

BOC ADC ID Management Platform Configuration

USER GUIDE

Version 1.0  
September 9, 2021

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Changed By | Changes |
| September 09, 2021 | Version 1.0 | Maryna Nikolaienko | Original Version. |
| September 20, 2021 | Version 1.1 | Keith Brickey | Change Document Title to “BOC ADC ID Management Platform Configuration User Guide” |

Table of Contents

[ADC OA Admin 4](#_Toc83939622)

[ADC IM Platform 8](#_Toc83939623)

[Configuration menu 8](#_Toc83939624)

[New ID Request Process 8](#_Toc83939625)

[ID Recertification Process 11](#_Toc83939626)

[ID ticket and Password Management Process 12](#_Toc83939627)

[ID Management 13](#_Toc83939628)

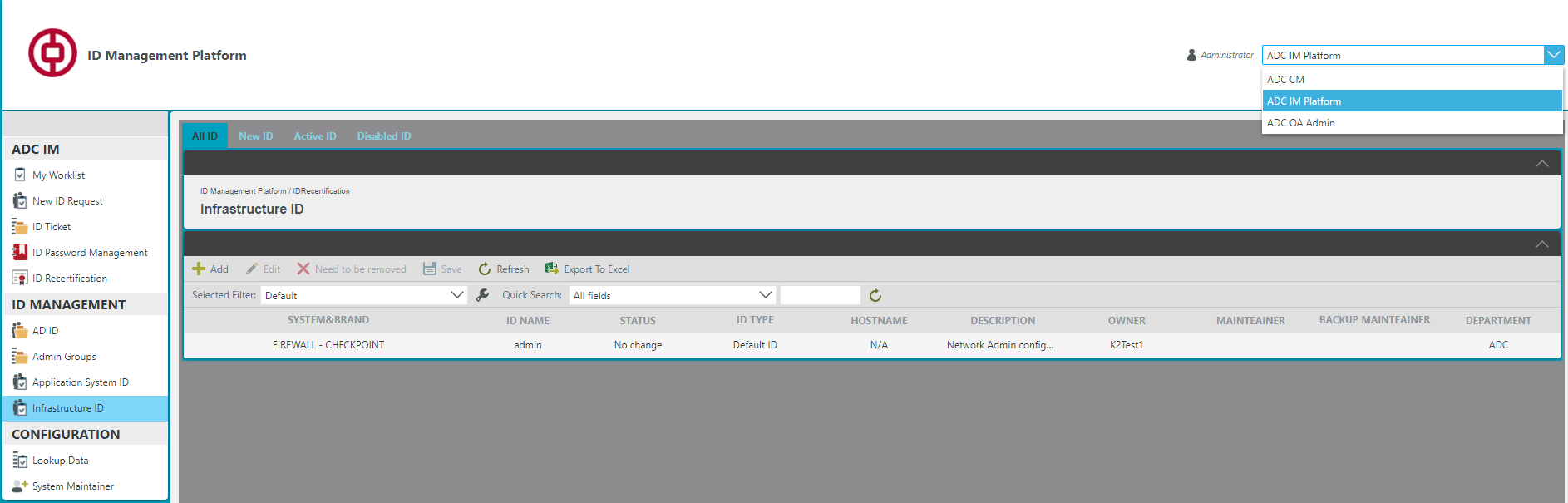
[ADC IM 13](#_Toc83939629)

[ID Password Management 13](#_Toc83939630)

[ID Recertification 13](#_Toc83939631)

This article provides a user guide for the BOC ADC ID MANAGEMENT PLATFORM process that uses the K2 Five application framework. The BOC ADC application consists of three desktops:

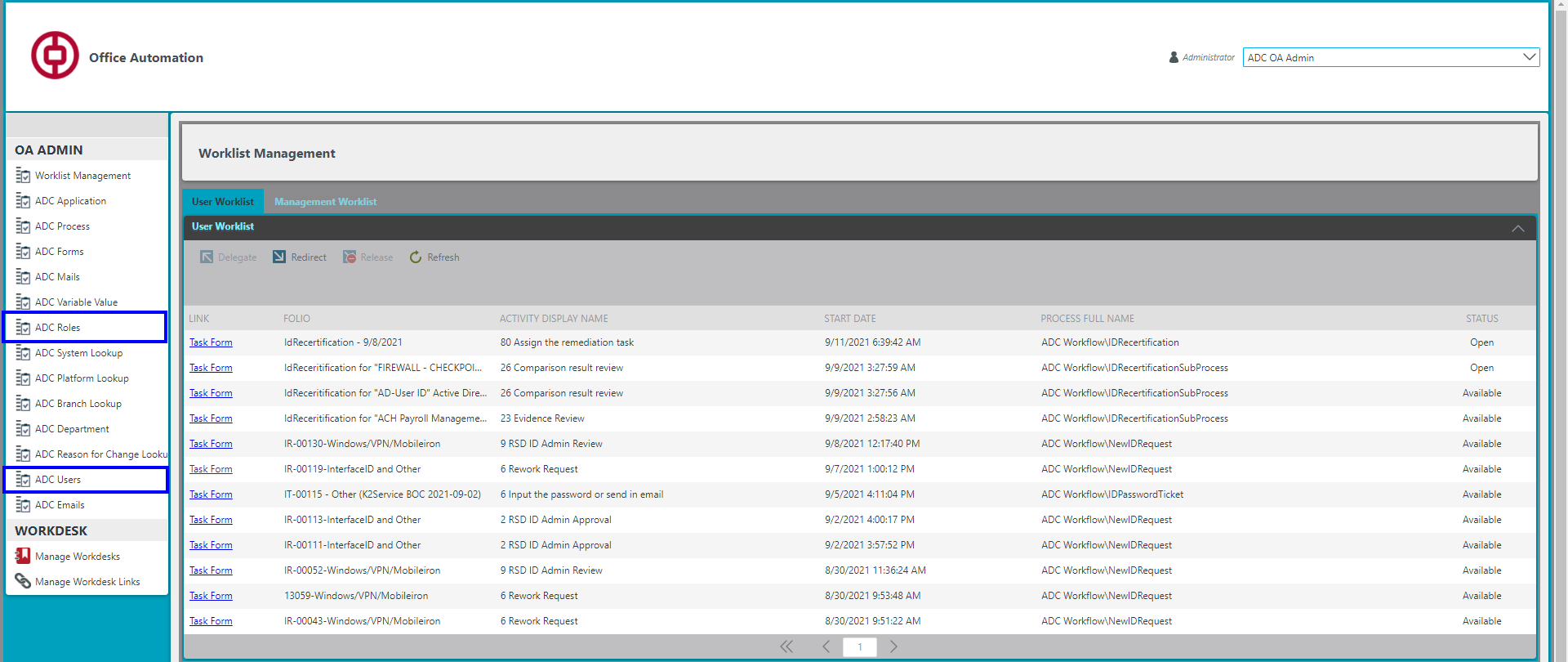
* ADC CM
* ADC IM Platform
* ADC OA Admin

In the upper right corner of the header, there is a drop-down list for selecting a desktop. Left menu items and dropdown items are limited to limit visibility to selected role members.

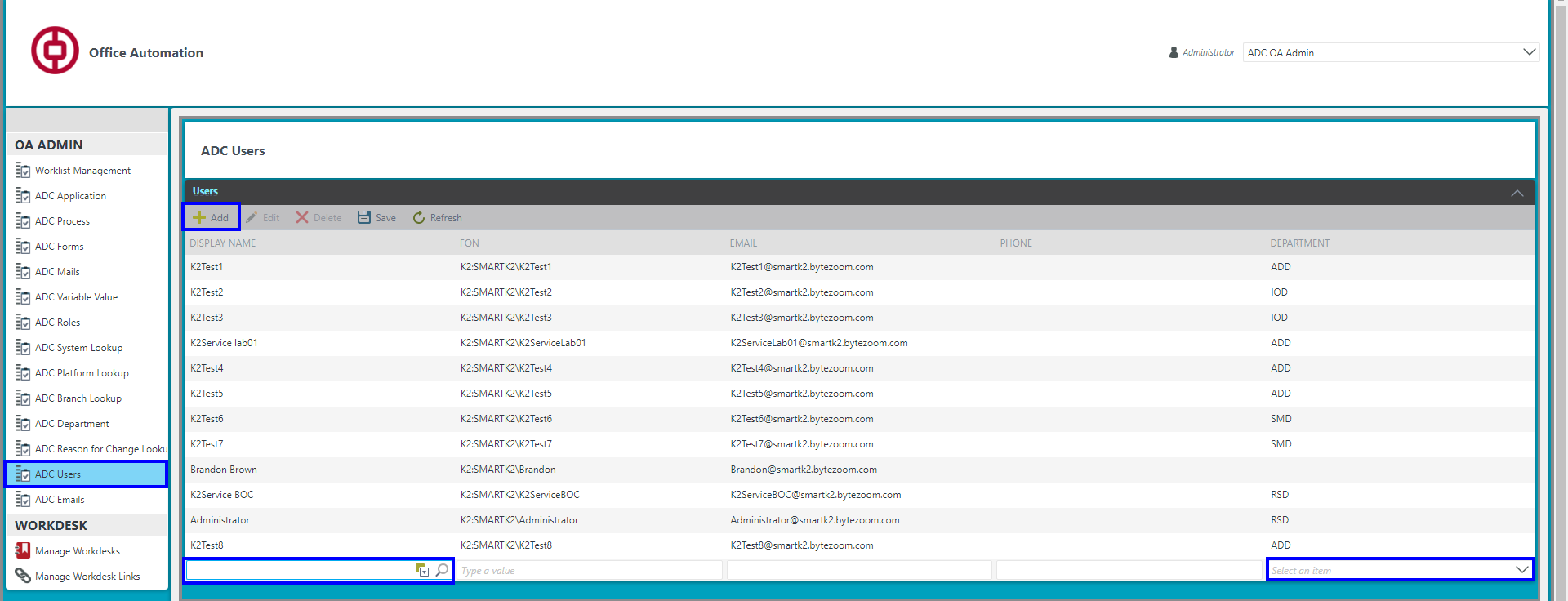
# ADC OA Admin

This menu is available for the administrator only. All process settings are made in this menu.

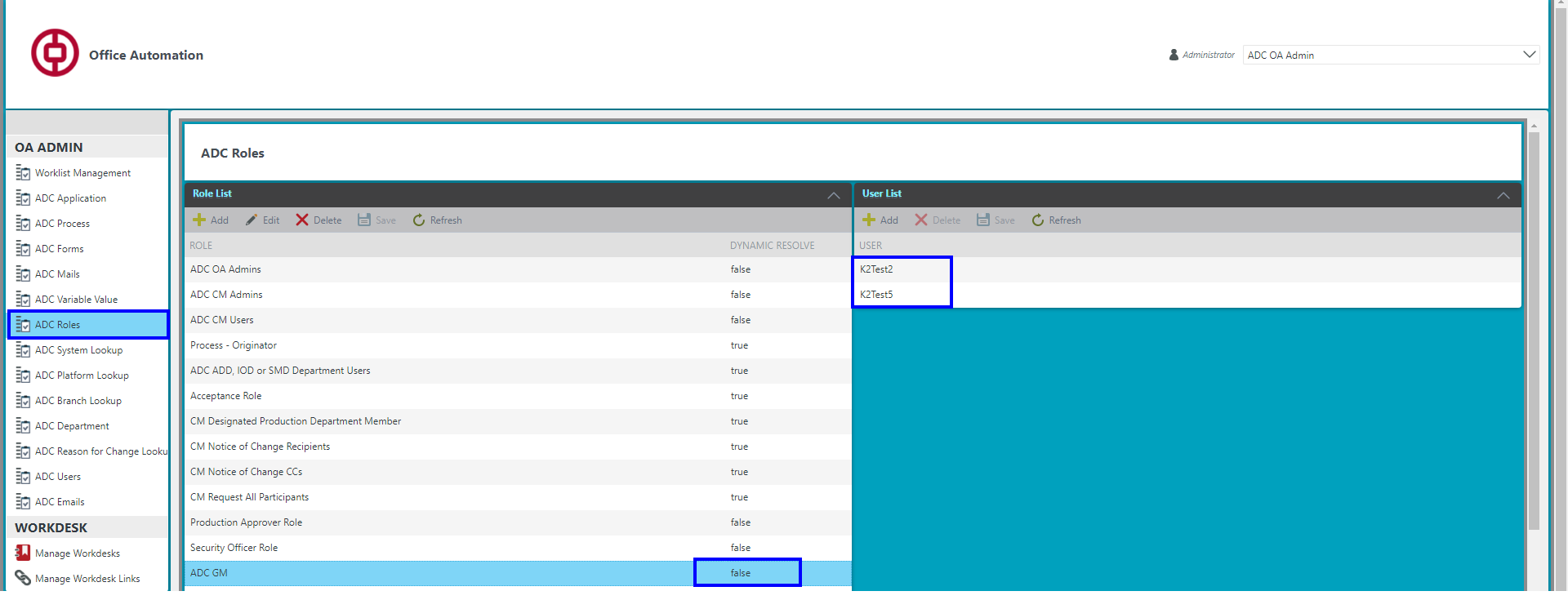
You need to configure in the OA Admin menu:



* ***ADC User*** - when adding a new user to the Display Name, it is possible to use the Picker, (To find the desired name, start entering the name or one word from the name and click on the magnifying glass to search. Has control buttons "OK", "Cancel") after entering the username user data will be added from Active Directory to populate). After adding user data, be sure to select the Department to which it belongs.



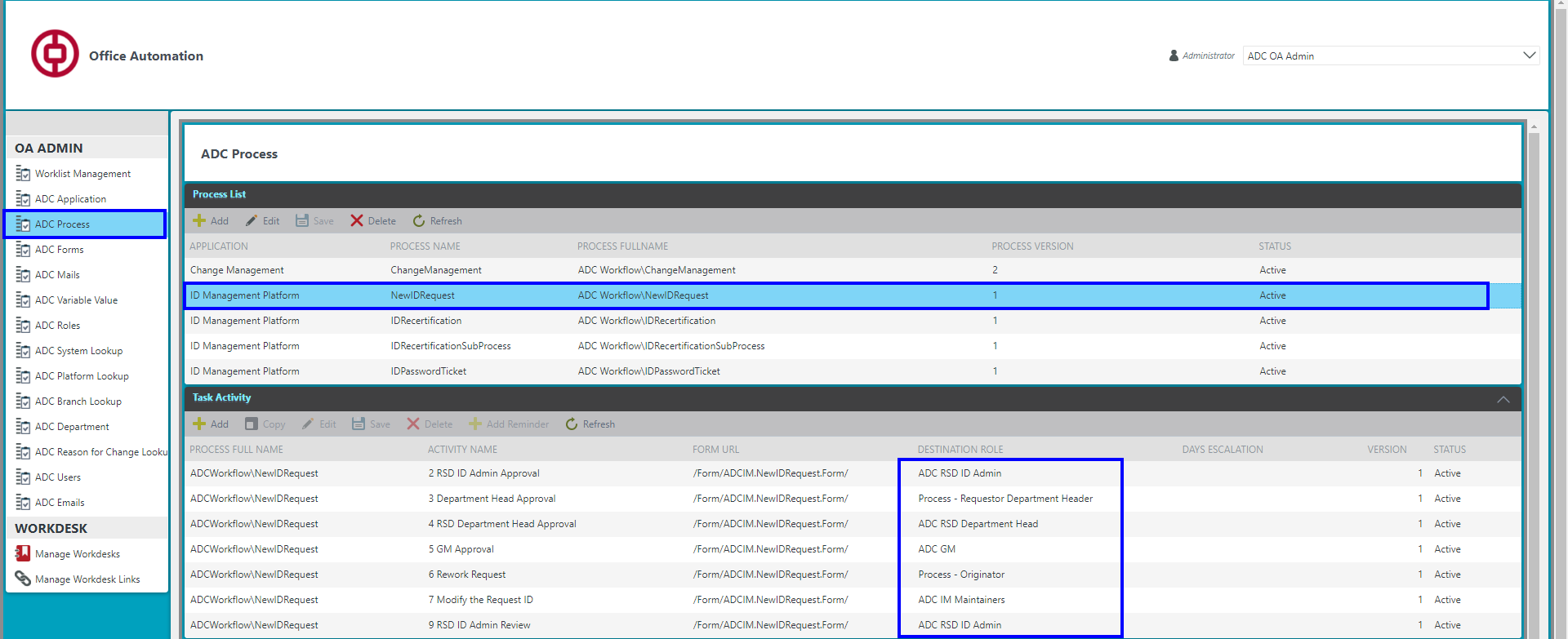
* ***ADC Department -*** in the ADC department menu, it is necessary to set users as Department Headers in the Head FQN field of the corresponding department Изображение выглядит как текст, снимок экрана, внутренний

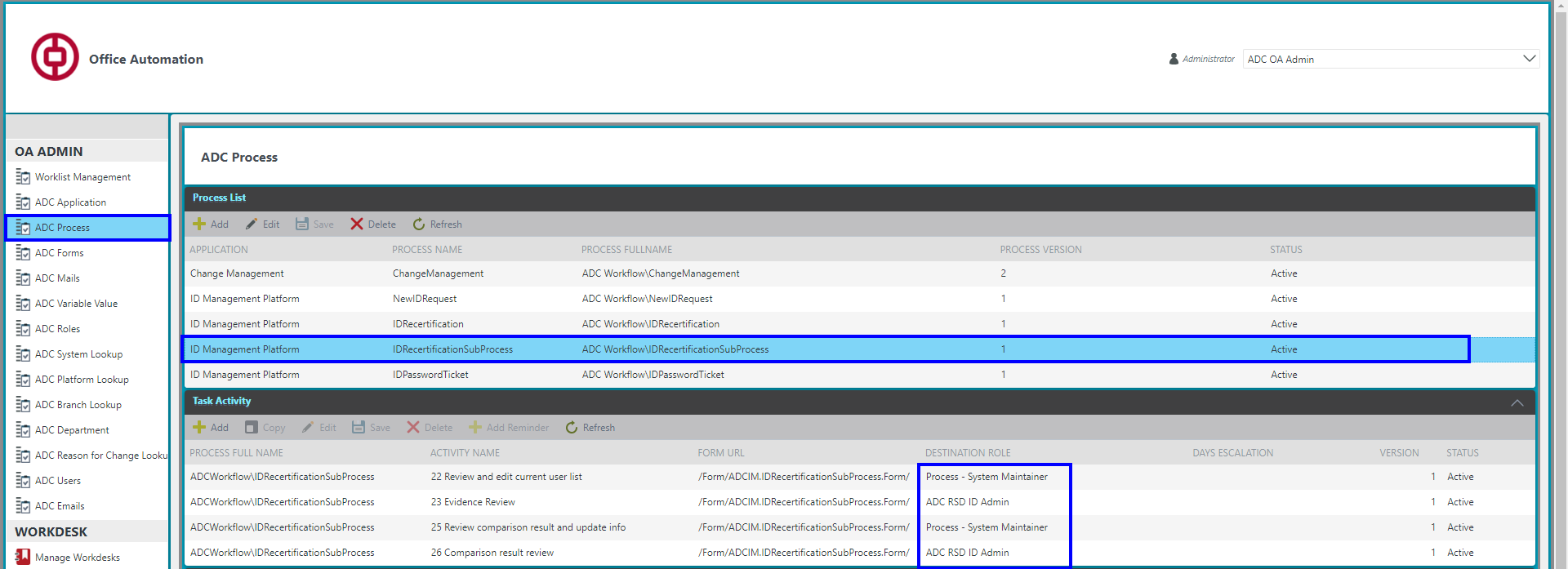
  Автоматически созданное описание
* ***ADC Roles*** bind users to those roles that are used in new processes. If the role is static, you need to configure users in this role

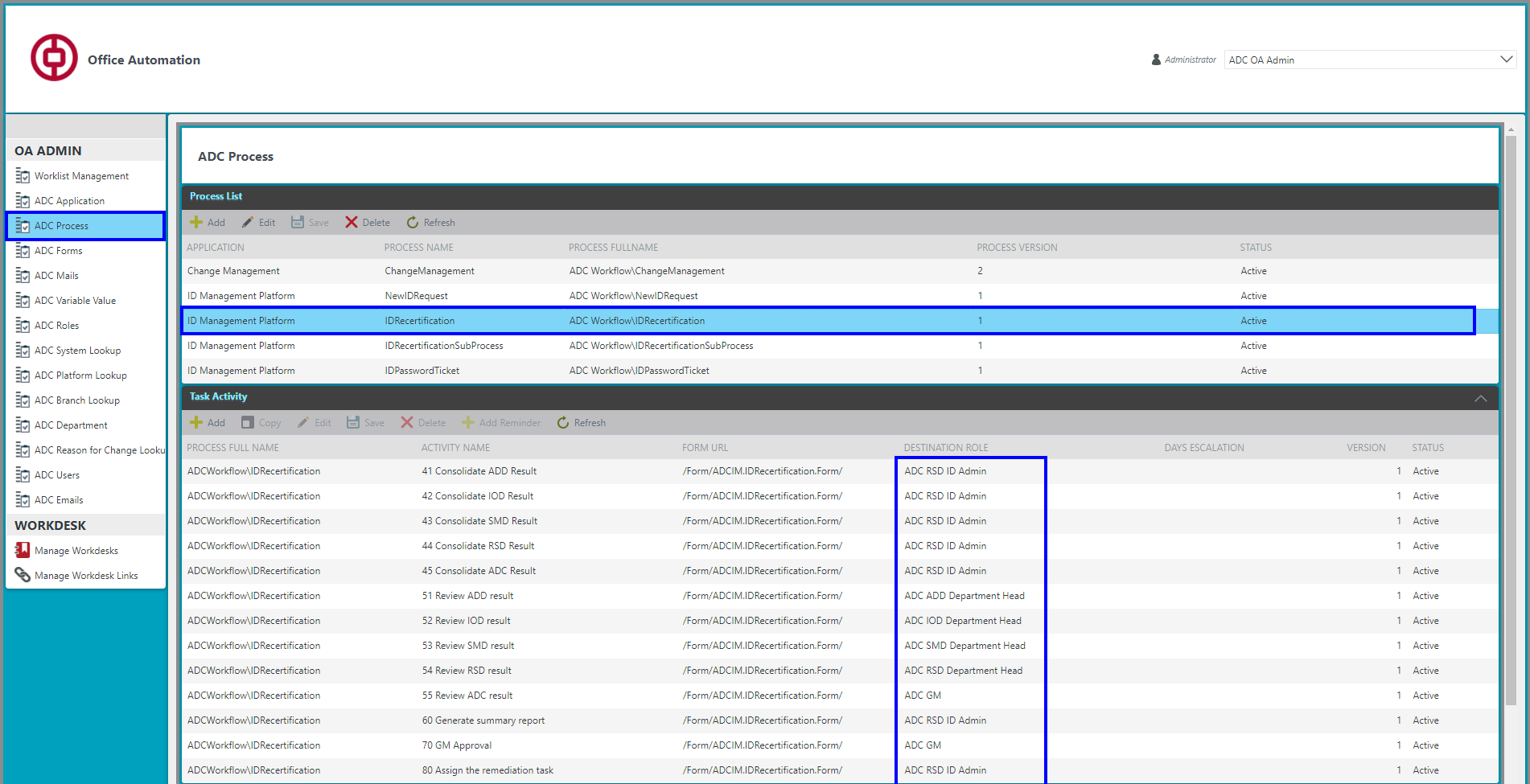
If the role is dynamic, the role will be installed automatically in the User List.

You can clarify the required Description Roles for each process by going to the ADC Process menu and selecting the required process.

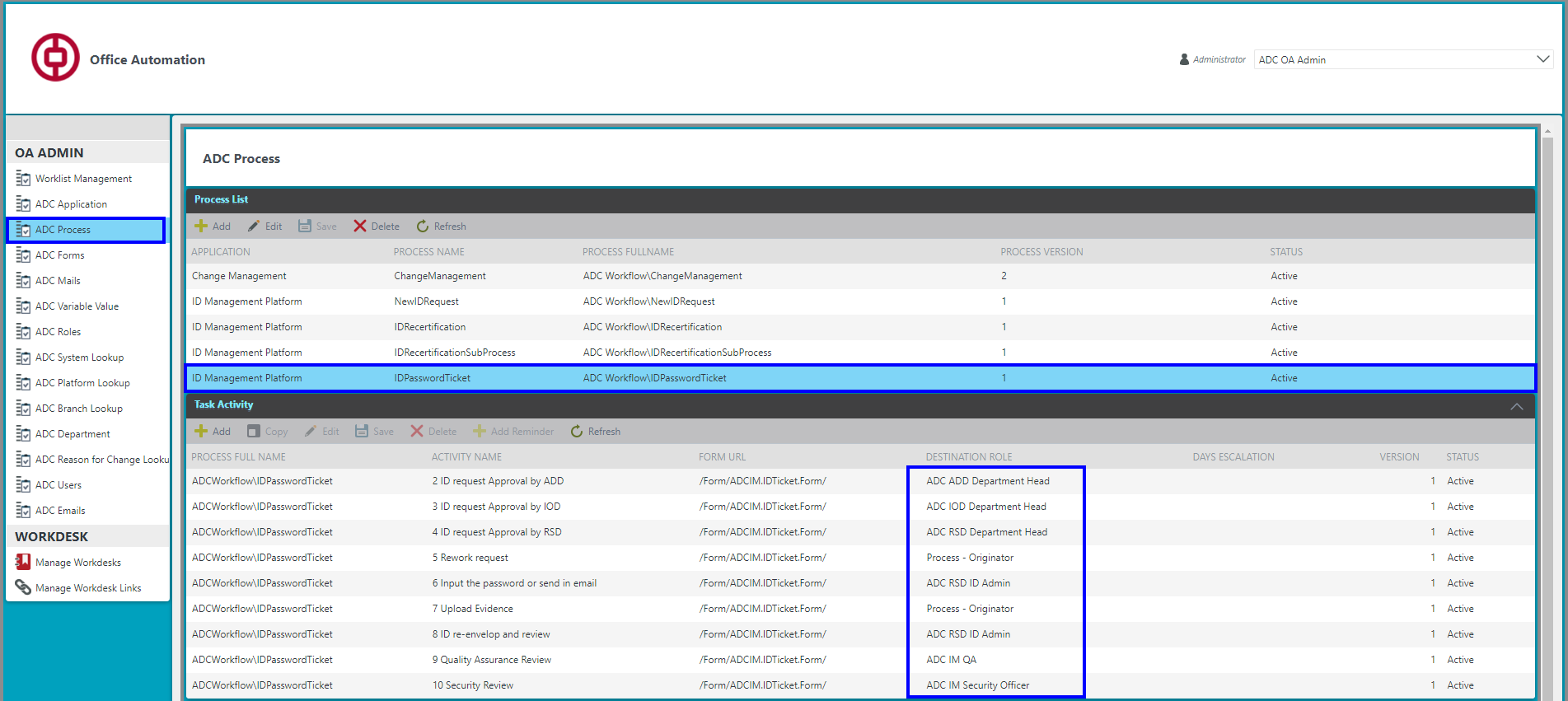
Roles required for the New ID Request Process



For the ID Recertification Process, the required roles will be located in two applications: IDRecertificationSubProcess and IDRecertification.



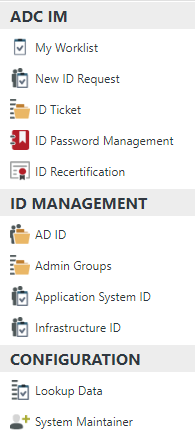
Roles required for ID ticket and Password Management Process



# ADC IM Platform

This section will discuss how the ADC IM Platform menu works and the settings that need to be made before starting processes.

The ADC IM Platform menu consists of three sections: ADC IM, ID Management and Configuration.

The **ADC IM** contains a worksheet with current tasks by process.

In **ID Management** is available only for RSD ID Admin - sees completely all systems and Maintainers - has access only to his systems by which he is assigned as Maintainer.

The Configuration section is available for configuring only RSD ID Admin

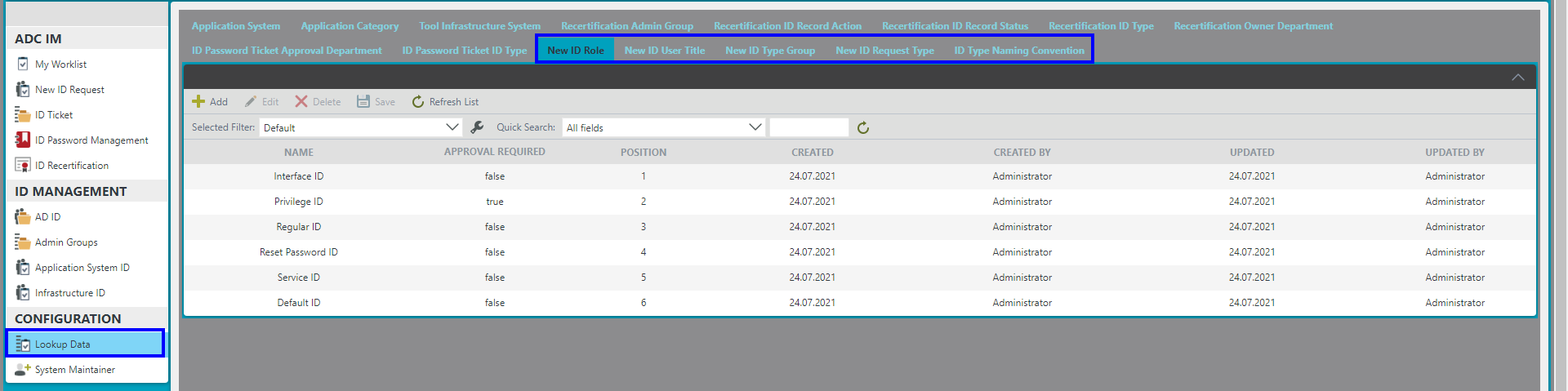
## **Configuration menu**

In the Configuration menu, the administrator needs to enter the settings for working with processes, namely the Lookup Data and System Maintainer.

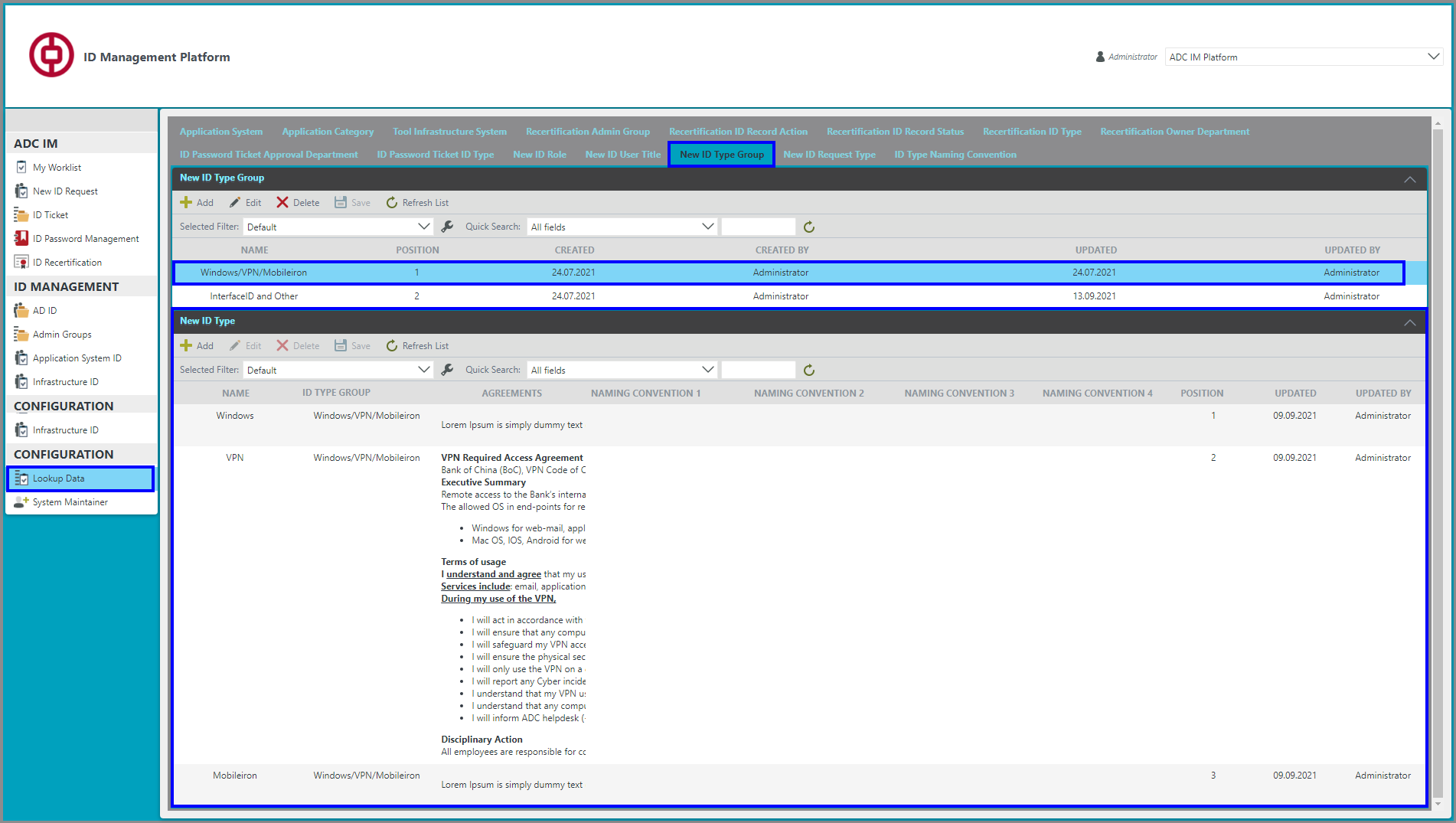
Let's consider the individual settings for each process.

### New ID Request Process

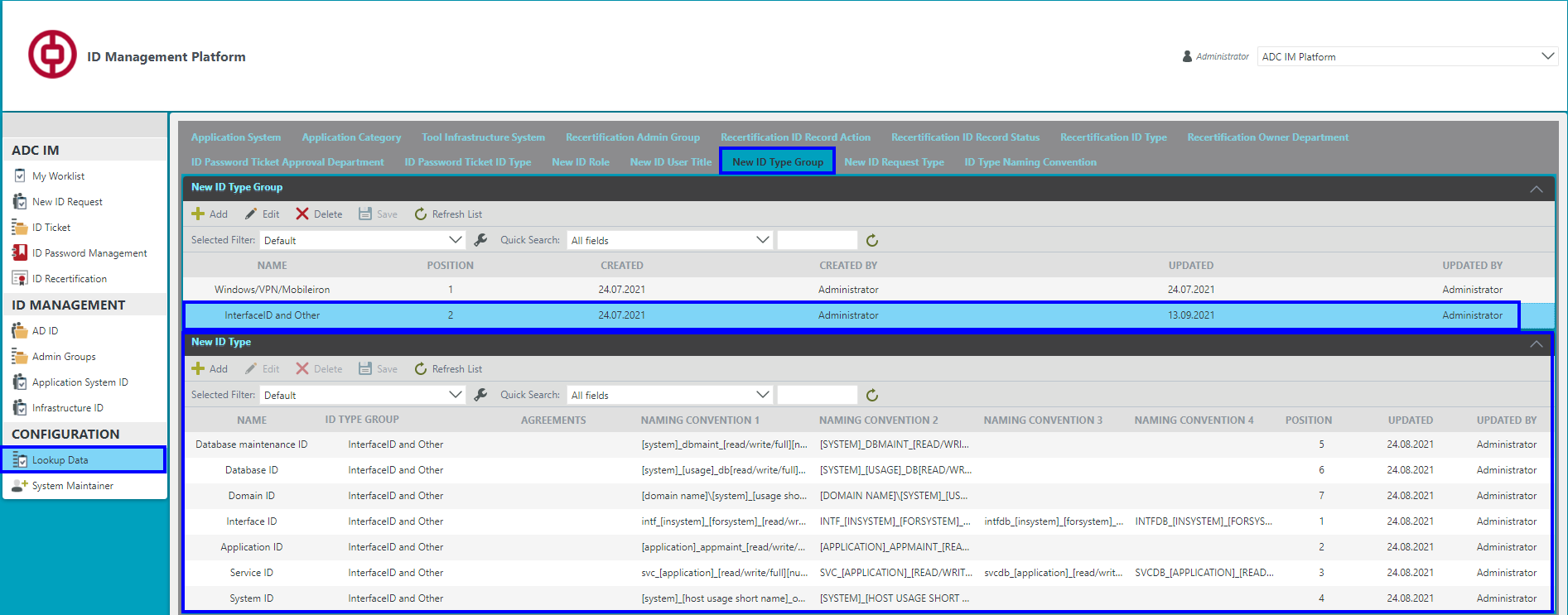
* In the Lookup Data section there are five tabs that must be filled in once for the New ID Request Process.

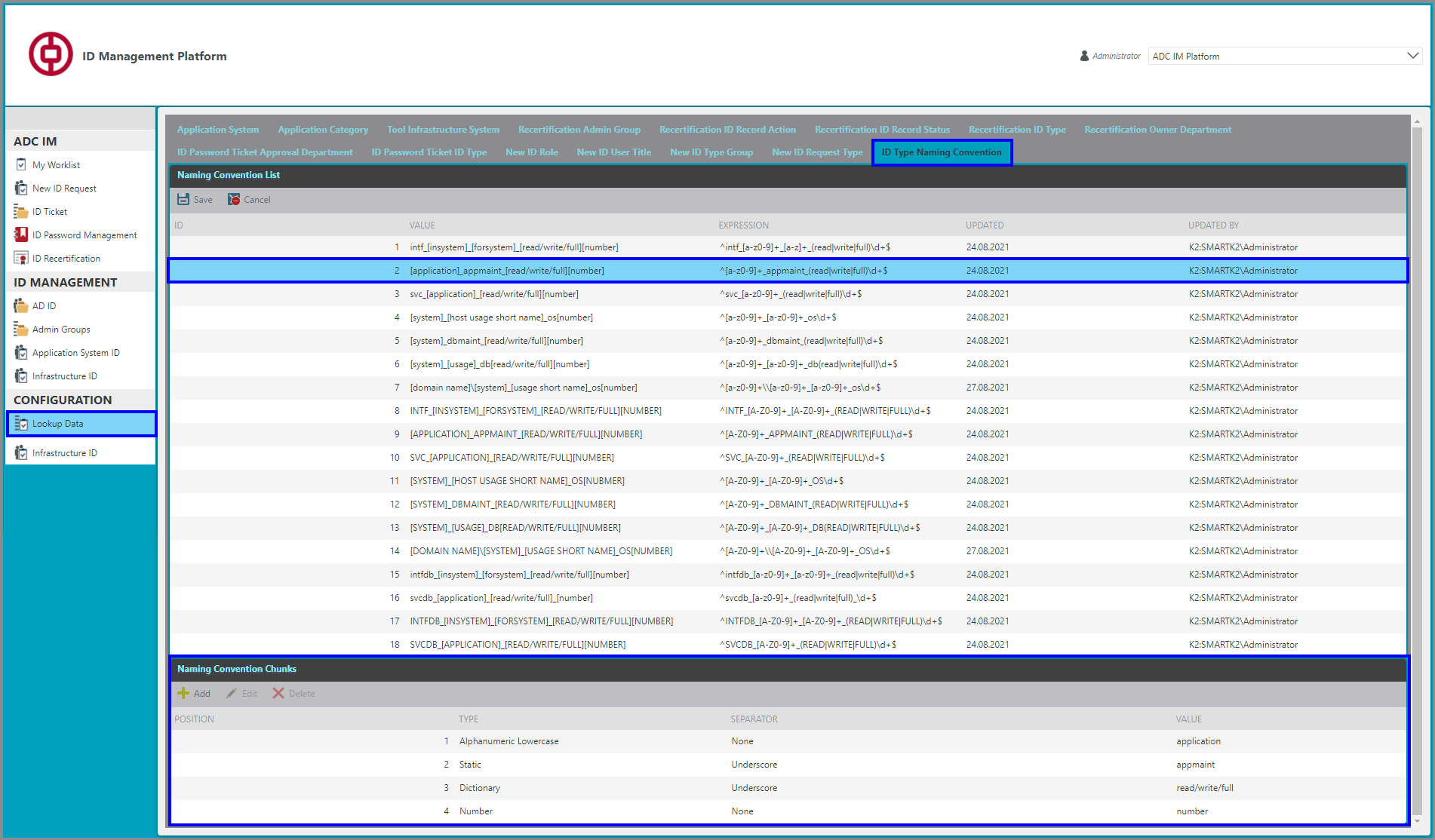
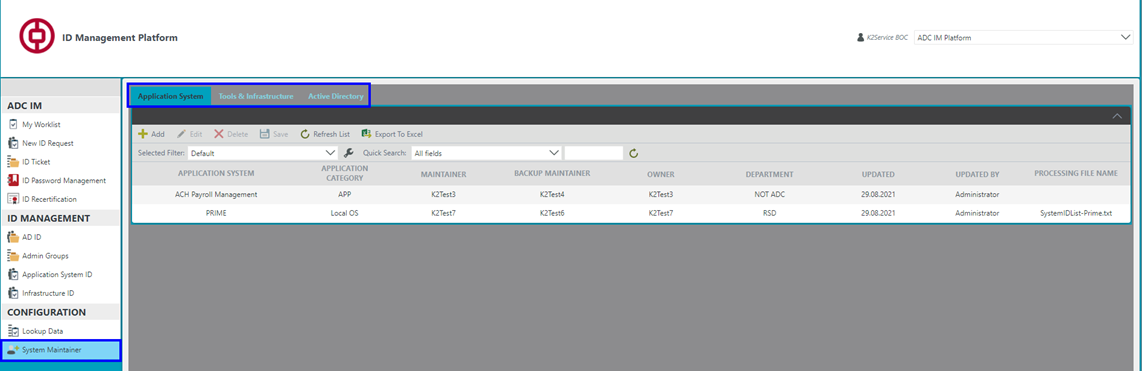


* In the **New Id Type Group tab**, specify the names of the Windows / VPN / Mobileiron and InterfaceID and Other groups. To record "Windows / VPN / Mobileiron", you must enter the text of the agreement in the New ID Type

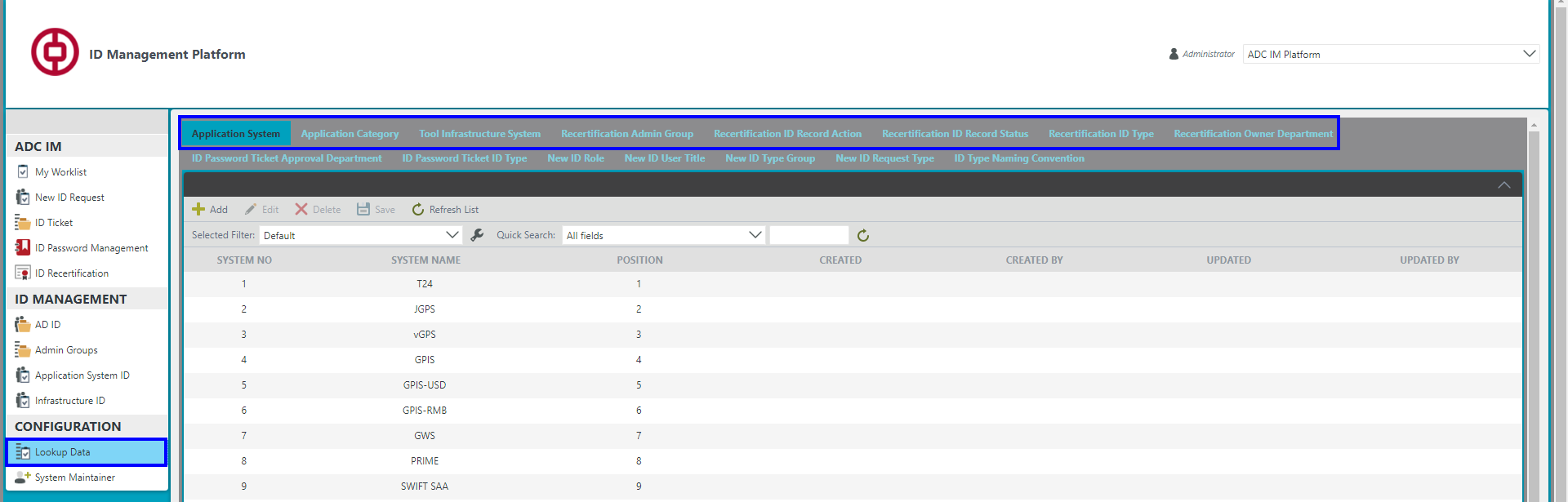


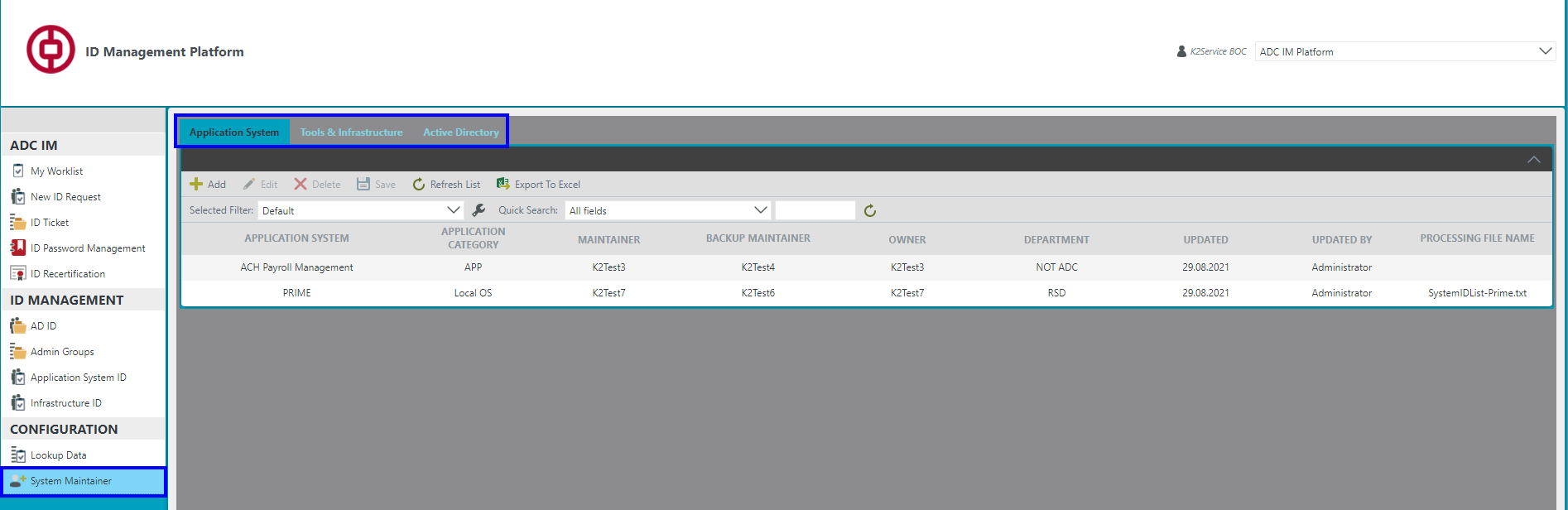
To record “InterfaceID and Other”, it is necessary to enter in the New ID Type for each Name ID Type the possible use cases for entering the Naming Convention register



* **New ID User Title** tab shows Title Name for "Windows / VPN / Mobileiron". In the column "APPROVAL REQUIRED" you can configure the condition under which Title name a request is sent to get approval from GM. In the column "TEMP PERIOD REQUIRED" you can configure the conditions for which name Title of mandatory filling Temp Period.
* The **New ID Role** tab shows the Role Name ID for “InterfaceID and Other”. In the column "APPROVAL REQUIRED" the condition of the administrator role is configured, in which it is necessary to obtain approval from the CEO of ADC
* On the **New ID Request Type** tab, the types that will be displayed in the request type are specified.
* In the **ID Type Naming Convention** tab, the input standards for “InterfaceID and Other” Naming Convention 
* For ID Type Group, the system installs the appropriate Maintainers according to the **System Maintainer** list.

### **ID Recertification Process**

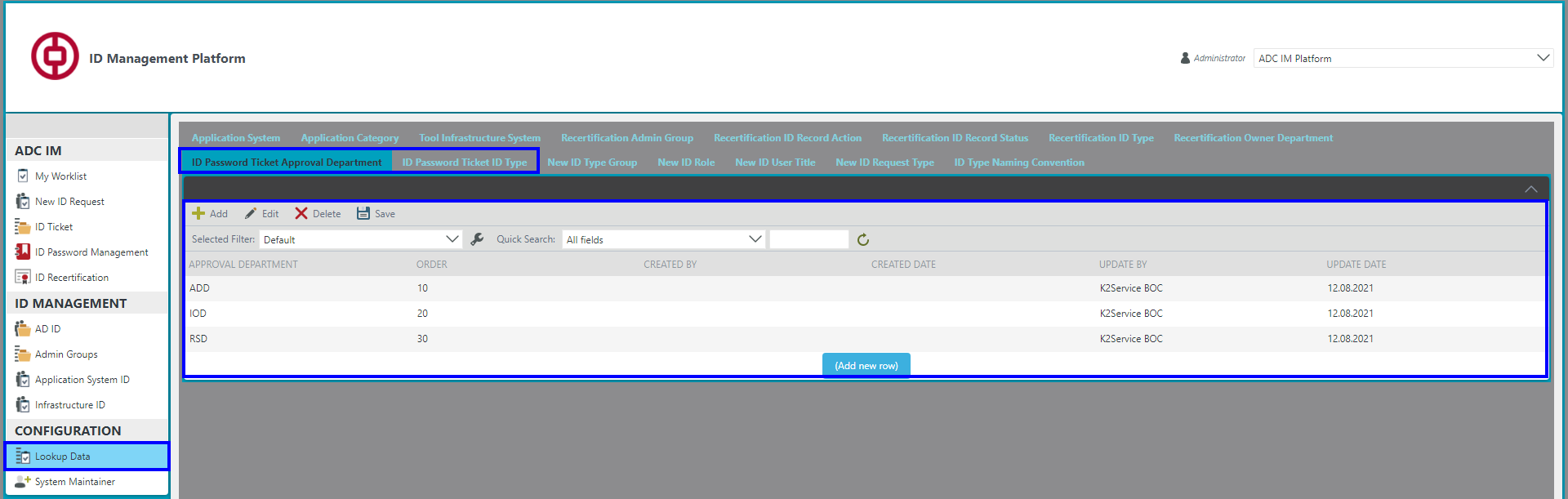
* In the Lookup Data section for this process, there are eight tabs that must be filled in once for the current process.
* For theApplication System ID process, you must add the **Application System** and **Application Category** lists
* For the Infrastructure ID process, you need to fill in the **Tool Infrastructure System**, namely System Name and Brand
* For the Admin Group process, the **Recertification Admin Group** table is filled, namely Group Name
* Fill in the **Recertification ID Record Action**, specify the name of the Action and mark for which process it will be applied
* Fill in the **Recertification ID Record Status**, indicate the name of the Status and mark for which process it will be applied
* Fill in the **Recertification ID Type** indicates the ID Type for Application System and Tool Infrastructure System
* In the **Recertification Owner Department** tab, a list of departments that are used in the ID Recertification process is entered
* Before starting to work with the "**ID Recertification Process**" it is necessary that the administrator has configured the Section "**System Maintainer**". This section contains three tabs: Application System; Tools & Infrastructure; Active Directory - which includes three categories of AD-ServiceID; Admin Groups; AD-User ID.



To work with data, a toolbar is found in the workspace.

In the column Application System, Tool Infrastructure System, AD Category - all data will change depending on the selected system. For each system, a maintainer, a backup maintainer, an owner, and a default department are specified. If you need automatic processing of the list of users, specify the file name for automatic processing in the column "PROCESSING FILE NAME". The system checks the availability of this file every hour in a special directory.

### **ID ticket and Password Management Process**

* In the Lookup Data section there are two tabs that must be filled in once for the ID ticket and Password Management Process.
* In the tab **ID ticket and password management process**, we indicate the name of the Approval Department
* In the **ID Password Ticket ID Type** tab, specify the name of the ID Type

## **ID Management**

This menu is for ID Recertification Process. RSD ID Admin sees all systems in this section. Maintainers have access only to those systems for which they are assigned as a maintainer. All AD-ServiceID and AD-User ID categories are located in the AD ID folder. Until the ID Recertification Process is completed, the ID Management menu will not be available. After the ID Recertification Process is completed, all changes made will be transferred to ID Management.

## **ADC IM**

After the above listed manipulations have been successfully completed, it is necessary to perform a one-time execution for ID Password Management and ID Re-certification process directly uploading documents

### ID Password Management

For the current process, you can manually fill in the database of users and passwords using the toolbar or Import a list with ready data

Изображение выглядит как текст

Автоматически созданное описание

By default, the master key will have the value *"****TestKey****",* which will be used when starting the process. After that, the user will be able to change this value.

### ID Recertification

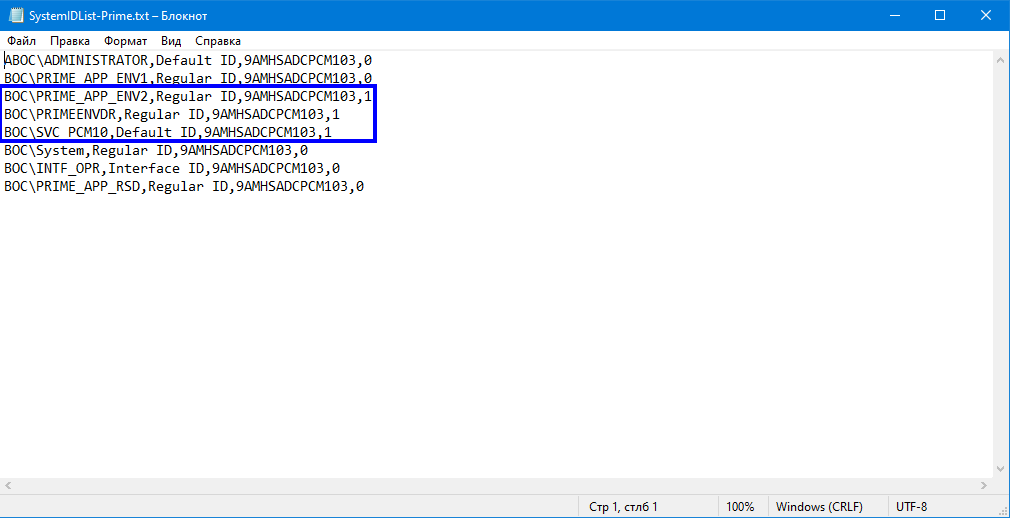
For this process, the very first time you need to Import a file with last Recertification Report

Изображение выглядит как текст, снимок экрана, внутренний, другой

Автоматически созданное описание

Wait until all records from the file are processed; this may take some time. Those processes that are not added to the System Maintainer - they will not be launched when the process starts. If the process is started for the first time after loading the Excel file, the data will have this value regardless of the Excel data Status = No Change, Action - N/A, Department = value entered in the System Maintainer

Automatic file processing with user sheet help

For this function, it is necessary to use a file with similar data in a specific directory, from which the system will unload it for processing and move it to a folder with the corresponding date when this file was processed.

After that, the automatic branch of file processing will be launched and as a result we will get an example of this kind of result