

Credentialing Payee Accounts in CloudCheckr CMx

Credentialing AWS payee accounts in CloudCheckr CMx allows for maximum benefits for your organization and for your customers. Credentialing accounts allows:

- Best Practice Reports
- Inventory of the account
- Use of compliance frameworks like CIS, PCI and HIPAA
- Reserved instance recommendations
- Tagging information and reporting

Whenever a Payee account is added to the organization, it is strongly recommended that the account be credentialed immediately. If the organization is using AWS ControlTower, the CloudCheckr credentialing process can be automated. Please refer to [this video](#).

STEP 1

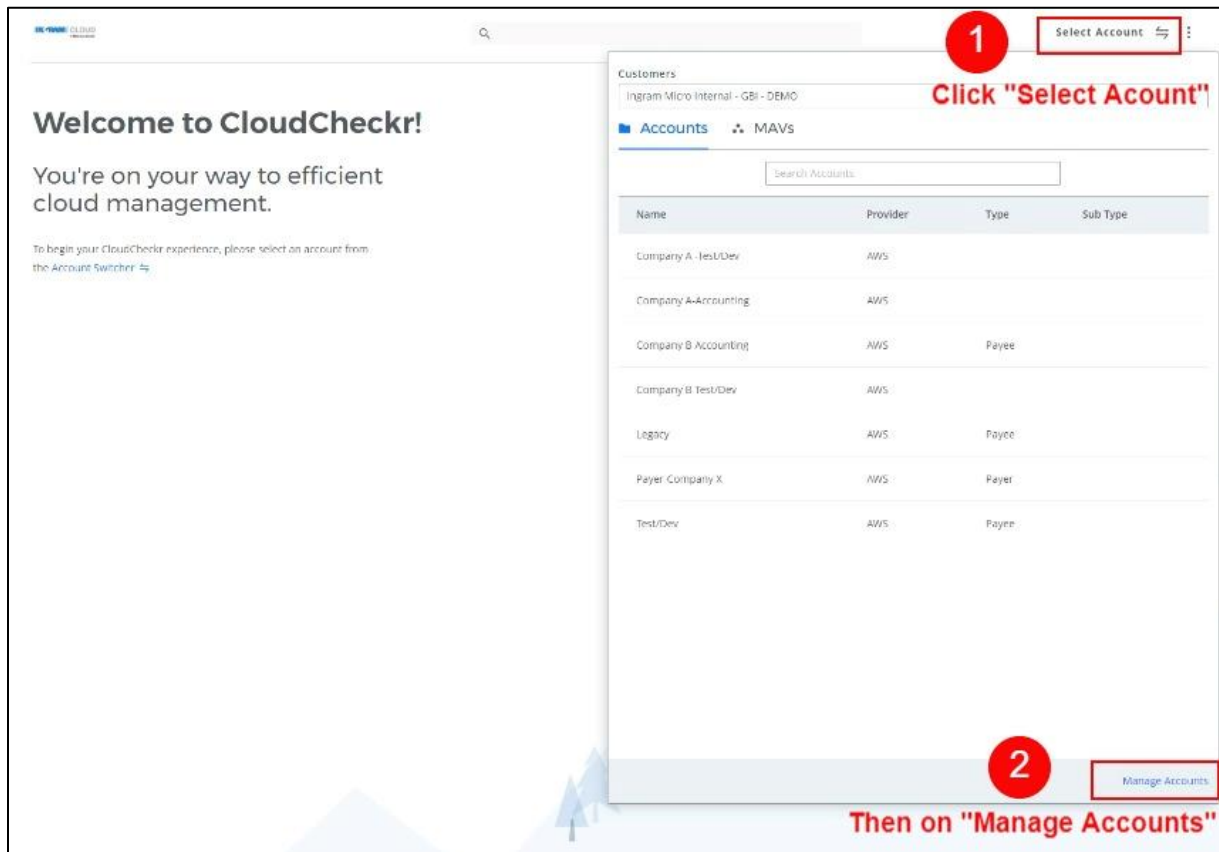
- Login to the AWS Account that you wish to credential.

(Continue to Next Page)

STEP 2

Login to CloudCheckr CMx.

- Navigate to "Select account" and then click on "manage accounts" page.



Welcome to CloudCheckr!

You're on your way to efficient cloud management.

To begin your CloudCheckr experience, please select an account from the Account Switcher.

1 **Select Account**

Click "Select Account"

2 **Manage Accounts**

Then on "Manage Accounts"

Name	Provider	Type	Sub Type
Company A - Test/Dev	AWS		
Company A - Accounting	AWS		
Company B - Accounting	AWS	Payee	
Company B - Test/Dev	AWS		
Legacy	AWS	Payee	
Payer - Company X	AWS	Payer	
Test/Dev	AWS	Payer	

(Continue to Next Page)

- Next, click on “List” and then locate the account that needs to be credentialed. Click on the red ‘X’ (or yellow exclamation point)

View by: Hierarchy **List**

Search Accounts Table

Name	Provider	Credentials	Provider ID	Type	Sub Type	Payer ID	Created	Parent Group	Legacy ID
Company A-Test/Dev	AWS						12/16/20	Demo Company	25
Company A Accounting	AWS						12/02/20	Demo Company	10
Company B Accounting	AWS		048824450751	Payee		085479309886	09/07/18		5
Company B Test/Dev	AWS						10/15/19		7
Legacy	AWS		089753618136	Payee		085479309886	09/01/18		3
Payer-Company X	AWS		085479309886	Payer			08/31/18		2
Test/Dev	AWS		115783089165	Payee		085479309886	09/04/18		4

- On the following screen click on the “Manage Credentials” link.

View by: Hierarchy **List**

Search Accounts Table

Name	Provider	Credentials	Provider ID	Type	Sub Type
Company A-Test/Dev	AWS				
Company A-Accounting	AWS				
Company B Accounting	AWS		048824450751	Payee	
Company B Test/Dev	AWS				
Legacy	AWS		089753618136	Payee	
Payer-Company X	AWS		085479309886	Payer	
Test/Dev	AWS		115783089165	Payee	

Edit Account

Name required
Company A-Accounting

Manage Credentials Missing credentials
Manage Billing Data Source

Location
Clear this field to move the account to Root
☐ Demo Company

Payee Organization
(Only applicable if account is a Payer)
Place new payees at hierarchy root (default)

Attributes
Country: US Customer: Company A

Details

ID
f6a7e754-896e-4713-9fbf-dba2bbca27c

Created Date
12/02/20

Legacy Account ID
10

Cloud Provider
AWS

STEP 3

- Click on the hyperlink that launches a CloudFormation Stack. This will route directly into the AWS console and display a CloudFormation template.

NOTE: If you click on this link *before* you login to your AWS account, it will not take you to the correct screen.

The screenshot shows the AWS IAM console 'Edit AWS Credentials' page for account ID 213133241983. The page includes a sidebar with navigation icons, a search bar, and a header with the account ID. The main content area has a 'Toggle Manual vs. CloudFormation' section. Under the 'CloudFormation' tab, there are 10 numbered steps. Step 2, 'Click the [Launch CloudFormation Stack](#) link.', is highlighted with a red box. A red arrow points from the text 'Click on the hyperlink' to this link. Below the instructions, there is an 'AWS Role ARN' input field and an 'Update' button.

NOTE: Before launching CloudFormation stack, double check that you are in the correct AWS account



STEP 4

- Once in the AWS Management Console and on the Quick Create stack Page:
 - Under **Stack name**: Keep the name the same; however, it is helpful to add the Year and Month at the end for tracking purposes (ex. cc-iam-stack-202204).
 - Scroll down to **CloudTrailBucket**. Here you have the option of adding the Bucket name for your CloudTrail if you want CloudCheckr to ingest the information stored in CloudTrail.
 - Click on **I acknowledge that AWS CloudFormation might create IAM resources**.
 - Then click **Create stack**

Quick create stack

Template

Template URL
https://s3.amazonaws.com/df-cc-4172017/cc_aws_cfn_iam_stack.template.json

Stack description
-

Stack name

Stack name
cc-iam-stack

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

IAM Role

ExternalAccount
CloudCheckr Account
352813966189

ExternalId
CloudCheckr External ID
CC-F2D7A68EA2FBD11C6365109F30688A3

AccountType
Account Type
Standard

Inventory

InventoryAndUtilization
Use CloudCheckr to process inventory and utilization data?
True

Billing

CostPermissions
Use CloudCheckr to process billing data?
True

BillingBucket
AWS Detailed Billing Report Bucket

CurBucket
AWS Cost and Usage Report Bucket

Security

Security
Use CloudCheckr to process security data?
True

CloudTrailBucket
AWS CloudTrail Bucket

CloudWatch Flow Logs

CloudWatchFlowLogs
Use CloudCheckr to process CloudWatch Flow Logs data?
True

Capabilities

The following resource(s) require capabilities: [AWS::IAM::Role]
This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the **required permissions**. [Learn more](#)

☐ I acknowledge that AWS CloudFormation might create IAM resources.

Cancel Create change set **Create stack**

Adding the date to the Stack name can be helpful to track how long ago the stack was created.

When credentialing a Payee account, DO NOT enter the S3 Bucket names for the CUR or for Billing. This information comes from the Payer

When entering the S3 Bucket name, make sure that it is an exact match to the S3 bucket name.

STEP 5

- Next, click on the “Resources” tab.

The screenshot shows the AWS CloudFormation console for the stack 'cc-iam-stack-202104'. The 'Resources' tab is selected, and a red arrow points to it with the text 'Click on the Resources Tab'. The stack is in a 'CREATE_IN_PROGRESS' state. The left sidebar shows a list of stacks, with 'cc-iam-stack-202104' highlighted. The main content area shows the 'Events' tab with one event: '2021-04-14 15:06:13 UTC-0400' with status 'CREATE_IN_PROGRESS' and reason 'User Initiated'.

STEP 6

- Once stack creation is complete, click on the IAMRole hyperlink, as shown below.

The screenshot shows the AWS CloudFormation console for the stack 'cc-iam-stack-202104'. The 'Resources' tab is selected, and the stack is in a 'CREATE_COMPLETE' state. A red box highlights the 'IAMRole' resource, and a red arrow points to the 'IAMRole' hyperlink. The left sidebar shows a list of stacks, with 'cc-iam-stack-202104' highlighted. The main content area shows the 'Resources' tab with five resources: 'CloudWatchFlowLogsPolicy', 'CostPolicy', 'IAMRole', 'InventoryPolicy', and 'SecurityPolicy'. The 'IAMRole' resource is highlighted with a red box, and a red arrow points to the 'IAMRole' hyperlink. The status of all resources is 'DELETE_COMPLETE'.

When the stack creation is complete, click on this hyperlink

STEP 7

- Copy the Role ARN from the following screen.

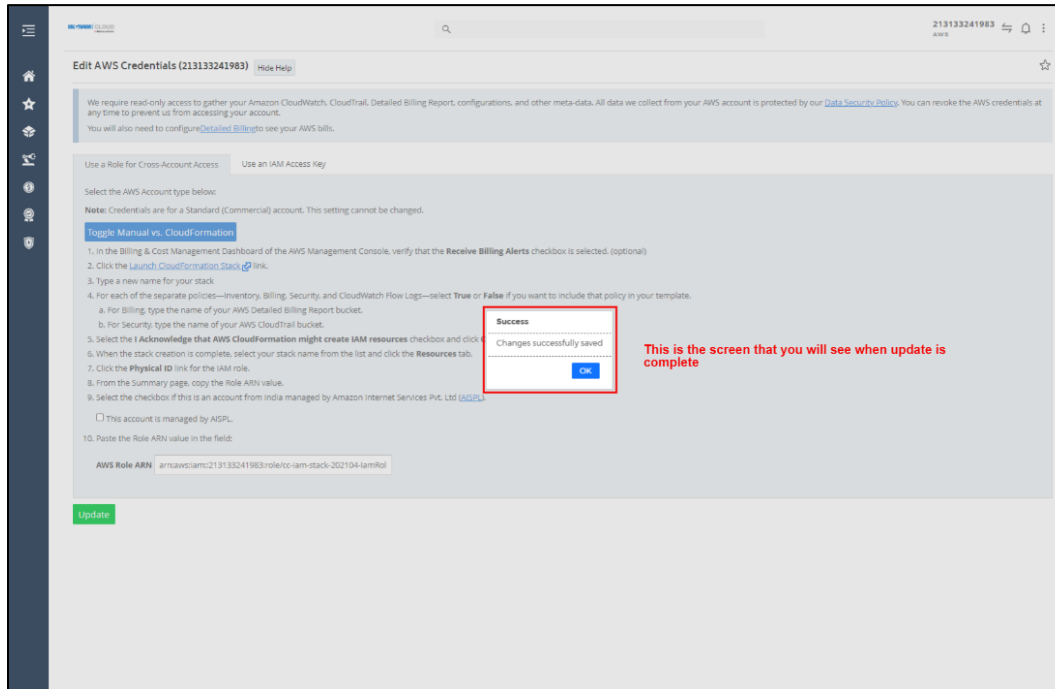
The screenshot shows the AWS IAM console 'Summary' page for the role 'cc-iam-stack-202104-lamRole-BUG7VU5SD5HE'. The 'Role ARN' is 'arn:aws:iam::213133241983:role/cc-iam-stack-202104-lamRole-BUG7VU5SD5HE'. A red box highlights the Role ARN, and a red arrow points to the copy icon next to it with the text 'Click on this icon to copy the Role ARN'.

STEP 8

- Go back to CloudCheckr CMx and Paste the Role ARN in the text field and then click "Update"

The screenshot shows the CloudCheckr CMx 'Edit AWS Credentials' page. The 'AWS Role ARN' field is highlighted with a red box, and a red arrow points to it with the text 'Paste the Role ARN into this field'. The 'Update' button is also highlighted with a red box, and a red arrow points to it with the text 'Click "Update"'.

- You will see the following confirmation once CloudCheckr has validated that it has permission to access the AWS account.



- The account is now fully credentialed. It can take 1-2 hours for the information to fully populate in CloudCheckr.

ADDITIONAL NOTES

If you do not have access to the end customer's AWS account, you may copy the hyperlink that launches the CloudFormation Stack (Step 3) and send that to your end customer. They can then:

- Log into AWS account
- Click the provided CloudFormation stack (or open in another tab of your web browser)
- Follow steps 4-7
- End customer to email role ARN back to you
- Partner to complete Step 8



(Continue to Next Page)

TIP

Click on the bell icon on the top right corner of the screen to see “Notifications.” This can tell you the last time an update was done and allow you to prompt an immediate update, rather than waiting for the scheduled update.

The screenshot shows the 'Edit AWS Credentials' page in the AWS IAM console. The page title is 'Edit AWS Credentials (213133241983)' with a 'Hide Help' link. A red arrow points to the 'Notifications' icon in the top right corner, with the text: 'You can click on the "Notifications" icon to get update on the account'. The main content area has two tabs: 'Use a Role for Cross-Account Access' (selected) and 'Use an IAM Access Key'. Below the tabs, there is a 'Note' about Standard (Commercial) accounts. A red arrow points to the 'Update Now' button in the 'Billing Data' section, with the text: 'Click "Update Now" if you want to prompt CloudCheckr to manually update earlier than scheduled'. The 'Billing Data' section shows 'Billing Data Checked 1 Hour Ago' and '53 Reports Updated 3 Minutes Ago'. The 'Account Notifications' section shows 'You do not have permissions to check WorkSpaces' and 'You do not have permissions to check Elastic File System'. The 'AWS Role ARN' field is populated with 'arn:aws:iam::213133241983:role/cc-iam-stack-202104-iamRole'. The 'Update' button is at the bottom left.