Duo-integratie configureren met Active Directory en ISE voor tweevoudige verificatie op AnyConnect/Remote Access VPN-clients

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Netwerkdiagram en -scenario **Communicatieproces** Active Directory-configuraties Twee configuraties Configuratie van twee autorisatieproxy **Cisco ISE-configuraties** Cisco ASA RADIUS/ISE-configuratie Cisco ASA VPN-configuratie voor externe toegang Testen Problemen oplossen Fouten in het werk

Inleiding

In dit document wordt de duo push-integratie met AD en ISE beschreven als twee-factor verificatie voor AnyConnect-clients die met ASA zijn verbonden.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- RA VPN-configuratie op ASA
- RADIUS-configuratie op ASA
- ISE
- Active Directory
- Duo-toepassingen

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Microsoft 2016-server
- ASA 9.14(3)18
- ISE-server 3.0
- Duo Server

• Duo Verificatie Proxy Manager

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Dit document beschrijft hoe u Duo push-integratie met Active Directory (AD) en Cisco Identity Service Engine (ISE) kunt configureren als tweevoudige verificatie voor AnyConnect-clients die verbinding maken met Cisco adaptieve security applicatie (ASA).

Netwerkdiagram en -scenario



Communicatieproces

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

- 1. Primaire verificatie gestart naar Cisco ISE-id
- 2. Cisco ISE stuurt een verificatieaanvraag naar de Duo-verificatieproxy
- 3. Primaire verificatie maakt gebruik van Active Directory of RADIUS
- 4. Duo Authenticatie Proxy-verbinding ingesteld met Duo Security over TCP-poort 443
- 5. Secundaire authentificatie via de dienst van Duo Security
- 6. Duo authenticatie proxy ontvangt authenticatiereactie
- 7. Cisco ISE-toegang verleend

Gebruikersaccounts:

- Active Directory Admin: Dit wordt gebruikt als de directory account om de Duo Auth Proxy te laten binden aan de Active Directory-server voor primaire verificatie.
- Testgebruiker van Active Directory
- Duo testgebruiker voor secundaire verificatie

Active Directory-configuraties

Windows-server is vooraf geconfigureerd met Active Directory Domain-services.

Opmerking: Als RADIUS Duo Autor Proxy Manager op dezelfde Active Directory-hostmachine wordt uitgevoerd, moeten de NPS-rollen (Network Policy Server) worden verwijderd/verwijderd. Als beide RADIUS-services worden uitgevoerd, kunnen ze conflicten veroorzaken en gevolgen hebben voor de prestaties.

Om een AD-configuratie voor verificatie en gebruikersidentiteit op gebruikers van Remote Access VPN te realiseren, zijn een paar waarden vereist.

Al deze gegevens moeten worden gecreëerd of verzameld op de Microsoft Server voordat de configuratie kan worden uitgevoerd op de ASA- en Duo Auth-proxyserver.

De belangrijkste waarden zijn:

- Domeinnaam. Dit is de domeinnaam van de server. In deze configuratiehandleiding is agarciam.cisco de domeinnaam.
- IP/FQDN-adres van server. Het IP-adres of FQDN wordt gebruikt om de Microsoft-server te bereiken. Als een FQDN wordt gebruikt, moet een DNS-server worden geconfigureerd binnen ASA en Duo Auth proxy om de FQDN op te lossen.

In deze configuratiehandleiding is deze waarde agarciam.cisco (die zich oplost in 10.28.17.107).

- Serverpoort. De poort die wordt gebruikt door de LDAP-service. Standaard gebruiken LDAP en STARTTLS TCP-poort 389 voor LDAP en gebruikt LDAP over SSL (LDAPS) TCP-poort 636.
- root-CA. Als LDAPS of STARTTLS wordt gebruikt, is de wortel CA die wordt gebruikt om het SSL certificaat te ondertekenen dat door LDAPS wordt gebruikt vereist.
- Gebruikersnaam en wachtwoord voor map Dit is het account dat door Duo Auth proxy server wordt gebruikt om te binden aan de LDAP-server en gebruikers te verifiëren en te zoeken naar gebruikers en groepen.
- Basisnaam en Groepsnaam (DN). De Base DN is het vertrekpunt voor Duo Auth proxy en vertelt de Active directory om te beginnen met zoeken naar gebruikers en hen te verifiëren.

In deze configuratiegids, wordt het worteldomein agarciam.cisco gebruikt aangezien de Basis DN en Groep DN Duo-GEBRUIKERS zijn.

1. Om een nieuwe Duo gebruiker, op Windows Server toe te voegen, navigeer naar **Windows** pictogram linksonder en klik op **Windows-beheerprogramma's**, zoals in de afbeelding.



2. Ga in het venster Windows-beheertools naar Active Directory-gebruikers en -computers.

Vouw in het paneel Active Directory-gebruikers en -computers de domeinoptie uit en navigeer naar de map **Gebruikers**.

In dit configuratievoorbeeld wordt Duo-USER gebruikt als doelgroep voor secundaire authenticatie.

→ 小 檜 → Control i	Panel > System and Security > Administrat	tive Tools			Active Directory Users and Comp	puters		
Quick access Desktop Pictures Og System32 This PC Desktop Decuments Decktop Documents Desktop Documents Documents Documents Documents Documents Documents Documents	Panel > System and Security > Administrat Terminal Services Active Directory Administrative Center 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 Computer Management Connection Manager Administration Kit Definition and Optimize Drives Disk Glavers	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 6:19 AM	Type File folder 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 Comp File Action View Help Active Directory Users and Com Active Directory Users and Com Saved Queries Saved	Image: Second	Type User User User User Security Group Security Group Security Group Security Group Security Group	Members in Members of A user accor Members of A user accor Members in DNS Admini DNS clients of Designated a
Downloads on Mac Music Pictures Videos Local Disk (C:) DVD Drive (D:) SSS_ Network	Disk Cleanup DNS Event Viewer Group Policy Management Internet Information Services (IIS) Manager ISCSI Initiator Local Security Policy Microsoft Azure Services ODBC Data Sources (32-bit)	7/16/2016 6:19 AM 7/16/2016 6:19 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 7/16/2016 6:19 AM	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	<>	Domain Ada Domain Co Domain Co Domain Gue Domain Users DOUC-USERS duo2 Enterprise K Enterprise R Enterprise R	Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group	Designated a All workstati All domain o All domain o All domain o Designated i Members of Members of

3. Klik met de rechtermuisknop op de map **Gebruikers** en selecteer **Nieuw** > **Gebruiker**, zoals in de afbeelding.

Active Directory Users and Comp	uters			-	×
File Action View Help] 🙆 📑 🔽 🗖	1 🙁 🐮 👕	' 🗾 'its		
Active Directory Users and Com Saved Queries Saved Queries Delegate Conto Find	Name Administrator agarciam alanad alanduo Allowed RO Cloneable D rol D	Type User User User Security Group Security Group Security Group User 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		<
New All Tasks View Refresh Export List Properties Help < >>	> > Enterprise	Computer Contact Group InetOrgPerson msDS-KeyCredent msDS-ResourcePr msDS-ShadowPrir msImaging-PSPs MSMQ Queue Alia Printer	tial opertyList ncipalContainer		~
Create a new object		User Shared Folder			

4. Specificeer in het venster Nieuwe gebruiker-object de identiteitskenmerken van deze nieuwe gebruiker en klik op **Volgende**, zoals in de afbeelding.

New Object - User		×			
Create in:	agarciam.cisco/Users	0			
First name:	duovpn				
Full name: duovpn					
User logon name:		s			
duovpn	@agarciam.cisco ~	2			
User logon name (pre	Windows 2000):	s			
AGARCIAM	duovpn				
	\frown				
	< Back Next > Cancel				

5. Bevestig het wachtwoord en klik op Volgende. Voltooien zodra de gebruikersinformatie is geverifieerd.

New Object - User	×
Create in: agarciam.cisco/Users	c
Password:	ar
User must change password at next logon User cannot change password Password never expires Account is disabled	s s :(s
< Back	lext > Cancel

6. Wijs de nieuwe gebruiker toe aan een specifieke groep, klik met de rechtermuisknop op de groep en selecteer **Toevoegen aan een groep**, zoals in de afbeelding.

Active Directory Users and Com	puters			-		×
File Action View Help						
← → 2 🖂 📈 🗋 🗡 🖡	0 🗟 📄 🔽 🖬	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 Gue Domain Gue Domain Gue Domain Gue Domain Gue Cloneable D Domain Co Domain Gue Domain Gue Cloneable D Domain Gue	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			
< >	R Enterprise	Add to a group Disable Account	of this group		10	~
Allows you to add the selected object	s to a group yo	endere recount				

7. Typ in het paneel Groepen selecteren de naam van de gewenste groep en klik op Namen controleren.

Selecteer vervolgens de naam die overeenkomt met uw criteria en klik op OK.

Select Groups	×
Select this object type:	
From this location:	Object Types
agarciam.cisco	Locations
Enter the object names to select (examples):	
	Check Names
	of
	of
Advanced OK	Cancel

8. Dit is de gebruiker die in dit document als voorbeeld wordt gebruikt.

Twee configuraties

1. Log in op uw Dudo Admin portal.

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

2.In het linker zijpaneel, navigeer naar **Gebruikers**, klik op **Add User** en typ de naam van de gebruiker die overeenkomt met onze Active Domain-gebruikersnaam, en klik vervolgens op **Add User**.



3. Vul in het nieuwe gebruikerspaneel de spatie in met alle benodigde informatie.

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 F²

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	 Active Require multi-factor authentication (default). Bypass Allow users to skip two-factor authentication and log in w Disabled Automatically deny access This controls the user's two-factor authentication process.
Groups	You don't have any editable groups. Add one. Groups can be used for management, reporting, and policy. Le
Notes	

:In dit document wordt de methode Duo push for mobile devices gebruikt, dus moet er een telefoonapparaat worden toegevoegd.

Klik op **Telefoon toevoegen**.

Phones You may rearrange the phones by dragging and drop	ping 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		1

5. Typ het telefoonnummer van de gebruiker en klik op **Telefoon toevoegen**.

Dashboard > Users > duovpn > Add Phone

Add Phone

i Learn more	about Activating Duo Mobile 🖆.
Туре	Phone Tablet
Phone number	Optional. Example: "+52 1 222 123 4567"
	Add Phone

6. Navigeer naar **Gebruikers** op het linkerpaneel Duo Admin en klik op de nieuwe gebruiker.

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 ad	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			.com	1	
Need Help? Chat with Tech Support D					

Opmerking:In het geval u op dit moment geen toegang hebt tot uw telefoon, kunt u de e-mailoptie selecteren.

7.Navigeren naar telefoons sectie en klik op Duo Mobile activeren.

Phones You may rearran	ge the phones by dragging an	d dropping in the table.	Learn more about activating	a replacement phone 🗗	
Alias	Device	Platform	Model	Security Warnings	
phone1	1000	Android 10	0.011×10^{-10}	✓ No warnings	Activate Duo Mobile

8. Klik op Generate Duo Mobile Activeringscode.



9. Selecteer **E-mail** om de instructies via e-mail te ontvangen, typ uw e-mailadres en klik op **Instructies per e-mail verzenden**.

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 minar Bin san asan

10. U ontvangt een e-mail met de instructies, zoals getoond in de afbeelding.

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. Open de Duo Mobile App vanaf uw mobiele apparaat en klik op **Add** dan selecteer **Use QR code** en scan de code uit de instructies e-mail.

12. Nieuwe gebruiker wordt toegevoegd aan uw Duo Mobile App.

Configuratie van twee autorisatieproxy

1.Download en installeer Duo Auth Proxy Manager van https://duo.com/docs/authproxy-reference.

Opmerking:In dit document is Duo Auth Proxy Manager geïnstalleerd op dezelfde Windows-server waarop Active Directory-services worden gehost.

2. Navigeer in het Duo Admin-paneel naar toepassingen en klik op Protect a Application.



3. Zoek in de zoekbalk naar Cisco ISE-straal.

Protect an Application

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

4. Kopieer de integratiesleutel, de beveiligingssleutel en de API Hostname. U hebt deze gegevens nodig voor de configuratie van de Duo-verificatieproxy.



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	5.00040g.demi//1019t.047	Сору
Secret key	•••••W6ho	Сору
	Don't write down your secret key or share it with anyo	ne.
API hostname	(0+30/00/2010/00/2017/00/2017	Сору

5. Start de Duo Authenticatie Proxy Manager applicatie en vul de configuratie voor zowel de Active Directory-client als de ISE Radius Server in en klik op **Valideren**.

Opmerking: Als de validatie niet successol is, raadpleegt u het tabblad debug voor meer informatie en corrigeert u dit.

Authentication Proxy is running	Up since: 3/5/2022, 9:2	3:04 AM	Version: 5.6. Update your Auther	0 Rest
Validation passed Configuration has passed validation	and is ready to be saved	←		
Configure: authproxy.cfg		Unsaved Changes	s Output	
<pre>18 ; number to the section name (19 20 [ad_client] 21 host=10.28.17.107 22 service_account_username=Admin 23 service_account_password= FEAF 24 search_dn=DC=agarciam,DC=cisco 25 [26 [radius_server_auto] 27 ikey=Untributert_hitheration 28 skey=Y9e97rtPiATPiPTTPTTFATF 29 api_host=api_afrt4710.cleateur 30 radius_ip_1=10.28.17.101 31 radius_secret_1=Wergen117! 32 failmode=safe 33 client=ad_client 34 port=1812 35 36</pre>	e.g. [ad_client2]) istrator mill/1 whalWopgPewCodg 1095 ton		Running [info] [info] [info] [info] [info] [info] [info] [info] [info]	The Duo Authentication Proxy Connecti several minutes Testing section 'main' with configura {'debug': 'True', 'log_max_files': '10', 'log_max_size': '20971520', 'test_connectivity_on_startup': 'tru There are no configuration problems Testing section 'ad_client' with conf {'debug': 'True', 'host': '10.28.17.107', 'search_dn': 'DC=agarciam,DC=cisco', 'service_account_password': '*****', 'service_account_password': '*****', 'service_account_username': 'Adminis There are no configuration problems Testing section 'radius_server_auto' ['ani hest': 'ani ad7c472d duescervit
Validate Save				Learn how to c

Cisco ISE-configuraties

1. Log in op het ISE-beheerportal.

2.Breid het tabblad Cisco ISE uit en navigeer naar **beheer**, klik vervolgens op **Network Resources** en klik op **Externe RADIUS-servers**.

Cisco ISE -	Q What page are you looking for	or?		
Dashboard	Context Visibility	Operations	-Policy-	Administration
Recent Pages	System		Network Resources	
External Identity Sources Policy Sets Network Device Profiles External RADIUS Servers RADIUS Server Sequences Live Logs	Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks		Network Devices Network Device Crow Network Device Prof External RADIUS Ser RADIUS Server Sequ NAC Managers External MDM	vers ences

3. Klik op het tabblad Externe RADIUS-servers op Toevoegen.

■ Cisco ISE		Admi	nistration • Network Resourc	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. Vul de spatie in met de RADIUS-configuratie die wordt gebruikt in de Duo Authenticatie Proxy Manager en klik op **Indienen**.

Network Devices Networ	k Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequ
* Name	DUO_NEW			
Description			<i>b</i>	
* Host IP	10.28.17.107			
* Shared Secret	·········	Show		
Enable KeyWrap				
* Key Encryption Key		Show		
* Message Authenticator Code Key		Show		
Key Input Format	ASCII O HEXADE	CIMAL		
* Authentication Port	1812	(Valid Range 1 to 65	535)	
* Accounting Port	1813	(Valid Range 1 to 65	535)	
* Server Timeout	5	Seconds (Valid Ran	ge 1 to 120)	
* Connection Attempts	3	(Valid Range 1 to 9)		
Radius ProxyFailover Expiration	300	(valid Range 1 to	o 600)	

5. Navigeer naar het tabblad **RADIUS-serversequenties** en klik op **Add**.



6. Specificeer de naam van de reeks en wijs de nieuwe externe RADIUS-server toe. Klik op Indienen.

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. Navigeer van het menu Dashboard naar **Beleid** en klik op **Beleidssets**.



8. Wijs de RADIUS-sequentie toe aan het standaardbeleid.

Opmerking:In dit document wordt de Duo-reeks op alle verbindingen toegepast, dus wordt het standaardbeleid gebruikt. De beleidstoewijzing kan naar behoefte variëren.

Policy Sets

Image: Search Image: Search <td< th=""><th>Status Policy Set Name</th><th>Description</th><th>Conditions</th></td<>	Status Policy Set Name	Description	Conditions
Image: Constraint of the second se	Search		
Default Default policy set	 BUDIA 		Radius-User-Name EQUALS isevpn
Default Default policy set	• · · ·		Radius-NAS-Port-Type EQUALS Virtual
	Oefault	Default policy set	

Cisco ASA RADIUS/ISE-configuratie

1. Configureer ISE RADIUS-server onder AAA-servergroepen, navigeer naar **Configuration** en klik vervolgens op **Apparaatbeheer** en vouw het gedeelte **Gebruikers/AAA uit**, selecteer **AAA-servergroepen**.

Bookmarks bookmark a page, right-click on a node in the	AAA Server Groups
riagation tree and select "Add to bookmarks".	Server Group Pro
Go 📋 Delete	
	ad-agarciam ID
O O Device Management	
Management Access	
8 Licensing	
System Image/Configuration	
Plansing Availability and Scalability	Find:
E Logging	
Shart Call-Home	Servers in the Selector
Service Module Settings	Servers in the Selected
	Server Name or IP Addres
	10.28.17.101
Se LDAP Attribute Man	
Se AAA Kerberos	
Se Authentication Prompt	
Do AAA Access	
Dynamic Access Policies	
S User Accounts	
A Password Policy	
Change My Password	
Login History	
Certificate Management	
P DHCP	
B DNS	
DECT ADI Agant	
Service Setup	
Firewall	
Remote Access VPN	Find
A Site-to-Site VPN	Find:

2. Klik in het paneel AAA-servergroepen op Add.

Server Group Protocol Accounting Mode Reactivation Mode Dead Time Max Failed Attempts Add Edit Dele Find: O Match Case Servers in the Selected Group Server Name or IP Address Interface Timeout Add Edit Dele Move Up Move Dow	AAA Server Grou	aps						-
Find: Servers in the Selected Group Server Name or IP Address Interface Timeout Add Edit Delete Move Up Move Dow	Server Group	Protocol	Accounting Mo	de Reactivation Mod	le Dead Tir	me Max Fa	ailed Attempts	Add
Find: Match Case Servers in the Selected Group Server Name or IP Address Interface Timeout Add Edit Delete Move Up Move Dow	- 1	- 12		_				Edit
Find: O Match Case		-						Delet
Find: O Match Case Servers in the Selected Group Server Name or IP Address Interface Timeout Add Edit Delete Move Up Move Dow								
Find: Match Case Servers in the Selected Group Server Name or IP Address Interface Timeout Add Edit Delete Move Up Move Dow								
Find: O Match Case								
Find: Match Case Servers in the Selected Group Server Name or IP Address Interface Timeout Add Edit Delete Move Up Move Up Move Dow								
Find: Match Case Servers in the Selected Group Server Name or IP Address Interface Timeout Add Edit Delete Move Up Move Dow								
Find: Match Case Servers in the Selected Group Server Name or IP Address Interface Timeout Add Edit Delete Move Up Move Dow								
Servers in the Selected Group Server Name or IP Address Interface Timeout Edit Delete Move Up Move Dow								
Servers in the Selected Group Server Name or IP Address Interface Timeout Edit Delete Move Up Move Dow	P. 4							
Server Name or IP Address Interface Timeout Add Edit Delete Move Up Move Dow	Find:			Aatch Case				
Edit Delete Move Up Move Dow	Find:	elected Group		Aatch Case				
Delete Move Up Move Dow	Find: Servers in the Se Server Name or IP	elected Group	ace Timeout	Aatch Case				Add
Delete Move Up Move Dow	Find: Servers in the Se Server Name or IP	elected Group Address Interfa	ace Timeout	Aatch Case				Add
Move Up Move Dow	Find: Servers in the Se Server Name or IP	elected Group Address Interfa	ace Timeout	Aatch Case				Add Edit
Move Dow	Find: Servers in the Se Server Name or IP	elected Group Address Interfa	ace Timeout	Aatch Case				Add Edit Delete
	Find: Servers in the Se Server Name or IP	elected Group Address Interfa	ace Timeout	Aatch Case				Add Edit Delete Move Up
	Find: Servers in the Se Server Name or IP	elected Group Address Interfa	ace Timeout	Aatch Case				Add Edit Delete Move Up

3. Selecteer de naam van de servergroep en specificeer **RADIUS** als het te gebruiken protocol en klik vervolgens op **OK**.

• • •	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 Interval: 24 Hours					
Enable Active Directory Agent mode					
ISE Policy Enforcemen	ISE Policy Enforcement				
Enable dynamic authorization					
Dynamic Authoriz	ation Port: 1700				
Use authorization only mode (no common password configuration required)					
VPN3K Compatibility Option *					
	Help Cancel OK				

5. Selecteer uw nieuwe servergroep en klik op **Add** onder de **Server in het** paneel **Geselecteerde groep**, zoals in de afbeelding.

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts	Ado
ISE	RADIUS	Single	Depletion	10	3	
LOCAL	LOCAL					Edit
ni nannina	-		•	10	4	
						Dele
F '						
Find:		🛛 🖂 🗌 Mat	ch Case			
Find:		🛇 🙆 🗆 Mat	ch Case			
Find:		🛛 🖓 🗌 Mat	ch Case			
Find:	elected Group	_ 🖸 🙆 — Mat	ch Case			
Find:	elected Group	G G Mat	ch Case			
Find: Servers in the Server Name or IP	elected Group	G G Mat	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	Ce Timeout	ch Case		(Add
Find: Servers in the Server Name or IP	elected Group Address Interfa	CCC Timeout	ch Case		(Add Edit
Find: Servers in the Server Name or IP	elected Group Address Interfa	Ce Timeout	ch Case		(Add Edit
Find: Servers in the Server Name or IP	elected Group Address Interfa	Ce Timeout	ch Case			Add Edit Delete
Find: Servers in the 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	Ce Timeout	ch Case		(Add Edit Delete

6. Selecteer in het venster **AAA-server bewerken** de interfacenaam, geef het IP-adres van de ISE-server op, typ de geheime RADIUS-toets en klik op **OK**.

Opmerking: al deze informatie moet overeenkomen met de informatie die in Duo Verification Proxy Manager is opgegeven.

• •	Edit AAA Server
Server Group: ISI Interface Name:	outside
Server Name or IP Address: 1	0.28.17.101
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

CLI-configuratie.

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

Cisco ASA VPN-configuratie voor externe toegang

```
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
```

Testen

1. Open de **AnyConnect**-app op uw pc-apparaat. Specificeer de hostnaam van de VPN ASA Head-end en log in met de gebruiker die is gemaakt voor Duo secundaire verificatie en klik op **OK**.

000	Sec	AnyConnect ure Mobility Client	cisco
	Please enter yo	our username and passwo	ord.
	Cisco A	nyConnect 192.168	3.100.100
	Please enter your	username and passw	ord.
_	Group:		•
	msgstringESMEX	duovpn	-
	MEX-PASS	•••••	
			Cancel OK

- 2. U hebt een Duo-push-melding ontvangen op het opgegeven Duo Mobile-apparaat.
- 3. Open de Duo Mobile App-melding en klik op Goedkeuren.





4. Accepteer de banner en er wordt een verbinding tot stand gebracht.

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.	
	AMP Enabler: Waiting for configuration	

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

De Duo-verificatieproxy wordt geleverd met een debug-tool die de redenen voor fouten en fouten weergeeft.

Fouten in het werk

Opmerking: De volgende informatie wordt opgeslagen in C:\Program Files\Duo Security Authenticatie Proxy\log\connectiviteit_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'}
נידתנן	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': ' and and the second parts 'client': 'ad_client', 'debug': 'True', 'failmode': 'safe', 'ikey': The second of the second
[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 in the analyse and, 'client': 'ad_client', 'debug': 'True', 'failmode': 'safe', 'failmode': 'safe', 'ikey': 'the analyse and the analyse a</pre>
[info] [info] [info]	<pre>Testing section 'radius_server_auto' with configuration: {'api_host': 'qnl dial?'Late and light dial.'' 'client': 'ad_client', 'debug': 'True', 'failmode': 'safe', 'ikey': 'late fact the fact the</pre>
<pre>[info] [info] [info] [info] [info]</pre>	<pre></pre>
<pre>[info] [info] [info] [info] [info] [info]</pre>	Testing section 'radius_server_auto' with configuration: {'api_host': 'all all line 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]	<pre>Testing section 'radius_server_auto' with configuration: {'api_host': 'all all' intermediates' 'client': 'ad_client', 'debug': 'True', 'failmode': 'safe', 'ikey': 'iterrated interfaction' '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', 'log_max_files': '10',</pre>
<pre>[info] [info] [info] [info] [info] [info]</pre>	<pre>Testing section 'radius_server_auto' with configuration: {'api_host': 'apl and 'the mental param', 'client': 'ad_client', 'debug': 'True', 'failmode': 'safe', 'ikey': 'the mental is the field of the field</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]	
[info]	Testing section 'radius_server_auto' with configuration:
[info]	{'api_host': 'eal-adreatat.duosecuring.cmm',
	'client': 'ad_client',
	'debug': 'True',
	'failmode': 'safe',
	'ikey': 'nmharonong ukengruky',
	'port': '1812',
	'radius_ip_1': '10.28.17.101',
	'radius_secret_1': '******',
	'skey': '******[40]'}
[info]	The RADIUS Server has no connectivity problems.
[info]	
[info]	SUMMARY
[info]	No issues detected

1. Connectiviteitsproblemen, verkeerde IP, onoplosbare FQDN/Hostname op Active Directory-configuratie.



2. Verkeerd wachtwoord voor beheerder op Active Directory.

[ad_client]

Debugs.

[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. Wrong Base Domain.



Debugs.



4. Foute RADIUS-waarde.



Debugs

	and a manufact t
[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. Controleer of ISE-server access-request pakketten verstuurt.

6	*Ethernet0					
Fil	e Edit View Go	Capture Analyze St	atistics Telephony Wirele	ss Tools He	slp	
1	📕 🔬 💿 📃 🛅	X 🖸 🍳 👄 👳 🤋	2 7 J 📃 📃 Q G	Q 👳		
	radius	1				
No.	Time	Source	Destination	Protocol	Length Tefo	<u> </u>
7*	1511 6020.521457	10.28.17.101	10.28.17.107	RADIUS	877 Access-Req	uest 1-31
₄∟	1513. 6024.344735	10.28.17.107	10.28.17.101	RADIUS	191 Access Acc	ept id=31
>	Frame 151115: 877 Ethernet II, Src: Internet Protocol User Datagram Prot RADIUS Protocol	bytes on wire (701 VMware_b3:a4:2f (0 Version 4, Src: 10 ocol, Src Port: 42	6 bits), 877 bytes cap 0:50:56:b3:a4:2f), Dst 28.17.101, Dst: 10.28 022, Dst Port: 1812	tured (7016 : V%ware_b3: :17.107	bits) on interfac b4:3e (00:50:56:1	ce \Device\NPF_{CA092CEE-5 33:b4:3e)
	Code: Access-Re Packet identifi Length: 835 Authenticator: : [The response t ~ Attribute Value > AVP: t=User-I	<pre>quest (1) er: 0x1f (31) 38a28ca3ca6bbc2618 o this request is Pairs Name(1) 1=8 val=du</pre>	19c5304b1be6e3 in frame 151332] ovpn			
	> AVP: t=User-I	Password(2) 1=18 v	al=Encrypted			
	> AVP: t=NAS-IN	P-Address(4) 1=6 v	a1=192.168.100.100			
	> AVP: t=Called	d-Station-Id(30) 1	=17 val=192.168.100.10	9		
	> AVP: t=Callin	ng-Station-Id(31)	1=13 val M.II.d1.11	-		
	> AVP: t=Proxy	-State(33) 1=25 va	1=466972737450726f7879	3d31302e32382	2e31372e313031	
	> AVP: t=Proxy	-State(33) 1=76 va	1=436973636f2053656375	7265204143533	37366535323735612	d396362302d313165632d63
	> AVP: t=NAS-P	ort-Type(61) l=6 v	al=Virtual(5)			
	> AVP: t=Tunne	1-Client-Endpoint(66) l=13 val=10.99.65.	53		

6. Om te bevestigen dat de Duo-verificatieproxy werkt, biedt Duo de tool <u>NTRadPing</u> om pakketten voor toegangsaanvragen en antwoorden met Duo te simuleren.

6.1 Installeer NTRadPing op een andere PC en genereer verkeer.

Opmerking: In dit voorbeeld wordt de 10.28.17.3 Windows-machine gebruikt.

6.2 Configuratie met de eigenschappen die op de configuratie van de ISE-straal worden gebruikt.

NTRadPing Test	t Utility			- 0	X
RADIUS Server/port: Reply timeout (sec.):	3	1812 Retries: 6	NTRadPing 1.5 - RADIUS S 1999-2003 Master Soft SpA - It http://www.dialwa	erver Testing taly - All rights sys.com/	f ool reserved
RADIUS Secret key: User-Name: Password:	Herry F il	C CHAP	MASTERSOFT*		
Request type: Additional RADIUS A	Authentication Request	•	RADIUS Server reply: See Support Service and a server is the server is a server of a set of the server is the ser	an prinz WZ-W Alfred (* 1 Angel (* 1 Angel (* 1 Angel (* 1) Angel	*2
Add Remove	Clear list Lo	 vad Save	Send Help	•	Close

6.3 Configureer de Duo Authenticatie Proxy Manager als volgt.



6.4. Navigeer naar uw NTRadPing tool en klik op **Verzenden**. U ontvangt een duo push-melding op het toegewezen mobiele apparaat.

INTRadPing Test	Utility			-		×
RADIUS Server/port:	10.28.17.107	1812	NTRadPing 1.5 - RADIUS Se @ 1999-2003 Master Soft SnA - It	erver Testi alu - All ric	ing Tool	nved
Reply timeout (sec.):	3 R	etries: 6	http://www.dialways.com/			
RADIUS Secret key:	!Mexvpn!17!		ms			
User-Name:	duovpn			U		
Password:	RECEIPTION	CHAP	MASTERSOFT	DIALWA	AYS	
Request type:	Authentication Request	0	RADIUS Server reply:			
Additional RADIUS A	thibutes:	Sending authentication request to server Transmitting packet, code=1 id=12 length no response from server (timed out), ner- received response from the server in 4000 reply podict eade=2 id=12 length=49 response: Access-Accept 	10.28.17.10 =46 =Memot (#1) D millisecot	17:1812 s		
	•	•				
Add Remove	Clear list Load.	. Save	Send Help	0	Clos	e

+	700 20.866684	10.28.17.3	10.28.17.107	RADIUS	88 Access-Request id=13,	Duplicate Request
÷	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					
>	thernet 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: 20202020202031363436393335333230					
	[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					

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.