Article
Alessandro Marin · Jan 8, 2018 4m read

DeepSee: Setting up security - Part 1 of 5

I have a few cubes and numerous dashboards and I am ready to deploy them to our end users and administrators. How to configure DeepSee so that **users don ' t disrupt each other ' s areas and are restricted** from using functionalities specific to developers?

Running a Business Intelligence IT system often requires configuring a security model. This tutorial will show how to set up a simple security model for DeepSee.

The security model consists of three user types. First, we will create a simple DeepSee user who can access but cannot edit DeepSee dashboards. The second user type will be allowed to access pivot tables in Analyzer and view, edit, and create dashboards. Finally, " Admin " users will have more extensive control on the implementation, such as access to Architect.

We will also see how to secure and control the visibility of model elements such as pivot tables, dashboards, cubes, etc. Tips to troubleshoot issues will hopefully make it easier to implement a security model.

Before you start

In this post we will set up basic security model. Please get familiar with this page about Setting Up Security for DeepSee.
If you are testing or creating a proof of concept do not use the SAMPLES database or namespace, which has special setting. Instead, work on a namespace (e.g. APP) withdedicated database(s) (e.g. APP-DATA).
To follow along with this tutorial, create a APP namespace based on a APP-DATA database in the Security Management Portal [SMP] > Configuration > System Configuration > Namespaces. Assign a new %DBAPP-DATA resource to the newly created database. Make sure the default web application for the APP namespace (/csp/app) is DeepSee enabled. It is assumed you have a Server or Custom installation where you can log in Caché with a user having sufficient privileges to run the operations in this post.

Granting read-only access to dashboards

In a typical implementation end users are allowed to use Analytics but not editing the implementation itself. In this section we are going to define a user type that can only access but cannot edit DeepSee dashboards.

Create a DSUser role

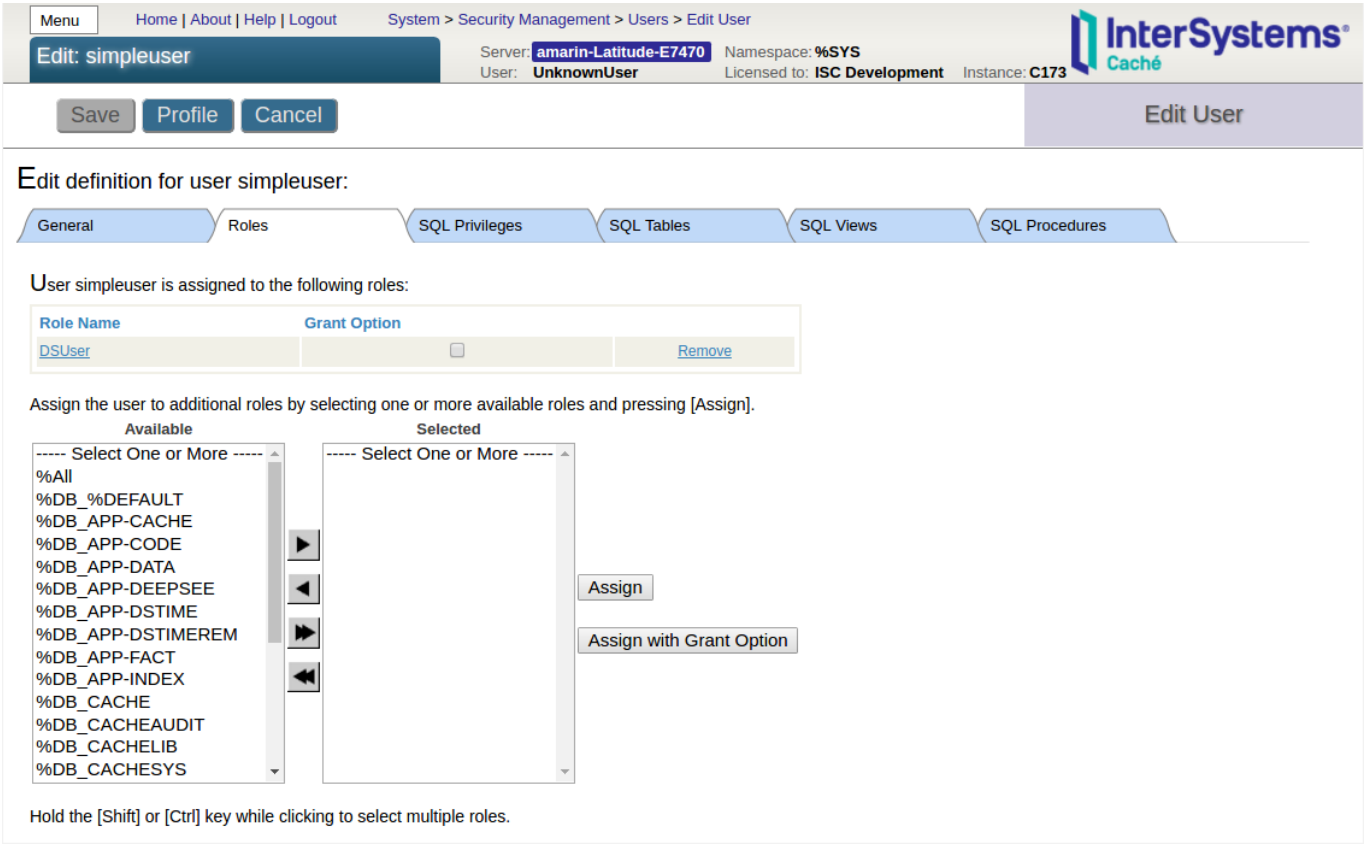
According to the documentation (see the row for the task " Viewing the User Portal apart from the Analyzer or the mini Analyzer with no ability to create dashboards " row in the table) we need USE permissions for the %DeepSeePortal resources.
Create a DSUser role including the following resources:

Resource	Permission
%DeepSeePortal	USE
%DBAPP-DATA	RW

The U and RW permissions for the resource in the table above should be set automatically when you assign the roles. Depending on your namespace, database, and mapping configurations, you will need RW permission on resource securing databases. In our example %DBAPP-DATA is needed to access the default database for the APP namespace.

Create simpleuser

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



Test simpleuser

Open an incognito/private window of your browser and log in as simpleuser. From the management portal check that Architect and Analyzer tabs in the DeepSee section are greyed out. Navigate to User Portal and confirm that simpleuser can view dashboards. Also confirm that simpleuser can neither see the save button for dashboards nor the " + " icon on User portal to create folder items. Notice that simpleuser can see pivot tables in User Portal, but trying to view a pivot table should show that the user is not authorized to view the page. In a following section of part 5 we will see later how to hide pivot tables from User Portal.

Tip: Use two browser windows. One browser window can be used to log in with an administrator user (for example SYSTEM or SuperUser) that is able to change system settings. In the other window run a browser in incognito (Chrome)/private (Firefox, Edge) mode where a test user is logged in. Incognito/private mode will make sure that the browser cache from the other window will not interfere with your job and cause any unexpected behavior.

Tip: In the management portal use the Menu button in the top-left corner to quickly navigate to the Users, Roles, Resources, and Web Applications pages.

Troubleshoot: Public permissions

A common problem is finding that some functionalities are allowed in spite of the security model. As explained more extensively in a section of part 5, a common cause for this unexpected behavior is public permissions on resources. For example, you may see that simpleuser is able to create new dashboards in User Portal. If the %DeepSeePortalEdit resource is still assigned public USE permissions, any user will be able to create pivot tables and dashboards. To solve this problem, remove the USE public permissions from the %DeepSeePortalEdit resource.

In part 2 we will create a second user type granting the ability to edit and create DeepSee pivot tables and dashboards.

#Access control #Beginner #Best Practices #Security #InterSystems IRIS BI (DeepSee)

Source URL:https://community.intersystems.com/post/deepsee-setting-security-part-1-5