Artículo
Alessandro Marin · 8 ene, 2018 Lectura de 2 min

DeepSee: Setting up security - Part 2 of 5

In part 1 we started working on a security model for DeepSee and create a user type having privileges typical of end users. In this part we are going to create a second user type with ability to edit and create DeepSee pivot tables and dashboards.

Granting full access to Analyzer and Dashboards

Create a DSPowerUser role

According to the documentation (see the rows for the tasks "Full access to the Analyzer or Mini Analyzer" and "Creating a new Dashboard" in the table) we need USE permissions on the %DeepSeeAnalyzerEdit and %DeepSeePortal resources to grant full access to Analyzer, and USE permissions on the %DeepSeePortalEdit resource to create and edit dashboards. Notice that %DeepSeeAnalyzer is not needed when %DeepSeeAnalyzerEdit is granted.
Create a DSPowerUser role including the following resources with USE permissions:

Resource	Permission
%DeepSeeAnalyzerEdit	USE
%DeepSeePortal	USE
%DeepSeePortalEdit	USE
%DBAPP-DATA	RW

Create poweruser

In Users page > Create New User create a poweruser with the DSUser role assigned as shown in the following screenshot

Test poweruser

Open an incognito/private window of your browser and log in as poweruser. The Architect tab in the DeepSee section should still be grayed out. Navigate to Analyzer and User Portal and confirm that poweruser can view, create and edit pivot tables and dashboards.

Tip: To avoid having to log in to the SMP several times with the same user, do one of the following:

- Use the same GroupId in webapps. For all web applications the user is going to access, use the same Id in Web Applications page > your web application > Group By ID field.
- Enable cookie creation for CSP and login cookie in the appropriate web applications: SMP > System Administration > Security > System Security > Authentication/CSP Session Options > check Allow creation of Login Cookies. Web Applications > select a web application > check Login Cookie. Do this for all web applications the user is going to access.

I suggest using one of these methods for the web application associated with the namespace (in our example /csp/app/) to avoid having to login when trying to access DeepSee functionalities in that namespace. If you notice that your user is asked to log again, find the web application from the url or from the Audit log, then follow one of the two methods outlined in the bullet points above.

In [part 3](#) we will create one more user type providing privileges typically needed by an administrator/developer in analytics.

[#Control de acceso](#) [#Principiante](#) [#Seguridad](#) [#InterSystems IRIS BI (DeepSee)](#)