Identity and Access Management

Ext.prc.007.10 | 11.11.2025

UPM 25.x

ZINFI Confidential & Proprietary
Shared Under NDA

Contents

Overview

ZINFI's UPM platform is used by many different user groups that execute the channel management processes of individual organizations. UPM includes a variety of Access tools that are provided to manage access by sales, customer service, and marketing departments to create, modify, update, and remove records in the UPM database.

The accuracy of UPM data is a key driver for integrating Access solutions across the UPM system. Our UPM solution enables a tiered, delegated administration model, whereby customers have access to self-service workflows for registering, creating new identities, inviting partners/users, and authorizing partners/users.

Managing the complexities of security administration is another primary concern of the UPM platform. The foundation of the platform's security management is a role-based access control model. ZINFI UPM provides a set of security features that define permissions for access to the data as well as to the features and Applications of UPM.

Role-based security ensures that data is accessible to users based on organizational hierarchy. Profiles are created to ensure that users have permission to access only the features, Applications, and data administration tools that are relevant to them. The establishment of groups allows organizations to extend data-level access to other users with similar job profiles.

Acronyms

CMM Channel Marketing Manager

The primary channel marketing lead for portal and campaign content management and necessary Application setup for CPA, CP, NCP, etc.

CPA Channel Partner Administrator

The primary administrator from the partner organization is in charge of managing user access, lead distribution, incentives management, etc.

CP Channel Partner

A user from a partner organization with appropriate access rights for various Applications, which have been set by CMM and CPA.

PMC Partner Marketing Concierge

Engages and supports partners in various activities including running campaigns, partner support, etc.

Base Architecture

UPM's Access features can be used to control user access to transactions (such as converting an opportunity) and activities related to an object type (such as creating or deleting a product). UPM also provides a framework for controlling **User** access to individual business objects, and for controlling the use of those business objects with respect to **Profiles** and **Groups**.

User: A user is an individual who manages records within the organization.

Profiles: Profiles in UPM determine which users can access Applications as well as which operations the users can perform within those Applications. When configuring profile settings in UPM, an administrator may choose to enforce restrictions for entire Applications or selected fields on the records in an Application, as explained in the following sections. To fully leverage UPM's security model, both permission types can be used together for a given role and be effectively used by your organization.

Groups: Groups are collections of users. These are used to simplify management; a change in the access rights assigned to a group is automatically applied to all users in that group.

The access control engine in ZINFI's UPM is an authorization concept that exists at two levels of abstraction:

With **Application-level permissions (governed by profile)**, administrators can create different profiles and assign regular users to the profiles. UPM adheres to the most restrictive policy to determine the user's appropriate access levels. Profiles control multiple layers of actions pertaining to Applications and access for users/groups within the UPM:

With **record-level permissions (governed by group)**, UPM's Record Visibility configurator intelligently assists administrators in setting up and restricting access at the record level. Layouts of pages can be effectively configured via UPM's state-of-the-art Workflow configuration tool to designate the fields (of a record) to be accessible by a user in an application:

Application-Level Management

Application-level management defines which users see which business Applications/objects and forms the initial level of Access. Application-level management allows you to easily control access to individual Applications by specific users (Refer Fig. 2). You can allow your partners to manage access to Applications like prospects, contacts, accounts, MDF, companies, etc., while at the same time, you remain in control of the finer levels of information with access to reports.

Application-level management is driven by the following parameter(s):

Parameter(s)	Description	Additional Comments
Application(s)	Identifies which Applications the profile will be associated with. **(Ref. Fig. 1)**	Applications (courses, opportunities, content library, etc.) can be added to the specific profile with the respective Application display name.

Application Level

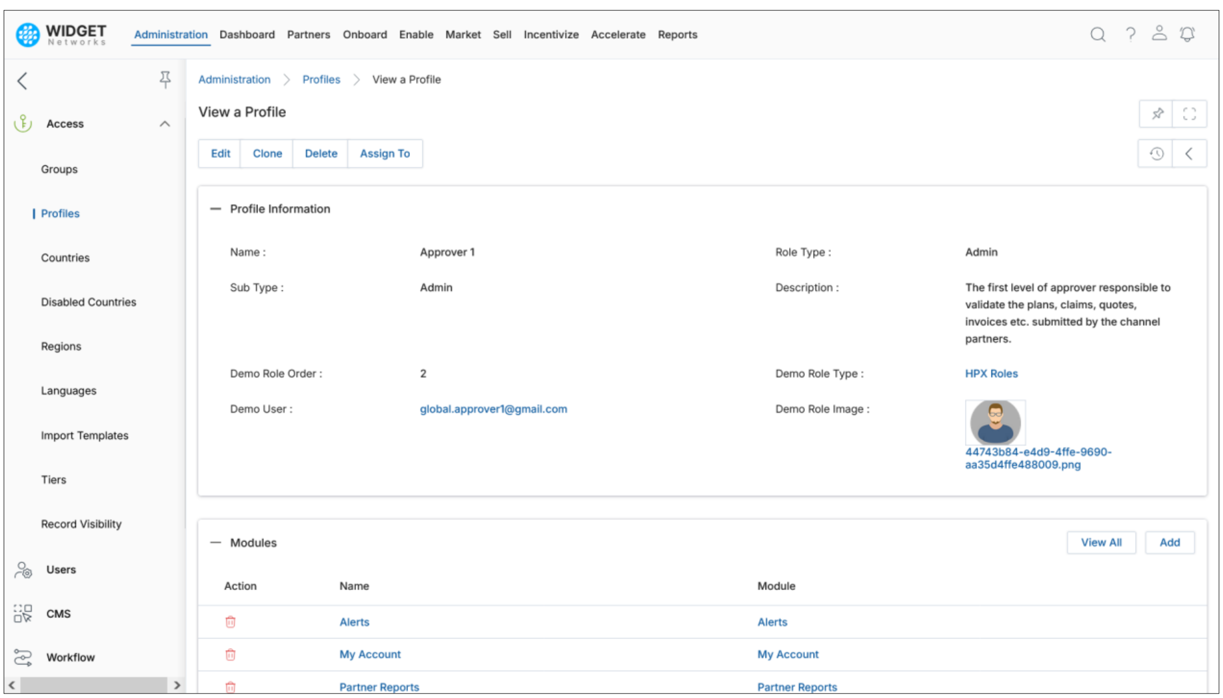


Figure 1: Add Applications to Profile Access

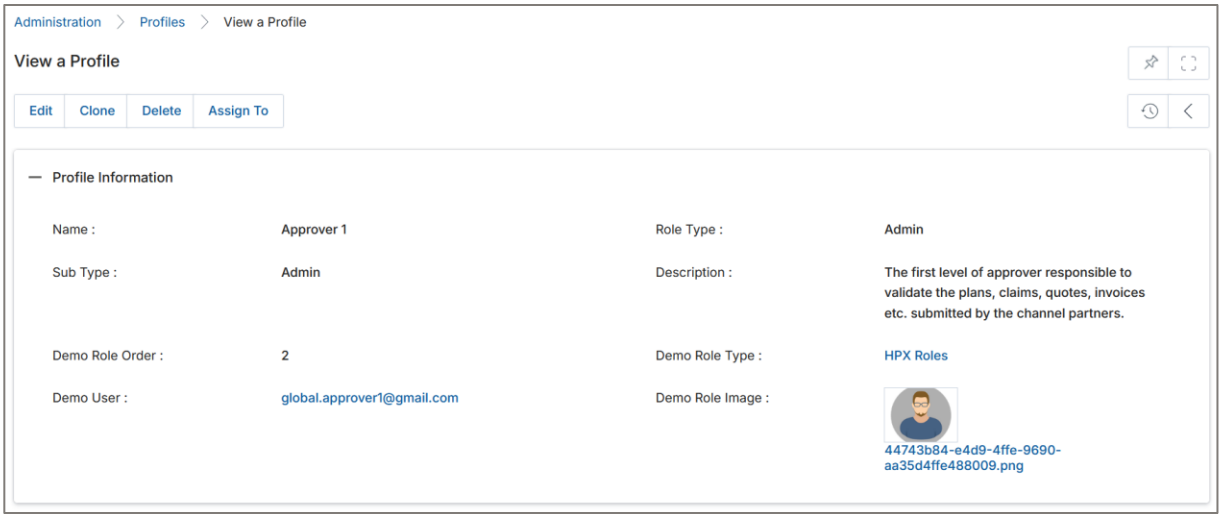


Figure 2: Selection of Role Type for a specific Application

Figure 3: Adding Application Shortcuts 1

Application-level access is the most restrictive of all access levels and shortcuts can be created to be displayed in UPM's left menu bar (refer to Fig. 3). It provides read-only or read-write permission to users for each Application residing in the application, as depicted in *Figure 4*.

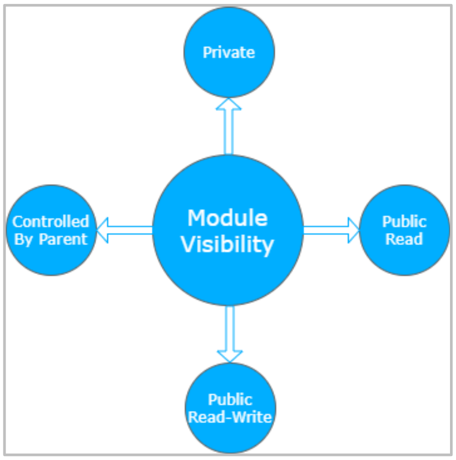


Figure 4: Application-Level Permissions

Private

This is the default level of access given to each Application. With the access level set to **Private**, a user can perform the following actions:

- View (read) his/her record.
- Modify (write) his/her record.
- Delete his/her record.

Note: Throughout the application, for all access levels, records can only be deleted by that record's owner—i.e., the user who has created the record.

If any Application has this privilege and there is no rule for that Application or no manual sharing assigned with the user/group, then only those record(s) that are created by that user him/herself will be visible to that user. Beyond this, Group Specific Rule and Sharing Rule can also be applied for that Application.

Public Read

With the access level set to **Public Read**, all records are made visible to all users only in read-only mode. Hence, a user can perform the following actions:

- Can view any user's created record.
- Cannot edit other user's records, since they would be available in read-only mode.

Note: Records can be modified only by setting a custom rule and/or manual sharing.

Public Read-Write

With the access level set to **Public Read-Write**, all records are made visible to all users in read-write mode. Hence, a user can perform the following actions:

- Can **view** any user's created record.
- Can **edit** any user's created record.

Note: In the hierarchical image depicted, Application Visibility is at the bottom of the hierarchy. Therefore, if there is Public Read-Write permission for any Application, then there is no need to set up any rule for that Application.

Controlled By Parent

With the access level set to **Controlled By Parent**, the access properties of the parent Application are applied to the child (target) Application. That means if the parent Application has ***Public Read*** access, then for a specific parent record, all the child records would be viewable by all users.

To make this clearer, let's consider the Application **Notes**. When the Notes Application is attached to the Prospect Application (having Public Read permission), all users would be able to view every note attached by multiple users against a specific prospect.

Record-Level Management

In UPM, different types of groups (sets of users) can be created to manage a set of common records. Users associated with a specific group can access the records shared with a particular group and perform any necessary operations on those records.

In UPM, Record Visibility is typically used to control which groups of users can access a record (see Figure 7). However, using record-level, group-based permissions, an administrator may choose to extend the purpose of groups to control who can perform certain operations on a record. When enabled, regular users can control a record's visibility to grant access such as viewing, editing, exporting, importing, and deleting permission to specific users or user groups through the following:

- Group Specific Rule
- Sharing Rule
- Manual Sharing

Group-Specific Rule

The specific Rule (see Figure 5) is a vertical approach that provides read-only or read-write permission to groups bound by this rule. Users belonging to those groups gain access to the group's assigned permission.

The rule is categorized into three types:

- Group Hierarchy
- Group Based

- Admin Visibility

Note: After the assignment of this rule to a group, the **Primary** group of users belonging to that group will be affected. Users under **Additional Group** will not be affected.

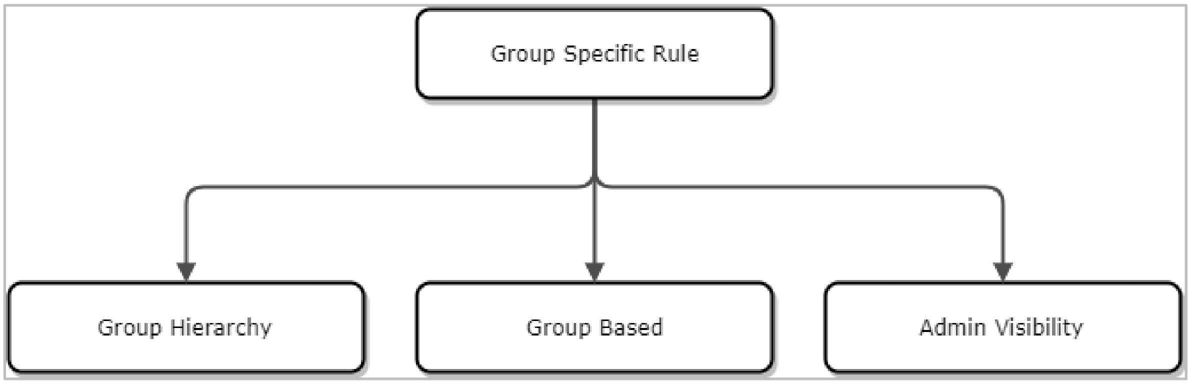


Figure 5: Group Specific Rule Categorization

Group Hierarchy

Group Hierarchy enables the record visibility of a specific group to its immediate members vertically in the hierarchy chain in read-write mode.

For example, in Figure 6 below, let's say we have enabled ***Group Hierarchy*** initiating from group CMM for group **PMC** for the Application **Contacts**. Considering the hierarchical order of groups (in the same vertical hierarchy chain) wherein CP reports to CPA, and CPA reports to PMC, users of group PMC will be able to view user records under groups CPA and CP in read-write mode. Similarly, CPA will be able to view user records under group CP in read-write mode but will not be able to view records under group CPA.

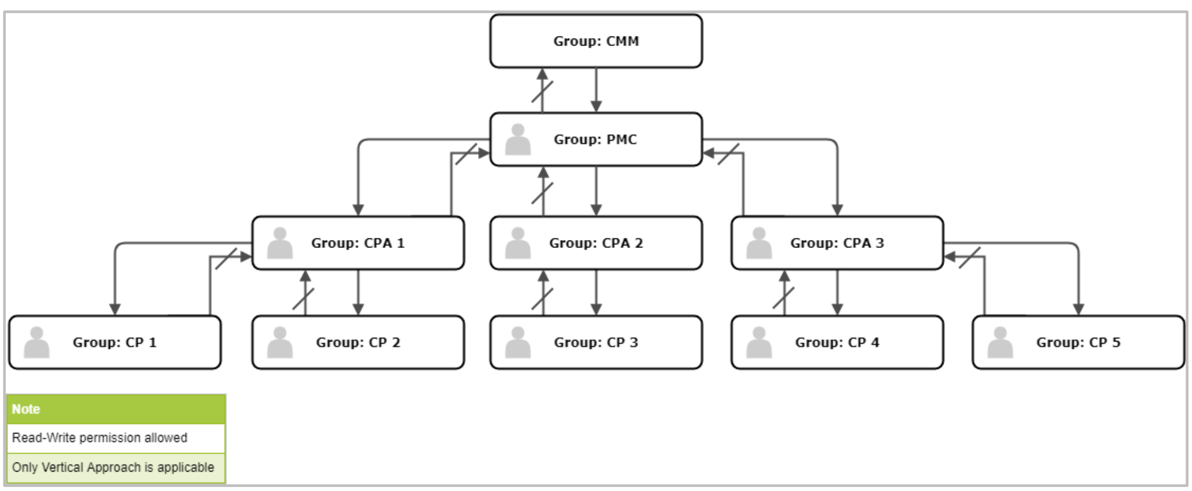


Figure 6: An Example of Group Hierarchy

Group Based

Group-based rules enable record visibility for a group's own members when enabled against a specific group in read-only mode. A user's own records would have read-write permission only.

For example, let's say we have enabled ***Group Based*** in the Application **Documents** for group **CP**. In that case, the logged-in user (if he/she is a member of the CP group) can access the records created by others who are associated with the CP group in read-only mode.

Admin Visibility

Admin Visibility refers to the highest authority given to any group under Group Specific Rule. This approach is implemented at both the Application level and the group level. If any group has this privilege, then the users under this group can access all the records of that Application with read-write permission.

For example, if we enable ***Admin Visibility*** in the Application **Accounts** for group **CMM**, then all the members of group CMM can access all the records of the Application Accounts with read-write privilege.

Sharing Rule

Sharing Rule is a horizontal approach to Record Visibility Management which enables sharing of records to different groups, either by group name or by criteria. The sharing Rule is applied at the Application level.

There are two types of Sharing Rules:

- Group Based assignment.
- Criteria-based Based assignment.

Group Based Assignment

This feature (see Figure 9) is used to create a rule to assign all records of a group to another group, either in read-only or read-write mode for a specific Application. Assigning records to multiple groups can be done by creating multiple rules for that Application.

Criteria Based Assignment

This feature (see Figure 10) is used to share records of any group to a specific group for a specific Application, based on one or more criteria, either in read-only or read-write mode. The criteria are applied to specific fields of that Application. Records can be assigned to multiple groups by creating multiple rules for that Application.

Record Level - List of Figures

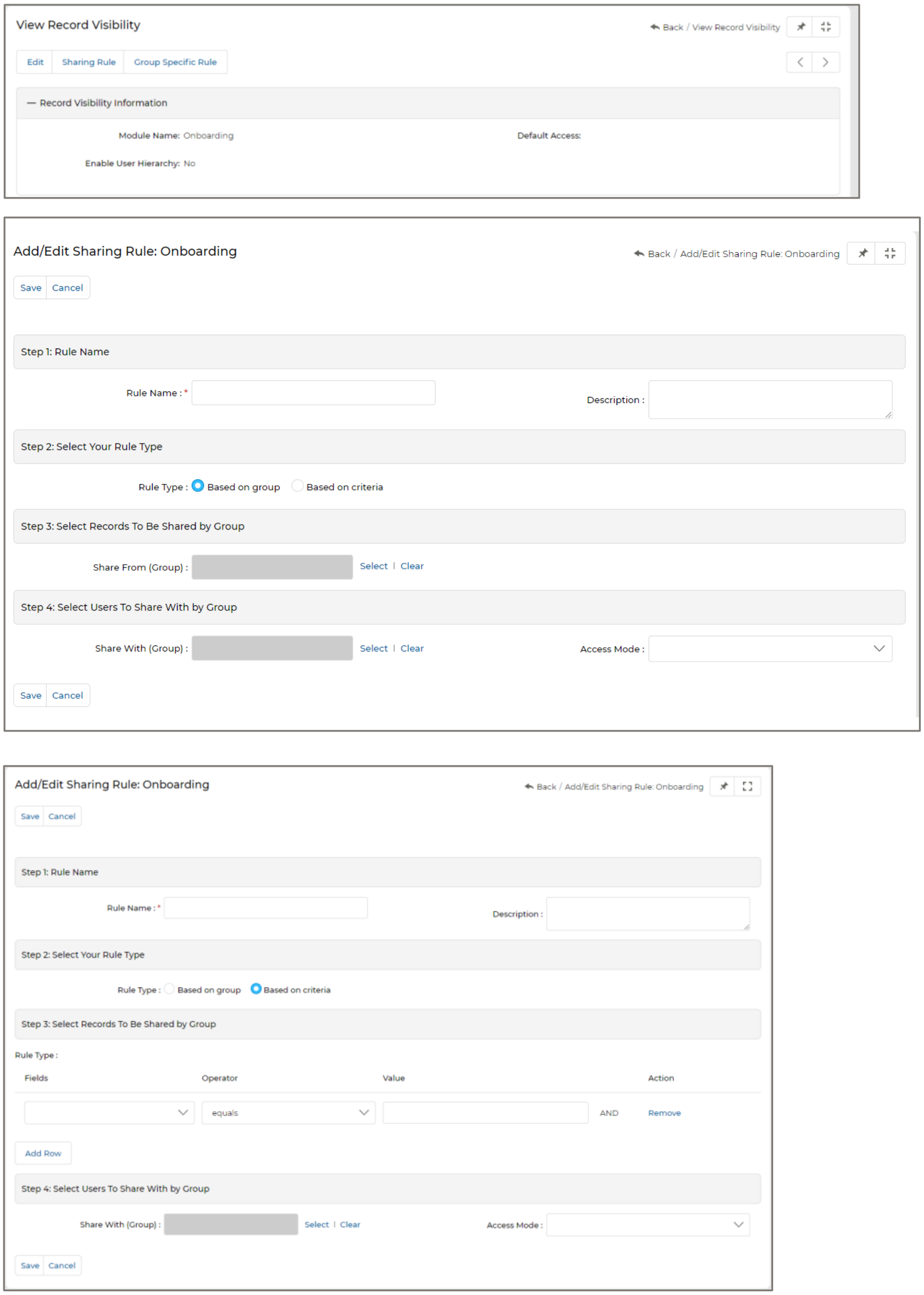


Figure 7: Group Specific Rule

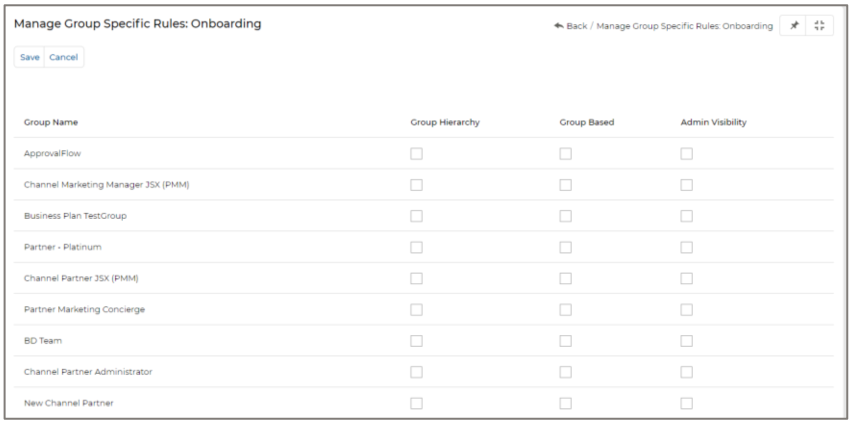


Figure 8: Sharing Rule - Group Base

Manual Sharing

Manual Sharing is the broadest access provided in the hierarchical structure of Record Visibility Management. Manual sharing provides additional access beyond the organization-wide defaults and sharing rules.

Manual Sharing is applied at the record level. With this approach, we can assign any record to any user or group with read-only or read-write permission.

How Do I Apply Manual Sharing?

To apply Manual Sharing, go to the ***details page*** of a record, and then click on **Assign To**. The options for manual sharing will appear and then you can select the necessary criteria to achieve the level of sharing required.

Applications for Which Record Visibility Can Be Implemented

Record Visibility is implemented for the following zones and Applications:

- **Sales:** Prospects, Contacts, Accounts, Opportunities, Assets, Tasks, Notes, Documents
- **Marketing:** Products, Campaigns, Assets, Emails, Web Syndication
- **Profile:** Partner Prospects, Partner Contacts, Partner Accounts, User Management
- **CMS** Application for the top menu

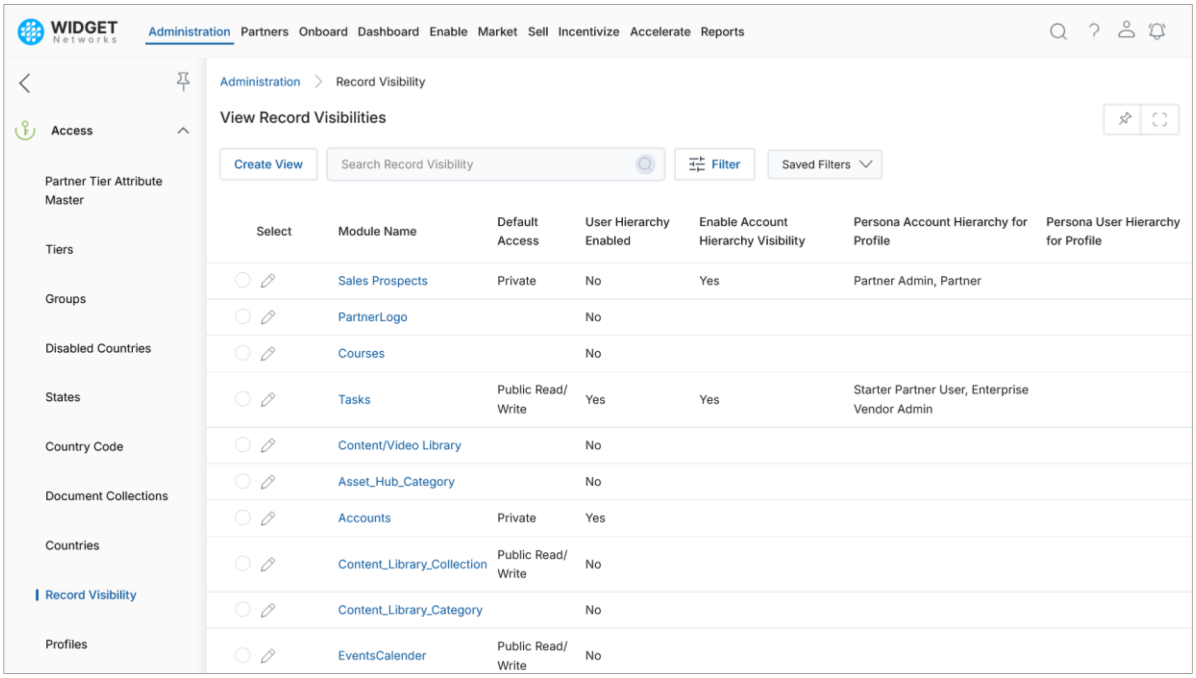
Application-Level Activity

Application Name	Default Access	User Hierarchy	Sharing Rule	Group Hierarchy	Group Based	Admin Visibility	Manual Sharing
Accounts	✓	✓	✓	✓	✓	✓	✓
Asset Management	✓	✓	✓	✓	✓	✓	✓
Business Plan	✗	✗	✗	✗	✗	✓	✗

Campaign Management	✓	✓	✓	✓	✓	✓	✓
Contacts	✓	✓	✓	✓	✓	✓	✓
Contracts	✗	✗	✗	✗	✗	✓	✗
Documents	✓	✓	✓	✓	✓	✓	✗
Emails	✓	✓	✓	✓	✓	✓	✓
Engage	✓	✓	✓	✓	✓	✓	✗
Notes	✓	✓	✓	✓	✓	✓	✓
Opportunities	✓	✓	✓	✓	✓	✓	✓
Partner Accounts	✓	✓	✓	✓	✓	✓	✓
Partner Contacts	✓	✓	✓	✓	✓	✓	✓
Partner Prospects	✓	✓	✓	✓	✓	✓	✓
Products	✓	✓	✓	✓	✓	✓	✓
Prospects	✓	✓	✓	✓	✓	✓	✓
Syndication	✓	✓	✓	✓	✓	✓	✓
System Email	✗	✗	✗	✗	✗	✓	✗
Task Management	✓	✓	✓	✓	✓	✓	✓
Tier Management	✗	✗	✗	✗	✗	✓	✗
Training Management	✗	✗	✗	✗	✗	✓	✗
User Management	✓	✓	✓	✓	✓	✓	✗

Record Visibility

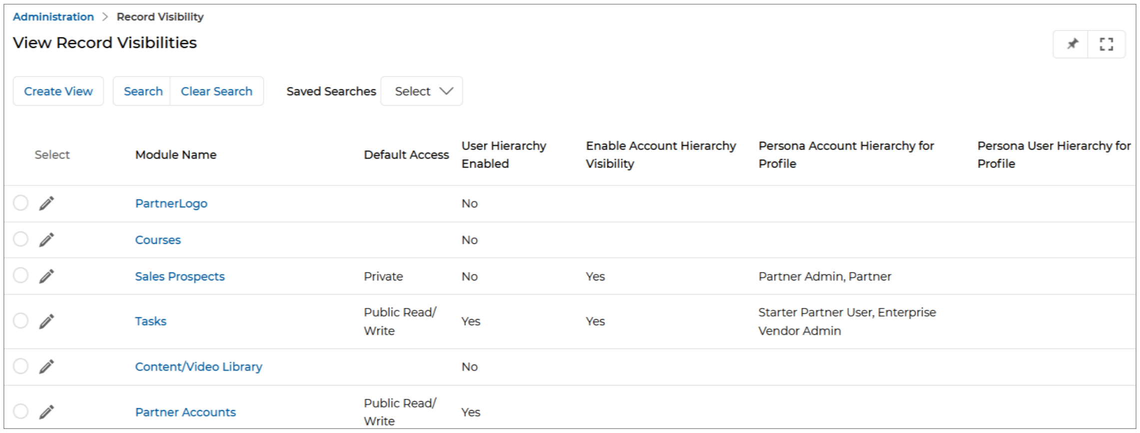
1. Click on **Administration** on the top menu.
2. Click on **Access > Record Visibility** from the left menu bar.



View Record Visibility

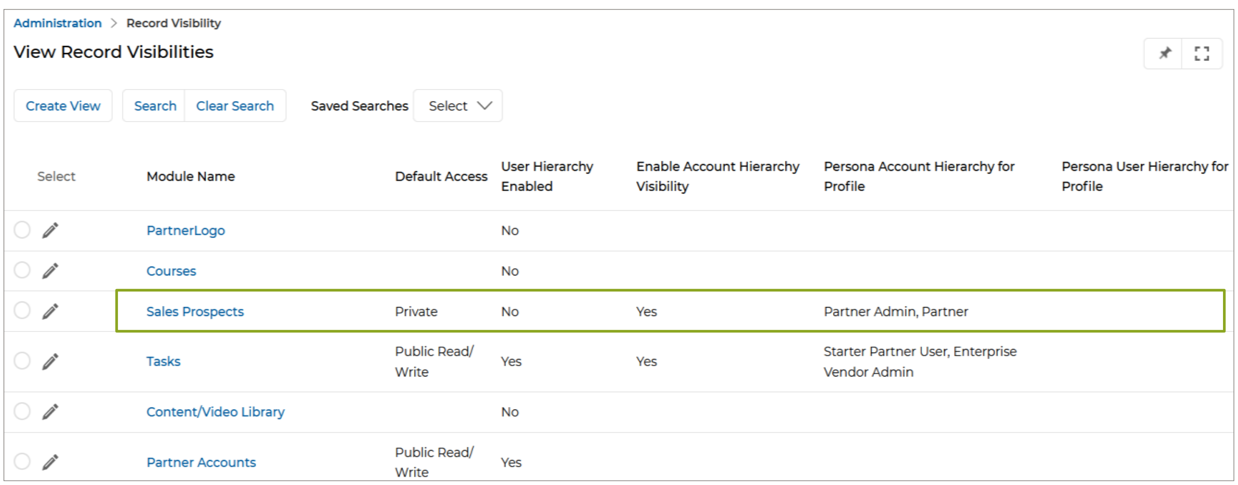
1. The top part of the page provides some actions:
    a. **Create View** – This lets you create your view with a set of columns as needed.
    b. **Search** – Opens a new pop-up window where you can put search criteria to find desired records.
    c. **Clear Search** – Clears the search made.
    d. **Saved Searches** – Shows a list of saved searches in the search dropdown. When selected, two more options are shown:
        i. **Edit** – Provides the option to update the selected search name.
        ii. **Delete** – Deletes the selected search name from the search drop-down.
2. For each record in the grid, if you click on:

a. **Application Name** – Opens the Applications' details page.



View Record Visibility Details

1. Click on the **Name/Title** of any Records Visibility (in this example Sales Prospects) listing to see the details page.



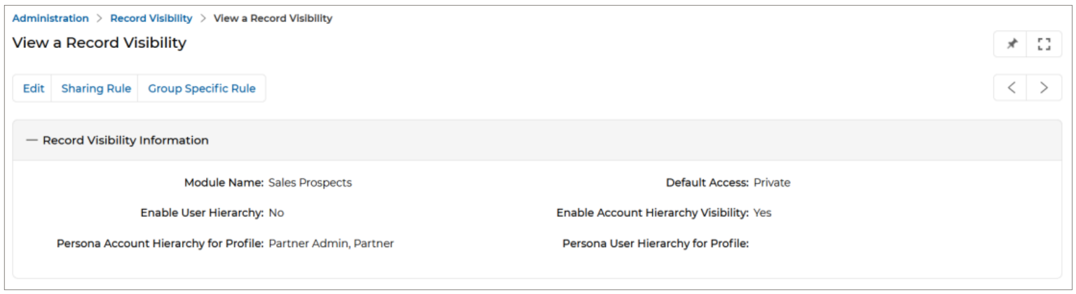
2. Once in the details page, you will see various buttons and sections, such as:
   a. **Buttons:**
      i. **Edit** – Open the page in Edit mode to update field values.
      ii. **Sharing Rule** – Rules shared with groups/users. Please refer to the "Applying Sharing Rule" section for more details.
      iii. **Group Specific Rule** – Click to Manage Group Specific Rules for the specific Application.
   b. **Record Visibility Information:**
      i. **Module Name** – Name of the Application.
      ii. **Default Access** – Type of access given to the rule. The available list of access types is Public Read/Write, Public Read, Controlled by Parent, and Private.

iii. **Enable User Hierarchy** – Accessibility of the rule given to the user or not.

iv. **Enable Account Hierarchy Visibility** - Select 'yes' to Enable Account Hierarchy Visibility for the Sales Prospects.

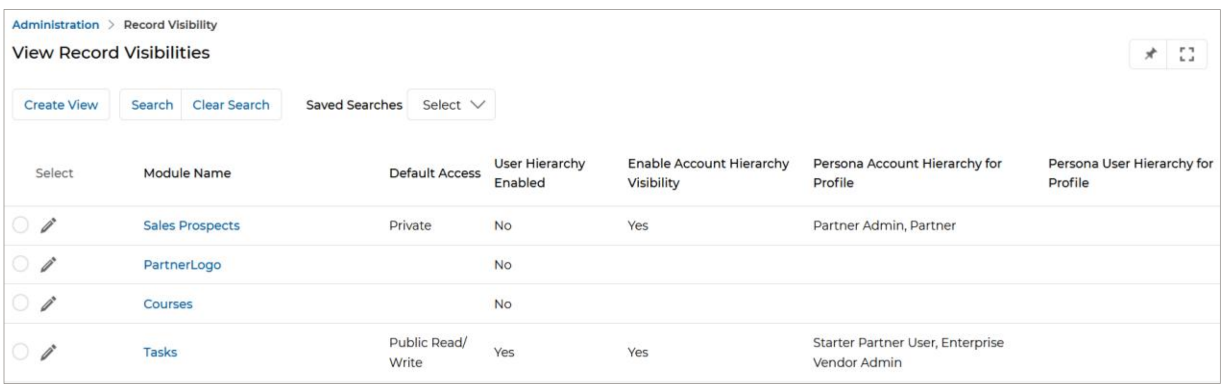
v. **Persona Account Hierarchy for Profile** - Select the Profiles of the Parent Partner Account, which can view the records of the Child Partner Accounts.

vi. Persona User Hierarchy for Profile - Select the Profiles of the Parent Partner Account, which can view the records of the Child Partner Accounts.



Edit Record Visibility Details

1. To **Edit** an existing Record Visibility record (in this example Sales Prospects) – click on the small pencil icon on the View Record Visibility page.



Select	Module Name	Default Access	User Hierarchy Enabled	Enable Account Hierarchy Visibility	Persona Account Hierarchy for Profile	Persona User Hierarchy for Profile
	Sales Prospects	Private	No	Yes	Partner Admin, Partner	
	PartnerLogo		No			
	Courses		No			
	Tasks	Public Read/ Write	Yes	Yes	Starter Partner User, Enterprise Vendor Admin	

2. Once you are in the **Add/Edit a Record Visibility** page, you will see various buttons and sections such as:

   a. Buttons:

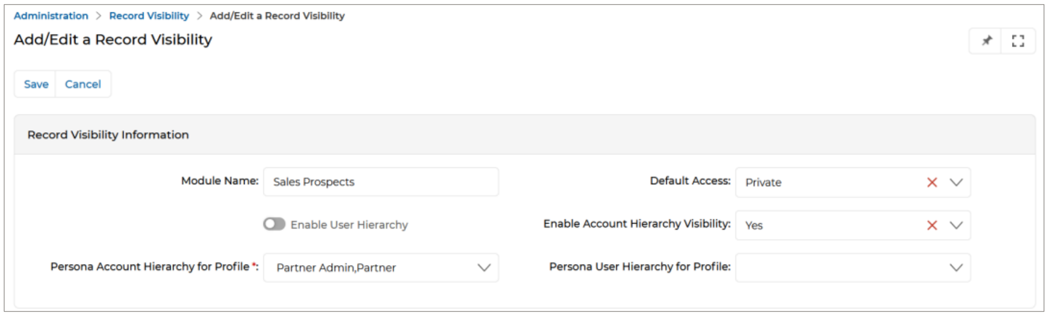
   i. Save – Saves the current page information.

   ii. Cancel – Quits the page without saving the updated information.

   b. Record Visibility Information:

   i. **Module Name** – Name of the Application.

ii. **Default Access** – Type of access given to the rule. The available list of access types is Public Read/Write, Public Read, Controlled by Parent, and Private.



iii. **Enable User Hierarchy** – Accessibility of the rule given to the user or not.

iv. **Enable Account Hierarchy Visibility** - Select 'yes' to Enable Account Hierarchy Visibility for the Sales Prospects.

v. **Persona Account Hierarchy for Profile** - Select the Profiles of the Parent Partner Account, which can view the records of the Child Partner Accounts.

vi. **Persona User Hierarchy for Profile** - Select the Profiles of the Parent Partner Account, which can view the records of the Child Partner Accounts.

3. Once you are done, click **Save**.

Enable Account Level Visibility for an Entity

It is very convenient to set up and configure visibility for all records of a specific UPM Application using Workflow. Enable Account Level Visibility feature updated at Workflow offers a unique solution – once enabled for a UPM Application by the Admin, all Users/Partners mapped to the same Account will have visibility to all records of that Application, irrespective of the creator/adder of that record for that Application.

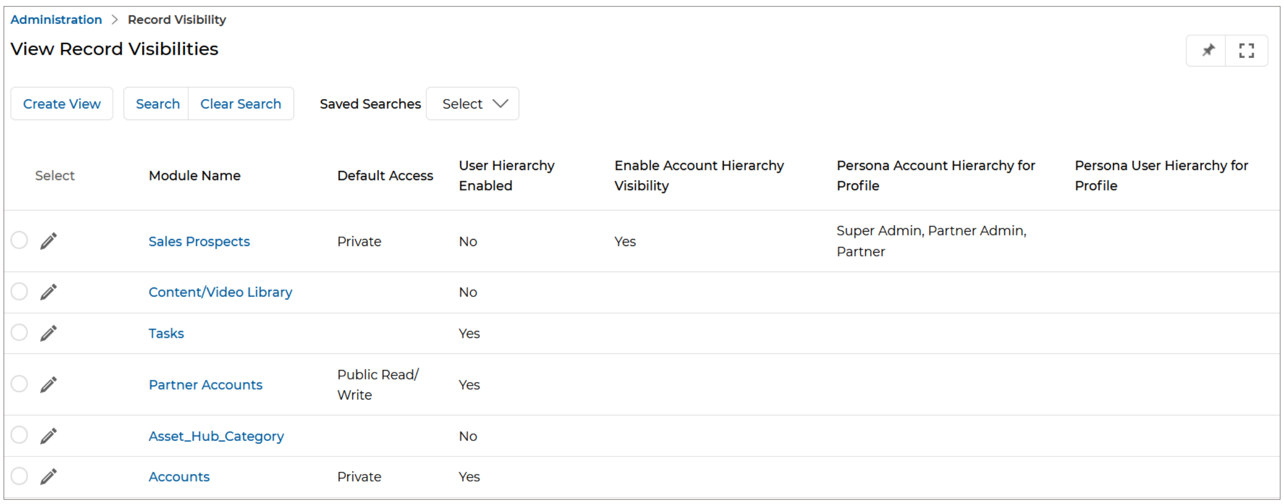
The Admin opens the Application in Development Mode at Workflow and accesses the Details section. If the Admin wants to grant permission to let all the Partners/Users mapped to the same Account and residing at the same access level - view records of that specific Entity/Application – irrespective of the Creator/Record Adder, he needs to enable the toggle key - Enable Account Level Visibility, respective to the Object/Entity ex.: Prospect. Enabling the toggle key will grant permission to all Users/Partners mapped to the specific Account to view all records – irrespective of the Creation Owner; and click Save. Disabling the toggle key will only allow the Admin and the Creator of the Record – Partner/User to view the record.

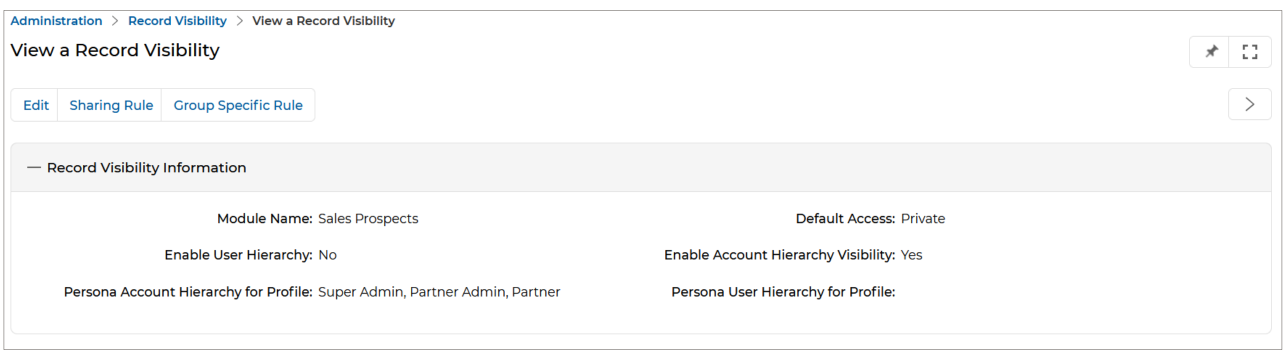
Therefore, Prospect records created by any Partner User/Contact mapped to the same Account will be visible to all Partner Users/Contacts mapped to that Account.

Record Visibility settings are enabled by default for every new application, allowing admins to immediately configure Visibility Setting Rules, such as hierarchy or group-specific access rules.

Whenever a new application is created, it will appear in the Record Visibility application, allowing admins to control settings such as:

- Default Access
- User Hierarchy settings
- Group-specific rules for record access

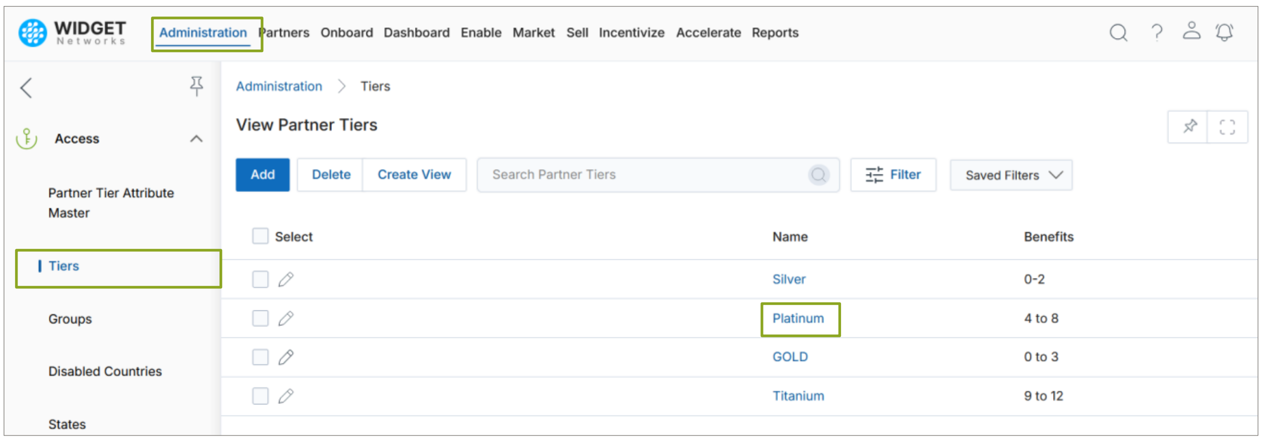




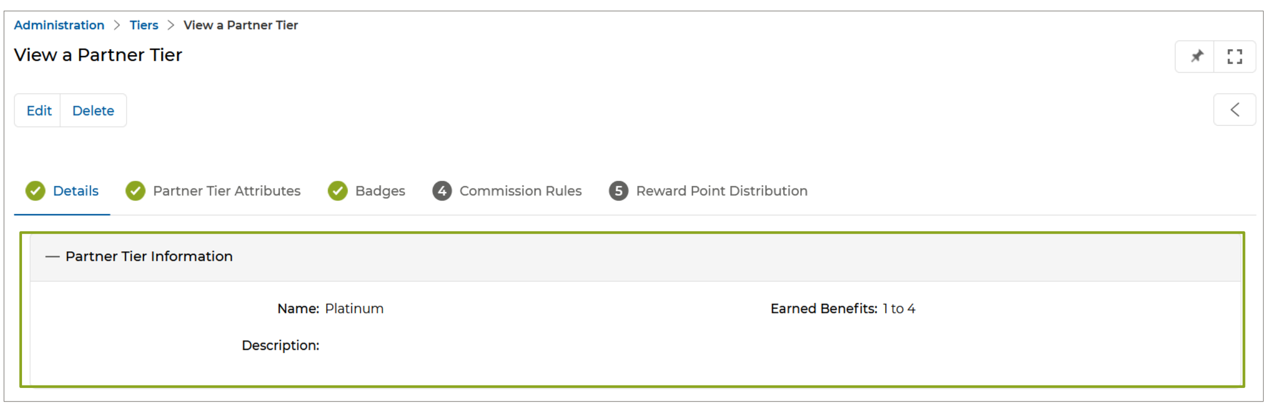
Automatic Partner Tier Assignment Based on Partner Score

The Automatic Partner Tier Assignment feature streamlines partner management by assigning a partner tier to the Partner Account based on the partner's score. This functionality is configurable within the Partner Tier Attributes settings via Access Management, where administrators can define rules and conditions for tier assignments.

- We must navigate **Administration > Access > Tiers** to reach the **View Partner Tiers** page, which lists all the Partner Tiers**.**

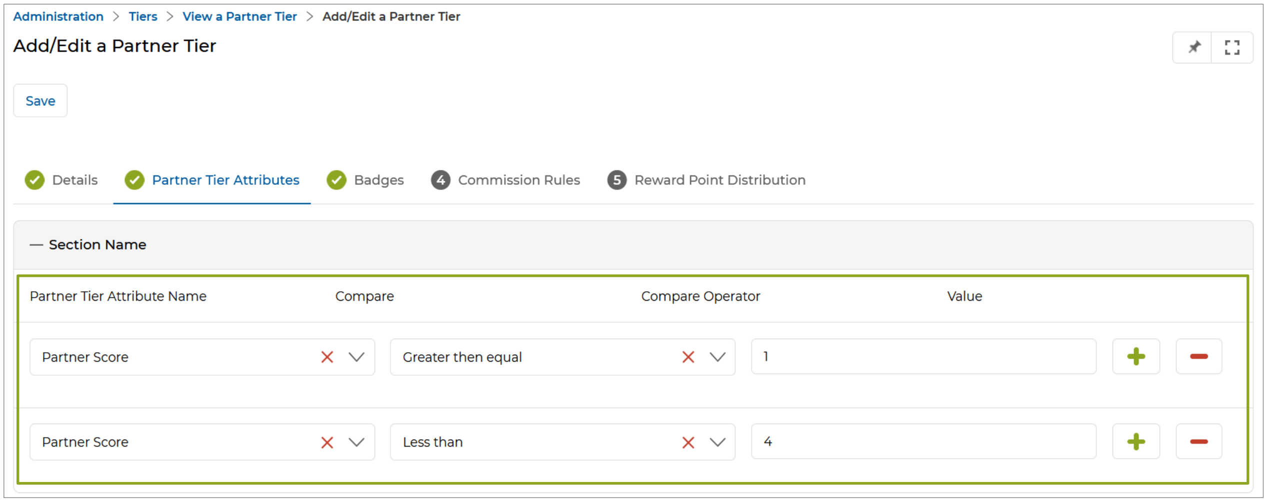


- To define Partner Tier Attributes for the Platinum Partner Tier - we go to the details page of the Partner Tier - Platinum.



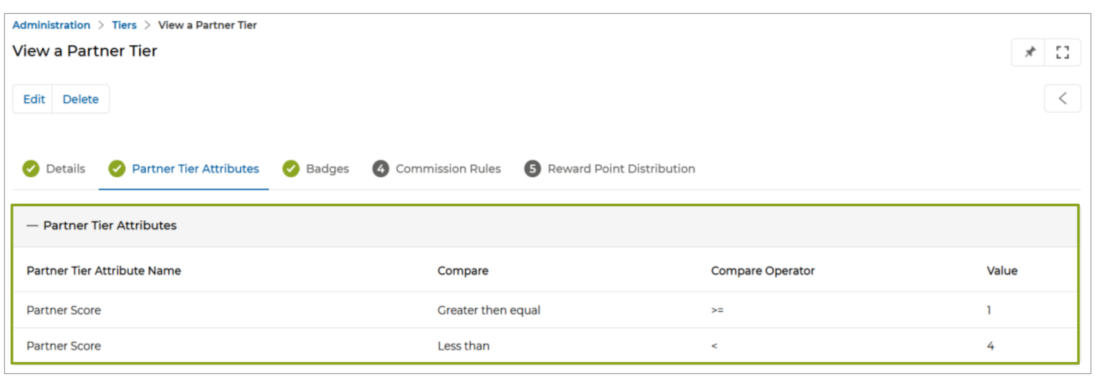
- In the Partner Tier Attributes tab, we need to configure the values for the auto-assignment of the Partner Tier. In our example case, we configure Partner Score as the attribute for auto-assignment of the Platinum Partner Tier, so that when the Partner Score of a Partner Account is between 1 and less than 4, the Account will be automatically assigned the Platinum Partner Tier.

- The following Partner Tier Attributes are defined as –



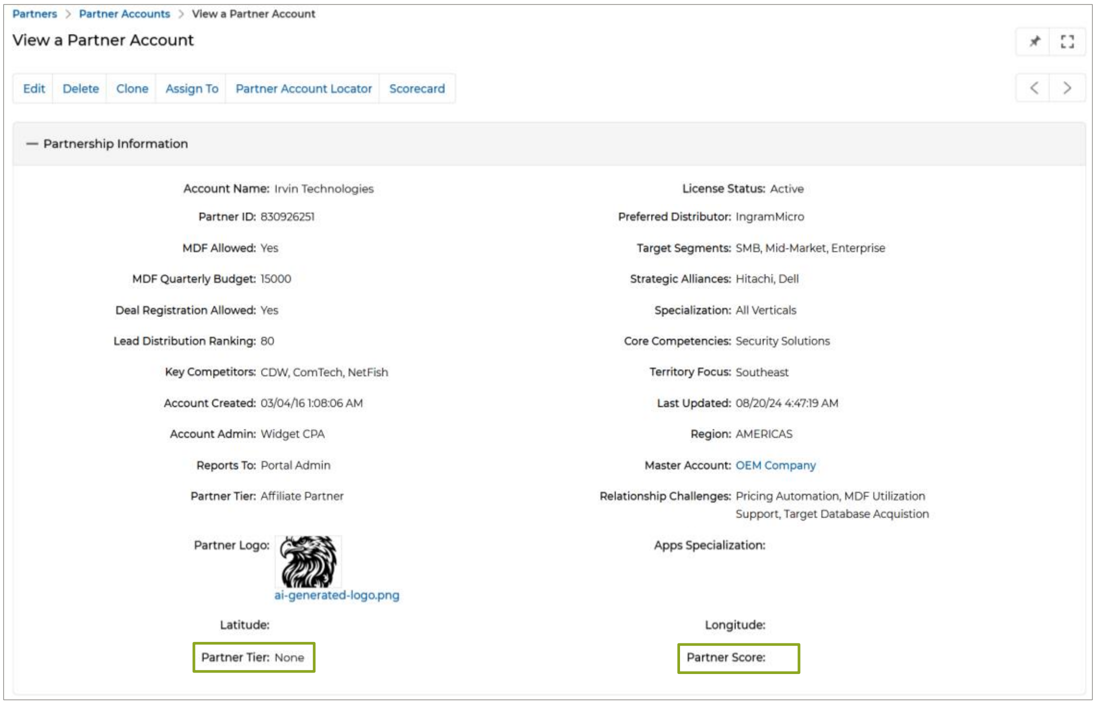
  - **Partner Tier Attribute Name**—This refers to the specific attribute of a partner that is being evaluated. In the example given, "Partner Score" is the attribute being assessed.
  - **Compare** —This indicates the action of evaluating or assessing the Partner Tier Attribute against a certain criterion or value.
  - **Compare Operator –** This is the logical operator used to compare the Partner Tier Attribute with a specified value.
  - **Value** – This is the value against which the Partner Tier Attribute is compared using the specified operator.

  We defined two attributes – one whose Partner Score value is >= 1 AND the other has a Partner Score value of < 4. When a Partner Account's score falls within this range, then Platinum Partner Tier will be auto-assigned to the Account.

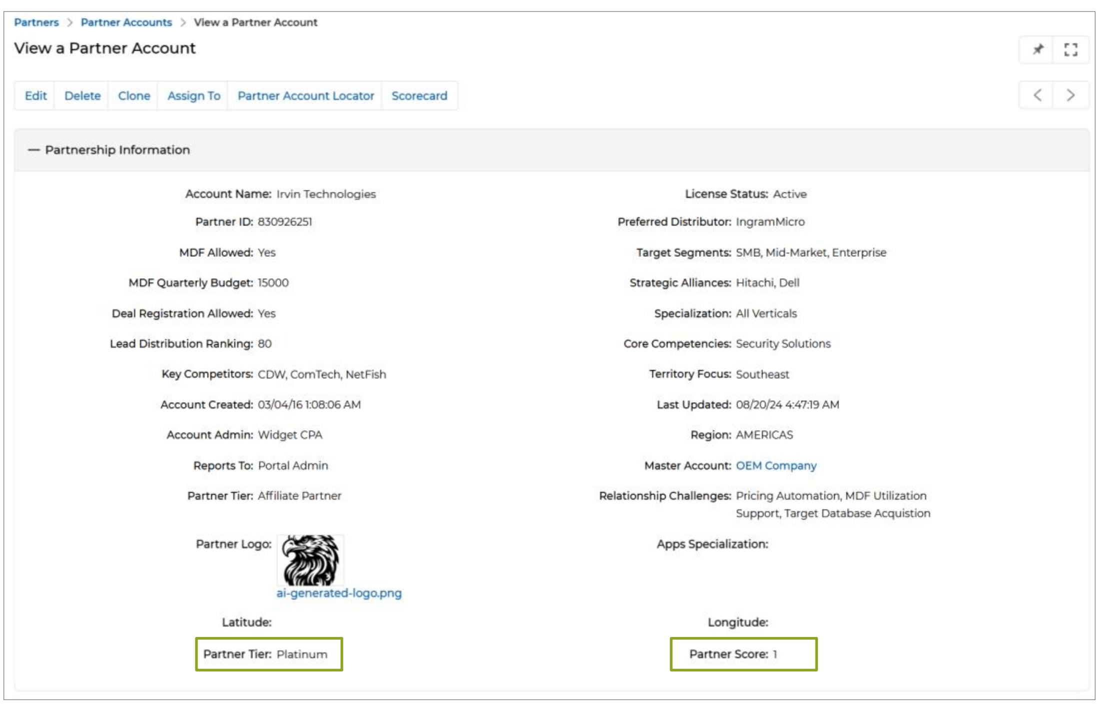


- We navigate to **Partners > Partners > Partner Accounts** to reach the **View Partner Accounts** page, listing all Partner Accounts.

- We go to the **Add/Edit a Partner Account** page of a Partner Account and view the **Partner Score** and **Partner Tier,** which are not yet configured.



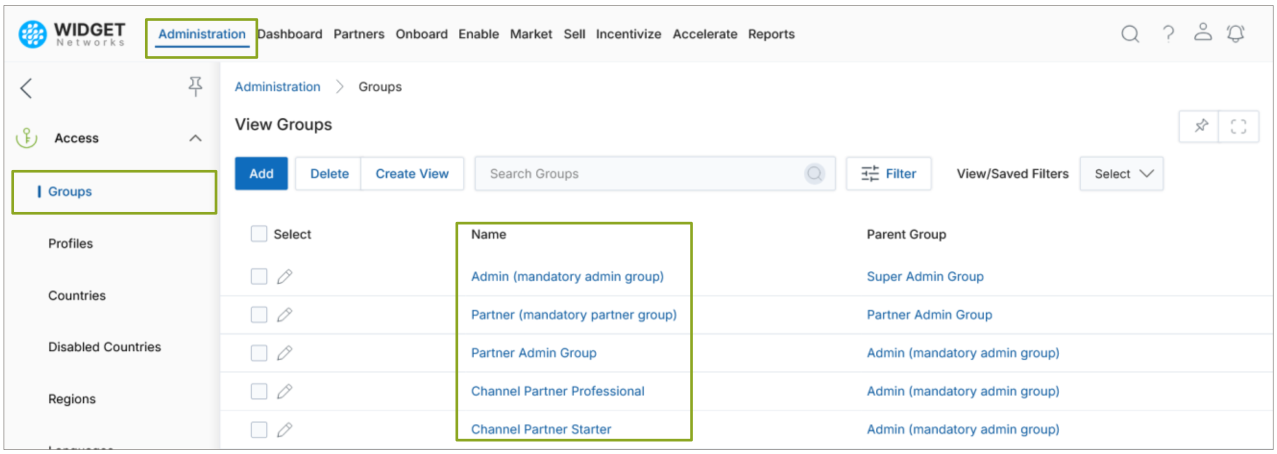
- Now, if we update the Partner Score Field with ‘1’ in the Partner Score field and click Save, we will find the Partner Tier automatically updated to the “Platinum Tier”.



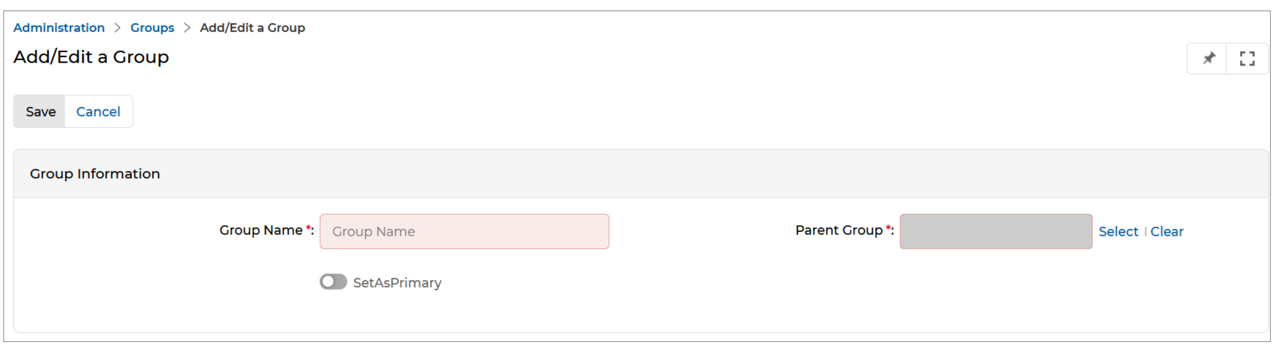
Auto Group Assignment based on Attributes

This feature offers significant benefits by automating group assignments based on Group Attributes such as ‘Country’ and ‘Partner Tier’, reducing manual effort and ensuring accuracy.

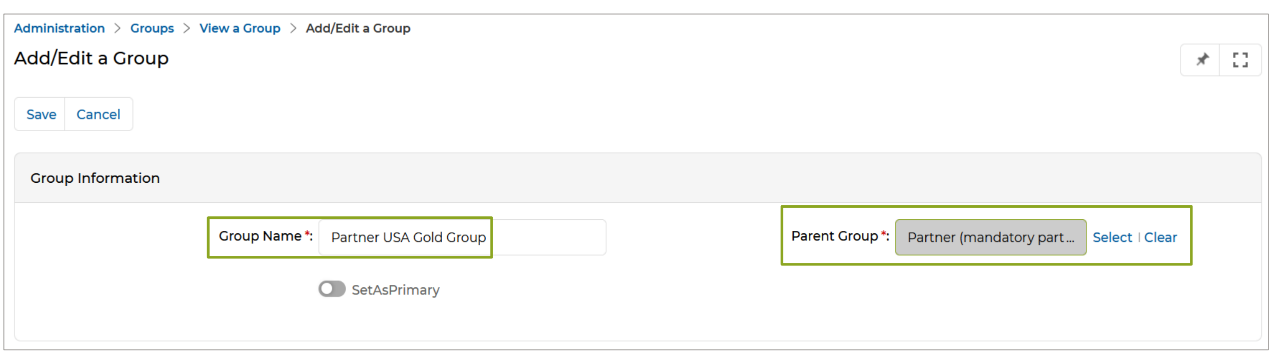
- We must navigate **Administration > Access > Groups** to reach the **View Groups** page where all the Groups are listed.



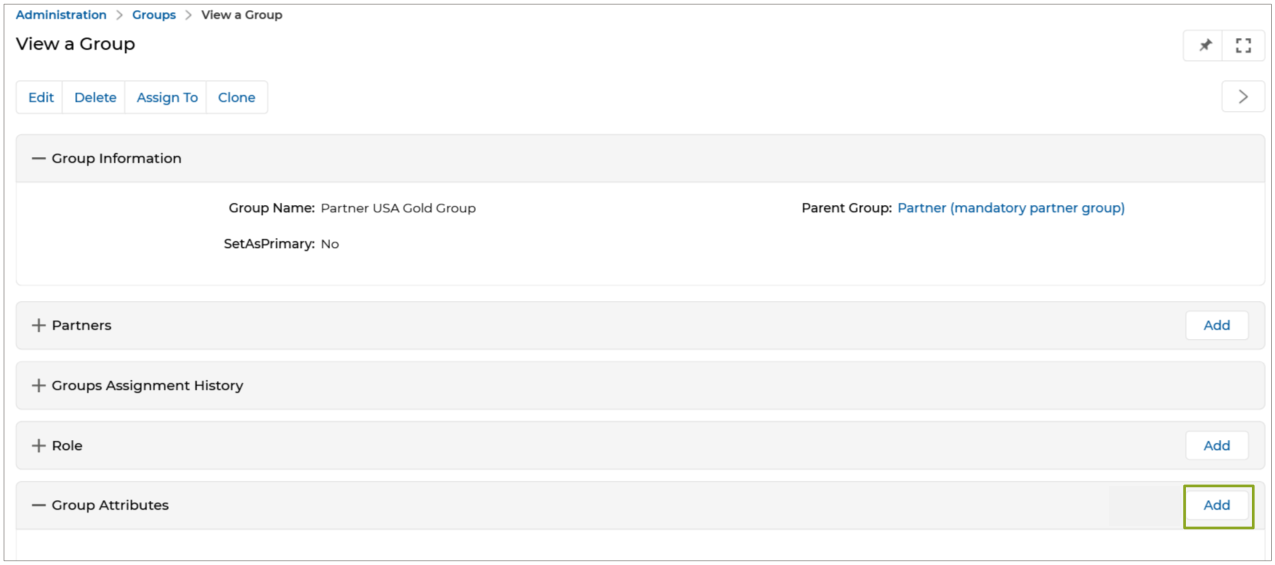
- We click the Add button and reach the Add/Edit Group page, where we can create a new Group.



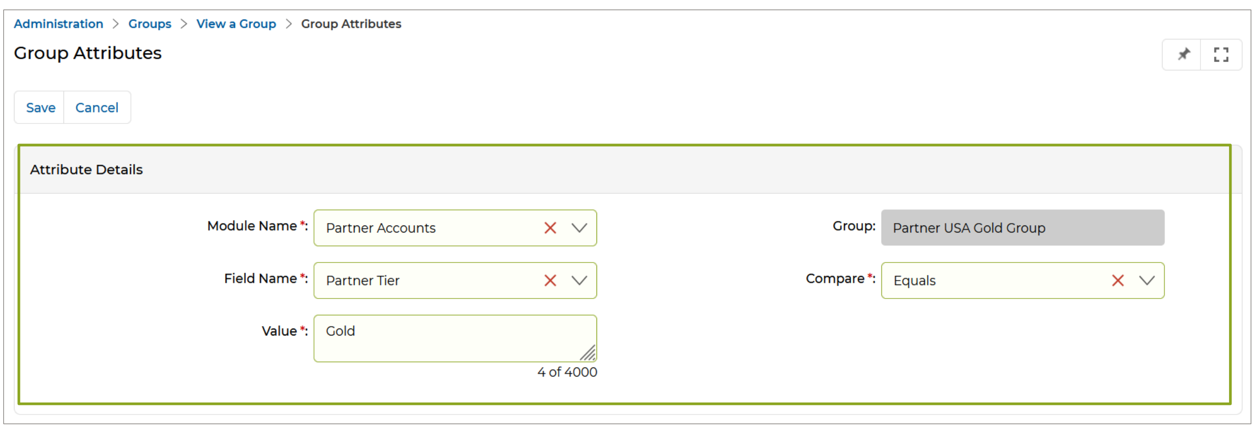
- We provide the Group Name (Partner USA Gold Group), select Parent Group, and click Save.



- We click the Add button associated with Group Attributes to configure Group Attributes, which takes us to the Group Attributes page. The ‘Partner USA Gold Group’ will be auto-assigned to the User if the User's Partner Account is Gold Partner Tier AND the User’s Country is USA.



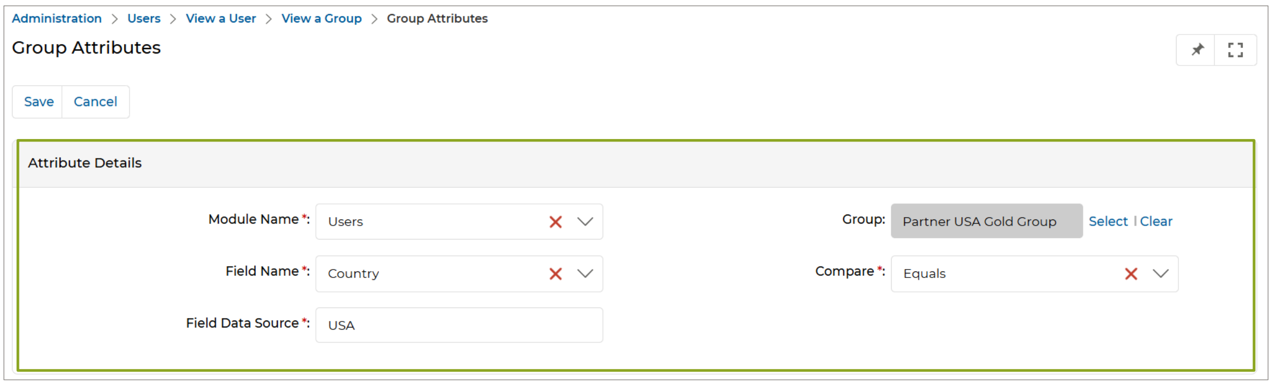
- We define the value of a Group Attribute by providing details in the fields of the Attribute Details section:



  - **Module Name**: This specifies that in this example, the attribute applies to the **Partner Accounts** module, meaning the condition is evaluated for Partner Account records.
  - **Field Name:** This attribute is used to filter Partner Accounts based on their **Partner Tier**.
  - **Value:** The system will check if the **Partner Tier** value is **Gold** and apply the attribute condition accordingly.
  - **Group:** Any Partner Account that meets the condition (**Partner Tier = Gold**) will be automatically assigned to the **Partner USA Gold Group.**

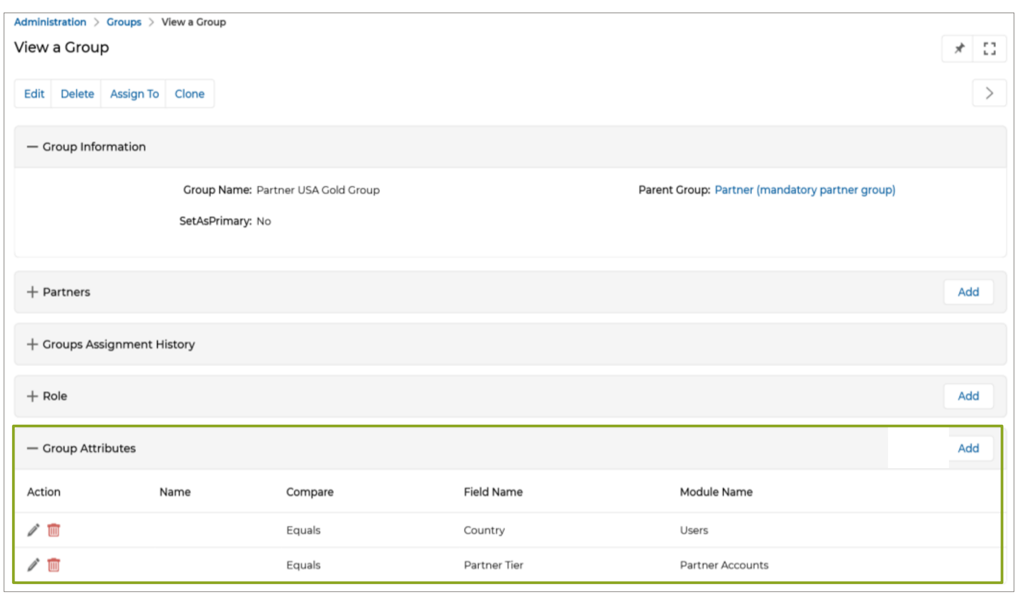
- Compare: The system will assign the Partner Tier based on the selected comparison operator. In this case, we use **Equals**, meaning only Partner Accounts where the **Partner Tier** exactly matches the specified value will meet the criteria. Other available comparison operators include **Not Equals, Like, In, and Contains**.

- Similarly, we define the value of another Group Attribute in the Attribute Details section by providing details in the following fields:

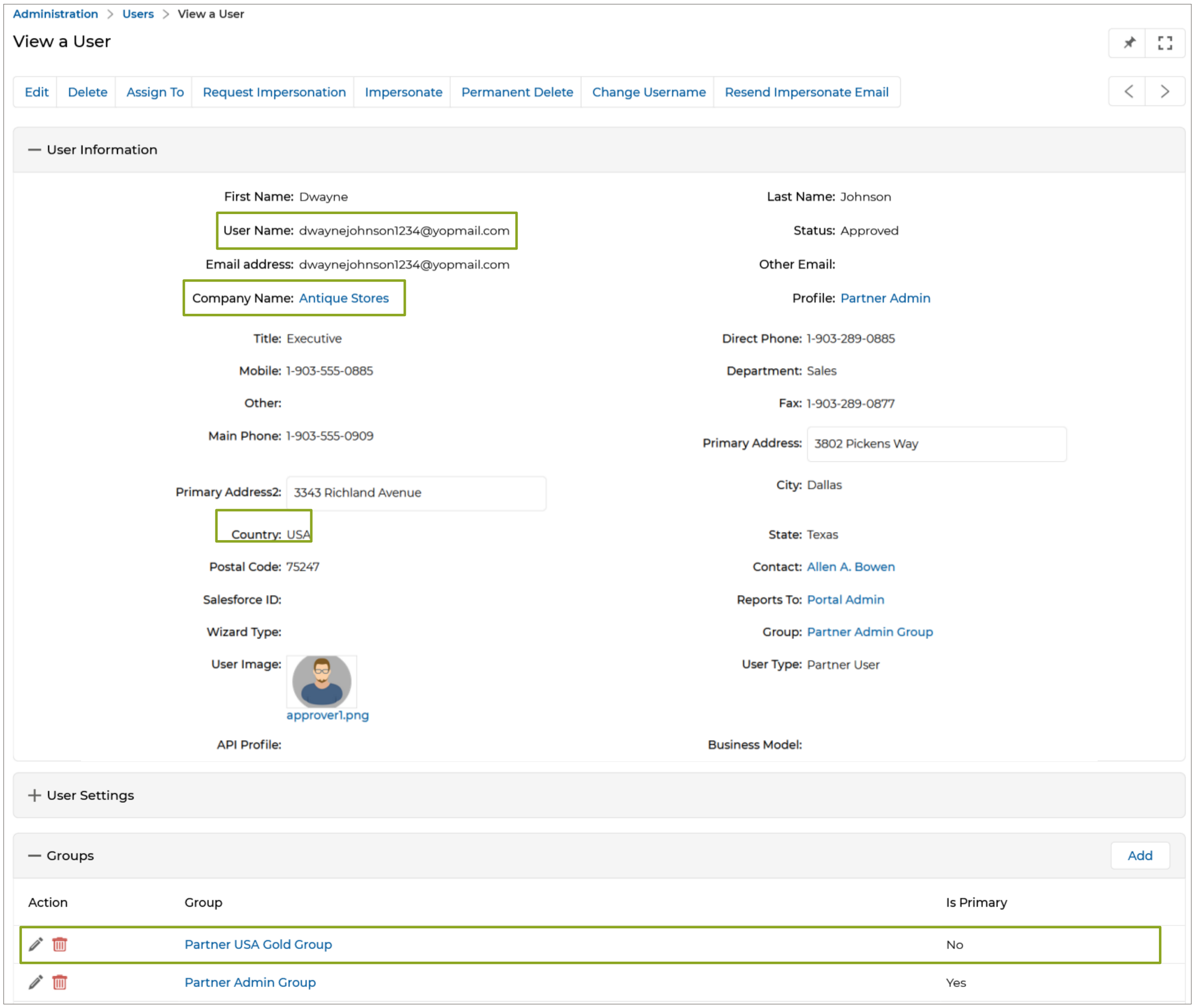


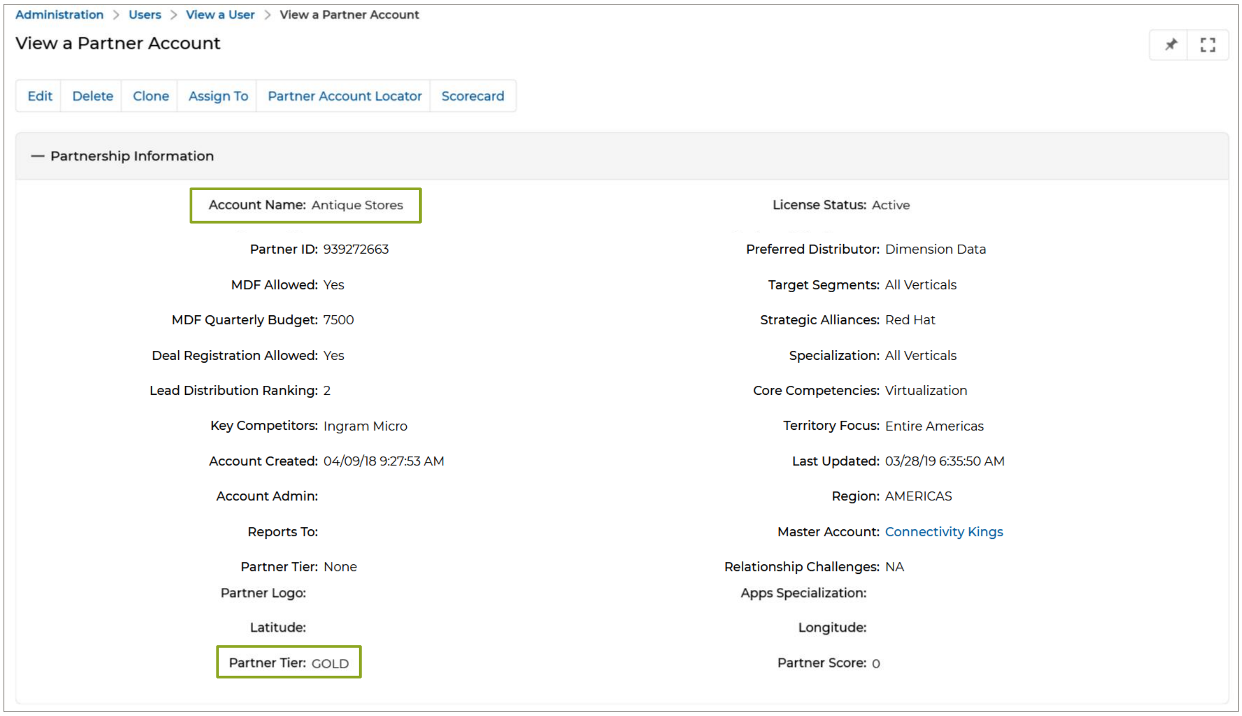
  - **Module Name**: This specifies that in this example the attribute applies to the **Users** module, meaning the condition is evaluated for user records.
  - **Field Name:** This attribute is used to **filter users** based on their country.
  - **Field Data Source:** The system will check if the user's **Country** value matches **"USA"**.
  - **Group:** Any user that meets the condition (**Country = USA**) will be automatically assigned to the **Partner USA Gold Group**.
  - **Compare:** The system will assign users to the group only if their **Country** exactly matches "USA".

- The Group Attributes with its values will be visible on the Group Attributes related list on the View a Group page.



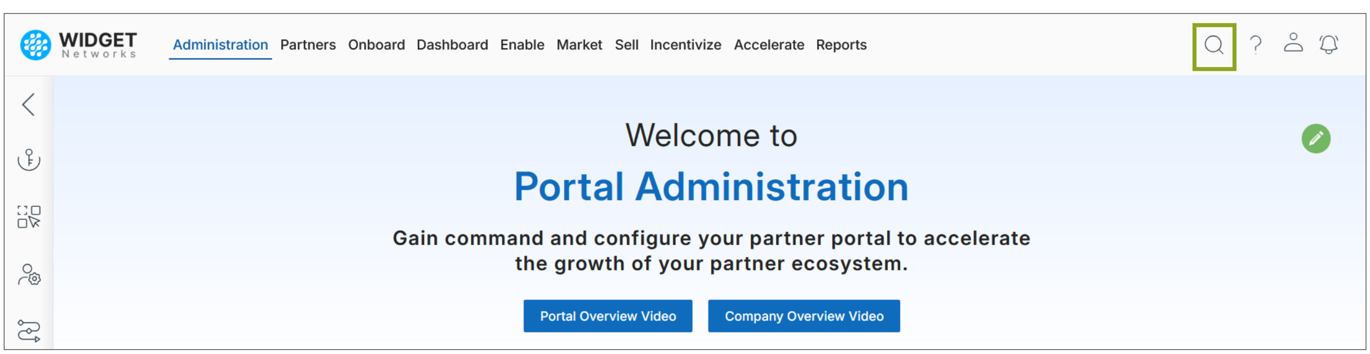
- We navigate to the details page of a User whose country is USA and the Partner Tier of their Partner Account is Gold and the 'Partner USA Gold Group' has been auto-assigned to the User.



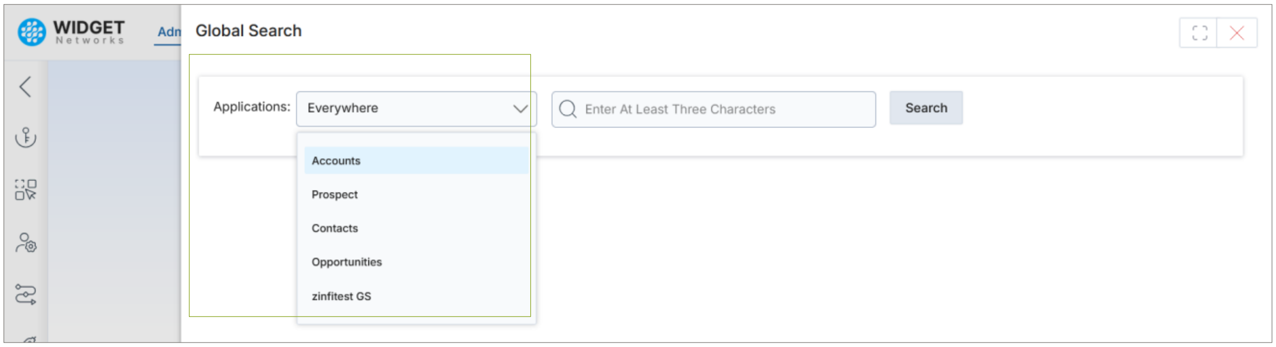


Global Search of Assigned Applications

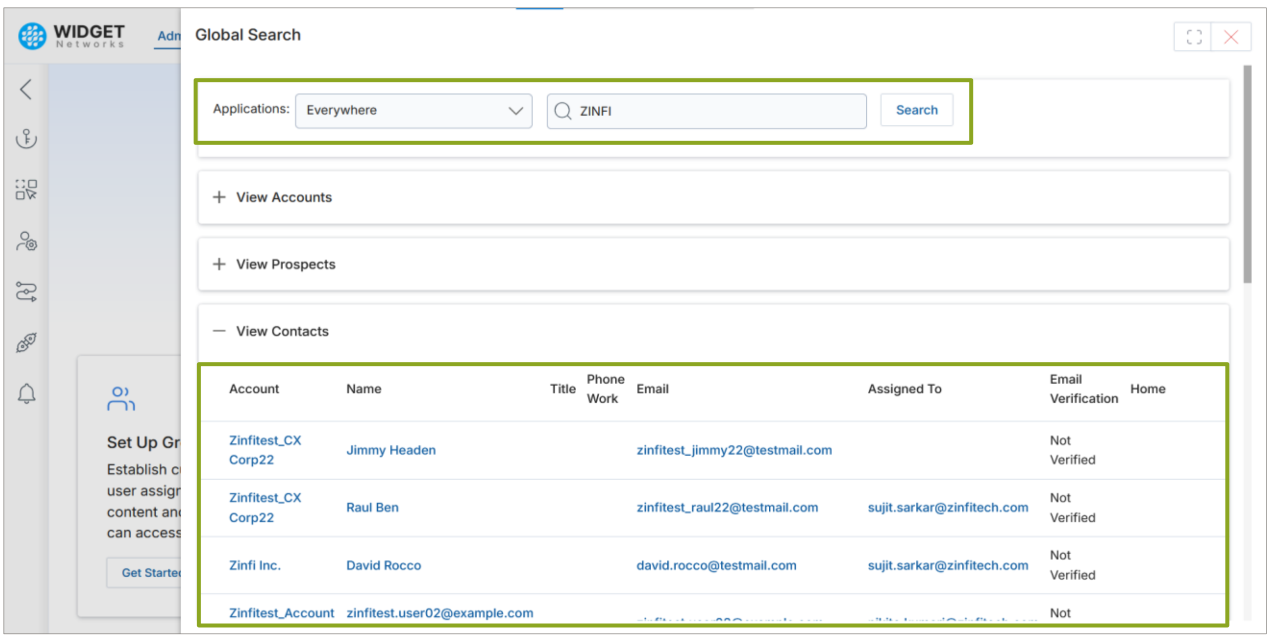
Once a User logs into the UPM portal, he can search for records associated with Applications assigned to him by using the UPM Global Search Engine. Global Search allows the User to search the entire records set associated with all UPM, eliminating the necessity to view the Application and search for the specific record(s). This feature is useful for UPM Portals with a large amount of data or content, as it helps Admin and Partner Users quickly locate the information without the need to navigate through menus or browse through different Applications manually to extract the specific Record.



- Clicking the Global Search icon will open **the Global Search** Page.
- Clicking the first drop-down menu will show the list of all the Applications associated with the Profile of the User. The User can select All or specific Application(s) from the list to search the desired Record.



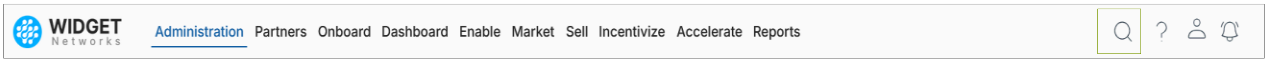
- In the below example, when the User chooses the Prospect Application from the dropdown menu and enters **'ZINFI'** as the search criterion in the second field, clicking the Search button will extract and display any Prospect records associated with the name **'ZINFI'** as shown in the image below.



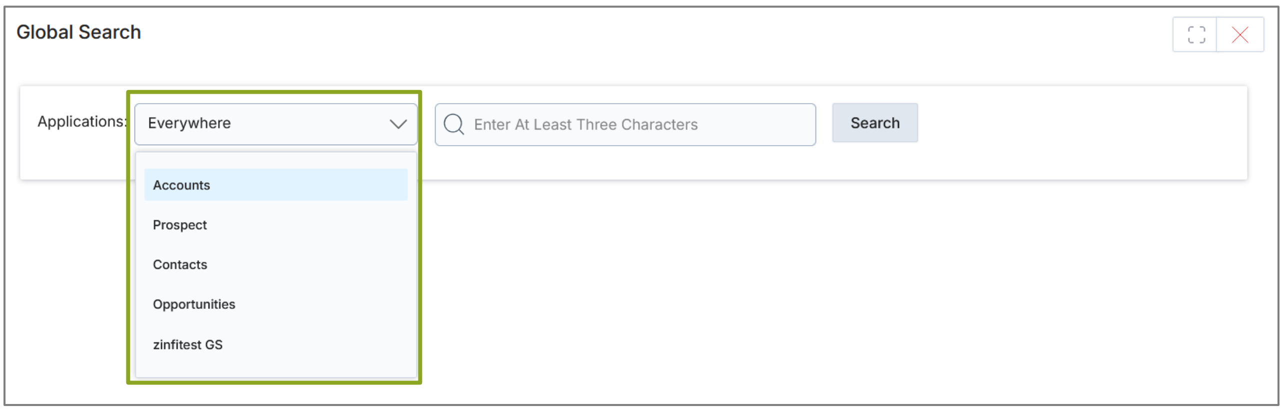
Global Search Enhancement

The Global Search Enhancement feature aims to significantly upgrade the existing search capabilities within the UPM system by introducing advanced functionalities that make searching more efficient and user-friendly. This enhancement will provide users with improved accuracy in search results, incorporating phonetic search options to account for variations in spelling and pronunciation and auto-completion features to suggest and complete search queries as users type. By leveraging these improvements, the Global Search Enhancement will enable users to find relevant information more quickly and accurately, streamlining their workflow and enhancing their overall experience within the UPM system.

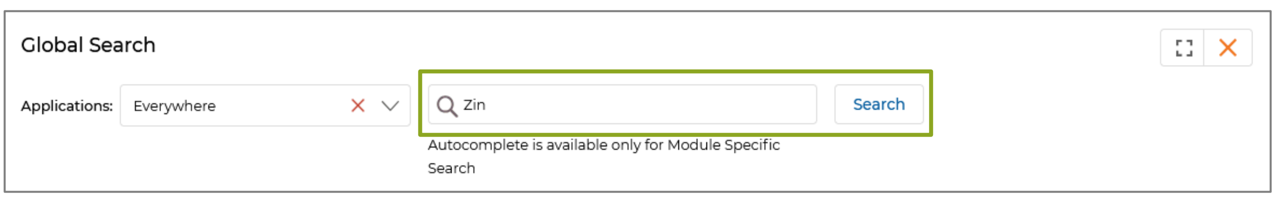
- Clicking the Global Search icon will open the **Search** page.



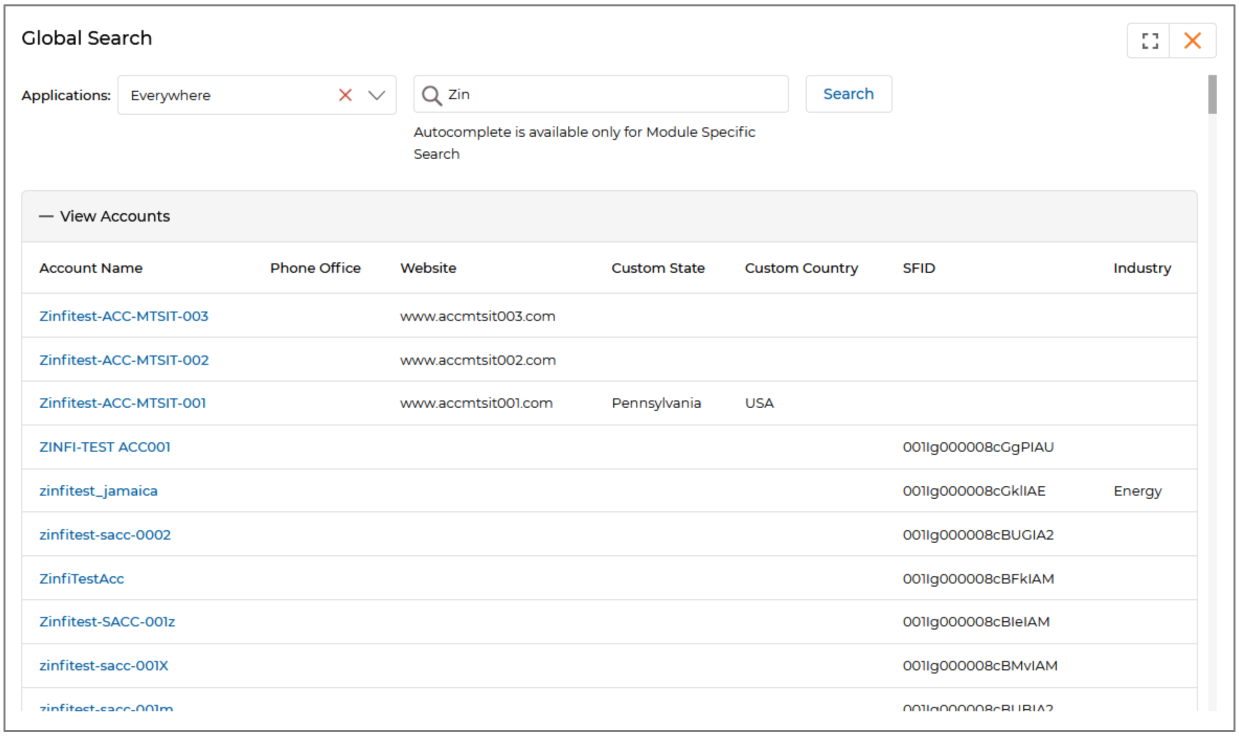
- Clicking the drop-down menu associated with Applications will show the list of all applications related to the User's Profile.
- The default value in the dropdown list is Everywhere. The User must select Everywhere or a specific Application(s) from the list to search for any value. Selecting Everywhere enables the User to search values across all the applications listed in the dropdown while selecting a specific application enables the user to search values associated with the selected application.



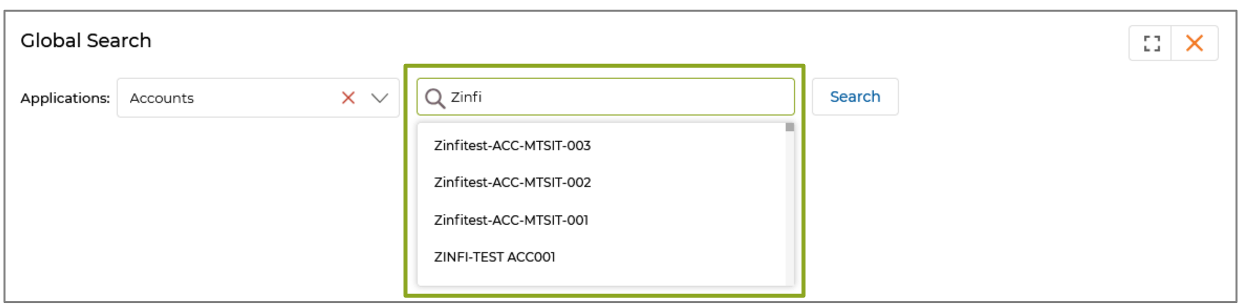
- At least three letters in the search field must be keyed to activate the **Search** button.



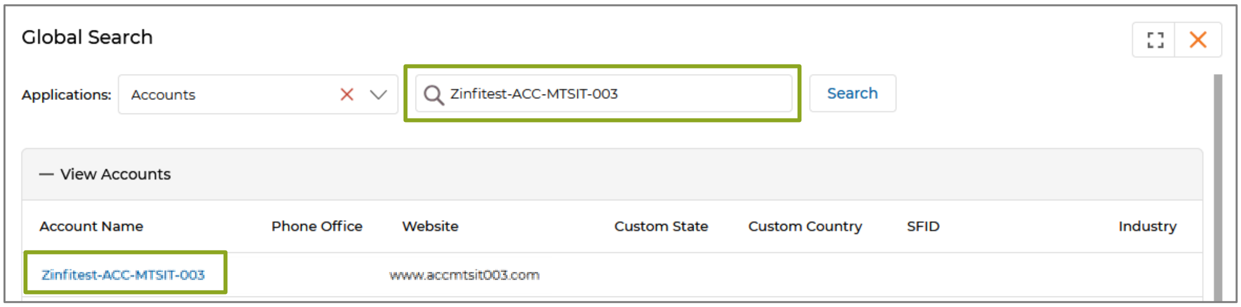
- In the above example, when the User chooses 'Everywhere' from the dropdown menu and enters **'Zin'** as the search criterion in the second field, clicking the Search button will extract and display any records associated with the name **'Zin'** across all applications as shown in the image below.



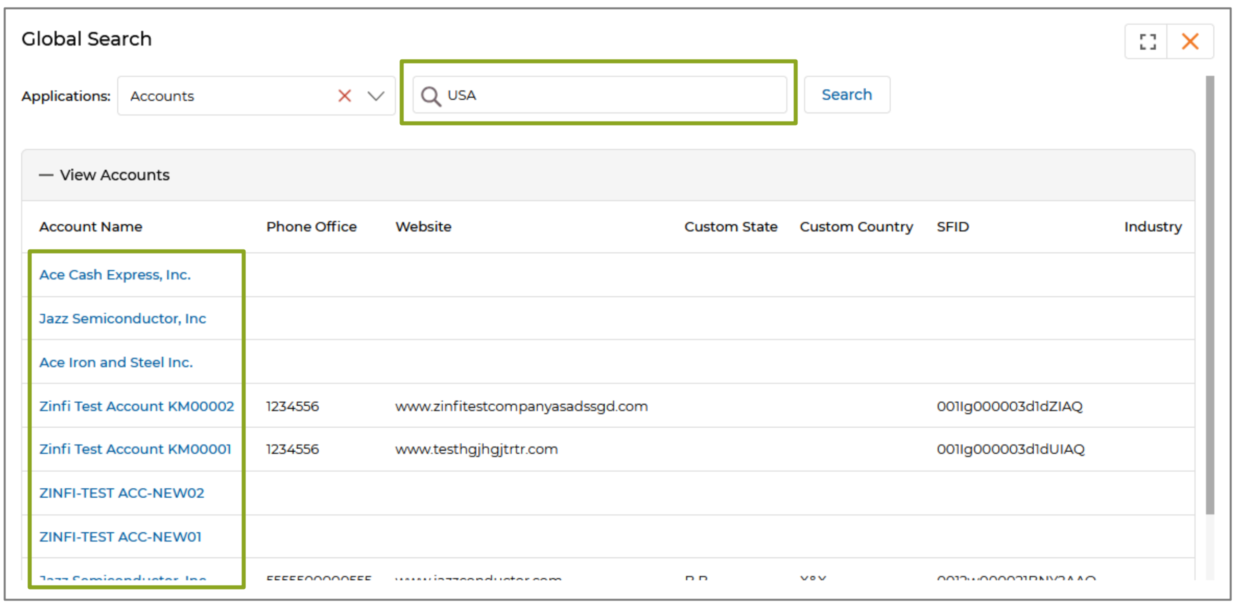
- Individual applications can also be selected, and records related to selected applications can be extracted.
- When typing the search criterion after selecting the individual application, the search field will provide a list of possible suggestions for searchable criteria that the user can utilize.



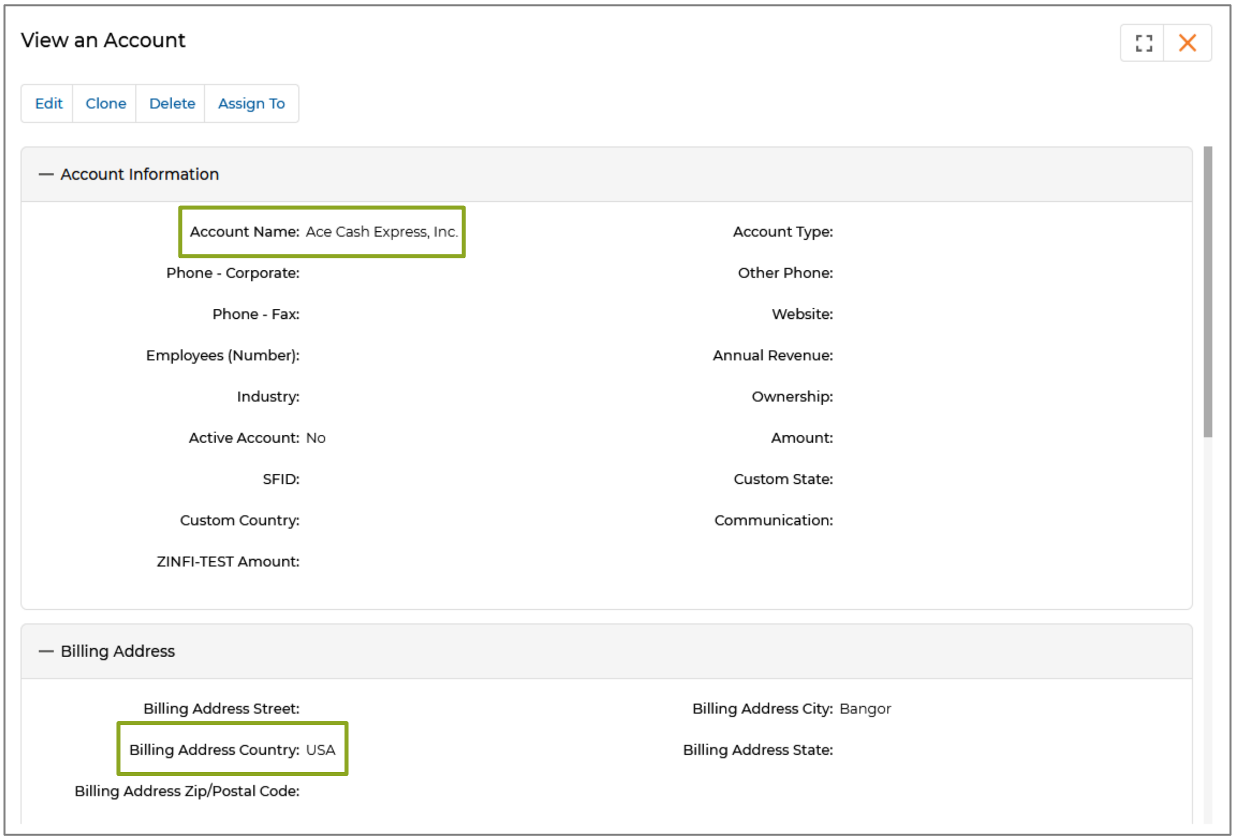
- Once a suggested search criterion is utilized, the searched record with a parameterized value matching the searched text will be shortlisted.



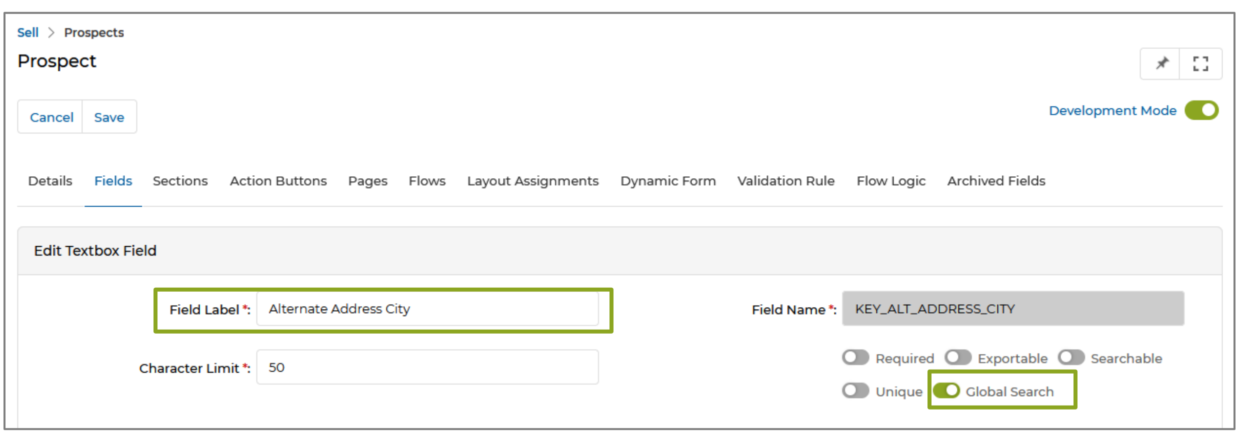
- Fuzzy search capabilities have also been integrated into Global Search. This feature allows you to search records by any parameter values of the records. In the image below, the search text has been given as "**USA**" in the Search field. Once the Search button is hit, the list of records with parameterized values matching the searched text will be shortlisted.



- Using the abovementioned criteria, the user can search records that contain 'USA'. If the user goes to the details page of any record, he will find 'USA'.



- Global Search functionality of field related to any application listed in Global Search can be enabled/disabled from Workflow.
- The user needs to go to the Workflow and enable or disable Global Search using the associated toggle key.
- Enabling toggle key will make the field available for Global Search while disabling the toggle key will remove the field from Global Search.



Field-Level Management

To control data access precisely across UPM, we can allow users to view specific fields in a specific object, but then restrict the individual records they're allowed to see. Record-level management, as discussed earlier, determines which individual records users can view and edit in each object they have access to in their profile. The permissions on a record are always evaluated according to a combination of object-level, field-level, and record-level permissions.

With UPM's Workflow, field-level management allows you to restrict users' access to view and edit specific fields in a specific record of a specific Application. The UPM instance deployed at your organization would be a repository of data integrated with field-level management, restricting field access to everyone.

The fields that users see on detail and edit pages are a combination of page layouts and record-level management settings. Workflow lets us:

- Create page layouts to organize the fields on list, detail, and edit pages.
- Hide a field by omitting it from the layout.

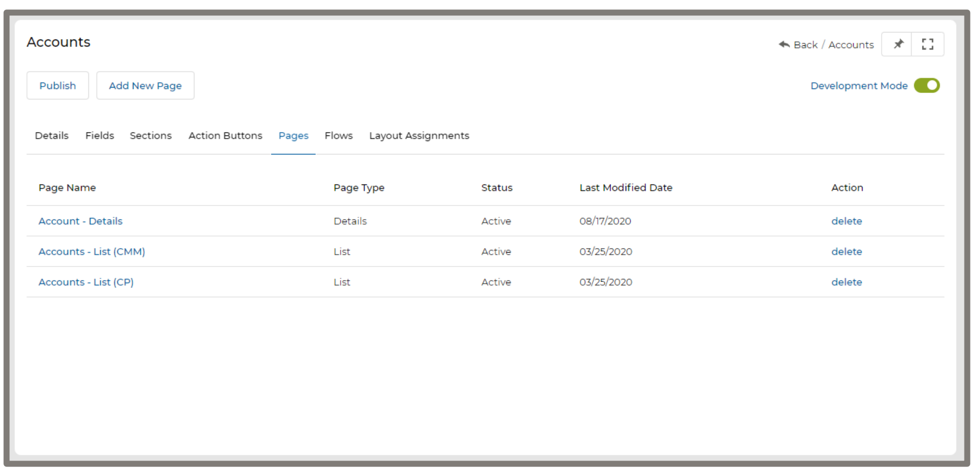
Configuring Page Layouts

Workflow Pages lets you create your page which constitutes the actions button, sections, and fields that have already been created.

Pages are generally of two types:

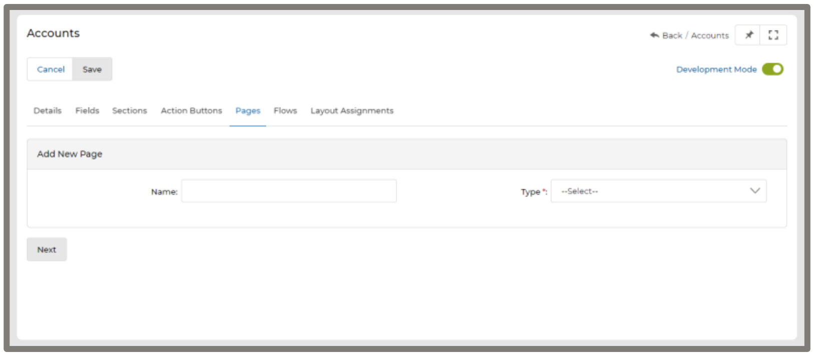
- **List pages** – these are the pages that show the listings of records or content (the View or Library pages)
- **Detail pages** – these are pages that hold the details of records or content (the clickthrough into details)

Existing pages can be viewed and edited as per the figure below:



Pages can also be cloned to be used by other Applications.

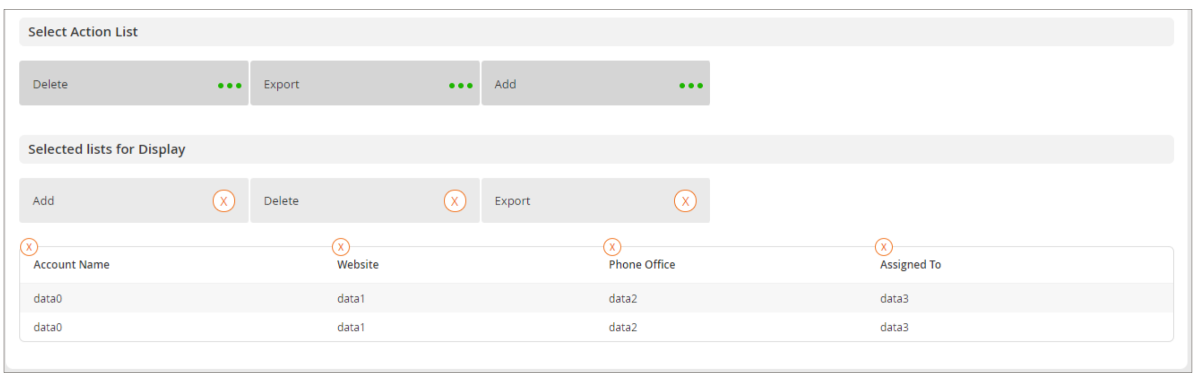
Add a NEW List Page



1. **Name:** What is the name of this page?
2. **Type:** Select *List* as the type for this page.

The following operations are carried out next:

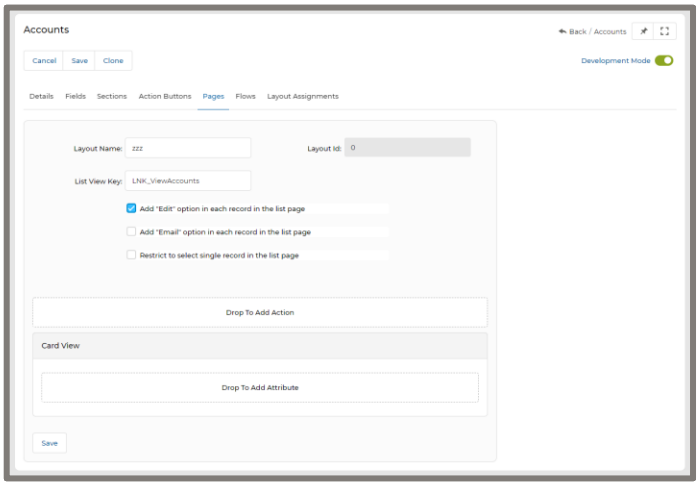
1. Select fields to display the set attribute list.
2. The edit option for each record on the list page can be enabled or disabled.
3. The selection of a single record can be restricted by enabling the restrict option.
4. The actions list can be generally set and selected to be displayed for the list page so that records can be added, deleted, or exported as per the figure below:



Add a NEW Details Page

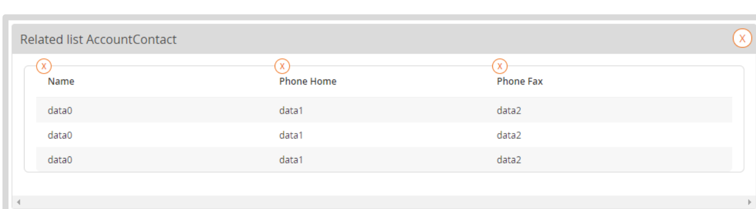
The following operations are possible in creating a details page:

1. Add sections.
    a. Add fields.

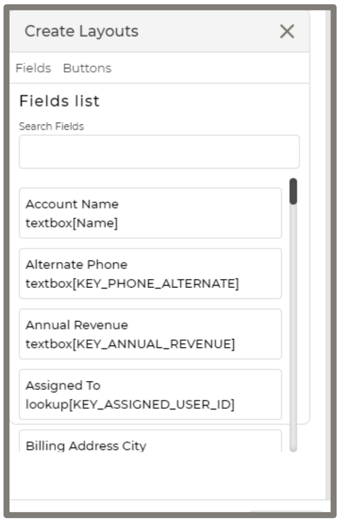


i. Fields can be marked as read-only on the Add and Edit page.

2. Add action buttons.
3. Add a related list.
    a. Select fields to display in the related list.
    b. Add actions of the related list
4. Add, Edit, and Delete are the default options.
5. Can be configured to add only one record in the related list.
6. The Add, Edit, and Delete options can be hidden here.
7. The Add/ Edit page can be set to open as a pop-up rather than as a new tab.
8. The records in the related list become locked as soon as the parent record is approved, but you can provide an Add option in the approved record.



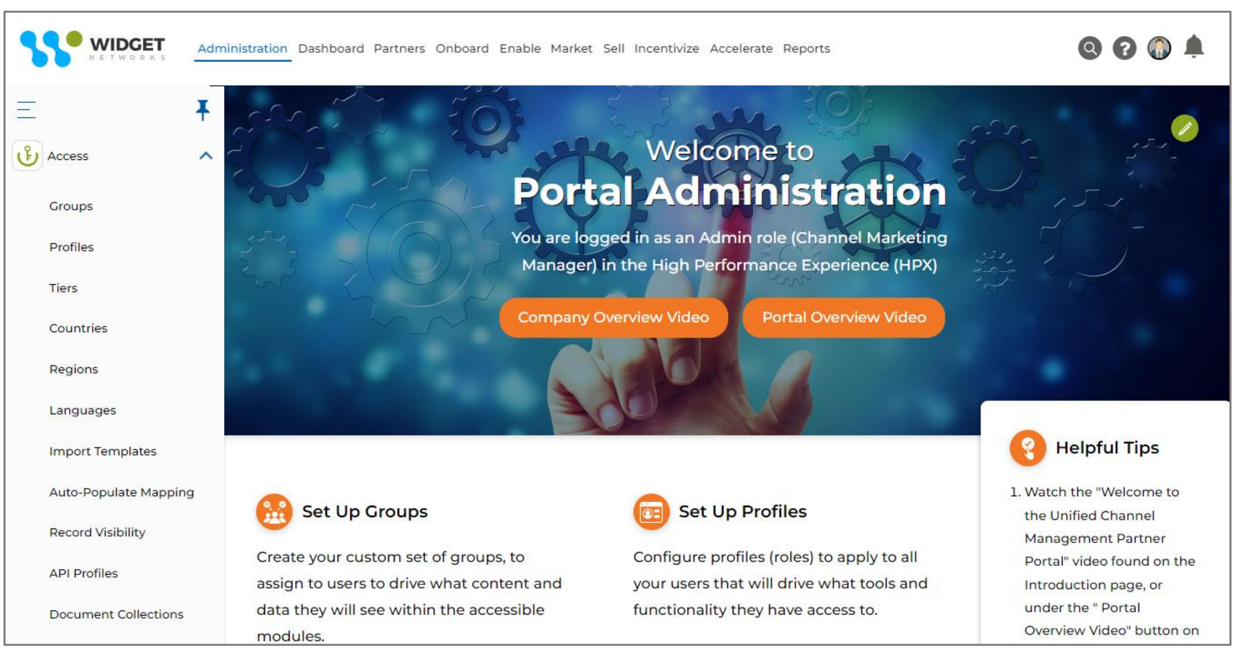
Pages layouts can be set by selecting objects from the list depicted in the figure below:



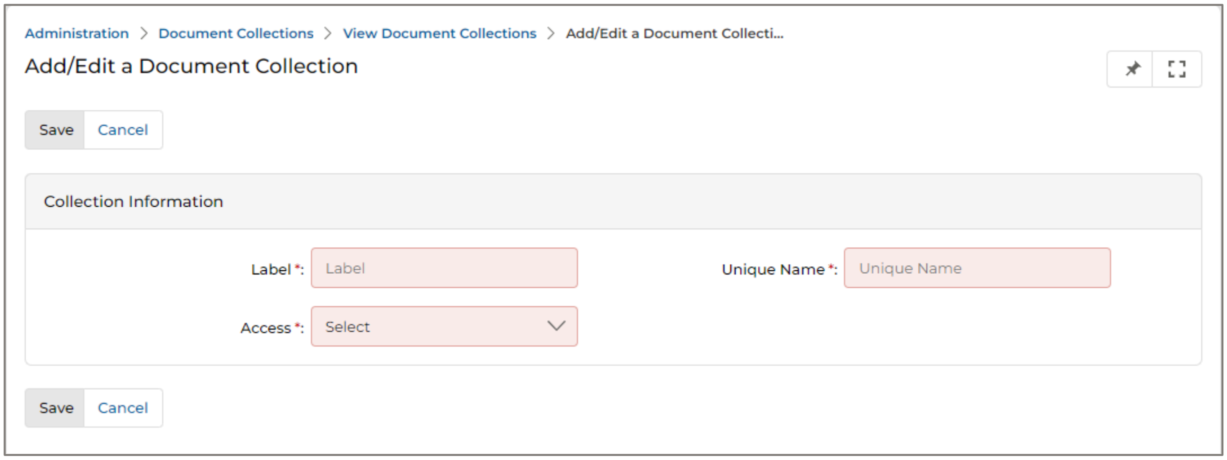
Manage File Collections

This feature provides an add-on shortcut menu "Documents Collections" to the Access Application allowing the admin to define as well as manage (Add/Edit) the specific locations/folders where associated images for documents, assets, and respective collaterals will be stored. This feature is introduced as a back-end feature and will be only utilized by the Admin with communication with ZINFI's Engineering team.

- Click on **Access > Document Collections** from the left menu.



- Clicking the Add or the Edit button associated with any document will take you to the "Add/Edit a Document Collection" page, as shown in the image below.



The various fields contained in the "Collection Information" section are discussed below.

a. Label – Provide a user-friendly name for the Label.

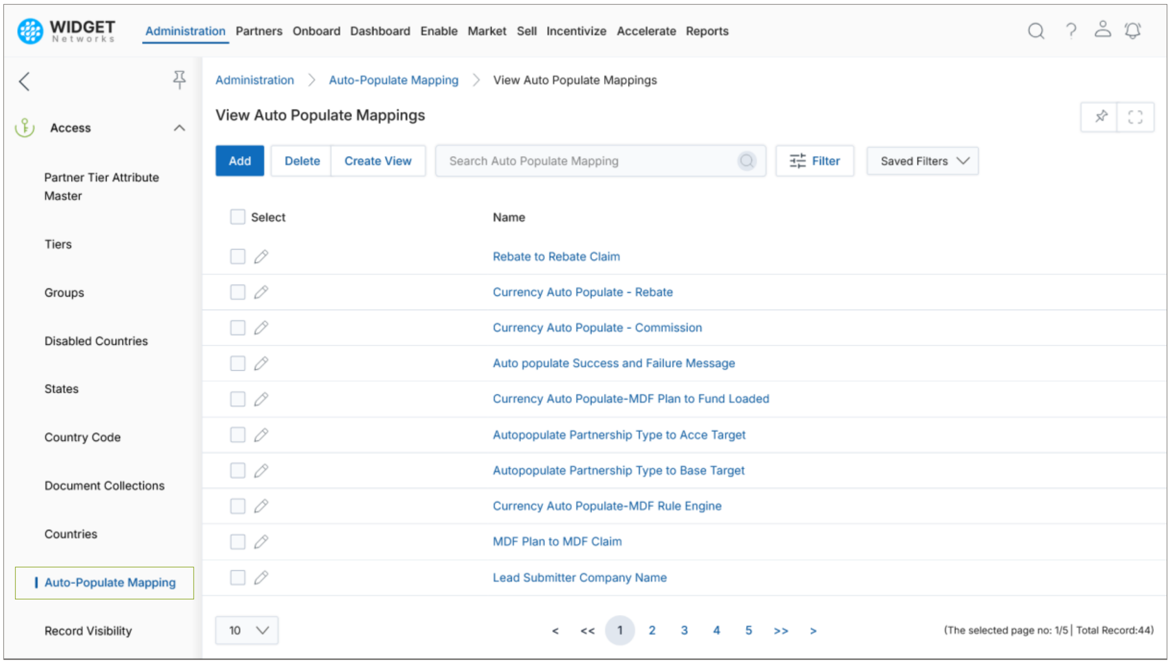
b. Unique Name – Reflects the name of the folder where the respective images/files will get stored when they are uploaded to the system.

c. Access – Clicking the dropdown arrow select the Scope Resolution/Accessibility of the Folder and set it as "Public" or "Private". Click Save to Save the Collection.

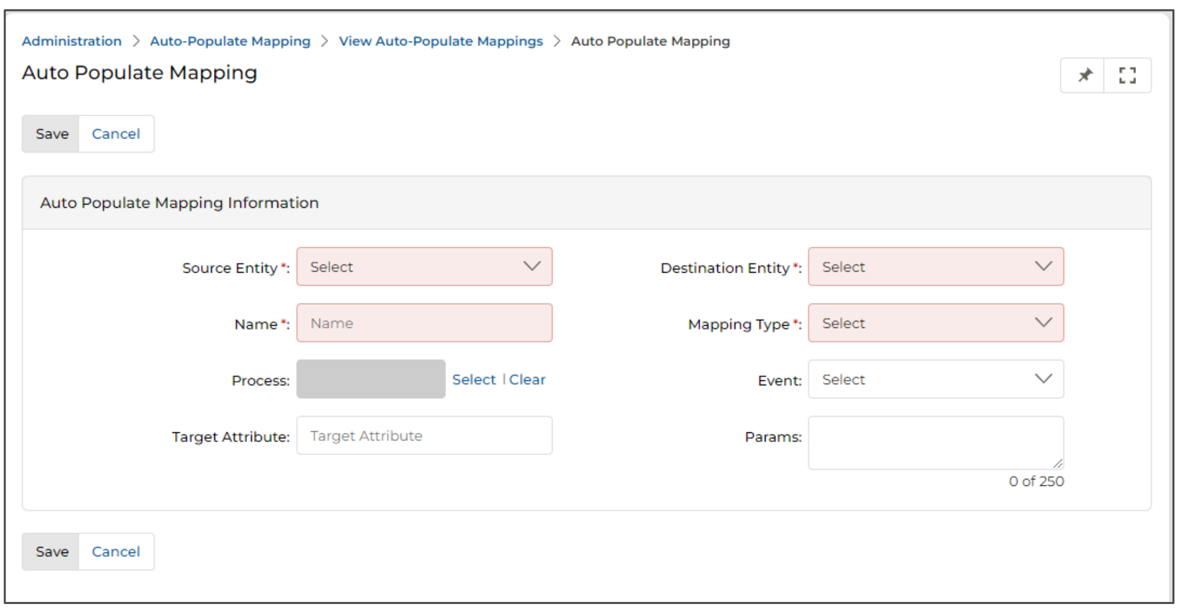
Auto Populate Mapping for Related Applications

Massive update for ZINFI's related Applications comes with a specific feature allowing Admins to retain attributes seamlessly between related UPM Applications. For example, we want to retain a custom Field/Attribute of a Prospect when we are converting the Prospect to a Contact. Normally, all fields of a specific UPM Application are not retained by default, when being converted to another Application Record. With this feature, we can retain the existing field of an application record and copy it to the related UPM Application.

1. Click on **Administration** on the top menu.
2. Click on **Access > Auto Populate Mapping** from the left menu bar.



3. To **Edit** an existing Mapping – click on the small pencil icon. To **Add** a new Mapping – click on the “Add” button at the top of the View Auto Populate Mappings page.



4. Once you are in the **Add/Edit an Auto Populate Mapping** page, check the following information:

   a. Auto Populate Mapping Information

      i. **Source Entity** – The UPM entity/Application whose fields/values are going to get retained.

ii. **Destination Entity** – The UPM entity/Application where the fields/values will be copied or retained.

iii. **Name** – Name of the new Auto Populate Mapping.

iv. **Mapping Type** – Field Mapping Type between the UPM Entities can be any one of the three types – Auto Populate – where fields are auto-copied over, Duplicate – where fields will be duplicated for the destination entity and Event – when the fields will be copied when an event occurs.

v. **Process** – Appropriate Process can be chosen from the list of Dynamic Processes/Stored Procedures.

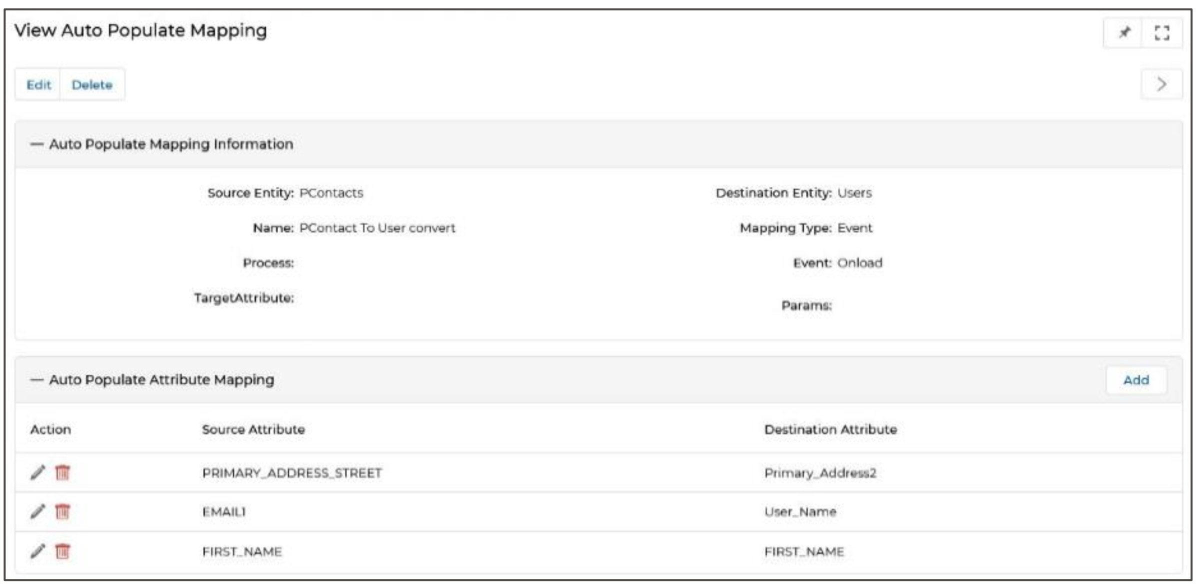
vi. **Event** – It can either be On Change or Onload, based on the Field application type.

vii. **Target Attribute** – Any Target Attribute to be associated can be provided.

viii. **Params** – Parameters can be defined to override and preset configurations. Once you are done, click **Save**.

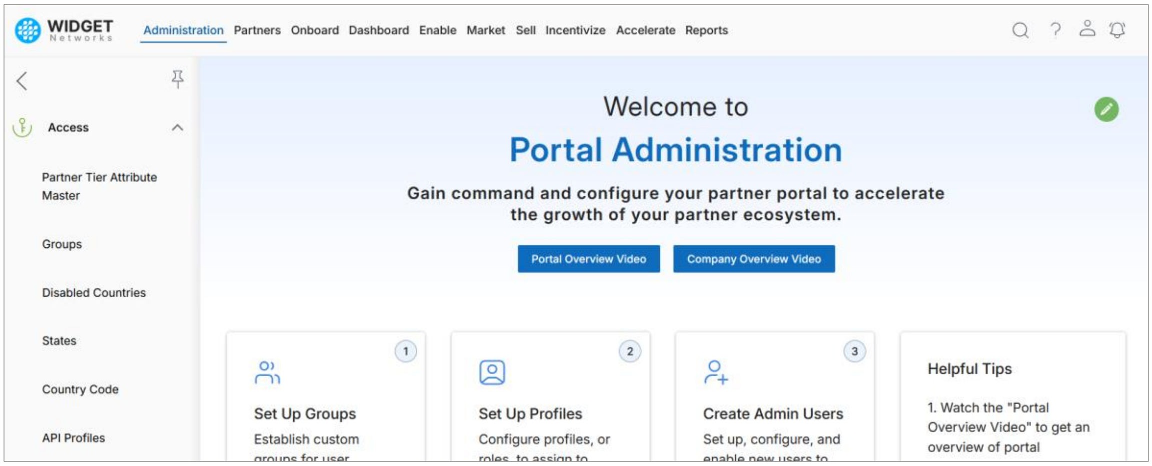
b. Auto Populate Attribute mapping

i. The List of Mapped Attributes can be viewed and managed.

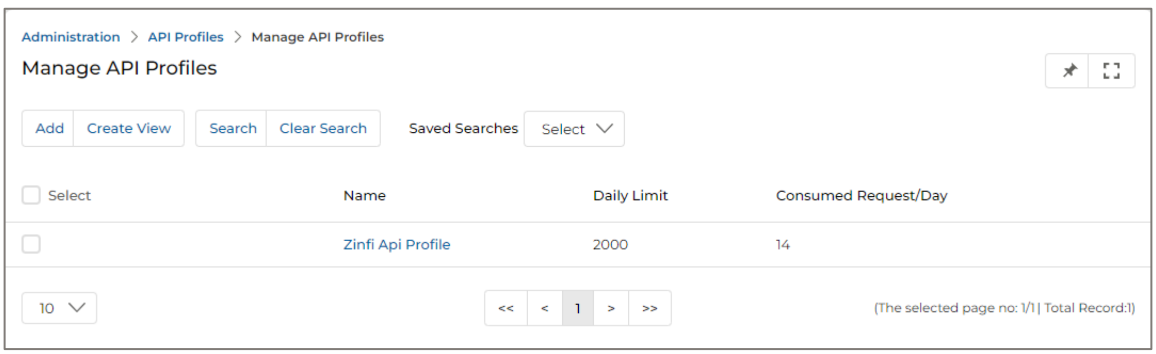


Manage API Profiles

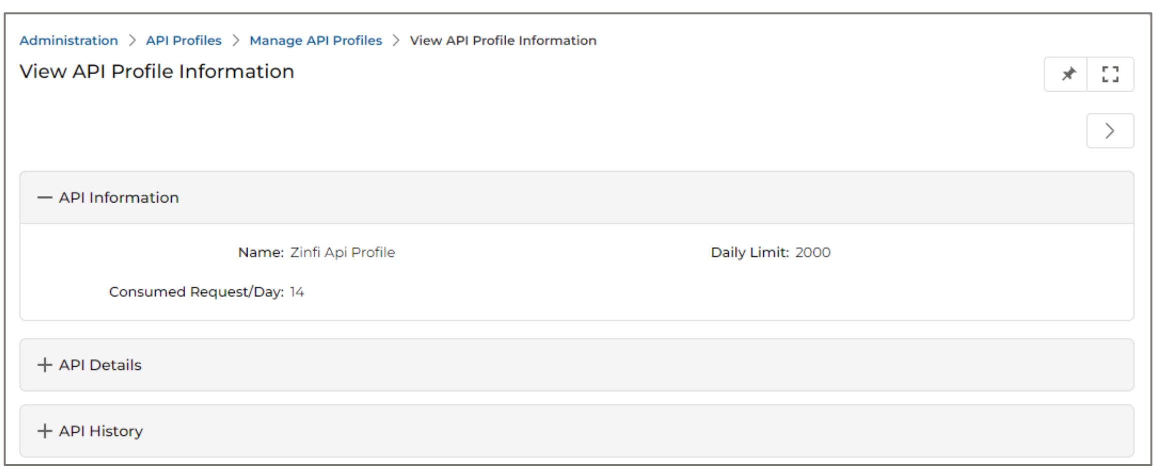
The latest upgrade features the hot rod release allowing third-party systems to access our UPM APIs to manipulate UPM records. Users provided access to API Profile are allowed to utilize the ZINFI UPM API which can be created and shared on request. Click on **Administration** on the top menu. Click on **Access > API Profiles** from the left menu.



- Clicking “API Profile” from the left menu will take you to the “Manage API Profiles” page that displays the Names of all UPM API Profiles.



- Clicking the name of any specific API Profile will take you to the “View API Profile Information” page that reflects the details of the specific API profile.



The various sections contained in this page are discussed below:

a. **API Information**:

   I. Name – Name of the API.

   II. Daily Limit – Daily API calls allowed.

   III. Consumed Request/Day – Consumed API Calls/Requests for the specific day.

b. **API Details**: Contains the details of the APIS Listed along with their Name, Service Information, and Description, along with the respective API structures and their description.

— API Details

Action	Name	Service information	Description
	List of Module Data	Module Data list	Sample Request { "ProcessId":"A9B34876-A194-4D75-ACDF-AEB986C50862", "ProcessData":{ "EntityId":"9", "totalItems":0, "pageNo":1, "numPages":0, "pageSize":10, "maxSize":10, "orderBy":"[Modify.Date]", "orderType":"desc", "Lang":"en-US", "Logic":"", "LayoutId":"0", "globalVariable":{ "campaignTypeId":"0", "campaignTypeText":"", "campaignId":"0", "campaignText":"", "campaignStatusId":"0", "campaignStatusText":"" }, "Mode":"list", "searchInfo":{ "selectedSearchId":"0", "searchType":"" }, "returnType":"list", "EntityDetailsPrevNextPageNo":1, "selectedLayoutId":"0" } }
	Save Module Data	ModuleSaveDate	Sample Request { "data":{ "Id":"", "EMAIL1":"johnny@email.com", "KEY_TITLE":"Mr", "FirstName":"Audry", "LastName":"Crosetti", "KEY_Phone":"(619) 6274611", "KEY_PHONE_FAX":null, "PHONE_MOBILE":null, "LEAD_SOURCE":null, "Key_Campaign":{ "CampaignStatus":"", "CampaginType":"", "Campagin":"", "LeadId":"" }, "STATUS":null, "COMPANY_NAME":"Paychex", "KEY_COMPANY_WEBSITE":null, "EMPLOYEE_RANGE":null, "INDUSTRY_TYPE":null, "KEY_CustomField1":null, "Competitor_Name":null, "Competitor_Description":null, "Competitor_Strength":null, "Competitor_Weakness":null, "KEY_PRIMARY_ADDRESS_STREET":null, "KEY_PRIMARY_ADDRESS_STREET2":null, "KEY_PRIMARY_ADDRESS_CITY":null, "KEY_PRIMARY_ADDRESS_COUNTRY":null, "KEY_PRIMARY_ADDRESS_STATE":null, "KEY_PRIMARY_ADDRESS_POSTALCODE":null, "KEY_ALT_ADDRESS_STREET":null, "KEY_ALT_ADDRESS_STREET2":null, "KEY_ALT_ADDRESS_CITY":null, "KEY_ALT_ADDRESS_COUNTRY":null, "KEY_ALT_ADDRESS_STATE":null, "KEY_ALT_ADDRESS_POSTALCODE":null, "KEY_DESCRIPTION":null, "LEAD_SOURCE_Value":null, "STATUS_Value":null, "KEY_PRIMARY_ADDRESS_COUNTRY_Value":null, "KEY_PRIMARY_ADDRESS_STATE_Value":null, "KEY_ALT_ADDRESS_COUNTRY_Value":null, "KEY_ALT_ADDRESS_STATE_Value":null }, "enitiy":"9", "mode":"n" }

c. **API History**: This summary provides a detailed view of the API Profiles associated with UPM users.

— Api_History   View All

Action	Name	IpAddress	User	Created On
	Save Module Data	NA	Widget CMM	02/19/2020 6:12:08 AM
	List of Module Data	150.129.179.18	Widget CMM	07/27/2018 12:21:15 PM
	Save Module Data	150.129.179.18	Widget CMM	07/27/2018 12:20:20 PM
	Save Module Data	150.129.179.18	Widget CMM	07/27/2018 12:20:06 PM
	List of Module Data	150.129.179.18	Widget CMM	07/27/2018 12:18:56 PM

Click to View More

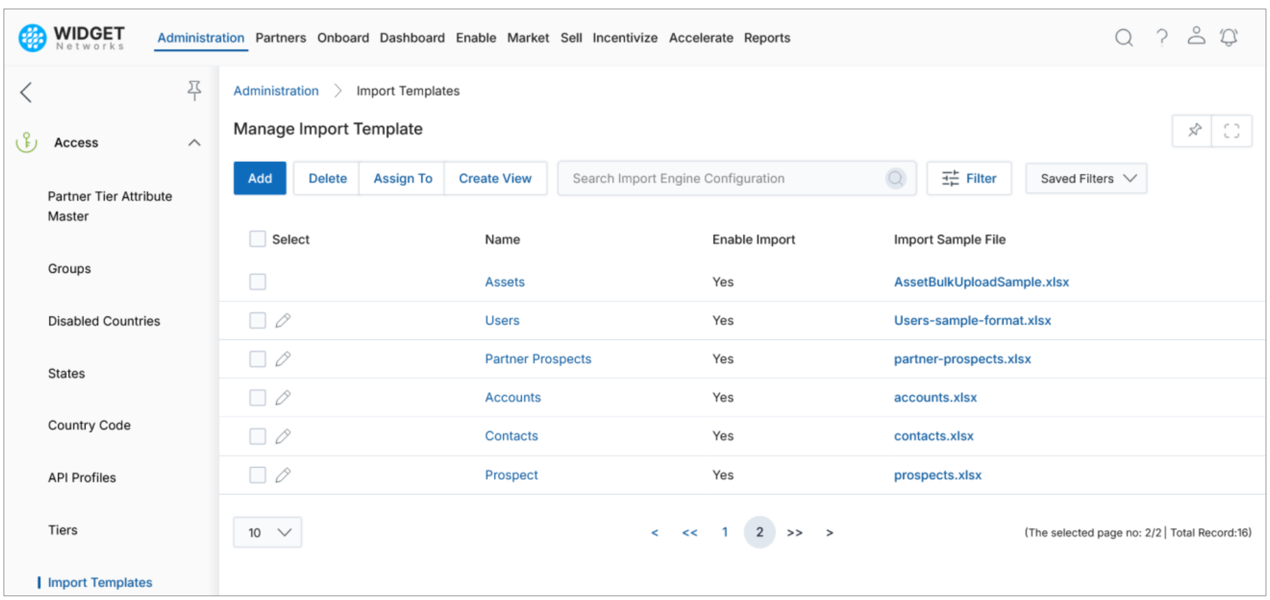
Manage Import Templates

This feature is updated with the ability to upload and manage Application-specific Import Engine Templates for the processing of the UPM Import Engine. As we know, the Import Engine allows us to bulk import records of a specific Application/Object. Featuring a configurable engine, you can use it to configure the import of records in standard global formats viz. CSV, xlsx, etc., and insert/update bulk UPM records for both standard and custom entities of UPM. The Sample Import Files with Application Parameters as Columns are utilized to feed/import records for that Application. In the below example, the Opportunities Sample Import Excel File is provided.

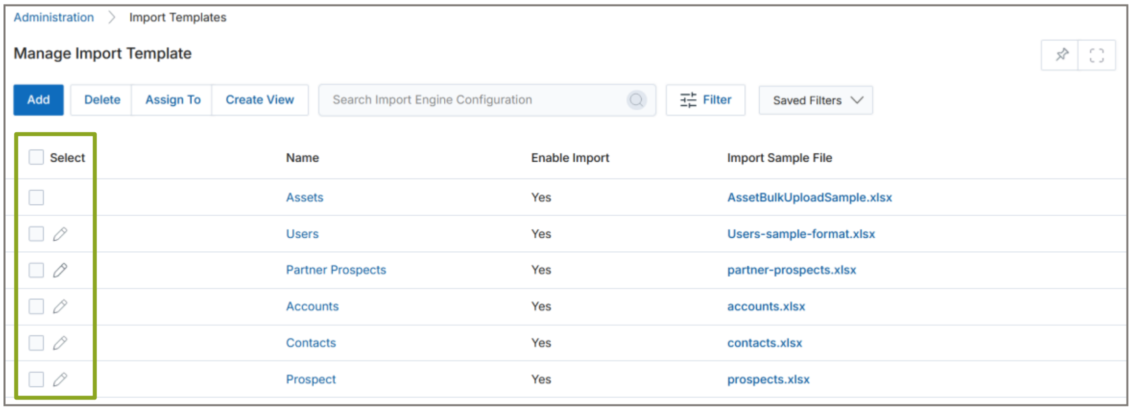
A	B	C	D	E	F	G	H	I	J
Opportunity Name	Sales stage	Amount	Expected Close date	Currency ISO Code	Lead Source	Account	Contact	Pricebook	Quarter
ZQ_Opp_6	1 - Prospecting	400	04/27/2021	Pound Sterling	Employee	ZQ-ACC-006	zinfitest_user006@yopmail.com	Zinfi_test_Price book	FY20Q2
ZQ_Opp_7	5 - Needs Analysis	110	04/25/2021	Pound Sterling	Direct mail	ZQ-ACC-007	zinfitest_user007@yopmail.com	Zinfi_test_Price book	FY20Q3
ZQ_Opp_8	10 - Closed Won	120	04/26/2021	US Dollar	Web site	ZQ-ACC-008	zinfitest_user008@yopmail.com	Zinfi_test_Price book	FY20Q4

'Import Templates' allows you to configure and assign any number of Import Templates, with the desired fields (mandatory and non-mandatory) and get them associated with the "Download Sample Data" feature of the Import engine of the desired Application. This feature is an added advantage to the sales reps and partner users while importing data in bulk in the respective Application as it provides the sample/base worksheet to enter record data.

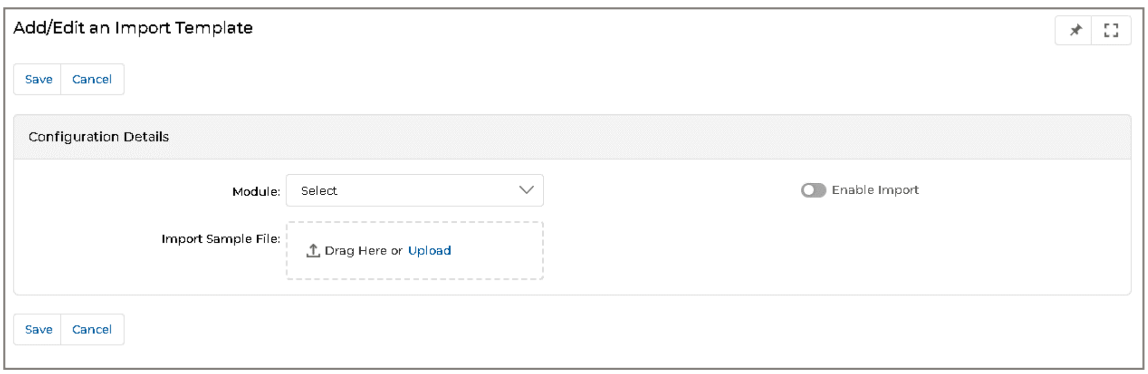
- Click on **Administration** on the top menu.
- Click on **Access > Import Templates** from the left menu bar.



- To create a new import template, click the "Add" button, and to bring in changes to an existing one, click the small pencil icon associated with the template.



- Clicking the "**Add**" or the "**Edit**" button will take you to the following page as shown in the image below.



a. **Configuration Details:**

i. **Module –** Clicking the drop-down arrow, select the "Application" for which this import template would be associated with.

ii. **Enable Import –** Enable the toggle key to make this operative.

iii. **Import Sample File –** Drag here or upload from your system the newly configured sample file for importing records.

- Once you are done, click on the **Save** button.
- An example of a custom-specific format is contained in the Excel sheet as shown in the image below.

1	First Name	Last Name	Email	Company	Country	
2	David	Rocco	david@testmail.com	Zinfi Inc.	USA	
3						
4						

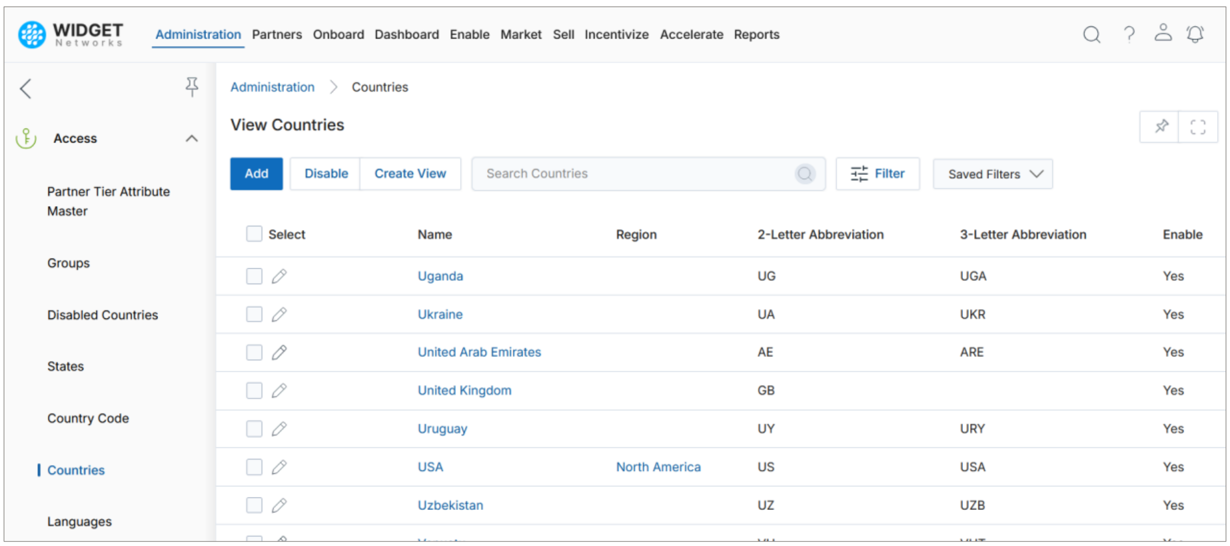
Country-Language Association and Selection Page Management

ZINFI's Unified Channel Management (UPM) platform comes with a complete multilingual engine that allows your organization to provide a fully localized experience to users, regardless of their geographic location or the languages they speak. The ZINFI channel management platform provides a multilingual-based UI/UX dependent on the selection of applicable Country(s) and Language(s).

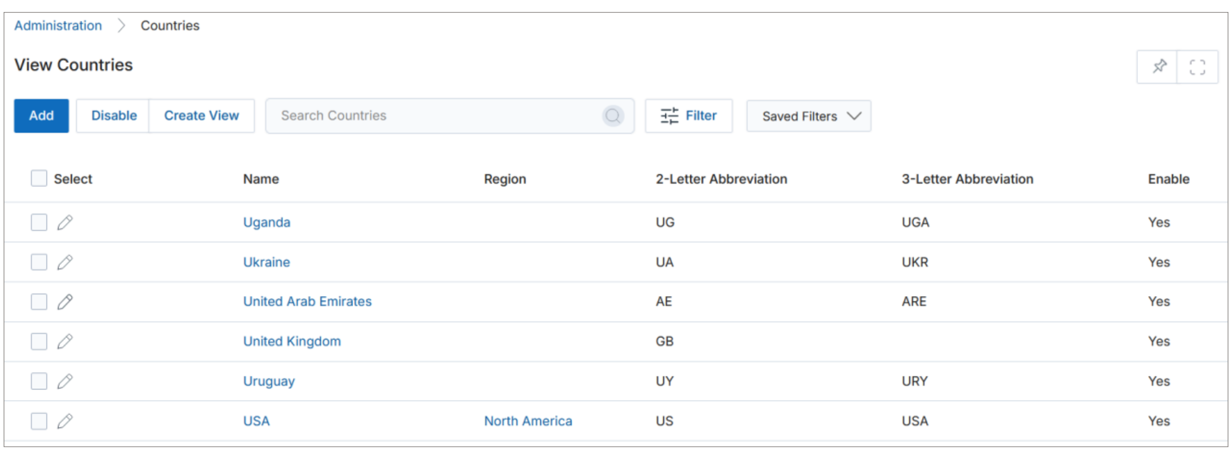
‘Countries’ allows you to set up any number of countries as a segmentation method for record assignment and viewership. The UPM update features the association of Languages to a Country for the management of associated Languages and allows you to set up any number of languages as a segmentation method.

ZINFI provides 10 basic languages (associated with specific Country(s)) OOTB to support localized UI out of the box and allows the User to preset the “Country and Language” before login or from UPM Settings – to provide a localized interface translate to that language.

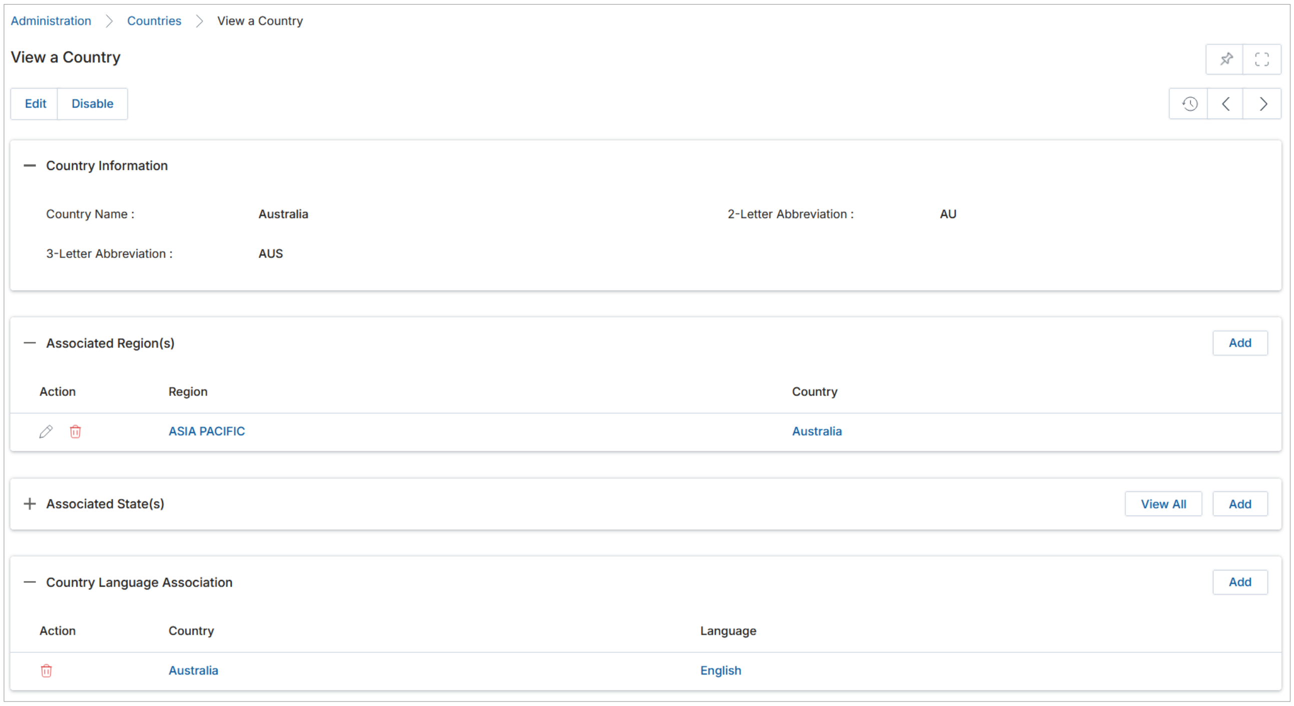
- Click on **Administration** on the top menu.
- Click on **Access > Countries** from the left menu bar.



- Click on the Country Name of any Country listing to see the details page.

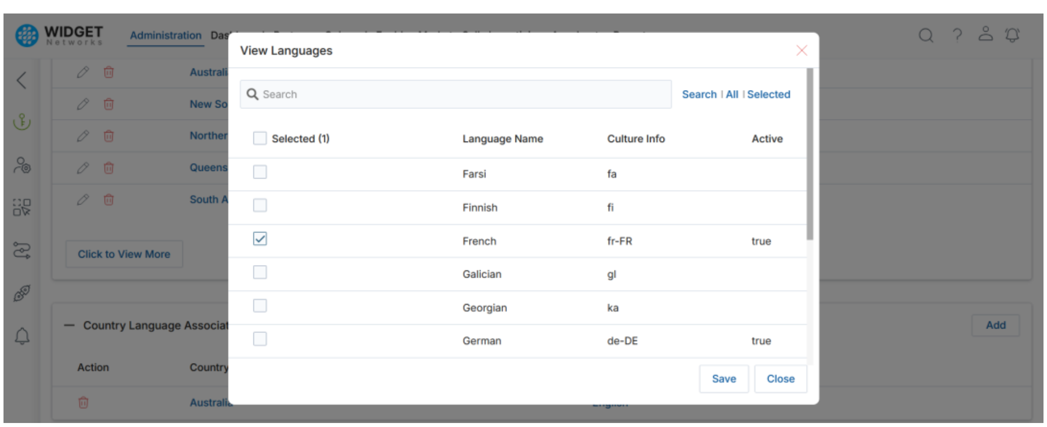


- Once in the details page, you will see various buttons and sections, such as:



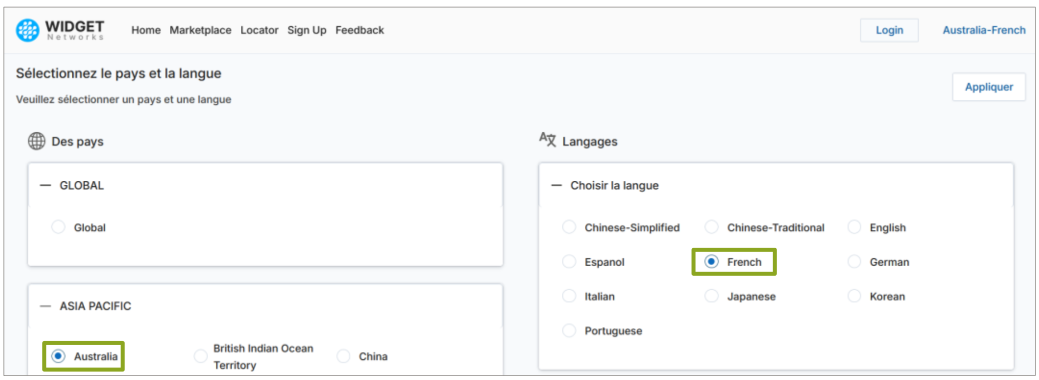
- **Country Language Association**: This section allows the admin to associate specific languages to any selected country. The selected language should always be in the 'Active' status for it to be displayed to the user in the pre-login/settings page.

- Clicking the 'Add' button a pop-up window will appear that will allow you to select and associate the required languages to the specific country. Once the languages are selected by providing a checkmark on the boxes as shown in the image below click on the 'Save button.

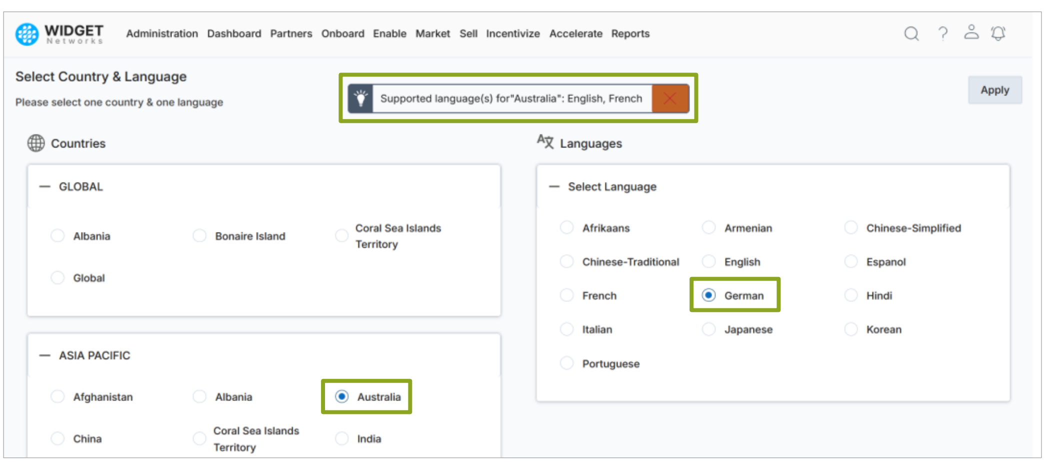


- The newly selected languages will now be displayed in the ‘Country Language Association’ related list.

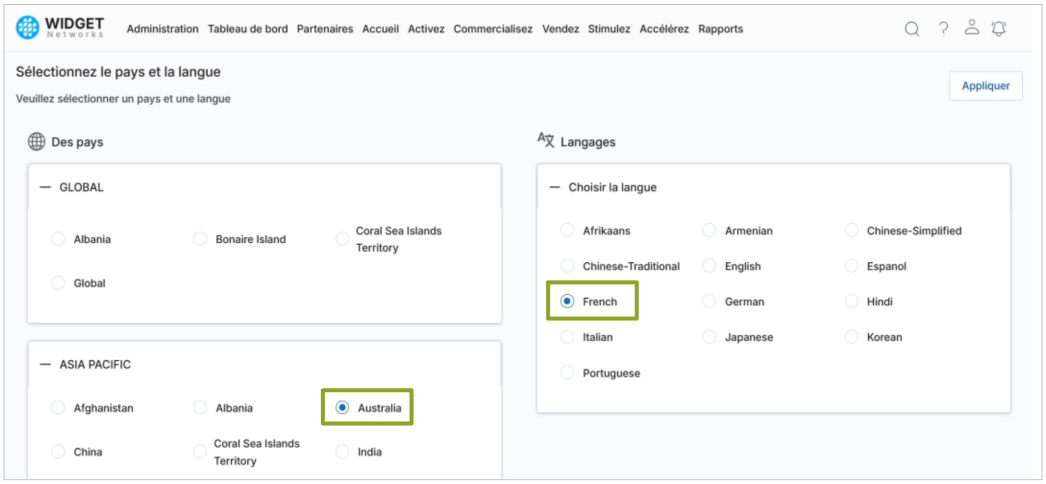
- In the pre-login Page - when the user selects the specific country the newly selected languages will get reflected along with the existing default ones.



- Whenever a user attempts to select a country with a language from the Country-Language page (either during login or while changing preferences post login), the system validates the selection against the configuration in in Country-Language Association in Access Management.



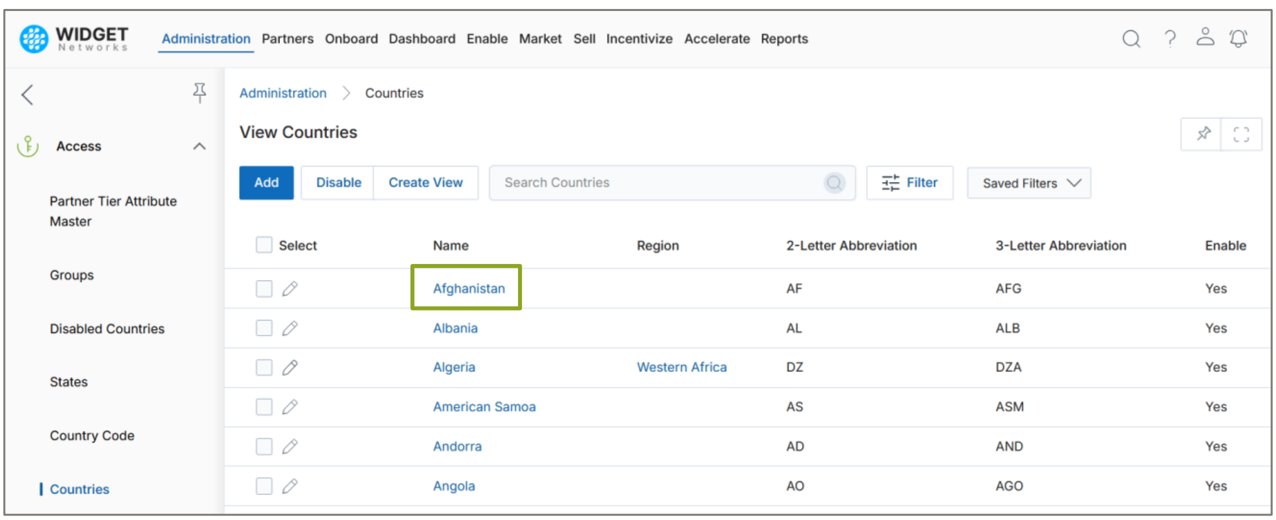
- Next, select Australia as country with French as language.
- The Apply button becomes enabled, the selection is saved successfully, and the portal UI is updated and displayed in French.



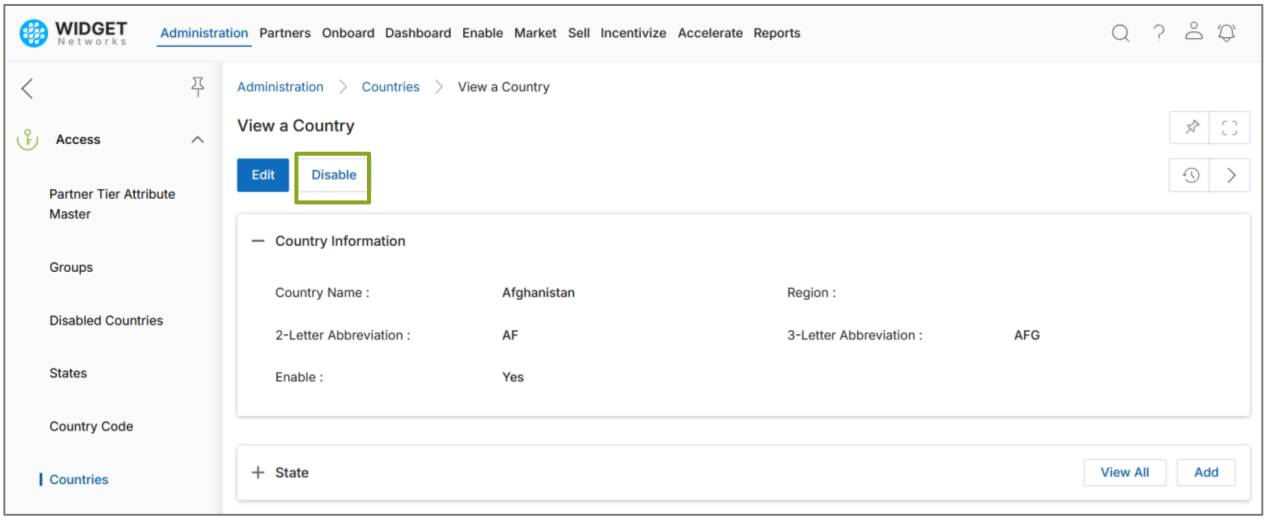
Enabling/Disabling Countries

Enhancements have been introduced to the ‘Countries’ functionality within applications. The Country application stores all data related to countries used across the platform, including language pages, related lists, and dropdown areas, and serves as a dependent field for States. Clients often encounter issues with changed country names or the need to restrict access to certain countries. With this update, countries can now be easily managed by enabling or disabling them as required.

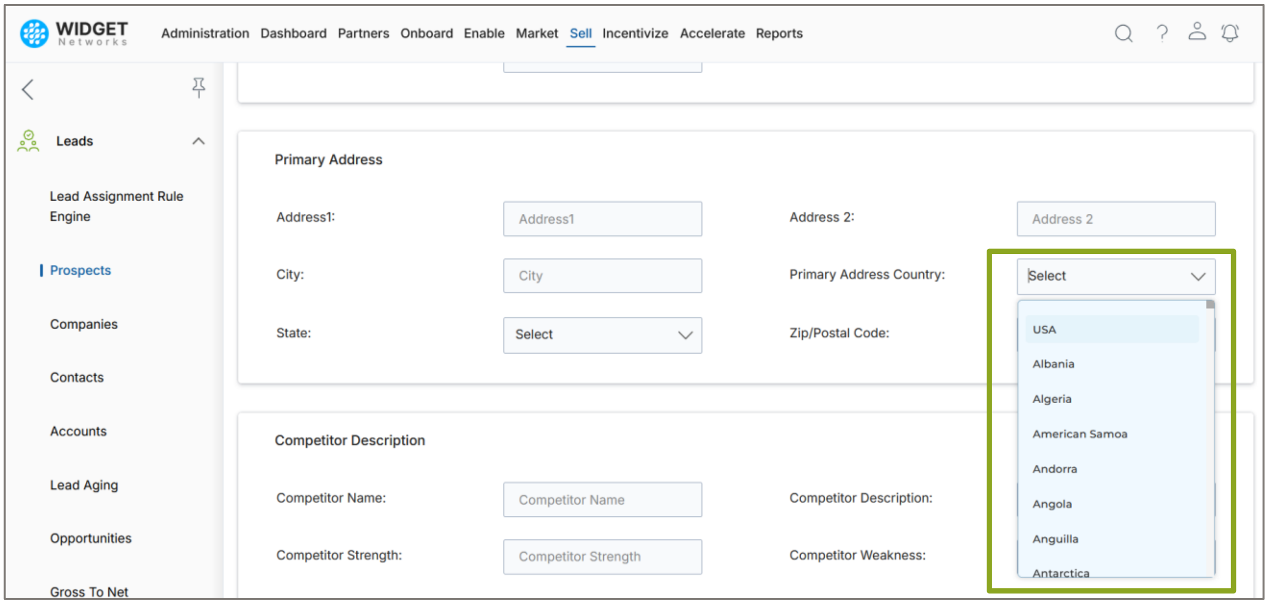
1. To understand this feature, navigate to **Administration** > **Access** > **Countries.** The View Countries page contains all the generated ‘Countries’.



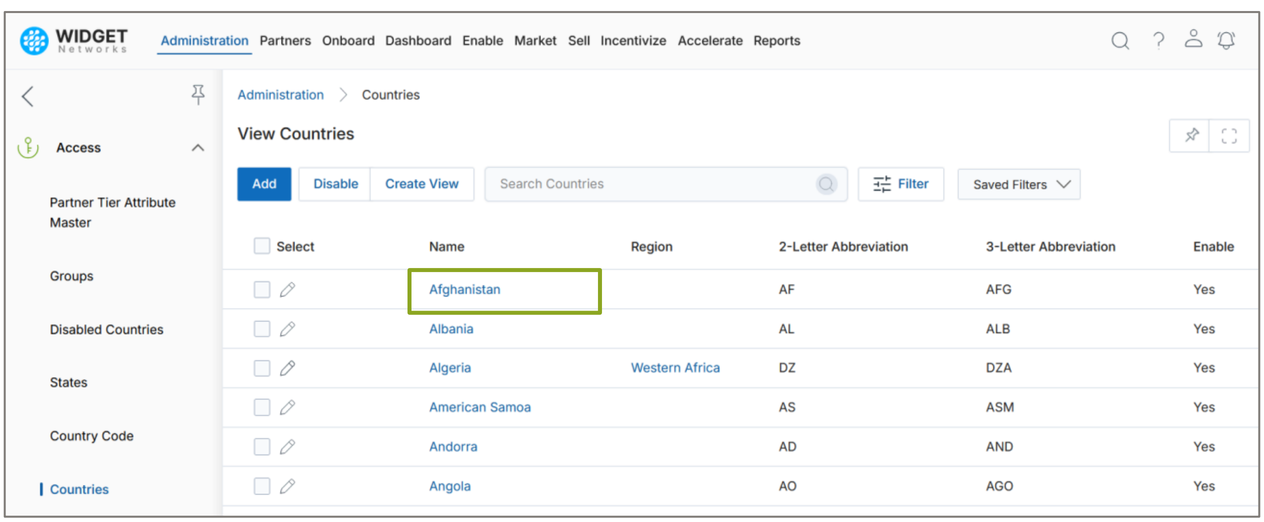
2. To disable a country, navigate to the details page of the specific country and click the "Disable" button. The country will then be removed from the "View Countries" page and added to the "View Disabled Country" list, which can be accessed by going to Administration > Access > Disabled Country.



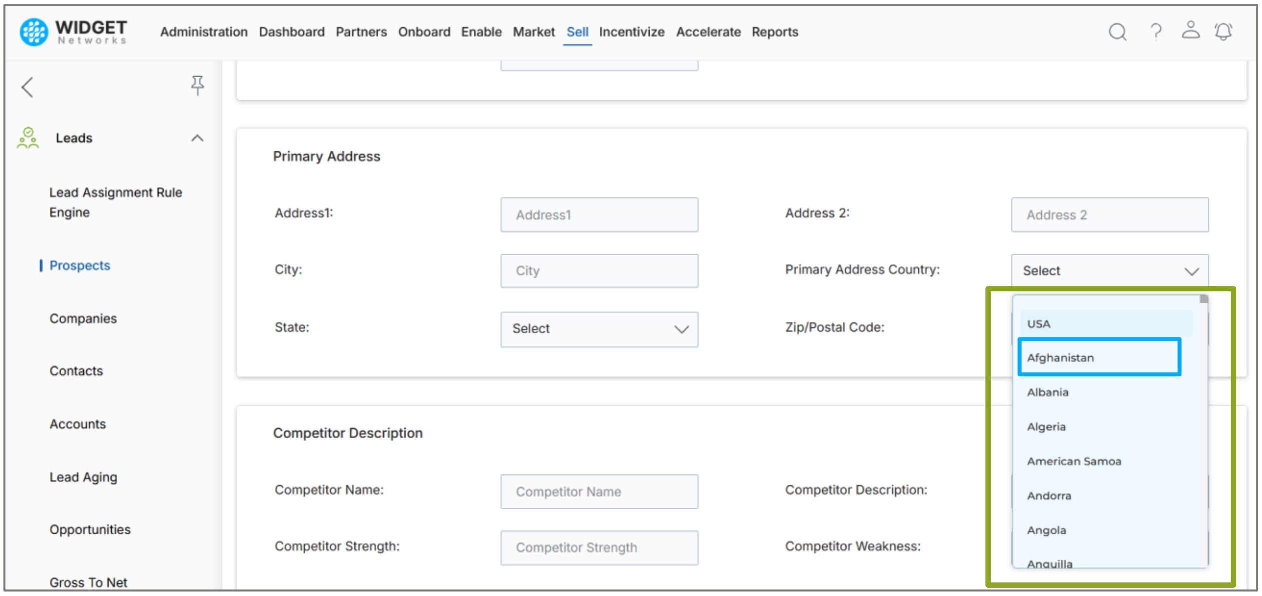
3. When a country's name is disabled, it will not be displayed when creating new records. The image below demonstrates that the country name 'Afghanistan', which has been disabled, does not appear in the dropdown list for the 'Primary Address Country' field while creating a new prospect.



4. The disabled country can be enabled by clicking the 'Enable button. The enabled country will appear on the "View Countries" page, accessible via Administration > Access > Countries as shown in the image below.

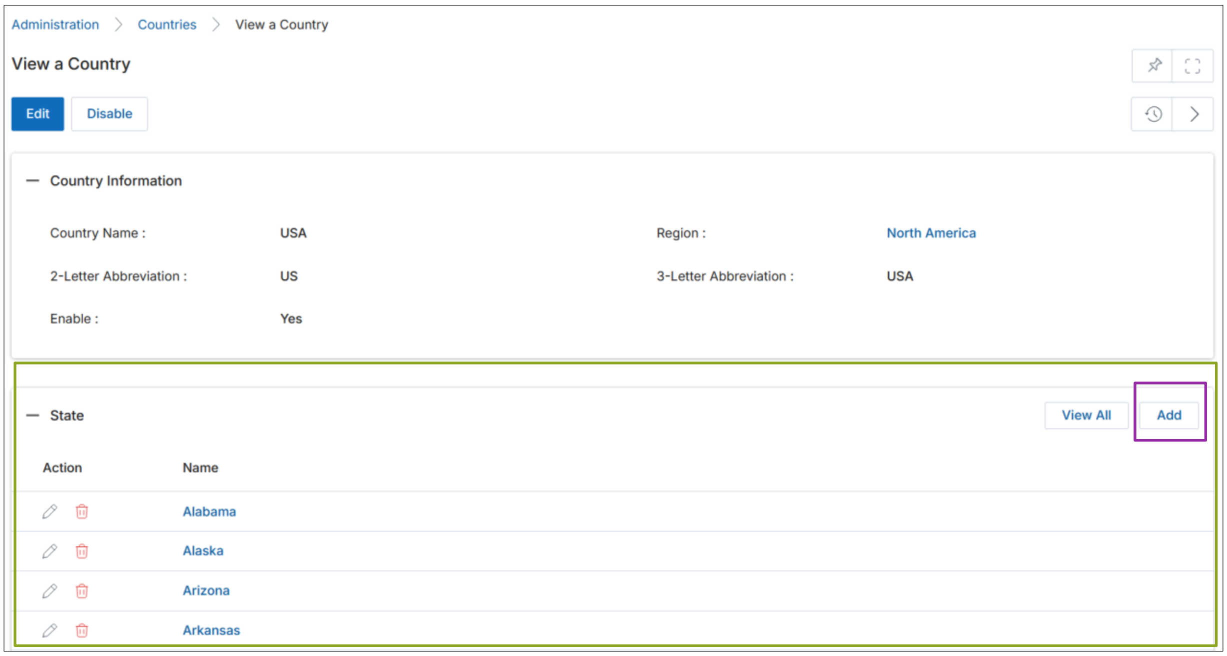


5. When a country name is enabled, it will be displayed when creating new records. The image below shows the country name 'Afghanistan', which has been enabled, appearing in the dropdown list for the 'Primary Address Country' field while creating a new prospect.

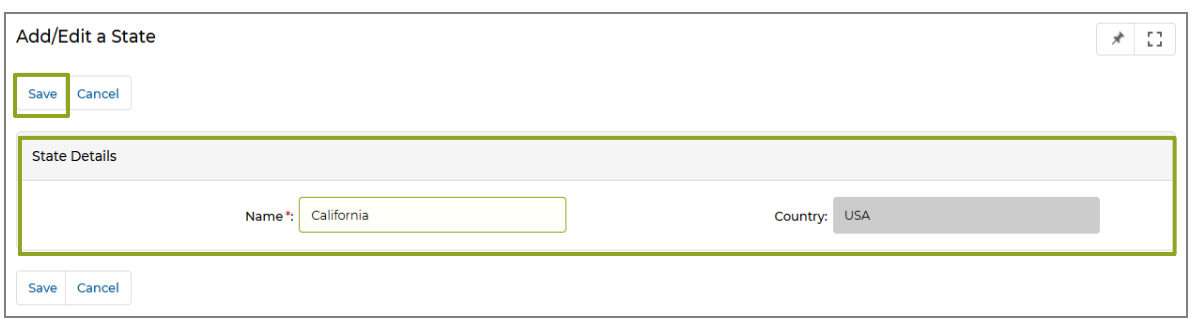


Manage States of a Country

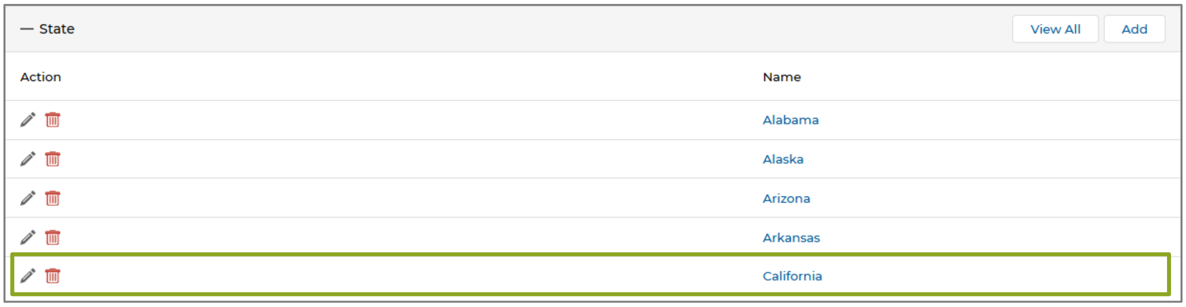
The OEM Admin enjoys the privilege of managing the States of respective Countries. Options are now available for the Admin to Add, Edit, or Delete - States are available in the Related List on the Country's details page. Including this feature gives the Admin greater control to configure a Country with States.



- In the UPM, the Admin traverses from Access to Countries. The Admin needs to go to the details page of the specific Country where a list of States is available in the 'State' Related List.
- Clicking the 'Add' button associated with the Related List will take the Admin to the Add/Edit a State page, where he has to provide the name of the State he wishes to add and click Save. The Admin wants to add 'California' as the new State in this example.



- Once the details are saved, the Admin will be redirected to the View a Country page. In the 'State' Related List, we will see that 'California' has been added as the new State.

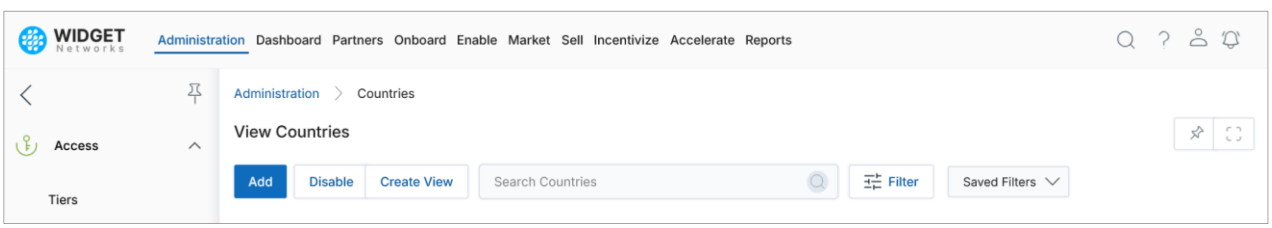


- By clicking the small pencil icon, the Admin can Edit any State's name. To delete a State from the list, the Admin must click the trash bin icon.

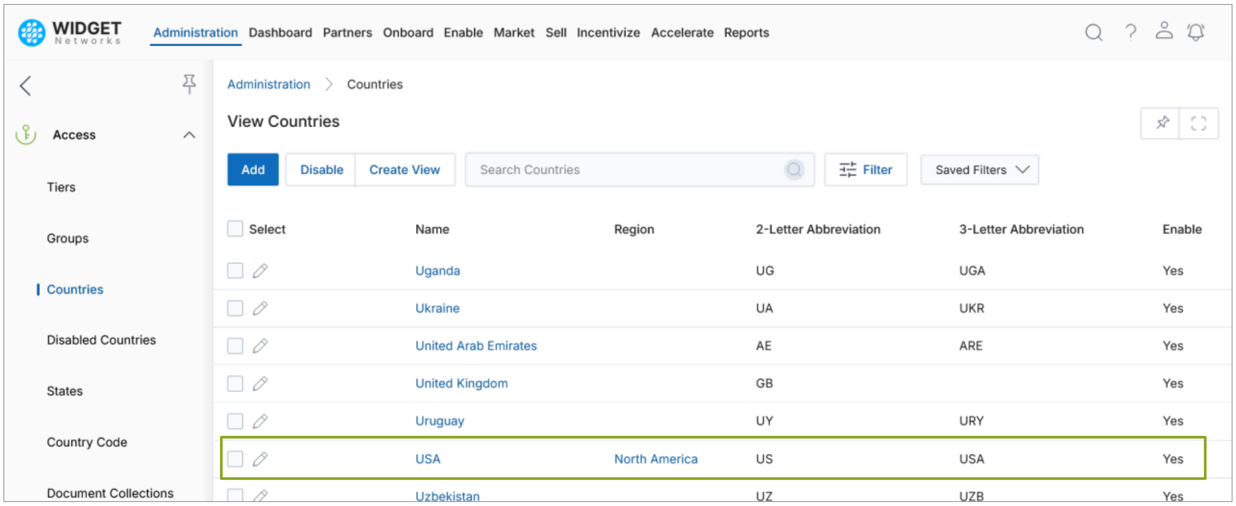
Mandatory Region Association and Abbreviation Enforcement in Country Master

As part of ongoing efforts to ensure data consistency and maintain region-based compliance across global records, the Country Master application has been enhanced with stricter validation and improved mapping integrity.

- Navigate to Administration > Access > Countries.

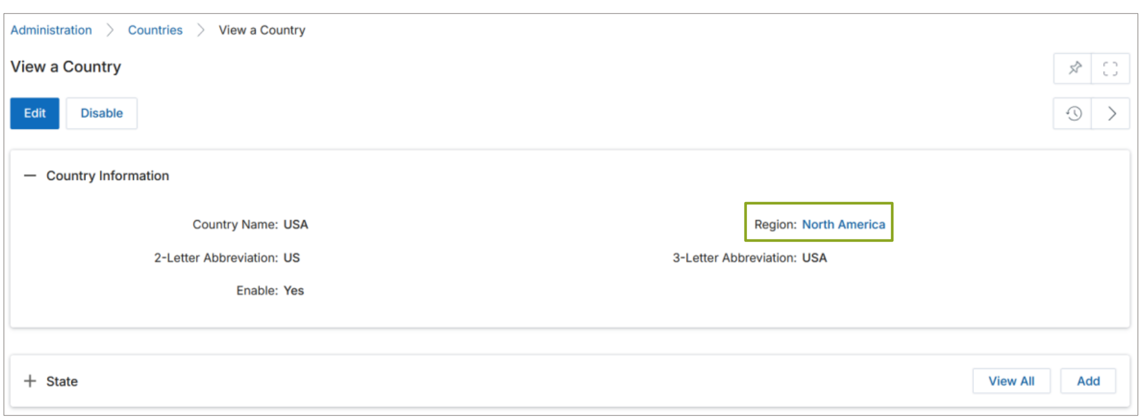


- Click Add or Edit an existing country.



- Select Region and provide 2-Letter Abbreviation and 3-Letter Abbreviation and save the record.

- **Mandatory Region Tagging**
  - Every country added or edited must now be associated with a specific region.
  - This enforces a strict one-to-one relationship, ensuring that a country cannot be left without regional classification or be linked to multiple regions unintentionally.



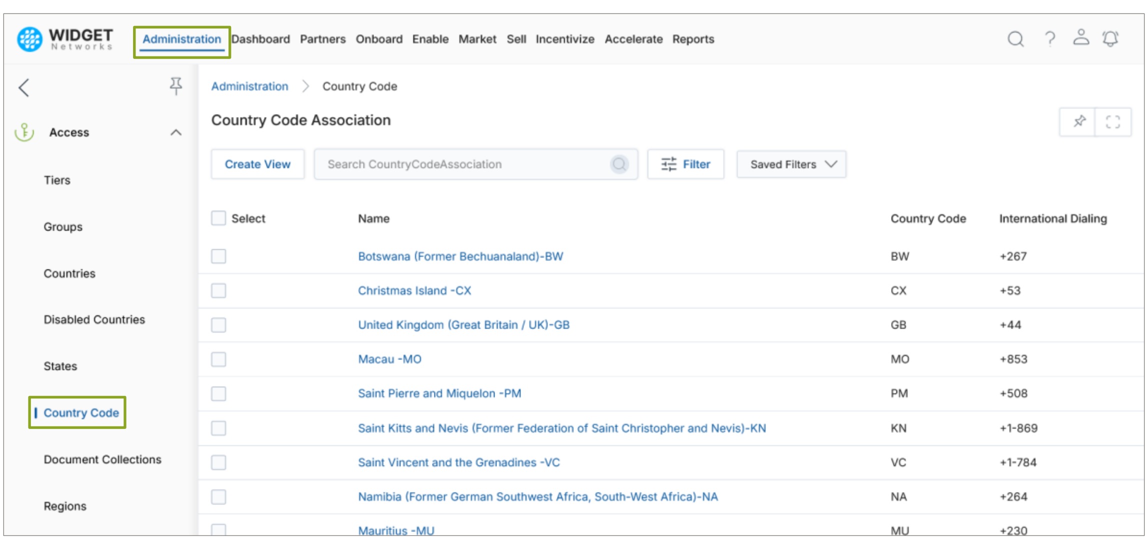
- **Enforced Abbreviation Fields**
  - The system now requires valid ISO-standard two-letter and three-letter abbreviations for every country.
  - These abbreviations are critical for downstream processes, including CRM synchronization and third-party data exchanges.

Note: *All existing country records have been updated to include valid region associations and abbreviation codes to maintain continuity and data accuracy across the platform.*

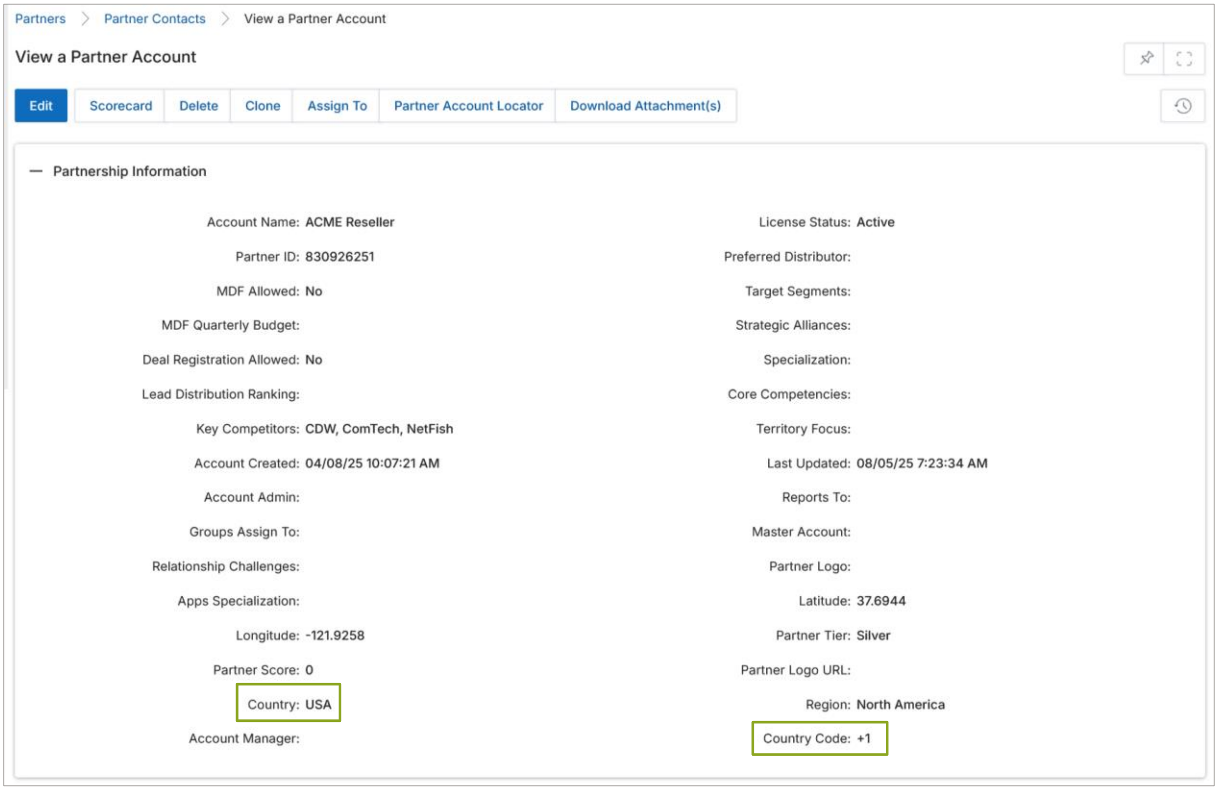
Mandatory Country Code Configuration across Applications

To ensure standardization of contact records and improve international communication, full integration of country dial codes has been introduced across key applications. With this update, all phone numbers throughout the platform are now accompanied by the appropriate country codes.

- Navigate to Administration > Access > Country Code.
- The whole list of countries with Country Codes and International Dialing Codes will be visible.



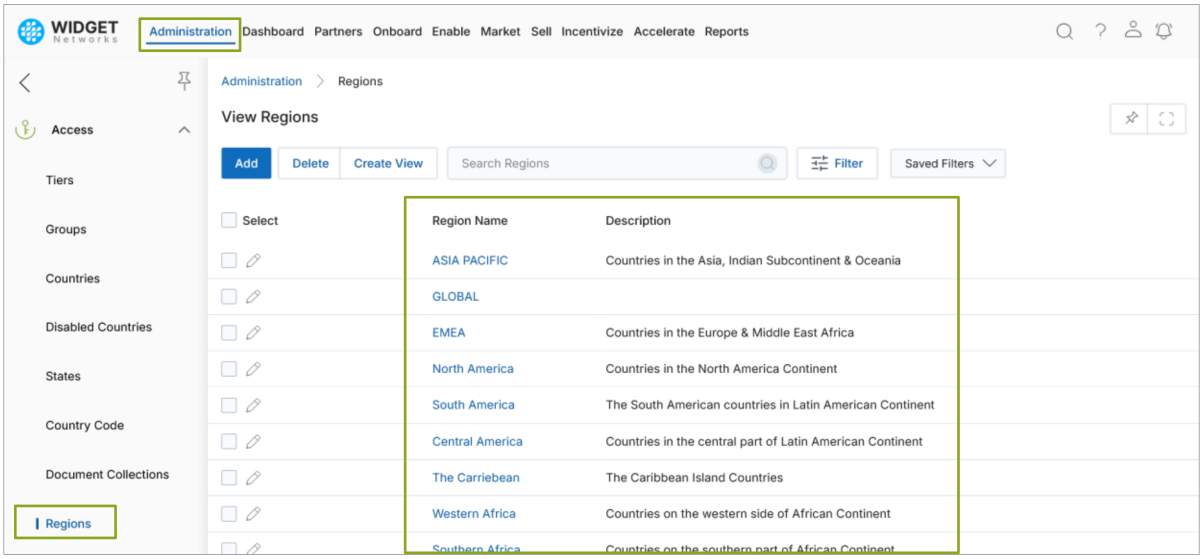
- A new dropdown field has been added for selecting country dial codes (e.g., +1 for USA, +91 for India).
- This dropdown appears in Partner Contacts, Contacts, Partner Accounts, Accounts, and User applications.
- Users must now explicitly choose the correct country code while entering or updating a phone number.
- This eliminates ambiguity and ensures consistent formatting of contact records.



Country-Region Mapping with Abbreviation Support

To improve transparency and ensure complete regional mapping, the Region application has been enhanced to display complete country abbreviation details alongside their mappings.

- The region listing now displays both two-letter and three-letter country abbreviation codes for each mapped country.
- Navigate to Administration > Access > Regions.
- Click the desired Region and view the associated list of Country(s) with the Region.



- This gives users immediate visibility into standardized identifiers without toggling between applications.
- Administrators can easily verify if countries are correctly configured and associated within their respective regions.

Configurable Date-Time Format

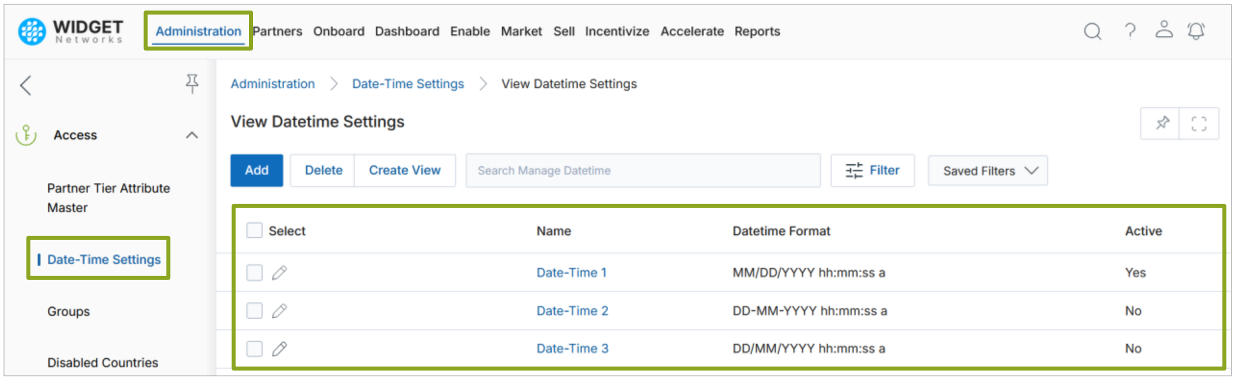
The Configurable Portal Date-Time Format feature allows portal administrators to configure the default date-time format for their portal. Once configured, this format is applied uniformly across all portal pages and components, including list pages, view pages, and add/edit pages.

Previously, the platform used a fixed MM/DD/YY format across the portal without customization options. Administrators can choose from multiple formats (e.g., DD/MM/YYYY, YYYY/MM/DD, etc.) based on their regional or organizational preference. The selected format becomes the active date-time format for that portal and automatically deactivates all other formats.

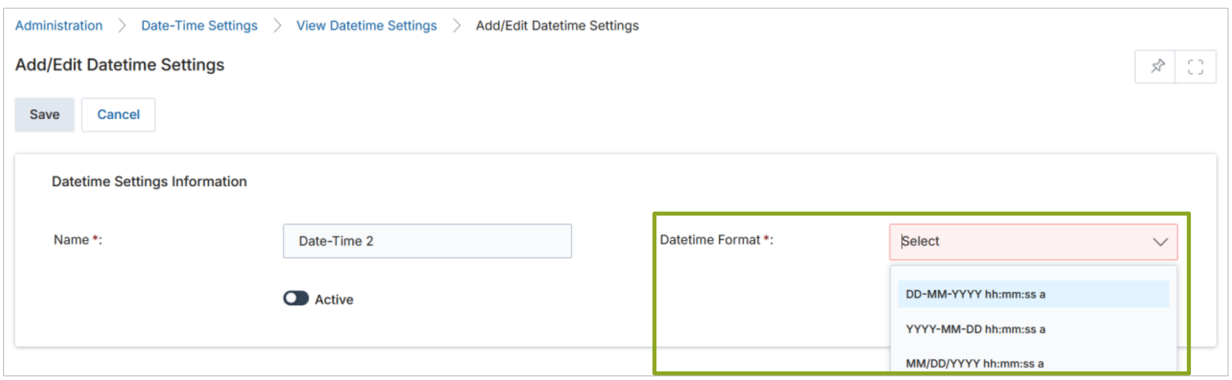
This change ensures consistency across the portal and reduces user confusion when entering, viewing, or exporting date-time data.

- Log in to the UPM as an administrator.

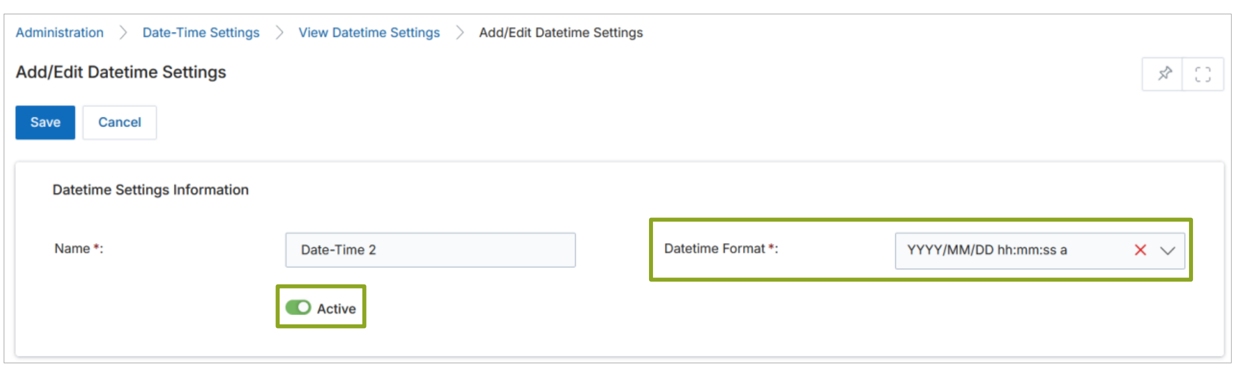
- Navigate to Administration > Access > Date-Time Settings to open the View Date-Time Settings page, which displays all active and inactive date-time formats.

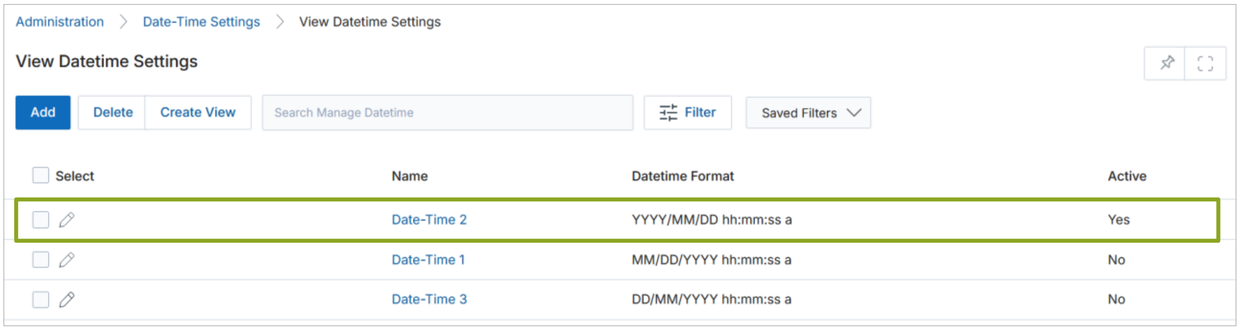


- Open the Add/Edit Date-Time Settings page and review the available formats (e.g., DD/MM/YYYY, YYYY/MM/DD, MM/DD/YYYY) in the Date-Time Format dropdown list.

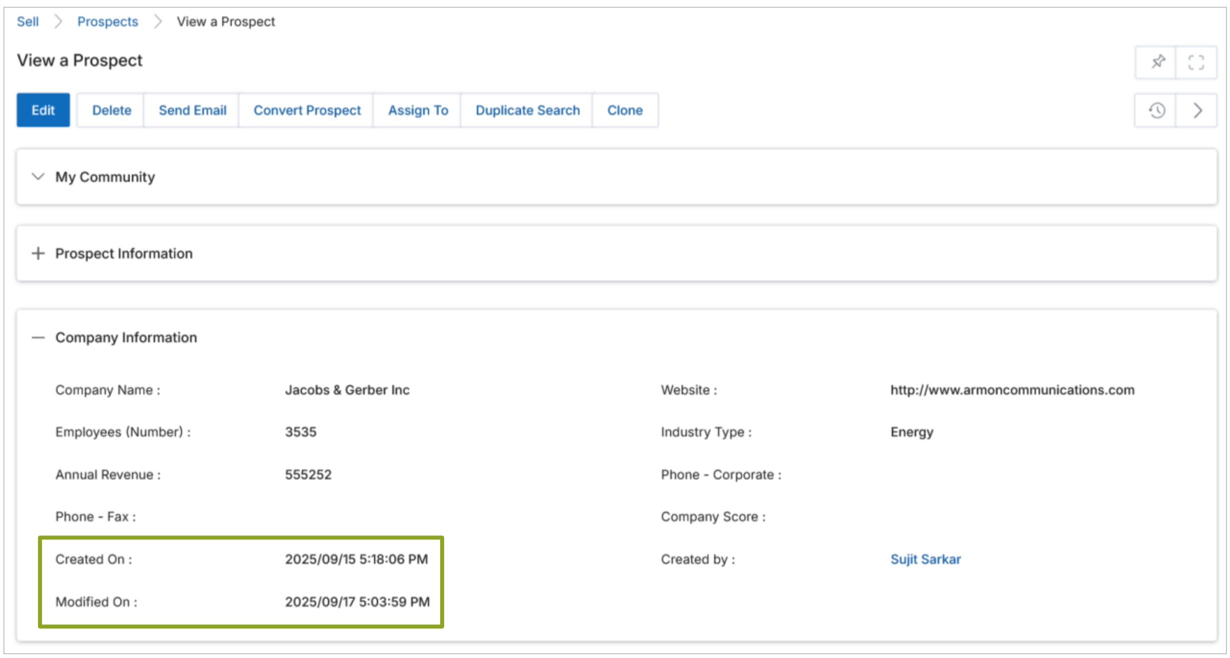


- Select the desired format and mark it as Active. Once activated, all other formats are automatically set to Inactive.





- In the following example, verify the changes by navigating to the Prospect Details page, where the selected date-time format is applied consistently and displayed correctly.



Summary of Features

The following functions are available through Access:

- Control all rights and rules that influence access control. Administrators can assign these rights and rules to users and roles.
- Make changes to user integration in business operations, such as changing the role or organizational unit.
- Change the access control for changed objects during runtime.

- Define the relationship between objects and users—for example, for organizational units, partner companies, areas, or product lines.

Note: Access initially provides users temporary full access to new objects that they create. When users save, rules-based access control for these objects is implemented and replaces the temporary full access.

