



# Enable Customer Managed Keys for your Organization on Microsoft Azure

<sup>©</sup> Copyright Informatica LLC 2023, 2025. Informatica and the Informatica logo are trademarks or registered trademarks of Informatica LLC in the United States and many jurisdictions throughout the world. A current list of Informatica trademarks is available on the web at https://www.informatica.com/trademarks.html

# Abstract

This article explains how to create your own native master encryption key for Informatica Intelligent Cloud Services on Microsoft Azure. 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 2025

# **Table of Contents**

Overview	2
Steps for creating and enabling the key	3
Step 1. Create a key vault	4
Step 2. Create the key	4
Step 3. Authorize Informatica's enterprise Azure application to access the key	6
Step 4. Allow Informatica's application to use the key vault	7
Frequently asked questions	9

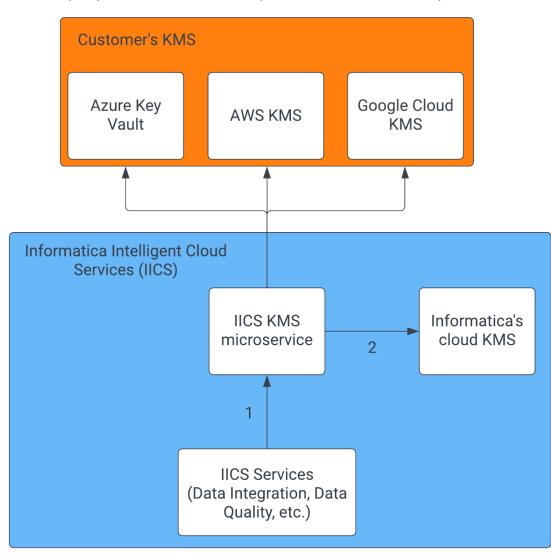
# **Overview**

Informatica Intelligent Cloud Services protects your organization's sensitive data in the cloud using organizationspecific 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 a Microsoft Azure POD, then you must store your CMK in Azure Key Vault. You can't store it in AWS KMS or Google Cloud KMS.

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 Azure Key Vault 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 Azure Key Vault, create a key vault.

- 2. In the key vault you created, generate the key to use as your CMK.
- 3. Authorize Informatica's enterprise Azure application to access the key.
- 4. Allow Informatica's enterprise application to use the Azure AD application credentials and tenant ID so that it can fetch an access token and make cryptographic calls to the key vault.

#### Step 1. Create a key vault

In Azure Key Vault, create a key vault to store your CMK. Note the key vault URI because you will need it when you allow Informatica's application to use the key vault.

- 1. Log in to the Azure portal.
- 2. In the Search box, enter Key Vault.
- 3. From the results list, select Key Vault.
- 4. In the Key Vault section, select Create.
- 5. On the **Basics** tab, configure the key vault details and click **Next**.
- 6. On the Access configuration tab, select the Vault access policy permission model, review and update the other access policies as needed, and click Next.
- 7. On the Networking tab, review the networking details and click Next.
- 8. On the Tags tab, add tags to the key vault and click Next.
- 9. On the **Review + create** tab, review the key vault configuration and click **Create**.
- 10. After deployment completes, click **Go to Resource** to view the key vault you just created and note the vault URI.
- 11. Under **Objects**, select **Keys** and check your permissions.

If you see the message "This operation is not allowed by RBAC," perform the following steps to configure your role assignment:

- a. Click Access control (IAM).
- b. On the Role assignments tab, click Add > Add role assignment.
- c. On the Add role assignment page, open the Role tab, and select the Key Vault Administrator role.
- d. On the **Members** tab, assign the Key Vault Administrator role to yourself or the user that you want to be the key vault administrator.
- e. On the Review + assign tab, verify the role assignment settings.
- f. Click Review + assign.

The key vault administrator should be able to create keys at this point.

#### Step 2. Create the key

In the key vault you created, create a symmetric key to use as your CMK. Note the key name and version because you will need them when you allow Informatica's application to use the key vault.

- 1. In the Search box, enter Key Vault.
- 2. From the results list, select the key vault you created in "Step 1. Create a key vault" on page 4.
- 3. In the left panel under **Objects**, select **Keys**.
- 4. Select Generate/Import.

5. Select **Generate** from the drop-down list, and configure the following options:

Property	Value
Name	Key name, for example, informatica-encryption-key
Кеу туре	RSA
RSA key size	2048
Set activation date	Enabled
Activation date	Today's date and time
Enabled	Yes
Set key rotation policy	Optionally, configure a key rotation policy.

#### Create a key

Options	Generate			$\sim$
Name * 🕡	informatica-encryption-key			~
Key type 🛈	• RSA			
	○ RSA-HSM ○ EC-HSM			
RSA key size	<ul> <li>2048</li> <li>2048</li> </ul>			
	<ul> <li>→ 3072</li> <li>→ 4096</li> </ul>			
	0 4096			
Set activation date (i)	$\checkmark$			
Activation date	12/22/2022	<b></b>	4:00:28 PM	
	(UTC-08:00) Pacific Time (US & Canada)			$\sim$
Set expiration date 🕕				
Enabled	Yes No			
Tags	0 tags			
Set key rotation policy	Not configured			
Confidential Key Options				
Exportable ①				
Immutable (i)				
Confidential operation policy 🕕				
connucliation policy ()				$\sim$

- 6. Click Create.
- 7. Click the key and note the key name and version.

### Step 3. Authorize Informatica's enterprise Azure application to access the key

In Informatica Intelligent Cloud Services Administrator, open the **Settings** page and enable customer managed keys for your organization. Then grant the Informatica KMS Connect app permissions to access your CMK.

**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:

😑 🔶 Informatica 🛤	leninistrator 🗡					kmo v   F	8
Gragonization	O twong					Save	8
🛃 Licenses	Define the user account settings, including group and role assignments.						
🙆 SAML Setup	User Information	Login Se	diam				
n Metering		_	-				-
🄀 Settings	First Norme:" Terry	Authentic	140	Ive	*		11
O Users	Last Name:* Wong	User Nar		ong			-11
4 User Groups	Job Title:* IICS Key Administrator	Max Logi	n Attempts: 10		Ŧ		-11
	Phone Number:* 650-385-5000	Account	Status: Pena	ing Activation			- 11
User Roles	Email * Vacance Update Email	Initial App	alication: Defa	oh.			-11
💑 Runtime Environm	Description:	Foro	e password reset on	next login			-11
/ Connections							-11
🗯 Add-On Connectors							-11
31 Schedules	Assigned User Groups and Roles						-11
🥪 Add-On Bundles	Enabled Group Name Description	Enabled	Role Name		Description		-11
Swogger Files	No data to display		Admin		Role for performing administrative tasks for an a	rganization. Has full access to all licensed s	- 11
			Customer 360 A	nalyst	Customer 360 role for Analysts.		- 11
📷 logs			Customer 360 D		Customer 360 role for Data Stewards.		- 1-1
			Customer 360 N		Customer 360 role for Managers.		- 1-1
			Data Integration		Role to preview doto		- 1-1
			Data Integration	Tosk Executor	Role to run Data Integration tasks		- 1-1
			Data Owner Data Prep Admir		Data Prep Admin role for cloud application		- 1-1
			Data Prep Admin Data Steward		Data Prep Admin role for close application		- 1.1
			Dataloader Adm	in .	Role for the Dataloader Admin User.		- 14
			Deployer		Role used by deployer		
			Designer		Role for creating assets, tasks, and processes. C	an configure connections, schedules, and ru	
			Key Admin		Role to manage key rotation settings.		
		-	MDM D		иби б		

- 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. In Step 1. Authorize Application, enter the Tenant ID of your Azure Subscription.

= 🔖 Informatica Administrator 🗸		kms ∨		
nganization 🔀 Settings				
🖗 Licenses General Security				
Customer Managed Keys			~ ×	
Metering     Configure customer managed keys:				
✗ Settings ✓ Enable Customer Managed Ke	ys			
Users Type:*	Azure Key Vault			
4 User Groups				
User Roles Step 1. Authorize Application	Sino Jaho			
Runtime Environm	Sfao loba-			
Connections Step 2. Configure Managed K				
31 Schedules Key Vault URL*				
Add-On Bundles Key Name:*				
Swagger Files Key Version:*				
🔁 Logs	Test Managed Key			
Advanced Clusters				

Tip: You can find the Tenant ID under Properties in Azure Active Directory.

- 6. Click Authorize.
- 7. When prompted, sign in to your Azure account.

Note: You must sign in with a user account that has the Cloud Application Administrator role.

8. In the Permissions requested dialog, click Accept to grant permissions to the Informatica KMS Connect app.

#### Step 4. Allow Informatica's application to use the key vault

Allow the Informatica KMS Connect app to use the Azure AD application credentials and tenant ID. To do this, first create an access policy for the Informatica KMS Connect app in Azure Key Vault, and then enter the key information on the **Settings** page in Informatica Intelligent Cloud Services.

- 1. Log in to the <u>Azure portal</u>.
- 2. In the Search box, enter Key Vault.
- 3. From the results list, select Key Vault.
- 4. Select the key vault you created in <u>"Step 1. Create a key vault" on page 4.</u>
- 5. In the left panel, select Access Policies.
- 6. Click Create to create a new access policy for the Informatica KMS Connect app.
- 7. Grant the following permissions:

Get List Decrypt Encrypt Unwrap Key

#### Wrap Key

#### Create an access policy

customer-nmk-vault-1		
Select a template	$\checkmark$	
Key permissions	Secret permissions	Certificate permissions
Key Management Operations	Secret Management Operations	Certificate Management Operations
Select all	Select all	Select all
✓ Get	Get	Get
🖌 List	List	List
Update	Set	Update
Create	Delete	Create
Import	Recover	Import
Delete	Backup	Delete
Recover	Restore	Recover
Backup	Privileged Secret Operations	Backup
Restore	Select all	Restore
Cryptographic Operations		Manage Contacts
Select all	Purge	Manage Certificate Authorities
Decrypt		Get Certificate Authorities
Encrypt		List Certificate Authorities
<ul> <li>Unwrap Key</li> </ul>		Set Certificate Authorities
<ul> <li>Onwiap Key</li> <li>Wrap Key</li> </ul>		Delete Certificate Authorities
Verify		Privileged Certificate Operations
Sign		Select all
L Sign		_

- 8. Under Principal, search for Informatica KMS Connect and select it.
- 9. Click Next.
- 10. Review and create the access policy.
- 11. Log in to Informatica Intelligent Cloud Services Administrator with a user account that has both the Admin and Key Admin roles.
- 12. Open the **Settings** page and click the **Security** tab.
- 13. Click the edit (pencil) icon.

14. In Step 2. Configure Managed Key, enter the Key Vault URI, Key Name, and Key Version:

Ξ	🔶 Informatica 🗛	Administrator V	km: v   F 9	?
÷	Organization	🔀 Settings		
	Licenses	Oeneral Security		
6	SAML Setup	Customer Managed Keys	~ ×	
0	Metering	Configure customer managed keys:		
×	Settings	✓ Enable Customer Managed Keys		
2	Users			
44	User Groups	Type:* Azure Key Vault		
-	User Roles	Step 1. Authorize Application		
ē	Runtime Environm	Tenont ID.* 5fee19e-4282-9126-178-02546600 Authorize with a different Tenont ID		
ļ,	Connections			
ļ,	Add-On Connectors	Step 2. Configure Managed Key		
31	Schedules	Kay Youk URL* https://ics couve.net/		
<b></b>	Add-On Bundles			
	Swagger Files	Key Version:* 619e		
R	Logs			
	Advanced Clusters			

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

A success message appears if the test was successful.

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 Azure portal.
- In the Azure portal, verify that the status of the CMK is active.
- In the Azure portal, 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 Azure Key Vault?

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

Informatica Intelligent Cloud Services automatically detects key rotation. When the CMK is rotated in Azure Key Vault, 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 Azure Key Vault?

If you need to update the CMK, first provision a new CMK in Azure Key Vault. 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 Azure Key Vault active until you update the key details in Informatica Intelligent Cloud Services.

You can delete the old version of the CMK in Azure Key Vault 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:

$\equiv$	Informatica Adm	ministrator V	kms∨ ₽2?
-	Organization	💥 Settings	
6	Licenses	General Security	
2	SAML Setup	Customer Managed Keys	✓ ×
<b>(</b>	Metering	- Configure customer managed keys:	
×	Settings	Enable Customer Managed Keys	
2	Users		
44	User Groups	Warning	
	User Roles	1 This action will disable Customer Managed Keys for your organization.	
1-00	Runtime Environm		
1	Connections	Continue Concel	

When you do this, be sure to keep the current version of the CMK in Azure Key Vault 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 Azure Key Vault 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 Azure Key Vault.

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 Azure Key Vault.

#### 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 Azure Key Vault and create a new one.

**Warning:** Deleting the CMK in Azure Key Vault 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 Azure portal, delete the CMK.
- 3. In the Azure portal, 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 Azure Key Vault 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 Azure Key Vault.

## **Author**

Informatica Intelligent Cloud Services Documentation Team