# Sangfor HCI and Thales CipherTrust KMS Implementation Guide

**Product Version** 6.8.0

# Overview:

This implementation guide provides step-by-step instructions for deploying Sangfor HCI and Thales CipherTrust KMS together to create a comprehensive data security solution. Sangfor HCI is a hyper-converged infrastructure platform that integrates computing, storage, and networking in a single appliance, while Thales CipherTrust KMS provides a secure and centralized platform for managing encryption keys.

# Prerequisites:

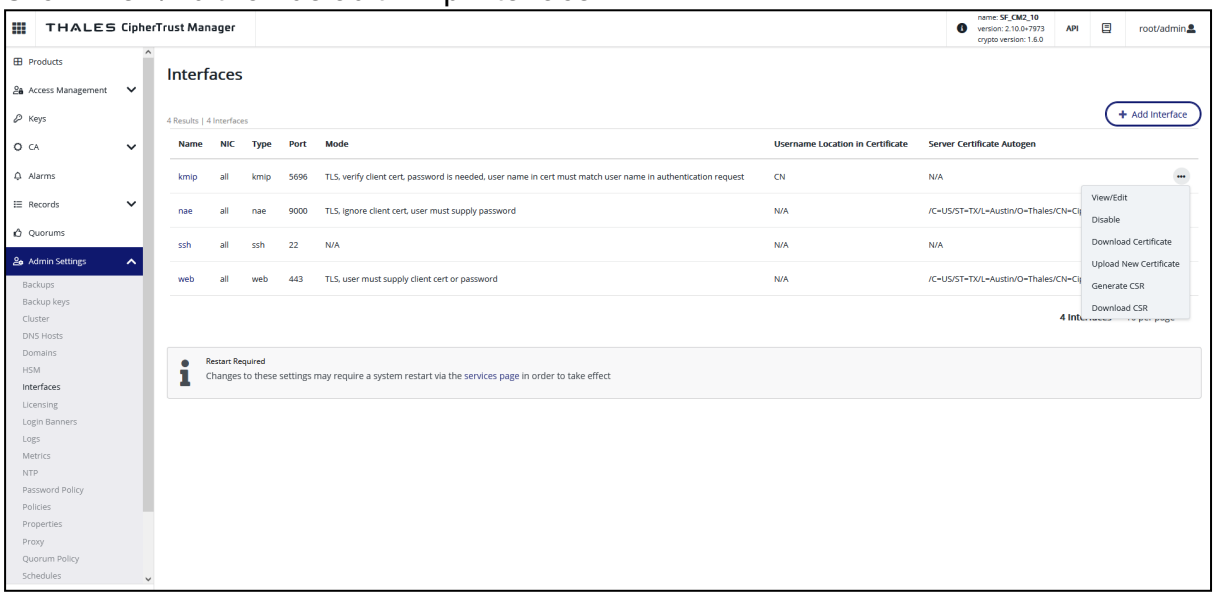
Before deploying Sangfor HCI and Thales CipherTrust KMS, ensure that the following prerequisites are met:
Sangfor HCI hardware and software have been installed and configured.
Thales CipherTrust KMS hardware and software have been installed and configured.
A network connection has been established between the Sangfor HCI and Thales CipherTrust KMS appliances.

# Table of Content:

# CipherTrust Manager system configuration

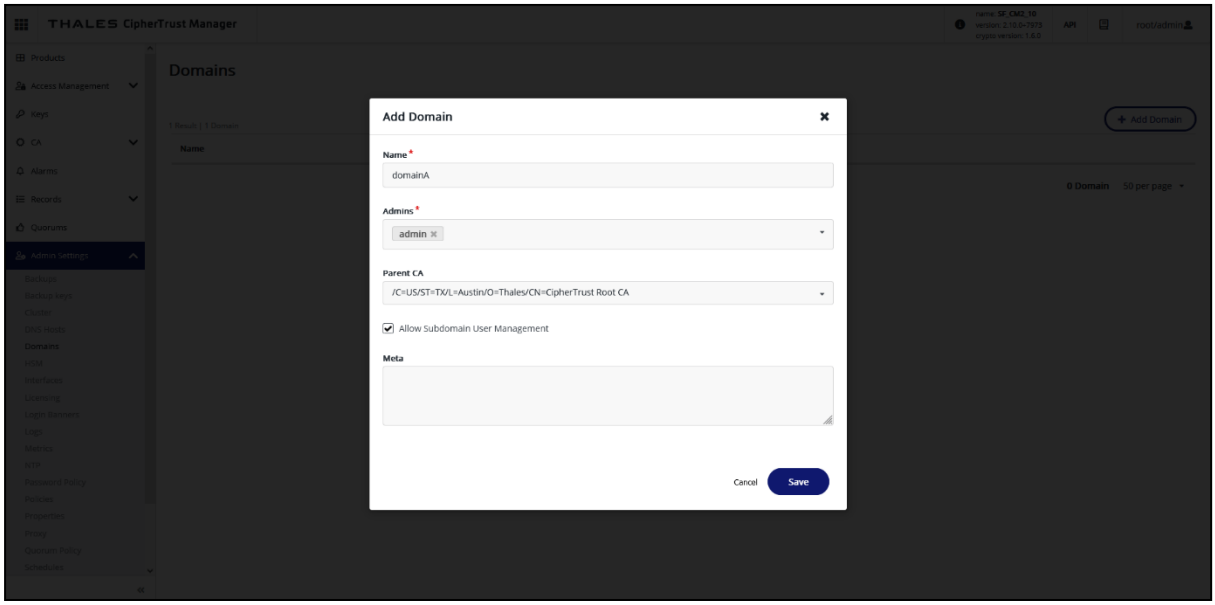
## Update KMIP interface Mode

Go to “Admin Settings” → “Interfaces”
Click “View/Edit” on default kmip interface



## Create Sub Domain

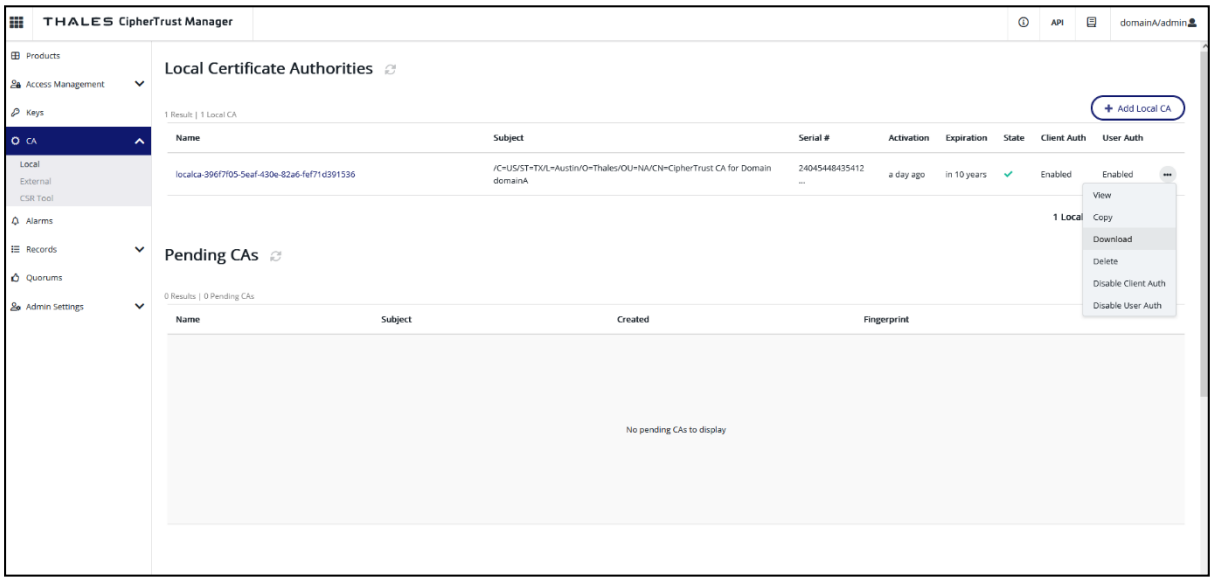
Go to “Admin Settings” → “Domains”
Click “+Add Domain”
Name: domainA
Admin: admin
Parent CA: select default root CA



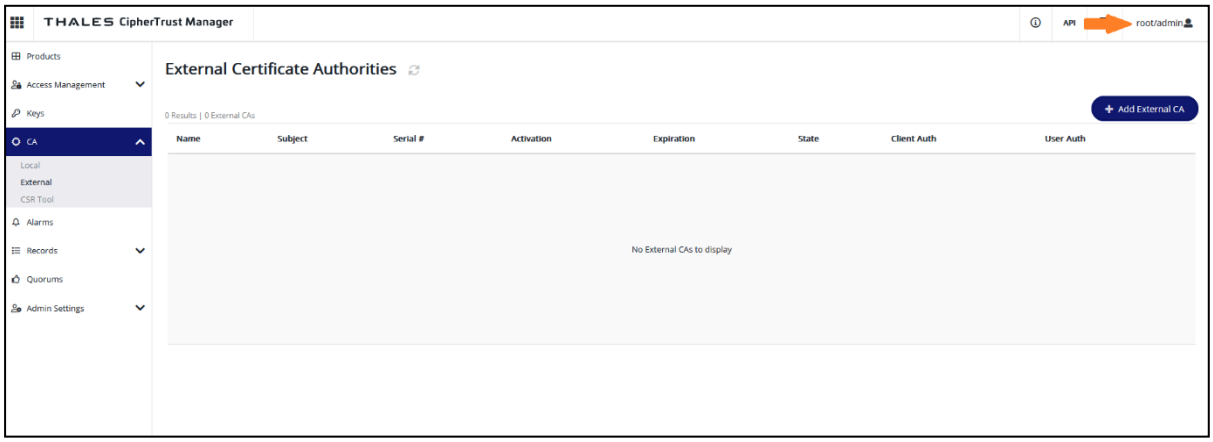

Result:

## Import sub domain CA certificate to root domain

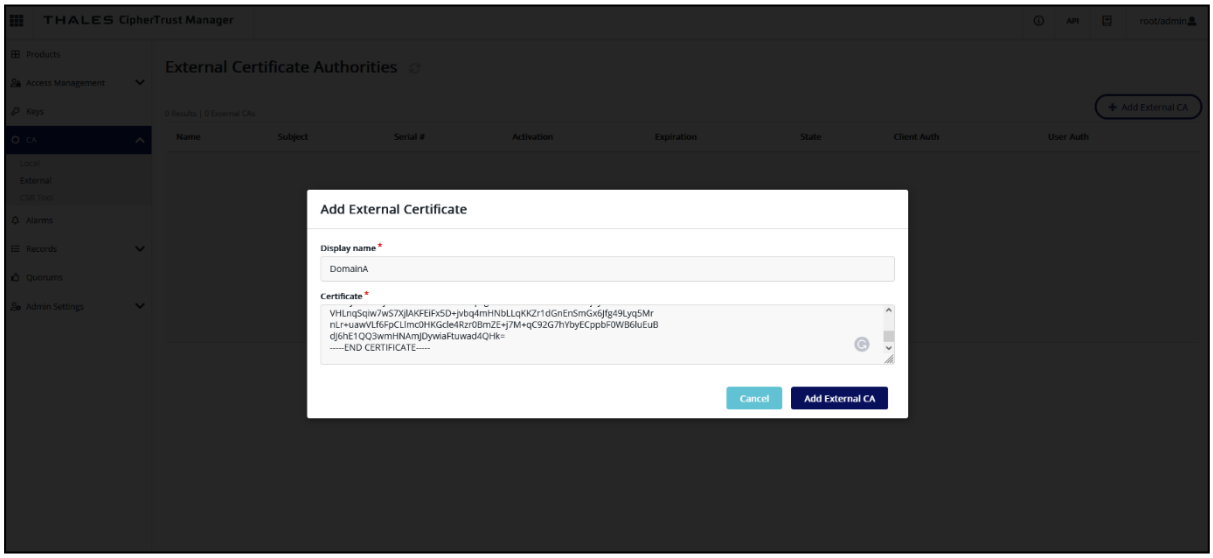
Switch to sub domain **domainA** at top-right corner
Click “CA” → “Local”
Click “Download” to download domainA default CA certificate




Import sub domainA CA certificate to root domain External CA List
Switch to root domain at top-right corner
Click “CA” → “External” → “Add External CA”



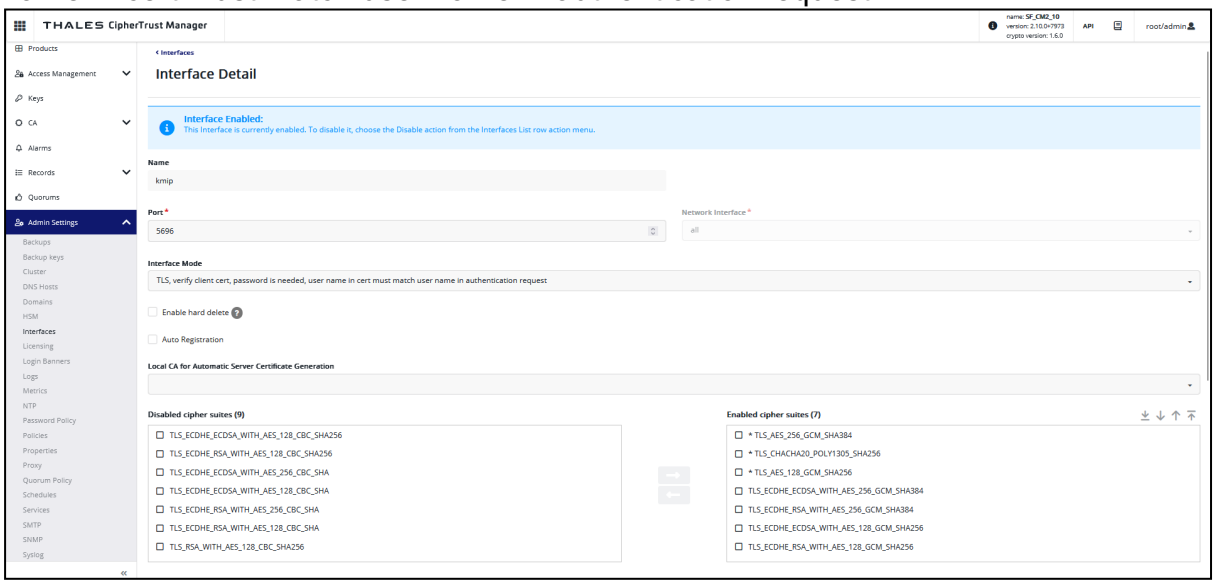
Display name: DomainA
Certificate: paste the domainA CA certificate content
Click “Add External CA”




Result:

## Update KMIP interface configuration

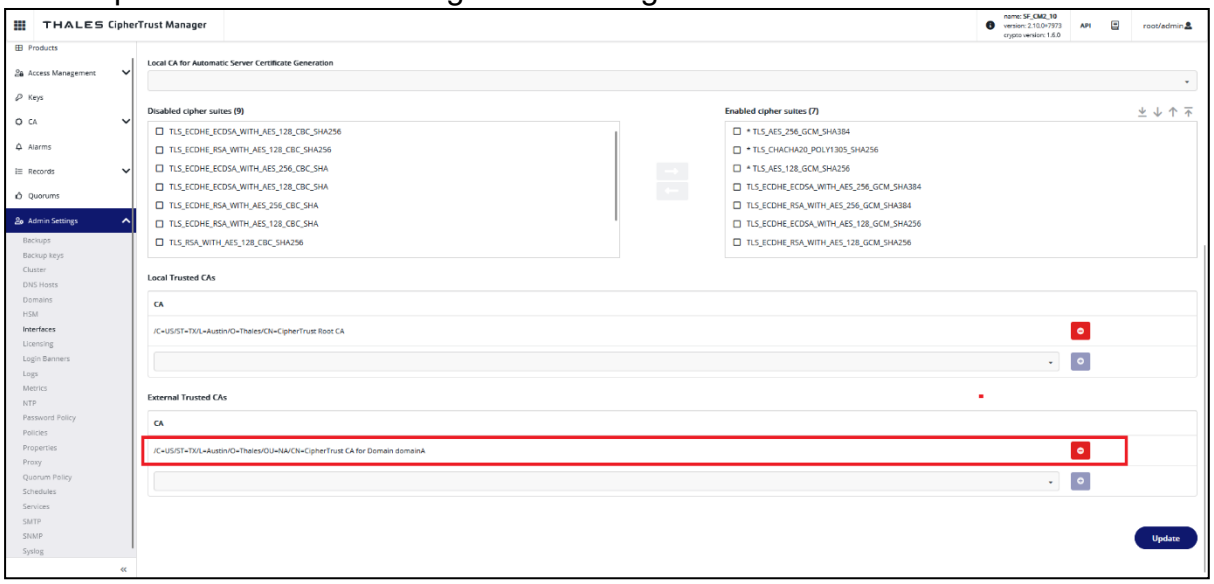
Change the interface Mode to “TLS, verify client cert, password is needed, user name in cert must match user name in authentication request ”



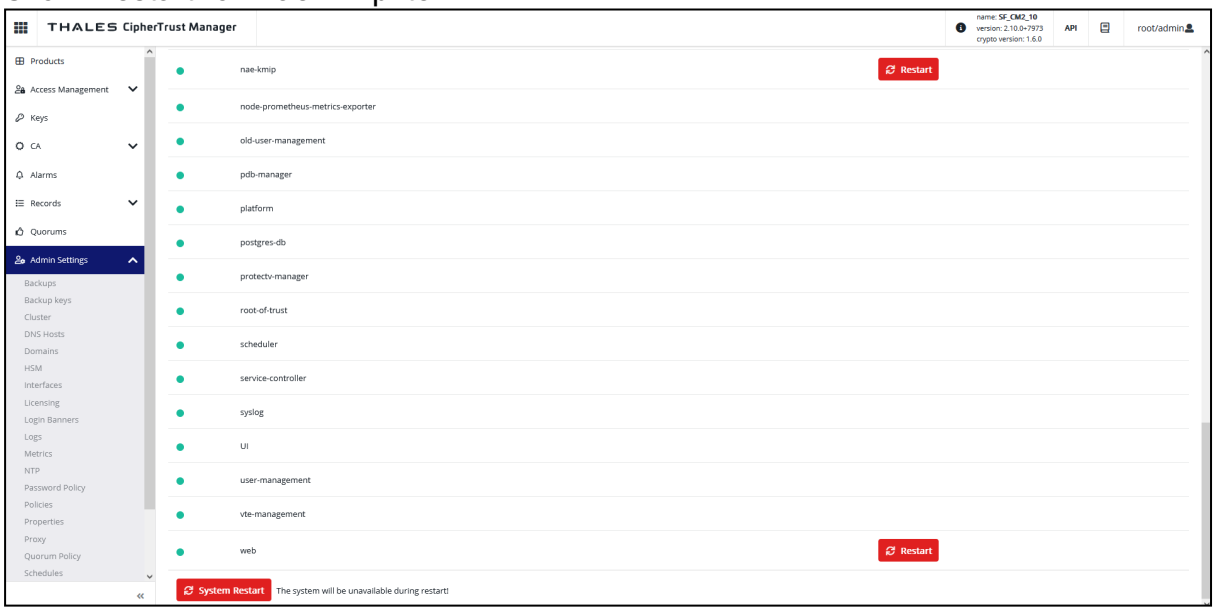

Scroll down to External Trusted CA section

Click “+” to add the sub domain domainA CA certificate

Click “Update” to save the configuration change



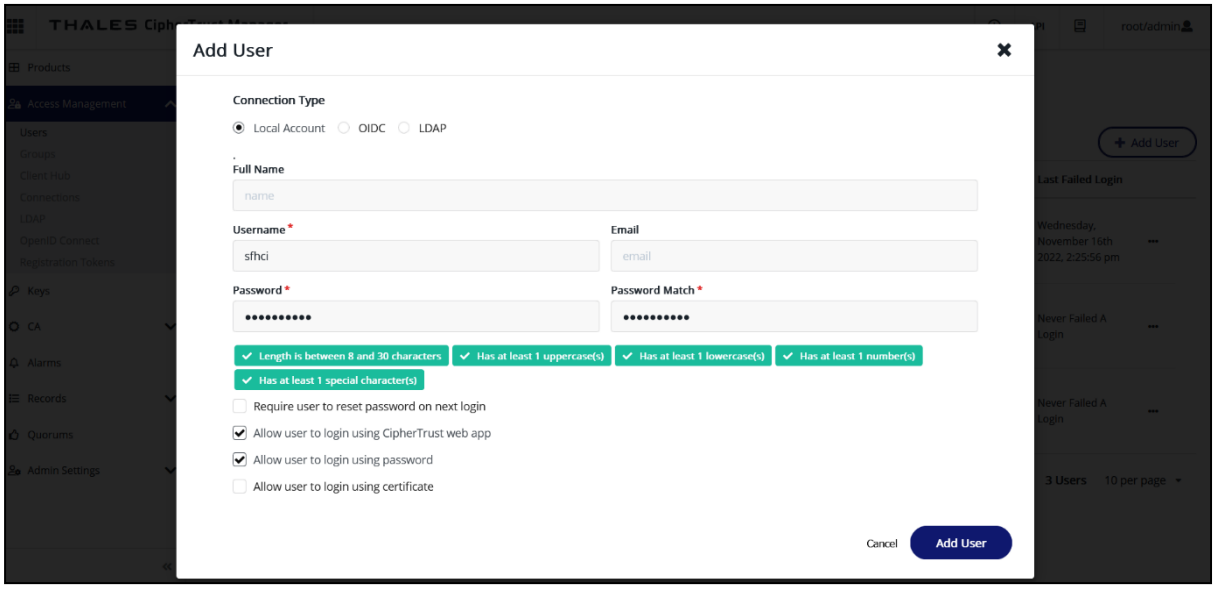
Restart the KMIP service after configuration change
Go to “Services”
Click “Restart” on nae-kmip item



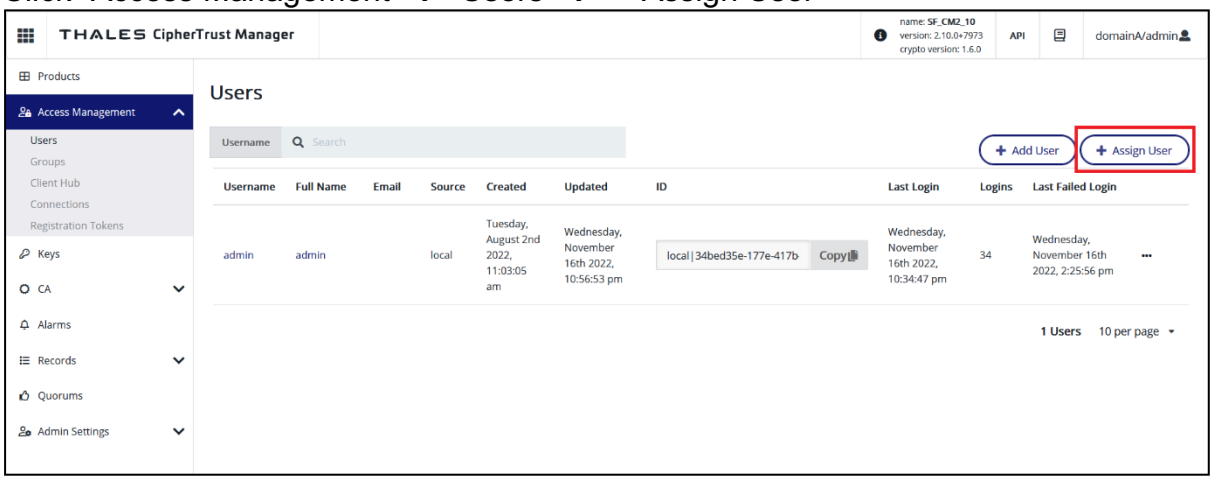
# KMIP client registration on CipherTrust Manager

## Create users for Sangfor HCI login to CipherTrust Manger via KMIP interface

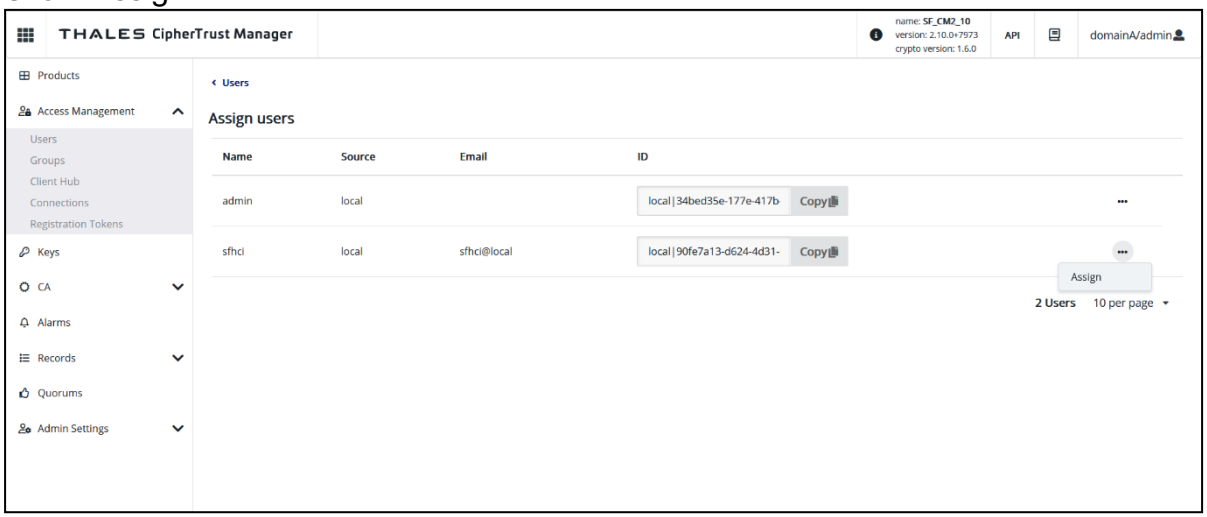
Create user “sfhci” at root domain and assign it to sub domain domainA
Access Management → Users → + Add User
Username: sfhci
Password: type a secure password
Click “Add User”



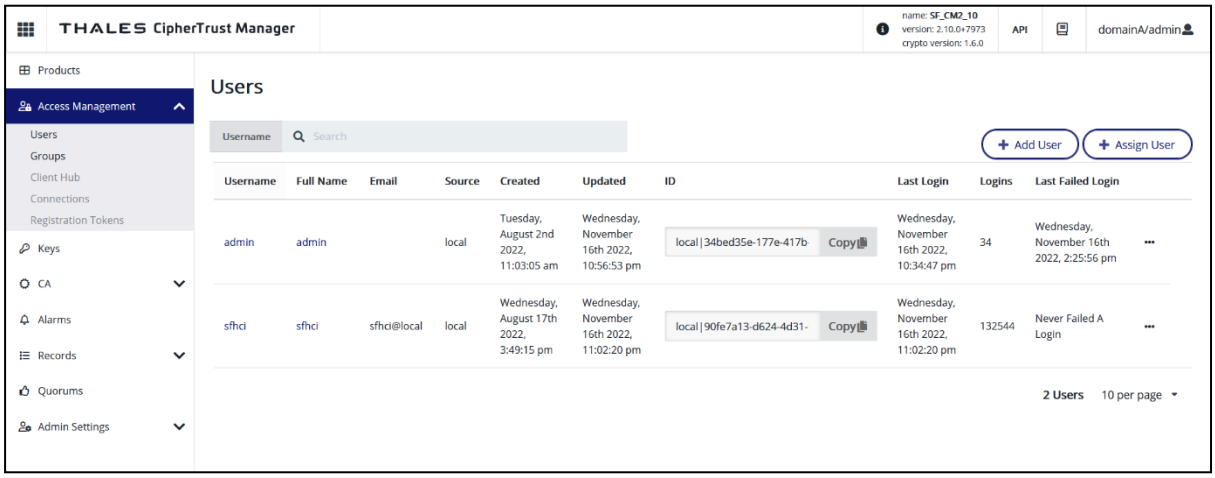

Assign user “sfhci” from root to domainA
Switch to sub domain domainA at top-right corner
Click “Access Management” → “Users” → “+ Assign User”



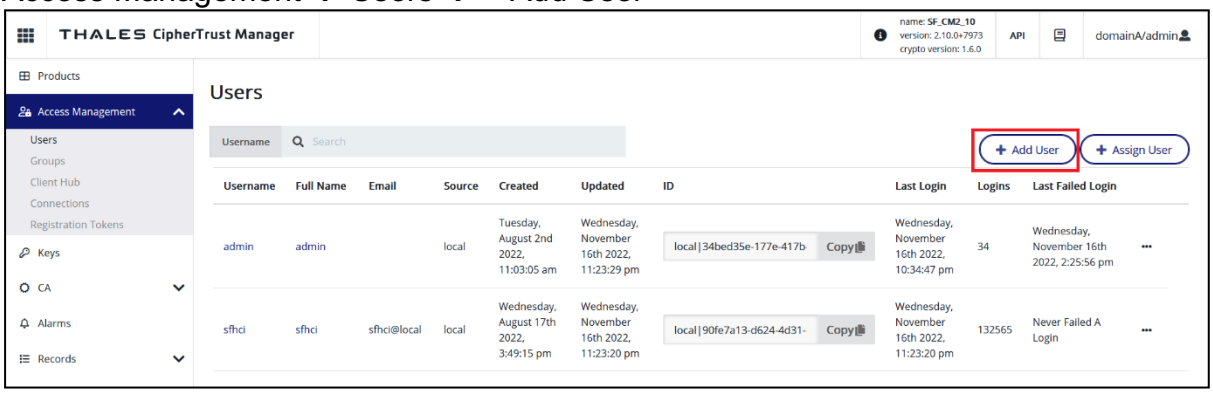
Click “Assign”



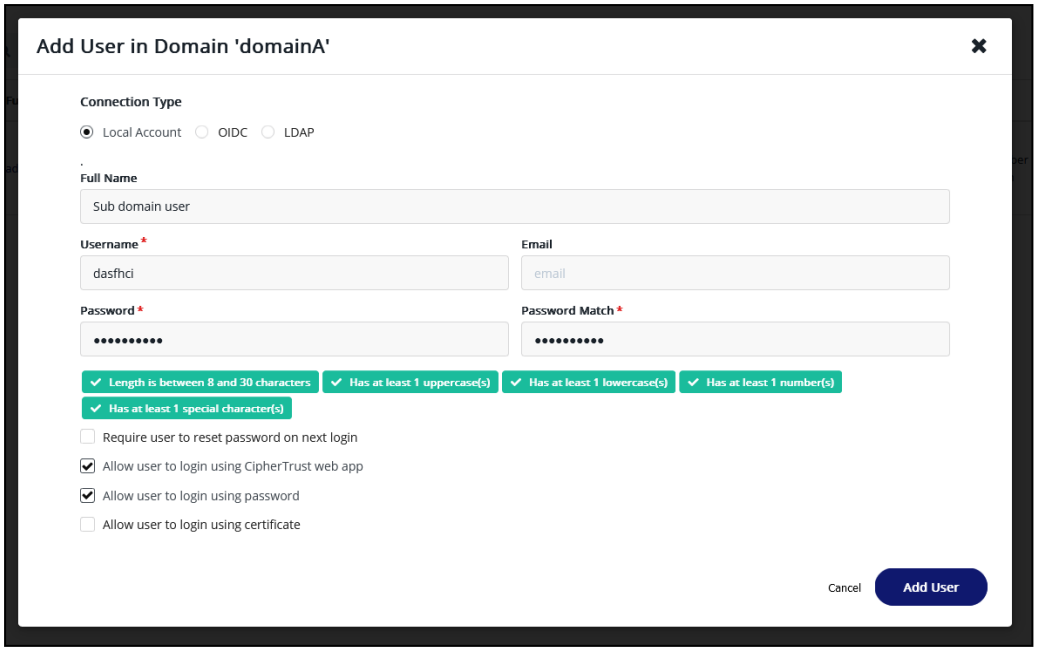

Result:



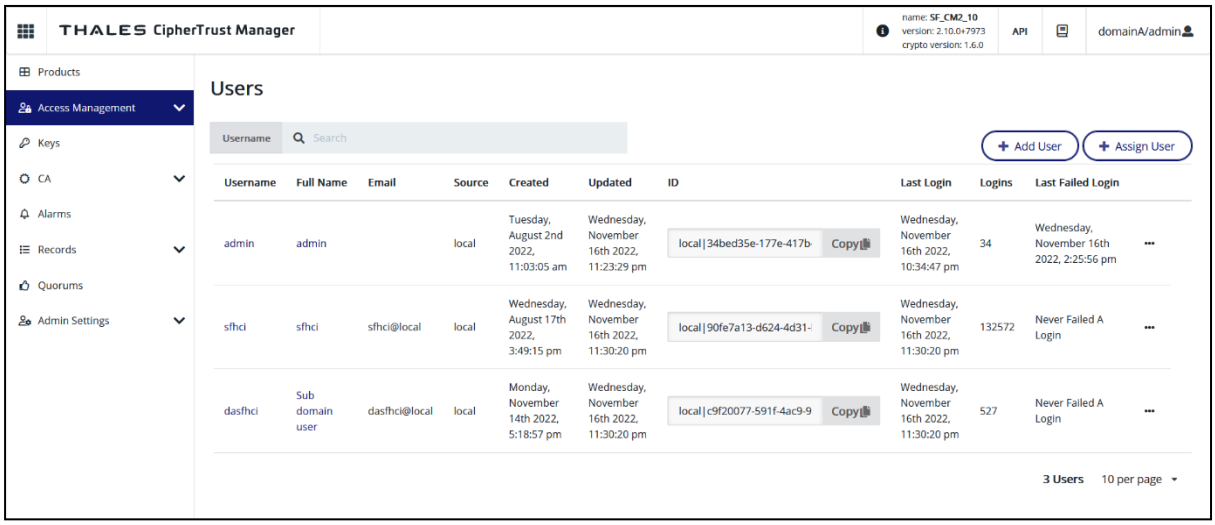

Create user “dasfhci” at domain domainA
Access Management → Users → + Add User




Username: dasfhci
password: type a secure password
Click “Add user”

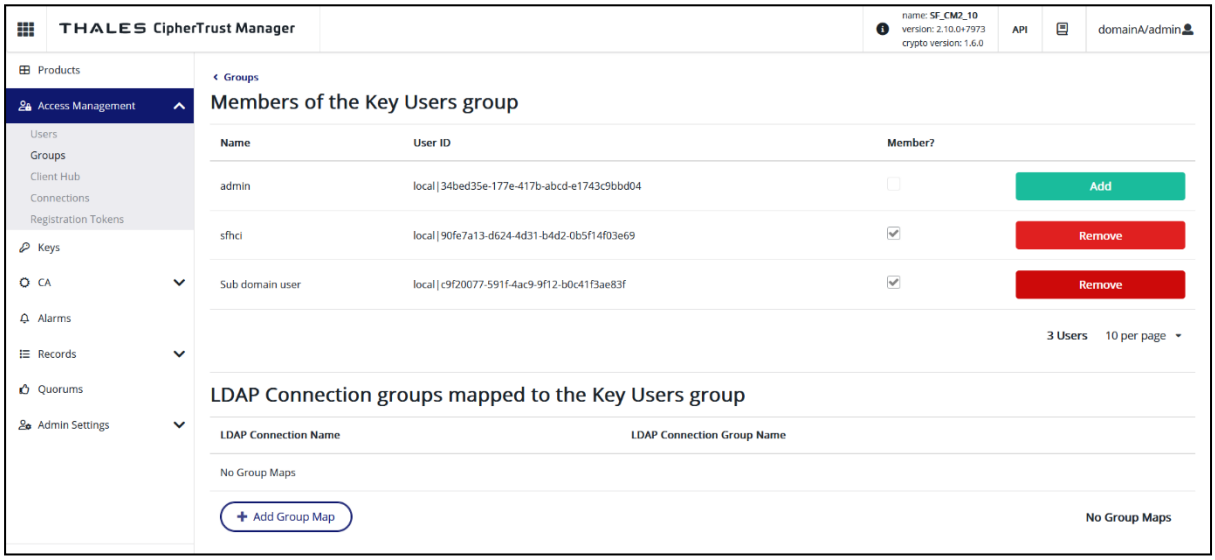

Add User in Domain 'domainA'
Connection Type
Local Account
OIDC
LDAP
Full Name
Sub domain user
Username *
dasfhci
Email
email
Password *
Password Match *
Length is between 8 and 30 characters
Has at least 1 uppercase(s)
Has at least 1 lowercase(s)
Has at least 1 number(s)
Has at least 1 special character(s)
Require user to reset password on next login
Allow user to login using CipherTrust web app
Allow user to login using password
Allow user to login using certificate
Cancel
Add User

Result:


THALES CipherTrust Manager
name: SF_CM2_10
version: 2.10.0+7973
crypto version: 1.6.0
API
domainA/admin
Products
Access Management
Keys
CA
Alarms
Records
Quorums
Admin Settings
Users
Username
Search
Add User
Assign User
Username
Full Name
Email
Source
Created
Updated
ID
Last Login
Logins
Last Failed Login
admin
admin
local
Tuesday, August 2nd 2022, 11:03:05 am
Wednesday, November 16th 2022, 11:23:29 pm
local|34bed35e-177e-417b-
Copy
Wednesday, November 16th 2022, 10:34:47 pm
34
Wednesday, November 16th 2022, 2:25:56 pm
sfhci
sfhci
sfhci@local
local
Wednesday, August 17th 2022, 3:49:15 pm
Wednesday, November 16th 2022, 11:30:20 pm
local|90fe7a13-d624-4d31-
Copy
Wednesday, November 16th 2022, 11:30:20 pm
132572
Never Failed A Login
dasfhci
Sub domain user
dasfhci@local
local
Monday, November 14th 2022, 5:18:57 pm
Wednesday, November 16th 2022, 11:30:20 pm
local|c9f20077-591f-4ac9-9
Copy
Wednesday, November 16th 2022, 11:30:20 pm
527
Never Failed A Login
3 Users
10 per page

Add users to “Key Users” group
At domainA
Click “Access Management” → “Groups” → filter with “Key Users” → “View/Edit”

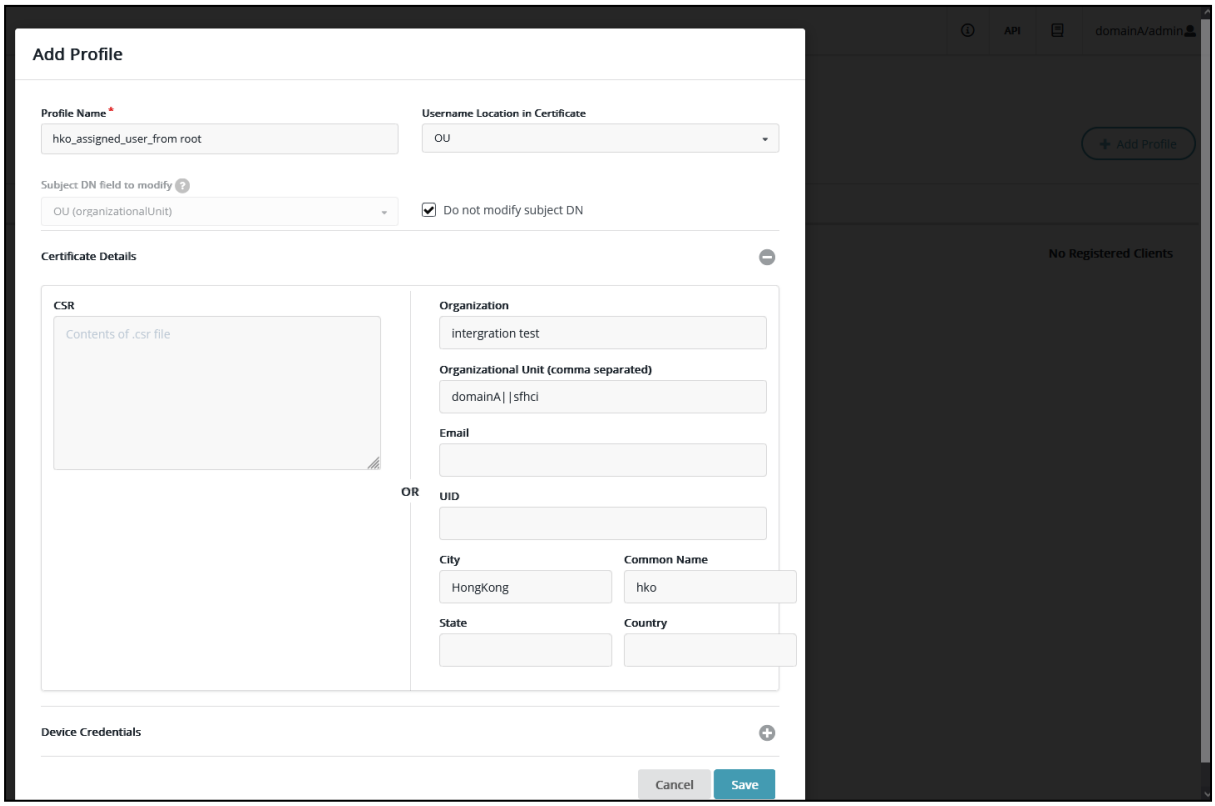

Click “Add” on **sfhci** and **Sub domain user (dasfhci)**
Result:




## Create KMIP Client Profile for sfhci user at domainA

Go to “Products” → “KMIP” → “Client Profile”
Click “+ Add Profile”
Profile Name: hko_assigned_user_from root
Username Location in Certificate: select OU (KMIP user authentication will take the username form the Organization Unit filed in the client certificate)
Organizational Unit: **domainA||sfhci**

Common Name: hko

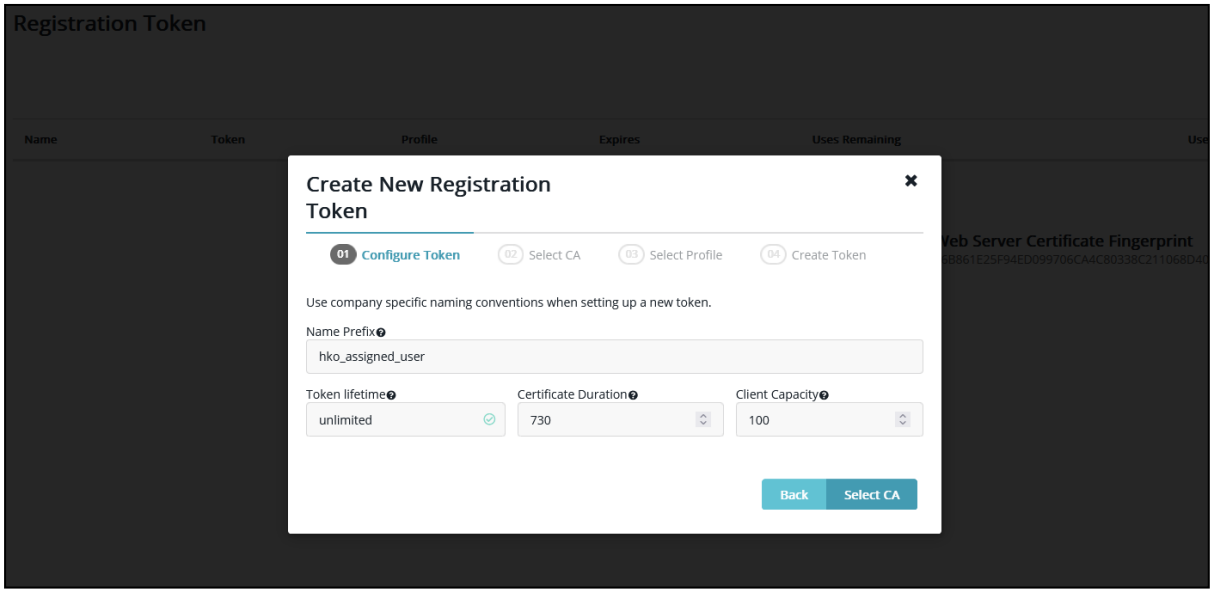



Result:

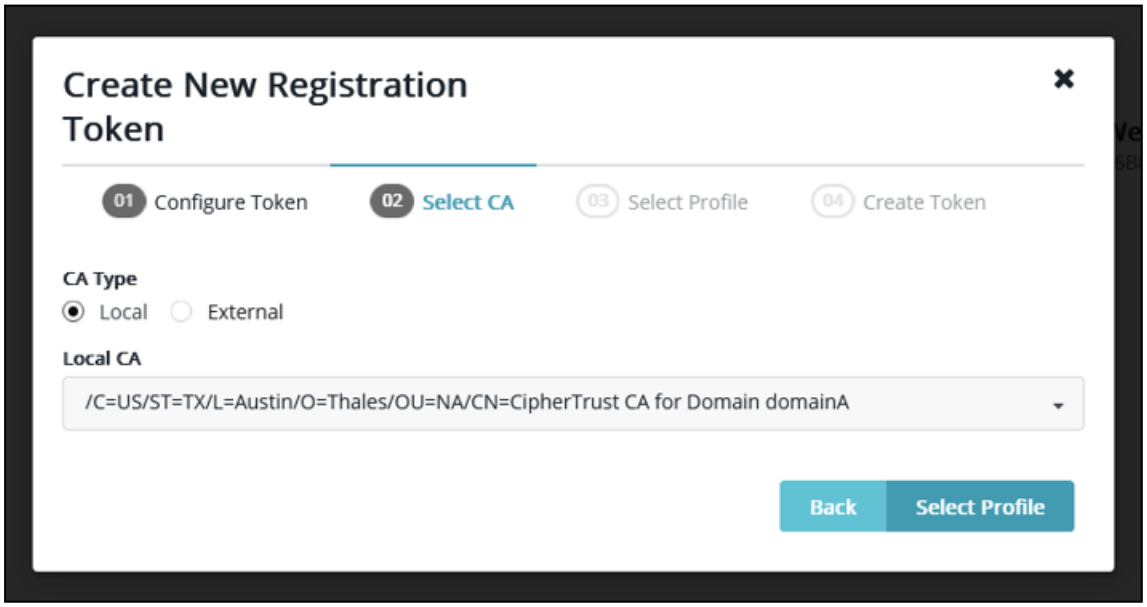
## Create KMIP Registration Token for sfhci user at domainA

Go to “Registration Token” tab
Click “+ New Registration Token”

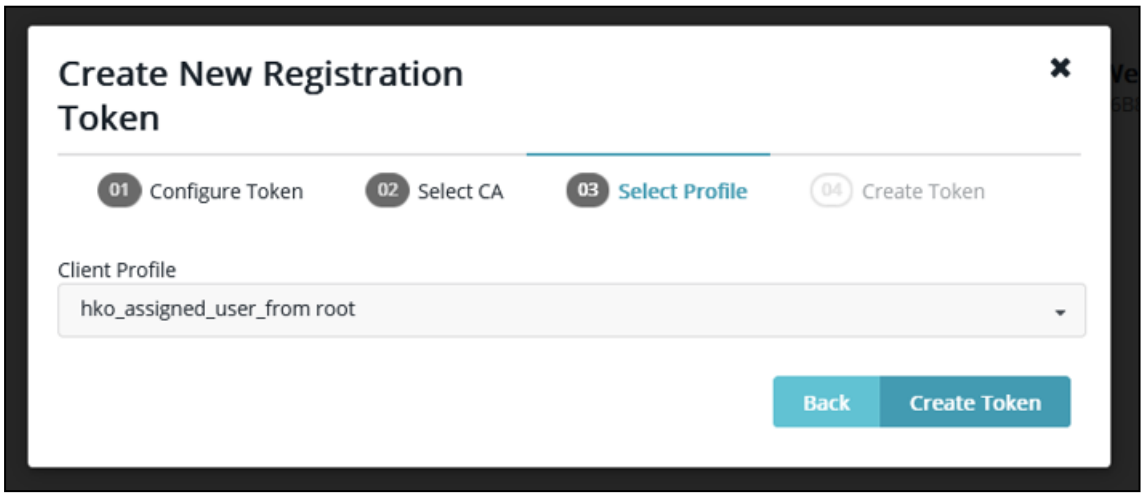
Name Prefix: hko_assigned_user
Click “Select CA”



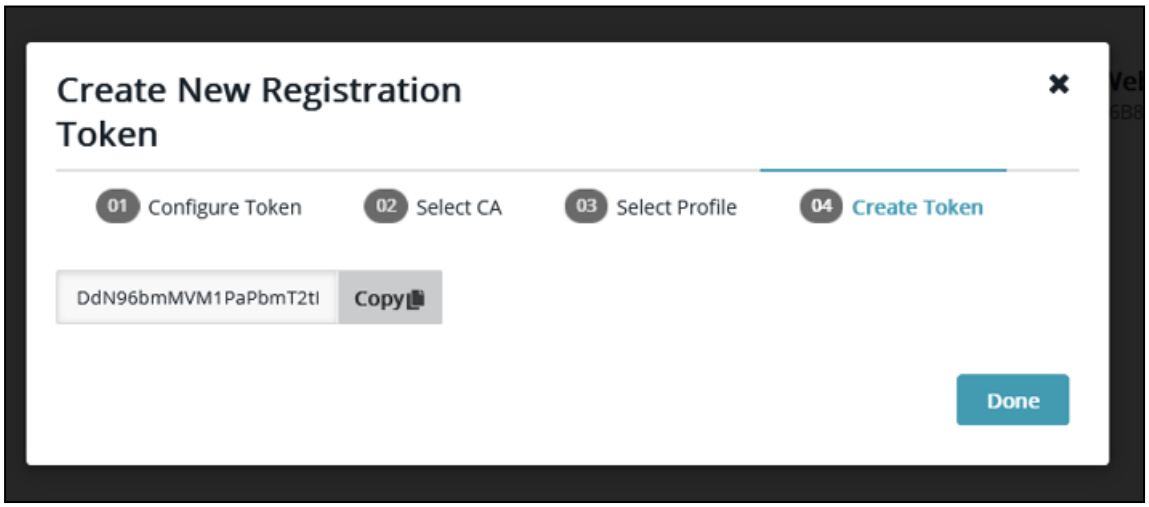

Select the client certificate issuer CA (domainA default CA)
Click “Select Profile”



Client Profile: select “hko_assigned_user_from root”
Click “Create Token”

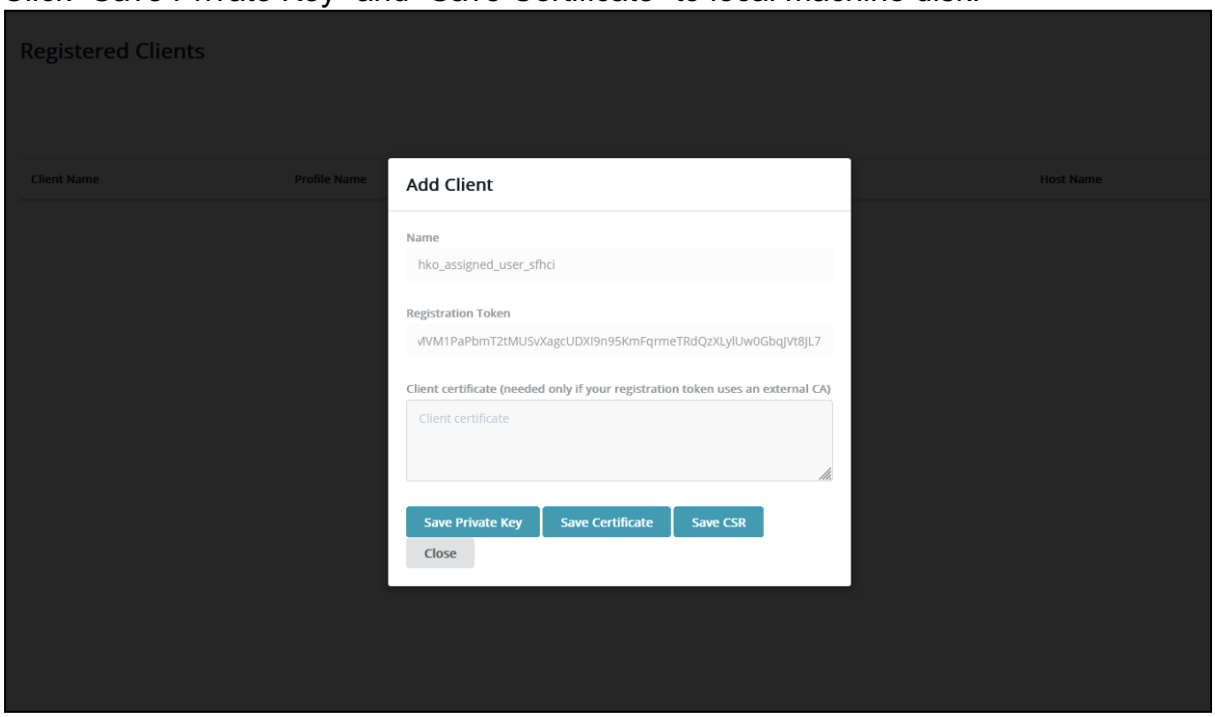



Click “Copy” to copy the token
Click “Done”



## Register KMIP client with the registration token for sfhci user at domainA

Go to Registered Client page
Click “+Add Client”
Name: hko_assigned_user_sfhci
Registration Token: paste the token, the one created at “Registration token” page
Click “Save”
Click “Save Private Key” and “Save Certificate” to local machine disk.




Rename the private key file as sfhci_pri.key
Rename the certificate as sfhci.pem

## Create KMIP Client Profile for dasfhci user at domainA

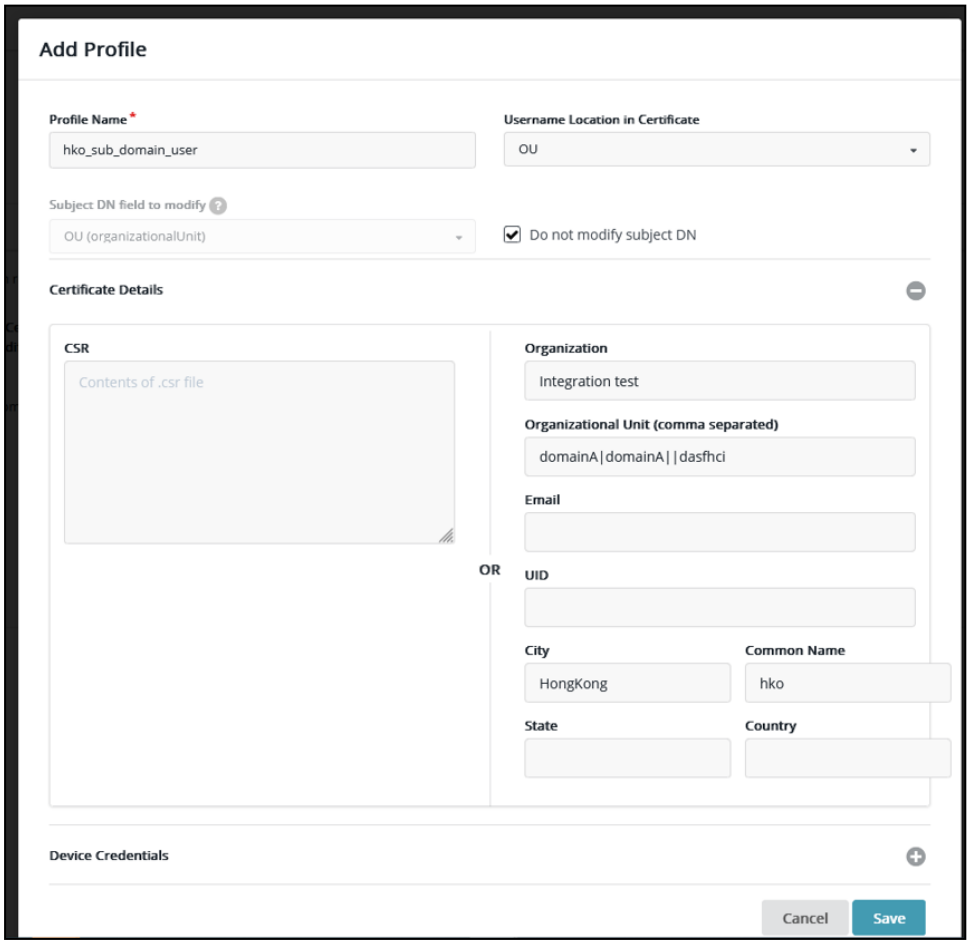
Go to “Products” → “KMIP” → “Client Profile”
Click “+ Add Profile”
Profile Name: hko_sub_domain_user
Username Location in Certificate: select OU (KMIP user authentication will take the username form the Organization Unit filed in the client certificate)
Organizational Unit: **domainA|domainA||sfhci**

- `<domain>|<auth-domain>||<username>`

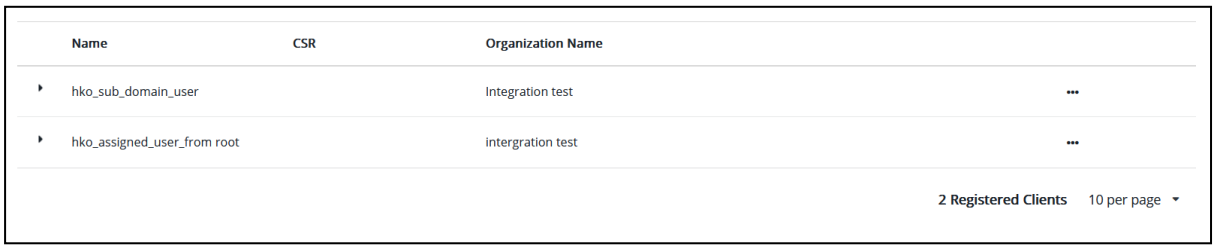
CM 2.10 KMIP reference

A local user created inside a specific domain, named "auth-domain". For example, domain|auth-domain||joe.

Common Name: hko



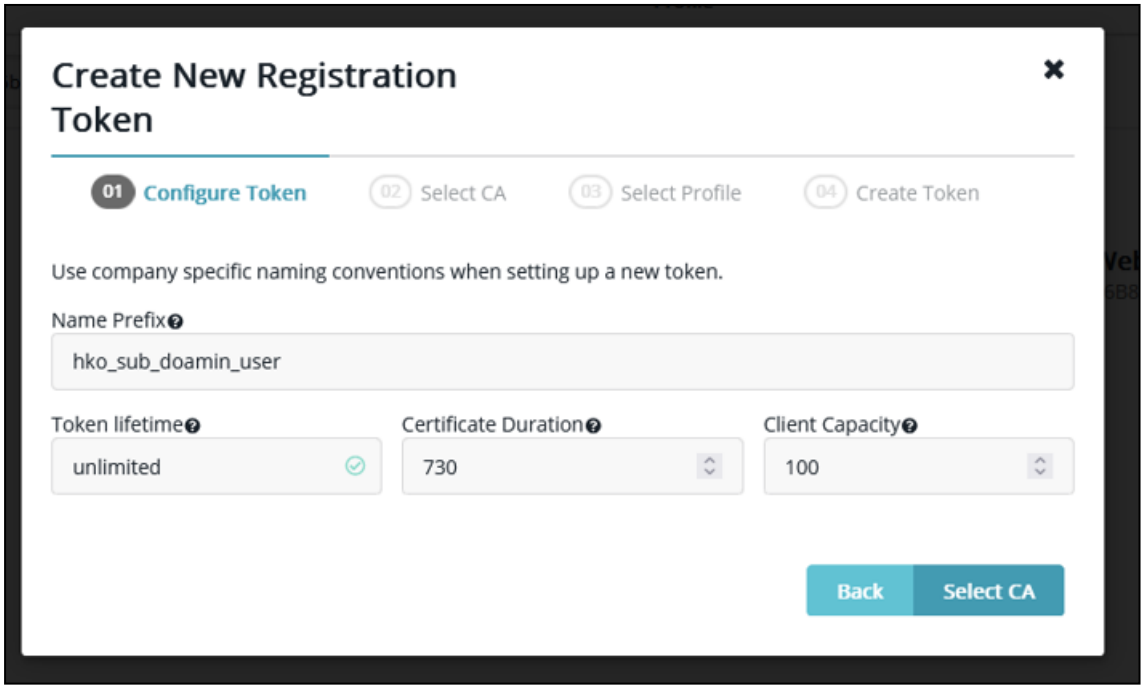

Result:



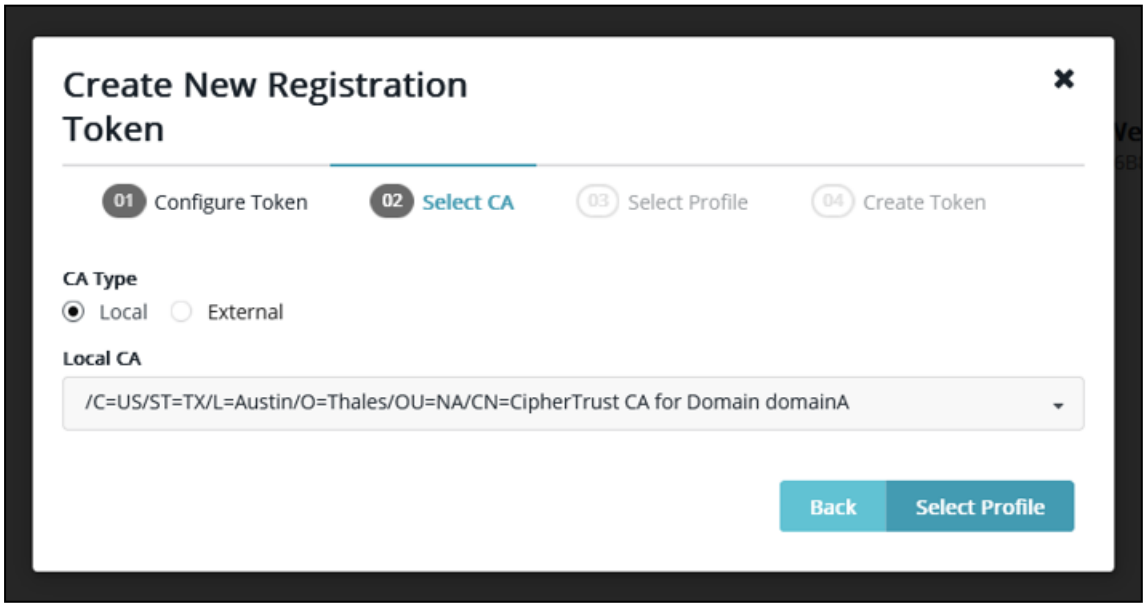
## Create KMIP Registration Token for dasfhci user at domainA

Go to “Registration Token” tab
Click “+ New Registration Token”

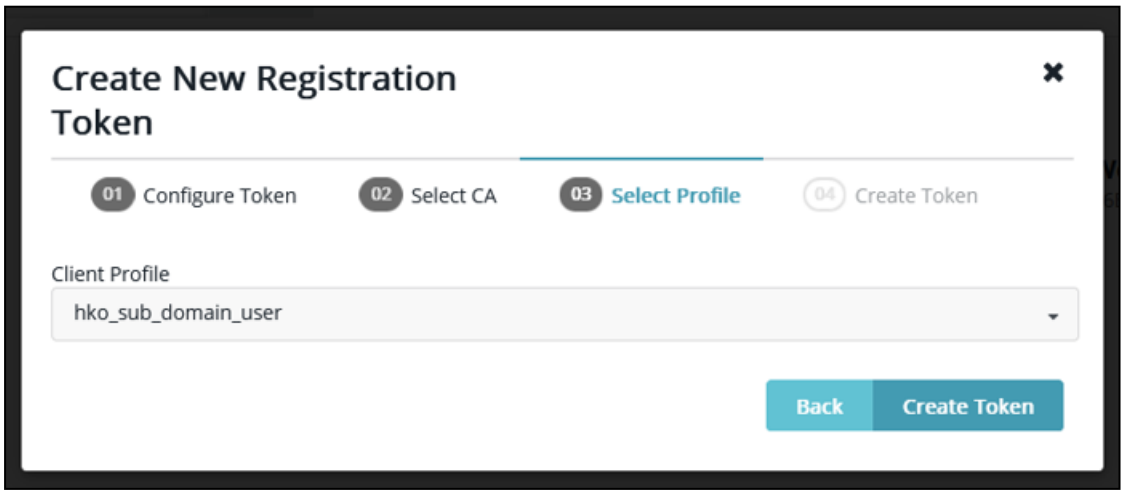
Name Prefix: hko_sub_domain_user
Click “Select CA”



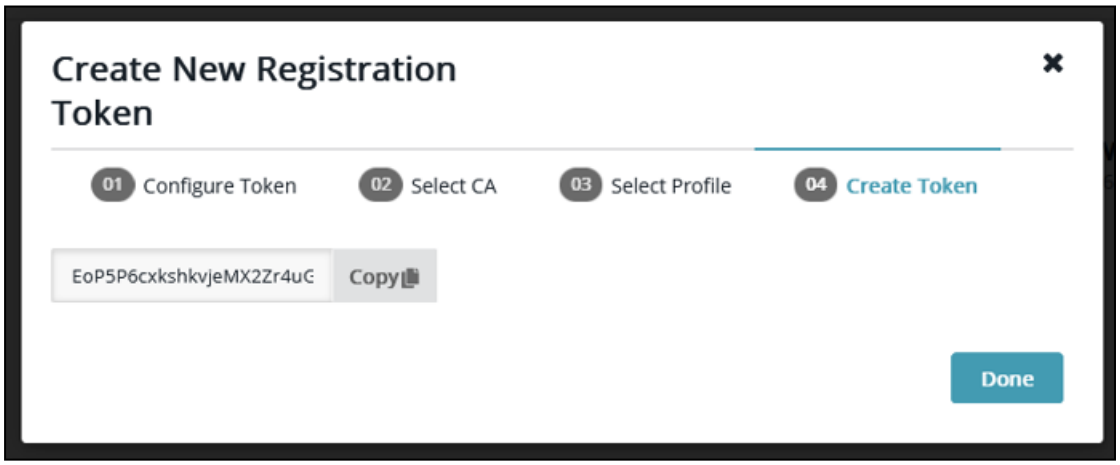

Select the client certificate issuer CA (domainA default CA)
Click “Select Profile”



Client Profile: select “hko_sub_domain_user”
Click “Create Token”

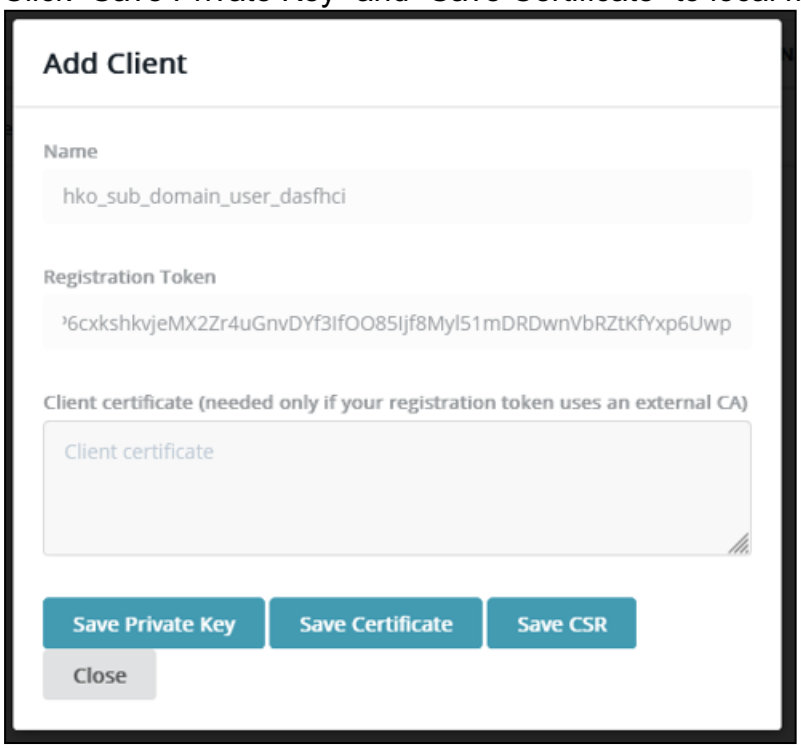



Click “Copy” to copy the token
Click “Done”



## Register KMIP client with the registration token for dasfhci user at domainA

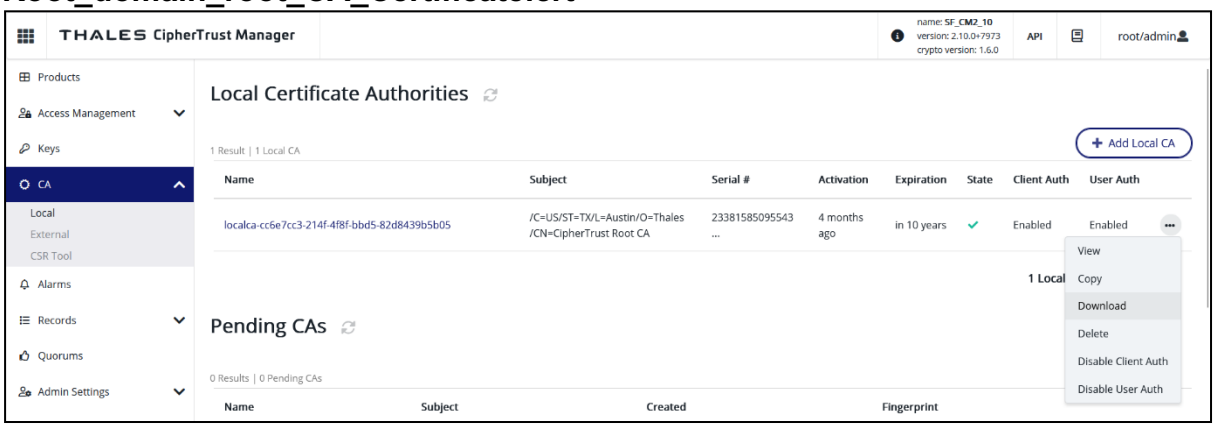
Go to Registered Client page
Click “+Add Client”
Name: hko_sub_domain_user_dasfhci
Registration Token: paste the token, the one created at “Registration token” page
Click “Save”
Click “Save Private Key” and “Save Certificate” to local machine disk.




Rename the private key file as dasfhci_pri.key
Rename the certificate as dasfhci.pem

## Download CipherTrust Manager CA certificate at root domain

Go to CA → Local
Download the root certificate, rename the file name as
**Root_domain_root_CA_Certificate.crt**




## Combine the KMIP client certificate and key into one file

Linux command line: cat sfhci_pri.key sfhci.pem > **sfhci_certificate.pem**
Linux command line: cat dasfhci_pri.key dasfhci.pem > **dasfhci_certificate_combined.pem**

Created item:
Assigned user “sfhci” with Key users group for KMIP connection to sub domain **domainA**
sfhci KMIP client certificate (730 days): **sfhci.pem**
sfhci KMIP client certificate private key: **sfhci_pri.key**
sfhci KMIP client certificate with private key: **sfhci_certificate.pem**
Created user “dasfhci” with Key users group for KMIP connection at sub domain **domainA**
dasfhci KMIP client certificate (730 days): **dasfhci.pem**
dasfhci KMIP client certificate private key: **dasfhci_pri.key**
dasfhci KMIP client certificate with private key: **dasfhci_certificate_combined.pem**

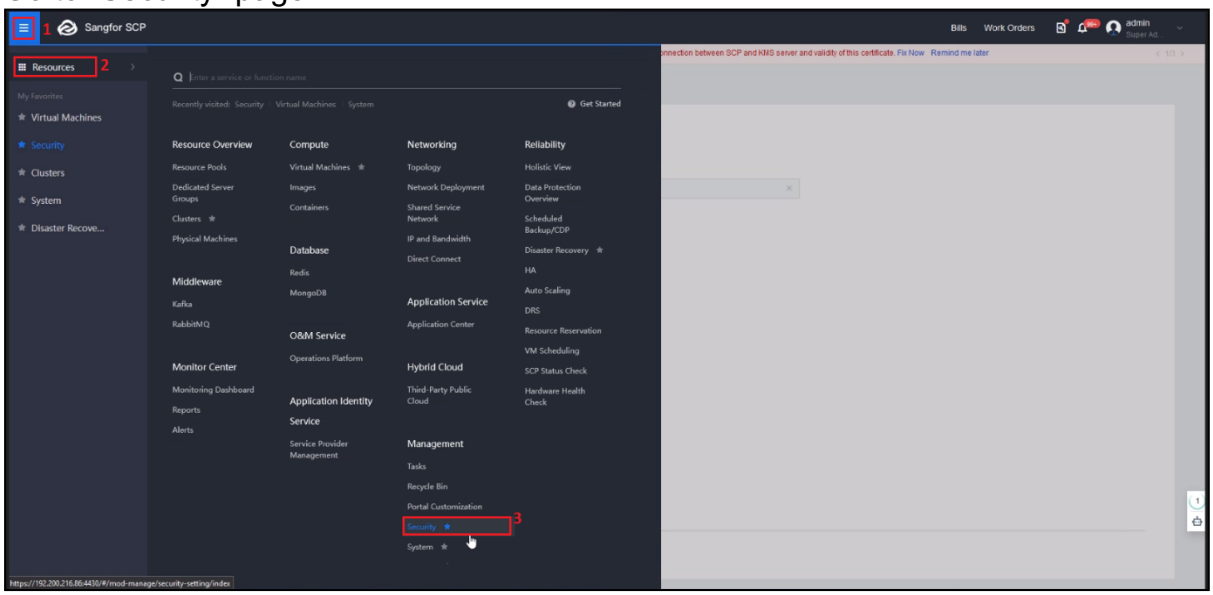
CipherTrust Manager root domain default CA certificate:
**Root_domain_root_CA_Certificate.crt**

| User list | | |
|---|---|---|
| | **root** | **domainA** |
| admin | Yes | Yes (assigned from root) |
| sfhci | Yes | Yes (assigned from root) |
| dasfhci | No | Yes |

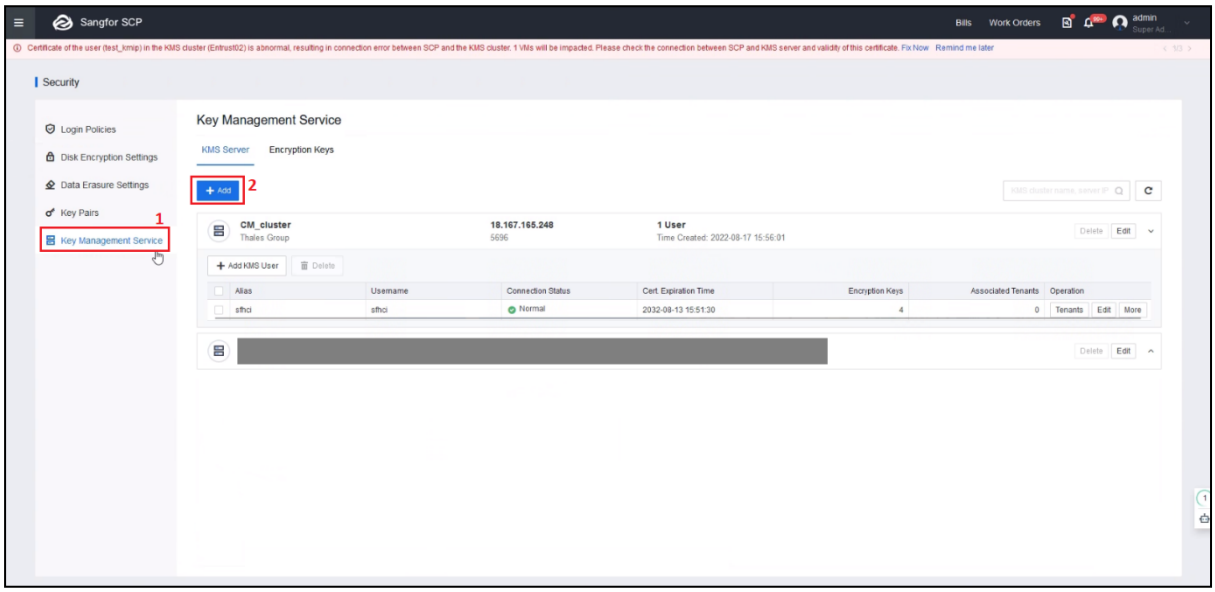
# Sangfor Cloud Platform KMS server connection configuration

## Add a KMS server with dasfhci user

Open Sangfor Cloud Platform web console:
Go to “Security” page



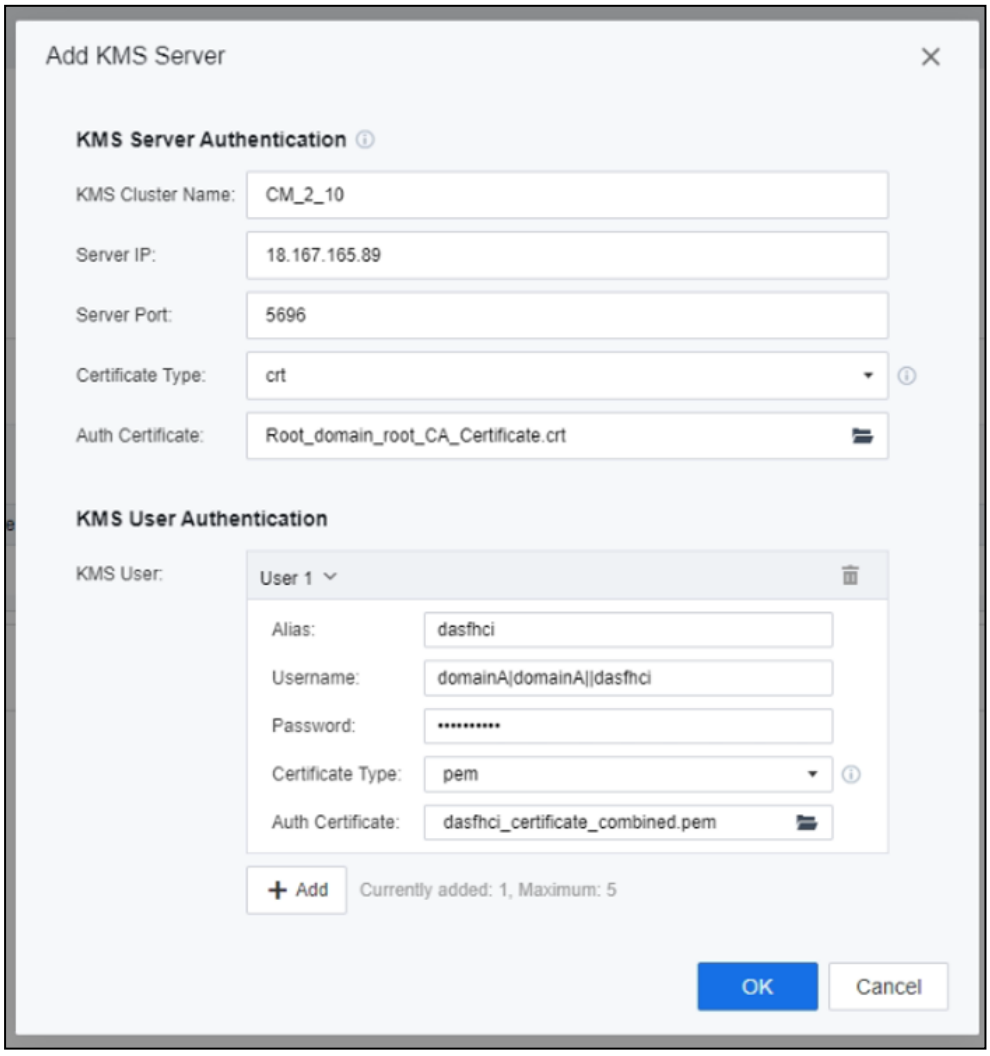

Click “Key Management Service”
Click “+Add”



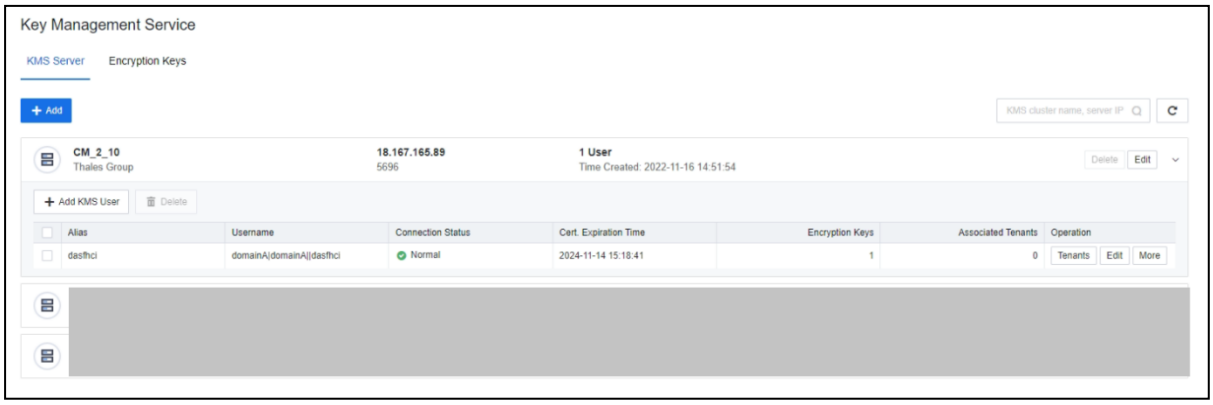

KMS Server Authentication
KMS Cluster Name: **CM_2_10**

Server IP: **18.167.165.89** (CipherTrust Manager IP address)
Server Port: **5696** (CipherTrust Manager default KMIP interface)
Certificate Type: **pem**
Auth Certificate: upload "**Root_domain_root_CA_Certificate.crt**"
KMS User Authentication
Alias: **dasfhci**
Username: **domainA|domainA||dasfhci**
Password: (the one created at CipherTrust Manager for user dasfhci)
Certificate Type: **pem**
Auth Certificate: upload "**dasfhci_certificate_combined.pem**"

Click "OK"

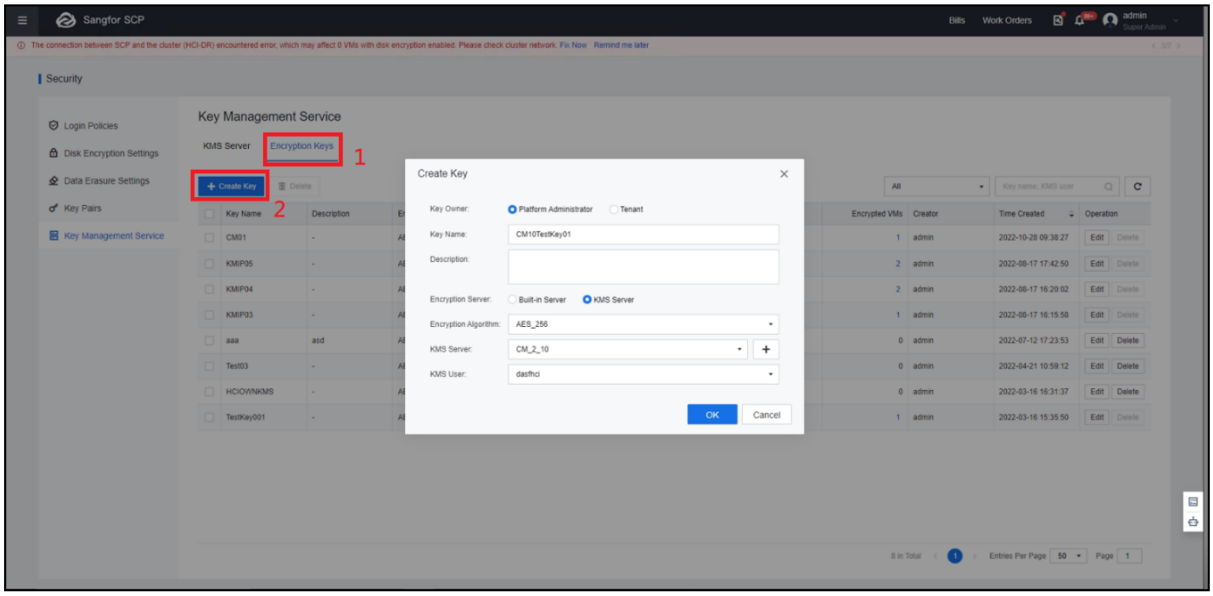


Result:

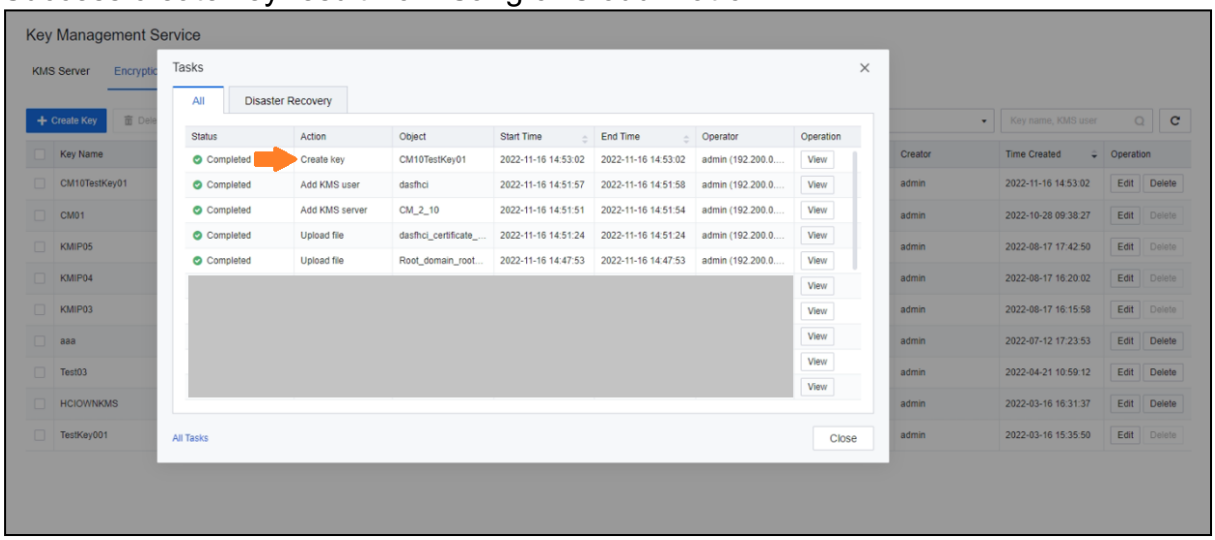

Key Management Service
KMS Server
Encryption Keys
Add
KMS cluster name, server IP
CM_2_10
Thales Group
18.167.165.89
5696
1 User
Time Created: 2022-11-16 14:51:54
Delete
Edit
Add KMS User
Delete
Alias
Username
Connection Status
Cert. Expiration Time
Encryption Keys
Associated Tenants
Operation
dasfhci
domainA|domainA|dasfhci
Normal
2024-11-14 15:18:41
1
0
Tenants
Edit
More

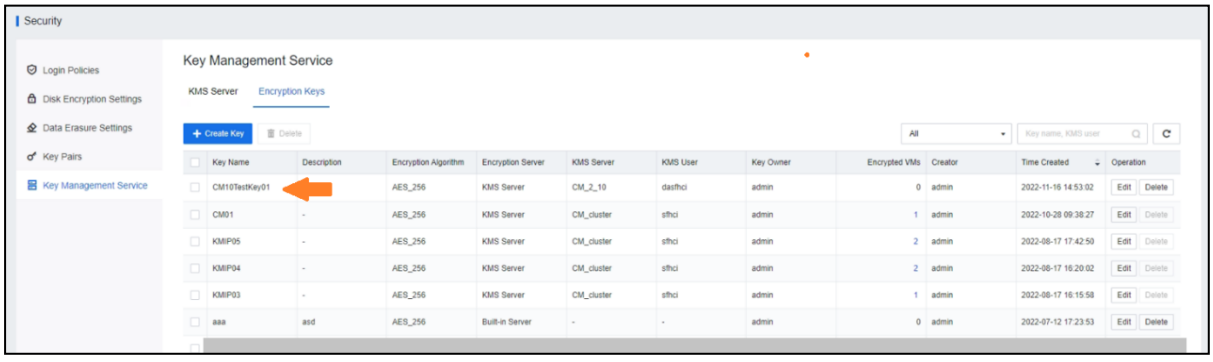
## Create an AES encryption key with dasfhci user

Click “Encryption Keys”
Click “+Create Key”
Key Name: **CM10TestKey01** (Any name)
Encryption Server: KMS Server
Encryption Algorithm: AES_256
KMS Server: CM_2_10
KMS User: dasfhci
Click “OK”

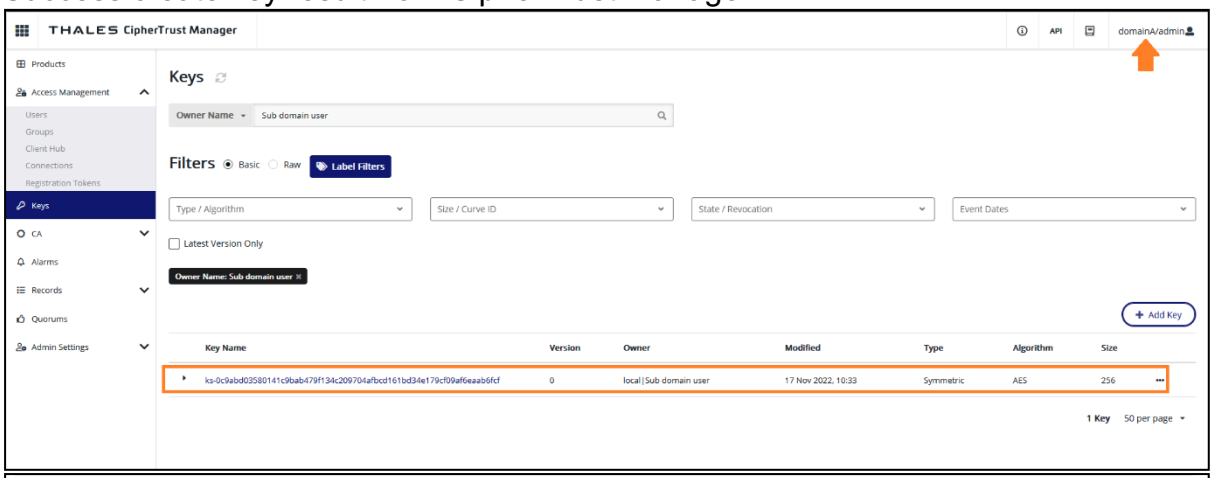



Success create key result from Sangfor Cloud Platform:



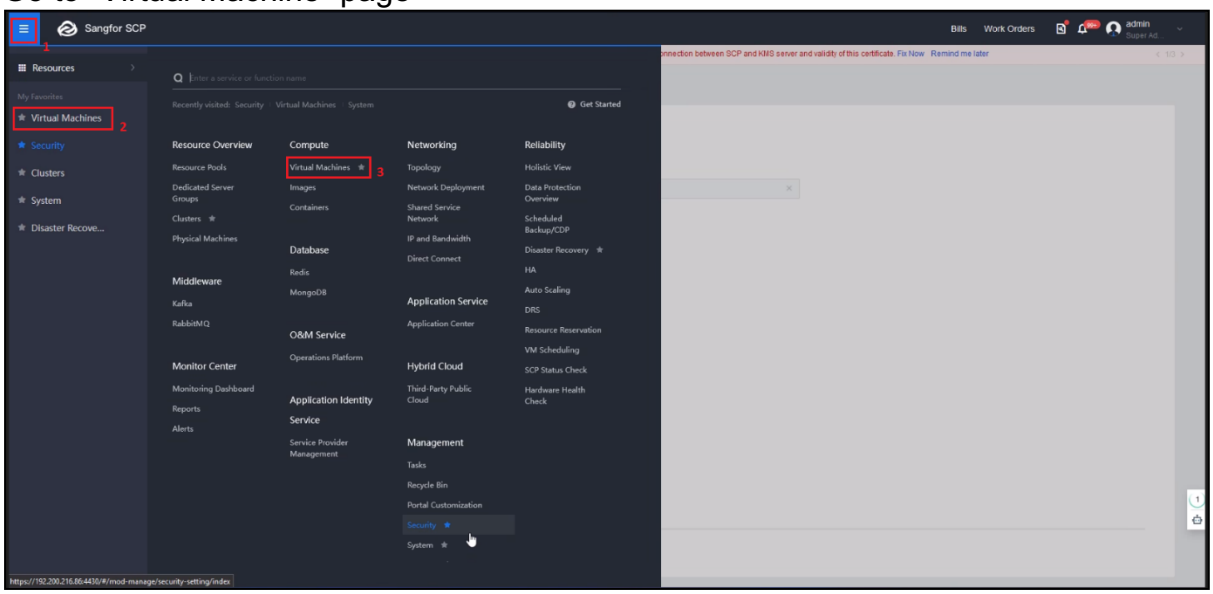



Success create key result from CipherTrust Manager



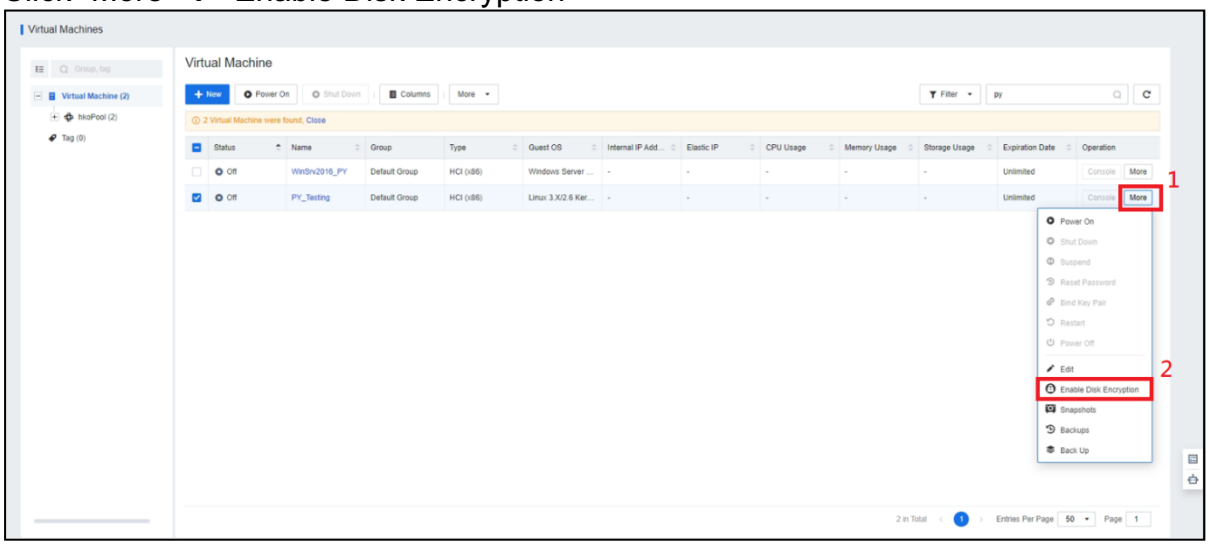

## Encrypt the virtual machine

Go to “Virtual Machine” page

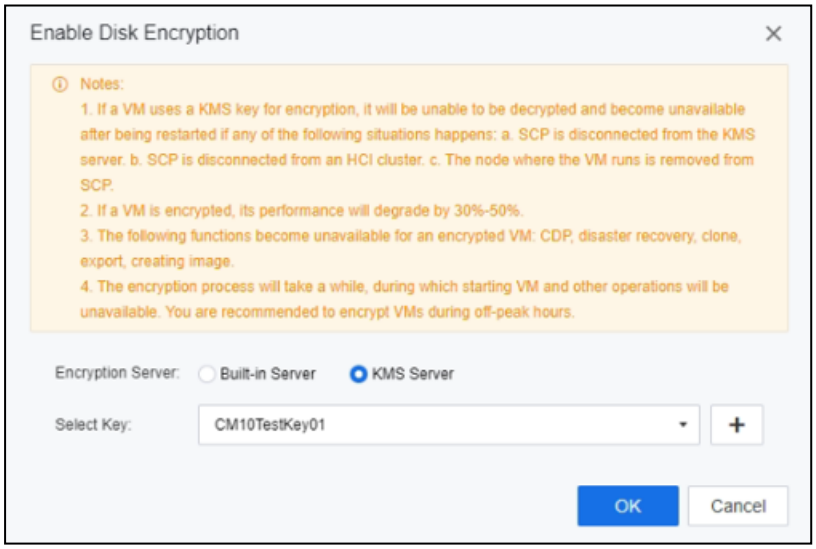



Ensure the virtual machine is in power off status

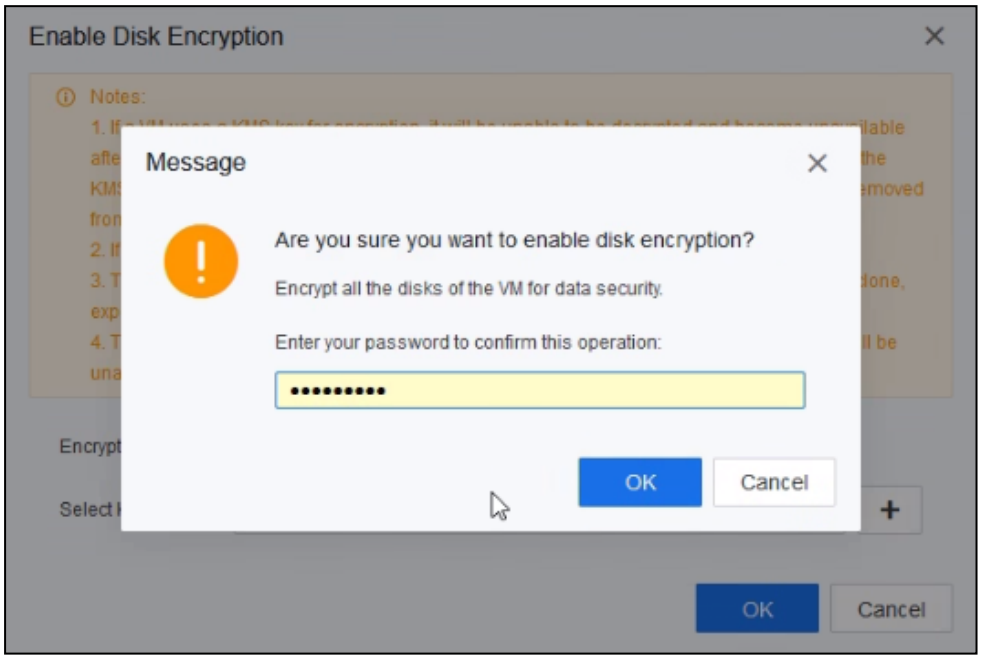
Click “More” → “Enable Disk Encryption”



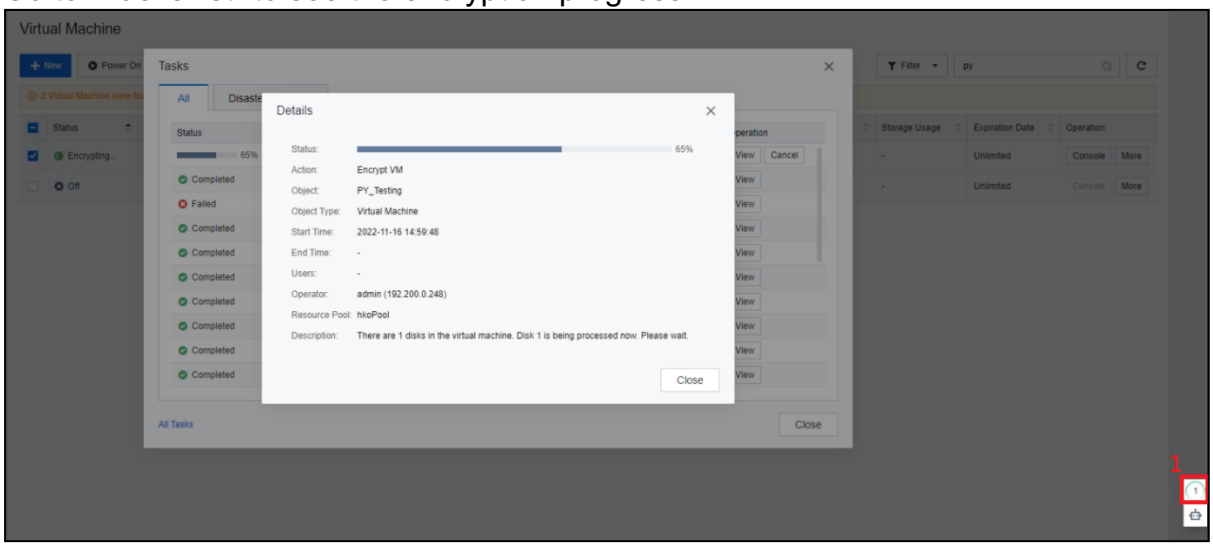
Encryption Server: KMS Server
Select Key: **CM10TestKey01**
Click “OK”




Type Sangfor Cloud Platform admin password to proceed the encryption
Click “OK”

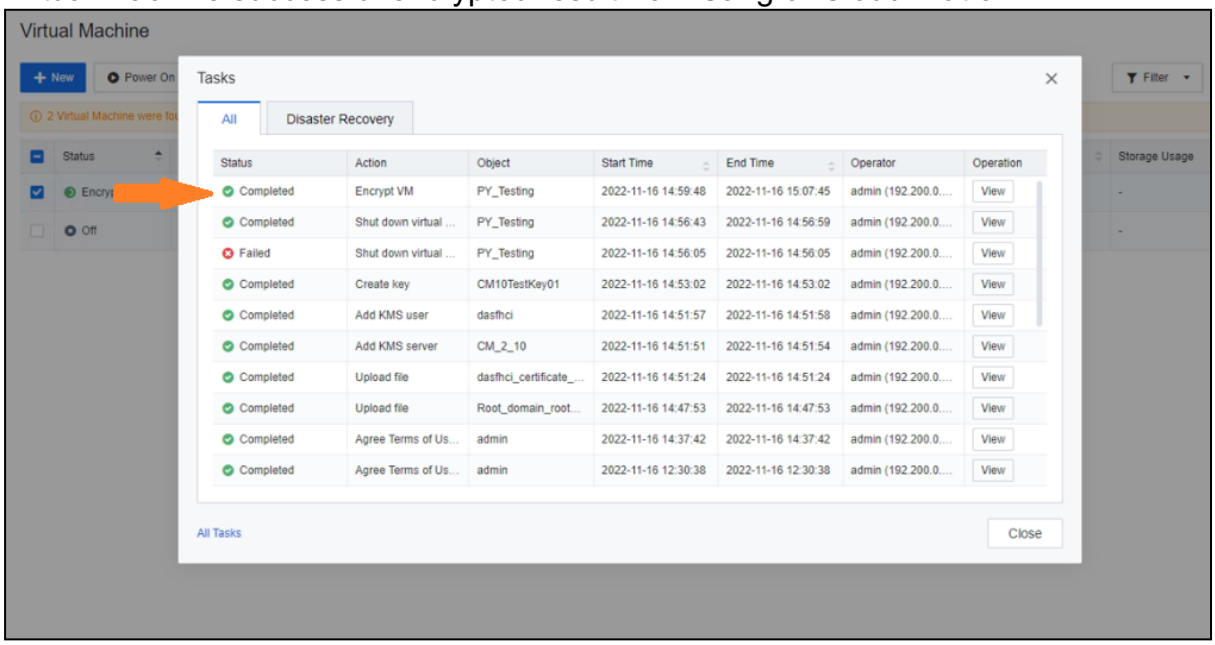


Go to “Tasks list” to see the encryption progress

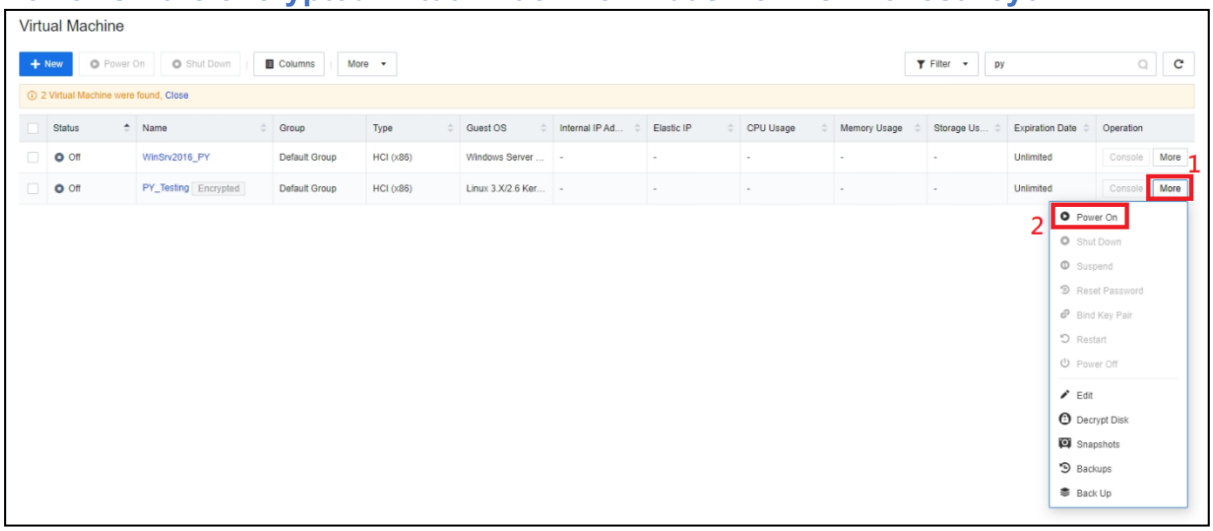



Success use key status from CipherTrust Manager:

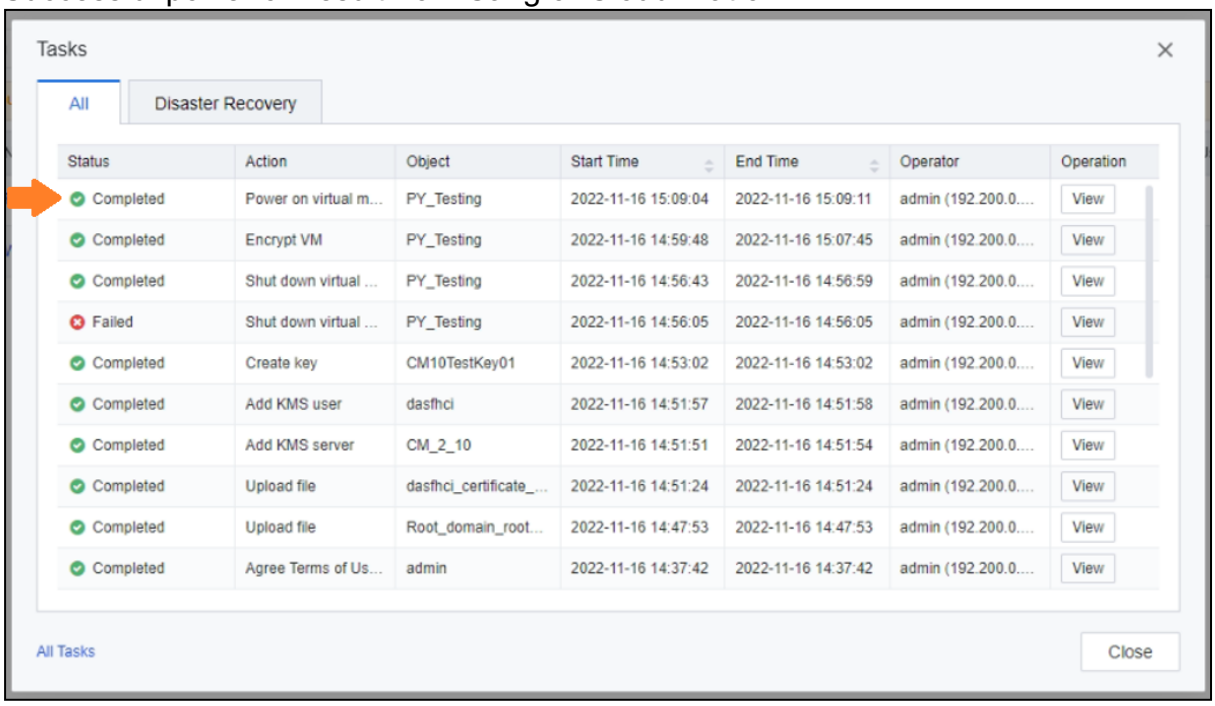

Virtual machine successful encrypted result from Sangfor Cloud Platform



## Power On the encrypted virtual machine - dasfhci – CM10TestKey01




Successful power on result from Sangfor Cloud Platform:

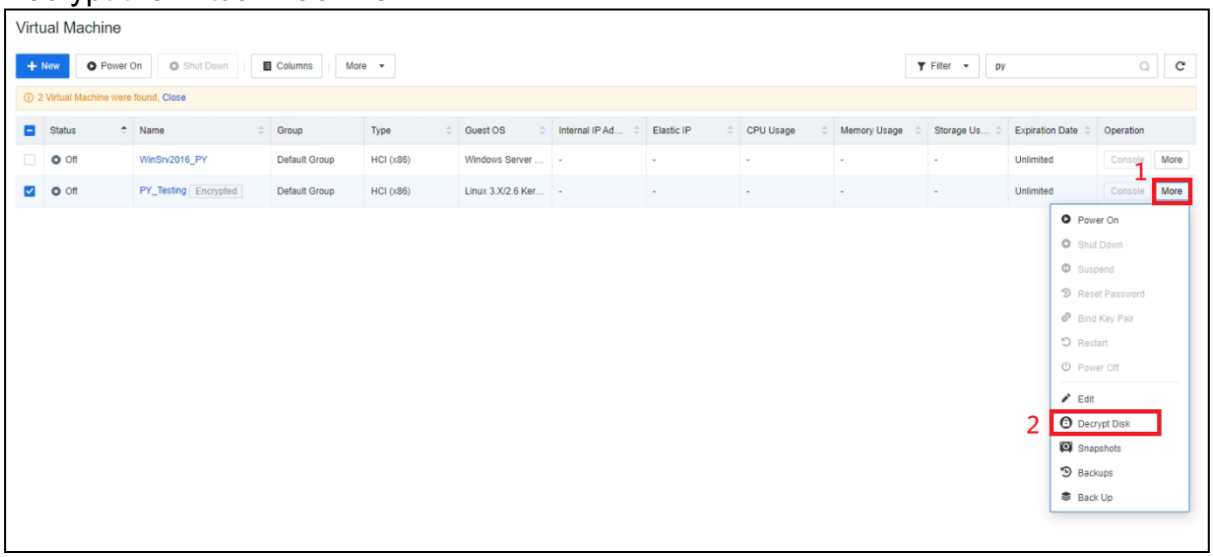



Successful power on result from CipherTrust Manager:

## Decrypted virtual machine - dasfhci – CM10TestKey01

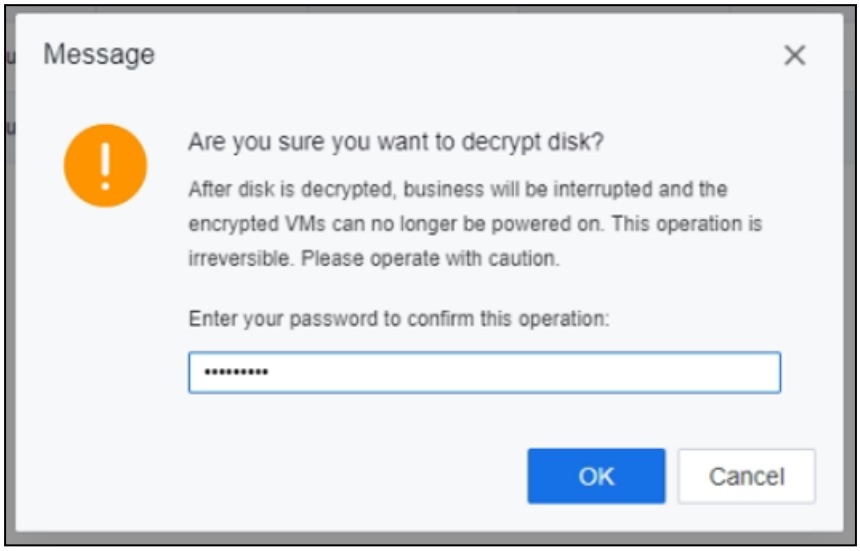
Ensure the virtual machine is in power off status

Decrypt the virtual machine

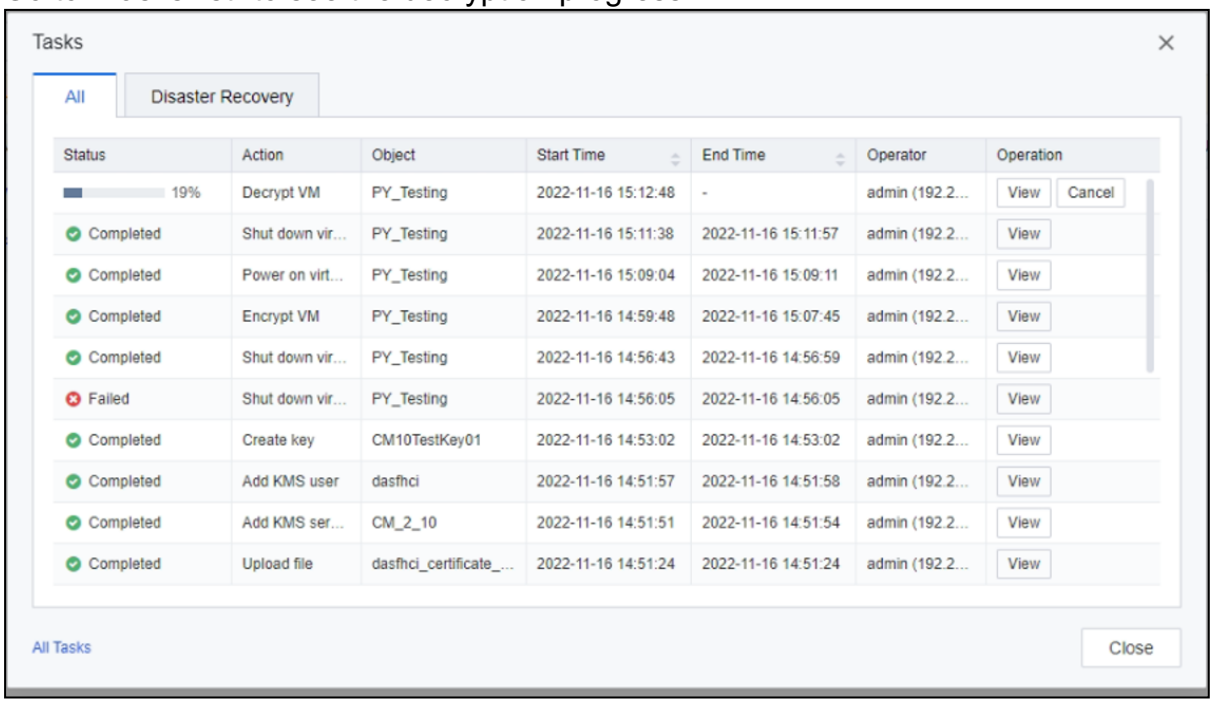



Type Sangfor Cloud Platform admin password to proceed the decrypt virtual machine action

Click “OK”

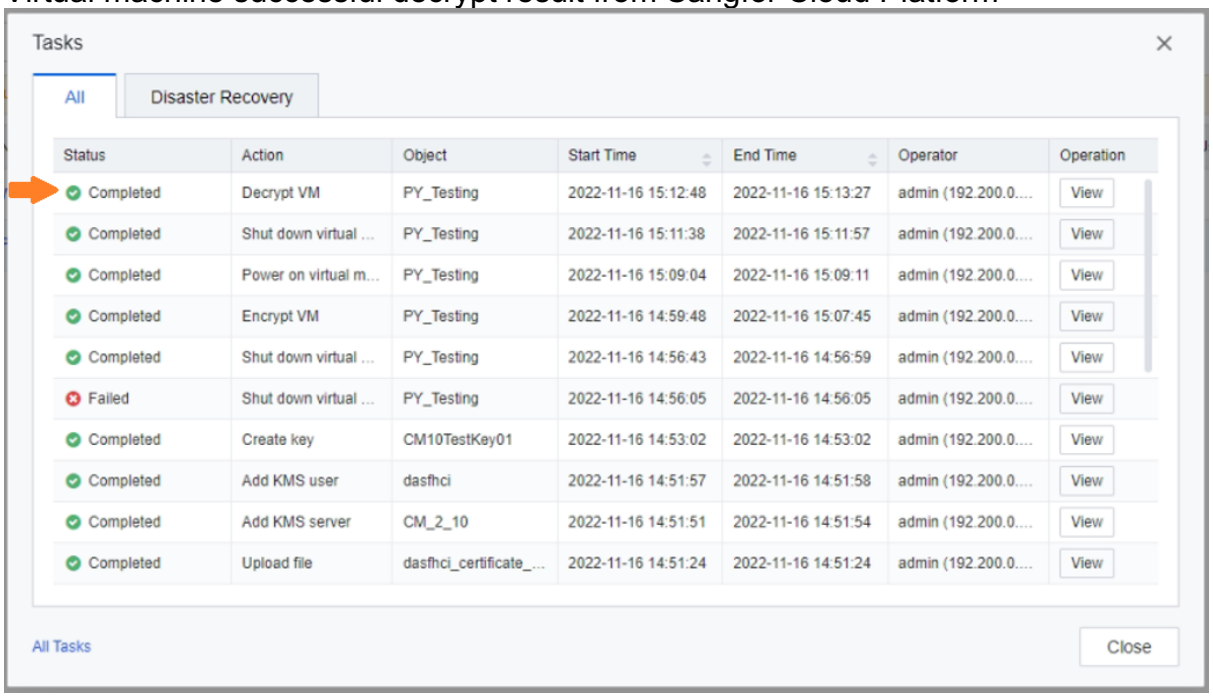


Go to “Tasks list” to see the decryption progress



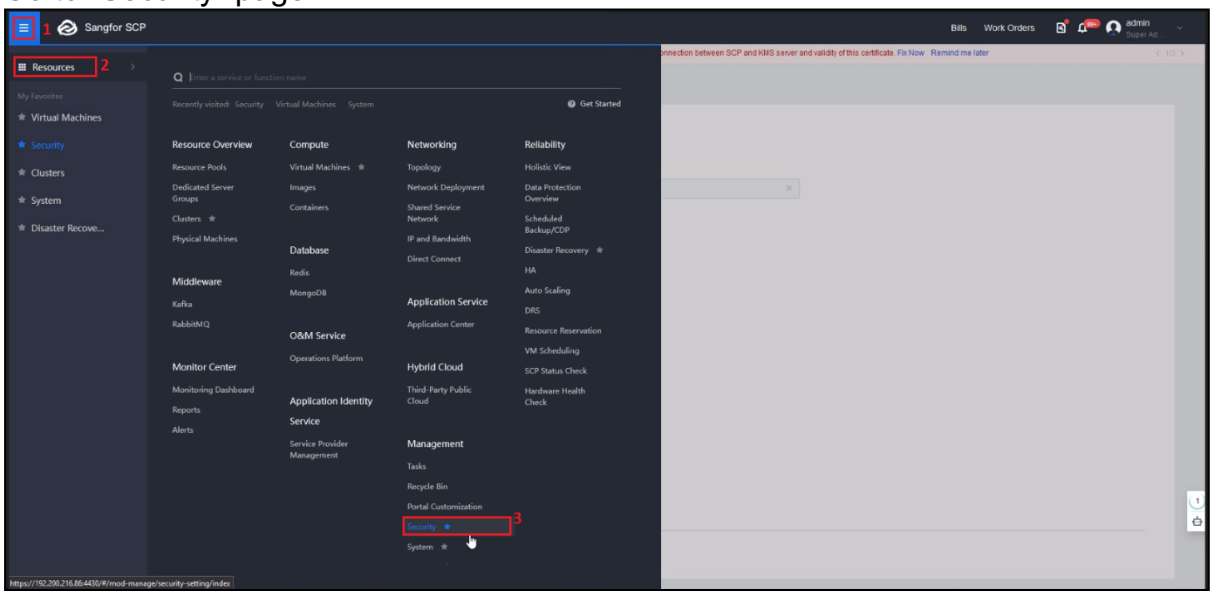

Success use key status from CipherTrust Manager:


Virtual machine successful decrypt result from Sangfor Cloud Platform



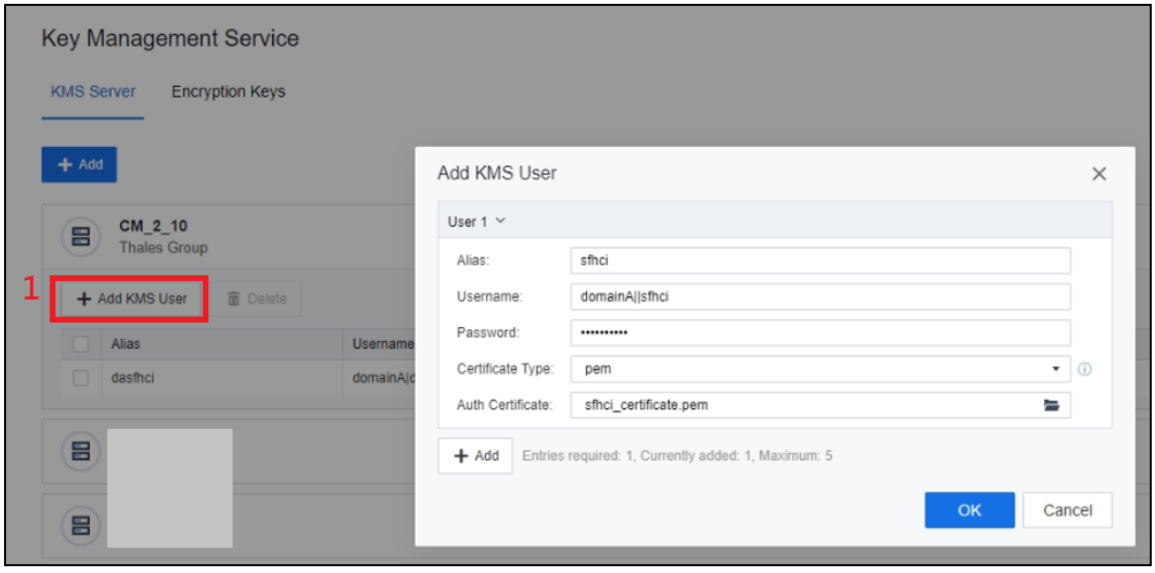
## Add a KMS user - sfhci

Open Sangfor Cloud Platform web console:
Go to “Security” page

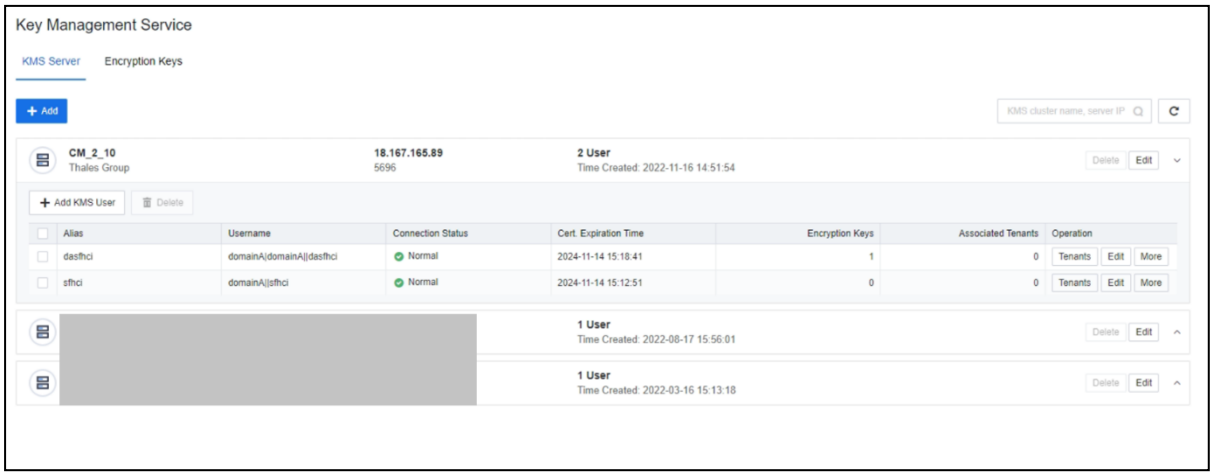



Click “Key Management Service”
Click “+Add KMS User”

Alias: **sfhci**
Username: **domainA||sfhci**
Password: (the one created at CipherTrust Manager for user dasfhci)
Certificate Type: **pem**
Auth Certificate: upload “**sfhci_certificate.pem**”
Click “OK”

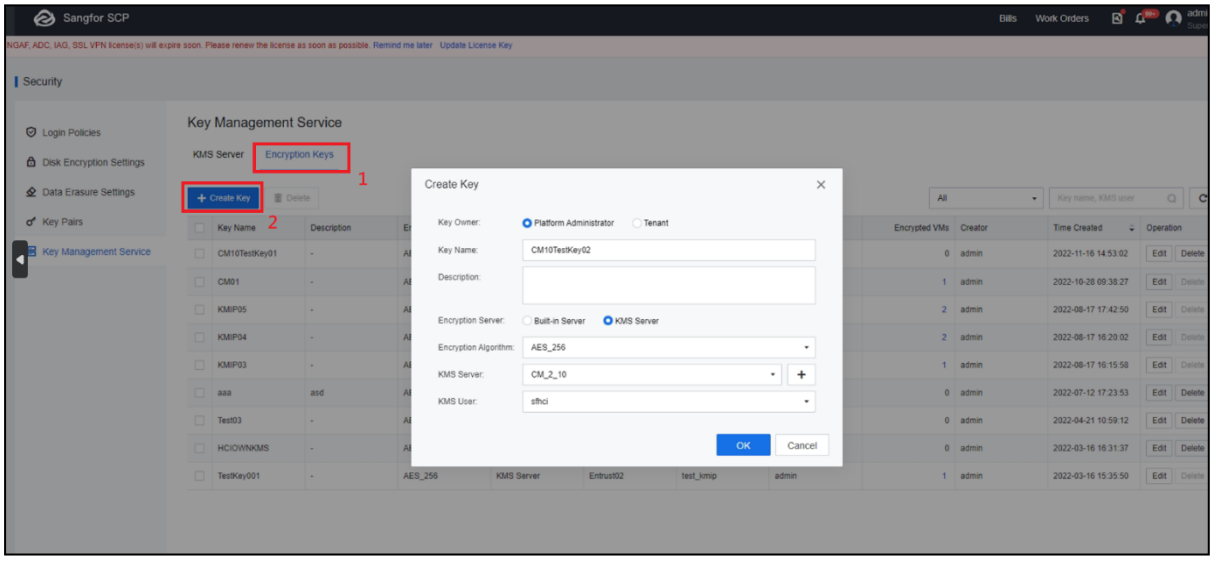


Result:

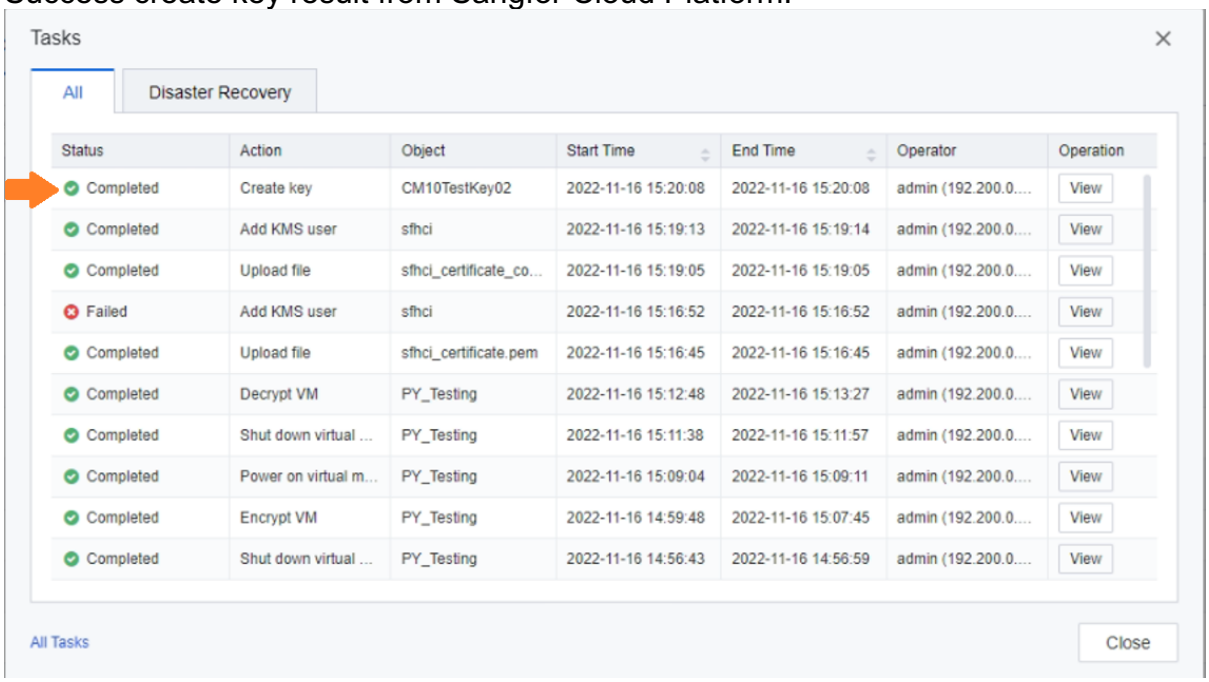

Key Management Service
KMS Server
Encryption Keys
Add
KMS cluster name, server IP
CM_2_10
Thales Group
18.167.165.89
5696
2 User
Time Created: 2022-11-16 14:51:54
Delete
Edit
Add KMS User
Delete
Alias
Username
Connection Status
Cert. Expiration Time
Encryption Keys
Associated Tenants
Operation
dasfhci
domainA|domainA||dasfhci
Normal
2024-11-14 15:18:41
1
0
Tenants
Edit
More
sfhci
domainA||sfhci
Normal
2024-11-14 15:12:51
0
0
Tenants
Edit
More
1 User
Time Created: 2022-08-17 15:56:01
Delete
Edit
1 User
Time Created: 2022-03-16 15:13:18
Delete
Edit

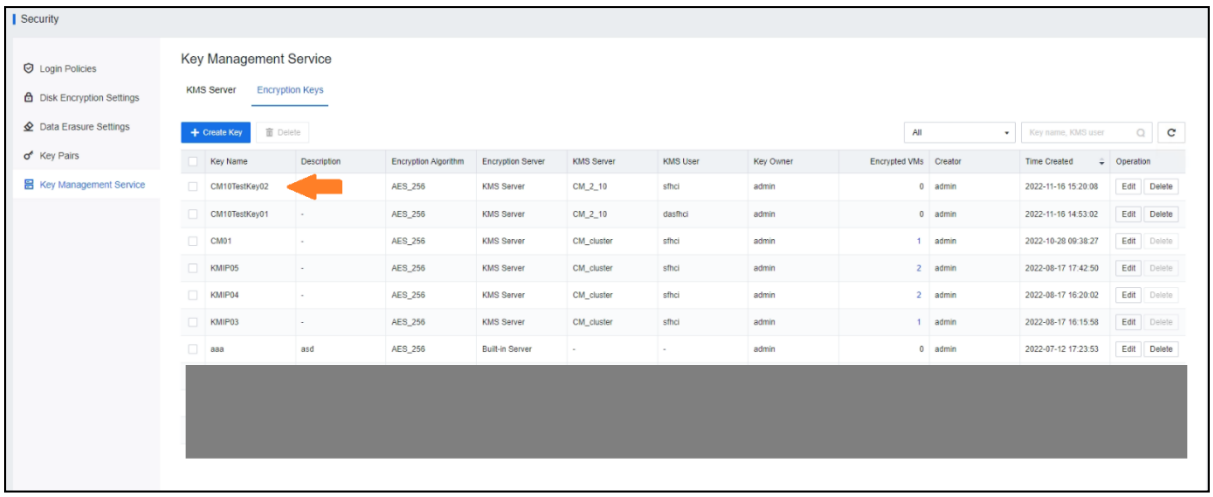
## Create an AES encryption key with sfhci user

Click “Encryption Keys”
Click “+Create Key”
Key Name: **CM10TestKey02** (Any name)
Encryption Server: KMS Server
Encryption Algorithm: AES_256
KMS Server: CM_2_10
KMS User: sfhci
Click “OK”

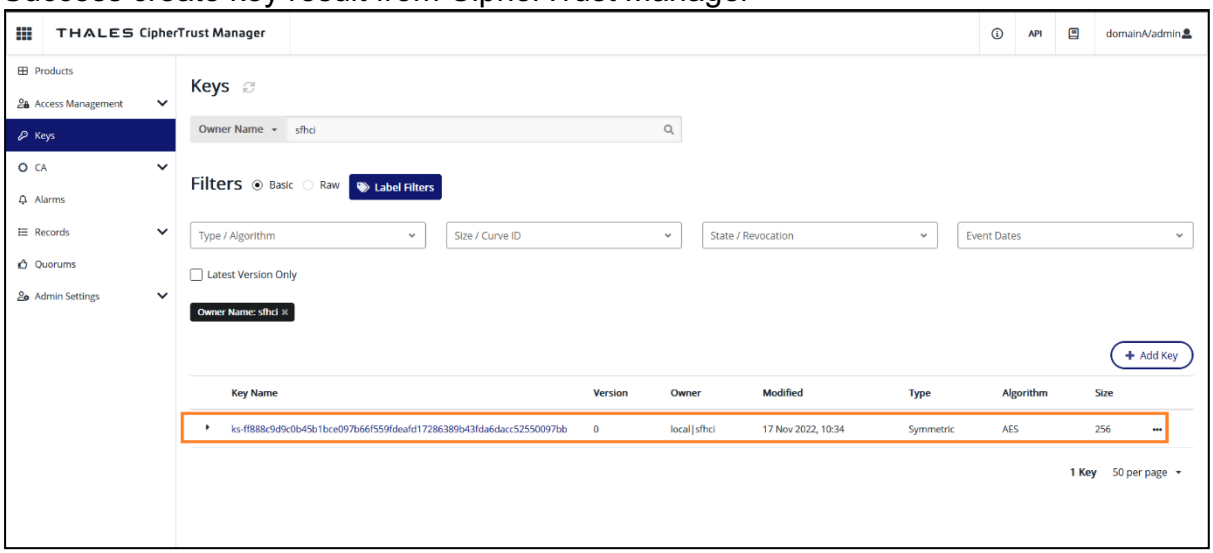



Success create key result from Sangfor Cloud Platform:



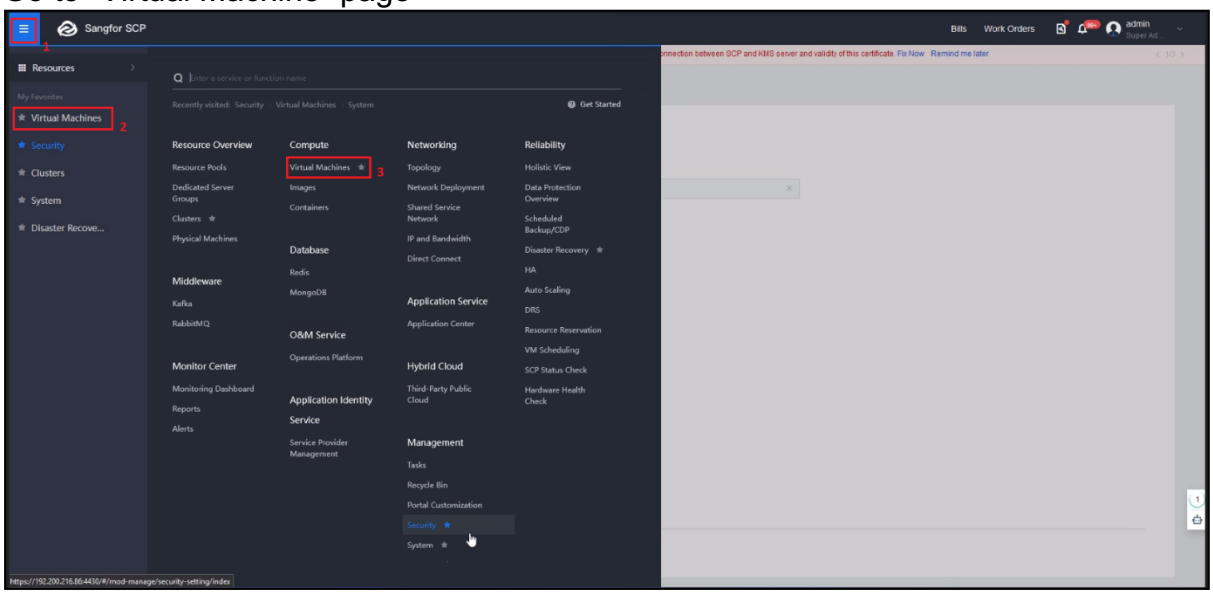



Success create key result from CipherTrust Manager



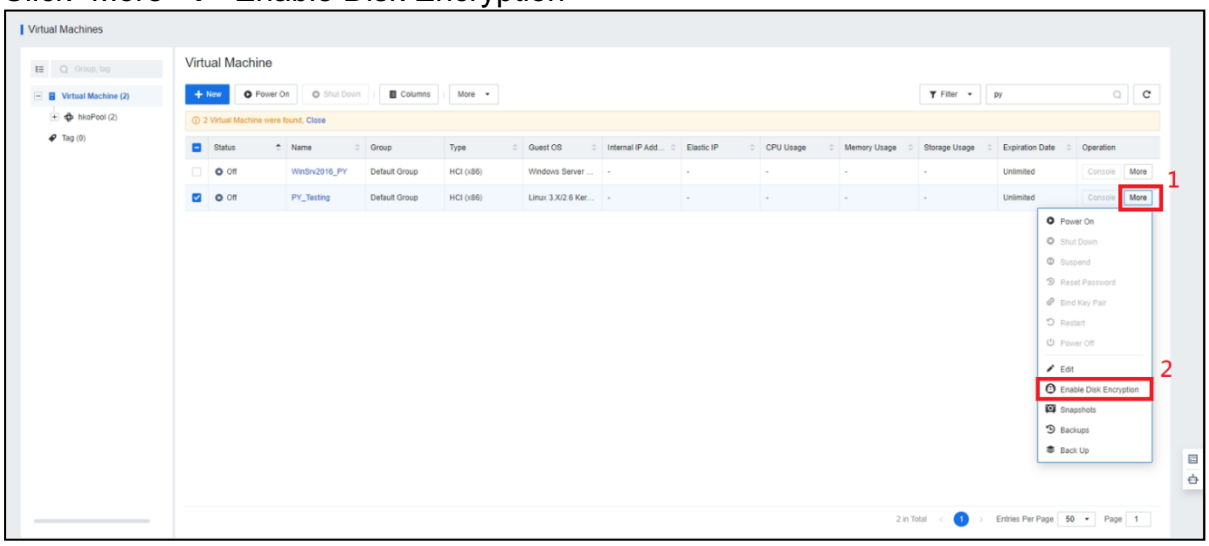

## Encrypt the virtual machine

Go to “Virtual Machine” page

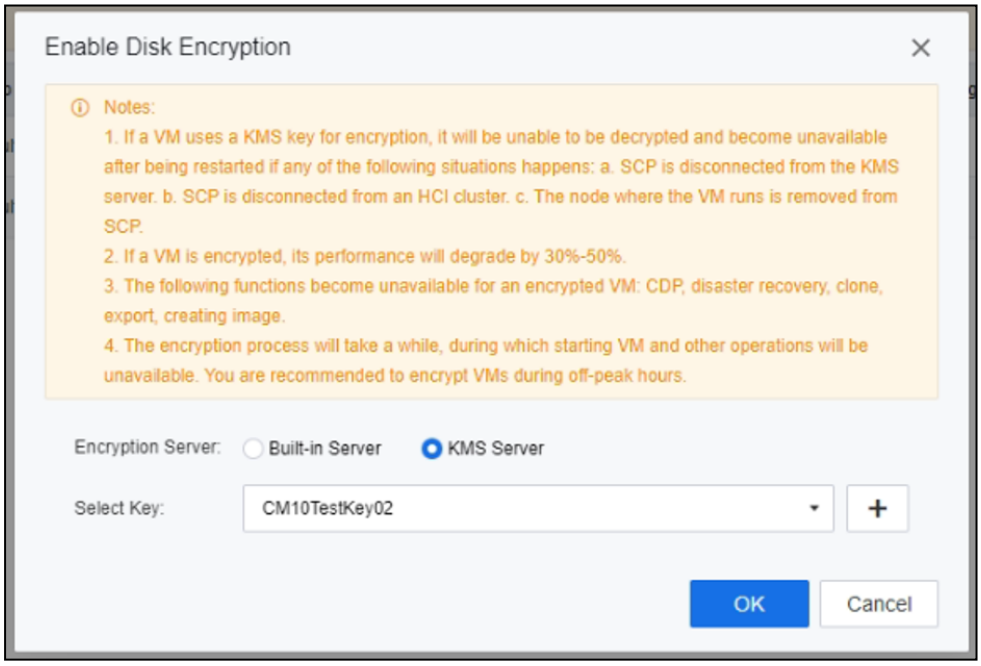



Ensure the virtual machine is in power off status

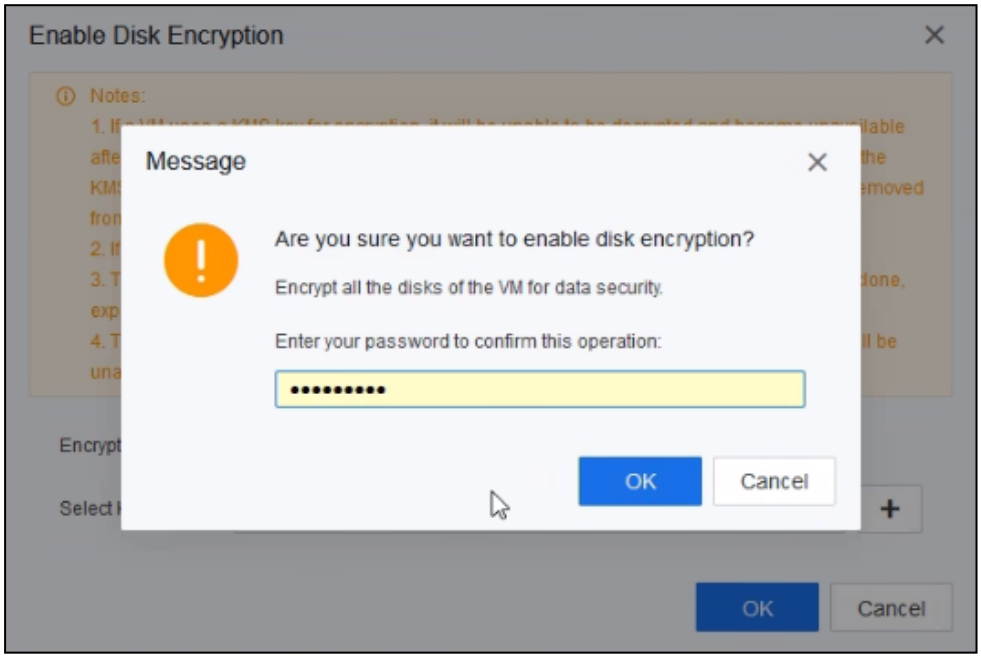
Click “More” → “Enable Disk Encryption”



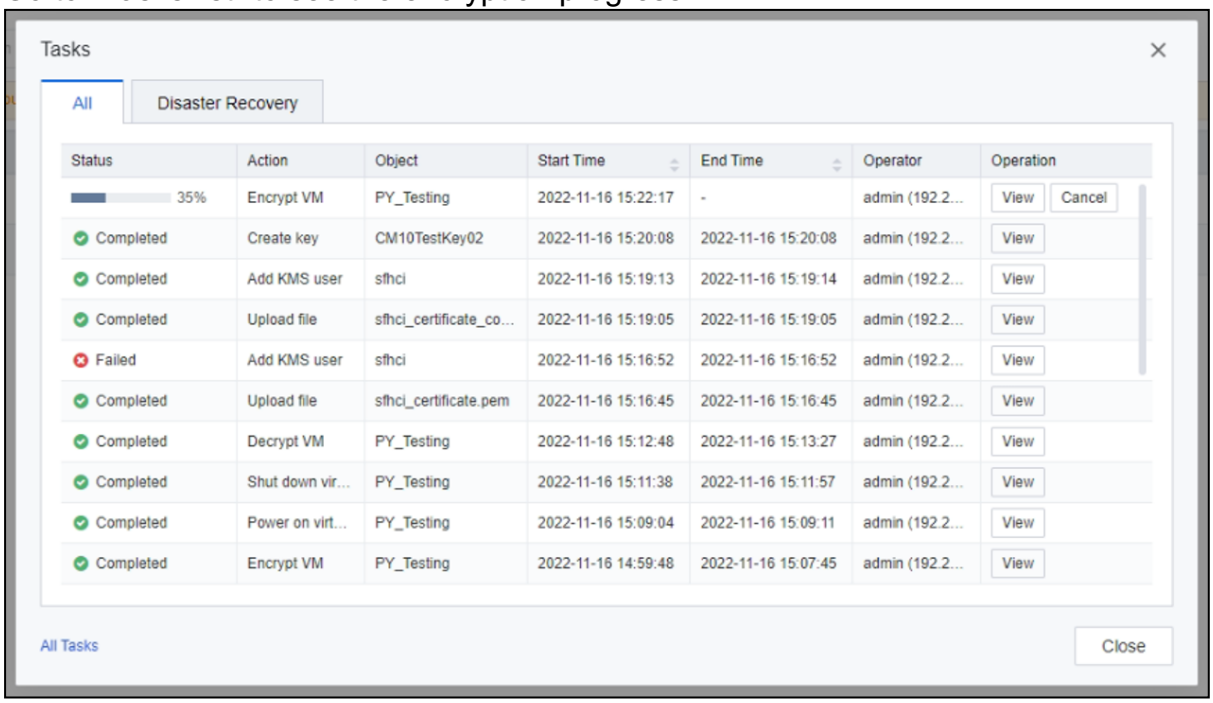
Encryption Server: KMS Server
Select Key: **CM10TestKey02**
Click “OK”




Type the Sangfor Cloud Platform admin password to proceed the encryption
Click “OK”

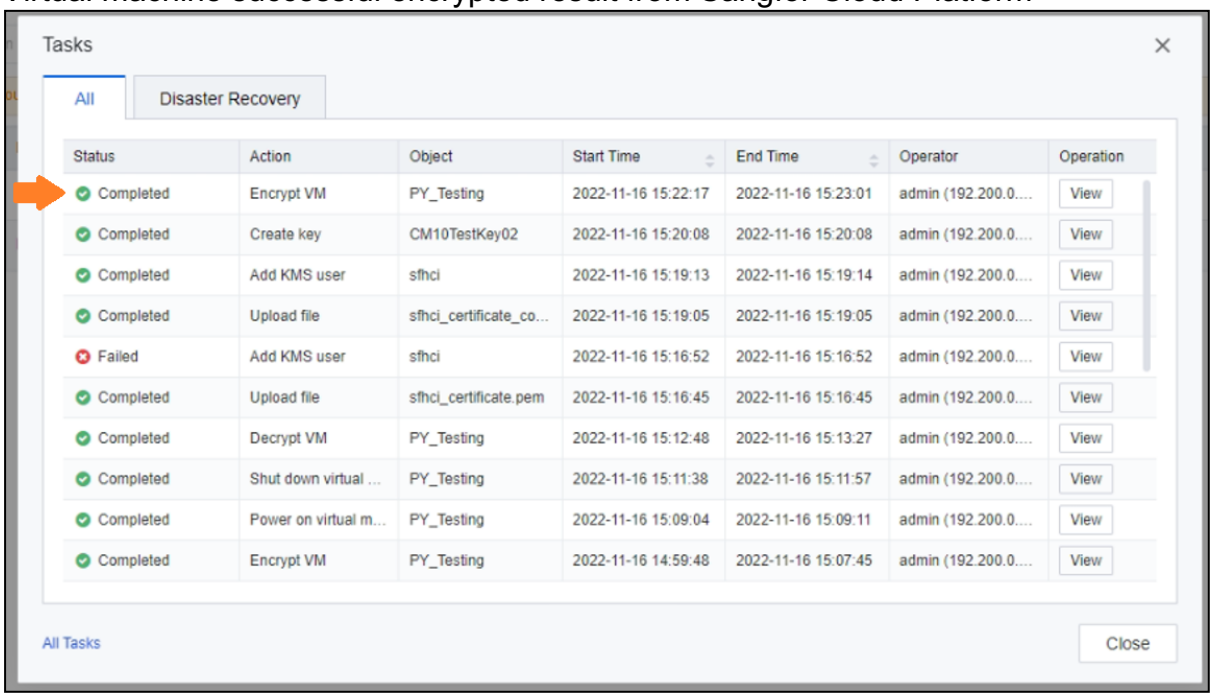


Go to “Tasks list” to see the encryption progress

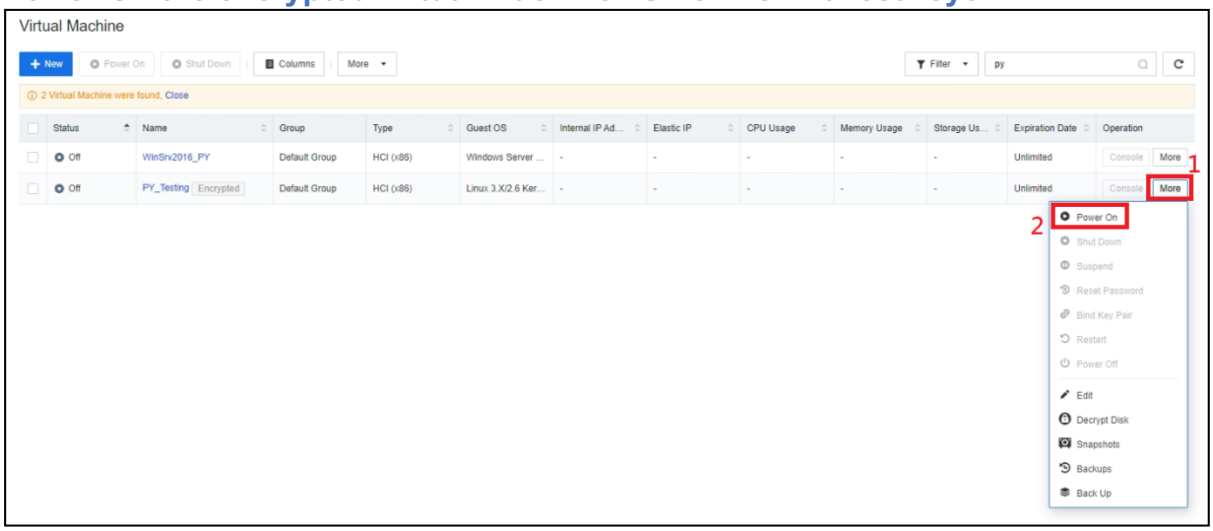



Success use key status from CipherTrust Manager:

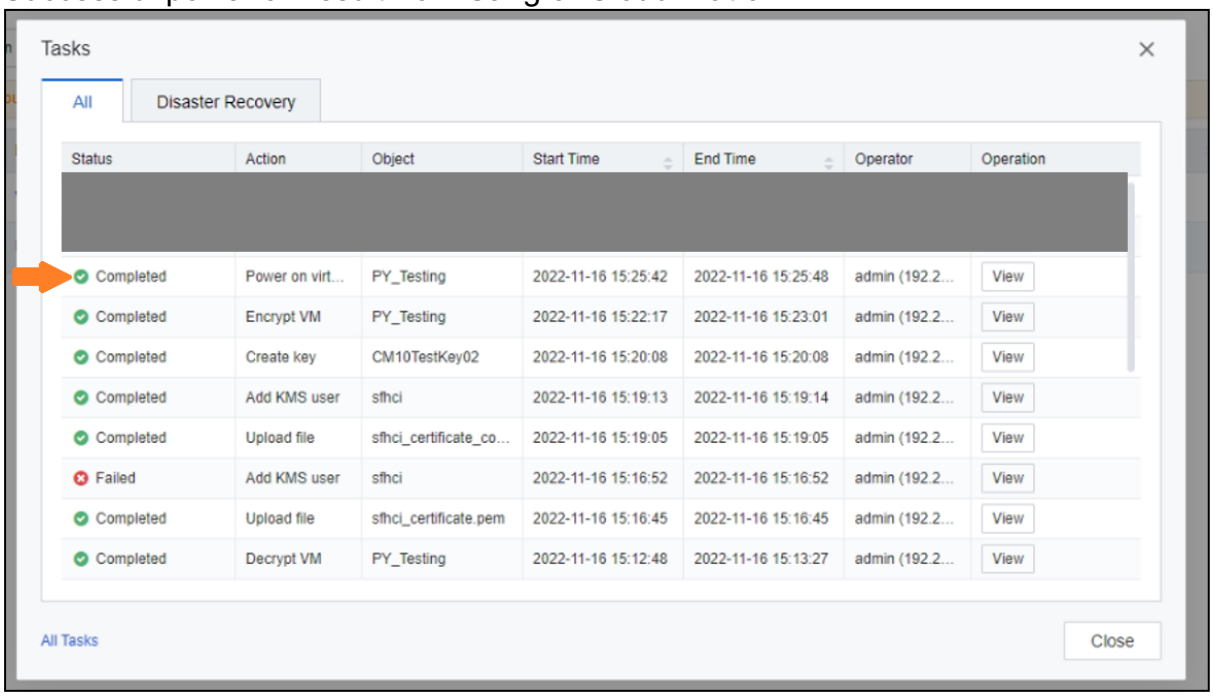

Virtual machine successful encrypted result from Sangfor Cloud Platform



## Power On the encrypted virtual machine - sfhci – CM10TestKey02




Successful power on result from Sangfor Cloud Platform:

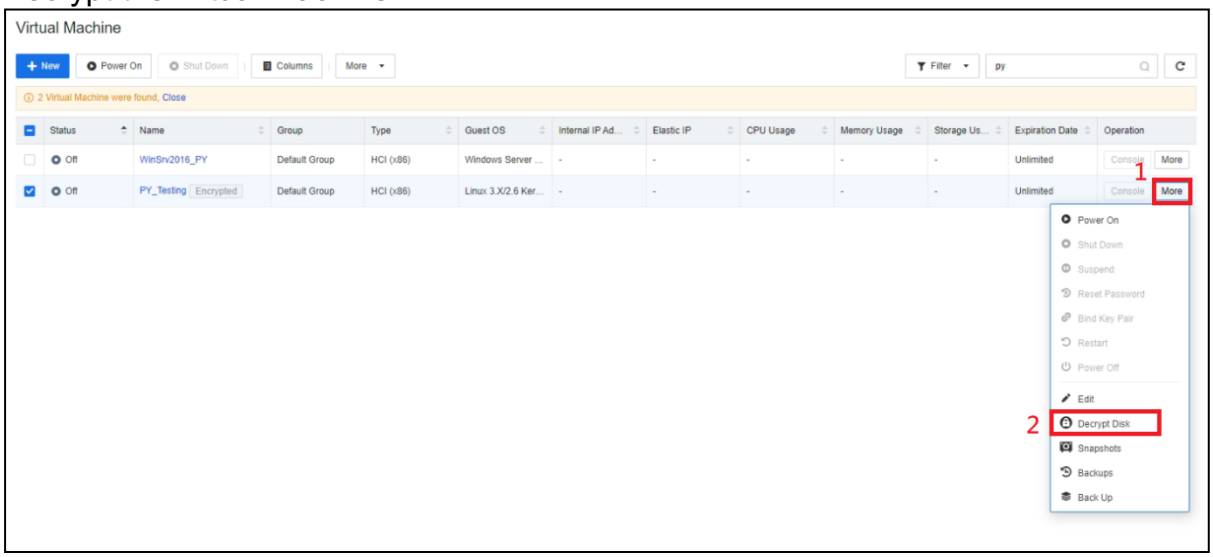



Successful power on result from CipherTrust Manager:

## Decrypted virtual machine - sfhci – CM10TestKey02

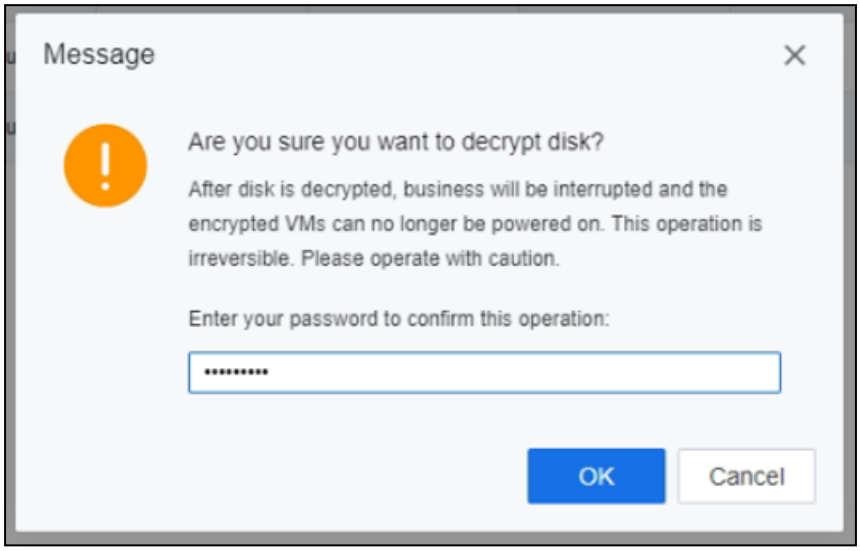
Ensure the virtual machine is in power off status

Decrypt the virtual machine

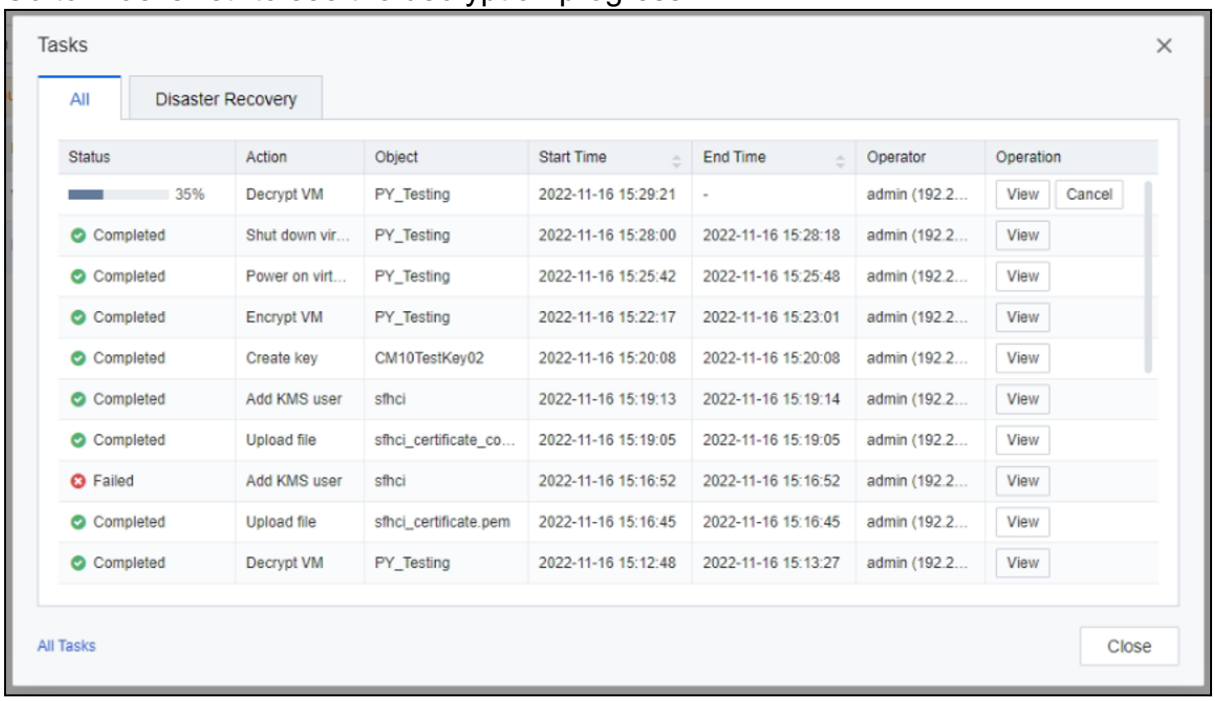



Type Sangfor Cloud Platform admin password to proceed the decrypt virtual machine action

Click “OK”

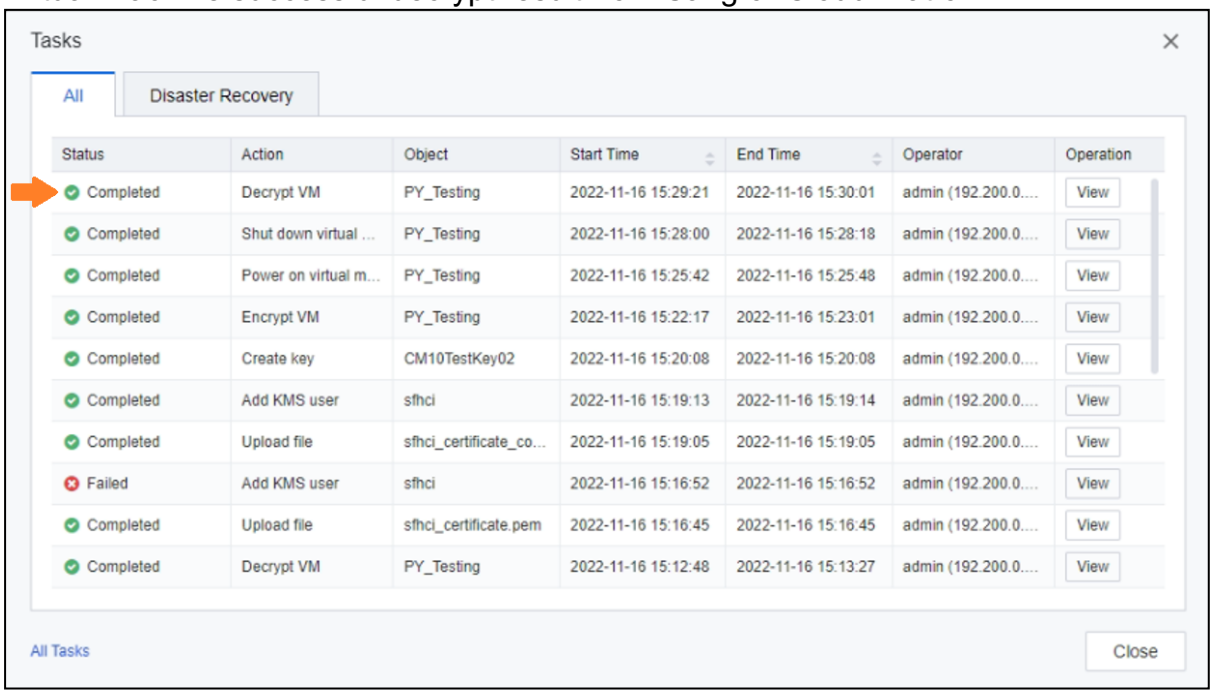


Go to “Tasks list” to see the decryption progress




Success use key status from CipherTrust Manager:


Virtual machine successful decrypt result from Sangfor Cloud Platform



# Conclusion:

Sangfor HCI and Thales CipherTrust KMS provide a powerful data security solution that is easy to manage, highly scalable, and cost-effective. By following this implementation guide, you can quickly deploy Sangfor HCI and Thales CipherTrust KMS, and begin securing your data in a matter of hours. Whether you are looking to deploy a new hyper-converged infrastructure or enhance your existing data security and management capabilities, Sangfor HCI and Thales CipherTrust KMS are a powerful combination that can help you achieve your goals