Access - DUO MFA Integration

This lab will cover how to integrate DUO Multi-Factor Authentication with WorkspaceONE Access. This is another common multi-factor authentication method being used by our customers.

Part 1: Setup Trial

Part 2: Setup Integration

Part 3: Test Integration

NOTE: For the authentication policy simply replace DUO MFA where you had VMware Verify (Intelligent Hub) as they serve a similar purpose.

Part 1 :Setup DUO Trial



1. On you **ControlCenter** VM navigate to **google.com** and search for **DUO Multifactor.** Now click on 30 Day Free Trial. Alternatively browse to the following link - https://signup.duo.com/ trial

Trust Every User With	Try out Duo Access edition free fo security.	r 30 days to experience powerful access Frank
Verify the identity of your users with two-factor authentication and the health of their devices before they connect to the apps you want them to access.	sfrank.aw@gmail.com	• (201) 555-0123
US government agencies/contractors, learn more about our FedRAMP Authorized editions.	Livefire ■ I'm an MSP, Reseller, or Partn ✓ By signing up I agree to the <u>Te</u>	201 - 500 employees
Automication 4 day or 10 minute	V I'm not a robot	reCAPTCHA Privacy-Temus
	Information you provide i Looking for help v <u>browse our s</u>	s subject to Duo Security's <u>Privacy Policy.</u> ith Duo? Read our <u>User Guide,</u> or <u>elf-service support resources</u> .

2. Fill in the requested information and click **Start My Trial**.

NOTE: Ensure you are using a valid Phone number as we will verify the admin account for virtual devices using SMS.

Please check your email to complete your registration.				
We have sent you an email with a verification link.				
			_	
Welcome to Duo, Simeon Frank 😕 Intex 🛪			ē	ß
Duo Security <no-reply@duosecurity.com> to me *</no-reply@duosecurity.com>	10:01 AM (3 minute	es ago) 🕁	*	:
You're almost there! We just need to verify your email address to complete your r Verify Your Email After activation, you can manage your account at <u>https://admin.duosecurity.com</u> . If you have any questions or need help, please visit our <u>supp</u> - Your friends at Duo	registration. port page.			

3. You will now have to open your e-mail to confirm your registration.

• Click on Verify Your Email.

	New Admin Setup
	Simeon Frank
	sfrank.aw@gmail.com
Welcome,	Simeon!
You have I with the D	been added to the Livefire organization uo role of Owner .
Get starte the button	d using the Duo admin panel by clicking I below.
	Get started

4. You will be greeted with the New Admin Setup page. Click on **Get started**.

	New Admin Setup	
	Simeon Frank	
	sfrank.aw@gmail.com	
Create you	Ir password	
Must be at le	east 12 characters long.	
Confirm yo	our password	
	-	
	Continue	

5. You will be prompted to create a new password. Once you have set a random memorable password click **Continue**.



6. You will now be asked to setup your smart phone with Duo Mobile App.



7. For **both** physical or if you are using the emulator **Download** the **DUO Mobile** application from the app store. Open the application after it has downloaded.

NOTE: If you are using a **Android Emulator** skip to step number 11 and on your web browser on **Controlcenter** click **Don't have a smartphone? Skip for now**

All you will have to do with the **Android Emulator** for Part 1 is have it downloaded. The rest of the instructions for Part 1 to get Duo Trial setup.

App Store <a> O9:41 ✓
- - - - - - - - - -
Welcome to Duo Mobile
Duo helps you log in securely. You'll use this app to approve your logins after entering your username and password on your computer.
"Duo Mobile" Would Like to Send You Notifications Notifications may include alerts, sounds and icon badges. These can be configured in Settings.
Don't Allow Allow
New to Duo?
ADD ACCOUNT
Looking to recover your accounts?

8. Allow the application to send you notifications by clicking **Allow**.



9. Still in the DUO mobile application click ADD ACCOUNT

◀ App S	itore 奈	09	41	
Cano	el	Add Ad	count	
	"Dı	o Mobile"	Would Like to	D
		Access th	e Camera	
	Duc en	Mobile will us roll accounts	se your camera to using QR codes.	
	Der	t Allow	01/	
	Du	I L AIIOW	UK	
Sca	an an act	ivation barco	de to link Duo N	Aobile to
		your ac	count.	
	ſ			
		No Bar	code?	

10. Allow the application to now access the camera by clicking **OK**.

	New Admin Setup	
	Simeon Frank strark.tw@gmail.com	
Nex to d bard	 let's enable Duo Push. Use your smartphone ownload the Duo Mobile app and scan the code below. 	
	Don't have a smartphone? Skip for now	
Edit	DUO ADMIN Livefire	⊢ ≡ nulator
	274 113	C
	About passcodes	
!	We have detected some securit issues with your device that rec your attention.	ty Juire

11. **Physical Device:** Now **scan** the **QR code** from the website that should still be open in your browser. You will now see an entry in the DUO Mobile app with the title **DUO ADMIN**

Android Emulator: If you are using a in your web browser on **Controlcenter** click **Don't have** a smartphone? Skip for now and continue with a **Text Me** option for verification.



12. In your browser you will now be presented with an option to use **Duo Push** or **Text**. If you have a physical device you can use Duo Push.

NOTE: If you are using the **Android emulator** simply use **Text Me** option for registering the administrator.



13. **(Skip if you are using emulator)** The Duo Mobile application will receive a notification to approve or deny the authentication. Click **Approve**.

DU e	Q Search for users, groups, applications, or devices	u Livefi	re ID: 2151-9289-87	Simeon Frank 🗸
Dashboard Device Insight Policies	Dashboard > Applications > Protect an Application Protect an Application			
Applications Protect an Application Single Sign-On Users Groups Endpoints	Add an application that you'd like to protect with Duo two-facto You can start with a small "proof-of-concept" installation — it ta add others. Documentation: Getting Started M Choose an application below to get started.	r authentication. kes just a few minutes, and you're the on	iy one that will see it, until y	rou decide to
2FA Devices Administrators	Filter by keywords: VPN, Microsoft, SAML	Protection Type		
Trust Monitor Reports Settings	1Password	2FA	Documentation 더	Protect
Billing Need Help?	AWS Directory Service	2FA	Documentation 🗗	Protect
Chat with Tech Support Id Email Support Call us at 1-855-386-2884 Account ID	Admin API	2FA	Documentation 더	Protect

14. You should now be authenticated into the trial **Duo Admin page.** We will now add a user to DUO.

NOTE: Active Directory connector is available also admins can perform a bulk upload of users.

DUO	Q Search for users, gro	oups, applications, or de	vices	(u Livefire ID: 2151-9289	9-87 Simeon Frank ~
Dashboard	Dashboard > Users					
Device Insight	Llooro			Directory Surg	- Import Linera - Bulk Epr	
Policies	Users			Directory Sync	S I Import Osers I Buik Enr	oli Users Add User
Applications	Need to activate a re	placement phone? Lea	rn more about Reactivating [Duo Mobile ⊑ [*] .		
Single Sign-On				_		
Users	0	0	0	0	0	0
Add User	Total Users	Not Enrolled	Inactive Users	Trash	Bypass Users	Locked Out
Pending Enrollments						
Bulk Enroll Users	Select (0) V			Б	oport - Q Search	
Import Users						
Directory Sync						
Bypass Codes		Looks	like you have no use	ers, click Add Us	er to add one.	
Groups						

15. In the **DUO Admin console** navigate to **Users > Add User**

ÐUƏ	Search for users, groups	, applications, or devices
Dashboard	Dashboard > Users > Add U	Jser
Device Insight	Add User	
Policies	Most applications allow use	re to oproll themselves after they complete primary a
Applications	Learn more about adding us	sers []
Single Sign-On		
Users	Username	mark
Add User		Should match the primary authentication username.
Pending Enrollments		
Bulk Enroll Users		
Import Users		
Directory Sync		Add User
Bypass Codes		

16. Enter the **username** of your unique user created earlier in the Active Directory and that has been synced to Workspace ONE Access.

Click Add User to continue.

mark		Logs	
			2
This user has not enrolled yet. See our enrollme	ent documentation 🗗 to learn more about enr	olling use	ers.
Username mark			
Username allases + Add a usernam Users can have up to Optionality, you may (e.g., Username allar	ne alias) 8 aliases. shoose to reserve using an alias number for a speci s 1 should only be used for Employee ID).	ic alias	
Full name Mark Debio			
Email mark@euc-livefire	e.com		
Status Active Require two far Stypess Styp two-factor i Disabled Automatically de This controls the use afractions	ctor authentication (default) authentication any access r's two-factor authentication process.		
Created Feb 15, 2021 8:4	8 AM (UTC)		
Last login Never authentica	ted		
Save Changes	s		

17. Enter the **Full name** of the unique user (If you used **Mark Debio** before continue) and the **e-mail address**. Please ensure that this e-mail matches the email of the user attribute in WorkspaceONE Access.

• Leave the remainder of the settings as default on this page and click **Save Changes**

Part 2: WorkspaceONE Access and DUO integration

DUO	 Search for users, groups, applications, or devices 	u Livefire	ID: 2151-9289-87	Simeon Frank 🗸
Dashboard	Dashboard > Applications > Protect an Application			
Device Insight				
Policies	Protect an Application			
Applications	Add an application that you'd like to protect with Duo two-factor	authentication.		
Protect an Application	You can start with a small "proof-of-concept" installation - it tak	es just a few minutes, and you're the only	one that will see it, until y	ou decide to
Single Sign-On	add others.			
Users	Observe an angliantian balance and started			
Groups	Gnoose an application below to get started.			
Endpoints				
2FA Devices	WEB SDK			
Administrators	Application	Protection Type		
Trust Monitor				
Reports	Partner WebSDK	2FA	Documentation 🗗	Protect
Settings	~			
Billing				
	Web SDK	2FA	Documentation 🗗	Protect
Need Help?				

1. In the **DUO admin console** navigate to **Applications** > **Protect an Application** then search for **WEB SDK**.

• Click **Protect** next to WEB SDK

Successfully added Web SDF	K to protected applications. Add another.	
Dashboard > Applications > Wet	s SDK ntation ௺ to integrate Duo into your custom web appl	Authentication Log 📋 Remove Applicatio
Details		Reset Secret Key
Integration key	DI5WTWNZN7GHAJY5FMIJ	select
Secret key	Click to view.	select
API hostname	Don't write down your secret key or share it with anyone.	select
Universal Prompt 🔊	See Update Progress Progress updating across all applications.	Get More Information C Learn more about the new prompt experience.
	App Update Ready Update Application This is a required backend update with minimal chang if you did not develop this integration, contact the app	nges 🖸 to users' authentication experience. pp provider for an update.

2. Note down the Integration key, Secret Key and API hostname in notepad.

NOTE: Be carful to not introduce spaces or returns when doing a copy and paste.

Settings	
Туре	Web SDK
Name	WorkspaceONE Access Duo Push users will see this when approving transactions.
Self-service portal	Let users remove devices, add new devices, and reactivate Duo Mobile See Self-Service Portal documentation ^I .

3. Scroll down to **settings** and change the **Name field** to **WorkspaceONE Access**

Hostname Whitelist	ing		
Whitelist hostnames	When enabled, this control ensures that the Duo Prompt is only sho hostname." This prevents attackers from tricking end users into usin For more information, see the documentation E.	wn when it is ng the Duo Pr	requested from an "Approved applicatic compt with malicious copycat websites.
	Only allow access for approved application hostnames		
	Save		
Activate the Unive	rsal Prompt for Web SDK	×	
We recommend activating t change it back anytime on	he new Universal Prompt C experience for users of this application. You can the application page.		
Activate Now No, th	anks		

- 4. At the bottom of the page
 - Select Save
 - In the Activate the Universal Prompt for Web SDK window
 - Select Activate Now

(8) Workspace O	NE [™] Access									Tenant Ad	min ↓ AW-EMUSK
Dashboard - Users	s & Groups Catalog 👻	Identity & Access Mana	gement	Roles				Q Sear	rch users, gro	ups or applicat	tions
	1		Logins								
	Users Logged i	n Today		WED	THU	FRI	SAT	SUN	MON	TUE	
	Users and Groups		Арр	popularity						7 Days	
	23 Total users	61 Total groups	Launches	0							
	User L emusk (System Do…	Last Login just now		-1	WED	THU	FRI	SAT	SUN	MON	

5. On the **Controlcenter** server

• Open a new tab,

• Log into the WorkspaceONE Access Admin Console

shboard	▼ Use	ers & Groups	Catalog -	Identity & Acce	ss Management	Roles		c
tories	Identity I	Providers	Password Reco	- very Assistant	Authentication N	Nethods	Policies	
		Authe Importa sure yo	entication Met ant: When you disa u update the acces	hods for Buil ble an authenticat ss policy rules to s	t-in Identity P ion method, the au select another auth	roviders uthenticatio entication r	n method is removed as method.	s a choice in the acce
		Auth	entication Method	5	Configure			Status
		Verify	y (Intelligent Hub)		ø			Enabled
		VMw	are Verify		ø			Enabled
		Mobi	ile SSO (for iOS)		Ø			Enabled
		Pass	word (Local Direct	cory)	Ø			Enabled
		Mobi	ile SSO (for Andro	d)	ø			Enabled
		Toke	n Auth Adapter		Ø			Enabled
		DUO	Security		Ø			Disabled
		Work Toke	space ONE UEM n	External Access	Ø			Enabled

6. Navigate to **Identity & Access Management > Authentication Methods** and click on the **pencil** next to **DUO Security**.

DUO Security				
Enable Duo Securit	у 🖌			
	Enable mult	tifactor authentication with Duo Admin UI		
Integration Key*				
	Integration	Key obtained from Duo Admin UI		
Secret Key*				
	Secret Key	obtained from Duo Admin UI		
API host Name*	api-8043d	149b.duosecurity.com		
	API host na	me obtained from Duo Admin UI		
Username format*	Usernam	e 🗸		
	Username f	format as represented in Duo Admin UI		
Duo Authentication	120			
Timeout (sec)*				
Cari: X 🚍 CVE X (🛱 Loci X O Fav: X			
- → C ① ■ adn		O Duc × M Gm: × M Wei × O Wor ×	Workspace ONE* Ac	cess
	nin-ac300324.duosecurity.c	Duc x M Gm: x M Wei x Wor x om/applications/DISSE2ZG5ITBIXJ8/YX4	Workspace ONE* Ac Dashboard Users & Group	Cess Catalog - Identify & Access Manag
roups	nin-ac300324.duosecurity.o	Duc x M Gm: x M Wei x Wor x Om/applications/DISSEZZG5ITBD/JB/YX4	Workspace ONE* Ac Dashboard + Users & Group Directories Identity Providers	Cess Catalog - Identity & Access Manag Password Recovery Assistant Authen
iroups indpoints EA Davidoar	Details Client ID	Duc X M Gm: X M Wei X Wor X Om/applications/DISSEZCOSITBIX/8/VV4	Workspace ONE* Act Dashboard Users & Group Directories Identity Providers DUO Security	Cests Catalog • Identity & Access Manag Password Recovery Assistant Authen
roups ndpoints FA Devices dministrators	Details Client ID Client secret	De: X M Ge: X M Wei X O Wei X One (Application)/DISS22GS/TBX/8/7X4 CISS22GS/TBX/8/7X4 Older to view	Workspace ONE* Acc Dashboard Users & Group Directories Identity Providers DUO Security Each Duo Security	Catalog Mentity & Access Manag Password Recovery Assistant Authen
roups hdpoints 'A Devices fministrators ust Monitor	nin-ac300324.duosecurity.c Details Client ID Client secret	Don x M Gin x M Wei x O Wo x entrapplication(DISSE2205/TB/CR/VA DISSE2205/TB/CR/VA DissE2205/TB/CR/VA Dist wire deen your deat second 2 Provide to pryon	Workspace ONE* Acc Dashboard Users & Group Directories Identity Providers DUO Security Enable Duo Security	COSS Coss Catalog Coss Coss Coss Coss Coss Coss Coss Cos
roups ndpoints "A Devices dministrators ust Monitor eports	Details Client ID Client weret API hostname	Dux X M Gim X M Wei X O Wo X metroplication/QUSSE22031BX/B/V4 Disse22037BX/B/V4 Cick to see: Distribute them part detert second of the set of the second second s	Workspace ONE [®] Ac Dashboard - Users & Group Directories Mentity Providers DUO Security Frashie Duo Security Integration Kof	COSS Coss Coss Coss Coss Coss Coss Coss Co
iroups Endpoints EFA Devices Administrators rust Monitor Reports Reports	Inn-ac300324.duosecurity.co Details Client ID Client vecret API hostname	Dex X M Gin X M Wei X W Wei X Or SE2203780/CB/VX DisSE2203780/CB/VX DisSE2203780/CB/VX Dist tarte dees your deef vision if intervision if wyon ap-ar00003284.doopcuty.com	Workspace ONE [®] Ac Dashboad - Users & Group Directories Meeting Providers DUO Security Fashin Duo Security Integration Ker	CESS Catalog • Monthly & Access Manag Password Recovery Assistant Author Ensite multitactor authoritication with Dua A Imagention Key obtained from Dua Admit UI
Sroups Endpoints IFA Devices Administrators Frust Monitor Reports Settings Settings	Inin-ac300324.duosecurity.co Details Cilient ID Cilient secret API hostname Universal Promot	Dex X M Gin X M Wei X W Wo X Or SSE2205/TBX/B/VX DisSE2205/TBX/B/VX DisSE2205/TBX/B/VX Dist tant deam your deet second a Nace the aryon g+ad000324 disceasivity.com	Workspace ONE" Ac Databased Users & Group Droccoles dently Provides DUO Security Eaching Duo Security Insegnation Ker Form Ker	Cost Catalog • Monitory A. Access Manag Password Recovery Assistant Authors Enablem multitation with Data A Integration Key obtained from Data Admit UI Integration Key obtained from Data Admit UI
Sroups Endpoints PFA Devices Administrators frust Monitor Reports Settings Settings Sitting	In rac200324 duosecurity o Details Client ID Client servet API hothome Universal Prompt	Dux X M Gin X M Wei X W Wo A mtAsphilation/DUS52205/TBX/LBX/94 DisSE2205/TBX/LBX/94 Clock to vaix Dist with data your data social of Maca da aryon apractoosed address of a Maca da aryon apractoosed address of a Maca da aryon	Workspace ONE" Ac Databased Users & Group Torecoles deatby Provides DUO Security Insegration Key Creek Key AP host Name*	Cess Cess Ceating Centremy Cen
roups Andpoints FA Devices Aministrators Aministrators Aministrators Another Aministrators Aministra	Details Clevet ID Clevet ID Clevet Roman API Rostname Universal Prompt	Dux X M Gin X M We X O Wo X OrseE22037E0/UR/M4 OrseE22037E0/UR/M4 OrseE2037E0/UR/M4 OrsE2037E0/UR/M4 OrsEE2037E0/UR/M4 Or	Workspace ONE® Active Database Users 4 Group Torcole DUO Security Poshe Deo Security Indee Deo Security Regration Ker Keret Ker API host Kame*	Coss Catalog Determiny 4, Access Manage Resourced Recovery Assisteet Catalog Recovery Assisteet Catalo
roups ndpoints FA Devices dramitatalors tusi Monitor etitings etitings etitings millione for the fact Second of milliones of the fact Second of milliones of the fact Second of the fact	In nac200324 duprecurity of Details Clent ID Clent servet APR hostname Unterstal Prompt	Dux X Mi Sim X Mi Wei X	Workspace ONE" Active statement Dere statement Users a Group Droctois denty Produce DUO Security Eable Duo Security Deterpration Ko Cerer Kor* AP host Reme* Usersame format*	Cost Catalog Variably & Access Maak Password Recovery Assistant Author Catalog multifactor authoritication with Don A Exaited multifactor authoritication with Don A Integration Key obtained from Don Admin UI ap-ac300324.durasecurity com API host name datained from Don Admin UI
inops	in esclosiz24 dusrecurity o Details Client ID Client secret API hothame Universal Prompt	Dux X M Gin X M We X P Wo X On SE2205/TBX/LB/V4 DISSE2205/TBX/LB/V4 DISSE2205/TBX/LB/V4 DISSE2205/TBX/LB/V4 DISSE205/TBX/LB/V4 DISSE205/	Workspace ONE" Ac The standard Users & Group Torcole Month Provides DUO Security Ender Duo Security End	Cost Cost Co
Sroups Sroups FA Devices Administrators Administrators Aleports Settings Settings Settings Administrators Admin	in in ac200124 duotecurity o Details Clease ID Clease servert API bashname Universal Prompt	Dux X M Gin X M Wei X W Wo X Onservices and the service of the service o	Workspace ONE" Ac The standard Ware	Catalog United & Access Manage Casavord Recovery Assistant Actess Casavord Recovery Assistant Actes Casavord Recovery Actes Casav

- 7. On the **DUO Security** page
 - Enable the following next to:

- Select the check box next to Enable DUO Security,
- Next to Integration Key, Paste your Client ID
- Next to Secret Key paste your Client Secret
- Next to API host name , paste API hostname
- Next to Username Format, from the dropdown select Username
- Select Save.

d ▼ Users a	& Groups Catalog	- Identity & A	ccess Management	Roles			Q Search users, groups or app	lications	
Identity Pro-	viders Password	Recovery Assistant	Authentication I	Methods Policie	es			Manage	Setup
	Identity Provid	ers (3)					Add Identity Provider		
	Identity Provi	Auth Methods	Directory	Network Ran	Connector(s)	Туре	Status		
	System Identity Provider	Password (Local Directory)	System Directory	ALL RANGES		Built-in	Enabled		
	Built-in	Mobile SSO (for iOS) Certificate (cloud deployment) User Risk Score Device Compliance (with Workspace ONE UEM) Password (cloud deployment)	LivefireSync UEMLocalDirecto sfmusk	ALL RANGES	ws1- connector.euc- livefire.com	Built-in	Enabled		

8. Now navigate to Identity & Access Management > Identity Providers > Built-in

Authentication Methods	Select which authentication methods the Id	P will use to authenticate users.
	Authentication Methods	Associate Authentication Method
	Verify (Intelligent Hub)	
	Password (Local Directory)	
	DUO Security	
	Certificate (cloud deployment)	
	Devertaged Cartificate	
KDC Certificate Export	Download Certificate	use in a Mohile Device Management profile
	Save Cancel	

9. Wait for the **Authentication Methods** to load and **click** the **check box** to enable **DUO Security**. Click **Save** at the bottom of the page.

8 w	orkspace ONE™ Access			
Dashboar	rd 👻 Users & Groups Catalog 👻	Identity & Access Management Roles		Q Search
Directories	s Identity Providers Password Recover	y Assistant Authentication Methods	Policies	
	ADD POLICY EDIT DELETE	EDIT DEFAULT POLICY	WORK RANGES	
	Policy Name	Applies to	R	ule
	<pre>default_access_policy_set</pre>	1 Application(s) 3	Rule(s)

10. Navigate to **Identity & Access Management** > **Policies** > and click the **EDIT DEFUALT POLICY**

1 Definition		You can create a list of ru	les to access the applications se	lected. For each rule, select th	ne IP network range,	the type
2 Configuration		application before reauth	enticating.	iods, and the maximum numb	er of hours users car	i use ine
2 comgutation						
3 Summary		Network Range	Device Type	Authentication	Re-authenticate	
		# ALL RANGES	Web Browser	Certificate (cloud depl	8 Hour(s)	×
		# ALL RANGES	Workspace ONE App	Password (cloud deplo	2160 Hour(s)	×
		II ALL RANGES	Windows 10	Certificate (cloud depl	8 Hour(s)	×
		⊕ ADD POLICY RULE				
				CA	NCEL BACK	NEXT
_	If a	user's network range is	ALL RANGES	CA	NCEL BACK	NEXT
_	If a and the user	user's network range is * accessing content from *	ALL RANGES Web Browser	¢2	ANCEL BACK	NEXT ✓ ① ✓ ①
	If a and the user and	user's network range is * accessing content from * d user belongs to group(s)	ALL RANGES Web Browser Q. Select Groups	C 4	ANCEL BACK	× 0 ∞ 0
1	if a and the user and	user's network range is • accessing content from • d user belongs to group(s)	ALL RANGES Web Browser Q. Select Groups Rule applies to all users if no gro	C2	ANCEL BACK	× 0 × 0 _ 0
	If a and the user . and and user is registeri	user's network range is * accessing content from * d user belongs to group(s) ing FIDO2 authenticator *	ALL RANGES Web Browser Q. Select Groups Rule applies to all users if no gro	c# up(s) selected.	NCEL BACK	NEXT ✓ ① ✓ ① ✓ ① ✓ ① ④ ④ ③
	if a and the user and and user is registeria	user's network range is • accessing content from • d user belongs to group(s) ing FIDO2 authenticator • Then perform this action	ALL RANGES Web Browser Q. Select Groups Rule applies to all users if no gro No Authenticate using	C#	ANCEL BACK	× 0 × 0 0 0 × 0 0 × 0
	if a and the user and and user is registerio then the user	user's network range is • accessing content from • d user belongs to group(s) ing FIDO2 authenticator • Then perform this action r may authenticate using •	ALL RANGES Web Browser Q. Select Groups Rule applies to all users if no gro No Authenticate using Password (cloud deployment)	Cr	INCEL BACK	NEXT ✓ 0 ✓ 0 0 ✓ 0 × 0 × 0 × 0
	If a and the user and and user is registeri then the user	user's network range is • accessing content from • d user belongs to group(s) ing FIDO2 authenticator • Then perform this action • may authenticate using • end	ALL RANGES Web Browser Q. Select Groups Rule applies to all users if no gro No Authenticate using Password (cloud deployment) DUO Security	cz	NCEL BACK	NEXT ✓ 0 ✓ 0 ✓ 0 ✓ 0 ✓ 0 ✓ 0 ✓ 0 ✓ 0 ✓ × ×

11. Edit the **Web Browser Policy** and change the form of authentication to **Password(cloud deployment)** and click on the plus + sign and add **DUO Security** as second form of authentication.

- Then make sure you keep Password (Local Directory) as the fallback method of authentication
- Click **SAVE** at the bottom of the page.
- **NOTE**: If you did the previous lab using **VMware Verify (Intelligent Hub)** you can simply replace that authentication method with **DUO Security** for the same user flow.

	Device Type	Authentication	Re-authenticate	
# ALL RANGES	Web Browser	Password (cloud deplo	8 Hour(s)	×
# ALL RANGES	Workspace ONE App	Password (cloud deplo	2160 Hour(s)	×
# ALL RANGES	Windows 10	Certificate (cloud depl	8 Hour(s)	×
		C/	ANCEL BACK	NEXT
Application(s)				
Configuration				
Configuration				

12. Click **Next** on the configuration page and click **SAVE** on the Summary page to close the edit policy wizard.

Part 3: Test DUO Multi-Factor Authentication



1. Navigate to your **W10Client01** vm open a new **incognito** web browser and navigate to the **WorskspaceONE Access** URL.

- Select the euc-livefire domain and click Next
- Type in the **username** and **password** for the unique user that you added to DUO above. (example: **Mark** and **VMware1**!)



2. You should now see the **DUO** splash screen, click **Start setup**



3. Select Tablet and click Continue

NOTE: You can choose mobile phone however this requires a GSM number. Notice some of the different device types that are supported.

Workspace ONE"
 Settings What type of tablet are you adding? IOS (IPad, IPod Touch) Android Back Continue
vmware [.]

4. Now choose your operating system and click Continue

• **NOTE**: Due to the fact that we cannot use the camera on the Android emulator we will be forced to use an e-mail registration method. If you have been using a physical Android or iOS You can skip the email registration and scan the barcode with the physical device.



5. Click I have Duo Mobile and open the Duo Mobile app on your device



6. **PHYSICAL DEVICE** On your mobile phone in the Duo Application. click the Plus + in the top right to start the camera and scan the QR code generated in the browser.

Android Emulator click the Email me an activation link instead button.

NOTE: The **DUO webpage** will expire during registration, this is not a problem simply navigate back to your WorkspaceONE Access URL.

Workspace ONE*
Email
1. Enter an email address that you can check on your Android device. We'll send you a special link that you can click to activate Duo Mobile.
manfredvogal@gmail.com Send email
Continue below.

6a. **Android Emulator** type your e-mail address into the field and click Send email.

~	O O	>						
	Duo Mobile Activation Gelen Kutusu x	z						
	Duo Security <no-reply@duosecurity.com> 02:14 (0 dakika önce) ☆ ♠</no-reply@duosecurity.com>	:						
	To activate the app, click and open this link with Duo Mobile: <u>https://m-ac300324.duosecurity</u> .com/android/usxwLxhKqj8U2BLIBPCx							
	 ▲ Yanıtla ➡ Yönlendir 							

6b. Android Emulator open your e-mail and click on the link in your email.



6c. **Android Emulator** copy the activation code string from your browser then open the Android emulator and click the **Duo Mobile Application** and click the **+** in the top right and corner click **No Barcode** and click **DUO Security Enabled Account** and then **paste** you Activation code from the link in the e-mail that you received.



7. Once scanned the QR code will show with a green checkmark and click **Continue** to proceed

0
Workspace ONE*
⊂ ios
Default Device:
IOS
 When I log in:
✓ Ask me to choose an authentication method Automatically send this device a Duo Push
Saved
Continue to Login
vm ware:

8. Now click on the drop down When I log in: Automatically send this device a Duo Push

Click Continue to Login

<u>~</u>	
Workspace ONE*	
Send Main Purch	
Enter a Passcode	
Enroliment successfull This is the Duo login prompt that you'll normally see when logging	
in. Dismiss	
vm ware [.]	

9. Click **Send Me a Push** on the next screen and you will be prompted with a push notification on your mobile.



10. **Approve** the Login request in the DUO app on your mobile or tablet.

Apps VM	lware Intelligent Hub	× +				
← → C	aw-manfre	ed.vidmprev	i ew.com /catalo	g-portal/ui#/ap	ps	
	Favorites	Apps	People	For You	Support	
	Q Sear	ch Apps				
				All Apps	Categories ~	0
AII A	upps					
:	SAML TEST APP					
Web	osite (i) y					

11. You should now be authenticated to Workspace ONE Access as your unique user.

ashboard	Dashboard > Users							
Device Insight	Users		Direct	ory Sync Import	Users Bi	ik Enroll Use	Add User	
pplications	Need to activate a	replacement phone? L	.eam more about F	Reactivating Duo Mo	alle Cf.			
Single Sign-On								
sers Id User	1 Total Users	O Not Enrolled	0 Inactive Users	0 Trash	0 Bypa	ss Users	0 Locked Out	
ending Envolments ulk Envoll Users	Select (0)~	-		Export ~	Q Search			
nport Users irectory Sync	Username .	Name	Frail	Phones	Tokers	Status	LastLorin	
ypass Codes iroups		Taking .	mark@euc-	Phone	1.5611	2004	Mar 17, 2021	
indpoints	mark	Mark Debio	livefire.com	1		Active	10:12 AM	
Recent Activ	vity						Full U	ser Logs
Transform (UTC)	David line						Council Courter	
Timestamp (UTC)	Result Use	ar Application		Access Devic	0		Second Factor	
10:12:33 AM MAR 17, 2021	Granted ma	irk Workspace	ONE Access	> Windows	10		 Duo Push Istanbul, 34, 	Turkey
9:12:13 AM MAR 17, 2021	✓ Enrolled ma	irk Workspace	ONE Access	> Windows	10		 Unknown Fai Location Unk 	tor nown
Phones fou may rearrange aplacement phone Alias	e the phones by dragg e C. Device	ging and droppin	g in the table. tform Mo	Learn more a del	bout activ	ating a Secu	Ad rity Warnings	d Phone
phone1	Google Android S For X86_64	idk Built And 10	droid Go Fo	ogle Android r X86_64	Sdk Built	ි S මා B vi di	creen unlocked iometric erification isabled	1
Indpoints								
os	Browsers			Last Used			Security Warni	ngs
Windows 10	Chrome	89.0.4389.90		Mar 17, 2021	10:11 AM		🛷 No warnin	gs
Windows 10	Chrome	89.0.4389.90		Mar 17, 2021 Mar 17, 2021	10:11 AM 9:16 AM		✓ No warnin✓ No warnin	gs gs

12. In the **DUO admin console** under **users** click on **Mark**. you should now see in the **users** field the last login as well as details about recent authentication on certain endpoints.

NOTE: The default setting for non-registered user is to prompt them to enroll. This means even users that are non-existent in DUO can still go through the registration process and authenticate using MFA.

	Q. Search for users, groups, applications, or devices Image: Universe of the search for users, groups, applications, or devices Image: Universe of the search for users, groups, applications, or devices Simeon Frank >
Dashboard	
Device Insight	Policy saved successfully.
Policies	
Applications	Dashboard > Policies
Single Sign-On	Policies 30 days left
	Duo's policy engine gives you the ability to control how your users authenticate, from
-	where, using which types of devices. Policies can be defined system-wide, per
Groups	Learn more about using policies. C
Endpoints	
2FA Devices	Global Policy This policy always applies to all applications. Edit Global Policy
Administrators	
Trust Monitor	Senabled New User policy Deny access to unenrolled users.
Reports	
Settings	Authentication policy Authentication policy
Billing	oomiguroo.
Edit Policy	X
You're editing the Global Po	blicy which is used by all applications. This can be overridden with custom policies.
Learn more about policies	ß
Revert to default	
Policy name	New User policy
Global Policy	Require enrollment
lisers	Prompt unenrolled users to enroll whenever possible.
New User policy	Allow arress without 2FA
Authentication policy	Allow users unknown to Duo to pass through without two-factor authentication. Users who exist in Duo and
Gen location	have not enrolled will be required to enroll.
Devices	Deny access
Device Health application	Deny authentication to unenrolled users.
 Operating systems 	This controls what happens after an unenrolled user passes primary authentication.
Browsers	
	Save Policy

13. In the DUO Admin Console navigate to Policies and click Edit Global Policy

You're editing the Global P Learn more about policies Revert to default	에cy which is used by all applications. This can be overridden with custom policies. 더
Policy name	New User policy
Global Policy	Require enrollment
Users	Prompt unenrolled users to enroll whenever possible.
New User policyAuthentication policyUser location	Allow access without 2FA Allow users unknown to Duo to pass through without two-factor authentication. Users who exist in Duo and have not enrolled will be required to enroll.
Devices Device Health application Remembered devices Operating systems	 Deny access Deny authentication to unenrolled users. This controls what happens after an unenrolled user passes primary authentication.

14. In the **New User Policy** select **Deny access** and click **Save Policy**. This will ensure that non registered users will not be able to register their devices and use MFA.

~
Workspace ONE"
username
user1
password
euc-livefire.com
Sign in
Forgot password?
Change to a different domain
vm ware:
Workspace ONE*
We're sorry, access is not allowed because you are not enrolled. Please contact your organization's IT help desk for assistance.
vm ware:

15. Open a new Incognito (make sure you are logged out of the previous user)

Authenticate using Jill and VMware1! notice you are not allowed to setup an account as this is not a pre-registered user.

This concludes the WorkspaceONE integration with DUO MFA.

Author: Simeon Frank