GSI

gShield Authentication

gShield Benefits

- Improved Credentials Security
- Stronger Data Security
- Protection for Mission Critical Data
- Minimally Invasive – One-Time User Event
- Only Product Compatible with JD Edwards

gShield Functionality

- Two-factor Authentication (2FA)
- 1st Component: Username and Password
- 2nd Component: Email Address or Mobile Number
- 6 Digit Authentication Code/ QR Code
- One-time Event per Device

GSI

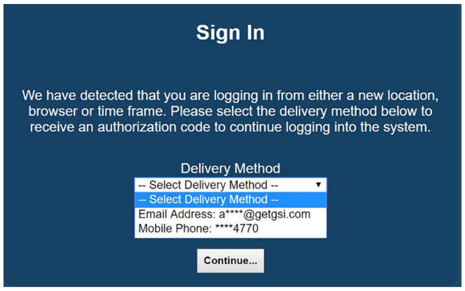
ERP Expertise.
Business IQ. Cloud Sense.

Are you concerned about unauthorized access to your JD Edwards system? System credentials can be acquired through cyber-attacks and other malicious activity including phishing campaigns, malware-trojans, keyloggers, remote administration tools (RAT), brute force attacks, paper notes, and other methods.

GSI's gShield Authentication protects your organization's mission critical information in JD Edwards, providing an additional layer of credentialed security when a user is logging in to the system. GShield Authentication uses two factor authentication (2FA) technology, also known as multi-factor authentication, to provide a second level of validation beyond your JD Edwards username and password credentials.

gShield AUTHENTICATION

This second level of authentication is quickly validated by sending a code to the user's email or mobile phone, or by generating a QR Code using Google Authenticator or Authy. The resulting code is entered on an authentication page before the user is granted access to JD Edwards.

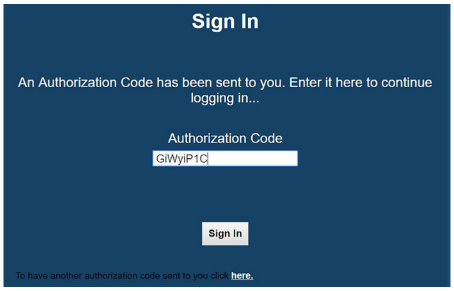


Sign In

We have detected that you are logging in from either a new location, browser or time frame. Please select the delivery method below to receive an authorization code to continue logging into the system.

Delivery Method

-- Select Delivery Method --
-- Select Delivery Method --
Email Address: a****@getgsi.com
Mobile Phone: ****4770



Sign In

An Authorization Code has been sent to you. Enter it here to continue logging in...

Authorization Code: GiWyiP1C

To have another authorization code sent to you click here.

Two Factor Authentication

Two-factor authentication (2FA) was created to prevent unauthorized access to your systems caused by cyber-attacks and other malicious activity. 2FA uses an authentication system to double check your identity when logging into an application or website by utilizing a combination of two separate components of authentication. These components generally fall into three categories: 1) something you know, 2) something you have in your possession, 3) something specific to you (i.e. fingerprints, etc.). An example of this would be withdrawing cash from a bank machine. The only way you can withdraw cash is by having a bank card (something you possess) and a PIN (something you know).

ORACLE® Platinum Partner

gShield Authentication

GSI has implemented gShield Authentication in a similar manner. The first of the two components is something you know, your username and password. You will enter these credentials when attempting to log into the system. GShield Authentication has two options for the second component (something in your possession): 1) email address, 2) mobile phone number. There are three options as to what is sent to the second component. The first is a 6-digit authorization code sent either via SMS (text) to your phone, or via a registered email account. Once you have the received the code, you will enter it on the two-factor authentication page before being granted access to the system.

The last option is a QR code, which is based on your username, the name of the site being accessed and the current date/time. This type of authentication is called a Time-based One-time password (TOTP). After being presented with the QR code, you will scan the code with your mobile device with an app such as Google Authenticator or Authy. After scanning the QR code, the mobile app will present you with a 6-digit authentication code. This code is valid for only a 30 second time period; after which it will be regenerated and presented to you.

According to industry experts, up to 95% of data breaches are perpetrated by hackers that have first stolen users' credentials and then used those credentials to commit fraudulent activities. Implementing a strong 2FA solution can help eliminate this threat to your JD Edwards system.

To learn more about securing your data using gShield Authentication, please visit www.GetGSI.com/gShield-Authentication.

GSI, Inc.

As a certified Oracle Platinum Partner and a recognized industry leader, GSI, Inc. (GetGSI.com) specializes in providing a broad spectrum of business, functional, and technical consulting services for Oracle JD Edwards, Oracle NetSuite, Oracle Cloud, Salesforce and other enterprise applications. The company also offers an extensive array of cloud/hosting options to meet the specific requirements of an organization including: Oracle Cloud, Amazon Web Services (AWS), Microsoft Azure and JDE Cloud⁹. GSI's comprehensive suite of solutions include AppCare, a 24/7 managed service; GENIUS, an advanced monitoring application; GENISYS, a solution for modeling, measuring and maximizing system performance; gShield, a security application and RapidReconciler®, its inventory reconciliation software. GSI consulting services are backed by its signature 100% guarantee. Founded in 2004, the rapidly growing company is headquartered in Atlanta with locations nationwide. GSI, Inc. was named to Inc. Magazine's Inc. 5000 list of fastest growing companies for two consecutive years.

RapidReconciler is a registered trademark of GSI, Inc. All other trade names are the property of their respective owners.

Credentials can be stolen through:

- Phishing campaigns
- Malware/Trojans
- Keyloggers
- Remote Administration Tool (RAT)
- Brute force attacks
- Same credentials across all accounts
- Easy to guess passwords
- Shoulder surfing
- Information taken from notes on PC

ORACLE
JD Edwards

GSI

ERP Expertise.
Business IQ. Cloud Sense.