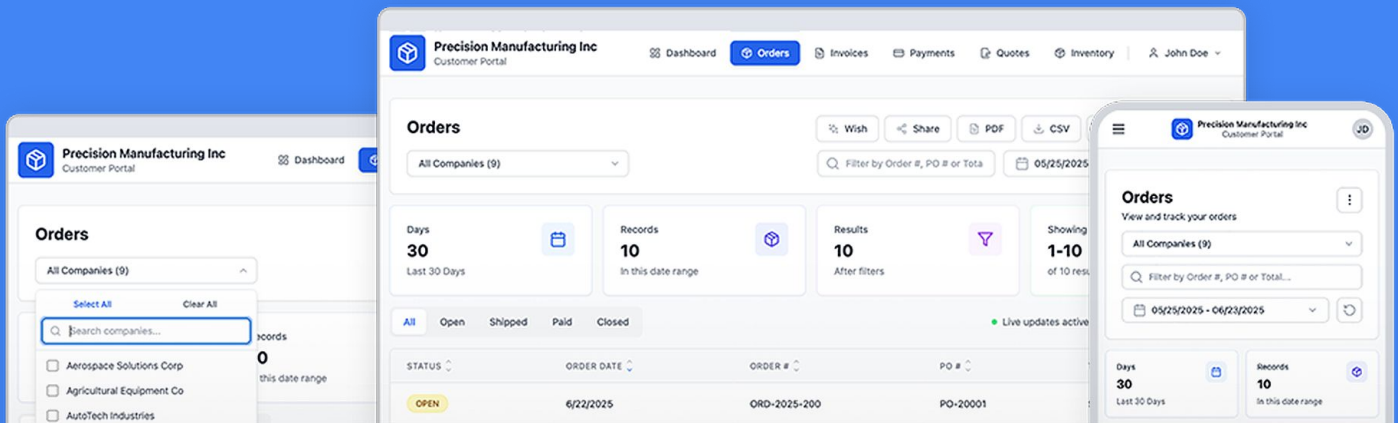
EXPERT INTERNET MARKETING

Security Overview

Customer Portal for Global Shop Solutions

SECURE. SCALABLE. TRUSTED BY MANUFACTURERS SINCE 2010.



EXECUTIVE SUMMARY

Manufacturers using Global Shop Solutions ERP can now provide their customers with secure, real-time access to invoice, payment, order, quote, inventory and purchase order information through the integrated Customer Portal. We protect your data with multiple layers of security, like a digital fortress. Our approach focuses on these key areas:

- Your Server
- Sending Data
- Our Server
- Our Portal

Whether you're managing one customer or thousands, security remains at the core of every interaction.

Copyright 2025 Expert Internet Marketing. All rights reserved.

SECURITY ON YOUR SERVER

SECURITY	EXECUTIVE DESCRIPTION	TECHNICAL DESCRIPTION
Read-Only Access	The connector has read-only permission, meaning it can only copy data from your database but can never change or delete it.	The application's database access is limited to SELECT statements, enforcing a read-only operational model to preserve source data integrity.
AES-256 Authenticated Encryption	Your database passwords are scrambled using the same highly secure encryption standard that banks and governments rely on to protect classified information.	Database credentials are encrypted client-side using AES-256-GCM, with the key derived via PBKDF2, providing authenticated encryption to protect configuration data at rest.
Local-Only Credential Processing	Your database login details never leave your computer and are only used to connect directly to your database.	Database credentials are used exclusively for local ODBC connection establishment and are never exfiltrated or transmitted over the network.
Code Authenticity	The application is digitally signed to prove it's authentic and hasn't been altered, a check that Windows performs automatically for your safety.	The executable is protected by an Authenticode signature, which the OS validates during process creation to ensure code integrity and prevent tampering.
Limited Permissions	The application is purpose-built to be safe and lacks the ability to access other programs or change system settings.	The application operates with the principle of least privilege, with no file system, registry, or process interaction capabilities beyond its explicit operational scope.
Strict Data Whitelisting	The connector is only allowed to touch specific, pre-approved data tables, preventing it from ever accessing unauthorized information.	Data access is restricted by a hardcoded table name whitelist that prevents runtime modification, effectively blocking access to any non-approved database objects.
Secure Query Validation	To prevent database attacks, the connector is built to reject any request that doesn't follow a strict set of pre-approved safety rules.	To mitigate SQL injection vectors, the application validates all table and column identifiers against a restrictive regex filter before query construction.
Automatic Sensitive Data Redaction	To prevent accidents, sensitive data like passwords and keys are automatically removed from log files before they are saved.	The logging service employs regex-based data masking to redact credentials and API tokens from all log outputs, preventing sensitive information leakage.
Pre-Startup Security Validation	Before starting, the application runs a safety check on itself to make sure all its security features are configured correctly.	The application performs a series of startup validations to ensure its security components are correctly configured before any processing begins.

Copyright 2025 Expert Internet Marketing. All rights reserved.

SECURITY SENDING DATA

FEATURE	EXECUTIVE DESCRIPTION	TECHNICAL DESCRIPTION
Short-Lived JWT Authentication	The connector uses a temporary access token that expires after 24 hours, at which point it automatically and securely obtains a new one from the server.	The client utilizes JWTs with a 24-hour lifetime and automatically re-authenticates to acquire a new token upon expiration.
End-to-End TLS Encryption	All your data is sent over the internet using the same secure, encrypted connection that banks use for online banking.	Data in transit is protected end-to-end using HTTPS with modern TLS 1.2/1.3 cipher suites enforced on the server.

SECURITY ON OUR SERVER

FEATURE	EXECUTIVE DESCRIPTION	TECHNICAL DESCRIPTION
Google Cloud Infrastructure	Our systems run on Google's world-class cloud platform, benefiting from the same security and reliability that powers services like Gmail and YouTube.	The backend infrastructure is hosted on Google Cloud Platform (GCP), leveraging its secure-by-design infrastructure and managed security services.
Data-at-Rest Encryption	Once your data arrives at our servers, it is immediately scrambled using the same powerful, bank-level encryption used to protect financial records.	All data at rest, including persistent disks and storage buckets, is encrypted by default using AES-256 within the Google Cloud environment.
Third-Party Audited Compliance	Our cloud provider is regularly audited by independent experts to prove it meets the highest global standards for security, privacy, and operational excellence.	The underlying infrastructure maintains compliance with key industry attestations, including SOC 2 and ISO 27001, which are validated by independent third-party audits.

THIS AREA IS INTENTIONALLY LEFT BLANK.

Copyright 2025 Expert Internet Marketing. All rights reserved.

SECURITY ON THE PORTAL

SECURITY	EXECUTIVE DESCRIPTION	TECHNICAL DESCRIPTION
Network and Application DDoS Mitigation	We provide automatic defenses against common network-level attacks, with advanced protection against more complex application attacks available as an optional upgrade.	The infrastructure includes baseline mitigation for network-layer (L3/L4) volumetric attacks, and customers can opt-in to a managed WAF for application-layer (L7) protection.
CRM-Integrated User Authentication	Only active customer contacts listed in your Global Shop Solutions CRM are allowed to create an account or log in to the portal.	The authentication mechanism is coupled with an external CRM system, which acts as the authoritative source for user identity and status verification.
Robust Password Strength Enforcement	Our portal uses the same advanced password-checking technology pioneered by Dropbox to ensure your password is truly strong and not easily guessable.	The password policy leverages a proven strength-estimation library, originally developed by Dropbox, to score password resilience against modern cracking techniques and block common patterns, moving beyond simple complexity rules.
Multi-Tenant Data Isolation	Each user can only see data for the specific companies they are assigned to, keeping everyone's information private.	A multi-tenant data architecture enforces strict data segregation, ensuring that user sessions are scoped to only access resources associated with their organization.
Containerized Tenant Isolation	Each company's portal runs as a separate, isolated application to prevent any one customer from affecting another.	The platform employs tenant isolation at the application layer, containerizing each customer's instance to prevent cross-tenant data leakage or performance impact.
AI-Driven Bot and Threat Mitigation	Our systems are guarded by a smart, AI-driven security shield that learns from global threats in real-time to automatically block malicious bots and hacking attempts.	We deploy an integrated, AI-powered security platform that provides multi-layered defense through real-time threat detection, a WAF, proactive bot mitigation, and runtime protection against zero-day exploits.
Timely Security Patch Application	We protect our systems by automatically applying the latest security updates and patches to our servers as they become available.	A comprehensive patch management policy ensures timely application of security updates to the OS and software stack, minimizing the exploitability window for known vulnerabilities.
Periodic Security Hardening Reviews	We regularly review all our features against the latest security standards to find and fix potential risks before they become a problem.	The SDLC incorporates recurring security reviews and threat modeling based on frameworks like OWASP to ensure features are hardened against emerging threats.

END

Copyright 2025 Expert Internet Marketing. All rights reserved.