# Access Management

## Construction Document

# Table of contents

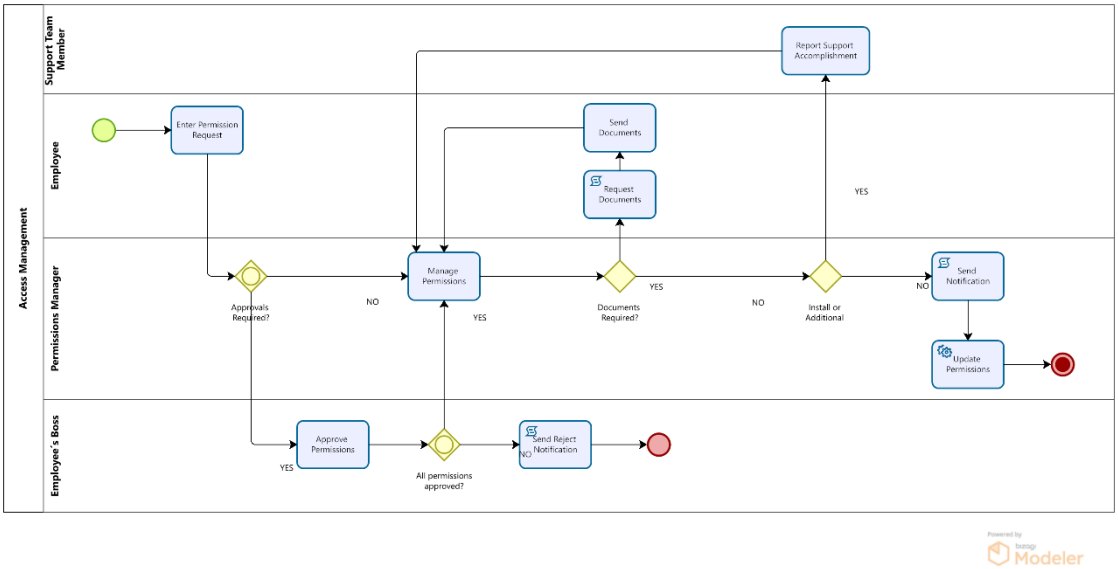
Your IT Department faces difficult challenges every day and providing an excellent service is not an easy task. The information in your company must flow easily throughout the organization in a quick and secure way. Thus, you must ensure its availability and have the necessary resources to access it.

The question is: how can your IT department know what information must be available to each user? And how can you control that every user has access only to the information that is strictly necessary? The answer is in adoption of the ITIL practices.

ITIL is a framework for the management of technological resources that is focused on ensuring customer satisfaction while achieving strategic goals through the definition of standards that allow control, operation and management of them.

Bizagi's Access Management Process template is based on the principals of ITIL practices to help you guarantee the availability of information to the users that really need it. With this template it is possible to create requests for activating or deactivating permissions over applications, modules, folders or services. It is also possible to manage approvals, enable a complete control of the activities that must be carried out in each request and update the list of user´s active permissions. In addition, you will be able to control the user's access through easy communication between the Permissions management, Human Resources and Information Security Management areas. This way you can not only attend requests faster but also create a communication channel to warrant the confidentiality and security of the information.

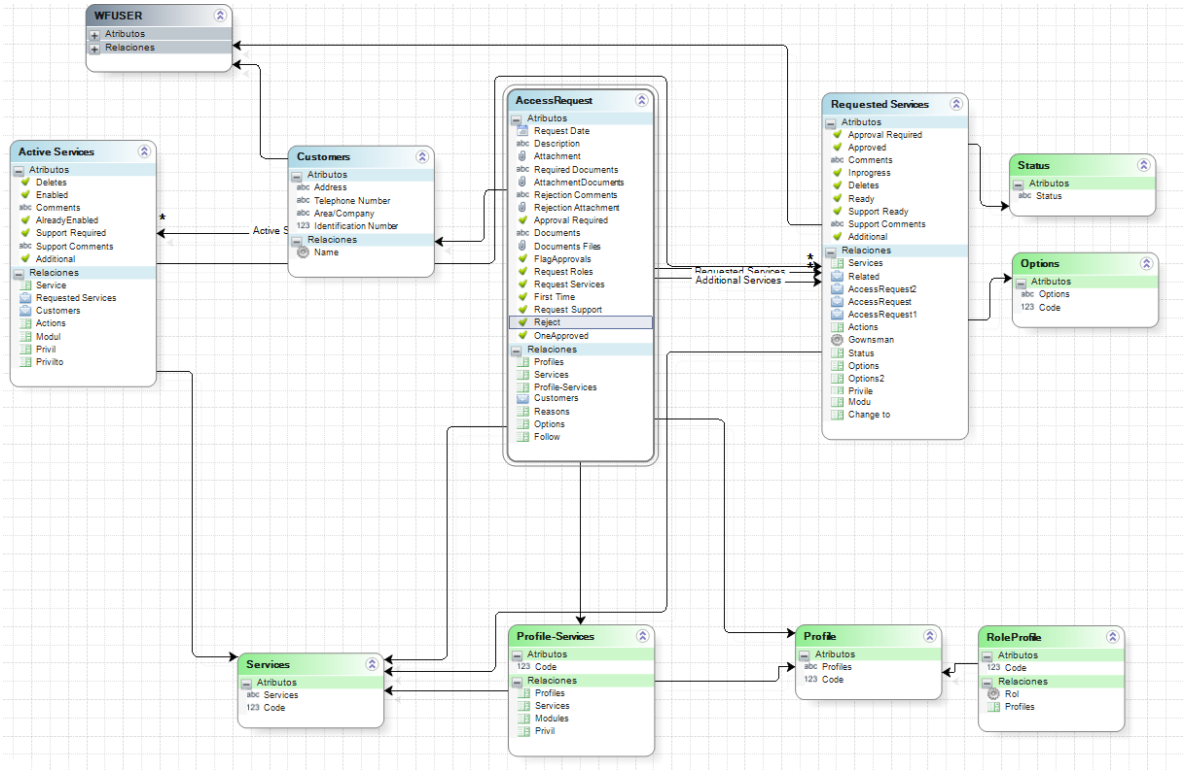
# Process description




The process starts with a request for activation or deactivation of the permissions for an employee. Once the general information of the request and the list of required actions for each permission have been entered, the process requests approvals by the user's Boss if necessary. Then, the Permissions Manager reviews the request and executes the required actions.  It is possible that additional actions are needed to complete the request, like on-site installations; if so, they are requested. When all actions have been executed, the list of user´s active permissions are updated, and a notification is sent to the employee with the permissions summary. Finally, the case is closed.

# Main Facts in the Process Construction

## Data Model




The process entity is *Permission Request* which has all the attributes and relationships necessary to save case information.

Several parameter tables were created to enable the user to define the information needed for each case. The main parameter entities are “Profiles” and “Permissions”, these entities store the information of the profiles and permissions defined by the organization. Other important entities are “Profiles-Permissions” and “Roles-Profiles” which establish the relationships between the associated permissions of a profile and the associated profiles of a role.

To store the information related to the employee´s active permissions, the master entity “Employee” is used. This entity has a relationship with the system entity WFUSER to obtain the user´s data. A relationship with the master entity “Permissions” has also been defined to identify the type of permissions.

The information of the actions requested over permissions is stored in the master entity “Permissions of the Request”. Its relationship with the parameter entity “Options” allows requesting installation or additional support, to reject the request or finish the execution of the requested actions. Once a case is finished, this table updates the master entity “Active Permissions.”

## Main Parameter Entities

**Permissions**
Permission refers to documents, folders, applications and/or services of the Service Catalogue with manageable access. This parameter entity is used to define the permissions that the organization manages.

**Modules**
This is a Sub-classification of an application, folder and/or service. This parameter entity is used to define the modules that the organization manages.

**Privileges**
This is the Level of authority that a user has over a document, folder, application and/or service of the Service Catalogue. This parameter entity is used to define the privileges that the organization manages.

**Profiles**
Profile is a group of related permissions. A role can have one or more profiles. This parameter entity is used to define the profiles established by the organization.

**Profiles-Permissions**
A profile has one or more related permissions. This parameter entity is used to define the permissions related to each profile.

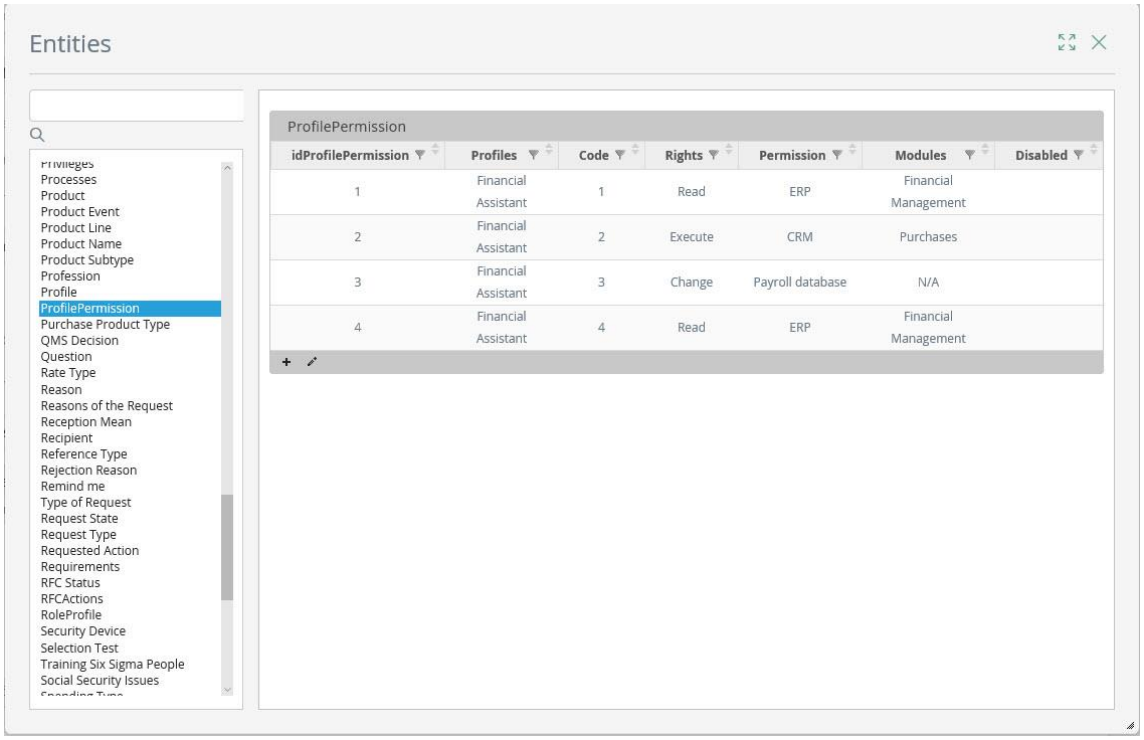
**Roles-Profiles**
A role is a Conduct or role carried out by a person in the organization. In Bizagi, a user can have one or more roles and a role can have one or more related profiles. This parameter entity is used to define the profiles associated to the different roles.

IMPORTANT: You must set the values for each entity mentioned above. If these entities are not properly configured and parameterized, the process will not be executed in the correct manner. To parameterize, we recommend following this order: Permissions, Modules, Privileges, Profiles, Profiles-Permissions, Roles-Profiles. Below you will find a guide about how to add information to these entities.

## Add Values to Parameter Tables from the Work Portal

Bizagi processes should always have an administrator in charge of parameterization to ensure that the data handled by the process is always correct. In the development environment these tables can be managed from Bizagi Studio, but when projects are in production, they can only be managed from the Work Portal.

To add or edit values to parameter tables from the Work Portal, go to the option Admin, Entities. A complete list of the entities involved in the process will be displayed; select the table you wish to add or edit values. A form will be enabled to enter the required values.

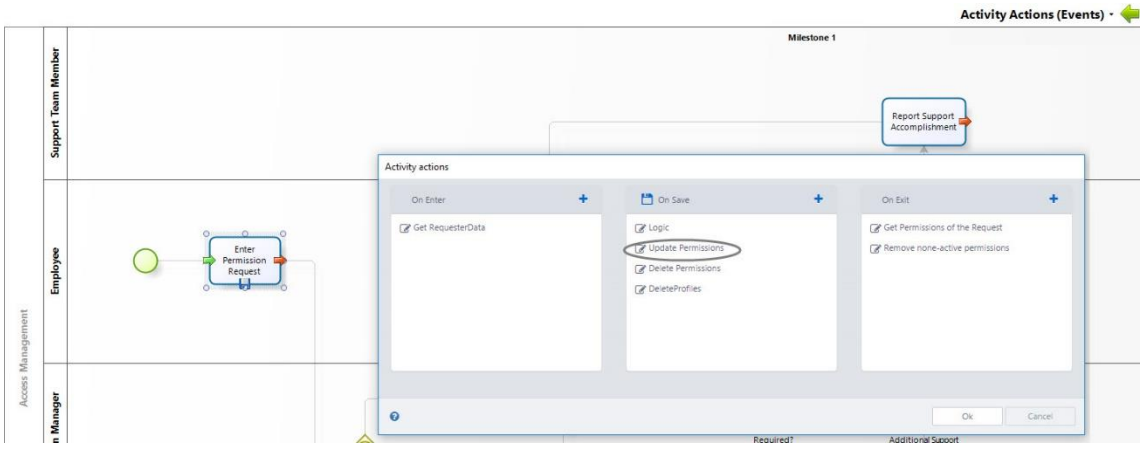



Once the table is selected you will be able to add or edit values as necessary.

## Important Rules

### Update Permissions of the Request

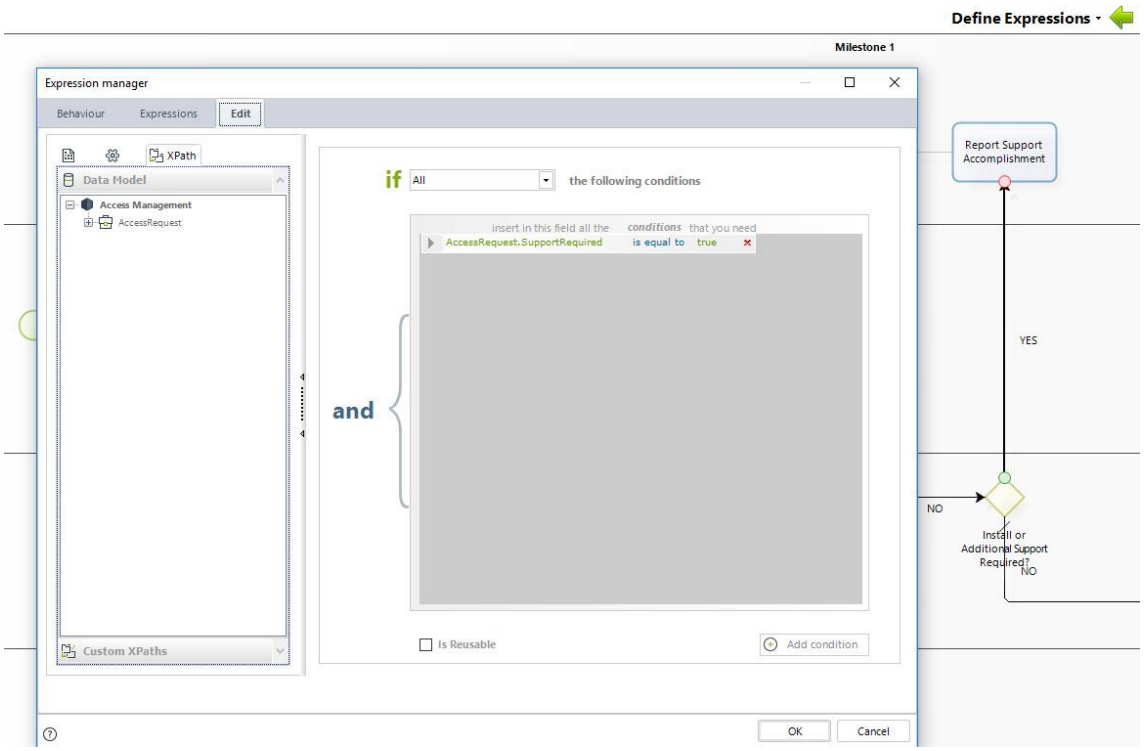
In the "Enter Request" activity it is necessary to update the permissions of the request according to the profiles that the user chose. For this reason, an 'on-save' rule is used to search the selected profiles in the master entity "Profiles of the Request", search the permissions related to each profile and add new records to the table "Permissions of the Request" for each related permission. A rule is also defined to delete the records of the permissions that are not related to any profile of the request.




### Set Paths

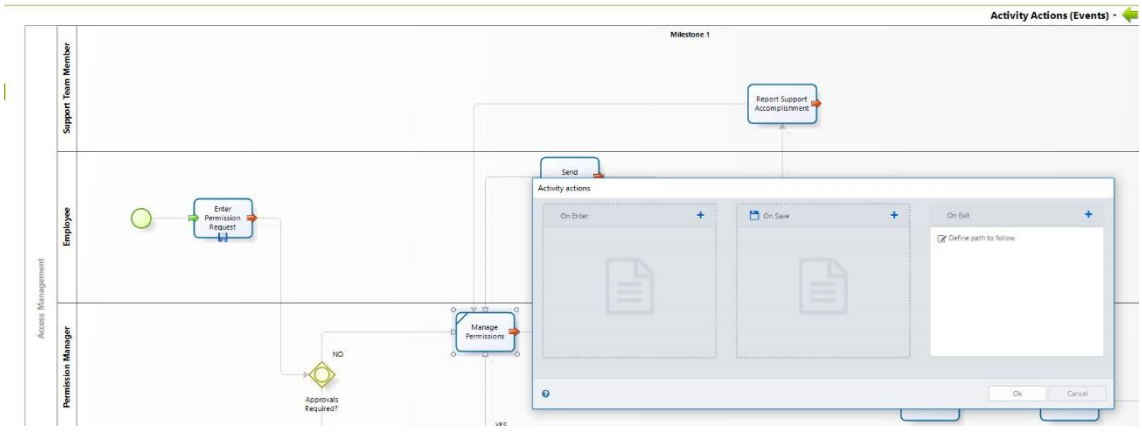
In the "Manage Permissions" activity, the conditions necessary to define the path that the process will follow are set automatically. That is if installation or additional support was requested to one or more permissions of the request, the "Support Required" attribute must be set to True. This way the gateway

"Installation or additional support required?" evaluates the condition and the process passes to the "Report Service Accomplishment" Activity. If support was not requested for any permission the "Support Required" attribute is set to False and the process will take the path to the activity that sends the notification.




## Validations

It is necessary to update the list of the user´s active permissions in Bizagi. To do this, a rule is used in the "Manage Permissions" Activity. This rule searches in the "Requested Permissions" table for any record with a status other than Ready or Rejected. This way any record that meets this condition has not been managed, therefore a validation message must be issued to advise that all the permissions must be managed.



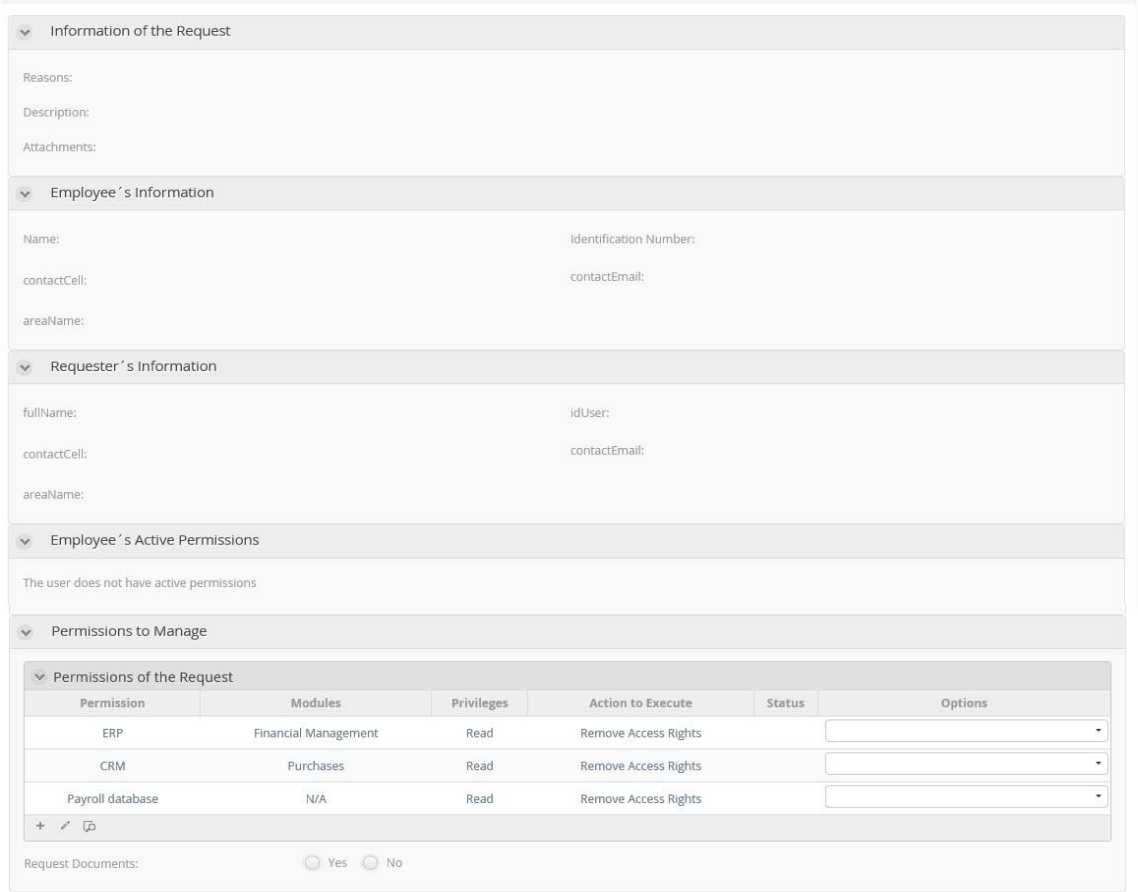
# Forms

## Master Entity Filters

In all activities of the process there are filters that allow presenting the information according to that which the user needs and thus allowing easy query and addition.

In the "Enter Request" activity, the master entity "Active Permissions" is filtered to differentiate the permissions that are already enabled and the permissions of the request. This way the edition on the records of active permissions is not allowed, but it is on the records of requested permissions.


In the "Approve Permissions" activity and "Record Service Accomplishment" the master entity "Permissions of the Request" is displayed. A filter is used to show only the records to which those actions have been requested, this way, these actions will only be performed for the necessary permissions.



## Calculate Response Times

Bizagi provides organizations with management indicators that are fully comprehensive and easy to interpret based on accurate, real time business information, allowing process owners to make agile flow adjustments and better, more efficient decisions to optimize the performance of business processes.

Through the Sensor Analytics menu and its options Stopwatches and Counters, Bizagi offers a feature as a tool for continuous process improvement to review and control:

Time and number of cases between any two tasks in the process.
Number of activations of a given task.
SLA comparisons.

You can easily configure this feature to control the response times of the different permission requests. For more information go to http://help.bizagi.com/bpmsuite/en/index.html?sensors.htm