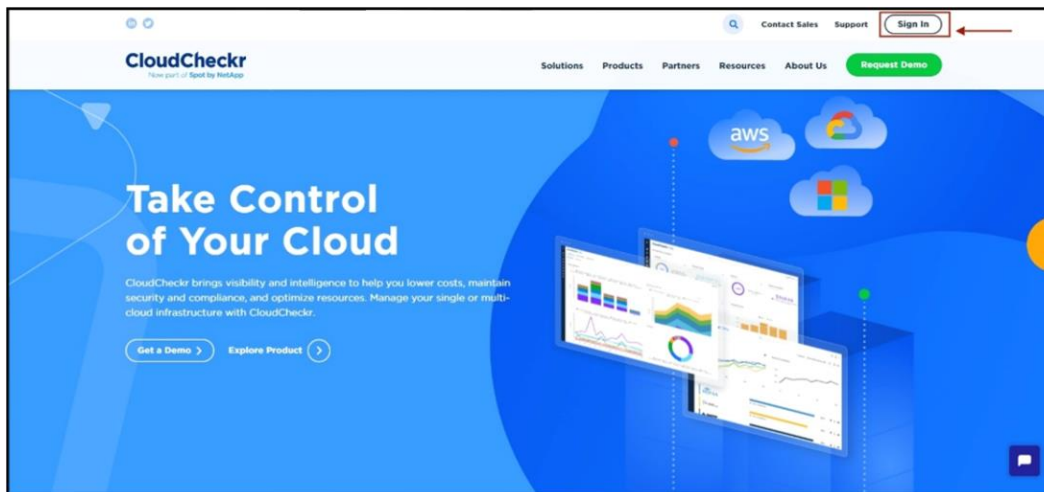


Credentialing Users in CloudCheckr CMx

To login to CloudCheckr CMx, Go to CloudCheckr.com and click on “Login” or go directly to us.CloudCheckr.com



Note: Users with Full Administration permissions from the legacy CloudCheckr will be able to login using the same email and password; however, if they do not have Full Administration permission, they will need new permissions associated with their email address.

If you are unable to log in, or are unable to see any accounts to select, please talk to your company's CloudCheckr Administrator and request that your access be updated in CMx.

GRANTING USER ACCESS

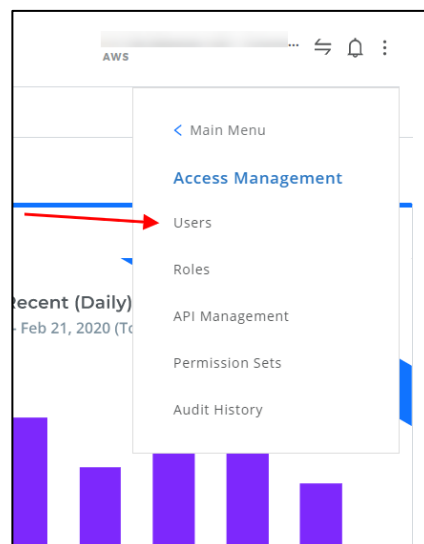
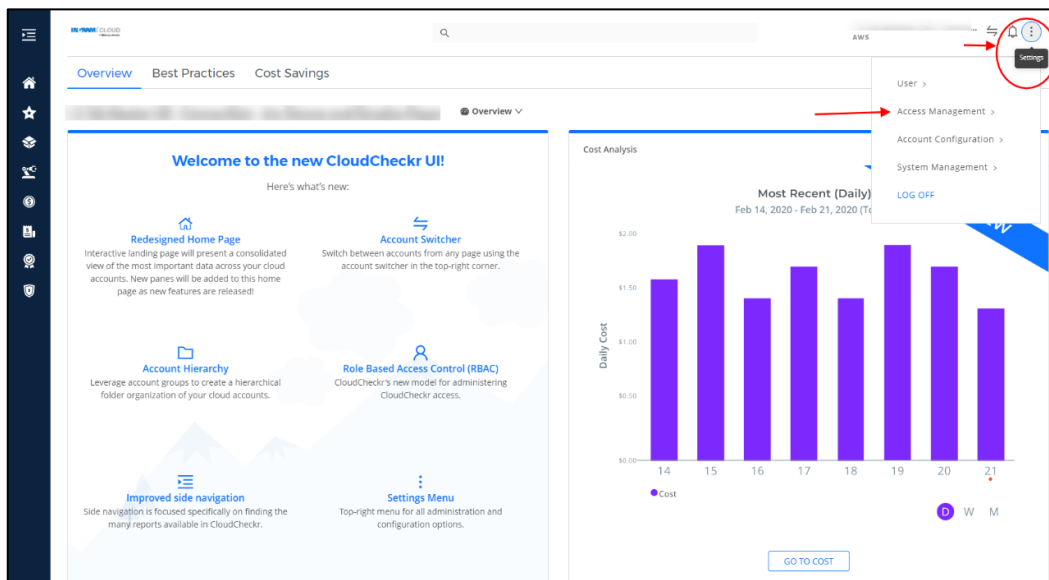
There are 3 components involved with granting access to CloudCheckr.

- **Users:** a user is the individual with valid CloudCheckr username and password that enables them to login to the application. A user will also need a role to be able to access accounts and/or features within CloudCheckr
- **Permission Sets:** A permission set is a template that contains a collection of permissions which, when applied to a role, allow a user to see or manage reports or features. Permission sets can be applied to one or many roles.

- Roles: A role is where the user and the permission sets are combined to grant access to accounts, MAVS and Account Hierarchy folders.

USERS

- To review a list of users, go to **Settings > Access Management > Users**. The users from the legacy Cloudcheckr user interface have already been migrated into CMx and you will only need to configure the relevant permissions.



- On this screen, it is possible to add a new user, view when a user last logged in and what role(s) has been assigned to a user.

- Users without a role assigned will not be able to see or select any accounts to review.

Review 'Last Login' and consider removing people who have never logged in or have not logged in for a long time

No Roles assigned for these users

☐	User	Role(s)	Created	Last Login	Activated?	Personal Notes	Org Notes	ID
☐	t...@ingrammicro.com	(2) Sigma Solutions - End See More	06/21/19	Never	Yes			694d002-a584-4b5c-bd39-079c79d1aa54
☐	...@ingrammicro.com	(4) Beta Company - See More	09/27/18	10/02/18	Yes			dd36b167-a9e0-43c0-a6e6-63ce45d45718
☐	...@ingrammicro.com	Training Role	03/02/21	03/05/21	Yes			5a02843a-f2ae-4b50-8ceb-a6d81b533e85
☐	...@ingrammicro.com		06/21/19	Never	Yes			3b2937a2-deaf-4e75-a62b-cbaaa7803342
☐	...@ingrammicro.com	(2) Test for Demo, End See More	07/20/20	Never	No		role needed for architecture of custome See More	9f4ce2ab-b0c7-4749-bef7-d577ed105804
☐	...@ingrammicro.com	Test for Demo	09/28/18	Never	No			13a55b72-fdf7-4c60-b9b1-d653126aa256
☐	...@ingrammicro.com		01/21/21	02/22/21	Yes			63dc4c24-8b35-44e2-8ebf-ec9cbead3e0

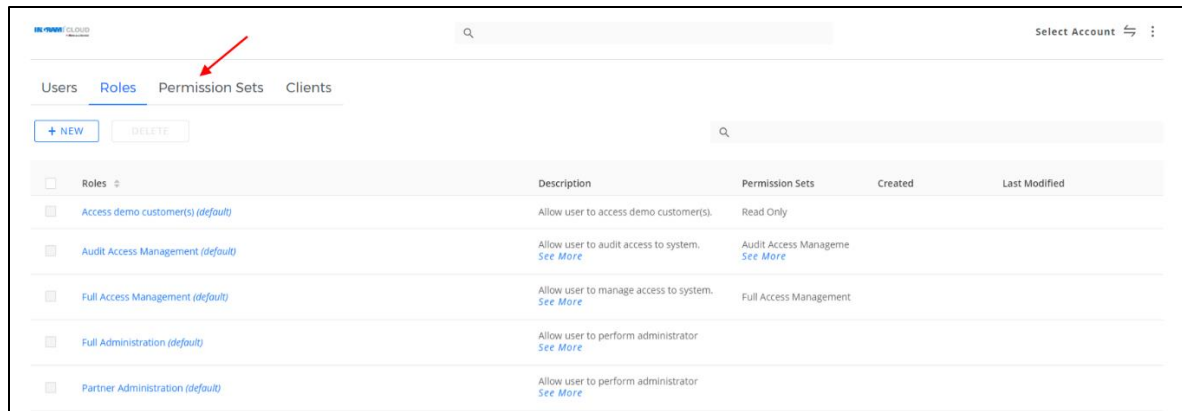
Showing 7 of 7

Note: This is a good opportunity to clean up your user list. If someone has not logged in for an extended period or is no longer with the organization, consider removing them as an authorized user. It is also important to communicate with your end users so they can notify you of any changes to their authorized user list.

(Continue to next page)

PERMISSION SETS

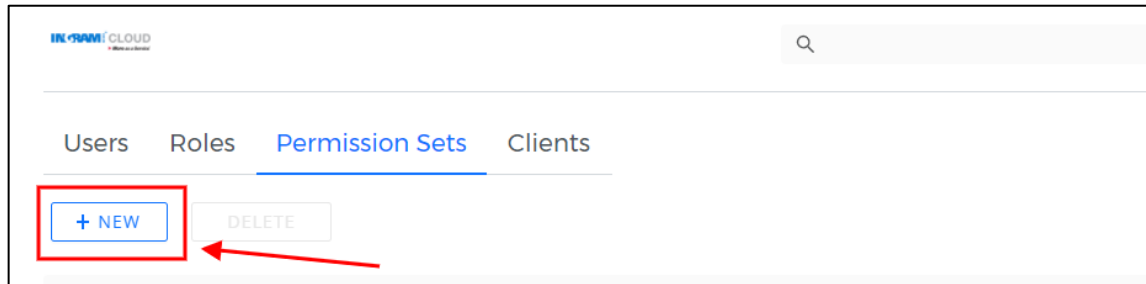
- Click on **Permission Sets**



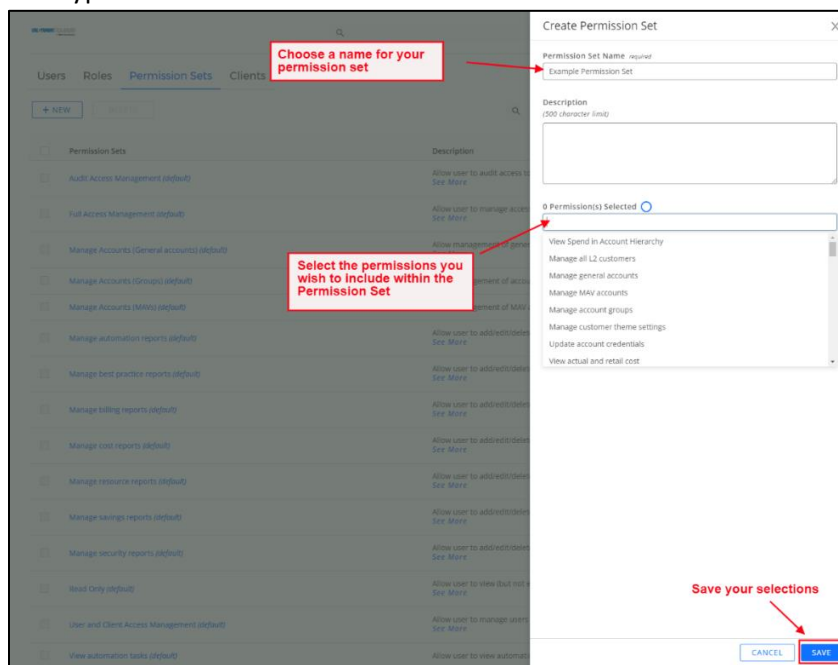
- Here is a list of default permission sets available for easy selection. It is also possible, and recommended, to create custom permission sets that allow for granular control over exactly which features and reports the user can see. Taking the time to create custom permission sets that match your exact use case will save time in the long run as you will be able to re-use them with each new customer and user.

☐ User and Client Access Management (default)	Allow user to manage users and clients. See More		
☐ View automation tasks (default)	Allow user to view automation reports		
☐ View best practice reports (default)	Allow user to view best practice reports.		
☐ View billing reports (default)	Allow user to view billing reports.		
☐ View compliance reports (default)	Allow user to view compliance reports		
☐ View cost reports (default)	Allow user to view cost reports.		
☐ View resource reports (default)	Allow user to view resource reports		
☐ View savings reports (default)	Allow user to view savings reports.		
☐ View security reports (default)	Allow user to view security reports		
Default Permission Sets			
☐ End User - List Cost only no other data	This set is for accounting roles and does See More	07/20/20	07/20/20
☐ End User - List Only		09/28/20	09/28/20
☐ End User - Read Only Technical		08/06/20	08/06/20
☐ End User - Test		08/07/20	08/07/20
☐ Internal Accounting Teams	This is for Reseller Accounting Teams - See More	08/07/20	08/07/20
Customized Permission Sets			

- To create a Permission Set, click on “+NEW”



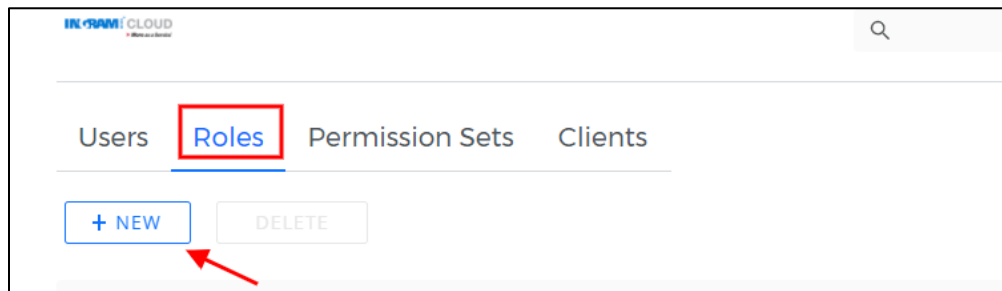
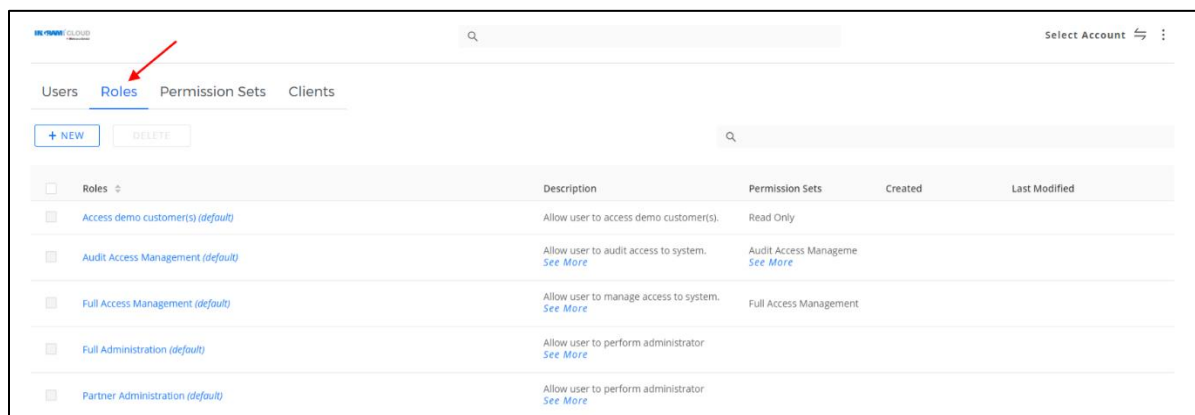
- Give the Permission Set a Name. Then select the permissions to include in this set. You may want to consider adding “internal” or “end user” to permission set names to easily identify which user type gets a particular permission set.
- Every Permission set needs a cost permission added to it. For End Users, select “LIST cost only.” For Internal users, you may want to allow them access to actual and list cost or perhaps just one of the two cost types.



ROLES

Before creating a role, take into consideration the general job description and access needed for the role. For example, consider restricting end users so they can only look at the accounts and MAVs for their own company. For internal users, consider restricting access to just the features needed to perform their duties. Depending on how your company has integrated CloudCheckr into your business model, you can restrict a user from seeing some or all of CloudCheckr's features, as well as only being able to see their accounts.

- Click on **Roles** and click on "+NEW"



- When choosing how to name a role, consider adding the name of the company for which the role may be used and what type of user is getting the role. For Example, Company X – Management or Company Y – Finance or MyCompany – Tech Team.

Tip: After you enter the “Name” field, you must save before going to the next step.

Role Management

Create New Role

SAVE **CANCEL**

Name required **Created** **Last Modified**

Acme Corp-Technical End User

Description
(500 character limit)

Assets

Users **Permission Sets** **Accounts** **Clients**

0 User(s) Selected [User Management](#)

- Under “User(s)” select the user you want to add to this Role

Role Management

Acme Corp-Technical End User

SAVE **DELETE**

Name required **Created** **Last Modified**

Acme Corp-Technical End User 03/08/2021, 06:08:14 PM 03/08/2021, 06:08:14 PM

Description
(500 character limit)

Assets

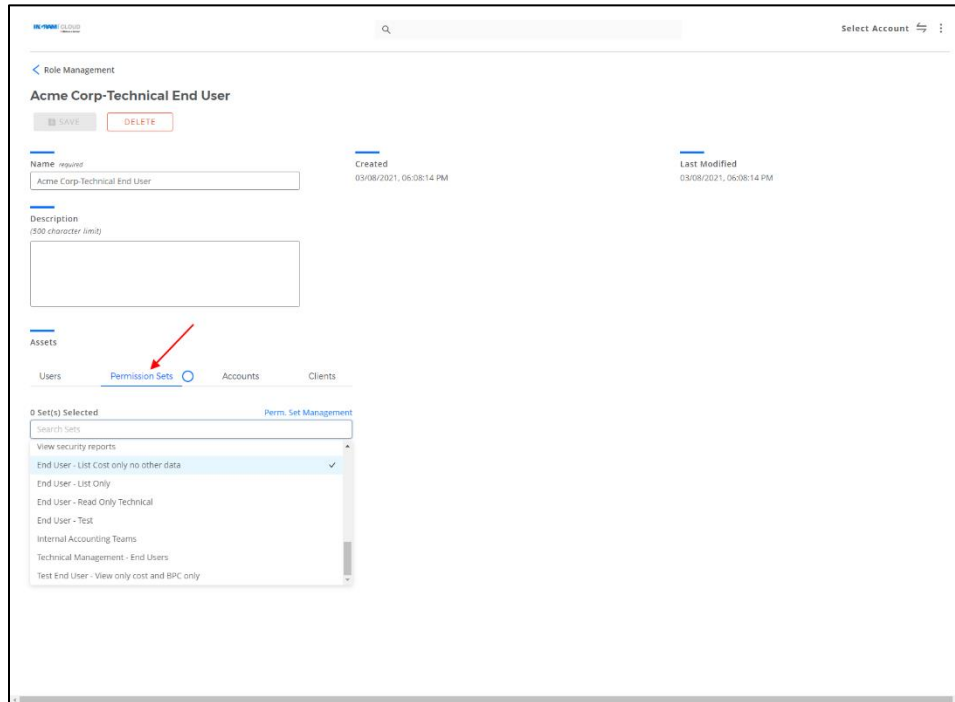
Users **Permission Sets** **Accounts** **Clients**

0 User(s) Selected [User Management](#)

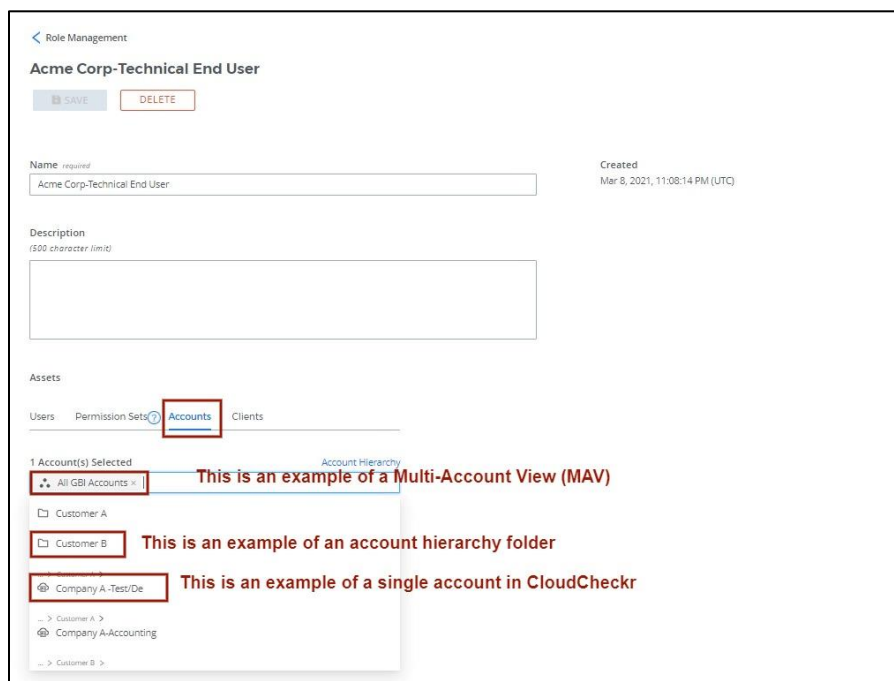
Search Users

- bertrand.brellier@ingrammicro.com
- neal.flaxman@ingrammicro.com
- Amena.Khan+Demo@ingrammicro.com
- douglas.herman@ingrammicro.com
- testcustomer@ingrammicro.com
- usfian00adm@ingrammicro.com
- vinod.lakshminarayanawamy@ingrammicro.com

- Under Permission Sets, you can choose more than one permission set, should you decide this user needs extra privileges within CloudCheckr



- Next, under the Accounts tab, you can select which accounts all users with this role have access to. If you have setup Account Hierarchies, you can use that rather than selecting individual accounts.



- Once you have made all your selections, make sure to hit SAVE again.

Role Management

Acme Corp-Technical End User

SAVE **DELETE**

Name required

Acme Corp-Technical End User

Created
03/08/2021, 06:08:14 PM

Last Modified
03/08/2021, 06:08:14 PM

Description
(500 character limit)

Assets

Users **Permission Sets** **Accounts** **Clients**

0 Client(s) Selected [Client Management](#)

Search Clients

- If you click “Roles Management” at the top left of the screen and click on the Roles tab, you will see the role you just created.

☐	Roles	Description	Permission Sets	Created	Last Modified
☐	Access demo customer(s) (default)	Allow user to access demo customer(s).	Read Only		
☐	Audit Access Management (default)	Allow user to audit access to system. See More	Audit Access Management See More		
☐	Full Access Management (default)	Allow user to manage access to system. See More	Full Access Management		
☐	Full Administration (default)	Allow user to perform administrator See More			
☐	Partner Administration (default)	Allow user to perform administrator See More			
☐	User and Client Access Management (default)	Allow user to manage users and clients. See More	User and Client Access See More		
☐	Acme Corp - Technical End User	(2) View cost reports. See More		08/10/20	08/10/20

- To see the roles that were added to the selected user, click on “Users” at the top of the screen. Users can have multiple roles. This means it is not necessary to create a new permission set every time you want to add a privilege.

Users Roles Permission Sets Clients						
+ NEW DELETE						
☐	User	Role(s)	Created	Last Login	Activated?	Personal Notes
☐	bertrand.brelier@ingrammicro.com	(2) Sigma Solutions - See More	06/21/19	Never	Yes	
☐	neal.flaxman@ingrammicro.com	(4) Beta Company - Accounting Users, Acme Corp - Technical End User, Enduser view, Sigma Solutions - Power User See Less	09/27/18	10/02/18	Yes	

Creating permission sets and roles that coincide with how you and your end users use CloudCheckr can really save time and promote a more secure CloudCheckr environment.

It is a best practice to regularly review user access lists to ensure that users who no longer need access to CloudCheckr are removed.