevice Certificate Device Certificate identifies the ASA to the remote access clients. Certain Secure Client features (Always-On, IPsec/IXEV2) require that valid device certificate be available on the ASA. Device Certificate: vpn-ipsec-trustpoint:unstructuredNamv Manage	u
	< Back Next > It in Help	_

Confirm Settings of VPN Protocol

Step 4. Client Images

Click Add button to add secure client image, click Next button.

Secure Client VPN Conne	ection Setup Wizard	×
Steps	Client Images	
1. Introduction	ASA can automatically upload the latest Secure Client package to the	he client device when it accesses the enterprise network.
2. Connection Profile Identification	A regular expression can be used to match the user-agent of a bro You can also minimize connection setup time by moving the image u	wser to an image. sed by the most commonly encountered operation system to
3. VPN Protocols	the top of the list.	
4. Client Images	A still a subside a start of a	
5. Authentication Methods	Add Keplace Delete 7 +	
6. SAML Configuration	Image	Regular expression to match user-agent
7. Client Address Assignme	disk0:/cisco-secure-client-win-5.1.3.62-webdeploy-49.pkg	
 Network Name Resolutio Servers 		
9. NAT Exempt		
10. Secure Client Deployme		
11. Summary		
	You can download Secure Client packages from Cisco by searching	'Secure Mobility Client' or <u>click here</u> ,
	< Back Next >	Riff Help

Client Images

Step 5. Authentication Methods

Click New button to add a new aaa server, click Next button.

Server Group Name : radius-grp

Authentication Protocol : RADIUS

Server IP Address : 1.x.x.191

Interface : inside



Authentication Methods

Step 6. SAML Configuration

Click Next button.

Secure Client VPN Conne	ection Setup Wizard	×
Steps	SAML Configuration	
 Introduction Connection Profile Identification VPN Protocols Client Images Authentication Methods SAML Configuration Client Address Assignme Network Name Resolutio Servers NAT Exempt Secure Client Deployme Summary 	This step allows you to configure a SAML and the authenticaion method. Authentication Method: AAA AAA AAA Server Group: radus-grp Use LOCAL if Server Group fails SAML Identity Provider SAML Server : None V Manage	
_	< Back Next >	Riff Help

SAML Configuration

Step 7. Client Address Assignme

Click **New** button to add a new IPv4 pool, click **Next** button.

Name : vpn-ipsec-pool

Starting IP Address : 172.16.1.20

Ending IP Address : 172.16.1.30

Subnet Mask : 255.255.255.0

Secure Client VPN Conne	ction Setup Wizard		×	Secure Client VPN Conne	ction Setup Wizard				×
Steps I. Introduction C. Connection Profile Identification VHV Protocols C. Cent Images S. Authentication Methods S. Authentication Methods S. Authentication Methods S. SAML Configuration T. Client Address Assignment Methods Name Resolutio Servers N. NAT Exempt S. Secure Client Deployme S. Summary S. S	Clerk Address Assignment This step allows you to create a new address pool or select an be assigned addresses from the pools when they connect. IPV6 address Pool in only supported for SSL connection. Iddress Pool: Select Nem Details of the selected address pool Nam Star Star Star	n existing address pool for IPv4 and IPv add IPv4 Pool me: vpr-prec-pool attrag IP Address IP Address IP Address IP 25-255-255.0 OK Cancel	ró. The Secure Clients will	Steps I. Introduction Connection Profile Identification UPM Protocols Cent Images Cent Images Cent Images Cent Images Cent Index Centification Cent Index Centification Cent Index Centification Cen	Clerk Address Assignm This step allows you to be assigned addresses IPv6 address pool is ori IPv6 address pool is ori Address Pool you rips Details of the select Starting IP Address: Ending IP Address: Submet Mask:	ert create a new address pool or sel from the pools when they comes or or eccod v New in address pool interface pool interf	nct an existing address pool for IPv4 a t.	nd IPv6. The Secure Clerk	s wil
	< Back Next >		Rifl Help		< gack Next >			Riff	lelp

Client Address Assign

Step 8. Network Name Resolution Servers

Input information for DNS and domain, click Next button.

DNS Servers : 1.x.x.57

Domain Name : ad.rem-system.com

Secure Client VPN Conne	ction Setup Wizard	×
Steps	Network Name Resolution Servers	
 Introduction Connection Profile Identification VPN Protocols Client Images Authentication Methods SAML Configuration Client Address Assignme Network Name Resolution Servers NAT Exempt Secure Client Deployme Summary 	This step lets you specify how domain names are resolved for the remote user when accessing the internal network. DNS Servers: Domain Name: ad.rem-system.com	
	< gack Next > Riff Hel	P

Network Name Resolution Servers

Step 9. NAT Exempt

Click Next button.

Secure Client VPN Conne	ection Setup Wizard	×
Steps	NAT Exempt	
I. Introduction Connection Profile Identification VPN Protocols Client Images Authentication Methods SAML Configuration Client Address Assignme Network Name Resolutio Servers NAT Exempt Secure Client Deployme I. Summary	If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation.	
	< Back Next > 単初	Help

NAT Exempt

Step 10. Secure Client Deployment

Select Allow Web Launch, click Next button.

Secure Client VPN Conne	ection Setup Wizard X
Steps 1. Introduction	Secure Client Deployment Secure Client program can be installed to a client device by one of the following two methods:
2. Connection Prone Identification 3. VPN Protocols 4. Client Images	 Web launch - On accessing the ASA using a Web Browser, the Secure Client package will be automatically installed; Pre-deployment - Manually install the Secure Client package.
 Authentication Methods SAML Configuration Client Address Assignme 	Caution: Web launch is global setting, it affects all connections. Secure Client SSL connections and clientless SSL connections will NOT work if it is turned off.
 Network Name Resolutio Servers NAT Exempt 	For pre-deployment, please remember to include the client profile 'disk0:/vpn-ipsec-tunnel-grp_client_profile.xml' from the ASA in your Secure Client package, otherwise IPsec connection will NOT work.
10. Secure Client Deployment 11. Summary	
	< gack Next > Rin Help

Step 11. Save Settings

Click **Finish** button and save the settings.

Secure Client VPN Conne	ction Setup Wizard		X S Warning X	
VPN Wizard	Summary Here is the summary of the configuration.		ASDM received messages below when one or more of the commands below were sent to the ASA. [OK] means success, [ERROR] means failure, [INFO] means information and [WARNING] means warning	
	Name Summary Name/Alas of the Connection Profile VPN Access Interface Device Digital Certificate VPN Protocols Enabled Secure Clear Images Authentication Server Group SAML Address Pool for the Cleart DMS Network Address Translation	Value vpn-ipsec-truntel-grp outside vpn-ipsec-trustpoint:unstructuredName=ciscoasa, CN IPsec only I package radus-grp Server: Authentication Method: aaa 172:16.1.30 Server: Domain Name: The protected traffic can be subjected to network address translation	[CK] je local pool ypn-ipsec-pool 172.16.1.20-172.16.1.30 mask: 255.255.255.0 [CK] ji wite clent profied "disk0:/ypn-ipsec-tunnel-grp_clent_profile.xml" to ASA [CK] wite clent profile "disk0:/ypn-ipsec-tunnel-grp_clent_profile [CK] anayconnet profiles vpn-ipsec-tunnel-grp_clent_profile [CK] asa-server radius-grp (niskde) host 1.1: //191 [CK] asa-server radius-grp (niskde) host 1.1: //191 [CK] asa-server radius-grp (niskde) host 1.1: //191 [CK] anay-policy GroupPolicy_vpn-ipsec-tunnel-grp internal [CK] group-policy GroupPolicy_vpn-ipsec-tunnel-grp attributes [CK] moturpin [CK] motuppolicy GroupPolicy_vpn-ipsec-tunnel-grp attributes [CK] motuppolicy GroupPolicy_vpn-ipsec-tunnel-grp attributes [CK] motuppolicy GroupPolicy_vpn-ipsec-tunnel-grp attributes [CK] motuppolicy GroupPolicy_vpn-ipsec-tunnel-grp attributes [CK] motuppolicy GroupPolicy_vpn-ipsec-tunnel-grp_attributes [CK] motuppolicy GroupPolicy_vpn-ipsec-tunnel-grp_attributes [CK] group-policy GroupPolicy_vpn-ipse	
	< Back Einish	取通 M		

Save Settings

Step 12. Confirm and Export Secure Client Profile

Navigate to **Configuration > Remote Access VPN > Network (Client) Access > Secure Client Profile**, click **Edit** button.

Ele View Iools Wigards Window Help	e 🔇 Refresh 🔇 Back 💭 Forward 🦻 Help			Type topic to search Ge	cisco
Device List Bookmarks	Configuration > Remote Access VPN > Network (Client) Acces	ss > Secure Client Profile			
Bodimarks ∂ ² ₽ × To boolmark a page, right-click on a node in the navigation tree and select. "Add to boolmarks". ● 6 ● 0 <	This panel is used to manage Secure Client Profiles and perform groupload and download of client profiles between local machine and de The profile Usage field is introduced with the Secure Mobility Solution Add Clief Edit 22 Change Group Policy Clieft Delete 2 Import	p assignment for Secure Clerk version 2.5 or later. You can select a provide. 	vife to edit, change group or to delete. You can select the 'Add' buttor and later.	to add a new profile. Pressing the Import or Export bu	tton is for
Inetwork (Client) Access	Profile Name	Profile Usage	Group Policy	Profile Location	
Secure Clent Connection Profiles Secure Clent Costonization(Localization Costonization(Localization Costonization(Localization Secure Clent Profile Secure Clent Software	Ison-basec-turnel-gro_client_profile	Any-Connect VPN Profile	GroupPolicy_upn-ipsec-tunnel-grp	disk0:/vpn-ipsec-tunnel-grp_ckent_profile.xml	



Confirm the detail of profile.

- Display Name (required) : ciscoasa (IPsec) IPv4
- FQDN or IP Address : 192.168.1.1
- **Primary Protocol** : IPsec

Secure Client Profile Editor - v	pn-ipsec-tunnel-grp	_client_profile					Server List Entry					×
Profile: vpn-ipsec-tunne	l-grp_client_pr	ofile					Server Load Balancin	g Servers SCEP M	able Certificate Pinning			
UN Operation (Part 1)	Server List						Primary Server	_	_	Connection Information	an .	
Backup Servers							Display Name (re	equired) (iscolera)	(Psec) (Pv4	Primary Protocol	9ж –	
- Centificate Priving - E Centificate Matching	Hostname	Host Address	User Group	Backup Server List	SCEP	Mobile Setting	FQDN or IP Add		User Group	C ASA gateway		
- Centricate Envolment Huble Polcy				- 210 000			192.168.1.1		1	Auth Method Du	ring 3/E Negotiation	EAP-AnyConnect ~
Server Lat		-					Group UPL			B/E Identity (30	5 gateway only)	
	L											
	Note: it is highly of	ecommended that at	least one server be-	defined in a profile.		A51		Robert Server				
						EdR		Host Address			AM	
											Hove Up	
											Move Down	
											Delete	
									OK.	Cancel		

Confirm Secure Client Profile

Click **Export** button to export the profile to local PC.

File View Tools Wizards Window Help				Type topic to search
Home 🖧 Configuration 😥 Monitoring 🔲 Sav	re 🔇 Refresh 🔇 Back 💭 Forward 🦻 He	p		
Device List Bookmarks	Configuration > Remote Access VPN > Networ	k (Client) Access > Secure Client Profile		
Bookmarks di P ×				
To bookmark a page, right-click on a node in the navigation	This namel is used to manage Secure Client Profiles.	and nerform group assignment for Secure Client version 2.5 or lat	er. You can select a profile to edit, change group or to delete. You can	select the 'Add' button to add a new profile. Pression the Import or Evnor
tree and select "Add to bookmarks".	and download of client profiles between local maching	ne and device.		
🐵 Go 🏢 Delete	The profile Usage field is introduced with the Secure	Mobility Solution. This field contains different profile usage in Sec	ure Client version 3.0 and later.	
Remote Access VPN d ¹ P	🗣 Add 🛃 Edit 💥 Change Group Policy 📋 D	elete 🛃 Impert 🕾 Export 🚮 Validate		
- ? Introduction				2 7 Lo 20
Network (Client) Access	Profile Name	Profile Usage	Group Policy	Profile Location
Secure Client Connection Profiles	vpn-ipsec-tunnel-grp_client_profile	AnyConnect VPN Profile	GroupPolicy_vpn-ipsec-tunnel-grp	disk0:/vpn-ipsec-tunnel-grp_client_profile.xml
Secure Client Customization/Localization				
Resources				
Script		Export Secure Client Profile	×	
Cill Test and Mercaner		Coport Secure Crient Prome	^	
Customized Installer Transforms		This papel is used to export Secure Client profile from	device to the local file system	
Localized Installer Transforms		This parents used to export secure caesic provertion	device to the local life system	
- Fo Secure Clent Profile				
Secure Client Software				
Secure Client External Browser		Profile Name: vpn-ipsec-tunnel-grp_client_profile		
- Up Dynamic Access Policies				
Group Policies		Local Bables Collinguity of 21th Dates Street	Dedteslues in Reversion	
IPsec(IKEv1) Connection Profiles		Local Pach: C:(Users(),J. L. , M., Dr. C. Clack	Desktop(vpn-pr	
- IPsec(IKEv2) Connection Profiles				
- 🐻 Secure Mobility Solution				
Address Assignment				
🕀 🐻 Advanced				
Clientless SSL VPN Access		Export Cancel	Help	
AAA/Local Users				
FA Dochure (for Serure Firewall)				

Export Secure Client Profile

Step 13. Confirm Detail of Secure Client Profile

Open Secure Client Profile by browser, confirm that the primary protocol for host is IPsec.

Step 14. Confirm Settings in ASA CLI

Confirm the IPsec settings created by ASDM in the ASA CLI.

// Defines a pool of addresses ip local pool vpn-ipsec-pool 172.16.1.20-172.16.1.30 mask 255.255.255.0 // Defines radius server aaa-server radius-grp protocol radius aaa-server radius-grp (inside) host 1.x.x.191 timeout 5 // Define the transform sets that IKEv2 can use crypto ipsec ikev2 ipsec-proposal AES256 protocol esp encryption aes-256 protocol esp integrity sha-256 sha-1 crypto ipsec ikev2 ipsec-proposal AES192 protocol esp encryption aes-192 protocol esp integrity sha-256 sha-1 crypto ipsec ikev2 ipsec-proposal AES protocol esp encryption aes protocol esp integrity sha-256 sha-1 crypto ipsec ikev2 ipsec-proposal 3DES protocol esp encryption aes protocol esp integrity sha-256 sha-1 crypto ipsec ikev2 ipsec-proposal DES protocol esp encryption aes protocol esp integrity sha-256 sha-1 // Configures the crypto map to use the IKEv2 transform-sets crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2 ipsec-proposal AES256 AES192 AES 3DES DES crypto map outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP crypto map outside_map interface outside // Defines trustpoint crypto ca trustpoint vpn-ipsec-trustpoint enrollment self subject-name CN=ciscoasa keypair ipsec-kp crl configure // Defines self-signed certificate crypto ca certificate chain vpn-ipsec-trustpoint certificate 6651a2a2 308204ed 308202d5 a0030201 02020466 51a2a230 0d06092a 864886f7 0d01010b ac76f984 efd41d13 073d0be6 f923a9c6 7b quit // IKEv2 Policies crypto ikev2 policy 1 encryption aes-256 integrity sha256 group 5 prf sha256 lifetime seconds 86400 crypto ikev2 policy 10 encryption aes-192 integrity sha256

group 5 prf sha256 lifetime seconds 86400 crypto ikev2 policy 20 encryption aes integrity sha256 group 5 prf sha256 lifetime seconds 86400 crypto ikev2 policy 40 encryption aes integrity sha256 group 5 prf sha256 lifetime seconds 86400 // Enabling client-services on the outside interface crypto ikev2 enable outside client-services port 443 // Specifiies the certificate the ASA uses for IKEv2 crypto ikev2 remote-access trustpoint vpn-ipsec-trustpoint // Configures the ASA to allow Cisco Secure Client connections and the valid Cisco Secure Client images webvpn enable outside enable anyconnect image disk0:/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1 anyconnect profiles vpn-ipsec-tunnel-grp_client_profile disk0:/vpn-ipsec-tunnel-grp_client_profile.xml anyconnect enable tunnel-group-list enable // Configures the group-policy to allow IKEv2 connections and defines which Cisco Secure Client profile group-policy GroupPolicy_vpn-ipsec-tunnel-grp internal group-policy GroupPolicy_vpn-ipsec-tunnel-grp attributes wins-server none dns-server value 1.x.x.57 vpn-tunnel-protocol ikev2 default-domain value ad.rem-system.com webvpn anyconnect profiles value vpn-ipsec-tunnel-grp_client_profile type user // Ties the pool of addressess to the vpn connection tunnel-group vpn-ipsec-tunnel-grp type remote-access tunnel-group vpn-ipsec-tunnel-grp general-attributes address-pool vpn-ipsec-pool authentication-server-group radius-grp default-group-policy GroupPolicy_vpn-ipsec-tunnel-grp tunnel-group vpn-ipsec-tunnel-grp webvpn-attributes group-alias vpn-ipsec-tunnel-grp enable

Step 15. Add Cryptographic Algorithm

In ASA CLI, add group 19 to IKEv2 Policy.



Note: For IKEv2/IPsec connections, Cisco Secure Client no longer supports Diffie-Hellman (DH) groups 2, 5, 14, and 24 as of version 4.9.00086. This change can result in connection failures due to cryptographic algorithm mismatches.

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# group 19
ciscoasa(config-ikev2-policy)#
```

Configuration in Windows Server

You need to add a domain user for VPN connection. Navigate to**Active Directory Users and Computers**, click**Users**. Add vpnuser as domain user.

Active Directory Users and Computers						
File Action View Help						
🗢 🔿 🙍 🚮 🦨 🖬 🗶 🖾 🖉 📷 🖏	a in 🔻 🖬 a					
Active Directory Users and Computers Uninserver.ad.rem-system.com Saved Quenes Gamputers Domain Controllers ForeignSecurityPrincipals Manaped Service Accounts	Name Administrator Allowed RODC Passwor Cett Publishers Cett Publishers CettaultAccount DefaultAccount Denied RODC Passworc	Vpn user Properties Member Of Remote control General Address	Dial-in Er Remote Desktop 5 Account Profile	nvironment Services Profile Telephones	? X Sessions COM+ Organization	t for administering the computer/domain s group can have their passwords replicated to s group are permitted to publish certificates to s group that are domain controllers may be cl managed by the system. s group cannot have their passwords replicate stors Group
	DnsUpdateProxy Domain Admins Domain Computers Domain Controllers Domain Gouests Domain Users Demain Users Enterprise Admins Enterprise Key Admins	Enst name: Last name: Digplay name: Description: Offige:	vpnl user vpn user	jotais:		o are permitted to perform dynamic updates o ninistrators of the domain s and servers joined to the domain trollers in the domain sts rs ninistrators of the enterprise s group can perform administrative actions on
	Enterprise Read-only Di Group Policy Creator O Guest Key Admins MaR User ndes_user Protected Users RAS and IAS Servers Read-only Domain Con Schema Admins	_elephone number: Emgal: ₩eb page:			Qther	s group are Read-Only Domain Controllers in t s group can modify group policy for the domain t for guest access to the computer/domain s group can perform administrative actions on s group are afforded additional protections ag roup can access remote access properties of u s group are Read-Only Domain Controllers in t ninistrators of the schema
	vpn user	0	K Cancel	800Y	Help	

Add Domain User

Add the domain user to member of Domain Admins and Domain Users.

on user Properties			?	×	vpn user Pro	operties				?	×
Remote control	Remote I	Desktop Services Profile	CC	M+	Remote	control	Remote	Desktop Se	ervices Profile	CON	M+
Member Of	Dial-in	Environment	Sessio	ons	General	Address	Account	Profile	Telephones	Organiz	ation
General Address	Account	Profile Telephones	Organi	ization	Membe	r Of	Dial-in	Env	ironment	Session	ns
User logon name:					Member of	f:					
vpnuser		@ad.rem-system.com		\sim	Name		Active Direct	tory Domain	Services Folder		٦
User logon name (pre-	Windows 200	0):			Domain .	Admins	ad.rem-syste	m.com/Use	ers		
AD\		vpnuser			Domain	Users	ad.rem-syste	m.com/Use	ers .		
User must chan User cannot cha Password never Store password Account expires	ge password a ange password expires using reversib	t next logon d le encryption		~	Add	oup: D	Remove Iomain Users There is r	no need to	change Primary	group unle	
Ne <u>v</u> er					Set Prin	nary Group	you have	Macintosh	clients or POSID	(-compliant	t
◯ <u>E</u> nd of:	Monday .	June 10, 2024					αμμιταικ	n na .			
0	K (Cancel Apply	н	lelp		0	K	Cancel	Apply	He	

Domain Admins and Domain Users

Configuration in ISE

Step 1. Add Device

Network Devices	Network Device Gro	oups Netw	ork Device Profiles	External RAD	DIUS Servers	RADIUS Server Sequences
Network Devices Default Device Device Security Settings	Netwo Netwo Nan Des	work Devices List > A work Devices	SAv			
		IP Address 🛛 🗸	*IP: 1.070-0.61	/ 32	0	
	Dev	ice Profile 🗰	Cisco	~ (0	
	Mod	del Name		~		
	Sof	tware Version		~		
	Net	work Device Gro	up			
	Loc	ation All	Locations		Y Set To Def	ault
	IPS	EC No)		✓ Set To Def	ault
	Dev	ice Type All	Device Types		Y Set To Def	ault
		RADIU	S Authentication Set	ttings		
		RADIUS U	DP Settings			
		Protocol	RADIUS			
		Shared Sec	ret cisco123		н	ide

Navigate to**Administration > Network Devices**, click**Add**button to add ASAv device.

Add Device

Step 2. Add Active Directory

Navigate to**Administration > External Identity Sources > Active Directory**, click**Connection**tab, add Active Directory to ISE.

- Join Point Name: AD_Join_Point
- Active Directory Domain: ad.rem-system.com



Add Active Directory

Navigate to Groups tab, selectSelect Groups From Directoryfrom drop-down list.

Select Groups from Directory

ClickRetrieve Groupsfrom drop-down list. Checkad.rem-system.com/Users/Domain Computersandad.rem-system.com/Users/Domain Usersand clickOK.

=		Engine		×	
н	Bookmarks	Identities Groups E	Select Directory Groups		
	Dashboard) 🗆 Ceronicare Ab	This dialog is used to select groups from the Directory.		
15	Context Visibility	AD_Join_Poin	Name SID Type ALL		
×	Operations	C LDAP	Filter Filter Filter		
0	Policy	RADIUS Token		. 1	
10	Administration	C RSA SecuriD	Name Group SID Group Type		
- di	Work Centers	SAML Id Provide	ad.rem-system.com/Users/DrsAdmins S-1-5-21-4193742415-4133520026-20462399. DOMAIN LOCAL	1	
		🖾 Social Login	ad.rem-system.com/Users/DnsUpdateProxy 5-1-5-21-4193742415-4133520026-20462399. GLOBAL		
3	Interactive Help		ad.rem-system.com/Users/Domain Admins S-11-S-21-4193742415-4133520026-20462399 GLOBAL		
			ad.rem-system.com/Users/Domain Computers S-1-5-21-4193742415-4133520026-20462399 GLOBAL		
			ad.rem-system.com/Users/Domain Controllers S+1-5+21-4193742415-4133520026-20462399 GLOBAL		
			ad /em+system.com/Users/Domain Guests S+1+5+21+4193742415+4133520026+20462399 GLOBAL		
			ad.rem-system.com/Users/Domain Users. S-1-5-21-4193742415-4133520026-20462399 GLOBAL		
			ad.rem-system.com/Users/Enterprise Admins S+1+5+21+4193742415+4133520026+20462299 UNIVERSAL	(I	
			ad rem-system.com/Users/Enterprise Key Admine S-1-5-21-4193742415-4133520026-20462399_ UNIVERSAL	- 1	
			ad.rem-system.com/Users/Enterprise Read-only 5-1-5-21-4193742415-4133520026-20462399 UNIVERSAL		
			ad.rem-system.com/Users/Group Policy Creator S-1-5-21-4193742415-4133520026-20462399 GL08AL		
			4		
			Cancel		

Add Domain Computers and Users

Step 3. Add Identity Source Sequesce

Navigate toAdministration > Identity Source Sequences, add an Identity Source Sequence.

- Name: Identity_AD
- Authentication Search List: AD_Join_Point

≡	ababa Identity Services I	Engine Administration / Identity Management
н	Bookmarks	Identities Groups External Identity Sources Identity Source Sequences Settings
51	Dashboard	Identity Source Servences List > Identity AD
뱅	Context Visibility	Identity Source Sequence
×	Operations	
U	Policy	V Identity Source Sequence
80	Administration	Identity_AD
ń	Work Centers	Description
	Interactive Help	Certificate Based Authentication Select Certificate Authentication Profile Y Authentication Search List A set of identity sources that will be accessed in sequence until first authentication succeeds
		Available Selected
		Internal Endpoints AD_Join_Point Internal Users Guest Users All_AD_Join_Points

Add Identity Source Sequences

Step 4. Add Policy Set

Navigate to **Policy > Policy Sets**, click + to add a policy set.

- Policy Set Name : VPN_Test
- Conditions : DEVICE Device Type EQUALS All Device Types
- Allowed Protocols / Server Sequence : Default Network Access

≡	dentity Services Engine		Policy / Policy Set		🔺 Evaluation Mode 🛋 Days 🛛 🖉 🧔 🗘	A
Щ	Bookmarks	Policy Sets			Reset Reset Policyset Hitcounts Sav	/o
5	Dashboard	Status Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence Hits Actions Vi	iew
10	Context Visibility	Q Search				
×	Operations	VPN Test		DEVICE-Device Type EQUALS All	Default Network Access A + 30 263	
0	Policy	•		Device Types		·

Add Policy Set

Step 5. Add Authentication Policy

Navigate to Policy Sets, click VPN_Test to add an authentication policy.

- Rule Name : VPN_Authentication
- Conditions : Network Access Device IP Address EQUALS 1.x.x.61
- Use : Identity_AD

∨Authentication	Policy(2)
-----------------	-----------

+ Status Rule Name	Conditions	Use	Hits	Actions
Q Search				
VPN_Authentication		Identity_AD //	10	ŝ

Add Authentication Policy

Step 6. Add Authorization Policy

Navigate to Policy Sets, click VPN_Test to add an authorization policy.

- **Rule Name** : VPN_Authorization
- Conditions : Network_Access_Authentication_Passed
- **Results** : PermitAccess

		Results	Results				
+) Status Rule Name	Conditions	Profiles	Security Groups	Hits	Actions		
Q Search							
VPN_Authorization	Network_Access_Authentication_Passed	PermitAccess			ŝ		

Verify

Step 1. Copy Secure Client Profile to Win10 PC1

Copy the secure client profile to the C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile directory.



```
Copy Profile to PC
```

Step 2. Initiate VPN Connection

On the endpoint, run Cisco Secure Client and input the username and password, then confirm that Cisco Secure Client connects successfully.

Connection Succeeded

Step 3. Confirm Syslog on ASA

In the syslog, confirm that the IKEv2 connection succeeded.

<#root>

```
May 28 20xx 08:xx:20: %ASA-5-750006: Local:192.168.1.1:4500 Remote:192.168.1.11:50982 Username:vpnuser
New Connection Established
```

May 28 20xx 08:xx:20: %ASA-6-751026: Local:192.168.1.1:4500 Remote:192.168.1.11:50982 Username:vpnuser

Step 4. Confirm IPsec Session on ASA

run show vpn-sessiondb detail anyconnect command to confirm the IKEv2/IPsec session on ASA.

<#root>

ciscoasa#

show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

```
Username : vpnuser Index : 23
Assigned IP : 172.16.1.20 Public IP : 192.168.1.11
Protocol : IKEv2 IPsecOverNatT AnyConnect-Parent
License : AnyConnect Premium
Encryption : IKEv2: (1)AES256 IPsecOverNatT: (1)AES256 AnyConnect-Parent: (1)none
Hashing : IKEv2: (1)SHA256 IPsecOverNatT: (1)SHA256 AnyConnect-Parent: (1)none
Bytes Tx : 840 Bytes Rx : 52408
Pkts Tx : 21 Pkts Rx : 307
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GroupPolicy_vpn-ipsec-tunnel-grp
Tunnel Group : vpn-ipsec-tunnel-grp
Login Time : 08:13:20 UTC Tue May 28 2024
Duration : 0h:10m:10s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 01aa003d0001700066559220
Security Grp : none
```

IPsecOverNatT Tunnels: 1 AnyConnect-Parent Tunnels: 1 AnyConnect-Parent: Tunnel ID : 23.1 Public IP : 192.168.1.11 Encryption : none Hashing : none Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 19 Minutes Client OS : win Client OS Ver: 10.0.15063 Client Type : AnyConnect Client Ver : 5.1.3.62 IKEv2: Tunnel ID : 23.2 UDP Src Port : 50982 UDP Dst Port : 4500 Rem Auth Mode: userPassword Loc Auth Mode: rsaCertificate Encryption : AES256 Hashing : SHA256 Rekey Int (T): 86400 Seconds Rekey Left(T): 85790 Seconds PRF : SHA256 D/H Group : 19 Filter Name : Client OS : Windows Client Type : AnyConnect IPsecOverNatT: Tunnel ID : 23.3 Local Addr : 0.0.0.0/0.0.0.0/0/0 Remote Addr : 172.16.1.20/255.255.255.255/0/0 Encryption : AES256 Hashing : SHA256 Encapsulation: Tunnel Rekey Int (T): 28800 Seconds Rekey Left(T): 28190 Seconds Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Bytes Tx : 840 Bytes Rx : 52408 Pkts Tx : 21 Pkts Rx : 307

Step 5. Confirm Radius Live Log

Navigate to **Operations > RADIUS > Live Logs**in ISE GUI, confirm the live log for vpn authentication.

=	dealer Identity Services E	vices Engine						Operations / RADIUS				🔺 ې 💿 🎝 کې ۲۰۰۰ مونگې کمان مخاصفه ا				٩
Л	Bookmarks	Live Logs Live Sessions														
51	Dashboard															
N	Context Visibility	Misconfigured Supplicants			Misconfigured Network Devices 📀				RADIUS Drops		Client Stopped Responding			Repeat Counter 💿		
*	Operations	0			0				0		0			0		
0	Policy											Defrech	Show	Web		
8.	Administration											Never	V Latest 20 r	cords 🗸 Las	t 3 hours 🗸	
តី	Work Centers	C to Reset Repeat Counts										FB	e 🗸 😐			
		Time	Status	Details	Repeat	Endpoint	Identity	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization P	IP Address	Network De	Device Port	Identity Grou	
٢	Interactive Help	×				Endpoint ID	Identity	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profi	IP Address	Vetwork Devic	Device Port	Identity Group	
		May 28, 2024 05:13:42	•	0	0	00.50.5	vpnuser	Windows10-Workstation	${\rm VPN}_{\rm o}{\rm Test} \gg {\rm VPN}_{\rm o}{\rm Authentication}$	${\sf VPN}_{\circ}{\sf Test} \rightarrowtail {\sf VPN}_{\circ}{\sf Authorization}$	PermitAccess					
		May 28, 2024 05:13:42		ò		00.50.5	vpnuser	Windows10-Workstation	VPN_Test >> VPN_Authentication	VPN_Test >> VPN_Authorization	PermitAccess		ASAu		Workstation	

Radius Live Log

Click Status to confirm the detail of live log.

Cisco ISE					
Overview			Steps		
Event	5200 Authentication succeeded		Step ID	Description	Latency (ms)
			11001	Received RADIUS Access-Request	
Username	vpnuser		11017	RADIUS created a new session	1
Endpoint Id	00:50:56:98:77:A4 ⊕		15049	Evaluating Policy Group	36
Endpoint Profile	Windows10-Workstation		15008	Evaluating Service Selection Policy	1
			15048	Queried PIP - DEVICE.Device Type	6
Authentication Policy	VPN_Test >> VPN_Authentication		15041	Evaluating Identity Policy	20
Authorization Policy	VPN_Test >> VPN_Authorization		15048	Queried PIP - Network Access.Device IP Address	2
Authorization Result	PermitAccess		22072	Selected identity source sequence - Identity_AD	6
			15013	Selected Identity Source - AD_Join_Point	1
			24430	Authenticating user against Active Directory - AD_Join_Point	4
Authentication Details	uthentication Details			Resolving identity - vpnuser	38
Source Timestamp	2024-05-28 17:13:42.897		24313	Search for matching accounts at join point - ad.rem- system.com	0
Received Timestamp	2024-05-28 17:13:42.897		24319	Single matching account found in forest - ad.rem- system.com	0
Policy Server	ise33-01		24323	Identity resolution detected single matching account	0
Event	5200 Authentication succeeded		24343	RPC Logon request succeeded - vpnuser@ad.rem- system.com	23
Username	vpnuser		24402	User authentication against Active Directory succeeded - AD_Join_Point	3
Endpoint Id	00:50:56:98:77:A4		22037	Authentication Passed	1
Calling Station Id	192.168.1.11		24715	ISE has not confirmed locally previous successful machine authentication for user in Active Directory	1
Endpoint Profile	windows10-workstation		15036	Evaluating Authorization Policy	1
Authentication Identity	AD_Join_Point		24209	Looking up Endpoint in Internal Endpoints IDStore - vpnuser	0
Store			24211	Found Endpoint in Internal Endpoints IDStore	9
Identity Group	Workstation		15048	Queried PIP - Network Access.AuthenticationStatus	2
Audit Session Id	01aa003d0001700066559220		15016	Selected Authorization Profile - PermitAccess	7
Authentication Method	PAP ASCI		22081	Max sessions policy passed	6
Participation method			22080	New accounting session created in Session cache	0
Authentication Protocol	PAP_ASCII		11002	Returned RADIUS Access-Accept	2
Network Device	ASAv				

Detail of Live Log

Troubleshoot

The cryptographic algorithms mismatch can result in connection failures. This is an example of when an algorithms mismatch issue occurs. Executing Step 15 of section Configuration in ASDM can solve the issue.

Step 1. Initiate VPN Connection

On the endpoint, run the Cisco Secure Client and confirm that the connection failed due to a cryptographic algorithms mismatch.

The cryptographic algorithms required by the secure gateway do not match those supported by AnyConnect.

Connection Failed

Step 2. Confirm Syslog in CLI

In the syslog, confirm that the IKEv2 negotiation failed.

<#root>

```
May 28 20xx 08:xx:29: %ASA-5-750002: Local:192.168.1.1:500 Remote:192.168.1.11:57711 Username:Unknown I May 28 20xx 08:xx:29: %ASA-4-750003: Local:192.168.1.1:500 Remote:192.168.1.11:57711 Username:Unknown I
```

Failed to find a matching policy

Reference

AnyConnect Over IKEv2 to ASA with AAA and Certificate Authentication