Configure Duo Integration with Active Directory and ISE for Two-Factor Authentication on Anyconnect/Remote Access VPN Clients

Contents

 Introduction

 Prerequisites

 Requirements

 Components Used

 Network Diagram and Scenario

 Communication Process

 Active Directory Configurations

 Duo Configurations

 Cisco ISE Configurations

 Cisco ASA RADIUS/ISE Configuration

 Cisco ASA Remote Access VPN Configuration

 Texubleshoot

 Work Debugs

Introduction

This document describes Duo push integration with AD and ISE as Two-Factor Authentication for AnyConnect clients connected to ASA.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- RA VPN configuration on Adaptive Security Appliance (ASA)
- RADIUS configuration on ASA
- Identity Services Engine (ISE)
- Active Directory (AD)
- Duo applications

Components Used

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

• Microsoft 2016 Server

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Network Diagram and Scenario



Communication Process

Duo Two-Factor RADIUS Authentication for Cisco ISE

- 1. Primary authentication initiated to Cisco ISE.
- 2. Cisco ASA sends authentication request to the Duo Authentication Proxy.
- 3. Primary authentication uses Active Directory or RADIUS.
- 4. Duo Authentication Proxy connection established to Duo Security over TCP port 443.
- 5. Secondary authentication via Duo Security's service.
- 6. Duo authentication proxy receives authentication response.
- 7. Cisco ISE access granted.

User Accounts:

- Active Directory Admin: This is used as the directory account to allow the Duo Auth Proxy to bind to the Active Directory server for primary authentication.
- Active Directory test user
- Duo test user for secondary authentication

Active Directory Configurations

Windows server is pre-configured with Active Directory Domain services.

Note: If RADIUS Duo Auth Proxy Manager runs on the same Active Directory host machine, Network Policy Server (NPS) Roles must be uninstalled/deleted. If both RADIUS services run, they can conflict and impact performance.

In order to achieve AD configuration for authentication and user identity on Remote Access VPN users, a few values are required.

All these details must be created or collected on the Microsoft Server before configuration can be done on the ASA and Duo Auth proxy server.

The main values are:

- Domain Name. This is the domain name of the server. In this configuration guide, agarciam.cisco is the domain name.
- Server IP/Fully Qualified Domain Name (FQDN) Address. The IP address or FQDN used to reach the Microsoft server. If an FQDN is used, a DNS server must be configured within ASA and Duo Auth proxy to resolve the FQDN.

In this configuration guide, this value is agarciam.cisco (which resolves to 10.28.17.107).

- Server port. The port used by the LDAP service. By default, LDAP and STARTTLS uses TCP port 389 for LDAP, and LDAP over SSL (LDAPS) uses TCP port 636.
- Root CA. If LDAPS or STARTTLS is used, the root CA used to sign the SSL certificate used by LDAPS is required.
- Directory Username and Password. This is the account used by Duo Auth proxy server to bind to the LDAP server and authenticate users and search for users and groups.
- Base and Group Distinguished Name (DN). The Base DN is the point of departure for Duo Auth proxy and it tells the Active directory to begin the search for and authenticate users.

In this configuration guide, the root domain agarciam.cisco is used as the Base DN and Group DN is Duo-USERS.

1. In order to add a new Duo user, on Windows Server, navigate to Windows icon at the bottom left and click Windows Administrative tools, as shown in the image.



2. On Windows Administrative tools window, navigate to Active Directory Users and Computers.

On the Active Directory Users and Computers panel, expand the domain option and navigate to **Users** folder.

In this configuration example, Duo-USERS is used as the target group for secondary authentication.

→ - ↑ 🖄 > Con	trol Panel > System and Security > Administra	tive Tools			Active Directory Users and Comp	outers		– 🗆 ×
Convertes Convertes	trol Panel > System and Security > Administral Name Terminal Services Active Directory Administrative Center Active Directory Domains and Trusts Active Directory Stress and Services Active Directory Users and Services Active Directory Users and Computers Active Directory Directory Computers Active Directory Directory Computers Active Directory Directory Computers Active Directory Comp	tive Tools Date modified 7/16/2016 6/23 AM 7/16/2016 6/39 AM	Type File folder Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut	Size 2 KB 2 KB 2 KB 2 KB 2 KB 2 KB 2 KB 2 KB	Active Directory Users and Comp File Action View Help Active Directory Users and Com Saved Queries	Junters Administrator Janne Administrator Jagarciam Jeser Jagarciam Jeser Jagarciam Jeser	Description Built-in account for ad Members of this group c Members of this group t A user account manage Members in this group c DNS Administrators Gro DNS Administrators Gro DNS deministrators Gro	×
Downloads on Mac Music Pictures Videos Local Disk (C:) DVD Drive (D:) SSS_; Network	Dirak Cleanup Dirak Cleanup Dirak Dirak Dirak Event Viewer Jin Group Policy Management Jinternet Information Services (IIS) Manager Jinternet Information Local Security Policy Microsoft Azure Services Jintersoft Azure Services	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	۲	Domain Co Security Group Domain Con Security Group promain Con Security Group Domain Users Shurity Group Douglass Shurity Group proteprise A Security Group Interprise K Security Group	All overkstations and ser All domain controllers i All domain guests All domain users Designated administrato Members of this group Members of this group	×

3. Right click on the **Users** folder and select **New > User**, as shown in the image.

Active Directory Users and Comp	uters			-	×
File Action View Help		= 49 6. 0or m			
Active Directory Users and Com Saved Queries Saved Queries Save	Name Administrator agarciam alanad alanduo Allowed RO Cert Publish Coneable D	Type User User User User Security Group Security Group Security Group	Description Built-in account for ad Members in this group c Members of this group Members of this group t		^
Delegate Contr Find	rol :o D	User Security Group	A user account manage Members in this group c		
New All Tasks View Refresh Export List Properties	>	Computer Contact Group InetOrgPerson msDS-KeyCreden msDS-ResourcePr msDS-ShadowPri	tial ropertyList		
Create a new object	KEnterprise	msDS-ShadowPh msImaging-PSPs MSMQ Queue Ali Printer User	as ,		~
		Shared Folder			

4. On the New Object-User window, specify the identity attributes for this new user and click **Next**, as shown in the image.

New Object - User	×	
Create in: agarciam.cisco/Users	0	n
First name: duovpn Initials:	30	: с
Last name:		
Full name: duovpn	s	ir
	s	0
User logon name:	S	C
duovpn @agarciam.cisco ~	:0	C
Llees leese some (sm Windows 2000):	s	ir
User logon name (pre-windows 2000).	n	ir
AGARCIAM	nt	ls
	e	d
	— st	a
Z Back Next > Cance	, air	n
Cance	· air	n

5. Confirm password and click Next, then Finish once user information is verified.

New Object - User	×
Create in: agarciam.cisco/Users	0
Password:]
Confirm password:	
User must change password at next logon	s
User cannot change password	s
Password never expires	c
Account is disabled	s
	n
	nt
\sim	e
	st .
< Back Next >	Cancel
Account is disabled	ni ni ce st Cancel iii

6. Assign the new user to an specific group, right click it and select **Add to a group**, as shown in the image.

Active Directory Users and Comp	puters				×
File Action View Help					
🗢 🔿 🖄 📰 🔏 🖬 🗙 🛙	i 🖬 🗟 🖬	1 🗏 🐮 🕯 🦷	1 🗾 🐍		
Active Directory Users and Com Saved Queries Saved Queries Builtin Builtin Computers Solution ForeignSecurityPrincipal: Managed Service Accour Users	Name Administrator agarciam alanad alanad alanduo Allowed RO Cert Publish Cert Publish Cloneable D DefaultAcco DefaultAcco Denied ROD DnsUpdateP DnsUpdateP Domain Ad Domain Co Domain Co Domain Gue Domain Gue Domain Users duo2 DUO-USERS	Type User User User Security Group Security Group	Description Built-in 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 DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain users		*
	A Enterprise	Copy	d administrato		0.4
< >>	R Enterprise	Disable Account	of this group		~
Allows you to add the selected object	ts to a group yo				

7. On the Select groups panel, type the name of the desired group and click **Check names**.

Then, select the name that matches your criteria and click $\mathbf{Ok}.$

Select Groups	× _
Select this object type: Groups or Built-in security principals	iect Types
From this location:	:01
agarciam.cisco	ocations
Enter the object names to select (examples):	\frown
DUO-USERS	eck Names
	of t
Advanced OK	Cancel n t

8. This is the user that is used on this document as an example.

Duo Configurations

1. Log into your Duo Admin portal.

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

2.On the left side panel, navigate to **Users**, click **Add User** and type the name of the user that matches our Active Domain username, then click **Add User**.

DUO	Q Search for users, groups, a	pplications, or devices
Dashboard	Dashboard > Users > Add Use	r
Device Insight		
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

3. On the new user panel, fill in all the necessary information.

Policies	Uasnboard > Users > duovpn		
Applications	duovpn		Logs Send Enrollment Email
Single Sign-On			
Users	(i) This user has not en	olled yet. See our enrollment documentation II to learn more about enrolling users.	
Add User			
Pending Enrollments			
Bulk Enroll Users	Username	duovpn	
Import Users			
Directory Sync	Username aliases	+ Add a username alias	
Groupo		Users can have up to 8 aliases. Optionally, you may choose to reserve using an alias number for a specific alias	
Groups		(e.g., Username alias 1 should only be used for Employee ID).	
Endpoints			
2FA Devices	Full name	test von user	
Trusted Endpoints		LOO ARII DOO	
Trust Monitor			
Reports	Email	Com	
Settings			
	Status	Active Require multi-factor authentication (default)	
Need Help?			
Email Support		 Bypass Allow users to skip two-factor authentication and log in with only a password. Passwordless a 	authentication is not skipped.
Call us at 1-855-386-2884			
Versioning		Automatically deny access	
Core Authentication Service:		This controls the user's two-factor authentication process.	
Admin Panel:			
D235.6			
Read Release Notes	Groups	You don't have any editable groups. Add one.	
Account ID		Groups can be used for management, reporting, and policy. Learn more about groups C	
2910-6030-53			
Deployment ID DUO63 C			
Helpful Links	Notes		
Documentation C			
User Guide C		For internal use.	
Knowledge Base			

4. Under user devices, specify the secondary authentication method.

Note: In this document, Duo push for mobile devices method is used, so a phone device needs to be added.

Click Add Phone.

hones but may rearrange the phones by dragging and dropping in the table. Learn more about	Add Phone
This user has	no phones. Add one.
ndpoints	
This use	r has no devices.
lardware Tokens	Add Hardware Token
This user has no h	hardware tokens. Add one.
ypass Codes	Add Bypass Code
This user has no	bypass codes. Add one.

5. Type in the user phone number and click Add Phone.

Dashboard > Users > duovpn > Add Phone

Add Phone



6. On the left Duo Admin panel, navigate to Users and click the new user.

Dashboard	Dashboard > Users						
Device Insight				Disector	Core L Immedi		
Policies	Users			Directory	Sync 1 Import	USERS I DUIK ER	roli Osers Add Oser
Applications	You have users w	no have not activated Duo N	Nobile. Click here to send them a	ctivation links.			
Single Sign-On	Need to activate a	replacement phone? Learn	more about Reactivating Duo Me	obile 🗗.			
Users ┥							
Add User	5	0	2	1	0		0
Pending Enrollments	Total Users	Not Enrolled	Inactive Users	Trash	Bypass	Users	Locked Out
Bulk Enroll Users		_					
Import Users	Select (0) ∽ ····				Export 🗸	Q Search	
Bypass Codes							
Groups	Username 🔺	Name	Email	Phones	Tokens	Status	Last Login
Endpoints				1		Active	Mar 8, 2022 6:50 PM
2FA Devices				1		Active	Mar 5 2022 7:04 PM
Trusted Endpoints						710110	Mar 0, 2022 11041 M
Trust Monitor	•••••			1		Active	Never authenticated
Reports	duovpn).com	1		Active	Never authenticated
Settings			— — — o.com	1		Active	Mar 5, 2022 7:16 PM
Need Help? Chat with Tech Support []							

Note: In case you do not have access to your phone at the moment, you can select the email option.

7.Navigate to **Phones** section and click **Activate Duo Mobile**.

Phones You may rearrange	the phones by dragging and dro	pping in the table. L	earn more about activating a rej	blacement phone 다.		Add Phone
Alias	Device	Platform	Model	Security Warnings		
phone1	5 5 5 T	Android 10	1.00 × 10	√ No warnings	Activate Duo Mobile	Ê

8. Click Generate Duo Mobile Activation Code.



9. Select **Email** in order to receive the instructions via email, type your email address and click **Send Instructions by email**.

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 CAR THERE WAS
Send links via	 SMS €mail
Email	ay i mine il nove a con

10. You receive an email with the instructions, as shown in the image.

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:



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 the Duo Mobile App from your mobile device and click **Add**, then select **Use QR code** and scan the code from the instructions email.

12. New user is added to your Duo Mobile App.

Duo Auth Proxy Configuration

1. Download and Install Duo Auth Proxy Manager from Cisco Duo Authentication

Note: In this document, the Duo Auth Proxy Manager is installed on the same Windows Server that hosts Active Directory services.

2. On the Duo Admin Panel, navigate to Applications and click Protect an Application.

Due	Q. Search for users, groups, applications, or devices	4-4- 1000	Cisco ID: 31/ 8-6008-65	alan 🗸
Dashboard Device Insight	Dashboard > Applications Applications		Protect an App	
Applications	_			\mathbf{X}
Single Sign-On Users	Manage your update to the new Universal Prompt experience, all in one place.	0		×
Groups Endpoints	Get Started Get More Information	0		
2FA Devices Trusted Endpoints		Export ~	Q Search	

3. On the search bar, look for Cisco ISE Radius.

Protect an Application

0	Add an application that you'd like to protect with Duo two-factor a You can start with a small "proof-of-concept" installation — it take Documentation: Getting Started C Choose an application below to get started.	authentication. es just a few minutes, and	d you're the only one that will see it, until you decide to add others.
ise Applicat	tion	Protection Type	
Cakamai	Akamai Enterprise Application Access	2FA	Documentation C ⁴ Protect
ahaha cisco	Cisco ISE RADIUS	2FA	Documentation D Protect

4. Copy the Integration key, Secret key, and the API Hostname. You need this information for the Duo Authentication Proxy configuration.

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. Run the Duo Authentication Proxy Manager application and complete the configuration for both Active Directory client and ISE Radius Server and click **Validate**.

Note: If validation is not successful, refer to the debug tab for details and correct accordingly.

Tuo Authentication Proxy Manager			- 🗆 X
Authentication Proxy is running	Up since: 3/5/2022, 9:23:04 AM	Version: 5.6.0 pdate your Authentication Proxy	Restart Service Stop Service
Validation passed Configuration has passed validation and	is ready to be saved		
Configure: authproxy.cfg	Unsaved Changes	Output	
<pre>18 ; number to the section name (e.g) 19 20 [ad_client] 21 host=10.28.17.107 22 service_account_username=Administ 23 service_account_password= H=x11 24 search_dn=DC=agarciam,DC=cisco 25 26 [radius_server_auto] 27 ikey=Lint = Lint = Lint = Lint 28 skey=Y0+07x18ja7214H1g77i6.16644 29 api_host=api_aft4730.6047411; 30 radius_ip_1=10.28.17.101 31 radius_secret_1=Maximalif; 32 failmode=safe 33 client=ad_client 34 port=1812 35 36 Validate Save </pre>	j, [ad_client2]) trator .μr] hlv9pg9990°Ωdg AltCm	Running The Duo Authentication Proxy several minutes [info] Testing section 'main' with [info] {'debug': 'True', 'log_max_files': '10', 'log_max_size': '20971520', 'test_connectivity_on_start [info] There are no configuration p [info] [info] Testing section 'ad_client' [info] {'debug': 'True', 'host': '10.28.17.107', 'search_dn': 'DC=agarciam,D 'service_account_password': 'service_account_username': [info] There are no configuration p [info] [info] Testing section 'radius_serv [info] Testing section 'radius_serv	<pre>/ Connectivity Tool. This may take configuration: up': 'true'} oroblems with configuration: C=cisco', '*****', 'Administrator'} roblems rer_auto' with configuration: upcocyrity com! am how to configure the Authentication Proxy</pre>

Cisco ISE Configurations

1. Log into the ISE Admin portal.

2.Expand Cisco ISE tab and Navigate to Administration, then click Network Resources, and click External RADIUS Servers.



3. On External Radius Servers tab, click Add.

E Cisco ISE	Administration • Network Resources					
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences		
External R	ADIUS Servers		1			
	🗋 Duplicate 🍵 Delete					
Name Name:	Currently Sorted	Description				

4. Fill in the blank with the RADIUS configuration used in the Duo Authentication Proxy Manager and click **Submit**.

Network Devices Networ	k Device Groups Network	Device Profiles	External RADIUS Servers	RADIUS Server Sequences	NAC Managers	External MDM	More
* Name	DUO_NEW						
Description							
* Host IP	10.28.17.107						
* Shared Secret	······· +	Show					
Enable KeyWrap							
* Key Encryption Key	Sho	w					
* Message Authenticator Code Key	Sho	w					
Key Input Format	ASCII HEXADECIMAL						
* Authentication Port	1812	(Valid Range 1 to 655	35)				
* Accounting Port	1813	(Valid Range 1 to 655)	35)				
* Server Timeout	5	Seconds (Valid Range	e 1 to 120)				
* Connection Attempts	3	(Valid Range 1 to 9)					
Radius ProxyFailover Expiration	300	(valid Range 1 to	600)				

5. Navigate to **RADIUS Server Sequences** tab and click **Add**.



6. Specify the name of the sequence and assign the new RADIUS External server, click Submit.

RADIUS Server Sequences List > New RADIUS Server Sequence

RADIUS Server Sequence



\sim 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. Navigate from the Dashboard menu to **Policy**, and click **Policy Sets**.

Cisco ISE	Q. What page are you looking	ig for?	
Dashboard	Context Visibility	Operations Policy	Adm
Recent Pages Policy Sets	Policy Sets	Profiling	
External RADIUS Servers External Identity Sources	Posture	Client Provisio	alog
Network Device Profiles Live Logs	Policy Elements		
	Dictionaries Conditions		

8. Assign the RADIUS Sequence to the default policy.

Note: In this document, the Duo sequence to all of the connections is applied, so Default policy is used. Policy assignment can vary as per requirements.

Policy S	ets					Reset Reset Policyset H	itcount
(+) S	itatus	Policy Set Name	Description	Con	ditions	Allowed Protocols / Server Sequence	Hits
Q	Search						
	0	81.91N		Ŧ	Radius-User-Name EQUALS isevpn	Default Network Access $\overline{\mbox{\ \ s}} $	3
	0	i n 1		U	Radius-NAS-Port-Type EQUALS Virtual	DUO_Sequence	22
	0	Default	Default policy set			 Default Network Access $\ igodot \propto \ \wedge \ +$	0
		T				EQ	
		1				Allowed Protocols	eset
						Default Network Access	
						Proxy Sequence	
						DUO_Sequence	1.

Cisco ASA RADIUS/ISE Configuration

1. To configure ISE RADIUS Server under AAA Server groups, navigate to **Configuration**, then click **Device Management**, expand the **Users/AAA** section, and select **AAA Server Groups**.

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		

app on your PC device. Specify the hostname of the VPN ASA Headend and log in with the user created for Duo secondary authentication, and click **OK**.

.000	Sec	AnyConnect ure Mobility Client	cisco
	VPN: Please enter yo	ur username and passwo	rd.
	Cisco A	nyConnect 192.168	.100.100
	Please enter your	username and passwo	ord.
_	Group:		C
	msgstringESMEX	duovpn	-
	MEX-PASS	••••	
			Cancel OK

- 2. You received a Duo push notification on the specified user Duo Mobile device.
- 3. Open the Duo Mobile App notification and click **Approve**.





4. Accept the banner, and the connection is established.





Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Duo Authentication Proxy comes with a debug tool that displays error and failure reasons.

Work Debugs

Note: The next information is stored in C:\Program Files\Duo Security Authentication Proxy\log\connectivity tool.log.

Output

```
Running The Duo Authentication Proxy Connectivity Tool. This may take
        several minutes...
[info] Testing section 'main' with configuration:
[info] {'debug': 'True',
         'log_max_files': '10',
         'log_max_size': '20971520',
         'test_connectivity_on_startup': 'true'}
       There are no configuration problems
[info]
[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] There are no configuration problems
```

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

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

1. Connectivity issues, wrong IP, unresolvable FQDN/Hostname on Active Directory configuration.

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. Wrong password for Administrator user on Active Directory.



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>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.

3. Wrong Base Domain



Debugs



4. Wrong ikey RADIUS value

[radius_server_auto]
ikey=U_NUUOU_L_KHRNZ6EZ1
skey=Jacolini – I i i i i i i i i i i i i i i i i i
api_host=apl = 🗖 📲 🖬 🖬 🖛 🖜 ity.com
radius_ip_1=10.28.17.101
<pre>radius_secret_1=!Mexvpn!17!</pre>
failmode=safe
<pre>client=ad_client</pre>
port=1812

Debugs

	and a susception of the
[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. Verify ISE Server sends Access-Request packets.

*Ethernet0

Fil	e Ed	it Viev	v Go	Capture	Analyze	Statistics	Telephony	Wirel	less T	ools I	Help			
í.		ی ک		X C	۹ 👄 🕫	s 🗟 🖲	A 🗔 🔳	0,0	ର୍ ଭ୍	琵				
	radius													
No.		Time		Source		(Destination		8	Protocol	Length	Info	~	
	1511	. 6020	521457	10.28	3.17.101		10.28.17.10	97		RADIUS	877	Access-Requ	est j-31	
4	1513	_ 6024	.344735	10.28	3.17.107		10.28.17.1	91		RADIUS	191	Access Acce	pt id=31	
>	Fram	15111	5: 877	bytes o	n wire (7016 bits	;), 877 byt	es cap	ptured	(701	6 bits)	on interface	e \Device\NPF	{CA092CEE-5
>	Ethe	net II	, Src:	Where	b3:a4:2f	(00:50:5	6:b3:a4:21), Dst	t: VMb	are bi	3:b4:3e	(00:50:56:b)	3:b4:3e)	
>	Inte	rnet Pr	otocol	Version	4, Src:	10.28.17	7.101, Dst:	10.2	8.17.1	.07				
>	User	Datagr	am Pro	tocol, S	inc Pont:	42022, 0	ost Port: 1	812						
~	RADI	US Prot	ocol											
	C	ode: Ac	cess-R	equest (1)									
	P	acket i	dentif	ier: 0x1	f (31)									
	L	ength:	835											
	A	uthenti	cator:	38a28ca	3ca6bbc26	51819c530	4b1be6e3							
	- E	The res	ponse 1	to this	request i	is in fra	me 151332]							
	✓ A [*]	ttribut	e Valu	e Pairs										
	> AVP: t=User-Name(1) l=8 val=duovpn <													
	>	AVP:	t=User	Passwor	d(2) l=18	8 val=Enc	rypted							
	> AVP: t=NAS-IP-Address(4) l=6 val=192.168.100.100													
	>	AVP:	t=NAS-R	Port(5)	1=6 val=3	344064								
	>	AVP:	t=Call(d-Stati	on-Id(30)) l=17 va	1=192.168.	100.10	99					
	> AVP: t=Calling-Station-Id(31) l=13 val M.II.41.11													
	>	AVP:	t=Proxy	-State(33) 1=25	val=4669	7273745072	6f7879	93d313	02e323	82e3137	72e313031		
	>	AVP:	t=Proxy	-State(33) 1=76	val=4369	73636f2053	656375	572652	841435	53373665	5353237356120	1396362302d31	3165632d63
	>	AVP:	t=NAS-I	ort-Typ	e(61) 1=6	5 val=Vir	tual(5)							
	> AVP: t=Tunnel-Client-Endpoint(66) 1=13 val=10.99.65.53													

6. In order to confirm Duo Authentication Proxy server works, Duo provides the tool <u>NTRadPing</u> to simulate Access-request packets and response with Duo.

6.1 Install NTRadPing on a different PC and generate traffic.

Note: In this example, the 10.28.17.3 Windows machine is used.

6.2 Configure with the attributes used on ISE Radius configuration.

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: Harmar F i	ms l			
User-Name: duovpn				
Password: CHAP	MASTERSOFT DIALWAYS			
Request type: Authentication Request 💌 0	RADIUS Server reply:			
Additional RADIUS Attributes:	See Segmethand a serger of the server 32 2002 1022 2022 International consideration of the server of			
Add Remove Clear list Load Save	Send Help Close			

6.3 Configure the Duo Authentication Proxy Manager as follows.

[radius_server_auto]
ikey="http://www.setter.com/
skey=Jac3
api_host=ari_nd7c172n.chmarch_iii; com
radius_ip_1=10.28.17.101
<pre>radius_secret_1=!Meximu!17!</pre>
radius_ip_2=10.28.17.3
radius_secret_2=!Mex 7!

6.4. Navigate to your NTRadPing tool and click **Send**. You receive a Duo push notification on the assigned mobile device.

INTRadPing Test	t 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:	NOODOODOOK	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), new etternet (#1) received response from the server in 4000 millisecords reply packet code=2 id=12 length=48 response: Access-Accept 			
Add Remove	e Clear list Load	Save	Send Help Close			

115	700 201000004	10.20.17.5	10.20.17.107	RADIUS	oo Access-Request 10=15, Duplicate Request	
<u>م</u> ليه	737 22.184895	10.28.17.107	10.28.17.3	RADIUS	90 Access-Accept id=13 🚽	
1	Ecomo 700, 22 hutor	on wine (704 bits	> 99 buter cantured (704 hits) on	n interface \Davice\NDE {CA002CEE_EE28_4E04_0310_2DE23160DD60} id	٥
5	Ethernet TT Sect 1	Share b3.f2.72 (00	3-50-56-b3-f2-72) Det.	Whate back	h4.3a (00.50.56.h3.h4.3a)	•
5	Internet Destoral V	lansion A Sect 10	28 17 3 04+- 10 28 17	107	6413e (6613613610310413e)	
10	Uses Detraces Dest	version 4, Src. 10.	20.17.5, DSt. 10.20.17	.107		
1	user Datagram Proto	beol, are port: all	100, DST POPT: 1012			
Ť	KADIUS Protocol					
	Code: Access-Rec	quest (1)				
	Packet identifie	er: 0xd (13)				
	Length: 46					
	Authenticator: 2	2020202020203136343	36393335333230			
	[Duplicate Reque	est Frame Number: 5	32]			
	[The response to	o this request is i	in frame 737]			
	✓ Attribute Value	Pairs				
	> AVP: t=User-N	<pre>iame(1) l=8 val=duo</pre>	wpn			
	> AVP: t=User-P	assword(2) l=18 va	1=Encrypted			