Setting Up Multi-Factor Authentication (MFA)

Last Modified on 28/10/2026 6:15 am AEST

Multi-factor authentication (MFA) adds a second step when you log in to StrataMax. As well as your password, you enter a six-digit code from an authenticator app on your smartphone or tablet. Even if someone learns your password, they cannot log in without your phone.

You set MFA up once, which takes only a few minutes. After that, logging in takes a few extra seconds.

MFA must be turned on for your organisation before the *StrataMax Managers Portal* can be enabled. You can also choose to use MFA when logging in to the StrataMax application itself, but that is optional.

Before you ask for MFA to be turned on

MFA is switched on for everyone in your organisation at once. If you are the person arranging it, check these points first:

- MFA must always be on to use the StrataMax Managers Portal, so it has to be switched on before the portal can be enabled for your organisation. Using MFA for the StrataMax application as well is optional, so tell the Support Team whether you want it for the Managers Portal only or for both.
- Everyone who uses MFA needs a smartphone or tablet to run an authenticator app.
- Each person sets up MFA on their own phone, with their own login, the next time they log in. Logins are never shared.
- StrataMax does not provide backup codes. Each person should turn on the backup option in their authenticator app (see Step 1).
- If someone loses their phone, your administrator can deny their access straight away, and the Support Team can reset their MFA (see *Lost or stolen phone* below).
- Tell your team beforehand, and ask for MFA to be switched on at a quiet time.

To have MFA turned on, contact the Support Team.

What you need

- Your StrataMax login (email address and password)
- A smartphone or tablet, with the ability to install an app

- MFA switched on for your organisation

In this article, "phone" means your smartphone or tablet.

Step 1: Install an authenticator app

An authenticator app is a free app that shows a new six-digit code every 30 seconds. It works without mobile signal or wi-fi, and it never needs your password.

Any standard authenticator app works with StrataMax. Two common free choices are:

- ***Microsoft Authenticator*** (iPhone, iPad and Android). It can back up your codes to the cloud (a personal Microsoft account, plus iCloud on iPhone) so you can restore them on a new phone. A backup restores to the same type of device only, so Apple to Apple or Android to Android.
- ***Google Authenticator*** (iPhone, iPad and Android). When you sign in to a Google account in the app, your codes sync to a new phone. Without an account, it can export your codes from the old phone to the new one using a QR code.

If your organisation already uses another authenticator app, you can use that instead. Check that it can back up or move your codes to a new phone.

TIP! Download the app from the App Store (iPhone) or Google Play (Android) only. Searching for "authenticator" shows many lookalike apps, so check the publisher is Microsoft Corporation or Google LLC.

Before you add StrataMax, open the app and turn on its backup or sync option. That is what lets you move to a new phone without setting MFA up again. StrataMax does not provide backup codes, so the app's own backup is your safety net. See the vendors' instructions: *Microsoft: Back up and recover account credentials in the Authenticator app* and *Google Authenticator help*.

Step 2: Link the app to your StrataMax login

1. On your computer, log in to StrataMax with your email address and password. The*StrataMax Multi-Factor Authentication* window appears with a QR code.



2. On your phone, open the authenticator app and choose *Add account* (usually a + button).
3. If the app asks what type of account to add, choose *Other account*, then choose to scan a QR code. The wording differs slightly between apps. If asked, allow the app to use your camera.
4. Point your phone at the QR code on your computer screen. A new StrataMax entry appears in the app, with a six-digit code.
5. Type the current six-digit code into the *Enter the 6-digit code from your app to complete setup* field in StrataMax, then select *Verify & Complete Setup*.

> The code changes every 30 seconds. If it changes while you are typing, enter the new one.

If you cannot scan the QR code

1. In the StrataMax window, find *Can't scan? Enter this key manually.* The setup key is shown underneath.
2. In the authenticator app, choose *Add account*, then *Enter a setup key* (or *Enter code manually*).
3. Enter a name you will recognise, such as StrataMax followed by your email address. Type or paste the setup key, and make sure the key type is *time-based* if the app asks.
4. Type the six-digit code from the app into StrataMax and select *Verify & Complete Setup*.

> Do not email, screenshot or print the QR code or the setup key. Anyone who has them can generate your codes. If you want to keep the setup key as a backup, store it in a password manager.

Step 3: Log in with a code

From now on, each time you log in to StrataMax:

1. Enter your email address and password as usual, then select *Login*.

2. When the message *Multi-factor authentication required* appears, open your authenticator app and find your StrataMax entry.
3. Type the six-digit code into the StrataMax window and select *Submit*.



Getting a new phone

A new phone does not mean setting up MFA again. Your authenticator app can move your codes across, so StrataMax carries on working with no reset.

1. Keep your old phone. Do not erase, trade in or recycle it until you have finished these steps and logged in to StrataMax with a code from the new phone.
2. Move your codes using the method you set up in your authenticator app:
    - ***Microsoft Authenticator:*** install the app on the new phone and sign in with the same Microsoft account you used for the backup. Your entries are restored. A backup restores to the same type of device only (Apple to Apple, Android to Android).
    - ***Google Authenticator:*** install the app on the new phone and sign in with the same Google account, and your codes sync. If you do not use an account, on the old phone choose *Transfer codes*, then *Export codes*. On the new phone, choose *Import codes* and scan the QR code shown.
    - ***Another app:*** follow that app's own instructions for moving accounts to a new phone.
3. Log in to StrataMax and check that the six-digit code from the new phone is accepted. Only then retire the old phone.

TIP! If your authenticator app tells you that accounts were recently exported and you did not do it, someone else may have your codes. Tell your administrator straight away.

If you cannot move your codes, for example because the old phone has already been wiped and there

was no backup, you will need your MFA reset. See *Resetting MFA* below.

Lost or stolen phone

1. Tell your administrator straight away. In *Security Setup*, your administrator removes your access permissions for the affected areas so nobody can use your login while the phone is missing. For example, if you use MFA for the *StrataMax Managers Portal*, they right-click that area and select *Deny*. If you use MFA for your whole StrataMax account, they deny access to the whole account in the same way.
2. Change your StrataMax password.
3. When you have a replacement phone, contact theSupport Team to reset your MFA (see below).
4. When the reset is done, repeat Step 2 on your new phone. Your administrator can then restore your access.

Resetting MFA

If you need our help to reset MFA, contact theSupport Team. For your security, we will always call you back on your organisation's company phone line to confirm the request before we reset anything.

Troubleshooting

StrataMax says my code is wrong

Wait for the next code and type it before it changes. If codes keep failing, check that your phone's date and time are set to *automatic*. A wrong clock is the most common cause. In Google Authenticator for Android you can also use *Time correction for codes*.

My phone will not scan the QR code

Allow camera access for the authenticator app in your phone settings and increase your screen brightness. If it still will not scan, use the setup key method in Step 2.

No QR code appears when I log in

MFA may not be switched on for your organisation yet. Ask your manager, or contact theSupport Team.

I use more than one phone or tablet

Scan the same QR code on each device during Step 2. A device cannot be added later without resetting MFA.

I do not have a smartphone or tablet

MFA needs an authenticator app on a smartphone or tablet. There is no other option at present, so everyone who uses MFA needs one. Raise this with your manager before MFA is turned on for your

organisation.