TD SYNNEX

PartnerFirst Digital Bridge

Digital Bridge Security & Trust

Secure. Scalable. Trusted by the Channel.

Security Built Into Every Connection

PartnerFirst Digital Bridge protects customer data with enterprise-grade security at every layer. Every connector uses encrypted communication, isolated environments, and modern authentication — ensuring safe, seamless automation without added complexity.

Key Security Principles

Zero Access to Credentials

TD SYNNEX never stores passwords or OAuth tokens. Authentication happens through secure, temporary API handshakes.

Encrypted Data in Motion

All communication uses HTTPS with TLS 1.2+ encryption and travels through secured, audited infrastructure.

No Data Stored

No customer-sensitive data is stored. Only the minimum required information is processed to complete each action.

OAuth2 Credential Management

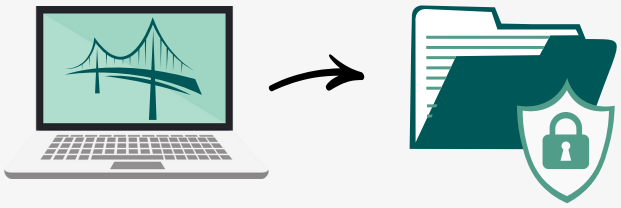
Customers fully control access keys and tokens, which can be updated or revoked at any time.

EC Express Authentication

All connectors use TD SYNNEX's validated, encrypted authentication framework for consistent, secure access.

Why It Matters

- Protects sensitive data end-to-end
- Reduces exposure by eliminating credential storage
- Ensures every API call is validated and encrypted
- Supports secure automation at scale
- Backed by TD SYNNEX engineering and DevSecOps reviews



Built for Secure Automation

Secure by Design

APIs and templates are accessible only after authentication.

Segmented Environments

Integrations run in isolated containers to ensure full separation of customer data.

Continuously Audited

Connectors are reviewed and monitored by TD SYNNEX Engineering for safe configuration and compliance

PartnerFirst Digital Bridge

For more information, contact your TD SYNNEX representative or visit tdsynnex.com/na/us/digital-bridge/ms-apps