insightsoftware

Identity Administration & Access Control (IDAAC) User Guide

Real Estate Manager

Version 26.1

Document Information

Notices

Copyright

Disclaimer

This guide is designed to help you to use the Real Estate Manager applications effectively and efficiently. All data shown in graphics are provided as examples only. The example companies and calculations herein are fictitious. No association with any real company or organization is intended or should be inferred.

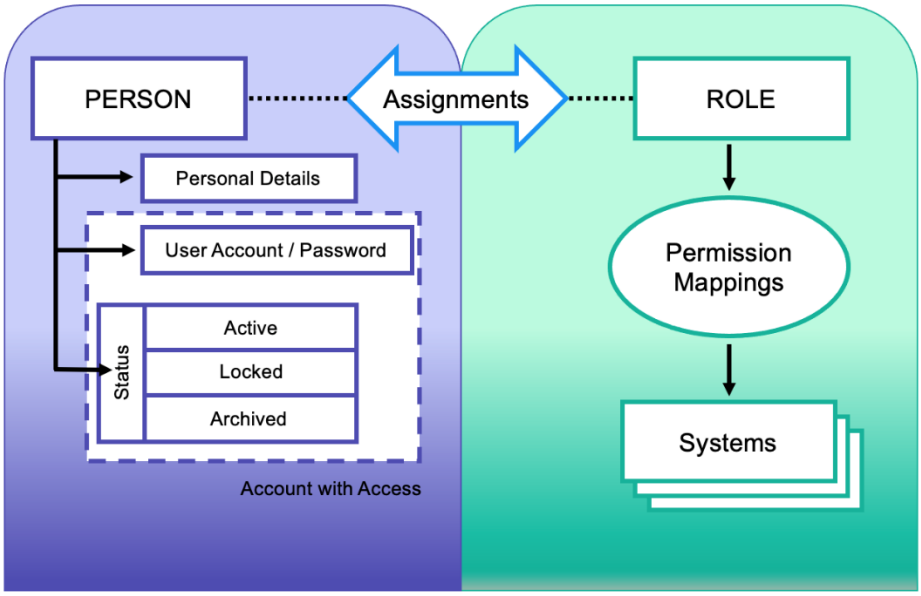
Contents

Identity Administration & Access Control (IDAAC)

Overview

IDAAC (Identity Administration & Access Control) is the centralized management application which controls access to LeaseAccelerator's Real Estate Manager.

Access control within IDAAC is split into two main divisions: users and roles.



Manage Users

The Manage Users feature allows individual users to be set up and managed. This includes actions such as adding a user, defining their personal details (i.e. name and email), enabling/disabling users, assigning them to roles, and resetting forgotten passwords for existing users.

Manage Roles

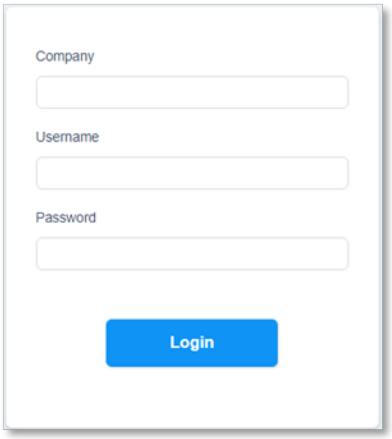
The Manage Roles feature is where roles are defined and managed. Each role has its own set of permissions, which define what users can and cannot do. Users are then assigned to the appropriate roles.

Accessing IDAAC

Logging In

Follow the steps below to log in.

1. Go to https://re.leaseaccelerator.com/idaac/.
2. Enter your **Company, Username, Password**, and then click **Login**.



3. If this is the first time you are accessing IDAAC, you will be prompted to set a new password. Enter and confirm the password.
4. You are taken to the IDAAC home page.

Logging Off

To log off, click **Log Off** in the top right corner of the page.

Forgot Password

If you forgot your password, contact your IT Department or in-house IDAAC representative to have the access issues resolved.

Manage Users

The Manage Users feature allows individual user accounts to be set up and managed.

This includes such actions as:

- Adding a user
- Defining their personal details
- Enabling/disabling users
- Assigning roles
- Resetting passwords

Add Users

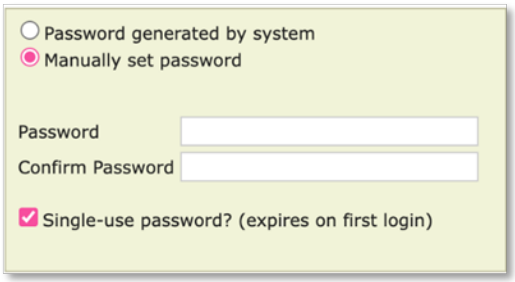
Follow the steps below to add a new user.

1. Click **Manage Users**.
2. Select the **Add Users** tab.
3. Enter details for:
   a. **First Name**
   b. **Last Name**
   c. **Email Address**
   d. **Username**

> **Note:** Note: It is recommended that all usernames and email addresses be entered in lowercase lettering.

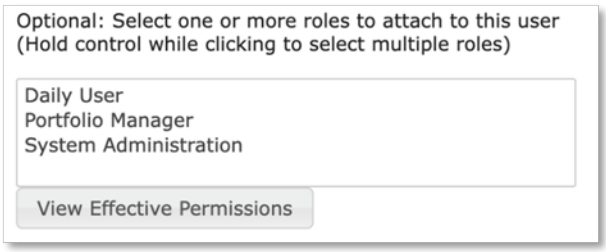
4. Choose the desired option for password creation.

> **Note:** If you choose to manually set a password for the user, enter and confirm the password in the fields that appear.



5. Select one or more roles to attach to this user.

> **Note:** To select multiple roles, hold Control while clicking each role.



6. Click the **Add User** button.

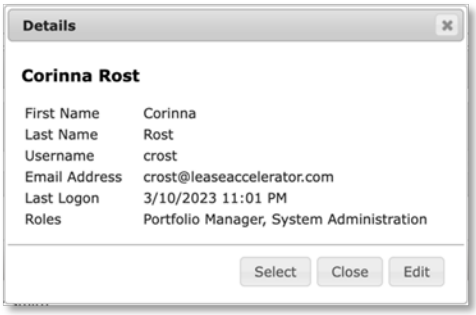
Editing a User

Once a user has been created, you may edit the details for that user within the Manage Users workspace, including their personal details and assigned roles. By editing a user's record, you may also update their password, either with a permanent password or a single-use password that will expire after the first log in.

1. Click **Manage Users**.

2. On the **Find Users** tab, search for the user's name. You may choose to apply access or keyword filters.

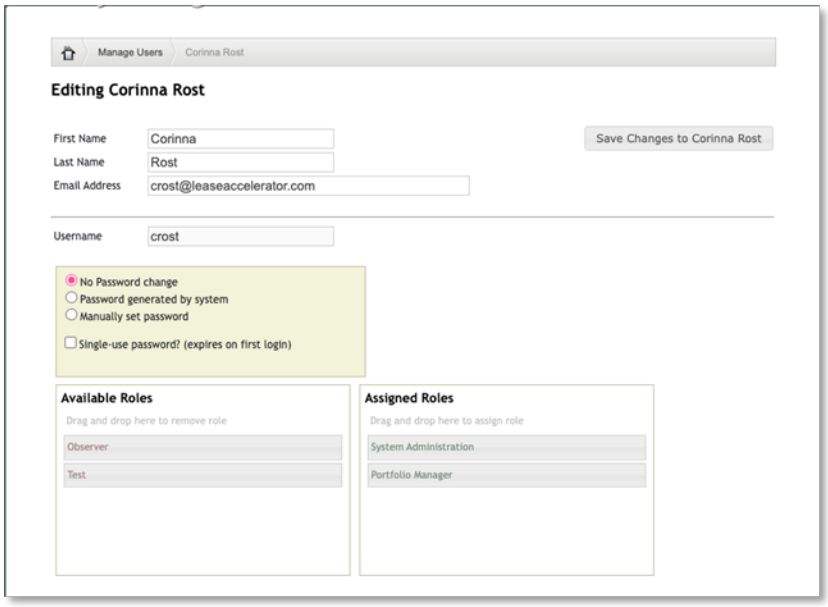
3. Once the user is located, click on their name and in the Details pop-up, select **Edit**.



4. You may update a user's First Name, Last Name, Email Address, and Username.

5. You may provide a new password, either permanent or single use.

6. You may also add or remove Assigned Roles by dragging and dropping desired role to/from the **Assigned Roles** box.



7. Once all updates have been made, click the **Save Changes** button for that user.

Account Statuses

Each user account will have a status, which gives specific information about the state of the user record.

The list of status types includes:

- **Active** - the user has current access granted.

- **Disabled** - the user's access has been revoked.

- **Archived** - the user record has been archived, thereby visibly removing it from all systems without actually deleting it.

- **Locked** - the user is not currently permitted access. This may be due to a violated security requirement such as too many incorrect login attempts or it could be due to a manual lock that has been placed on the account.

To change the status of any user, you must use the Batch Action functionality.

Batch Actions

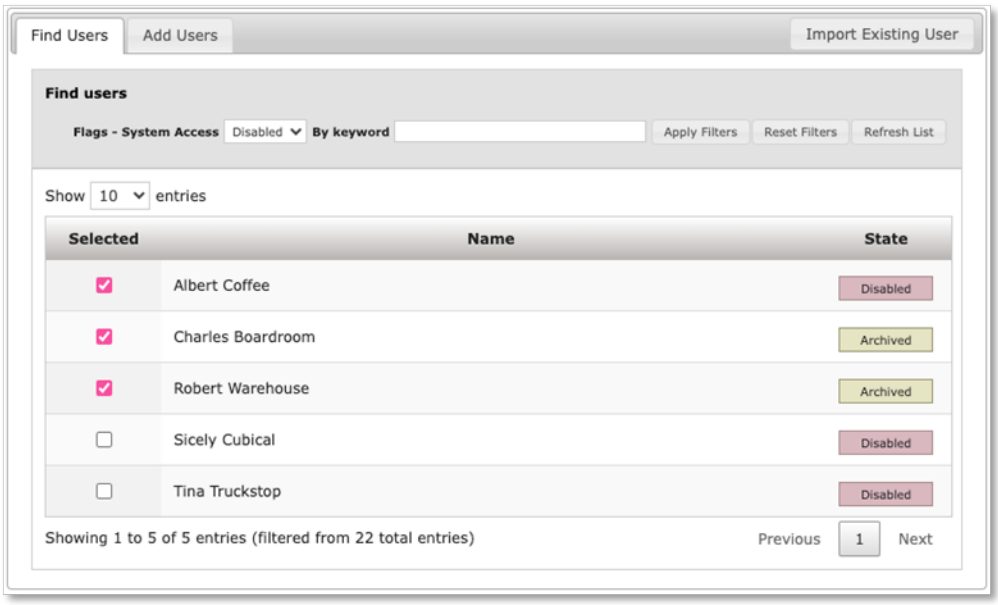
Batch Actions allow user updates to be performed on multiple user accounts simultaneously. This can be a useful time saver when an identical, repetitive action needs to be applied to a pool of users.

Available Batch Actions

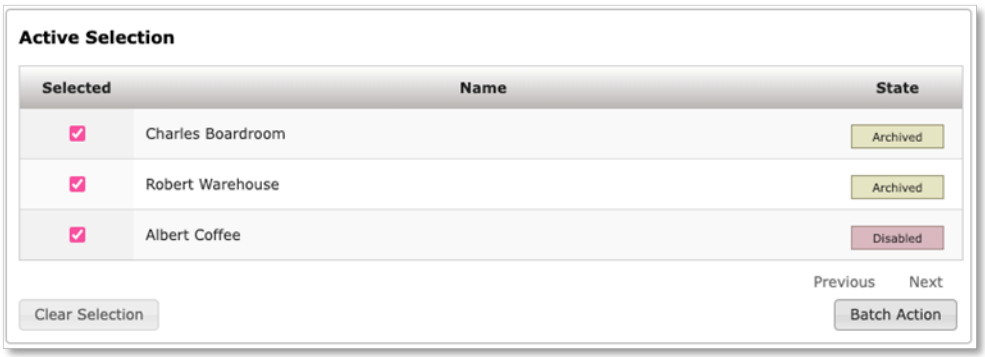
- **Assign Roles**: Assign the same roles for assignment to a group of users.
- **Remove Roles**: Remove assigned roles for a group of users.
- **Send an Email:** Compose and send an email to a group of users.
- **Lock Password**: Disable all system access by locking user accounts.
- **Unlock Password:** Restore all system access by unlocking previously locked accounts.
- **Re-enable Account:** Restore system access to users that were previously disabled.
- **Disable Account:** Prevent system access but retain user records.
- **Activate:** Restore any previously archived user accounts.
- **Archive:** Disable all system access and remove their visible presence from the system, meaning they cannot be assigned to any asset or contract or have any associated tasks assigned to them.
- **Update Password**: Update password for selected group of users, by either assigning an individual password manually or having the system generate and email a secure password.

1. Click **Manage Users**.
2. On the **Find Users** tab, search for a group of users by applying access or keyword filters.

3. Once desired users are located, click the **checkbox** to the left of the names.

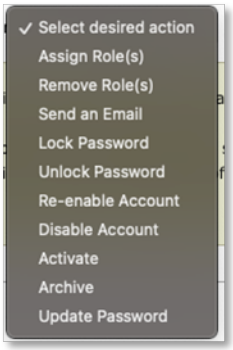


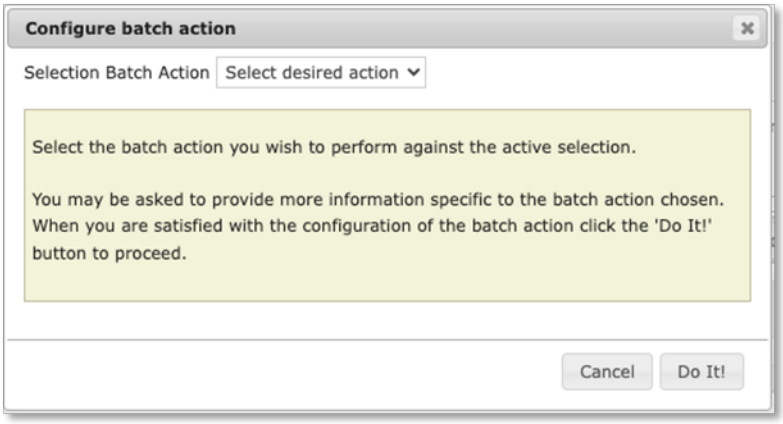
4. You will see the names appear in the Active Selection section.



5. Click **Batch Action**.

6. In the Configure batch action pop-up, select the desired action from the drop-down.



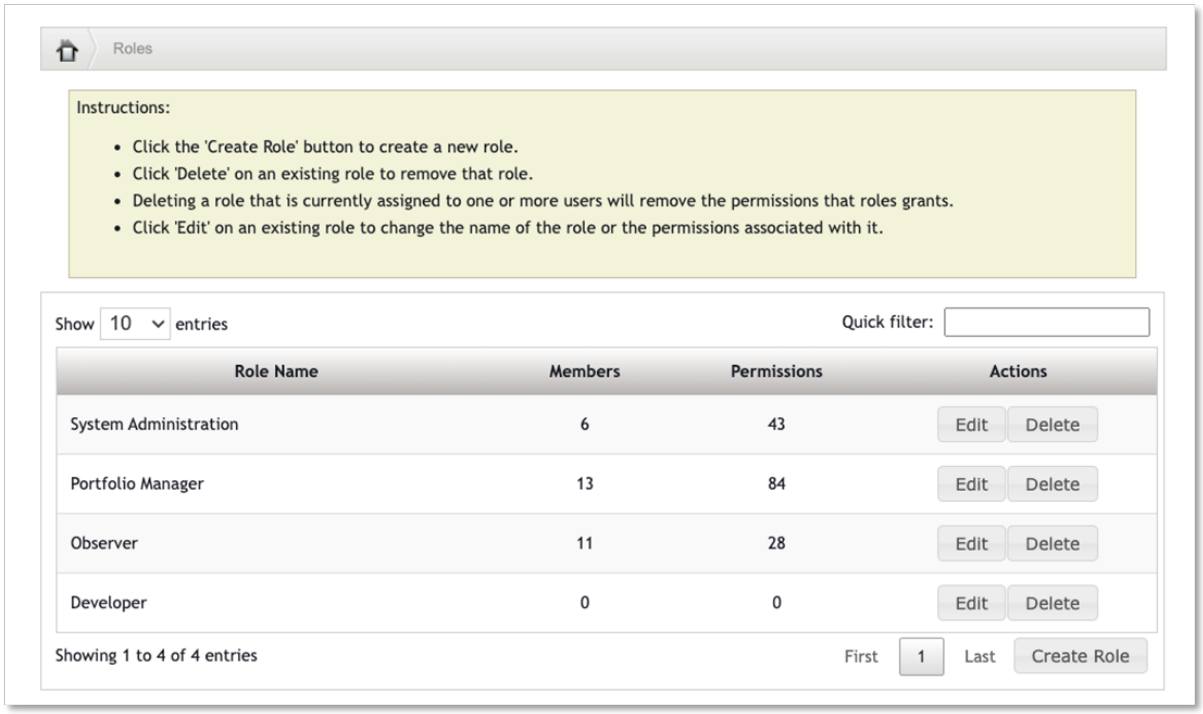


7. Click **Do It**!
8. Click **Confirm** in the confirmation pop-up.
9. Click **Close** in the Results pop-up.

Manage Roles

Access permissions for the various systems are managed within IDAAC by creating roles. Each role has its own set of permissions which defines what users can and cannot do. Individual users are then assigned to roles as needed.

The Roles workspace shows the names of all the roles currently defined within IDAAC. For each role there is a count showing the number of users that have been granted this role and the number of permissions associated with the role.



Creating a New Role

IDAAC allows for the creation of customized access roles with Real Estate Manager by giving the ability to choose which permissions a role is allowed. Within the Manage Roles workspace, there is a tree of functional areas within Real Estate Manager. Permissions are assigned by clicking the checkbox next to each desired functional area.

Some functional areas, such as Asset Management, require either **Condition-Based** or **Direct** access permissions to be defined.

Condition-Based Access Permission

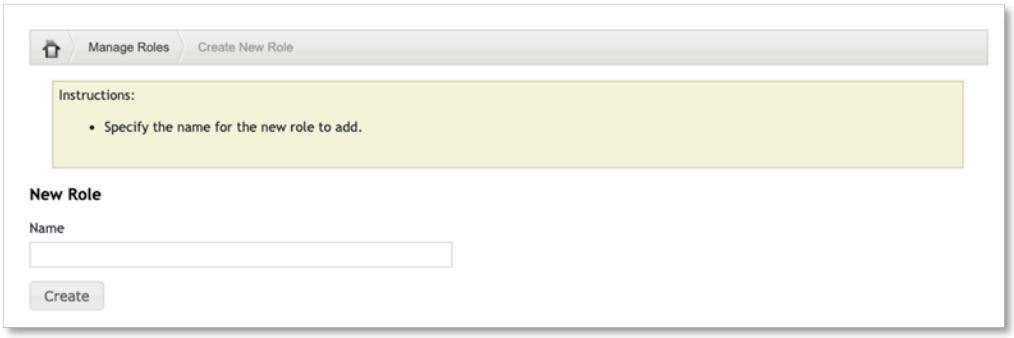
Condition-based access permission grants users access to certain logical entities on the basis of filter criteria.

Direct Access Permission

Direct access permission assigns access specifically to individual logical entities. This approach gives finer-grain control but at the expense of future flexibility should portfolio details change or be added to.

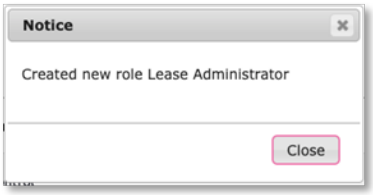
To create a new role, follow these steps:

1. Click **Manage Roles.**
2. Within the Roles workspace, click **Create Role**.
3. Enter the name of the new role in the **Name** field.



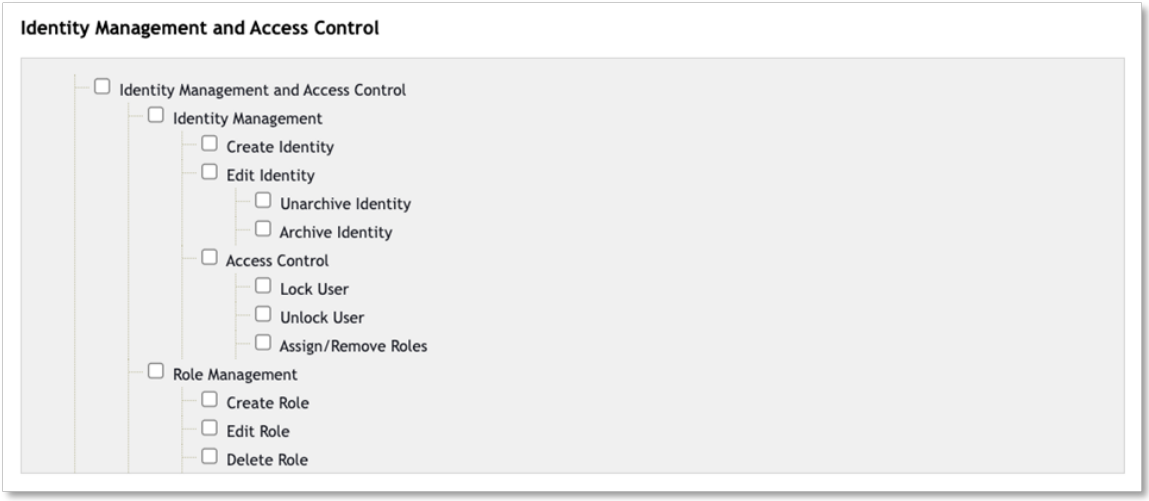
4. Click **Create**.

5. Click **Close** on the Notice pop-up that tells you a new role has been created.



6. Under Role Permissions, start with the **Identity Management and Access Control** section and check the box next to any permission this role should have. Checking the top box in the tree does not automatically check any nested boxes. You must check individual boxes if you want to add those permissions to the role.

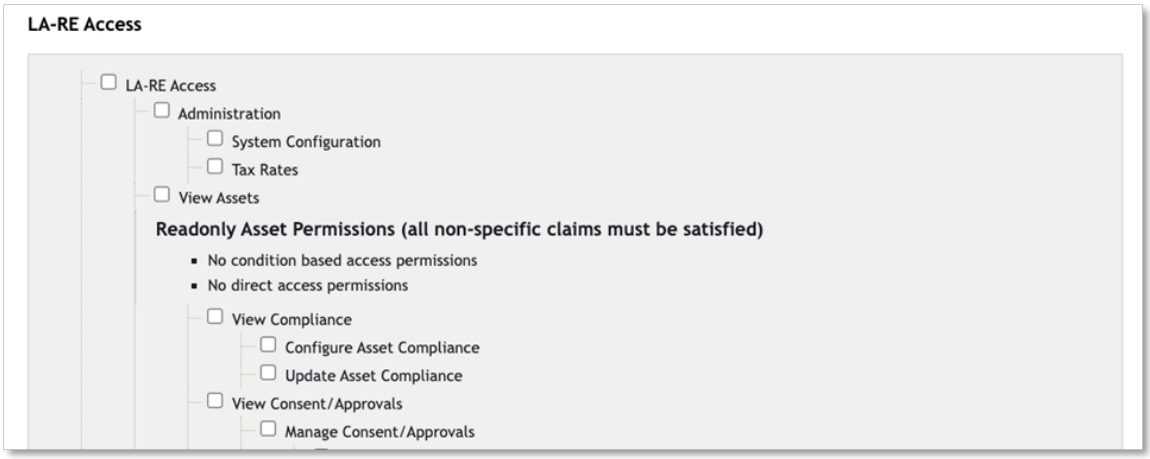
7. For information on each functional permission, please see the Permissions Index at the end of the user guide.



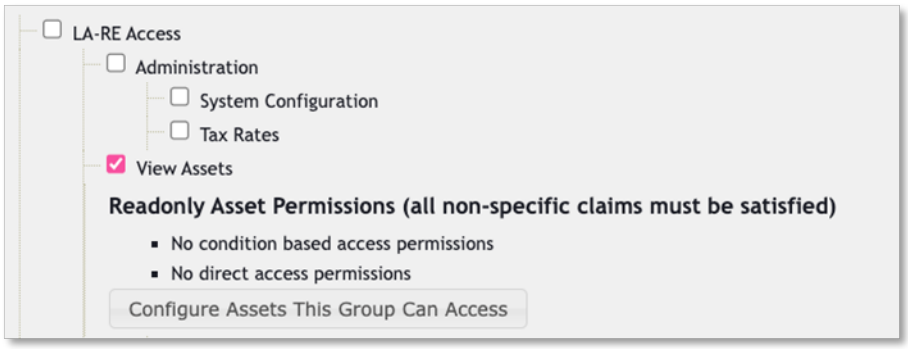
8. Now look at **LA-RE Access** and check the box next to any permission this role should have.

9. Remember, checking the top box in the tree does not automatically check any nested boxes. You must check individual boxes if you want to add those permissions to the role.

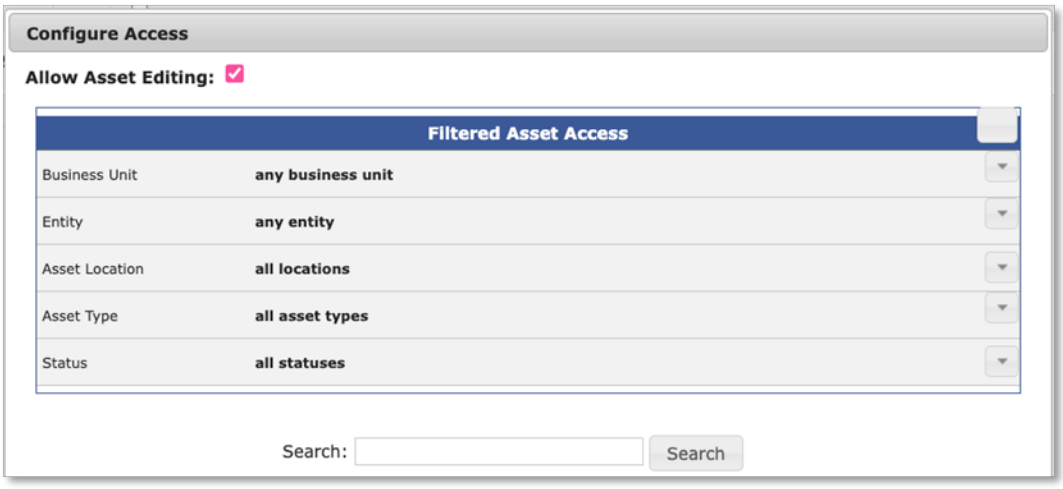
10. For information on each functional permission, please see the Permissions Index at the end of the user guide.



11. If the role should have permission to view assets, check the **View Assets** box and the **Configure Assets This Group Can Access** button will appear.



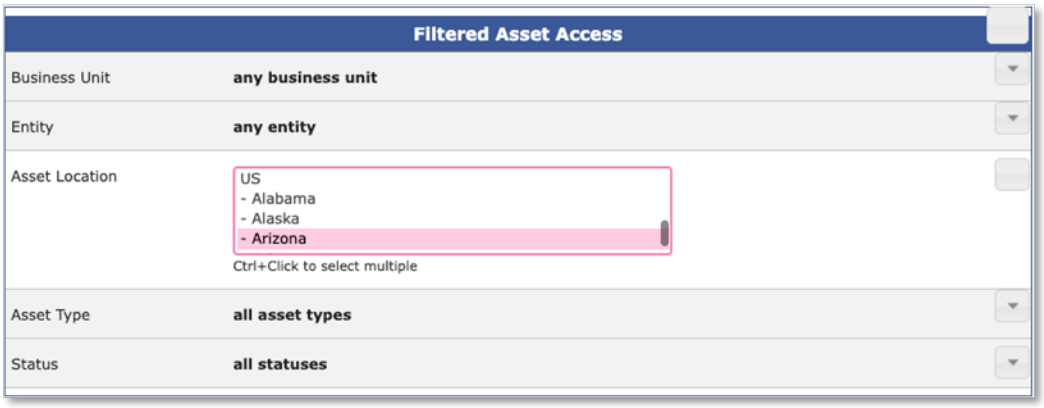
12. Click **Configure Assets This Group Can Access** and in the Configure Access pop-up, start by indicating whether this role will be able to edit assets. If yes, check the box next to **Allow Asset Editing**.



13. Next, if you are using condition-based access, you can use the filters in the Filtered Asset Access section. You can grant access by Business Unit, Entity, Asset Location, Asset Type, or Asset Status. By using condition-based access, the role will have access to existing assets along with any future assets added to the selected filter.

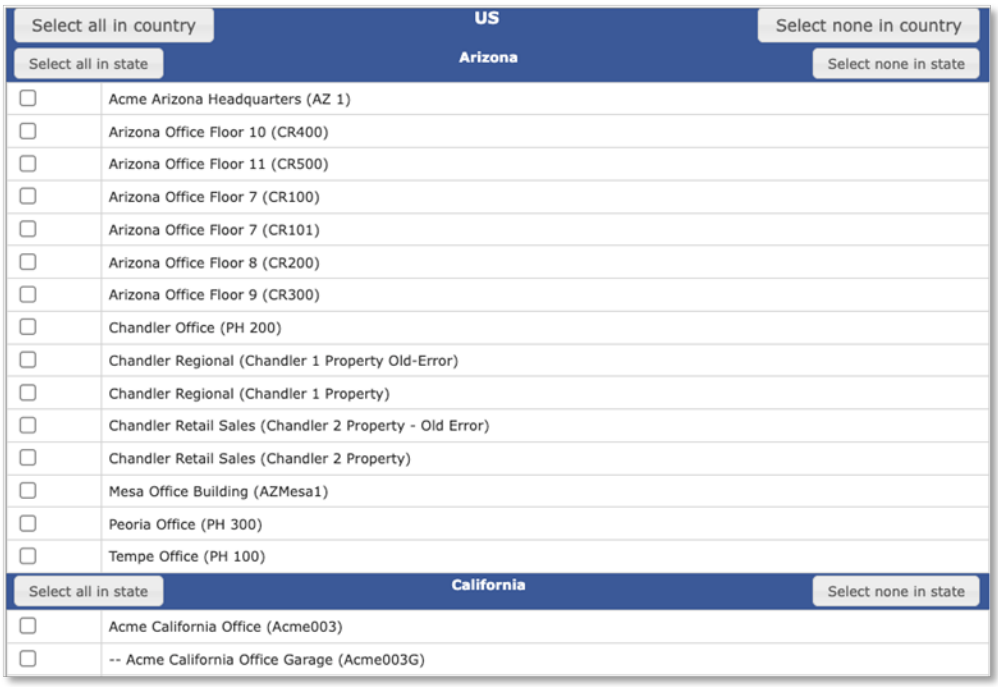
14. For example, if you grant access by Asset Location and select a particular state, the role would have access to all assets currently in the state and any assets added to that state in the future.

> **Note:** While you may select more than one filter for access, the more levels you choose, the stricter the access control will be.



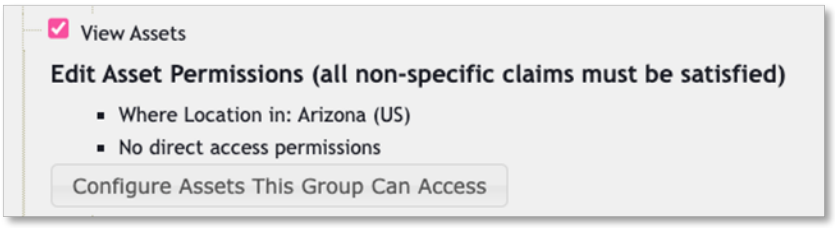
15. If you would like to use direct access permission, then check boxes in the individual country sections. By checking individual assets, the role will only have access to those assets and if any are added in the future, the role will not have immediate access to them. The role would need to be updated. This allows for the strictest access control.

> **Note:** Even if you **Select all in country,** when a new asset is added, the role will have to be updated to have access to the new asset.



16. Once all relevant boxes have been checked, click **Okay** at the bottom of the pop-up.

17. The Asset Permissions will be updated to reflect your selections.

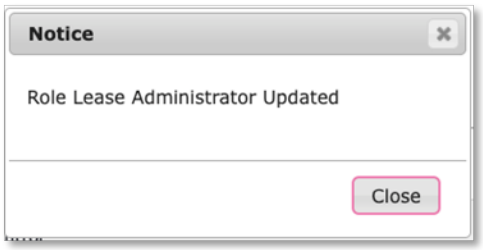


18. Returning to the Permissions workspace and the functional tree, continue to check boxes for permissions to functions that this role should have access to including viewing/managing the following:

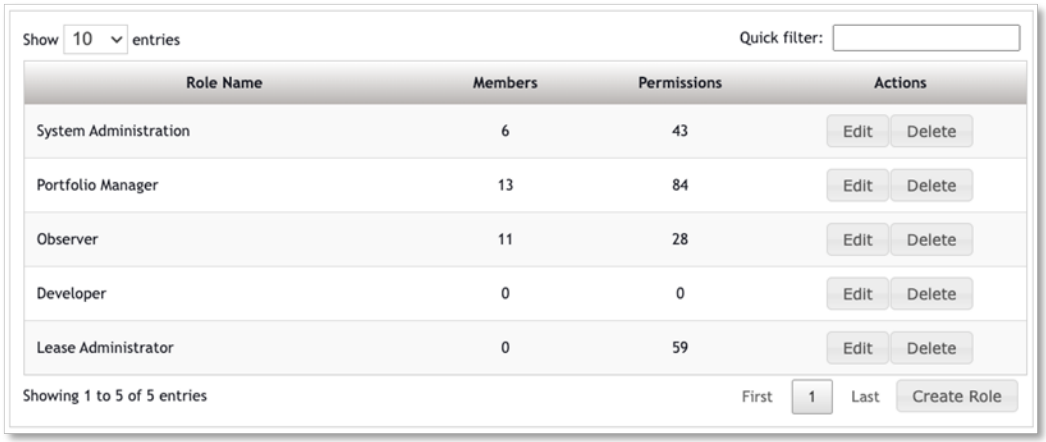
    - Compliance
    - Consent/Approvals
    - Contracts
    - Asset Management
    - Exit Costs
    - Files

- Insurance Records
- Divisions/Subdivisions
- Tasks
- Valuations
- Invoices
- Reporting
- Lease Accounting Synchronization

19. Once all relevant boxes have been checked, click **Update Role** at the top of the workspace.
20. Click **Close** on the Notice pop-up.



21. To return to the list of roles, click the **Manage Roles** hyperlink. You'll see the newly created role listed at the bottom.



Editing a Role

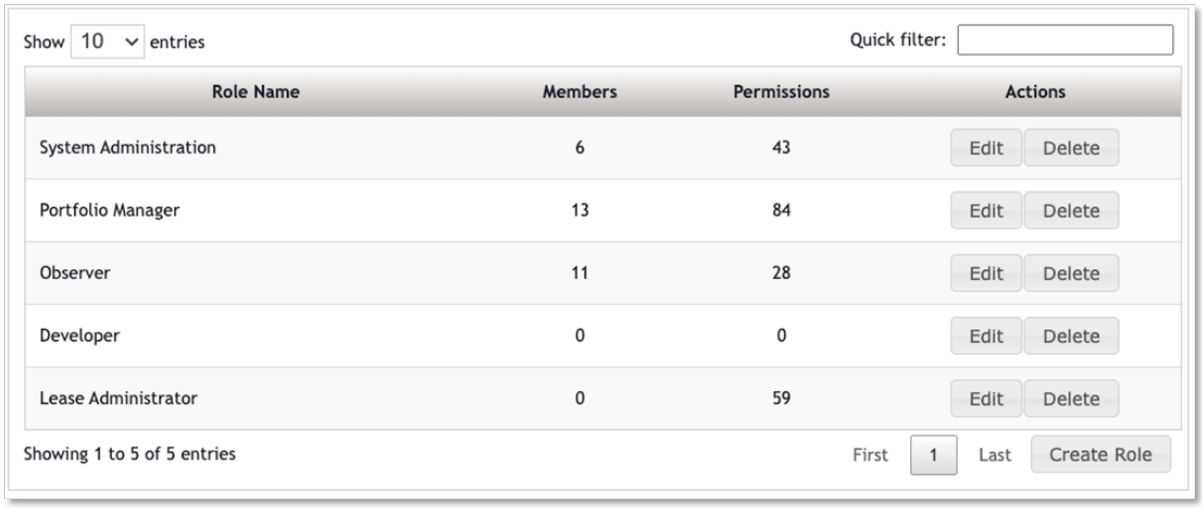
Editing an existing role follows the same path as creating a new role except that you will click **Edit** instead of **Create Role** in the Manage Roles workspace.

1. Click **Manage Roles**.
2. Within the Roles workspace, click **Edit** for the role that you wish to change.
3. In the Role Permissions section, you can check or uncheck boxes as necessary for the changes you wish to make.
4. For information on each functional permission, please see the Permissions Index at the end of the user guide.
5. If you wish to change the asset access for the role, click the **Configure Assets This Group Can Access** button.
6. In the pop-up, update the access either by filtering or selecting specific assets. Once done, click **Okay**.
7. When all changes have been made, click **Update Role** at the top of the workspace.
8. Click **Close** in the Notice pop-up.
9. To get back to the Manage Roles workspace, click the **Manage Roles** hyperlink at the top of the workspace.

Deleting a Role

To delete an existing role, once in the Manage Roles workspace, click **Delete** for the role you wish to remove. This is a permanent action and cannot be undone. Deleting a role that is currently assigned to one or more users will remove the permissions that role grants.

Important: If you delete the only assigned role for a user, they will not have access to the system and will receive an error when attempting to log in.



Permissions Index

Identity Management and Access Control

Permission	Definition
Identity Management and Access Control	Allows access to IDAAC.
Identity Management	Allows user to view the Manage Users workspace.
Create Identity	Allows user to create a new user.
Edit Identity	Allows user to edit an existing user.
Unarchive Identity	Allows user to reactivate a user that has been archived.
Archive Identity	Allows user to archive a user.
Access Control	Allows user to view the access control for a user.
Lock User	Allows user to lock a user record.
Unlock User	Allows user to unlock a previously locked record.
Assign/Remove Roles	Allows user to assign or remove roles.
Role Management	Allows user to view the Manage Roles workspace.
Create Role	Allows user to create a new role.
Edit Role	Allows user to edit an existing role.
Delete Role	Allows user to delete an existing role.

LA-RE Access

Permission	Definition
LA-RE Access	Allows access to Real Estate Manager.
Administration	Allows user to view and make changes in the Administration workspace.
System Configuration	Allows user to view and make changes to System Configuration.
Tax Rates	Allows user to view and make changes to Tax Rates.
View Assets	Allows user to view assets in the Asset Management workspace.
View Compliance	Allows user to view Compliance tab for an asset.
Configure Asset Compliance	Allows user to configure compliance items for an asset.
Update Asset Compliance	Allows user to update compliance items for an asset.
View Consent/Approvals	Allows user to view Consent/Approvals tab for an asset.
Manage Consent/Approvals	Allows user to view options for Consents/Approvals for an asset.
Edit All Consent/Approvals	Allows user to change all Consent/Approvals fields.
Edit Consent Approval Type	Allows user to change the Approval Type.
Edit Consenting Authority	Allows user to change the Consenting Authority.
Edit Date of Consent	Allows user to change the Date of Consent.
Edit Consent Date of Substantial Commencement	Allows user to change the Date of Substantial Commencement.
Edit Consent Description	Allows user to change the Consent description.

Permission	Definition
Edit Consent Document Location	Allows user to change the Consent document location.
Edit Consent Files	Allows user to download or send Consent files.
Edit Consent Guarantee Amount	Allows user to change the Consent guarantee amount.
Edit Consent Guarantee Currency	Allows user to change the Consent guarantee currency.
Edit Consent Guarantee Details	Allows user to change the Consent guarantee details.
Edit Consent Lapse Dates	Allows user to change the lapse dates for a Consent.
Edit Consent Relevant Lot	Allows user to change the relevant lot/DP for a Consent.
Edit Consent Renewal Dates	Allows user to change the renewal dates for a Consent.
Edit Consent Variation Date	Allows user to change the date for a Variation Consent.
Edit Consent Variation Summary	Allows user to change the summary for a Consent Variation.
View Contracts	Allows user to view contracts for an asset.
View Contract Clauses	Allows user to view any contract clauses on a contract.
Edit Contract Clauses	Allows user to change contract clauses on a contract.
Edit Contracts	Allows user to edit an existing contract.
Delete Contracts	Allows user to delete an existing contract.
Edit Contract Notes	Allows user to change any contract notes.
View Contract Files	Allows user to view any files attached to a contract.
Edit Contract Files	Allows user to upload/remove any files for a contract.
View Contract Incentives	Allows user to view any contract incentives.
Edit Contract Incentives	Allows user to change any contract incentives.
Asset Management	Allows user to view Asset Management workspace.
Delete Assets	Allows user to delete existing assets.
Edit Asset Notes	Allows user to change any notes on an asset.
View Exit Costs	Allows user to view any exit costs for an asset.
Manage Exit Costs	Allows user to change any exit costs for an asset.
View Files	Allows user to view files attached to an asset.
Remove Files	Allows user to remove files attached to an asset.
Upload Files	Allows user to upload files to an asset.
View Insurance Records	Allows user to view any insurance records for an asset.
Remove Insurance Records	Allows user to remove any insurance records for an asset.
Add/Edit Insurance Records	Allows user to add or change any insurance records for an asset.
View Subdivisions	Allows user to view the Subdivisions tab in an asset.
Manage Subdivisions	Allows user to add, delete, and change subdivisions in an asset.
View Tasks	Allows user to view the Tasks tab in an asset.
Manage Tasks	Allows user to add, delete, and change tasks in an asset.
Edit Due Date	Allows user to change the due date for a task.
Manage Task Files	Allows user to see any files attached to a task.
Remove Task Files	Allows user to remove any files attached to a task.

Permission	Definition
Upload Task Files	Allows user to upload any files attached to a task.
View Valuations	Allows user to view the Valuations tab in an asset.
Manage Valuations	Allows user to add, delete, and change valuations for an asset.
Budgets and Forecasting	Allows user to see the Budgets and Forecasting workspace.
View Contacts	Allows user to view Contact Management workspace.
Contact Management	Allows user to add, delete, and change contacts.
View Invoices	Allows user to see the Invoice Management workspace.
Invoice Management	Allows user to add, delete, and change invoices.
Lease Accounting Feature Access	Allows user to view features for lease accounting.
Lease Accounting Export Management	Allows user to view and manage lease accounting exports.
Lease Accounting LOIS Export	Allows user to create lease accounting exports.
View Lease Accounting Readiness Review History	Allows user to view existing Lease Accounting Readiness Reviews.
Approve Lease Accounting Readiness Reviews	Allows user to approve pending Lease Accounting Readiness Reviews.
Create Lease Accounting Readiness Reviews	Allows user to initiate and create a Lease Accounting Readiness Review.
Delete Submitted Lease Accounting Readiness Reviews	Allows user to delete submitted Lease Accounting Readiness Reviews.
Un-Delete Submitted Lease Accounting Readiness Reviews	Allows user to un-delete or bring back Lease Accounting Readiness Reviews that were previously deleted.
View Synchronization Logs	Allows user to view the synchronization logs created when leases are synced with Lease Accounting Manager.
Payment System	Allows user to view the Payments Management workspace.
Manage Payment Submissions	Allows user to add, delete, and change payment batches.
Approve Invoices for Payment	Allows user to approve invoices in payment batches.
Submit Invoices for Payment	Allows user to submit payment batches.
Revert Invoices Approved for Payment	Allows user to revert approved payment batches.
Shared Payment Batch Access	Allows user to completely delete a payment batch.
Reporting	Allows user to view the Reporting workspace.
Asset Reports	Allows user to generate Asset reports.
Compliance Reports	Allows user to generate Compliance reports.
Contact Reports	Allows user to generate Contact reports.
Contract Reports	Allows user to generate Contract reports.
Permission	Definition
Financial Reports	Allows user to generate Financial reports.
Global Report Management	Allows user to generate custom reports.

Version Summary

Version	Changes/Updates	Date
23R4	Guide created.	10/24/2023
24R1	Minor updates made.	12/22/2023
24R2.3	Updated formatting for ISW.	09/18/2024