



# workplace\_

Multi-Factor Authentication

# MFA: Making sure you're really you

As threats from bad actors become more and more complex and increasingly successful, every organization in the financial industry needs to step up security to make sure that employees, the company, and customers are safe. Studies show that up to 70% of breaches come from stolen passwords. Multi-factor authentication (MFA) has proven to greatly reduce the risks associated with stolen passwords.

To do this, Workplace now requires the use of MFA when signing in. We call this feature "sign-in verification," and all it takes is a simple but necessary second step to sign into the Workplace environment.

Imagine you had a bike lock with a combination. If you wrote it down somewhere, someone could easily find out the combination and take off with your bike. All they needed was your password to access something that belongs to you.

Now, what if you had a second lock (otherwise known as a second factor) and this one has a key! Even if someone got your combination, they would not be able to steal your bike because they would need to have the physical key, and you are not giving up your key to them.

That scenario is exactly like your work. Your bike represents your files, emails, applications, and systems. The combination lock is your password and the key is your phone. This makes it extra secure because someone has to have a piece of information and a physical key in order to get in to your systems. This multi-factor system helps keep you, your company, and your customers safe.

# The value-add of MFA

Here are three reasons why turning on sign-in verification is a value add for your organization.

## **1. Your employee's bad password habits will no longer put your firm at risk.**

Most users are known to use the same passwords over and over again. There have been multiple major security breaches that have exposed just about everyone's passwords in the past 10 years. While your users may have changed their passwords since then, users tend to re-use old passwords after they run out of password ideas. Using MFA requires that the user use something they are in possession of, in addition to their password, to gain access to the system. In the case of Workplace, this item is your cell phone. Stealing a password will not allow a bad actor to gain access to your Workplace account.

## **2. You can change your passwords less frequently.**

The latest NIST guidelines for password do require multi-factor authentication. However, the guidelines also toned down the requirements to change passwords frequently. Now, users can create better passwords that last longer in addition to using multi-factor.

## **3. You now get MFA for every website that you add to Workplace**

Workplace's "websites" feature allows Workplace to manage your credentials and providing single-sign on to all of your favorite websites. The websites feature will also allow users to generate secure, random passwords for your websites. By activating sign-in verification and creating a random secure password for every website, your users will effectively have gained multi-factor authentication for every website they use. Individual website breaches will no longer require you to change your password on every site you visit!

# Things to note for MFA setup

Once multi-factor authentication is turned on, there are two ways for users to authenticate.

1. A user needs to respond to the MFA notification
2. A Company Manager must approve the sign-in attempt

Users will need to be able to respond to a notification on their mobile devices in order to log in. This also means that if they have not set up the Workplace app, they will not receive the notification!

Make sure your users have installed Workplace Android or Workplace iOS before you turn this one, or the Company Manager will have to approve a lot of sign-in attempts in the Admin Dashboard.

The following pages contain information on how Company Managers and Users can setup MFA.



# Setting up MFA for Company Managers

Here's how to turn on multi-factor authentication with sign-in verification for your company. If you have users that do not have smart phones, we still have you covered! You can also enable multi-factor authentication via SMS. Reach out to us to find out how.

**Step 1:** Have all your users download and sign into the Workplace Android or Workplace iOS app. This is important to make sure that all your users can get in.

**Step 2:** As a Company Manager, navigate to **Manage** > select **View all settings**

**Step 3:** Select **Company** and on the left sidebar of the following page select **Security options**

**Step 4:** Down at the bottom of the page select **Edit** and change **User MFA default** to **Sign-in verification**. At the bottom of the page, select **Save changes**.

**Step 5:** Toward the top of the page, select **Groups**, and on the following page select the **All Users** group and on the left sidebar of the following page select **Security options**

**Step 6:** Down at the bottom of the page select **Edit** and change **Require two factor authentication** to **Sign-in verification**. At the bottom of the page, select **Save changes**.

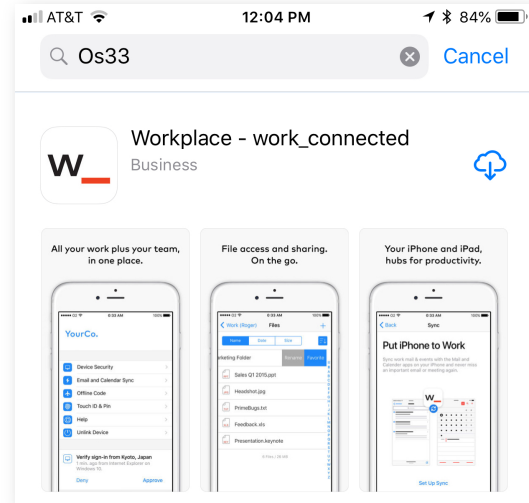
You may also refer to the following article from our Help Center.

<https://help.workplace.co/hc/en-us/articles/115007922108-Manage-the-company-s-sign-in-verification>

# Setting up MFA for Users

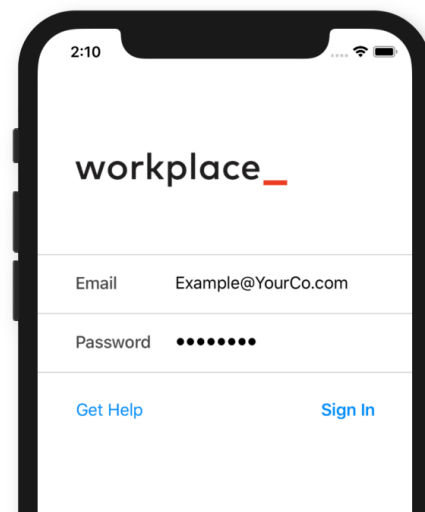
## Step 1

Download [Workplace Android](#) or [Workplace iOS](#)



## Step 2

Sign into the app and go through the setup process. Make sure to allow notifications!



## Step 3

Work with your company manager to turn on multi-factor authentication for your organization. You can always reach out to your Customer Success Manager or to our Help Desk for more information.

## Step 4

Use your phone as your second factor to sign into Workplace.

### Security options for [redacted]

Edit the company's security options and click the SAVE button.

Notification email:	<input type="text"/>	<input checked="" type="checkbox"/>
Allow forgot password:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Prohibit reuse of previous:	<input type="text" value="8"/>	passwords. <input checked="" type="checkbox"/>
Maximum password age:	<input type="text" value="90"/>	days. <input checked="" type="checkbox"/>
Session expires after idling:	<input type="text" value="120"/>	minutes. <input checked="" type="checkbox"/>
User MFA default:	<div>Sign-in verification <input checked="" type="checkbox"/></div>	

These security options defaults will be set automatically each time a user or group are created. The company manager can restrict users and groups inside the company to use two factor authentication.

If set to Inherited, users inherit this setting from groups and this setting can be overridden on a per-user basis in a user's security options.


If set to None, users authenticate using a password only.

If set to SMS, users are required to authenticate using SMS multi factor authentication.

If set to Symantec VIP, users are required to authenticate using Symantec VIP credential id and security code.

If set to Sign-in verification, users are required to authenticate using Sign-in verification multi factor authentication.

Symantec VIP credentials provided:	by your provider <input checked="" type="checkbox"/>
Allowed Countries:	<input checked="" type="checkbox"/> All <input checked="" type="checkbox"/>



When you sign into Workplace on a computer, you'll get a notification on your phone, asking you to verify your sign-in. When you **Approve** the sign-in verification, Workplace on the computer will allow you to continue access.

EMAIL US

customersuccess@os33.com

CALL US

800 646 0700

VISIT US

www.os33.com