ADAPTIVE SECURITY
Analytics Requirement

The Security Challenge

For application teams, security scenarios can be complex and have very precise requirements. Considerations may include partitioning multi-tenant data, limiting access to individual records in the data, or securing different parts of the application, workflow, and capabilities. Implementing these scenarios in an analytic application can be a daunting task. If software engineers have to recreate or replicate authentication and authorization information in the analytics tool, it will negatively impact their ability to maintain, grow, and adapt the product over time.

3 THINGS TO KNOW

Logi can seamlessly inherit your existing security model and supports multi-tenancy, so you can manage all security settings in a single place as you do today.

SecureKey is our SSO approach to pass any/all rights, roles or other security information (i.e. tenant or client info).

We support SSO direct authentication, LDAP/AD, Windows authentication and many more.

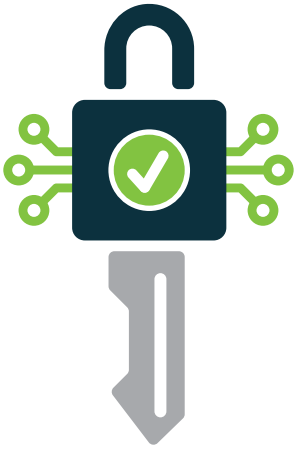
Adding Analytics Capabilities while Preserving Your Existing Security Model

At Logi, most of the companies we talk to have invested significant time and effort on a sophisticated security model. They've designed their security to allow the right parties access to the right data throughout their application. However, few analytics vendors leverage those existing security models—resulting in an inefficient structure that stores user information across multiple systems. This ends up causing:

- **Wasted Developer Time.** Instead of iterating on the core IP, developers are forced to address security problems caused by replication or mapping.
- **Poor User Experience.** If security is not replicated on the right schedule, it could lead to limited access for users, potential security risks, and an overall poor experience.
- **Limited Scalability and Flexibility.** As you make changes to your security permissions and to the data model, it could require reimplementation and limit sharing possibilities between groups with different access levels.
- **It Delays Your GA.** Replicating, testing, and deploying a duplicate security model requires time and testing resources that will inevitably delay your release date.
- **No support for multi-tenant deployments.** Many analytics vendors build proprietary security systems that do not support multi-tenant deployments or the sophisticated security requirements of analytic applications.

7900 Westpark Drive, Suite A200 + McLean, Virginia 22102 + 1.800.564.4965 + LogiAnalytics.com

ADAPTIVE SECURITY
Analytics Requirement

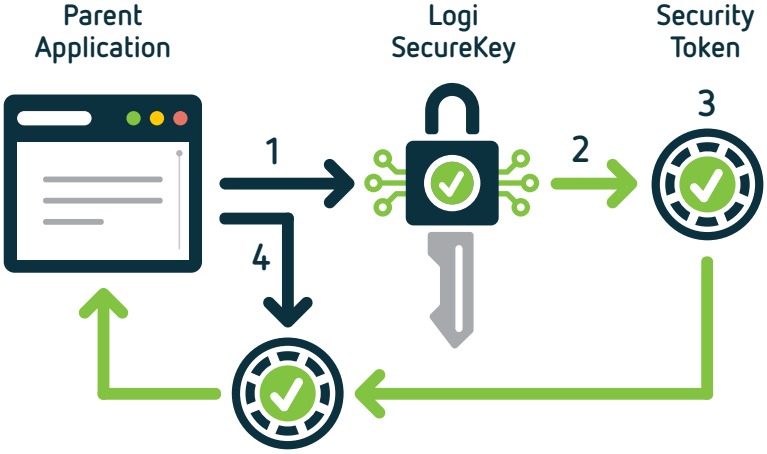


Logi's Solution: SecureKey

The foundation of Logi's approach is SecureKey, an adaptive security model that allows your existing application to manage users as it does today. SecureKey is a token-based API that enables you to reuse your existing authentication and authorization mechanisms to control access to Logi's analytics. Security is then dynamically leveraged to control access at the full page level, component level, or down to the row and column granularity of the data. This enables you to reuse report components across user roles/tenants and enable secure sharing of content between users, all while ensuring each user only sees the data and content they have the right to see.

SecureKey allows you to support secure, multi-tenant capable embedded analytics that act as a seamless part of your application. There's no need to manage users across multiple applications or deal with complex customizations or techops administration.

How SecureKey Works:



1. Your app sends an HTTP request to Logi for a security token
2. Logi receives and authenticates request
3. Logi returns unique session token with specified permissions and begins session
4. After the token is sent back, the token is used in subsequent requests for that session as part of authentication.

SecureKey Benefits:

- Relies on existing user roles and rights in multi-tenant architectures
- Provides data security at the row, column, and table level
- Always in sync with changes to user roles, rights, or access changes
- Passes important information—like which database to use for the current customer — for shared multi-tenant environments

Learn more at LogiAnalytics.com

7900 Westpark Drive, Suite A200 + McLean, Virginia 22102 + 1.800.564.4965 + LogiAnalytics.com