

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.

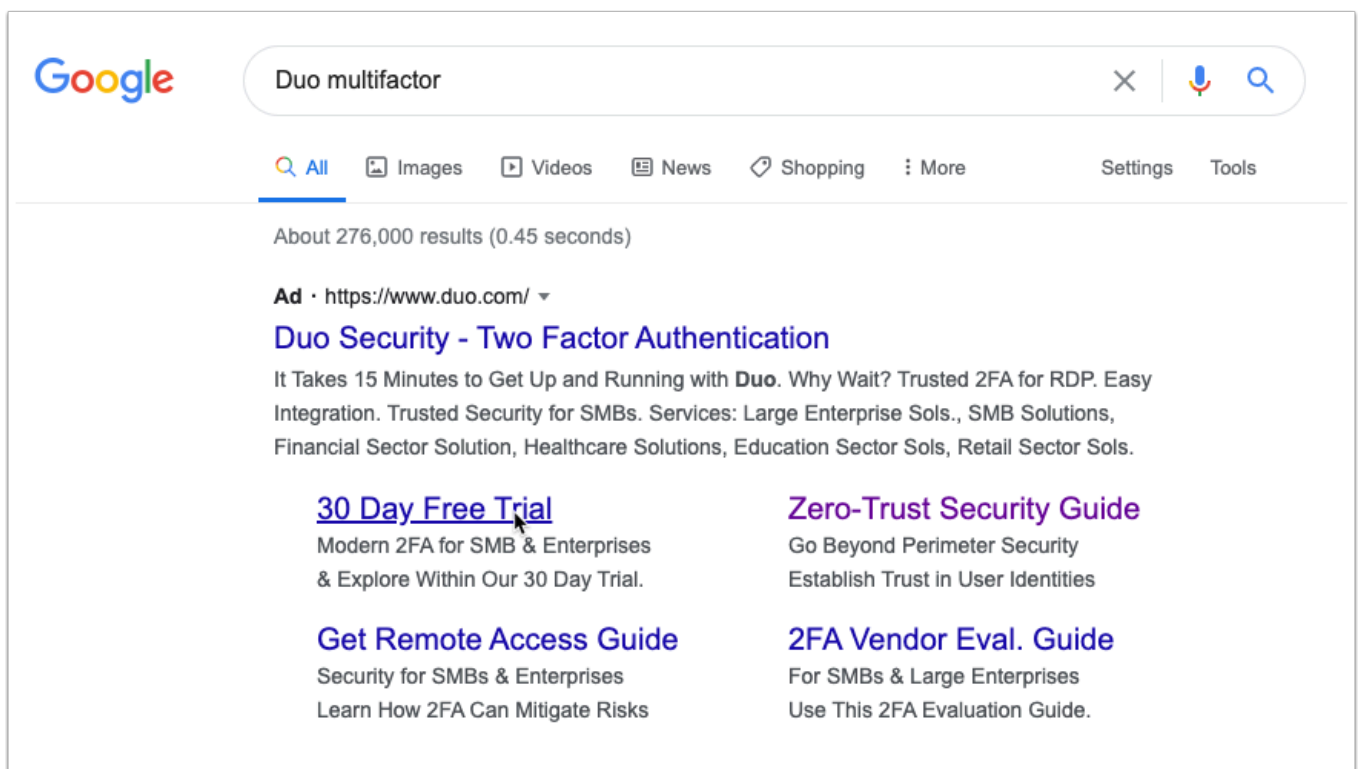
Part 1: Setup Trial

Part 2: Setup Integration

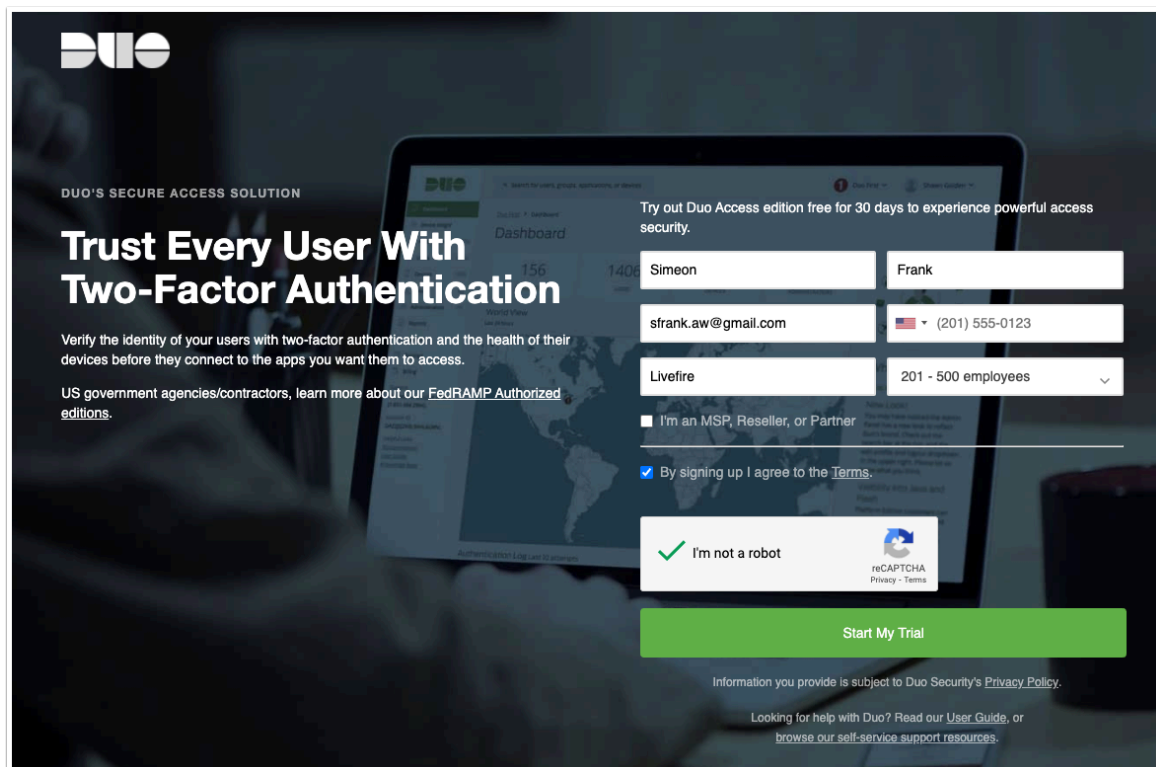
Part 3: Test Integration

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

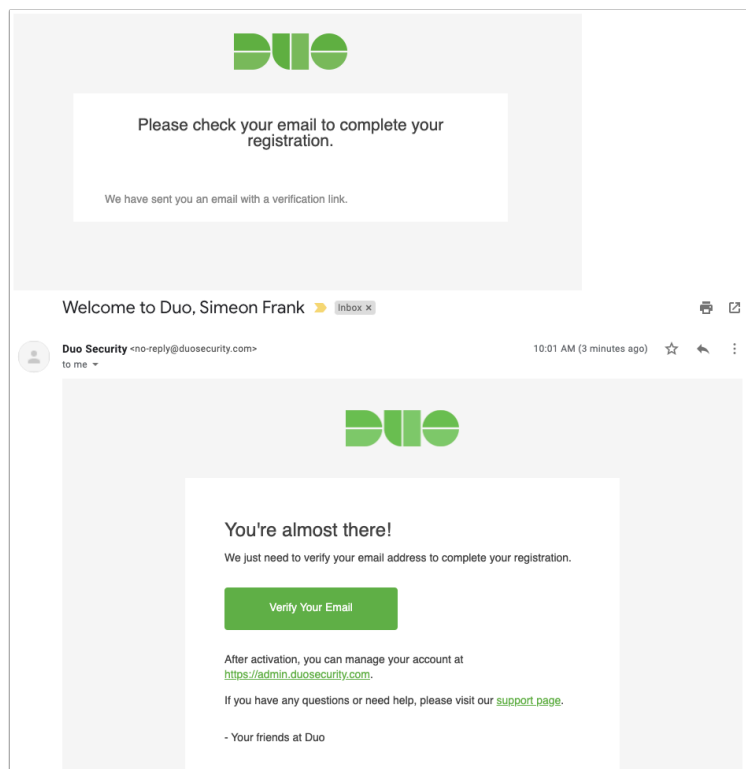


1. On you **ControlCenter** VM navigate to [google.com](https://www.google.com) and search for **DUO Multifactor**. Now click on 30 Day Free Trial. Alternatively browse to the following link - <https://signup.duo.com/trial>



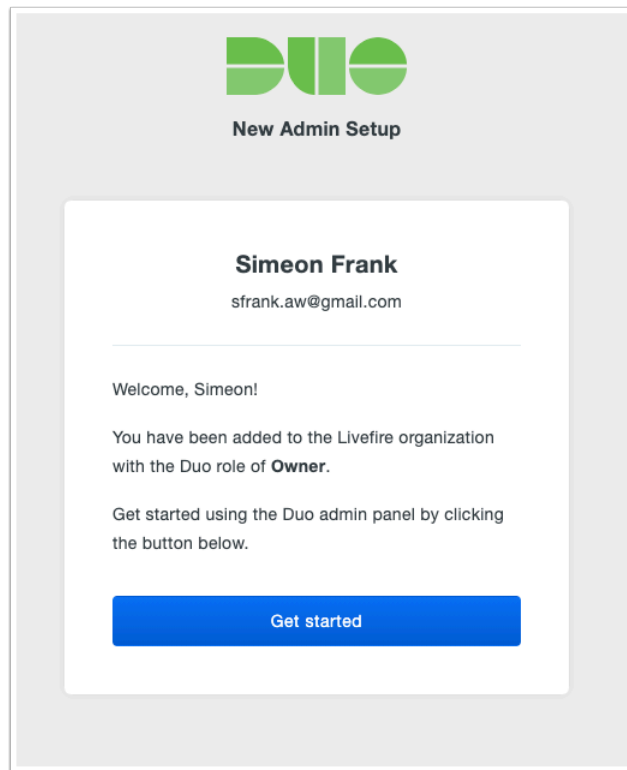
2. Fill in the requested information and click **Start My Trial**.

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

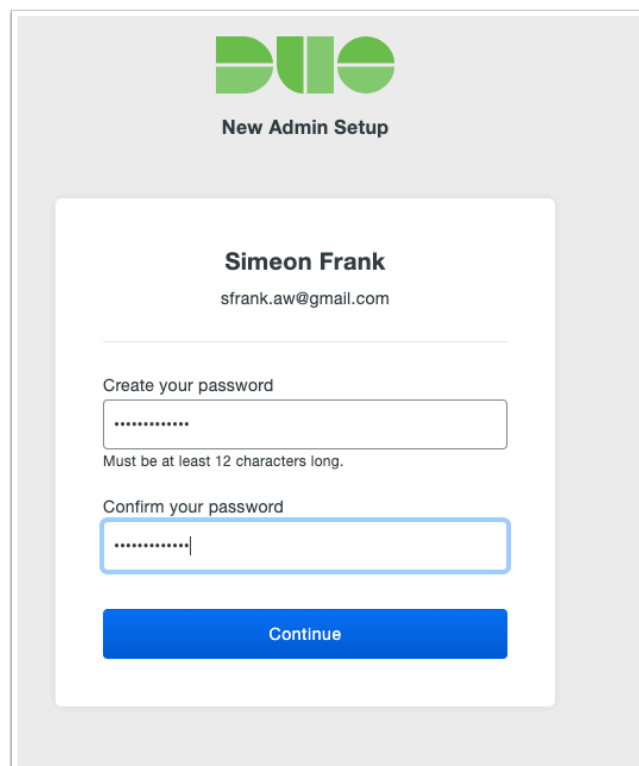


3. You will now have to open your e-mail to confirm your registration.

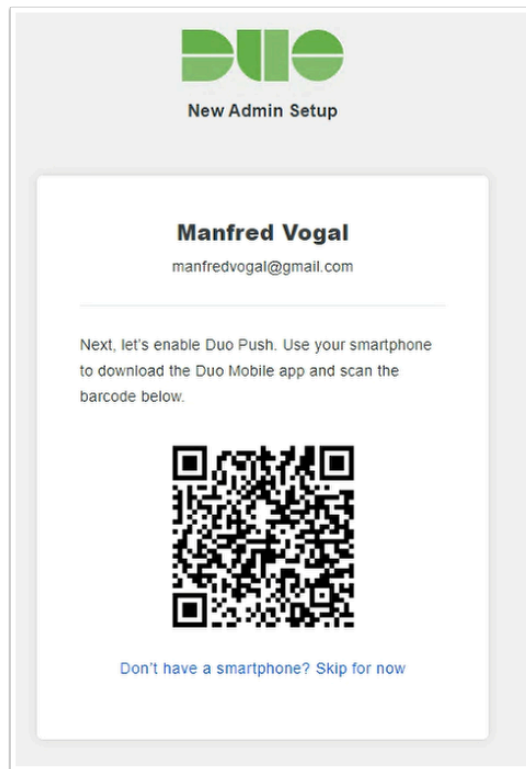
- Click on **Verify Your Email**.



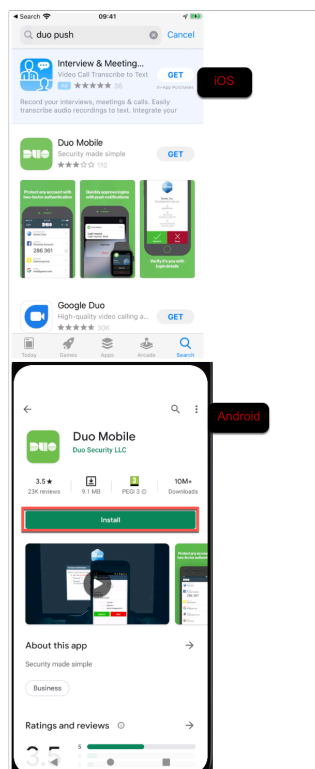
4. You will be greeted with the New Admin Setup page. Click on **Get started**.



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



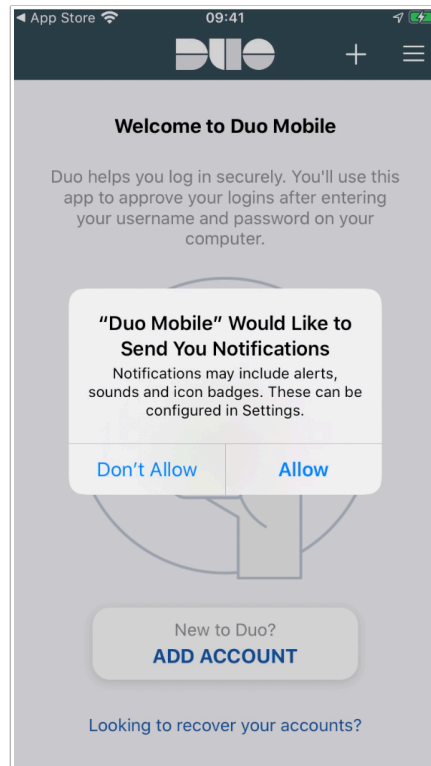
6. You will now be asked to setup your smart phone with Duo Mobile App.



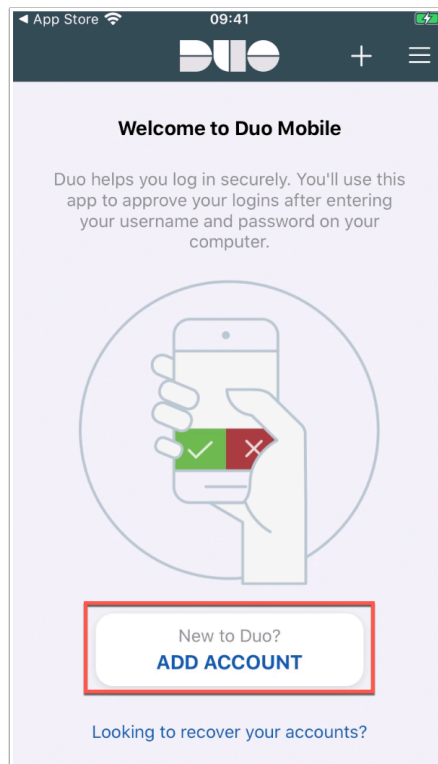
7. For **both** physical or if you are using the emulator **Download** the **DUO Mobile** application from the app store. Open the application after it has downloaded.

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**

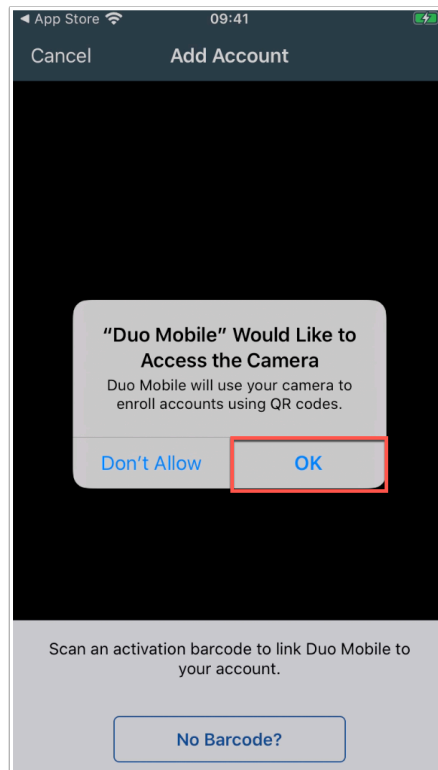
All you will have to do with the **Android Emulator** for Part 1 is have it downloaded. The rest of the instructions for Part 1 to get Duo Trial setup.



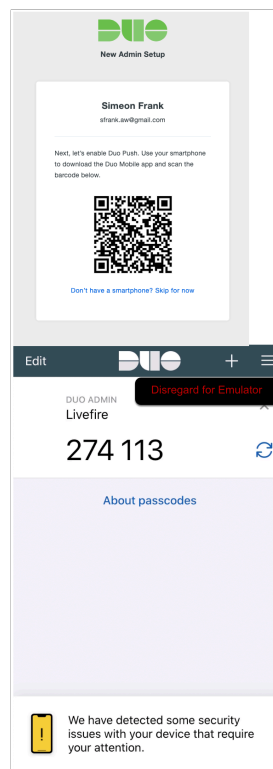
8. Allow the application to send you notifications by clicking **Allow**.



9. Still in the DUO mobile application click **ADD ACCOUNT**

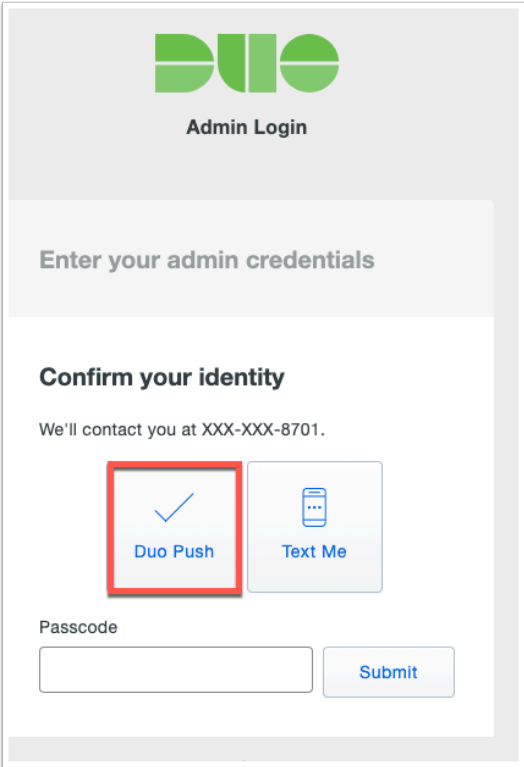


10. Allow the application to now access the camera by clicking **OK**.



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**

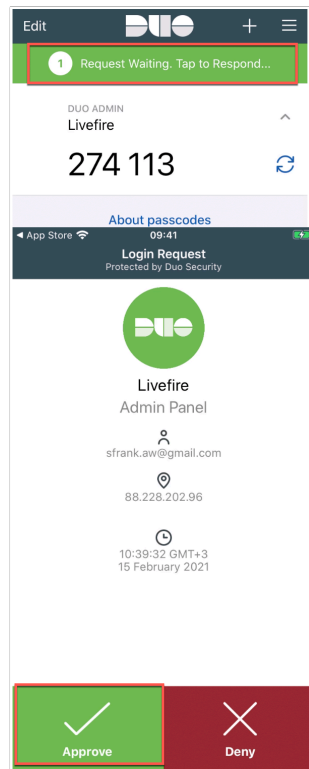
Android Emulator: If you are using a in your web browser on **Controlcenter** click **Don't have a smartphone? Skip for now** and continue with a **Text Me** option for verification.



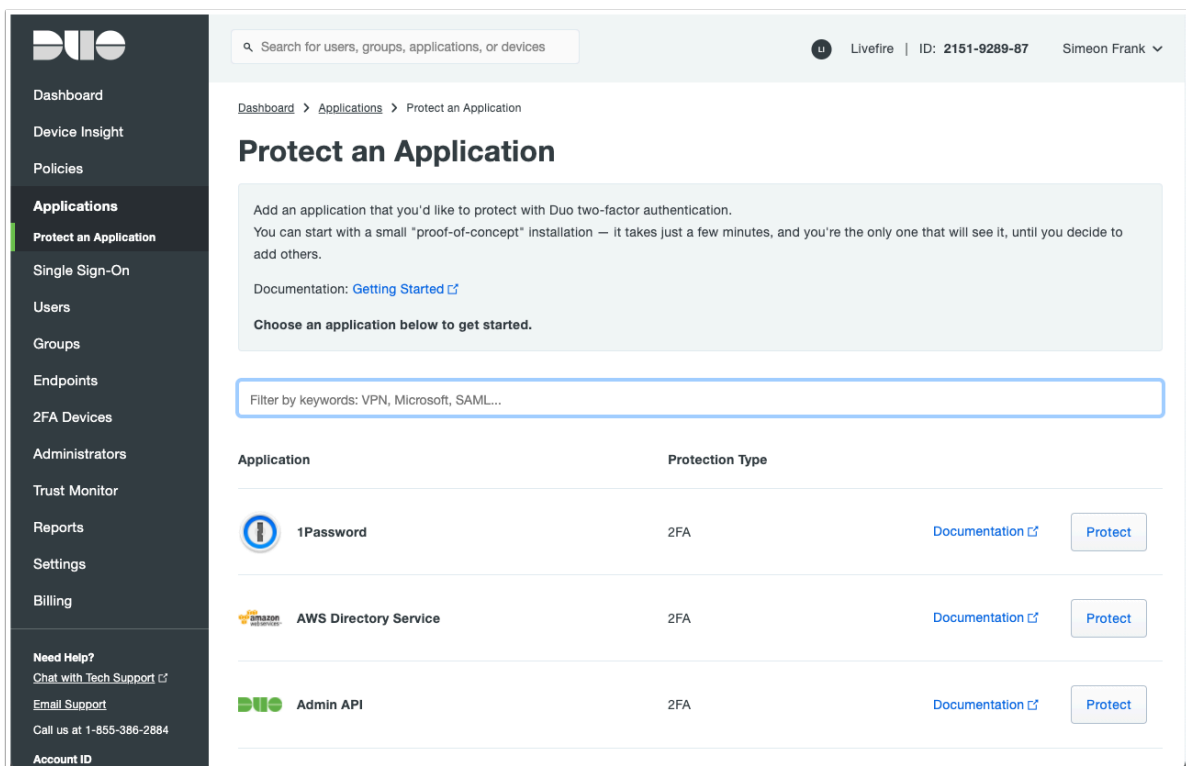
The image shows the Duo Admin Login interface. At the top is the Duo logo and the text "Admin Login". Below this is a section titled "Enter your admin credentials". The main section is titled "Confirm your identity" and includes the text "We'll contact you at XXX-XXX-8701.". There are two buttons: "Duo Push" (with a checkmark icon) and "Text Me" (with a mobile phone icon). The "Duo Push" button is highlighted with a red square. Below the buttons is a "Passcode" input field and a "Submit" button.

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.

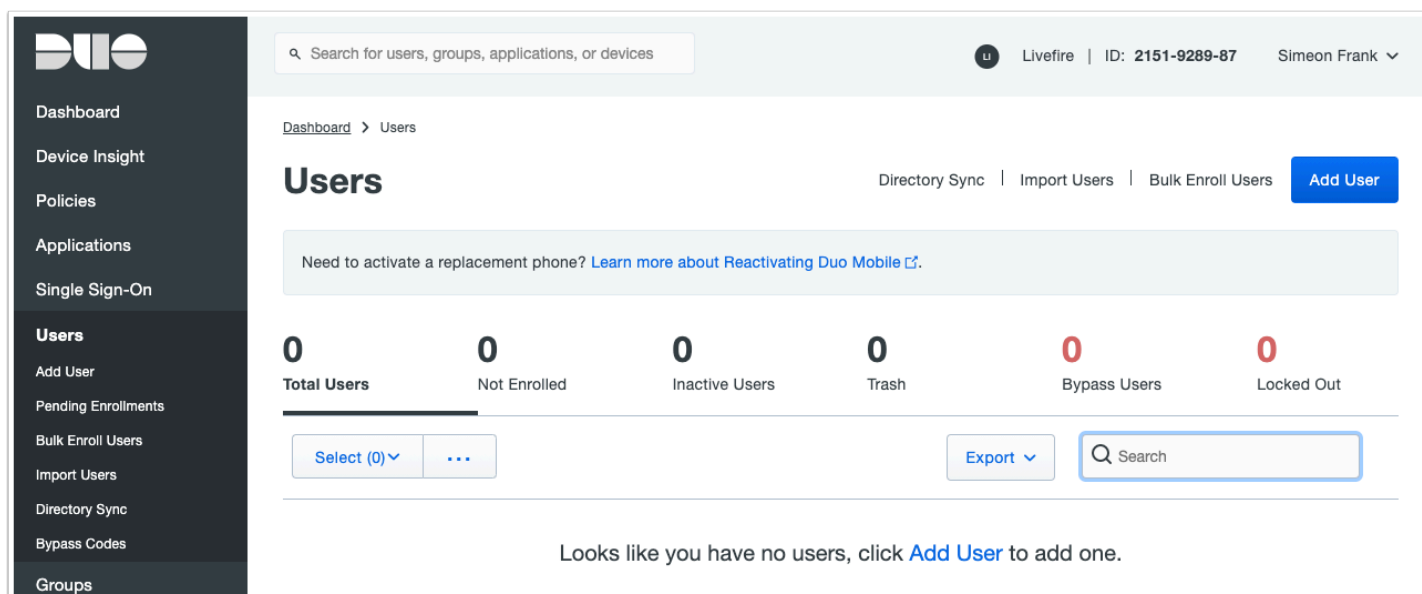


13. **(Skip if you are using emulator)** The Duo Mobile application will receive a notification to approve or deny the authentication. Click **Approve**.



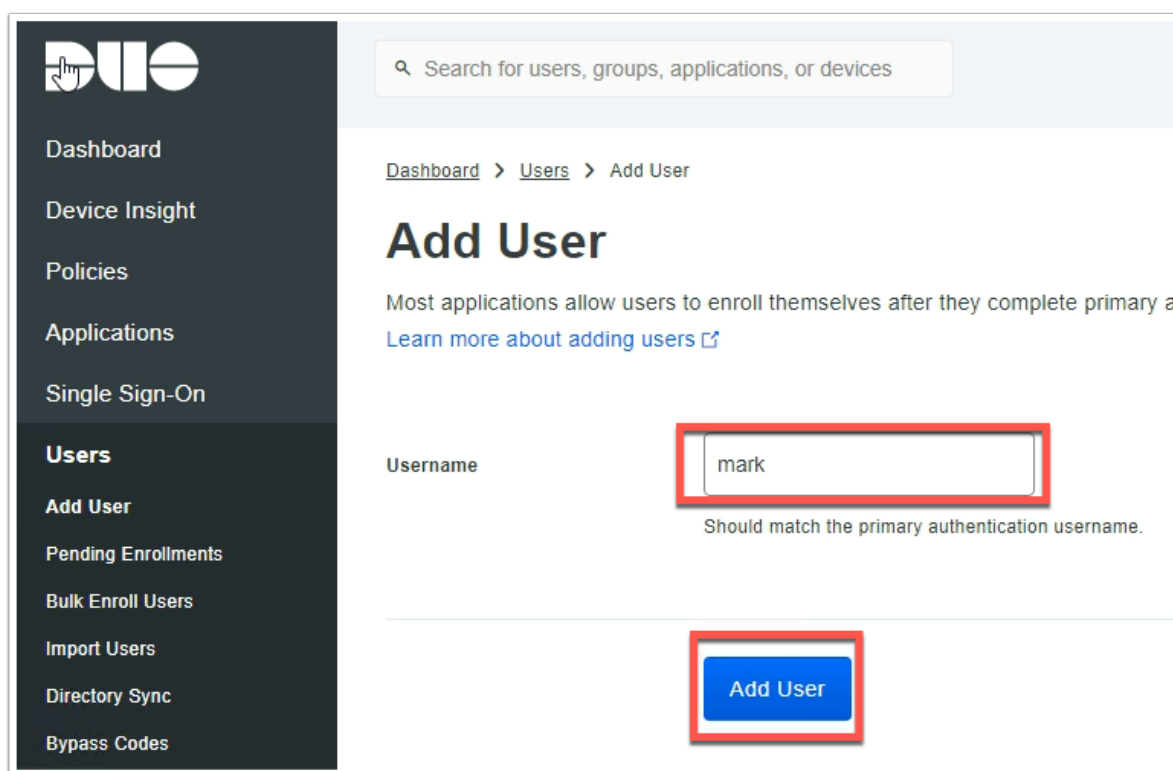
14. You should now be authenticated into the trial **Duo Admin page**. We will now add a user to DUO.

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



The screenshot shows the DUO Admin console interface. On the left is a dark sidebar with navigation links: Dashboard, Device Insight, Policies, Applications, Single Sign-On, Users (highlighted), Add User, Pending Enrollments, Bulk Enroll Users, Import Users, Directory Sync, Bypass Codes, and Groups. The main content area has a search bar at the top. Below it, the breadcrumb is 'Dashboard > Users'. The title 'Users' is displayed, followed by links for 'Directory Sync', 'Import Users', 'Bulk Enroll Users', and an 'Add User' button. A message states: 'Need to activate a replacement phone? [Learn more about Reactivating Duo Mobile](#).' Below this is a summary row with six categories, each showing a count of 0: Total Users, Not Enrolled, Inactive Users, Trash, Bypass Users, and Locked Out. At the bottom of this row are buttons for 'Select (0)' and 'Export'. A search bar is also present. A message at the bottom says: 'Looks like you have no users, click [Add User](#) to add one.'

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



The screenshot shows the 'Add User' page in the DUO Admin console. The sidebar is the same as in the previous screenshot, with 'Add User' highlighted under the 'Users' section. The main content area has a breadcrumb 'Dashboard > Users > Add User'. The title 'Add User' is displayed, followed by a message: 'Most applications allow users to enroll themselves after they complete primary a [Learn more about adding users](#).' Below this is a form with a 'Username' label and a text input field containing the text 'mark'. A red box highlights the input field. Below the input field is a note: 'Should match the primary authentication username.' At the bottom of the form is a blue 'Add User' button, which is also highlighted with a red box.

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 | S

This user has not enrolled yet. See our [enrollment documentation](#) to learn more about enrolling users.

Username

mark

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
(e.g., Username alias 1 should only be used for Employee ID).

Full name

Mark Debio

Email

mark@euc-liveware.com

Status

☒ Active
Require two-factor authentication (default)

☐ Bypass
Skip two-factor authentication

☐ Disabled
Automatically deny access

This controls the user's two-factor authentication process.

Applications

Created

Feb 15, 2021 8:48 AM (UTC)

Last login

Never authenticated

Save Changes

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

The screenshot shows the Duo Admin Console interface. On the left, the navigation sidebar has 'Applications' and 'Protect an Application' highlighted. The main content area is titled 'Protect an Application'. It includes a search bar with 'WEB SDK' entered. Below the search bar, there is a table with two columns: 'Application' and 'Protection Type'. The table lists two applications: 'Partner WebSDK' and 'Web SDK'. The 'Web SDK' entry is highlighted, and its 'Protect' button is circled in red.

Application	Protection Type
Partner WebSDK	2FA
Web SDK	2FA

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 SDK to protected applications. [Add another.](#)

[Dashboard](#) > [Applications](#) > Web SDK

Web SDK

Authentication Log | Remove Application

See the [Duo Web SDK Documentation](#) to integrate Duo into your custom web application.

Details

Reset Secret Key

Integration key

DI5WTWNZN7GHAJY5FMJ

select

Secret key

Click to view.

select

Don't write down your secret key or share it with anyone.

API hostname

api-8043d49b.duosecurity.com

select

Universal Prompt

See Update Progress

Progress updating across all applications.

Get More Information

[Learn more about the new prompt experience.](#)

App Update Ready

Update Application

This is a required backend update with [minimal changes](#) to users' authentication experience.
If you did not develop this integration, contact the app provider for an update.

2. **Note** down the **Integration key**, **Secret Key** and **API hostname** in notepad.
- NOTE:** Be careful to not introduce spaces or returns when doing a copy and paste.

Settings

Type

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](#).

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

Hostname Whitelisting

Whitelist hostnames When enabled, this control ensures that the Duo Prompt is only shown when it is requested from an "Approved applicatic hostname." This prevents attackers from tricking end users into using the Duo Prompt with malicious copycat websites. For more information, see the [documentation](#).

☐ Only allow access for approved application hostnames

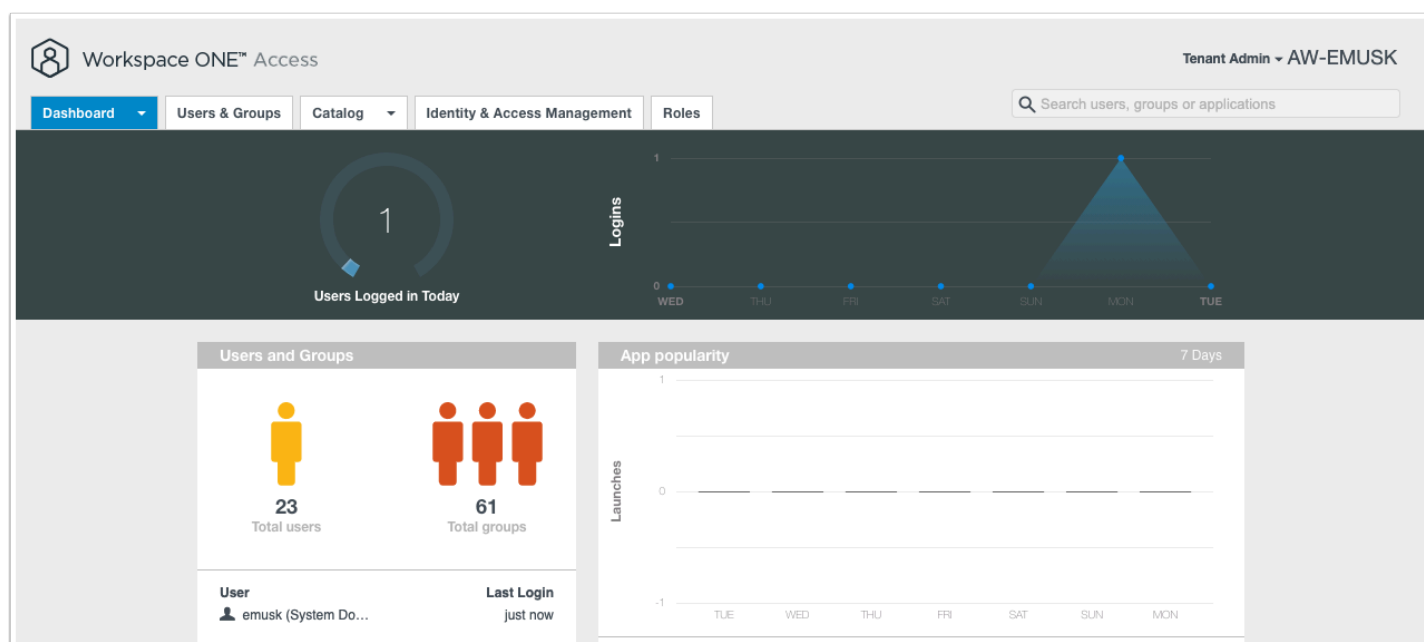
Save

Activate the Universal Prompt for Web SDK

We recommend activating the new [Universal Prompt](#) experience for users of this application. You can change it back anytime on the application page.

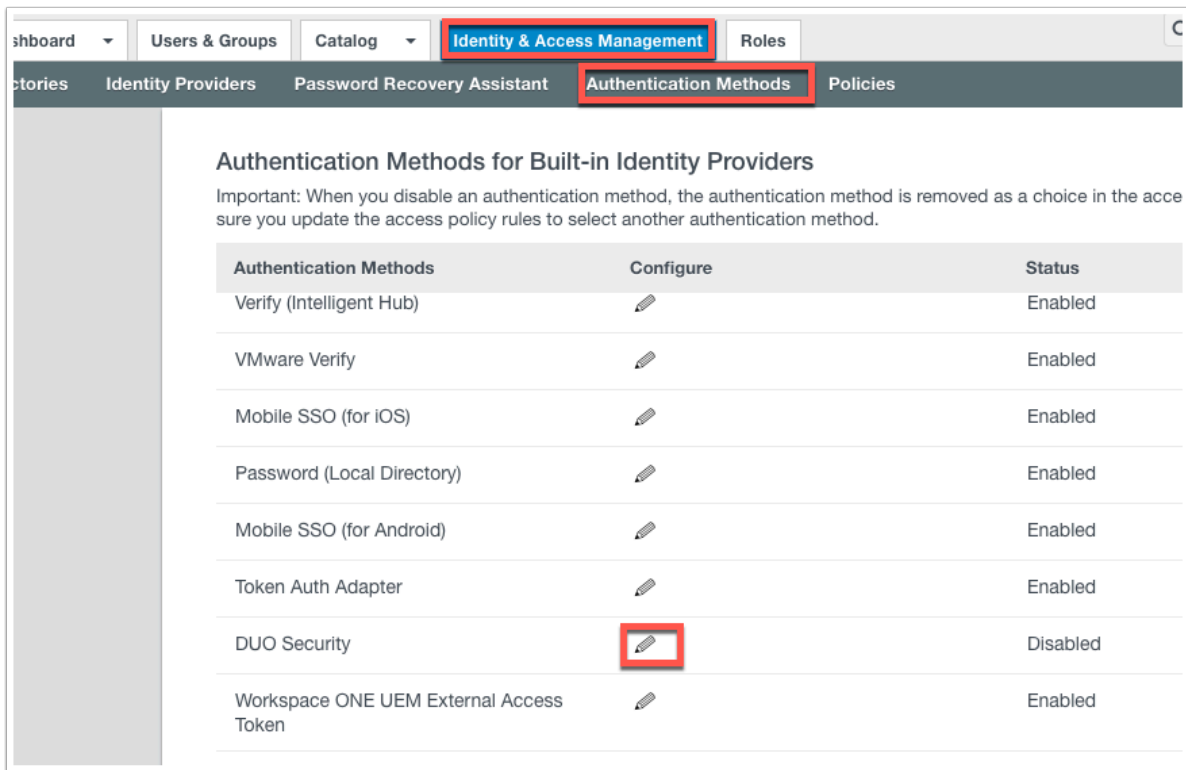
Activate Now **No, thanks**

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

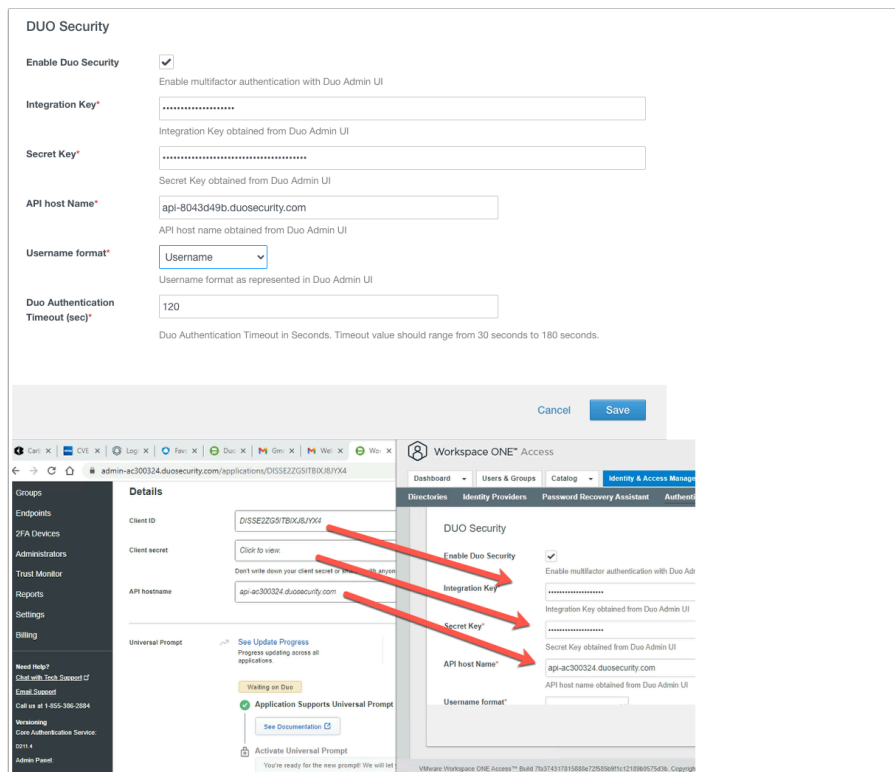


5. On the **Controlcenter** server
 - Open a new tab,

- Log into the **WorkspaceONE Access Admin Console**

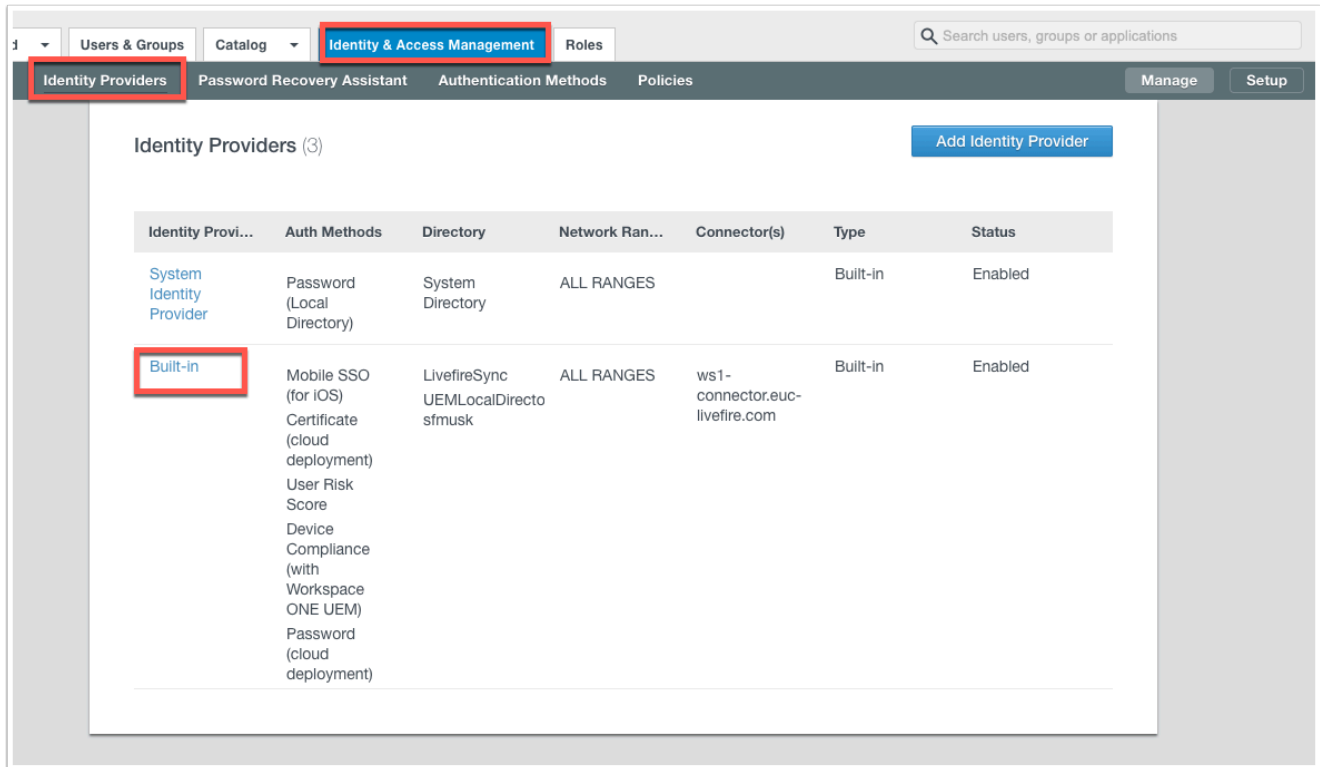


- Navigate to **Identity & Access Management > Authentication Methods** and click on the **pencil** next to **DUO Security**.



- 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**.



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

Authentication Methods Select which authentication methods the IdP will use to authenticate users.

Authentication Methods	Associate Authentication Method
Verify (Intelligent Hub)	<input checked="" type="checkbox"/>
Password (Local Directory)	<input checked="" type="checkbox"/>
DUO Security	<input checked="" type="checkbox"/>
Certificate (cloud deployment)	<input checked="" type="checkbox"/>

KDC Certificate Export [Download Certificate](#)
Export the KDC server root certificate for use in a Mobile 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.

Workspace ONE™ Access

Dashboard ▾ Users & Groups Catalog **Identity & Access Management** Roles Q Search

Directories Identity Providers Password Recovery Assistant Authentication Methods **Policies**

[ADD POLICY](#) [EDIT](#) [DELETE](#) [EDIT DEFAULT POLICY](#) [NETWORK RANGES](#)

	Policy Name	Applies to	Rule
<input type="radio"/>	default_access_policy_set	1 Application(s)	3 Rule(s)

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

Edit Policy

1 Definition
2 Configuration
 3 Summary

You can create a list of rules to access the applications selected. For each rule, select the IP network range, the type of devices that can access the applications, the auth methods, and the maximum number of hours users can use the application before reauthenticating.

Network Range	Device Type	Authentication	Re-authenticate
ALL RANGES	Web Browser	Certificate (cloud depl...	8 Hour(s) X
ALL RANGES	Workspace ONE App ...	Password (cloud depl...	2160 Hour(s) X
ALL RANGES	Windows 10	Certificate (cloud depl...	8 Hour(s) X

ADD POLICY RULE

CANCEL BACK NEXT

If a user's network range is * ALL RANGES ⓘ

and the user accessing content from * Web Browser ⓘ

and user belongs to group(s) ⓘ
 Select Groups...
 Rule applies to all users if no group(s) selected.

and user is registering FIDO2 authenticator * No ⓘ

Then perform this action Authenticate using... ⓘ

then the user may authenticate using * Password (cloud deployment) ⓘ ⓘ

and DUO Security X

If the preceding method fails or is not applicable, then Password (Local Directory) ⓘ ⓘ

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.

You can create a list of rules to access the applications selected. For each rule, select the IP network range, the type of devices that can access the applications, the auth methods, and the maximum number of hours users can use the application before reauthenticating.

Network Range	Device Type	Authentication	Re-authenticate
:: ALL RANGES	Web Browser	Password (cloud depl...	8 Hour(s) ×
:: ALL RANGES	Workspace ONE App ...	Password (cloud depl...	2160 Hour(s) ×
:: ALL RANGES	Windows 10	Certificate (cloud depl...	8 Hour(s) ×

[+ ADD POLICY RULE](#)

[CANCEL](#) [BACK](#) [NEXT](#)

1 Application(s)

Configuration


Policy Rule 1

If a user's network range is **ALL RANGES**
 and the user is accessing content from **Web Browser**
 and the user belongs to the group(s) **All Users**
 then the user may authenticate using **Password (cloud deployment) & DUO Security**

[CANCEL](#) [BACK](#) [SAVE](#)

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



Workspace ONE™


Select Your Domain

euc-livewire.com

☐ Remember this setting

Next

vmware



Workspace ONE™

username
mark

password

euc-livewire.com

Sign in

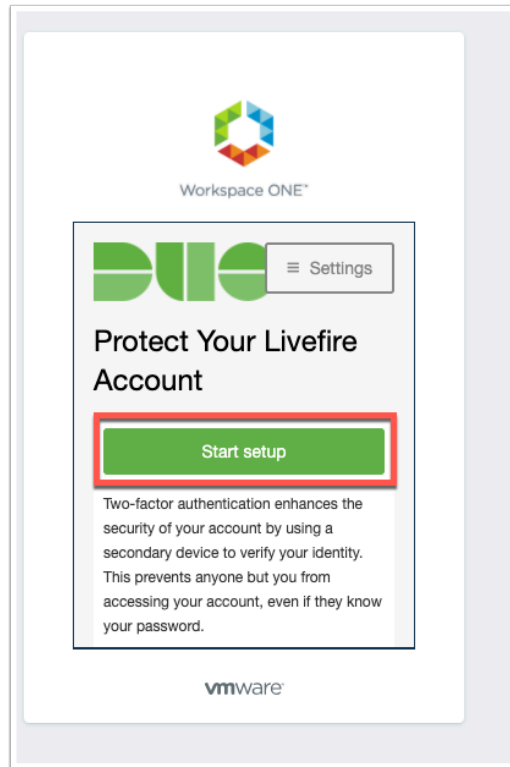
[Forgot password?](#)

[Change to a different domain](#)

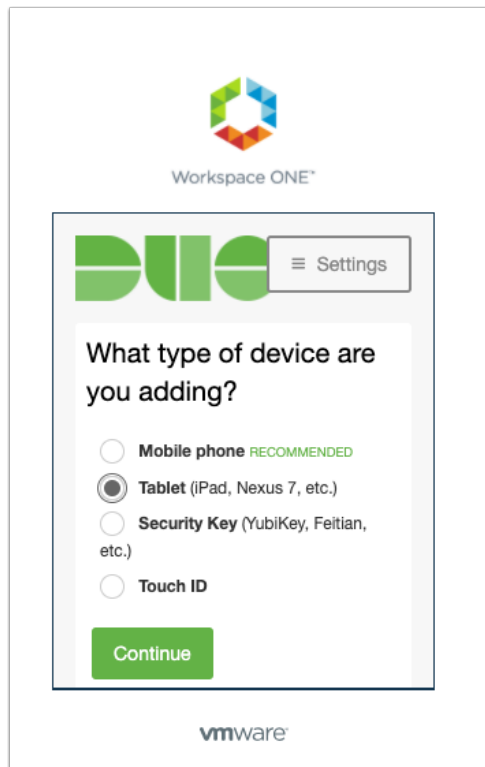
vmware

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

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

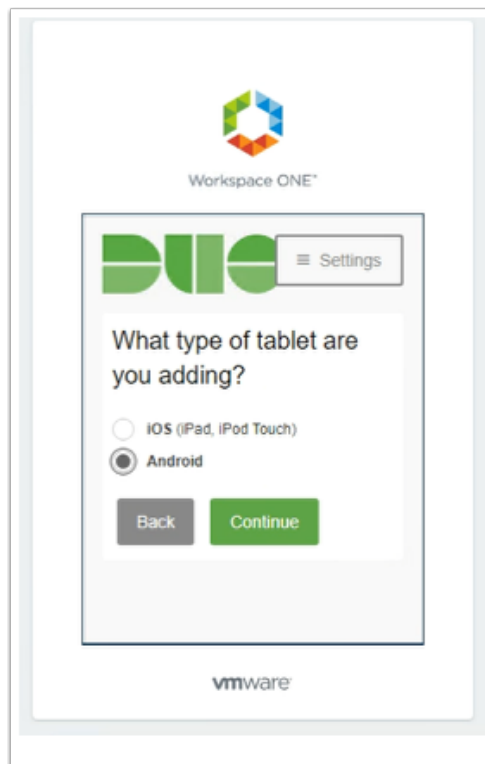


2. You should now see the **DUO** splash screen, click **Start setup**



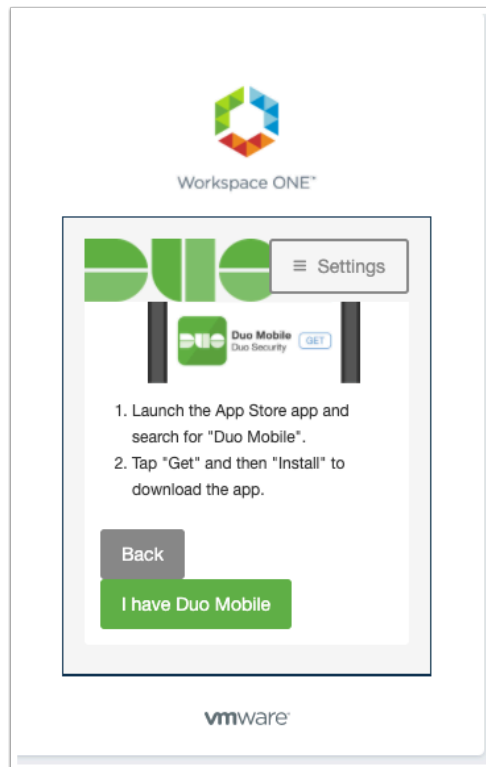
3. Select **Tablet** and click **Continue**

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



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.



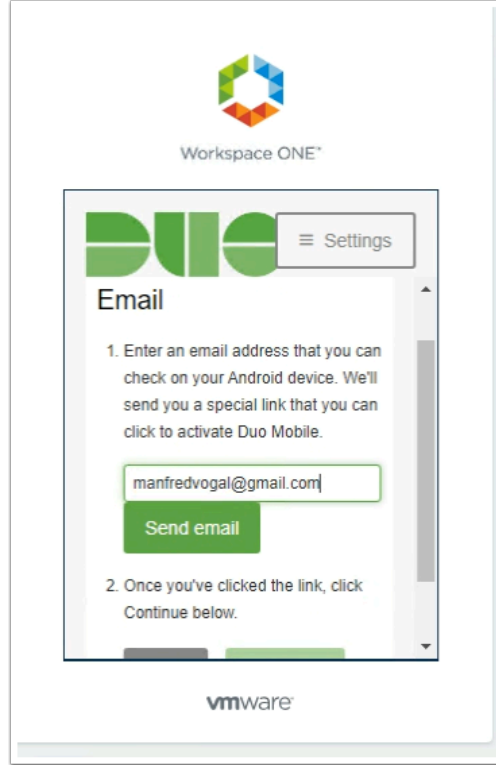
5. Click **I have Duo Mobile** and open the **Duo Mobile** app on your device



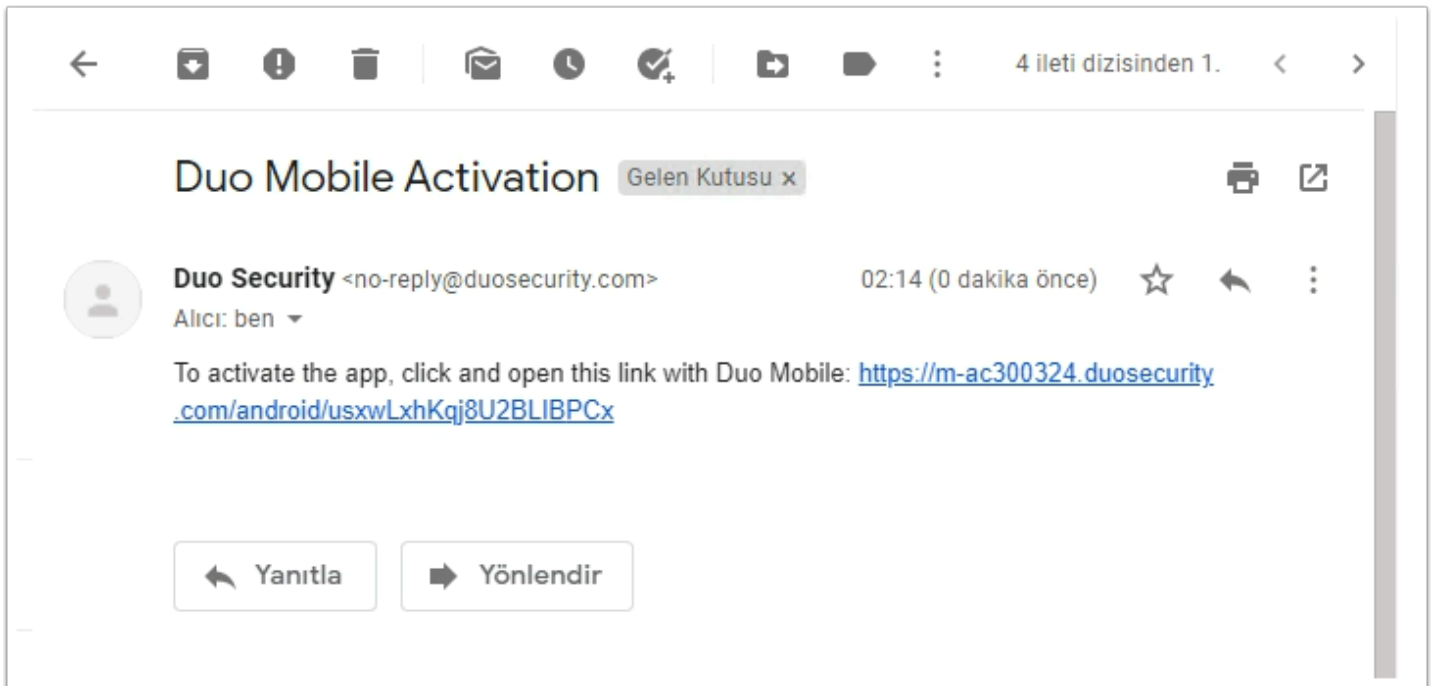
6. **PHYSICAL DEVICE** On your mobile phone in the Duo Application. click the Plus + in the top right to start the camera and scan the QR code generated in the browser.

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

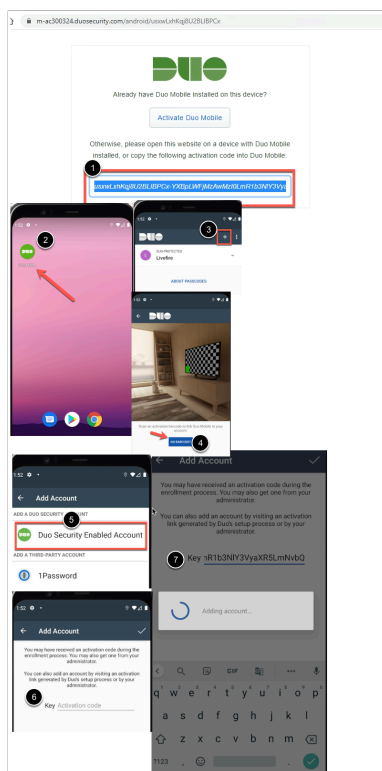
NOTE: The **DUO webpage** will expire during registration, this is not a problem simply navigate back to your WorkspaceONE Access URL.



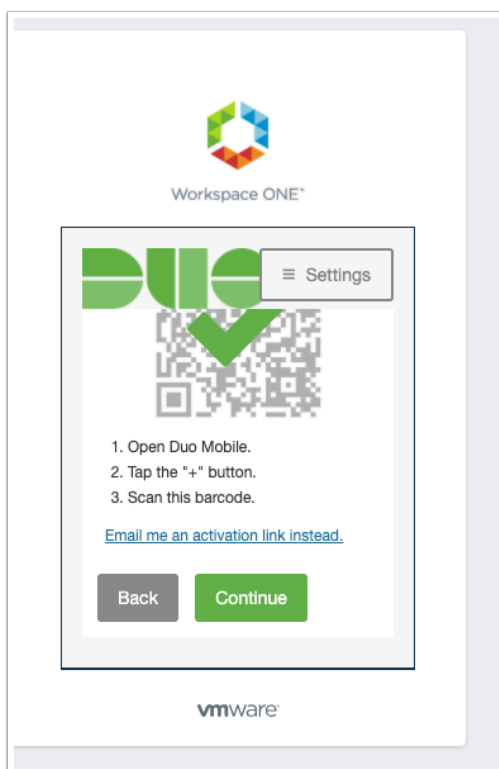
6a. **Android Emulator** type your e-mail address into the field and click Send email.



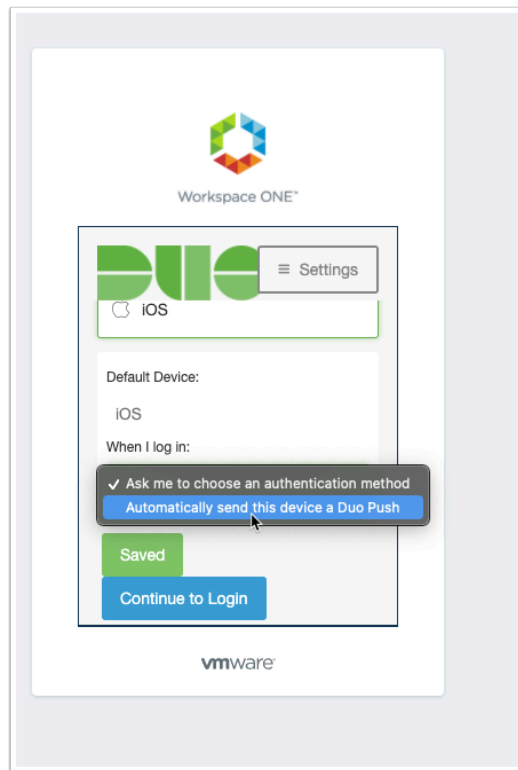
6b. **Android Emulator** open your **e-mail** and **click** on the link in your email.



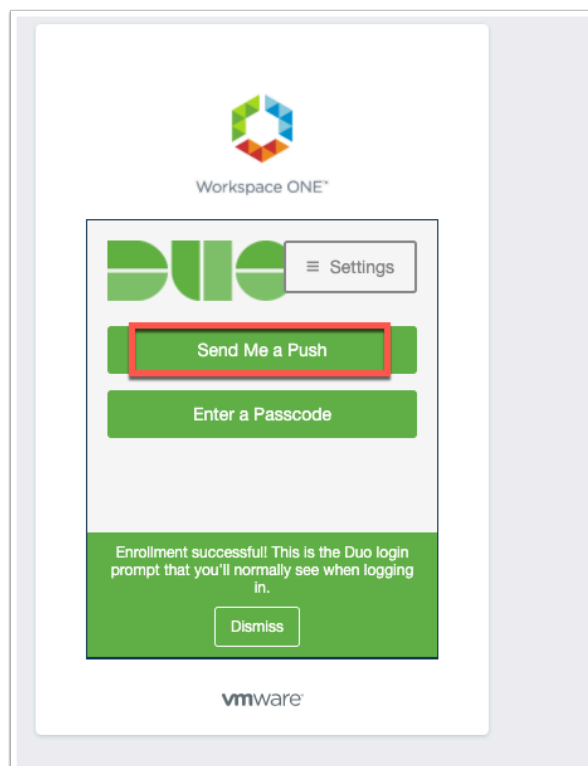
6c. **Android Emulator** copy the activation code string from your browser then open the Android emulator and click the **Duo Mobile Application** and click the **+** in the top right and corner click **No Barcode** and click **DUO Security Enabled Account** and then **paste** you Activation code from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



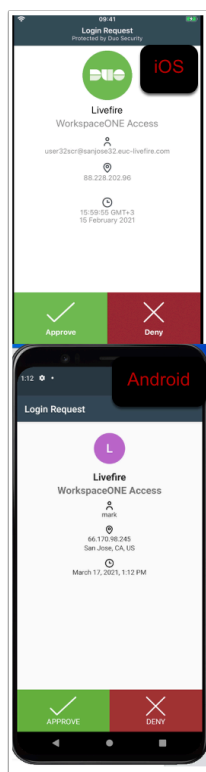
7. Once scanned the QR code will show with a green checkmark and click **Continue** to proceed



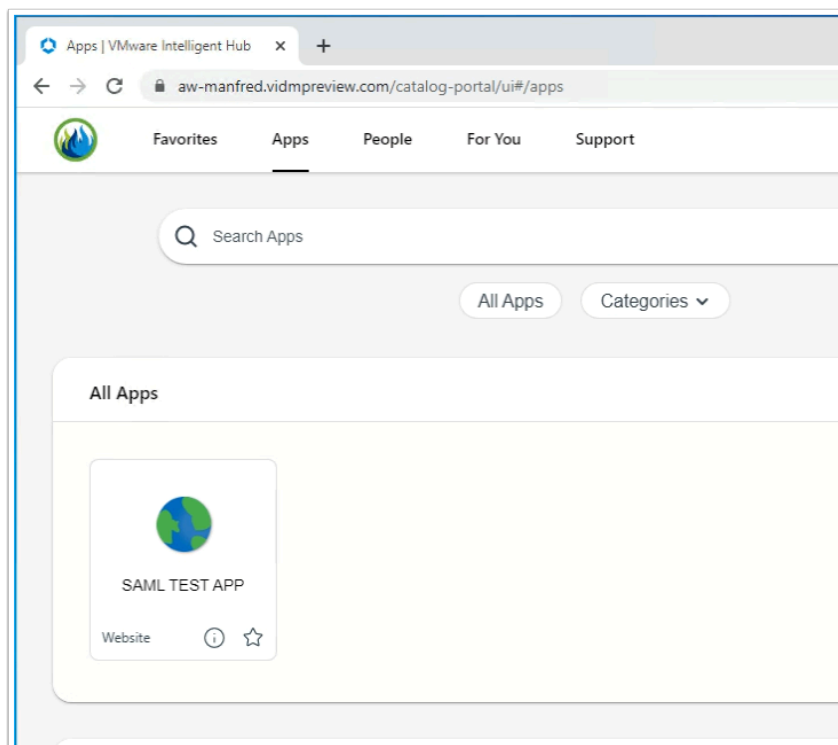
8. Now click on the drop down **When I log in:** **Automatically send this device a Duo Push**
Click **Continue to Login**



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.



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

Dashboard
Device Insight
Policies
Applications
Single Sign-On
Users
Add User
Pending Enrollments
Bulk Enroll Users
Import Users
Directory Sync
Groups
Endpoints

Users

Directory Sync | Import Users | Bulk Enroll Users [Add User](#)

Need to activate a replacement phone? [Learn more about Reactivating Duo Mobile](#) [?](#)

1 Total Users
0 Not Enrolled
0 Inactive Users
0 Trash
0 Bypass Users
0 Locked Out

Select (0)
Export
Search

<input type="checkbox"/>	Username	Name	Email	Phone	Tokens	Status	Last Login
<input type="checkbox"/>	mark	Mark Debio	mark@livefire.com	1		Active	Mar 17, 2021 10:12 AM

Recent Activity

Full User Logs

Timestamp (UTC)	Result	User	Application	Access Device	Second Factor
10:12:33 AM MAR 17, 2021	✓ Granted User approved	mark	WorkspaceONE Access	Windows 10	Duo Push Istanbul, 34, Turkey
9:12:13 AM MAR 17, 2021	✓ Enrolled	mark	WorkspaceONE Access	Windows 10	Unknown Factor Location Unknown

Phones

You may rearrange the phones by dragging and dropping in the table. [Learn more about activating a replacement phone](#) [?](#)

[Add Phone](#)

Alias	Device	Platform	Model	Security Warnings
phone1	Google Android Sdk Built For X86_64	Android 10	Google Android Sdk Built For X86_64	Screen unlocked Biometric verification disabled

Endpoints

OS	Browsers	Last Used	Security Warnings
Windows 10	Chrome 89.0.4389.90	Mar 17, 2021 10:11 AM	✓ No warnings
Android 10		Mar 17, 2021 9:16 AM	✓ No warnings

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.

Duo
Dashboard
Device Insight
Policies
Applications
Single Sign-On
Users
Groups
Endpoints
2FA Devices
Administrators
Trust Monitor
Reports
Settings
Billing

Search for users, groups, applications, or devices
Livefire | ID: 2151-9289-87 | Simeon Frank

Policy saved successfully.

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 application, or for specific groups. [Learn more about using policies](#) [?](#)

Global Policy

This policy always applies to all applications.

Enabled
New User policy
Deny access to unenrolled users.

Authentication policy
Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.

Edit Global Policy

Edit Policy

You're editing the Global Policy which is used by all applications. This can be overridden with custom policies. [Learn more about policies](#) [?](#)

[Revert to default](#)

Policy name
Global Policy

New User policy

Require enrollment
Prompt unenrolled users to enroll whenever possible.

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.

Deny access
Deny authentication to unenrolled users.
This controls what happens after an unenrolled user passes primary authentication.

Save Policy

Access - DUO MFA Integration

Export Date: 2024-01-09 04:27:40 -0500

Page 26

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

Edit Policy

You're editing the Global Policy which is used by all applications. This can be overridden with custom policies.

[Learn more about policies](#)

[Revert to default](#)

Policy name

Global Policy

Users

- ✓ [New User policy](#)
- ✓ [Authentication policy](#)
- ✓ [User location](#)

Devices

- ✓ [Device Health application](#)
- ✓ [Remembered devices](#)
- ✓ [Operating systems](#)
- ✓ [Browsers](#)

New User policy

☐ **Require enrollment**
Prompt unenrolled users to enroll whenever possible.

☐ **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.

☒ **Deny access**
Deny authentication to unenrolled users.
This controls what happens after an unenrolled user passes primary authentication.

Save Policy

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.

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