Set up two-factor authentication

With two-factor authentication, use a secure, app-generated token to verify your administrative account. This is a time-based, one-time password that is generated using an app on your mobile device used to securely sign in to the administrative portal from a previously unverified browser or device.

Recommended apps for authentication include Google Authenticator, Microsoft Authenticator, or Authy.

To turn on two-factor authentication for your account:

1. Click on your username in the top right of the page.
2. On the My Profile page, under Account Information, your 2-Step Verification status is displayed. Click **Manage Settings** to update your authentication settings.
3. Click **Enable 2-Step Verification**.
4. Enter your password and click **Authenticate**.

   Verification codes are sent to the email address associated with your account to verify future login attempts.
5. Click **Switch to Token-Based Verification** to enable verification via an app. We recommend that you upgrade to our more secure token-based verification.
6. Enter your password and click **Authenticate**.
7. Scan the QR code provided with your chosen authenticator app. You will be provided a time-based token, which is entered in the Verification Code field below the QR code.

   Once complete, a confirmation message is displayed.

To turn off token-based verification, click **Use Email Verification**. To turn off two-factor authentication verification, click **Disable 2-Step Verification**.

Revision #4

Created 26 July 2022 15:37:11

Updated 26 July 2022 15:47:40