How-To Library

Informatica

Enable Customer Managed Keys for your Organization on Google Cloud

Abstract

This article explains how to create your own native master encryption key for Informatica Intelligent Cloud Services on Google Cloud. 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 Februrary 2024

Table of Contents

Overview

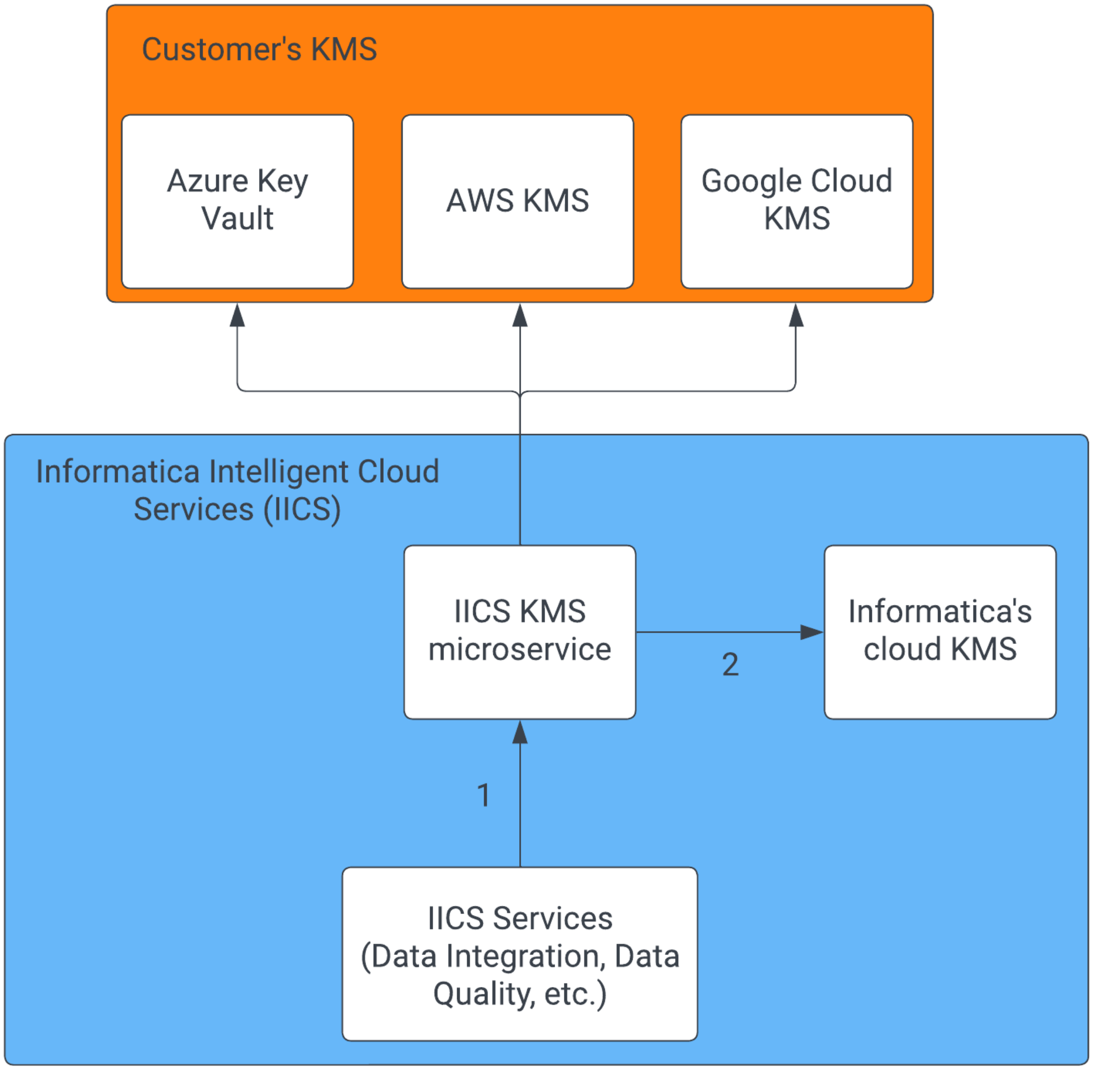
Informatica Intelligent Cloud Services protects your organization's sensitive data in the cloud using organization-specific encryption keys that are generated and stored in the Informatica Intelligent Cloud Services key management service (KMS). To prevent malicious access, the keys are encrypted using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

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 a Google Cloud POD, then you must store your CMK in Google Cloud KMS. You can't store it in AWS 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 a customer managed key

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

To create and enable a CMK, complete the following steps:

1. In the Google Cloud console, create an access role for Informatica Intelligent Cloud Services.

2. Create a Cloud KMS key ring and the key to use as your CMK.
3. Grant key access to Informatica's service account.
4. In Informatica Intelligent Cloud Services Administrator, enable customer managed keys on the **Settings** page.

Step 1. Create a role in the Google Cloud console

In the Google Cloud console, create an access role for Informatica Intelligent Cloud Services and give the role the appropriate cryptographic permissions.

1. Log in to the Google Cloud console.
2. In the **Search** bar, enter `Roles`.

   The **IAM & Admin Roles** page opens.
3. Click **Create Role**.
4. Set the role **Name** to `informatica-kms-access`.
5. Enter a **Title** and **Description**, and keep the default setting for **Role launch stage**.
6. Click **Add Permissions** and add the following permissions to the role:

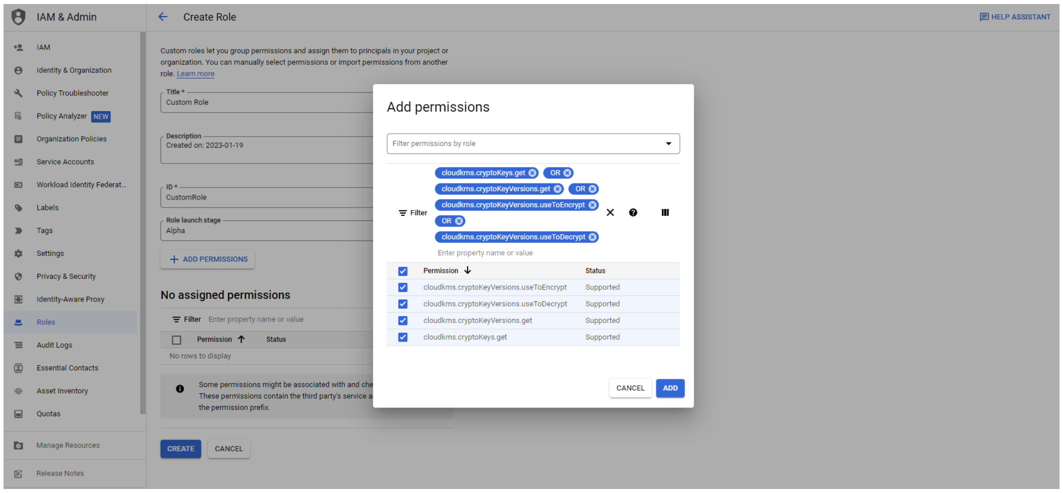
   cloudkms.cryptoKeyVersions.useToEncrypt

   cloudkms.cryptoKeyVersions.useToDecrypt

   cloudkms.cryptoKeyVersions.get

   cloudkms.cryptoKeys.get

   Tip: Use the **All Services** and **All Types** drop-down lists to filter and select permissions by services and types.



Custom roles let you group permissions and assign them to principals in your project or organization. You can manually select permissions or import permissions from another role. Learn more

Title *: Custom Role

Description: Created on: 2023-01-19

ID *: CustomRole

Role launch stage: Alpha

No assigned permissions

□	Permission ↑	Status

No rows to display

Some permissions might be associated with and che
These permissions contain the third party's service a
the permission prefix.

☑	Permission ↓	Status
☑	cloudkms.cryptoKeyVersions.useToEncrypt	Supported
☑	cloudkms.cryptoKeyVersions.useToDecrypt	Supported
☑	cloudkms.cryptoKeyVersions.get	Supported
☑	cloudkms.cryptoKeys.get	Supported

7. Click **Add**.
8. Click **Create**.

Step 2. Create the Google Cloud KMS key ring and key

Create a key ring and the symmetric key that you want to use as your CMK. Note the project, location, key ring name, key name, and key version because you will need them when you enable customer managed keys in Informatica Intelligent Cloud Services.

1. In the Google Cloud console **Search** bar, enter `Key Management`.

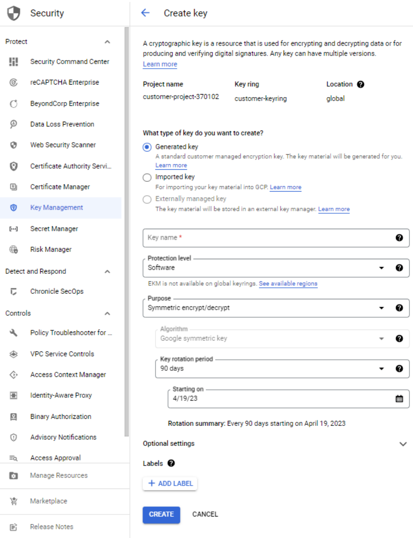
   The **Key Management** page opens.

2. Click **Create key ring**.
3. Configure the following properties for the key ring:

Property	Value
Key ring name	informatica-cmk-keyring
Location type	Region
Region	Select the appropriate region.

4. Click **Create**.
5. Select the key ring you just created.
6. Click **Create key**.
7. Configure the following properties for the key:

Property	Value
Key type	Generated key
Key name	Enter a meaningful name, for example, informatica-cmk-key.
Protection level	Software
Purpose	Symmetric encrypt/decrypt
Key rotation period	Optionally, configure a key rotation period.



Create key

A cryptographic key is a resource that is used for encrypting and decrypting data or for producing and verifying digital signatures. Any key can have multiple versions. Learn more

Project name	Key ring	Location
customer-project-370102	customer-keyring	global

What type of key do you want to create?

● Generated key
A standard customer managed encryption key. The key material will be generated for you. Learn more

○ Imported key
For importing your key material into GCP. Learn more

○ Externally managed key
The key material will be stored in an external key manager. Learn more

Key name *

Protection level: Software
EKM is not available on global keyrings. See available regions

Purpose: Symmetric encrypt/decrypt

Algorithm: Google symmetric key

Key rotation period: 90 days

Starting on: 4/19/23

Rotation summary: Every 90 days starting on April 19, 2023

8. Click **Create**.
9. Open the key and note the project, location, key ring name, key name, and key version.

Step 3. Grant key access to Informatica's service account

Grant key access to Informatica's service account to give Informatica Intelligent Cloud Services cryptographic permissions on the CMK.

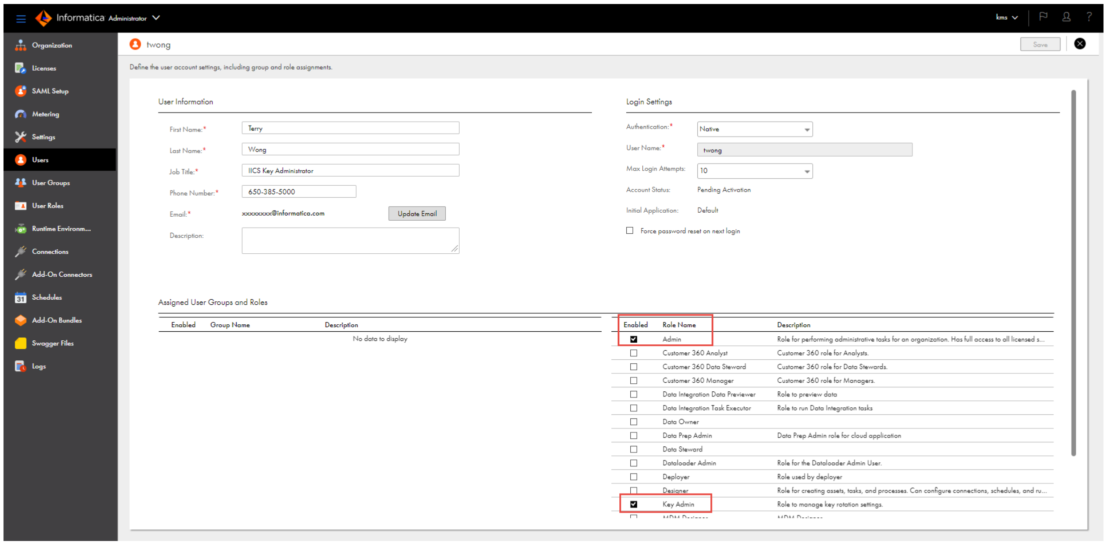
1. In the Google Cloud console, select the key you created and open the **Permissions** tab.
2. Click **Grant Access** to select the permissions to grant to the key.
3. In the dialog box that appears, under **Add Principals**, enter Informatica's service account principal: `svc-informatica-kms-connect@infa-ichsprod-iicspod1.iam.gserviceaccount.com`
4. Under **Assign roles**, search for the role you created in "Step 1. Create a role in the Google Cloud console" on page 4.
5. Click **Save**.

   Informatica Intelligent Cloud Services now has cryptographic permissions on the key.

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

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

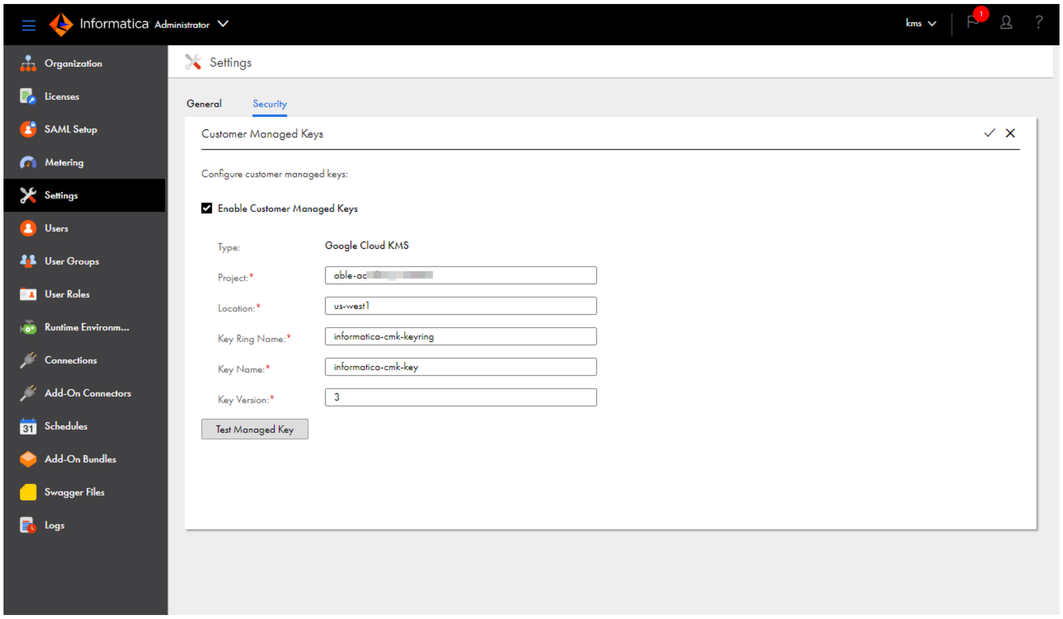
Assigned User Groups and Roles

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 **Project**, **Location**, **Key Ring Name**, **Key Name**, and **Key Version** for the CMK you created in "Step 2. Create the Google Cloud KMS key ring and key" on page 4:



Customer Managed Keys ✓ ✕

Configure customer managed keys:

☑ Enable Customer Managed Keys

Type: Google Cloud KMS

Project:* able-ac[redacted]

Location:* us-west1

Key Ring Name:* informatica-cmk-keyring

Key Name:* informatica-cmk-key

Key Version:* 3

Test Managed Key

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 Google Cloud console.
- In the Google Cloud console, verify that the status of the CMK is active.
- In the Google Cloud 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 Google Cloud KMS?

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

Informatica Intelligent Cloud Services automatically detects key rotation. When the CMK is rotated in Google Cloud KMS, Informatica Intelligent Cloud Services decrypts your organization's keys using the old CMK and then encrypts them using the new CMK.

What if I need to update the CMK in Google Cloud KMS?

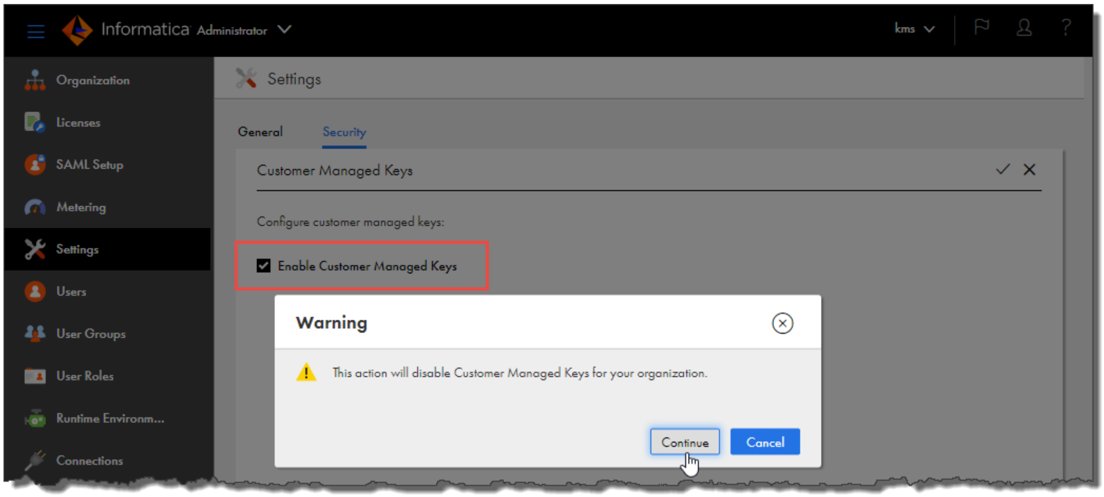
If you need to update the CMK, first provision a new CMK in Google Cloud KMS. Then, update the key details on the **Settings** page in Informatica Intelligent Cloud Services Administrator.

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

You can delete the old version of the CMK in Google Cloud 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:



Customer Managed Keys

Configure customer managed keys:

☑ 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 Google Cloud 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 Google Cloud 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 Google Cloud 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 Google Cloud 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 Google Cloud KMS and create a new one.

Warning: Deleting the CMK in Google Cloud 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 Google Cloud console, delete the CMK.
3. In the Google Cloud 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 Google Cloud 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 Google Cloud KMS.

Author

Informatica Intelligent Cloud Services Documentation Team