DUO with Active Directory and Cisco ISE with WTI TACACS Client



Introduction

This document describes how to configure Duo push integration with Active Directory (AD) and Cisco Identity Service (ISE) as Two-Factor Authentication that connect to WTI Radius client.

Components used

- Windows Active Directory
- Duo
- Duo Authentication Proxy Manager
- Cisco ISE
- WTI TACACS client

Communication process

- 1. WTI makes an authentication request to Cisco ISE
- 2. Cisco ISE sends authentication request to the Duo Authentication Proxy
- 3. Duo Proxy sends a request to Active Directory
- 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 return to WTI with Access Accept + Radius attribute 41 and WTI permits the user access.

Active Directory Configurations

1. Navigate to Active Directory Users and Computers > Add new User and Password. In this example we created **duouser** account in active directory users and computers.

	Active Directory Users and Compute
File Action View Help	
🗢 🔿 📶 🤞 📋 🗙 🖾 🖬 🔝 🖏	\$ 1 7 D \$
Active Directory Users and Computers [ADC.wti-lab.com] Saved Queries Minute	Name Type Sadminuser User Salmin Security Group - Global
 ▶ and Admins ▶ and Block Hardware OU 	duouser User User Security Group - Global Security Group - Global
 ▷ Builtin ▷ Clients ▷ Computers ▷ DESKTOPS ▷ Demain Controllers ▷ ♂ dot1x ▷ GreignSecurityPrincipals 	Cuouser Properties User Published Certificates Member OF Password Replication Dial-in Object User Security Environment Sessions Remote control Security Group - Global Remote Desktop Services Profile COM+ Attribute Editor User General Address Account Profile Telephones Organization User logon name: User General User General General
 ▷ a Groups a Groups a Toepartment b LostAndFound b Microsoft Exchange Security Groups b Program Data b System b System b System b Users 	User @wti4ab.com User User logon name (pre-Windows 2000): User WTI-LAB\ duouser Logon Hours Log On To Unlock account Account options:
 Microsoft Exchange System Objects MTDS Quotas TPM Devices 	□ User must change password at next logon ^ ☑ User cannot change password _ ☑ Password never expires _ □ Store password using reversible encryption ~ Account expires _ ● Never _ ○ End of: _ Saturday _ March 4, 2023
	OK Cancel Apply Help

Duo configuration

1. Log in into your Duo Admin portal

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

DU O	Search for users, groups	s, applications, or devices
Dashboard	Dashboard > Users > Add	Jser
Policies	Add Usor	
Applications	Add USEI	to aproll themselves offer they complete primary authentication
Users	Learn more about adding u	sers C
Add User		
Pending Enrollments	Heername	duousor
Bulk Enroll Users	Username	
Import Users		Should match the primary authentication username.
Directory Sync		
Bypass Codes		
Groups		Add User
2FA Devices		

- 3. On the new user's panel, fill in the blank all the necessary information.
- 4. Under user devices specify the secondary authentication method. Click Add Phone

Phones fou may rearrange the phones by dragging and dropping in the table. Learn more about activating a replacement phone 🗗.	Add Phone
This user has no phones. Add one.	
Endpoints	
This user has no devices.	
Hardware Tokens	Add Hardware Token
This user has no hardware tokens. Add one.	
Bypass Codes	Add Bypass Code
This user has no bypass codes. Add one.	
NebAuthn & U2F	Add Security Key

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

Dashboard	>	Users	>	duovpn	>	Add Phone

Learn more a	about Activating Duo Mobile 다.
Туре	 Phone Tablet
Phone number —	Optional. Example: *+52 1 222 123 4567*
	Add Phone

Activate Duo Mobile

This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows 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. Alta - Antoli - Alta
Send links via	SMS Email
Email	ay malan ilin sen soon

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



9. You receive an email with the instructions, as show in the image



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

10. 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.

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

Duo Authentication Proxy Configuration

1. Download and Install Duo Auth Proxy manager from https://duo.com/docs/authproxy-reference.

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



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

Protect an Application		
Add an application that you'd like to protect with Duo two You can start with a small "proof-of-concept" installation Documentation: Getting Started 12 Choose an application below to get started.	p-factor authentication. — it takes just a few minutes, and you're the o	nly one that will see it, until you decide to add others.
ise Application	Protection Type	
Change Akamai Enterprise Application Access	2FA	Documentation 🖸 Protect
cisco Cisco ISE RADIUS	2FA	Documentation E Protect

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

Dashboard > Applications > Cisco ISE RADIUS 1

Cisco ISE RADIUS 1

Follow the Cisco ISE RADIUS instructions ☑.

Details

Integration key	t to characterize and the second of	Сору
Secret key	••••••W6ho	Сору
	Don't write down your secret key or share it with an	iyone.
API hostname	(p+10/00/2010/001007/00/0022)	Сору

5. Run the Duo Authentication Proxy manager application and complete the configuration for both Active Directory client ISE Radius server and click Validate.

Duo proxy config: authproxy.cfg

The Duo proxy config file should be on the machine you installed the Duo proxy program, at this file location:

Windows

C:\Program files\Duo Security Authentication Proxy\conf\authproxy.cfg

Linux

/opt/duoauthproxy/conf/authproxy.cfg



Below is sample configuration of authproxy.cfg

- Primary authenticator, Windows Active Directory Server is on 172.16.0.14
- Duo Authentication Proxy manager is on Windows Server **172.16.0.40**
- WTI Device is on 172.16.0.44
- Cisco ISE is on **172.16.0.49**

[ad_client] host=172.16.0.14 service_account_username=duouser service_account_password=duosecret search_dn=DC=wti-lab,DC=com security_group_dn=CN=DUO,OU=IT Department,DC=wti-lab,DC=com

Cisco ISE Configurations

Step 1: Create TACCAS profile and TACACS command set

To configure the profile, navigate to **Work Centers** > **Policy Elements**. On the left-hand side select Results and click the dropdown arrow.

Overview Identities	User	Identity Groups	Ext Id Sources	Networ	k Resources	Policy Elements
Conditions	>	TACACS I	Profiles			
Network Conditions	>					
Results Allowed Protocols	~	\mathcal{C} Refresh + Add	🗋 Duplicate 🗍	Trash \smallsetminus //	² Edit	
TACACS Command Sets		Name		Туре	Description	
TACACS Profiles		Default Shell Pr	ofile	Shell	Default Shell Profile	2
		Deny All Shell P	Profile	Shell	Deny All Shell Profi	le
		WLC ALL		WLC	WLC ALL	
		WLC MONITOR		WLC	WLC MONITOR	
		WTI Admin		Shell		
		WTI User		Shell		

Overview Identitie	es L	Jser Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets
Conditions	>	TACACS Profiles > WTI TACACS Profile	Admin			
Network Conditions	>	Nomo		-		
Results	~	WTI Admin				
Allowed Protocols TACACS Command Sets		Description				
TACACS Profiles						
		Task Attribute View	Raw View			
		Common Tasks				
		Common Task Type Sh	ell 🗸			
		~	Default Privilege	15	✓ (Select 0 to	o 15)
		~	Maximum Privilege	15	✓ (Select 0 to	o 15)

For WTI Admin access level with privilege level 15.

Privilege levels for the different access levels:

View Only – 0-4 User – 5-9 Superuser – 10-14 Admin – 15

Add a command set in TACACS Command Sets to permit all. Click Add from the top menu and fill out as below:

Overview	Identities	U	ser Identity Groups	Ext Id Sources	Network Resources	Policy Elements
Conditions		>	TACACS Command Set Command Set	s > PermitAllCommands		
Network Condition	s	>	Name			
Results		~	PermitAllCommand	ls	_	
Allowed Protocol TACACS Comma TACACS Profiles	s and Sets		Description			
					h.	
			Commands	at is not listed below		
			Permit any command th	at is not listed below	-	

Step 2: Create network Device

1. Navigate to Administrator > Network Resource > Network Device > Default Device Enable TACACS and define shared secret.

Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server	r Sequences	NAC Managers	External MDM	Location
	Enable RAI	DIUS						
Network Devices	RADIUS UDP Se	ettings						
Default Device	* Shared Secret	t			Show			
Device Security Settings			_					
	Use Second Sh	nared Secret		0				
					Show			
	RADIUS DTLS S	Settings 👔						
	DTLS Required			0				
	Shared Secret		radi	us/dtls	()			
	Issuer CA of ISE	E Certificates for CoA	S	elect if required (optio	× (i)			
	General Setting	35						
	Enable KeyWrap	p		0				
	* Key Encryptic	on Key	_		Chow			
					Show			
	* Message Aut	thenticator Code Key			Show			
	Key Input Form:	at	0					
	,		•					
	TACACS Auther	ntication Settings					1	
	Enable TAC	CACS						
	Shared Secret							
					Snow	Retire		
	Enable Single C	Connect Mode						
			0	Legacy Cisco Device	Single Connect Sur	oport		
			0		io connect day			

Step 3: Connect or join Active Directory user with Cisco ISE

1. Navigate to Administration then click Identity Management and click External Identity Sources.

Cisco ISE	Q What page are you looking for?		
Dashboard	Context Visibility Operations	Policy Administration Work Cente	rs
Recent Pages	System	Network Resources	pxGrid Services
Identity Source Sequences Groups Identities External Identity Sources	Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access	Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services	Summary Client Management Diagnostics Settings Feed Service Profiler
	Settings	Device Portal Management	Threat Centric NAC
	Identity Management Identities Groups External Identity Sources Identity Source Sequences Settings	Blocked List BYOD Certificate Provisioning Client Provisioning Mobile Device Manageme My Devices Custom Portal Files Settings	Third Party Vendors

2. On External Identity Sources tab, Navigate to Active Directory and click Add

■ Cisco ISE	Administration · Identity Management				
Identities Groups External Iden	ntity Sources Identity Source Sequences Settings				
External Identity Sources	Active Directory				
 Certificate Authentication F Active Directory AD-WTI-LAB 	Join Point Name Active Directory Domain AD-WTI-LAB wti-lab.com				

3. Under Connection section. Fill in the all requirement and click submit.

≡	Cisco ISE	Administration · Identity Management						
Ider	ntities Groups Exte	rnal Identity So	urces Ide	entity Source	Sequences Se	ettings		
E	ixternal Identity Sources	Conr	ection	Allowed Doma	ins PassivelD	Groups	Attributes	Advanced Settings
	> 🛅 Certificate Authentica	* Joi	n Point Name	AD-WTI	I-LAB		Ū	
	Active Directory	* Act Doma	ive Directory in	wti-lab.	com		<u></u>	
	👻 AD-WTI-LAB							
	🗎 LDAP	+ Joir	+ Leave	A Test User	🕺 Diagnostic Tool	\bigcirc Refresh Table		
	ODBC		ISE Node		∧ ISE Node R	Status	Domain Controller	Site
	> 🛅 RADIUS Token		CiscolSE.w	ti-lab.com	STANDALONE	Operational	DCWin2022.wti-lab.co	om Default-First-Site-Name
	RSA SecurID							

4. Navigate to **Groups** tab and click **Add** > **Select Group from Directory**.

≡ Cisc	o ISE	Administration · Identity Management							
Identities	Groups	External Ide	ntity Sourc	es Ide	ntity Source Seq	uences Settin	igs		
External I	dentity Source	s	Connect	ion /	Allowed Domains	PassiveID	Groups	Attributes	Advanced Settings
> 🗖	Certificate Aut	entication F	🖉 Edit	$+$ Add \sim	Delete Group	Update SID Values			
~ 🗖	Active Director	y		Name		,	∧ SID		
4	AD-WTI-LAB			wti-lab.com/	IT Department/DUO		S-1-5-21-2	2346001846-3831695	5603-2264274261-2642
🗖 L0	DAP								

 Configuration for RADIUS communication between ISE and DUO. Navigate to Work Center > Device Administration > Ext Id Sources

Cisco	Q What page are you lookin			
Dashboard	Context Visibility	Operations Policy	Administration Work Centers	
Recent Pages	Network Access	TrustSec	Profiler	Device Administration
Ext Id Sources External Identity Sources Identity Source Sequences Policy Sets Device Admin Policy Sets Settings	Overview Identities Id Groups Ext Id Sources Network Resources Policy Elements Policy Sets Troubleshoot	Overview Components TrustSec Policy Policy Sets SXP ACI Troubleshoot Reports	Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements	Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports

6. On RADIUS Token click Add.

■ Cisco ISE				Administration · Identity Management				
Identities	Groups	External Ider	ntity Sourc	es Id	entity Source	Sequences	Settings	
External I	dentity Source	es ŵ	RAD	IUS T	oken Id	entity	Sources	
	Certificate Aut	hentication F	🖉 Edit	+ Add	Duplicate	蕑 Delete		
~ L 4	AD-WTI-LAB	У		Name			∧ Description	
	DAP			TEST				
🗖 0	DBC							
> 🗖	RADIUS Token]						

- 7. Starting from the left to right, configure the settings within each tab menu item as follow.
- a. In General tab, configure the name for the configuration.

b. In Connection tab, configure the primary server details. (Primary Server is DUO Proxy Authentication Server)

 Certificate Authentication F Active Directory WTI-LAB-AD-User LDAP ODBC RADIUS Token RSA SecurID SAML Id Providers Social Login General Connection Authentication Authentication Port Host IP 172.16.0.40 Shared Secret Show Authentication Port 1812 Server Timeout Seconds () Server Timeout Seconds () Connection Attempts Connection Attempts Total Authentication Port 	External Identity Sources	RADIUS Token List > TEST RADIUS Token Identity Sources
 RSA SecurID SAML Id Providers Social Login Host IP 172.16.0.40 Shared Secret Show Authentication Port 1812 Server Timeout 60 Seconds () Connection Attempts 3 	 Certificate Authentication F Active Directory WTI-LAB-AD-User LDAP ODBC RADIUS Token 	General Connection Authentication Authentication
* Authentication Port * Authentication Port * Server Timeout * Connection Attempts 3 ①	 RSA SecurID SAML Id Providers Social Login 	 Primary Server Host IP T72.16.0.40 () Shared Secret
		Authentication Port Authentication Port Authentication Port 1812 Server Timeout 60 Seconds (1) Connection Attempts 3 (1)

8. Create Identity Source sequences. Navigate to Administration > Identity management > Identity Sources Sequence

Cisco ISE	Q What page are you looking for?	
Dashboard	Context Visibility Operation	ns Policy Administration
Recent Pages User Identity Groups Ext Id Sources External Identity Sources Policy Sets Device Admin Policy Sets	System Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access	Network Resources Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services
	Settings	Device Portal Management
	Identity Management Identities Groups External Identity Sources Identity Source Sequences Settings	Blocked List BYOD Certificate Provisioning Client Provisioning Mobile Device Manageme My Devices Custom Portal Files Settings

9. In Identity Sources Sequence click **Add** name identity source sequence and select authentication available search list and click Save.

⊟ Cisco	ISE		Admi	nistration • Identity Manageme
Identities	Groups	External Identity Sources	Identity Source Sequences	Settings
Identity S	Source Sequend	ces List > DUO_Sequence		
Identit	ty Source S	Sequence		
	titu Source Sou	700700		
* Nan	ne			
Desci	ription			
Desci	npuon			
	L			
∨ Ce	rtificate Base	ed Authentication		
	Select Certifi	icate Authentication Profile	\checkmark	
∨ Au	thentication	Search List		
	A set of ide	ntity sources that will be accessed	in sequence until first authentication	n succeeds
	Availabl	e	Selected	
	Internal	Endpoints	TEST	
	Internal	Users	AD-WTI-LAB	
	Guest U	sers		

Step 4: Create TACACS Policy Set

- 1. Navigate to Work Centers > Device Administration > Device Admin Policy Set
- 2. Under Policy set click (+) to add new policy set.



Policy Set Name: DUO TACACS with AD Condition: DEVICE-Device Type EQUALS All Device Type Allowed Protocols: Default Device Admin

3. Authentication Policy

Rule Name: Default Use: **DUO_Sequence**

\vee Aut	henticatio	n Policy (1)					
+	Status	Rule Name	Conditions		Use	Hits	Actions
0) Search	1					
				+			
	0	Default			DUO_Sequence 🛛 🗸	3	ŝ

3. Authorization Policy – create two authorization policy, one for WTI_Admin and another for WTI_User.

imes Authorization Policy (2)					
		Results			
+ Status Rule Name	Conditions	Command Sets	Shell Profiles	Hits	Actions
Q Search					
Ø WTI Admin	AD-WTI-LAB-ExternalGroups EQUALS wti-lab.com/IT Department/DUO	PermitAllCommands \times \rightarrow +	WTI Admin 🛛 🖂 — +	16	錼

For WTI Admin

Rule Name: WTI Admin Condition: AD-WTI-LAB-ExternalGroup EQUALS wti-lab.com/IT Department/DUO Profile: WTI Admin



For WTI User

Rule Name: WTI user Condition: AD-WTI-LAB-ExternalGroup EQUALS wti-lab.com/IT Department/DUO Profile: WTI user



WTI TACACS Setting

1. Go to /N option 28 for TACACS

2. TACACS Setting

TACACS: [Shared]	
1. Enable: 2. Primary host/address: 3. Secondary host/address: 4. Secret Word: 5. Fallback Timer: 6. Fallback Local: 7. Authentication Port:	On 172.16.0.49 (defined) 15 Sec On (All failures) 49
8. Default User Access: 9. Account Management Module: 10 Session Management Module: 11. Service Name: 12. Debug: 13. Ping Test	Off Enabled Enabled wti Off