Record Visibility

Ext.prd.003.03 | 06.07.25

UPM 25.x

ZINFI Confidential & Proprietary
Shared Under NDA

Contents

 |

Preface

One of the major new features of UPM is **Record Visibility**, which organizations can use to restrict groups and users with specific privileges while providing better data security.

The privileges assigned regulate the functions a user can perform on records—both on specific records and in general. The access levels determine which records these privileges apply to. For example, although the privileges may include the capability to delete account records, a user's access level determines exactly which records the user can delete.

UPM includes four distinct access levels that are presented in order to increase authority.

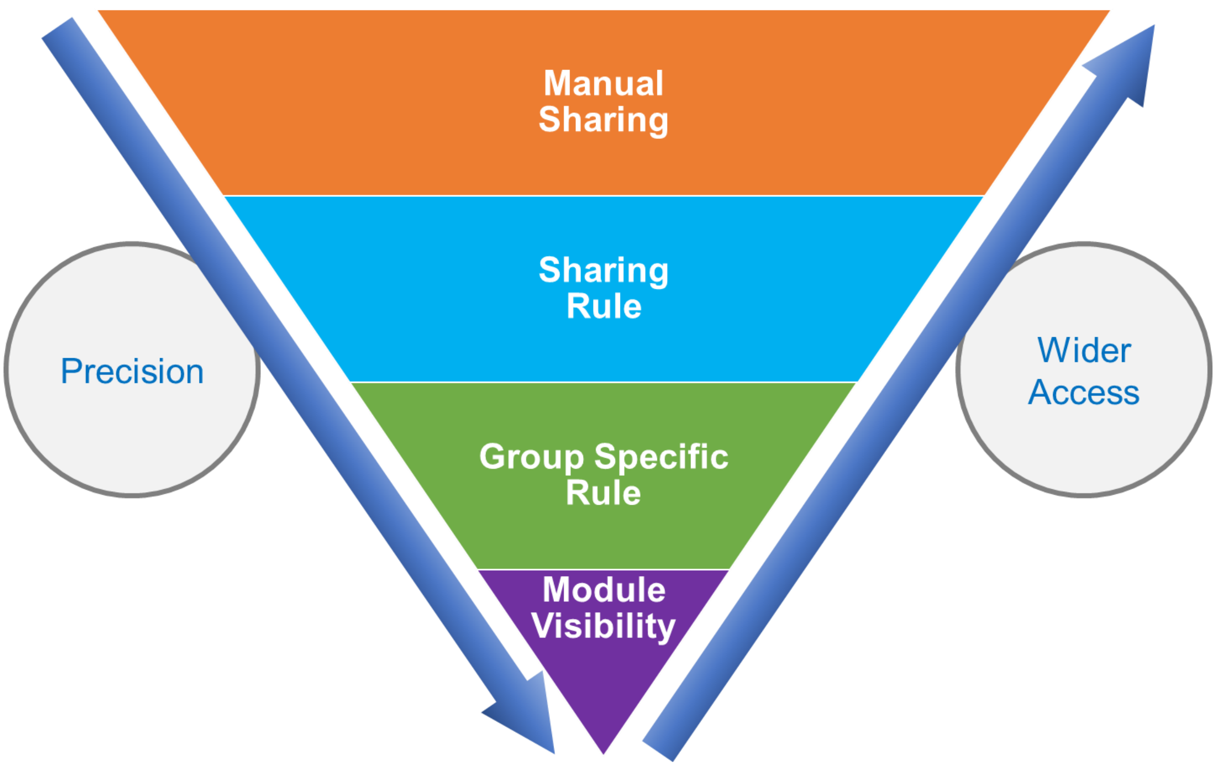


Figure 1: Hierarchical View of Record Visibility Management

Module Visibility

Module-level access is the most restrictive of all access levels. It provides read-only or read-write permission to users for each module residing in the application, as depicted in *Figure 2*.

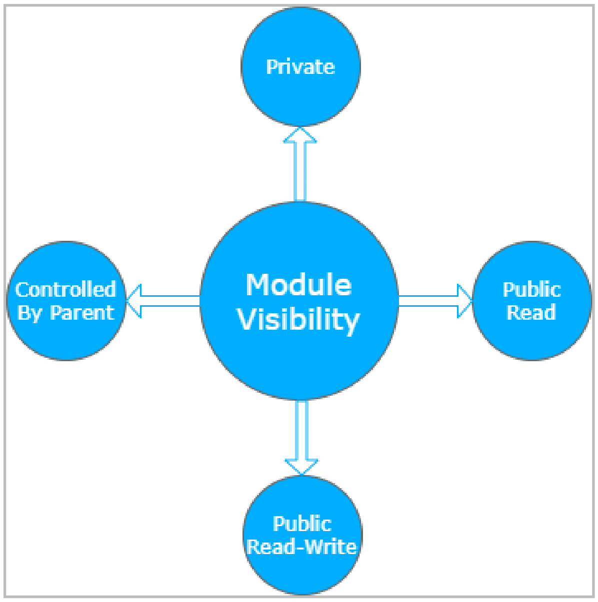


Figure 2: Module-Level Permissions

Private

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

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

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

If any module has this privilege and there is no rule for that module 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, a Group Specific Rule and Sharing Rule can also be applied for that module.

Public Read

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

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

  Note: It is possible to enable record modification by creating a custom rule and/or setting records to 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:

- View any user's created record.
- Edit any user's created record.

  Note: In the hierarchical image depicted in *Figure 1*, Module Visibility is at the bottom of the hierarchy. That means if there is Public Read-Write permission for any module, there is no need to set up any rule for that module.

Controlled By Parent

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

To make this clearer, let's consider the module Notes. When the module Notes is attached to the module Prospect (having Public Read permission), all users would be able to view every note attached by multiple users against a specific prospect. See *Figure 3.*

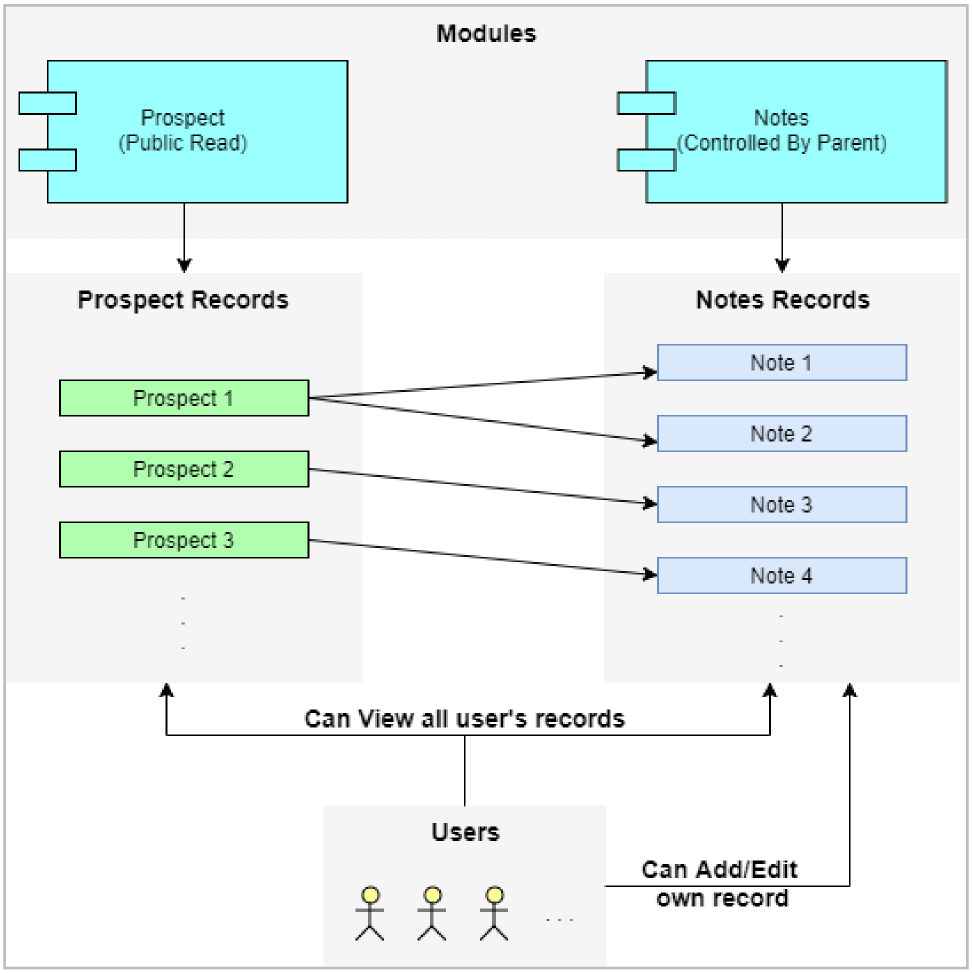
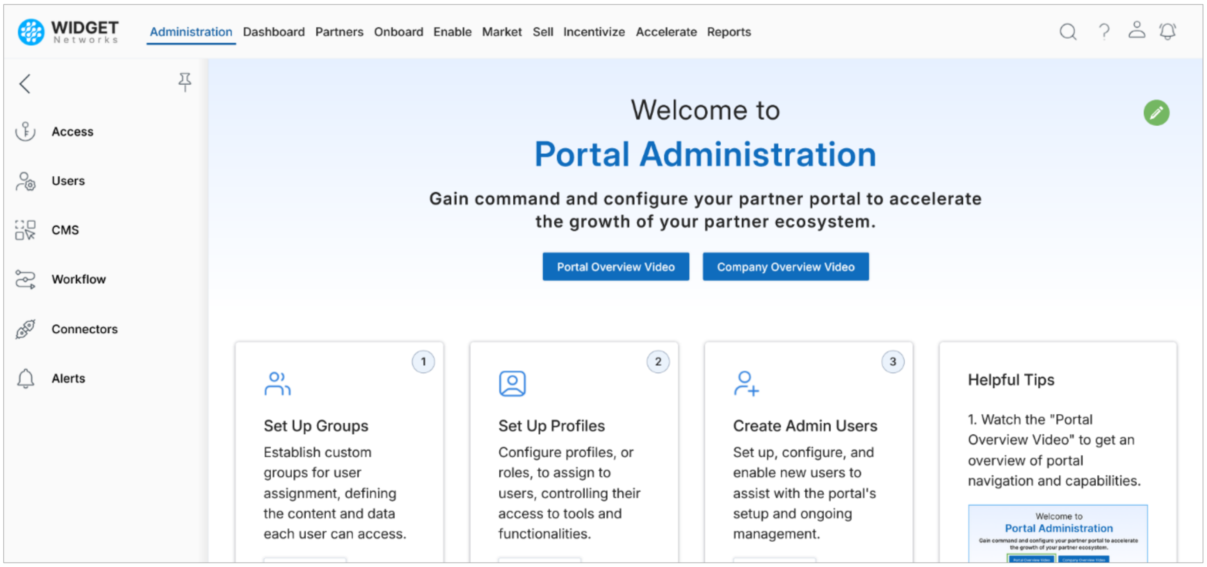


Figure 3: An Example of Controlled By Parent

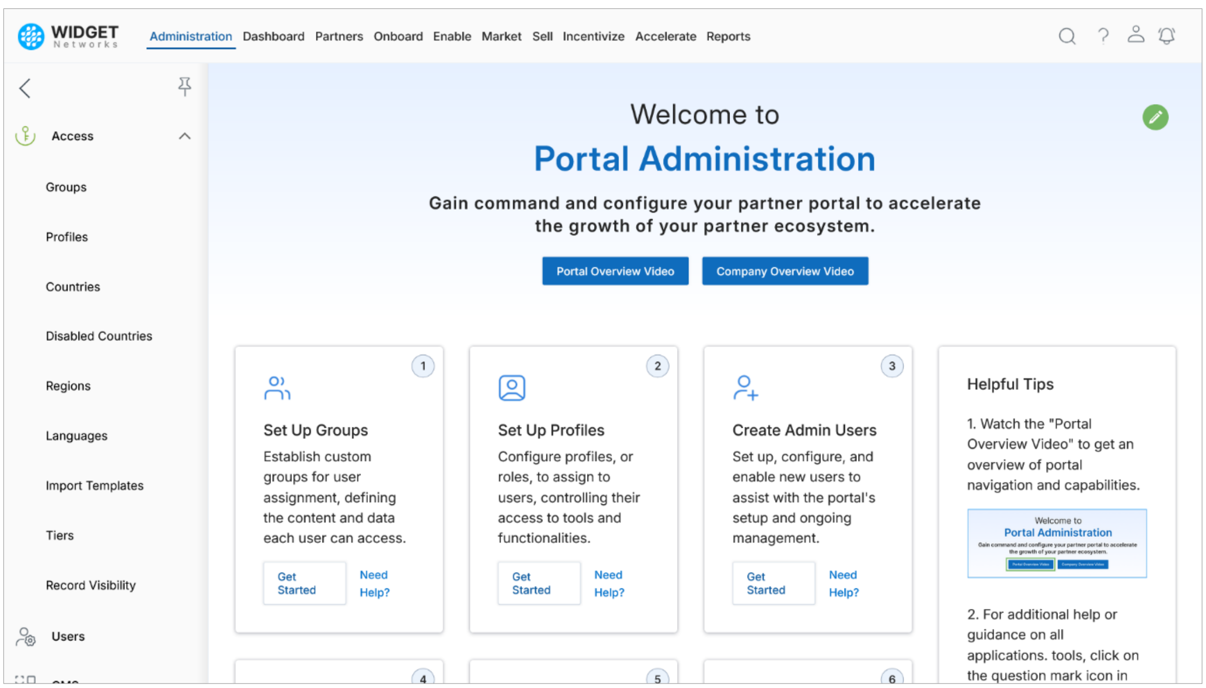
Setting Module-Level Access

Here are the steps for setting module-level access:

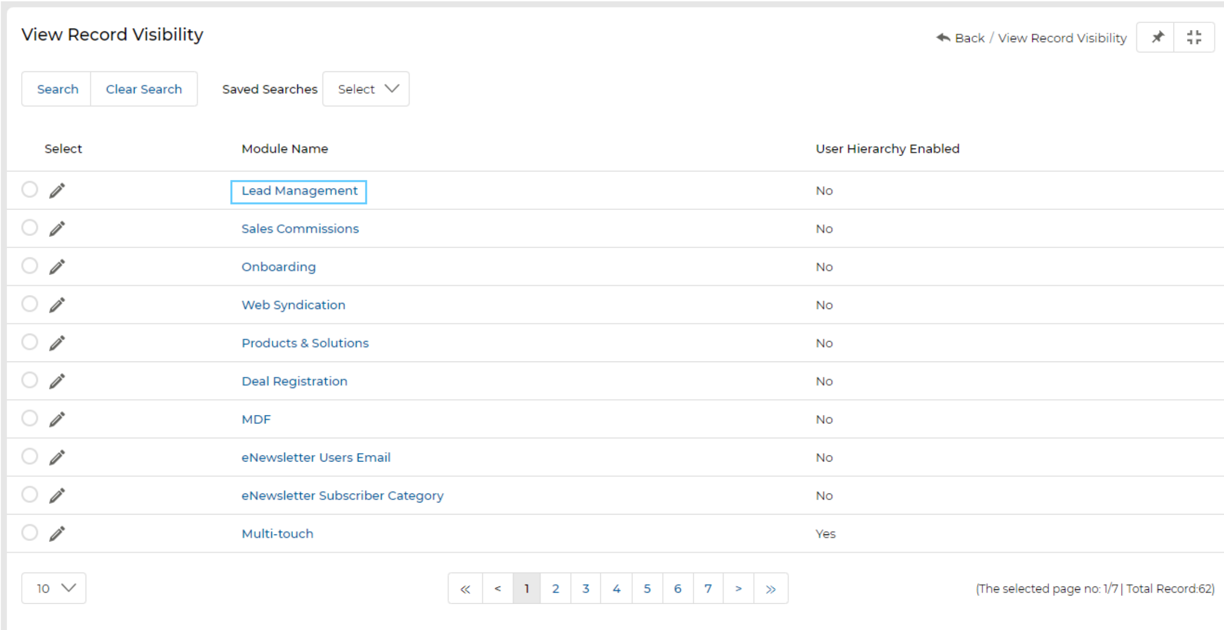
1. Click on **Administration**.



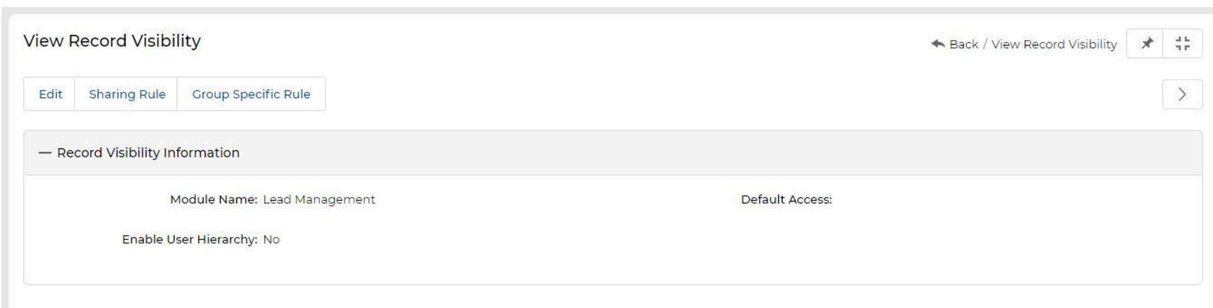
2. On the left panel, under **Access Management,** click on **Record Visibility**.



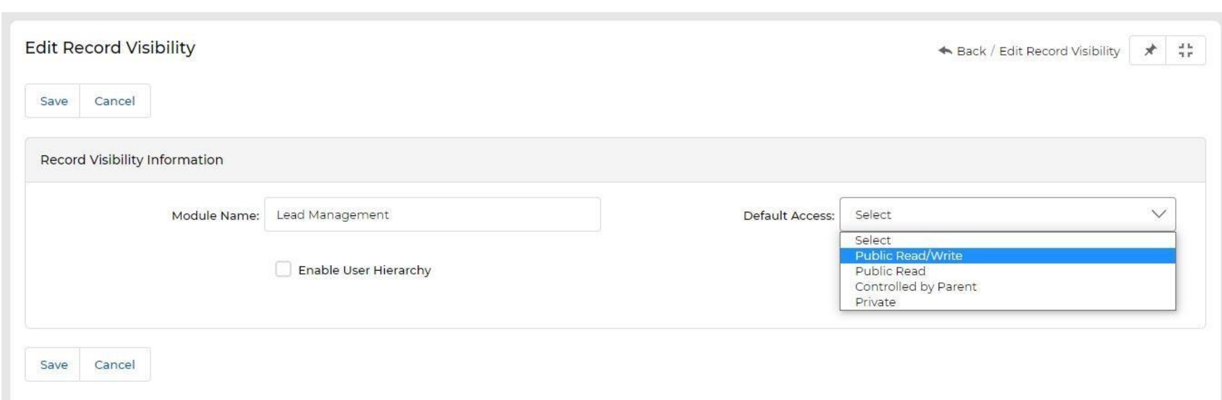
3. The listing page of **Rule Setup** opens. Now click on the module name to view the details page.



4. Once in the details page of the module, click on **Edit** to make changes to the module-level access for the selected module.



5. Choose the access level as necessary for each module by clicking on the pull-down menu in the **Default Access** column. Make your selection, and then click on **Save**.



User Hierarchy

User Hierarchy enables record visibility of a specific module vertically to its immediate members in the hierarchy chain either in read-only or read-write mode, depending upon that module's assigned accessibility level.

For example, consider the module Campaign Management (assigned access level: **Private**) as depicted in *Figure 4* below. User types depicted in the figure are channel marketing manager (CMM), channel partner administrator (CPA), channel partner (CP) and partner marketing consultant (PMC). When **User Hierarchy** is enabled for the module, CMMs will be able to view CPA users' and CP users' records in read-only mode (except its own record, which will be available in read-write mode) under the same vertical hierarchy chain. Similarly, CPAs will be able to view CP records and so on, but will not be able to view CMM records.

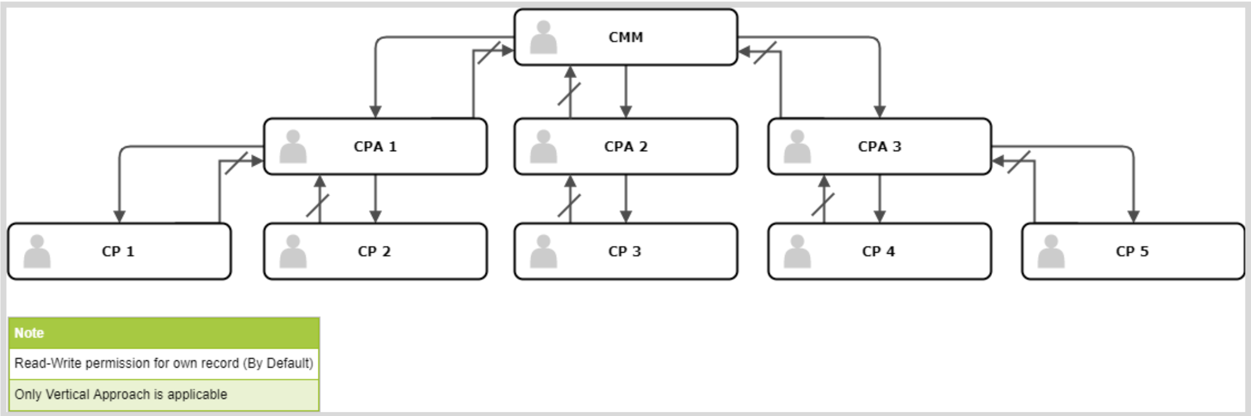


Figure 4: An Example of User Hierarchy

Group Specific Rule

Group Specific Rule is a vertical approach which 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 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.

.

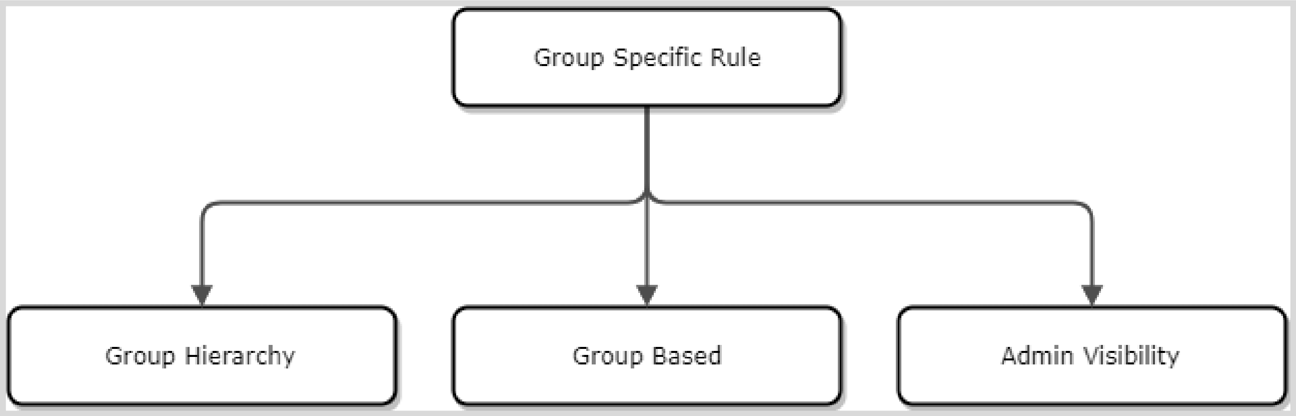


Figure 5: Group Specific Rule Categorization

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 the PMC group for the module 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.

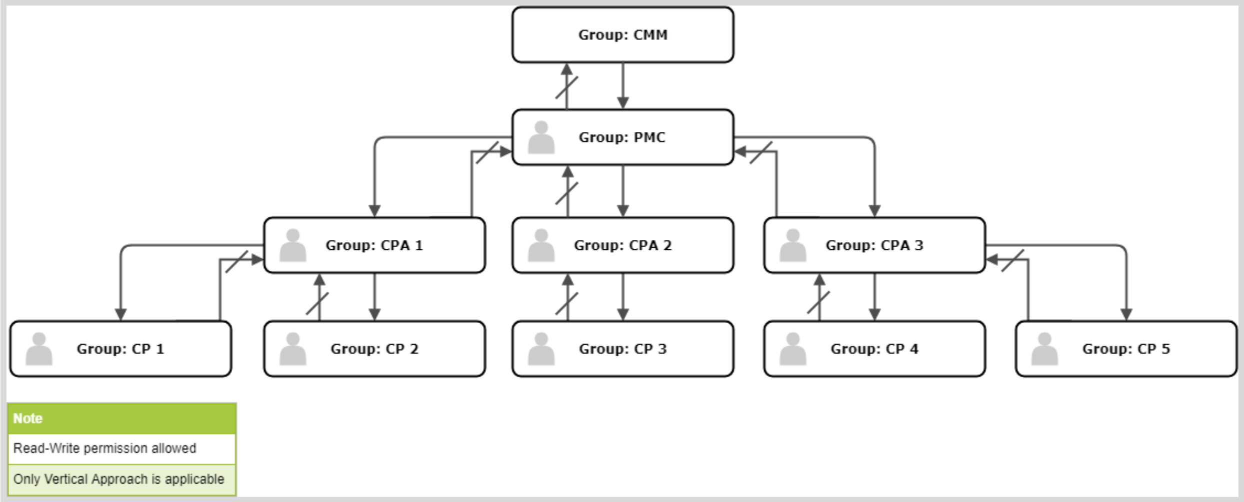


Figure 6: An Example of Group Hierarchy

Group Based

Group Based enables record visibility for its own group 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 module 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

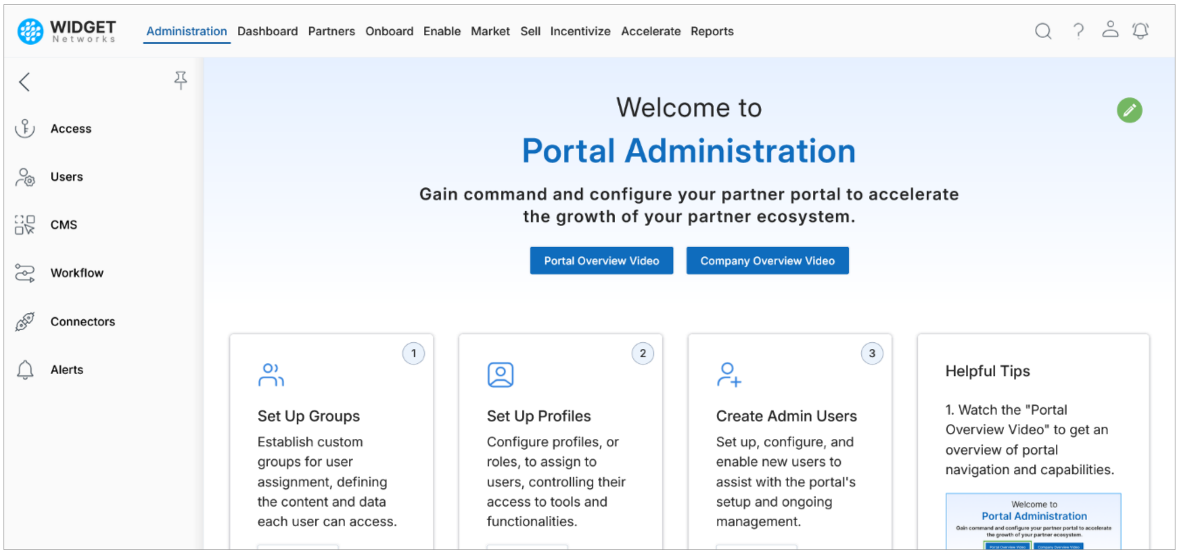
Admin Visibility is the highest authority given to any group under Group Specific Rule. This approach is implemented at both the module level and the group level. If any group has this privilege, then the users under this group can access all the records of that module with read-write permission.

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

Setting Group Specific Rule

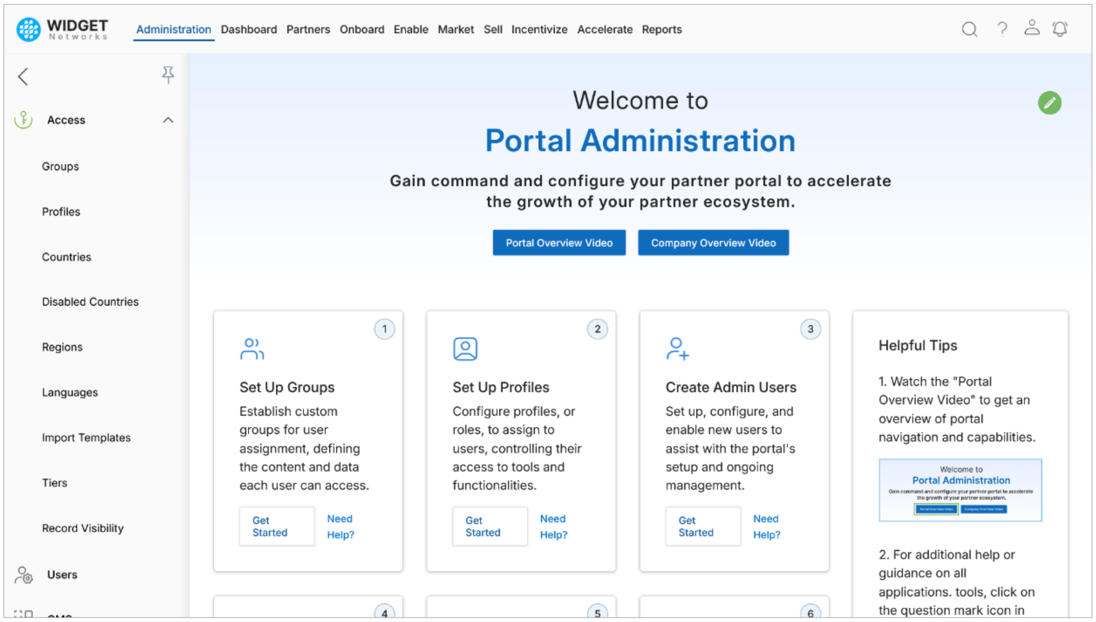
Here are the steps for setting Group Specific Rule:

1. Click on the top-right dropdown menu and choose **Administration**.

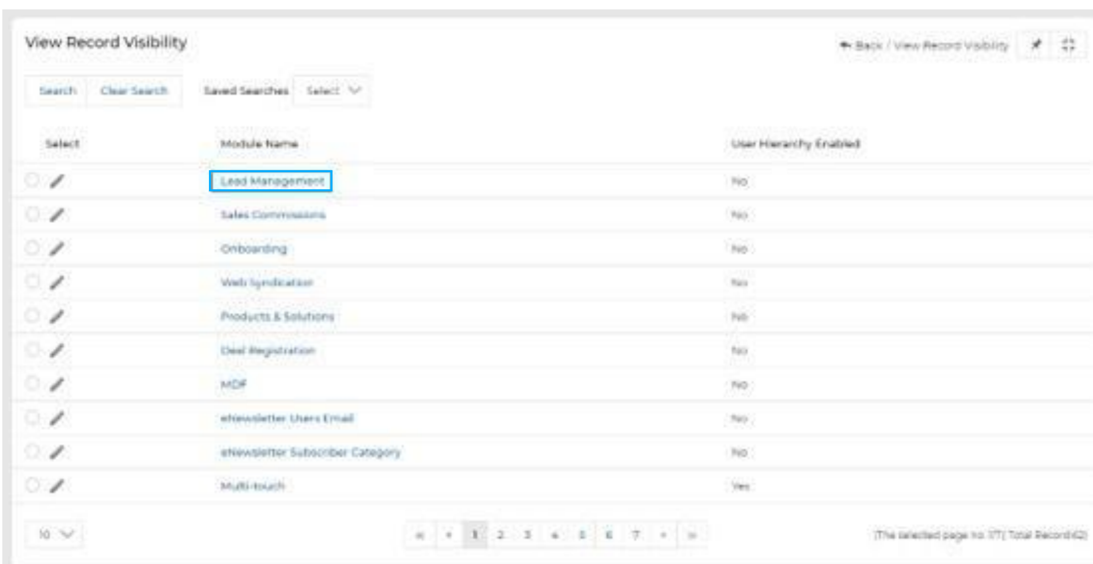


2. On the left panel, under **Access Management,** click on **Record Visibility**.

 |

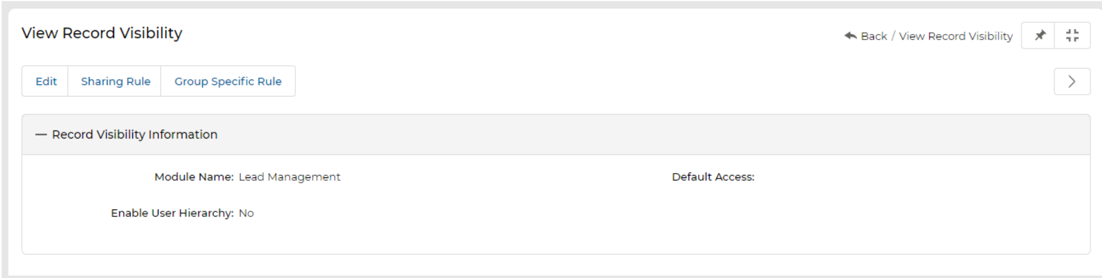


3. The listing page of **Rule Setup** opens. Now click on the module name to view the details page.

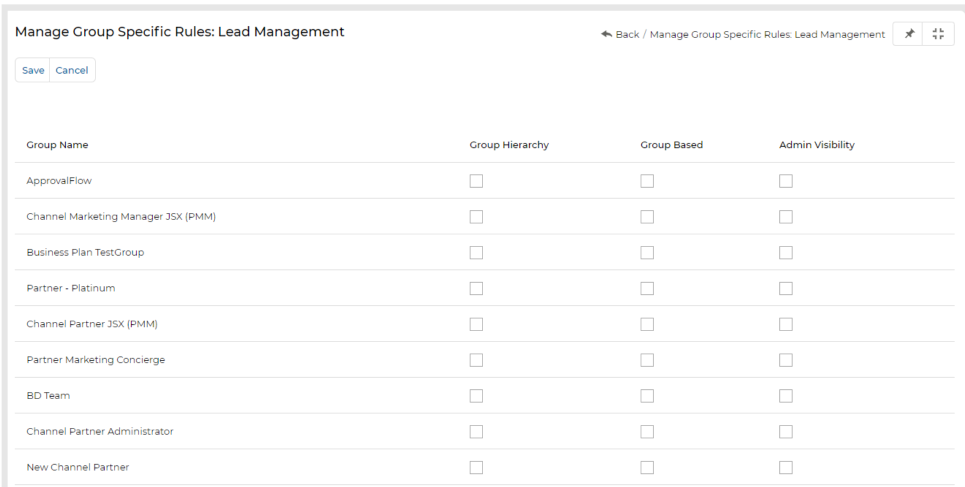


4. Once in the details page of the module, click on **Group Specific Rule** to make changes to the module-level access for the selected module.

 |



5. Select the rule category you want to apply, and then click on **Save**.



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. Sharing Rule is applied at the module level.

There are two types of Sharing Rule:

1. **Group To Group** assignment
2. **Criteria Based** assignment

Group To Group Assignment

This feature 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 module. Records can be assigned to multiple groups by creating multiple rules for that module.

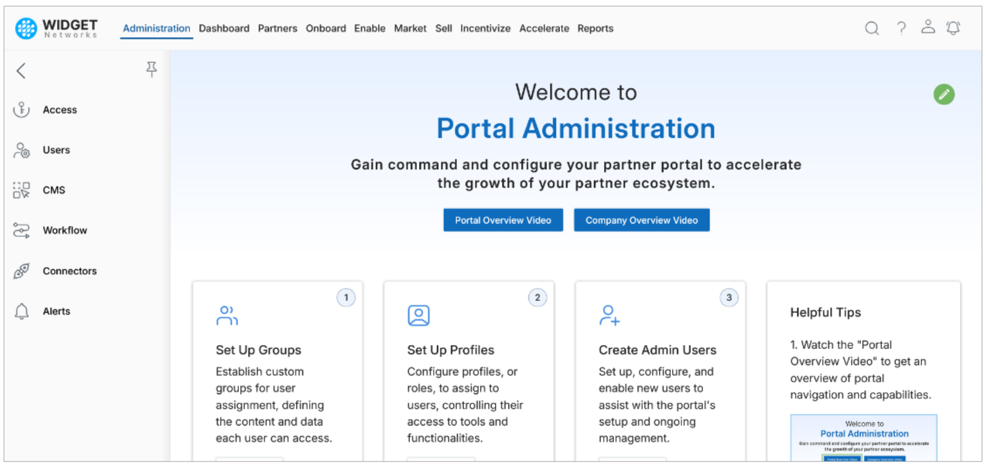
Criteria Based Assignment

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

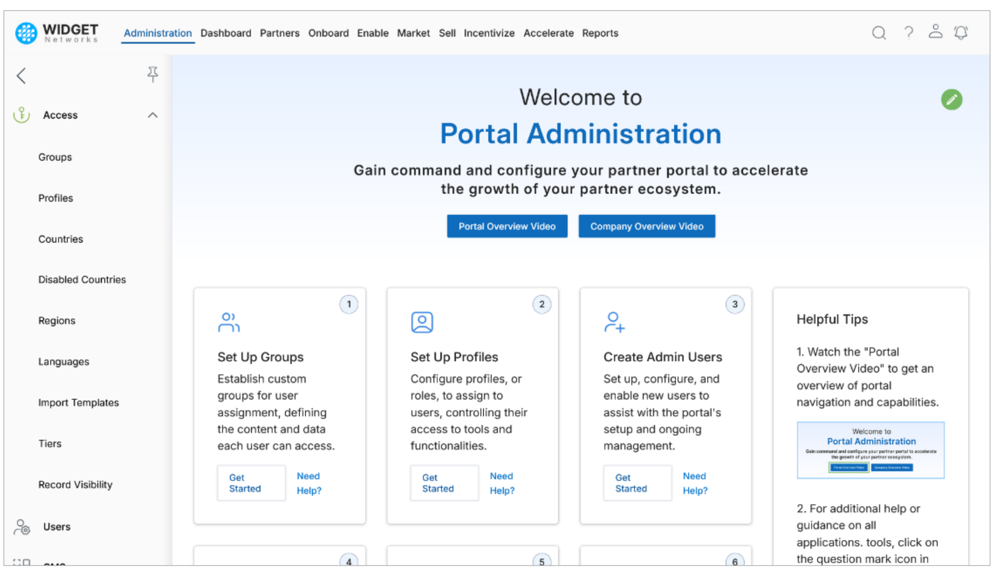
Setting Sharing Rule

Here are the steps for setting Sharing Rule:

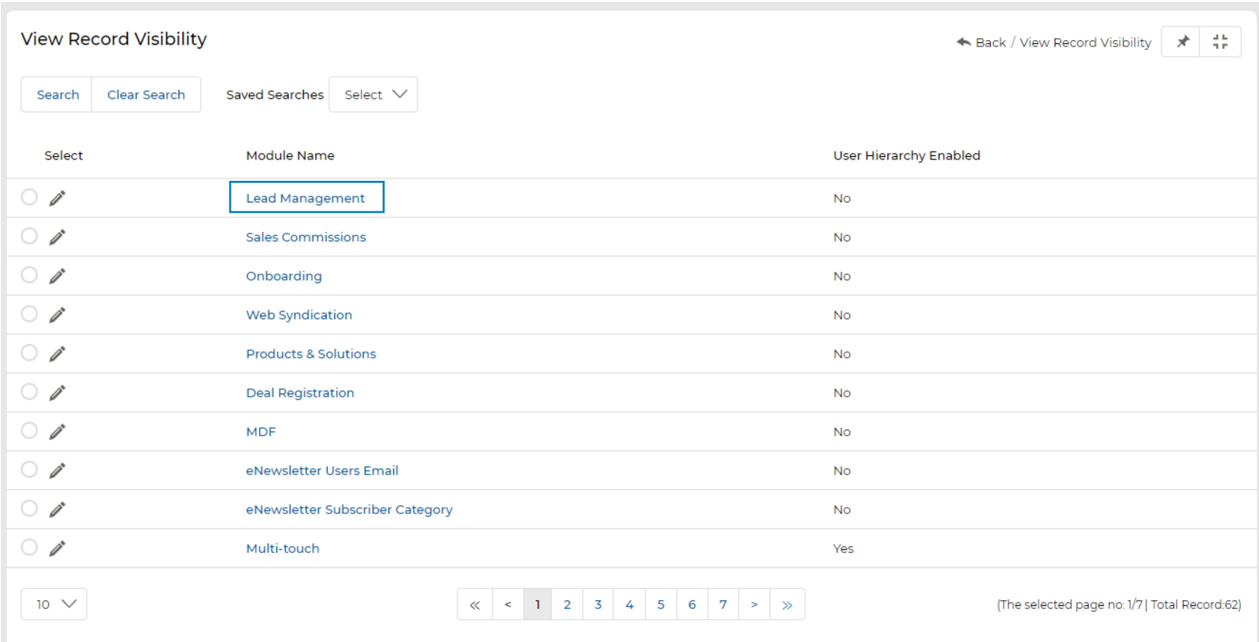
1. Click on the top-right dropdown menu and choose **Administration**.



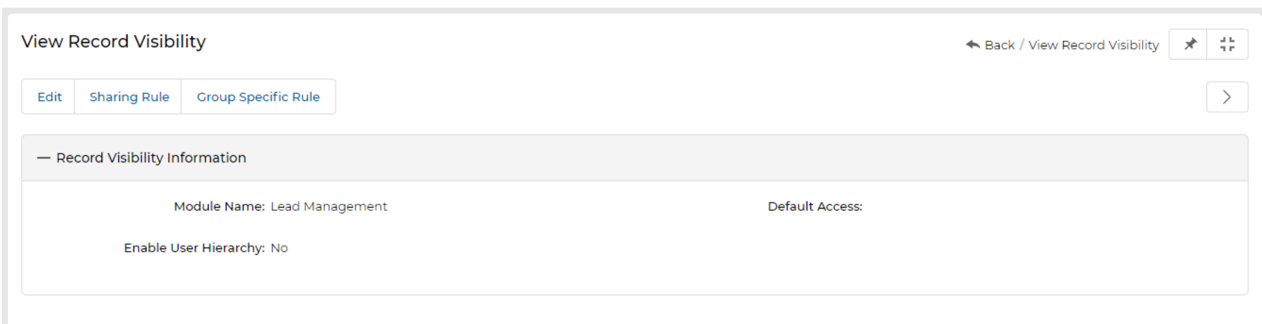
2. On the left panel, under **Access Management,** click on **Record Visibility**.



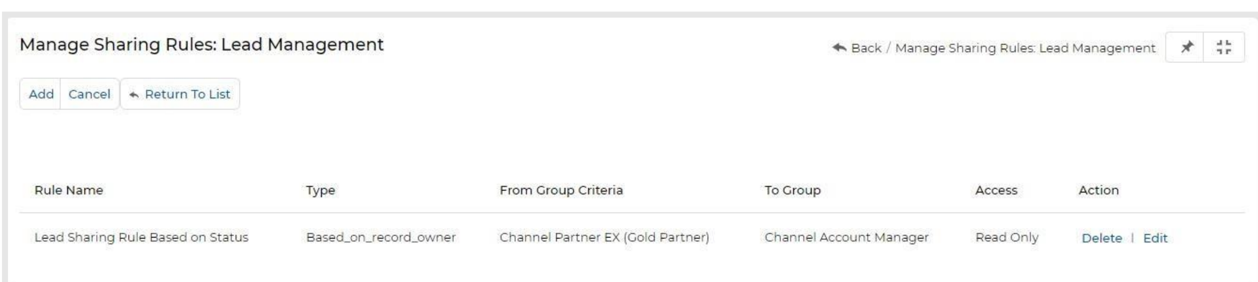
3. The listing page of **Rule Setup** opens. Now click on the module name to view the details page.



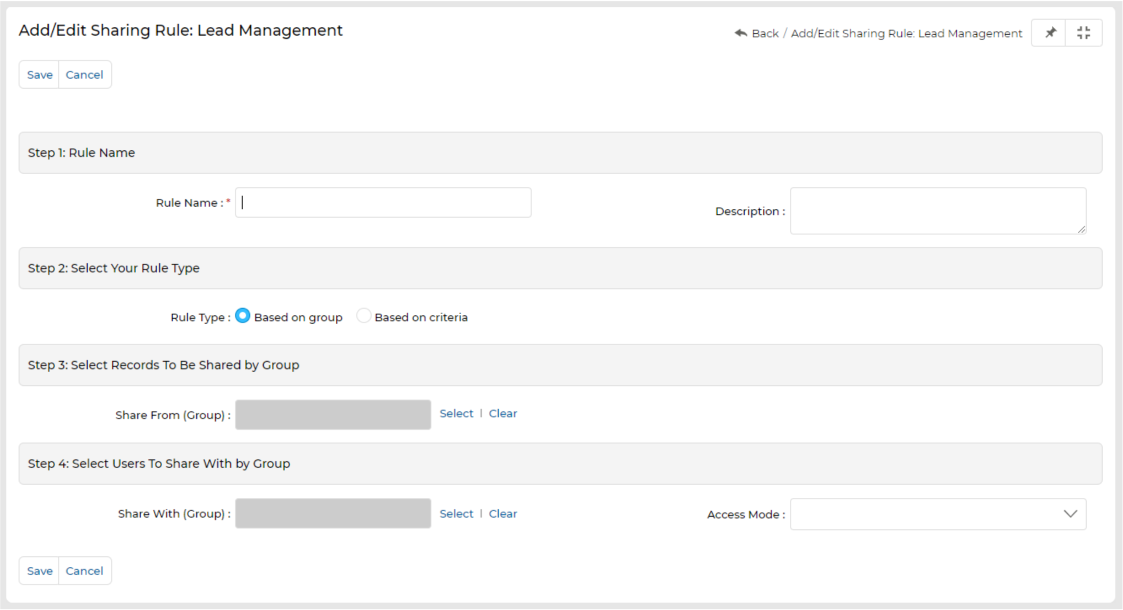
4. Once in the details page of the module, click on **Sharing Rule** to make changes to the module-level access for the selected module.



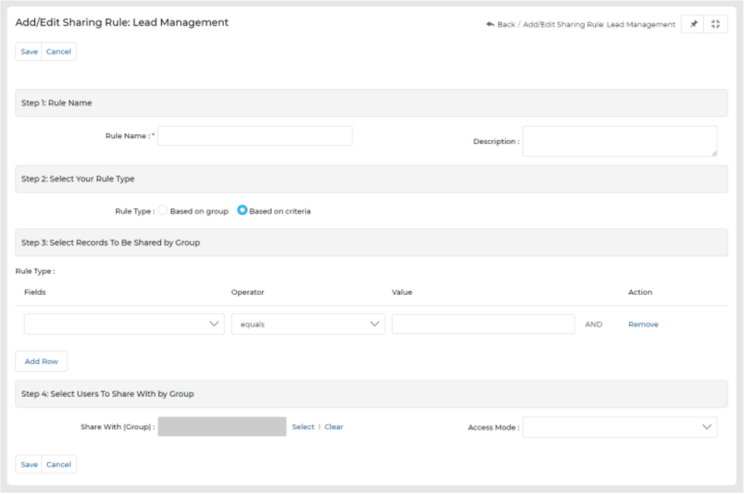
5. View the list of existing rules which have already been defined. Click **Add** to create a new rule.



6. For **Group To Group** sharing:
    a. Enter a **Rule Name**.
    b. Under **Rule Type** select **Based on group**.
    c. Select records to be shared at **Share from (Group)** and select users to share with at **Share with (Group)**.
    d. Choose the appropriate record access mode, then click on **Save** to create the rule.



7. For **Criteria Based** sharing:
    a. Enter a **Rule Name**.
    b. Under **Rule Type** select **Based on criteria**.
    c. Choose criteria from the available fields under that selected module.
    d. Select users to share with at **Share with (Group)** .
    e. Choose the appropriate access mode, then click on **Save** to create the rule.



 |

Manual Sharing

Manual Sharing is the broadest access provided in the hierarchical structure of Record Visibility Management.

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.

Modules for Which Record Visibility Can Be Implemented

Record Visibility can be implemented for the following zones and modules:

1. **Sales:** Prospects, Contacts, Accounts, Opportunities, Assets, Tasks, Notes, Documents
2. **Marketing:** Products, Campaigns, Assets, Emails, Web Syndication
3. **Profile:** Partner Prospects, Partner Contacts, Partner Accounts, User Management
4. **CMS** module for the top menu

Module-Level Activity

Module 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	✓	✓	✓	✓	✓	✓	✗

