Multi-Factor Authentication

Multi-Factor Authentication (MFA) is an important security option that is available to StockMate users. A Tenant setting can be used to enforce the use of MFA for all users, or individual users can select to use the MFA functionality without the Tenant mandate.

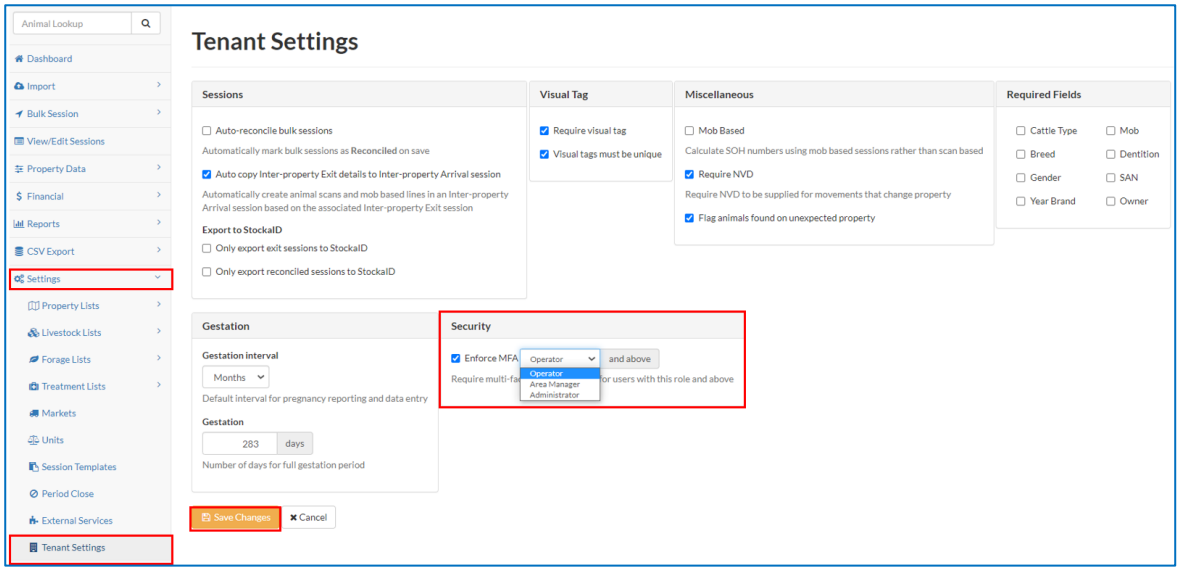
Once MFA has been enforced, an Authenticator App (Google Authenticator or Microsoft Authenticator) will need to be installed on a tablet/smart phone to produce time-based 6-digit codes required for Website login and App sync.

1.1 Activating Multi-Factor Authentication

1.1.1 Activate Multi-Factor Authentication via Tenant Settings

- **Note:** Only users with the Administrator Role are able to adjust the Tenant Settings to activate MFA across the tenancy.

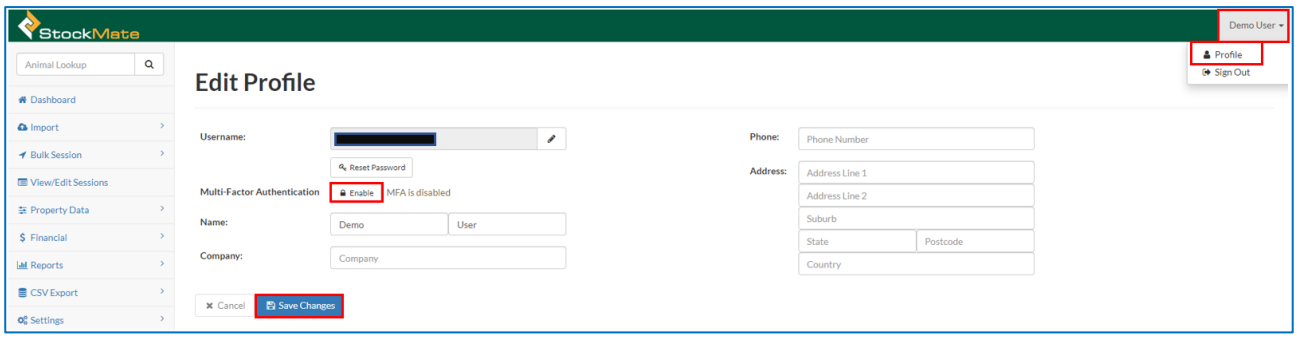
1. Select Settings, Tenant Settings, tick 'Enforce MFA' and select role option. Select Save Changes.
   - **Note:** All users with the select role and above will have MFA enforced.



1.1.2 Activate Multi-Factor Authentication – Individual User

Any user has the ability to activate the use of MFA for themselves.

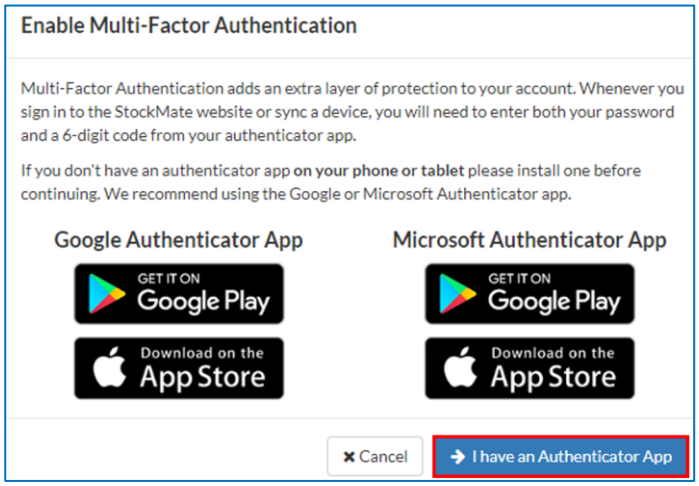
1. Select Username, Profile, Enable and Save Changes.



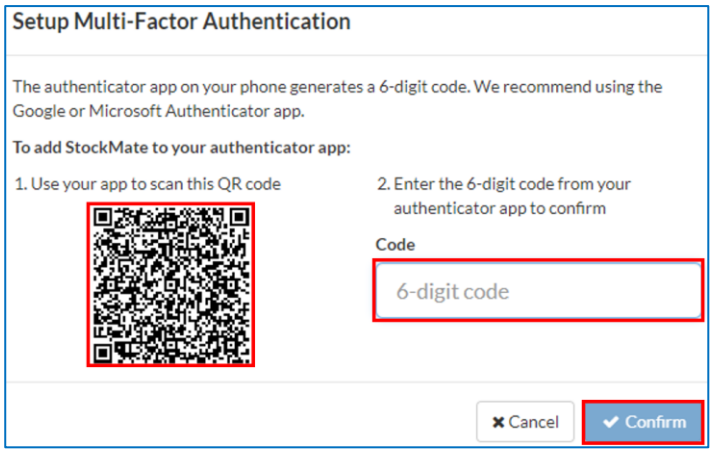
1.2 Authentication Setup

Once MFA has been enforced, on next login a 6-digit code will be required to be entered. Each user will require their own account on an Authentication App, they will need access to the device with the Authentication app whenever they login to the StockMate Website or App, or begin a Sync on the App. StockMate will prompt the user to download the Authentication App and assist with set up steps.

1. Enter Username and Password on StockMate Website login screen.
2. Download either Google Authenticator App or Microsoft Authenticator App on tablet/smart phone. On Web Select I have an Authenticator App.



3. On the Authentication App add a new account, select Scan a QR code.
4. Scan the QR code on the Authentication App. On the Website enter the 6-digit code generated by the Authentication App, select Confirm.



5. A one-time recovery code will be generated. Please write it down and keep it in a safe place. This can be used if ever the device with the Authentication App is lost or stolen to disable MFA for the user and allow user login.
   - **Note:** If the Tenant Setting requires MFA for the user, the user will be prompted to setup MFA upon their next login to StockMate.

1.3 Using Multi-Factor Authentication

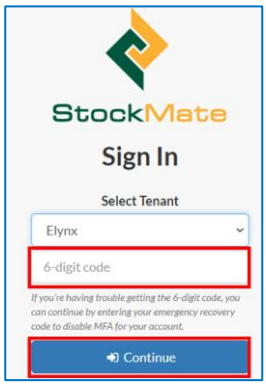
When MFA is enforced, each time a user logs on to the Website they will be required to enter their username and password followed by the 6-digit code generated by the Authentication App. On the StockMate App the 6-digit code will be required whenever the app contacts the web (upon sync, and on certain login occasions).

- **Note:** Change of password via Profile requires entry of 6-digit code.

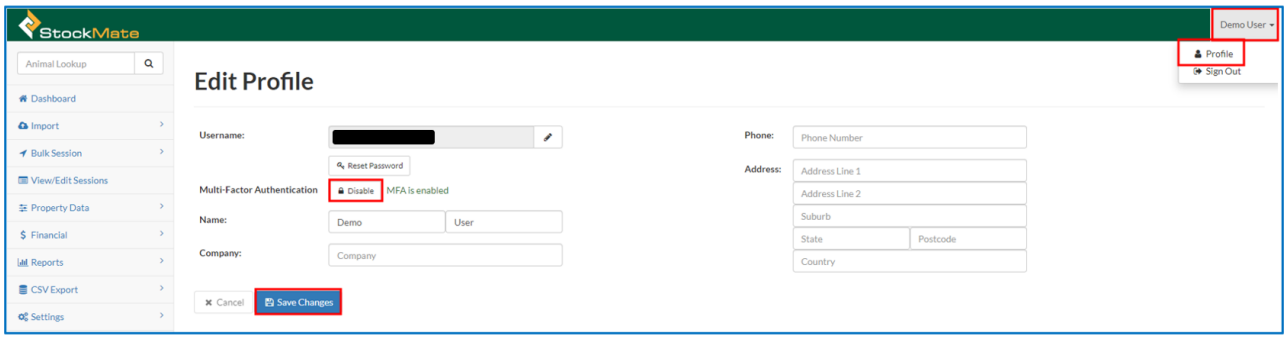
1.4 Disabling Multi-Factor Authentication

1. MFA can be disabled by entering the one-time recovery password, on website login if ever access to the Authentication App is lost.
   - **Note:** If the Tenant Setting requires MFA for the user, the user will be prompted to setup MFA upon their next login to StockMate.

   a. Enter Username and Password on Website login screen.
   b. Instead of entering the 6-digit code, enter the one-time recovery password to automatically disable MFA. Select Continue to login.



2. A user is able to disable their own MFA via their User Profile.
   a. Select Username, Profile, Disable, Enter 6-digit code, Disable, Save Changes.



3. A user with Administrator role is able to disable MFA for the Tenant via Tenant Settings.