Mandiant

USE GOOGLE AUTHENTICATOR FOR AUTHENTICATION

Setting up Google Authenticator for use is a two-step process. First the administrator configures the platform to use Google Authenticator, and then each user must configure their own account to use their Google Authenticator Token.

> If you have a software-based TOTP (Time-based One-Time Password) token that does not support SAML, you can try to use this option. For example, Symantec VIP has been successfully setup using the Google Authenticator option.

Administrator setup: Enable Google Authenticator

1. Go to **Settings** > **User Settings**. The User Settings page opens.
2. From the **Authorization Sources** drop-down, select **Google Authenticator**.
3. Click **Update Authentication Settings**. The authentication method is saved.
4. Restart your Director by selecting **System** from the Settings Menu and clicking **Reboot**. This is required before the new Authentication method is completely applied.

   > Existing user accounts are still configured with Local User Authentication by default. You must uncheck the **Local User Authentication** checkbox for each existing user that you want to enable for Google Authenticator.

   Once the Director is rebooted, the platform is ready for users to update their preferences to enable Google Authenticator.

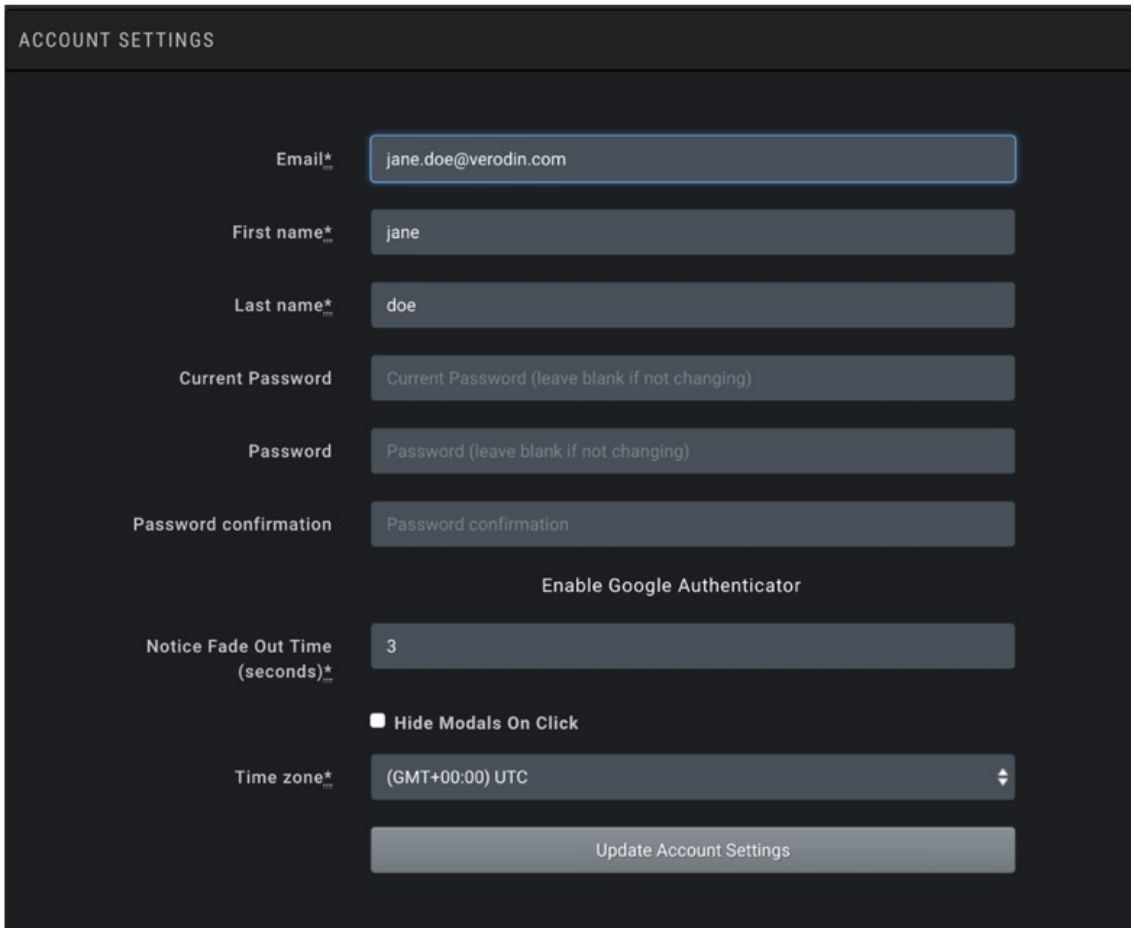
End user setup: Enable Google Authenticator for a user account

When administrators enable Google Authenticator, they also configure timing around the token timeout and time drift. These default to 3 minutes and 1 minute respectively. If users have issues with the tokens being accepted, these times might need to be increased.

Administrators configure the platform to allow Google Authenticator, but users must enable Google Authenticator on their own accounts, as described in the following procedure.

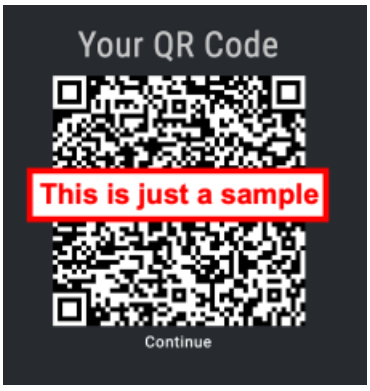
1. Sign into the Director and open **User** > **User Preferences**.

   > If your administrator has enabled Google Authenticator, you will see a Two factor code field. This field is optional until you complete this procedure.



User Preferences

2. Click **Enable Google Authentication**.
   This step brings up a QR code that's specific to your Validation Platform account.



Google Authenticator QR Code

3. Open Google Authenticator, select add **+**, select **scan barcode**. The code is created in Google Authenticator tied to your Validation Platform user name.
4. Click **Continue** under the QR Code to return to User Preferences.
   The next time you sign-in, you are required to enter the Google Authenticator token. If you do not, you will receive

an Invalid Username or Password message.

Restore Two-Factor Authentication access for a user

Use the following steps if a user is no longer able to authenticate to MSV (on-prem) using two-factor authentication (2FA). For example, the user lost their mobile device, got a new mobile device, or accidentally deleted the MSV entry in their authenticator app.

> These steps require assistance from an MSV user with administrative privileges.

Temporarily enable local authentication for the user (admin)

1. Sign into the on-prem Director as a user with administrative privileges, and then go to **Settings > User Settings**.
2. Click the pencil icon under the Actions column associated with the user and then select **Local User Authentication**. This allows the user to sign in locally and then reestablish their 2FA connection.

Reconfigure two-factor authentication (user)

1. As the user who lost 2FA access, from the on-prem Director sign-in page, go through the forgot password steps and set a new password.

   > If you're not sure about where to sign in, work with your administrator.

2. When signed in, access `https://DIRECTOR_IP/two_factor`, where *DIRECTOR_IP* is the IP address of the Director you're already signed into. You should see a QR code.
3. Using your mobile device, scan the QR code and go through the steps to enroll in two-factor authentication.
4. Sign out from the Director session.

Disable local authentication for the user (admin)

1. As a user with admin privileges, sign into the on-prem Director and go to **Settings > User Settings**.
2. Click the pencil icon under the Actions column associated with the user and then deselect **Local User Authentication**. The user can sign in again using 2FA.