

Authenticator App and User Security Enhancements

DireXions 2026

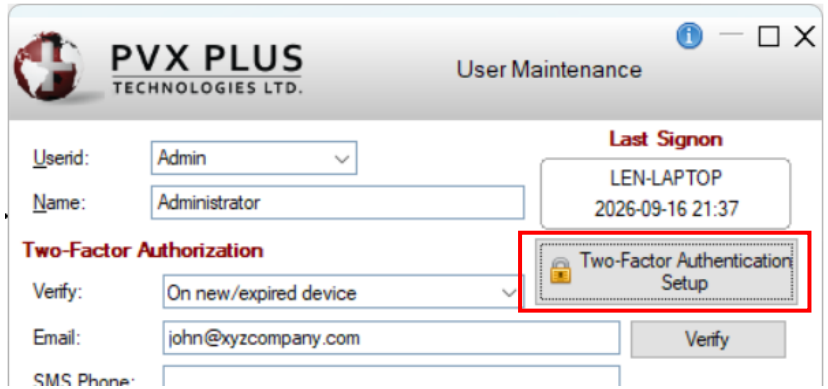
Authenticator Apps and User Security

- Added an Authenticator App as another two-factor authentication (2FA) option for NOMADS/iNomads applications
- Users scan a QR code to set up Microsoft Authenticator, Google Authenticator, or another TOTP-compatible app
    - The QR code is the enrollment/setup mechanism. It contains the secret used to configure the authenticator app
- Uses industry-standard Time-Based One-Time Passwords (TOTP)
    - TOTP verification codes are generated directly by the Authenticator App and change periodically, so the authentication process does not depend on receiving an email or text message
- Users enter the time-sensitive verification code generated by their Authenticator App when signing in
- Provides an alternative to authentication codes delivered by email or SMS
- Helps strengthen application security without requiring additional authentication hardware

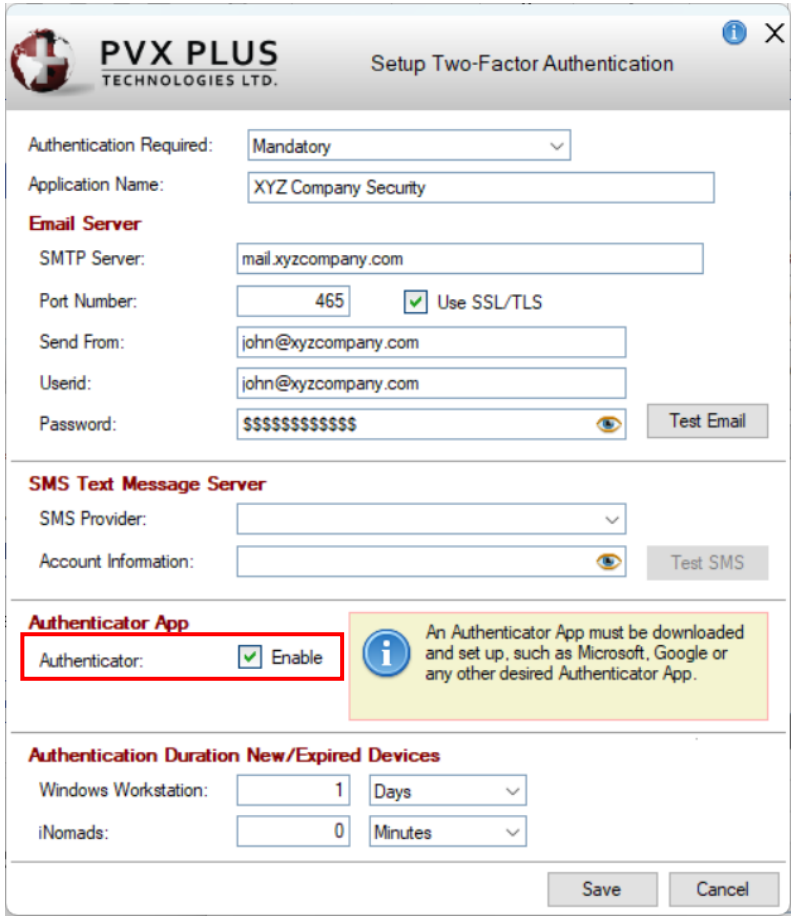
Authenticator Apps and User Security

Enabling the Authenticator App

- In User Maintenance, select the Two-Factor Authentication Setup button



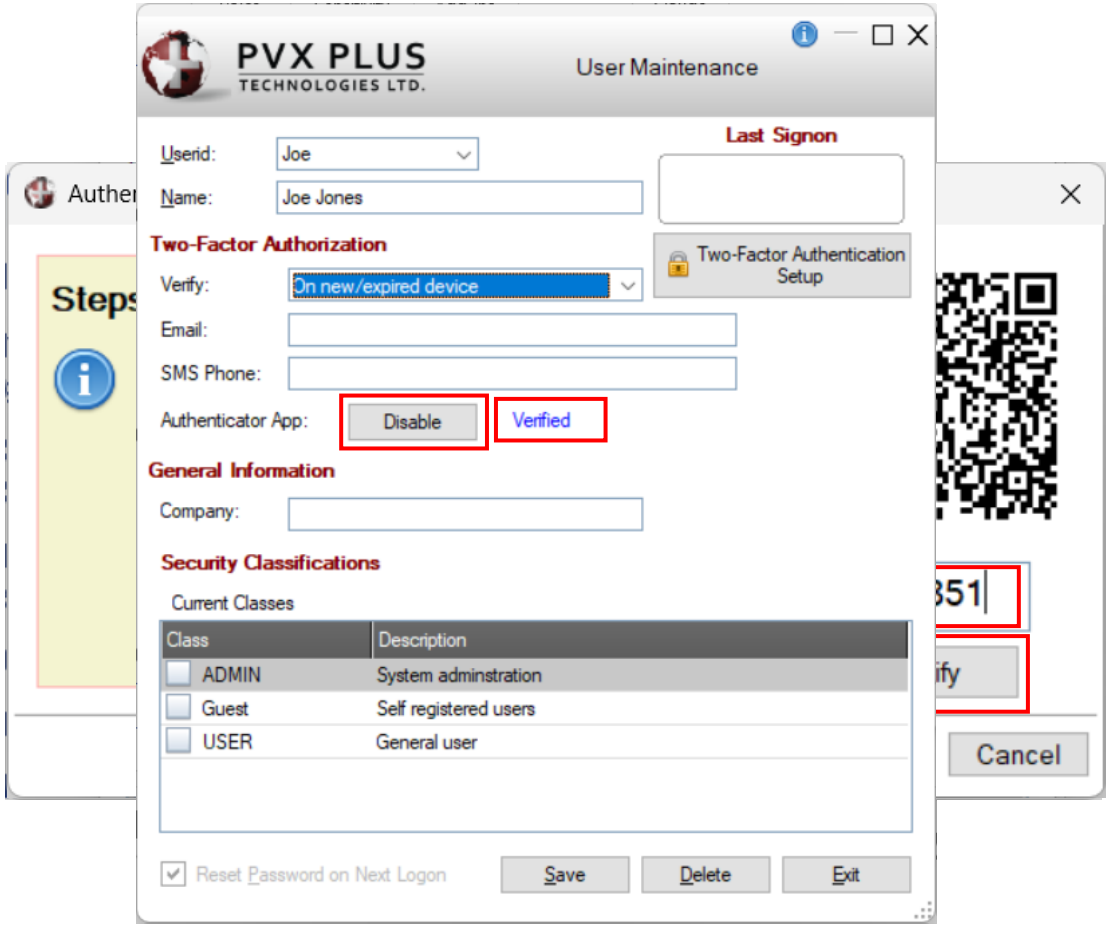
- From the Setup Two-Factor Authentication Setup dialog, check the Authenticator Enable check box in the Authenticator App section
- Once enabled, it becomes available for configuration when setting up a user



Authenticator Apps and User Security

Enabling the User

- Requires Authenticator App
- In User Maintenance a new Authenticator App section was added
- Selecting the Setup button launches the Authenticator Setup dialog
- In this dialog, with your Authenticator App on your phone, scan the QR Code
- When the QR Code is scanned a new entry is created on the App with a verification code
- Enter the verification code and select the Verify button
- If verification was successful a Verified message is displayed with a Disable button
- Selecting Disable button will remove the Authentication



Authenticator Apps and User Security

Sign On

- When the user signs on they enter their User Id and Password
- Upon acceptance the Two-Factor Verification dialog is displayed
- On the App a TOTP verification code is generated for the user
- In the Two-Factor Verification dialog enter the generated verification code and select Verify
- If accepted, it continues with the next step

Note: When signing in, if the user has email or SMS verification, they will be asked to select which authentication method to use

