# Configuración de la integración Duo con Active Directory e ISE para la autenticación de dos factores en clientes VPN de acceso remoto/Anyconnect

# Contenido

Introducción **Prerequisites Requirements Componentes Utilizados** Antecedentes Diagrama y escenario de la red Proceso de comunicación **Configuraciones de Active Directory Configuraciones Duo** Configuración de proxy de autenticación Duo Configuraciones de Cisco ISE Configuración RADIUS/ISE de Cisco ASA Configuración de VPN de acceso remoto de Cisco ASA Prueba Troubleshoot Depuraciones de trabajo

# Introducción

Este documento describe la integración de inserción Duo con AD e ISE como la autenticación de dos factores para los clientes de AnyConnect conectados a ASA.

# Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de VPN de RA en ASA
- Configuración RADIUS en ASA
- ISE
- Directorio activo
- Aplicaciones Duo

### **Componentes Utilizados**

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Microsoft 2016 Server
- ASA 9.14(3)18

- Servidor ISE 3.0
- Servidor Duo
- Administrador de proxy de autenticación Duo

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

#### Antecedentes

Este documento describe cómo configurar la integración de inserción Duo con Active Directory (AD) y Cisco Identity Service Engine (ISE) como autenticación de dos factores para los clientes de AnyConnect que se conectan a Cisco Adaptive Security Appliance (ASA).

#### Diagrama y escenario de la red



### Proceso de comunicación

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

- 1. Autenticación principal iniciada a Cisco ISE
- 2. Cisco ISE envía una solicitud de autenticación al proxy de autenticación dúo
- 3. La autenticación principal utiliza Active Directory o RADIUS
- 4. Conexión del proxy de autenticación dúo establecida para seguridad dúo a través del puerto TCP 443

- 5. Autenticación secundaria a través del servicio Duo Security
- 6. El proxy de autenticación dúo recibe respuesta de autenticación
- 7. Acceso a Cisco ISE concedido

Cuentas de usuario:

- Administrador de Active Directory: se utiliza como cuenta de directorio para permitir que el proxy de autenticación Duo se enlace al servidor de Active Directory para la autenticación principal.
- usuario de prueba de Active Directory
- Usuario de prueba Duo para autenticación secundaria

#### **Configuraciones de Active Directory**

El servidor de Windows está preconfigurado con los servicios de dominio de Active Directory.

**Nota**: Si RADIUS Duo Auth Proxy Manager se ejecuta en el mismo equipo host de Active Directory, los roles del servidor de directivas de redes (NPS) deben desinstalarse/eliminarse; si se ejecutan ambos servicios RADIUS, pueden entrar en conflicto y afectar al rendimiento.

Para lograr la configuración de AD para la autenticación y la identidad de usuario en usuarios de VPN de acceso remoto, se requieren algunos valores.

Todos estos detalles deben crearse o recopilarse en Microsoft Server antes de poder realizar la configuración en el servidor proxy ASA y Duo Auth.

Los valores principales son:

- Nombre de dominio. Este es el nombre de dominio del servidor. En esta guía de configuración, agarciam.cisco es el nombre de dominio.
- Dirección IP/FQDN del servidor. La dirección IP o FQDN utilizado para alcanzar el servidor de Microsoft. Si se utiliza un FQDN, se debe configurar un servidor DNS dentro de ASA y el proxy de Duo Auth para resolver el FQDN.

En esta guía de configuración, este valor es agarciam.cisco (que se resuelve en 10.28.17.107).

- Puerto del servidor. El puerto utilizado por el servicio LDAP. De forma predeterminada, LDAP y STARTTLS utilizan el puerto TCP 389 para LDAP, y LDAP sobre SSL (LDAP) utiliza el puerto TCP 636.
- CA raíz. Si se utiliza LDAPS o STARTTLS, se requiere la CA raíz utilizada para firmar el certificado SSL utilizado por LDAPS.
- Nombre de usuario y contraseña del directorio. Esta es la cuenta utilizada por el servidor proxy Duo Auth para enlazar al servidor LDAP y autenticar usuarios y buscar usuarios y grupos.
- Nombre distinguido (DN) de base y grupo. El DN base es el punto de partida para el proxy de Duo Auth e indica al directorio activo que comience la búsqueda y autentique a los usuarios.

En esta guía de configuración, el dominio raíz agarciam.cisco se utiliza como DN base y el DN de grupo es Duo-USERS.

1. Para agregar un nuevo usuario Duo, en Windows Server, navegue hasta el icono **Windows** en la parte inferior izquierda y haga clic en **Windows Administrative tools**, como se muestra en la imagen.



2. En la ventana Herramientas administrativas de Windows, navegue hasta **Usuarios y equipos de Active Directory**.

En el panel Usuarios y equipos de Active Directory, expanda la opción de dominio y desplácese a la carpeta **Usuarios**.

En este ejemplo de configuración, Duo-USERS se utiliza como el grupo de destino para la autenticación secundaria.

-> - 🛧 🏭 > Control	Panel > System and Security > Administrat	tive Tools			Active Directory Users and Comp	puters		
	Panel > System and Security > Administrat ame Active Directory Administrative Center Active Directory Domains and Trusts Active Directory Domains and Trusts Active Directory Domains and Trusts Active Directory Sites and Services Active Directory Users and Computers Active Directory Users and Computers Active Directory Users and Computers ADSI Edit Component Services Component Services Computer Management Connection Manager Administration Kit Deframment and Octimize Drives	tive Tools  Date modified  7/16/2016 6:23 AM 7/16/2016 6:19 AM 7/16/2016 6:18 AM 7/16/2016 6:18 AM 7/16/2016 6:18 AM	Type File folder Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut	Size 2 K8 2 K8 2 K8 2 K8 2 K8 2 K8 2 K8 2 K8	Active Directory Users and Comp File Action View Help Active Directory Users and Com Saved Queries Builtin Computers S Domain Controllers S Domain Controllers ForeignSecurityPrincipal Outputs Users	Image: Second	Type User User User User Security Group Security Group Security Group Security Group Security Group	Members in Members of A user acco Members of DNS Admini DNS clients
Downloads     Downloads on Mac     Downloads on Mac     Music     Pictures     Videos     Local Disk (C:)     DVD Drive (D:) SSS.;     Network		7/16/2016 6:19 AM 7/16/2016 6:19 AM 7/16/2016 6:18 AM 7/16/2016 6:18 AM 7/16/2016 6:19 AM 7/16/2016 6:19 AM 7/16/2016 6:19 AM 7/16/2016 6:19 AM	Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut	2 KB 2 KB 2 KB 2 KB 2 KB 2 KB 2 KB 2 KB	۲ ا	Domain Ad     Domain Co     Domain Co     Domain Gue     Domain Users     Duo-usEES     duo2     Enterprise A     Enterprise A     Enterprise A     Enterprise A	Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group	Designated All workstat All domain All domain All domain Designated Members of Members of

3. Haga clic con el botón derecho del ratón en la carpeta **Users** y seleccione **New** > **User**, como se muestra en la imagen.

Active Directory Users	and Computers		-	×
File Action View He	lelp ]   🗙 🗊 🙆 📑   🚺	🖬 🗏 📚 🛍 🍸 🧕 🗞		
Active Directory Users a Saved Queries Saved Queries Saved Queries Builtin Builtin Computers Sal Domain Control GreignSecurity Managed Servic Users Dele Find	and Com Name Administr agarciam alanad alanduo Principal: Control d	Type     Description       stor     User       User     Built-in account for ad       User     User       User     Members in this group c       ch     Security Group       b     Security Group       D     Security Group       Members of this group c       b     Security Group       D     Security Group       Members of this group t       co     User       A user account manage       D     Security Group		^
New All T View Refr Expo Prop Helş	v > Tasks > v > resh ort List perties p	Computer Contact Group InetOrgPerson msDS-KeyCredential msDS-ResourcePropertyList msDS-ShadowPrincipalContainer msImaging-PSPs MSMQ Queue Alias		
< Create a new object	> M Enterprise	Printer .		v
		Shared Folder		

4. En la ventana Nuevo Usuario de Objeto, especifique los atributos de identidad para este nuevo usuario y haga clic en **Siguiente**, como se muestra en la imagen.

New Object - User		×
Create in:	agarciam.cisco/Users	c
First name:	duovpn	3
Last name:		
Full name:	duovpn	s
		S
User logon name:		S
duovprij	@agarciam.cisco V	ľ
User logon name (pre	-Windows 2000):	s
AGARCIAM	duovpn	
		l l
	Rack Next Car	cel 3
	Contract > Can	ai ai

5. Confirme la contraseña y haga clic en **Next**, luego en **Finish** cuando se verifique la información del usuario.

lew Object - User		×
🧏 Create in: ag	garciam.cisco/Users	0
Password: Confirm password:	•••••••••••	эс
User must change pas	sword at next logon	s
User cannot change p	assword	s
Password never expire	s	a c
Account is disabled		s
		n
		nt
	$\frown$	e
		- st
	< Back Next > Cancel	_ [

6. Asigne el nuevo usuario a un grupo específico, haga clic con el botón derecho en él y seleccione **Agregar** a un grupo, como se muestra en la imagen.

Active Directory Users and Comp	puters			-		×
File Action View Help						
(= =) 🖄 📰 🔏 🗊 🗙 🛙	i 🖬 📑 🚺 🖬	1 🙁 🐮 🕅	1 🔟 😹			
Active Directory Users and Com Saved Queries Saved Queries Builtin Computers Domain Controllers Signature ForeignSecurityPrincipal: Managed Service Accour Users	Name Administrator agarciam alanad alanad alanduo Allowed RO Cert Publish Cloneable D DefaultAcco DefaultAcco Denied ROD DnsAdmins DnsUpdateP Domain Ad Domain Co Domain Co Domain Gue Domain Gue Domain Gue Domain Gue Domain Users duo2 DUO-USERS duovpn Enterprise	Type User User User Security Group Security Group	Description Built-in account for ad Members in this group c Members of this group Members of this group t A user account manage Members in this group c DNS Administrators Gro DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain users			
< >	A Enterprise	Add to a group	of this group		1	~
Allows you to add the selected objects to a group yo		Disable Account				

7. En el panel Seleccionar grupos, escriba el nombre del grupo deseado y haga clic en **Comprobar nombres**.

A continuación, seleccione el nombre que coincida con los criterios y haga clic en Aceptar.

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

8. Este es el usuario que se utiliza en este documento como ejemplo.

# **Configuraciones Duo**

1. Inicie sesión en el portal de administración de Dudo.

Admin Login	
Enter your admin credentials	
Password Forgot password? Log in	
Confirm your identity	

2.En el panel lateral izquierdo, navegue hasta **Usuarios**, haga clic en **Agregar usuario** y escriba el nombre del usuario que coincida con su nombre de usuario de dominio activo, luego haga clic en **Agregar usuario**.



3. En el nuevo panel de usuario, rellene el espacio en blanco con toda la información necesaria.

#### Policies

Applications

Single Sign-On

#### Users

Add User

Pending Enrollments

Bulk Enroll Users

Import Users

Directory Sync

Bypass Codes

Groups

Endpoints

2FA Devices

**Trusted Endpoints** 

Trust Monitor

Reports

Settings

Need Help? <u>Chat with Tech Support</u> <u>Email Support</u> Call us at 1-855-386-2884 Versioning Core Authentication Service: D235.6

Admin Panel:

D235.6

Read Release Notes

Account ID 2910-6030-53

Deployment ID DUO63 대

Helpful Links

User Guide F<sup>2</sup>

Dasnboard > Users > duovpn

# duovpn

-

This user has not enrolled yet. See our enrollment documentation I to learn

Username	duovpn
Username aliases	+ Add a username alias Users can have up to 8 aliases. Optionally, you may choose to reserve using an alias number fo (e.g., Username alias 1 should only be used for Employee ID).
Full name	test <u>vpn</u> user
Email	.com
Status	<ul> <li>Active Require multi-factor authentication (default).</li> <li>Bypass Allow users to skip two-factor authentication and log in w</li> <li>Disabled Automatically deny access</li> <li>This controls the user's two-factor authentication process.</li> </ul>
Groups	You don't have any editable groups. Add one. Groups can be used for management, reporting, and policy. Le
Notes	

: En este documento se utiliza el método Duo push para dispositivos móviles, por lo que es necesario agregar un dispositivo telefónico.

Haga clic en Agregar teléfono.

Phones You may rearrange the phones by dragging and dro	pping in the table. Learn more about activating a replacement phone 🗅.	(
	This user has no phones. Add one.	
Endpoints		
	This user has no devices.	
Hardware Tokens		Add
	This user has no hardware tokens. Add one.	
Bypass Codes		Ad
	This user has no bypass codes. Add one.	
WebAuthn & U2F		

5. Escriba el número de teléfono del usuario y haga clic en Agregar teléfono.

Dashboard > Users > duovpn > Add Phone

# Add Phone

i Learn more a	about Activating Duo Mobile ピ.
Туре	<ul> <li>Phone</li> <li>Tablet</li> </ul>
Phone number	Optional. Example: "+52 1 222 123 4567"
	Add Phone

6. En el panel izquierdo Duo Admin, navegue hasta Users y haga clic en el nuevo usuario.

Dashboard	Dashboard > Users				
Device Insight	Llooro			Director	Suna Lim
Policies	Users			Director	y Sync T Im
Applications	You have users w	ho have not activated Duo M	Nobile. Click here to send them ac	ctivation links.	
Single Sign-On	Need to activate a	a replacement phone? Learr	more about Reactivating Duo Mo	obile 🖆.	
Users ┥					
Add User	5	0	2	1	0
Pending Enrollments	Total Users	Not Enrolled	Inactive Users	Trash	By
Bulk Enroll Users		_			
Import Users	Select (0) ∽ ····				Export ~
Directory Sync					
Bypass Codes	Username 🔺	Name	Email	Phones	Tokens
Groups					
Endpoints				1	
2FA Devices	-			1	
Trusted Endpoints					
Trust Monitor				1	
Reports	duovpn		.com	1	
Settings			e e e.com	1	
Need Help? Chat with Tech Support D					

Nota: En caso de que no tenga acceso a su teléfono en este momento, puede seleccionar la opción de correo electrónico.

7. Navegue hasta la sección Teléfonos y haga clic en Activar Duo Mobile.

Phones You may rearrang	ge the phones by dragging a	nd dropping in the table. I	Learn more about activating	a replacement phone 🗗.	
Alias	Device	Platform	Model	Security Warnings	
phone1	1000	Android 10	$0.015\times 10^{-10}$	🗸 No warnings	Activate Duo Mobile

8. Haga clic en Generar Duo Mobile Activation Code.



9. Seleccione **Correo electrónico** para recibir las instrucciones por correo electrónico, escriba su dirección de correo electrónico y haga clic en **Enviar instrucciones por correo electrónico**.

## 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	1. 1 In . 19 (18 - 198).
Send links via	SMS Email
Email	aya mina ilin sen asan

10. Recibe un correo electrónico con las instrucciones, como se muestra en la imagen.

#### This is an automated email from Duo Security.

Your organization invites you to set up Duo Mobile on your phone. You will find instructions from your Duo administrator below. If you have questions, please reach out to your organization's IT or help desk team.

This email will help you add your Cisco account to Duo Mobile on this device:



Just tap this link from + r copy and paste it into Duo Mobile manually:



If you're not reading this from +



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. Abra la aplicación Duo Mobile desde su dispositivo móvil y haga clic en **Agregar**, luego seleccione **Usar código QR** y escanee el código desde el correo electrónico de instrucciones.

12. Se agrega un nuevo usuario a la aplicación Duo Mobile.

### Configuración de proxy de autenticación Duo

1.Descargue e instale Duo Auth Proxy Manager desde https://duo.com/docs/authproxy-reference.

**Nota**: En este documento, Duo Auth Proxy Manager está instalado en el mismo servidor de Windows que aloja los servicios de Active Directory.

2.En el panel Duo Admin, navegue hasta Applications y haga clic en Protect an Application.



3. En la barra de búsqueda, busque Cisco ISE Radius.

### **Protect an Application**

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

4. Copie la clave de integración, la clave secreta y el nombre de host de la API. Necesita esta información para la configuración de Duo Authentication Proxy.



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	5.00040a.0001717552047	Сору
Secret key	•••••W6ho	Сору
	Don't write down your secret key or share it with anyone.	
API hostname	(043.0000 /001000000 /100200 /	Сору

5. Ejecute la aplicación Duo Authentication Proxy Manager y complete la configuración para el cliente de Active Directory y el servidor ISE Radius y haga clic en **Validar**.

**Nota**: Si la validación no se realiza correctamente, consulte la ficha debug para obtener detalles y corrija en consecuencia.

Duo Authentication Proxy Manager			
Authentication Proxy is running	<b>Up since:</b> 3/5/2022, 9:23:04 AM	Version: 5.6. Update your Auther	0 Rest
Validation passed     Configuration has passed validation an	id is ready to be saved 🛛 🗲		
Configure: authproxy.cfg	Unsav	ed Changes Output	:
<pre>18 ; number to the section name (e. 19 20 [ad_client] 21 host=10.28.17.107 22 service_account_username=Adminis 23 service_account_password= H_AAT 24 search_dn=DC=agarciam,DC=cisco 25 26 [radius_server_auto] 27 ikey=Untrial to the transmiss 28 skey=K9ee7rd*ifeT14H17e77i6A466ad 29 api_host=api_siteT14H17e77i6A466ad 29 api_host=api_siteT14H17e77i6A466ad 29 api_host=api_siteT14H17e77i6A466ad 29 api_host=api_siteT14H17e77i6A466ad 20 radius_ip_1=10.28.17.101 31 radius_secret_1=Untrial17! 32 failmode=safe 33 client=ad_client 34 port=1812 35 36</pre>	.g. [ad_client2]) strator hulfi hlV3papedVC2dg ty:εtm	Running [info] [info] [info] [info] [info] [info] [info] [info] [info] [info]	The Duo Authentication Proxy Connections everal minutes Testing section 'main' with configurate {'debug': 'True', 'log_max_files': '10', 'log_max_size': '20971520', 'test_connectivity_on_startup': 'true There are no configuration problems 
Validate			Learn how to c

## **Configuraciones de Cisco ISE**

1. Inicie sesión en el portal ISE Admin.

2.Expanda la pestaña Cisco ISE y navegue hasta **Administration**, luego haga clic en **Network Resources** y haga clic en **External RADIUS Servers**.

×	Cisco ISE 🔫	Q What page are you looking f	or?		
	Dashboard	Context Visibility	Operations	-Policy	Administration
	Recent Pages External Identity Sources Policy Sets Network Device Profiles External RADIUS Servers RADIUS Server Sequences Live Logs	System Deployment Licensing Certificates Logging Maintenance Upgrade Haalth Checke		Network Resources Network Devices Network Device Crow Network Device Prof External RADIUS Ser RADIUS Server Sequ NAC Managers	iles vers lencos
		Backup & Restore		Location Services	

3. En la pestaña External Radius Servers, haga clic en Add.

■ Cisco ISE		Admi	inistration • Network Resource	ces
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences
External R	ADIUS Servers		1	
C Edit + Add	🗋 Duplicate 🍵 Delete			
Name Name	Currently Sorted	Description		

4. Rellene el espacio en blanco con la configuración RADIUS utilizada en el Administrador de Proxy de Autenticación Duo y haga clic en **Enviar**.

Network Devices Network	k Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequ
* Name Description	DUO_NEW			
* Wast ID	10 28 17 107		R	
nostie	10.28.17.107			
* Shared Secret	······· <b>-</b>	Show		
Enable KeyWrap				
* Key Encryption Key		Show		
* Message Authenticator Code Key		Show		
Key Input Format		CIMAL		
* Authentication Port	1812	(Valid Range 1 to 65	535)	
* Accounting Port	1813	(Valid Range 1 to 65	535)	
* Server Timeout	5	Seconds (Valid Rang	ge 1 to 120)	
* Connection Attempts	3	(Valid Range 1 to 9)		
Radius ProxyFailover Expiration	300	(valid Range 1 to	600)	

#### 5. Acceda a la pestaña Secuencias de Servidor RADIUS y haga clic en Agregar.



6. Especifique el nombre de la secuencia y asigne el nuevo servidor externo RADIUS. Haga clic en Enviar.

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. En el menú Panel, acceda a **Política** y haga clic en **Juegos de Políticas**.



8. Asigne la secuencia RADIUS a la política por defecto.

**Nota**: En este documento, se aplica la secuencia Duo a todas las conexiones, por lo que se utiliza la política predeterminada. La asignación de políticas puede variar según los requisitos.

#### Policy Sets

Searcl	'n			
0	81.91W		Ŧ	Radius-User-Name EQUALS isevpn
0	1 m 1		Ø	Radius-NAS-Port-Type EQUALS Virtual
0	Default	Default policy set		
	1			

# Configuración RADIUS/ISE de Cisco ASA

1. Configure el servidor RADIUS de ISE en Grupos de servidores AAA, navegue hasta **Configuración**, haga clic en **Administración de dispositivos** y expanda la sección **Usuarios/AAA**, seleccione **Grupos de servidores AAA**.

Bookmarks bookmark a page, right-click on a node in the viagation tree and select "Add to bookmarks"	AAA Server Groups Server Group Pr
Co Delete	ISE R.
So Delete	LOCAL
O O Device Management	
Management Access	
86 Licensing	
System Image/Configuration	
In the second se	Find:
	- mu.
Smart Call-Home	
24 Cloud Web Security	Servers in the Selecte
Service Module Settings	Server Name or IP Addre
Contraction of the second seco	10.28.17.101
Ava Server Groups	
20 LDAP Attribute Map	
AAA Kerberos	
Paramic Access	
B Password Policy	
Change My Bassword	
Certificate Management	
2 DNS	
DECT ADLAgent	
Device Setup	
Firewall	
Remote Access VPN	Find:
	FING.

2. En el panel AAA Server Groups, haga clic en Add.

AAA Server Groups							
Server Group	Protocol	Accounting Mo	de Reactivation Mod	le Dead Ti	me Max I	ailed Attempts	Add
lige and	1		<b>.</b>		•		Edit
Find:			Natch Case				
Find:	ed Group		Aatch Case				
Find: Servers in the Selecto Server Name or IP Addr	ed Group ress Interfac	ce Timeout	Aatch Case				Add
Find: Servers in the Selecto Server Name or IP Addr	ed Group ress Interfa	ce Timeout	Match Case				Add
Find: Servers in the Selecto Server Name or IP Addr	ed Group ress Interfa	ce Timeout	Aatch Case				Add Edit Delete
Find: Servers in the Selecto Server Name or IP Addr	ed Group ress Interfac	ce Timeout	Aatch Case				Add Edit Delete Move Up
Find: Servers in the Selector Server Name or IP Addr	ed Group ress Interfa	ce Timeout	Aatch Case				Add Edit Delete Move Up Move Dow

3. Seleccione el nombre del grupo de servidores y especifique **RADIUS** como el protocolo que desea utilizar y, a continuación, haga clic en **Aceptar**.

• • •	Add AAA Server Group
AAA Server Group:	ISE
Protocol:	RADIUS 📀 🔶
Accounting Mode:	🔘 Simultaneous 🛛 🔾 Single
Reactivation Mode:	O Depletion O Timed
Dead Time:	10 minutes
Max Failed Attempts:	3
Enable interim ac	counting update
Update Interv	al: 24 Hours
Enable Active Dir	ectory Agent mode
ISE Policy Enforcemer	nt
🗌 Enable dynamic a	uthorization
Dynamic Authoriz	zation Port: 1700
Use authorization	only mode (no common password configuration required)
VPN3K Compatibility	∕ Option ¥
	Help Cancel OK

5. Seleccione el nuevo grupo de servidores y haga clic en **Agregar** en **Servidores en el** panel **Grupo Seleccionado**, como se muestra en la imagen.

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts	Add
ISE	RADIUS	Single	Depletion	10	3	
LOCAL	LOCAL					Edit
ni neorriene			•	10	4	
						Dele
Cind			ah Casa			
Find:		🕞 🙆 🗌 Mat	ch Case			
Find:		🛇 🙆 🗆 Mat	ch Case			
Find:		🛛 🖂 🗌 Mat	ch Case			
Find:	elected Group	🛛 🖂 🗆 Mat	ch Case			
Find: Servers in the Se	elected Group	Mat	ch Case			
Find: Servers in the Se Server Name or IP	elected Group	Ce Timeout	ch Case		(	Add
Find: Servers in the Se Server Name or IP	elected Group Address Interfa	Ce Timeout	ch Case		(	Add
Find: Servers in the Se Server Name or IP	elected Group Address Interfa	CCC Timeout	ch Case		(	Add
Find: Servers in the Se Server Name or IP	elected Group Address Interfa	Ce Timeout	ch Case		(	Add Edit
Find: Servers in the Se Server Name or IP	elected Group Address Interfa	CCC Timeout	ch Case		(	Add Edit
Find: Servers in the Se Server Name or IP	elected Group Address Interfa	Ce Timeout	ch Case		(	Add Edit Delete
Find: Servers in the Se Server Name or IP	elected Group Address Interfa	Ce Timeout	ch Case		(	Add Edit Delete
Find: Servers in the Se Server Name or IP	elected Group Address Interfa	Ce Timeout	ch Case			Add Edit Delete

6. En la ventana **Edit AAA Server**, seleccione el nombre de la interfaz, especifique la dirección IP del servidor ISE, escriba la clave secreta RADIUS y haga clic en **Ok**.

**Nota**: Toda esta información debe coincidir con la especificada en 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	2: 🔽
SDI Messages	
Message Table	*
Help	Cancel OK

Configuración de CLI.

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

### Configuración de VPN de acceso remoto de 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 DU0
tunnel-group ISE-users webvpn-attributes
group-alias ISE enable
dns-group DNS-CISC0
```

# Prueba

1. Abra la aplicación **Anyconnect** en su dispositivo PC. Especifique el nombre de host de la cabecera VPN ASA e inicie sesión con el usuario creado para la autenticación secundaria Duo y haga clic en **Aceptar**.

000	Sec	AnyConnect ure Mobility Client	cisco
	VPN: Please enter yo	ur username and password.	Connect
	Cisco A	nyConnect   192.168.10	00.100
	Please enter your	username and password	
_	Group:		0
	msgstringESMEX	duovpn	
	MEX-PASS	••••	
			Cancel OK

2. Recibió una notificación de inserción Duo en el dispositivo Duo Mobile del usuario especificado.

3. Abra la notificación de Duo Mobile App y haga clic en Aprobar.





4. Acepte el banner y se establecerá la conexión.

000	AnyConnect Secure Mobility Client	cisco
	VPN: Please respond to banner.	
	192.168.100.100	Connect
	Cisco AnyConnect -	Banner
		Disconnect Accept
* *		

•••	AnyConnect Secure Mobility Client	cisco
00:00:04	VPN: Connected to 192.168.100.100. 192.168.100.100	Disconnect  IPv4
	System Scan: Compliant. Network access allowed.	Scan Again
	Roaming Security: Umbrella is active.	
<b>P</b>	AMP Enabler: Waiting for configuration	
* 2		

# Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Duo Authentication Proxy incluye una herramienta de depuración que muestra los motivos de error y fallo.

### Depuraciones de trabajo

**Nota**: La siguiente información se almacena en C:\Program Files\Duo Security Authentication Proxy\log\connectivity\_tool.log.

Output	
Running	The Duo Authentication Proxy Connectivity Tool. This may take
tinfa]	several minutes
[info]	Idebug's 'True'
[TUIO]	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': '******',
11-5-3	'service_account_username': 'Administrator'}
ניזחנן	There are no configuration problems
[info]	
[info] [info]	 Testing section 'radius_server_auto' with configuration:
[info] [info] [info]	 Testing section 'radius_server_auto' with configuration: {'api_host': '
[info] [info] [info]	 Testing section 'radius_server_auto' with configuration: {'api_host': 'all all all all all all all all all al
[info] [info] [info]	 Testing section 'radius_server_auto' with configuration: {'api_host': 'a a a a a a a a a a a a a a a a a 'client': 'ad_client', 'debug': 'True',
[info] [info] [info]	<pre> Testing section 'radius_server_auto' with configuration: {'api_host': 'all and and and and and and and and and and</pre>
[info] [info] [info]	 Testing section 'radius_server_auto' with configuration: {'api_host': ' <b>and and the second parts</b> 'client': 'ad_client', 'debug': 'True', 'failmode': 'safe', 'ikey': <b>The second of the second</b>
[info] [info] [info]	Testing section 'radius_server_auto' with configuration: {'api_host': 'apl and line
[info] [info] [info]	Testing section 'radius_server_auto' with configuration: {'api_host': 'all all all all all all all all all al
[info] [info] [info]	Testing section 'radius_server_auto' with configuration: {'api_host': 'and and and and and and and and and and
[info] [info] [info]	<pre></pre>
[info] [info] [info]	<pre>Testing section 'radius_server_auto' with configuration: {'api_host': 'all and if the analysis and', 'client': 'ad_client', 'debug': 'True', 'failmode': 'safe', 'failmode': 'safe', 'ikey': 'the analysis and 'the analysis', 'port': '1812', 'radius_ip_1': '10.28.17.101', 'radius_secret_1': '******', 'skey': '******[40]'} There are no configuration problems</pre>
[info] [info] [info]	<pre>Testing section 'radius_server_auto' with configuration: {'api_host': 'qnl dial?'Late and light defined. 'client': 'ad_client', 'debug': 'True', 'failmode': 'safe', 'ikey': tate and the test defined. 'port': '1812', 'radius_ip_1': '10.28.17.101', 'radius_secret_1': '*****', 'skey': '*****[40]'} There are no configuration problems</pre>
[info] [info] [info] [info]	<pre></pre>
<pre>[info] [info] [info] [info] [info]</pre>	Testing section 'radius_server_auto' with configuration: {'api_host': 'and affiliate a section and 'a section'. 'client': 'ad_client', 'debug': 'True', 'failmode': 'safe', 'ikey': 'safe', 'ikey': 'safe'. 'port': '1812', 'radius_ip_1': '10.28.17.101', 'radius_secret_1': '******', 'skey': '******[40]'} There are no configuration problems Testing section 'main' with configuration: {'debug': 'True',
[info] [info] [info] [info] [info]	Testing section 'radius_server_auto' with configuration: {'api_host': 'all all life and and and and all and all all all and and all all all all all all all all all al
[info] [info] [info] [info] [info]	<pre>Testing section 'radius_server_auto' with configuration: {'api_host': 'apl and 'the mean line and 'the sector',  'debug': 'True',  'failmode': 'safe',  'ikey': 'the sector' is a sector',  'radius_ip_1': '10.28.17.101',  'radius_secret_1': '******',  'skey': '******[40]'} There are no configuration problems Testing section 'main' with configuration: {'debug': 'True',  'log_max_files': '10',  'log_max_size': '20971520',</pre>

[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'}
[info]	The LDAP Client section has no connectivity issues.
[info]	, <u></u>
[info]	Testing section 'radius_server_auto' with configuration:
[info]	{'api_host': 'api_educe.ai.duceccuring.cmm',
	'client': 'ad_client',
	'debug': 'True',
	'failmode': 'safe',
	'ikey': 'nTharonom's skerezer',
	'port': '1812',
	'radius_ip_1': '10.28.17.101',
	'radius_secret_1': '******',
	'skey': '******[40]'}
[info]	The RADIUS Server has no connectivity problems.
[info]	9 <del></del>
[info]	SUMMARY
[info]	No issues detected

1. Problemas de conectividad, IP incorrecta, FQDN/nombre de host no resuelto en la configuración de Active Directory.



2. Contraseña incorrecta para el usuario Administrador en Active Directory.



Depuraciones.

[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>3</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 base incorrecto.



Depuraciones.



4. Valor de RADIUS de clave incorrecta.



Depuraciones



5. Compruebe que el servidor ISE envía paquetes de solicitud de acceso.

#### \*Ethernet0



6. Para confirmar que el servidor proxy de autenticación Duo funciona, Duo proporciona la herramienta <u>NTRadPing</u> para simular paquetes de solicitud de acceso y respuesta con Duo.

6.1 Instale NTRadPing en un equipo diferente y genere tráfico.

Nota: En este ejemplo se utiliza la máquina Windows 10.28.17.3.

6.2 Configure con los atributos utilizados en la configuración de ISE Radius.

NTRadPing Test	Utility		- 0	×
RADIUS Server/port: Reply timeout (sec.):	10.28.17.107 <b>4</b>	1812 Retries: 6	NTRadPing 1.5 - RADIUS Server Testing Tool © 1999-2003 Master Soft SpA - Italy - All rights reserv http://www.dialways.com/	red
RADIUS Secret key: User-Name: Password:	duovpn	T CHAP	MASTERSOFT'	
Request type:	Authentication Request	• 0	RADIUS Server reply:	
Additional RADIUS A	tsibutes:		Construction and the second second of the Second	
Add Remove	Clear list Lo	ad Save	Send Help Close	

6.3 Configure Duo Authentication Proxy Manager de la siguiente manera.



6.4. Desplácese hasta la herramienta NTRadPing y haga clic en **Enviar**. Recibirá una notificación de inserción Duo en el dispositivo móvil asignado.

NTRadPing Test	Utility			– 🗆 ×
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	Retries	6	http://www.dialways.com/
ADIUS Secret key:	[Mexvpn!17!			
lser-Name:	duovpn	_		
assword:	IODODODODOD		CHAP	MASTERSOFT DIALWAYS
Request type:	Authentication Requ	est 💌	0	RADIUS Server reply:
				Transmitting packet, code=1 id=12 length=46 no response from server (inned out); non-offenot (#1) received response from the server in 4000 millisecords reply packet soda=2 id=12 length=49 response: Access-Accept 
	-		•	
			- 1	

+	700 20.866684	10.28.17.3	10.28.17.107	RADIUS	88 Access-Request id=13, Duplicate Request
eL.	737 22.184895	10.28.17.107	10.28.17.3	RADIUS	90 Access-Accept id=13 🚽

> Frame 700: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface \Device\NPF\_{CA092CEE-5528-4E0A-9310-2D523160DD60}, id 0

- > Ethernet II, Src: VMware\_b3:f2:72 (00:50:56:b3:f2:72), Dst: VMware\_b3:b4:3e (00:50:56:b3:b4:3e)
- > Internet Protocol Version 4, Src: 10.28.17.3, Dst: 10.28.17.107
- > User Datagram Protocol, Src Port: 51188, Dst Port: 1812

RADIUS Protocol Code: Access-Request (1) Packet identifier: 0xd (13) Length: 46 Authenticator: 2020202020203136343639335333230 [Duplicate Request Frame Number: 532] [The response to this request is in frame 737]

✓ Attribute Value Pairs

- > AVP: t=User-Name(1) l=8 val=duovpn 🔫
- > AVP: t=User-Password(2) l=18 val=Encrypted

#### Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).