# Sentinel Visualizer®

# Advanced Security Feature

The Advanced Security add-on (additional fee, over-and-above the basic licensing fee) for Sentinel Visualizer allows a System Administrator to define Users and Groups and control their read, edit, and delete permissions at a granular level. Topics can be defined to provide a great degree of control over what Users can view and do with the data.

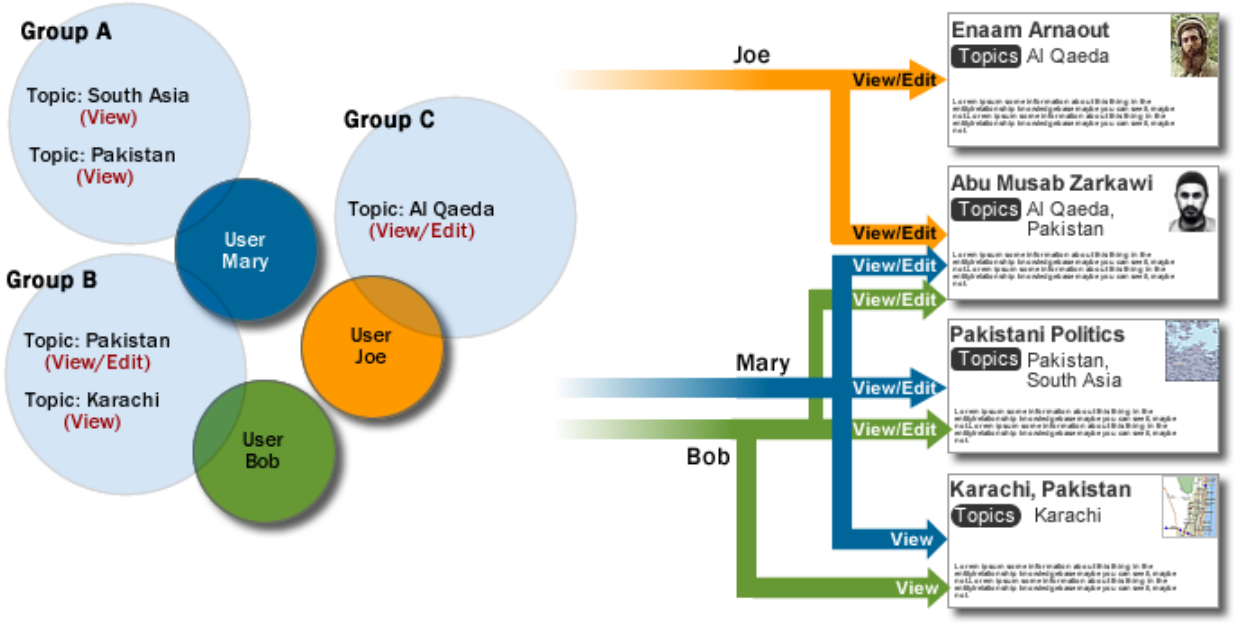
## Users and Groups

The cornerstone of the Advanced Security Feature is the concept of Users and Groups. A User is an account that you define to allow a specific person to gain access to the Sentinel Visualizer database. A Group is a collection of User accounts to simplify the management of User rights.

## Permissions

An Administrator assigns View and Edit permissions based on Topics. Data is assigned to Topics and user access is determined by whether the user/group has rights to the topic. Permissions may also be granted to Users for retrieving saved **network visualizations** (diagrams).

In this illustration, there are three groups: A, B and C, and three users: Mary, Joe and Bob. Mary is a member of two groups and




these two groups are assigned to several topics. So, Mary can View and Edit the “Abu Musab Zarkawi” and “Pakistani Politics” entities but can only view the “Karachi, Pakistan” topic. Put simply: Users belong to Groups; Groups are associated with Topics, Permissions are set at the Group/Topic level; Data records have one or more Topics.

## Distributing Network Diagrams

The Advanced Security feature allows diagrams (network visualizations) to be defined as:

- **Public**: viewable by anyone — including *Reader* Users — who has access to the Sentinel Visualizer database
- **Private**: viewable only by the User who created the diagram
- **Granular**: viewable by only the Users/Groups assigned with those permissions

FMS Advanced Systems Group

FMS, Inc. · 8150 Leesburg Pike, Suite 1250 · Vienna VA 22182 · USA · 703-356-4700 · fmsasg.com · info@fmsasg.com