و Active Directory عم يئانثلا لماكتلا نيوكت ءالمع ىلع لماوعلا ةيئانث ةقداصملل ISE AnyConnect/Remote Access VPN

تايوتحملا

مدقملا، قمدق ملا، متاب لمات ال تاب لمات ال تاب لمات مدخت مالا تانوكملا، مریزانی سل او قك شرار لی طی طختارا مس رل میں المیتالا اقدام میں لیا تانی وگت میں المات مرا لی المات مرا لی المات الممات المات المات المات المات المات المات المات المات المات المات

ةمدقملا

ءالمعل لماوعلا ةيئانث ةقداصمك ISE و AD عم جودزملا عوفدملا لماكتلا دنتسملا اذه فصي AnyConnect ب نيلصتملا ASA.

ةىساسألا تابلطتملا

تابلطتملا

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- (ASA) فيكتلل لباقلا نامألا زاهج ىلع RA VPN نيوكت
- ASA ىلع RADIUS نيوكت
- (ISE) ةيوەلا تامدخ كرحم •
- مدخ Active Directory (AD)
- ةيئانثلا تاقىبطتلا

ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملاو جماربلا تارادصإ ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست:

- Microsoft 2016 مداخ
- ASA 9.14(3)18
- ISE Server 3.0
- يئانث مداخ •
- يئانثلا ةقداصملا ليكوريدم •

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا ءاشنإ مت. تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألا عيمج تأدب رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ليغشتلا ديق كتكبش.

ويرانيسلاو ةكبشلل يطيطختلا مسرلا



لاصتالا ةيلمع

<u>Cisco ISE ل لماوعلا ةيئانث RADIUS ةقداصم</u>

- .1 ىلإ ةيساسألا ةقداصملا عدب مت .1 Cisco ISE.
- .يئانثلا ةقداصملا ليكو ىلإ ةقداصملا بلط Cisco نم ASA لسري .2
- .RADIUS وأ Active Directory ةيساسألا ةقداصملا مدختست .3
- مقر TCP ذفنم ربع يئانثلا نامألل هؤاشنإ مت يذلا يئانثلا ةقداصملا ليكو لاصتا .4 443.
- .يئانثلا نامألا ةمدخ ربع ةيوناث ةقداصم .5
- .ةقداصملا ةباجتسإ Duo ةقداصم ليكو ىقلتي .6
- .Cisco ISE لوصو حنم مت .7

:نيمدختسملا تاباسح

- ةقداصم ليكول حامسلل ليلد باسحك باسحلا اذه مدختسي :Active Directory لوؤسم . قيساسألا ةقداصملل Active Directory مداخب طبرلاب Duo
- رابتخإ مدختسم Active Directory
- ةيوناثلا ةقداصملل يئانث رابتخا مدختسم •

Active Directory تانيوكت

Active Directory. لاجم تامدخ عم اقبسم Windows مداخ نيوكت مت

کا ک فيضملا زاهجلا سفن یلع لمعي RADIUS Duo Proxy Manager ناك اذإ :ةظحالم Active ل فيضملا زاهجلا سفن یلع لمعي Active نم لك ليغشت مت اذإ .(NPS) ةكبشلا جهن مداخ راودأ فذح/تيبثت ةلازإ بجيف ،Directory يتمدخ .

مزلي ،Remote Access VPN يمدختسم ىلع مدختسملا ةيوهو ةقداصملل AD نيوكت قيقحتل ميقلا نم ليلق ددع رفوت.

نيوكتلا ءارجإ ةيناكمإ لبق Microsoft مداخ ىلع اهعيمجت وأ ليصافتلا هذه عيمج ءاشنإ بجي و ASA ةقداصم ليكو مداخ ىلع

:يە ةيسيئرلا ميقلا

- مسا وه مسا وه اذه . لاده نيوكتلا ليلد يف .مداخلا لاجم مسا وه اذه .لاجملا مسا لاجمل.
- مدختسملا FQDN وأ IP ناونع .(FQDN) لماكلاب لەؤملا لاجملا مسا/مداخلل IP ناونع ليكو لخاد DNS مداخ نيوكت بجي ،FQDN مادختسا مت اذإ .Microsoft مداخ ىلإ لوصولل ASA لحل ةيئانثلا ققداصملاو ASA

ميقلا هذه نوكت ،اذه نيوكتلا ليلد يف agarciam.cisco (الماتي الحلامي المتي عندان العلي العلي الميل الميل الميل ال

- و LDAP مدختسي ،يضارتفا لكشب .ةمدخ LDAP لا ب لمعتسي ءانيملا .مداخلا ذفنم SSL (LDAPs ذفنم TCP 636. دفنم STARTTLS و ،LDAP و ،TCP لا 889 CP
- قدصملا عجرملا نوكي ،STARTTLS وأ LDAP مادختسإ ةلاح يف .رذجلا قدصملا عجرملا ابولطم LDAPs ةطساوب ةمدختسملا SSL ةداهش عيقوتل مدختسملا رذجلا.
- ليكو مداخ لبق نم مدختسملا باسحلا وه اذه .رورملا ةملكو ليلدلا مدختسم مسا نع ثحبلاو نيمدختسملا ةقداصمو LDAP مداخب طبرلل يئانثلا ةقداصملا تاعومجملاو نيمدختسملا.
- ليكول قالطنالاا ةطقن وه يساسألاا DN). DN (العام محملاو ةدعاقل لزيمملا مسالا ل لوقي وهو Duo ةقداصم عن مدختسملا نع ثحبلاا أدبي نأ Active Directory ل لوقي وهو Duo ةقداصم

ةيساسألا DN ةكبشك agarciam.cisco رذجلا لاجملا مادختسإ متي ،اذه نيوكتلا ليلد يف

.Duo-users يه ةعومجملاب ةصاخلا DN ةكبشو

يف Windows ةنوقيأ ىلإ لقتنا ،Windows Server ىلع ،ديدج يئانث مدختسم ةفاضإل .1 ةروصلا يف حضوم وه امك ،ةيرادإلا Windows تاودأ قوف رقناو راسيلا لفسأ.



2. كل لقتن Sctive Directory Users and Computers. يل لقتنا Active Directory Users and Computers. دلجم ىل لقتناو لجمل رايخ عيسوتب مق

Users.

.ةيوناثلا ةقداصملل فده ةعومجمك Duo-Users مادختسإ متي ،اذه نيوكتلا لاثم يف

i∰ ⊇ = = File Home Share	Shortcut Tools Administrative Tool	ls -			×	
← → · ↑ 10 × Con	trol Panel > System and Security > Administra	tive Tools			Active Directory Users and Computers -	×
Ourick access Desktop Downloads Pictures Pictures System32 Downloads Downloads Downloads Downloads Downloads Downloads Downloads Downloads Downloads	trol Panel » System and Security » Administra Name Attive Directory Administrative Center Active Directory Domains and Trusts Active Directory Domains and Trusts Active Directory Meddel 644 Windows Po Active Directory Users and Computers Active Directory Users and Computers Active Directory Users and Computers Active Directory Users and Computers Computer Management Computer Management Computer Management Connection Manager Administration Kit Dirk Cleanup Dirk Cleanup Monto Composition Computers	we Tools Date modified 7/16/2016 6:33 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 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 Shortcut Shortcut	Size 2 KB 2 KB 2 KB 2 KB 2 KB 2 KB 2 KB 2 KB	■ Active Unectory Users and Computers File Action Unectory Users and Computers ■ Active Unectory Users and Computers ■ Active Unectory Users and Computers ■ Swed Queries ■ Swed Queries ■ Demain Controllers ■ Demain Controllers ■ Demain Controllers ■ Provide Directory Users and Computers ■ Demain Controllers ■ Demain Controllers	on be
Music Pictures Videos Local Disk (C:) DVD Drive (D:) SSS.; Network	Event Viewer Group Policy Management Group Policy Management Sinternet Information Services (IIS) Manager Gost Initiator Local Security Policy Microsoft Azure Services OBBC Data Sources (42-bit) OBBC Data Sources (42-bit)	7/16/2016 6:18 AM 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 6:18 AM	Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut	2 KB 2 KB 2 KB 2 KB 2 KB 2 KB 2 KB 2 KB	Comain Com. Security Group All domain controllers i Comain Gues. Security Group All domain guests Comain Users Scurity Group All domain users Comain Users Scurity Group All domain users Comain Users Scurity Group Designated administrato Controprise K Security Group Members of this group Comain Users Scurity Group Members of this group	~

.ةروصلا يف حضوم وه امك ،مدختسم < ديدج ددحو Users دلجملا قوف نميألا سواملا رزب رقنا .3

Active Directory Users and Comp	outers			-	×
File Action View Help					
(+ +) 🖄 🚾 🔏 🛄 🗶 🖫	0 🗟 🗟 🖬	1 🙎 🐮 🗊 🦷	1 🔟 🗟		
Active Directory Users and Com Saved Queries Saved Queries Save	Name Administrator agarciam alanad alanduo Allowed RO Cert Publish 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	> S Enterprise Enterprise	Computer Contact Group InetOrgPerson msDS-KeyCreden msDS-ResourcePr msDS-ShadowPri msImaging-PSPs MSMQ Queue Ali Printer	tial ropertyList ncipalContainer		~
Create a new object		User 🗲			
		Shared Folder			

ل رقناو ديدجلا مدختسملا اذهل ةيوهلا تامس نييعتب مق ،ديدج نئاك مدختسم ةذفان يف .4 ةروصلا يف حضوم وه امك ،يلاتلا.

New Object - User	×	
Create in: agarciam.cisco/Users	0	n
First name: duovpn Initials:	3C	. С
Last name:		
Full name: duovpn	s	ir
User logon name:	s	0
duovpn @agarciam.cisco ~	.c	
User logon name (pre-Windows 2000):	si	ir ir
AGARCIAM\ duovpn	nt	ts
	e	d
	sti	a' n
< Back Next > Cano	iii	n

تامولعم نم ققحتلا درجمب ءاەنإ مث ،يلاتلا قوف رقناو رورملا ةملك ديكأتب مق .5 مدختسملا.

New Object - User	×
Create in: agarciam.cisco/Users	0
Password:	3C
Confirm password:	
User must change password at next logon	s
User cannot change password	s
Password never expires	c
Account is disabled	s
	n
	e
	st
< Back Next > C	ancel ai

ددحو اەقوف نميألا سواملا رزب رقنا ،ةنيعم ةعومجم ىلا ديدجلا مدختسملا نييعتب مق .6 ةروصلا يف حضوم وہ امك ،ةعومجم ىلا ةفاضا

Active Directory Users and Comp	puters				-		×
File Action View Help							
(+ +) 🖄 🔟 🦌 🗓	i 🖬 📑 🖬 🖬	1 🕺 🔌 🛍 🦷	' 🗾 🔍				
Active Directory Users and Com Saved Queries Saved Queries Builtin Computers Solution ForeignSecurityPrincipal: Managed Service Accour Users	Name Administrator agarciam alanad alanduo Allowed RO Cert Publish Cloneable D Cloneable D Cloneable D DefaultAcco DefaultAcco Denied ROD DnsUpdateP Domain Ad Domain Ad Domain Con Domain Con 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 DNS clier Designato All works All doma All doma	on account 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 ed administrato tations and ser in controllers i in guests in users			~
< >	Enterprise	Add to a group		d administrato of this group			~
Allows you to add the selected object	ts to a group yo	Disable Account				1	

.ءامسألا نم ققحتلا رقناو ةبولطملا ةعومجملا مسا بتكا ،تاعومجملا ديدحت ةحول يف .7

قفاوم قوف رقناو ةئفلا قباطي يذلا مسالا ديدحتب مق مث.

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

8. لاثمك دنتسملا اذه ىلع ەمادختسا متي يذلا مدختسملا وه اذه.

ةيئانثلا تانيوكتلا

1. لوؤسم لخدم ىلإ لوخدلا ليجستب مق

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

مسا بتكاو مدختسم ةفاضإ قوف رقنا ،Users ىلإ لقتنا ،ىرسيلا ةيبناجلا ةحوللا يف.2 .مدختسم ةفاضإ قوف رقنا مث ،Active Domain يف مدختسملا مسا قباطي يذلا مدختسملا

	 Search for users, groups, a 	applications, or devices
Dashboard	Dashboard > Users > Add Use	er
Device Insight	Add User	
Policies	Most applications allow users	to enroll themselves after they complete primary authentication.
Applications	Learn more about adding use	rs 🗹
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

ةيرورضلا تامولعملا لك ألما ،ديدجلا مدختسملا ةحول يف .3.

Policies	Uashboard > Users > duovph		
Applications	duovpn		Logs Send Enrollment Email
Single Sign-On			
Users Add User Pending Enrollments Bulk Enroll Users	Username	duovpn	
Import Users Directory Sync Bypass Codes Groups	Username aliases	+ Add a username alias Users can have up to 8 aliases. Optionally, you may choose to reserve using an alias number for a specific alias	
Endpoints		(e.g., Username alias 1 should only be used for Employee ID).	
2FA Devices Trusted Endpoints	Full name	test <u>xpn</u> user	
Trust Monitor	E		
Reports	Email	.com	
Settings Need Help? Chat with Tech Support Cf Email Support Call us at 1-855-386-2884 Versioning Core Authentication Service: D235.6 Admin Panel: D235.6	Status	 Active 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*	Groups	You don't have any editable groups. Add one. Groups can be used for management, reporting, and policy. Learn more about groups C	
Deproyment ID DUO63 C Helpful Links Documentation C User Guide C Knowledge Base C	Notes	For internal use.	

.ةيوناثلا ةقداصملا ةقيرط ددح ،مدختسملا ةزهجأ تحت .4

،ةلومحملا ةزهجألل يئانثلا عفدلا بولسأ مادختسإ متي ،دنتسملا اذه يف :ةظحالم 🔌 فتاه زاهج ةفاضإ مزلي كلذل.

فتاه فيضي ةقطقط.

hones u may rearrange the phones by dragging and dropping in the table. Learn more about activating a replacement phone [3]. This user has no phones. Add one.	Add Phone
This user has no phones. Add one.	
	\smile
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

.فتاه ةفاضإ قوف رقناو مدختسملا فتاه مقر بتكا .5

Dashboard > Users > duovpn > Add Phone

Add Phone



.ديدجلا مدختسملا قوف رقناو Users ىلإ لقتنا ،ىرسىلا Duo ةرادإ ةحول يف .6

Dashboard	Dashboard > Users						
Device Insight	lleore			Director	Svnc Import Lies	are Bulk Enroll Lleare	Add Llear
Policies	03615			Director	y cyne i' import oad	STATE DUR EINON COOLS	
Applications	i You have users w	ho have not activated Du	o Mobile. Click here to send them a	ctivation links.			
Single Sign-On	Need to activate	a replacement phone? Le	arn more about Reactivating Duo M	obile 🖸.			
Users 🔶							
Add User	5	0	2	1	0	0	
Pending Enrollments	Total Users	Not Enrolled	Inactive Users	Trash	Bypass Use	ers Locke	d Out
Bulk Enroll Users							
Import Users	Select (0) ~ ···				Export ~	Q Search	
Directory Sync							
Bypass Codes		News	Core I	Dhanna	Teleses	Charles Land Land	-
Groups	Username 🔺	Name	Email	Phones	Tokens	Status Last Log	in
Endpoints				1		Active Mar 8, 2	2022 6:50 PM
2FA Devices				1		Active Mar 5. 2	2022 7:04 PM
Trusted Endpoints							
Trust Monitor	-			1		Active Never a	uthenticated
Reports	duovpn).com	1		Active Never a	uthenticated
Settings			o.com	1		Active Mar 5, 2	2022 7:16 PM
Need Help? Chat with Tech Support []							

💊 رايخ ديدحت كنكمي ،ةظحللا هذه يف كفتاه ىلإ لوصولا ةيناكمإ مدع ةلاح يف :ةظحالم ينورتكلإلا ديربلا.

. Duo Mobile طيشنت قوف رقناو فتاوهلا مسق ىلإ لقتنا.7

Phones You may rearrange the phones by dragging and dropping in the table. Learn more about activating a replacement phone C.						Add Phone
Alias	Device	Platform	Model	Security Warnings		
phone1	1000	Android 10	$(a,b,b) \in \mathcal{A}^{n}$	🗸 No warnings	Activate Duo Mobile	Î

.لقنتلا ءانثأ Duo طيشنت زمر ءاشنإ قوف رقنا .8

	 Search for users, groups, ap 	oplications, or devices
Dashboard	Dashboard	Activate Duo Mobile
Device Insight Policies	Activate Duo	Mobile
Applications	This form allows you to genera mobile device or authenticate v	te a new activation code for this phone's Duo Mobile appli via Duo Push.
Single Sign-On	Note: Generating an activation	code will invalidate any existing Duo Mobile credentials fo
Groups	Phone	a la secon
Endpoints		
2FA Devices Phones	Expiration	24 hours ~ after generation
Hardware Tokens WebAuthn & U2F		Generate Duo Mobile Activation Code

كديرب ناونع بتكا ،ينورتكلإلا ديربلا ربع تاميلعتلا يقلتل ينورتكلإلا ديربلا ددح .9 ينورتكلإلا ديربلا ربع تاميلعتلا لاسرا قوف رقناو ينورتكلإلا.

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 1760 Mili 1966.
Send links via	SMS Email
Email	ag i miner line vers a ver

.ةروصلا يف حضوم وه امك ،تاميلعتلا نمضتي اينورتكلإ اديرب ىقلتت .10

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 +

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. زمر مادختسإ ددح مث ،ةفاضإ قوف رقناو لومحملا كزاهج نم Duo Mobile قيبطت حتفا تاداشرإلاب صاخلا ينورتكلإلا ديربلا نم زمرلا صحفاو.

. Duo Mobile قيبطت ىلإ ديدج مدختسم ةفاضإ متت

يئانثلا ةقداصملا ليكو نيوكت

💊 سفن ىلع "يئانثلا ةقداصملا ليكو ريدم" تيبثت متي ،دنتسملا اذه يف :ةظحالم Active Directory مداخ مي يذلا ا

2. قيبطت ةيامح قوف رقناو تاقيبطتال يلإ لقتنا، Duo ةرادإ ةحول يف.



3. نع ثحبا ،ثحبالا طيرش ىلع Cisco ISE RADIUS.

Pro	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 C Protect				
altalta cisco	Cisco ISE RADIUS	2FA	Documentation D Protect				

4. جاتحت .تاقىبطتالا ةجمرب ةەجاو فىضم مساو ،ىرسالا خاتەمالاو ،لماكتالا خاتەم خسنا قۇداصمالا لىكو نىوكتال تامولغمالا ەذە يال 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

~



5. ليمع نم لكل نيوكتلا لمكأو Duo Authentication Proxy Manager قيبطت ليغشتب مق Active Directory مداخو ISE Radius قوف رقناو ISE Radius مداخو

اءاطخألاا حيحصت بيوبتلاا ةمالع ىلإ عجرا ،احجان ةحصلا نم قوّحتلا نكي مل اذإ :ةظحالم 📎 كلذل اقفو ححصو ليصافتلا يلع لوصحلل.

Duo Authentication Proxy Manager			- 🗆 ×
Authentication Proxy is running	Up since: 3/5/2022, 9:23:04 AM	Version: 5.6.0 date your Authentication Proxy	Restart Service Stop Service
Validation passed Configuration has passed validation and	d is ready to be saved		
Configure: authproxy.cfg	Unsaved 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= First 24 search_dn=DC=agarciam,DC=cisco 25 [26 [radius_server_auto] 27 ikey=Untrimining[1] 28 skey=K0m27rt8].77.101 29 api_host=api_sfraction.climate.unit 29 radius_ip_1=10.28.17.101 31 radius_secret_1=Wmmpn117! 32 failmode=safe 33 client=ad_client 34 port=1812 35 36 Vandate Save </pre>	g. [ad_client2]) trator ml/T mlVQpq9990Ccdp yS Kem	Running The Duo Authentic several minutes [info] Testing section ' [info] {'debug': 'True', 'log_max_files': 'log_max_size': 'test_connectivi [info] There are no conf [info]	<pre>station Proxy Connectivity Tool. This may take main' with configuration: '10', '20971520', ty_on_startup': 'true'} figuration problems</pre>

Cisco ISE تانيوكت

ISE. لوؤسم ةباوب ىلإ لوخدلا لجس .1

،ةكبشلا دراوم قوف رقنا مث ،ةرادإلا ىلإ لقتناو Cisco ISE بيوبتلا ةمالع عيسوتب مق. مداوخ قوف رقناو .

Cisco ISE -	Q What page are you looking	lor?		
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		Network Resources Network Devices Network Device Crown Network Device Prof External RADIUS Server Sequence NAC Managers	iles vers liencos
	Health Checks Backup & Restore		External MDM Location Services	

.ةفاضإ قوف رقنا ،ةيجراخلا RADIUS مداوخ بيوبتلا ةمالع يف .3

E Cisco ISE Administration · Network Resources					
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	
External RADIUS Servers					
	🗍 Duplicate 🍵 Delete				
Name Name:	Currently Sorted	Description			

4. ليكو ريدم) Duo Authentication Proxy Manager يف مدختسملا RADIUS نيوكتب غارفلاا ألما. لااسرا قوف رقناو (ةقداصملا.

Network Devices Netwo	ork Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	NAC Managers	External MDM	More
* Name	DUO_NEW ┥						
Description							
			R				
* Host IP	10.28.17.107						
* Shared Secret	······· +	Show					
Enable KeyWrap							
* Key Encryption Key		Show					
 Message Authenticator Code Ke 	Зу	Show					
Key Input Format	o ascii 🔿 hexai	DECIMAL					
* Authentication Port	1812	(Valid Range 1 to 6	5535)				
* Accounting Port	1813	(Valid Range 1 to 6	5535)				
* Server Timeout	5	Seconds (Valid Ra	nge 1 to 120)				
* Connection Attempts	3	(Valid Range 1 to 9	9)				
Radius ProxyFailover Expiration	300	(valid Range 1	to 600)				

.ةفاضإ قوف رقناو RADIUS مداخ تالسلست بيوبتلا ةمالع ىلإ لقتنا.

■ Cisco ISE	Administration • Network Resources						
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences			
For Policy Export go to Adm	erver Sequence	S Policy Export Page		1			

.لاسرا قوف رقنا ،ديدجلا يجراخلا RADIUS مداخ نييعتب مقو لسلستلا مسا ددح .6

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



جەنلا تاعومجم قوف رقناو ،جەنلا ىلإ تامولعملا ةحول ةمئاق نم لقتنا .7



كلذل ،تالاصتالا ةفاكل يئانث لسلست قيبطت متي ،دنتسملا اذه يف :ةظحالم 📎 .تابلطتملا بسح جەنلا نييعت فلتخي نأ نكمي .يضارتفالا جەنلا مادختسإ متي

Policy Sets					Reset Policyset H	litcount
🕂 Statu	s Policy Set Name	Description	Cor	nditions	Allowed Protocols / Server Sequence	Hits
Q Sear	ch					
0	ar 219		Ŧ	Radius-User-Name EQUALS isevpn	Default Network Access 🛛 🖂 +	3
0	14.1			Radius-NAS-Port-Type EQUALS Virtual	DUO_Sequence	22
0	Default	Default policy set			Default Network Access 🛛 🔿 +	0
	1				ΞQ	
	1				Allowed Protocols	eset
					Default Network Access	
					DUO_NEW	
					DUO Sequence	

Cisco نم ASA RADIUS/ISE نيوكت

قوف رقنا مث ،نيوكتلا ىلإ لقتنا ،AAA مداوخ تاعومجم نمض ISE RADIUS مداخ نيوكتل .1 AAA مداوخ تاعومجم ددحو ،AAA/نيمدختسملا مسق عيسوتب مقو ،ةزهجألا ةرادإ

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 AAA Server Group Server Group ISE LOCAL ad-agarciam	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		

ثبلاو لابقتسالا ةطقنب صاخلا فيضملا مسا ددح .يصخشلا رتويبمكلا زاهج ىلع ةقداصملل هؤاشنإ مت يذلا مدختسملا مادختساب لوخدلا لجسو VPN ASA ب ةصاخلا قفاوم قوف رقناو ،ةيئانثلا ةيوناثلا

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

- ددحملا Duo Mobile زاهج ىلع Duo عفد مالعإ تيقلت دقل .2.
- .ةقفاوملا قوف رقناو Duo Mobile App مالعإ حتفا .3





.لاصتالا ءاشنإو ،راعشلا لوبق





اهحالصإو ءاطخألا فاشكتسا

اهحالصإو نيوكتلا ءاطخأ فاشكتسال اهمادختسا كنكمي تامولعم مسقلا اذه رفوي. لشفلاو أطخلا بابسأ ضرعت ءاطخأ حيحصت ةادأ عم Duo Authentication Proxy يتأي.

💊 يف ةيلاتلا تامولعملا نيزخت متي :ةظحالم C:\Program Files\Duo Security Authentication Proxy\log\Connectivity_tool.log.

-		5	1	 	
υ	I	ì	i	п	п
_	-		-	 -	

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]										
	Testing section 'ad_client' with configuration:									
[info]	Testing section 'ad_client' with configuration:									
[info] [info]	Testing section 'ad_client' with configuration: {'debug': 'True',									
[info] [info]	Testing section 'ad_client' with configuration: {'debug': 'True', 'host': '10.28.17.107',									
[info] [info]	Testing section 'ad_client' with configuration: {'debug': 'True', 'host': '10.28.17.107', 'search_dn': 'DC=agarciam,DC=cisco',									
[info] [info]	Testing section 'ad_client' with configuration: {'debug': 'True', 'host': '10.28.17.107', 'search_dn': 'DC=agarciam,DC=cisco', 'service_account_password': '*****',									
[info] [info]	<pre>Testing section 'ad_client' with configuration: {'debug': 'True', 'host': '10.28.17.107', 'search_dn': 'DC=agarciam,DC=cisco', 'service_account_password': '******', 'service_account_username': 'Administrator'}</pre>									

```
[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'}
[info]
       The LDAP Client section has no connectivity issues.
[info]
[info] Testing section 'radius_server_auto' with configuration:
[info] {'api_host': 'asi_adicate dissecurity.cmp',
         'client': 'ad_client',
         'debug': 'True',
         'failmode': 'safe',
         'ikey': ""The conversion of the second second
         '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. نيوكت يف لحلل لباق ريغ FQDN/Hostname نيوكت يف لحلل لباق ريغ Active نيوكت يف لحلل لباق ريغ 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. كلع Active Directory مدختسمل ةحيحص ريغ رورم ةملك Administrator ىلع



ءاطخألا حيحصت

[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>4</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.

ئطاخ ساسأ لاجم .3



ءاطخألا حيحصت



ةحيحص ريغ RADIUS ةميق .4

ءاطخألا حيحصت

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

5. لوصولا بلط مزح لسري ISE مداخ نأ نم ققحت.

*Ethernet0

Fil	e Edi	t Viev	v Go	Capture	Analyze	Statistics	Telephony	Wir	reless	Tools	Help			
A		50			۹ 👄 🕫) 🕾 🖗	£ 🗐 🔳	Q,	୍	A 🖽				
	radus													
No.		Time		Source		1	Destination			Protocol	Length	Info	<u> </u>	
	1511.	. 6020	.521457	10.2	8.17.101		10.28.17.10	97		RADIUS	5 877	Access-Reque	st j- 31	
4	1513	. 6024	.344735	10.2	8.17.107		10.28.17.10	91		RADIUS	5 191	Access Accep	rt id=31	
>	Frame	15111	15: 877	bytes o	on wire ()	7016 bit:	s), 877 byt	es c	aptur	ed (701	6 bits)	on interface	\Device\NPF	{CA092CEE-5
>	Ether	net II	, Src:	Where	b3:a4:2f	(00:50:5	56:b3:a4:21), D	st: V	Mware_b	3:b4:3e	(00:50:56:b3	:b4:3e)	
>	Inter	net Pr	otocol	Version	4, Src:	10.28.17	7.101, Dst:	10.	28.17	.107		-		
>	User	Datagr	am Pro	tocol, S	inc Port:	42022, 0	Ost Port: 1	812						
~	RADIU	S Prot	tocol											
	Co	de: Ac	cess-R	equest (1)									
	Pa	cket i	dentif	ier: 0x1	f (31)									
	Le	ngth:	835											
	Au	thenti	cator:	38a28ca	3ca6bbc26	51819c530	4b1be6e3							
	- 11	he nes	ponse	to this	request i	is in fra	me 151332]							
	✓ At	tribut	e Valu	e Pairs										
	>	AVP:	t=User	-Name(1)	l=8 val=	duovpn	-							
	>	AVP:	t=User	-Passwor	d(2) l=18	3 val=Enc	rypted							
	>	AVP:	t=NAS-:	IP-Addre	ss(4) l=6	5 val=192	.168.100.1	66						
	>	AVP:	t=NAS-I	Port(5)	1=6 val=3	44064								
	>	AVP:	t=Call	ed-Stati	on-Id(30)	1=17 va	1=192.168.	100.	100					
	2	AVP:	t=Call:	ing-Stat	ion-Id(31	l) 1=13 v	al M. H. d							
	>	AVP:	t=Prox	y-State(33) 1=25	val=4669	7273745072	6f78	793d3	1302e32	382e313	72e313031		
	2	AVP:	t=Prox	y-State(33) 1=76	val=4369	73636f2053	6563	75726	5204143	5337366	535323735612d	396362302d31	3165632d63_
	>	AVP:	t=NAS-I	Port-Typ	e(61) 1=6	val=Vir	tual(5)							
	2	AVP:	t=Tunn	el-Clien	t-Endpoir	nt(66) 1=	13 val=10.	99.6	5.53					

6. بلط مزح ةاكاحمل <u>NTRadPing</u> ةادألاا Duo رفوي ،يئانثلاا ةقداصملا ليكو مداخ لمع ديكأتل مادختساب ةباجتسالاو لوصولا

.تانايبلا رورم ةكرح ءاشنإو فلتخم رتويبمك ىلع NTRadPing تيبثت 6.1

📎 ناهج مادختساٍ متي ،لاثملا اذه يف :ةظحالم Windows 10.28.17.3.

ISE Radius. نيوكت يف ةمدختسملا تامسلا مادختساب نيوكتلا 6.2

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 il	ms los
User-Name: duovpn	
Password: CHAP	MASTERSOFT DIALWAYS
Request type: Authentication Request	RADIUS Server reply:
Additional RADIUS Attributes:	See Segmethand and appendix server 19 20-22 10222 Internation 2 and 0 colors" (vol) in ear with the statement of the school serve should be the school which is the school server in the script (a) mathemetic server in the school of 27.00 - Homeson news, and the school of the school of the school server is the school of the school of the school server is the school of the school of the school of the school server is the school of the schoo
Add Remove Clear list Load Save	Send Help Close

6.3 يلي امك Duo Authentication Proxy Manager نيوكتب مق

[radius_server_auto]
ikey=****
skey=Jac3
api_host=ari_nd7c172n.chmarch_rity.com
radius_ip_1=10.28.17.101
<pre>radius_secret_1=!Mexmunt17!</pre>
radius_ip_2=10.28.17.3
<pre>radius_secret_2=!Mex 7!</pre>

ىلع يئانثلا عفدلاب اراطخإ ىقلتت .لاسرإ قوف رقناو NTRadPing ةادأ ىلإ لقتنا .6.4 .نيعملا لومحملا زاهجلا

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-ottempt (#1) received response from the server in 4000 millisecords 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							

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما