DXOP 2 Factor Authentication

With the demand for increased security and to drastically reduce the incidence of online identify theft, fraud, and access, DataExpress offers Two Factor Authentication (2FA) for its HTTP/S file transfer protocol.

2FA, a subset of Multi Factor Authentication, forces a user to provide additional validation beyond password-only protection at time of logon. 2FA validates both a user-known password as well as a system generated one-time secret key.

The DXOP 2FA service offering is based on the Google Authenticator application which is widely available for both iOS and Android phones

2FA Features

- DXOP interfaces with the Google Authenticator Library
- One-Time secret key is generated and sent to the user
- At logon, user is prompted to authenticate with a random one-time phone-generated code
- Random code changes every 30 seconds

2FA Administration

- 2FA is a licensed module requiring a new product license
- DXOP administrators can turn on/off 2FA per user
- A new secret key can be generated in the case of suspected compromise

2FA Configuration

- Once 2FA is turned on for a user, a secret key is generated and sent to the user
- Two delivery options are available, either Text String or QR Code
- The secret key is copied or scanned into the app, and the user is ready to go
- Each login request will challenge for a new authentication code
- Failure to provide a valid code will deny the user access

2FA FEATURES

- ADMINISTRATOR CONFIGURABLE
- ADDED SECURITY
- OPTIONAL ON/OFF PER USER