Exago BI **Security**

Exago's customizable access controls, secure browsing, and APIs ensure you maintain total control over your application's security and comply with data safety standards.

APIs

Exago BI's flexible APIs allow you to store as much or as little information as you like in a base configuration file, then populate the rest via the API at runtime for specific users and sessions.

- Anything set via the API is stored in an AES 128 encrypted file on disk until the session is loaded, at which point the information is stored in memory, and the encrypted file is deleted.
- For REST APIs, we use REST authentication headers to secure the interface.
- The REST API does not need to be exposed to the web, so entry points into the application are isolated and only accessible to designated servers.

Secure Browsing

Since Exago BI is 100% browser-based, we recommend using only HTTPS connections and take every precaution to keep you and your clients data private while accessing the application.

- Exago uses multiple levels of input/output sanitization, blacklisting, and whitelisting to prevent cross-site scripting attacks.
- The administrator has the ability to enable anti-forgery tokens to prevent cross-site request forgery (CSRF) attacks.
- Cookieless Sessions can be optionally configured to store secret session identifying information in the page, which is secured via the standard https connection.
- The Admin console is password protected with the password being stored as a hashed encrypted value and the configuration file itself is encrypted using AES-128 with a 24-character cipher key.

"We spent a fair bit of time looking at other .NET OEM and embedded BI solutions, but only Exago could be seamlessly integrated with our application and meet our extensive database user security model and filtering requirements."

-Tom Gimpel | **SofterWare**
VP Product Development Delivery

"Exago's multi-tenant option gives us security knowing that we can put something in the cloud, have one Exago instance, and have more control over how users access the interface."

-Jared Fletcher | **Quorum Business Solutions**
Data Analyst

Compliance

Exago BI does not copy or save any data passed to it while running reports, so it does not interfere with your application's adherence to relevant compliance standards.

- No copies of the data persist longer than any files in the temp directory are allowed.
- All data is stored in temporary files on the web server and you dictate the cleanup time for those files.
- Roles and tenanting let you control which data each of your clients can access at all times.
- Exago BI can be run on a FIPS compliant server which restricts use of unsecured encryption algorithms.
- Exago supports web farms and uses load balancing on our scheduler service for disaster recovery plans and high availability.

Support

Our Technical Support team provides you with full-time secure support using encrypted or sample data when working within debug packages. Many of our healthcare and financial services clients perform regular penetration testing on our web application with the assistance of our Support team.

Contact us to discuss your integration and security options in more detail.

exago

Get in touch!
info@exagoinc.com
www.exagoinc.com
(203) 225 - 0876