How-To Library

Informatica®

Enable Customer Managed Keys for your Organization on Amazon Web Services

Abstract

This article explains how to create your own, customer managed, master encryption key for Informatica Intelligent Cloud Services on Amazon Web Services. The master encryption key is used to encrypt your organization-specific encryption keys. The key that you create is controlled and maintained by you. You can use it to control and restrict access to your organization's data.

Supported Versions

- Informatica Intelligent Cloud Services February 2024

Table of Contents

Overview

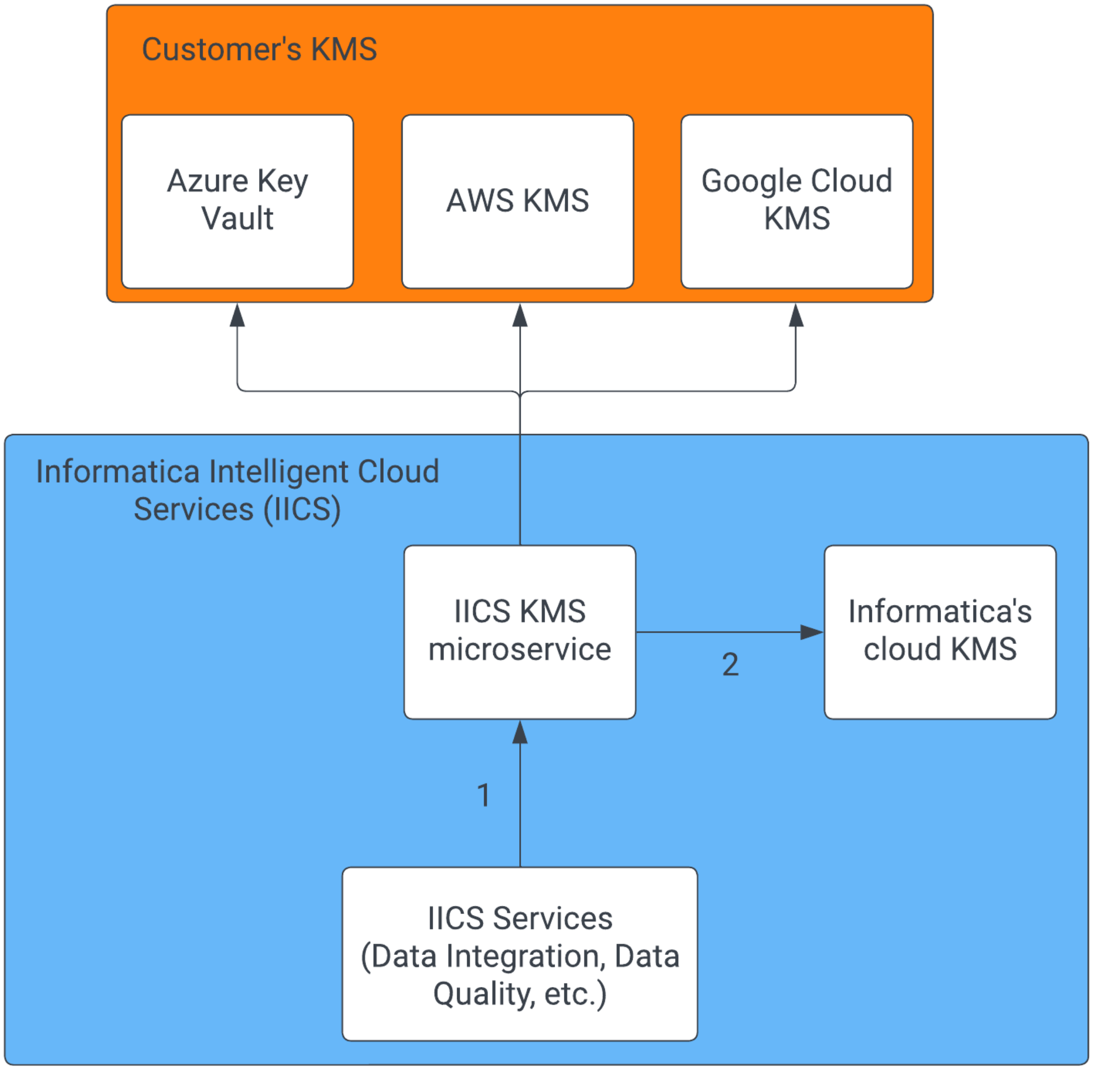
Informatica Intelligent Cloud Services protects your organization's sensitive data in the cloud using organization-specific encryption keys that are generated and stored in the Informatica Intelligent Cloud Services key management service (KMS). To prevent malicious access, the keys are encrypted using a master key that is stored in the cloud provider's KMS.

If you prefer, you can create a customer managed key (CMK). When you create a CMK, you control access to it. However, you'll need to grant Informatica Intelligent Cloud Services access to the CMK so that it can encrypt and decrypt your organization's sensitive data.

Creating a CMK offers the following benefits:

- You can restrict and control any access to your data.
- You can restrict the decryption of your data in the event of a data breach.
- You create and hold the key material in your KMS. The key is never exposed to your cloud service provider.
- You maintain full control of the key throughout its lifecycle. You can revoke access or delete the key at any time.

The following image shows how Informatica Intelligent Cloud Services interfaces with your CMK:



1. Informatica Intelligent Cloud Services interfaces with the Informatica Intelligent Cloud Services KMS agnostically.
2. Non-customer managed keys go to Informatica's cloud KMS.

Note: When you create a CMK, your KMS and Informatica Intelligent Cloud Services POD must use the same cloud provider. For example, if your Informatica Intelligent Cloud Services POD is USW1 on AWS, then you must store your CMK in AWS KMS. You can't store it in Google Cloud KMS or Azure Key Vault.

After you create and enable a CMK, you can revoke it at any time by disabling customer managed keys in Informatica Intelligent Cloud Services Administrator. If you do this, you'll go back to using Informatica's master key.

Steps for creating and enabling the key

To create and use a CMK, you provision the key in AWS KMS and enable cross-account access with Informatica Intelligent Cloud Services. Then you enable customer managed keys in Informatica Intelligent Cloud Services.

To create a CMK, complete the following steps:

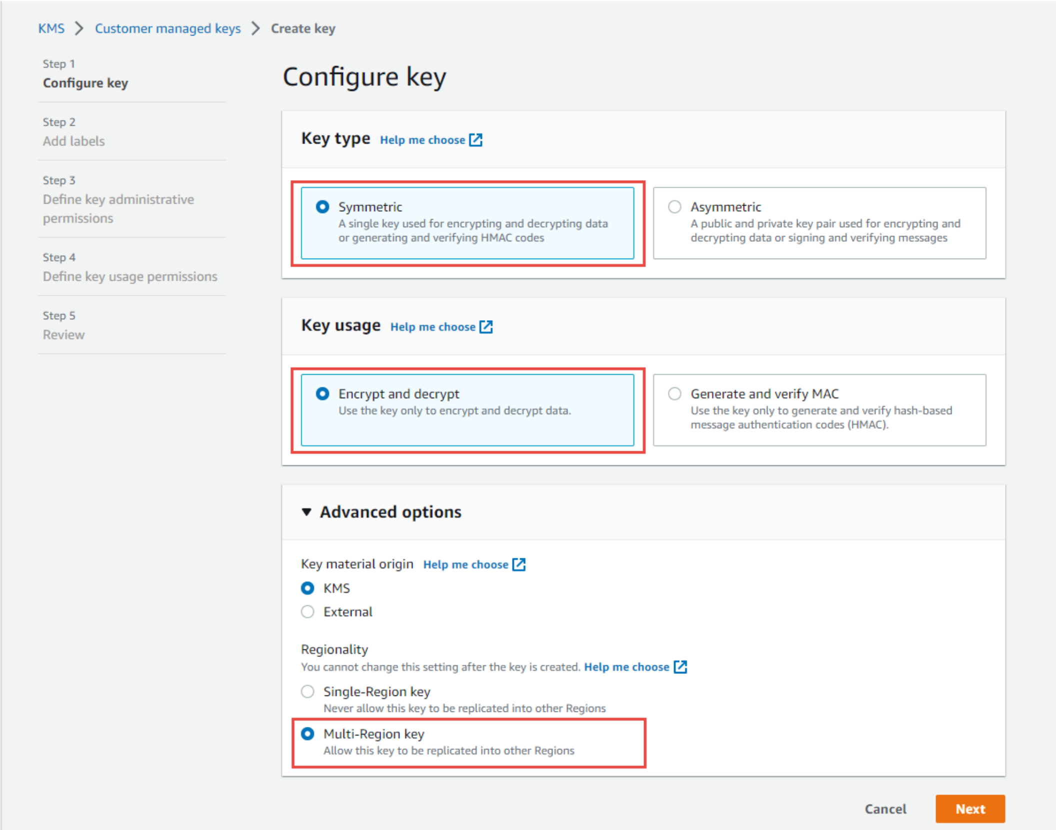
1. In AWS KMS, create the key to use as your CMK.

2. Create an IAM policy for the key.
3. Create an IAM role and attach the policy to the role so that Informatica can access the key.
4. In Informatica Intelligent Cloud Services Administrator, enable customer managed keys on the **Settings** page.

Step 1. Create the key in AWS KMS

Create a symmetric key to use as your CMK. Note the key ARN because you'll need it when you enable customer managed keys in Informatica Intelligent Cloud Services.

1. Log in to the [AWS Management Console]().
2. In the search bar, search for **Key Management Service**.
3. Select **Customer managed keys**, and click **Create key**.
4. In **Key type**, select **Symmetric**.
5. In **Key usage**, select **Encrypt and decrypt**.
6. Expand the **Advanced options**, and select **Multi-Region key**.



KMS > Customer managed keys > Create key

Step 1
Configure key

Step 2
Add labels

Step 3
Define key administrative permissions

Step 4
Define key usage permissions

Step 5
Review

Configure key

Key type Help me choose

● Symmetric
A single key used for encrypting and decrypting data or generating and verifying HMAC codes

○ Asymmetric
A public and private key pair used for encrypting and decrypting data or signing and verifying messages

Key usage Help me choose

● Encrypt and decrypt
Use the key only to encrypt and decrypt data.

○ Generate and verify MAC
Use the key only to generate and verify hash-based message authentication codes (HMAC).

▼ Advanced options

Key material origin Help me choose
● KMS
○ External

Regionality
You cannot change this setting after the key is created. Help me choose

○ Single-Region key
Never allow this key to be replicated into other Regions

● Multi-Region key
Allow this key to be replicated into other Regions

7. Click **Next**.
8. Enter an alias for the key, and optionally add a description and tags.

   Tip: Enter an alias that indicates the type of data you plan to protect or the application you plan to use with the KMS key.
9. Select the IAM users and roles who can administer the key through the KMS API.
10. Click **Next**.
11. Select the IAM users and roles that can use the KMS key in cryptographic operations.

12. Click **Next**.
13. Review the key configuration and policy, and then click **Finish**.
14. Click the key you just created and note the key ARN.

Step 2. Create an IAM policy for the key

In the AWS Management Console, create an IAM policy for the CMK to define its permissions. Note the policy name because you'll need it when you create an IAM role to access the key.

1. In the search bar, search for **IAM**.
2. Under **Access Management**, navigate to **Policies**.
3. Click **Create Policy**, switch to the JSON view, and enter the following text:

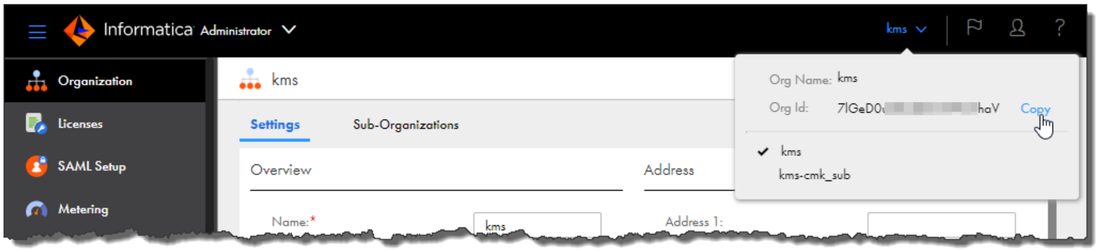
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:DescribeKey"
      ],
      "Resource": "{your key ARN}"
    }
  ]
}
```

4. Click **Next**.
5. Optionally, add tags to the policy.
6. Click **Next**.
7. Enter a meaningful name for the policy, for example, `Informatica-KMS-Access`, and click **Create policy**.

Step 3. Create an IAM role to access the key

In the AWS Management Console, create an IAM role to allow Informatica Intelligent Cloud Services to access your CMK. Note the role ARN because you'll need it when you enable customer managed keys in Informatica Intelligent Cloud Services.

To complete this step, you'll need your Informatica Intelligent Cloud Services organization ID. You can find your organization ID in the upper right corner when you log in to any service in Informatica Intelligent Cloud Services:



Org Name: kms

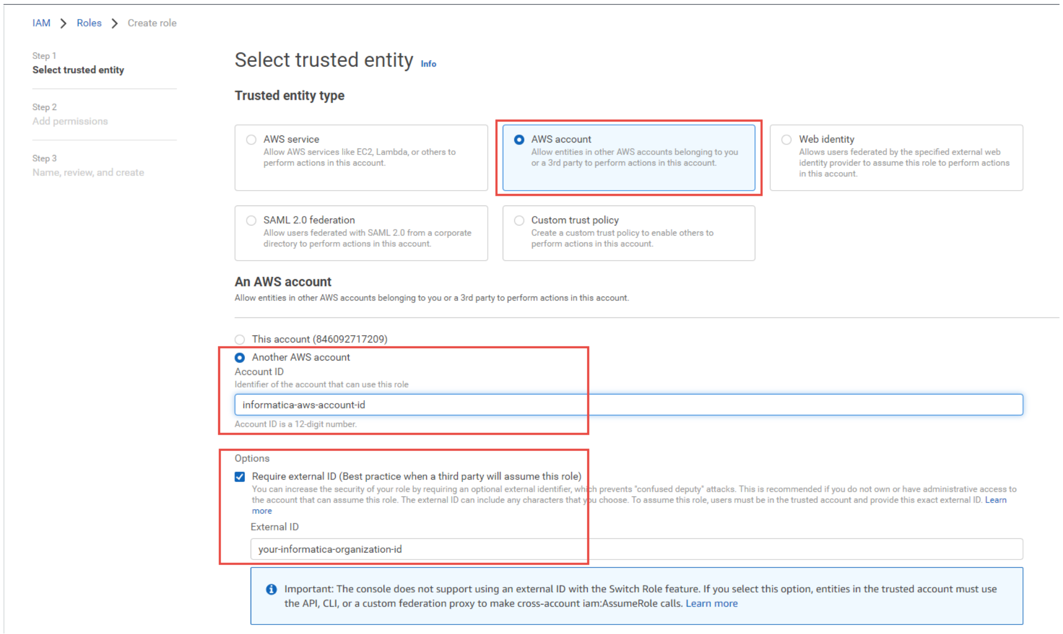
Org Id: 7lGeD0[redacted]haV

Name:* kms

Address 1:

1. In the search bar, search for **IAM**.
2. Under **Access Management**, navigate to **Roles** and click **Create role**.
3. Set the trusted entity type to **AWS account**.
4. In the **Account ID** field, enter Informatica's AWS account ID: `130917795281`

5. Enable **Require external ID**, and enter your Informatica Intelligent Cloud Services organization ID as the external ID:



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity Info

Trusted entity type

○ AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

● AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

An AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ This account (846092717209)
● Another AWS account
Account ID
Identifier of the account that can use this role
informatica-aws-account-id
Account ID is a 12-digit number.

Options
☑ Require external ID (Best practice when a third party will assume this role)
You can increase the security of your role by requiring an optional external identifier, which prevents "confused deputy" attacks. This is recommended if you do not own or have administrative access to the account that can assume this role. The external ID can include any characters that you choose. To assume this role, users must be in the trusted account and provide this exact external ID. Learn more
External ID
your-informatica-organization-id

Important: The console does not support using an external ID with the Switch Role feature. If you select this option, entities in the trusted account must use the API, CLI, or a custom federation proxy to make cross-account iam:AssumeRole calls. Learn more

6. Click **Next**.
7. Search for the policy you created in “Step 2. Create an IAM policy for the key” on page 5, for example, `Informatica-KMS-Access`, and select it.
8. Click **Next**.
9. Enter a name for the role.

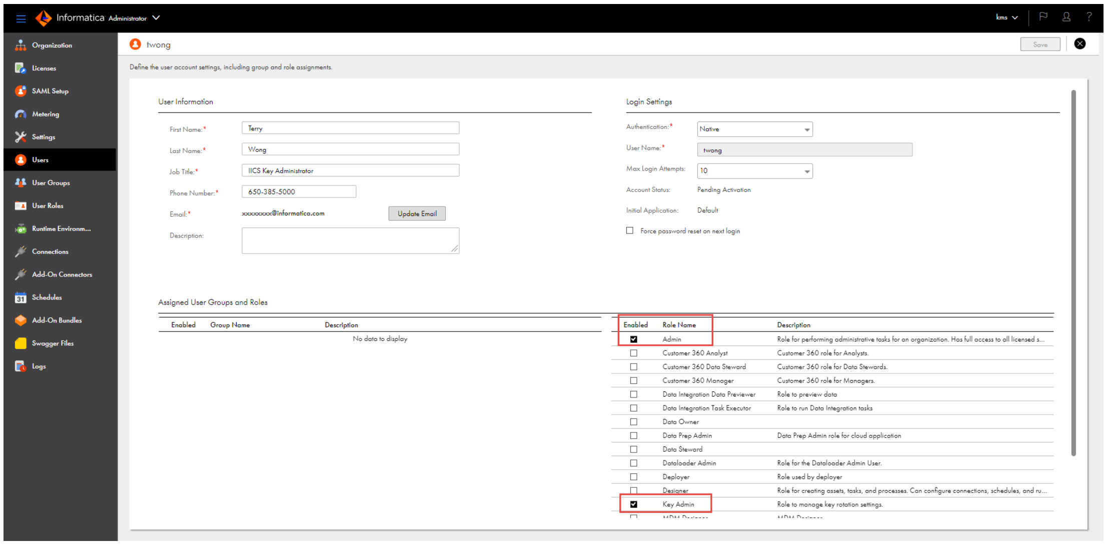
   Important: The role name must use the following prefix: `informatica-kms-cmk-access-role-`

   For example, you might name the role, `informatica-kms-cmk-access-role-prod`.
10. Review the role permissions and click **Create role**.
11. On the **Roles** page, select the role you created and note the role ARN.

Step 4. Enable customer managed keys in Informatica Intelligent Cloud Services

In Informatica Intelligent Cloud Services Administrator, open the **Settings** page and enable customer managed keys for your organization.

Note: Before you can complete this step, you need to assign at least one administrative user the **Admin** and **Key Admin** roles on the user details page in Administrator:



twong

Define the user account settings, including group and role assignments.

User Information

First Name:* Terry

Last Name:* Wong

Job Title:* IICS Key Administrator

Phone Number:* 650-385-5000

Email:* xxxxxxxx@informatica.com Update Email

Description:

Login Settings

Authentication:* Native

User Name:* twong

Max Login Attempts: 10

Account Status: Pending Activation

Initial Application: Default

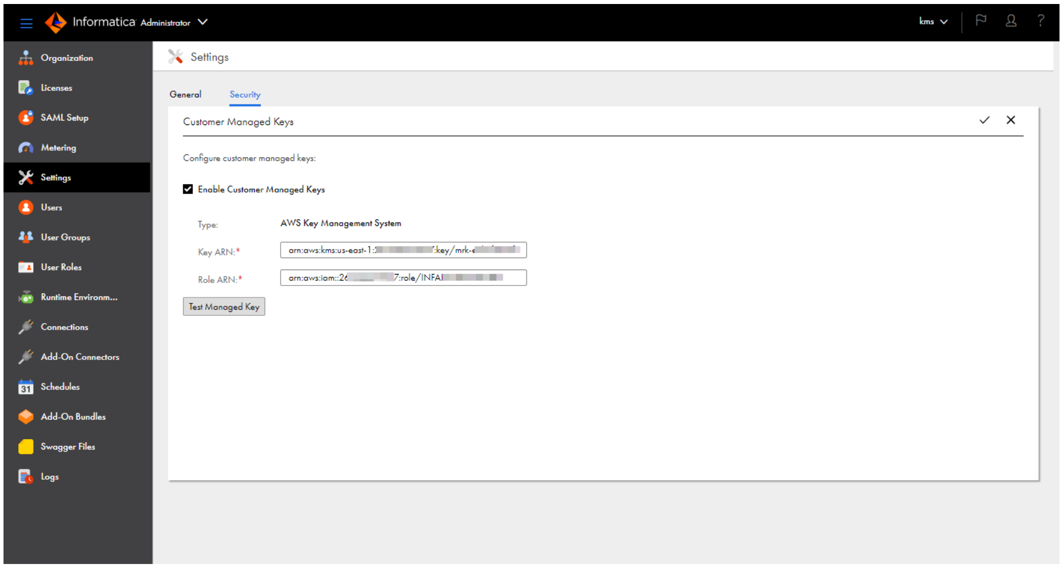
□ Force password reset on next login

Assigned User Groups and Roles

Enabled	Group Name	Description
No data to display		

Enabled	Role Name	Description
☑	Admin	Role for performing administrative tasks for an organization. Has full access to all licensed s...
□	Customer 360 Analyst	Customer 360 role for Analysts.
□	Customer 360 Data Steward	Customer 360 role for Data Stewards.
□	Customer 360 Manager	Customer 360 role for Managers.
□	Data Integration Data Previewer	Role to preview data
□	Data Integration Task Executor	Role to run Data Integration tasks
□	Data Owner	
□	Data Prep Admin	Data Prep Admin role for cloud application
□	Data Steward	
□	Dataloader Admin	Role for the Dataloader Admin User.
□	Deployer	Role used by deployer
□	Designer	Role for creating assets, tasks, and processes. Can configure connections, schedules, and ru...
☑	Key Admin	Role to manage key rotation settings.

1. Log in to Informatica Intelligent Cloud Services Administrator with a user account that has both the Admin and Key Admin roles.
2. Open the **Settings** page and click the **Security** tab.
3. Click the edit (pencil) icon.
4. Enable the **Enable Customer Managed Keys** option.
5. Enter the **Key ARN** that you created in "Step 1. Create the key in AWS KMS" on page 4 and the **Role ARN** that you created in "Step 3. Create an IAM role to access the key" on page 5:



Customer Managed Keys

Configure customer managed keys:

☑ Enable Customer Managed Keys

Type: AWS Key Management System

Key ARN:* arn:aws:kms:us-east-1:[redacted]:key/mrk-[redacted]

Role ARN:* arn:aws:iam::2[redacted]7:role/INFA[redacted]

6. Click **Test Managed Key** to test the key.

   A success message appears if the test was successful.

7. Click the save (checkmark) icon to save your changes.

   Note: It can take up to 24 hours for the key to become active.

Frequently asked questions

When I clicked **Test Managed Key** in Informatica Intelligent Cloud Services, the test failed. What should I do?

If you get an error when testing the key, perform the following checks:

- In Informatica Intelligent Cloud Services Administrator, verify that the key settings on the **Settings** page match the settings for the CMK in the AWS Management Console.
- In the AWS Management Console, verify that the status of the CMK is active.
- In the AWS Management Console, verify that the permissions on the CMK allow Informatica cryptographic access to the key.

If you continue to encounter errors, contact Informatica Global Customer Support.

What happens if the CMK is rotated in AWS KMS?

You can rotate the key in AWS KMS manually or on a schedule. Rotating a key creates a new version of the key. The old version of the key remains in AWS KMS and is used for decryption only.

Informatica Intelligent Cloud Services cannot detect key rotation in AWS KMS. Therefore, you'll need to disable customer managed keys in Informatica Intelligent Cloud Services and reenable it.

1. On the **Settings** page in Informatica Intelligent Cloud Services Administrator, click the **Security** tab and note the **Key ARN** and **Role ARN**.
2. Disable the **Enable Customer Managed Keys** option.
3. Enable the **Enable Customer Managed Keys** option, reenter the key ARN and role ARN, and click the save (checkmark) icon.

What if I need to update the CMK in AWS KMS?

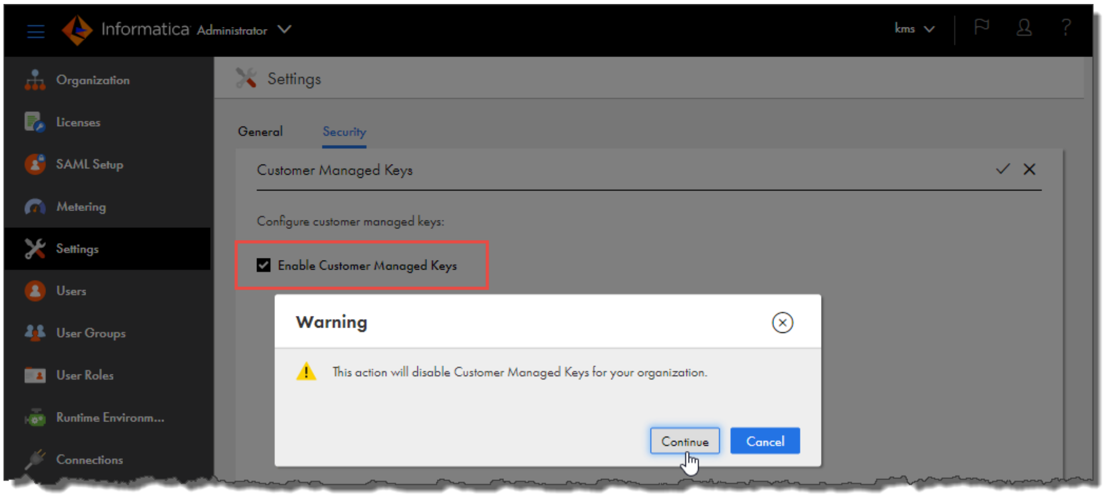
If you need to update the CMK, first provision a new CMK in AWS KMS. Then, update the key details on the **Settings** page in Informatica Intelligent Cloud Services Administrator.

Note: Be sure to keep the old version of the CMK in AWS KMS active until you update the key details in Informatica Intelligent Cloud Services.

You can delete the old version of the CMK in AWS KMS after you update the key details on the **Settings** page in Informatica Intelligent Cloud Services Administrator.

What if I want Informatica to manage key encryption?

If you want Informatica to manage key encryption, you can disable the **Enable Customer Managed Keys** option on the **Settings** page in Informatica Intelligent Cloud Services Administrator:



☑ Enable Customer Managed Keys

Warning: This action will disable Customer Managed Keys for your organization.

When you do this, be sure to keep the current version of the CMK in AWS KMS active. If the CMK is not active, disabling customer managed keys in Informatica Intelligent Cloud Services fails.

When you disable this option, your organization's encryption keys are once again encrypted using encryption keys that are managed by Informatica. It can take up to 10 minutes for the Informatica encryption keys to become active.

You can disable or delete the CMK in AWS KMS after you disable the **Enable Customer Managed Keys** option in Administrator.

What if I want to temporarily revoke Informatica's access to the CMK?

If you want to temporarily revoke Informatica's access to the CMK, you can disable the key in AWS KMS.

When you disable the CMK, Informatica Intelligent Cloud Services can no longer unencrypt your organization's encrypted data, and any jobs that use the data will fail until you reactivate the CMK in AWS KMS.

How do I replace the CMK if I suspect it has been compromised?

If you want to replace the CMK, you can delete the key in AWS KMS and create a new one.

Warning: Deleting the CMK in AWS KMS results in permanent loss to any encrypted data in Informatica Intelligent Cloud Services and causes the jobs that use the data to fail.

If you need to replace the CMK, perform the following steps so that you don't lose access to the encrypted data and jobs don't fail:

1. In Administrator, open the **Settings** page, click the **Security** tab, and disable the **Enable Customer Managed Keys** option.
2. In the AWS Management Console, delete the CMK.
3. In the AWS Management Console, create a new CMK.
4. On the **Settings** page in Informatica Intelligent Cloud Services Administrator, re-enable the **Enable Customer Managed Keys** option and enter the details for the new CMK.

Can I delete the CMK if I don't want Informatica to access any of my encrypted data?

Warning: Deleting the CMK in AWS KMS results in permanent loss to any encrypted data in Informatica Intelligent Cloud Services and causes the jobs that use the data to fail.

If you're sure that you want Informatica to forgo all access to your encrypted data in Informatica Intelligent Cloud Services, you can delete the CMK in AWS KMS.

Author

Informatica Intelligent Cloud Services Documentation Team