



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:

Overview:	2
Prerequisites:	2
Content:	3
CipherTrust Manager system configuration	4
KMIP client registration on CipherTrust Manager	10
Sangfor Cloud Platform KMS server connection configuration	23
Conclusion:	44

CipherTrust Manager system configuration

Update KMIP interface Mode

Go to "Admin Settings" → "Interfaces"

Click "View/Edit" on default kmip interface

THALES CipherTrust Manager

name: SE_CM2_10
version: 2.10.0-7973
crypto version: 1.6.0

API root/admin

Interfaces

4 Results | 4 Interfaces [+ Add Interface](#)

Name	NIC	Type	Port	Mode	Username Location in Certificate	Server Certificate Autogen
kmip	all	kmip	5696	TLS, verify client cert, password is needed, user name in cert must match user name in authentication request	CN	N/A
nae	all	nae	9000	TLS, ignore client cert, user must supply password	N/A	/C=US/ST=TX/L=Austin/O=Thales/CN=Ci
ssh	all	ssh	22	N/A	N/A	N/A
web	all	web	443	TLS, user must supply client cert or password	N/A	/C=US/ST=TX/L=Austin/O=Thales/CN=Ci

Restart Required
Changes to these settings may require a system restart via the services page in order to take effect

4 Interfaces

Create Sub Domain

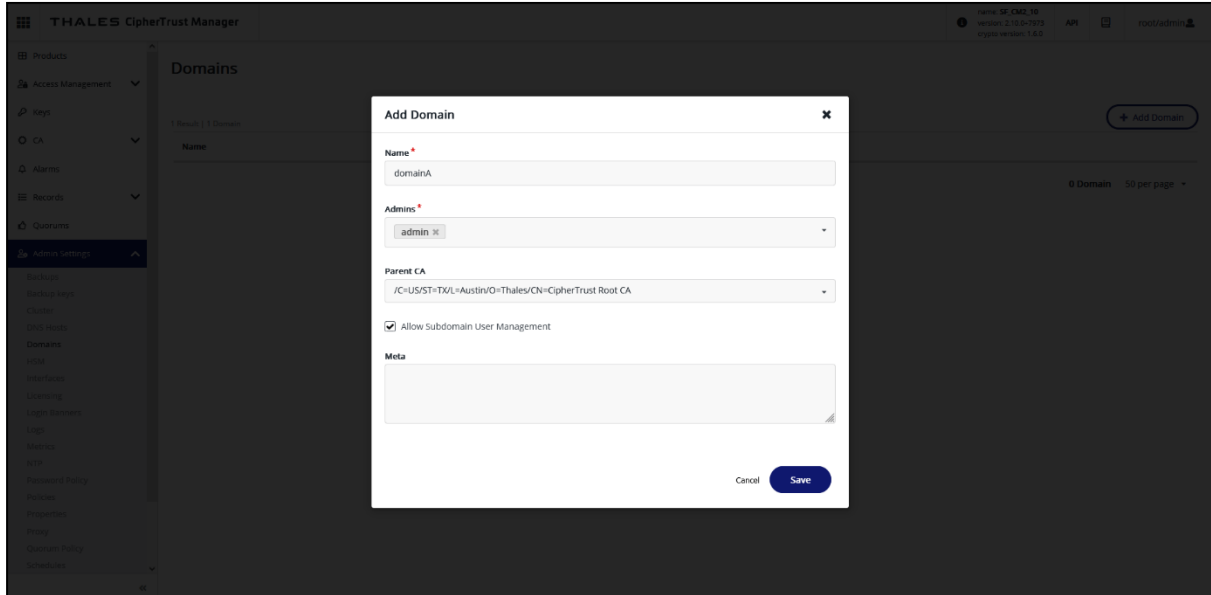
Go to “Admin Settings” → “Domains”

Click “+Add Domain”

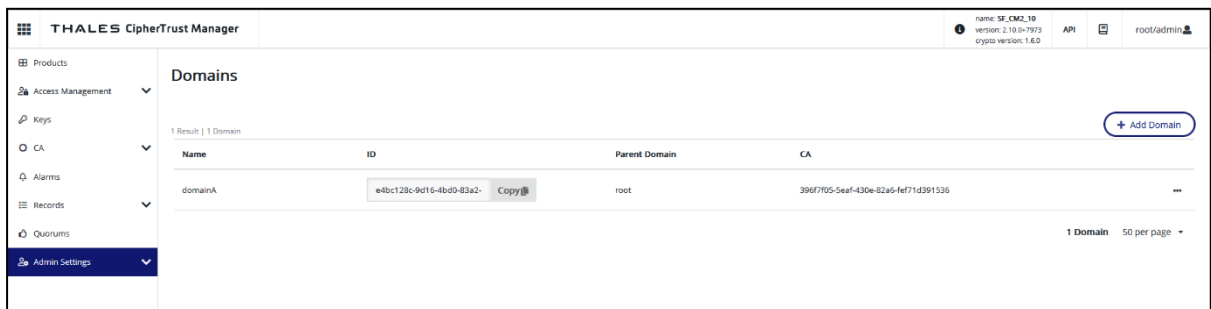
Name: domainA

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

The screenshot shows the THALES CipherTrust Manager interface. The top right corner displays the user 'domain/admin'. The left sidebar has 'CA' selected, with 'Local' highlighted. The main content area is titled 'Local Certificate Authorities' and shows a table with one entry:

Name	Subject	Serial #	Activation	Expiration	State	Client Auth	User Auth
localca-396f705-5eaf-430e-82a6-fef71d391536	/C=US/ST=TX/L=Austin/O=Thales/OU=NA/CN=CipherTrust CA for Domain domainA	24045448435412	a day ago	in 10 years	✓	Enabled	Enabled

A context menu is open over the first row, showing options: View, Copy, Download, Delete, Disable Client Auth, and Disable User Auth. Below the table, there is a section for 'Pending CAs' which is currently empty, displaying '0 Results | 0 Pending CAs' and 'No pending CAs to display'.

Import sub domainA CA certificate to root domain External CA List

Switch to root domain at top-right corner

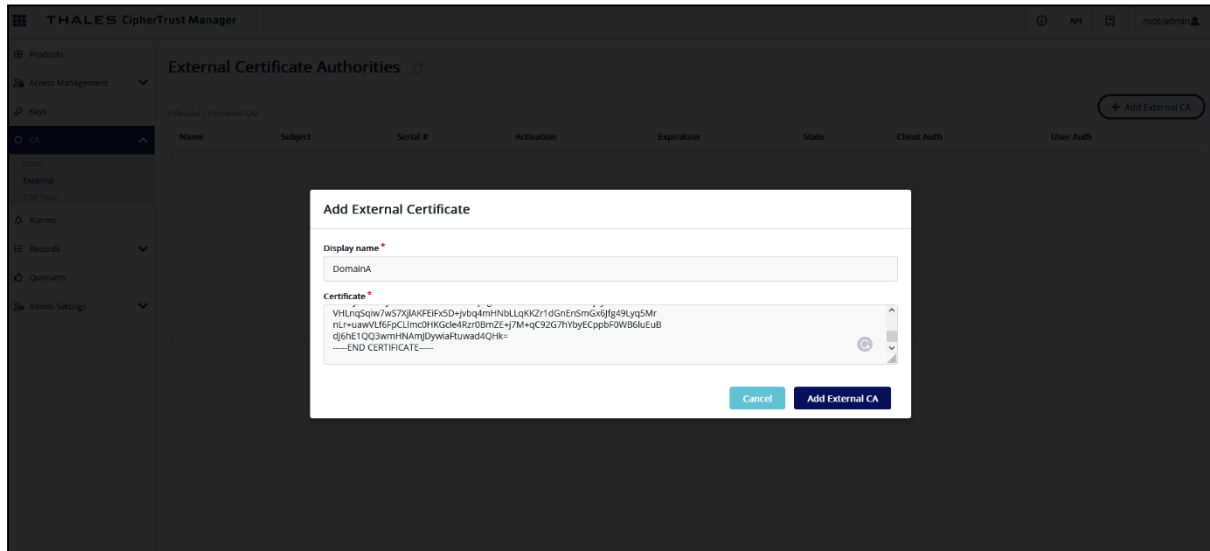
Click “CA” → “External” → “Add External CA”

The screenshot shows the THALES CipherTrust Manager interface. The top right corner displays the user 'root/admin'. The left sidebar has 'CA' selected, with 'External' highlighted. The main content area is titled 'External Certificate Authorities' and shows a table with no entries:

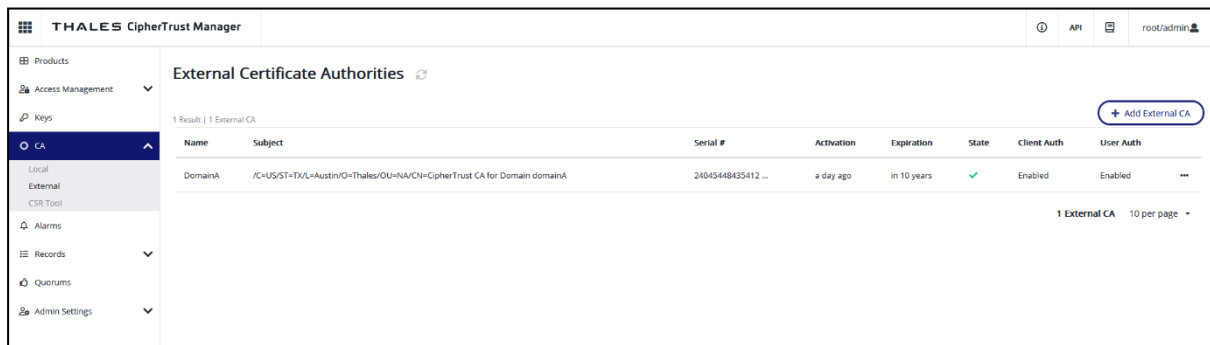
Name	Subject	Serial #	Activation	Expiration	State	Client Auth	User Auth
------	---------	----------	------------	------------	-------	-------------	-----------

Below the table, there is a section for 'External CAs' which is currently empty, displaying '0 Results | 0 External CAs' and 'No External CAs to display'.

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 ”

THALES CipherTrust Manager | name: SP_CMG_10 | version: 2.10.0-9793 | crypto version: 1.6.0 | API | root/admin

Products

- Access Management
- Keys
- CA
- Alarms
- Records
- Quorums
- Admin Settings**
- Backups
- Backup keys
- Cluster
- DNS Hosts
- Domains
- HSM
- Interfaces
- Licensing
- Login Barriers
- Logs
- Metrics
- NTP
- Password Policy
- Policies
- Properties
- Proxy
- Quorum Policy
- Schedules
- Services
- SMTP
- SNMP
- System

Interfaces

Interface Detail

Interface Enabled:
This interface is currently enabled. To disable it, choose the Disable action from the Interfaces List row action menu.

Name: kmpip

Port: 5696

Network Interface: all

Interface Mode: TLS, verify client cert, password is needed, user name in cert must match user name in authentication request

Enable hard delete

Auto Registration

Local CA for Automatic Server Certificate Generation

Disabled cipher suites (9)

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256

Enabled cipher suites (7)

- * TLS_AES_256_GCM_SHA384
- * TLS_CHACHA20_POLY1305_SHA256
- * TLS_AES_128_GCM_SHA256
- * TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Scroll down to External Trusted CA section

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

Click “Update” to save the configuration change

THALES CipherTrust Manager | name: SP_CMG_10 | version: 2.10.0-9793 | crypto version: 1.6.0 | API | root/admin

Products

- Access Management
- Keys
- CA
- Alarms
- Records
- Quorums
- Admin Settings**
- Backups
- Backup keys
- Cluster
- DNS Hosts
- Domains
- HSM
- Interfaces
- Licensing
- Login Barriers
- Logs
- Metrics
- NTP
- Password Policy
- Policies
- Properties
- Proxy
- Quorum Policy
- Schedules
- Services
- SMTP
- SNMP
- System

Local CA for Automatic Server Certificate Generation

Disabled cipher suites (9)

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256

Enabled cipher suites (7)

- * TLS_AES_256_GCM_SHA384
- * TLS_CHACHA20_POLY1305_SHA256
- * TLS_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Local Trusted CAs

CA

/C=US/ST=TX/L=Austin/O=Thales/CN=CipherTrust Root CA

External Trusted CAs

CA

/C=US/ST=TX/L=Austin/O=Thales/OJ=NA/CN=CipherTrust CA for Domain domainA

Update

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

The screenshot displays the THALES CipherTrust Manager web interface. The top navigation bar includes the product name, version information (name: SF_CM2_10, version: 2.10.0-7973, crypto version: 1.6.0), and the user 'root/admin'. The left sidebar shows a menu with 'Admin Settings' expanded. The main content area lists various services, each with a green status indicator and a red 'Restart' button. The 'nae-kmip' service is the first item in the list. At the bottom of the page, there is a red 'System Restart' button with a warning message: 'The system will be unavailable during restart!'.

Service Name	Status	Action
nae-kmip	Running	Restart
node-prometheus-metrics-exporter	Running	
old-user-management	Running	
pdb-manager	Running	
platform	Running	
postgres-db	Running	
protectv-manager	Running	
root-of-trust	Running	
scheduler	Running	
service-controller	Running	
syslog	Running	
UI	Running	
user-management	Running	
vte-management	Running	
web	Running	Restart

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”

THALES CipherTrust Manager

Products

Access Management

Users

Groups

Client Hub

Connections

LDAP

OpenID Connect

Registration Tokens

Keys

CA

Alarms

Records

Quorums

Admin Settings

root/admin

Full Name

name

Username *

sfhci

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

Assign user “sfhci” from root to domainA

Switch to sub domain domainA at top-right corner

Click “Access Management” → “Users” → “+ Assign User”

THALES CipherTrust Manager

name: SF_CM2_10
version: 2.10.0+7973
crypto version: 1.6.0

API

domainA/admin

Products

Access Management

Users

Groups

Client Hub

Connections

Registration Tokens

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, 10:56:53 pm	local 34bed35e-177e-417b Copy	Wednesday, November 16th 2022, 10:34:47 pm	34	Wednesday, November 16th 2022, 2:25:56 pm

1 Users 10 per page

Click "Assign"

THALES CipherTrust Manager

Products

Access Management

Users

Assign users

Name	Source	Email	ID
admin	local		local 34bed35e-177e-417b
sfhci	local	sfhci@local	local 90fe7a13-d624-4d31-

Assign

2 Users 10 per page

Result:

THALES CipherTrust Manager

Products

Access Management

Users

Users

+ 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, 10:56:53 pm	local 34bed35e-177e-417b	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, 11:02:20 pm	local 90fe7a13-d624-4d31-	Wednesday, November 16th 2022, 11:02:20 pm	132544	Never Failed A Login

2 Users 10 per page

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

THALES CipherTrust Manager

Products

Access Management

Users

Users

+ 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	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, 11:23:20 pm	local 90fe7a13-d624-4d31-	Wednesday, November 16th 2022, 11:23:20 pm	132565	Never Failed A Login

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 * **Email**

dasfhci 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: SE_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

[+ Add User](#) [+ Assign User](#)

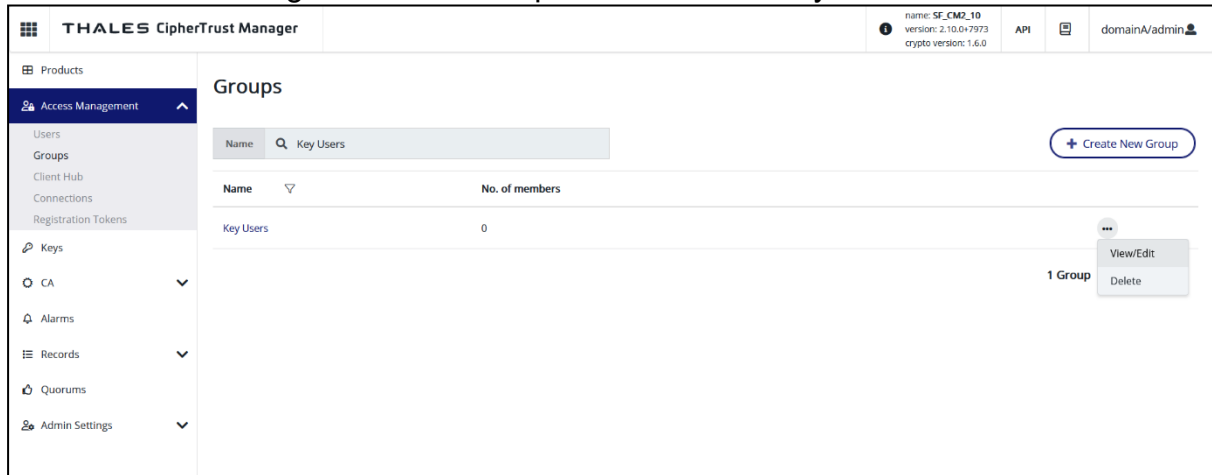
Username	Full Name	Email	Source	Created	Updated	ID	Last Login	Logins	Last Failed Login
admin	admin		local	Tuesday, August 2nd 2022, 11:03:05 am	Wednesday, November 16th 2022, 11:23:29 pm	local 34bed35e-177e-417b- Copy	Wednesday, November 16th 2022, 10:34:47 pm	34	Wednesday, November 16th 2022, 2:25:56 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

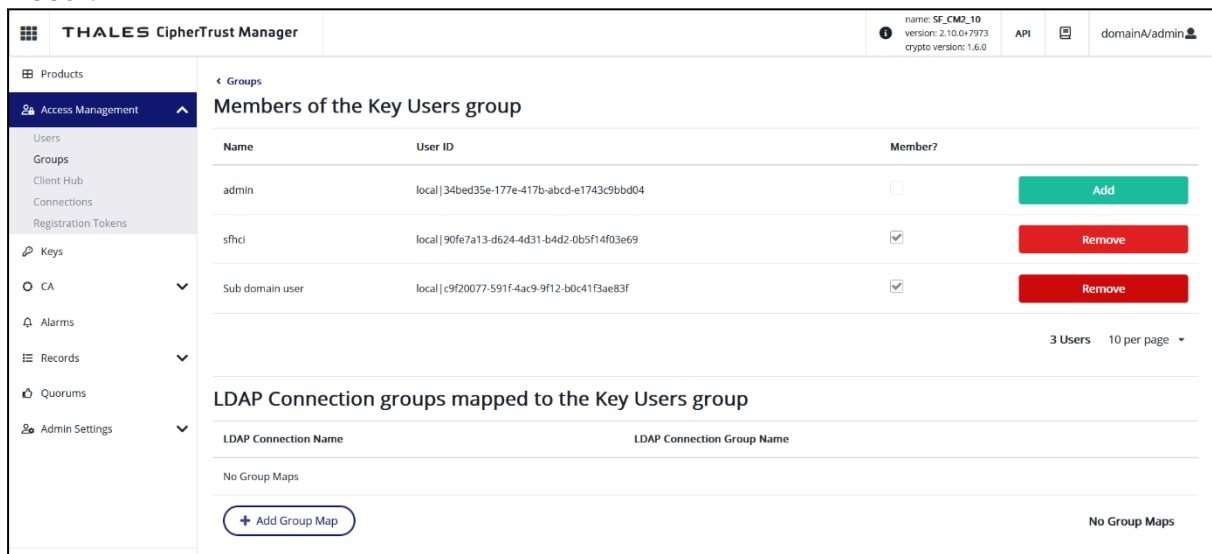
At domainA

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 from the Organization Unit filed in the client certificate)

Organizational Unit: **domainA|sfhci**

Common Name: hko

Add Profile

Profile Name ^{*}
hko_assigned_user_from root

Username Location in Certificate
OU

Subject DN field to modify [?]
OU (organizationalUnit) Do not modify subject DN

Certificate Details

CSR
Contents of .csr file

Organization
intergration test

Organizational Unit (comma separated)
domainA| |sfhcl

Email

OR

UID

City
HongKong

Common Name
hko

State

Country

Device Credentials

Cancel Save

Result:

Client Profiles

Success
Profile hko_assigned_user_from ro created

+ Add Profile

Name	CSR	Organization Name
hko_assigned_user_from root		intergration test

1 Registered Client 10 per page

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”

Registration Token

Name	Token	Profile	Expires	Uses Remaining	Use
------	-------	---------	---------	----------------	-----

Create New Registration Token

01 Configure Token 02 Select CA 03 Select Profile 04 Create Token

Use company specific naming conventions when setting up a new token.

Name Prefix

Token lifetime Certificate Duration Client Capacity

Back Select CA

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

Create New Registration Token

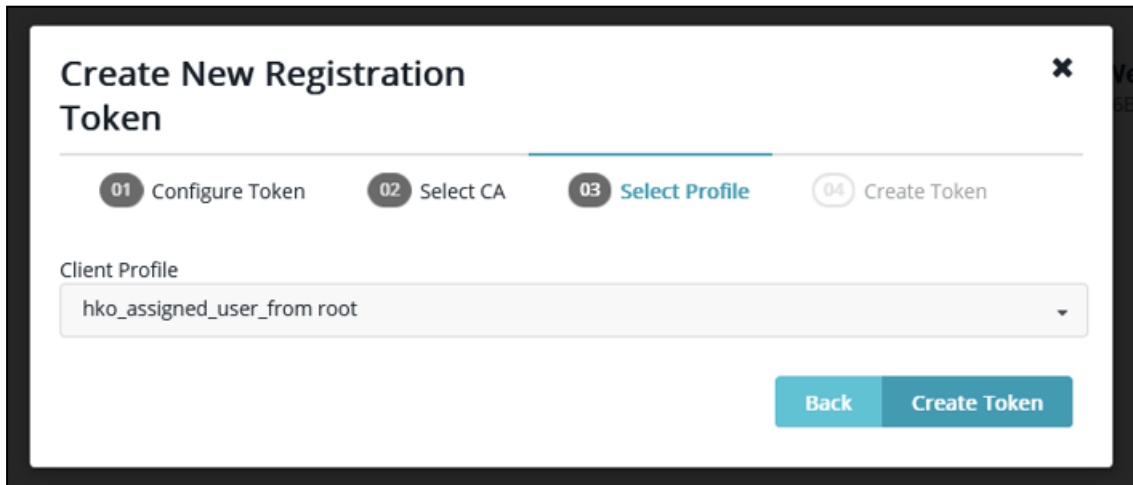
01 Configure Token 02 Select CA 03 Select Profile 04 Create Token

CA Type
 Local External

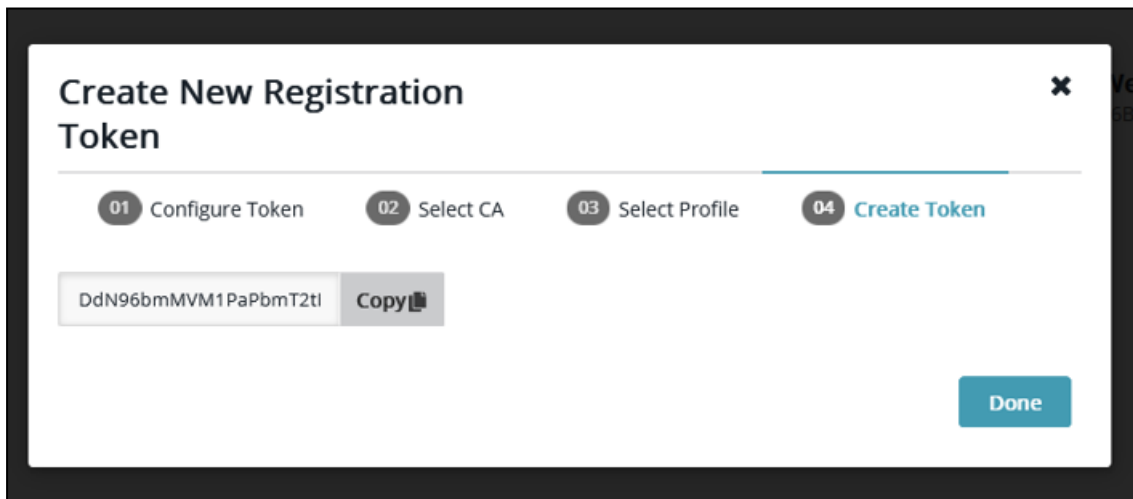
Local CA

Back 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

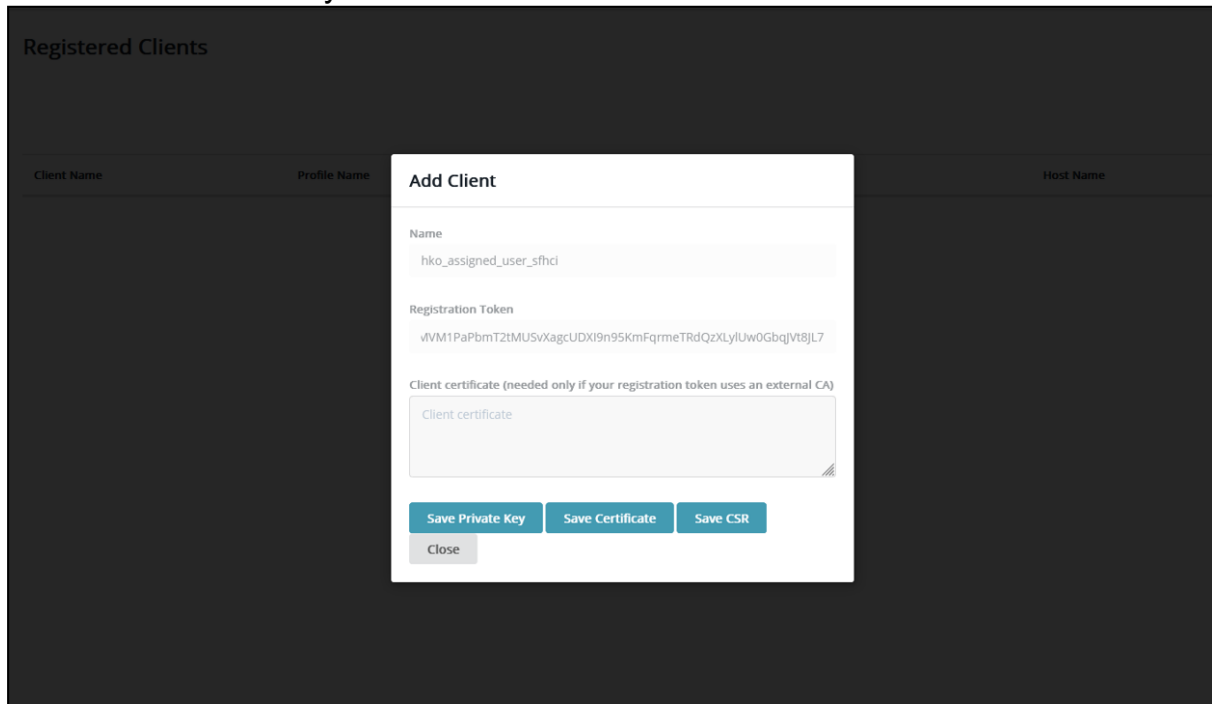
Click "+Add Client"

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.



The screenshot shows a web interface for managing registered clients. The main area is titled "Registered Clients" and contains a table with columns for "Client Name", "Profile Name", and "Host Name". A modal dialog box titled "Add Client" is open, allowing the user to create a new client. The dialog has the following fields and buttons:

- Name:** A text input field containing "hko_assigned_user_sfhci".
- Registration Token:** A text input field containing "vVM1PaPbmT2tMUSvXagcUDXI9n95KmFqrmeTRdQzXLyUw0GbqJt8JL7".
- Client certificate (needed only if your registration token uses an external CA):** A text area for entering a client certificate.
- Buttons:** "Save Private Key", "Save Certificate", "Save CSR", and "Close".

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 from 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:

Name	CSR	Organization Name	
▸ hko_sub_domain_user		Integration test	...
▸ hko_assigned_user_from root		intergration test	...

2 Registered Clients 10 per page ▾

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"

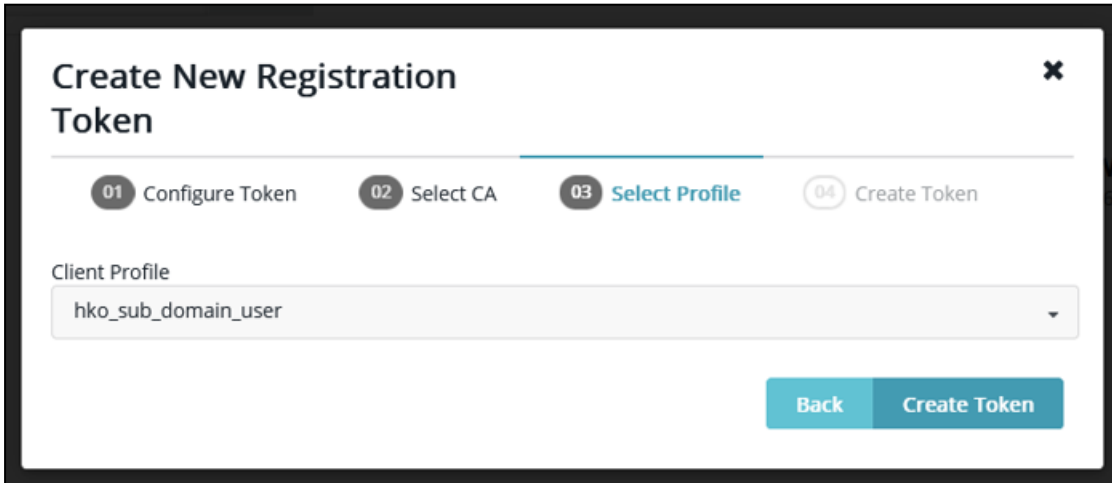
The screenshot shows a dialog box titled "Create New Registration Token" with a close button (X) in the top right corner. Below the title is a progress bar with four steps: 01 Configure Token (highlighted), 02 Select CA, 03 Select Profile, and 04 Create Token. Below the progress bar is a note: "Use company specific naming conventions when setting up a new token." The "Name Prefix" field contains "hko_sub_doamin_user". Below this are three fields: "Token lifetime" set to "unlimited" with a checkmark icon, "Certificate Duration" set to "730" with a dropdown arrow, and "Client Capacity" set to "100" with a dropdown arrow. At the bottom right are two buttons: "Back" and "Select CA".

Select the client certificate issuer CA (domainA default CA)

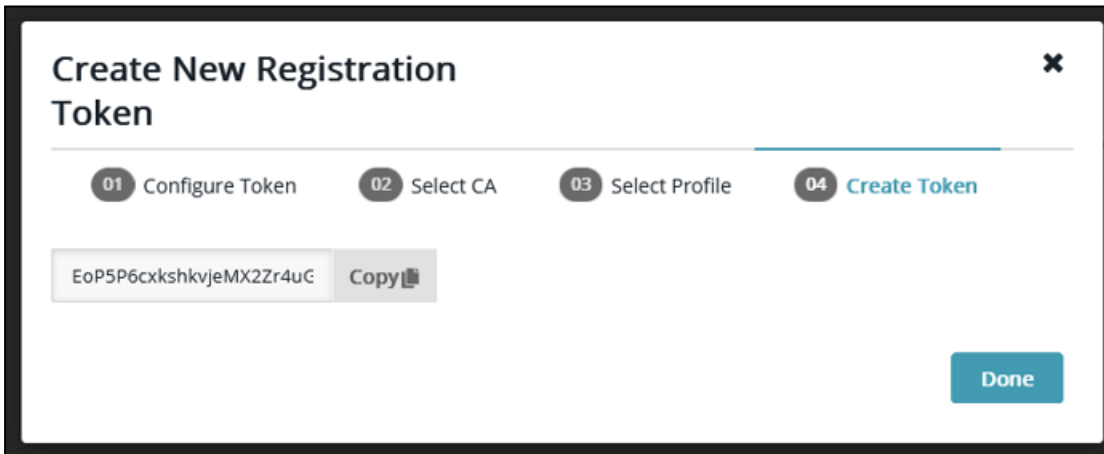
Click "Select Profile"

The screenshot shows the same dialog box, now at step 02: Select CA. The progress bar highlights step 02. Below the progress bar is the "CA Type" section with two radio buttons: "Local" (selected) and "External". Below this is the "Local CA" section with a dropdown menu showing the selected CA: "/C=US/ST=TX/L=Austin/O=Thales/OU=NA/CN=CipherTrust CA for Domain domainA". At the bottom right are two buttons: "Back" and "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.

Add Client

Name
hko_sub_domain_user_dasfhci

Registration Token
'6cxkshkvjeMX2Zr4uGnvDYf3IfOO85Jjf8Myl51mDRDwnVbRZtKfyxp6Uwp

Client certificate (needed only if your registration token uses an external CA)
Client certificate

Save Private Key Save Certificate Save CSR Close

Rename the private key file as dasfhci_pri.key

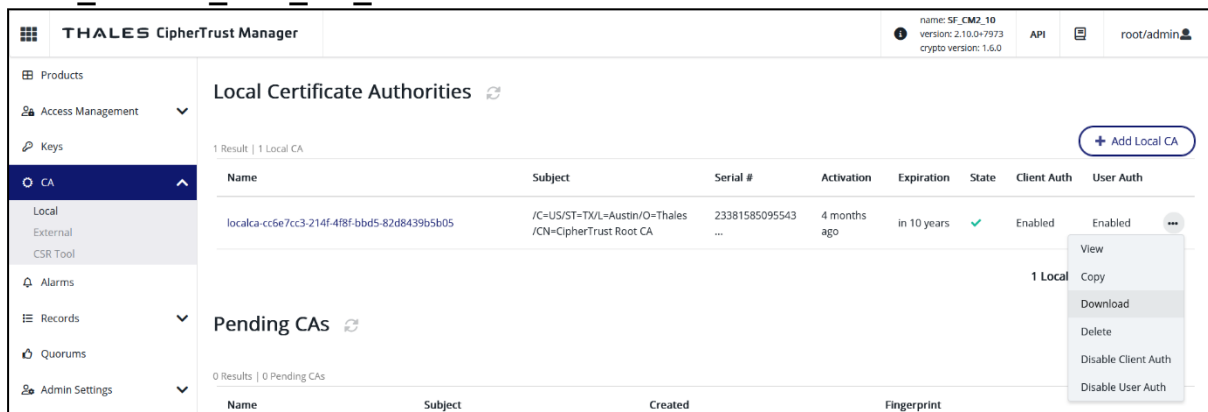
Rename the certificate as dasfhci.pem

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

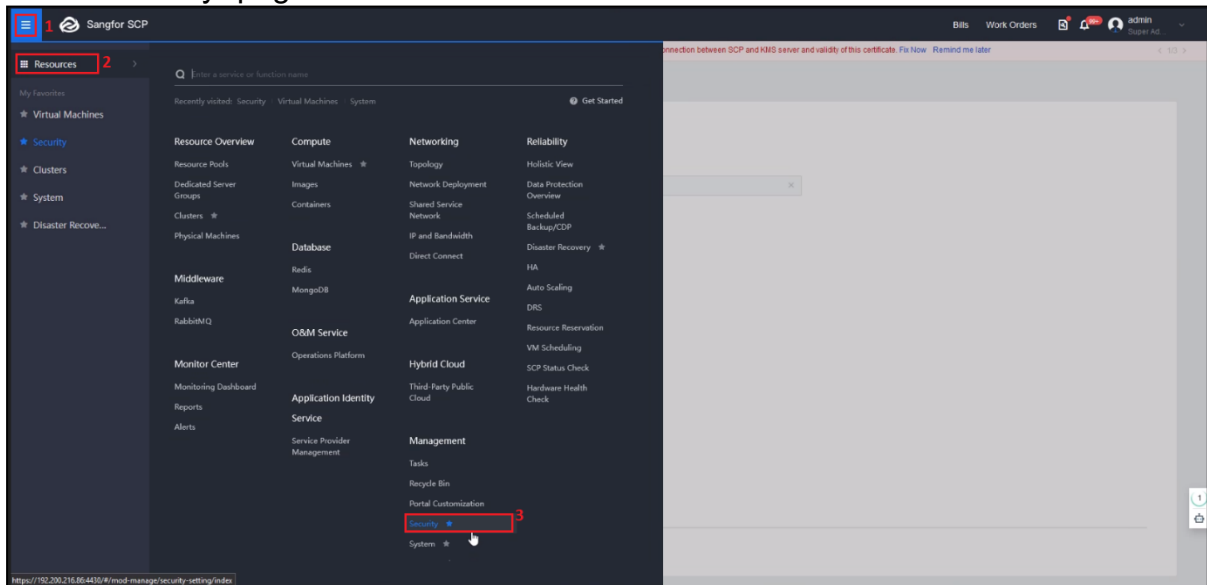
User list		
	root	domainA
admin	Yes	Yes (assigned from root)
sfhci	Yes	Yes (assigned from root)
dasfhci	No	Yes

Sangfor Cloud Platform KMS server connection configuration

Add a KMS server with dasfhci user

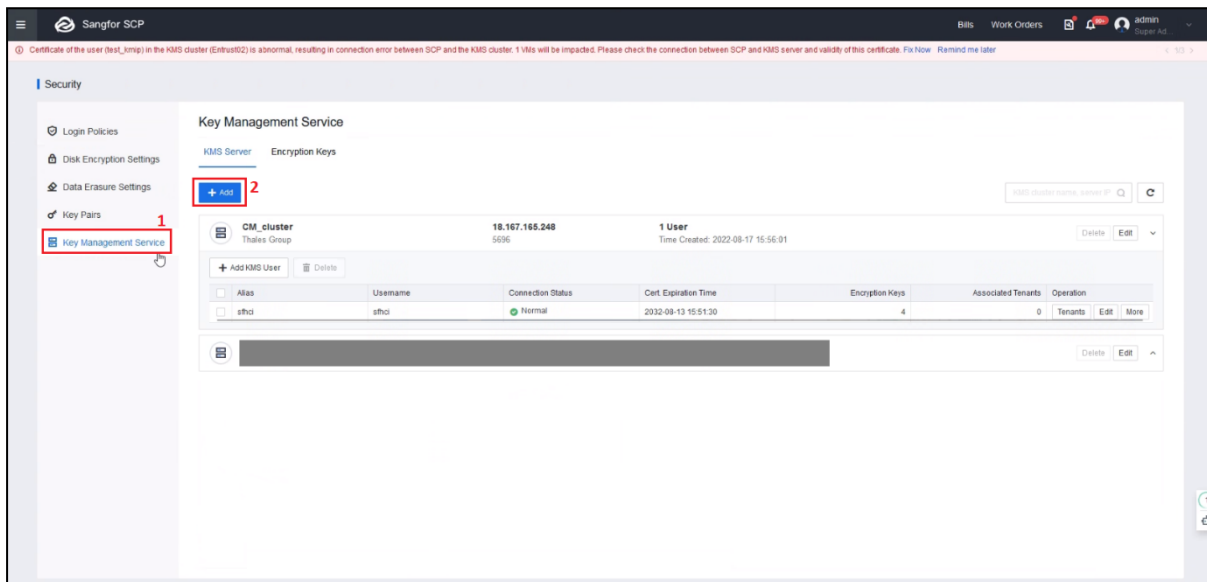
Open Sangfor Cloud Platform web console:

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"

Add KMS Server

KMS Server Authentication

KMS Cluster Name: CM_2_10

Server IP: 18.167.165.89

Server Port: 5696

Certificate Type: crt

Auth Certificate: Root_domain_root_CA_Certificate.crt

KMS User Authentication

KMS User: User 1

Alias: dasfhci

Username: domainA|domainA||dasfhci

Password:

Certificate Type: pem

Auth Certificate: dasfhci_certificate_combined.pem

+ Add Currently added: 1, Maximum: 5

OK Cancel

Result:

Key Management Service

KMS Server Encryption Keys

[+ Add](#) KMS cluster name, server IP

CM_2_10
Thales Group **18.167.165.89** **1 User**
5696 Time Created: 2022-11-16 14:51:54 Delete Edit

[+ Add KMS User](#)

Alias	Username	Connection Status	Cert. Expiration Time	Encryption Keys	Associated Tenants	Operation
<input type="checkbox"/> desfhci	domainA\domainA\desfhci	● 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)

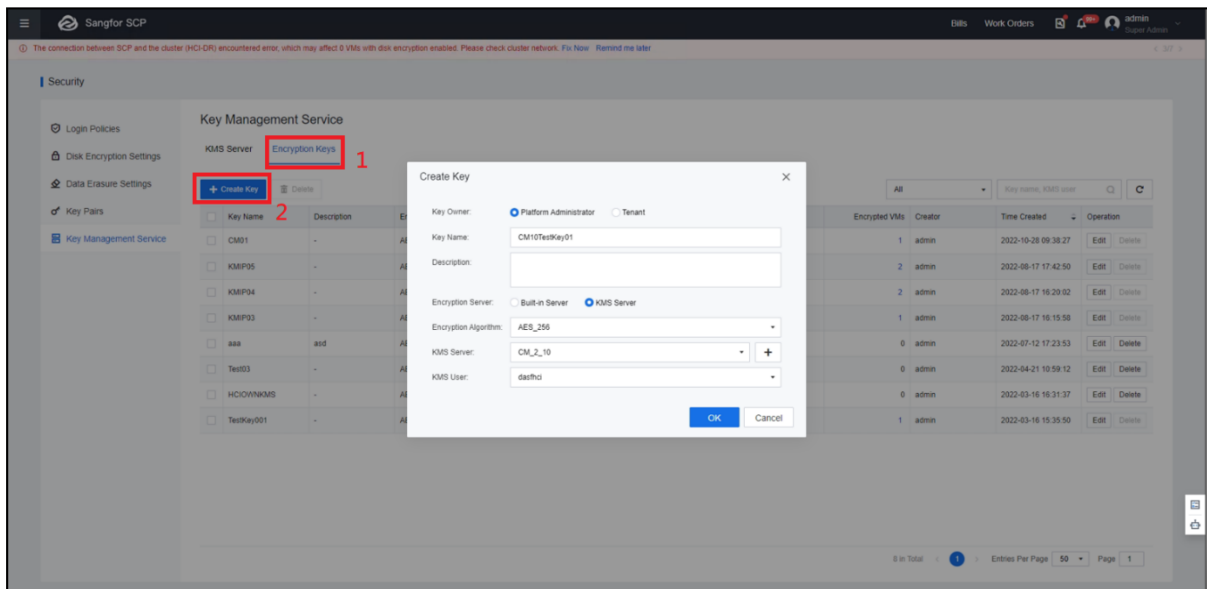
Encryption Server: KMS Server

Encryption Algorithm: AES_256

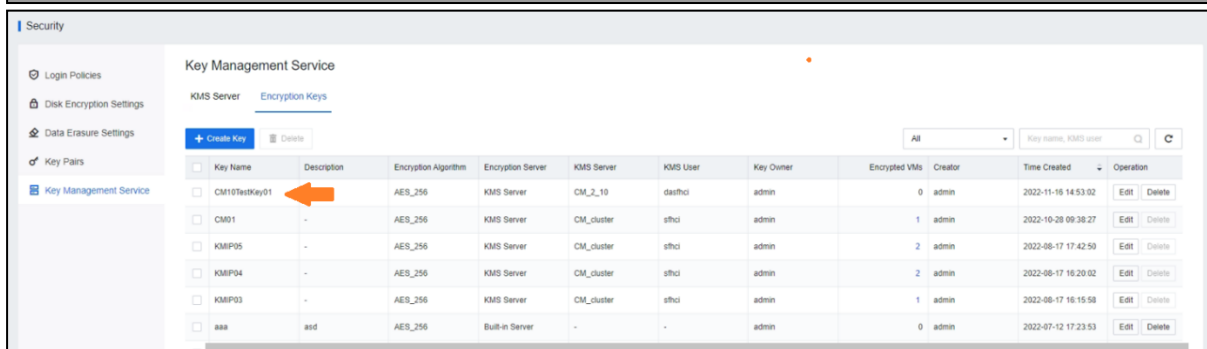
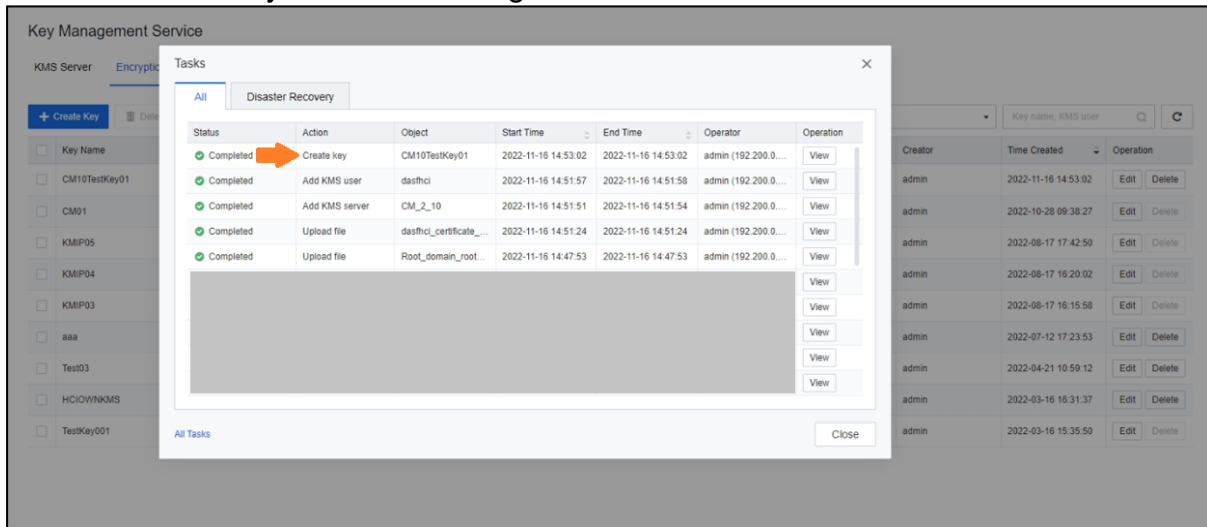
KMS Server: CM_2_10

KMS User: dasfhci

Click “OK”



Success create key result from Sangfor Cloud Platform:



Success create key result from CipherTrust Manager

THALES CipherTrust Manager | domainA/admin

Keys

Owner Name: Sub domain user

Filters: Basic | Raw | Label Filters

Type / Algorithm: | Size / Curve ID: | State / Revocation: | Event Dates: |

Latest Version Only

Owner Name: Sub domain user

[+ Add Key](#)

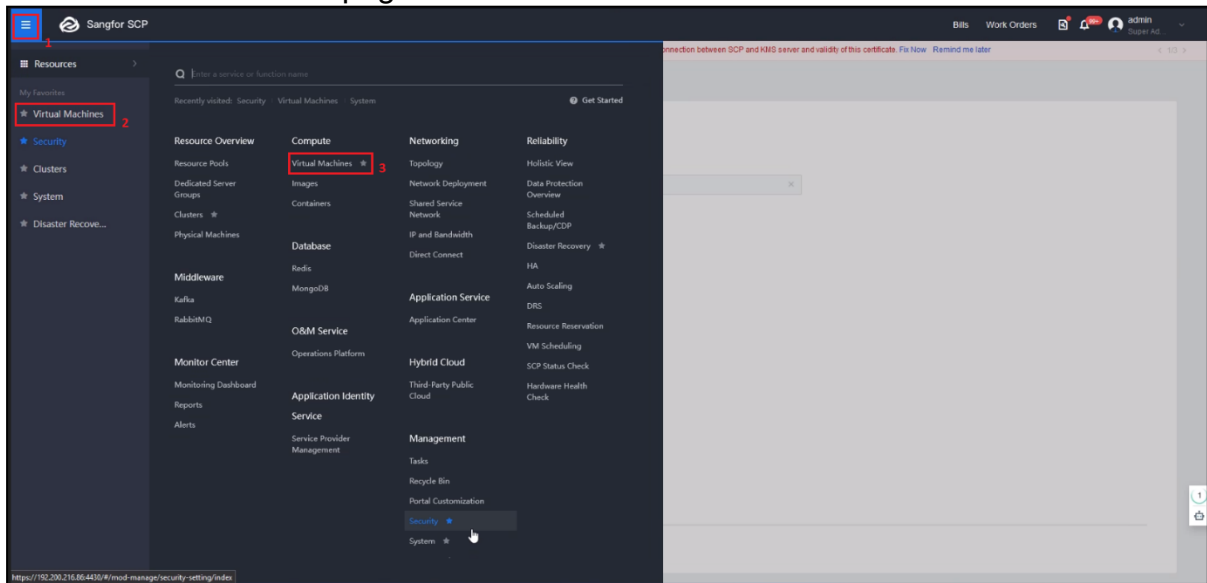
Key Name	Version	Owner	Modified	Type	Algorithm	Size
ks-0c9abd03580141c9bab479f134c209704fbc161bd34e179cf09af6eaab6fcf	0	local Sub domain user	17 Nov 2022, 10:33	Symmetric	AES	256

1 Key 50 per page

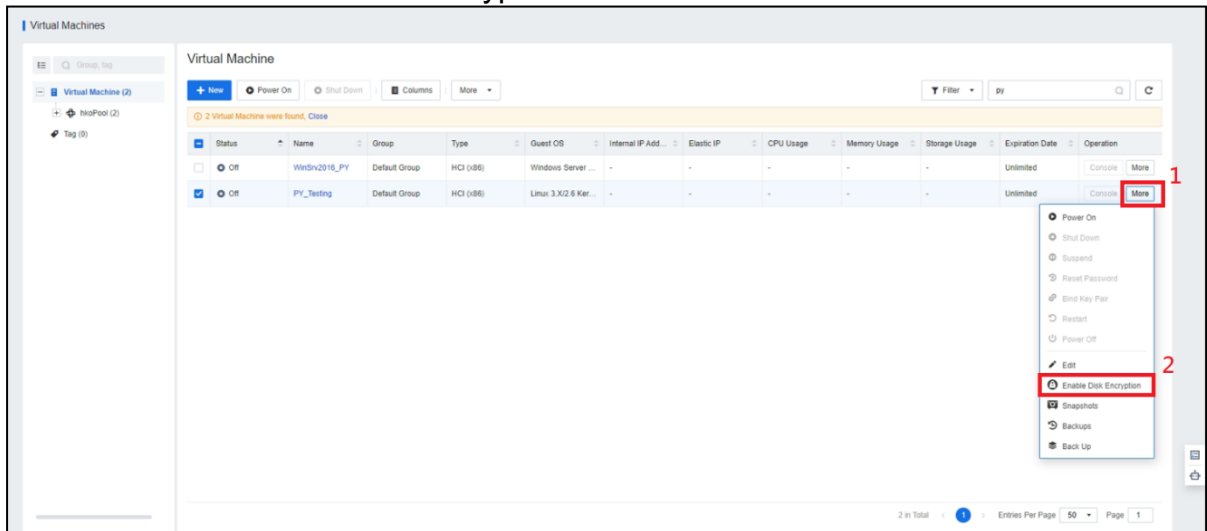
Status	Level	Time	Event	Details
✓	INFO	Nov 16th 2022 - 14:52:31	Create Key	<pre>{ "id": "0c9abd03580141c9bab479f134c209704fbc161bd34e179cf09af6eaab6fcf", "uri": "kylo:kylo-e4bc128c-5d16-4bd9-83a2-8172245a1318::vault:keys:ks-0c9abd03580141c9bab479f134c209704fbc161bd34e179cf09af6eaab6fcf-v0", "name": "ks-0c9abd03580141c9bab479f134c209704fbc161bd34e179cf09af6eaab6fcf", "size": 256, "ownerId": "local c9f20077-591f-4ac9-9f12-bbc41f3ae83f", "algorithm": "AES", "usageMask": 12, "objectType": "Symmetric Key" }</pre>
✓	INFO	Nov 16th 2022 - 14:52:31	Kmip Authentication	<pre>{ "userId": "local c9f20077-591f-4ac9-9f12-bbc41f3ae83f", "userName": "dasfnci" }</pre>

Encrypt the virtual machine

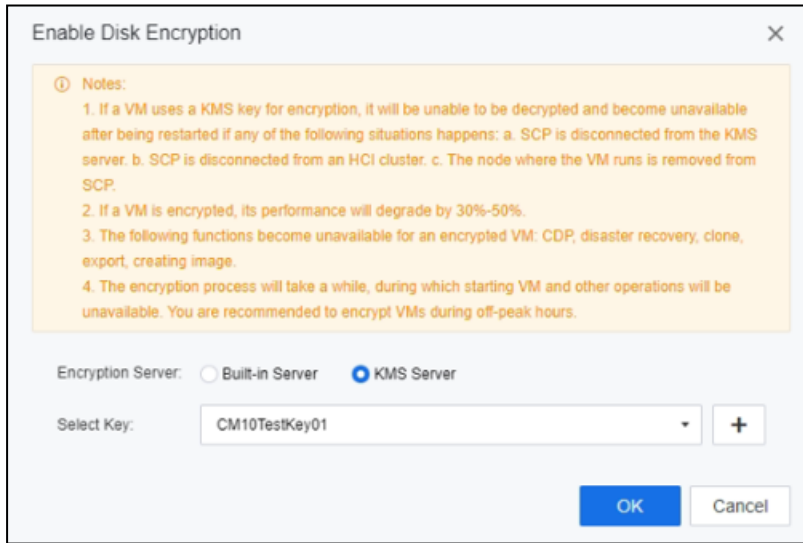
Go to “Virtual Machine” page



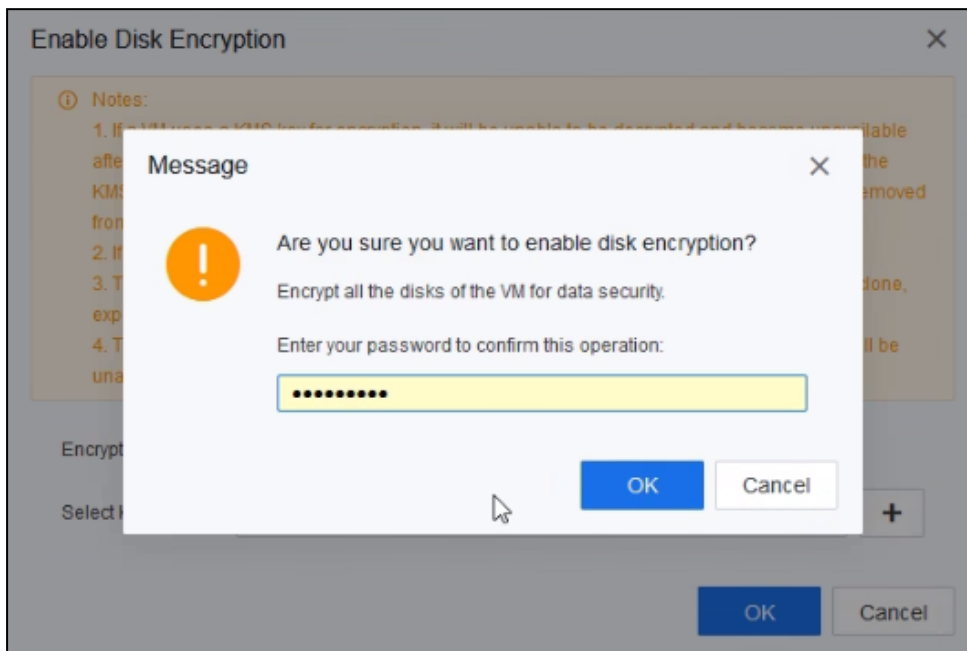
Ensure the virtual machine is in power off status
Click “More” → “Enable Disk Encryption”



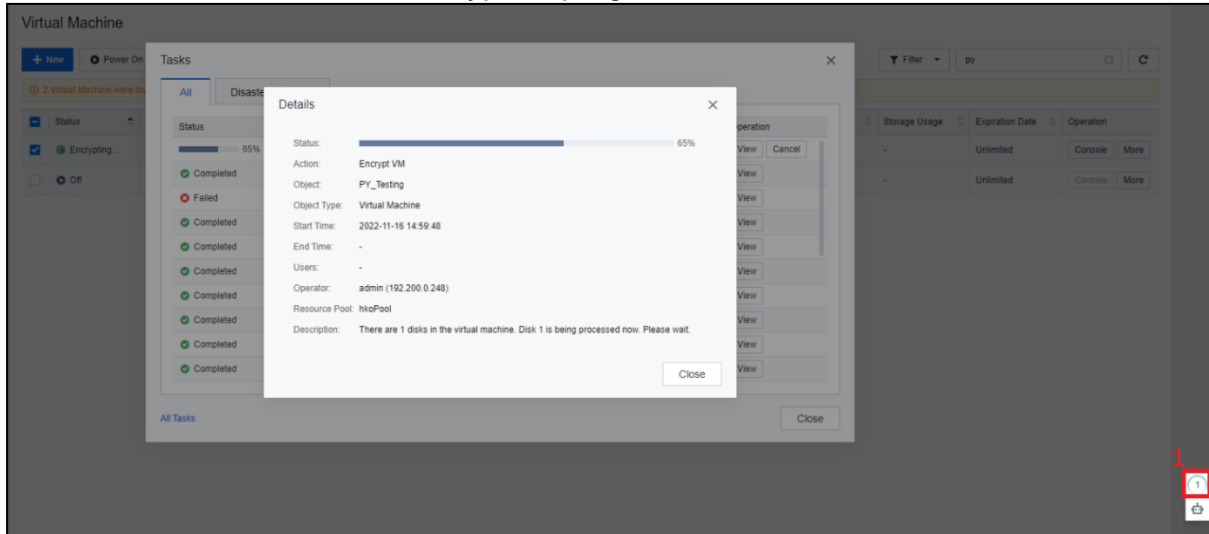
Encryption Server: KMS Server
Select Key: **CM10TestKey01**
Click "OK"



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



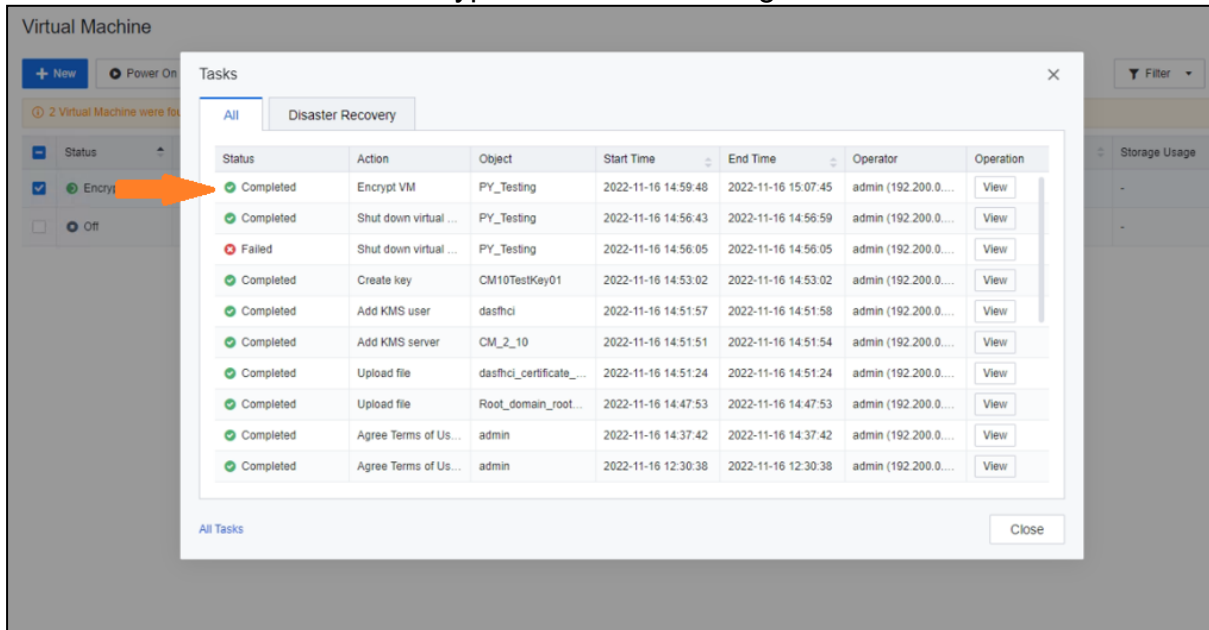
Go to "Tasks list" to see the encryption progress



Success use key status from CipherTrust Manager:

INFO	Nov 16th 2022 - 14:59:23	Use Key	{ "Identifier": "0c9ab403580141c9bab479f134c209704fbc0d161bd34e179cf09af6caab6fcf" }	dasfhci	SF_CM2_10	218.253.76.106	...
INFO	Nov 16th 2022 - 14:59:23	Kmip Authentication	{ "userId": "local c9f20077-591f-4ac9-9f12-b0c41f3ae83f", "username": "dasfhci" }		SF_CM2_10	218.253.76.106	...

Virtual machine successful encrypted result from Sangfor Cloud Platform



Power On the encrypted virtual machine - dasfhci – CM10TestKey01

Virtual Machine

+ New Power On Shut Down Columns More

Filter py

2 Virtual Machines were found. Close

Status	Name	Group	Type	Guest OS	Internal IP Ad...	Elastic IP	CPU Usage	Memory Usage	Storage Us...	Expiration Date	Operation
Off	WinSrv2016_PY	Default Group	HCI (x86)	Windows Server ...	-	-	-	-	-	Unlimited	Console More
Off	PY_Testing Encrypted	Default Group	HCI (x86)	Linux 3.X/2.6 Ker...	-	-	-	-	-	Unlimited	Console More

More

- Power On
- Shut Down
- Suspend
- Reset Password
- Bind Key Pair
- Restart
- Power Off
- Edit
- Decrypt Disk
- Snapshots
- Backups
- Back Up

Successful power on result from Sangfor Cloud Platform:

Tasks

All Disaster Recovery

Status	Action	Object	Start Time	End Time	Operator	Operation
Completed	Power on virtual m...	PY_Testing	2022-11-16 15:09:04	2022-11-16 15:09:11	admin (192.200.0...	View
Completed	Encrypt VM	PY_Testing	2022-11-16 14:59:48	2022-11-16 15:07:45	admin (192.200.0...	View
Completed	Shut down virtual ...	PY_Testing	2022-11-16 14:56:43	2022-11-16 14:56:59	admin (192.200.0...	View
Failed	Shut down virtual ...	PY_Testing	2022-11-16 14:56:05	2022-11-16 14:56:05	admin (192.200.0...	View
Completed	Create key	CM10TestKey01	2022-11-16 14:53:02	2022-11-16 14:53:02	admin (192.200.0...	View
Completed	Add KMS user	dasfhci	2022-11-16 14:51:57	2022-11-16 14:51:58	admin (192.200.0...	View
Completed	Add KMS server	CM_2_10	2022-11-16 14:51:51	2022-11-16 14:51:54	admin (192.200.0...	View
Completed	Upload file	dasfhci_certificate_...	2022-11-16 14:51:24	2022-11-16 14:51:24	admin (192.200.0...	View
Completed	Upload file	Root_domain_root...	2022-11-16 14:47:53	2022-11-16 14:47:53	admin (192.200.0...	View
Completed	Agree Terms of Us...	admin	2022-11-16 14:37:42	2022-11-16 14:37:42	admin (192.200.0...	View

All Tasks Close

Successful power on result from CipherTrust Manager:

INFO	Nov 16th 2022 - 15:08:37	Use Key	{ "identifier": "0c9ab03580141c9bab479f134c209704fbcdd161bd34e179cf09af6eaab6fcf" }	dasfhci	SF_CM2_10	218.253.76.106	...
INFO	Nov 16th 2022 - 15:08:37	Kmip Authentication	{ "userId": "local c9f20077-591f-4ac9-9f12-b0c41f3ae83f", "username": "dasfhci" }		SF_CM2_10	218.253.76.106	...

Decrypted virtual machine - dasfhci – CM10TestKey01

Ensure the virtual machine is in power off status

Decrypt the virtual machine

Status	Name	Group	Type	Guest OS	Internal IP Ad.	Elastic IP	CPU Usage	Memory Usage	Storage Us...	Expiration Date	Operation
<input type="checkbox"/>	WinSrv2016_PY	Default Group	HCI (x86)	Windows Server ...	-	-	-	-	-	Unlimited	Console ¹ More
<input checked="" type="checkbox"/>	PY_Testing Encrypted	Default Group	HCI (x86)	Linux 3.X/2.6 Ker...	-	-	-	-	-	Unlimited	Console ² Decrypt Disk

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

Click "OK"

Message

Are you sure you want to decrypt disk?

After disk is decrypted, business will be interrupted and the encrypted VMs can no longer be powered on. This operation is irreversible. Please operate with caution.

Enter your password to confirm this operation:

OK Cancel

Go to "Tasks list" to see the decryption progress

Tasks

All Disaster Recovery

Status	Action	Object	Start Time	End Time	Operator	Operation
19%	Decrypt VM	PY_Testing	2022-11-16 15:12:48	-	admin (192.2...	View Cancel
Completed	Shut down vir...	PY_Testing	2022-11-16 15:11:38	2022-11-16 15:11:57	admin (192.2...	View
Completed	Power on virt...	PY_Testing	2022-11-16 15:09:04	2022-11-16 15:09:11	admin (192.2...	View
Completed	Encrypt VM	PY_Testing	2022-11-16 14:59:48	2022-11-16 15:07:45	admin (192.2...	View
Completed	Shut down vir...	PY_Testing	2022-11-16 14:56:43	2022-11-16 14:56:59	admin (192.2...	View
Failed	Shut down vir...	PY_Testing	2022-11-16 14:56:05	2022-11-16 14:56:05	admin (192.2...	View
Completed	Create key	CM10TestKey01	2022-11-16 14:53:02	2022-11-16 14:53:02	admin (192.2...	View
Completed	Add KMS user	dasfhci	2022-11-16 14:51:57	2022-11-16 14:51:58	admin (192.2...	View
Completed	Add KMS ser...	CM_2_10	2022-11-16 14:51:51	2022-11-16 14:51:54	admin (192.2...	View
Completed	Upload file	dasfhci_certificate_...	2022-11-16 14:51:24	2022-11-16 14:51:24	admin (192.2...	View

All Tasks Close

Success use key status from CipherTrust Manager:

INFO Nov 16th 2022 - 15:12:22 Use Key { "identifier": "0c9abd03580141c9bab479f134c289704afbcd161bd34e179cf09af6eaab6fcf" } SF_CM2_10 218.253.76.106 ...

INFO Nov 16th 2022 - 15:12:22 Kmp Authentication { "userId": "local|c9f28077-591f-4ac9-9f12-b0c41f3ae83f", "username": "dasfhci" } SF_CM2_10 218.253.76.106 ...

Virtual machine successful decrypt result from Sangfor Cloud Platform

Tasks

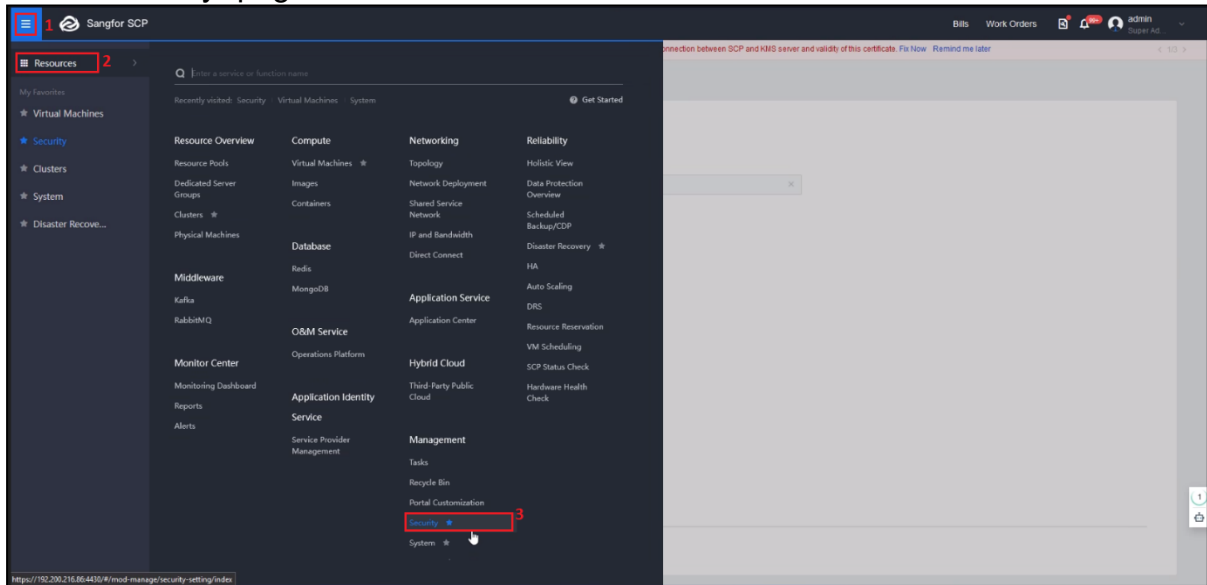
All Disaster Recovery

Status	Action	Object	Start Time	End Time	Operator	Operation
Completed	Decrypt VM	PY_Testing	2022-11-16 15:12:48	2022-11-16 15:13:27	admin (192.200.0...	View
Completed	Shut down virtual ...	PY_Testing	2022-11-16 15:11:38	2022-11-16 15:11:57	admin (192.200.0...	View
Completed	Power on virtual m...	PY_Testing	2022-11-16 15:09:04	2022-11-16 15:09:11	admin (192.200.0...	View
Completed	Encrypt VM	PY_Testing	2022-11-16 14:59:48	2022-11-16 15:07:45	admin (192.200.0...	View
Completed	Shut down virtual ...	PY_Testing	2022-11-16 14:56:43	2022-11-16 14:56:59	admin (192.200.0...	View
Failed	Shut down virtual ...	PY_Testing	2022-11-16 14:56:05	2022-11-16 14:56:05	admin (192.200.0...	View
Completed	Create key	CM10TestKey01	2022-11-16 14:53:02	2022-11-16 14:53:02	admin (192.200.0...	View
Completed	Add KMS user	dasfhci	2022-11-16 14:51:57	2022-11-16 14:51:58	admin (192.200.0...	View
Completed	Add KMS server	CM_2_10	2022-11-16 14:51:51	2022-11-16 14:51:54	admin (192.200.0...	View
Completed	Upload file	dasfhci_certificate_...	2022-11-16 14:51:24	2022-11-16 14:51:24	admin (192.200.0...	View

All Tasks Close

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**

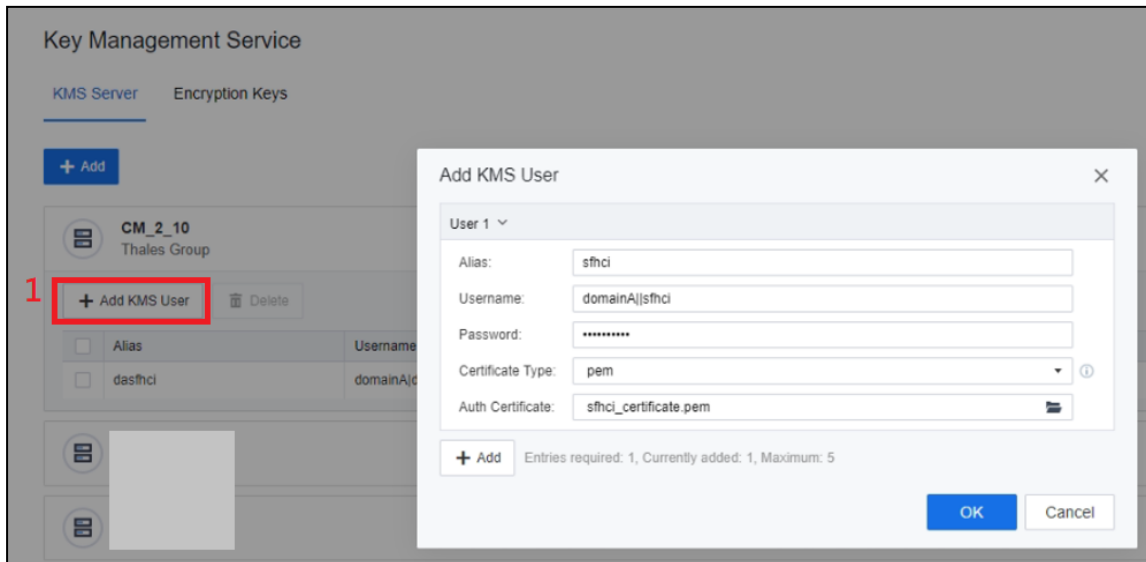
Username: **domainA|sfhci**

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

[+ Add KMS User](#)

<input type="checkbox"/>	Alias	Username	Connection Status	Cert. Expiration Time	Encryption Keys	Associated Tenants	Operation
<input type="checkbox"/>	desfhci	domainA\domainA\desfhci	● Normal	2024-11-14 15:18:41	1	0	<input type="button" value="Tenants"/> <input type="button" value="Edit"/> <input type="button" value="More"/>
<input type="checkbox"/>	sfhci	domainA\sfhci	● Normal	2024-11-14 15:12:51	0	0	<input type="button" value="Tenants"/> <input type="button" value="Edit"/> <input type="button" value="More"/>

1 User Time Created: 2022-08-17 15:56:01

1 User Time Created: 2022-03-16 15:13:18

Create an AES encryption key with sfhci user

Click “Encryption Keys”

Click “+Create Key”

Key Name: **CM10TestKey02** (Any name)

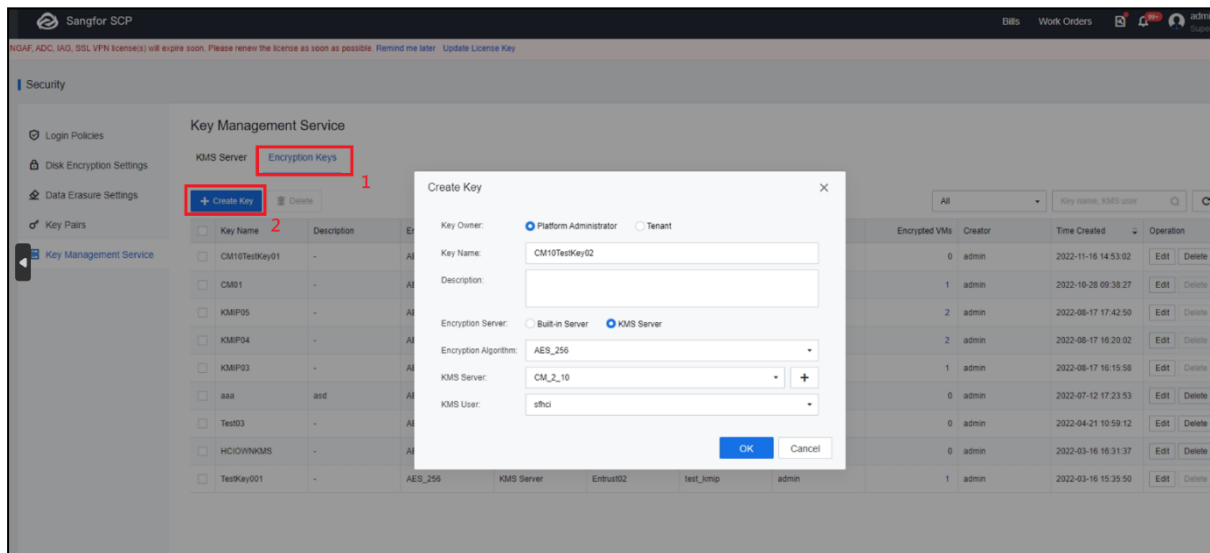
Encryption Server: KMS Server

Encryption Algorithm: AES_256

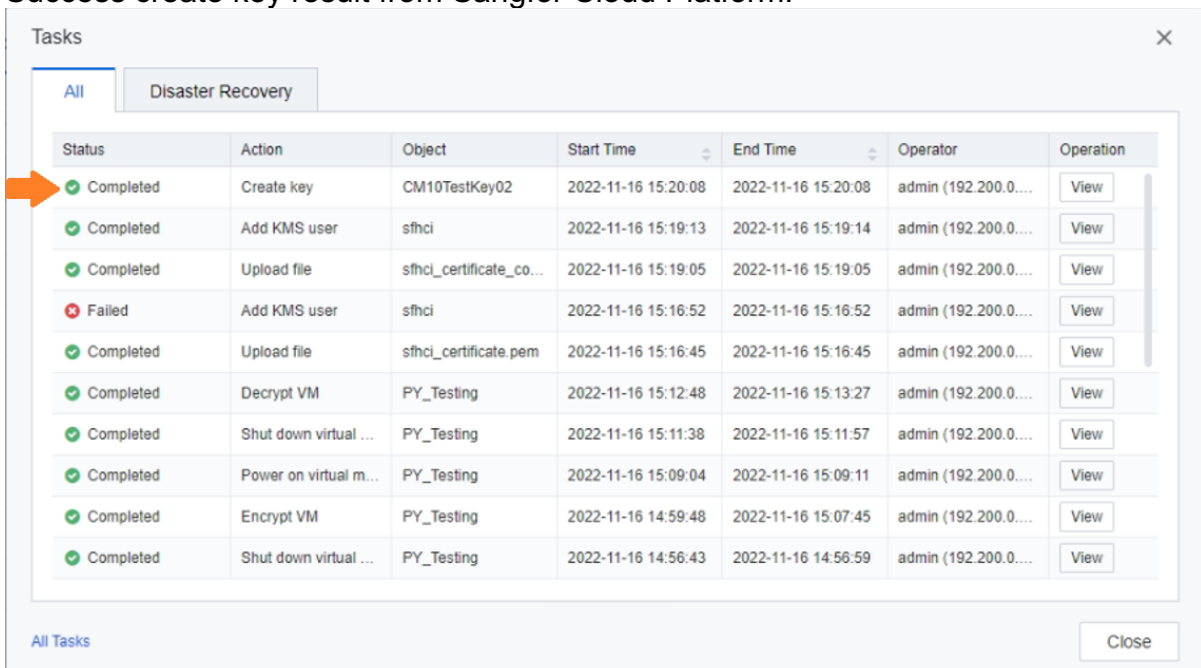
KMS Server: CM_2_10

KMS User: sfhci

Click “OK”



Success create key result from Sangfor Cloud Platform:



Security

Key Management Service

KMS Server Encryption Keys

+ Create Key Delete

All Key Name: KMS user

Key Name	Description	Encryption Algorithm	Encryption Server	KMS Server	KMS User	Key Owner	Encrypted VMs	Creator	Time Created	Operation
<input type="checkbox"/> CM10TestKey02		AES_256	KMS Server	CM_2_10	sfhci	admin	0	admin	2022-11-16 15:20:06	Edit Delete
<input type="checkbox"/> CM10TestKey01	-	AES_256	KMS Server	CM_2_10	dasfhd	admin	0	admin	2022-11-16 14:53:02	Edit Delete
<input type="checkbox"/> CM01	-	AES_256	KMS Server	CM_cluster	sfhci	admin	1	admin	2022-10-26 09:38:27	Edit Delete
<input type="checkbox"/> KMP05	-	AES_256	KMS Server	CM_cluster	sfhci	admin	2	admin	2022-08-17 17:42:50	Edit Delete
<input type="checkbox"/> KMP04	-	AES_256	KMS Server	CM_cluster	sfhci	admin	2	admin	2022-08-17 16:20:02	Edit Delete
<input type="checkbox"/> KMP03	-	AES_256	KMS Server	CM_cluster	sfhci	admin	1	admin	2022-08-17 16:15:58	Edit Delete
<input type="checkbox"/> aaa	asd	AES_256	Built-in Server	-	-	admin	0	admin	2022-07-12 17:23:53	Edit Delete

Success create key result from CipherTrust Manager

THALES CipherTrust Manager

Keys

Owner Name: sfhci

Filters: Basic Raw Label Filters

Type / Algorithm Size / Curve ID State / Revocation Event Dates

Latest Version Only

Owner Name: sfhci

+ Add Key

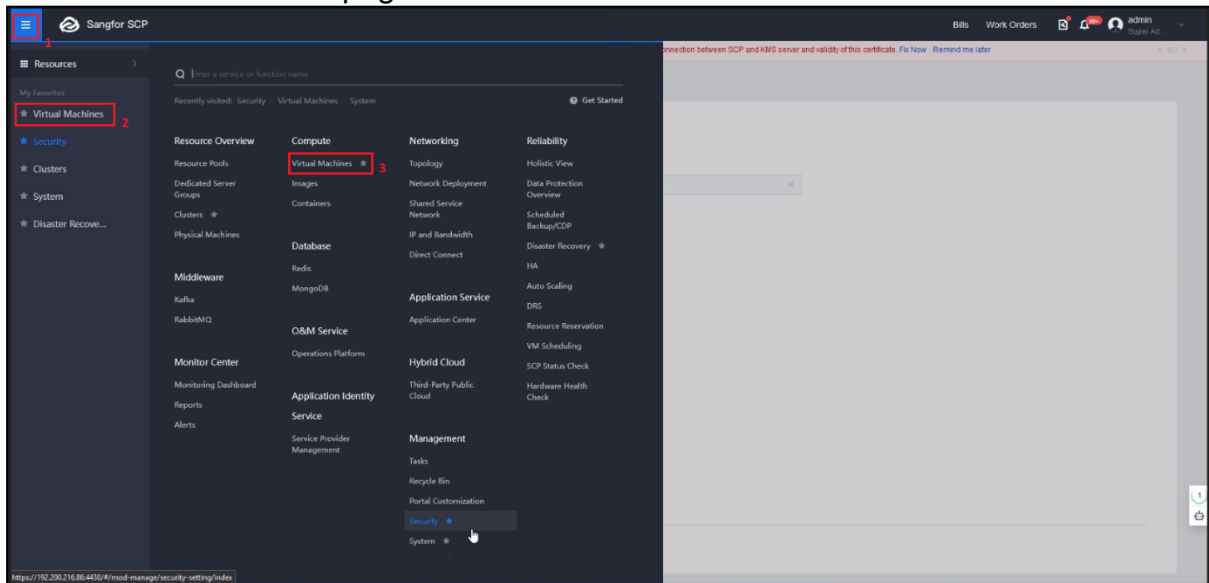
Key Name	Version	Owner	Modified	Type	Algorithm	Size
ks-ff888c9d9c0b45b1bce097b66f559fdeaf17286389b43fda6dacc52550097bb	0	local sfhci	17 Nov 2022, 10:34	Symmetric	AES	256

1 Key 50 per page

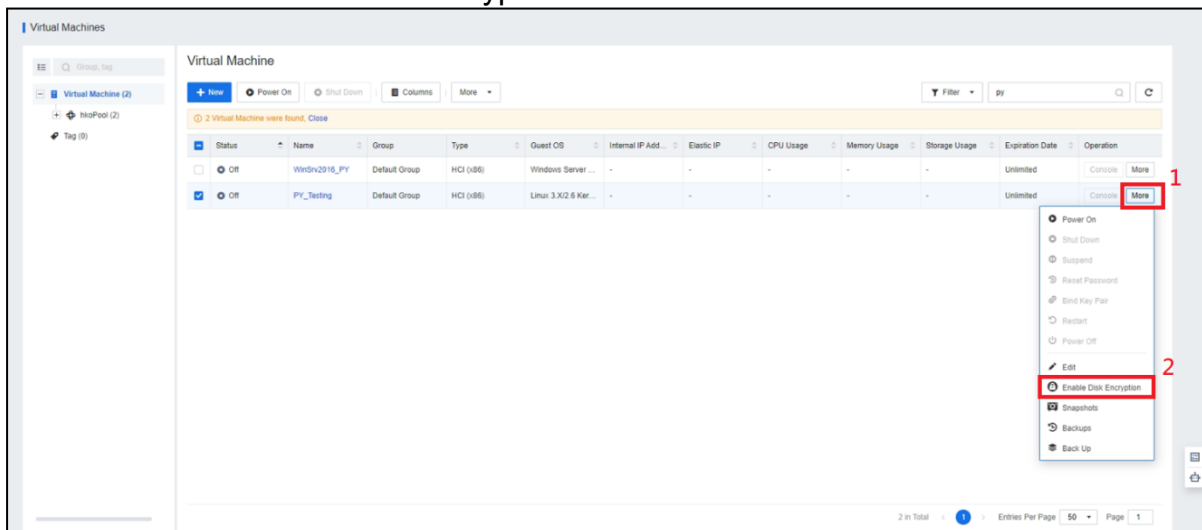
INFO	Nov 16th 2022 - 15:19:37	Create Key	<pre>{ "id": "ff888c9d9c0b45b1bce097b66f559fdeaf17286389b43fda6dacc52550097bb", "url": "kylo:kylo-e4bc128c-9d16-4bd0-83a2-8172245a1318:vault:keys:ks-ff888c9d9c0b45b1bce097b66f559fdeaf17286389b43fda6dacc52550097bb-v0", "name": "ks-ff888c9d9c0b45b1bce097b66f559fdeaf17286389b43fda6dacc52550097bb", "size": 256, "ownerId": "local 90fe7a13-d624-4d31-b4d2-0b5f14f03e69", "algorithm": "AES", "usageMask": 32, "objectType": "Symmetric Key" }</pre>	sfhci	SF_CM2_10	218.253.76.106
INFO	Nov 16th 2022 - 15:19:37	Kmp Authentication	<pre>{ "userId": "local 90fe7a13-d624-4d31-b4d2-0b5f14f03e69", "username": "sfhci" }</pre>		SF_CM2_10	218.253.76.106

Encrypt the virtual machine

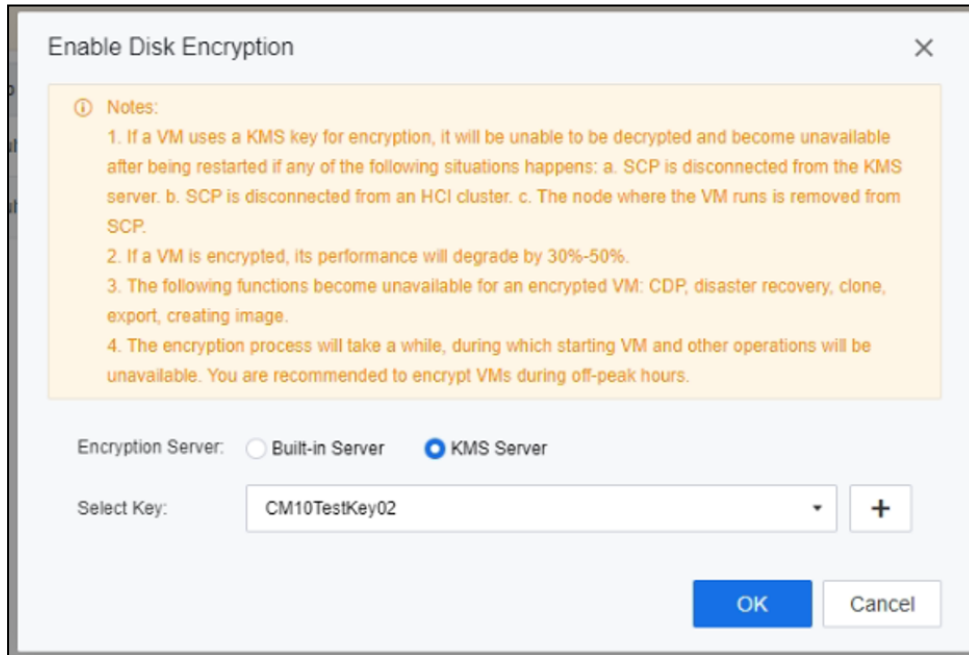
Go to “Virtual Machine” page



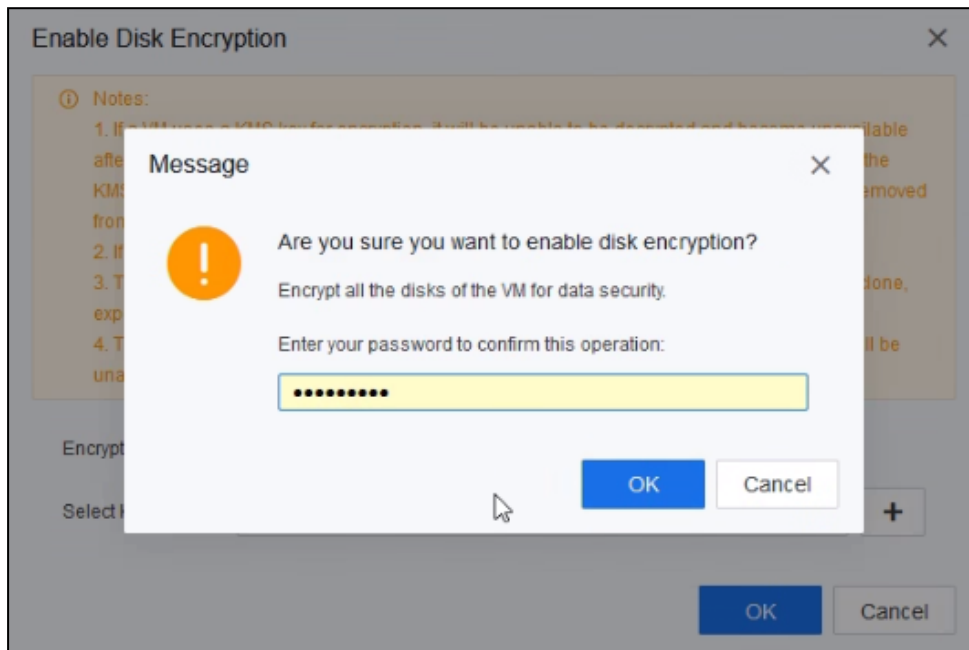
Ensure the virtual machine is in power off status
Click “More” → “Enable Disk Encryption”



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

Tasks

All Disaster Recovery

Status	Action	Object	Start Time	End Time	Operator	Operation
35%	Encrypt VM	PY_Testing	2022-11-16 15:22:17	-	admin (192.2...	View Cancel
Completed	Create key	CM10TestKey02	2022-11-16 15:20:08	2022-11-16 15:20:08	admin (192.2...	View
Completed	Add KMS user	sfhnci	2022-11-16 15:19:13	2022-11-16 15:19:14	admin (192.2...	View
Completed	Upload file	sfhnci_certificate_co...	2022-11-16 15:19:05	2022-11-16 15:19:05	admin (192.2...	View
Failed	Add KMS user	sfhnci	2022-11-16 15:16:52	2022-11-16 15:16:52	admin (192.2...	View
Completed	Upload file	sfhnci_certificate.pem	2022-11-16 15:16:45	2022-11-16 15:16:45	admin (192.2...	View
Completed	Decrypt VM	PY_Testing	2022-11-16 15:12:48	2022-11-16 15:13:27	admin (192.2...	View
Completed	Shut down vir...	PY_Testing	2022-11-16 15:11:38	2022-11-16 15:11:57	admin (192.2...	View
Completed	Power on virt...	PY_Testing	2022-11-16 15:09:04	2022-11-16 15:09:11	admin (192.2...	View
Completed	Encrypt VM	PY_Testing	2022-11-16 14:59:48	2022-11-16 15:07:45	admin (192.2...	View

All Tasks Close

Success use key status from CipherTrust Manager:

INFO Nov 16th 2022 - 15:21:59 Use Key { "Identifier": "ff888c9d9c0b45b1cce097b66f559fdeaf17268389b43fda6dacc525508977b" } sfhnci SF_CM2_10 218.253.76.106 ...

INFO Nov 16th 2022 - 15:21:59 Kmp Authentication { "userId": "local|90fe7a13-d624-4d31-b4d2-0b5f14f03e69", "username": "sfhnci" } SF_CM2_10 218.253.76.106 ...

Virtual machine successful encrypted result from Sangfor Cloud Platform

Tasks

All Disaster Recovery

Status	Action	Object	Start Time	End Time	Operator	Operation
Completed	Encrypt VM	PY_Testing	2022-11-16 15:22:17	2022-11-16 15:23:01	admin (192.200.0...	View
Completed	Create key	CM10TestKey02	2022-11-16 15:20:08	2022-11-16 15:20:08	admin (192.200.0...	View
Completed	Add KMS user	sfhnci	2022-11-16 15:19:13	2022-11-16 15:19:14	admin (192.200.0...	View
Completed	Upload file	sfhnci_certificate_co...	2022-11-16 15:19:05	2022-11-16 15:19:05	admin (192.200.0...	View
Failed	Add KMS user	sfhnci	2022-11-16 15:16:52	2022-11-16 15:16:52	admin (192.200.0...	View
Completed	Upload file	sfhnci_certificate.pem	2022-11-16 15:16:45	2022-11-16 15:16:45	admin (192.200.0...	View
Completed	Decrypt VM	PY_Testing	2022-11-16 15:12:48	2022-11-16 15:13:27	admin (192.200.0...	View
Completed	Shut down virtual ...	PY_Testing	2022-11-16 15:11:38	2022-11-16 15:11:57	admin (192.200.0...	View
Completed	Power on virtual m...	PY_Testing	2022-11-16 15:09:04	2022-11-16 15:09:11	admin (192.200.0...	View
Completed	Encrypt VM	PY_Testing	2022-11-16 14:59:48	2022-11-16 15:07:45	admin (192.200.0...	View

All Tasks Close

Power On the encrypted virtual machine - sfhci – CM10TestKey02

Virtual Machine

+ New Power On Shut Down Columns More

Filter Filter by

2 Virtual Machines were found. Close

Status	Name	Group	Type	Guest OS	Internal IP Ad...	Elastic IP	CPU Usage	Memory Usage	Storage Us...	Expiration Date	Operation
Off	WinSrv2016_PY	Default Group	HCI (x86)	Windows Server ...	-	-	-	-	-	Unlimited	Console More
Off	PY_Testing Encrypted	Default Group	HCI (x86)	Linux 3.X2.6 Ker...	-	-	-	-	-	Unlimited	Console More

Power On Shut Down Suspend Reset Password Bind Key Pair Restart Power Off Edit Decrypt Disk Snapshots Backups Back Up

Successful power on result from Sangfor Cloud Platform:

Tasks

All Disaster Recovery

Status	Action	Object	Start Time	End Time	Operator	Operation
Completed	Power on virt...	PY_Testing	2022-11-16 15:25:42	2022-11-16 15:25:48	admin (192.2...	View
Completed	Encrypt VM	PY_Testing	2022-11-16 15:22:17	2022-11-16 15:23:01	admin (192.2...	View
Completed	Create key	CM10TestKey02	2022-11-16 15:20:08	2022-11-16 15:20:08	admin (192.2...	View
Completed	Add KMS user	sfhci	2022-11-16 15:19:13	2022-11-16 15:19:14	admin (192.2...	View
Completed	Upload file	sfhci_certificate_co...	2022-11-16 15:19:05	2022-11-16 15:19:05	admin (192.2...	View
Failed	Add KMS user	sfhci	2022-11-16 15:16:52	2022-11-16 15:16:52	admin (192.2...	View
Completed	Upload file	sfhci_certificate.pem	2022-11-16 15:16:45	2022-11-16 15:16:45	admin (192.2...	View
Completed	Decrypt VM	PY_Testing	2022-11-16 15:12:48	2022-11-16 15:13:27	admin (192.2...	View

All Tasks Close

Successful power on result from CipherTrust Manager:

INFO	Nov 16th 2022 - 15:25:15	Use Key	{ "Identifier": "fff888c9d9c0b45b1bce97b66f559fdea7d17286389b43fda6dacc525508097bb" }	sfhci	SF_CM2_10	218.253.76.106	...
INFO	Nov 16th 2022 - 15:25:15	Kmp Authentication	{ "userId": "local190fe7a13-d624-4d31-b442-0b5f14f03e69", "username": "sfhci1" }		SF_CM2_10	218.253.76.106	...

Decrypted virtual machine - sfhci – CM10TestKey02

Ensure the virtual machine is in power off status

Decrypt the virtual machine

Status	Name	Group	Type	Guest OS	Internal IP Ad.	Elastic IP	CPU Usage	Memory Usage	Storage Us...	Expiration Date	Operation
<input type="checkbox"/>	WinSvc2016_PY	Default Group	HCI (x86)	Windows Server ...	-	-	-	-	-	Unlimited	Console 1 More
<input checked="" type="checkbox"/>	PY_Testing Encrypted	Default Group	HCI (x86)	Linux 3.X/2.6 Ker...	-	-	-	-	-	Unlimited	Console 2 More

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

Click "OK"

Message

Are you sure you want to decrypt disk?

After disk is decrypted, business will be interrupted and the encrypted VMs can no longer be powered on. This operation is irreversible. Please operate with caution.

Enter your password to confirm this operation:

OK Cancel

Go to "Tasks list" to see the decryption progress

The screenshot shows a 'Tasks' window with a 'Disaster Recovery' tab. A table lists various tasks. The first task, 'Decrypt VM' for 'PY_Testing', is currently in progress with a 35% completion bar. Other tasks include 'Shut down virtual machine', 'Power on virtual machine', 'Encrypt VM', 'Create key', 'Add KMS user', and 'Upload file', all of which are marked as 'Completed'.

Status	Action	Object	Start Time	End Time	Operator	Operation
35%	Decrypt VM	PY_Testing	2022-11-16 15:29:21	-	admin (192.200.0.10)	View Cancel
Completed	Shut down virtual machine	PY_Testing	2022-11-16 15:28:00	2022-11-16 15:28:18	admin (192.200.0.10)	View
Completed	Power on virtual machine	PY_Testing	2022-11-16 15:25:42	2022-11-16 15:25:48	admin (192.200.0.10)	View
Completed	Encrypt VM	PY_Testing	2022-11-16 15:22:17	2022-11-16 15:23:01	admin (192.200.0.10)	View
Completed	Create key	CM10TestKey02	2022-11-16 15:20:08	2022-11-16 15:20:08	admin (192.200.0.10)	View
Completed	Add KMS user	sfhci	2022-11-16 15:19:13	2022-11-16 15:19:14	admin (192.200.0.10)	View
Completed	Upload file	sfhci_certificate_co...	2022-11-16 15:19:05	2022-11-16 15:19:05	admin (192.200.0.10)	View
Failed	Add KMS user	sfhci	2022-11-16 15:16:52	2022-11-16 15:16:52	admin (192.200.0.10)	View
Completed	Upload file	sfhci_certificate.pem	2022-11-16 15:16:45	2022-11-16 15:16:45	admin (192.200.0.10)	View
Completed	Decrypt VM	PY_Testing	2022-11-16 15:12:48	2022-11-16 15:13:27	admin (192.200.0.10)	View

Success use key status from CipherTrust Manager:

The screenshot shows a log viewer with two entries. The first entry is an 'INFO' message from 'Nov 16th 2022 - 15:28:58' regarding 'Use Key' with a long identifier string. The second entry is an 'INFO' message from the same date and time regarding 'Kmp Authentication' with user ID and username details.

```

{
  "Identifier": "ff888cd9c0b45b1bce097b66f559fdeaf17286389b43fda6decc52550097bb"
}

{
  "userId": "local|90fe7a13-d624-4d31-b4d2-0b5f14f8a699",
  "username": "sfhci"
}
  
```

Virtual machine successful decrypt result from Sangfor Cloud Platform

This screenshot is similar to the first one, but the 'Decrypt VM' task for 'PY_Testing' is now marked as 'Completed' with a green checkmark. An orange arrow points to this row in the table.

Status	Action	Object	Start Time	End Time	Operator	Operation
Completed	Decrypt VM	PY_Testing	2022-11-16 15:29:21	2022-11-16 15:30:01	admin (192.200.0.10)	View
Completed	Shut down virtual machine	PY_Testing	2022-11-16 15:28:00	2022-11-16 15:28:18	admin (192.200.0.10)	View
Completed	Power on virtual machine	PY_Testing	2022-11-16 15:25:42	2022-11-16 15:25:48	admin (192.200.0.10)	View
Completed	Encrypt VM	PY_Testing	2022-11-16 15:22:17	2022-11-16 15:23:01	admin (192.200.0.10)	View
Completed	Create key	CM10TestKey02	2022-11-16 15:20:08	2022-11-16 15:20:08	admin (192.200.0.10)	View
Completed	Add KMS user	sfhci	2022-11-16 15:19:13	2022-11-16 15:19:14	admin (192.200.0.10)	View
Completed	Upload file	sfhci_certificate_co...	2022-11-16 15:19:05	2022-11-16 15:19:05	admin (192.200.0.10)	View
Failed	Add KMS user	sfhci	2022-11-16 15:16:52	2022-11-16 15:16:52	admin (192.200.0.10)	View
Completed	Upload file	sfhci_certificate.pem	2022-11-16 15:16:45	2022-11-16 15:16:45	admin (192.200.0.10)	View
Completed	Decrypt VM	PY_Testing	2022-11-16 15:12:48	2022-11-16 15:13:27	admin (192.200.0.10)	View

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