Automated Safeguards for IAM - Group & User Self Service

Overview

The purpose of these IAM automated safeguards is two-fold;

1. To ensure that, as a customer, you can leverage proper IT governance when using ClearDATA by having granular control over which of your users can perform which functions (Identity Safeguards)
2. To ensure that, as customer, you can have direct access to the AWS API and console, while still ensuring your compliance stance is maintained (API Safeguards)

Creating Users

ClearDATA will start you off with an Administrator account, which will allow you to create users and assign them to groups. This Administrator is configured as part of the on boarding process and is assigned to the **DPHI-Administrators** group. Members of this group are IAM users who can administer users on the */cleardata/customer/* path. On the ClearDATA AWS Platform, you are only allowed to create users on a specific IAM path, */cleardata/customer/*.

> ⓘ **AWS Console Info**
>
> The AWS Console does not support setting a path on user creation, you must use the AWS CLI to create users.

Once the administrator has configured their machine with their IAM keys, you can run a create-user command

Create User

```
aws iam create-user --path /cleardata/customer/ --user-name USERNAME
```

Once a user is created, assigning this user to groups can be done from the console - Security credentials for user can also be configured in the console. Of course, the AWS CLI can still be used to manage the user - As an example, once a user has been created, it can be assigned to a group using the add-user-to-group command:

Add User To Group

```
aws iam add-user-to-group --group-name GROUPNAME --user-name USERNAME
```

Available groups

Users can be assigned by a member of the **DPHI-Administrators** group to up to ten groups. The table below provides the initial list of groups that is deployed in an AWS account

> ⓘ **Group Names**
>
> Groups starting with **DPHI** are available to all customers. Groups starting with **Safeguards** are available to all customers with Automated Safeguards.

Group	AWS Service	Description
DPHI-SuperUser		A group that encompasses all the other DPHI groups except DPHI-Administrators

DPHI-Cloudformation	CloudFormation	This role only grants rights to the CloudFormation service. Your principal will also need rights to the individual components Cloudformation would provision.
DPHI-Cloudfront	CloudFront	Includes the necessary rights needed to create Cloudfront distributions, including limited rights to ELB, IAM, S3 and Cloudwatch
DPHI-CloudtrailAdmin	CloudTrail	Ability to read all Trails and create new Trails
DPHI-Cloudwatch	Cloudwatch	Metrics and logging rights
DPHI-Ecs	ECS ECR	ECS and ECR rights for use with the ClearDATA Container Product
DPHI-Ec2	EC2	EC2 rights to spin up instances that are • from AMI that are tagged *cleardata:customer-allow* • in security groups that are tagged *cleardata:customer-allow*
DPHI-Kms	KMS	
DPHI-Lambda	Lambda	
DPHI-LoadBalancing	ALB	Allows updating of SSL certificate, registering/deregistering instances from the LB, modify target groups in ALBs
DPHI-LoadBalancingAdmin		
DPHI-RDS	RDS	Limited access to RDS, including the ability to take and restore snapshots If Automated Safeguards are enabled, full rights are available
DPHI-ReadOnly		Read-only access
DPHI-Route53	Route53	
DPHI-S3	S3	
DPHI-Ses	SES	
DPHI-Sns	SNS	
DPHI-Sqs	SQS	Access to existing SQS queues
DPHI-Waf	WAF	
Safeguards-Administrators		A group that encompasses all the other *Safeguard* groups
Safeguards-APIGateway	API Gateway	
Safeguards-Athena	Athena	
Safeguards-ComprehendMedical	Comprehend Comprehend Medical	

Safeguards-Config	AWS Config	
Safeguards-DynamoDB	DynamoDB	
Safeguards-EC2	EC2	Additional access to EC2 including the ability to modify security groups
Safeguards-ElastiCache	ElastiCache	
Safeguards-Elasticsearch	Elasticsearch	
Safeguards-Firehose	Kinesis Firehose	
Safeguards-Glue	Glue	
Safeguards-Kinesis	Kinesis Data & Video Streams	
Safeguards-Redshift	Redshift	
Safeguards-Sagemaker	Sagemaker	
Safeguards-SQS	SQS	Additional SQS permission, including the ability to create queues
Safeguards-StepFunctions	Step Functions	
Safeguards-Transcribe	Transcribe	
Safeguards-TransferSFTP	Transfer for SFTP	
Safeguards-Translate	Translate	
Safeguards-Xray	X-Ray	

Additional groups and policies can be created by our Support team to meet your API and console access requirements. In addition, ClearDATA can combine existing policies into a custom group.

Please contact our Support team should you need more information on the reference architectures associated with the permissible AWS services