LUMEN APPLICATION SECURITY MODEL

Matt Hilt, Research Scientist
Numerica Corporation
matt.hilt@numerica.us, 970-207-2221

The security of law enforcement data is paramount. In order to protect such data from inadvertent disclosure or unauthorized use, Lumen is designed to satisfy the requirements of the FBI Criminal Justice Information Systems (CJIS) Security Policy. Lumen provides the ability to shared law enforcement data among consenting agencies, but allows each agency to partially limit what information is shared. This document gives an overview of the security measures put in place in order to enable this feature. Please contact Numerica for additional details.

Access Tokens

Lumen uses **access tokens** to enforce permissions within the application; these are short words describing groups of users that can have different restrictions on data viewing. Numerica engineers define the tokens for each customer during the onboarding process. Usually a customer has a single token, but more can be added if needs dictate. A token called "shared" is added to the department if the customer is participating in a data sharing agreement with other agencies.

User Tokens

When new users are added to Lumen**, the user administrator can determine which access tokens the user will obtain**. Generally users should obtain all the tokens available to the customer. However, if the customer has setup a special permissions group (*e.g.* internal affairs or similar sensitive categories), then the user may obtain only a subset of the available tokens. Users must have the "shared" token in order to view data from other agencies.

Data Collections and Collection Tokens

Lumen uses the concept of data collections to separate portions of the customer's data. For instance, each database table imported from an RMS is stored as a separate data collection. Mugshots or scanned documents are examples of other potential data collections. Each of these collections is assigned default access tokens during customer onboarding; these tokens may be the same as the customer tokens, or they may be a subset of the customer tokens. **Collections that should only be viewed by certain users should have a restricted set of tokens.**

Document Tokens

Tokens are attached to customer documents when Lumen's backend servers process them. A document belongs to exactly one data collection, and the collection defines the maximum set of tokens that may be attached to a document. **Each individual document may receive fewer tokens (i.e. a more restrictive set) than its parent collection according to the content of the document**. For example, documents from a database table with a true/false column called "restrict" might be limited from inter-agency sharing when the restrict value is true.

User Access

When a user performs a search, the resulting documents are first checked to ensure that the user can view them. **The user must possess at least one access token that is attached to the document in order to view that document in the search results**. Similar checks are done for accessing the full document via our API.