Configurazione dell'integrazione Duo con Active Directory e ISE per l'autenticazione a due fattori su client VPN Anyconnect/Remote Access

Som	mario	
Sonn	nano	

Introduzione Prerequisiti **Requisiti** Componenti usati Premesse Esempio e diagramma reticolare Processo di comunicazione Configurazioni di Active Directory Duo **Duo Auth Proxy Configuration** Configurazioni Cisco ISE Configurazione Cisco ASA RADIUS/ISE Configurazione VPN di accesso remoto Cisco ASA Test Risoluzione dei problemi Debug del lavoro

Introduzione

In questo documento viene descritta l'integrazione push Duo con AD e ISE come autenticazione a due fattori per i client AnyConnect connessi all'appliance ASA.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- · Configurazione VPN Autorità registrazione su ASA
- Configurazione RADIUS su ASA
- ISE
- Active Directory
- Applicazioni Duo

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Server Microsoft 2016
- ASA 9.14(3)18
- ISE Server 3.0
- Duo
- Duo Authentication Proxy Manager

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

In questo documento viene descritto come configurare Duo Push Integration con Active Directory (AD) e Cisco Identity Service Engine (ISE) come autenticazione a due fattori per i client AnyConnect che si connettono a Cisco Adaptive Security Appliance (ASA).

Esempio e diagramma reticolare



Processo di comunicazione

https://duo.com/docs/ciscoise-radius

- 1. Autenticazione primaria avviata su Cisco ISE
- 2. Cisco ISE invia una richiesta di autenticazione al proxy di autenticazione Duo

- 3. L'autenticazione primaria utilizza Active Directory o RADIUS
- 4. Connessione Duo Authentication Proxy stabilita a Duo Security sulla porta TCP 443
- 5. Autenticazione secondaria tramite il servizio Duo Security
- 6. Il proxy di autenticazione Duo riceve una risposta di autenticazione
- 7. Accesso Cisco ISE concesso

Account utente:

- Amministratore di Active Directory: questo account viene utilizzato come account di directory per consentire al proxy di autenticazione Duo di eseguire il binding al server di Active Directory per l'autenticazione primaria.
- Utente test Active Directory
- · Duo test user per autenticazione secondaria

Configurazioni di Active Directory

Il server Windows è preconfigurato con Servizi di dominio Active Directory.

Nota:se Gestione proxy di autenticazione RADIUS Duo viene eseguito sullo stesso computer host di Active Directory, è necessario disinstallare/eliminare i ruoli di Server dei criteri di rete. Se vengono eseguiti entrambi i servizi RADIUS, possono verificarsi conflitti e influire sulle prestazioni.

Per ottenere la configurazione di Active Directory per l'autenticazione e l'identità degli utenti su utenti VPN ad accesso remoto, sono necessari alcuni valori.

Tutti questi dettagli devono essere creati o raccolti sul server Microsoft prima di poter eseguire la configurazione sull'appliance ASA e sul server proxy Duo Auth.

I valori principali sono:

- Nome dominio. Nome di dominio del server. In questa guida alla configurazione, il nome di dominio è agarciam.cisco.
- Indirizzo IP/FQDN del server. Indirizzo IP o FQDN utilizzato per raggiungere il server Microsoft. Se si utilizza un FQDN, è necessario configurare un server DNS all'interno di ASA e del proxy di autenticazione Duo per risolvere l'FQDN.

In questa guida alla configurazione, questo valore è agarciam.cisco (che si risolve in 10.28.17.107).

- Porta server. La porta utilizzata dal servizio LDAP. Per impostazione predefinita, LDAP e STARTTLS utilizzano la porta TCP 389 per LDAP, mentre LDAP over SSL (LDAPS) utilizza la porta TCP 636.
- CA radice. Se si utilizza LDAPS o STARTTLS, è necessaria la CA radice utilizzata per firmare il certificato SSL utilizzato da LDAPS.

- Nome utente e password della directory. Questo è l'account usato dal server proxy Duo Auth per eseguire il binding al server LDAP e autenticare gli utenti e cercare utenti e gruppi.
- Nome distinto (DN) di base e gruppo. Il DN di base è il punto di partenza per il proxy Duo Auth e indica ad Active Directory di iniziare la ricerca e l'autenticazione degli utenti.

In questa guida alla configurazione, il dominio radice agarciam.cisco viene utilizzato come DN di base e il DN gruppo è Duo-USERS.

1. Per aggiungere un nuovo utente Duo, in Windows Server passare all'icona Windows in basso a sinistra e fare clic su Strumenti di amministrazione di Windows, come mostrato nell'immagine.

≡	Recent	tly added	Windows Server		
		Notepad++			
	Z	PuTTYgen		Σ	2
		PSFTP	Server Manager	Windows PowerShell	Windows PowerShell ISE
	Expan	4 ~			
	Most	used	Windows		
		Duo Authentication Proxy Manager	Administrativ	Task Manager	Control Panel
		Command Prompt			
	-	Snipping Tool	Remote	10)	
		Wireshark	Desktop	Event Viewer	File Explorer
	Ń	Paint			
	9	Google Chrome			
	D				
		Duo Security New			
8	G				
0	9	Google Chrome New			
Ф	N				
	P-1	Notepad++			
	م		<u> </u>	• •	

2. Nella finestra Strumenti di amministrazione di Windows passare a Utenti e computer di Active Directory.

Nel pannello Utenti e computer di Active Directory espandere l'opzione dominio e passare alla cartella Utenti.

In questo esempio di configurazione, Duo-USERS viene utilizzato come gruppo di destinazione per l'autenticazione secondaria.

→ ↑ 倍 > Con	trol Panel > System and Security > Administra	tive Tools			Active Directory Users and Compute	ers		- C	1 X
Control C	trol Panel » System and Security » Administra Name Attive Directory Administrative Center Active Directory Domains and Trusts Active Directory Domains and Trusts Active Directory Domains and Trusts Active Directory Stess and Services Active Directory Stess and Services Active Directory Stess and Services Active Directory Users and Computers Active Directory Users and Computers Active Directory Users and Computers Active Directory Users and Computers Component Services Component Services Computer Management Defragment and Optimize Drives Disk Cleanup Disk Cleanup Active Directory	tive Tools Tr/14/2016 623 AM 7/16/2016 623 AM 7/16/2016 623 AM 7/16/2016 620 AM 7/16/2016 620 AM 7/16/2016 619 AM 7/16/2016 619 AM 7/16/2016 619 AM 7/16/2016 618 AM	Type File folder Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut	Size 2 KB 2 KB 2 KB 2 KB 2 KB 2 KB 2 KB 2 KB	Active Directory Users and Computer File Action View Help Active Directory Users and Com Saved Queries Builtin Buil	ers		o perform dynamic u	ipdates on
Pictures Videos Local Disk (C:) DVD Drive (D:) SSS_;	Event Viewer Group Policy Management Group Policy Management Signature formation Services (IIS) Manager Jocal Security Policy Microsoft Azure Services	7/16/2016 &18 AM 7/16/2016 &19 AM 7/16/2016 &19 AM 7/16/2016 &19 AM 7/16/2016 &18 AM 7/16/2016 &19 AM	Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut	2 KB 2 KB 2 KB 2 KB 2 KB 2 KB		Domain Gue. Security Group Domain Users Security Group DUO-USERS Security Group duo2 Security Group Security Group Enterprise K Security Group	All domain guests All domain users Designated administrato Members of this group		
🧼 Network	Microsoft Azure Services ODBC Data Sources (32-bit) ODBC Data Sources (64-bit)	7/16/2016 6:19 AM 7/16/2016 6:18 AM 7/16/2016 6:18 AM	Shortcut Shortcut	2 KB 2 KB 2 KB		Enterprise R Security Group	Members of this group		

3. Fare clic con il pulsante destro del mouse sulla cartella Users (Utenti) e selezionare New > User (Nuovo utente), come mostrato nell'immagine.

Active Directory Users and	Computers			-	×
File Action View Help					
🗢 🔿 🙍 🚾 🔏 🗋 🕻	K 🗊 🙆 📑 🔽 t	an 🐍 🔌 în 🤊	7 🧕 🕱		
Active Directory Users and C Saved Queries Saved Queries Builtin Builtin Computers Domain Controllers ForeignSecurityPrint Managed Service Action	ipal: cour Rest Cour Rest Rest Rest Rest Rest Rest Rest Rest	Type Type User User User Security Group Security Group Security Group	Description Built-in account for ad Members in this group c Members of this group Members of this group t		• • • • • • • • • • • • • • • • • • •
Delegate Find	Control :o D	. User Security Group	A user account manage Members in this group c		
New All Tasks View Refresh Export Li Properti Help	> > > st	Computer Contact Group InetOrgPerson msDS-KeyCreden msDS-ResourceP msDS-ShadowPri msImaging-PSPs	tial ropertyList incipalContainer		
< Create a new object	Enterprise Enterprise	MSMQ Queue Ali Printer User Shared Folder	ias .		~

4. Nella finestra Nuovo oggetto-utente, specificare gli attributi di identità per il nuovo utente e fare clic su Avanti, come mostrato nell'immagine.

New Object - User	×	
Create in: agarciam.cisco/Users		on
First name: duovpn Initials:	9	CC
Last name:		
Full name: duovpn	s	ir
	s	0
duovpn @agarciam.cisco ~	S	
Liser logon name (pre-Windows 2000):	s	ir
AGARCIAM\ duovpn	r	iir ite
	.6	ed
		ta'
< Back Next > Cance	l ai	in
	1	

5. Confermare la password e fare clic su Avanti, quindi su Fine una volta verificate le informazioni sull'utente.

New Object - User	×
Create in: agarciam.cisco/Users	0
Password: Confirm password:	30
 User must change password at next logon User cannot change password Password never expires Account is disabled 	s s c n n
< Back Next > C	ancel aii

6. Assegnare il nuovo utente a un gruppo specifico, fare clic con il pulsante destro del mouse e selezionare Aggiungi a un gruppo, come mostrato nell'immagine.

Active Directory Users and Com	puters	-			-	×
File Action View Help						
🗢 🔿 🙋 📅 🖌 🖬 🗡 🕼	1 🖬 📑 🖬 🖬	1 🙎 🐮 🗊 🦷	' 🗾 🗿			
Active Directory Users and Com Saved Queries Saved Queries Builtin Builtin Computers Domain Controllers Sim ForeignSecurityPrincipal: Managed Service Accour Users	Name Administrator agarciam alanad alanduo Allowed RO Cert Publish Cort Publish Coneable D DefaultAcco DefaultAcco Denied ROD Donain ROD Donain Ad Domain Ad Domain Co Domain Co Domain Gue Domain Gue Domain Users duo2 DUO-USERS	Type User User User Security Group Security Group	Description Built-in a Members Members A user ac Members DNS Adm DNS clier Designato All works All doma All doma	on ccount for ad s in this group c s of this group s of this group t count manage s in this group c ninistrators Gro ed administrato tations and ser in controllers i in guests in users		
< >	R Enterprise	Add to a group Disable Account		of this group		 ~
Allows you to add the selected object	ts to a group yo	a static Account				

7. Nel pannello Seleziona gruppi, digitare il nome del gruppo desiderato e fare clic su Controlla nomi.

Selezionare quindi il nome che corrisponde ai criteri e fare clic su OK.

Select Groups	×	
Select this object type: Groups or Built-in security principals	Object Types	-
From this location:	Object Types	:01
agarciam.cisco	Locations	
Enter the object names to select (examples):	\sim	
DUO-USERS	Check Names) †
	\smile	of 1
Advanced OK	Cancel	bu n t

8. Utente utilizzato come esempio nel documento.

Duo

1. Accedere al portale di amministrazione Dudo.

Admin Login	
Enter your admin credentials .com Log In as someone else	
Password Forgot password? Log in	
Confirm your identity	

2. Nel riquadro a sinistra, passare a Utenti, fare clic su Aggiungi utente e digitare il nome dell'utente corrispondente al nome utente di Active Domain, quindi fare clic su Aggiungi utente.

DUO	Q Search for users, groups, a	oplications, or devices
Dashboard	Dashboard > Users > Add Use	r
Device Insight	Add User	
Policies	Most applications allow users	to enroll themselves after they complete primary authentication.
Applications	Learn more about adding user	s 🖸
Single Sign-On		
Users	Username	duovpn
Add User 😽 😽		Should match the primary authentication username.
Pending Enrollments		
Bulk Enroll Users		
Import Users	(
Directory Sync		Add User

3. Nel nuovo pannello utente, compilare il campo vuoto con tutte le informazioni necessarie.

Policies	Uasnboard > Users > duovpn		
Applications	duovpn		Logs Send Enrollment Email
Single Sign-On			
Users Add User Pending Enrollments Bulk Enroll Users Import Users Directory Sync	() This user has not end Username Username aliases	olled yet. See our enrollment documentation [2] to learn more about enrolling users. duovpn	
Bypass Codes Groups Endpoints		Users can have up to 8 aliases. Optionally, you may choose to reserve using an alias number for a specific alias (e.g., Username alias 1 should only be used for Employee ID).	
2FA Devices Trusted Endpoints	Full name	test <u>ypn</u> user	
Trust Monitor Reports	Email	.com	
Settings Need Help? Chat with Tech Support C' Email Support Call us at 1-855-386-2884 Versioning Core Authentication Service: D235.6 Admin Panel: D235.6	Status	 Active Require multi-factor authentication (default). Bypass Allow users to skip two-factor authentication and log in with only a password. Passwordless Disabled Automatically deny access This controls the user's two-factor authentication process. 	authentication is not skipped.
Read Release Notes C Account ID 2910-6030-53	Groups	You don't have any editable groups. Add one. Groups can be used for management, reporting, and policy. Learn more about groups C	
DU063 대 Helpful Links Documentation 대 User Guide 대 Knowledge Base 대	Notes	For internal use.	

4. In Periferiche utente specificare il metodo di autenticazione secondaria.

Nota:in questo documento viene utilizzato il metodo Duo push per i dispositivi mobili, quindi è necessario aggiungere un dispositivo telefonico.

Fare clic su Aggiungi telefono.

hones	
	Add Phone
This user has no phones. Add one.	
ndpoints	
This user has no devices.	
ardware Tokens	Add Hardware Token
This user has no hardware tokens. Add one.	
ypass Codes	Add Bypass Code
This user has no bypass codes. Add one.	
/ebAuthn & U2F	Add Security Key

5. Digitare il numero di telefono dell'utente e fare clic su Aggiungi telefono.

Dashboard > Users > duovpn > Add Phone

Add Phone



6. Nel pannello di sinistra Duo Admin, passare a Users e fare clic sul nuovo utente.

Dashboard	Dashboard > Users						
Device Insight	lleere			Director	Suga I Import I	leare Bulk Fr	
Policies	Users			Directory	y Sync T Import C	SUS I DUKE	
Applications	i You have users w	ho have not activated Duo I	Mobile. Click here to send them a	ctivation links.			
Single Sign-On	Need to activate a	a replacement phone? Lean	n more about Reactivating Duo Me	obile 🖆			
Users 🗲							
Add User	5	0	2	1	0		0
Pending Enrollments	Total Users	Not Enrolled	Inactive Users	Trash	Bypass U	Jsers	Locked Out
Import Users							
Directory Sync	Select (0) ✓ ····				Export ~	Q Search	
Bypass Codes	llearnama .	Nama	Email	Phones	Tokons	Status	Last Logia
Groups	Osemane _	Ivanie	Linda	Filolies	IOKEIIS	Status	Last Login
Endpoints				1		Active	Mar 8, 2022 6:50 PM
2FA Devices				1		Active	Mar 5, 2022 7:04 PM
Trusted Endpoints							
Trust Monitor				1		Active	Never authenticated
Reports	duovpn		.com	1		Active	Never authenticated
Settings			.com	1		Active	Mar 5, 2022 7:16 PM
Need Help? Chat with Tech Support I							

Nota:se al momento non hai accesso al telefono, puoi selezionare l'opzione email.

7.Passare alla sezione Telefoni e fare clic su Attiva Duo Mobile.

Phones You may rearrang	e the phones by dragging and dr	opping in the table. L	earn more about activating a re	eplacement phone 🗗.	l	Add Phone
Alias	Device	Platform	Model	Security Warnings		
phone1	2 C 2 C 2 C	Android 10	$(1,1,2,\ldots,2,1)$	✓ No warnings	Activate Duo Mobile	Ê

8. Fare clic su Generate Duo Mobile Activation Code.



9. Seleziona Email per ricevere le istruzioni via email, digita il tuo indirizzo email e fai clic su Send Instructions by email (Invia istruzioni per posta elettronica).

Dashboard > • XXX TH TM6 > Activate Duo Mobile

Activate Duo Mobile

This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allow: mobile device or authenticate via Duo Push.

Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the r

Phone	a di ka Wasaka
Send links via	SMS Email
Email	ay i mian ilin ven avan

10. Si riceve un messaggio di posta elettronica contenente le istruzioni, come illustrato nell'immagine.





Don't have Duo Mobile yet? Install it first:

iPhone: https://itunes.apple.com/us/app/duo-mobile/id422663827

Android: https://play.google.com/store/apps/details?id=com.duosecurity.duomobile

11. Aprire Duo Mobile App dal dispositivo mobile e fare clic su Aggiungi, quindi selezionare Usa codice QR e digitalizzare il codice dall'e-mail di istruzioni.

12. Il nuovo utente viene aggiunto alla tua Duo Mobile App.

Duo Auth Proxy Configuration

1. Scaricare e installare Duo Auth Proxy Manager da https://duo.com/docs/authproxy-reference.

Nota:in questo documento Duo Auth Proxy Manager è installato sullo stesso Windows Server che ospita i servizi Active Directory.

2. Nel pannello Duo Admin, passare ad Applicazioni e fare clic su Proteggi un'applicazione.



3. Sulla barra di ricerca, cerca Cisco ISE Radius.

Protect an Application

0	Add an application that you'd like to protect with Duo two-factor a You can start with a small "proof-of-concept" installation — it take Documentation: Getting Started C Choose an application below to get started.	uthentication. Is just a few minutes, and	you're the only one that will see it, until you decide to add others.
isd Applica	tion	Protection Type	
Cakamal	Akamai Enterprise Application Access	2FA	Documentation E [*] Protect
altalta cisco	Cisco ISE RADIUS	2FA	Documentation D Protect

4. Copiare la chiave di integrazione, la chiave segreta e il nome host dell'API. Queste informazioni sono necessarie per la configurazione del proxy di autenticazione Duo.

Successfully added Cisco ISE RADIUS to protected applications. Add another.

Dashboard > Applications > Cisco ISE RADIUS 1

Cisco ISE RADIUS 1

Follow the Cisco ISE RADIUS instructions ⊡.

Details

~

Integration key	5.500408.5896°/202585247	Сору
Secret key	•••••W6ho	Сору
	Don't write down your secret key or share it with any	yone.
API hostname	(343 0700 700 000 000 000 700 000 7	Сору

5. Eseguire l'applicazione Duo Authentication Proxy Manager e completare la configurazione sia per il client Active Directory che per ISE Radius Server, quindi fare clic su Convalida.

Nota: se la convalida ha esito negativo, fare riferimento alla scheda debug per i dettagli e correggerla di conseguenza.

Duo Authentication Proxy Manager	- 🗆 X
Authentication Proxy is running Up since: 3/5/2022, 9:23:04	AM Version: 5.6.0 Restart Service Stop Service
Validation passed Configuration has passed validation and is ready to be saved	— —
Configure: authproxy.cfg Ur	Isaved Changes Output
<pre>18 ; number to the section name (e.g. [ad_client2]) 19 20 [ad_client] 21 host=10.28.17.107 22 service_account_username=Administrator 23 service_account_password= HEAMTLAT 24 search_dn=DC=agarciam,DC=cisco 25 26 [radius_server_auto] 27 ikey=Untplain[L[AlTHLAT 28 skey=KGP@fartBiA27"HTTp?7i6AlfSwh1VDpapeWrCdg 29 api_host=api_aft64730.clumtt.urlty.tom 30 radius_ip_1=10.28.17.101 31 radius_secret_1=Wextp111?! 32 failmode=safe 33 client=ad_client 34 port=1812 35 36</pre>	Running The Duo Authentication Proxy Connectivity Tool. This may take several minutes [info] Testing section 'main' with configuration: [info] Testing section 'main' with configuration: [info] {'debug': 'True', 'log_max_files': '10', 'log_max_size': '20971520', 'test_connectivity_on_startup': 'true'} [info] There are no configuration problems [info]
Validate Save	Learn how to configure the Authentication Proxy

Configurazioni Cisco ISE

1. Accedere al portale di amministrazione di ISE.

2. Espandere la scheda Cisco ISE e passare ad Amministrazione, quindi fare clic su Risorse di rete e selezionare Server RADIUS esterni.

	Q What page are you looking	for?		
Dashboard	Context Visibility	Operations	-Policy-	Administration
Recent Pages	System		Network Resources	
External Identity Sources Policy Sets Network Device Profiles External RADIUS Servers RADIUS Server Sequence Live Logs	Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks		Network Devices Network Device Crow Network Device Prof External RADIUS Ser PADIUS Server Sequ NAC Managers External MDM	iles vers iencs
	Backup & Restore		Location Services	

3. Nella scheda Server Radius esterni, fare clic su Aggiungi.

■ Cisco ISE		Administration · Network Resources						
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences				
External R	ADIUS Servers		1					
	🗍 Duplicate 🌐 Delete							
Name Name:	Currently Sorted	Description						

4. Compilare il campo vuoto con la configurazione RADIUS utilizzata in Duo Authentication Proxy Manager e fare clic su Invia.

Network Devices Networ	k Device Groups	Network Device	Profiles E	xternal RADIUS Servers	RADIUS Server Sequences	NAC Managers	External MDM	More
* Name	DUO_NEW ┥							
Description				ß				
* Host IP	10.28.17.107							
* Shared Secret	······· +	_	Show					
Enable KeyWrap								
* Key Encryption Key		Show						
* Message Authenticator Code Key		Show						
Key Input Format	O ASCII O HEXAI	DECIMAL						
* Authentication Port	1812	(Valid	Range 1 to 65535)				
* Accounting Port	1813	(Valid	Range 1 to 65535)				
* Server Timeout	5	Seco	nds (Valid Range 1	to 120)				
* Connection Attempts	3	(Valid	Range 1 to 9)					
Radius ProxyFailover Expiration	300	()(v	alid Range 1 to 60	0)				
							Su	

5. Passare alla scheda Sequenze server RADIUS e fare clic su Aggiungi.

		Adm	nistration • Network Resour	ces
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences
RADIUS Se	inistration > System > Backup & Restore >	S Policy Export Page		1

6. Specificare il nome della sequenza e assegnare il nuovo server esterno RADIUS, quindi fare clic su Invia.

RADIUS Server Sequences List > New RADIUS Server Sequence

RADIUS Server Sequence



✓ User Selected Service Type

Select the set of external RADIUS servers to use to process requests. Servers are accessed in sequence until a response is r



7. Passare dal menu del dashboard a Criterio e fare clic su Set di criteri.



8. Assegnate la sequenza RADIUS al criterio di default.

Nota:in questo documento viene applicata la sequenza Duo a tutte le connessioni, quindi viene utilizzato il criterio predefinito. L'assegnazione dei criteri può variare in base ai requisiti.

Policy	Sets					Reset	Reset Policyset Hi	tcount
÷	Status	Policy Set Name	Description	Con	iditions	Allowed Protocols	/ Server Sequence	Hits
Q	Search	1						
	ø	81 D 1 N		Ŧ	Radius-User-Name EQUALS isevpn	Default Network A	access $\boxtimes -+$	3
	ø	18. X		Ø	Radius-NAS-Port-Type EQUALS Virtual	DUO_Sequence	$\boxtimes \sim +$	22
	ø	Default	Default policy set			Default Network A	access 🖾 🔨 +	0
		Ĩ				EQ		
		I				Allowed Protocols		eset
						Default Netwo Proxy Sequence	ork Access	
						DUO_NEW		
						DUO Sequen	ce	

Configurazione Cisco ASA RADIUS/ISE

1. Configurare il server ISE RADIUS in gruppi di server AAA, passare a Configurazione, quindi fare clic su Gestione dispositivi ed espandere la sezione Utenti/AAA, quindi selezionare Gruppi di server AAA.

o t avi	Home Configuration Monitoring Save Device Lip Beokmarks Bookmarks bookmark a page, right-click on a node in the agation tree and select "Add to bookmarks". Go The Delete	Refresh Ba	ack () ation : ips Pro RA LO
0	O O Device Management		
>	Management Access		
>	8 Licensing		
>	System Image/Configuration		
>	High Availability and Scalability		
>		Find:	
	Smart Call-Home		
	Security	Servers in the Se	elected
	Service Module Settings	Server Name or IP	Addres
0		10 28 17 101	Addre:
	19 AAA Server Groups	10.20.17.101	
	Se I DAP Attribute Map		
	AAA Kerberos		
	Authentication Prompt		
	🗣 AAA Access		
	Dvnamic Access Policies		
	User Accounts		
	A Password Policy		
	G Change My Password		
	Login History		
5	Certificate Management		
>	P DHCP		
	B DNS		
Σ	UND TO THE REAL PROPERTY OF TH		

, selezionare il nome dell'interfaccia, specificare l'indirizzo IP del server ISE e digitare la chiave segreta RADIUS, quindi fare clic su Ok.

Nota: tutte queste informazioni devono corrispondere a quelle specificate in Duo Authentication Proxy Manager.

• •	Edit AAA Server
Server Group:	SE
Interface Name:	outside 🔫 ——
Server Name or IP Address:	10.28.17.101
Timeout:	10 seconds
RADIUS Parameters	
Server Authentication Port:	1645
Server Accounting Port:	1646
Retry Interval:	10 seconds 📀
Server Secret Key:	•••••
Common Password:	
ACL Netmask Convert:	Standard 😂
Microsoft CHAPv2 Capable	: 🔽
SDI Messages	
Message Table	×
Help	Cancel OK

Configurazione CLI.

```
aaa-server ISE protocol radius
dynamic-authorization
aaa-server ISE (outside) host 10.28.17.101
key *****
```

Configurazione VPN di accesso remoto Cisco ASA

ip local pool agarciam-pool 192.168.17.1-192.168.17.100 mask 255.255.255.0 group-policy DUO internal group-policy DUO attributes banner value This connection is for DUO authorized users only! vpn-tunnel-protocol ikev2 ssl-client split-tunnel-policy tunnelspecified split-tunnel-network-list value split-agarciam address-pools value agarciam-pool tunnel-group ISE-users type remote-access tunnel-group ISE-users general-attributes address-pool agarciam-pool authentication-server-group ISE default-group-policy DUO tunnel-group ISE-users webvpn-attributes group-alias ISE enable dns-group DNS-CISCO

Test

1. Apri l'app Anyconnect sul tuo dispositivo PC. Specificare il nome host dell'headend VPN ASA e accedere con l'utente creato per l'autenticazione secondaria Duo, quindi fare clic su OK.

000	Sec	AnyConnect ure Mobility Client	cisco	
	VPN: Please enter yo	ur username and passw	vord.	
	Cisco A	nyConnect 192.16	8.100.100	
	Please enter your	username and passw	vord.	
_	Group:		-	0
	msgstringESMEX	duovpn		
	MEX-PASS	••••		
			Cancel)

- 2. È stata ricevuta una notifica di push Duo sul dispositivo mobile Duo dell'utente specificato.
- 3. Aprire la notifica di Duo Mobile App e fare clic su Approva.





4. Accettare il banner e stabilire la connessione.





Risoluzione dei problemi

In questa sezione vengono fornite informazioni utili per risolvere i problemi di configurazione.

Duo Authentication Proxy viene fornito con uno strumento di debug che visualizza i motivi dell'errore.

Debug del lavoro



Nota:le informazioni successive sono memorizzate in C:\Program Files\Duo Proxy di autenticazione di sicurezza\log\connectivity_tool.log.

Output

Running	The Duo Authentication Proxy Connectivity Tool. This may take
	several minutes
[info]	Testing section 'main' with configuration:
[info]	{'debug': 'True',
	'log_max_files': '10',
	'log_max_size': '20971520',
	<pre>'test_connectivity_on_startup': 'true'}</pre>
[info]	There are no configuration problems
[info]	
[info]	Testing section 'ad_client' with configuration:
[info]	{'debug': 'True',
	'host': '10.28.17.107',
	'search_dn': 'DC=agarciam,DC=cisco',
	'service_account_password': '*****',
	'service_account_username': 'Administrator'}

```
[info]
        Testing section 'radius_server_auto' with configuration:
[info]
        {'api_host': 'apl affect?'Laboratelly.com',
[info]
         'client': 'ad_client',
         'debug': 'True',
         'failmode': 'safe',
         'ikey': Lange Lot Manager ...
         'port': '1812',
         'radius_ip_1': '10.28.17.101',
         'radius_secret_1': '******',
         'skey': '********[40]'}
        There are no configuration problems
[info]
[info] Testing section 'main' with configuration:
[info] {'debug': 'True',
         'log_max_files': '10',
         'log_max_size': '20971520',
         'test_connectivity_on_startup': 'true'}
[info] There are no connectivity problems with the section.
```

```
[info] There are no connectivity problems with the section.
[info]
[info] Testing section 'ad_client' with configuration:
[info] {'debug': 'True',
         'host': '10.28.17.107',
         'search_dn': 'DC=agarciam,DC=cisco',
         'service_account_password': '******',
         'service_account_username': 'Administrator'}
       The LDAP Client section has no connectivity issues.
[info]
[info]
[info] Testing section 'radius_server_auto' with configuration:
[info] {'api_host': 'asi_adice.ci.ducaccurite.cmp',
         'client': 'ad_client',
         'debug': 'True',
         'failmode': 'safe',
         'ikey': ""There's Northern Sciences
         'port': '1812',
         'radius_ip_1': '10.28.17.101',
         'radius_secret_1': '******',
         'skey': '****** [40]'}
       The RADIUS Server has no connectivity problems.
[info]
[info]
[info] SUMMARY
[info] No issues detected
```

1. Problemi di connettività, IP errato, FQDN/nome host non risolvibile nella configurazione di Active Directory.

Output

'host': '10.28.17.106', 'search_dn': 'DC=agarciam,DC=cisco', 'service_account_password': '*****', 'service_account_username': 'Administrator'} [warn] The LDAP Client section has connectivity problems. [warn] The LDAP host clear connection to 10.28.17.106:389 has connectivity problems. [error] The Auth Proxy was not able to establish a connection to 10 .28.17.106:389.

2. Password errata per l'utente Administrator in Active Directory.



Debug

[info]	The Auth Proxy was able to establish a connection to 10.28.17
	.107:389.
[info]	The Auth Proxy was able to establish an LDAP connection to 10
	.28.17.107:389.
[error]	The Auth Proxy was unable to bind as Administrator.
[error]	Please ensure that the provided service account credentials
	are correct.
[debug]	Exception: invalidCredentials: 8009030C: LdapErr: DSID
	-0C090516, comment: AcceptSecurityContext error, data 52e,
	v3839 <mark>-</mark>
[warn]	The Auth Proxy did not run the search check because of the
	problem(s) with the bind check. Resolve that issue and rerun
	the tester.

3. Dominio di base errato.



Debug



4. Valore RADIUS chiave errato.

[radius_server_auto]
ikey=U_NUL_LUGAL_KHRNZ6EZ1
skey=Jackinski i trudi. 17 mil 1911 - History Salimari da mika 👥
api_host=apl = 🗖 📲 🖬 🖬 🖛 🖜 ity.com
radius_ip_1=10.28.17.101
<pre>radius_secret_1=!Mexvpn!17!</pre>
failmode=safe
<pre>client=ad_client</pre>
port=1812

Debug

	and a second tell
[error]	The ikey value provided is invalid.
[info]	
[info]	SUMMARY
[warn]	Checks for external connectivity were not run. Please fix the
	configuration and try again.

5. Verificare che il server ISE invii pacchetti di richiesta di accesso.

*Ethernet0

File	e Edit	View	Go	Capture	Analyze	Statistics	Telephony	Wireles	is Tools	Help		
£.	•				۹ 👄 🕫	9 🗟 🧕	£ 🗐 🔳	ର୍ ପ୍	۹ 👳			
	radius				1							
No.		Time		Source			Destination		Protoco	l Length	Terfo	
	1511.	6020.5	21457	10.28	3.17.101		10.28.17.1	07	RADIU	IS 877	Access-Request	t 刘 = 31
<u>مل</u>	1513.	6024.3	44735	10.28	3.17.107		10.28.17.1	01	RADIU	IS 191	Access Accept	id=31
>	Frame	151115	: 877	bytes o	n wire (7016 bits	;), 877 by	tes capt	tured (70	16 bits)	on interface \	Device\NPF_{CA092CEE-5
>	Ether	net II,	Snc:	Where_	b3:a4:2f	(00:50:5	6:b3:a4:21	f), Dst:	Whare_	b3:b4:3e	(00:50:56:b3:b	04:3e)
>	Inter	net Pro	tocol	Version	4, Snc:	10.28.17	7.101, Dst:	10.28	17.107			
>	User	Datagra	m Prof	tocol, S	inc Pont:	42022, 0	Ost Port: 1	1812				
~	RADIU	S Proto	col									
	Co	de: Acc	ess-Re	equest (1)							
	Pa	cket id	entifi	ier: 0x1	f (31)							
	Le	ngth: 8	35									
	Au	thentic	ator:	38a28ca	3ca6bbc26	51819c530	4b1be6e3					
	[T	ne nesp	onse t	to this	request :	is in fra	me 151332	1				
	Y At	tribute	Value	e Pairs			-					
	~	AVP: to	-User-	Name(1)	1=8 val=	duovpn	-					
	2	AVP: to	-User-	Passwor	d(2) 1=18	3 val=Enc	rypted					
	2	AVP: to	NAS-1	P-Addre	ss(4) 1=0	5 val=192	.168.100.1	.00				
	2	AVP: to	NAS-P	Port(5)	1=6 val=3	44064						
	2	AVP: to	Calle	d-Stati	on-1d(30)	1=17 va	1=192.168.	100.100	,			
		AVP: to	-Calli	ing-Stat	100-10(3)	() 1=13 V	a1 N		121202-2		20.010001	
	2	AVP: U	-Proxy	-State(33) 1=25	va1=4069	72/3/450/2	01/8/93	05150205	23826313	/20313031	C262220242121666222462
		AVP: C	-Proxy	-state(22) 1=/6 2(61) 1-6	val=4369	/ 303012053	0303/5/	20520414	55557566	333323733612039	03023020313103032003
		AVP: U	-1943-P	1-Clice	e(OI) I=c	+(66) 1-	13 val-10	00 65 5	3			
		AVP: U	- runne	i -ciien	c-enopoir	r(00) 1=	15 Val=10.	55.05.5	5			

6. Per verificare il corretto funzionamento del server proxy di autenticazione Duo, Duo fornisce lo strumento <u>NTRadPing</u> per simulare i pacchetti di richiesta di accesso e la risposta con Duo.

6.1 Installare NTRadPing su un PC diverso e generare traffico.

Nota:nell'esempio viene utilizzato il computer Windows 10.28.17.3.

6.2 Eseguire la configurazione con gli attributi utilizzati nella configurazione ISE Radius.

INTRadPing Test Utility	– 🗆 X				
RADIUS Server/port 10.28.17.107	NTRadPing 1.5 - RADIUS Server Testing Tool © 1999-2003 Master Soft SpA - Italy - All rights reserved				
Reply timeout (sec.): 3 Retries: 6	http://www.dialways.com/				
RADIUS Secret key: Harmy F i	mrc \				
User-Name: duovpn					
Password: CHAP	MASTERSOFT DIALWAYS				
Request type: Authentication Request 💌 0	RADIUS Server reply:				
Additional RADIUS Attributes:	See Super-Stational and the second 22 2012 1022 Instantian a served work of the second 12 2012 1022 In a second second to the school area should (1) the second second second second (1) and we can even the school of 7000 - Bandward www.caref.color(second school) algorization to device of the school algorization to device of the				
Add Remove Clear list Load Save	Send Help Close				

6.3 Configurare Duo Authentication Proxy Manager come segue.

[radius_server_auto]
ikey="There's there's set as a set of the se
skey=Jac3
api_host=ani=nd7c172n.dumnerinity.com
radius_ip_1=10.28.17.101
<pre>radius_secret_1=!Mexnum *17!</pre>
radius_ip_2=10.28.17.3
radius_secret_2=!Mex 7!

6.4. Passare allo strumento NTRadPing e fare clic su Invia. Si riceve una notifica push Duo sul dispositivo mobile assegnato.

INTRadPing Test	Utility		- 🗆 X
RADIUS Server/port:	10.28.17.107	1812	NTRadPing 1.5 - RADIUS Server Testing Tool © 1999-2003 Master Soft SpA - Italy - All rights reserved
Reply timeout (sec.):	3 Ret	ries: 6	http://www.dialways.com/
RADIUS Secret key:	!Mexvpn!17!		ms
User-Name:	duovpn		
Password:	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	CHAP	MASTERSOFT DIALWAYS
Request type:	Authentication Request 💌	0	RADIUS Server reply:
Additional RADIUS A	ttributes:	_	Sending authentication request to server 10.28.17.107:1812 Transmitting packet, code=1 id=12 length=46 no response from server (uned out), non-offerent (#1) received response from the server in 4000 milliseconds reply packet code=2 id=12 length=49 response: Access:Accept attribute dump Reply-Message=Success. Logging you in
Add Remove	e Clear list Load	Save	Send Help Close

	700 20.866684	10.28.17.3	10.28.17.107	RADIUS	88 Access-Request id=13,	, Duplicate Request	
ąL	737 22.184895	10.28.17.107	10.28.17.3	RADIUS	90 Access-Accept id=13	←	
>	Frame 700: 88 byte	s on wire (704 bit:	s), 88 bytes captured	(704 bits) on	interface \Device\NPF {CA	092CEE-5528-4E0A-9310-2D523160DD60	}, id 0
>	Ethernet II, Src:	VMware_b3:f2:72 (00	0:50:56:b3:f2:72), Dst	: VMware_b3:b	4:3e (00:50:56:b3:b4:3e)		
>	Internet Protocol	Version 4, Src: 10	.28.17.3, Dst: 10.28.1	7.107			
>	User Datagram Prot	cocol, Src Port: 51	188, Dst Port: 1812				
~	RADIUS Protocol						
	Code: Access-Re	quest (1)					
	Packet identifi	er: 0xd (13)					
	Length: 46						
	Authenticator:	2020202020203136343	36393335333230				
	[Duplicate Requ	est Frame Number: 5	532]				
	[The response t	to this request is i	in frame 737]				
	✓ Attribute Value	Pairs					
	> AVP: t=User-	Name(1) l=8 val=duc	ovpn				
	> AVP: t=User-	Password(2) l=18 va	al=Encrypted				
1							

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).