Column-Level Security with Information Design Tool: Using Business Security Profiles to Secure Objects and Customize the Reporting Experience

One of the new universe security features in Information Design Tool (IDT) is the Business Security Profile, which allows universe designers to assign column-level security on objects and apply profiles directly to users and groups. Business Security Profiles provide advanced and flexible object security, which is an overall improvement compared to the all-or-nothing approach with legacy Universe Design Tool.

Pros and Cons

The added flexibility means fewer universes to develop and maintain since you can achieve more with a single universe. I am particularly pleased that SAP included a distinction between “Create Query” and “Display Data” object security. This is a relatively simple security method with powerful possibilities.

There is no denying that all these new features (and the extra steps involved at every level) have greatly complicated the universe design process. The learning curve is steep, but I still find many of these features useful. Business Security Profiles are assigned directly to users and groups from the IDT Security Editor. I personally find this quick and easy, but it could pose a challenge to organizations with distinct admin and designer roles. While SAP still has some bugs to work out, the feature generally works as intended.

*Note - currently Business Security Profiles are only functional with Webi in the Java-based (Rich Internet Application) viewing mode. With the security method I outline below, a profiled user who opens the Webi query browser in HTML mode will not see any objects (definitely not ideal... but at least still secure). This should be resolved in SP4 Patch 10 and SP6 (SAP Note: 1800742).

Use Case

I first discovered this feature while working with an OEM client developing a packaged BusinessObjects universe along with dashboards and canned reports. The dashboards/reports rely heavily on web services that utilize derived tables and customized objects in the universe. We also wanted to provide simple ad-hoc reporting capabilities from the same universe. With the old Universe Designer, we would have to compromise by either leaving all objects visible or creating a second universe specifically for ad-hoc reporting. The only object-level option in previous versions was restricting access levels (Public, Private, etc). This is unsuitable for our needs because it would prevent end-users from refreshing the dashboards and canned reports.

Business Security Profiles offer more flexibility since they allow a distinction between “Create Query” and “Display Data” object security. I was able to grant Create Query access to end-users for only the ad-hoc objects, and then grant Display Data access on all objects in the universe. Users can refresh the dashboards and canned reports but only they see the ad-hoc objects when creating their own Webi queries.
First Step - Business Layer Views
The simplest way to create Business Security Profiles is to utilize Business Layer Views (another new feature). These are simply a way to group relevant classes and objects.

To create a business layer view in IDT, open the blx and click the Manage Views icon

Here I created a Business Layer View for Ad-hoc Webi Users, leaving the AdminOnly class un-checked

Note that I also created an AdminOnly view to be explicitly denied for ad-hoc users. This shouldn’t be necessary, but it’s the only work-around I found to address a bug with Display Data permissions.
AdminOnly View will be explicitly denied

Second Step - Creating a Business Security Profile

Business Security Profiles are created in the IDT Security Editor.

Select the desired universe and add a Business Security Profile to configure column-level security (row-level security is still available through Data Security Profiles). Although it’s possible to directly grant and deny access to individual classes/objects, it’s much easier to leverage Business Layer Views.

Granting “Create Query” access on a granular view will only display the granted objects in the Webi query browser, and any objects not in the granted view are hidden by default. The result is similar to setting object access levels but the workflow is vastly different (access levels are still available on individual objects under advanced properties).

Column-level security is assigned under the “Display Data” tab. This grants or denies access to the data retrieved by the objects. In my case, I still need the hidden admin objects to refresh in the background of dashboards and canned reports, so I granted display data access to all objects in the universe.

For reasons I can’t explain, granting display data on all objects still prevented the admin objects from refreshing. Through much trial and error, I discovered that creating an additional view for the admin objects, and then explicitly denying “Create Query” access on that admin view, did the trick.

New Business Security Profile – I granted “Create Query” access to the Ad-hoc view and denied access to the AdminOnly view
Granted “Display Data” access on all objects
Third Step – Assign Users/Groups
You can directly assign users and groups to Security Profiles from the IDT Security Editor. The workflow is fairly straightforward since the entire process is contained within IDT (although the interface does tend to lag). Personally, I really like this feature and I’m glad it wasn’t relegated to the CMC. That being said, it does blur the lines between universe design and BOE security. Organizations with distinct designer and BOE admin roles can expect additional challenges.

Assign Users/Groups to Business Security Profile
Overall, Business Security Profiles are a useful resource when you need a single universe to perform multiple roles. It was a little tricky at first, but I successfully leveraged IDT security to address ad-hoc needs and saved myself the trouble of developing and maintaining a second universe.

Marshall Kelley, Business Intelligence Consultant
Decision First Technologies
Marshall.kelley@decisionfirst.com
Twitter: @kmarshallkelley

Marshall Kelley is a business intelligence consultant specializing in SAP BusinessObjects tools and solutions. With Decision First, Marshall provides customized solutions for customers across all industries. He utilizes a wide-range of front-end BusinessObjects products and is experienced in BusinessObjects configuration, administration, and end-user training.