# PROTECT OF K2 FIVE CORPORATE APPLICATION USING AUTHORIZATION FRAMEWORK

**Roman Duban**
PhD, Kryvyi Rih Economic Institute of Kyiv
National Economic University named after Vadym Hetman,
e-mail: duban_rm@kneu.dp.ua, http://orcid.org/0000-0002-6484-921X, Ukraine
**Sergei Neverov**
PhD, Kryvyi Rih Economic Institute of Kyiv
National Economic University named after Vadym Hetman,
e-mail: neverov_sl@kneu.dp.ua, http://orcid.org/0000-0002-4080-2863, Ukraine
**Anna Duban**
Postgraduate, Kryvyi Rih National University,
e-mail: anna.duban@krpd.edu.ua, http://orcid.org/0000-0001-8489-5259, Ukraine

**Abstract.** The article deals with the possibilities of protecting corporate applications that have been built on the K2 five platform. using new functions that provide an authorization package. Security settings are made with the new tools provided by the authorization framework. The peculiarities of setting up and implementing the benefits of this type of protection are considered. The expediency of using built-in roles for organizing of access to system resources is substantiated. Described how to transfer settings between environments.
**Keywords:** BPM, security, roles, K2 five.

*DOI: http://dx.doi.org/10.23856/3104*

## Introduction

A characteristic feature of digital transformation at the enterprise is full-scale automation of enterprise processes with the use of modern information technology. Particular success in the automation of enterprise processes can be achieved by applying automation systems that combine with low-code or zero-code approach. This type of platform allows business and IT members to create and develop applications together. And the issue of corporate application security is always relevant and important. Especially, taking into account the growing tendency of hacking and unauthorized access both inside and outside the enterprise.

## A craft of workflows and combine legacy applications

During years, companies implement various programs, which potentially reduce the time of execution of certain operations, provide a control functions and allow them to receive reports. It contributes to increasing the competitiveness of enterprises. Some systems cannot withstand the test of time and no longer apply, while others can successfully develop and help in business management. A fully-fledged joint application of enterprise systems from different manufacturers, implemented impromptu, may be a problem. The diverse architecture of the programs and the value of accumulating data complicates the integration and support of these systems. At the same time, innovative web-based applications with a convenient and functional user interface allow you to work more productively and provide mobility. To resolve such issues, the BPM K2 software platform by SourceCode Technology Holdings can be used with success.

K2 software platform provides scalability and affordability and based on Microsoft stack of information technologies and requires Microsoft Server with IIS and Microsoft SQL Server. Such a base already contributes to the protection of corporate applications environment. K2 software platform provides the ability to create automation processes of different scales and designer to develop flexible web applications without writing code that integrates with workflows. In general, the web application built on the K2 platform is a collection of forms and views organized by categories. These forms are called SmartForms, these can contain different web-controls, including views, and determine interactive behavior through flexible rules. Data mining takes place through special objects called SmartObjects. SmartObjects access data from various sources through a special ServiceBrokers. Currently, there are a large number of ServiceBrokers to provide integration with various data bases, APIs and services. The K2 Workflows also manipulate data through SmartObjects and interact with SmartForms. The architecture is quite flexible and allows third-party developers to join the expansion of the functionality through the development and providing of their own web-controls, ServiceBrokers, etc.

The K2 platform is a web-based system and provides interfaces for various functional parts of the system: K2 Designer, Management panel, and Workspace. Authentication of users is due to the integration of K2 with Active Directory of a domain. Also available are other sources of user authentication information such as a database, LDAP, Azure or oAuth. Usually, any authenticated user has access to the Workspace where the links to the K2 application forms are displayed. K2 Designer is used to developing K2 applications. It shows all categories, SmartForms, Views, SmartObjects, Workflows and provides functionalities to create new and edit existing items. Access to K2 Designer can be configured via Management panel and should be limited only for developers group. Management panel is used to administrating K2 server: Servers, Environments, Features, Authentication, Integration, Users and Roles, Workflows, Licensing.

All the examples given in this article are made on a demonstration virtual server, which can be downloaded from the knowledge base on official K2 web-site. The demo domain name is denallix.com.

**Using of K2 authorization framework**

First of all, two simple applications with identical structure were created in the K2 designer: App A and App B.

The applications show on figure 1 in K2 Designer panel. Detailed information about creating process of K2 applications can be found in official K2 documentation.

Also, in Active Directory Server Console created groups of users for both applications, App A and App B: Admins, Developers, Users. That are located inside a new organizational unit called K2 Application.

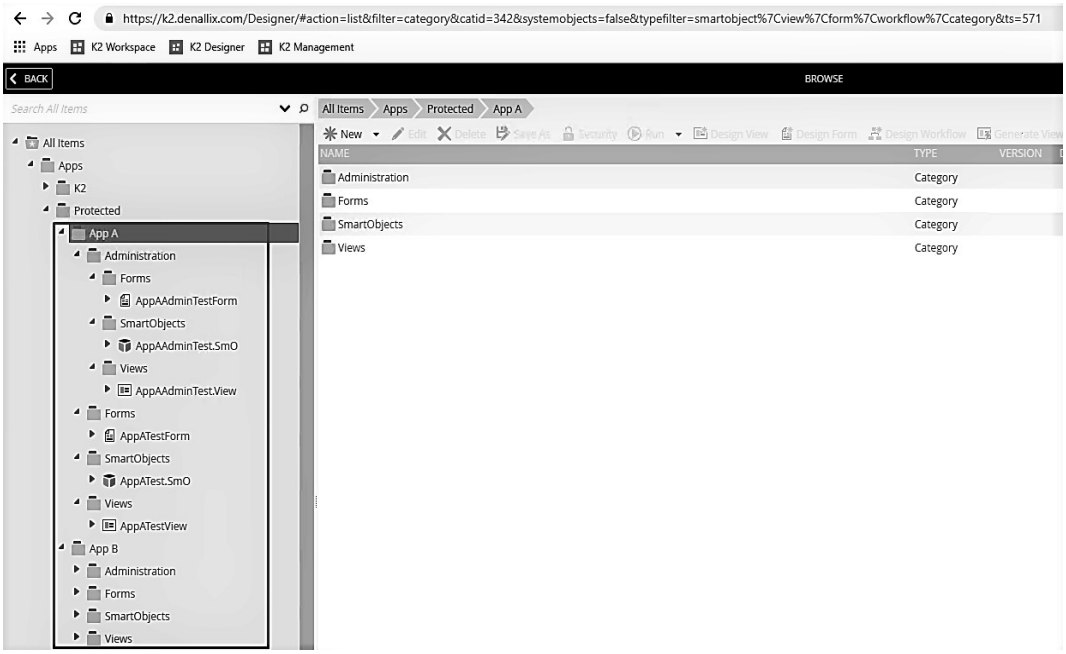


**Fig. 1. K2 Applications in K2 Designer panel**

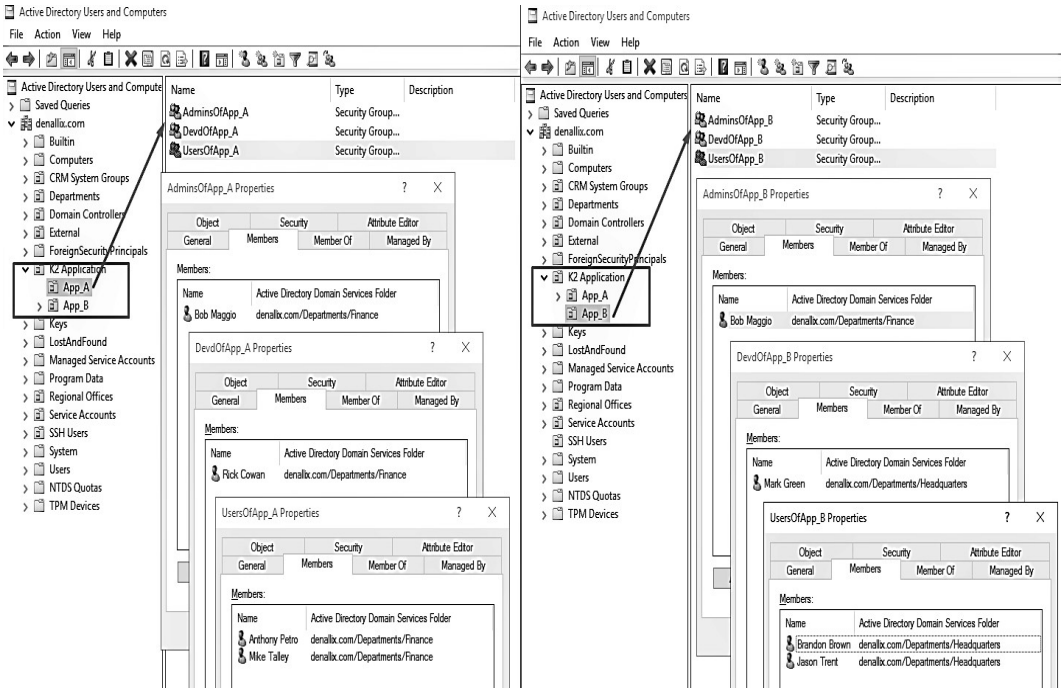


**Fig. 2. Active Directory Group and Users**

Figure 2 shows the following:

- K2 Application Organization Unit was created in the root of domain;
- App_A and App_B Organization Units were created in the K2 Application;
- AdminsOfApp_A, DevdOfApp_A, UsersOfApp_A were created in the App_A;
- AdminsOfApp_B, DevdOfApp_B, UsersOfApp_B were created in the App_B;
- Member Users were added to each created Groups in the Members tab of group item properties:
- AdminsOfApp_A: Bob Maggio;
- DevsOfApp_A: Rick Cowan;
- UsersOfApp_A: Anthony Petro, Mike Talley;
- AdminsOfApp_B: Bob Maggio;
- DevsOfApp_B: Mark Green;
- UsersOfApp B - Brandon Brown, Jason Trent.

The specified domain, organizational structure and user names are fictitious, and any coincidence is an accident. The given structure is necessary for understanding of further adjustments.

The next configuration step is organizing K2 Roles with the created Active Directory groups. To perform these settings in the K2 Management panel, select the Users->Roles menu item. Then add new Roles by click on New button and create roles for each AD groups of K2 applications: “AppAUsers”, “AppADevs”, “AppAAdmins”, “AppBUsers”, “AppBDevs”, “AppBAdmins” as it shows on Figure 3.

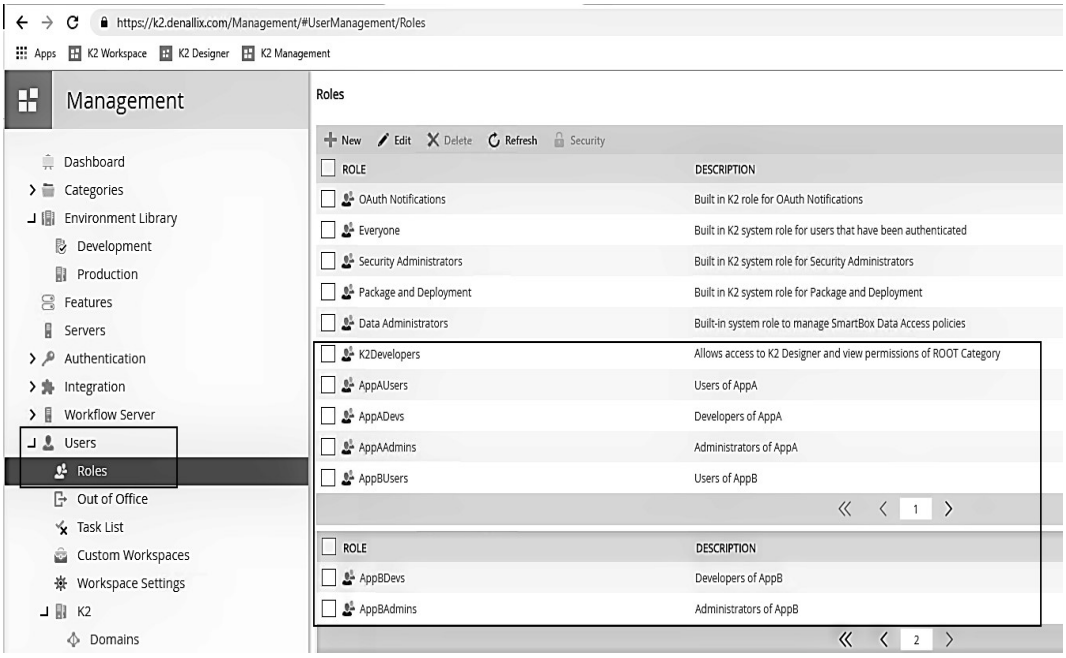


**Fig. 3. K2 Roles**

Also, K2Developers Role was created. The role is use for configure permissions to K2 Designer panel and Categories, as it shows on figures 4 and 5.

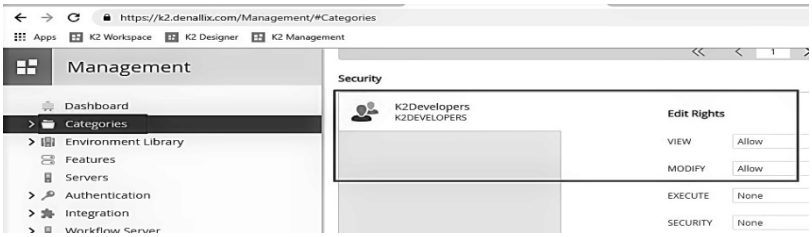


**Fig. 4. Root Category permission**

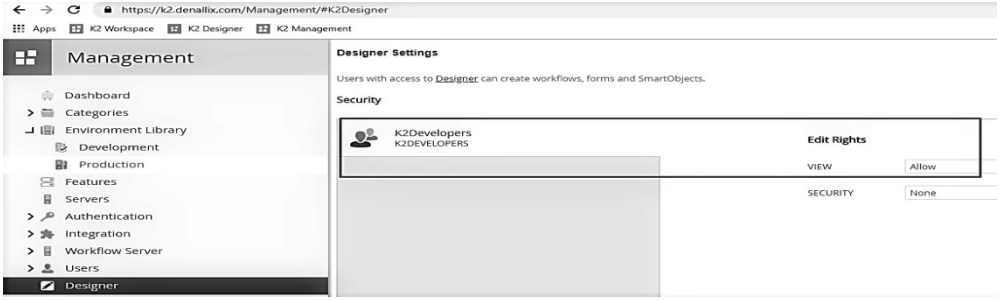


**Fig. 5. K2 Designer permission**

Each K2 Role can contain both groups and individual users. The role can be changed after create as it shows on the figure 6.

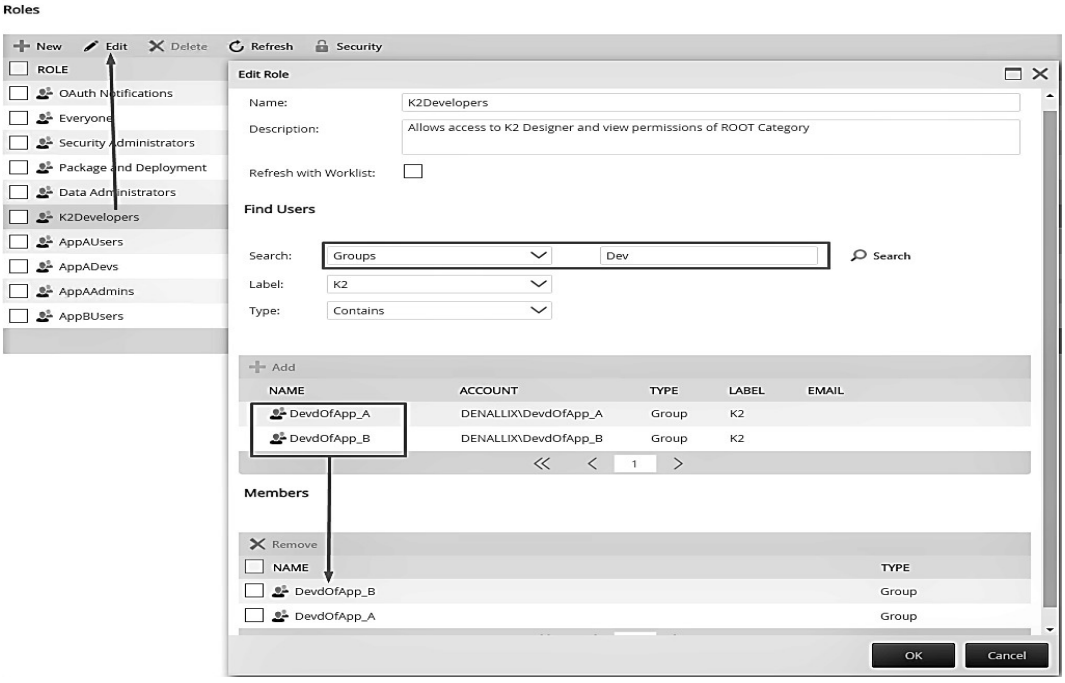


**Fig. 6. K2Developers role Edit window**

When root directory permissions are changing, it should be noted that certain system categories require permission to allow execute for Everyone role. There need to be careful with permissions of those categories because it affects the correct working of Workspace. These categories was showed on figure 7 and include the following: System, Workflow, Workflow Reports, Apps\K2\SmartStarters, Apps\K2\Workdesk.

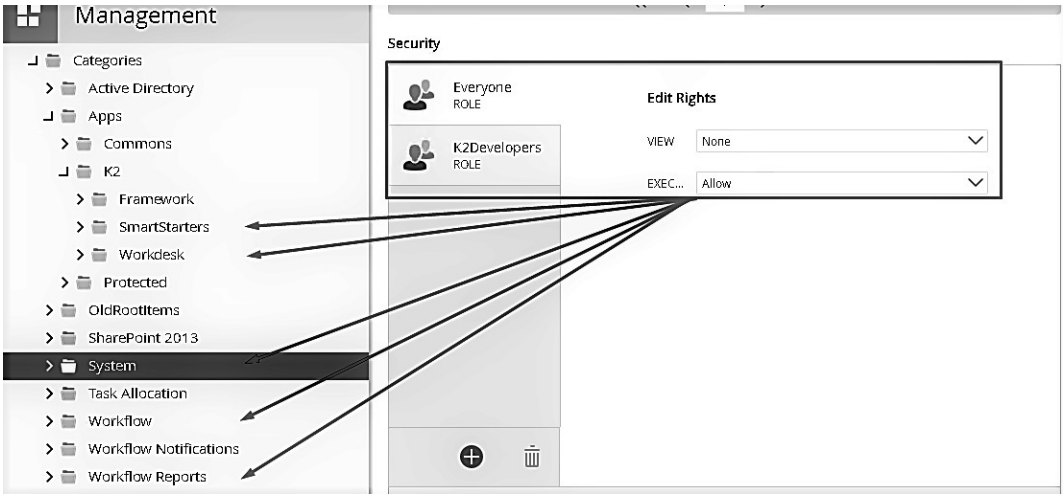


**Fig. 7. System categories require allow execute permissions**

Consider the permission settings of K2 applications that require protection directly. First of all, needs to Break Inheritance of Demo application categories and Management category. Remove access rights as it shows figure 8.

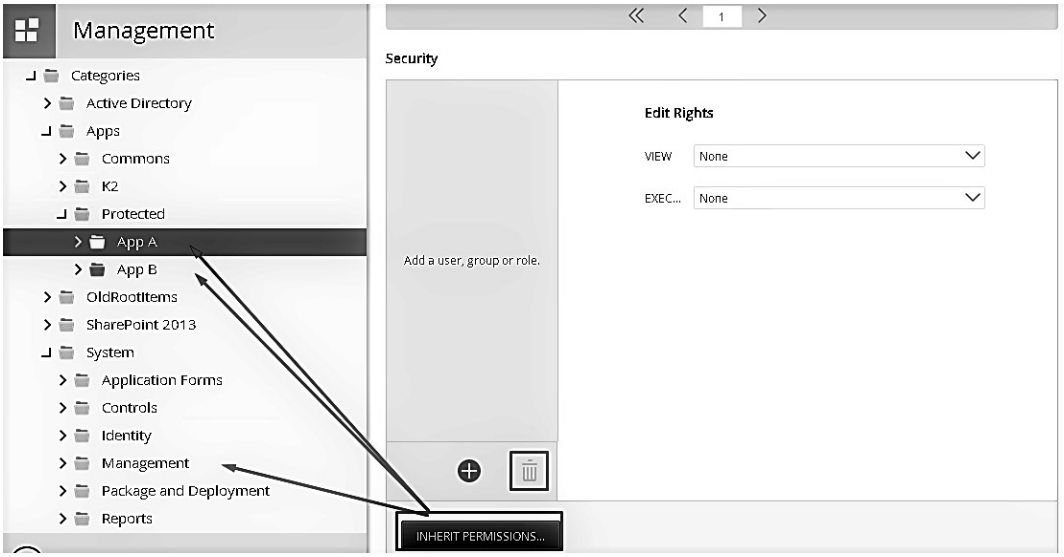


**Fig. 8. Remove access rights from protected categories**

Categories select one by one: System\Management, Apps\Protected\App A, Apps\Protected\App B; and "BREAK INHERITANCE" button uses to disable categories permissions rights inheritance. Than need to remove all Users, Group and Roles from selected categories security rights. After that, permissions of Demo K2 Applications categories are configuring:

- AppADevs Role was added to Apps\Protected\App A category security part and AppBDevs Role was added to Apps\Protected\App B category security part. Also, allow rights for VIEW, MODIFI and EXECUTE actions were set.

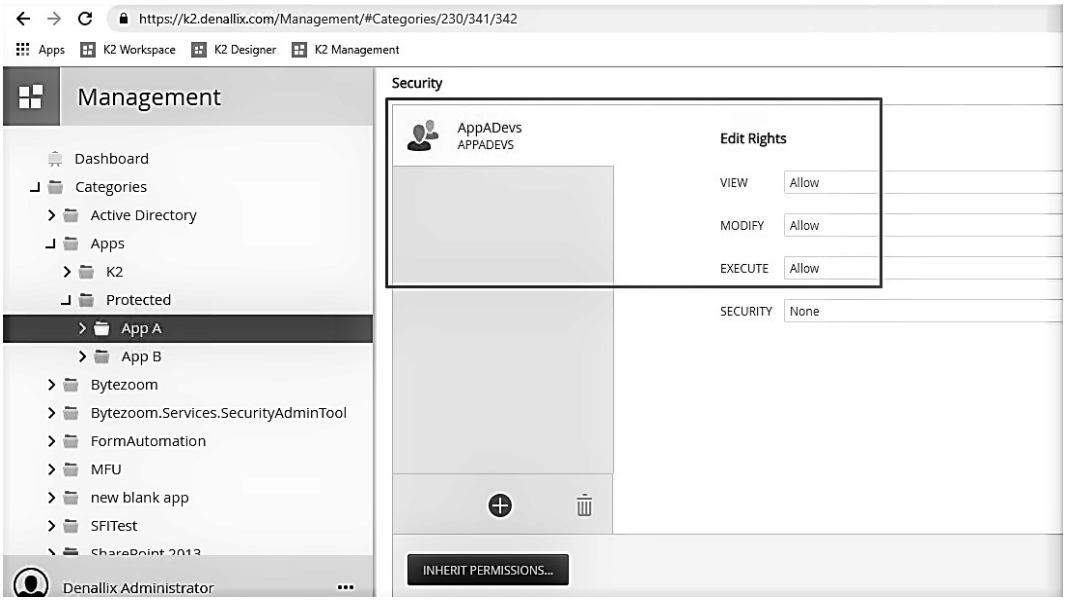


**Fig. 9. Developer roles permission to the category**

- AppAUsers Role was added to Apps\Protected\App A\Forms category security part and AppBUsers Role was added to Apps\Protected\App B\Forms category security part. Also, allow rights for EXECUTE action was set.

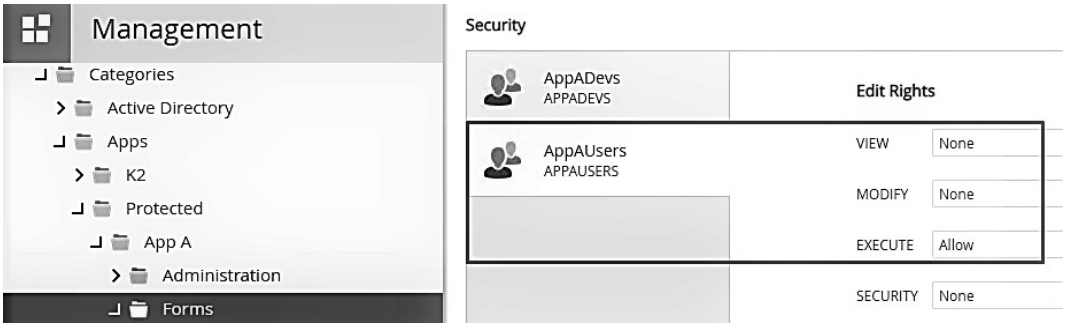


**Fig. 10. User roles permission to the category**

- AppAAdmins Role was added to Apps\Protected\App A\Administration\Forms category security part and AppBAdmins Role was added to Apps\Protected\App B\Administration\Forms category security part. Also, allow rights for EXECUTE action was set.

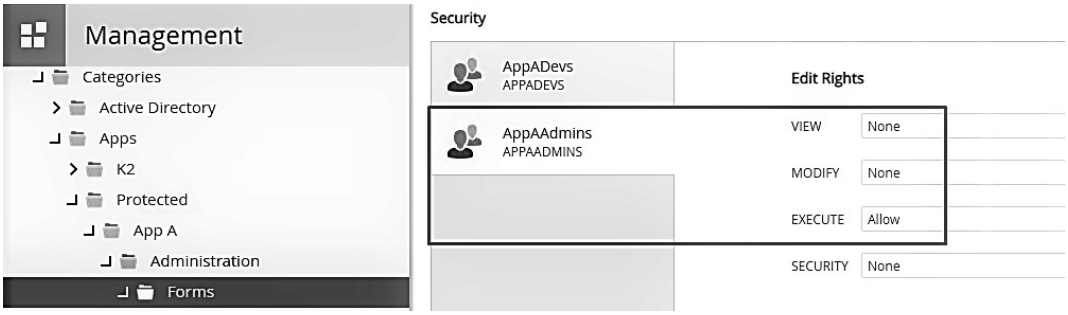


**Fig. 11. Administrator roles permission to the category**

To check permissions settings of K2 Applications, need to authorize in K2 with users from different roles.

Anthony Petro is member of AppAUsers Role. And he does not have access to K2 Designer. He will see error message if try to open K2 Designer, as it shows on figure 12.

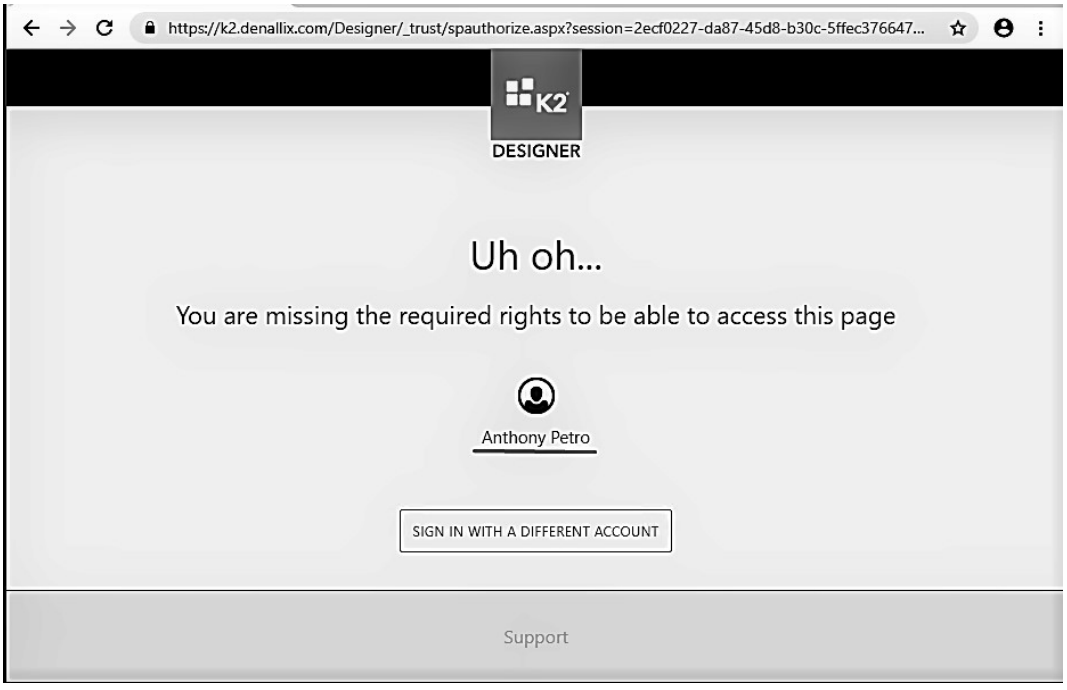


**Fig. 12. The user has not access to K2 Designer**

Also, Anthony Petro does not have access to App Admin Forms and Management forms. And he will receive follow messages if try to open the forms directly.

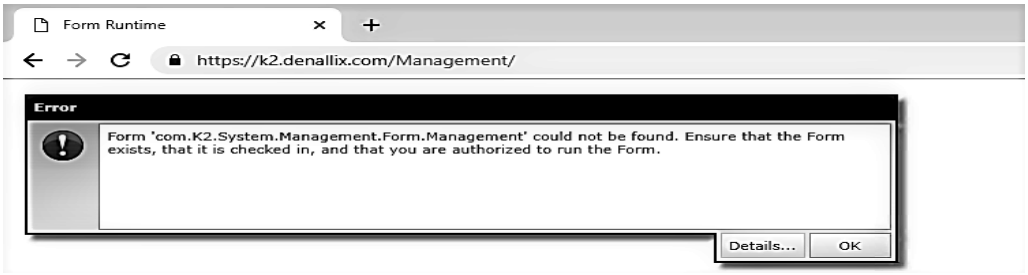


**Fig. 13. The user has not access to K2 Management panel**

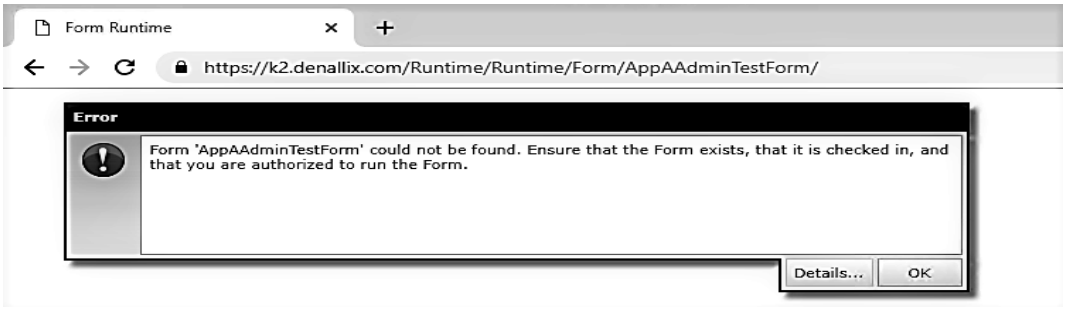


**Fig. 14. The user has not access to the Application Admin form**

But, Anthony Petro has access to the AppA Form and can see it in his Workspace forms.

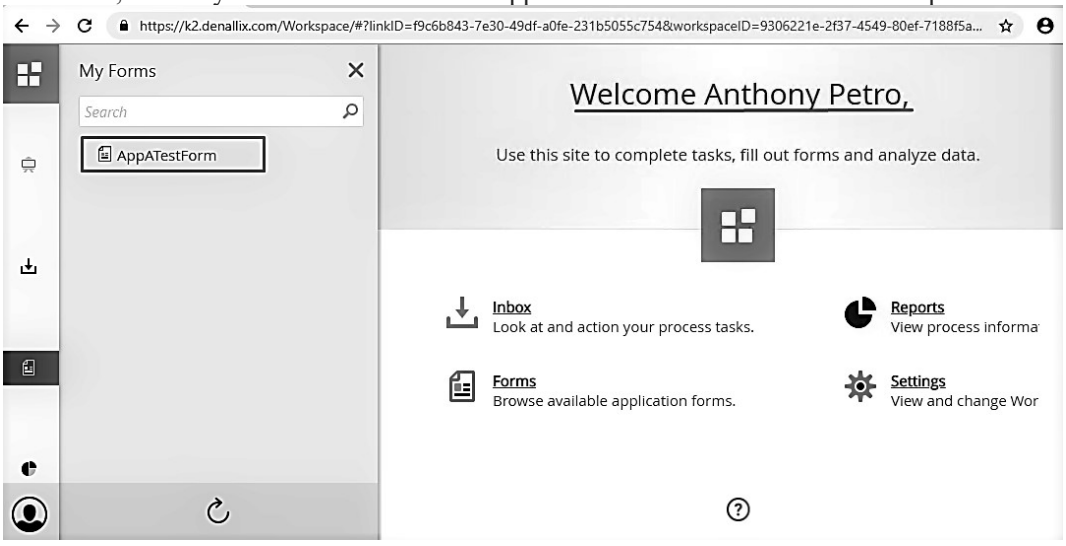


**Fig. 15. The user has access to the Application form on his Workspace**

Another user Rick Cowan is member of AppADevs Role. And he has access to K2 Designer and has access to AppA category. But he should not be able to view the AppB category, because he is only AppA developer. As it shows on figure 16, he can`t see AppB category in SmartObjects Services Tester utility also.

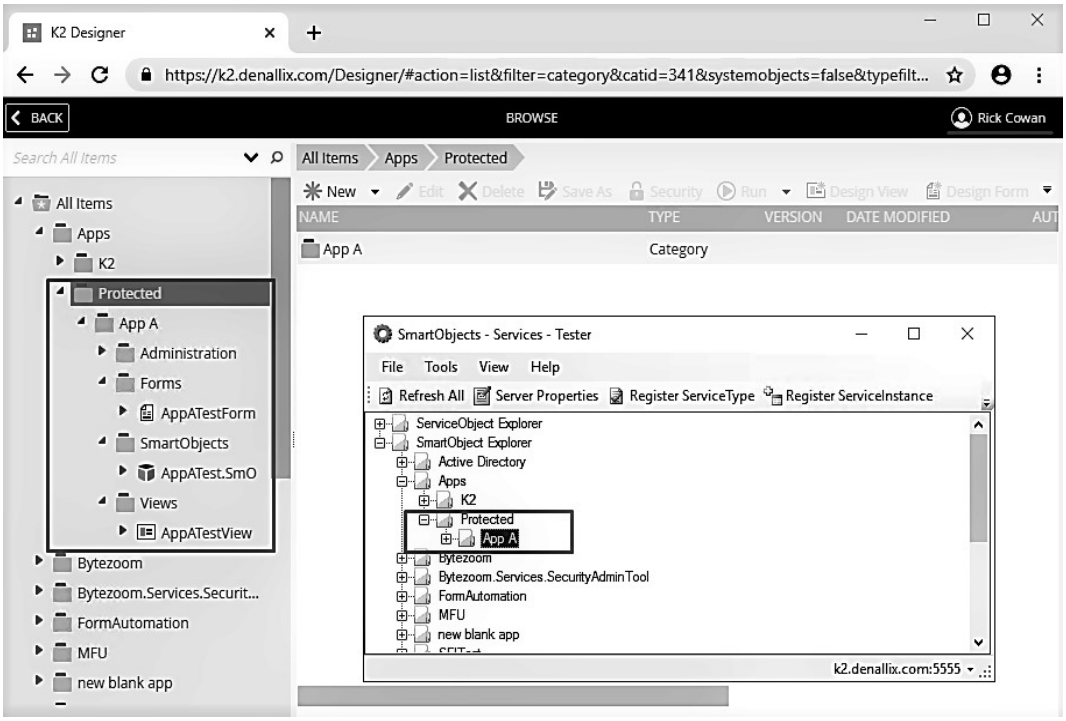


**Fig. 16. The developer user of AppA has access to K2 Designer and the category**

## Conclusions and suggestions

Having considered the example above, we can conclude that the solution to the security configuration issue in applications on K2 platform is facilitated by authorization framework provided in K2 Five. Particular attention deserves the configurations of rights using the built-in K2 Roles. Roles can include both individual users and groups and it's convenient to control that list in one place. The ability to flexibly configure access rights through the web-interface allows corporations to address the gap-issue between business executives and IT professionals. Even if the development of K2 applications is made on outsourcers. The production environment may have the same set of access rights for the roles, but members of the roles may be different. This approach facilitates migration and support of applications in the development, testing and deployment process.

However, it should be noted that the built-in means do not allow the transfer of custom rights of access to another environment. In another environment may be missing roles that have certain rights. Solving the issue of migrating categories rights is implemented in an ServiceBroker by a third party developer, which is the technical K2 partner.

It is K2 Five Security Admin Service Broker developed by Bytezoom LLC. This tool provides the ability to export the privileges of the selected category to the JSON format. And

import this configuration into the destination environment. In this case, the missing roles on the destination server will be created automatically. The JSON format is also convenient for manual changes so it can be used to quickly set of the configuration for a large number of categories. Moreover, it can be used to control the version of the changes. This ServiceBroker also includes features that allow user to get full reports of designated categories permissions and to edit role-members through SmartObjects. It is likely that such convenient features will appear in new versions of K2.

**References**

*Anderson, H., Kaji, C., Leisegang, S., Macori, I., Malherbe, G., Montgomery, J., Murphy, C., O'Connor, C., Del Piccolo, S., Schaffer, E., Apergis, J., Geier, C., Petro, A., Talley (2009). Professional K2 blackpearl. Birmingham, UK: Wrox Press Ltd. [in English].*

*Ani, U. D., He, H., Tiwari, A. (2018). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. Journal of Systems and Information Technology. DOI: 10.1108/JSIT-02-2018-0028. [in English].*

*Hesson, M., Al-Ameed, H. (2007). Online security evaluation process for new e-services. Business Process Management Journal, Vol. 13 Issue: 2, 223-246. DOI: 10.1108/14637150710740473. [in English].*

*Manfreda, A., Štemberger, M. I. (2018). Establishing a partnership between top and IT managers: A necessity in an era of digital transformation. DOI: 10.1108/ITP-01-2017-0001. [in English].*

*Shaughnessy, H. (2018). Creating digital transformation: strategies and steps. Strategy & Leadership, Vol. 46 Issue: 2, 19-25. DOI: 10.1108/SL-12-2017-0126. [in English].*