|  |
| --- |
| Using multi-factor authentication (MFA) - Google |

# Using multi-factor authentication (MFA) – Google

It is recommended that you enable multi-factor authentication (MFA) in your organisation. MFA is an added step in the sign-in process which improves your security by requiring you to use a separate device to help verify your identity. This makes it almost impossible for a hacker to gain access to your account without also having your mobile phone. Google calls MFA “2-Step Verification” (2VS).

## What you need to do as an organisation

Follow these steps to enable 2VS:

1. **Inform staff about 2VS.**

Explain what 2VS is and why your organisation is using it.

1. **Allow users to turn on 2VS.**

Sign in to the [Google Admin console](file:///C:\Users\mleboze\AppData\Local\Temp\1.%20Edited%20Resources\admin.google.com) with your administrator account credentials and follow the steps in the [Allow users to turn on 2 Step Verification video](https://youtu.be/70N7TosV4h0). This will allow users to turn on 2VS but will not enforce 2VS yet.

1. **Ask staff to set up their 2VS.**

So your staff can turn on (“enrol in”) 2VS, send them these instructions: [Turn on 2-Step Verification](https://support.google.com/accounts/answer/185839). Give them a date by which they should complete their set-up.

1. **Track progress of staff completing their set-up.**

To track progress, see [Track users' enrolment in 2 Step Verification](https://www.youtube.com/watch?v=sCC9bpnPvy4). Remind staff if you need to.

1. **Enforce 2VS.**

Now all staff have set up their 2VS, it’s time to activate 2VS enforcement. Repeat step 2, but now, select **Enforcement** > **On**. Check that **Any** is selected for **Methods** (unless you have specified an enforcement method to your staff). To let users avoid repeated 2SV checks on trusted devices, under **Frequency**, check **Allow user to trust the device**.

## What to expect as an administrator

You can expect some initial support inquiries from users as they start using 2VS. You may need to provide guidance on setting up and using 2VS methods (eg, authenticator app, SMS, phone calls).

You can monitor 2VS progress and compliance status in the Admin console (see step 4 above).

## What staff can expect

Staff will receive email notifications and prompts to enrol in 2VS. These instruct them to follow on-screen instructions to set up 2VS by choosing a second verification step, such as a mobile app, security key, or phone call.

Once 2VS has been set up and enforced (step 5 above), staff may be prompted to use 2VS when attempting to access Google services or applications (eg, enter a temporary code that is sent to their mobile phone device via SMS or authenticator app). This will happen when the system detects what it considers a “risky” activity, for example trying to sign in from an unusual location.

Staff can manage their 2VS settings in their Google account settings.