TRUENAS

Integration Guide

Applicable Devices:
KMES Series 3

TABLE OF CONTENTS

[1] INTEGRATION OVERVIEW

[1.1] ABOUT TRUENAS

From TrueNAS's Documentation Hub: "TrueNAS is the world's most popular Open Source storage operating system and is the most efficient solution for managing and sharing data over a network. It is the simplest way to create a safe, secure, centralized, and easily accessible place for your data. TrueNAS Open Storage provides unified ZFS-based storage for file, block, object, and application data."

[1.2] WHAT IS KMIP?

The Key Management Interoperability Protocol (KMIP) is an extensible communication protocol that defines message formats for the manipulation of cryptographic keys on a key management server. This facilitates data encryption by simplifying encryption key management. Keys may be created on a server and then retrieved, possibly wrapped by other keys. Both symmetric and asymmetric keys are supported, including the ability to sign certificates. KMIP also allows for clients to ask a server to encrypt or decrypt data, without needing direct access to the key.

[1.3] PURPOSE OF THE INTEGRATION

KMIP on TrueNAS Enterprise is used to integrate the system within an existing centralized key management infrastructure and use a single trusted source (i.e., the KMES Series 3) for creating, using, and destroying SED passwords and ZFS encryption keys.

[1.4] OVERVIEW OF THE STEPS NEEDED FOR INTEGRATION

1. Create TLS certificates for connection and authentication between the TrueNAS instance and the KMES Series 3
    a. Generate and sign the TrueNAS certificate
    b. Generate and sign the KMIP server connection pair certificate
2. Create new user on the KMES Series 3 for TrueNAS
3. Configure the TLS certificate for the KMIP server connection pair
4. Import TLS certificates into TrueNAS
5. Configure KMIP in TrueNAS
6. Test the connection between TrueNAS and the KMES Series 3
7. Create an encrypted dataset, which allows TrueNAS to start using KMIP

[2] PREREQUISITES

Supported Hardware:

- KMES Series 3, version 6.1.3.11 and above, with the *KMIP* license enabled

[3] CONFIGURE TLS CERTIFICATES FOR THE CONNECTION BETWEEN TRUENAS AND THE KMES SERIES 3

Before KMIP connections can occur, the TrueNAS instance and KMES Series 3 must establish a mutual trust relationship by validating their respective digitally signed certificates.

In the following subsections, certificates will be generated and signed for TrueNAS and the KMIP server connection pair on the KMES Series 3. The certificates will be registered both in TrueNAS and for the KMIP server connection pair on the KMES Series 3 and will be used each time a TCP/IP session secured by TLS is established.

[3.1] GENERATE AND SIGN THE TRUENAS CERTIFICATE

There are two optional methods for generating and signing the TrueNAS certificate:

1. Using an external CA
2. Using the KMES Series 3 as the CA

[3.1.1] Method 1: Using an external CA

For this method, the external CA certificate(s) need to be imported into an empty Certificate Container on the KMES. A Certificate Signing Request (CSR) will then be generated, which the external CA will use to issue a TLS certificate for the TrueNAS instance. The certificate will then be imported into the Certificate Container on the KMES that contains the external CA certificate.

1. Go to the *Certificate Authorities* menu and click the **Add CA...** button at the bottom of the page.
2. Specify a name for the Certificate Container, such as "Externally Issued", then click **OK**. The new Certificate Container will be listed in the Certificate Authorities menu.
3. Right-click on the newly created **Externally Issued** Certificate Container and select **Edit**. In the *Certificate Authority* dialog, check the box that says, "Can be used for PKI authentication", then click **OK** to save.
4. Right-click again on the **Externally Issued** Certificate Container and select **Import** -> **Certificate(s)...**. This will open the *Import Certificates* dialog.
5. Click the **Add...** button in the bottom left-hand portion of the dialog, then find and select the external CA certificate(s) that will be issuing the TrueNAS TLS certificate. The CA certificate(s) will populate in the Verified section of the *Import Certificates* dialog.
6. Click **OK** to save. The external CA certificate(s) should be listed now in tree form under the **Externally Issued** Certificate Container.
7. Next, we'll create a placeholder code signing certificate, from which a CSR can be generated. Right-click on the lowest level CA certificate in the tree and select **Add Certificate** -> **Pending...**. This will open the *Create X.509 Certificate* dialog.
8. In the *Subject DN* tab, set a Common Name for the certificate, such as "TrueNAS".

9. Leave all other values as the default and click **OK**. The **TrueNAS** placeholder certificate will be listed now under the external CA certificate(s).
10. Right-click on placeholder **TrueNAS** certificate and select **Export** -> **Signing Request...**. This will open the *Create PKCS #10 Request* dialog.
11. Leave all of the settings in the *Subject DN* tab as the default values.
12. In the *V3 Extensions* tab, select the "Example TLS Client Certificate" profile.
13. In the *PKCS #10 Info* tab, specify a save location for the CSR, then click **OK**. There should be a message stating that the certificate signing request was successfully written to the location you specified.
14. The CSR file then needs to be taken to an external certificate authority. Using the CSR, the external CA will issue a TLS certificate.

    NOTE: After the external CA issues the code signing certificate, it needs to be copied to the storage medium that is configured on the KMES.
15. In the *Certificate Authorities* menu on the KMES, right-click on the placeholder **TrueNAS** certificate and select **Replace** -> **With Signed Certificate...**. This will open the *Import Certificates* dialog.
16. Click the **Add...** button in the bottom left-hand portion of the dialog, then find and select the externally signed TLS certificate in the file browser. The certificate will populate under the CA certificate(s) in the Verified section of the *Import Certificates* dialog.
17. Click **OK** to save.
18. The remaining steps in this section involve exporting the TrueNAS certificate as a PKCS #12 file. To be able to do this, there is a configuration option that must be enabled. Navigate to *Configuration* -> *Options* and check the box next to the first menu option, which says, "Allow export of certificates using passwords". Then click **Save**.
19. Now, right-click on the TrueNAS certificate and select **Export** -> **PKCS12...**.
20. In the *Export PKCS12* window, ensure that "Export Selected" is selected and change the Cipher Options to "AES-256". Note, and optionally modify the file name, then click **Next >**.
21. Set a password for the PKCS #12 file, then click **Next >**.
22. Click **Finish** and the PKCS #12 file will be saved to the location that was specified.
23. **NOTE:** This PKCS #12 file contains the signed TrueNAS certificate, associated private key, and the root certificate, all encrypted under the password that was set for the file.

[3.1.2] Method 2: Using the KMES Series 3 as the CA

1. Go to the *Certificate Authorities* menu and click the **Add CA...** button at the bottom of the page.
2. Specify a name for the Certificate Container, such as "KMES Issued", then click **OK**. The new Certificate Container will be listed in the Certificate Authorities menu.

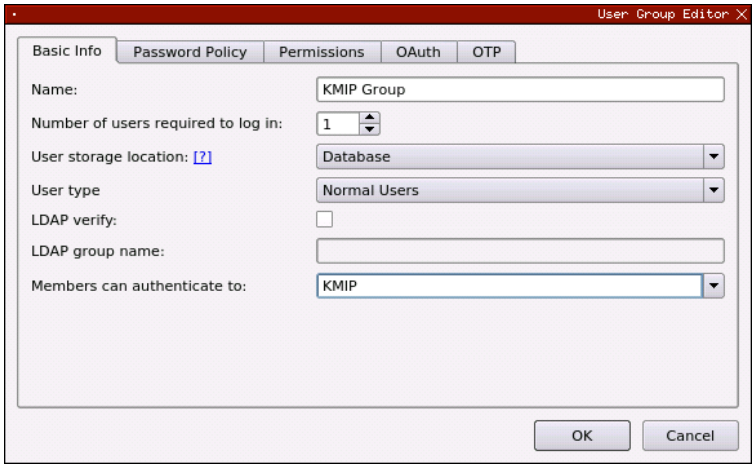
3. Right-click on the newly created **KMES Issued** Certificate Container and select **Edit**. In the *Certificate Authority* dialog, check the box that says, "Can be used for PKI authentication", then click **OK** to save.
4. Right-click again on the **KMES Issued** Certificate Container and select **Add Certificate -> New Certificate...**
5. In the *Subject DN* tab, set a Common Name for the certificate, such as "Root".
6. In the *Basic Info* tab, change the Major key to the **PMK**. All other settings can be left as the default values.
7. In the *V3 Extensions* tab, select the "Example Certificate Authority" profile, then click **OK**. The **Root** CA certificate will be listed now under the "KMES Issued" Certificate Container.
8. Right-click on the **Root** CA certificate that was just created and select **Add Certificate** -> **New Certificate...**.
9. In the *Subject DN* tab, set a Common Name for the certificate, such as "TrueNAS".
10. In the *V3 Extensions* tab, change the profile to "Example TLS Client Certificate", then click **OK** to finish generating the certificate.
11. The remaining steps in this section involve exporting the TrueNAS certificate as a PKCS #12 file. To be able to do this, there is a configuration option that must be enabled. Navigate to *Configuration -> Options* and check the box next to the first menu option, which says, "Allow export of certificates using passwords". Then click **Save**.
12. Now, right-click on the TrueNAS certificate and select **Export** -> **PKCS12...**.
13. In the *Export PKCS12* window, ensure that "Export Selected" is selected and change the Cipher Options to "AES-256". Note, and optionally modify the file name, then click **Next >**.
14. Set a password for the PKCS #12 file, then click **Next >**.
15. Click **Finish** and the PKCS #12 file will be saved to the location that was specified.

NOTE: This PKCS #12 file contains the signed TrueNAS certificate, associated private key, and the root certificate, all encrypted under the password that was set for the file.

[3.2] CREATE A NEW USER FOR TRUENAS

A new user needs to be created on the KMES Series 3, which TrueNAS will use for authentication during KMIP connections. The name of this user needs to match exactly what is set as the **Common Name** for the signed TrueNAS certificate. This is how the KMES Series 3 authenticates the TrueNAS device that is connecting via KMIP.

1. Navigate to the *Users* menu, then click the **Add Group...** button.
2. In the *Basic Info* tab, set the fields to how they are shown below (**NOTE:** The name of the group can be anything.)



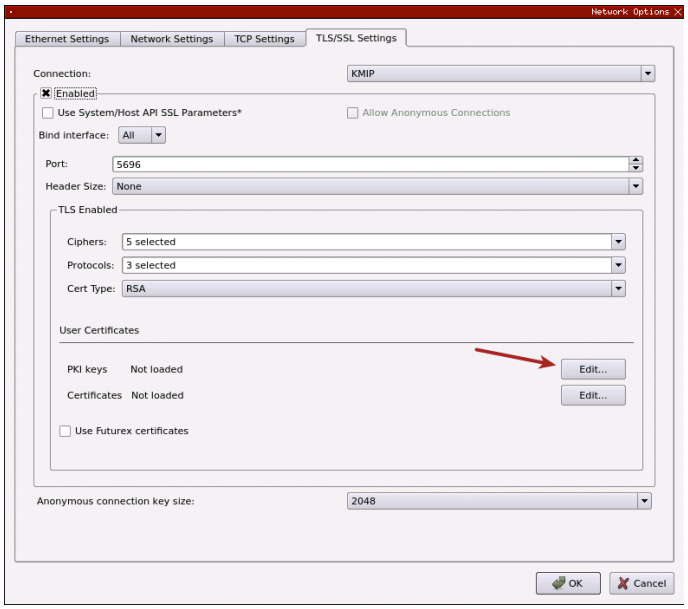
3. In the *Permissions* tab, enable all permissions for the group.
4. Click **OK** to save.
5. Right-click on the newly created User Group, then select **Add** -> **User...**.
6. Set "TrueNAS" as the user name (to match the Common Name of the TrueNAS certificate), then set a password.
7. Navigate to the *PKI Auth* tab, then click the **Add Trusted Certificate Authority** button next to KMIP.
8. Select the Certificate Container that contains the TrueNAS TLS certificate, then click **OK**.
9. It should show "Registered" next to KMIP now. Click **OK** to save.

[3.3] CONFIGURE TLS CERTIFICATE FOR THE KMIP SERVER CONNECTION PAIR

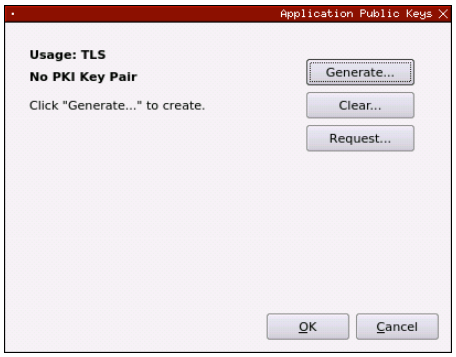
[3.3.1] Generate a new PKI key pair and CSR for the KMIP connection pair

1. Navigate to the *Configuration* menu, then double-click on *Network Options*. Under the *TLS/SSL Settings* tab, click the **Connection** dropdown and select the **KMIP** connection pair.
2. Enable the KMIP connection pair if it is not already enabled.
3. Uncheck **Use System/Host API SSL Parameters** if it is selected.

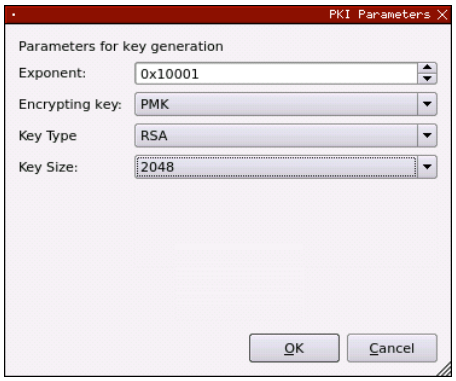
4. In the User Certificates section, click the **Edit...** button next to PKI keys.



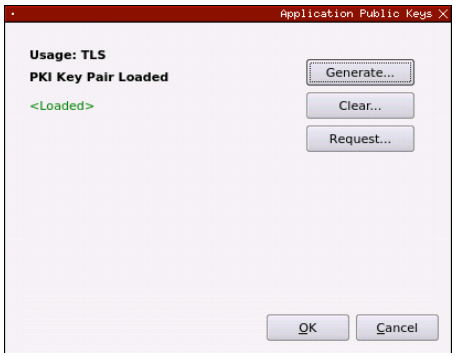
5. Click the **Generate...** button to create a new PKI Key Pair.



6. Click **Yes** and bypass the warning about SSL not being functional until new certificates are imported.
7. This will open the *PKI Parameters* dialog. Set the **PMK** as the Encrypting key, then change the Key Size to **2048**. Click **OK**.



8. The *Application Public Keys* dialog should now show that the PKI Key Pair is **Loaded**. If this is the case, click **Request...**.



9. The values in the *Subject DN* tab can be left as default. In the *V3 Extensions* tab, set the profile to **Example TLS Server Certificate**. In the *PKCS #10 Info* tab, specify a save location and name for the CSR file, then click **OK**.
10. A message box should appear saying that the certificate signing request was successfully written to the specified location. Click **OK** in this box.
11. Click **OK** in the *Application Public Keys* dialog, then click **OK** once more in the main *Network Options* dialog.

[3.3.2] Sign the KMIP connection pair CSR

1. Navigate to the *Certificate Authorities* menu, then right-click on the root CA certificate that issued the TrueNAS TLS certificate in section 3.1 and select **Add Certificate** -> **From Request...**.
2. In the file browser, find and select the KMIP connection pair CSR. Certificate information should populate in the *Create X.509 From CSR* window.
3. Leave all settings exactly as they are and click **OK** to save.
4. The signed KMIP server certificate should be listed now under the root CA certificate that issued it.

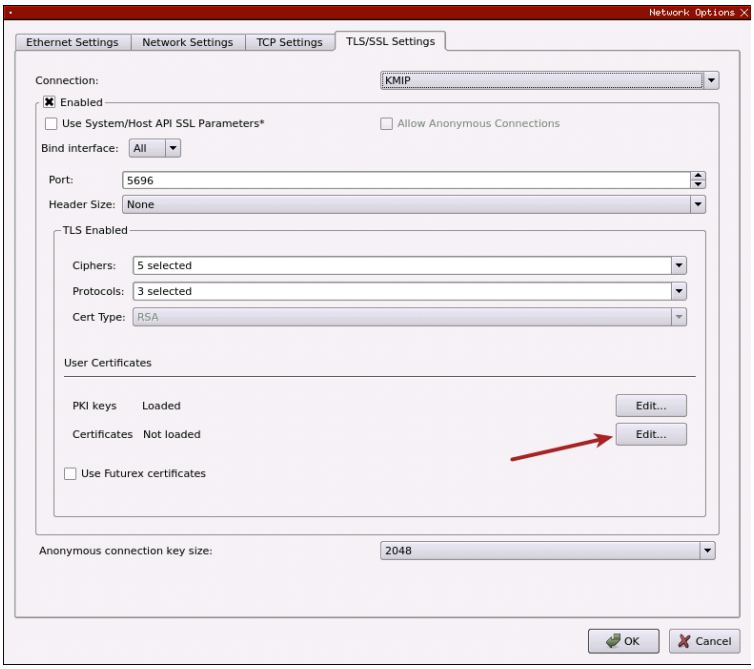
[3.3.3] Export all of the certificates in the certificate tree

For both the root CA certificate and the signed KMIP connection pair certificate, right-click on them and select **Export** -> **Certificate(s)...**. In the *Export Certificate* dialog for each, change the encoding to **PEM**, then specify a save location for the file.

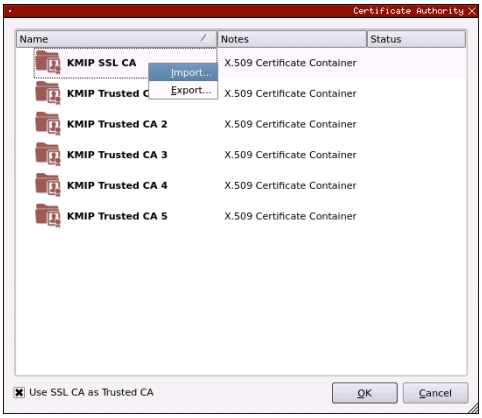
[3.3.4] Import the signed KMIP connection pair certificate

1. Navigate to the *Configuration* menu, then double-click on *Network Options*. Under the *TLS/SSL Settings* tab, click the **Connection** dropdown and select the **KMIP** connection pair.

2. In the User Certificates section, click the **Edit...** button next to Certificates.

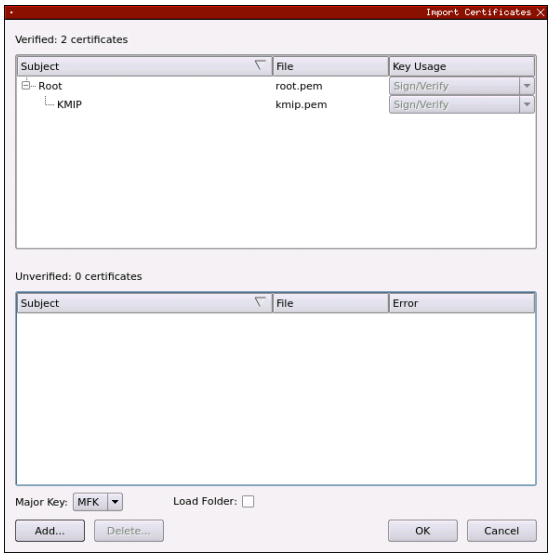


3. In the *Certificate Authority* dialog, right-click on the **KMIP SSL CA** X.509 Certificate Container, then select **Import...**.



4. In the *Import Certificates* dialog, click the **Add...** button at the bottom of the window. In the file browser, select both the root CA certificate and the signed KMIP server certificate and click **Open**. The certificates

should now be listed in the "Verified" section of the *Import Certificates* dialog. Click **OK** to save.



5. It should now say **Signed loaded** next to "Certificates" in the User Certificates section of the *Network Options* dialog. Click **OK** to save.

[4] IMPORT TLS CERTIFICATES INTO TRUENAS

In this section, the TrueNAS TLS certificate created in the previous section will be imported into TrueNAS, along with the CA certificate that issued the TLS certificates for both TrueNAS and the KMIP server connection pair on the KMES Series 3.

Before doing so, it is necessary to extract the certificates and private key from the PKCS #12 file exported from the KMES Series 3 in section 3.1. This will be done using OpenSSL.

[4.1] EXTRACT THE PKCS #12 FILE

1. Open a terminal application that has OpenSSL installed.
2. Navigate to the directory where the PKCS #12 file is saved.
3. Run the following OpenSSL command to extract the certificates and private key from the PKCS #12 file and save them to a new file:

   ```
   $ openssl pkcs12 -in tree.p12 -out tree.pem -nodes
   ```

   The command will prompt for the import password. Enter the password that was specified when the PKCS #12 file was exported from the KMES.
4. Open the output file (e.g., tree.pem) to view the TrueNAS certificate, it's associated private key, and the CA certificate that issued both the TrueNAS certificate and the KMIP server connection pair certificate. These will need to be copied and pasted into the TrueNAS web interface in the next subsection.

[4.2] IMPORT THE CA CERTIFICATE

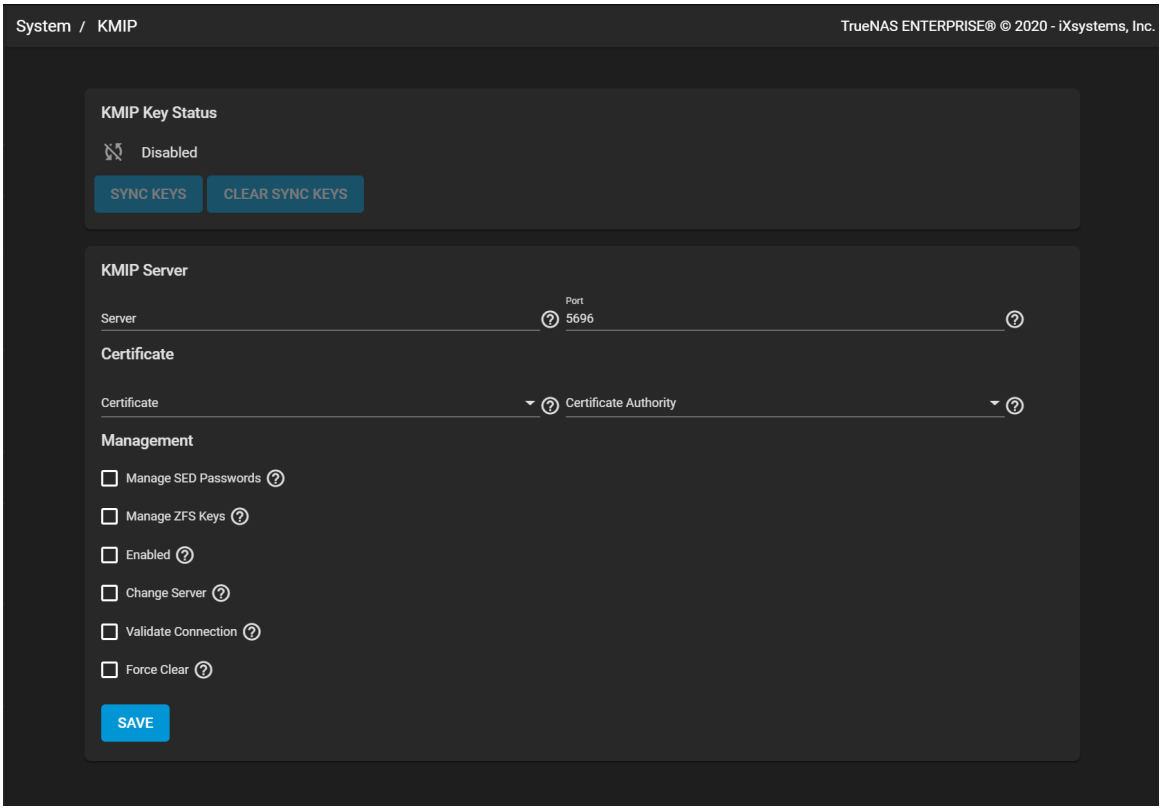
1. Log in to the TrueNAS web interface.
2. Go to *System -> CAs* and click **ADD**.
3. In the Type drop down menu, select **Import CA**.
4. Enter a memorable name for the CA, then paste the CA certificate that was extracted from the PKCS #12 file into the Certificate field.
5. Leave the Private Key and Passphrase fields empty and click **SUBMIT**.

[4.3] IMPORT THE TRUENAS CERTIFICATE

1. Log in to the TrueNAS web interface.
2. Go to *System -> Certificates* and click **ADD**.
3. In the Type drop down, select **Import Certificate**.
4. Enter a memorable name for the certificate, then paste the TrueNAS certificate and private key that were extracted from the PKCS #12 file into the appropriate fields.
5. Leave the Passphrase field empty and click **SUBMIT**.

[5] CONFIGURE KMIP IN TRUENAS

1. Log in to the TrueNAS web interface.
2. Go to *System* -> *KMIP* to complete the configuration.



3. Enter the KMES Series 3 IP address or host name and the default KMIP connection port, 5696. Select the *Certificate* and *Certificate Authority* that were imported in the previous section. To check that the Certificate and CA chain is correct, check the *Validate Connection* box and click **SAVE**.
4. When the certificate chain is verified, choose the encryption values, SED passwords, or ZFS data pool encryption keys to move to the KMES Series 3. Set *Enabled* to begin moving the passwords and keys immediately after clicking **SAVE**.
5. Refreshing the KMIP page shows the current KMIP Key Status.

To cancel a pending key synchronization, set *Force Clear* and click **SAVE**.

[6] CREATE AN ENCRYPTED DATASET

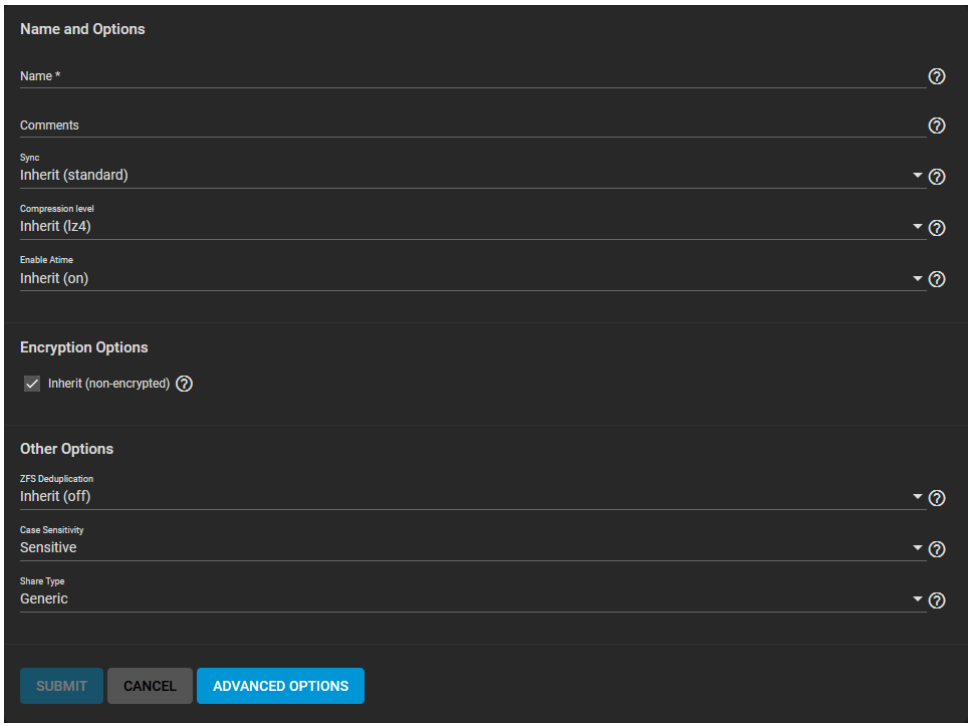
The last step required for the TrueNAS / KMES Series 3 integration is to create at least one encrypted dataset, which allows TrueNAS to start using KMIP.

Datasets exist inside storage Pools, so if a storage Pool does not already exist, one needs to be created. Please refer to the following article on the TrueNAS Documentation Hub for setting up a storage Pool: https://www.truenas.com/docs/core/gettingstarted/storingdata/

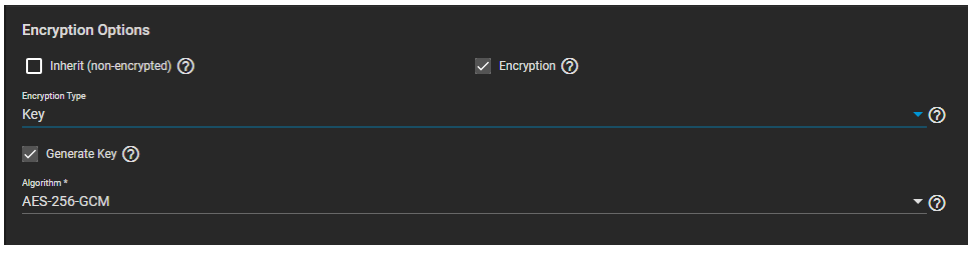
[6.1] ENCRYPTING A NEW DATASET

New datasets within an existing unencrypted storage pool can also be encrypted without having to encrypt the entire pool. To encrypt a single dataset, complete the following steps:

1. Go to *Storage* -> *Pools*, click the three vertical dots on the far right-hand side of the menu for an existing dataset, and click **Add Dataset**.



2. In the *Encryption Options* area, unset *Inherit* and check *Encryption*.



3. Choose which type of authentication to use: a **Key** or a **Passphrase**. Then click **SUBMIT**.

If the type of authentication chosen for the new dataset was **Key**, the ZFS key will be created on the KMES Series 3 and retrieved by TrueNAS as needed. If the **Passphrase** option was chosen, the passphrase will only be created via KMIP if TCG OPAL capable disks are attached to the NAS being used.

APPENDIX A: XCEPTIONAL SUPPORT

In today's high-paced environment, we know you are looking for timely and effective resolutions for your mission-critical needs. That is why our Xceptional Support Team does whatever it takes to ensure you have the best experience and support possible. Every time. Guaranteed.

- 24x7x365 mission critical support
- Level 1 to level 3 support
- Extremely knowledgeable subject matter experts

At Futurex, we strive to supply you with the latest data encryption innovations as well as our best-in-class support services. Our Xceptional Support Team goes above and beyond to meet your needs and provide you with exclusive services that you cannot find anywhere else in the industry.

- Technical Services
- Onsite Training
- Virtual Training
- Customized Consulting
- Customized Software Solutions
- Secure Key Generation, Printing, and Mailing
- Remote Key Injection
- Certificate Authority Services

Toll-Free: 1-800-251-5112

E-mail: support@futurex.com

ENGINEERING CAMPUS

864 Old Boerne Road

Bulverde, Texas, USA 78163

Phone: +1 830-980-9782

+1 830-438-8782

E-mail: info@futurex.com

XCEPTIONAL SUPPORT

24x7x365

Toll-Free: 1-800-251-5112

E-mail: support@futurex.com

SOLUTIONS ARCHITECT

E-mail: solutions@futurex.com