NCENCRYPT™

CONFIGURATION GUIDE

NC Encrypt

Version 8.5

Document Date 22/03/2023

archTIS

Copyright Information

Technical support

For licensing or technical support information, please submit your requests via the archTIS Help Center at https://www.archtis.com/support/. For more information, visit www.archtis.com.

Table of Contents

1. Introduction

NC Encrypt is an optional add-on encryption and key management solution for NC Protect. This document covers the requirements and configuration steps to implement NC Encrypt and the Thales CipherTrust Manager Connector for the NC Protect for M365 and SharePoint On-Premises versions. A separate guide is available to cover the NC Protect installation.

NC Encrypt provides encryption capabilities out-of-the-box for organizations using NC Protect that prefer to manage their own encryption keys or do not have Azure RMS. NC Encrypt provides additional encryption and decryption capabilities using a company's own master key. Alternatively, a default AES-256 based encryption key can be dynamically created to get you started. From the moment that you install NC Encrypt, your documents are secured immediately by the system generated encryption key. At any time in the future, you can switch to Bring Your Own Key (BYOK) via the NC Protect administration portal.

The NC Encrypt Thales CipherTrust Manager Connector extends the capabilities of NC Encrypt to use Key Management Tools and Hardware Secure Modules (HSMs). CipherTrust Manager is available as both virtual and physical appliances that integrate with HSMs to securely store keys at the highest level of trust. For more information on CipherTrust Manager, refer to their respective guides.

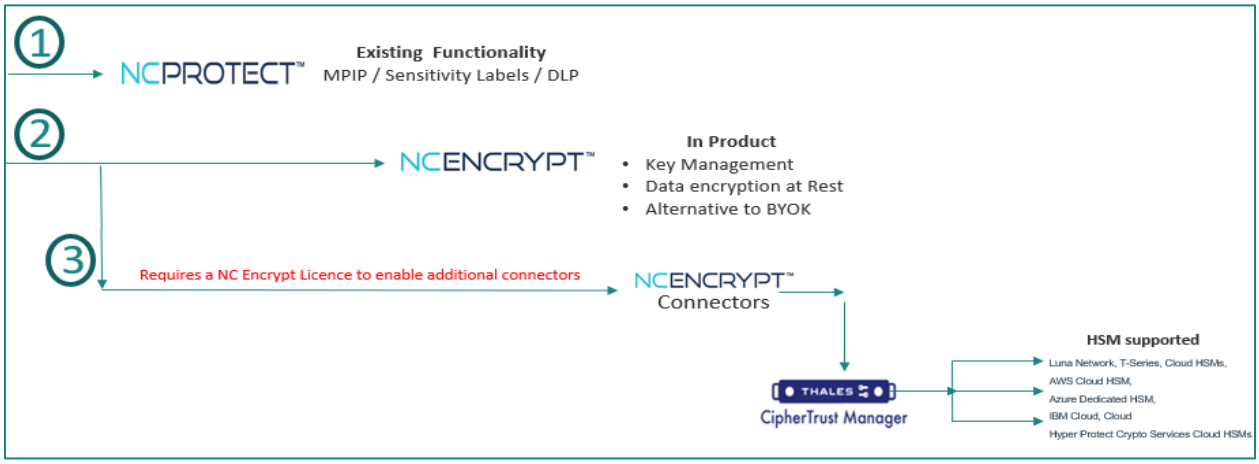


Figure 1.1: NC Protection Encryption solution

- NCPROTECT™
  - Existing protection based on MPIP, Sensitivity labels, DLP and the configured NC Protect rules
- NCENCRYPT™
  - Optional licensed module.
  - Enables in-product encryption and key management for those that need an additional level of control of their encryption keys and documents at rest
- NCENCRYPT™ Connectors
  - Provides connectivity to VSMs and HSMs via Thales CipherTrust Manager
  - Enabled with an NC Encrypt license

2. Requirements

NC Encrypt is an optional module for NC Protect. To enable NC Encrypt and the NC Encrypt connector - Thales CipherTrust Manager , the following licenses are required:

- NC Protect
- NC Encrypt
    - NC Encrypt Thales CipherTrust Manager Connector.

3. Licensing NC Encrypt

NC Protect is installed with a 30-day temporary key. This includes NC Encrypt, but not the CipherTrust Manager Connector. If the optional CipherTrust Manager Connector is required, you will need to request a license from archTIS support.

Before the 30-day temporary key expires, you will need to install the NC Protect that includes the NC Encrypt module license. Contact your archTIS account manager for more details.

On receipt of the new NC Protect license with the NC Encrypt module and connector, upload the license file from NC Protect's Administration portal (Licensing menu).

Once uploaded, the NC Encrypt module will continue to be available in the NC Protect administration portal.

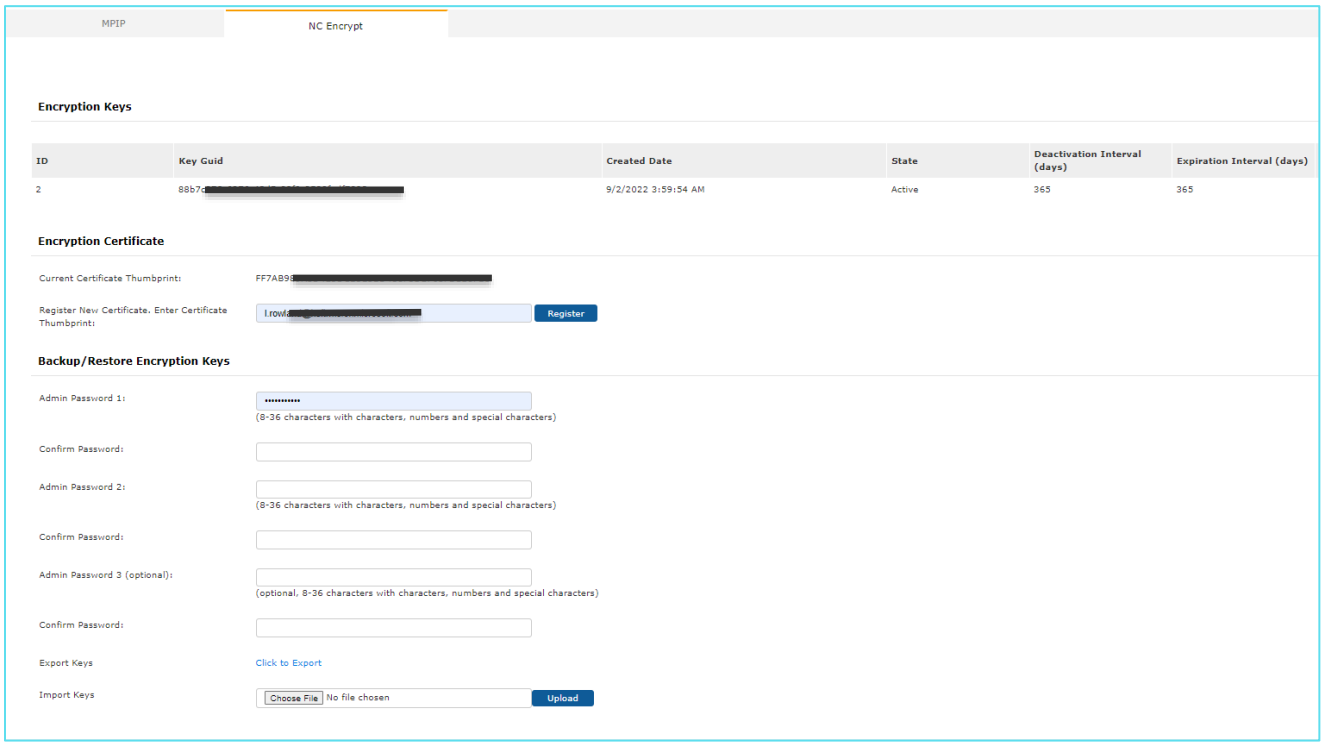


Figure 3.1: NC Encrypt tab as shown in NC Protect for M365

4. Configure NC Encrypt

NC Protect for M365: When installed, NC Protect generates its own Private Key SSL certificate (expires in 12 months) with the installer prompting for a password to be assigned to it. These are stored in the TLS/SSL settings of NC Protect's application service. As this certificate is generated by NC Protect, for security and best practices of BYOK (Bring Your Own Key), the customer should purchase their own certificate and replace NC Protect's SSL certificate.

For NC Protect for SharePoint On-Premises and File Shares: You will need to supply your own certificate.

4.1 Backup, Change/Install your own SSL cert

4.1.1 Microsoft 365

The initial NC Protect installer generated a Private Key SSL certificate with a password set during the install and placed them in the TLS/SSL settings of the NC Protect's application service. This certificate will allow NC Encrypt to be fully utilised with Sharing Rules.

However, for security and best practices, it is recommended that you replace this with your company's certificate.

To replace this certificate:

1. First, ensure that you back up your current Keys especially if you have been encrypting documents. Backing up and restoring the current key(s) allows existing encrypted documents to be supported.
    i. Navigate to **NC Protect Settings > General > Encryption > NC Encrypt** tab
    ii. Fill in the required details (3 x administration passwords) and click **Export** to get the encryption keys.
2. From Microsoft Azure Portal, navigate to NC Protect's application service TLS/SSL settings and delete the current SSL certificate
3. Purchase/create and upload your own private key certificate (*.pfx) into NC Protect's application service TLS/SSL and protect it with a valid password.

Once the new certificate is uploaded:

1. From NC Protect's application service private key certificate (TLS/SSL settings), copy the Thumbprint value
2. Go to NC Protect's application service > Configuration, locate, edit the application setting "ENCRYPTION_CERTIFICATE" and paste the copied Thumbprint value into the Value field.
3. Click OK and Save the Configuration changes.
   Note: Restart NC Protect application service to register the new certificate
4. From the NC Protect portal, go to Encryption > Encrypt tab and import the keys you backed up above:
    i. Choose the file (NCProtectExportEncryptionKeys.txt) and click upload,
5. Once completed, use your Sharing or Secure Document Reader Rules to verify that you can decrypt/open previously encrypted documents.

Note: If NC Protect's application service Private Key SSL certificate is lost/deleted or changed, the exported encryption key will need to be reimported again after new cert is installed so that users can decrypt existing encrypted documents.

4.1.2 SharePoint On-Premises

1. Ensure you backup your current keys
    i. Navigate to Central Administration > General Application Settings > NC Protect > Configuration
    ii. Under NC Encryption, fill in the required details (3 x administration passwords) and click **Export** to get the Encryption keys
2. Create or use a Secure Store Service application
    i. Central Administration > Application Management> Manage Service Applications > New > Secure Store Service
    ii. Refer to the following site for more information on adding a Secure Store service: https://learn.microsoft.com/en-us/SharePoint/administration/configure-the-secure-store-service
3. Create a Target Application to the store certificate and certificate password
    i. Select the Secure Store Service created/selected, and click Manage (Generate New Key if required)
    ii. Click on New to create "New Secure Store Target Application"
    iii. For NC Encrypt to store the SSL certificate, name the Target Application ID as "**NCEncrypt**", enter Display Name and contact email then click Next
    iv. For CipherTrust Manager to store the SSL certificate, name the Target Application ID as "**Thales**", enter Display Name and contact email then click Next
    v. Create/add the 2 field types: **Certificate** and **Certificate Password**

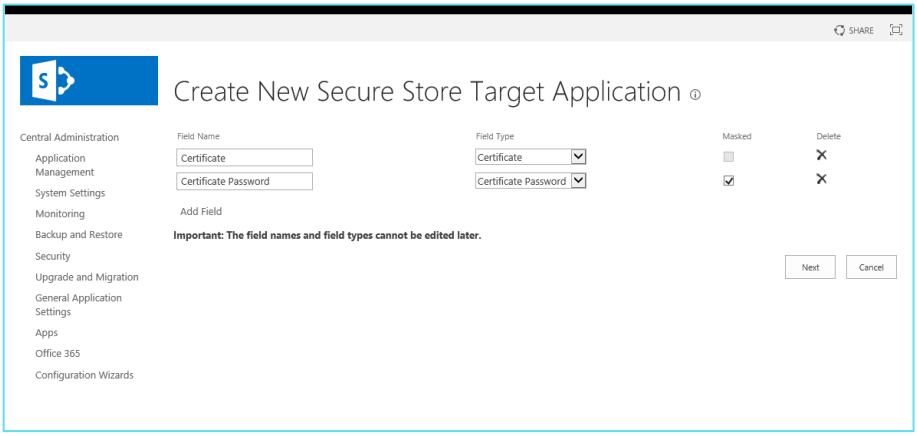


Figure 4.1: SharePoint On-Prem Secure Store Target Application

    vi. Ensure that the service accounts used by the SharePoint timer job or SharePoint web application, are set to have access to the Secure Store Service Application.

vii. Set the credentials to upload the new certificate into the Secure Store Target Application. [Take note of the password obtained during generation of the password via OpenSSL command when creating the certificate manually].

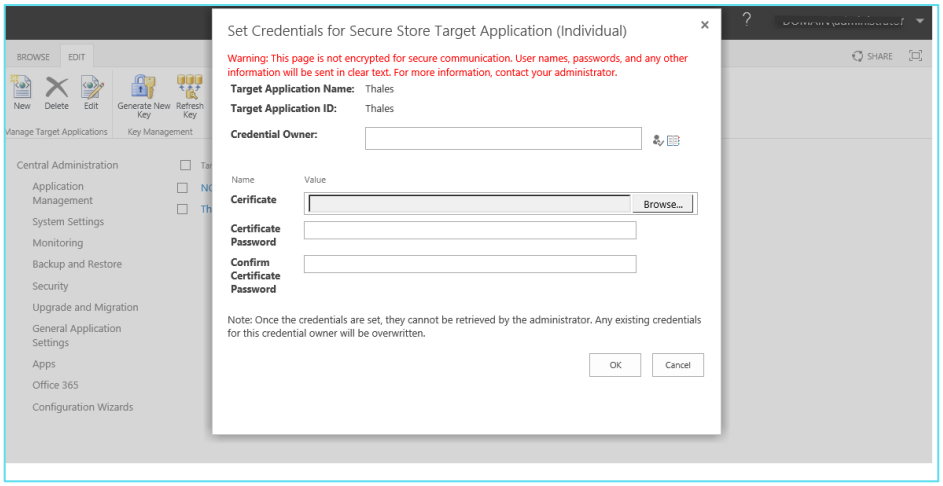


Figure 4.2: SharePoint On-Prem – Credentials for Secure Store Target Application

vii. Make sure that the Credential Owner is set to the Service Accounts behind the SharePoint timer job and SharePoint web application.

viii. Perform IIS Reset

4. Start using NC Encrypt as the encryption type in Sharing Rules

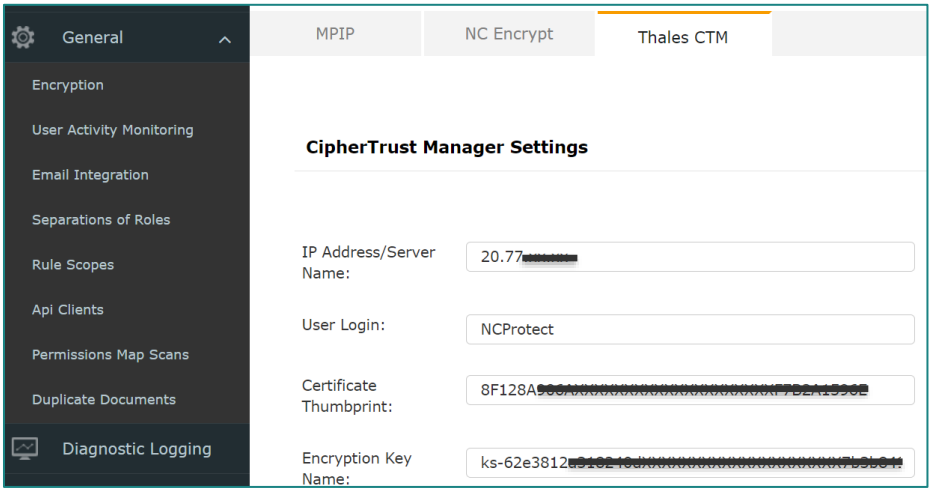
5. NC Encrypt Connectors: Thales CipherTrust Manager

Connecting NC Encrypt to Thales CipherTrust Manager leverages an industry standard Key Management tool with connectivity to Hardware Secure Modules (HSMs).

The NC Encrypt CipherTrust Manager connection require the following values:

- IP Address/ Server Name: Address your CipherTrust Manager instance
- User Login: Name of User defined in CipherTrust Manager that NC Encrypt will use to connect**
- Certificate Thumbprint: User Certificate**
- Encryption Key Name: CipherTrust Manager managed key that will be used by NC Encrypt

**Access to CipherTrust Manager can be based on User + Password or User + Certificate-based authentication. NC Encrypt connection to CipherTrust Manager is through the User + Certificate-based authentication.



The above information is obtained using the following key procedures:

1. Prepare CipherTrust Manager to be accessed and used by NC Encrypt
2. Obtain a PFX digital certificate that can be uploaded into the NC Protect environment. This certificate can be purchased from a few vendors, or from a self-signed certificate generated from CipherTrust Manager. The setup up below covers the self-signed certificate from CipherTrust Manager.
3. Enable NC Encrypt Connector for Thales CipherTrust Manager in NC Protect.

5.1 Prepare CipherTrust Manager

This section covers the steps to be performed in CipherTrust Manager to generate the information required for the NC Encrypt Thales CipherTrust Manager Connector.

For all other information such as setting up HSM's with CipherTrust Manager, please refer to the appropriate CipherTrust Manager Administration guides.

To prepare CipherTrust manager, follow the steps outlined below. These are based on the steps outlined in the CipherTrust Manager administration guide for Certificate Based Authentication (required for NC Encrypt). Note that the steps may vary depending on the version of CipherTrust Manager you have installed.
The instruction below are from CipherTrust Manager v**2.8**:
https://thalesdocs.com/ctp/cm/**2.8**/admin/cm_admin/certificate-based-auth/index.html

5.1.1: Enable the "Certificate based Login" Option for a User

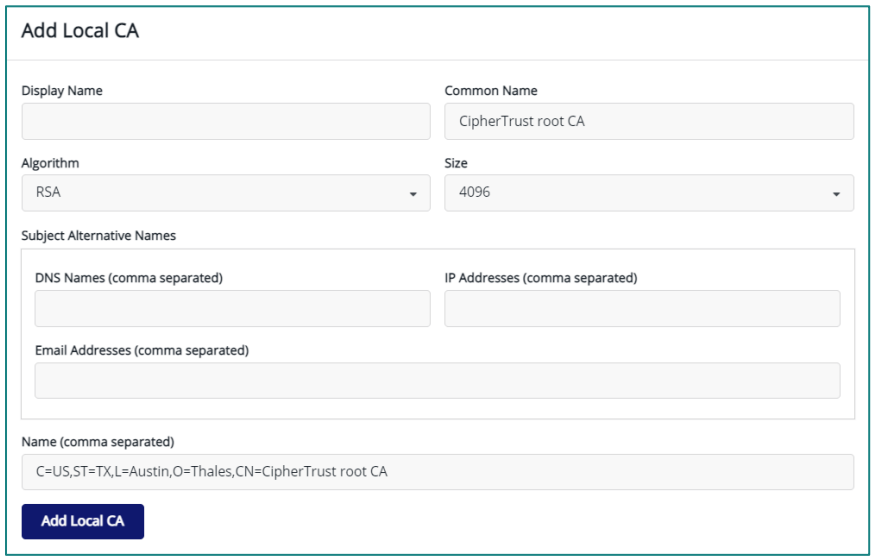
1. Log on to CipherTrust Manager as an administrator. Navigate to **Access management > Users**.
2. Enable the "**Certificate based Login**" option for the user:
    - **For existing users (eg "NCProtect"):**
        a. Click the action button for that user, then click **Manage**.
        b. Click **CONFIGURE CERTIFICATE LOGIN**. Select **Allow user to login using certificate**.
        c. Specify **Certificate Subject Distinguished Name** for the user.
        d. Click **Update Certificate Login**.
    - **For new users:**
        a. Click **Create New User**. Specify **Username** (eg "NCProtect" for the user.
        b. Select **Allow user to login using certificate**.
        c. Specify **Certificate Subject Distinguished Name** for the user.
        d. Click **Create**.
3. Ensure that that User is member of the Admin group.

5.1.2: Create and Download the Web Certificate

USING LOCAL CERTIFICATE AUTHORITY (CA)

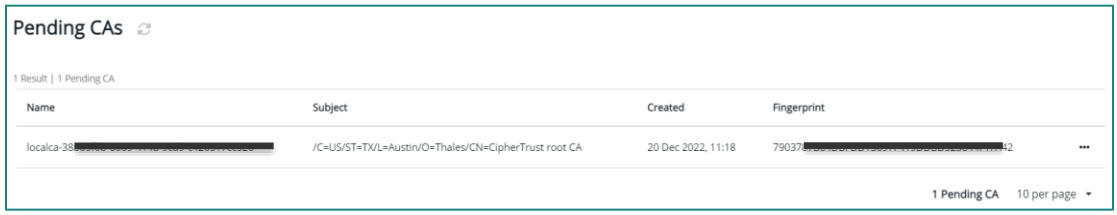
1. If your CipherTrust Manager is already configured with a CA, go to step 4 to issue a certificate, else continue below.
2. Go to **CA** > **Local**.
3. Click **Add Local CA**.
    a. Enter the Common Name for this certificate.
    b. Select desired algorithm (RSA or ECDSA).

c. In the Name (comma separated) field, specify the same details that were specified in the Certificate Subject Distinguished Name field while creating the user eg "C=US,ST=TX,L=Austin,O=Thales,CN=CipherTrust root CA"

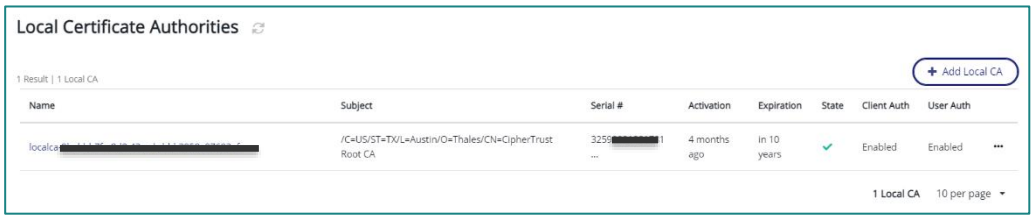


d. Click **Add Local CA**

e. Under Pending CA's, clicking on the shortcut menu (ellipses) against the Local CA you just created and (for this set up) select Self-sign. When prompted, select the Duration (days) (eg 365) and Save



f. Under Name, click the link of the newly generated local CA.



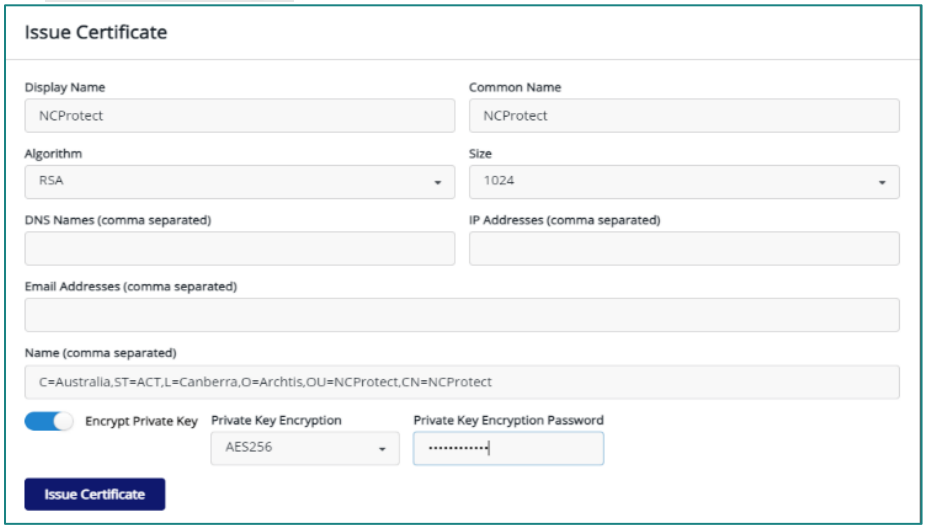
4. Click **Issue Certificate**.

    a. Enter the **Common Name** for this certificate.

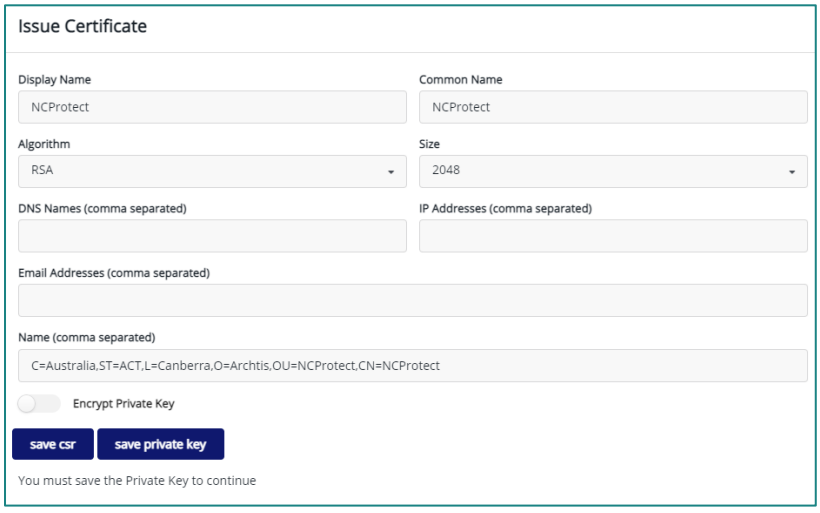
    This common name should be the same common name that you specified while creating the user.

    b. Select the desired algorithm (RSA or ECDSA).

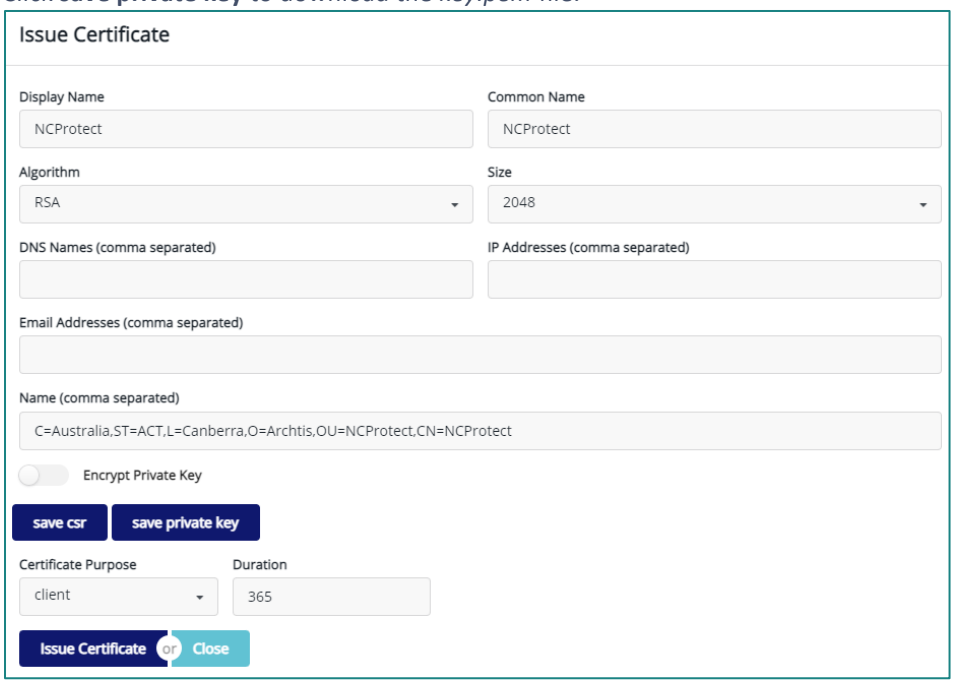
    c. In the **Name** field, specify the same details that you specified in the certificate_subject_dn property of the user.



    d. Click **Issue Certificate**.



e. Click **save private key** to download the *key.pem* file.



f. Click **Issue Certificate**. The newly created certificate is displayed in the certificates list.

5. Download the certificate issued by the local CA and save it at the same location where the private key is saved.

5.1.3: Create and Install pkcs12 Formatted Certificate using OpenSSL

1. Install OpenSSL on your machine.
2. Use the following command to convert the key and certificate into a pkcs12 formatted *.pfx file:

```
openssl pkcs12 -export -out example.pfx -inkey key.pem -in certificate.pem
```

***Where*:**

- **key.pem** is the private key
- **certificate.pem** is the certificate file
- **example.pfx** is the pkcs12 formatted web certificate that will need to be uploaded into the App Services TLS/SSL list or installed in the web browser

3. When prompted, enter a Password (and verify) for the PFX certificate

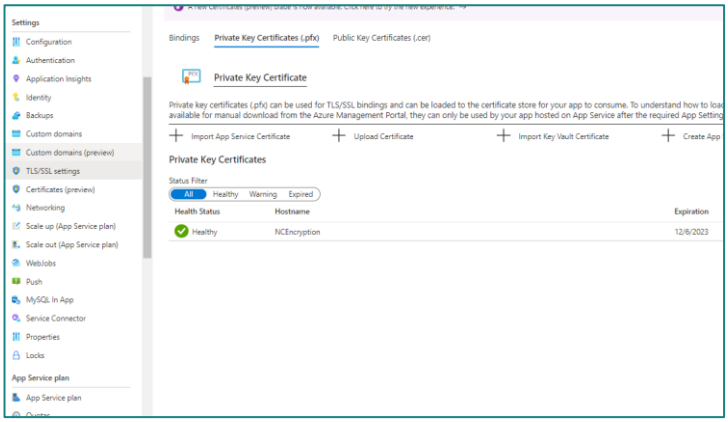
This creates a .pfx certificate (*example.pfx* in the above command) at the same location.

5.2 Configure and enable NC Encrypt CipherTrust Manager Connector

Section 5.1 covered the process of creating and uploading the certificate into your environment. Once done, follow the steps below to connect NC Encrypt to CipherTrust Manager.

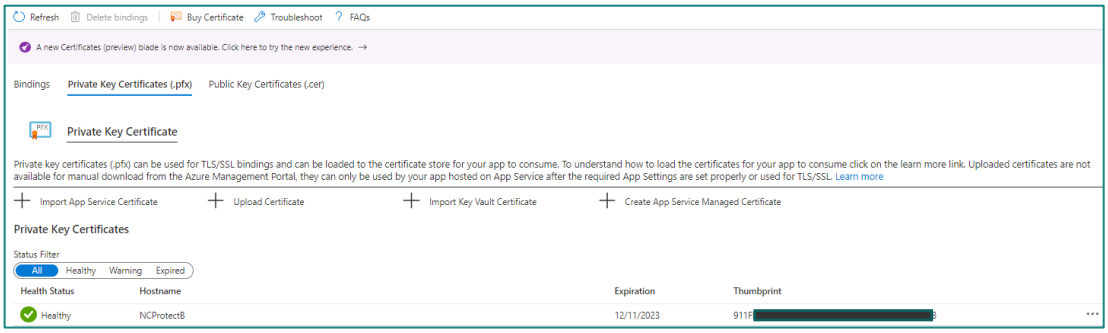
5.2.1 Microsoft 365

1. If you're already encrypting documents with NC Encrypt, back up your current NC Protect keys (see **Section 4.1** above)
2. Go to the Azure Portal > NC Protect's application service -> TLS/SSL Settings -> Private Key Certificates and upload your PFX digital certificate (see section 5.1 above).



Note: Restart NC Protect application service to register the new certificate

3. Import and install the *.pfx* certificate. You can now use the web certificate for logging on to CipherTrust Manager



4. Navigate to NC Protect Admin -> Encryption -> Thales tab

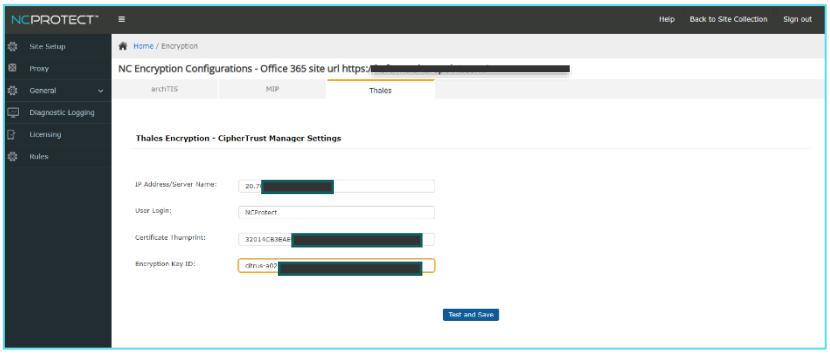


Figure 5.3: NC Protect admin portal - Thales tab

i. Enter the IP address of the CipherTrust Manager instance you're connecting NC Protect to

ii. Enter the User Login of the new user created in the above Thales CipherTrust Manager section above

iii. Enter the certificate Thumbprint - copied from NC Protect's application service TLS/SSL settings (Azure Portal > NC Protect app service > TLS/SSL Settings > private key certificates and click on the previously uploaded PFX certificate).

iv. Enter the Encryption Key ID from the CipherTrust Manager (navigate to Keys). There should be one key there by default

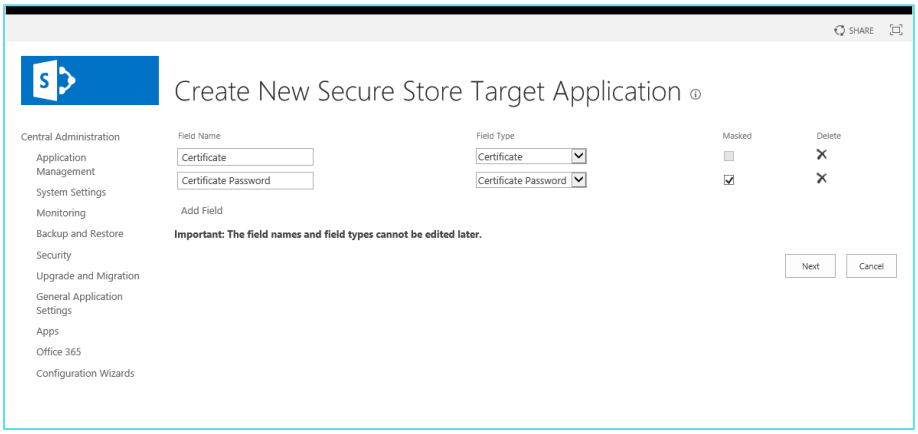
v. Click Test and Save

5. Once enabled, and configured, the encryption type of 'Thales' will now be available in the Sharing Rule.

5.2.2 SharePoint On-Premises

1. If you're already encrypting documents with NC Encrypt. back up your current NC Protect keys (see **Section 4.1** above)
2. Create or use a Secure Store Service application
   i. Central Administration > Application Management> Manage Service Applications > New > Secure Store Service
   ii. Refer to the following site for more information on adding a Secure Store service: https://learn.microsoft.com/en-us/SharePoint/administration/configure-the-secure-store-service
3. Create a Target Application to the store certificate and certificate password
   i. Select the Secure Store Service created/selected, and click Manage (Generate New Key if required)
   ii. Click on New to create "New Secure Store Target Application"
   iii. The target application ID must be named "**Thales**". Enter Display Name and contact email then click Next
   iv. Create/add the 2 field types: **Certificate** and **Certificate Password** and click Next
   Figure 5.4: SharePoint On-Prem -New Secure Store Target Application

   v. Ensure that the service accounts used by the SharePoint timer job or SharePoint web application,

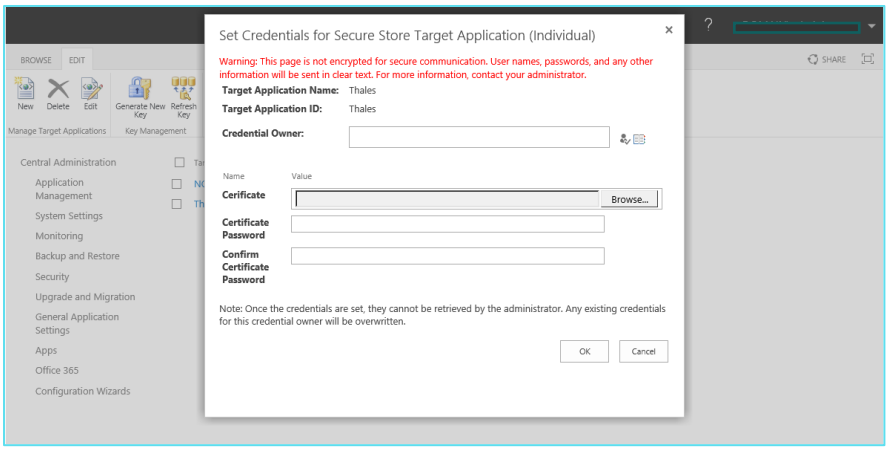


   are set to have access to the Secure Store Service Application.

   vi. On the "Set Credentials for Secure Store Target Application" window, upload the PFX certificate that you purchased/created (see section **5.1** above) and set the password

vii. Make sure that the Credential Owner is set to the Service Accounts behind the SharePoint timer job and SharePoint web application

Figure 5.5: SharePoint On-Prem -New Secure Store Target Application



6. Navigate to NC Protect Admin -> Encryption -> Thales CTM tab

vi. Enter the IP address of the CipherTrust Manager instance you're connecting NC Protect to

vii. Enter the User Login of the new user created in the above CipherTrust Manager section above

viii. **NOTE**: The Thumbprint will not be used/required. For On-premises, NC Protect will search for an use the Secure Store Target Application ID of "Thales" as defined above.

ix. Enter the Encryption Key ID from CipherTrust Manager (navigate to Keys). There should be one key there by default

x. Click Test and Save

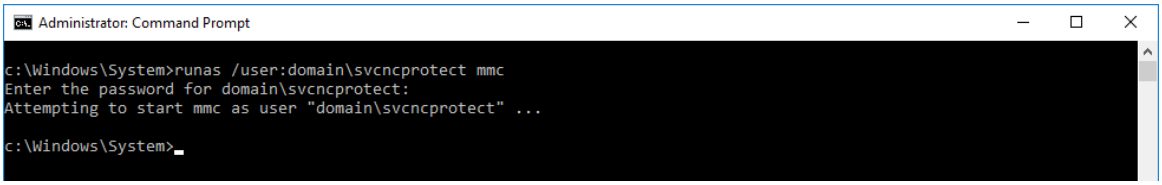
7. Once enabled, and configured, the encryption type of 'Thales' will now be available in the Sharing Rule.

5.2.3 NC Protect for File Shares

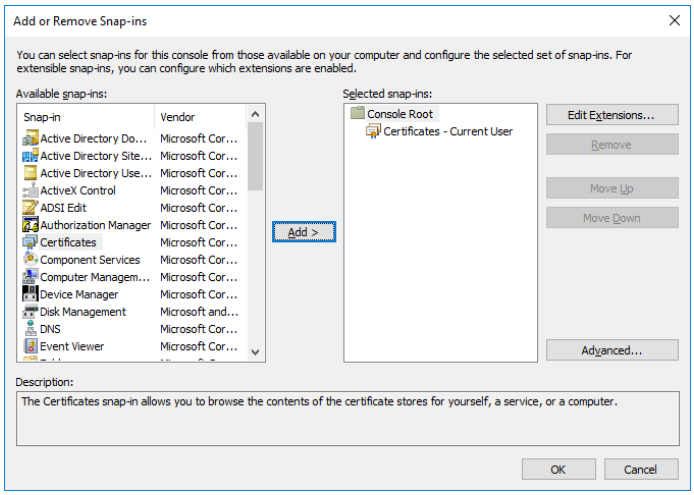
1. Run Microsoft Management Console (MMC) from CMD console using the service account set during the NC Protect installation to run NC Protect File Share and Scheduled Task:

   c:\Windows\System>runas /user:domain\svcncprotect mmc

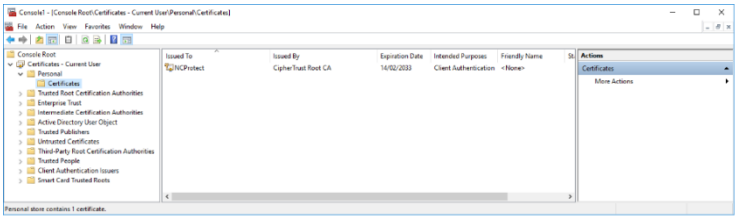
2. Provide service account password



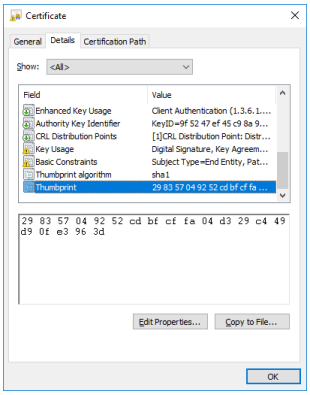
3. In Microsoft Management Console add the Certificates Snap-in



4. In Certificates window import the pfx file generated in the above section



5. Select certificate and note the thumbprint



6. Restart IIS
7. In NC Protect Admin enter the details to configure the CipherTrust Manager integration, including the thumbprint of the certificate you have imported above, but also IP address, user, and encryption key identifier.

8. Hit Test and Save.

Note: With Self-Signed certificates, you might encounter a "Could not load Encryption Certificate" message after hitting 'Test and Save'. This can occur when a certificate validation error is returned when attempting to save the configuration. Refer to the next section on allowing for CipherTrust Manager self-signed certificates to be used by NC Protect.

5.2.4 CipherTrust Manager Self-Signed Certificates

When using self-signed certificates (eg created from CipherTrust Manager) NC Protect may require the issuer of the self-signed certificate to be defined with NC Protect.

This is done by adding the following entry : SelfSignForNCProtect == "**ciphertrust**"
In one or more of the following areas (depending on the NC Protect product installed):

1. NC Protect for M365 : NC Protect's Resource Group > Storage Account > Settings table
2. NC Protect for SharePoint On-Prem : NC Protect's Configuration table
3. NC Protect for File Shares : `NUCDB` SQL Database > Configuration' Table

Where : "ciphertrust" is a string contained in the issuer name/address. This allows the self signed certificate chaining to be passed by NC Protect during the server certificate validation callback.