evolve

Two-Factor Authentication Guidance

The purpose of this guidance is to explain how to turn on multifactor authentication for some popular applications.

Two-factor authentication (2FA), also known as multifactor authentication, is an extra layer of security used to verify the identity of the person trying to gain access to an account. Passwords can be stolen by cyber criminals to gain access to your accounts, so 2FA makes it much more difficult for them to gain access even if they can steal your password.

When 2FA is switched on, you'll have to provide a second factor in order to access your account. This is typically either by text message, an authentication app or a backup code, whereby an authentication app is considered the most secure. Some services will have 2FA switched on by default, but many do not. The following sections detail instructions on how to turn on 2FA for some popular business applications.

Microsoft 365

To allows users in your organisation to turn on 2-step:

1. Sign in to your admin center.
2. Select **Users** and **Active users**.
3. In the **Active users** section, Click on **Multi-factor authentication**.
4. On the **Multi-factor authentication** page, select a user to enable this for one user or you can perform a bulk update by clicking **update in bulk**.
5. Click on **Enable** under **quick steps**.
6. In the pop-up window, click on **enable multi-factor authentication**.

G Suite

To allow users in your organisation to turn on 2-step:

1. Sign in to your Google Admin console.
2. From the Admin console Home page, navigate to **Security**, then **Basic settings**.
   a. You may have to click **More controls** at the bottom.
3. Under **Two-step verification**, check **Allow users to turn on 2-step verification**.
4. Click **Save**.

To help your users to enrol in 2-step:

1. Tell your users to enrol in 2-step:
   a. Go to your Google Account.
   b. On the left navigation panel, click **Security**.
   c. On the signing in to Google panel, click **2-Step Verification**.
   d. Click **Get started**.
   e. Follow the steps on the screen.
2. Provide instructions for enrolling in 2SV methods:
   a. Security keys
   b. Google prompt
   c. Google Authenticator app
   d. Backup codes
   e. Text message or phone call

For further optional steps, such as enforcing 2FA to all users, see instructions here.

Citrix Cloud Workspace

To turn on 2-step for your organisation:

1. Sign in to your Citrix Cloud console.

2. Click the three lines in the top left corner, then click **Identity and Access Management.**
3. Under **Authentication**, find **Active Directory + Token (Tech Preview)**. If it says **Not Configured**, click the 3 dots next to this and click **Connect**.
4. If Cloud Connectors is already installed, then the **Connect to Active Directory** subsection should already have a green check mark. In the **Configure Token** subsection, just click **Save and Finish**.
5. Next, go back to the three lines in the top left corner and click **Workspace Configuration**.
6. Under **Authentication**, select **Active Directory + Token**.
7. Check the disclaimer and click **Confirm**.
8. When users now go to the login screen, they will need to enter a password token. There will be a link that says **Don't have a token?**, which prompts the user to step up an authentication method.

TeamViewer

To turn on 2-step for your account:

1. Sign in to your TeamViewer account.
2. Click your profile name, then click **Edit profile**.
3. Click **General**, then under the **Two factor authentication** section, click **Activate**.
4. Using an authenticator app on your mobile device, scan the QR code that appears on the screen. The app will automatically generate a code.
5. Enter the code generated by the app on the next page of the activation wizard.
6. The next time you log in to your account, TeamViewer will ask for a security code from the app.

LogMeIn

To turn on 2-step for your account:

1. Sign in to your LogMeIn account.
2. At the top of the page, click your LogMeIn ID, then **Account settings**.
3. Under the **Security** section, look for **Two-step verification is OFF** and click **get started**.
4. Choose the primary method you want to use to receive codes by clicking either **Set up mobile app** or **Set up text message**.
5. Follow the instructions for either method.
6. Finally, click **Activate** at the bottom of the page to turn on 2-step verification.

To enforce 2-step to anyone using your account:

1. In LogMeIn Central, click **Users** then **Login Policy**.
2. Under **Login process**, select **Two-factor authentication**.
3. Click **Switch on**.

For instructions on how to set up 2FA for many more applications (both business and personal accounts), please visit TeleSign's Turn it On tutorial archive, which is available here.