IBM Security Key Lifecycle Manager, Version 4.1 messages

Contents

Messages

Depending on the outcome of an operation, IBM® Security Guardium® Key Lifecycle Manager might provide an informational, warning, or error message.

Message syntax

The message syntax contains elements for the product identifier, as well as which part of the product issued the message, the message number, and an indicator that the message content contains information, a warning, or error description.

Messages have the following syntax:

```
CTGUUXXXXZ
```

where:

CTG
Identifies the IBM Security Guardium Key Lifecycle Manager product.

UU
Identifies which part of the product issued the message. For example:

KM
The Guardium Key Lifecycle Manager server issued the message.

KO
Password policy messages.

KS
The IBM Security Guardium Key Lifecycle Manager key server issued the message.

KP
KMIP messages.

XXXX
Is the message number, such as 0001.

Z
Is the character I for informational message, W for warning message, or E for error message.

For example:

```
CTGKM0545E: An error occurred exporting a certificate.
```

Error and warning messages

These are the IBM Security Guardium Key Lifecycle Manager error and warning messages.

Note: These messages are applicable for the earlier versions of the product as well.

File Deleted **Antigen for Exchange removed getadmingroupname.vbs since it was found to match the FILE FILTER= unnamed: *.vbs file filter.**

Explanation:
The problem is typically caused on Windows systems by antivirus installation software.

System action:
Installation fails.

Administrator response

Take these steps:

1. Obtain and reinstall the `getadmingroupname.vbs` file.
2. Change the antivirus file filter to avoid removing this file.
3. Install IBM Security Guardium Key Lifecycle Manager again.

CTGKM2101E Location specified in replication.BackupDestDir is not a valid directory.

Explanation:
replication.BackupDestDir must specify a valid directory.

System action:
The operation fails.

Administrator response:
Correct setting of replication.BackupDestDir to a valid directory.

CTGKM2102E No valid replication config file exists. It will be created.

Explanation:
No valid replication config file exists. It will be created.

System action:
The operation fails.

Administrator response:
No action required.

CTGKM1015E Key server is down.

Explanation:
The key server is an internal component that the Guardium Key Lifecycle Manager server contains. There might be a protocol or a certificate error or the database might not be started when the Guardium Key Lifecycle Manager server comes up.

System action:
Keys are not served.

Administrator response:
You might need to correct a protocol or certificate specification or start the database. Examine the audit log for error messages. After making corrections, restart the Guardium Key Lifecycle Manager server. You might need to contact IBM Support.

CTGKM1016E TCP port not available.

Explanation:
The TCP port did not initialize. Guardium Key Lifecycle Manager is not ready to accept key requests on the TCP port. It might be that another process has the port or that the socket timed out.

System action:
The TCP port fails to initialize and TCP communication fails.

Administrator response:
Ensure that no other program is using the TCP port. If the other process must have the port, specify a new TCP port number. Then restart the Guardium Key Lifecycle Manager server. If the problem continues, examine the audit log. After making corrections, restart the Guardium Key Lifecycle Manager server. You might need to contact IBM Support.

CTGKM1017E TLS failed to initialize.

Explanation:
The TLS port did not initialize. Guardium Key Lifecycle Manager is not ready to accept key requests from a client on the TLS port. It might be that another process has the port or that the socket timed out.

System action:
The TLS port fails to initialize and TLS communication fails.

Administrator response:
Ensure that no other program is using the TLS port. If the other process must have the port, specify a new TLS port number. Then restart the Guardium Key Lifecycle Manager server. If the problem continues, examine the audit log. After making corrections, restart the Guardium Key Lifecycle Manager server. You might need to contact IBM Support.

CTGKM1018E KMIP failed to initialize.

Explanation:
An internal error occurred. IBM Security Guardium Key Lifecycle Manager could not complete initialization for KMIP. It might be that another process has the port or that the socket timed out.

System action:
The KMIP TLS port fails to initialize and IBM Security Guardium Key Lifecycle Manager cannot accept KMIP requests from a client.

Administrator response:
Ensure that no other program is using the KMIP TLS port. If the other process must have the port, specify a new KMIP TLS port number. Then restart the Guardium Key Lifecycle Manager server. If the problem continues, examine the audit log. After making corrections, restart the Guardium Key Lifecycle Manager server. You might need to contact IBM Support.

CTGKM1020E Each port value must be unique. Two or more of the port values configured have the same value.

Explanation:
TCP, TLS, and KMIP TLS cannot use the same port.

System action:
The TCP, TLS, or KMIP TLS port values will not be saved until the values are updated to be unique values.

Administrator response:
Set the TCP, TLS, and KMIP TLS ports to unique values.

CTGKM1050E An entry in a required field is missing, or an entry is not valid. The field is highlighted below.

Explanation:
You attempted to change to another page or to submit changes when either a required field is not complete or you entered a value that is not valid.

System action:
Additional page help appears by the field that has the error.

Administrator response:
Correct the entry. Then submit the change again.

CTGKM1051E **Because this certificate is currently the ${0} certificate and is in use, it cannot be deleted. If you still wish to delete this certificate, you must change the ${0} certificate.**

Explanation:
You cannot delete a certificate that is currently specified as the default or the system partner certificate, or a certificate that is currently assigned as the in-use TLS/KMIP server certificate.

System action:
The operation fails.

Administrator response:
Specify another certificate as the current default or system partner certificate, or the in-use TLS/KMIP server certificate. Then try to delete this certificate again.

CTGKM1052W **Certificate will be deleted only if it is not currently used by any device. Any ${0} written previously using this certificate will be non-readable if the certificate is deleted. Are you sure you would like to try to delete ${1}?**

Explanation:
You cannot delete a certificate that is currently used by a device. Delete certificates only when the data protected by those certificates is no longer needed.

System action:
If you proceed, the certificate is deleted. Deleting a certificate marks the certificate as destroyed in the database and deletes the material from the keystore.

Administrator response:
Continue to delete the certificate, assuming it is not in use by a device.

CTGKM1053W **Are you sure you would like to delete the device with device serial number ${0}?**

Explanation:
This message confirms that you want to delete the selected device.

System action:
Confirming the message deletes the device.

Administrator response:
Ensure that the serial number correctly identifies the device that you intend to delete. Then click **OK** to delete the device.

CTGKM1054E **Because this key group is currently the ${0} key group and is in use, it cannot be deleted. If you still wish to delete this key group, you must change the ${0} key group.**

Explanation:
IBM Security Guardium Key Lifecycle Manager could not delete a key group that is a default.

System action:
The key group is retained in the IBM Security Guardium Key Lifecycle Manager database.

Administrator response:
Ensure that the key group is not the default or reassign another key group to be the system default. Then try the operation again.

CTGKM1055W **Deleting a key group deletes all the keys within a key group. Any data protected by these keys will be non-readable if the keys are deleted. Are you sure you would like to delete ${0}?**

Explanation:
Deleting a key group marks the key group and all keys in the group as destroyed in the database and deletes the material from the keystore.

System action:
If you proceed, the key group and all keys in the key group are deleted.

Administrator response:
Ensure that data protected by the keys in the key group is no longer needed. Then continue the delete operation.

CTGKM1056W **Directory ${0} does not exist. Do you want to create it?**

Explanation:
The selected directory path that is specified to store the keystore does not currently exist.

System action:
If you continue, the directory is created.

Administrator response:
Confirm that you want to create the directory to store the keystore.

CTGKM1057W **Deleting a key will render any data protected by the key non-readable. Are you sure you would**

like to delete the following key: ${0}?

Explanation:
Deleting a key marks the key as destroyed in the database and deletes the material from the keystore. Data protected by the key is no longer readable.

System action:
If you proceed, the key is deleted.

Administrator response:
Ensure that data protected by the key is no longer needed. Then continue the delete operation.

CTGKM1058W Delete ${0}. Warning: Critical data will be deleted. Do you want to continue?

Explanation:
You are about to delete a backup file. This message asks you to confirm the deletion.

System action:
If you continue, the backup file is deleted.

Administrator response:
Ensure that the data protected by this backup level is no longer needed, or is replicated in another level. Then continue the delete operation.

CTGKM1059E Path entered is not valid.

Explanation:
The path that you entered is not a valid path.

System action:
The path does not exist.

Administrator response:
Specify a correct, existing path. Then try again.

CTGKM1060W Warning: If you delete ${0}, the level of this backup cannot be restored. Do you want to continue?

Explanation:
Deleting a backup file means you cannot restore the level again.

System action:
If you proceed, the backup file is deleted.

Administrator response:
Ensure that data protected by this backup level is no longer needed, or is replicated in another level. Then continue the delete operation.

CTGKM1061W Creating backup to ${0}. Do you want to continue?

Explanation:
This operation writes a backup file to the specified location.

System action:
The operation writes a backup file to the location in this message.

Administrator response:
Confirm that you want the backup file written to the specified location. Then continue.

CTGKM1062W The system will be restored from ${0}. The key and configuration data will be restored to the level of the backup that you select. Any changes made after the selected backup will be lost, including the metadata. After restoring from this backup, the server will be restarted automatically. The server will not be available during the restart process. After the server is restarted, you must restart the browser session (Log in again to use the product user interface). Do you want to continue?

Explanation:
The key and configuration data are restored to the level of the backup that you select. Any changes made after the selected backup are lost, including the metadata.

System action:
The key and configuration data are restored to the level of the backup you select. Later changes are lost.

Administrator response:
Confirm that you want to restore from this backup level. When the operation completes, manually restart the Guardium Key Lifecycle Manager server.

CTGKM1063E A default key group needs to include at least one key.

Explanation:
There are no keys in the default key group. Values in fields on this page might specify no keys, fail to add needed keys, or delete existing keys to zero.

System action:
The operation fails.

Administrator response:
Ensure that the key group has at least one valid key. Then try again to specify the key group as the default.

CTGKM1064E You cannot delete this certificate, which is currently used by ${0} tape drives as either a system default, or as a partner certificate. First, use the appropriate ${0} management panel to specify a different certificate as the system default or partner certificate. Then, delete the certificate.

Explanation:
You cannot delete a certificate that is in use as the system default or partner certificate.

System action:
The operation fails.

Administrator response:
First, use the appropriate ${0} management panel to specify a different certificate as the system default or partner certificate. Then, delete the certificate.

CTGKM1065W The number of keys returned exceeds the limit of ${0} records, which are displayed. You might need to specify a different filter for your search. Then try again.

Explanation:
The search returned more keys than the limit allows.

System action:
The search fails.

Administrator response:
You might need to specify a different filter for your search. Then try again.

CTGKM1066W Critical data is added. Create a backup to ensure that you can restore this data later.

Explanation:
Critical data is added such as certificates or keys.

System action:
Data is added.

Administrator response:
To ensure that you can restore critical data in case of loss, create a backup file.

CTGKM1067W Are you sure you would like to delete ${0}? ${0} will no longer become a default in the future.

Explanation:
This operation deletes assignment of the certificate or key group as a future default rollover.

System action:
The system deletes the assignment as a rollover for the certificate or key group. The action does not delete the certificate or key group.

Administrator response:
Determine that there is no requirement to use the certificate or key group as a future default. Then continue.

CTGKM1068E You need to select at least one type of default.

Explanation:
You attempted to specify a certificate for future use as a rollover without also specifying that the certificate will be the default or partner certificate, or both, on an effective date.

System action:
The operation pauses until you specify that the selected certificate is a default or partner certificate, or both, on the effective date.

Administrator response:
Specify use as either the default or partner certificate, or both, for the certificate. Then continue.

CTGKM1069E Select a certificate from the list.

Explanation:
To continue, the operation requires that you select a certificate.

System action:
The operation pauses until you specify a certificate.

Administrator response:
Select a valid certificate. Then continue.

CTGKM1070E There is no certificate defined. Close this panel and add a certificate.

Explanation:
A required certificate is not in place.

System action:
The operation fails.

Administrator response:
Add the necessary certificate. Then try again.

CTGKM1071E IBM Security Guardium Key Lifecycle Manager application does not appear to be in a running state. The Guardium Key Lifecycle Manager server may be down at the moment or is still starting. Make sure that the Guardium Key Lifecycle Manager server is up and try your request again.

Explanation:
The Guardium Key Lifecycle Manager server might be down at the moment or is still starting.

System action:
The operation fails.

Administrator response:
Ensure that the Guardium Key Lifecycle Manager server is running. Then try your request again.

CTGKM1075E Insufficient permission to see the information provided on this page.

Explanation:
Your role does not have the necessary permission to view the data.

System action:

The page does not display the information.

Administrator response:
Obtain a user ID with the required permission. Then try again.

CTGKM1076W The current TLS/KMIP server certificate has been updated. Restart the server to put this change into effect. Then create a backup to ensure that you can restore this data.

Explanation:
An update occurred to the current TLS/KMIP server certificate.

System action:
The certificate update completes.

Administrator response:
Restart the server to put this change into effect. Then create a backup to ensure that you can restore this data.

CTGKM1077W The current TLS server certificate has been updated. In order for this change to go into effect you must restart the server.

Explanation:
An update occurred to the current TLS server certificate.

System action:
The certificate update completes.

Administrator response:
Restart the server to put this change into effect. Then create a backup to ensure that you can restore this data.

CTGKM1078W Are you sure you would like to delete certificate ${0}?

Explanation:
Deleting a certificate marks the certificate as destroyed in the database and deletes the material from the keystore. Delete certificates only when the data protected by those certificates is no longer needed. Deleting certificates is similar to erasing the data. After certificates are deleted, data protected by those certificates is not retrievable.

System action:
If you continue, the certificate is deleted.

Administrator response:
Ensure that the certificate and the data that it protects are not needed. Then continue.

CTGKM1080E Insufficient permission to perform this action.

Explanation:
Your role lacks one or more permissions required to take the action.

System action:
The action fails.

Administrator response:
Obtain a user ID with the required permissions. Then try again.

CTGKM1081W Are you sure that you want to delete device group ${0}?

Explanation:
You might delete an empty device group such as myLTO. You cannot delete a device group if any devices, keys or certificates are in that group. You also cannot delete a device family that IBM Security Guardium Key Lifecycle Manager provides.

System action:
If you continue, the device group is deleted.

Administrator response:
Determine whether the empty device group is a valid candidate to delete. Then continue.

CTGKM1082E Select a certificate from the list.

Explanation:
The operation requires that you specify a certificate.

System action:
The operation waits for your selection.

Administrator response:
Select a certificate. Then continue.

CTGKM1087W Are you sure you would like to reject device ${0}?

Explanation:
The device is in a pending device list. You must accept or reject the device request to be served keys. You can only reject devices for device groups that you have permissions to create. By repeating a request, the device might appear again in the pending list.

System action:
Rejection removes the device from the pending list.

Administrator response:
Ensure that you do not want keys served to the device. Then reject the request.

CTGKM1088W Creating more than 1000 keys may take a few minutes. Do you want to continue?

Explanation:
Creating a large number of keys requires a significant time interval.

System action:
If you continue, IBM Security Guardium Key Lifecycle Manager creates the keys.

Administrator response:
Ensure that you have time for this operation to complete. Then continue.

CTGKM1089E Insufficient permission to accept this device.

Explanation:
You can only accept devices for device groups that you have permissions to create.

System action:
The operation fails. Acceptance enables serving keys to the device and removes the device from the pending list.

Administrator response:
Obtain a user ID that enables you to accept devices from the pending list. Then try again.

CTGKM1091E Unknown device family id: ${0}

Explanation:
The device family for the operation is unknown.

System action:
The operation fails.

Administrator response:
Collect any information that might be in the audit log. You might need to contact IBM Software Support.

CTGKM1092W Keystore file ${0} already exists. Would you like to use this existing keystore?

Explanation:
The keystore name that you specified matches the name of an existing keystore.

System action:
If you continue, the operation uses the existing keystore.

Administrator response:
Determine whether the existing keystore is appropriate to use. Then continue.

CTGKM1093W No machines were found for the ${0} device family.

Explanation:
Adding machines requires that you first specify whether device requests are automatically approved or held pending your approval.

System action:
The operation cannot be done at this time.

Administrator response

To add machines, use the ${0} management panel to specify one of these choices:

- Automatically accept all new device requests for communication.
- Hold new device requests pending approval.

CTGKM1094W Do not use the setting of Automatically accept for the ${0} device family. This setting allows generation and serving of keys to ${0} storage servers before you can perform a backup.

Explanation:
This setting is not appropriate for devices in this device family.

System action:
The operation fails.

Administrator response:
Select to manually add devices for communication, or to hold new device requests pending your approval. Then continue.

CTGKM1095W Changing the device group of a certificate from an ${0} causes the certificate to be unavailable to devices in other device groups that previously referenced the certificate. Are you sure you want to continue?

Explanation:
This message occurs if you attempt to change (or update) an UNKNOWN certificate.

System action:
If you continue, the assignment for this certificate is changed. This certificate will only be able to be used by devices in the selected device group or later modified to a different device group within the same device family.

Administrator response:
If you are sure the certificate belongs to this device family, select **OK** to continue with the device group assignment.

CTGKN1003E File name entered for the certificate to be imported is not valid. Double-click on the ${0} column of the selected certificate entry to enter a valid path and file name.

Explanation:
The file name that you entered is not a valid file name.

System action:
The file name does not exist in the specified path.

Administrator response:
Specify a correct, existing path and file name. Then try again.

CTGKN1005W This panel cannot be accessed before a master keystore has

been created. Click on the master keystore link to create it now.

Explanation:
First, you must create a master keystore.

System action:
The content of the page is not displayed until a keystore is created.

Administrator response:
Create the master keystore. Then try again.

CTGKN1006I Key name specified is not a known key.

Explanation:
The key that you specified is unknown.

System action:
The operation fails.

Administrator response:
Obtain a valid key name. Then try again.

CTGKN1007E Insufficient permission to import the certificate.

Explanation:
Your role must have the permissions to the create action and to the appropriate device group. Or, your role must have the permission to the configure action to import a TLS or KMIP, certificate.

System action:
The import operation fails.

Administrator response:
Obtain a user ID with the required permissions. Then try again.

CTGKN1008E Insufficient permission to add additional keys to the key group.

Explanation:
Your role must have permissions to the modify action and to the appropriate device group.

System action:
The operation fails.

Administrator response:
Obtain a user ID with the permissions required to add keys to a key group. Then try again.

CTGKN1011W You cannot go to the Key and Device Management panel because the certificate belongs to an ${0} device group.

Explanation:
Because the certificate belongs to an UNKNOWN or CONFLICTED device group, the system cannot display a specific key and device management panel for a device group.

System action:
The system issues this warning.

Administrator response:
Click on the Key and Device Management navigation link and select the panel for the device group that you want to use this certificate.

CTGKN1012W Are you sure you would like to reject the certificate with a subject distinguished name of ${0} and issuer distinguished name of ${1}?

Explanation:
The message confirms that you want to reject the selected client device communication certificate that was pushed to the Guardium Key Lifecycle Manager server from a device.

System action:
Confirming the message will remove the certificate from IBM Security Guardium Key Lifecycle Manager. The certificate will not be able to be used for secure communications between the device and the server. The certificate will not be added to the keystore.

Administrator response:
Ensure that the subject distinguished name and issuer distinguished name correctly identify the client device communication certificate that you intend to reject. Then click **OK** to remove the certificate. For more information to identify the certificate before rejection, click **Cancel** and then select **View** for the certificate.

CTGKN1014E The selected certificate has expired and therefore cannot be accepted. Select Reject to remove it from the table.

Explanation:
A client device communication certificate that was pushed to the Guardium Key Lifecycle Manager server from a device has expired before being accepted. Expired certificates cannot be accepted.

System action:
The certificate is not added to the IBM Security Guardium Key Lifecycle Manager keystore.

Administrator response:
Select **Reject** to remove the certificate from the list of pending client device communication certificates.

CTGKM0002E Command failed: *VALUE_0*

Explanation:
The specification of the command, or one or more parameters in the command, is incorrect.

System action:
The command fails.

Administrator response:

Examine the error message, which might indicate which parameter caused the error. Retype the command string, and then try the command again.

CTGKM0003E Unhandled exception.

Explanation:
Unhandled exception.

System action:
The command fails.

Administrator response:
Examine the exception message, and then try the command again.

CTGKM0082E TLS connection cannot be established because the server certificate with alias *VALUE_0* has expired or is invalid. Configure a server certificate and retry the operation.

Explanation:
The server certificate that is specified in the `SKLMConfig.properties` file has expired.

System action:
TLS handshake fails and TLS connection cannot be established.

Administrator response:
Configure a valid TLS server certificate in the database. Restart the server. Check logs for more information.

CTGKM0100E Cannot obtain audit and key serving parameters information.

Explanation:
An internal component of the IBM Security Guardium Key Lifecycle Manager server is not running, such as the key server.

System action:
The internal component fails to obtain audit and debug information.

Administrator response:
Contact IBM Support.

CTGKM0101E Cannot update audit information.

Explanation:
A change was not written to the SKLMConfig.properties file.

System action:
A property value is not updated.

Administrator response:
Ensure that the SKLMConfig.properties file is write enabled. Then, try the operation again. If the problem persists, contact IBM Support.

CTGKM0102E Cannot update key serving parameter or port information.

Explanation:
A change was not written to the SKLMConfig.properties file.

System action:
A property value is not updated.

Administrator response:
Ensure that the SKLMConfig.properties file is write enabled. Then, try the operation again. If the problem persists, contact IBM Support.

CTGKM0103E Cannot retrieve keystore information.

Explanation:
The keystore information was not available from the database.

System action:
The database is not available.

Administrator response:
Ensure that the database is available. Correct any database server runtime errors that you identify. Then, try the operation again.

CTGKM0104E Cannot add keystore.

Explanation:
The keystore information might not be available from the database. Alternatively, the directory for the keystore file cannot be found. You might not have access to the directory. There might be more information in the message that describes the problem.

System action:
The keystore is not added.

Administrator response:
Ensure that the database is available. Additionally, determine that the directory exists for the keystore file. Additional information in the message might guide your response. Make appropriate changes. Then, try the operation again.

CTGKM0110E Retrieval of TLS/KMIP certificates failed:

Explanation:
The attempt to obtain a list of TLS/KMIP certificates was not successful. The database might not be available, or a connection to the IBM Security Guardium Key Lifecycle Manager server might not be available.

System action:
A list of certificates is not retrieved.

Administrator response:
Ensure that connections to the database and IBM Security Guardium Key Lifecycle Manager server are available. If a connection problem exists, make the appropriate corrections. Then, try the operation again.

CTGKM0112E TLS/KMIP certificate submit failed:

Explanation:
You might not have permission to write to the certificate request file. Alternatively, there might not be sufficient free disk space, or the database might not be available.

System action:
The certificate request is not created.

Administrator response:
Ensure that your permissions are correct, that there is sufficient free disk space, and that the database connection is available. If not, make the appropriate corrections. Then, try the operation again.

CTGKM0114E Certificate label and description (common name) are required fields.

Explanation:
An empty or null value was found for a certificate name, or the description (common name) for the certificate might be missing in the certificate request.

System action:
The operation fails.

Administrator response:
Specify a unique value for the certificate name and specify a common name for the certificate. Then, try the operation again.

CTGKM0115E Certificate was not selected.

Explanation:
A certificate was not selected from the list of valid, active certificates for communication with the server.

System action:
The operation fails.

Administrator response:
Select a valid certificate, Then, try the operation again.

CTGKM0116E Selected certificate does not match any active certificates in the keystore.

Explanation:
An exception occurred in internal processes.

System action:
The selected certificate does not match any of the list of certificates in the keystore. The certificate might have been manually deleted from the keystore, but not from metadata in the database.

Administrator response:
Select a different certificate. Then, try the operation again. You might need to ensure that your database metadata is a match to the contents of the keystore.

CTGKM0117E Cannot create directory *DIRECTORY_NAME* .

Explanation:
You might not have the correct access to create the directory, or the specified path might have an error. The directory might already exist. There might be additional information.

System action:
The create directory operation fails.

Administrator response:
Ensure that your access allows you to create a directory and that the specified path is valid. Additional information might also guide your response. Make appropriate changes. Then try the operation again.

CTGKM0118E Directory with the name you specified already exists.

Explanation:
The specified directory name already exists in the file system.

System action:
The create directory operation fails.

Administrator response:
Ensure that the specified directory does not already exist in the file system.

CTGKM0119E Cryptographic object not found: *VALUE_0*

Explanation:
The cryptographic object for given unique identifier or name does not found.

System action:
The PUSH operation fails.

Administrator response:
Ensure that you have provided correct unique identifier or name for the cryptographic object to be pushed to client.

CTGKM0120E Either cryptographic object's unique identifier(uuid) or name is required. Please provide one.

Explanation:
Either cryptographic object's unique identifier(uuid) or name is required. Please provide one.

System action:
The PUSH operation fails.

Administrator response:
Ensure that either cryptographic object's unique identifier(uuid) or name is provided for PUSH operation.

CTGKM0200E Cannot add device.

Explanation:
The device might already exist, or the database might not be available. There might be additional information.

System action:
The device add operation fails.

Administrator response:
Determine whether you correctly specified the device. Alternatively, you might need to confirm that the database is available. Additional information in this message might also guide your response. Make corrections. Then, try the operation again.

CTGKM0201E Cannot modify device.

Explanation:
The device might already exist, or the database might not be available. There might be additional information.

System action:
The device modify operation fails.

Administrator response:
Determine whether you correctly specified the device. Alternatively, you might need to confirm that the database is available. Additional information in this message might also guide your response. Make corrections. Then, try the operation again.

CTGKM0202E Cannot delete device.

Explanation:
The device might not exist, or the database might not be available. There might be additional information.

System action:
The device delete operation fails.

Administrator response:
Determine whether you correctly specified the device. Alternatively, you might need to confirm that the database is available. Additional information in this message might also guide your response. Make corrections. Then, try the operation again.

CTGKM0205E Cannot retrieve template defaults.

Explanation:
Internally-processed template default information was not available from the database.

System action:
The operation fails.

Administrator response:
Determine whether the database is available. Correct any database server runtime errors that you identify. Then, try the operation again. You might need to contact IBM Support.

CTGKM0206E Cannot retrieve certificates.

Explanation:
A list of certificates was not available. The IBM Security Guardium Key Lifecycle Manager database might not be available. There might be additional information.

System action:
Certificate retrieval fails.

Administrator response:
Confirm that the database is available. You might need to restart the IBM Security Guardium Key Lifecycle Manager server. Additional information in this message might also guide your response. Make corrections. Then, try the operation again.

CTGKM0207E Cannot create certificate.

Explanation:
IBM Security Guardium Key Lifecycle Manager could not create a certificate in the keystore. There might be a problem with the certificate information or a problem with the keystore. There might be additional information.

System action:
The certificate create operation fails.

Administrator response:
Ensure that the required certificate information is correct. You might use the tklmKeyStoreList command to ensure that the keystore is available. Additional information in this message might also guide your response. Correct errors. Then, try the operation again.

CTGKM0208E Cannot modify certificate.

Explanation:
IBM Security Guardium Key Lifecycle Manager could not modify information for the specified certificate. If you specify that the certificate is a system default or partner certificate, the properties file might not be available. If you modify the Trust setting for a certificate, refer to additional information in this message.

System action:
The certificate modify operation fails.

Administrator response:
Ensure that the properties file is available, and that you have write access. Additional information in this message might guide your response. Correct errors. Then, try the operation again.

CTGKM0209E Cannot delete certificate.

Explanation:
IBM Security Guardium Key Lifecycle Manager could not delete a certificate that is a system default or partner, or associated with a device. This message might have additional information.

System action:
The certificate delete operation fails.

Administrator response:
Ensure that the certificate is not a system default or partner certificate, and that the certificate has no associated devices. Additional information in this message might also guide your response. Then, try the operation again. If the delete operation is successful, ensure that you back up the keystore again to retain its current state.

CTGKM0210E Cannot update setting to accept requests from all drives.

Explanation:
An attempt was made to change the drive.acceptUnknownDrives property in the SKLMConfig.properties file. The file might be write protected. Alternatively, an internal component such as the key server component returned an error or was not available. This message might provide additional information.

System action:
The operation fails.

Administrator response:
Ensure that the SKLMConfig.properties file is write enabled. If an internal component failed, you might restart the IBM Security Guardium Key Lifecycle Manager server. Then, try the operation again. Additional information in this message might guide your response.

CTGKM0211E Cannot retrieve IBM Security Guardium Key Lifecycle Manager status.

Explanation:
An internal component such as the key server component returned an error or was not available. The SKLMConfig.properties file might be write protected. This message might provide additional information.

System action:
Server status retrieval fails.

Administrator response:
Ensure that the SKLMConfig.properties file is write enabled. You might restart the IBM Security Guardium Key Lifecycle Manager server. Then, try the operation again. Additional information in this message might guide your response.

CTGKM0214E Cannot retrieve key groups.

Explanation:
IBM Security Guardium Key Lifecycle Manager database might not be available. Alternatively, an internal component such as the key server component returned an error or was not available. This message might provide additional information.

System action:
The operation fails.

Administrator response:
Confirm that the database is available. You might need to restart the IBM Security Guardium Key Lifecycle Manager server. Additional information in this message might also guide your response. Make corrections. Then, try the operation again.

CTGKM0215E Cannot create key group.

Explanation:
You might have specified a value that is not valid for a key group. Alternatively, IBM Security Guardium Key Lifecycle Manager database might not be available or an internal component such as the key server component returned an error or was not available.

System action:
The operation fails.

Administrator response:
Ensure that your values for a key group are valid. Ensure that the database is available. If an internal component failed, you might restart the IBM Security Guardium Key Lifecycle Manager server. Then, try the operation again.

CTGKM0216E Cannot modify this key group.

Explanation:
An attempt failed to modify this key group. There might be more information in the message that describes the problem.

System action:
The modification requested for this key group does not occur. No keys are added to or deleted from the key group.

Administrator response:
Additional information might guide your response. Make appropriate changes. Then try the operation again.

CTGKM0217E Cannot delete key group that is a system default, or that is associated with a device or pending device.

Explanation:
IBM Security Guardium Key Lifecycle Manager could not delete a key group that is a system default, or that is associated with a device. There might be additional information in this message.

System action:
The key group is retained in the IBM Security Guardium Key Lifecycle Manager database.

Administrator response:
Ensure that the key group is not the system default, and that the key group also has no associated devices. Additional information in this message might also guide your response. Then, try the operation again.

CTGKM0218E Cannot create the following keys in this key group.

Explanation:
An attempt failed to create keys for this key group. There might be more information in the message that describes the problem.

System action:
The keys are not created, or are not added as members of the key group.

Administrator response:
Additional information might guide your response. Make appropriate changes. Then try the operation again.

CTGKM0219E Because this certificate is currently expired and the validate certificates check is enabled, cannot make this certificate the System Default or System Partner.

Explanation:
The certificate has expired and is no longer available for use.

System action:
The operation fails.

Administrator response:
Select another certificate. This certificate has expired.

CTGKM0220E Cannot retrieve available keys.

Explanation:
An attempt failed to retrieve all available symmetric keys. There might be more information in the message that describes the problem.

System action:
The keys are not found.

Administrator response:
Additional information might guide your response. Make appropriate changes. Then try the operation again.

CTGKM0221E Cannot retrieve keys from key group.

Explanation:
An attempt failed to retrieve keys from a key group. There might be more information in the message that describes the problem.

System action:
The keys are not found.

Administrator response:
Additional information might guide your response. Make appropriate changes. Then try the operation again.

CTGKM0222E Device serial number is not valid *VALUE_0* , must be 12 characters for 3592 and DS8000 device families or 1-48 characters long for DS5000 device family, contain valid characters, and cannot have leading or trailing whitespace.

Explanation:
The device serial number for a device be exactly 12 characters for 3592 and DS8000 device families or 1-48 characters for DS5000 family and follow a specific format.

System action:
The operation fails.

Administrator response:
Ensure that your specification is 12 valid characters in length and contains alphanumeric, period, dash, semicolon, and underscore characters, or a space that is not in the first or last position. Additional information in this message might also guide your response. Correct the problem and try the operation again.

CTGKM0223E Device already exists with device serial number *VALUE_0* , Device group *VALUE_1* *VALUE_2* , World Wide Name

Explanation:
You specified values for a device that already exists in the database.

System action:
The device create operation fails.

Administrator response:
Specify values for a device that does not currently exist in the database. Then, try the operation again.

CTGKM0224E World wide name is not valid *VALUE_0*

Explanation:
IBM Security Guardium Key Lifecycle Manager requires that a worldwide name be 8 characters or less in length.

System action:
The operation fails.

Administrator response:
Specify a worldwide name that meets the length requirement of 8 characters or less. Then, try the operation again.

CTGKM0225E Cannot add device with device serial number *VALUE_0* *VALUE_1* *VALUE_2* because the specified key *VALUE_1* does not exist in keystore *VALUE_2*.

Explanation:
You attempted to create a device and associate it with a key that was not found in the IBM Security Guardium Key Lifecycle Manager keystore.

System action:
The device add operation fails.

Administrator response:
Specify an alternate key. Then, try the operation again.

CTGKM0226E The certificate is not active and cannot be the System Default or System partner certificate.

Explanation:
The validate certificates check is enabled. The process determined that this certificate is not active and cannot be the System Default or System Partner.

System action:
The operation fails.

Administrator response:
Select a certificate that is in active state and try the operation again.

CTGKM0227E Cannot retrieve available key groups.

Explanation:
The key groups information was not available from the database.

System action:
The key groups are not retrieved.

Administrator response:
Ensure that the database is available. Then, try the operation again.

CTGKM0228E Cannot retrieve key information.

Explanation:
An attempt failed to retrieve key information. There might be more information in the message that describes the problem.

System action:
The operation fails.

Administrator response:
Additional information might guide your response. Make appropriate changes. Then try the operation again.

CTGKM0229E Cannot retrieve keys.

Explanation:
An error occurred while retrieving a list of keys. There might be more information in the message that describes the problem.

System action:
The operation fails.

Administrator response:
Additional information might guide your response. Make appropriate changes. Then, try the operation again.

CTGKM0230E Cannot create keys.

Explanation:
An attempt to create a key or keys did not complete. There might be more information in the message that describes the problem.

System action:
The operation fails.

Administrator response:
Additional information might guide your response. Make appropriate changes. Then, try the operation again.

CTGKM0231E Cannot modify key membership.

Explanation:
An attempt to modify key membership did not complete. There might be more information in the message that describes the problem.

System action:
The operation fails.

Administrator response:
Additional information might guide your response. Make appropriate changes. Then, try the operation again.

CTGKM0232E Cannot delete key.

Explanation:
The key that you intend to delete, might not be found, or there might be a database error. There might be more information in the message that describes the problem.

System action:
The key is not deleted.

Administrator response:
Additional information might guide your response. Make appropriate changes. Then, try the operation again.

CTGKM0233E Cannot list backup files.

Explanation:
Cannot retrieve the data for the backup files.

System action:
The list backup files operation fails.

Administrator response:
Check the log entries to find out the reason for the failure. Make appropriate changes. Then, try the operation again.

CTGKM0234E Cannot locate default backup directory.

Explanation:

Cannot read the property value for the backup directory.

System action:
Failed to read backup directory.

Administrator response:
Check the log entries to find out the reason for the failure. Make appropriate changes. Then, try the operation again.

CTGKM0235E Cannot obtain the progress of the running process.

Explanation:
Cannot obtain the progress of the running backup or restore process.

System action:
Failed to get the progress of the running process.

Administrator response:
Check the log entries to find out the reason for the failure. Make appropriate changes. Then, try the operation again.

CTGKM0236E Cannot obtain the progress state of the running process.

Explanation:
Cannot obtain the progress state of the running backup or restore process.

System action:
Failed to get the progress state of the running process.

Administrator response:
Check the log entries to find out the reason for the failure. Make appropriate changes. Then, try the operation again.

CTGKM0237E Cannot obtain the process result of the completed process.

Explanation:
Cannot obtain the process result of the completed backup or restore process.

System action:
Failed to get the process result of the completed process.

Administrator response:
Check the log entries to find out the reason for the failure. Make appropriate changes. Then, try the operation again.

CTGKM0238E Cannot create backup.

Explanation:
Cannot initiate the backup process.

System action:
Failed to initiate the backup process.

Administrator response:
Check the log entries to find out the reason for the failure. Make appropriate changes. Then, try the operation again.

CTGKM0239E Cannot restore from backup.

Explanation:
Cannot initiate the restore from backup process.

System action:
Failed to initiate the restore from backup process.

Administrator response:
Check the log entries to find out the reason for the failure. Make appropriate changes. Then, try the operation again.

CTGKM0240E Cannot delete backup.

Explanation:
Cannot delete the backup process.

System action:
Failed to delete the backup process.

Administrator response:
Check the log entries to find out the reason for the failure. Make appropriate changes. Then, try the operation again.

CTGKM0242E Failed to create backup to *backup_file* .

Explanation:
Cannot back up the IBM Security Guardium Key Lifecycle Manager system.

System action:
Backup operation failed to back up the IBM Security Guardium Key Lifecycle Manager system.

Administrator response:
Check the log entries to find out the reason for the failure. Make appropriate changes. Then, try the operation again.

CTGKM0244E Failed to restore from *backup_file* .

Explanation:
Cannot restore the IBM Security Guardium Key Lifecycle Manager system.

System action:
Restore operation failed to restore the IBM Security Guardium Key Lifecycle Manager system.

Administrator response:
Check the log entries to find out the reason for the failure. Make appropriate changes. Then, try the operation again.

CTGKM2912W Import failed due to conflict arose because of <Variable_IDs/Aliases>.

Explanation:
For a successful import, follow the resolution process.

CTGKM0245E The key name specified is not known.

Explanation:
You might have incorrectly specified the key name value. Alternatively, IBM Security Guardium Key Lifecycle Manager database might not be available or an internal component such as the key server component returned an error or was not available.

System action:
The operation fails.

Administrator response:
Ensure that your value for a key name is valid and is in the keystore. Ensure that the database is available. If an internal component failed, you might restart the IBM Security Guardium Key Lifecycle Manager server. Then, try the operation again.

CTGKM0246E Cannot identify the next key to be used from this key group.

Explanation:
An attempt failed to determine the next key to be used from this key group. There might be more information in the message that describes the problem.

System action:
The operation fails.

Administrator response:
Additional information might guide your response. Make appropriate changes. Then try the operation again.

CTGKM0247E Cannot retrieve future write defaults.

Explanation:
An error occurred while retrieving a list of future write defaults. There might be more information in the message that describes the problem.

System action:
The operation fails.

Administrator response:
Additional information might guide your response. Make appropriate changes. Then, try the operation again.

CTGKM0248E Cannot retrieve current system default.

Explanation:
An internal component such as the key server component returned an error or was not available. The SKLMConfig.properties file might be write protected. This message might provide additional information.

System action:
System default retrieval fails.

Administrator response:
Ensure that the SKLMConfig.properties file is write enabled. You might restart the IBM Security Guardium Key Lifecycle Manager server. Then, try the operation again. Additional information in this message might guide your response.

CTGKM0249E Cannot add future write default.

Explanation:
You might have specified a value that is not valid for a future write default. Alternatively, IBM Security Guardium Key Lifecycle Manager database might not be available or an internal component such as the key server component returned an error or was not available.

System action:
The operation fails.

Administrator response:
Ensure that your values for a future write default are valid. Ensure that the database is available. If an internal component failed, you might restart the IBM Security Guardium Key Lifecycle Manager server. Then, try the operation again.

CTGKM0250E Cannot delete future write default.

Explanation:
IBM Security Guardium Key Lifecycle Manager could not delete a future write default. There might be additional information in this message.

System action:
The future write default is retained in the IBM Security Guardium Key Lifecycle Manager database.

Administrator response:
Additional information in this message might guide your response. Make appropriate changes. Then, try the operation again.

CTGKM0251E Future write default's effective date cannot be later than the certificate expiration date.

Explanation:
If the certificate expires before the future write default's effective date, then this future write default will not be effective.

System action:
Adjust the future write default's effective date.

Administrator response:
Extend the certificate expiration date if necessary.

CTGKM0252E Algorithm type for *backup_file* application is not valid.

Explanation:
This is not a valid algorithm type for the intended application. For IKEV2SERVER and IKVE2CLIENT, the only algorithm type supported is ECDSA. Cannot import this key or certificate for this application.

System action:
Import operation fails.

Administrator response:
Generate an ECDSA type of certificate or key for IKVE2SERVER or IKEV2CLIENT and then try the import operation.

CTGKM0253E Device serial number for LTO base device *VALUE_0* must be either 10, 12 or 24 characters long, contain valid characters, and cannot have leading or trailing whitespace.

Explanation:
The device serial number for a device must be either 10, 12 or 24 characters in length and contain only allowed characters.

System action:
The operation fails.

Administrator response:
Ensure that the device serial number you enter is 10, 12 or 24 valid characters in length and contains alphanumeric, period, dash, semicolon, and underscore characters, or a space that is not in the first or last position. Additional information in this message might also guide your response. Correct the problem and try the operation again.

CTGKM0255E Cannot delete key. Key is the last active member of a device.

Explanation:
The current active member key of a device or group cannot be deleted.

System action:
The key is not deleted.

Administrator response:
Additional information might guide your response. Make appropriate changes. Then, try the operation again.

CTGKM0256E Incorrect key size *VALUE_0*.

Explanation:
This is not a valid key size type for the intended application. For IKEV2SERVER and IKVE2CLIENT, the only key size supported is 521 bits. Cannot import this key or certificate for this application.

System action:
Import operation fails.

Administrator response:
Generate correct size of ECDSA type of certificate or key for IKVE2SERVER or IKEV2CLIENT and then try the import operation.

CTGKM0257E Unable to accept the Pending Client Device Communication Certificate.

Explanation:
The certificate name might already exist, the certificate material might already exist under a different name, or the IBM Security Guardium Key Lifecycle Manager database might not be available. There might be additional information.

System action:
Accept operation fails.

Administrator response:
Determine if you specified a unique certificate name. Alternatively, you might need to confirm that the database is available. Additional information in this message might also guide your response. Make corrections. Then, try the operation again.

CTGKM0258E Unable to reject the Pending Client Device Communication Certificate.

Explanation:
The certificate might not exist, or the IBM Security Guardium Key Lifecycle Manager database might not be available. There might be additional information.

System action:
Reject operation fails.

Administrator response:
Refresh the page to determine if the certificate still exists in the pending list. Alternatively, you might need to confirm that the database is available. Additional information in this message might also guide your response. Make corrections. Then, try the operation again.

CTGKM0259E Unable to gather additional information on the selected Pending Client Device Communication Certificate.

Explanation:
The certificate information was not available from the database.

System action:
View operation fails.

Administrator response:
Ensure that the IBM Security Guardium Key Lifecycle Manager database is available. Correct any database server runtime errors that you identify. Then, try the operation again.

CTGKM0260E Keystore internal error occurred.

Explanation:
An internal error occurred while creating or loading the keystore.

System action:
Keystore operation fails.

Administrator response:

Verify that IBM Security Guardium Key Lifecycle Manager is initialized correctly.

CTGKM0261E Alias {0} already exists.

Explanation:

System action:
Keystore operation fails.

Administrator response:
Specify a different alias.

CTGKM0262E The certificate expiration period cannot be later than *VALUE_0* years. This value can be changed by use of the configuration parameter called maximum.keycert.expiration.period.in.years.

Explanation:
The certificate expiration period cannot be later than the configured years. This value can be changed by use of the configuration parameter called maximum.keycert.expiration.period.in.years.

System action:
Adjust the maximum.keycert.expiration.period.in.years if necessary.

Administrator response:
Adjust the maximum.keycert.expiration.period.in.years if necessary.

CTGKM0263E You have successfully restored your system from *backup_file* You will be required to manually restart the server as automatic restart failed. Please refer to the Backup and restore section of IBM Security Guardium Key Lifecycle Manager documentation, on how to start and stop the server on distributed systems.

Explanation:
Backup was successfully restored but restart failed.

System action:

Administrator response:

CTGKM0400E You must specify a value for: *VALUE_0*

Explanation:
You attempted to update a key value, but you specified a null parameter.

System action:
The key is not updated.

Administrator response:
Enter a valid parameter value and try the update operation again.

CTGKM0401E The alias name prefix (3 characters) is not alphabetic: *VALUE_0*

Explanation:
An alias prefix for a key must be three characters in length, and the characters must be alphabetic, which are the characters A-Z case insensitive.

System action:
The key or keys are not created.

Administrator response:
Specify a three character value for the key alias using the alphabetic characters A-Z, which are case insensitive.

CTGKM0402E The alias range (*VALUE_0* , *VALUE_1*) is not valid.

Explanation:
The first hexadecimal number in an alias range must smaller than the last hexadecimal number that you specify.

System action:
The keys are not created in the specified range.

Administrator response:
Ensure that the values that you specified for the alias range are valid hexadecimal numbers, and that the initial number is less than the final number in the range. For example, specify a range such as xyz01-fff. Then, try the operation again.

CTGKM0403E The alias does not contain all alphabetic characters: *VALUE_0*

Explanation:
The alias value must contain only alphabetic characters.

System action:
The key or keys are not created.

Administrator response:
Ensure that the value that you specified for the key alias contains only alphabetic characters. Then, try the operation again.

CTGKM0404E The alias range length is too large.

Explanation:
The alias range that you specified exceeds a IBM Security Guardium Key Lifecycle Manager limit.

System action:
The key or keys are not created.

Administrator response:
Specify a smaller alias range. Then, try the operation again.

CTGKM0405E The alias range end value must be greater than or equal to the alias range start value.

Explanation:
The last hexadecimal number in an alias range must greater than or equal to the first hexadecimal number that you specify.

System action:
The keys are not created in the specified range.

Administrator response:
Ensure that the values that you specified for the alias range are valid hexadecimal numbers, and that the final number is greater than or equal to the initial number in the range. For example, specify a range such as xyz01-fff. Then, try the operation again.

CTGKM0406E The alias range is too large.

Explanation:
The alias range that you specified exceeds a IBM Security Guardium Key Lifecycle Manager limit.

System action:
The keys are not created in the specified range.

Administrator response:
Specify a smaller alias range. Then, try the operation again.

CTGKM0407E The alias range string contains a non-hexadecimal value.

Explanation:
The numbers that specify an alias range must be hexadecimal numbers.

System action:
The keys are not created in the specified range.

Administrator response:
Specify an alias range using only hexadecimal values. Then, try the operation again.

CTGKM0408E Cannot locate certificate chain with alias *VALUE_0*

Explanation:
The alias that you specified for a certificate does not contain a certificate chain.

System action:
The operation fails.

Administrator response:
Ensure that the alias that you specified contains a certificate chain. Then, try the operation again.

CTGKM0409E Check the file name. Cannot export the key to *VALUE_0* .

Explanation:
There is a write error to the file on which an export operation was attempted. There is possibly an error in the relative or full path, or the name of the file that IBM Security Guardium Key Lifecycle Manager creates to store private keys.

System action:
The key is not exported.

Administrator response:
Ensure that you correctly specified the relative or full path, and the name of the file to store the exported keys. If you do not specify a path name, the value of the *SKLM_HOME* directory is used. Then, try the operation again.

CTGKM0410E Error occurred while exporting the key to output stream.

Explanation:
The certificate export operation did not write to the file on which an export operation was attempted. There is possibly an error in the relative or full path, or the name of the file that IBM Security Guardium Key Lifecycle Manager creates to store the certificate.

System action:
The certificate is not exported.

Administrator response:
Ensure that the path and file name are correct. Then, try the operation again.

CTGKM0411E *VALUE_0* is not a secret key entry in the keystore.

Explanation:
The specified secret key is not in the keystore.

System action:
An operation fails, such as exporting a secret key.

Administrator response:
You might use the tklmKeyList command to view the keys contained in the keystore. Correct any errors in your specification. Then, try the operation again.

CTGKM0412E *VALUE_0* is not a private key entry in the keystore.

Explanation:
The specified private key is not in the keystore.

System action:
The operation fails, such as exporting a private key to a PKCS12 file.

Administrator response:
You might use the tklmKeyList command to view the private keys contained in the keystore. Correct any errors in your specification. Then, try the operation again.

CTGKM0413E Unsupported private key algorithm: *VALUE_0*

Explanation:

This is not one of the key algorithms that IBM Security Guardium Key Lifecycle Manager supports.

System action:
The key operation fails. For example, you might be trying to import a private key that does not match a supported RSA or DSA algorithm.

Administrator response:
Use a different key that complies with an asymmetric key algorithm that IBM Security Guardium Key Lifecycle Manager supports.

CTGKM0414E File size is zero.

Explanation:
The specified key file is empty, from which you are attempting to import a key. There is no data in the file.

System action:
The operation fails.

Administrator response:
Ensure that the key file is correctly populated, and that you have a valid key file from a trusted source. Then, try the operation again.

CTGKM0415E Cannot find the file *VALUE_0*

Explanation:
The key file was not found during a key import operation.

System action:
The key import operation fails.

Administrator response:
Ensure that you specified the correct path and filename. Then, try the operation again.

CTGKM0416E Cannot find the *VALUE_0* in the specified group.

Explanation:
The group member that you specified is not in the target group.

System action:
The operation fails.

Administrator response:
Ensure that your specifications of both the group member and the group are correct. You might first need to add the member to the group. Then, try the operation again.

CTGKM0417E Cannot delete a key from a device group.

Explanation:
The database stores group entries for keys in a key group type of group.

System action:
The group entry delete operation fails.

Administrator response:
Change your specification of the group type to a value of key group. Then, try the operation again.

CTGKM0419E Entry *VALUE_0* does not belong to any group.

Explanation:
The database stores entries in a group with a type of key group. The entry that you are attempting to delete was not found in any type of group.

System action:
The operation fails.

Administrator response:
Ensure that your specification of the entry uuid and the group name are correct. Then, try the operation again.

CTGKM0420E Key group is empty.

Explanation:
There are no keys in the group. This is an internal message that the key server might issue to a log.

System action:
The key operation fails.

Administrator response:
You might need to add keys to the key group.
The change is effective immediately. However, you might need to restart the IBM Security Guardium Key Lifecycle Manager server. Then, try the operation again.

CTGKM0421E Error occurred while encrypting the key.

Explanation:
Encryption failed during a secret key export operation to a file. There might be a problem with the encryption provider.

System action:
The export operation fails.

Administrator response:
Collect any information that might be in the audit log. You might need to contact IBM Support.

CTGKM0422E Error occurred while encoding data in PKCS12 format.

Explanation:
An exception occurred in internal processes.

System action:
The private key and certificate are not encoded.

Administrator response:
Collect any information that might be in the audit log and contact IBM Support.

CTGKM0423E Error occurred while verifying the key and certificate.

Explanation:
An exception occurred in internal processes.

System action:
The certificate request that you submitted to a CA and the certificate that returned, do not match. This might be an internal processing error.

Administrator response:
Collect any information that might be in the audit log and contact IBM Support.

CTGKM0424E Error occurred while decrypting the secret key.

Explanation:
An exception occurred in internal processes.

System action:
The secret key was not decrypted. This might be an internal processing error.

Administrator response:
Collect any information that might be in the audit log and contact IBM Support.

CTGKM0425E The alias prefix does not have 3 characters.

Explanation:
An alias prefix for a key must be 3 characters in length, and the characters must be alphabetic.

System action:
The key or keys are not created.

Administrator response:
Ensure that the value that you specified for the key alias contains 3 alphabetic characters. Then, try the operation again.

CTGKM0426E Cannot delete the certificate as it is associated with a private key entry.

Explanation:
You used the tklmCertDelete command to delete a certificate that has a private key associated with the certificate.

System action:
The certificate was not deleted.

Administrator response:
Use the tklmKeyDelete command to delete the key. The alias for the certificate and the key are the same, and are stored internally as a single entry.

CTGKM0427E Group name is longer than 64 characters: *VALUE_0*

Explanation:
The limit for a group name is 64 characters.

System action:
The operation fails.

Administrator response:
Specify a shorter group name that meets the character limit. Then, try the operation again.

CTGKM0428E Default key group cannot be deleted.

Explanation:
One or more devices use this key group as the default from which to obtain keys.

System action:
The key group delete operation fails.

Administrator response:
Ensure that no device uses this key group as the default from which to obtain keys. You might select another key group as the default. Then, try the operation again.

CTGKM0429E Alias range does not start with 3-letter prefix.

Explanation:
The alias range prefix must be 3 characters in length.

System action:
The operation fails.

Administrator response:
Specify a prefix that contains 3 characters for the alias range. Then, try the operation again.

CTGKM0430E Alias range does not have a hexdecimal range separated by dash.

Explanation:
A dash is the required separator between hexadecimal numbers in an alias range.

System action:
The range of keys is not created.

Administrator response:
Specify the alias range using a dash as the separator. Then, try the operation again.

CTGKM0431E Starting with version 2, this message is deprecated. aliasOne attribute must be specified for DS8000® device.

Explanation:
Starting with version 2, this message is deprecated. aliasOne is the required attribute for DS8000 device.

System action:
The device is not created.

Administrator response:
Specify the aliasOne attribute. Then, try the operation again.

CTGKM0432E Rollover task for type *VALUE_0* is already scheduled on effective date: *VALUE_1*

Explanation:
Effective date is unique for each rollover type

System action:
The rollover is not created.

Administrator response:
Specify different rollover date and type. Then, try the operation again.

CTGKM0433E Two-letter country code: *VALUE_0* is not valid.

Explanation:
The specified value does not have 2 letters.

System action:
The certificate or certificate request command fails.

Administrator response:
Specify a different country code. Then, try the command again.

CTGKM0434E Cannot delete the key because it is the default symmetric key: *VALUE_0*

Explanation:
The specified key is a default symmetric key.

System action:
The delete operation failed.

Administrator response:
Specify a different key and try the delete operation again.

CTGKM0435E All keys in the key group are used. There is no key available to use.

Explanation:
All keys in the key group are used. There is no key available to use.

System action:
The operation to get the next key failed

Administrator response:
Add a new key to the key group and try to get a key again.

CTGKM0436E The key group cannot be deleted, but the key group members are deleted successfully.

Explanation:
The key group is not deleted.

System action:
The key group delete operation failed.

Administrator response:
Examine the logs for information about the error. Make necessary corrections. Then, try the operation again. If the problem still exists, you might need to contact IBM Support.

CTGKM0437E The key group cannot be deleted, but some members may have been deleted.

Explanation:
The key group is not deleted.

System action:
The key group delete operation failed.

Administrator response:
Examine the logs for information about the error. Make necessary corrections. Then, try the operation again. If the problem still exists, you might need to contact IBM Support.

CTGKM0438E The last key in the default key group cannot be deleted.

Explanation:
The key is not deleted.

System action:
The key delete operation fails.

Administrator response:
The default key group needs to include at least one key.

CTGKM0439E Cannot delete the last key in the key group that is associated with a device.

Explanation:
The key is not deleted.

System action:
The key delete operation fails.

Administrator response:
The key group associated with a device needs to include at least one key.

CTGKM0440E Cannot delete the last key in the key group *VALUE_0* that is associated with a scheduled rollover.

Explanation:
The key is not deleted.

System action:
The key delete operation fails.

Administrator response:
The key group associated with a rollover need to have at least one key.

CTGKM0500E A keystore already exists in IBM Security Guardium Key Lifecycle Manager.

Explanation:
Only one IBM Security Guardium Key Lifecycle Manager keystore can exist.

System action:
The keystore add operation fails.

Administrator response:
Use the existing IBM Security Guardium Key Lifecycle Manager keystore. You cannot add an additional keystore. If you must use a new keystore, you must first remove the existing keystore and add a new one. In a running production environment, do not modify the keystore name. If you must modify the keystore name prior to production, ensure that you have a complete, current backup of your IBM Security Guardium Key Lifecycle Manager configuration.

CTGKM0501E No password.

Explanation:
You must specify a password for a IBM Security Guardium Key Lifecycle Manager keystore. The password must at least 6 characters in length.

System action:
The keystore operation fails.

Administrator response:
Specify a password for the IBM Security Guardium Key Lifecycle Manager keystore. For example, type a value such as my6pwd.

CTGKM0502E Keystore name must be specified.

Explanation:
You must specify a name for a IBM Security Guardium Key Lifecycle Manager keystore. IBM Security Guardium Key Lifecycle Manager uses this name in the database as a descriptive alias to identify the keystore.

System action:
The keystore operation fails.

Administrator response:
Specify a name as a descriptive alias for the IBM Security Guardium Key Lifecycle Manager keystore. For example, type `mySKLMKeystore`.

CTGKM0503E Duplicate keystore name.

Explanation:
A duplicate name exists in the database for the value that you specified as a descriptive alias for an IBM Security Guardium Key Lifecycle Manager keystore.

System action:
The keystore operation fails.

Administrator response:
Type a unique value for the name of the IBM Security Guardium Key Lifecycle Manager keystore. For example, type `mySKLMKeystore`.

CTGKM0504E Error occurred while creating the keystore:

Explanation:
You might not have correctly specified the values needed to add a file-based keystore.

System action:
The keystore operation fails.

Administrator response:
Ensure that you specified a unique value for the descriptive alias, the path and file name of the keystore, or the keystore type. For a RACF® keystore, you might have to specify the user ID or password differently. After modifying your entries, try the operation again.

CTGKM0505E Error occurred while loading the keystore:

Explanation:
This error occurs when you attempt to read data from an existing keystore.

System action:
The keystore operation fails.

Administrator response:
The data in the keystore might be corrupt, or the path specification or password value might be incorrect. If the keystore is corrupt, use a backup copy. Otherwise, respecify the path or password values, and try the operation again.

CTGKM0506E Internal database operation error.

Explanation:
An unexpected database error occurred.

System action:
The database operation did not complete as expected.

Administrator response:
Collect any information that might be in the audit log and contact IBM Support.

CTGKM0507E Validation error on input:

Explanation:
The value that you provided did not match an expected value.

System action:
The value was not written or retained.

Administrator response:
Ensure that the value you provided is valid. Then, try the operation again.

CTGKM0508E Failed to execute the command:

Explanation:
There is an error in the values provided for the tklmKeyStoreList command.

System action:
The command operation fails.

Administrator response:

Ensure that the command syntax and values are correct. Then, try the command again.

CTGKM0509E Password cannot be shorter than 6 characters.

Explanation:
The password strength rule requires a length of six or more characters.

System action:
The keystore operation fails.

Administrator response:
Specify a password that is at least six characters in length, and then try the operation again.

CTGKM0510E Keystore file path name is not specified.

Explanation:
You must specify a complete path to the keystore file.

System action:
The keystore operation fails.

Administrator response:
Specify a complete path to the keystore file, either as an absolute or relative path. Then, try the operation again. As a relative path, for example, you might specify a file name in an existing directory. IBM Security Guardium Key Lifecycle Manager appends the value of *SKLM_HOME* as the relative path.

CTGKM0511E User name is not specified.

Explanation:
You must specify a user name, which is required for a RACF type keystore.

System action:
The keystore operation fails.

Administrator response:
Specify the user ID that has authority to use the RACF keystore. Then, try the operation again.

CTGKM0512E Keystore type is not valid *KEYSTORE_TYPE*

Explanation:
You must specify a keystore type that IBM Security Guardium Key Lifecycle Manager supports.

System action:
The keystore operation fails.

Administrator response:
Specify a supported keystore type. Then, try the operation again.

CTGKM0513E Cannot find MBean:

Explanation:
This error might occur if you install IBM Security Guardium Key Lifecycle Manager and then move or delete some of its files.

System action:
Internal descriptive files are not found.

Administrator response:
Do not move or delete files from their installed locations without explicit, authorized instructions. You might need to contact IBM Support.

CTGKM0514E Target application usage must be specified.

Explanation:
Usage specifies how the certificate is used with a target application, either for secure communication using a TLS server protocol, or for communication with a device.

System action:
The certificate operation fails.

Administrator response:
Specify a valid value for the certificate usage. Then, try the operation again.

CTGKM0515E Certificate name must be specified.

Explanation:
The name uniquely identifies the certificate within the keystore.

System action:
The certificate operation fails.

Administrator response:
Specify the name for the certificate. Then, try the operation again.

CTGKM0516E Common name must be specified.

Explanation:
The common name (cn) is part of the unique identification for the certificate. For example, the value of cn is used in the subject name for a certificate, which can identify whether a certificate that is being imported matches an original certificate request.

System action:
The operation fails.

Administrator response:
Specify the common name for the certificate. Then, try the operation again.

CTGKM0517E Cannot form a valid X.500 name.

Explanation:
One or more of the values for the subject fields is not valid to generate a valid X.500 directory name, which must be unique to identify a self-signed certificate as an entry for a global directory service.

System action:
The X.500 name is not created.

Administrator response:

Ensure that you provided correct values for the subject fields that comprise an X.500 name, such that a certificate can be unambiguously identified. For example, ensure that the value for the cn field is unique, and that values are also complete in other fields.

CTGKM0518E Keystore does not exist.

Explanation:
A keystore must exist to contain the certificate. You might have entered an incorrect keystore name, or used a command that requires a value for the keystore, before creating the keystore.

System action:
The certificate operation fails.

Administrator response:
Specify a valid, existing keystore. You might need to create a keystore using either the tklmKeystoreAdd command, or the graphical user interface. Then, try the operation again.

CTGKM0520E Not the supported usage: *VALUE_0*

Explanation:
You specified an unsupported value for the target usage. The target application specifies how the certificate is used, either for secure communication using a TLS protocol, or for communication with a device such as a tape drive.

System action:
The certificate operation fails.

Administrator response:
Specify a valid target application for which the certificate is used. Then, try the operation again.

CTGKM0521E Unsupported certificate format: *VALUE_0*

Explanation:
You specified an value that is not valid for the certificate format. IBM Security Guardium Key Lifecycle Manager supports either a base64 and DER format for certificates.

System action:
The certificate operation fails.

Administrator response:
Specify either base64 or DER as the certificate format. Then, try the operation again.

CTGKM0522E No certificate information.

Explanation:
During a certificate operation, the certificate information was missing or null.

System action:
The certificate import operation fails.

Administrator response:
Ensure that you identified the certificate with a valid name. For example, run the tklmCertList command to find the certificate name. Then, try the operation again.

CTGKM0523E No keystore information.

Explanation:
During a certificate import or keystore delete operation, the keystore parameter was null. The value of the keystore is missing.

System action:
The certificate operation fails.

Administrator response:
Determine whether you identified the keystore with a valid name. For example, run the tklmKeystoreList command to find the keystore name. Then, try the operation again.

CTGKM0524E Keystore name or uuid must be specified.

Explanation:
During a certificate import or keystore delete operation, the keystore parameter was null. The value of the keystore is missing.

System action:
The certificate operation fails.

Administrator response:
Determine whether you identified the keystore with a valid name. For example, run the tklmKeystoreList command to find the keystore name. Then, try the operation again.

CTGKM0525E Parameter value(s) are not valid.

Explanation:
During general validation, at least one value was not found for a required parameter for the tklmCertCreate or tklmCertUpdate command.

System action:
The certificate operation fails.

Administrator response:
Specify the missing value or values. Then, try the operation again.

CTGKM0526E Certificate file name must be specified.

Explanation:
A certificate file name must be specified for the tklmCertExport or the tklmCertImport command.

System action:
The certificate operation fails.

Administrator response:
Specify the file name of the certificate. Then, try the operation again.

CTGKM0527E Certificate validity value *VALUE_0* is not valid

Explanation:
The length of time in days that you specified for the certificate does not fall within the expected range. The value must be 1 or greater.

System action:
The certificate operation fails.

Administrator response:
Specify a valid length of time in days during which the certificate can be used. Then, try the operation again.

CTGKM0528E Keystore name cannot exceed 64 characters.

Explanation:
For the tklmKeystoreAdd command, you specified a keystore name that exceeds a limit of 64 characters.

System action:
The certificate operation fails.

Administrator response:
Specify a keystore name that is 64 characters or less in length. Then, try the operation again.

CTGKM0529E An error occurred generating certificate request.

Explanation:
An exception occurred in internal processes.

System action:
The certificate request is not created.

Administrator response:
Verify the parameter values for the certificate request. Then, try the operation again.

CTGKM0530E Cannot find the certificate.

Explanation:
The value of the alias or uuid was not found when you attempted an operation such as deleting, exporting, or updating a certificate.

System action:
The certificate operation fails.

Administrator response:
Specify a valid alias or uuid for the target certificate. Then, try the operation again.

CTGKM0531E uuid must be specified.

Explanation:
A value is required for the uuid parameter for a delete operation.

System action:
The group delete operation fails.

Administrator response:
Ensure that you specified the correct value for the uuid of the group. You might use the tklmGroupList command to verify values. Then, try the operation again.

CTGKM0532E Compromise date cannot be later than today.

Explanation:
The date on which you specify that a key or a certificate is compromised cannot be a future date.

System action:
The operation fails.

Administrator response:
Specify a date that is not in the future, and then try the operation again.

CTGKM0533E Activation date, retirement date, expiration date and destroy date are not synchronized.

Explanation:
There is a mismatch in dates between several parameters, which must follow each other in time. A destroy date value must occur after an expiration date value, for example.

System action:
The update certificate operation fails.

Administrator response:
Enter values for dates that do not conflict in their sequence on the calendar. Then, try the operation again.

CTGKM0534E Cannot reset activation date, old activation date has passed:

Explanation:
If the date of activation is older than the current date, you cannot reset a new value for activation.

System action:
The operation fails.

Administrator response:
Use a different certificate. The activation date of this certificate cannot be reset.

CTGKM0535E Cannot reset retirement date, old retirement date has passed:

Explanation:
If the date of retirement is older than the current date, you cannot reset a new value for retirement.

System action:
The operation fails.

Administrator response:
Use a different certificate. This certificate is retired, and the retirement date cannot be reset.

CTGKM0536E Cannot reset destroy date, old destroy date has passed:

Explanation:
If the destroy date is older than the current date, you cannot reset a new value for the destroy date.

System action:
The operation fails.

Administrator response:
Use a different certificate. The destroy date of this certificate cannot be reset.

CTGKM0537E Cannot set state to be *VALUE_0* , current state is *VALUE_1* .

Explanation:
The current state of the certificate cannot be reset to the state that you specified. For example, you cannot set the state of an active certificate to a pre-active state.

System action:
The operation fails.

Administrator response:
Specify a different state for the certificate. Then, try the operation again.

CTGKM0538E Error setting new state: *VALUE_0* , certificate is already compromised.

Explanation:
A certificate that is in a compromised state cannot be set to an earlier state.

System action:
The operation fails.

Administrator response:
Specify a subsequent state. Then, try the operation again. Alternatively, you might need to use an uncompromised certificate.

CTGKM0539E Error setting new state: *VALUE_0* , certificate is not compromised.

Explanation:
A certificate must be in a compromised state before a subsequent state can be set.

System action:
The operation fails.

Administrator response:
First, change the state of the certificate to compromised. Then, try the operation again.

CTGKM0540E Certificate with alias *VALUE_0* already exists in keystore.

Explanation:
There is already a certificate in the keystore with the same alias as the one you are attempting to import.

System action:
The operation fails.

Administrator response:
Specify a different alias. Then, try the operation again.

CTGKM0541E uuid and certificate attributes must be specified.

Explanation:
There might be an error in the uuid value for a certificate.

System action:
The operation fails.

Administrator response:
Ensure that the uuid value of the certificate is valid. Then, try the operation again.

CTGKM0542E Not a valid encoded certificate file. Make sure to use the right file and it is not tampered or corrupted.

Explanation:
The import operation determined that the certificate file is not correctly encoded. It must be DER or base64 format.

System action:
The operation fails.

Administrator response:
Specify a certificate that has a DER or base64 format. Then, try the operation again.

CTGKM0543E An error occurred importing certificate: {0}

Explanation:
The certificate file might not exist, or you might have made an error in specifying the file name of the certificate.

System action:
The operation fails.

Administrator response:
Determine whether the certificate path and file name are correct, and whether the file is corrupt. Correct the problems. Then, try the operation again.

CTGKM0544E Cannot retrieve the certificate from keystore.

Explanation:
Your entries might have an error in specifying the certificate alias. Alternatively, the keystore might not contain the target certificate.

System action:
The operation fails.

Administrator response:
Determine whether you specified the certificate alias correctly. Alternatively, you might use the

tklmKeystoreList command to determine which certificates the keystore contains. Then, try the operation again.

CTGKM0545E An error occurred exporting certificate.

Explanation:
The file that you specified might be read-only, or you do not have permission to write the file to a specific location.

System action:
The export operation fails.

Administrator response:
Ensure that the file is write enabled, and that your permissions are valid. Then, try the export operation again.

CTGKM0546E Expiration date cannot be early than activation date: *VALUE_0*

Explanation:
The expiration date of a certificate must occur later in time than the activation date.

System action:
The operation fails.

Administrator response:
Specify an expiration date that is later than the activation date. Then, try the operation again.

CTGKM0547E Expiration date cannot be later than retirement date: *VALUE_0*

Explanation:
The expiration date of a certificate must occur earlier in time than the retirement date.

System action:
The operation fails.

Administrator response:
Specify an expiration date that is earlier than the retirement date. Then, try the operation again.

CTGKM0548E Expiration date cannot be later than destroy date: *VALUE_0*

Explanation:
The expiration date of a certificate must occur earlier in time than the destroy date.

System action:
The operation fails.

Administrator response:
Specify an expiration date that is earlier than the destroy date. Then, try the operation again.

CTGKM0549E Subject name of the certificate does not match subject name in certificate request.

Explanation:
The subject name of the certificate that returned from a Certificate Authority does not match the subject name in the original certificate request.

System action:
The import operation fails.

Administrator response:
Correct the file name or alias specification. Then, try the operation again.

CTGKM0550E Input value cannot be an empty string for parameter *VALUE_0* .

Explanation:
The entry for the attribute name must not be blank or a space.

System action:
The operation fails.

Administrator response:
Specify one or more valid characters for this entry. Then, try the operation again.

CTGKM0551E Cannot find keystore provider for keystore type *VALUE_0*

Explanation:
The keystore type does not match the set of supported providers.

System action:
The operation fails.

Administrator response:
Specify a supported keystore type. Then, try the operation again.

CTGKM0552E *VALUE_0* type keystore is not supported.

Explanation:
The keystore type is not in the set of supported providers.

System action:
The operation fails.

Administrator response:
Specify a supported keystore type. Then, try the operation again.

CTGKM0553E Cannot load *VALUE_0* keyring.

Explanation:
This error occurs when a problem is encountered attempting to load data from a SAF keyring.

System action:
The keystore load operation fails.

Administrator response:
The data in the SAF keyring might be corrupt, or the permissions to the SAF keyring, or the SAF keyring name might be incorrect. Respecify the keyring name

and verify the SAF permissions. Then, try the operation again.

CTGKM0554E Cannot generate *VALUE_0* keyring.

Explanation:
This error occurs when a problem is encountered when you attempt to create a new SAF keyring. The permissions to create the SAF keyring are incorrect, or the SAF keyring name is not correct.

System action:
The keystore store operation fails.

Administrator response:
Respecify the keyring name and verify the SAF permissions. Then, try the operation again.

CTGKM0555E Default property cannot be deleted: *VALUE_0*

Explanation:
You attempted to delete a property from the SKLMConfig.properties file that IBM Security Guardium Key Lifecycle Manager uses as a default property.

System action:
The configuration operation fails.

Administrator response:
Ensure that the property you intend to delete is a customized property, or a property other than a default property. Then, try the delete operation again.

CTGKM0556E Cannot find the property in configuration file: *VALUE_0*

Explanation:
Using the tkmlConfigDeleteEntry command, you attempted to delete a property that does not exist in the properties file.

System action:
The configuration operation fails.

Administrator response:
Ensure that the property exists. You might use the tklmConfigList command to list the contents of the IBM Security Guardium Key Lifecycle Manager configuration file. Specify the target property and try the delete operation again.

CTGKM0557E Cannot delete config.keystore.name property in configuration file

Explanation:
You attempted to delete the config.keystore.name property from the SKLMConfig.properties file. IBM Security Guardium Key Lifecycle Manager must use this property to identify the keystore.

System action:
The configuration operation fails.

Administrator response:
You might change the value of the config.keystore.name property, but you cannot delete the property itself. In a running production environment, do not modify the keystore name. If you must modify the keystore name prior to production, ensure that you have a complete, current backup of your IBM Security Guardium Key Lifecycle Manager configuration.

CTGKM0558E Keystore named *KEYSTORE_NAME* cannot be found. Another user may have renamed the keystore. Try the operation again.

Explanation:
While specifying a tklmKeystoreUpdate or tklmKeystoreDelete command, you did not specify the correct value for the storeName parameter to identify the existing IBM Security Guardium Key Lifecycle Manager keystore.

System action:
The operation fails.

Administrator response:
Specify the correct value for the existing keystore. In the SKLMConfig.properties file, the config.keystore.name property specifies the value of the IBM Security Guardium Key Lifecycle Manager keystore. You might also run the tklmKeyStoreList command to identify the keystore name.

CTGKM0559E Group name and type must be specified.

Explanation:
The group name is missing, or the group type is not valid.

System action:
The operation fails.

Administrator response:
Specify a value for the group name and a valid group type. Then, try the operation again.

CTGKM0560E *VALUE_0* cannot be null.

Explanation:
A value other than a space or blank is required.

System action:
The operation fails.

Administrator response:
Specify a supported value that is not a blank or a space. Then, try the operation again.

CTGKM0561E Unsupported group type: *VALUE_0*

Explanation:
The value that you specified for the group type is not supported.

System action:
The operation fails.

Administrator response:
Specify a supported value for a group type, such as keygroup. Then, try the operation again.

CTGKM0562E Cannot find the group: *VALUE_0*

Explanation:
The value of the group name that you specified does not match an existing group. The group name might be incorrect, or the group might not exist in the type of group that you specified.

System action:
The operation fails.

Administrator response:
Specify a group that exists in the group type that you intend to use. You might use the tklmGroupList command to verify that the group exists in an intended type. Then, try the operation again.

CTGKM0563E Cannot add a key to a device group.

Explanation:
The value of the group type is incorrect.

System action:
The operation fails.

Administrator response:
Specify keygroup as the group type. Then, try the operation again.

CTGKM0564E Cannot identify the entry: *VALUE_0*

Explanation:
The value of the entry that you specified does not match an existing certificate, key, or device. The certificate, key, or device identifier might be incorrect, or the identifier might not exist in the entry type that you specified.

System action:
The operation fails.

Administrator response:
Specify an entry that exists in the entry type that you intend to use. If you are deleting an entry from a group, you might first use the tklmKeyList command to verify that the entry exists in the intended type. Then, try the operation again.

CTGKM0565E Cannot find the key: *VALUE_0*

Explanation:
The key value that you specified does not match an existing key.

System action:
The operation fails.

Administrator response:
Specify a key that exists in the type that you intend to use. If you are deleting a key from a group, you might first use the tklmGroupList or the tklmKeyList command to verify that the key exists. Then, try the operation again.

CTGKM0566E Cannot add a certificate to a device group.

Explanation:
The value of the group type is incorrect.

System action:
The operation fails.

Administrator response:
Specify keygroup as the group type. Then, try the operation again.

CTGKM0567E Cannot find the certificate: *VALUE_0*

Explanation:
The certificate value that you specified does not match an existing certificate.

System action:
The operation fails.

Administrator response:
Specify a certificate that exists. You might first use the tklmCertList command to verify that the certificate exists. Then, try the operation again.

CTGKM0569E Cannot find the device: *VALUE_0*

Explanation:
The device value that you specified does not match an existing device.

System action:
The operation fails.

Administrator response:
Specify a device that exists. You might first use the tklmDeviceList command to verify that the device exists. Then, try the operation again.

CTGKM0570E Failed to add group entry.

Explanation:
The entry was not added to the group. This might be an internal error.

System action:
The operation fails.

Administrator response:
The audit log might contain information about the error. Collect the information and contact IBM Support.

CTGKM0571E File already exists: *VALUE_0*

Explanation:
The file that you are attempting to export matches the name of an existing file.

System action:
The operation fails.

Administrator response:
Specify a different path and file name. Then, try the operation again.

CTGKM0572E No provider available to support the JCECCARACFKS keystore on the system. Be sure that the IBMJCECCA provider is installed.

Explanation:
The keystore that you specified requires that the Java™ crypto hardware provider be configured on your system. The JCECCAKS and JCECCARACFKS keystores require the hardware crypto provider.

System action:
The operation fails.

Administrator response:
If you are on a distributed system, select a JCEKS keystore type. On z/OS® systems, configure the hardware provider in your Java crypto provider list. Then, try the operation again.

CTGKM0573E JCECCARACFKS keystore type is not supported on the system.

Explanation:
This keystore type is supported only in a z/OS environment.

System action:
The operation fails.

Administrator response:
Select a JCEKS keystore type for use on a distributed system. Then, try the operation again.

CTGKM0574E Cannot create JCECCARACFKS keystore:

Explanation:
You must previously specify the IBMJCECCA provider before creating a JCECCARACFKS keystore. Alternatively, you might not have the RACF authority to use the keyring.

System action:
The operation fails.

Administrator response:
Ensure that the IBMJCECCA provider is installed and configured for access. To determine whether you have the correct authority, take the steps that are specified in the <keyword conref = "../../common/common.dita#common/tklmshort"/> Installation and Configuration Guide. Make necessary corrections. Then, try the operation again.

CTGKM0575E Cannot load JCECCARACFKS keystore:

Explanation:
You must previously specify the IBMJCECCA provider before creating a JCECCARACFKS keystore. Alternatively, you might not have the RACF authority to create, load, or update the keyring.

System action:
The operation fails.

Administrator response:
Ensure that the IBMJCECCA provider is installed and configured for access. To determine whether you have the correct authority, take the steps that are specified in the <keyword conref = "../../common/common.dita#common/tklmshort"/> Installation and Configuration Guide. Make necessary corrections. Then, try the operation again.

CTGKM0576E No provider available to support the JCERACFKS keystore on the system. Be sure that the IBMJCE provider is installed.

Explanation:
You must previously specify the IBMJCE provider before creating a JCERACFKS keystore.

System action:
The operation fails.

Administrator response:
Ensure that the IBMJCE provider is installed and configured for access. Then, try the operation again.

CTGKM0577E JCERACFKS keystore type is not supported on the system.

Explanation:
This keystore type is supported only in a z/OS environment.

System action:
The operation fails.

Administrator response:
Select a JCEKS keystore type for use on a distributed system. Then, try the operation again.

CTGKM0578E Cannot create JCERACFKS keystore:

Explanation:
You must previously specify the IBMJCE provider before creating a JCERACFKS keystore. Alternatively, you might not have the RACF authority to create, load, or update the keyring.

System action:
The operation fails.

Administrator response:
Ensure that the IBMJCE provider is installed and configured for access. To determine whether you have the correct authority, take the steps that are specified in the <keyword conref = "../../common/

common.dita#common/tklmshort"/> Installation and Configuration Guide. Make necessary corrections. Then, try the operation again.

CTGKM0579E Cannot load JCERACFKS keystore:

Explanation:
You must previously specify the IBMJCE provider before creating a JCERACFKS keystore. Alternatively, you might not have the RACF authority to load the keyring.

System action:
The operation fails.

Administrator response:
Ensure that the IBMJCE provider is installed and configured for access. To determine whether you have the correct authority, take the steps that are specified in the <keyword conref = "../../common/common.dita#common/tklmshort"/> Installation and Configuration Guide. Make necessary corrections. Then, try the operation again.

CTGKM0580E Keystore name and certificate alias must be specified

Explanation:
Your command did not specify the keystore name or the certificate alias.

System action:
The operation fails.

Administrator response:
Specify the keystore name and the certificate alias correctly. Alternatively, you might use the tklmKeystoreList command to determine which certificates the keystore contains. Then, try the operation again.

CTGKM0581E Internal key server exception.

Explanation:
The IBM Security Guardium Key Lifecycle Manager data store returned an error when attempting to delete a certificate.

System action:
The operation fails.

Administrator response:
The audit log might contain information about the error. Collect the information and contact IBM Support.

CTGKM0582E Wrong password.

Explanation:
The existing keystore password that you provided did not match the actual password.

System action:
The operation fails.

Administrator response:
Specify the correct password value for the keystore. Then, try the operation again.

CTGKM0583E Group already exists: *VALUE_0*

Explanation:
The group that you are attempting to create already exists.

System action:
The operation fails.

Administrator response:
Specify an alternative name for the group. Then, try the operation again.

CTGKM0584E The key in the certificate to be imported does not match the key in the original certificate request.

Explanation:
The key of the certificate that returned from a Certificate Authority does not match the key in the original certificate request.

System action:
The operation fails.

Administrator response:
Import the certificate response using an alias that corresponds to this response. Then, try the operation again.

CTGKM0585E Error occurred while verifying the key and certificate.

Explanation:
This is an internal database error.

System action:
The operation fails.

Administrator response:
The audit log might contain information about the error. Collect the information and contact IBM Support.

CTGKM0586E Keystore name and key alias must be specified.

Explanation:
The keystore name or the key alias value is not correct. You might have attempted to list or delete a key and did not specify all required values, such as the keystore name.

System action:
The operation fails.

Administrator response:
Specify a valid keystore name and key alias. Alternatively, you might use the tklmKeyList command to determine which keys the keystore contains. Then, try the operation again.

CTGKM0587E Alias *VALUE_0* does not exist in the keystore *VALUE_1*

Explanation:
The key alias is incorrectly specified. The alias does not exist in the specified keystore.

System action:
The operation fails.

Administrator response:
Ensure that the alias value is correct. Then, try the operation again.

CTGKM0588E Error occurred while loading data from the file *VALUE_0*

Explanation:
This is an error in reading data from a key or certificate file.

System action:
The operation fails.

Administrator response:
Ensure that the path and filename are correct. Then, try the operation again.

CTGKM0589E Error occurred while retrieving the entry *VALUE_0* from the keystore *VALUE_1*

Explanation:
Both the path name and the keystore password must be correctly specified.

System action:
The operation fails.

Administrator response:
Ensure that the keystore path name and password are valid. Then, try the operation again.

CTGKM0590E The file does not have any data.

Explanation:
An attempt was made to import a private key from a private key file. The private key file is empty.

System action:
The operation fails.

Administrator response:
Ensure that you specified a file that contains the desired private key. Then, try the operation again.

CTGKM0591E *VALUE_0* has more than one key entry; it is not supported by import operation.

Explanation:
You used the tklmKeyImport command to import a PKCS12 file with more entries than IBM Security Guardium Key Lifecycle Manager supports. Only one private key can be imported, using this command.

System action:
The import key operation fails.

Administrator response:
Import the key from a file that contains only one private key. Then, try the operation again.

CTGKM0592E *VALUE_0* already exists.

Explanation:
The alias of a key that you attempted to import already exists in the keystore.

System action:
The import key operation fails.

Administrator response:
Specify a different alias. You might use the tklmKeyList command to view the keys that are currently in the keystore. Then, try the operation again.

CTGKM0593E Entry in *VALUE_0* is not the private key entry.

Explanation:
You attempted to import a private key. However, the entry in the PKCS12 file is not a private key entry. It might be a certificate entry.

System action:
The operation fails.

Administrator response:
You might need to obtain a different file, and validate that the file has a private key. Then, try the operation again.

CTGKM0594E No private key entry in the file *VALUE_0*

Explanation:
You attempted to import a private key. However, there is no private key entry in the PKCS12 file.

System action:
The operation fails.

Administrator response:
You might need to obtain a different file, and validate that the file has a private key. Then, try the operation again.

CTGKM0595E Key alias cannot exceed 12 characters in length.

Explanation:
A key alias for a set of multiple keys has a prefix that must be 3 characters long. If you create only one key, the value for the alias cannot exceed 12 characters.

System action:
The secret key or keys are not created.

Administrator response:
Specify an alias that does not exceed the character limit. Then, try the operation again.

CTGKM0596E Alias *VALUE_0* already exists in the keystore *VALUE_1*

Explanation:
You attempted to generate a key, but the key alias already exists in the keystore. A different alias is required.

System action:
The secret key or keys are not created.

Administrator response:
Specify a different alias. Then, try the operation again.

CTGKM0597E Error occurred while generating the secret key.

Explanation:
The Java Cryptography Extension attempted to generate a secret key, but the process failed.

System action:
The secret key or keys are not created.

Administrator response:
Try the operation again. If the problem continues, collect any information that might be in the audit log and then contact IBM Support.

CTGKM0598E The number of keys cannot be smaller than 1 or larger than 9999.

Explanation:
For the tklmSecretKeyCreate command, the value for the numOfKeys parameter must be a positive integer that is 1 or greater, and not larger than 9999.

System action:
The secret keys are not created.

Administrator response:
Specify a value for the number of keys that does not exceed the limit. Then, try the operation again.

CTGKM0599E Error occurred while adding the key to the keystore.

Explanation:
The tklmSecretKeyCreate or the tklmKeyImport command experienced an error attempting to add a key to the keystore.

System action:
The secret key or keys are not added to the keystore.

Administrator response:
Collect any information that might be in the audit log and then contact IBM Support.

CTGKM0600E Method Not Implemented: *VALUE_0*

Explanation:
This is an internal message that IBM Security Guardium Key Lifecycle Manager generates when a method call encounters an error condition.

System action:
The operation fails.

Administrator response:
This error should not occur in your environment. First, examine the audit log for exception information about the method call. You might need to contact IBM Support.

CTGKM0601E An error occurred adding/updating value for attribute *VALUE_0*

Explanation:
An attempt was made to write a null value to the SKLMConfig.properties file. The file might be write protected. Alternatively, an internal component such as the key server component returned an error or was not available.

System action:
The operation fails.

Administrator response:
Ensure that the SKLMConfig.properties file is write enabled. If an internal component failed, you might restart the IBM Security Guardium Key Lifecycle Manager server. Then, try the operation again. If the problem continues, examine the audit log for exception information about the update to the attribute. Make necessary corrections. Then, try the operation again. You might need to call IBM Support.

CTGKM0602E An error occurred getting the value for attribute *VALUE_0*

Explanation:
An attempt was made to read a value from the SKLMConfig.properties file. You might not be authorized to read the SKLMConfig.properties file.

System action:
The operation fails.

Administrator response:
Ensure that you have the correct authorization. If the problem continues, examine the audit log for exception information about the error. Make necessary corrections. Then, try the operation again. You might need to call IBM Support.

CTGKM0603E An error occurred deleting attribute *VALUE_0*

Explanation:
An attempt was made to delete an attribute value from the SKLMConfig.properties file. The file might be write protected. Alternatively, an internal component such as the key server component returned an error or was not available.

System action:
The operation fails.

Administrator response:

Ensure that the SKLMConfig.properties file is write enabled. If an internal component failed, you might restart the IBM Security Guardium Key Lifecycle Manager server. Then, try the operation again. If the problem continues, examine the audit log for exception information about the update to the attribute. Make necessary corrections. Then, try the operation again. You might need to call IBM Support.

CTGKM0604E An error occurred merging configuration with file *VALUE_0*

Explanation:
Merging in this context means that a problem occurred in merging two configuration files. This might occur during migration of configuration data from an existing Encryption Key Manager server. Data was not written from an existing configuration file into a new SKLMConfig.properties file. The new file might write protected, or you might not have sufficient authority.

System action:
The operation fails.

Administrator response:
Ensure that the SKLMConfig.properties file is write enabled and that you have appropriate access to the file. You might also examine the audit log for exception information. Make necessary corrections. Then, try the operation again. You might need to contact IBM Support.

CTGKM0605E An error occurred replacing configuration file with file *VALUE_0*

Explanation:
Configuration file replacement might occur during migration of configuration data from an existing Encryption Key Manager server. You might not have sufficient authority to replace the configuration file.

System action:
The operation fails.

Administrator response:
Ensure that you have appropriate access to the file. You might also examine the audit log for exception information. Make necessary corrections. Then, try the operation again. You might need to contact IBM Support.

CTGKM0615E Keystore password cannot exceed 175 single-byte or 87 double-byte characters.

Explanation:
Keystore password cannot exceed 175 single-byte or 87 double-byte characters.

System action:
Keystore password update fails.

Administrator response:
Enter a password not greater than 175 single-byte or 87 double-byte characters.

CTGKM0616E Device with UUID *VALUE_0* does not belong to the device group *VALUE_1*.

Explanation:
The device with the specified UUID does not belong to the specified device group.

System action:
Device list fails.

Administrator response:
Enter the correct device group, or leave it blank.

CTGKM0617E authorization.provider.class cannot be a numeric string.

Explanation:
authorization.provider.class cannot be a numeric string.

System action:
The operation fails.

Administrator response:
Specify a non-numeric value.

CTGKM0618E *VALUE_0* can only be positive integer.

Explanation:
The value must be an integer greater than zero.

System action:
The operation fails.

Administrator response:
Specify a positive integer.

CTGKM0620E Error parsing XML template.

Explanation:
This is an internal message that IBM Security Guardium Key Lifecycle Manager generates after problems occur reading an XML template file that has syntax errors.

System action:
The operation fails.

Administrator response:
This error should not occur in your environment. First, examine the audit log for exception information about the XML parsing error. You might need to contact IBM Support.

CTGKM0621E Error in XML element *VALUE_0* , expecting *VALUE_1*

Explanation:
This is an internal message that IBM Security Guardium Key Lifecycle Manager generates after problems occur reading an XML template file that has errors.

System action:
The operation fails.

Administrator response:
This error should not occur in your environment. First, examine the audit log for exception information about the error. You might need to contact IBM Support.

CTGKM0622E XML attribute *VALUE_0* missing for element *VALUE_1*

Explanation:
This is an internal message that IBM Security Guardium Key Lifecycle Manager generates after problems occur reading an XML template file that has errors.

System action:
The operation fails.

Administrator response:
This error should not occur in your environment. First, examine the audit log for exception information about the error. You might need to contact IBM Support.

CTGKM0623E Error in XML template attribute value *VALUE_0* for attribute *VALUE_1*

Explanation:
This is an internal message that IBM Security Guardium Key Lifecycle Manager generates after problems occur reading an XML template file that has errors.

System action:
The operation fails.

Administrator response:
This error should not occur in your environment. First, examine the audit log for exception information about the error. You might need to contact IBM Support.

CTGKM0624E Template *VALUE_0* not found.

Explanation:
This is an internal message that IBM Security Guardium Key Lifecycle Manager generates after problems occur attempting to read an XML template file.

System action:
The operation fails.

Administrator response:
This error should not occur in your environment. First, examine the audit log for exception information about the error. You might need to contact IBM Support.

CTGKM0630E Validation error: *VALUE_1* for parameter *VALUE_0*.

Explanation:
When a command is parsed, this error occurs if you enter a parameter value that is not valid.

System action:
The operation fails.

Administrator response:
Specify a valid value for the parameter. Then, try the operation again.

CTGKM0631E Missing required parameter *VALUE_0* .

Explanation:
The value that you specified for the required parameter is blank or missing.

System action:
The operation fails.

Administrator response:
Specify a valid value for the parameter. Then, try the operation again.

CTGKM0632E Missing required *VALUE_0* parameter *VALUE_1*

Explanation:
The required parameter value is blank or missing.

System action:
The operation fails.

Administrator response:
Specify a valid value for the required parameter. Then, try the operation again.

CTGKM0633E Validation error: *VALUE_1* is invalid for parameter *VALUE_0* *VALUE_2* . Specify one of these valid values:

Explanation:
The value that you specified for the parameter is not valid.

System action:
The operation fails.

Administrator response:
Ensure that the value that you specified is valid. Then, try the operation again.

CTGKM0634E Validation Error: *VALUE_1* for parameter *VALUE_0* , must be 16 characters long and contain valid characters.

Explanation:
When a command is parsed, this error occurs if you enter a parameter value that is not valid.

System action:
The operation fails.

Administrator response:
Specify a valid value for the parameter. Then, try the operation again.

CTGKM0635E **Incorrect syntax for required parameter attribute. Syntax is {attribute1}{attribute2}..{attributeN}.**

Explanation:
The syntax for the parameter 'attribute' was incorrect.

System action:
The operation fails.

Administrator response:
Correct the syntax, and try again.

CTGKM0640E **Certificate Request file already exists: *VALUE_0***

Explanation:
The file name that you specified in the certificate request matches a certificate request file name that currently exists.

System action:
The operation fails.

Administrator response:
Specify a different file name for the certificate request. For example, specify myUniqueRequest.crt. Then, try the operation again.

CTGKM0641E **Error in writing file *VALUE_0* : *VALUE_1***

Explanation:
You might not have authorization to write a certificate request file, or the path name that you specified is incorrect.

System action:
The operation fails.

Administrator response:
Ensure that you have appropriate access to the file, and that the path and file names are correctly specified. Then, try the operation again. You might also examine the audit log for exception information about the file operation. Make necessary corrections. Then, try the operation again. You might need to contact IBM Support.

CTGKM0645E **Device *VALUE_0* not found.**

Explanation:
An attempt to read device information used an identifier for the device does not match an existing device serial number. This is an internal error.

System action:
The operation fails.

Administrator response:
Determine whether the value that you specified matches an existing device, and that the specified type matches the device group. For example, you might use the tklmDeviceList command to identify existing devices of a given group. Correct the device specification. Then, try the operation again.

CTGKM0650E **Error while attempting to encrypt a file using algorithm: *error_msg***

Explanation:
Error occurred while attempting to encrypt a file using algorithm

System action:
Operation invoking the encryption fails.

Administrator response:
Error can occur for a number of reasons: missing algorithm, incorrect algorithm parameter, incorrect encryption key or key specification (password), incorrect padding mechanism. This error is not expected to occur. If it does, the IBM Security Guardium Key Lifecycle Manager administrator should investigate the cause.

CTGKM0651E **Error while attempting to decrypt a file using algorithm: *error_msg***

Explanation:
This error occurred while attempting to decrypt a file using the algorithm.

System action:
The operation fails.

Administrator response:
This error can occur for a number of reasons: missing algorithm, incorrect algorithm parameter, incorrect encryption key or key specification (password), or an incorrect padding mechanism. This error is not expected to occur. If it does, the IBM Security Guardium Key Lifecycle Manager administrator should investigate the cause.

CTGKM0660E **tklmCertList supports the optional parameters -usage and -v, and these parameter combinations: No parameters; or -uuid; or -alias and -keystoreName; or -attributes.**

Explanation:
The command failed because the combination of parameter values that you specified is not valid.

System action:
The operation fails.

Administrator response:
Specify no parameter, or specify a value for alias, or specify an attribute, or specify both a uuid and keystoreName. Then, try the operation again.

CTGKM0704E **Group name cannot contain \' \\ \'.**

Explanation:
The group name must not contain the characters \' \\ \' in the name.

System action:
The operation fails.

Administrator response:
Specify a group name that does not contain \' \\ \'. Then, try the operation again.

CTGKM0705E Either group name or group UUID must be specified.

Explanation:
The command requires that you specify either the group name or the group UUID.

System action:
The operation fails.

Administrator response:
Specify either a group name or group UUID. Then, try the operation again.

CTGKM0706E The key group with the name *VALUE_0* does not have the UUID *VALUE_1*.

Explanation:
The specified group name and group UUID do not match.

System action:
The operation fails.

Administrator response:
Correct the group name or UUID, or specify only one of the two. Then, try the operation again.

CTGKM0742E Key type not valid: *VALUE_0*.

Explanation:
Key type entered is not valid.

System action:
Key operation fails.

Administrator response:
Check the logs for more information.

CTGKM0750E Validation Error: *VALUE_0* for compromised, only y is allowed.

Explanation:
When you use the tklmCertUpdate command to specify that a certificate is compromised, the only valid value is y (compromised). You cannot change a compromised certificate to an uncompromised state.

System action:
The certificate state is not changed.

Administrator response:
Specify a value of y for the -compromised attribute. Then, try the operation again.

CTGKM0751E Conflicting parameter values specified for compromised and trusted.

Explanation:
When you use the tklmCertUpdate command to specify that a certificate is compromised, the certificate cannot be marked as trusted. A certificate can only be marked trusted if it is not in expired, retired or compromised state.

System action:
The certificate state is not changed.

Administrator response:
Do not specify a value of y for trusted if the certificate needs to be marked as compromised.

CTGKM0752E Validtion Error: *VALUE_0* for trusted, only y or n is allowed.

Explanation:
When you use the tklmCertUpdate command to specify a certificate is trusted or not, the only valid values are y (trusted) or n (not trusted).

System action:
The certificate attribute is not changed.

Administrator response:
Specify a value of y or n for the -trusted attribute. Then, try the operation again.

CTGKM0753E Certificate is not in a valid state to mark it trusted.

Explanation:
If the certificate is in compromised, destroyed, expired or retired state then it cannot be marked as trusted. Only certificates in an active or pre-active state can be marked as trusted.

System action:
The certificate attribute is not changed.

Administrator response:
Check the state of the certificate using the tklmCertList command. Do not specify trusted attribute to mark the certificate as trusted if the certificate state is compromised, destroyed, expired or retired.

CTGKM0760E Certificate with alias = *VALUE_0* cannot be deleted because this certificate is specified as a default or partner certificate.

Explanation:
Using the tklmCertDelete command, you cannot delete a certificate that is specified as the system default or partner certificate.

System action:
The certificate delete operation fails.

Administrator response:
Specify a different certificate as the system default or partner certificate. Ensure that the certificate that you

intend to delete no longer has the specification. Then, try the operation again.

CTGKM0761E Key with alias = *VALUE_0* cannot be deleted because the certificate associated with this key is specified as a default or partner certificate.

Explanation:
Using the tklmKeyDelete command, you cannot delete a key which certificate is specified as the system default or partner.

System action:
The key delete operation fails.

Administrator response:
Specify a different certificate as the system default or partner. Ensure that the key that you intend to delete no longer has the specification. Then, try the operation again.

CTGKM0775E Command is not supported in FIPS mode.

Explanation:
Algorithms used by this command are not supported in a FIPS mode environment.

System action:
Command Fails

Administrator response:
Change the value of the FIPS property to off and restart the server before using this command.

CTGKM0776W The number of device audit entries returned reaches the limit of 2000 records. Only the first 2000 entries are displayed. You might need to specify a different filter for your search.

Explanation:
The list operation only fetches the first 2000 rows.

System action:
The first 2000 entries are displayed.

Administrator response:
The result set reached the 2000 entries limit. Specify a different filter, and try the operation again.

CTGKM0800E Attempt to insert entry with preexisting primary key value failed on table *VALUE_0*

Explanation:
Using the tklmDeviceAdd command, a primary key in the database uniquely represents a device with a combination of several parameters (serialNumber, type, and worldwideName). The primary key already exists. The device that you attempted to add already exists in the database.

System action:
The device is not added to the database.

Administrator response:
Specify different values for the device that you intend to add. Then, try the operation again.

CTGKM0801E A key group name and a key alias cannot be same in the IBM Security Guardium Key Lifecycle Manager database. Specify a unique key group name and try again.

Explanation:
Before creating metadata for a key, IBM Security Guardium Key Lifecycle Manager verifies that a key group does not already exist with the same name as the alias. Similarly, before creating a key group, the IBM Security Guardium Key Lifecycle Manager verifies that a key does not exist with the same alias as the group name.

System action:
The create operation fails.

Administrator response:
If you are creating a key, specify a different alias name. If you are creating a key group, specify a different key group name.

CTGKM0802E The backup program could not determine the database name from the data source URL: *VALUE_0*

Explanation:
The IBM Security Guardium Key Lifecycle Manager determines the name of database to backup by parsing the data source URL that was specified during the installation of the database. The backup program failed because the database name could not be determined.

System action:
The database backup operation fails.

Administrator response:
Verify that the data source URL is correctly specified. Then, try the operation again.

CTGKM0803E The backup program could not determine the directory to which database files will be saved.

Explanation:
IBM Security Guardium Key Lifecycle Manager determines the directory to save the files by using the datastore.properties file. The backup program failed because the directory could not be determined.

System action:
The database backup operation fails.

Administrator response:
Verify that the IBM Security Guardium Key Lifecycle Manager has been configured correctly and the correct value for the tklm.backup.db2.dir property exists in the properties file.

CTGKM0804E The backup program failed because archival logging has not been enabled.

Explanation:
The IBM Security Guardium Key Lifecycle Manager requires that archival logging is enabled for the IBM Security Guardium Key Lifecycle Manager in order to perform an online backup. The installation program enables the archival logging.

System action:
The database backup operation fails.

Administrator response:
Verify that the IBM Security Guardium Key Lifecycle Manager has been configured correctly and that archival logging is enabled. To determine the logging method that Db2® currently uses, run this command:

```
db2 get db cfg for sklmdb
```

CTGKM0805E The backup program failed because the backup program could not write to the directory that was specified for the database files.

Explanation:
IBM Security Guardium Key Lifecycle Manager

Explanation:
requires that directory that is specified in the datastore.properties file exists for the property tklm.backup.db2.dir and is writeable. The Db2 backup utility found an error in the specified directory.

System action:
The database backup operation fails.

Administrator response:
Verify that the directory specified in the properties file exists and is writeable.

CTGKM0806E An error occurred reading the sklm.properties file.

Explanation:
IBM Security Guardium Key Lifecycle Manager reads the sklm.properties file to determine appropriate parameters to perform a database restore operation. An error occurred while reading this file.

System action:
The database restore operation fails.

Administrator response:
Ensure that the sklm.properties file is read enabled. If an internal component failed, you might restart the IBM Security Guardium Key Lifecycle Manager server. Then, try the operation again. If the problem continues, examine the audit log for exception information. Make necessary corrections. Then, try the operation again. You might need to contact IBM Support.

CTGKM0807E An error occurred getting the value for attribute *VALUE_0*

Explanation:
An attempt was made to read a value from the sklm.properties file. You might not be authorized to read the sklm.properties file.

System action:
The database restore operation fails.

Administrator response:
Ensure that you have the correct authorization. If the problem continues, examine the audit log for exception information about the error. Make necessary corrections. Then, try the operation again. You might need to call IBM Support.

CTGKM0808E The restore program could not determine the directory from which to restore database files.

Explanation:
IBM Security Guardium Key Lifecycle Manager determines the directory to restore the file from arguments specified to the restore program. If the arguments are not specified, it determines the directory from the datastore.properties file. The restore program failed because the directory could not be determined.

System action:
The database restore operation fails.

Administrator response:
Verify that IBM Security Guardium Key Lifecycle Manager has been configured correctly and a valid tklm.backup.db2.dir value exists in the datastore.properties file.

CTGKM0809E A null value was specified for the timestamp associated with the previously saved database files.

Explanation:
IBM Security Guardium Key Lifecycle Manager determines the timestamp to restore the file from arguments specified to the restore program. The restore program failed because the timestamp could not be determined.

System action:
The database restore operation fails.

Administrator response:
Verify that IBM Security Guardium Key Lifecycle Manager has been configured correctly.

CTGKM0850E An exception occurred during the restore operation. Examine the db2restore.log for exception information. Complete the restore operation before attempting any other IBM Security Guardium Key Lifecycle Manager tasks.

Explanation:
IBM Security Guardium Key Lifecycle Manager encountered an exception.

System action:
The database restore operation fails.

Administrator response:
Ensure that you have configured IBM Security Guardium Key Lifecycle Manager correctly. If the problem continues, examine the db2tklmrestore log for exception information about the error. Make necessary corrections. Then, try the operation again. You might need to contact IBM Support.

CTGKM0851E The group cannot be created because an entity (key) cannot be in multiple key groups. The entity *VALUE_0* is already a member of the group *VALUE_1*.

Explanation:
While creating a group, you specified an entity that already exists in another group. The entity cannot not be in multiple groups.

System action:
The group creation operation fails.

Administrator response:
Specify an entity (key) that does not exist in another group. Then, try the operation again.

CTGKM0852E The specified entity (key) *VALUE_0* cannot be added to the group because the entity cannot be in multiple groups. The entity is already a member of the group *VALUE_1*.

Explanation:
While adding an entity to a group, you specified an entity that already exists in another group. The entity cannot not be in multiple groups.

System action:
The group creation operation fails.

Administrator response:
Specify an entity (key) that does not exist in another group. Then, try the operation again.

CTGKM0900E Database connection failed on data source *VALUE_0* . Check to see if database server needs to be restarted or if database user's password needs to be updated.

Explanation:
The database may be down or the database user's password for accessing the IBM Security Guardium Key Lifecycle Manager database might need to be updated.

System action:
The database operation fails.

Administrator response:
Verify that the database is up or check if the database user's password for accessing the IBM Security Guardium Key Lifecycle Manager database might need to be updated, for example, after a mandated password change on the corresponding operating system account.

CTGKM0901E Backup directory could not be resolved. Try specifying a valid backup directory explicitly.

Explanation:
Backup directory could not be resolved.

System action:
The IBM Security Guardium Key Lifecycle Manager backup operation fails.

Administrator response:
Make sure that the backup directory provided to the backup operation is valid. Try specifying a valid backup directory explicitly. If this is the first time you are executing backup, find a directory suitable for IBM Security Guardium Key Lifecycle Manager backup and specify the directory explicitly on the backup command.

CTGKM0902E Default backup directory cannot be determined: *VALUE_0* .

Explanation:
The configuration property tklm.backup.dir cannot be found.

System action:
The IBM Security Guardium Key Lifecycle Manager backup operation fails.

Administrator response:
Ensure that the tklm.backup.dir parameter is set in the configuration file or provide the backupDirectory parameter to the backup operation.

CTGKM0903W IBM Security Guardium Key Lifecycle Manager restore is already in progress.

Explanation:
Only one restore/backup operation is allowed at any given time.

System action:

The requested operation will not be performed.

Administrator response:
Wait until the operation completes.

CTGKM0904W IBM Security Guardium Key Lifecycle Manager backup is already in progress.

Explanation:
Only one restore/backup operation is allowed at any given time.

System action:
The requested operation will not be performed.

Administrator response:
Wait until the operation completes.

CTGKM0905E Backup of *VALUE_0* failed: *VALUE_1* .

Explanation:
Backup failed unexpectedly.

System action:
Backup fails.

Administrator response:
Check the log entries to find out the reason for backup failure.

CTGKM0906E Specified backup file does not exist: *VALUE_0* .

Explanation:
The backup file does not exist.

System action:
The IBM Security Guardium Key Lifecycle Manager restore operation fails.

Administrator response:
Make sure that the backup file path provided to the restore operation is valid.

CTGKM0907E Restore of *VALUE_0* failed: *VALUE_1* .

Explanation:
Restore failed unexpectedly.

System action:
Restore fails.

Administrator response:
Check the log entries to find out the reason for restore failure.

CTGKM0908E Error reading manifest from the backup jar file: *VALUE_0* .

Explanation:
Backup manifest could be corrupted or incorrect for unknown reasons.

System action:
Restore fails.

Administrator response:
Check the log entries to find out the reason for restore failure.

CTGKM0909E Error making a backup copy of existing configuration file: *VALUE_0* .

Explanation:
Backup copy of a configuration file could not be made.

System action:
Restore fails.

Administrator response:
Check the log entries to find out the reason for restore failure.

CTGKM0910E I/O error while creating backup jar file *jar_file_name* \nError message: *error_msg* .

Explanation:
Input/Output file error occurred while creating the backup jar file.

System action:
Backup fails.

Administrator response:
Check the log entries to find out the reason for backup failure.

CTGKM0911E Entry in the jar has been modified since the backup file was created: \nJar file: *jar_file_name* \nJar entry name: *jar_entry_name* \nDestination: *destination*

Explanation:
An entry in the backup jar file has been changed since the jar file was created. This may indicate a corrupt file or a backup jar which has been tampered with in some way.

System action:
Restore fails.

Administrator response:
Check the integrity of the backup file in question. Use another backup jar file if available.

CTGKM0912E I/O error, missing or corrupt data detected while extracting jar file entry.\nJar file name: *jar_file_name* \nJar entry name: *jar_entry_name* \nDestination: *destination*

Explanation:
Backup jar file or an entry in the backup jar file is missing, corrupt or has been tampered with.

System action:
Restore fails.

Administrator response:
Check the integrity of the backup file in question. Use another backup jar file if available.

CTGKM0913E **I/O error while decrypting and/or extracting jar file. \nPossible cause: Incorrect password may have been provided, which results in the jar entry being decrypted incorrectly.**

Explanation:
I/O error occurred while decrypting and/or extracting a jar file entry. A common reason for this error is that a file was encrypted using one password and an incorrect or null password was provided to decrypt the file. Decryption will still take place, but the decrypted file is not valid and cannot be used in later stages of the restore.

System action:
Restore fails.

Administrator response:
Check the password provided for decryption. Check if the destination location contains sufficient disk space to hold the decrypted/extracted file. Check the log files for additional clues if necessary. Retry the operation.

CTGKM0914W **IBM Security Guardium Key Lifecycle Manager backup or restore operation is in progress. Database connections cannot be obtained at this moment. Try again later.**

Explanation:
To minimize the risk of data inconsistency, a IBM Security Guardium Key Lifecycle Manager backup or restore operation needs to be done while the database is not used by the IBM Security Guardium Key Lifecycle Manager server. This warning message will be displayed in the graphical user interface and/or log file.

System action:
Database connection is not possible and the IBM Security Guardium Key Lifecycle Manager operation requesting it fails.

Administrator response:
Retry your operation after the backup or restore is done.

CTGKM0915E **IBM Security Guardium Key Lifecycle Manager backup failed due to low disk space on the file system containing the backup directory *VALUE_0* .**

Explanation:
The database backup failed due to low disk space on the file system containing the backup directory.

System action:
The backup operation fails.

Administrator response:
Increase the available disk space on the file system containing the database backup directory. Then try the operation again.

CTGKM0916W **Warning: Information about this backup was not saved. However, the IBM Security Guardium Key Lifecycle Manager backup operation saved all the necessary files, which could be used for a restore operation in the future.**

Explanation:
A successful backup operation saves information about the backup in a file named SKLM_HOME/config/lastbackupinfo. However, the step to save this information failed, or the information is incorrect. You can still use the backup file for a restore operation. Possible reasons for failure: Another process was using the lastbackupinfo file, or permissions for the SKLM_HOME/config directory are incorrect.

System action:
The backup operation succeeded but the information about the most recent backup could not be saved.

Administrator response:
Verify that no other process is using the lastbackupinfo file and the SKLM_HOME/config directory has the correct read and write permissions. Then try the backup operation again if you want this information to be accurate.

CTGKM0917E **IBM Security Guardium Key Lifecycle Manager failed to determine the information about the last successful backup. Possible reasons: A backup was never done on this system, the file permissions are incorrect, or the file was deleted.**

Explanation:
After a successful backup, IBM Security Guardium Key Lifecycle Manager saves the information about the backup in a file named *SKLM_HOME*/config/lastbackupinfo. This file could not be read.

System action:
The IBM Security Guardium Key Lifecycle Manager fails to determine the information about the last successful backup.

Administrator response:
If you restored a backup from another system, this file may not be available. Verify that the *SKLM_HOME*/config/lastbackupinfo file exists and that the file has read permission. Run the operation again.

CTGKM0918E Cannot add a value to a single-valued KMIP attribute when a value already exists. Object uuid: *VALUE_0*, Object name: *VALUE_1*, Attribute name: *VALUE_2*.

Explanation:
Cannot add a value to a single-valued KMIP attribute when value already exists. Existing value can be modified or deleted.

System action:
The operation fails.

Administrator response:
Modify or delete the value. Then, try the operation again.

CTGKM0919E Cannot modify attribute value. Current® value is not defined at index *VALUE_0*. Object uuid: *VALUE_1*, Object name: *VALUE_2*, Attribute name: *VALUE_3*.

Explanation:
Cannot modify a value on a multi-valued KMIP attribute because the value does not exist at the specified index.

System action:
The operation fails.

Administrator response:
Modify or delete the value. Then, try the operation again.

CTGKM0920E Cannot delete attribute value. Incorrect attribute value index was specified: *VALUE_0*. Object uuid: *VALUE_1*, Object name: *VALUE_2*, Attribute name: *VALUE_3*.

Explanation:
Cannot delete a value because the value does not exist at the specified index.

System action:
The operation fails.

Administrator response:
Provide a valid index.

CTGKM0921E Cannot modify attribute value. New value is not provided. Object uuid: *VALUE_0*, Object name: *VALUE_1*, Attribute name: *VALUE_2*.

Explanation:
Cannot modify a value because a new value was not provided.

System action:
The operation fails.

Administrator response:
Provide a valid new value or delete the existing value.

CTGKM0922E Range Specification is not valid: *VALUE_0*

Explanation:
One or two range-capable values of the same range-capable attribute type are expected.

System action:
The operation fails.

Administrator response:
Provide a valid range. Then, try the operation again.

CTGKM0923E Unsupported parameter type detected: *VALUE_0*

Explanation:
Unsupported parameter type was specified.

System action:
The operation fails.

Administrator response:
Provide a valid parameter. Then, try the operation again.

CTGKM0924E Unsupported usage mask ' *VALUE_0* ' on object with uuid *VALUE_1*

Explanation:
Unsupported KMIP usage mask was detected in the data store.

System action:
The IBM Security Guardium Key Lifecycle Manager cannot retrieve object's data.

Administrator response:
Investigate the source of incorrect data and correct or delete it before trying again.

CTGKM0925E Cannot *VALUE_0* a value when no attribute value was supplied. Object uuid: *VALUE_1*, Object name: *VALUE_2*, Attribute name: *VALUE_3*.

Explanation:
Cannot perform the operation when no attribute value is passed.

System action:
The operation fails.

Administrator response:
Supply the value. Then, try the operation again.

CTGKM0926E Cannot *VALUE_0* a value when no attribute value currently exists. Object uuid: *VALUE_1*, Object

name: *VALUE_2*, Attribute name: *VALUE_3*.

Explanation:
Cannot perform the operation when that attribute does not exist on that object.

System action:
The operation fails.

Administrator response:
Add the attribute with its value.

CTGKM0927E Cannot *VALUE_0* a value when no attribute value currently exists at that index. Object uuid: *VALUE_1*, Object name: *VALUE_2*, Attribute name: *VALUE_3*. Index: *VALUE_4*.

Explanation:
Cannot perform the operation when that attribute does not exist on that object.

System action:
The operation fails.

Administrator response:
Add the attribute with its value.

CTGKM0928E Certificate alias cannot contain \' \\ \' or \' / \' or \' .

Explanation:
You cannot create a certificate with \' \\ \' or \' / \' or \' in the alias.

System action:
The operation fails.

Administrator response:
Specify an alias that does not contain \' \\ \' or \' / \' or \' . Then, try the operation again.

CTGKM0929E Error occurred while looking up version numbers.

Explanation:
Command could not be executed. On Windows systems, ensure that the environment variable ProgramFiles is set correctly. If you are running 64-bit Windows, ensure that the environment variable ProgramFiles(x86) is also correctly set.

System action:
The operation fails.

Administrator response:
Ensure that the required environment variables are correctly set.

CTGKM0930E Because this certificate is outside of its validity period and the validate certificates check is enabled, cannot assign this certificate to the device.

Explanation:
The certificate is outside of its validity period and not available for use.

System action:
The operation fails.

Administrator response:
Select another certificate.

CTGKM0931E Not all version numbers were successfully retrieved.

Explanation:
Some version numbers could not be retrieved. Ensure that the 'IBM ADE Service' service is running.

System action:
The operation fails.

Administrator response:
Ensure that the service 'IBM ADE Service' is running. To start the service in Windows, go to the Control Panel > Services. To start the service in Linux®, run the /usr/ibm/common/acsi/bin/acsisrv.sh command. Then, try the operation again.

CTGKM0932E The value of newAlias cannot be an empty string.

Explanation:
You must provide a value for newAlias.

System action:
The operation fails.

Administrator response:
Specify a value for newAlias. Then, try the operation again.

CTGKM0933E Certificate with alias *VALUE_0* is compromised and cannot be set as a system, partner, or device default.

Explanation:
A compromised certificate cannot be set as a system, partner, or device default.

System action:
The operation fails.

Administrator response:
Select another certificate to use as a default.

CTGKM0934E Key with alias *VALUE_0* is compromised and cannot be set as a device default.

Explanation:
A compromised key cannot be set as a device default.

System action:
The operation fails.

Administrator response:
Select another key to use as a default.

CTGKM0935E alias is required if newAlias is specified.

Explanation:
The alias parameter is required if newAlias is specified.

System action:
The operation fails.

Administrator response:
Specify an alias and try the operation again.

CTGKM0937E Target uuid is not valid for the rollover object to be deleted: *VALUE_0*

Explanation:
The target uuid is not valid for the rollover object.

System action:
The operation fails.

Administrator response:
Ensure that the target uuid is valid and try the operation again.

CTGKM0938E Device group of the target is not valid for the rollover object to be deleted: *VALUE_0*

Explanation:
The target device group is not valid for the rollover object.

System action:
The operation fails.

Administrator response:
Ensure that the target device group is valid and try the operation again.

CTGKM0940E Common name cannot exceed 256 characters.

Explanation:
Common name is too long. The maximum length allowed is 256 characters.

System action:
Certificate creation fails.

Administrator response:
Specify a common name not exceeding 256 characters, then try the operation again.

CTGKM0942E Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files are required. For more information, see the Backup and restore section of the product documentation in the IBM Knowledge Center.

Explanation:
For Stronger encryption we require Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files. For more information, see the Backup and restore section of the product documentation in the IBM Knowledge Center.

System action:

Administrator response:
Install the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files.

CTGKM0944E Password must be specified.

Explanation:
Password must be specified.

System action:

Administrator response:
Specify a password and try again.

CTGKM0945E Backup Identifier is missing.

Explanation:
Backup Identifier must be present.

System action:
Restore operation fails.

Administrator response:
Ensure that the backup identifier is present and retry the operation.

CTGKM0946E The system is not configured to use HSM. But, the backup you are trying to restore is protected by HSM-based encryption.

System action:
The restore operation fails.

Administrator response:
Configure the system with HSM-based configuration settings.

CTGKM0947E Backup system version below 4.1 is not supported with restore container system version. For more information, see the Backup and restore section of the product documentation in the IBM Knowledge Center.

Explanation:
For restore on container system we require mimimum version 4.1. For more information, see the Backup and restore section of the product documentation in the IBM Knowledge Center.

System action:

Administrator response:
Upgrade to version 4.1. Create the backup and then try restore again.

CTGKM1000E Error while invoking scheduled task handler:\n \tTask Id: *task_id*\n \tTask Type: *task_type*\n \tTask Name: *task_name*\n \tOriginal error message: *error_message*

Explanation:
Error occurred while instantiating a scheduled task handler class.

System action:
Task will not be executed. Audit log will contain a failure message.

Administrator response:
This should not happen under normal conditions. Make sure that the task handler class exists in the correct location and is specified correctly.

CTGKM1001E Required task name value is not defined.

Explanation:
Required task name value was detected missing when scheduling a task.

System action:
Task will not be scheduled.

Administrator response:
This should not happen under normal conditions. Make sure that the task information contains all required values before submitting it.

CTGKM1002E Required task type value is not defined.

Explanation:
Required task type value was detected missing when scheduling a task.

System action:
Task will not be scheduled.

Administrator response:
This should not happen under normal conditions. Make sure that the task information contains all required values before submitting it.

CTGKM1003E Error while scheduling a task:\n Original error message: *error_message*

Explanation:
Required task type value was detected missing when scheduling a task.

System action:
Task will not be scheduled.

Administrator response:
This should not happen under normal conditions. Make sure that the task information contains all required values before submitting it.

CTGKM1004E Error occurred while suspending a scheduled task:\n Original error message: *error_message*

Explanation:
Error occurred while suspending a scheduled task.

System action:
Task will not be suspended.

Administrator response:
This should not happen under normal conditions. Investigate the logs for clues.

CTGKM1005E Error occurred while resuming a suspended scheduled task:\n Original error message: *error_message*

Explanation:
Error occurred while resuming a suspended scheduled task.

System action:
Task will not be resumed.

Administrator response:
This should not happen under normal conditions. Investigate the logs for clues.

CTGKM1006E Error occurred while canceling a scheduled task:\n Original error message: *error_message*

Explanation:
Error occurred while canceling a scheduled task.

System action:
Task will not be canceled.

Administrator response:
This should not happen under normal conditions. Investigate the logs for clues.

CTGKM1007E Error occurred while purging a task:\n Original error message: *error_message*

Explanation:
Error occurred while purging a task.

System action:
Task will not be purged.

Administrator response:
This should not happen under normal conditions. Investigate the logs for clues.

CTGKM1008E Scheduler is not available:\n Original error message: *error_message*

Explanation:
Scheduler is not available.

System action:

Scheduler related operations fail.

Administrator response:
This should not happen under normal conditions. Investigate the logs and server startup log for clues. Restart the system. Check if the database server is operating correctly.

CTGKM1009E **Error in scheduler task detected:\n Original error message: *error_message***

Explanation:
Error in scheduler task detected.

System action:
Operations involving this task will fail.

Administrator response:
This should not happen under normal conditions. Investigate the logs for clues. Delete the task and reschedule.

CTGKM1072W **The system will be restored from ${0}. The key and configuration data will be restored to the level of the backup that you select. Any changes made after the selected backup will be lost, including the metadata. After restoring from this backup, the server will be restarted automatically. The server will not be available during the restart process. After the server is restarted, you must restart the browser session (Log in again to use the product user interface). Do you want to continue?**

Explanation:
The key and configuration data are restored to the level of the backup that you select. Any changes made after the selected backup are lost, including the metadata.

System action:
The key and configuration data are restored to the level of the backup you select. Later changes are lost.

Administrator response:
Confirm that you want to restore from this backup level. When the operation completes, manually restart the Guardium Key Lifecycle Manager server.

CTGKM1100E **Object (*object_type*) with identifier *object_id* cannot be found.**

Explanation:
The identifier value that you specified does not match an existing object.

System action:
The operation fails.

Administrator response:
Specify an identifier which corresponds to an existing object.

CTGKM1101E **Incorrect or missing parameter was passed to perform a data store operation. Parameter identifier: *parameter_id***

Explanation:
Incorrect input was specified for a data store operation.

System action:
The operation fails.

Administrator response:
Make sure that correct parameters are used as input.

CTGKM1107E **Error: symmetricKeySet *VALUE_1* for parameter *VALUE_0* .**

Explanation:
The passed symmetricKeySet is either not a valid key or key group.

System action:
The operation fails.

Administrator response:
Specify a valid value for the parameter. Then, try the operation again.

CTGKM1108E **Key Group for device group is not valid: *VALUE_1* for parameter *VALUE_0* .**

Explanation:
The passed symmetricKeySet key group is not the valid device group

System action:
The operation fails.

Administrator response:
Specify a valid value for the parameter. Then, try the operation again.

CTGKM1109E **Key for device group is not valid *VALUE_1* for parameter *VALUE_0* .**

Explanation:
The passed symmetricKeySet key is not the valid device group.

System action:
The operation fails.

Administrator response:
Specify a valid value for the parameter. Then, try the operation again.

CTGKM1110E **Certificate alias *VALUE_0* does not exist in this device group.**

Explanation:
The passed defaultAlias1/defaultAlias2 does not exist.

System action:
The operation fails.

Administrator response:
Specify a valid value for the parameter. Then, try the operation again.

CTGKM1111E Key Alias does not belong to device group *VALUE_1* for parameter *VALUE_0* .

Explanation:
The passed defaultAlias1/defaultAlias2 does not match the given device group.

System action:
The operation fails.

Administrator response:
Specify a valid value for the parameter. Then, try the operation again.

CTGKM1115E Cannot change the device group of this device. It is associated with a key or key group.

Explanation:
Cannot change the device group. The device is associated with a key or key group.

System action:
Cannot change the device group. The device is associated with a key or key group.

Administrator response:
Cannot change the device group. The device is associated with a key or key group.

CTGKM1116E Cannot change the device group of this device. The symmetric key alias of this device is being used as the default symmetric key alias of the device group, and cannot be moved.

Explanation:
Cannot change the device group. The symmetric key alias of this device is being used as the default symmetric key alias of the device group, and cannot be moved.

System action:
The operation fails.

Administrator response:
Cannot change the device group. The symmetric key alias of this device is being used as the default symmetric key alias of the device group, and cannot be moved.

CTGKM1117E Cannot change the device group membership. The key is used by one or more devices.

Explanation:
Cannot change the device group membership. The key is used by one or more devices.

System action:
The operation fails.

Administrator response:
Cannot change the device group membership. The key is used by one or more devices.

CTGKM1118E Cannot change the device group membership. The certificate is used by one or more devices.

Explanation:
Cannot change the device group membership. The certificate is used by one or more devices.

System action:
The operation fails.

Administrator response:
Cannot change the device group membership. The certificate is used by one or more devices.

CTGKM1119E Cannot change the device group membership. The certificate is used by one or more devices.

Explanation:
Cannot change the device group membership. The certificate is used by one or more devices.

System action:
The operation fails.

Administrator response:
Cannot change the device group membership. The certificate is used by one or more devices.

CTGKM1120E Cannot change the device group membership. The symmetric key is used by one or more devices.

Explanation:
Cannot change the device group membership. The symmetric key is used by one or more devices.

System action:
The operation fails.

Administrator response:
Cannot change the device group membership. The symmetric key is used by one or more devices.

CTGKM1121E Cannot change the device group membership. The group is used by one or more devices.

Explanation:
Cannot change the device group membership. The group is used by one or more devices.

System action:
The operation fails.

Administrator response:

Cannot change the device group membership. The group is used by one or more devices.

CTGKM1122E Cannot change the device group membership. The symmetric key is used by one or more devices.

Explanation:
Cannot change the device group membership. The symmetric key is used by one or more devices.

System action:
The operation fails.

Administrator response:
Cannot change the device group membership. The symmetric key is used by one or more devices.

CTGKM1123E Cannot change the device group membership. The symmetric key is being used by another device group.

Explanation:
Cannot change the device group membership. The symmetric key is being used by another device group.

System action:
Cannot change the device group membership. The symmetric key is being used by another device group.

Administrator response:
Cannot change the device group membership. The symmetric key is being used by another device group.

CTGKM1124E Cannot change the device group membership. The symmetric key is being used by another device.

Explanation:
Cannot change the device group membership. The symmetric key is being used by another device.

System action:
The operation fails.

Administrator response:
Cannot change the device group membership. The symmetric key is being used by another device.

CTGKM1125E Cannot change the device group membership. The certificate is being used by another device group.

Explanation:
Cannot change the device group membership. The certificate is being used by another device group.

System action:
The operation fails.

Administrator response:
Cannot change the device group membership. The certificate is being used by another device group.

CTGKM1126E Cannot change the device group membership. The certificate is being used by another device group.

Explanation:
Cannot change the device group membership. The certificate is being used by another device group.

System action:
The operation fails.

Administrator response:
Cannot change the device group membership. The certificate is being used by another device group.

CTGKM1127E Cannot change the device group membership. The certificate is being used by another device.

Explanation:
Cannot change the device group membership. The certificate is being used by another device.

System action:
The operation fails.

Administrator response:
Cannot change the device group membership. The certificate is being used by another device.

CTGKM1129E Target and source device groups family type does not match.

Explanation:

System action:

Administrator response:

CTGKM1130E Cannot delete a device group when keys, certificates, groups, or devices are attached to that device group.

Explanation:

System action:

Administrator response:

CTGKM1131E Key Alias Device Group does not match the device.

Explanation:

System action:

Administrator response:

CTGKM1132E Symmetric Key Alias device group does not match device.

Explanation:

System action:

Administrator response:

CTGKM1133E Cannot delete family device groups.

Explanation:

System action:

Administrator response:

CTGKM1134E Device group already exists.

Explanation:

System action:

Administrator response:

CTGKM1135E Incorrect device group family *VALUE_0*

Explanation:
The device family must exist.

System action:
The operation fails.

Administrator response:
Specify an existing device family.

CTGKM1136E Group device group does not match the secret key device group usage.

Explanation:
The group device group must match the secret key device group.

System action:
The operation fails.

Administrator response:
Group device group does not match the secret key device group usage.

CTGKM1137E Cannot add an empty key group as the default symmetricKeySet.

Explanation:
The key group must have keys.

System action:
The operation fails.

Administrator response:
Cannot add an empty key group as the default symmetricKeySet.

CTGKM1138E No attributes were specified for the device group attribute update operation.

Explanation:
No attribute-value pairs were specified to update information for a device group attribute.

System action:
The operation fails.

Administrator response:
Collect available audit log information and contact IBM Support.

CTGKM1139E Incorrect value for device group name *VALUE_0*

Explanation:
The device group name must follow the requirement: 1. Can only contain alphanumeric characters and underscore. 2. First character cannot be a digit. 3. Maximum length is 256.

System action:
The operation fails.

Administrator response:
The device group name must follow the requirement: 1. Name can only contain alphanumeric character and underscore 2. First character cannot be a digit. 3. Maximum length should be 256.

CTGKM1140E Device family *VALUE_0* cannot be used to create a device group.

Explanation:
The specified device family cannot be used for this operation.

System action:
Device group not created.

Administrator response:
Specify a different device family. Then, try again.

CTGKM1141E aliasOne and aliasTwo are not valid attributes for the LTO device group and DS5000 device group.

Explanation:
Key aliasOne and aliasTwo are not used by LTO and DS5000 device groups.

System action:
Device not created or updated.

Administrator response:
Remove the attributes aliasOne and aliasTwo. Then, try the operation again.

CTGKM1142E symAlias is not a valid attribute for a DS8000 device group and 3592 device group.

Explanation:
symAlias is not used by DS8000 and 3592 device groups.

System action:
Device not created or updated.

Administrator response:
Remove the attribute symAlias. Then, try the operation again.

CTGKM1143E Cannot delete enableKMIPDelete attribute. enableKMIPDelete

attribute must have a value of true or false.

Explanation:
enableKMIPDelete attribute must have a value of true or false.

System action:
The operation fails.

Administrator response:
Do not run this command to delete the enableKMIPDelete attribute value.

CTGKM1144E Value for enableKMIPDelete attribute is not valid. A valid value is true or false.

Explanation:
Value for enableKMIPDelete attribute is not valid. A valid value is true or false.

System action:
The operation fails.

Administrator response:
Specify true or false for the enableKMIPDelete attribute and try the operation again.

CTGKM1145E Expired or inactive Key Alias cannot be set as default.

Explanation:
The defaultAlias1 or defaultAlias2 is expired or inactive

System action:
The operation fails.

Administrator response:
Specify a valid value for the parameter. Then, try the operation again.

CTGKM1146E The device group *VALUE_0* does not support secret keys.

Explanation:
The device group does not support secret keys.

System action:
The operation fails.

Administrator response:
Specify a device group that supports secret keys. Then, try the operation again.

CTGKM1147E The device group *VALUE_0* does not support certificates.

Explanation:
The device group does not support certificates.

System action:
The operation fails.

Administrator response:
Specify a device group that supports secret keys. Then, try the operation again.

CTGKM1148E Value for enableMachineAffinity attribute is not valid. A valid value is true or false.

Explanation:
Value for enableMachineAffinity attribute is not valid. A valid value is true or false.

System action:
The operation fails.

Administrator response:
Specify true or false for the enableMachineAffinity attribute and try the operation again.

CTGKM1149E Value for device.AutoPendingAutoDiscovery attribute is not valid. Valid values are 0, 1 and 2.

Explanation:
Value for device.AutoPendingAutoDiscovery attribute is not valid. Valid values are 0, 1 and 2.

System action:
The operation fails.

Administrator response:
Specify valid values (0,1,2) for device.AutoPendingAutoDiscovery attribute and try the operation again.

CTGKM1150E Cannot delete machineAffinity attribute. machineAffinity must have a value of true or false.

Explanation:
machineAffinity attribute must have a value of true or false.

System action:
The operation fails.

Administrator response:
Do not run this command to delete the machineAffinity attribute value.

CTGKM1151E Cannot delete device.AutoPendingAutoDiscovery attribute. device.AutoPendingAutoDiscovery must have a value of 0, 1 or 2.

Explanation:
device.AutoPendingAutoDiscovery attribute must have a value of 0, 1 or 2.

System action:
The operation fails.

Administrator response:
Do not run this command to delete the device.AutoPendingAutoDiscovery attribute value.

CTGKM1153E Cannot add a DS5000 family device with symAlias specified.

Explanation:
You attempted to create a DS5000 family device and associate it with a key group.

System action:
The device add operation fails.

Administrator response:
Do not specify symAlias. Then, try the operation again.

CTGKM1154E Cannot associate a device with an empty key group.

Explanation:
Cannot associate a device with an empty key group.

System action:
The device update operation fails.

Administrator response:
Specify a different symAlias. Then, try the operation again.

CTGKM1156E Conflicted key *VALUE_0* cannot be moved to a new device group.

Explanation:
Conflicted key cannot be moved to a new device group.

System action:
The key update operation fails.

Administrator response:
Specify a different key alias. Then, try the operation again.

CTGKM1157E Unknown key can be moved to either *VALUE_0* or *VALUE_1* or *VALUE_2* device group only.

Explanation

Date	Change description
10 Feb 2021	Corrected the instance of 'TLSServer' to 'SSLServer'. Refreshed only the English language content.
08 Dec 2020	Initial version.

Explanation:

Explanation:
Unknown key cannot be moved to a device group other than DS8000, 3592, SSLSERVER.

System action:
The key update operation fails.

Administrator response:
Specify a different device group. Then, try the operation again.

CTGKM1158E Conflicted certificate *VALUE_0* cannot be moved to a new device group.

Explanation:
Conflicted certificate cannot be moved to a new device group.

System action:
The certificate update operation fails.

Administrator response:
Specify a different certificate alias. Then, try the operation again.

CTGKM1159E Unknown certificate can be moved to either *VALUE_0* or *VALUE_1* or *VALUE_2* device group only.

Explanation

Date	Change description
10 Feb 2021	Corrected the instance of 'TLSServer' to 'SSLServer'. Refreshed only the English language content.
08 Dec 2020	Initial version.

Explanation:
Unknown certificate cannot be moved to a device group other than DS8000, 3592, SSLSERVER.

System action:
The certificate update operation fails.

Administrator response:
Specify a different device group. Then, try the operation again.

CTGKM1160E Unknown device can be moved to either *VALUE_0* or *VALUE_1* device group only.

Explanation:
Unknown device cannot be moved to a device group other than LTO, 3592.

System action:
The device update operation fails.

Administrator response:
Specify a different device group. Then, try the operation again.

CTGKM1161E Conflicted certificate cannot be specified for a default rollover. This certificate is not valid: *alias*

Explanation:

Conflicated certificate cannot be specified for a default rollover.

System action:
The add rollover operation fails.

Administrator response:
Specify a different certificate alias. Then, try the operation again.

CTGKM1162E The device group *VALUE_0* does not support keys.

Explanation:
The device group does not support keys.

System action:
The operation fails.

Administrator response:
Specify a device group that support keys. Then, try the operation again.

CTGKM1163E The key with alias *VALUE_0* cannot be moved. Keys belonging to a key group cannot be moved between device groups.

Explanation:
Keys are not allowed to be moved between device groups if that key is member of any key group.

System action:
The key update operation fails.

Administrator response:
Specify a key which does not belong to a key group, then try again.

CTGKM1200E Error getting device groups for device family *VALUE_0* .

Explanation:
Exception occurred during the process.

System action:
The operation fails.

Administrator response:
See the log for more details.

CTGKM1201E Error getting device families for device group *VALUE_0* .

Explanation:
Exception occurred during the process.

System action:
See the log for more details.

Administrator response:
See the log for more details.

CTGKM1202E Error getting a list of device groups.

Explanation:
Exception occurred during the process.

System action:
See the log for more details.

Administrator response:
See the log for more details.

CTGKM1203E Error creating device group *VALUE_0* .

Explanation:
Exception occurred during the process.

System action:
See the log for more details.

Administrator response:
See the log for more details.

CTGKM1204E Error deleting device group *VALUE_0* .

Explanation:
Exception occurred during the process.

System action:
See the log for more details.

Administrator response:
See the log for more details.

CTGKM1205E Error setting machine affinity.

Explanation:
Exception occurred during the process.

System action:
See the log for more details.

Administrator response:
See the log for more details.

CTGKM1206E Error setting auto pending.

Explanation:
Exception occurred during the process.

System action:
See the log for more details.

Administrator response:
See the log for more details.

CTGKM1207E Error getting devices referencing key group.

Explanation:
Exception occurred during the process.

System action:
See the log for more details.

Administrator response:
See the log for more details.

CTGKM1208E Error getting devices referencing certificate.

Explanation:
Exception occurred during the process.

System action:
See the log for more details.

Administrator response:
See the log for more details.

CTGKM1209E Concurrent update error. Another user might have changed the data.

Explanation:
Exception occurred while performing a concurrent update.

System action:
See the log for more details.

Administrator response:
Refresh and try again.

CTGKM1210E An error occurred while accepting the pending device.

Explanation:
The device may have already been accepted, there may be an error in the additional fields specified while accepting this device, or the IBM Security Guardium Key Lifecycle Manager database might not be available. Additional information should accompany this message.

System action:
The device may not have been accepted, or the device was accepted but additional fields specified for the device may not have been set.

Administrator response:
The additional information accompanying this message might guide your response. You might need to confirm that the database is available.

CTGKM1211E An error occurred while rejecting the pending device.

Explanation:
The device may have already been rejected by another user or the IBM Security Guardium Key Lifecycle Manager database might not be available. Additional information should accompany this message.

System action:
The device may not have been rejected.

Administrator response:
The additional information accompanying this message might guide your response. You might need to confirm that the database is available.

CTGKM1212E An error occurred while setting the default key group.

Explanation:
IBM Security Guardium Key Lifecycle Manager database might not be available. Additional information should accompany this message.

System action:
Cannot update the default key group.

Administrator response:
The additional information accompanying this message might guide your response.

CTGKM1213E An error occurred while setting the default certificate.

Explanation:
IBM Security Guardium Key Lifecycle Manager database might not be available. Additional information should accompany this message.

System action:
Cannot update the default certificate.

Administrator response:
The additional information accompanying this message might guide your response.

CTGKM1214E An error occurred while setting the partner certificate.

Explanation:
IBM Security Guardium Key Lifecycle Manager database might not be available. Additional information should accompany this message.

System action:
Cannot update the partner certificate.

Administrator response:
The additional information accompanying this message might guide your response.

CTGKM1215W Not all keys were made. Some aliases of the keys for the specified key group collided with another key group generated at the same time. You might want to use Modify Key Group panel to add additional keys.

Explanation:
There were key alias conflicts and the total number of keys requested could not be created.

System action:
No action required.

Administrator response:
Use Modify Key Group panel to add additional keys.

CTGKM1301E The key group *VALUE_0* cannot be set as a system or device default, because all its keys are compromised.

Explanation:
Key groups containing only compromised keys cannot be set as a system or device default.

System action:
The operation fails.

Administrator response:
Add non-compromised keys to the key group, or specify a different key group.

CTGKM1302E The private key algorithm is *VALUE_0*, which is not supported for usage *VALUE_1*. The supported algorithms are: *VALUE_2*

Explanation:
The private key uses an encryption algorithm which is not supported for the specified device group.

System action:
The operation fails.

Administrator response:
Change the usage, or specify another private key with an appropriate encryption algorithm. Then, try the operation again.

CTGKM1303E Unable to access keystore file *VALUE_0*.

Explanation:
Keystore file is missing or not readable.

System action:
The operation fails.

Administrator response:
Ensure that the specified file exists and has the correct permissions.

CTGKM1307E Keys could not be released because no backup has been made.

Explanation:
A backup is required before keys can be released.

System action:
The operation fails.

Administrator response:
Make a backup, then try the operation again.

CTGKM1308E The configuration property *VALUE_0* cannot be manually updated or deleted.

Explanation:
The configuration property cannot be manually updated or deleted.

System action:
The operation fails.

Administrator response:
No action required.

CTGKM1400E Machine ID cannot be null.

Explanation:
Machine ID is a required attribute.

System action:
The operation fails.

Administrator response:
Specify a valid machine ID.

CTGKM1401E Either machine ID or machine text is required.

Explanation:
Either machine ID or machine text is required.

System action:
The operation fails.

Administrator response:
Specify either the machine ID or machine text. Then, try the operation again.

CTGKM1402E Machine UUID cannot be null.

Explanation:
Machine UUID cannot be a null attribute.

System action:
The operation fails.

Administrator response:
Specify a value for the machine UUID.

CTGKM1403E Device group does not exist.

Explanation:
The specified device group is not a valid or known device group.

System action:
The operation fails.

Administrator response:
Specify another valid device group.

CTGKM1404E Device group is not a DS5000 device group.

Explanation:
The specified device group is not a DS5000 device group or a member of the DS5000 device family.

System action:
The operation fails.

Administrator response:
Specify a valid DS5000 device group or DS5000 device family.

CTGKM1405E Device UUID cannot be null.

Explanation:
The specified device UUID cannot be empty or null.

System action:
The operation fails.

Administrator response:
Specify a valid device UUID.

CTGKM1406E Device does not exist.

Explanation:

The specified device does not exist or is not a valid device in IBM Security Guardium Key Lifecycle Manager.

System action:
The operation fails.

Administrator response:
Specify a valid and known device group.

CTGKM1407E No machine IDs exist.

Explanation:
No machine IDs exist in IBM Security Guardium Key Lifecycle Manager.

System action:
The operation fails.

Administrator response:
No machine IDs exist.

CTGKM1408E Machine ID/Text not found.

Explanation:
This Machine ID/Text does not exist or is not valid.

System action:
The operation fails.

Administrator response:
Specify a valid machine identifier.

CTGKM1409E Machine affinity is ON. The device is associated with at least one machine and cannot be deleted or rejected.

Explanation:
Machine affinity is ON. The device is associated with at least one machine and cannot be deleted or rejected.

System action:
The operation fails.

Administrator response:
Delete the machine device association before trying to delete or reject the device.

CTGKM1410E Either Machine UUID, Machine Text, or Machine ID is required.

Explanation:
A value is required for either machine UUID, machine text, or machine ID.

System action:
The operation fails.

Administrator response:
Specify the machine UUID, machine text, or machine ID, and try again.

CTGKM1411E Machine Identifier field must be between 1 (minimum) and 48 (maximum) characters in length.

Explanation:
Machine Identifier field should be between 1 and 48 characters in length.

System action:
The operation fails.

Administrator response:
Specify a machine identifier that is between 1 (minimum) and 48 (maximum) characters in length.

CTGKM1416E The specified machine must exist for the operation to succeed.

Explanation:
Machine device association cannot be added. The machine does not exist.

System action:
The operation fails.

Administrator response:
Specify a valid machine identifier for this association.

CTGKM1417E Machine does not exist and cannot be updated.

Explanation:
Machine lookup failed. It appears the machine does not exist.

System action:
The operation fails.

Administrator response:
Specify a valid machine identifier to update.

CTGKM1418E Machine text is not unique.

Explanation:
Machine text is not unique. There is already a machine ID with that machine text.

System action:
The operation fails.

Administrator response:
Specify a unique string for the machine text.

CTGKM1419E Machine has existing machine affinities.

Explanation:
The machine has existing machine affinities.

System action:
The operation fails.

Administrator response:
Delete all machine affinities before deleting the machine ID.

CTGKM1420E Device text is not unique.

Explanation:
There is already a device with that device text.

System action:
The operation fails.

Administrator response:
Specify a different unique device text.

CTGKM1422E serialNumber cannot be updated with the device group.

Explanation:
A serial number update is not supported for the device group.

System action:
The operation fails.

Administrator response:
Do not use a serial number as an attribute for this action.

CTGKM1423E *VALUE_0* is not allowed for a non-DS5000 device group.

Explanation:
This attribute is not allowed for a non-DS5000 device group.

System action:
The operation fails.

Administrator response:
Do not use this attribute for this action.

CTGKM1425E The machine device association or the device is not pending.

Explanation:
The machine device association or the device has been accepted or is not in pending status.

System action:
No action taken.

Administrator response:
You cannot accept a nonpending machine/device.

CTGKM1426E Machine ID is not unique.

Explanation:
The machine ID given is not unique in IBM Security Guardium Key Lifecycle Manager.

System action:
The operation fails.

Administrator response:
Specify a valid unique machine identifier.

CTGKM1427E Machine affinity already exists.

Explanation:
Machine affinity for this device and machine already exists in IBM Security Guardium Key Lifecycle Manager.

System action:
The operation fails.

Administrator response:
Specify a different unique machine identifier and device.

CTGKM1429E The DS5000 number of keys cannot exceed 12.

Explanation:
The DS5000 number of keys cannot exceed 12.

System action:
The operation fails.

Administrator response:
Specify a value between 0 and 12 for the number of keys.

CTGKM1430E This device has pending machine affinities. Reject the pending machine affinities first.

Explanation:
This pending device has pending machine affinities. Reject the pending machine affinities first.

System action:
The operation fails.

Administrator response:
Reject the pending machine affinities first.

CTGKM1431E Value for DS5000 number of keys is not valid. The value must be a positive integer.

Explanation:
The value for the DS5000 number of keys can only be a positive integer.

System action:
The operation fails.

Administrator response:
Specify a positive integer for the number of keys.

CTGKM1432E symmetricKeySet is not a valid attribute for a DS5000 device group.

Explanation:
symmetricKeySet is not used by DS5000.

System action:
Device group not created or updated.

Administrator response:
Remove the symmetricKeySet attribute and try the operation again.

CTGKM1433E Values for machineText *VALUE_1* and machineID *VALUE_0* do not match.

Explanation:
MachineText and MachineID do not match.

System action:
Machine device will not be listed.

Administrator response:

Specify a different value for machineText or machineID and try the operation again.

CTGKM1434E Machine Text must be between 1 and 96 characters in length.

Explanation:
The value of the machineText parameter must be between 1 and 96 characters in length.

System action:
The operation fails.

Administrator response:
Specify a value for the machineText parameter between 1 and 96 characters in length.

CTGKM1435E Machine ID/Text does not match the Machine UUID.

Explanation:
Machine ID/Text does not match the machine with the specified UUID.

System action:
The operation fails.

Administrator response:
Specify a different value for Machine ID/Text.

CTGKM1436E No machine affinity between device *VALUE_0* and machine *VALUE_1*.

Explanation:
Machine affinity is only supported for DS5000 devices.

System action:
The operation fails.

Administrator response:
Specify a DS5000 device.

CTGKM1500E NULL attribute array.

Explanation:
No attributes were specified for a new template.

System action:
The template is not created.

Administrator response:
Specify attributes for the template, then try the operation again.

CTGKM1501E Found inappropriate attribute for template: *VALUE_0*

Explanation:
The specified attribute is not supported by the template.

System action:
The template is not created.

Administrator response:
Remove or change the unsupported attribute, then try the operation again.

CTGKM1502E NULL template names array.

Explanation:
No template names were specified to be merged.

System action:
The template merge fails.

Administrator response:
Specify template names to be merged, then try the operation again.

CTGKM1503E Template with name *VALUE_0* not found.

Explanation:
The specified template was not found in the database.

System action:
The message processing fails because the template attributes cannot be read.

Administrator response:
Specify the correct template name and try again.

CTGKM1504E The authentication information in the request was not able to be validated, or there was no authentication information in the request when there SHOULD have been.

Explanation:
The authentication information is either missing or not valid.

System action:
The authentication failed because the information provided is not valid or missing.

Administrator response:
Specify the correct authentication information and try again.

CTGKM1505E The client does not have permission to perform the requested operation.

Explanation:
The client is not authorized to perform the requested operation.

System action:
The requested operation failed because the client does not have the permission.

Administrator response:
Make sure that the requested operation is authorized and retry the action.

CTGKM1506E The operation failed due to a cryptographic error.

Explanation:
The requested operation failed due to a cryptographic error.

System action:
The requested operation failed because the key cannot be read due to a cryptographic error.

Administrator response:
Please look at the exception message and take appropriate action.

CTGKM1507E An OPTIONAL feature specified in the request is not supported.

Explanation:
The requested OPTIONAL feature is not supported.

System action:
The request failed because the feature is not supported.

Administrator response:
Remove or change the feature, then try the operation again.

CTGKM1508E The client requested an operation that was not able to be performed with the specified parameters.

Explanation:
The specified parameters are not valid for the requested operation.

System action:
The requested operation failed because the specified parameters are not valid.

Administrator response:
Specify the correct parameters and try again.

CTGKM1509E Some data item in the request has an incorrect value.

Explanation:
Some of the parameter value in the request is not valid.

System action:
The requested operation failed because one or more of the attributes has an incorrect value.

Administrator response:
Make sure to pass in the correct attribute values and retry the action.

CTGKM1510E The request message was not understood by the server.

Explanation:
The message in the request was not understood by the server.

System action:
The processing of the message failed because it was not understood by the server.

Administrator response:
Specify the correct message in the request and try again.

CTGKM1511E A requested object was not found or did not exist.

Explanation:
The requested object was not found.

System action:
The requested operation failed because the object did not exist.

Administrator response:
Make sure to pass the identifier for the existing object and retry the action.

CTGKM1512E The operation requires additional OPTIONAL information in the request, which is not present.

Explanation:
The request is missing the OPTIONAL information required for the operation.

System action:
The requested operation failed because it is missing the OPTIONAL information required.

Administrator response:
Make sure to pass in the required OPTIONAL information and retry the action.

CTGKM1513E The object must be recovered from the archive before performing the operation.

Explanation:
The requested object is archived.

System action:
The requested operation failed because the object is archived.

Administrator response:
Make sure that the object is recovered and retry the action.

CTGKM1514E The operation was asynchronous, and the operation was canceled by the Cancel operation before it completed successfully.

Explanation:
The asynchronous operation was canceled before it completed successfully.

System action:
The requested operation failed because it was canceled before it completed successfully.

Administrator response:
No action required.

CTGKM1515E The operation requested by the request message is not supported by the server.

Explanation:

The requested operation is not supported by the server.

System action:
The requested operation failed because it is not supported by the server.

Administrator response:
Specify a supported operation then try the operation again.

CTGKM1516E The response to a request would exceed the maximum response size in the request.

Explanation:
The response size exceeds the maximum response size specified in the request.

System action:
The requested operation failed because the response size exceeds the maximum response size specified in the request.

Administrator response:
Increase the maximum response size in the request, then try the operation again.

CTGKM1517E Value out of range.

Explanation:
The specified value is out of range.

System action:
The requested operation failed because the value specified is out of the enumerated list.

Administrator response:
Specify the correct value and retry the action.

CTGKM1520E The server was not able to perform the requested operation.

Explanation:
An unexpected error occurred on the KMIP server.

System action:
This error is returned to the KMIP client.

Administrator response:
Please look at the exception message and take appropriate action.

CTGKM1521E The operation failed due to an inappropriate index.

Explanation:
The caller passed an incorrect index on a multivalued attribute.

System action:
This error is returned to the KMIP client.

Administrator response:
Specify another index, and try the operation again.

CTGKM1522E Attribute *VALUE_0* is not supported.

Explanation:
Attribute name is unknown or unsupported.

System action:
The operation fails.

Administrator response:
Specify a supported attribute name, and try the operation again.

CTGKM1523E Index must be specified for update or delete operation on a multivalued attribute.

Explanation:
Index was not specified for an update or delete operation on a multivalued attribute.

System action:
The operation fails.

Administrator response:
Specify an index, and try the operation again.

CTGKM1524E The operation *VALUE_0* is not supported.

Explanation:
The operation is not supported.

System action:
The operation fails.

Administrator response:
Specify a supported operation name, then try again.

CTGKM1525E The field *VALUE_0* is not supported for the attribute *VALUE_1*.

Explanation:
The field provided is not supported for the attribute.

System action:
The operation fails.

Administrator response:
Specify a field that is supported for the attribute, then try the operation again.

CTGKM1526E Date must be in the format *VALUE_0*, and represent a valid date.

Explanation:
The date supplied is not valid.

System action:
The operation fails.

Administrator response:
Specify a valid date in the correct format, then try the operation again.

CTGKM1527E Attribute values must be specified for add or update operation.

Explanation:
The add and update attributes operations require that attribute values be specified.

System action:
The operation fails.

Administrator response:
Specify the attribute values, then try the opreation again.

CTGKM1528E *VALUE_0* fields must be specified for attribute *VALUE_1*.

Explanation:
The listed fields are required when adding or updating this attribute.

System action:
The operation fails.

Administrator response:
Specify values for all the listed fields, then try the operation again.

CTGKM1529E Name for a custom attribute must begin with either *VALUE_0* or *VALUE_1*.

Explanation:
The name for a custom KMIP attribute must follow the stated requirements.

System action:
The operation fails.

Administrator response:
Specify a custom attribute name that meets the requirements, then try the operation again.

CTGKM1530E The value *VALUE_0* is not supported for the field *VALUE_1*.

Explanation:
The value is not supported for the specified field.

System action:
The operation fails.

Administrator response:
Specify a supported value, then try the operation again.

CTGKM1531E The value exceeds the limit for a multi-valued attribute.

Explanation:
The value exceeds the limit for a multi-valued attribute set by the IBM Security Guardium Key Lifecycle Manager server.

System action:
The operation fails.

Administrator response:
Set the property mv.attribute.max.values in SKLMConfig.properties file to a higher value and try again.

CTGKM1532E Value contains reserved wildcard characters that are not allowed.

Explanation:
The specified value contains reserved wildcard characters such as (* and %).

System action:
The requested operation failed because the value specified is not valid.

Administrator response:
Specify the correct value and retry the action.

CTGKM1533E The request cannot be processed.

Explanation:
The request from this device cannot be processed.

System action:
The requested operation fails.

Administrator response:
Check the setting for accepting devices for this device group through the graphical user interface. Take appropriate action either to accept this device from the pending list or set the flag to automatically accept all new devices. Then try the request again.

CTGKM1534E The request cannot be processed.

Explanation:
An internal error occurred and the request from this device cannot be processed.

System action:
The requested operation fails.

Administrator response:
Check the setting for accepting devices for this device group through the graphical user interface. Then retry the action.

CTGKM1535E *VALUE_0* is too large.

Explanation:
The object or attribute is oversized and cannot be processed.

System action:
The operation fails.

Administrator response:
The key bytes length exceeds the maximum length 8K supported by the keystore. Try again with a reduced size.

CTGKM1536E Key must be specified.

Explanation:
The key to create or register is not specified in the request.

System action:
The requested operation fails.

Administrator response:
Specify the key, then try the operation again.

CTGKM1537E Key group *VALUE_0* does not exist.

Explanation:
The specified key group in the request does not exist.

System action:
The requested operation fails.

Administrator response:
Specify an existing key group, then try the operation again.

CTGKM1538E Usage mask must be specified.

Explanation:
The usage mask must be specified for a symmetric key in the request.

System action:
The requested operation fails.

Administrator response:
Specify the usage mask, then try the operation again.

CTGKM1539E Algorithm *VALUE_0* not supported.

Explanation:
Algorithm not supported for the requested operation.

System action:
The requested operation fails.

Administrator response:
Specify a supported algortihm, then try the operation again.

CTGKM1540E Key size *VALUE_0* not supported for algorithm *VALUE_1*.

Explanation:
Key size is not supported for the algorithm specified in the request.

System action:
The requested operation fails.

Administrator response:
Ensure that the key size specified is supported by the algorithm. Try the operation again.

CTGKM1541E Unexpected key type, only register of SecretKey supported.

Explanation:
To register a key, it must be of type javax.crypto.SecretKey in the request.

System action:
The requested operation fails.

Administrator response:
Specify a key of type SecretKey, then try the operation again.

CTGKM1542E JCE problem with DESede or AES while generating a secret key.

Explanation:
JCE unable to generate a secret key with algorithm DESede or AES.

System action:
The requested operation fails.

Administrator response:
Ensure that the JCE provider supports the requested algorithm and try again.

CTGKM1543E Algorithm *VALUE_0* not supported by the provider for hashing.

Explanation:
The algorithm is not supported by the provider.

System action:
The requested operation fails.

Administrator response:
Specify an algorithm that is supported by the provider, then try the operation again.

CTGKM1544E The following attribute(s) are not allowed for the *VALUE_0* operation: *VALUE_1*

Explanation:
Some of the attributes are not allowed for the requested operation.

System action:
The requested operation fails.

Administrator response:
Remove the attributes that are not allowed, and try the operation again.

CTGKM1545E y-KeyGroupGetNext must supply a key group name.

Explanation:
The y-KeyGroupGetNext custom server attribute must supply a key group name.

System action:
The requested operation fails.

Administrator response:
Specify a key group name, then try the operation again.

CTGKM1546E An object with the nametype of *VALUE_0* and the namevalue of *VALUE_1* already exists.

Explanation:
The caller is trying to reuse an existing name for an object.

System action:
The requested operation fails.

Administrator response:
Specify a different nametype/namevalue. Then try the operation again.

CTGKM1547E This *VALUE_0* requires an instance of *VALUE_1*.

Explanation:
The caller is trying to set an unsupported value.

System action:
The requested operation fails.

Administrator response:
Specify a supported value, then try the operation again.

CTGKM1548E Unsupported object type: *VALUE_0*

Explanation:
The caller is requesting an operation on an unsupported object type.

System action:
The requested operation fails.

Administrator response:
Specify a supported object type, then try the operation again.

CTGKM1549E StorageStatusMask: *VALUE_0* is not valid.

Explanation:
The caller is requesting an unsupported storage status mask.

System action:
The requested operation fails.

Administrator response:
Specify a supported storage status mask and try the operation again.

CTGKM1550E No search attributes were specified on the LOCATE request.

Explanation:
The caller omitted required parameters.

System action:
The requested operation fails.

Administrator response:
Specify the search attributes in the LOCATE request, then try again.

CTGKM1551E The *VALUE_0* operation is not valid for an object of type *VALUE_1*.

Explanation:
The caller requested an operation that is inappropriate for that object.

System action:
The requested operation fails.

Administrator response:
Specify an operation supported for the object, then try again.

CTGKM1552E The *VALUE_0* attribute requires a non-null value.

Explanation:
The attribute cannot contain a null value.

System action:
Cannot process the message.

Administrator response:
Ensure that the attribute value is non-null, then try again.

CTGKM1553E The attribute name is not specified.

Explanation:
The attribute name is not specified.

System action:
The requested operation fails.

Administrator response:
Specify the attribute name, then try the operation again.

CTGKM1554E The attribute *VALUE_0* does not exist.

Explanation:
The specified attribute does not exist.

System action:
The requested operation fails.

Administrator response:
Specify an existing attribute, then try the operation again.

CTGKM1555E The index *VALUE_0* is not valid for a single-valued attribute.

Explanation:
For a single-valued attribute, the index can only be 0.

System action:
The requested operation fails.

Administrator response:
Specify the correct index for a single-valued attribute, then try the operation again.

CTGKM1556E The value at index *VALUE_0* does not exist.

Explanation:
The value at the specified index does not exist.

System action:
The requested operation fails.

Administrator response:

Ensure that a value exists at the specified index. Then, try the operation again.

CTGKM1557E Could not construct *VALUE_0* from the input provided. Underlying field name or error message *VALUE_1*

Explanation:
The caller provided input that could not be processed.

System action:
The requested operation fails.

Administrator response:
Specify a correct value for this attribute, then try the operation again.

CTGKM1558E No key material is available for the object with identifier *VALUE_0*.

Explanation:
No key material is available, possibly because none was ever sent to the server.

System action:
The requested operation fails.

CTGKM1559E No key material is available for the object with identifier *VALUE_0*. The object has been destroyed.

Explanation:
No key material exists on the server because the object has been destroyed.

System action:
The requested operation fails.

CTGKM1560E Object with UUID *VALUE_0* and type *VALUE_1* does not exist.

Explanation:
An object with the specified UUID and type does not exist.

System action:
The requested operation fails.

Administrator response:
Specify another UUID and type, then try the operation again.

CTGKM1561E Object with UUID *VALUE_0* could not be served for cryptographic use because it is not backed up.

Explanation:
Object with the specified UUID cannot be served for cryptographic use because it is not backed up.

System action:
The requested operation fails.

Administrator response:
Back up IBM Security Guardium Key Lifecycle Manager, then try the operation again.

CTGKM1562E Cannot register a key in a key group if no key material is supplied by the caller.

Explanation:
Keys that are in key groups must contain cryptographic material, but the caller is not providing any.

System action:
The requested operation fails.

CTGKM1563E Object with UUID *VALUE_0* could not be served for cryptographic use because it is not released.

Explanation:
Object with the specified UUID cannot be served for cryptographic use because it is not released. This message may also occur if the config property release.date is missing or wrongly formatted.

System action:
The requested operation fails.

Administrator response:
Run the tklmKeyRelease command to release keys, then try the operation again.

CTGKM1701E For DS5000 device group, device text must be less than 96 characters in length.

Explanation:
For the DS5000 device group, the value of the deviceText parameter must be less than 96 characters in length.

System action:
The operation fails.

Administrator response:
For DS5000 devices, specify a value for deviceText that is less than 96 characters in length.

CTGKM1702E Unable to generate more than 12 keys at a time for DS5000 group.

Explanation:
DS5000 keys can only generated 12 or less at a time.

System action:
The operation fails.

Administrator response:
Reduce the number of requested keys and try the operation again.

CTGKM1703E Incorrect device group ID : *VALUE_0*

Explanation:
Device group ID is not found.

System action:
The operation fails.

Administrator response:
Change the device group and try the operation again.

CTGKM1704E Device description cannot exceed 255 characters in length.

Explanation:
The device description exceeded 255 characters in length.

System action:
The operation fails.

Administrator response:
Change to a shorter description and try the operation again.

CTGKM1706E The certificate *VALUE_0* is scheduled for a future rollover, and cannot be moved or deleted.

Explanation:
A certificate which is scheduled for a future rollover cannot be moved or deleted.

System action:
The operation fails.

Administrator response:
Remove any pending rollovers for this certificate, then try the operation again.

CTGKM1707E The key group *VALUE_0* is scheduled for a future rollover, and cannot be moved or deleted.

Explanation:
A key group which is scheduled for a future rollover cannot be moved or deleted.

System action:
The operation fails.

Administrator response:
Remove any pending rollovers for this key group, then try the operation again.

CTGKM1901E Device group: *VALUE_0* is not a valid group for license count.

Explanation:
This device group must be one of the valid device groups listed in the license list.

System action:
Specify a correct group name.

Administrator response:
Specify a correct group name.

CTGKM1920E License feature is not enabled.

Explanation:
License feature can be enabled by setting enableLicenseCount to be true in the vendordata properties file under the agreement with IBM in the preinstall process of OEM skinning.

System action:
This indicates that the license feature is not enabled on this version of <keyword conref = "../../common/common.dita#common/tklmshort"/> .

Administrator response:
This indicates that the license feature is not enabled on this version of <keyword conref = "../../common/common.dita#common/tklmshort"/> .

CTGKM1921E Error occurred while trying to parse the license file. Key may be corrupted.

Explanation:
Error occurred while trying to parse the license file. Key may be corrupted.

System action:
The operation fails.

Administrator response:
This error should not occur. Contact IBM Support.

CTGKM1922E Error occurred while reading the license file. Verify that the specified file name is correct and the file is readable.

Explanation:
Error occurred while reading the license file. Verify that the specified file name is correct and the file is readable.

System action:
There is a problem reading the license file. Verify that the specified file name is correct and the file is readable.

Administrator response:
There is a problem reading the license file. Verify that the specified file name is correct and the file is readable.

CTGKM1923E InvalidKeyException occurred while trying to parse the license file.

Explanation:
InvalidKeyException occurred while trying to parse the license file.

System action:
Verify which Java security policy file is used in the JVM bundled with <keyword conref = "../../common/common.dita#common/tklmshort"/> . Contact IBM Support for further assistance.

Administrator response:
Verify which Java security policy file is used in the JVM bundled with <keyword conref = "../../common/common.dita#common/tklmshort"/> . Contact IBM Support for further assistance.

CTGKM1924E Error occurred while trying to parse the license file. Cipher initialization error.

Explanation:
Error occurred while trying to parse the license file, which is due to cipher initialization error.

System action:
The error may be due to jar files in the <keyword conref = "../../common/common.dita#common/tklmshort"/> JVM that are altered. Contact IBM Support for assistance.

Administrator response:
The error may be due to jar files in the <keyword conref = "../../common/common.dita#common/tklmshort"/> JVM that are altered. Contact IBM Support for assistance.

CTGKM1925E Unable to decrypt the license file.

Explanation:
Either the data in the license file are bad data, or the Cipher used for decryption is not initialized properly.

System action:
Verify that the license file is good. If the problem still exists, contact IBM Support.

Administrator response:
Verify that the license file is good. If the problem still exists, contact IBM Support.

CTGKM1926E Error occurred while parsing the content in the license file

Explanation:
After the license file is decrypted, the license content is processed. The error may be due to license content that was not generated properly.

System action:
Contact the license issuer for assistance.

Administrator response:
Contact the license issuer for assistance.

CTGKM1927E Incorrect license file. Device group name is missing.

Explanation:
After the license file is decrypted, the license content is processed. The error indicates that the device group name is not specified in the license.

System action:
Contact the license issuer for assistance.

Administrator response:
Contact the license issuer for assistance.

CTGKM1928E Incorrect license file. Timestamp is missing.

Explanation:
After the license file is decrypted, the license content is processed. The error indicates that the timestamp is not specified in the license.

System action:
Contact the license issuer for assistance.

Administrator response:
Contact the license issuer for assistance.

CTGKM1929E Incorrect license file. Timestamp value is not valid: *VALUE_0*.

Explanation:
After the license file is decrypted, the license content is processed. The error indicates that the timestamp specified in the license file is not correct.

System action:
Contact the license issuer for assistance.

Administrator response:
Contact the license issuer for assistance.

CTGKM1930E Incorrect license file. License count is missing.

Explanation:
After the license file is decrypted, the license content is processed. The error indicates that the license count is not found in the file.

System action:
Contact the license issuer for assistance.

Administrator response:
Contact the license issuer for assistance.

CTGKM1931E Incorrect license file. License count is not valid: *VALUE_0*.

Explanation:
After the license file is decrypted, the license content is processed. The error indicates that the license count value specified in the license file is not correct.

System action:
Contact the license issuer for assistance.

Administrator response:
Contact the license issuer for assistance.

CTGKM1932E No device group is enabled for license counting.

Explanation:
The device group list is specified in the vendordata properties file. The error indicates that the list is empty.

System action:
Contact IBM Support for assistance.

Administrator response:
Contact IBM Support for assistance.

CTGKM1933E License counting is not enabled for the specified device group: *VALUE_0*.

Explanation:
The specified device group is not in the list of the groups that have the license feature enabled.

System action:
Contact the license issuer for assistance.

Administrator response:
Contact the license issuer for assistance.

CTGKM1934E Unable to get license count information.

Explanation:
Unable to retrieve data for license count.

System action:
Contact the license issuer for assistance.

Administrator response:
Check the log entries to find out the reason for the failure. Make appropriate changes. Then, try the operation again.

CTGKM1935E The timestamp in the license file matches the license timestamp for the same device group in the database. Import failed.

Explanation:
You cannot import the same license file again. If the timestamp in the license file matches the timestamp of the license for the same device group, the import operation fails.

System action:
Do not import this license file.

Administrator response:
Do not import this license file.

CTGKM1936E dateAfter cannot be later than dateBefore.

Explanation:
dateAfter is after dateBefore. This will give an empty time interval.

System action:
The operation fails.

Administrator response:
Specify different dateAfter and dateBefore values, and try the operation again.

CTGKM2100E The value for replication.role is not valid. Accepted values are CLONE or MASTER.

Explanation:
The value for the replication.role must be CLONE or MASTER.

System action:
The operation fails.

Administrator response:
Correct setting of replication.role parameter to CLONE or MASTER.

CTGKM2103E The value for replication.MaxLogFileSize is not valid. Acceptable values are between 100 and 500000 bytes.

Explanation:
The replication log file size can be between 100 and 500000 bytes.

System action:
The operation fails.

Administrator response:
Correct setting of replication.MaxLogFileSize.

CTGKM2104E The value for replication.MaxLogFileNum is not valid. Acceptable values are between 2 and 100.

Explanation:
The value for replication.MaxLogFileNum must be between 2 and 100.

System action:
The operation fails.

Administrator response:
Correct setting of replication.MaxLogFileNum.

CTGKM2105E The value for replication.MaxBackupNum is not valid. Acceptable values are between 2 and 10.

Explanation:
The value for replication.MaxBackupNum must be between 2 and 10.

System action:
The operation fails.

Administrator response:
Correct setting of replication.MaxBackupNum.

CTGKM2106E Value for replication.MasterListenPort is not valid. Acceptable values are integers between 1 and 65535.

Explanation:
Valid values for replication.MasterListenPort are integers between 1 and 65535.

System action:
The operation fails.

Administrator response:
Correct setting of replication.MasterListenPort.

CTGKM2107E Value for replication.MasterListenPort is not a valid port number or is used as a port elsewhere in IBM Security Guardium Key Lifecycle Manager.

Explanation:
replication.MasterListenPort is not a valid port number, or is the same as one of restore.ListenPort, TransportListener.tcp.port, KMIPListener.ssl.port or TransportListener.ssl.port.

System action:
The operation fails.

Administrator response:
Correct setting of replication.MasterListenPort to a valid, available port number.

CTGKM2108E Value for the backup.CheckFrequency is not valid. Acceptable values are integers equal to or greater than 1.

Explanation:
Valid values for backup.CheckFrequency are integers equal to or greater than 1.

System action:
The operation fails.

Administrator response:
Correct setting of backup.CheckFrequency to be an integer equal to or greater than 1.

CTGKM2109E Command ignored. Backup time has already been set.

Explanation:
Command ignored. Backup time has already been set as per the backup.DailyStartReplicationBackupTime parameter.

System action:
Command ignored.

Administrator response:
No action required.

CTGKM2110E Value of backup.DailyStartReplicationBackupTime is not valid. It should be in HH:MM format.

Explanation:
Value of backup.DailyStartReplicationBackupTime should be a valid time in HH:MM format.

System action:
The operation fails.

Administrator response:
Correct backup.DailyStartReplicationBackupTime to be a valid time in HH:MM format.

CTGKM2112E The value for backup.BackupDescriptionText must not exceed 100 characters.

Explanation:
The value for backup.BackupDescriptionText must not exceed 100 characters.

System action:
The operation fails.

Administrator response:
Correct backup.BackupDescriptionText such that it does not exceed 100 characters.

CTGKM2113E The value for backup.ReleaseKeys is not valid. Accepted values are RESTORE, BACKUP or OFF.

Explanation:
The value for backup.ReleaseKeys must be one of RESTORE, BACKUP or OFF.

System action:
The operation fails.

Administrator response:
Correct backup.ReleaseKeys to be one of RESTORE, BACKUP or OFF.

CTGKM2114E Command ignored. To update this property, make sure the value of the enableKeyRelease parameter in the IBM Security Guardium Key Lifecycle Manager configuration file has been set to true.

Explanation:
In order to update the backup.ReleaseKeys, the value of the enableKeyRelease parameter in the IBM Security Guardium Key Lifecycle Manager configuration file should have been already set to true.

System action:
The operation fails.

Administrator response:
No action required.

CTGKM2115E restore.ListenPort parameter is not a valid port number. Accepted values are integers between 1 and 65535.

Explanation:
The value of restore.ListenPort parameter should be an integer between 1 and 65535.

System action:
The operation fails.

Administrator response:
Correct restore.ListenPort to be a valid port number.

CTGKM2116E The value of restore.ListenPort must not be shared with any other IBM Security Guardium Key Lifecycle Manager port parameter settings.

Explanation:
The value for the restore.ListenPort parameter cannot be the same as values for the replication.MasterListenPort, TransportListener.tcp.port, KMIPListener.ssl.port or TransportListener.ssl.port.

System action:
The operation fails.

Administrator response:
Correct restore.ListenPort to be a valid port number not used elsewhere in IBM Security Guardium Key Lifecycle Manager.

CTGKM2117E Value of restore.DailyStartReplicationRestoreTime is not valid. It should be in HH:MM format.

Explanation:
The value for restore.DailyStartReplicationRestoreTime should be a valid time in HH:MM format.

System action:
The operation fails.

Administrator response:
Correct restore.DailyStartReplicationRestoreTime to be a valid time in HH:MM format.

CTGKM2118E The value for the restore.NumAttemptRetryFailedRestore parameter must be between 0 and 2.

Explanation:
The value for the restore.NumAttemptRetryFailedRestore parameter must be between 0 and 2.

System action:
The operation fails.

Administrator response:
Correct restore.NumAttemptRetryFailedRestore to be between 0 and 2.

CTGKM2119E Value for restore.RevertToPreviousBackupOnFailure must be either true or false.

Explanation:
Value for configuration parameter restore.RevertToPreviousBackupOnFailure can only be either true or false.

System action:
The operation fails.

Administrator response:
Correct restore.RevertToPeviousBackupOnFailure to be either true or false.

CTGKM2120E Value for the backup.ClientPort(n) parameter must be an integer between 1 and 65535.

Explanation:
Value for the backup.ClientPort(n) parameter must be an integer between 1 and 65535.

System action:
The operation fails.

Administrator response:
Correct backup.ClientPort(n) to be an integer between 1 and 65535.

CTGKM2121E backup.ClientPort must not be shared with any other IBM Security Guardium Key Lifecycle Manager port parameter settings.

Explanation:
The value for the backup.ClientPort parameter cannot be the same as values for the replication.MasterListenPort, TransportListener.tcp.port, KMIPListener.ssl.port or TransportListener.ssl.port.

System action:
The operation fails.

Administrator response:
Correct restore.ListenPort to be a valid port number not used elsewhere in IBM Security Guardium Key Lifecycle Manager.

CTGKM2122E backup.EncryptionPassword must not be fewer than 6 characters or exceed 175 single-byte or 87 double-byte characters.

Explanation:
backup.EncryptionPassword cannot be null, fewer than 6 characters or longer than 175 single-byte or 87 double-byte characters.

System action:
The operation fails.

Administrator response:
Correct backup.EncryptionPassword to a valid value.

CTGKM2123E The backup.ObfuscatedEncryptionPassword parameter cannot be updated.

Explanation:

The backup.ObfuscatedEncryptionPassword parameter cannot be updated.

System action:
The operation fails.

Administrator response:
No action required.

CTGKM2124E The StopReplication has timed out!.

Explanation:
The StopReplication has timed out!.

System action:
The operation fails.

Administrator response:
No action required.

CTGKM2125E restore.TipadminPassword must not be fewer than 6 or more than 20 characters.

Explanation:
restore.TipadminPassword cannot be shorter than 6 characters or longer than 20 characters.

System action:
The operation fails.

Administrator response:
Correct restore.TipadminPassword to a valid value.

CTGKM2126E The restore.ObfuscatedTipadminPassword parameter cannot be updated.

Explanation:
The restore.ObfuscatedTipadminPassword parameter cannot be updated.

System action:
The operation fails.

Administrator response:
No action required.

CTGKM2201W Replication already in progress.

Explanation:
Replication request rejected as one is already in progress.

System action:
No action necessary.

Administrator response:
Re-try replication when the currently running one has completed.

CTGKM2202E Replication failed for

Explanation:
Replication has failed for the host listed.

System action:
No action necessary.

Administrator response:
No action necessary.

CTGKM2203E Replication failed with a connection error

Explanation:
Replication has failed for the host listed with a connection error.

System action:
Check debug for exceptions.

Administrator response:
Ensure that the hosts and ports listed are available.

CTGKM2204E Replication failed with a validation error

Explanation:
Replication has failed for the host listed with a validation error.

System action:
Check debug for exceptions.

Administrator response:
Check debug for exceptions.

CTGKM2206E IBM Security Guardium Key Lifecycle Manager Replication task has failed to start.

Explanation:
IBM Security Guardium Key Lifecycle Manager Replication start command has failed.

System action:
No action necessary.

Administrator response:
See other error messages for further explanation.

CTGKM2207W IBM Security Guardium Key Lifecycle Manager Replication task is already up.

Explanation:
IBM Security Guardium Key Lifecycle Manager Replication start command has been ignored as the task is already up.

System action:
No action necessary.

Administrator response:
No action necessary.

CTGKM2209E IBM Security Guardium Key Lifecycle Manager Replication task has failed to stop.

Explanation:

IBM Security Guardium Key Lifecycle Manager Replication stop command has failed.

System action:
No action necessary.

Administrator response:
See other error messages for further explanation.

CTGKM2210W IBM Security Guardium Key Lifecycle Manager Replication task is already down.

Explanation:
IBM Security Guardium Key Lifecycle Manager Replication stop command has been ignored as the task is already down.

System action:
No action necessary.

Administrator response:
No action necessary.

CTGKM2211E Command failed as the -confirm parameter is not set to Y.

Explanation:
IBM Security Guardium Key Lifecycle Manager Replication stop command will not work without the confirm parameter being specified as Y.

System action:
No action necessary.

Administrator response:
If stop is required, rerun the command with the -confirm parameter set to Y.

CTGKM2212E Replication timed out

Explanation:
Replication for the specified host timed out.

System action:
Check debug log.

Administrator response:
Correct any problems on master or clone systems and retry.

CTGKM2213W Replication result unknown for

Explanation:
Result for the replication of the specified host is unknown.

System action:
Check debug log.

Administrator response:
Check debug log.

CTGKM2214E Either both host name and port parameters must be coded, or neither.

Explanation:
The ReplicationNow command expects no parameters to replicate to all defined hosts, or both host name and port parameters to replicate to a single clone.

System action:
The ReplicationNow command fails.

Administrator response:
Re-run the command with correct parameters sepcified.

CTGKM2222E No valid replication configuration file exists.

Explanation:
Either no replication configuration file exists, or it is invalid.

System action:
No action required.

Administrator response:
Create a valid replication configuration file and retry the operation.

CTGKM2237E Replication failed.

Explanation:
Replication failed.

System action:
No action necessary.

Administrator response:
No action required.

CTGKM2243E Replication can only be invoked on the master machine.

Explanation:
Replication now invoked from CLI on a clone machine. However, it can only in invoked on the master machine.

System action:
No action necessary.

Administrator response:
Go to master machine and invoke replication.

CTGKM2244E *VALUE_0* can not be updated.

Explanation:
The config property referenced in the message can not be updated by the CLI. It is only updated by the product.

System action:
No action necessary.

Administrator response:
No action necessary.

CTGKM2245E Cannot modify the key

Explanation:
Attempt to modify the key did not complete. The key that you intend to update, might not be found, or there might be a database error. There might be

more information in the message that describes the problem.

System action:
The key was not modified.

Administrator response:
Additional information might guide your response. Make appropriate changes. Then, try the operation again.

CTGKM2246E Cannot update the replication.MaxBackupNum property. Specify an integer value that is between 2 - 10.

Explanation:
Value for replication.MaxBackupNum property must be an integer value that is between 2 - 100.

System action:
The operation fails.

Administrator response:
Specify a valid integer value that is between 2 - 10 for the replication.MaxBackupNum property.

CTGKM2247E Cannot update the replication.Incremental.CheckFrequency property. Specify an integer value that is equal to or greater than 60.

Explanation:
Value for replication.Incremental.CheckFrequency property must be equal to or greater than 60.

System action:
The operation fails.

Administrator response:
Specify a valid integer value that is equal to or greater than 60 for the replication.Incremental.CheckFrequency property.

CTGKM2248E Cannot update the replication.Incremental.Enable property. Specify one of these values: true, false.

Explanation:
Value for the replication.Incremental.Enable property must be true or false.

System action:
The operation to update the configuration property fails.

Administrator response:
Specify true or false as the value for the replication.Incremental.Enable property and retry the operation.

CTGKM2250E Cannot configure the backup.Client property because replication is not supported.

Explanation:
The backup.Client property cannot be updated because Replication is not supported in a containerized deployment.

System action:
Replication configuration fails.

Administrator response:
No action needed.

CTGKM2253E Replication failed. User name *VALUE_0* doesn't exists exists in this installation. Create the users and try again.

Explanation:
User name doesn't exist. Please create the users and try again.

System action:
The operation fails.

Administrator response:
Create the users and try again.

CTGKM2300E Client certificate push is disabled.

Explanation:
enableClientCertPush is set to false in the configuration file.

System action:
The operation fails.

Administrator response:
Change the value from false to true for the enableClientCertPush property in the SKLMConfig.properties file.

CTGKM2301E The number of pending client certificates has been reached.

Explanation:
The number of pending client certificates exceeds the configuration value for maxPendingClientCerts.

System action:
The operation fails.

Administrator response:
Increase the value for the maxPendingClientCerts property in the SKLMConfig.properties file.

CTGKM2302E The X509 certificate cannot be null.

Explanation:
The X509 certificate to be added to the pending client certificate list is null.

System action:

The operation fails.

Administrator response:
Add the X509 certificate and continue.

CTGKM2303E Client certificate exists in the pending client certificate list in the database: *VALUE_0*

Explanation:
Client certificate exists in the pending client certificate list in the database.

System action:
The operation fails.

Administrator response:
None.

CTGKM2304E Client certificate alias is required.

Explanation:
Client certificate alias is required.

System action:
The operation fails.

Administrator response:
Add the alias string and try again.

CTGKM2305E Client certificate UUID is required.

Explanation:
The client certificate UUID is required.

System action:
The operation fails.

Administrator response:
Add the UUID and try again.

CTGKM2306E Client certificate alias already in use: *VALUE_0*

Explanation:
The client certificate alias is already in use in the database and keystore.

System action:
The operation fails.

Administrator response:
Use a different alias and try again.

CTGKM2307E Client certificate UUID not found in the database: *VALUE_0*

Explanation:
The client certificate UUID was not found in the database.

System action:
The operation fails.

Administrator response:
Change to a valid UUID and try again.

CTGKM2308E There are no pending client certificates in the database.

Explanation:
There are no pending client certificates in the database.

System action:
The operation fails.

Administrator response:
No action.

CTGKM2311E maxPendingClientCerts does not fall within the valid value set of 1 to 999. *VALUE_0*

Explanation:
maxPendingClientCerts does not fall within the valid value set of 1 to 999.

System action:
The operation fails.

Administrator response:
Update the configuration parameter and try again.

CTGKM2312E enableClientCertPush is not true or false.

Explanation:
enableClientCertPush is not true or false.

System action:
The operation fails.

Administrator response:
Update the configuration parameter and try again.

CTGKM2313E maxPendingClientCerts does not fall within the valid value set of 1 to 999.

Explanation:
maxPendingClientCerts does not fall within the valid value set of 1 to 999.

System action:
The operation fails.

Administrator response:
Update the configuration parameter and try again.

CTGKM2314E Certificate expired. Expired certificate cannot be used as client certificate.

Explanation:
Certificate expired. Expired certificate cannot be used as client certificate.

System action:
Update operation fails.

Administrator response:
Specify a valid certificate alias and try the operation again.

CTGKM2901E Export directory could not be resolved. Try specifying a valid export directory explicitly.

Explanation:
Export directory could not be resolved.

System action:
The IBM Security Guardium Key Lifecycle Manager export operation fails.

Administrator response:
Make sure that the export directory provided to the export operation is valid. Try specifying a valid export directory explicitly. If this is the first time you are executing export, find a directory suitable for IBM Security Guardium Key Lifecycle Manager export and specify the directory explicitly on the export command.

CTGKM2902W IBM Security Guardium Key Lifecycle Manager export is already in progress.

Explanation:
Only one import/export operation is allowed at any given time.

System action:
The requested operation will not be performed.

Administrator response:
Wait until the operation completes.

CTGKM2903E Export of *VALUE_0* failed: *VALUE_1* .

Explanation:
Export failed unexpectedly.

System action:
Export fails.

Administrator response:
Check the log entries to find out the reason for export failure.

CTGKM2907E Device Group with name *VALUE_0* is not found.

Explanation:
Incorrect Correct Device Group Name is provided

System action:
Export fails.

Administrator response:
Please Provide the Correct Device Group Name.

CTGKM2910E Key Group with name *VALUE_0* is not found. .

Explanation:
Key Group mentioned in export manifest file not found

System action:
Export fails.

Administrator response:
Please check if the export file is not corrupted.

CTGKM2911E Import of *VALUE_0* failed: *VALUE_1* .

Explanation:
Import failed unexpectedly.

System action:
Import fails.

Administrator response:
Check the log entries to find out the reason for import failure.

CTGKM2912W Import is already in progress.

Explanation:
Only one import/export operation is allowed at any given time.

System action:
The requested operation will not be performed.

Administrator response:
Wait until the operation completes.

CTGKM2913W Export is already in progress.

Explanation:
Only one import/export operation is allowed at any given time.

System action:
The requested operation will not be performed.

Administrator response:
Wait until the operation completes.

CTGKM2914E The key is missing for decryption. Check whether the provided file is valid.

System action:
The operation fails.

Administrator response:
Specify the correct file and retry.

CTGKM2915E Specified export file does not exist: *VALUE_0* .

Explanation:
The export file does not exist.

System action:
The IBM Security Guardium Key Lifecycle Manager import operation fails.

Administrator response:
Make sure that the export file path provided to the import operation is valid.

CTGKM2916E Error reading manifest from the export jar file: *VALUE_0* .

Explanation:
Export manifest could be corrupted or incorrect for unknown reasons.

System action:
Restore fails.

Administrator response:
Check the log entries to find out the reason for import failure.

CTGKM2917E I/O error while decrypting and/or extracting export file. \nPossible cause: Incorrect password may have been provided, which results in the export entry being decrypted incorrectly.

Explanation:
I/O error occurred while decrypting and/or extracting a export file entry. A common reason for this error is that a file was encrypted using one password and an incorrect or null password was provided to decrypt the file. Decryption will still take place, but the decrypted file is not valid and cannot be used in later stages of the restore.

System action:
Import fails.

Administrator response:
Check the password provided for decryption. Check if the destination location contains sufficient disk space to hold the decrypted/extracted file. Check the log files for additional clues if necessary. Retry the operation.

CTGKM2918E Certificate with Alias name *VALUE_0* doesn't exists.

Explanation:
Certificate with Alias name doesn't exist. Please provide the exisiting alias.

System action:

Administrator response:
Certificate with alias name does not exist. Provide the existing alias.

CTGKM2919E Certificate with Alias name *VALUE_0* already exists.

Explanation:
Certificate with Alias name already exists. Please provide the different alias name.

System action:

Administrator response:
Certificate with alias name already exists. Provide a different alias name.

CTGKM2920E Key with Alias name *VALUE_0* already exists.

Explanation:
Key with Alias name already exists. Please provide the different alias name.

System action:

Administrator response:
Key with alias name already exists. Provide a different alias name.

CTGKM2921E Key with Alias name *VALUE_0* doesn't exists.

Explanation:
Key with Alias name doesn't exist. Please provide the exisiting alias.

System action:

Administrator response:
Key with alias name does not exist. Provide the existing alias.

CTGKM2922E Object with the given name *VALUE_0* doesn't exists.

Explanation:
Object with the given old name doesn't exist in the system. Please check the given old name.

System action:

Administrator response:
Device with serial number does not exist. Provide the serial number that is registered.

CTGKM2923E The given new name *VALUE_0* is already associated with an Object.

Explanation:
An Object with given new name already exists in the system. Please provide different new name for the object.

System action:

Administrator response:
Device with Serial number already exists. Provide a different serial number.

CTGKM2924E Successfully deleted *VALUE_0* .

Explanation:
Successfully deleted the export file.

System action:

Administrator response:

CTGKM2925E Error deleting file : *VALUE_0* .

Explanation:
An error occurred while deleting the export file.

System action:

Administrator response:

CTGKM2926E Getting error while generating UUID. InstanceID is not initialized.

Explanation:
System is not able to generate UUID as mandatory InstanceID is not initialized or generated properly while installation.

System action:

Administrator response:

CTGKM2927E Invalid file extension. Valid extensions are .cer or .der for baser64 and DER formats respectively.

Explanation:
User must export certificate file with valid extension.

System action:

Administrator response:
You must export the certificate file with valid extension.

CTGKM2928E Internal Server Error. Please contact IBM Support.

Explanation:

System action:
The operation fails.

Administrator response:
Check the log file to find the root cause and contact IBM Support.

CTGKM2934E Type is not valid

Explanation:

System action:
The type provided is not supported.

Administrator response:
Ensure that the type provided is supported by the system.

CTGKM2935E Requested operation not supported on this System.

Explanation:
The operation you are trying to execute is not supported on this System. This could be because the it is a Clone System or Read only System.

System action:
Login fails.

Administrator response:
Check if the System is Clone or Read only.

CTGKM2937E Error restarting IBM Security Guardium Key Lifecycle Manager Server, please check logs for more information.

Explanation:

System action:
The server restart operation fails.

Administrator response:
Check the log file to find the root cause and correct the problem.

CTGKM2938E Error creating Master Key Packets for Keystore Password Obfuscation.

Explanation:

System action:
The request has been halted.

Administrator response:
Review the log files. Make changes as needed and retry the request.

CTGKM2939E Error during Obfuscating Keystore Password.

Explanation:

System action:
The request has been halted.

Administrator response:
Review the log files. Make changes as needed and retry the request.

CTGKM2940E Error during DeObfuscating Keystore Password.

Explanation:

System action:

Administrator response:

CTGKM2941E Packet writing in file failed. Directory location doesn't exist.

Explanation:

System action:
The operation will return failure.

Administrator response:
Confirm that the directory exists and has the correct permissions.

CTGKM2942E Packet reading from file failed.

System action:
The request has been halted.

Administrator response:
Verify that the given file exist and it is valid and retry the operation.

CTGKM2946E Configuration of masters is Incomplete.

Explanation:

System action:
An error is logged.

Administrator response:

Specify the missing configuration attributes and try again.

CTGKM2947W No entry found with the mentioned Cluster Name. Please check the value passed.

Explanation:

System action:

Administrator response:
Specify a server which exists in the repository.

CTGKM2950E Port value for *VALUE_0* should be in the range 0-65535

Explanation:

System action:
The operation fails.

Administrator response:
Specify a valid port number and ensure that the port is not used by other applications on the system.

CTGKM2951E *VALUE_0* should be either Primary, Standby or Master

Explanation:

System action:
Multi-master configuration fails.

Administrator response:
Specify a valid role: Primary, Standby, Master

CTGKM2953E Multi-Master is already configured.

Explanation:

System action:

Administrator response:

CTGKM2954E Login request to the instance with hostname *VALUE_0* and port *VALUE_1* is unsuccessful.

Explanation:

System action:
Multi-master configuration fails.

Administrator response:
Ensure that the specified values for port and host name are correct.

CTGKM2955E Master key needs to be created on this server before the Multi-Master setup.

Explanation:

System action:

Administrator response:
Create a master key to continue with multi-master configuration.

CTGKM2956E Input value cannot be an exceed the size of *VALUE_0* for parameter *VALUE_1*

Explanation:

System action:
Multi-master configuration fails.

Administrator response:
Specify the valid values. Then, try the operation again.

CTGKM2957E Master with Instance ID *VALUE_0* already exists.

Explanation:

System action:
Multi-master configuration fails.

Administrator response:
Specify an instance ID that is valid and unique.

CTGKM2958E Master with Instance ID *VALUE_0* not found.

Explanation:

System action:
Operation fails.

Administrator response:
Verify that you specified the correct instance ID of master server.

CTGKM2959E *VALUE_0* should be STANDALONE (0), REPLICATION (1) or MULTI_MASTER (2)

Explanation:

System action:
Operation fails.

Administrator response:
Specify a valid value.

CTGKM2960E *VALUE_0* should be LOCAL (0), PRIMARY (1), STANDBY(2) or NODE (3)

Explanation:

System action:
Operation fails.

Administrator response:
Specify a valid value.

CTGKM2961E *VALUE_0* should be NOT_CONFIGURED (0), NODES_CONFIGURED (1), AGENTS_CONFIGURED (2), DB2_CONFIGURED (3), WAS_CONFIGURED (4) or CONFIGURED (5) or OUT_OF_SYNC (6)

Explanation:

System action:
Operation fails.

Administrator response:
Specify a valid value.

CTGKM2963E ***VALUE_0*** **should be within range 1-3.**

System action:
Operation fails.

Administrator response:
Specify a valid value.

CTGKM2964E **Standby Priority Index missing for Instance with Hostname** ***VALUE_0***

Explanation:

System action:
Operation fails.

Administrator response:
Specify a valid priority index number for standby master.

CTGKM2965E **Standby Priority Index for Instance with Hostname(s)** ***VALUE_0*** **and** ***VALUE_1*** **are same.**

Explanation:

System action:
Operation fails.

Administrator response:
Specify a valid priority index number for standby master.

CTGKM2966E **Invalid value for Standby Priority Index. The value must be in ascending order starting from 1.**

Explanation:

System action:
Operation fails.

Administrator response:
Verify the number of standby masters in the multi-master cluster.

CTGKM2967E **Multi-Master configuration must be done on Primary machine. Primary machine Hostname specified** ***VALUE_0*** **and This machine hostname** ***VALUE_1***

Explanation:

System action:

Administrator response:

CTGKM2968E **Instance with Hostname** ***VALUE_0*** **is already added.**

Explanation:

System action:
Operation fails.

Administrator response:

CTGKM2969E ***VALUE_0*** **should be either 0 or 1.**

System action:
Operation fails.

Administrator response:
Specify a valid value.

CTGKM2970E **Agent is not Running.**

Explanation:

System action:
Operation fails.

Administrator response:
Start the agent and retry the operation.

CTGKM2971E **Operating System for Standby System** ***VALUE_0*** **is different from that of Primary System.**

Explanation:

System action:
Operation fails.

Administrator response:
Ensure that the primary and standby systems have the same operating system and level.

CTGKM2972E **Request failed. Only one master is allowed to be removed at a time.**

Explanation:

System action:
Operation fails.

Administrator response:

CTGKM2973E **Request failed. The master server does not exist in the Multi-Master cluster.**

Explanation:

System action:
Operation fails.

Administrator response:

CTGKM2974E **Request failed. Primary master server of the cluster cannot be removed.**

Explanation:

System action:
Operation fails.

Administrator response:

CTGKM2975E Cannot remove the standby master server. Multi-Master cluster must have at least one standby master server.

Explanation:

System action:
Operation fails.

Administrator response:

CTGKM2976E WAS Configuration failed to update after removing master.

Explanation:

System action:
Operation fails.

Administrator response:

CTGKM2977E Stop Agent Services failed during remove master.

Explanation:

System action:
Operation fails.

Administrator response:
Ensure that the Stop Agent Service is up and running.

CTGKM2978E Restart servers failed.

Explanation:

System action:
Operation fails.

Administrator response:

CTGKM2979E Reset HADR failed during remove master.

Explanation:

System action:
Operation fails.

Administrator response:

CTGKM2980E Rollforward end of logs failed during remove master.

Explanation:

System action:
Operation fails.

Administrator response:

CTGKM2982E Standby master failed to Takeover as Primary.

Explanation:

System action:
Operation fails.

Administrator response:
See the log for more details.

CTGKM2983E Primary or Standby master server is missing in Multi-Master cluster. Adding server is not allowed in current state.

Explanation:

System action:
Operation fails.

Administrator response:
You must add a standby server to the cluster before adding master server.

CTGKM2984E Failed to start Agent on instance *VALUE_0* .

Explanation:

System action:
Operation fails.

Administrator response:
See the log for more details.

CTGKM2985E Failed to connect to *VALUE_0* .

Explanation:

System action:
Operation fails.

Administrator response:
See the log for more details.

CTGKM2986E Failed to add master.

Explanation:

System action:
Operation fails.

Administrator response:
See the log for more details.

CTGKM2987E Failed to remove master.

Explanation:

System action:
Operation fails.

Administrator response:
See the log for more details.

CTGKM2988E Failed to modify master.

Explanation:

System action:
Operation fails.

Administrator response:
See the log for more details.

CTGKM2990E Instance with IP/hostname *VALUE_0* not found.

Explanation:

System action:
Operation fails.

Administrator response:
See the log for more details.

CTGKM2991E Error fetching present SKLM Instance.

Explanation:

System action:
Operation fails.

Administrator response:
See the log for more details.

CTGKM2994E IOException while running *VALUE_0*.

System action:
Operation fails.

Administrator response:
Check the text of the Java IOException for possible reasons for the error.

CTGKM2995E AgentException while running *VALUE_0*.

System action:
Operation fails.

Administrator response:
Review the message for possible reasons for the error.

CTGKM2996E Error occurred while running *VALUE_0*.

System action:
Operation fails.

Administrator response:
Check the log file and correct the problem.

CTGKM2997E Exception occurred while running *VALUE_0*.

System action:
Operation fails.

Administrator response:
Attempt to diagnose the cause of the error based on the exception text.

CTGKM2998E KLMException while running *VALUE_0*.

System action:
Operation fails.

Administrator response:
Attempt to diagnose the cause of the error based on the exception text.

CTGKM2999E Master Key creation failed.

Explanation:

System action:
Operation fails.

Administrator response:
See the log for more details.

CTGKM3000E Master Key Transmission failed on master *VALUE_0* .

Explanation:

System action:
Operation fails.

Administrator response:
See the log for more details.

CTGKM3001E Error refreshing master *VALUE_0* . Showing the last updated status.

Explanation:

System action:
Refresh operation fails.

Administrator response:
See the log for more details.

CTGKM3003E Promoting standby to primary failed.

Explanation:

System action:
Operation fails.

Administrator response:
See the log for more details.

CTGKM3004E The master with Host name / IP address *VALUE_0* already exist in the cluster.

Explanation:

System action:
Operation fails.

Administrator response:

CTGKM3006E Couldn't verify if HADR role while executing *VALUE_0* .

Explanation:

System action:
Operation fails.

Administrator response:

CTGKM3010E Scheduler could not be found:\n Original error message: *error_message*

Explanation:
Error in scheduler task detected.

System action:
Operations involving scheduler will fail.

Administrator response:
This should not happen under normal conditions. Investigate the logs and server startup log for clues. Restart the server.

CTGKM3011E Invalid exisiting Db2 password. DB Password updation service failed.

Explanation:

System action:
DB2 password update operation failed.

Administrator response:
Specify a valid password for the DB2 administrator ID. Verify that the user ID has a password that is valid and ready to use.

CTGKM3013E DB Password updation service for SKLM instance failed.

Explanation:

System action:
DB2® password update operation failed.

Administrator response:
See the log files for more details.

CTGKM3015E Database password update service for IBM Security Guardium Key Lifecycle Manager Multi-Master cluster failed.

Explanation:

System action:
password update operation fails.

Administrator response:
Check the log to identify the root cause. Correct the problem, and then rerun the REST service to change the password on the Multi-Master setup.

CTGKM3016E Invalid range. Keys with given prefix in alias range already generated.

Explanation:
The specified alias range prefix is already generated.

Administrator response:
Specify a different prefix for the alias range. Then, try the operation again.

CTGKM3017E Invalid range. Keys with given prefix in alias range doesn't exist.

Explanation:

System action:
The operation fails.

Administrator response:
Specify a valid range. Then, try the operation again.

CTGKM3019E Setup of Isolated Server failed.

Explanation:

System action:
Setting up the isolated master in read-only mode is failed.

Administrator response:
Check the log entries to find out the reason for the failure. Make appropriate changes. Then, try the operation again.

CTGKM3020E Not a recognized device group: *VALUE_0*

Explanation:
The specifed device group does not match any device group stored in the database.

System action:
The operation fails.

Administrator response:
Specify a valid device group and try again.

CTGKM3021E Operation cannot be null.

Explanation:
The specifed KLMOperation object is null. This is an internal error.

System action:
The operation fails.

Administrator response:
This is an internal error that external users should not see. Contact IBM Support.

CTGKM3022E User *VALUE_0* does not have appropriate permission to perform this operation. Depending on what the target resource is, it usually requires at least one of the listed permission(s): *VALUE_1* .

Explanation:
The user does not have the appropriate permissions for this operation.

System action:
The operation fails.

Administrator response:
Check the user's permission. Refer to the product documentation in the IBM Knowledge Center to understand the permissions required for this operation. Set up appropriate permissions for the user and try again.

CTGKM3023E User *VALUE_0* does not have a valid IBM Security Guardium Key Lifecycle Manager role. Some roles require both device group and action permissions. Verify that the user's role has appropriate permissions.

Explanation:
User does not have a valid IBM Security Guardium Key Lifecycle Manager role.

System action:
The operation fails.

Administrator response:
Check the user's permission. Refer to the product documentation in the IBM Knowledge Center to understand the permissions required for this operation. Set up appropriate permissions for the user and try again.

CTGKM3024E No permission set defined for operation *VALUE_0*.

Explanation:
No permission set defined for the specified operation.

System action:
The operation fails.

Administrator response:
This is an internal error that external users should not see. Contact IBM Support.

CTGKM3025E Operation *VALUE_0* requires device group permission, but specified resource is null.

Explanation:
The specified operation requires device group permission but the device group resource is not specified.

System action:
The operation fails.

Administrator response:
The specified operation requires device group permission but the device group resource is not specified. This is an internal error that external users should not see. Contact IBM Support.

CTGKM3026E The target resource's device group name cannot be null.

Explanation:
At permission checking, the target resource's device group name is not specified.

System action:
This is an internal error that external users should not see. Contact IBM Support.

Administrator response:
This is an internal error that external users should not see. Contact IBM Support.

CTGKM3027E Device group must be specified.

Explanation:
Device group must be specified while invoking AuthorizationService.getPermission to get a user's IBM Security Guardium Key Lifecycle Manager permission.

System action:
The operation fails.

Administrator response:
The call to AuthorizationService.getPermission(KLMUserSession, String) must have a device group parameter specified. This is usually an internal error that external users should not see. If this API is invoked by another application, the application needs to adjust the parameter.

CTGKM3028E Cannot merge these two permissions.

Explanation:
If two IBM Security Guardium Key Lifecycle Manager permissions have different device groups, they cannot be merged.

System action:
The operation fails.

Administrator response:
The call to KLMPermission.merge(KLMPermission) cannot merge the specified permission. This is usually an internal error that external users should not see. If this API is invoked by another application, the application needs to adjust the parameters.

CTGKM3029E No device group information specified.

Explanation:
No device group information specified in the KLMDeviceType object.

System action:
The operation fails.

Administrator response:
KLMDeviceType object must include the device group name or device group ID. The caller needs to adjust the parameter.

CTGKM3030E User has no permission to query certificates. Check the user's permissions.

Explanation:
Access is denied for query certificate operation. Check the user's permissions.

System action:
The operation fails.

Administrator response:
Check user's role and permissions. Assign appropriate permissions to the user. Then, try again.

CTGKM3031E User has no permission to query keys. Check the user's permissions.

Explanation:
The permissions associated with the user role are not appropriate for query key operation.

System action:
The operation fails.

Administrator response:
Check the user's role and permissions. Assign appropriate permissions to the user. Then, try again.

CTGKM3032E User has no permission to query key groups. Check the user's permissions.

Explanation:
The permissions associated with the user role are not appropriate for query key group operation.

System action:
The operation fails.

Administrator response:
Check the user's role and permissions. Assign appropriate permissions to the user. Then, try again.

CTGKM3033E User has no permission to query devices. Check user's permission.

Explanation:
The permissions associated with the user role is not appropriate for query device operation.

System action:
The device query fails.

Administrator response:
Check user's role and permission set. Assign appropriate permissions to the user.

CTGKM3034E Cannot do 3592 rollover operation for non-3592 device group certificate.

Explanation:
The certificate's device group must match the rollover device group.

System action:
The operation fails.

Administrator response:
Check the device group of the certificate and modify it to match the target rollover device group, or choose a different certificate for the rollover.

CTGKM3035E Cannot do LTO rollover operation for a non-LTO device group key group.

Explanation:
The key group's device group must match the rollover device group.

System action:
The operation fails.

Administrator response:
Check the device group of the certificate and modify it to match the target rollover device group, or choose a different key group for the rollover.

CTGKM3036E Cannot find the specified rollover task.

Explanation:
Cannot find the specified rollover task from the database.

System action:
The operation fails.

Administrator response:
Correct the specified rollover task parameters. Then, try again.

CTGKM3037E Failed to create key group *VALUE_0* and keys with prefix *VALUE_0*

Explanation:
Failed to create the key group and keys with specified prefix.

System action:
The operation fails.

Administrator response:
Look at the logs for more information and retry. If the failure still exists, contact IBM support.

CTGKM3038E Cannot change the key in a DS5000 key group to another key group.

Explanation:
DS5000 key group and keys are bound together. You cannot change the group membership of an individual DS5000 key directly.

System action:
The operation fails.

Administrator response:
You are not allowed to change the key of a DS5000 key group to another key group.

CTGKM3039E Cannot change the key's group membership. The key is used by one or more devices.

Explanation:
Cannot change the key's group membership. The key is used by one or more devices.

System action:
The operation fails.

Administrator response:
You are not allowed to change the key of a DS5000 key group to another key group. The key is used by one or more devices.

CTGKM3040E **Object with identifier *object_id* cannot be found.**

Explanation:
The identifier value that you specified does not match an existing object.

System action:
The operation fails.

Administrator response:
Specify an identifier that corresponds to an existing object.

CTGKM3041E **User *object_id* has no access to the destroyed object. The destroyed object has no device group information and only the klmSecurityOfficer role can access it.**

Explanation:
When a KLM key or certificate is marked as destroyed, its data in the relation table are removed. There is no device group information. Only the klmSecurityOfficer role can access the object.

System action:
The operation fails.

Administrator response:
Log in as security officer to view the destroyed objects.

CTGKM3042E **The alias of the key that encrypts the secret key file must be specified.**

Explanation:
To import the secret key file, specify the alias of the public private key pair so that IBM Security Guardium Key Lifecycle Manager can get the private key to decrypt the file.

System action:
The operation fails.

Administrator response:
Specify the keyAlias when you run the tklmKeyImport command.

CTGKM3043E **Error occurred while loading data from the file *VALUE_0*. Make sure that the password is correct and the file has not been tampered with.**

Explanation:
This is an error in reading data from a key or certificate file.

System action:
The operation fails.

Administrator response:
Ensure that the path and filename are correct, and that the password is correct. Then, try the operation again.

CTGKM3044E **The file *VALUE_0* is reserved for internal IBM Security Guardium Key Lifecycle Manager keystore. Use another file name.**

Explanation:
User cannot create a new keystore that has the same location and file name as the internal IBM Security Guardium Key Lifecycle Manager keystore.

System action:
The operation fails.

Administrator response:
Use a different file name. Then, try the operation again.

CTGKM3045E **Value for configuration parameter Audit.eventQueue.max is not valid. A valid value is a non-negative integer.**

Explanation:
Audit.eventQueue.max is a non-negative integer.

System action:
The operation fails.

Administrator response:
Specify 0 or a positive integer and try the operation again.

CTGKM3046E **Value for configuration parameter Audit.handler.file.size is not valid. A valid value is a non-negative integer.**

Explanation:
Audit.handler.file.size is a non-negative integer.

System action:
The operation fails.

Administrator response:
Specify 0 or a positive integer and try the operation again.

CTGKM3047E **Value for configuration parameter Audit.handler.file.threadlifespan is not valid. A valid value is a non-negative integer.**

Explanation:
Audit.handler.file.threadlifespan is a non-negative integer.

System action:
The operation fails.

Administrator response:
Specify 0 or a positive integer and try the operation again.

CTGKM3048E Value for configuration parameter Audit.handler.file.multithreads is not valid. A valid value is true or false.

Explanation:
Audit.handler.file.multithreads parameter allows the use of multiple threads while logging audit events. The valid value is either true or false.

System action:
The operation fails.

Administrator response:
Specify true or false and try the operation again.

CTGKM3049E Configuration parameter tklm.backup.dir cannot be modified directly. To change to a different directory, specify the new directory when doing the next backup.

Explanation:
You cannot modify the current backup directory. To change to a different directory, specify the new directory when doing the next backup.

System action:
The operation fails.

Administrator response:
Do not use the tklmConfigUpdateEntry command to modify the tklm.backup.dir configuration parameter.

CTGKM3050E Value for configuration parameter cert.valiDATE is not valid. A valid value is true or false.

Explanation:
Valid value for cert.valiDATE is true or false.

System action:
The operation fails.

Administrator response:
Specify true or false as the value.

CTGKM3051E Keystore name cannot be modified by updating configuration parameter config.keystore.name directly. Use a keystore command to update the name.

Explanation:
Keystore name cannot be modified by updating config.keystore.name directly. Use a keystore command to update the name.

System action:
The operation fails.

Administrator response:
Keystore name cannot be modified by updating config.keystore.name directly. Use a keystore command to update the name.

CTGKM3052E Invlalid value for configuration parameter disableDatabaseBackup. A valid value is true or false.

Explanation:
Value for configuration parameter disableDatabaseBackup is not valid. A valid value is true or false.

System action:
The operation fails.

Administrator response:
Specify true or false as the input value.

CTGKM3053E Value for configuration parameter fips is not valid. A valid value is on or off.

Explanation:
Value for configuration parameter fips is not valid. A valid value is on or off.

System action:
The operation fails.

Administrator response:
Specify on or off as the input value.

CTGKM3054E Value for configuration parameter requireHardwareProtectionForSymmetricKeys is not valid. A valid value is true or false.

Explanation:
Value for configuration parameter requireHardwareProtectionForSymmetricKeys is not valid. A valid value is true or false.

System action:
The operation fails.

Administrator response:
Specify true or false as the input value.

CTGKM3055E Configuration parameter tklm.backup.db2.dir cannot be modified directly. To change to a different directory, specify the new directory when doing the next backup.

Explanation:
You cannot modify the current backup directory. To change to a different directory, specify the new directory when doing the next backup.

System action:
The operation fails.

Administrator response:
Do not use the tklmConfigUpdateEntry command to modify tklm.backup.db2.dir.

CTGKM3056E Value for configuration parameter tklm.encryption.pbe.algorithm is not valid. A valid value is PBEWithMD5AndTripleDES.

Explanation:
Value for configuration parameter tklm.encryption.pbe.algorithm is not valid. A valid value is PBEWithMD5AndTripleDES.

System action:
The operation fails.

Administrator response:
Specify PBEWithMD5AndTripleDES as the input value.

CTGKM3057E Value for configuration parameter TransportListener.ssl.clientauthentication is not valid. A valid value is 0, 1 or 2.

Explanation:
Value for configuration parameter TransportListener.ssl.clientauthentication is not valid. A valid value is 0, 1 or 2.

System action:
The operation fails.

Administrator response:
Specify 0, 1 or 2 as the input value.

CTGKM3058E Value for configuration parameter TransportListener.ssl.port is not valid. A valid value is an integer between 1 and 65535.

Explanation:
Value for configuration parameter TransportListener.ssl.port is not valid. A valid value is an integer between 1 and 65535.

System action:
The operation fails.

Administrator response:
Specify an integer between 1 and 65535 as the input value.

CTGKM3059E Value for configuration parameter TransportListener.ssl.protocols is not valid. A valid value is TLS, SSL_TLSv2 or TLSv1.2.

Explanation:
Value for configuration parameter TransportListener.ssl.protocols is not valid. A valid value is TLS, SSL_TLSv2 or TLSv1.2.

System action:
The operation fails.

Administrator response:
Specify TLS, SSL_TLSv2, or TLSv1.2 as the input value.

CTGKM3060E Value for configuration parameter TransportListener.ssl.timeout is not valid. A valid value is an integer between 1 and 120.

Explanation:
Value for configuration parameter TransportListener.ssl.timeout is not valid. A valid value is an integer between 1 and 120.

System action:
The operation fails.

Administrator response:
Specify an integer between 1 and 120 as the input value.

CTGKM3061E Value for configuration parameter TransportListener.tcp.port is not valid. A valid value is an integer between 1 and 65535.

Explanation:
Value for configuration parameter TransportListener.tcp.port is not valid. A valid value is an integer between 1 and 65535.

System action:
The operation fails.

Administrator response:
Specify an integer between 1 and 65535 as the input value and ensure that the port is not used by other applications on the system.

CTGKM3062E Value for configuration parameter TransportListener.tcp.timeout is not valid. A valid value is an integer between 1 and 120.

Explanation:
Value for configuration parameter TransportListener.tcp.timeout is not valid. A valid value is an integer between 1 and 120.

System action:
The operation fails.

Administrator response:
Specify an integer between 1 and 120 as the input value.

CTGKM3063E Value for configuration parameter stopRoundRobinKeyGrps is not valid. A valid value is true or false.

Explanation:
Value for configuration parameter stopRoundRobinKeyGrps is not valid. A valid value is true or false.

System action:

The operation fails.

Administrator response:
Specify true or false.

CTGKM3064E Value for configuration parameter useSKIDefaultLabels is not valid. A valid value is true or false.

Explanation:
Value for configuration parameter useSKIDefaultLabels is not valid. A valid value is true or false.

System action:
The operation fails.

Administrator response:
Specify true or false.

CTGKM3065E Value for configuration parameter zOSCompatibility is not valid. A valid value is true or false.

Explanation:
Value for configuration parameter zOSCompatibility is not valid. A valid value is true or false.

System action:
The operation fails.

Administrator response:
Specify true or false.

CTGKM3066E Value for configuration parameter pcache.refresh.interval is not valid. A valid value is a positive integer.

Explanation:
Value for configuration parameter pcache.refresh.interval is not valid. A valid value is a positive integer.

System action:
The operation fails.

Administrator response:
Specify a positive integer.

CTGKM3067E Failed to create the directory for the log file:

Explanation:
Cannot create a new directory as specified.

System action:
The operation fails.

Administrator response:
Specify a valid directory name and try again.

CTGKM3068E Cannot create the new log file: *VALUE_0*

Explanation:
Cannot create a new log file as specified.

System action:
The operation fails.

Administrator response:
Specify a valid file name and try again.

CTGKM3069E Not a valid file name. Specify a path and file name that is relative to SKLM_HOME.

Explanation:
Not a valid file name. Specify a path and file name that is relative to SKLM_HOME.

System action:
The operation fails.

Administrator response:
Specify a valid file and path name and try again.

CTGKM3071E Cannot set the certificate alias because the keystore is not defined.

Explanation:
There is no certificate alias to be set because the keystore is not defined.

System action:
The operation fails.

Administrator response:
Add or create a keystore for IBM Security Guardium Key Lifecycle Manager. Specify the certificate alias that exists in the keystore and try again.

CTGKM3072E The specified certificate has a different usage. Use a different certificate.

Explanation:
The specified certificate has a different usage. Use a different certificate.

System action:
The operation fails.

Administrator response:
Specify a different certificate alias and try again.

CTGKM3073E Cannot find the class in classpath: *VALUE_0*

Explanation:
Cannot find the class in classpath.

System action:
The operation fails.

Administrator response:
Make sure the class and package name are correct in the configuration file.

CTGKM3074E Not a valid class name. The class object cannot be instantiated: *VALUE_0*

Explanation:
Not a valid class name. The class object cannot be instantiated.

System action:
The operation fails.

Administrator response:
Make sure the class and package name are correct in the configuration file.

CTGKM3075E Not a valid class name. It must implement SecurityEventHandlerSpi class: *VALUE_0*

Explanation:
Not a valid class name. It must implement SecurityEventHandlerSpi class

System action:
The operation fails.

Administrator response:
Make sure the class and package name are correct in the configuration file.

CTGKM3076E Unsupported event type: *VALUE_0*

Explanation:
Unsupported event type.

System action:
The operation fails.

Administrator response:
Make sure the event type specified in the configuration file is correct.

CTGKM3077E Value for configuration parameter *VALUE_0* is not valid. Valid values are success, failure, or both that are separated by comma or semicolon.

Explanation:
Valid values are success, failure, or both that are separated by a comma or semicolon.

System action:
The operation fails.

Administrator response:
Make sure the value is success, failure, or both that are separated by a comma or semicolon.

CTGKM3078E Keystore is not defined. The TransportListener.ssl.ciphersuites parameter cannot be set to the specified value.

Explanation:
Keystore is not defined. The TransportListener.ssl.ciphersuites parameter cannot be set to the specified value.

System action:
The operation fails.

Administrator response:
Create the keystore and certificates and then try the operation again.

CTGKM3079E TrustManager and KeyManager are not initialized. The TransportListener.ssl.ciphersuites parameter cannot be set to the specified value.

Explanation:
TrustManager and KeyManager are not initialized. The TransportListener.ssl.ciphersuites parameter cannot be set to the specified value.

System action:
The operation fails.

Administrator response:
Create the keystore and certificates and then try the operation again.

CTGKM3080E TLSContext is not initialized. The TransportListener.ssl.ciphersuites parameter cannot be set to the specified value.

Explanation:
TLSContext is not initialized. The TransportListener.ssl.ciphersuites parameter cannot be set to the specified value.

System action:
The operation fails.

Administrator response:
Create the keystore and certificates and then try the operation again.

CTGKM3081E Not a supported cipher suite: *VALUE_0*

Explanation:
Not a supported cipher suite.

System action:
The operation fails.

Administrator response:
Specify a different value and try the operation again.

CTGKM3082E No TLS certificate alias defined in the configuration file. TrustManager and KeyManager are not initialized. The TransportListener.ssl.ciphersuites parameter cannot be set to the specified value.

Explanation:
No TLS certificate alias defined in the configuration file. TrustManager and KeyManager are not initialized.

The TransportListener.ssl.ciphersuites parameter cannot be set to the specified value.

System action:
The operation fails.

Administrator response:
Set config.keystore.ssl.certalias in the configuration file and try the operation again.

CTGKM3083E Configuration parameter tklm.encryption.password cannot be updated.

Explanation:
Configuration parameter tklm.encryption.password cannot be updated.

System action:
The operation fails.

Administrator response:
Configuration parameter tklm.encryption.password cannot be updated.

CTGKM3084E Value for configuration parameter numberOfKeys is not valid. A valid value is a positive integer

Explanation:
Value for configuration parameter numberOfKeys is not valid. A valid value is a positive integer, such as 12.

System action:
The operation fails.

Administrator response:
Specify a positive integer.

CTGKM3085E To export the secret key, user must have proper permissions on the certificate and public key that are used to encrypt the secret key file.

Explanation:
To export the secret key, user must have proper permissions on the certificate and public key that are used to encrypt the secret key file.

System action:
The operation fails.

Administrator response:
Give the user the proper permissions on the certificate and try again.

CTGKM3086E To import the secret key, user must have the proper permissions on the private key that is used to decrypt the secret key file.

Explanation:
To import the secret key, user must have the proper permissions on the private key that is used to decrypt the secret key file.

System action:
The operation fails.

Administrator response:
Give the user the proper permissions on the private key and try again.

CTGKM3087E Deletion is not permitted on the object. Check the enableKMIPDelete flag on the object's device group.

Explanation:
Deletion is not permitted on the object when the enableKMIPDelete flag is turned off.

System action:
The operation fails.

Administrator response:
Turn on the enableKMIPDelete flag on the object's device group and try the operation again.

CTGKM3088E Not a recognized device group internal identifier: *VALUE_0*

Explanation:
The specifed device group internal identifier does not match any device group stored in the database.

System action:
The operation fails.

Administrator response:
Contact IBM Support.

CTGKM3089E Credential is not specified in KMIPUserSession.

Explanation:
KMIPUserSession object must provide the user credential for authorization purpose

System action:
The authorization of the KMIP user failed.

Administrator response:
Check if the KMIP client provides an appropriate credential such as correct client certificate.

CTGKM3090E The KMIP user is not authorized to access the target object.

Explanation:
The KMIP user is not authorized to access the target object.

System action:
The authorization of the KMIP user failed.

Administrator response:
Check if the KMIP client provides appropriate credentials such as the correct client certificate.

CTGKM3091E There is no KMIP policy defined for the operation.

Explanation:
There is no KMIP policy defined for the operation.

System action:
The authorization of the KMIP user failed.

Administrator response:
The requested KMIP operation may not be supported. Contact IBM Support.

CTGKM3092E KLMResource is not properly instantiated.

Explanation:
KLMResource is not properly instantiated.

System action:
The authorization of the KMIP user failed.

Administrator response:
Contact IBM Support.

CTGKM3093E Device group must be specified as a KMIP user credential.

Explanation:
Device group must be specified as a KMIP user credential.

System action:
The authorization of the KMIP user failed.

Administrator response:
Check if the KMIP request message includes device metadata information.

CTGKM3094E Name or ID of a device group must be specified in device metadata as a KMIP user credential.

Explanation:
Name or ID of a device group must be specified in device metadata as a KMIP user credential.

System action:
The authorization of the KMIP user failed.

Administrator response:
Check if the KMIP request message includes a name or ID of a device group as part of device metadata information.

CTGKM3095E KMIP user's device metadata credential does not match device group information in the target resource.

Explanation:
KMIP user's device metadata credential does not match device group information in the target resource.

System action:
The authorization of the KMIP user failed.

Administrator response:
Contact IBM Support for assistance.

CTGKM3096E Credential in KMIP user session is not properly specified.

Explanation:
Credential in KMIP user session is not properly specified.

System action:
The authorization of the KMIP user failed.

Administrator response:
Contact IBM Support for assistance.

CTGKM3097E User has no authority to access the target object. Access requires action permission on device group, klmConfigure or klmSecurityOfficer permission.

Explanation:
User has no authority to access the target object. Access requires action permission on device group, klmConfigure or klmSecurityOfficer permission.

System action:
Authorization fails.

Administrator response:
Check if the user has appropriate permissions.

CTGKM3099E Keystore name *VALUE_0* for keystore UUID *VALUE_1* is not valid.

Explanation:
The specified keystore name is not valid.

System action:
The keystore list operation fails.

Administrator response:
Specify a different keystore name and try the operation again.

CTGKM3100E Value for configuration parameter lock.timeout is not valid. A valid value is a non negative integer.

Explanation:
The specified lock.timeout value is not valid.

System action:
The operation to update the lock.tmeout value failed.

Administrator response:
Specify a different value and try the operation again.

CTGKM3101E The operation failed as dependent data has been locked. Another user might be accessing the same data. Try the operation again later.

Explanation:
The dependant data has been locked and the current thread failed to acquire the lock on the data within

limited time frame. It may be because another user is accessing the same data.

System action:
Try the operation again.

Administrator response:
Try the operation again.

CTGKM3102E ***VALUE_0*** **and** ***VALUE_1*** **cannot use the same port.**

Explanation:
TCP, KMIP, TLS cannot use the same port.

System action:
The operation fails.

Administrator response:
Try the operation again.

CTGKM3103E Value for configuration parameter KMIPListener.ssl.port is not valid. A valid value is an integer between 1 and 65535.

Explanation:
Value for configuration parameter KMIPListener.ssl.port is not valid. A valid value is an integer between 1 and 65535.

System action:
The operation fails.

Administrator response:
Specify an integer between 1 and 65535 as the input value and ensure that the port is not used by other applications on the system.

CTGKM3104E Value for configuration parameter backup.keycert.before.serving is not valid. The value must be either true or false.

Explanation:
Value for configuration parameter backup.keycert.before.serving is not valid. The value must be either true or false.

System action:
The operation fails.

Administrator response:
Specify either true or false as the value.

CTGKM3105E Cannot use the certificate for key export operation. The certificate contains an EC key.

Explanation:
The certificate contains an EC public key. The IBM JVM 5.0 does not support key encryption using EC key.

System action:
The operation fails. Specify a different certificate and try the operation again.

Administrator response:
Specify a different certificate and try the operation again.

CTGKM3106E Key or certificate with alias or key prefix ***VALUE_0*** **was not served because it is not backed up.**

Explanation:
Keys or certificates must be backed up before they can be served.

System action:
The operation fails.

Administrator response:
First back up IBM Security Guardium Key Lifecycle Manager. Then, try the operation again.

CTGKM3107E Value for configuration parameter autoRestartAfterRestore is not valid. The value must be either true or false.

Explanation:
Value for configuration parameter autoRestartAfterRestore is not valid. The value must be either true or false.

System action:
The operation fails.

Administrator response:
Specify either true or false as the value.

CTGKM3109E Key or certificate with alias or key prefix ***VALUE_0*** **was not served because it has not been released.**

Explanation:
Keys or certificates must be released before they can be served. This message may also occur if the config property release.date is missing or wrongly formatted.

System action:
The operation fails.

Administrator response:
First, run the command tklmKeyRelease. Then try the operation again.

CTGKM3110E Value for configuration parameter enableKeyRelease is not valid. The value must be either true or false.

Explanation:
Value for configuration parameter enableKeyRelease is not valid. The value must be either true or false.

System action:
The operation fails.

Administrator response:
Specify either true or false as the value.

CTGKM3111E Value for configuration parameter requireSHA2Signatures is not valid. The value must be either true or false.

Explanation:
Value for configuration parameter requireSHA2Signatures is not valid. The value must be either true or false.

System action:
The operation fails.

Administrator response:
Specify either true or false as the value.

CTGKM3112E Cannot generate self signed certificate for GPFS Device Family.

Explanation:
Self signed certificate creation is not allowed for GPFS type of devices.

System action:
The certificate operation fails.

Administrator response:
Specify the correct Device Family where the certificate needs to be created.

CTGKM3221E Join Back to Cluster process has failed.

Explanation:

System action:
The operation fails.

Administrator response:
Check the log entries to find out the reason for the failure. Make appropriate changes. Then, try the operation again.

CTGKM3222E The Db2 admin group name cannot be longer than 8 characters.

Explanation:

System action:
Installation cannot continue until you correct the error.

Administrator response:

CTGKM3223E Initial Backup folder doesn't exist at target Standby Master.

Explanation:

System action:
The operation fails.

Administrator response:
Provide a correct folder identifier. Then, retry the operation.

CTGKM3224E Restoring process of Initial Backup failed at target Standby master.

Explanation:

System action:
The operation fails.

Administrator response:
Check the log entries to find out the reason for the failure. Make appropriate changes. Then, try the operation again.

CTGKM3225E Intial Backup file doesn't exists in initialbackup folder.

Explanation:

System action:
The operation fails.

Administrator response:

CTGKM3226E Validation failed for field *VALUE_0*.

System action:
The operation fails.

CTGKM3227W Not yet updated.

Explanation:
When you log in to the IBM Security Guardium Key Lifecycle Manager graphical user interface for the first time, the status of the Masters table in the Multi-master pane is displayed as `Not yet updated`.

System action:
Status of the Masters table is not updated.

Administrator response:
In the Masters table, select a Master, and click **Refresh Master**. The Masters table refreshes and displays the latest status.

CTGKM3229E The *VALUE_0* server failed the following prerequisite checks:

Explanation:

System action:
Prerequisite check failed.

Administrator response:
Review the requirements to add a master server to the multi-master server. Then, try the operation again.

CTGKM3230E Port *VALUE_0* is not a valid one.

System action:
Prerequisite check failed.

Administrator response:
Review the requirements to add a master server to the IBM Security Guardium Key Lifecycle Manager multi-master server. Then, try the operation again.

CTGKM3231E Operating system and Db2 levels don't match.

Explanation:

System action:

Prerequisite check failed.

Administrator response:
Review the requirements to add a master server to the multi-master server. Then, try the operation again.

CTGKM3232E User doesn't have permission to access the temp directory.

Explanation:

System action:
Prerequisite check failed.

Administrator response:
Review the requirements to add a master server to the multi-master server. Then, try the operation again.

CTGKM3233E Incoming instance *VALUE_0* contains master key and hence, can't be added to the cluster.

Explanation:

System action:
Prerequisite check failed.

Administrator response:
Review the requirements to add a master server to the multi-master server. Then, try the operation again.

CTGKM3234E Credentials of *VALUE_0* are not valid.

System action:
Prerequisite check failed.

Administrator response:
Review the requirements to add a master server to the IBM Security Guardium Key Lifecycle Manager multi-master server. Then, try the operation again.

CTGKM3235E Updating MultiMaster Config details failed while removing Standby Master.

Explanation:

System action:
Remove standby master server operation fails.

Administrator response:
Check the log to identify the root cause. Correct the problem, and then retry the standby master server removal operation.

CTGKM3237E Db2 credential check failed. Check whether Db2 server is running, and mapping of the host name to IP address on both the servers is correct.

Explanation:

System action:
The Add master operation fails.

Administrator response:
Ensure that the master server that is being added to the cluster has access to the database.

CTGKM3238E Exception occurred while updating replication configuration details.

Explanation:
During the replication setup, replication configuration fails.

System action:
The replication configuration operation fails.

Administrator response:
Check the IBM Security Guardium Key Lifecycle Manager log to identify the root cause. Correct the problem, and then retry the replication configuration operation.

CTGKM3239E Exception occurred while adding clone.

Explanation:
During the replication setup, replication configuration fails.

System action:
The replication configuration operation fails.

Administrator response:
Check the IBM Security Guardium Key Lifecycle Manager log to identify the root cause. Correct the problem, and then retry the replication configuration operation.

CTGKM3241E The IBM Security Guardium Key Lifecycle Manager version on the server is not the same as the IBM Security Guardium Key Lifecycle Manager version on the Multi-Master cluster.

Explanation:

System action:
The Add master operation fails.

Administrator response:
Ensure that the version of the master server to be added is the same as the version of the primary master server.

CTGKM3242E The operating system version or Db2 version of the server are different than those of the primary master server.

Explanation:
As a prerequisite check, the Add master operation validates whether the server has the same operating system and Db2 versions as those of the primary master server.

System action:
The Add master operation fails.

Administrator response:
Add a server that has the same operating system and Db2 versions as those of the primary master server, and retry the operation.

CTGKM3243E The Db2 user (For example, sklmdb41) does not have read-write permissions to the temp directory.

Explanation:
As a prerequisite check, the Add master operation validates the required permission to access the temp directory on the server. However, the validation fails.

System action:
The Add master operation fails.

Administrator response:
Ensure that the Db2 user (For example, sklmdb41) has read-write permissions to the temp directory on both the primary master server and the server to be added.

CTGKM3244E The server is unclean.

Explanation:
As a prerequisite check, the Add master operation validates whether the master server that is being added has any existing IBM Security Guardium Key Lifecycle Manager data, or whether the SKLMConfig properties file of the master server includes the config.keystore.ssl.certalias property. However, the validation fails.

System action:
The Add master operation fails.

Administrator response:
Ensure that the master server that is being added has a clean IBM Security Guardium Key Lifecycle Manager installation. Also, check whether the SKLMConfig properties file of the master server that is being added includes the config.keystore.ssl.certalias property.

CTGKM3245E The login credentials of the server are invalid.

Explanation:
As a prerequisite check, the Add master operation validates whether the server has the correct IBM Security Guardium Key Lifecycle Manager credentials. However, the validation fails.

System action:
The Add master operation fails.

Administrator response:
Specify valid login credentials for the server to be added, and retry the operation.

CTGKM3246E Agent of the remote instance is DOWN.

Explanation:
During the Add master operation, the primary master server tries to communicate with the agent, which runs on the remote master server that you want to add. However, the communication fails.

System action:
Test connection with the remote IBM Security Guardium Key Lifecycle Manager server fails.

Administrator response:
Ensure that the agent on the remote IBM Security Guardium Key Lifecycle Manager server is active and reachable.

CTGKM3247E The Db2 credentials of the server are different from those of the primary master server.

Explanation:
As a prerequisite check, the Add master operation validates the Db2 credentials of the master server that you want to add. However, the validation fails.

System action:
The Add master operation fails.

Administrator response:
Ensure that the Db2 credentials of the server to be added are the same as those of the primary master server.

CTGKM3248E Conflict report saved to file *VALUE_0* successfully.

Explanation:

System action:
The Join back ReadWrite master operation fails.

Administrator response:
Check the log entries to find out the reason for the failure. Make appropriate changes. Then, try the operation again. Check the logs to identify the root cause. Correct the problem and try again.

CTGKM3249E Failed to save join back conflict report. Please check logs for more information.

Explanation:

System action:
The Join back ReadWrite master operation fails.

Administrator response:
Check the logs to identify the root cause. Correct the problem and try again.

CTGKM3251E Failed to add a device in the group.

Explanation:
Device was not added to the PEER_TO_PEER device group.

System action:

Failed to add device to the PEER_TO_PEER device group.

Administrator response:
Check the logs to identify the root cause. Correct the problem and try again.

CTGKM3252E Invalid certificate. Certificate must have `Subject Alternative Name`.

Explanation:
The PEER_TO_PEER devices must have WWNN number in the **`Subject Alternative Name`** parameter of their certificate. The requesting certificate does not have this value. Hence, the operation fails.

System action:
Failed to add device to the PEER_TO_PEER device group.

Administrator response:
Use a valid certificate with the **`Subject Alternative Name`** parameter value and try again.

CTGKM3254E Filename provided is outside Data folder. Please provide a valid path and try again.

Explanation:

System action:

Administrator response:

CTGKM3255E You are not authorized to perform this action.

Explanation:
You do not have the required permissions to perform this action.

System action:
The operation fails.

Administrator response:
Assign the required permissions and retry the operation.

CTGKM3256E Cannot add device to the group *VALUE_0* because the number of devices in the group has reached its maximum limit.

Explanation:
Maximum two devices are allowed in a PEER_TO_PEER device group. The PEER_TO_PEER device group to which you tried to add a device already has two devices. Hence, the operation failed.

System action:
Failed to add device to the PEER_TO_PEER device group.

Administrator response:
Delete one of the existing devices in the PEER_TO_PEER device group and try again.

CTGKM3257E *VALUE_0* device type already exists in the group.

Explanation:
A PEER_TO_PEER device group can have two types of devices: Owner and Partner. The PEER_TO_PEER device group to which you tried to add a device already has these two device types. Hence, the operation failed.

System action:
Failed to add device to the PEER_TO_PEER device group.

Administrator response:
Delete the existing device type that you want to the PEER_TO_PEER device group and try again.

CTGKM3258E Cannot update the device certificate.

System action:
Failed to modify the device certificate in the PEER_TO_PEER device group.

Administrator response:
Check the logs to identify the root cause. Correct the problem and try again.

CTGKM3260E Failed to modify the certificate for the selected device.

System action:
Failed to modify the device certificate in the PEER_TO_PEER device group.

Administrator response:
Check the logs to identify the root cause. Correct the problem and try again.

CTGKM3261E Failed to delete the selected device.

Explanation:
Failed to delete the device certificate in the PEER_TO_PEER device group.

System action:
Failed to delete the device in the PEER_TO_PEER device group.

Administrator response:
Check the logs to identify the root cause. Correct the problem and try again.

CTGKM3263E Key addition is not allowed in the device group.

Explanation:

System action:

Administrator response:

CTGKM3264E Cannot modify the certificate because the WWNN value of the certificate does not match the existing name.

Explanation:
A device in the PEER_TO_PEER device group can be modified with the new certificate only if the WWNN value of the new certificate matches the WWNN value of the expired certificate.

System action:
Failed to modify the device in the PEER_TO_PEER device group with the new certificate.

Administrator response:
Ensure that the new certificate is valid and its WWNN value matches with the WWNN value of the expired certificate. Then, retry the operation.

CTGKM3265E Cannot access the file because the specified file path is invalid. Enter a valid file path within the data folder and try again.

Explanation:
The file path that you specified does not meet the policy requirements of IBM Security Guardium Key Lifecycle Manager.

System action:
File upload from the specified location fails.

Administrator response:
Ensure that you add the file in the approved file path and retry the file upload operation.

CTGKM3266E User is not authorized to perform this action.

Explanation:
The authenticated user does not have the permissions to perform the requested operation.

System action:
Requested operation fails to run.

Administrator response:
Check the permissions that are assigned to the user.

CTGKM3267E Invalid credentials to create the PEER_TO_PEER device group.

Explanation:
User can create PEER_TO_PEER device group through a KMIP request by using the KMIP extensions of IBM Security Guardium Key Lifecycle Manager. Invalid KMIP credentials are used to create the PEER_TO_PEER device group. Hence, the operation failed.

System action:
The operation to create device group through KMIP request fails.

Administrator response:
Check and correct the KMIP credentials in the KMIP request and try again.

CTGKM3268E Failed to create the PEER_TO_PEER device group.

Explanation:
Failed to create PEER_TO_PEER device group through KMIP request.

System action:
The operation to create device group through KMIP request fails.

Administrator response:
Check the logs to identify the root cause. Correct the problem and try again.

CTGKM3269E Failed to add the device to the device group. The device group does not exist.

Explanation:
Failed to add device to the PEER_TO_PEER device group through KMIP request because the device group was not found.

System action:
The Add device to device group operation fails.

Administrator response:
Create the device group and then add the device to it.

CTGKM3270E Failed to add device in the device group.

Explanation:

System action:
The Add device to the PEER_TO_PEER device group operation fails.

Administrator response:
Check the logs to identify the root cause. Correct the problem and try again.

CTGKM3271E Invalid request to create the PEER_TO_PEER device group.

Explanation:
The KMIP request structure for creating the PEER_TO_PEER device group is invalid.

System action:
The operation to create device group through KMIP request fails.

Administrator response:
Check and correct the KMIP request structure and try again.

CTGKM3272E Failed to accept pending client certificate for the PEER_TO_PEER device group.

Explanation:

System action:

Administrator response:

CTGKM3274E 'deviceRole' is mandatory parameter for the given 'applicationName'.

Explanation:

System action:

Administrator response:

CTGKM3275E Cannot create device group *VALUE_0*. The device group already exists.

Explanation:
Failed to create the PEER_TO_PEER device group because it already exists.

System action:
The operation to create device group through KMIP request fails.

Administrator response:
Specify a different name for the device group in the KMIP request structure and try again.

CTGKM3276E Invalid value *VALUE_0* device role.

Explanation:

System action:

Administrator response:

CTGKM3277E Invalid characters found in device group name *VALUE_0*.

Explanation:
Failed to create the PEER_TO_PEER device group because the device name in the KMIP request contains invalid characters.

System action:
The operation to create device group through KMIP request fails.

Administrator response:
In the KMIP request structure, specify a device group name with valid characters, and try again.

CTGKM3278E Invalid request for PEER_TO_PEER device group creation. WWNN value for the peer system is missing.

Explanation:
Failed to create the PEER_TO_PEER device group because the KMIP request does not include the WWNN value, which is a mandatory attribute in the KMIP request.

System action:
The operation to create device group through KMIP request fails.

Administrator response:
In the KMIP request structure, specify the WWNN value for the peer system, and try again.

CTGKM3279E Cannot add the device as the PEER member of the device group *VALUE_0* because its WWNN value is invalid.

Explanation:
Failed to add the device as the PEER member of the device group because its WWNN value does not match the WWNN value that is set by the owner of the device group. The device group WWNN value is set during the device group creation.

System action:
The operation to add device group fails.

Administrator response:
In the KMIP request structure, specify the device's WWNN value. Ensure that the value is the same as the WWNN value of the device group, and try again.

CTGKM3280E Device with WWNN *VALUE_0* already exists in the device group *VALUE_1*

Explanation:

System action:
The operation to add device group fails.

Administrator response:
Create another device group and add the device in it.

CTGKM3282E You are not authorized to perform this action.

Explanation:
You do not have the required permissions to perform this action.

System action:
The operation fails.

Administrator response:
Assign the required permissions and retry the operation.

CTGKM3285E Cannot add the master server. Host certificate of the master server to be added cannot be trusted.

Explanation:
Authentication of the master server to be added fails. Its host certificate was not issued by a trusted certificate authority, and cannot be trusted.

System action:
The add master server operation fails.

Administrator response:

Go to Advanced Configuration > Client device communication certificates page and add the certificate manually.

CTGKM3286E TLS connection with the master server to be added fails because the certificate of the master server is not received.

Explanation:
TLS connection with the master server to be added fails. Certificate of the host of the master server is not received.

System action:
The operation fails.

Administrator response:
Check the logs for more information.

CTGKM3287E Cannot add master server because the host certificate of the master server cannot be trusted.

Explanation:
Cannot trust the certificate of the host of the master server to be added.

System action:
The operation fails.

Administrator response:
Go to Advanced Configuration > Client device communication certificates page and add the certificate manually.

CTGKM3288E Cannot delete the template. The template UUID is incorrect or invalid.

Explanation:
The template cannot be deleted because the template UUID that is provided is invalid or incorrect.

System action:
The delete template operation fails.

Administrator response:
Specify a valid template UUID and retry the operation.

CTGKM3289E Cannot delete the secret data. The secret data UUID is incorrect or invalid.

Explanation:
The secret data cannot be deleted because the secret data UUID that is provided is invalid or incorrect.

System action:
The delete secret data operation fails.

Administrator response:
Specify a valid secret data UUID and retry the operation.

CTGKM3295E Device group master key is already enabled for device group *VALUE_0* .

Explanation:

System action:
The Enable master key for device group operation fails.

Administrator response:
Ensure that the master key for the device group is not already enabled before you perform the Enable master key for device group operation.

CTGKM3296E Device group master key is already disabled for device group *VALUE_0* .

Explanation:

System action:
The Disable master key for device group operation fails.

Administrator response:
Ensure that the master key for the device group is not already disabled before you perform the Disable master key for device group operation.

CTGKM3297E Cannot update the configuration property of the device group master key because the value already exists.

Explanation:
The value of the configuration property is not updated because the same value already exists.

System action:
The operation to update the device group master key configuration fails.

Administrator response:
Specify a different value for the configuration property and retry the operation.

CTGKM3298E Cannot update the configuration property of the device group master key. The new value *VALUE_0* is invalid.

Explanation:
An invalid value is specified for the configuration property VALUE_0. So the property is not updated.

System action:
The operation to update the device group master key configuration fails.

Administrator response:
Specify a valid value for the configuration property and retry the operation.

CTGKM3299E Device group master key rotation operation failed. Check logs for more information.

Explanation:
Processing fails during the Device group master key rotation operation.

System action:
The Disable master key for device group operation fails.

Administrator response:
Check the logs to identify the root cause. Correct the problem and try again.

CTGKM3304E Device group master key not enabled for device group *VALUE_0* .

Explanation:

System action:
The Device group master key rotation operation fails.

Administrator response:
Before you perform the Device group master key rotation operation, ensure that the device group master key is enabled for the device type.

CTGKM3305E Keys cannot be exported. Specify either an alias or a list of aliases.

Explanation:
To export keys, specify either an alias or a list of aliases.

System action:
The key export operation fails.

Administrator response:
Specify either alias or a list of aliases, and retry the operation.

CTGKM3306E The key cannot be imported because the file contains multiple aliases. Specify the alias of the key to be imported.

Explanation:
To import a key, the alias of the key to be imported must be specified.

System action:
The key import operation fails.

Administrator response:
Specify the alias of the key to be imported, and retry the operation.

CTGKM3307E Keys cannot be exported. Specify either aliases or aliasRange.

Explanation:
To export keys, specify either the aliases or range of aliases.

System action:
The key export operation fails.

Administrator response:
Specify either aliases or range of aliases, and retry the operation.

CTGKM3321E Error loading encryptor object of type: *VALUE_0* .

Explanation:

System action:

Administrator response:

CTGKM3322E Error occurred while performing encryption.

Explanation:

System action:

Administrator response:

CTGKM3323E Error occurred while performing decryption.

Explanation:

System action:
The decryption operation fails.

Administrator response:
Rerun the master key management or master key for device group management operation.

CTGKM3324E Error Creating new master key.

Explanation:

System action:

Administrator response:

CTGKM3325E Cannot update the master key. Check the debug log for more information.

Explanation:
The new master key cannot be applied because of an internal error. Check the debug log for more information.

System action:
The operation to update the master key fails.

Administrator response:
Check the debug log to identify the root cause. Correct the problem and retry the operation.

CTGKM3326E Error loading master key object.

Explanation:

System action:

Administrator response:

CTGKM3327E HSM is not configured correctly.

Explanation:
IBM Security Guardium Key Lifecycle Manager is not configured correctly to use HSM. The usemasterkeyinhsm property is set to 'true' but one or more required properties might not be configured correctly.

System action:
The operation fails.

Administrator response:
Review and correct the HSM configuration properties, and retry the operation.

CTGKM3329E **Selected certificate has already expired. Please select an active certificate.**

Explanation:

System action:

Administrator response:

CTGKM3330E **Key details cannot be displayed for multiple keys at a time. Select a row and try again.**

Explanation:
You can view details for only one key at a time, from the search results on the Search page.

System action:
Key details are not displayed.

Administrator response:
Select a key or a row in the search results table, and click View.

CTGKM3331E **The key cannot be exported. You can export only symmetric and private keys.**

Explanation:
You can export only symmetric and private keys.

System action:
The key is not exported.

Administrator response:
You can export only symmetric and private keys.

CTGKM3332E **Cannot update the master key because the same master key already exists.**

Explanation:
The master key to be updated already exists.

System action:
The operation to update master key fails.

Administrator response:
Specify a different master key and retry the operation. Check the debug log for more information.

CTGKM3334E **The key cannot be imported because a key with the same alias already exists. Use a different alias to import the key.**

Explanation:
To import a key, specify a unique alias.

System action:
The key will not be imported.

Administrator response:
Specify a unique alias, and retry the operation.

CTGKM3335E **Cannot import the key. Check the debug log for more information.**

Explanation:
The key cannot be imported because of an internal error. Check the debug log for more information.

System action:
Key import operation fails.

Administrator response:
Check the debug log file to find the root cause, correct the problem, and retry the operation.

CTGKM3336E **Cannot import the key because the export file does not contain a object with the alias mentioned. Check the export file and try again.**

Explanation:
The import key operation fails if the export file does not contain a object with the alias mentioned.

System action:
The key is not imported.

Administrator response:
Ensure that the export file contains an object with the mentioned alias, and retry the operation.

CTGKM3337E **Unable to clear the cache on the *VALUE_0* server. Check the debug log for more information.**

Explanation:
Cannot clear the cache on the VALUE_0 server because of an internal error.

System action:
The operation to clear cache fails.

Administrator response:
Check the debug log to identify the root cause. Correct the problem and retry the operation. Alternatively, try to clear the cache manually.

CTGKM3338E **Failed to perform *VALUE_0* operation. *VALUE_1* operation is pending.**

Explanation:

The Device group master key operation fails because another Device group master key operation is in progress.

System action:
The Device group master key operation fails.

Administrator response:
Before you start a Device group master key operation, ensure that no other Device group master key operation is in progress.

CTGKM3340E ***VALUE_0*** **field must be specified for attribute** ***VALUE_1*** **.**

Explanation:
The listed field is required when adding or updating this attribute.

System action:
The operation fails.

Administrator response:
Specify value for the listed field, then try the operation again.

CTGKM3342E **Unable to import the device group because a device group master key operation is pending.**

Explanation:
The import device group operation fails because a device group master key operation is in pending state.

System action:
The operation to import device group fails.

Administrator response:
Check debug log for the device group master key operation that is failed. Complete the pending operation and retry the import operation.

CTGKM3343E **Unable to export the device group because a device group master key operation is pending.**

Explanation:
The export device group operation fails because a device group master key operation is in pending state.

System action:
The operation to export device group fails.

Administrator response:
Check debug log for the device group master key operation that is failed. Complete the pending operation and retry the export operation.

CTGKM3344E **Unable to refresh or move the master key. Previous run of the master key refresh or movement was incomplete. Retry the operation with the same** ***VALUE_0*** **that was used in the previous run -** ***VALUE_1***

Explanation:
Previous run of the master key refresh or movement was incomplete. Retry the operation with the same VALUE_0 used in previous run - VALUE_1

System action:
The master key refresh or movement operation fails.

Administrator response:
Retry the master key refresh or movement operation with the same VALUE_0 - VALUE_1.

CTGKM3345E **Master Key Movement is already in progress.**

Explanation:

System action:
The Master key movement operation fails.

Administrator response:
Check the logs to identify the root cause. Correct the problem and retry the operation with the same masterKeySize value that was used in the previous run.

CTGKM3346E **Unable to get master key size from configuration** ***ERROR_MESSAGE***

Explanation:

System action:
The Get master key keysize operation fails.

Administrator response:
Check the logs to identify the root cause. Correct the problem and try again.

CTGKM3347E **Input parameters `source` and `destination` cannot have the same value.**

Explanation:
Master key movement operation fails because the **`source`** and **`destination`** values are the same.

System action:
The Master key movement operation fails.

Administrator response:
Modify the **`source`** or **`destination`** value and try again.

CTGKM3348E **Input parameters source and destination are required for Master Key movement.**

Explanation:

System action:
The Master key movement operation fails.

Administrator response:
Modify the source or destination value and try again.

CTGKM3351E **Error occurred while deleting the Java Keystore file.**

Explanation:

The Master key movement operation fails with an error.

System action:
The Master key movement operation fails.

Administrator response:
Check the logs to identify the root cause. Correct the problem and try again.

CTGKM3352E Unable to start the Device group master key operation because the Master key management operation is in progress.

Explanation:
The Device group master key operation cannot start while the Master key management operation is in progress.

System action:
The Device group master key operation fails.

Administrator response:
Start the Device group master key operation after the Master key management operation is completed.

CTGKM3353E Error when encrypting device group master key DB Table data with new MasterKey: *ERROR_MESSAGE*

Explanation:
Processing failed when creating new master key for encryption. Error when encrypting device group master key DB Table data with new MasterKey

System action:
The operation fails.

Administrator response:
Retry the operation

CTGKM3354E Error in encrypting data related to Multi-Master cluster with the new master key: *ERROR_MESSAGE*

Explanation:
Processing failed when creating new master key for encryption. Error when encrypting MM Instance DB Table data with new MasterKey

System action:
The operation fails.

Administrator response:
Retry the operation

CTGKM3355E Error in encrypting data related to opaque objects with the new master key: *ERROR_MESSAGE*

Explanation:
Processing failed when creating new master key for encryption. Error when encrypting OpaqueObject DB Table data with new MasterKey

System action:
The operation fails.

Administrator response:
Retry the operation

CTGKM3356E Cannot delete keystore on the following IBM Security Guardium Key Lifecycle Manager master servers: *ERROR_MESSAGE*

Explanation:
Processing failed when deleting java keystore.

System action:
The operation fails.

Administrator response:
Manually delete Keystore and tklm.encryption.password property from SKLMConfig.properties file.

CTGKM3357E Cannot delete HSM configuration properties on the following IBM Security Guardium Key Lifecycle Manager master servers: *ERROR_MESSAGE* .

Explanation:
Processing failed when deleting HSM configuration porperties.

System action:
The operation fails.

Administrator response:
Retry the operation

CTGKM3358E Prerequisite check failed. HSM is not configured on the following IBM Security Guardium Key Lifecycle Manager master servers: *ERROR_MESSAGE* .

Explanation:
Processing failed in Pre-requisite check.

System action:
The operation fails.

Administrator response:
Retry the operation with HSM configured on all instances.

CTGKM3359E Agent restart failed.

Explanation:
Processing failed in Restarting Agent.

System action:
The operation fails.

Administrator response:
Stop agent on all instances.

CTGKM3365E Unable to connect to the database: *ERROR_MESSAGE* .

Explanation:
Error occurred while connecting to the database.

System action:
The operation fails.

Administrator response:
Check the database connection.

CTGKM3366E Cannot perform the requested operation. A critical operation is in progress. Try after some time.

Explanation:
Processing failed in performing requested operation.

System action:
The operation fails.

Administrator response:
Complete other SKLM operation first.

CTGKM3367E IBM Security Guardium Key Lifecycle Manager master with hostname *VALUE_0* is not reachable.

Explanation:
Processing failed in performing requested operation on master.

System action:
The operation fails.

Administrator response:
Make sure all Master are up and reachable.

CTGKM3368E Cannot run master key management functions on this multi-master cluster because the following IBM Security Guardium Key Lifecycle Manager master servers are configured as read-write master servers: *VALUE_0* .

Explanation:
Processing failed in performing requested operation on master. It is configured as read write master.

System action:
The operation fails.

Administrator response:
Make sure no read - write master is present in cluster.

CTGKM3369E Failed to add master server because no server certificate is marked In Use.

Explanation:
Add master server operation fails.

System action:
The operation fails.

Administrator response:
Mark the required server certificate as In use and try again.

CTGKM3371E PKCS11 library path is not provided.

Explanation:
PKCS11 library path is not provided in the config file.

System action:
The operation fails.

Administrator response:
Provide PKCS11 library path in the config file and run the operation again.

CTGKM3372E PKCS11 library path provided is not a valid path *VALUE_0* .

Explanation:
PKCS11 library path is not valid in the config file.

System action:
The operation fails.

Administrator response:
Provide a valid PKCS11 library path in the config file and run the operation again.

CTGKM3373E HSM pin is null.

Explanation:
HSM pin is not provided in the config file.

System action:
The operation fails.

Administrator response:
Provide HSM pin in the config file and run the operation again.

CTGKM3380E The `TransportListener.ssl.protocols` configuration property of the server is different than that of the primary master server.

Explanation:
As a prerequisite check, the Add master operation validates whether the server has the same value for the **`TransportListener.ssl.protocols`** configuration property as that of the primary master server.

System action:
The Add master operation fails.

Administrator response:
Specify the same value for the **`TransportListener.ssl.protocols`** configuration property as that of the primary master server, and retry the operation.

CTGKM3381E Unable to refresh the master key because master key for none of the

device groups is due for rotation. Refresh the master key forcefully.

Explanation:
Master key for none of the device groups is due for rotation.

System action:
Master key refresh operation fails.

Administrator response:
Refresh the master key forcefully.

CTGKM3382E Request failed. You cannot delete this master server because you are logged in to it. Log in from another master server in the Multi-Master cluster and try again.

Explanation:
You cannot use this master server to delete itself.

System action:
The operation fails.

Administrator response:
Log in to another master server in the Multi-Master cluster to delete this master server.

CTGKM3383E Cannot add a standby master server because these HADR master servers are unreachable or out of sync: *VALUE_0*

Explanation:
Addition of standby master failed because some of the existing HADR master are unreachable or out of sync. Make sure all the HADR master servers are reachable and in sync with the cluster.

System action:
Addition of standby master fails.

Administrator response:
Ensure that all the HADR master servers are reachable and in sync with the cluster.

CTGKM3384W These HADR master servers are either unreachable or out of sync: *VALUE_0* . If you continue, these master servers will be out of sync and you will need to sync them later. Do you still want to continue?

Explanation:
You can add a non-HADR master server to the Multi-Master cluster even if one or more HADR master servers are unreachable or out of sync. You need to explicitly confirm this action before proceeding.

System action:
Non-HADR master server is added only after you confirm that you want to proceed even though some of the HADR master servers are unreachable or out of sync.

Administrator response:
Review the list of master servers that are unreachable or out of sync and proceed. You need to synchronize them later.

CTGKM3385W Values of the Db2 kernel parameters on server *VALUE_0* do not meet the minimum requirement. However, the server will be added to the cluster.

Explanation:
Db2 kernel parameters must meet the minimum requirements to configure a Multi-Master cluster. The appropriate values are available in the product documentation in the IBM Knowledge Center.

System action:
The master server will be added to the cluster.

Administrator response:
Set the appropriate values for the kernel parameters on the primary master server and on the server to be added, and then configure the Multi-Master cluster. For information about the parameter values, see the product documentation in the IBM Knowledge Center.

CTGKM3386W Values of the Db2 kernel parameters on this server do not meet the minimum requirement. However, the server will be added to the cluster.

Explanation:
Db2 kernel parameters must meet the minimum requirements to configure a Multi-Master cluster. The appropriate values are available in the product documentation in the IBM Knowledge Center.

System action:
The master server will be added to the cluster.

Administrator response:
Set the appropriate values for the kernel parameters on the primary master server and on the server to be added, and then configure the Multi-Master cluster. For information about the parameter values, see the product documentation in the IBM Knowledge Center.

CTGKM3391E Failed to synchronize the master server. Check logs for details.

Explanation:
The master server cannot be synchronized because of an internal error.

System action:
The Sync master server operation fails.

Administrator response:

Check the log file to find the root cause, correct the problem, and retry the operation.

CTGKM3393E Replication failed. At least one clone server must be added.

Explanation:

System action:

Administrator response:

CTGKM3394E Cannot change the role because replication server is running. Stop the replication server and try again.

Explanation:

System action:

Administrator response:

CTGKM3395E Search failed. Specify at least one search criterion and try again.

Explanation:

System action:

Administrator response:

CTGKM3397E Cannot synchronize this master server as it is a read-write master.

Explanation:
When you try to synchronize a master server that is in read-write mode, the operation fails. A read-write master server is temporarily out of the cluster, and hence, cannot be synced.

System action:
The Sync master server operation fails.

Administrator response:
Join the read-write master server to the cluster, and retry the operation.

CTGKM3398E Cannot synchronize this master server as it is already in sync.

Explanation:
You cannot synchronize a master server that is already in sync with the cluster.

System action:
The Sync master server operation fails.

Administrator response:
No action needed.

CTGKM3399E Cannot perform this operation. The connected database might be read-only.

Explanation:

System action:

Administrator response:

CTGKM3400E Single standby is not allowed to be removed because there exists NON HADR masters in the cluster. Delete NON HADR masters before breaking the cluster.

Explanation:

System action:

Administrator response:

CTGKM3401E Cannot remove this master server. It was the primary master server of the cluster.For more information, contact IBM Support.

Explanation:

System action:

Administrator response:

CTGKM3402E Cannot delete a standby master server because these HADR master servers are unreachable or out of sync: *VALUE_0*

Explanation:

System action:

Administrator response:

CTGKM3403E Master server *VALUE_0* is unable to connect to the database.

Explanation:

System action:

Administrator response:

CTGKM3405E Unable to obtain certificate or key because the specified ID *VALUE_0* is incorrect.

Explanation:
The VALUE_0 ID is incorrect.

System action:
The operation to obtain certificate or key fails.

Administrator response:
Specify a valid and correct ID and retry the operation.

CTGKM3406E Unable to complete the REST based key serving operation because the REST based key serving is not supported for the client *VALUE_0* .

Explanation:
VALUE_0 client is not of REST type. Hence REST key serving is not allowed.

System action:
The REST based key serving operation fails.

Administrator response:
Select a client that supports REST based key serving and retry the operation.

CTGKM3407E ***VALUE_0* user is not authorized to perform this operation.**

Explanation:
VALUE_0 user is not authorized to perform this operation.

System action:
The REST based key serving operation fails.

Administrator response:
Assign the klmClientUser user role to the user and retry the operation.

CTGKM3408E **Unable to obtain client details. Client with *VALUE_0* name not found.**

Explanation:
Client with VALUE_0 name does not exist in IBM Securiy Key Lifecycle Manager.

System action:
The operation to obtain client details fails.

Administrator response:
Specify a valid and correct client name and retry the operation.

CTGKM3410E **Unable to assign the certificate with alias *VALUE_0* to the client because the alias is incorrect.**

Explanation:
Client communication certificate with VALUE_0 alias does not exist in IBM Securiy Key Lifecycle Manager.

System action:
The certificate assignment operation fails.

Administrator response:
Specify a valid client communication certificate, and retry the operation.

CTGKM3414E **Unable to assign the user *VALUE_0* to the client. User with this name does not exist in the WebSphere® Application Server or does not have the klmClientUser user role assigned to it.**

Explanation:
User with VALUE_0 name does not exist in the WebSphere Application Server or does not have the klmClientUser user role assigned to it.

System action:
The user assignment operation fails.

Administrator response:
Specify a valid user name, and retry the operation.

CTGKM3415E **Cannot assign user *VALUE_0* to the client because the user is already associated with the client.**

Explanation:
Cannot assign VALUE_0 user to the client because it is already assigned to the client.

System action:
The user assignment operation fails.

Administrator response:
Specify a different user to be assigned to the client.

CTGKM3418E **Cannot remove user. User *VALUE_0* is not associated with client.**

Explanation:

System action:

Administrator response:

CTGKM3419E **Certificate is not communication certificate. Cannot assign to client.**

Explanation:

System action:

Administrator response:

CTGKM3421E **Cannot assign the certificate to the client because the client does not use KMIP for communication.**

Explanation:
The certificate cannot be assigned to the client because the client does not use KMIP for communication.

System action:
The certificate assignment operation fails.

Administrator response:
Use a client with type as KMIP, and retry the operation.

CTGKM3422E **Unable to obtain object details because the user is assigned to multiple clients. Specify a client name in the request and try again. name.**

Explanation:
Cannot obtain object details because the user is assigned to multiple clients.

System action:
The operation to list objects fails.

Administrator response:
Specify the client for which you want to obtain object details.

CTGKM3423E **Cannot assign certificate to the client because the certificate is already assigned to another client.**

Explanation:
The alias of the certificate that is to be assigned is already associated with another client. A certificate can be associated with one client only.

System action:
The operation to assign certificate fails.

Administrator response:
Specify a unique alias for the client communication certificate to be assigned to the client, and retry the operation.

CTGKM3424E **One or more values have changed since the last time you checked the eligibility of the server to be added to the cluster. Click Check Prerequisites and then add the server to the cluster.**

Explanation:

System action:

Administrator response:

CTGKM3425E **Client not present for certificate cannot process kmip request**

Explanation:

System action:

Administrator response:

CTGKM3426E **Cannot create or register the key because the specified cryptographic length is invalid. Specify a valid integer value and try again.**

Explanation:
The cryptographic length value is invalid. It must be an integer value.

System action:
The create or register key operation fails.

Administrator response:
Specify a valid integer value as the cryptographic length, and retry the operation.

CTGKM3427E **Unable to resolve the host name or IP address of the server. Check if both the servers are able to connect to each other using hostname.**

Explanation:
As a prerequisite check, the Add master server operation verifies whether both the servers (primary master server and server to be added) are able to connect to each other using their hostnames.

System action:
The Add master operation fails.

Administrator response:

CTGKM3428E **The server is unreachable. Check the network connectivity and ensure that the WebSphere Application Server is running.**

Explanation:
As a prerequisite check, the Add master server operation verifies whether the server is reachable.

System action:
The Add master operation fails.

Administrator response:
Check the firewall rules, network connectivity, and ensure that the WebSphere Application Server is running.

CTGKM3429E **Incorrect value for client name *VALUE_0***

Explanation:
The client name must follow the requirement: 1. Can only contain alphanumeric characters and underscore. 2. First character cannot be a digit. 3. Maximum length is 256.

System action:
The operation fails.

Administrator response:
The client name must follow the requirement: 1. Name can only contain alphanumeric character and underscore 2. First character cannot be a digit. 3. Maximum length should be 16.

CTGKM3430E **Unable to create client because a client with the same name *VALUE_0* already exists.**

Explanation:
Failed to create client with name VALUE_0 because a client with the same name already exists.

System action:
The create client operation fails.

Administrator response:
Specify a client name that does not exist in IBM Security Guardium Key Lifecycle Manager, and retry the operation.

CTGKM3431E **Cannot delete a client because cryptographic objects are associated with the client.**

Explanation:
Client cannot be deleted because one or more cryptographic objects, such as keys, certificates, secret data, or opaque data, are associated with the client.

System action:
The operation to delete client fails.

Administrator response:
Delete the cryptographic objects that are associated with the client. Then delete the client.

CTGKM3432E Failed to restart the Multi-Master cluster. Check logs for more information.

Explanation:
Failed to restart the Multi-Master cluster because of an internal error. Check logs for more information.

System action:
The Restart Cluster operation fails.

Administrator response:
Check the log file to find the root cause, correct the problem, and retry the operation.

CTGKM3434E Failed to stop the Multi-Master cluster. Check logs for more information.

Explanation:
The Multi-Master cluster cannot stop because of an internal error. Check the debug log for more information.

System action:
The stop cluster operation fails.

Administrator response:
Check the log file to find the root cause, correct the problem, and retry the operation.

CTGKM3436E The Agent is unreachable on one or more master servers: *VALUE_0*

Explanation:
The Agent status check fails. Hence, it is down on one or more master servers.

System action:
The Agent status check fails.

Administrator response:
Start the agent and retry the operation.

CTGKM3438E Served data archive failed because *VALUE_0* .

Explanation:

System action:

Administrator response:

CTGKM3439E Database on one or more instances is down : *VALUE_0*

Explanation:
The database is down on one or more master servers.

System action:
The database status check fails.

Administrator response:
Start the database, ensure that it is reachable, and then retry the operation.

CTGKM3440E WebSphere Application Server is unreachable on one or more master servers : *VALUE_0* .Check the network connectivity and ensure that the WebSphere Application Server is running.

Explanation:
WebSphere Application Server is down or unreachable on one or more master servers.

System action:
WebSphere Application Server status check fails.

Administrator response:
Start the WebSphere Application Server, ensure that it is reachable, and then retry the operation.

CTGKM3443E Cannot update the client name. Client with the name *VALUE_0* already exists.

Explanation:
Failed to update client name because a client with the same name already exists.

System action:
The operation to update client name fails.

Administrator response:
Specify a unique client name and retry the operation.

CTGKM3444E Cannot register key or certificate. The size of the key does not match the bitlength value.

Explanation:
The value that is derived from the keyMaterial parameter does not match the value of the bitlength parameter.

System action:
The operation to register key or certificate fails.

Administrator response:
Change the bitlength parameter value to match the value that is derived from the keymaterial parameter, and retry the operation.

CTGKM3449E The database password cannot be changed because of an internal error. Check the debug log for more information.

Explanation:
Failed to change the database password because of an internal error.

System action:
The operation to change the database password fails.

Administrator response:

Check the debug log to identify the root cause. Correct the problem and retry the operation.

CTGKM3450E Unable to stop HADR. Check logs for more information.

Explanation:
Failed to stop HADR in the Multi-Master cluster.

System action:
Stop HADR operations fails.

Administrator response:
Check logs file to find the root cause, correct the problem, and retry the operation.

CTGKM3451E The Db2 password cannot be changed. Check that the password is valid, and that the primary database is running and reachable from other master servers of the cluster.

Explanation:
Failed to change Db2 password because the password provided is invalid or the primary database in unreachable from other master servers.

System action:
Change Db2 password operation fails.

Administrator response:
Ensure the primary database is reachable to all the master servers and the password provided is valid.

CTGKM3453E Failed to update Db2 password in Websphere application server datasource.

Explanation:
The Update Db2 password in Websphere application server datasource failed because of an internal error.

System action:
The Change Db2 password operation fails.

Administrator response:
Check logs to find the root cause, correct the problem, and retry the operation.

CTGKM3454E Restore to the clone server failed. Check logs for more information

Explanation:

System action:
The replication process fails.

Administrator response:
Check logs for more information.

CTGKM3455E Unable to fetch master server details from the database. Ensure that the primary database is running.

Explanation:
Cannot fetch master server details from the database. The primary database might be unreachable or down.

System action:
The fetch master server details operation fails.

Administrator response:
Ensure that the primary database is running and reachable from all the master servers, and retry the operation.

CTGKM3456E Backup transfer to clone failed. Check debug log for more information.

Explanation:
The master server was backed up. However, transfer of the backup to the clone server failed.

System action:
The replication process failed.

Administrator response:
Check logs for more information.

CTGKM3457E Connection to the clone server failed. Check network connectivity.

Explanation:
The master server is unable to connect to the clone server.

System action:
The replication process failed.

Administrator response:
Check network connectivity between the master and clone servers.

CTGKM3458E Backup dates on the master and clone servers are out of sync.

Explanation:
Backup date on the master server is ahead of the current date on the clone server by at least one hour. Sync the system clocks of the servers.

System action:
The replication operation fails.

Administrator response:
Synchronize the system clocks of the master and clone servers.

CTGKM3459E Failed to create backup on the master server during the replication process. Check logs for more information.

Explanation:
Backup could not be created on the master server during the replication process.

System action:
The replication operation fails.

Administrator response:
Check the logs to identify the root cause.

CTGKM3460E User request failed. It is having unauthorized token in its header.

Explanation:
HTTP request has failed because XSRF token in request in missing or invalid.

System action:
Check for XSRF token in user request

Administrator response:
Check the logs for specific information.

CTGKM3461E Unable to delete the export file. Specify the correct file path and try again.

Explanation:
Export file path provided is not valid.

System action:
Export file delete failed.

Administrator response:
Specify a valid export file path.

CTGKM3462E Cannot *VALUE_0* the file the file *VALUE_0* because file does not exist or the given file path is invalid.

Explanation:
The specified file name is incorrect, the file does not exist, or the file path is invalid. The file must be located in the SKLM_DATA folder.

System action:
File download operation fails.

Administrator response:
Specify a valid file name and path to download the file.

CTGKM3463E Cannot *VALUE_0* file because the file type is invalid.

Explanation:
The file to be downloaded/uploaded has an invalid file type or extension. Only files with the following file extensions can be uploaded: cer, der, pem, p12, exp, csr, txt, zip, jar.

System action:
File download operation fails.

Administrator response:
Specify a valid file type.

CTGKM3464E File upload failed. Check logs for more information.

Explanation:
Unable to upload file.

System action:
File upload operation fails.

Administrator response:
Check the logs to identify the root cause. Correct the problem and try again.

CTGKM3466E Cannot upload the file *VALUE_0* because a file with the same name already exists on the server.

Explanation:
File cannot be uploaded.

System action:
File upload process fails.

Administrator response:
Specify a different name for the file, which does not match the name of the existing file on the server, or delete the file on the server, and try again.

CTGKM3467E REST API failed. Parameter *VALUE_0* is empty or has an invalid value.

Explanation:
A mandatory parameter is missing or has an invalid value.

System action:
REST API for upload or download fails.

Administrator response:
Ensure that the parameters in the REST API contain valid values, and run the REST API again.

CTGKM3468E Cannot create key group because a key group with the same name already exists on the server.

Explanation:
Cannot create key group because a key group with the same name already exists on the server.

System action:
The operation fails.

Administrator response:
Specify an alternative name for the key group. Then, try the operation again.

CTGKM3469E File *VALUE_0* upload not allowed. Its size exceeds maximum allowed limit.

Explanation:
File size is more then allowed size.

System action:
Not to upload any part of the file.

Administrator response:
Ensure that file size is in permissible range.

CTGKM3471E Invalid Component Type *VALUE_0* . Supported Component Type are

IPP, KMIP, REST, GUI, DATABASE, AGENT.

Explanation:

System action:

Administrator response:

CTGKM3472E Cannot upload file *VALUE_0* . The file format for the file extension is not valid.

Explanation:
The file format does not match the extension of the file, or the file might be corrupted.

System action:
The file is not uploaded.

Administrator response:
Ensure that the file is not corrupted and the file format matches the file extension. Then, retry the upload operation.

CTGKM3473E Failed to synchronize the databases of primary and standby master servers after data merging. Check the debug log for more information.

Explanation:
The database synchronization operation between primary and standby master servers failed after data merging.

System action:
Database synchronization operation fails.

Administrator response:
Check the debug log file to find the root cause, correct the problem, and retry the operation.

CTGKM3474E Cannot download the log file. Check the debug log for more information.

Explanation:
Downloading of the log file failed because of an internal error.

System action:
The file download operation fails.

Administrator response:
Check the debug log file to find the root cause, correct the problem, and retry the operation.

CTGKM3475E Failed to merge data from the primary master servers of the clusters. Check the debug log for more information.

Explanation:
Data merging between the two clusters failed during cluster merging operation.

System action:
Cluster merging operation fails.

Administrator response:
Check the debug log file to find the root cause, correct the problem, and retry the operation.

CTGKM3476E Data backup or restore operation failed during cluster merging. Check the debug log for more information.

Explanation:
Data backup on the primary master server or data restore on the standby master server failed during the merging of the two clusters.

System action:
The merge clusters operation fails.

Administrator response:
Check the debug log file to find the root cause, correct the problem, and retry the operation.

CTGKM3477E Failed to reconfigure Db2 HADR on a master server during cluster merging. Check the debug log for more information.

Explanation:
Reconfiguration of Db2 HADR on at least one HADR master server failed during merging of the two clusters.

System action:
The merge clusters operation fails.

Administrator response:
Check the debug log file to find the root cause, correct the problem, and retry the operation.

CTGKM3479E Failed to update the Multi-Master configuration properties file after cluster merging.

Explanation:
Updating the properties file after cluster merging failed.

System action:
No action required.

Administrator response:
No action required.

CTGKM3481E Failed to restart the agent. Restart agent manually on all master servers and try again.

Explanation:
The agent cannot be restarted.

System action:
The agent restart operation fails.

Administrator response:

Restart agent manually on all the master servers and try again.

CTGKM3483E Cannot merge the clusters because one or more master servers of the clusters are not reachable.

Explanation:
Merging of clusters is not possible because nodes of the cluster is not in network.

System action:
The operation to merge clusters fails.

Administrator response:
Check connectivity of all master servers and retry the operation.

CTGKM3484E SKLM Backup operation failed before merging data during dual cluster merge.

Explanation:
Merging of clusters is not possible because mandatory backup operation failed before data merge between dual clusters.

System action:
The operation to merge clusters fails.

Administrator response:
Check logs for more detailed information.

CTGKM3485E Cluster status updation for master *VALUE_0* failed.

Explanation:
Updating Cluster status in Primary DB for the given master failed.

System action:
NA

Administrator response:
Check parameters and try again.

CTGKM3488E Unable to get HADR status

Explanation:
Unable to get HADR status at this moment.

System action:
NA

Administrator response:
Check SKLM logs for more information

CTGKM3489E File *VALUE_0* is empty. Empty file upload is not allowed.

Explanation:
User is trying to upload zero bytes file.

System action:
Not to upload any part of the file.

Administrator response:
Ensure that file size is in permissible range.

CTGKM3490E Failed to update the communication certificates because the new certificate file is invalid.

Explanation:
The communication certificate file is corrupt or invalid. Valid certificate file formats are .cer, .der, .crt.

System action:
The certificate update operation fails.

Administrator response:
Specify a valid communication certificate file, and retry the operation.

CTGKM3493E Auto takeover failed on standby master server *VALUE_0* . Auto takeover will be attempted on the next available standby master server.

Explanation:

System action:

Administrator response:

CTGKM3494E Failed to update the device communication certificate because it is not trusted by the IBM Security Guardium Key Lifecycle Manager server.

Explanation:
The device communication certificate to be updated must be valid, CA signed, and trusted in the IBM Security Guardium Key Lifecycle Manager server.

System action:
The certificate update operation fails.

Administrator response:
Use a certificate that is trusted in the IBM Security Guardium Key Lifecycle Manager server, and retry the operation.

CTGKM3495E Failed to update the device communication certificates. Check logs for more information.

Explanation:
Failed to update the device communication certificates because of an internal error. Check logs for more information.

System action:
The certificate update operation fails.

Administrator response:

CTGKM3496E Unable to accept the pending client device communication certificate: *VALUE_0* . A client with

the same name already exists. Specify a different certificate name and try again.

Explanation:
Accepting pending client device certificate failed. A client of same name already exists.

System action:
Specify a different certificate name and try again.

Administrator response:
No Action

CTGKM3497E Failed to complete the KMIP request. The communication certificate has the registered WWNN value but is not trusted by the server. Use a trusted certificate and retry the operation.

Explanation:
The WWNN value of the client communication certificate in the KMIP request is registered with the device group but the certificate is not trusted in the IBM Security Guardium Key Lifecycle Manager server.

System action:
The KMIP operation fails.

Administrator response:
Use a trusted client communication certificate, and retry the operation.

CTGKM3498E Re configuration of Multi Master post restore is not allowed from Non Primary master of the Multi-Master Cluster.

Explanation:
This operation is not allowed from Non primary master .

System action:
The re configuration of Multi Master after restore operation fails.

Administrator response:
Perform operation on primary.

CTGKM3499E Re configuration of Multi Master post restore is Failed.

Explanation:
Re configuration of Multi Master post restore is Failed. Check logs for more information.

System action:
The re configuration of Multi Master after backup restore operation fails.

Administrator response:
Check logs for more information.

CTGKM3501E Cannot change the user password because IBM Security Guardium Key Lifecycle Manager is integrated with a non-file based repository.

Explanation:
The user password can be updated only when IBM Security Guardium Key Lifecycle Manager is integrated with file-based repository.

System action:
The operation to update password fails.

Administrator response:
None

CTGKM3502E Requested operation not supported on this System. Please provide HEALTH_AUTHORIZATION_TOKEN while running container.

Explanation:
The operation you are trying to execute is not configured on this System. This could be because HealthAuthorizationStr is not set while docker run.

System action:
Health status fails.

Administrator response:
Check if the system is configured for HealthAuthorizationStr.

CTGKM3503E Authentication Failure: Incorrect header property Health-Authorization.

Explanation:
Incorrect Health-Authorization specified.

System action:
Health service authorization fails.

Administrator response:
Specify correct Health-Authorization.

CTGKM3504E Cannot change the user password because the values given for the current or new password is incorrect. Specify the correct current password and ensure that the new password complies with the password policy.

Explanation:
The user password cannot be updated because the specified current password is incorrect, or the new password does not comply with the password policy.

System action:
The operation to update password fails.

Administrator response:
Specify the correct current password and ensure that the new password complies with the password policy.

CTGKM3505E The values for newUserPasword and confirmNewUserPassword do not match.

Explanation:
The user password cannot be updated because the values for newUserPasword and confirmNewUserPassword do not match.

System action:
The operation to update password fails.

Administrator response:
The values for newUserPasword and confirmNewUserPassword do not match. Specify the correct values and try again.

CTGKM3506E Cannot find the file *VALUE_0* . Make sure the path exist and it is not a directory.

Explanation:
The key file was not found.

System action:

Administrator response:

CTGKM3507E Request failed because the volume serial (volser) number for the device is missing. Volser Affinity for this device group is enabled

Explanation:
Request failed because the volume serial (volser) number for the device is missing. The device.enableVolserAffinity attribute for this device group is set to 'true'. Hence, the request must include the volume serial number.

System action:

Administrator response:

CTGKM3508E Failed to receive master key.

Explanation:

System action:

Administrator response:

CTGKM3512E Agent failed to start on this server.

Explanation:

System action:

Administrator response:

CTGKM3513E The agent certificate with alias *VALUE_0* has expired.

Explanation:

System action:

Administrator response:

CTGKM3515E Failed to import the agent keystore *VALUE_0* .

Explanation:

System action:

Administrator response:

CTGKM3518E Data synchronization run failed. Error in backing up data.

Explanation:

System action:

Administrator response:

CTGKM3519E Failed to copy *VALUE_0* on master server *VALUE_1* .

Explanation:

System action:

Administrator response:

CTGKM3521E Connection to agent on server *VALUE_0* failed with exception *VALUE_1* .

Explanation:

System action:

Administrator response:

CTGKM3529E Certificate expired. Expired certificate cannot be imported

Explanation:
Certificate expired. An expired certificate cannot be used imported in IBM Security Guardium Key Lifecycle Manager server.

System action:
Update operation fails.

Administrator response:
Specify a valid certificate alias and try the operation again.

CTGKM3530E This Operation is only supported on Multi master cluster.

Explanation:
This Operation is only supported on Multi master cluster.

System action:
This operation is not supported on this server.

Administrator response:
This operation ahould be tried only on Multi master cluster.

CTGKM3531E Values of the Db2 kernel parameters on this server do not meet the minimum requirements.

Explanation:
Db2 kernel parameters must meet the minimum requirements to configure a Multi-Master cluster. The appropriate values are available in the product documentation in the IBM Knowledge Center.

System action:
The Add master operation fails.

Administrator response:
Set the appropriate values for the kernel parameters on the primary master server and on the server to be added, and then configure the Multi-Master cluster. For information about the parameter values, see the product documentation in the IBM Knowledge Center.

CTGKM3532E Values of the Db2 kernel parameters on server *VALUE_0* do not meet the minimum requirements.

Explanation:
Db2 kernel parameters must meet the minimum requirements to configure a Multi-Master cluster. The appropriate values are available in the product documentation in the IBM Knowledge Center.

System action:
The Add master operation fails.

Administrator response:
Set the appropriate values for the kernel parameters on the primary master server and on the server to be added, and then configure the Multi-Master cluster. For information about the parameter values, see the product documentation in the IBM Knowledge Center.

CTGKM3535E Client Group with *VALUE_0* name not found. Specify the correct name and try again.

Explanation:
Client Group with VALUE_0 name does not exist.

System action:
The operation to obtain group details fails.

Administrator response:
Specify a valid and correct group name and retry the operation.

CTGKM3537E Error deleting client group with name *VALUE_0* .

Explanation:
Error occurred while deleting Group with VALUE_0 name.

System action:
The operation to delete group fails.

Administrator response:
Retry the operation.

CTGKM3538E Error while setting FIPS.

Explanation:
Error occured while setting FIPS.

System action:
The operation to set FIPS failed.

Administrator response:
Retry the operation.

CTGKM3539E Error while setting Security Configuration for *VALUE_0* parameter.

Explanation:
Error occured while setting Security Configuration for VALUE_0 parameter.

System action:
The operation to set VALUE_0 failed.

Administrator response:
Retry the operation.

CTGKM3540E Suite B should have either 128 or 192 or off as their values.

Explanation:
Suite B should have either 128 or 192 or off as their values.

System action:
The operation to set Suite B failed.

Administrator response:
Retry the operation with correct values.

CTGKM3541E securityLevel should have either HIGH or MEDIUM or WEAK or CUSTOM or off as their values.

Explanation:
securityLevel should have either HIGH or MEDIUM or WEAK or CUSTOM or off as their values.

System action:
The operation to set securityLevel failed.

Administrator response:
Retry the operation with correct values.

CTGKM3542E Unable to create the client group *VALUE_0* because a client group or a client with the same name already exists.

Explanation:
Failed to create client group with name VALUE_0 because a client group or a client with the same name already exists.

System action:
The create group operation fails.

Administrator response:
Specify a unique name for the client group, and retry the operation.

CTGKM3543E Error while getting Security Configuration.

Explanation:
Error occured while getting Security Configuration.

System action:
The operation failed.

Administrator response:
Retry the operation.

CTGKM3544E The following Cipher Suites *VALUE_0* are invalid.

Explanation:
Error occured while setting Cipher Suites.

System action:
The operation failed.

Administrator response:
Retry the operation.

CTGKM3546E Security Configurations with parameter value ALL, FIPS, Suite_B, SP800_131A, securityLevel and enabledCiphers are only allowed.

Explanation:
Security Configurations with parameter value ALL, FIPS, Suite_B, SP800_131A, securityLevel and enabledCiphers are only allowed.

System action:
The operation failed.

Administrator response:
Retry the operation with correct parameters.

CTGKM3551E Incorrect value for client group name *VALUE_0*

Explanation:
The client group name must follow the requirement: 1. Can only contain alphanumeric characters and underscore. 2. First character cannot be a digit. 3. Maximum length is 256.

System action:
The operation fails.

Administrator response:
The client group name must follow the requirement: 1. Name can only contain alphanumeric character and underscore 2. First character cannot be a digit. 3. Maximum length should be 256.

CTGKM3552E Unable to read the complete configuration file after trying 5 times.

Explanation:
Tried reading the configuration file 5 times but the items of the configuration file are less than 5 after 5 trials.

System action:
The operation fails.

Administrator response:
Retry the operation.

CTGKM3553E *VALUE_0* user is not part of any Client to perform this operation.

Explanation:
VALUE_0 user is not part of any Client to perform this operation

System action:
The REST based key serving operation fails.

Administrator response:
Make this user part of the Client and retry the operation.

CTGKM4000E The configuration property pkcs11.pin.obfuscated can not be updated.

Explanation:
The configuration property pkcs11.pin.obfuscated is set by the product and can not be updated by a user.

System action:
Update operation fails.

Administrator response:
Specify a configuration paramter that can be updated and try again.

CTGKM4001E Specified PKCS 11 configuration path or filename does not exist.

Explanation:
The path and/or file name specified does not exist.

System action:
Update operation fails.

Administrator response:
Specify a valid path and file name for the PKCS 11 configuration file.

CTGKM5001E *VALUE_0* association already exists.

Explanation:
Incorrect user managment association. Association already exists.

System action:
The operation fails.

Administrator response:
Change the association parameters and try the operation again.

CTGKM5002E ***VALUE_0* association doesn't exists.**

Explanation:
Incorrect user managment association. Association doesn't exists.

System action:
The operation fails.

Administrator response:
Change the association parameters and try the operation again.

CTGKM5003E **Default association *VALUE_0* cannot be deleted.**

Explanation:
Default association cannot be deleted.

System action:
The operation fails.

Administrator response:
Change the association parameters and try the operation again.

CTGKM5004E **Object with the same name {0} already exists.**

Explanation:

System action:
The operation fails.

Administrator response:
Specify a different name and try the operation again.

CTGKM5005E **Default object *VALUE_0* cannot be deleted.**

Explanation:
Default object cannot be deleted.

System action:
The operation fails.

Administrator response:
Change the parameters and try the operation again.

CTGKM5006E **Name *VALUE_0* must be alphanumeric maximum 256 characters length.**

Explanation:
Name must be alphanumeric or contain underscore character with maximum 256 characters length.

System action:
The operation fails.

Administrator response:
Change the parameters and try the operation again.

CTGKM5007E **Device Type corresponding to the role with name *VALUE_0* cannot be found.**

Explanation:
The role name that you specified does not match an existing Device Type.

System action:
The operation fails.

Administrator response:
Specify role name that corresponds to an existing Device Type.

CTGKM5008E **User name *VALUE_0* does not exist.**

Explanation:
User name does not exist. Please provide the existing username.

System action:
The operation fails.

Administrator response:
Specify username name that exists.

CTGKM5009E **No change found to be updated.**

Explanation:
No change found to be updated.

System action:
The operation fails.

Administrator response:
update the parameters to change.

CTGKM5010E ***VALUE_0* is a default role or group and cannot be modified.**

Explanation:
Default object cannot be modified.

System action:
The operation fails.

Administrator response:
Change the parameters and try the operation again.

CTGKM6002E **Bad Request: Invalid user authentication ID or invalid request format.**

Explanation:
An incorrect request format or user ID was used for authentication.

System action:
Request fails.

Administrator response:
Specify a correct request format and a valid user ID.

CTGKM6003E **Authentication failed. The specified user ID or password is incorrect, or your account is locked out. Specify the correct user ID and password, or wait for**

some time for the account to be unlocked, and try again.

Explanation:
The specified user ID or password is incorrect, or the account is locked causing authentication failure.

System action:
Login fails.

Administrator response:
Specify the correct user ID or password, or wait for some time for the account to be unlocked.

CTGKM6004E User is not authenticated or has already logged out.

Explanation:
User is not authenticated or has already logged out.

System action:
Login fails.

Administrator response:
Specify correct user id or password.

CTGKM6027E key group entry must specify either entry uuid, or alias.

Explanation:
Either uuid or alias should be provided for key group entry.

System action:
Key group entry add fails.

Administrator response:
Specify either uuid or alias.

CTGKM6051E Can not remove authentication method. Must set atleast one authentication configuration.

Explanation:
Set other authentication configuration before removing any.

System action:
The operation fails.

Administrator response:
Set other authentication configuration and retry the operation.

CTGKM6052E Cannot update port number. Specify an integer value between 1 and 65535.

Explanation:
Specify an integer value between 1 and 65535 as the port number.

System action:
The operation to update the port number fails.

Administrator response:
Specify an integer value between 1 and 65535 and retry the operation.

CTGKM6053E Cannot update the configuration because *VALUE_0* has an invalid value.

Explanation:
The configuration properties cannot be updated because the specified values are invalid.

System action:
The operation to update the configuration fails.

Administrator response:
Ensure that the properties in the REST API contain valid values, and run the REST API again.

CTGKM6054E Cannot update the configuration because *VALUE_0* has an invalid value. Possible values are : *VALUE_1* .

Explanation:
The configuration properties cannot be updated because the specified values are invalid.

System action:
The operation to update the configuration fails.

Administrator response:
Ensure that the properties in the REST API contain valid values, and run the REST API again.

CTGKM6055E Cannot update the configuration parameters because the required parameter License=accept is missing.

Explanation:
The configuration properties cannot be updated because terms in the License Agreements are not accepted.

System action:
The operation to update the configuration parameters fails.

Administrator response:
Set the License parameter to accept and retry the operation.

CTGKM6057E License activation failed.

Explanation:
License activation failed.

System action:
License activation operation fails.

Administrator response:
Upload a valid License file and retry the operation.

CTGKM6058E License is not activated.

Explanation:
License is not activated.

System action:
User operation fails.

Administrator response:
Upload a valid License file and retry the operation.

CTGKM6059E Incorrect value for user name. \nThe user name Can only contain alphanumeric characters, period and underscores.

Explanation:
The user name Can only contain alphanumeric characters, period and underscores.

System action:
The operation fails.

Administrator response:
Update username and retry the operation.

CTGKM6060E Previous run not completed. Must use the same master key size - *KEY_SIZE*

Explanation:
Processing failed when creating new master key for encryption. A previous run of this process was not completed. Must use the same master key size

System action:
The operation fails.

Administrator response:
Retry the operation

CTGKM6061E Unable to read/initialize status: *ERROR_MESSAGE*

Explanation:
Processing failed when creating new master key for encryption. Unable to read/initialize status

System action:
The operation fails.

Administrator response:
Retry the operation

CTGKM6062E Unable to create Master Key: MasterKey = null

Explanation:
Processing failed when creating new master key for encryption. Unable to create Master Key: MasterKey = null

System action:
The operation fails.

Administrator response:
Retry the operation

CTGKM6063E Error creating Master Key: *ERROR_MESSAGE*

Explanation:
Processing failed when creating new master key for encryption. Error creating Master Key

System action:
The operation fails.

Administrator response:
Retry the operation

CTGKM6064E Error when encrypting key DB Table data with new MasterKey: *ERROR_MESSAGE*

Explanation:
Processing failed when creating new master key for encryption. Error when encrypting key DB Table data with new MasterKey

System action:
The operation fails.

Administrator response:
Retry the operation

CTGKM6065E Error when encrypting certificate DB Table data with new MasterKey: *ERROR_MESSAGE*

Explanation:
Processing failed when creating new master key for encryption. Error when encrypting certificate DB Table data with new MasterKey

System action:
The operation fails.

Administrator response:
Retry the operation

CTGKM6066E Error when encrypting SecretData DB Table data with new MasterKey: *ERROR_MESSAGE*

Explanation:
Processing failed when creating new master key for encryption. Error when encrypting SecretData DB Table data with new MasterKey

System action:
The operation fails.

Administrator response:
Retry the operation

CTGKM6067E Error when updating MasterKey size configuration: *ERROR_MESSAGE*

Explanation:
Processing failed when creating new master key for encryption. Error when updating MasterKey size configuration

System action:
The operation fails.

Administrator response:

Retry the operation

CTGKM6068E Error when updating SKLM KeyStore with the new MasterKey: *ERROR_MESSAGE*

Explanation:
Processing failed when creating new master key for encryption. Error when updating SKLM KeyStore with the new MasterKey

System action:
The operation fails.

Administrator response:
Retry the operation

CTGKM6202E Can not remove authentication method. Set IBM Security Guardium Key Lifecycle Manager Administrator user in LDAP authentication method.

Explanation:
Set IBM Security Guardium Key Lifecycle Manager Administrator user in LDAP authentication method.

System action:
The operation fails.

Administrator response:
Set IBM Security Guardium Key Lifecycle Manager Administrator user in LDAP authentication method and retry the operation.

CTGKM7000E Either both Audit.syslog.server.host and Audit.syslog.server.port configuration parameters must be provided, or neither. When provided the value of Audit.isSyslog configuration parameter should be true.

Explanation:
Either both Audit.syslog.server.host and Audit.syslog.server.port configuration parameters must be provided, or neither. When provided the value of Audit.isSyslog configuration parameter should be true.

System action:
Login fails.

Administrator response:
Either both Audit.syslog.server.host and Audit.syslog.server.port configuration parameters must be provided, or neither. When provided the value of Audit.isSyslog configuration parameter should be true.

CTGKM7001E Value for configuration parameter Audit.syslog.server.port is not valid. A valid value is an integer between 1 and 65535.

Explanation:
Value for configuration parameter Audit.syslog.server.port is not valid. A valid value is an integer between 1 and 65535.

System action:
The operation fails.

Administrator response:
Specify an integer between 1 and 65535 as the input value.

CTGKM7002E Value for configuration parameter Audit.syslog.server.host is not valid. It should not be greater than 255 characters.

Explanation:
Value for configuration parameter Audit.syslog.server.host is not valid. It should not be greater than 255 characters.

System action:
The operation fails.

Administrator response:
Specify a valid value for host as the input value.

CTGKM7003E Value for configuration parameter Audit.isSyslog is not valid. The value must be either true or false.

Explanation:
Value for configuration parameter Audit.isSyslog is not valid. The value must be either true or false.

System action:
The operation fails.

Administrator response:
Specify either true or false as the input value.

CTGKM7004E Unable to connect to Server to log Audit events.

Explanation:
Unable to connect to Server to log Audit events.

System action:
The operation fails.

Administrator response:
Please check values of configuration parameters and check whether the server is running on the specific port.

CTGKM7005E Value for configuration parameter Audit.syslog.isSSL is not valid. The value must be either true or false.

Explanation:
Value for configuration parameter Audit.syslog.isSSL is not valid. The value must be either true or false.

System action:
The operation fails.

Administrator response:
Specify either true or false as the input value.

CTGKM8001E Failed to register client: *VALUE_0*

Explanation:
The client specified is already present in the Database

System action:
The client operation fails.

Administrator response:
Ensure that the client is not present in the Database. Then, try the operation again.

CTGKO0000E Password policy authority error occurred: *VALUE_0*

Explanation:
Unspecified general error occurred.

System action:
Cannot process the password policy authority request.

Administrator response:
Contact your administrator.

CTGKO0002E Cannot retrieve password policy from data store - *VALUE_0*. Cause: *VALUE_1*

Explanation:
Password policy could not be retrieved.

System action:
Cannot process the password policy authority request.

Administrator response:
Contact an administrator who has read and write access to the TKLMPasswordPolicy.xml file. This is usually the Tivoli® Integrated Portal administrator (TIPAdmin) or Guardium Key Lifecycle Manager administrator (SKLMAdmin). Only the TIPAdmin user can add or modify user profiles and test the password policy.

CTGKO0003E Cannot read the retrieved password policy - *VALUE_0*. Cause: *VALUE_1*

Explanation:
Cannot parse the password policy definition. The data might be corrupt.

System action:
Cannot process the password policy authority request.

Administrator response:
Contact an administrator who has read and write access to the TKLMPasswordPolicy.xml file. This is usually the Tivoli Integrated Portal administrator (TIPAdmin) or Guardium Key Lifecycle Manager administrator (SKLMAdmin). Only the TIPAdmin user can add or modify user profiles and test the password policy.

CTGKO0004E Cannot remove password policy from data store - *VALUE_0*. Cause: *VALUE_1*

Explanation:
The password policy is not removed from the data store.

System action:
Cannot process the password policy authority request.

Administrator response:
Contact an administrator who has read and write access to the TKLMPasswordPolicy.xml file. This is usually the Tivoli Integrated Portal administrator (TIPAdmin) or Guardium Key Lifecycle Manager administrator (SKLMAdmin). Only the TIPAdmin user can add or modify user profiles and test the password policy.

CTGKO0005E Cannot determine password policy location - *VALUE_0*. Cause: *VALUE_1*

Explanation:
Password policy location can not be determined. Check your product configuration

System action:
Cannot process the password policy authority request.

Administrator response:
Contact an administrator who has read and write access to the TKLMPasswordPolicy.xml file. This is usually the Tivoli Integrated Portal administrator (TIPAdmin) or Guardium Key Lifecycle Manager administrator (SKLMAdmin). Only the TIPAdmin user can add or modify user profiles and test the password policy.

CTGKO0100E Password policy violation was detected. Password is too long. Maximum length is *VALUE_0*.

Explanation:
The password length cannot exceed the value set in the password policy.

System action:
No password is set. A new user profile is not created.

Administrator response:
Submit a password not greater than the maximum allowed length. Retry the request or contact your administrator.

CTGKO0101E Password policy violation was detected. Password is too short. Minimum length is *VALUE_0*.

Explanation:

The password length cannot be less than the value set in the password policy.

System action:
No password is set. A new user profile is not created.

Administrator response:
Submit a password that has a valid minimum length. Retry the request or contact your administrator.

CTGKO0102E Password policy violation was detected. Password does not contain a required character. One of the following characters is required: *VALUE_0*.

Explanation:
The password must contain a required character specified in the password policy.

System action:
No password is set. A new user profile is not created.

Administrator response:
Submit a password containing one of the required characters. Retry the request or contact your administrator.

CTGKO0103E Password policy violation was detected. Password contains an incorrect character. Any of the following characters may not be used: *VALUE_0*.

Explanation:
The password cannot contain characters that password policy specifies should not be used.

System action:
No password is set. A new user profile is not created.

Administrator response:
Submit a password without incorrect characters. Retry the request or contact your administrator.

CTGKO0104E Password policy violation was detected. Password contains too many consecutive occurrences of the same character. Maximum number of occurrences is: *VALUE_0*.

Explanation:
The password cannot contain more than the maximum consecutive occurrences of the same character.

System action:
No password is set. A new user profile is not created.

Administrator response:
Submit a password that does not exceed the maximum consecutive occurrences of the same character. Retry the request or contact your administrator.

CTGKO0105E Password policy violation was detected. Password does not contain the minimum required number of numeric characters. Minimum number of numeric characters is: *VALUE_0*.

Explanation:
The password must contain a minimum number of numeric characters.

System action:
No password is set. A new user profile is not created.

Administrator response:
Submit a password containing at least the required minimum number of numeric characters. Retry the request or contact your administrator.

CTGKO0106E Password policy violation was detected. Password does not contain the minimum required number of alphabetic characters. Minimum number of alphabetic characters is: *VALUE_0*.

Explanation:
The password must contain a minimum number of alphabetic characters.

System action:
No password is set. A new user profile is not created.

Administrator response:
Submit a password containing at least the required minimum number of alphabetic characters. Retry the request or contact your administrator.

CTGKO0107E Password policy violation was detected. Password does not contain the minimum required number of unique characters. Minimum number of unique characters is: *VALUE_0*.

Explanation:
The password must contain a minimum number of unique characters.

System action:
No password is set. A new user profile is not created.

Administrator response:
Submit a password containing at least the minimum number of unique characters specified by the password policy. Retry the request or contact your administrator.

CTGKO0108E Password policy violation was detected. Password contains the user ID.

Explanation:
Password policy violation was detected.

System action:
No password is set. A new user profile is not created.

Administrator response:
Submit a password that does not contain the user ID. Retry the request or contact your administrator.

CTGKO0109E Password policy violation was detected. Password contains user name.

Explanation:
A password cannot contain any part of the user name.

System action:
No password is set. A new user profile is not created.

Administrator response:
Submit a password that does not contain any part of the user name. Retry the request or contact your administrator.

CTGKP5001E Unable to decode attribute value.

Explanation:
Cannot process a message. There is an error on the input received in the message.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP5002E Index may not be specified in Add Attribute operation.

Explanation:
Cannot process a message. There is an error on the input received in the message.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP5003E Service returned no KMIPCryptographicObject.

Explanation:
Internal error. After processing the message, KMIP service did not return KMIPCryptographicObject.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP5004E Unique Identifier mismatch : query does not match response.

Explanation:
Internal error. After processing the message, Unique Identifier in the query and response do not match.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP5005E Single valued attribute *VALUE_0* is already present.

Explanation:
Cannot process the message. Received multiple values for a single valued attribute. Expected only one value.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP5006E A non-zero index passed for a single valued attribute *VALUE_0*.

Explanation:
Cannot process the message. Index for the single valued attribute must to be zero.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP5007E A non-typed Digest appeared as an attribute.

Explanation:
Cannot process the message. There is an error on the input received in the message.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP5008E A non-string value appeared in a custom attribute.

Explanation:
Cannot process the message, incorrect value for custom attribute received. All custom attributes must be of type TEXT_STRING.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP5009E Unknown attribute name *VALUE_0*.

Explanation:
Cannot process the message, unrecognized attribute name.

System action:
The requested operation fails.

Administrator response:

Correct the input and retry the operation.

CTGKP5010E A non-typed Name appeared as an attribute.

Explanation:
Cannot process the message, unrecognized type for Name attribute.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP5012E Cannot obtain Guardium Key Lifecycle Manager keystore password.

Explanation:
Cannot process a message, internal error occurred.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP5013E Trustmanagers or keymanagers cannot be initialized.

Explanation:
Internal error occurred, could not complete initialization for KMIP TLS Listener. Make sure KMIP is configured correctly for TLS.

System action:
Guardium Key Lifecycle Manager is not ready to accept KMIP requests from a client.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP5014E KMIP TLS Listener did not come up.

Explanation:
Error occurred getting KMIP TLS Listener up. Guardium Key Lifecycle Manager is not ready to accept KMIP requests from a client.

System action:
Cannot accept KMIP messages.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP5015E The *VALUE_0* attribute requires a non-null value.

Explanation:
The attribute can not contain a null value.

System action:
Will not process the message.

Administrator response:
Correct the input and retry the message.

CTGKS0001E Keystore password for *VALUE_0* is null.

Explanation:
The keystore is not found in the IBM Security Guardium Key Lifecycle Manager database. The configuration file might not be synchronized with the database.

System action:
The keystore is not found.

Administrator response:
In the graphical user interface, access the Keystore configuration page. Determine whether the value on the page is the same as the value of the keystore name specified for the config.keystore.name property in the SKLMConfig.properties file. If the values are different, manually change the value of the property to match the value of the name in the graphical user interface, and restart the IBM Security Guardium Key Lifecycle Manager server. Then, try the operation again.

CTGKS0001W Could not determine key encoding to obtain key size to validate.

Explanation:
Some of the keys in a default key group cannot be validated. These cannot be used for LTO drives. However, the key group may still be valid.

System action:
Ensure that the default key group is valid and that LTO drives can be supported.

Administrator response:
Ensure that the default key group is valid and that LTO drives can be supported.

CTGKS0002E TCP Listener failed to come up.

Explanation:
Only one process can use the TCP port that the TCP Transport Listener requires to run. Another process has the port. Alternatively, the socket timed out.

System action:
The TCP Transport Listener is not available to the IBM Security Guardium Key Lifecycle Manager server.

Administrator response:
Ensure that no other program is using the TCP port. If the other process must have the port, specify a new TCP port number. Then, restart the IBM Security Guardium Key Lifecycle Manager server. If the problem continues, examine the audit log. After making corrections, restart the IBM Security Guardium Key Lifecycle Manager server. You might need to contact IBM Support.

CTGKS0003E TLS Listener failed to come up.

Explanation:
Only one process can use the TLS port that the TLS Transport Listener requires to run. Another process has the port.

System action:
The TLS Transport Listener is not available to the IBM Security Guardium Key Lifecycle Manager server.

Administrator response:
Ensure that no other program is using the TLS port. If the other process must have the port, specify a new Transport Listener TLS port number. Then, restart the IBM Security Guardium Key Lifecycle Manager server. If the problem continues, you might need to contact IBM Support.

CTGKS0004E Cannot obtain an instance of SecurityEventHandler.

Explanation:
In the SKLMConfig.properties file, the value for the Audit.handler.class property for a distributed system must be com.ibm.tklm.common.audit.file.SimpleFileSecurityEventHandler.

System action:
The operation fails.

Administrator response:
Determine whether the Audit.handler.class property specifies the correct default value, which should not be changed from the default value. Then, try the operation again.

CTGKS0005E TLS keymanagers failed to load.

Explanation:
Ensure that the specified TLS certificate actually exists in the keystore. Alternatively, the TLS certificate might be in an expired state.

System action:
The operation fails.

Administrator response:
Specify a valid TLS certificate that is not expired. Then, try the operation again.

CTGKS0006E Problem starting key server.

Explanation:
The key server internal component that is provided by the IBM Security Guardium Key Lifecycle Manager server did not start.

System action:
The internal component does not start.

Administrator response:
First, examine the audit log for exception information about the key server. You might need to contact IBM Support.

CTGKS0007E Error in property value for:

Explanation:
The value that is currently specified is not valid for the property.

System action:
The operation fails.

Administrator response:
Refer to documentation for the property. The value of the property is specified in the SKLMConfig.properties file. Specify a different value. Then, try the operation again. Changing some properties requires that you restart the IBM Security Guardium Key Lifecycle Manager server.

CTGKS0008E debug not initialized.

Explanation:
The files that are specified for debug output might be specified as read-only.

System action:
Initialization fails.

Administrator response:
Specify that the debug output files are writable. Then, try the operation again.

CTGKS0009E TKLMKeyManager not initialized.

Explanation:
The class TKLMKeyManager failed to initialize. The TLS port is not functional.

System action:
Keys and certificates are not available for key serving.

Administrator response:
Ensure that the TLS certificate is correctly configured in the config.keystore.ssl.certalias property. You might also examine the audit log for more information. Make any necessary corrections. Then, try the operation again.

CTGKS0010E TCP Listener went down.

Explanation:
Only one process can use the TCP port that the TCP Transport Listener requires to run. Another process has the port. Alternatively, the socket timed out.

System action:
The TCP Transport Listener is not available to the IBM Security Guardium Key Lifecycle Manager server.

Administrator response:
Ensure that no other program is using the TCP port. If the other process must have the port, specify a new TCP port number. Then, restart the IBM Security Guardium Key Lifecycle Manager server. If the problem

continues, examine the audit log. If no audit exception information is helpful, you might need to contact IBM Support.

CTGKS0011E TLS Listener went down.

Explanation:
The TLS Listener that IBM Security Guardium Key Lifecycle Manager server provides has failed, possibly because the TLS socket timed out, or because a port conflict occurred.

System action:
The operation fails.

Administrator response:
To restart the TLS Listener, you must restart the IBM Security Guardium Key Lifecycle Manager server. You might need to change the value of the port or the timeout interval. Then, try the operation again. If the TLS socket continues to time out again, or a port conflict continues, you might need to contact IBM Support.

CTGKS0012E The keystore name is null.

Explanation:
The key server component cannot locate the IBM Security Guardium Key Lifecycle Manager keystore.

System action:
IBM Security Guardium Key Lifecycle Manager cannot serve the keys.

Administrator response:
Ensure that the IBM Security Guardium Key Lifecycle Manager keystore is specified, and that the keystore exists. You might run the tklmKeyStoreList command to list the IBM Security Guardium Key Lifecycle Manager keystore, or examine the value of the config.keystore.name property in the SKLMConfig.properties file. If necessary, use the tklmKeyStoreAdd command to add a keystore. Then, try the operation again.

CTGKS0013E The keystore unique identifier is null.

Explanation:
No value was provided for the keystore Universal Unique Identifier (storeUuid).

System action:
IBM Security Guardium Key Lifecycle Manager cannot serve the keys.

Administrator response:
If you are running the tklmKeyStoreList command, you might alternatively specify the value of the keystore name. If you do not specify a value for either a keystore name or the Universal Unique Identifier, the command lists all keystores.

CTGKS0014E The drive serial number is null.

Explanation:
No value was provided for the device serial number.

System action:
No device is found.

Administrator response:
Specify a value for a valid device serial number that is 12 characters in length. Then, try the operation again.

CTGKS0015E The device with the device serial number *VALUE_0* does not exist in the database.

Explanation:
An incorrect value was provided for a device serial number.

System action:
The create operation fails.

Administrator response:
Ensure that you specified the correct device serial number. You might use the tklmDeviceList command to list the devices in the IBM Security Guardium Key Lifecycle Manager database. Then, try the operation again.

CTGKS0016E No attributes were specified for the device update operation.

Explanation:
No attribute-value pairs were specified to update information for a device.

System action:
IBM Security Guardium Key Lifecycle Manager cannot serve the keys.

Administrator response:
Collect available audit log information and contact IBM Support.

CTGKS0017E A certificate encoding exception occurred when converting the certificate to binary form. The device metadata could not be created for the device with the device serial number *VALUE_0* .

Explanation:
An internal error occurred.

System action:
The create device metadata operation fails.

Administrator response:
Collect available audit log information and contact IBM Support.

CTGKS0018E A certificate encoding exception occurred when converting the certificate to binary form. The device metadata could not be

updated for the device with the device serial number *VALUE_0* .

Explanation:
An internal error occurred.

System action:
The update device metadata operation fails.

Administrator response:
Collect available audit log information and contact IBM Support.

CTGKS0019E **The device with the device serial number *VALUE_0* does not exist in the database.**

Explanation:
An incorrect value was provided for a device serial number.

System action:
The delete operation fails.

Administrator response:
Ensure that you specified the correct device serial number. You might use the tklmDeviceList command to list the devices in the database. Then, try the operation again.

CTGKS0021E **The key server has no keystore defined. Keys cannot be served to devices.**

Explanation:
The key server component cannot locate the IBM Security Guardium Key Lifecycle Manager keystore.

System action:
Keys cannot be served to devices.

Administrator response:
Ensure that the IBM Security Guardium Key Lifecycle Manager keystore is specified, and that the keystore exists. You might run the tklmKeyStoreList command to list the IBM Security Guardium Key Lifecycle Manager keystore, or examine the value of the config.keystore.name property in the SKLMConfig.properties file. If necessary, use the tklmKeyStoreAdd command to add a keystore. Then, try the operation again.

CTGKS0022E **KeyGroup specified in symmetricKeySet alias is not valid. Either this key group does not exist or it does not have valid active symmetric keys.**

Explanation:
The key group does not exist or it does not have valid, active symmetric keys.

System action:
No keys are served from the key group.

Administrator response:
Ensure that the value is valid for the key group specified by the symmetricKeySet property in the SKLMConfig.properties file. Additionally, ensure that the keys are valid and active, and that they are in the keystore that is specified by the config.keystore.name property. Then, try the operation again.

CTGKS0023E **Keys will not be served to LTO devices.**

Explanation:
No value is set for the symmetricKeyset property in the SKLMConfig.properties file.

System action:
No keys are served to LTO Ultrium 4 tape drives.

Administrator response:
Specify a valid value for the symmetricKeySet property in the SKLMConfig.properties file. Then, try the operation again.

CTGKS0024E **symmetricKeyset must contain valid string with valid key alias. Valid symmetric key aliases are <= 12 characters or exactly 21 characters.**

Explanation:
Valid symmetric key aliases are less than or equal to 12 characters, or exactly 21 characters.

System action:
No keys are served to LTO Ultrium 4 tape drives.

Administrator response:
Specify valid values for the keyAliasList parameter of the symmetricKeyset property in the SKLMConfig.properties file. If this is a manual change, you must restart the IBM Security Guardium Key Lifecycle Manager server. Then, try the operation again.

CTGKS0025E **Error in symmetricKeySet alias range: Make sure the second number in the range is larger than the first.**

Explanation:
The second number in the alias range must be larger than the first number.

System action:
No keys are served to LTO tape drives.

Administrator response:
Specify a valid range for the keyAliasList parameter of the symmetricKeyset property in the SKLMConfig.properties file. If this is a manual change, you must restart the IBM Security Guardium Key Lifecycle Manager server. Then, try the operation again.

CTGKS0026E Error in symmetricKeySet aliases or key algorithm.

Explanation:
The symmetricKeySet property does not have a valid key specification.

System action:
No keys are served.

Administrator response:
Ensure that the symmetricKeySet parameter points to valid keys. If the zOSCompatibility flag is set on, then the valid algorithm for symmetric keys is DESede. Otherwise the valid algorithm is AES.

CTGKS0027E No valid DKI Aliases specified.Add AES or DESede symmetric keys to symmetricKeySet to support LTO drives.

Explanation:
A data key identifier alias is used only for an LTO tape drive. No valid keys of the necessary type are specified in the symmetricKeyset property in the SKLMConfig.properties file.

System action:
No keys are served to LTO tape drives.

Administrator response:
Add a valid range of AES or DESede symmetric keys to the symmetricKeySet property. Restart the IBM Security Guardium Key Lifecycle Manager server. Then, try the operation again.

CTGKS0028E Alias *VALUE_0* was not found in the keystore.

Explanation:
The alias pointed to by the symmetricKeySet property does not exist in the keystore.

System action:
The key is not served.

Administrator response:
Ensure that a valid key alias is specified. You might examine the current alias values that are specified for the symmetricKeySet property. Then, try the operation again.

CTGKS0029E Alias *VALUE_0* will not be served to LTO drives.

Explanation:
The alias pointed to by the symmetricKeySet property does not exist in the keystore.

System action:
The key is not served.

Administrator response:
Ensure that a valid key alias is specified. You might examine the current alias values that are specified for the symmetricKeySet property. Then, try the operation again.

CTGKS0030E Alias *VALUE_0* was in the keystore but is not a Symmetric KeyEntry.

Explanation:
The key alias pointed to by the symmetricKeySet property was found in the keystore, but the key is not a symmetric key.

System action:
The key is not served.

Administrator response:
Ensure that the key is a symmetric key and that the key is in active state. Then, try the operation again.

CTGKS0031E PKCS11Impl keystore type is not supported.

Explanation:
The symmetricKeySet property is pointing to PKCS11Impl keys, which are not supported. The supported algorithms are AES or DESede.

System action:
The key operation fails.

Administrator response:
Ensure that you are using symmetric keys that conform to the AES algorithm with a size of 256 bits or DESede algorithm with a size of 163 bits. Then, try the operation again.

CTGKS0032E Could not determine key encoding to obtain key size.

Explanation:
This is an internal error. Processing could not determine the key encoding.

System action:
The key operation fails.

Administrator response:
Ensure that you are using symmetric keys that conform to the AES algorithm with a size of 256 bits or DESede algorithm with a size of 163 bits. Then, try the operation again.

CTGKS0033E Expected AES key size is 32 bytes.

Explanation:
IBM Security Guardium Key Lifecycle Manager supports Advanced Encryption Standard (AES) key that are 32 bytes in length. This key has a different length.

System action:
The key operation fails.

Administrator response:
Ensure that you are using symmetric keys that conform to the AES algorithm with a size of 32 bytes. Then, try the operation again.

CTGKS0034E Cannot find Secretkey in the keystore with key alias *VALUE_0*

Explanation:
Processing cannot find the symmetric key in the keystore with the specified alias.

System action:
The key is not served.

Administrator response:
Ensure that a valid key alias is specified. You might examine the current alias values that are specified for the symmetricKeySet property. Then, try the operation again.

CTGKS0035E Unsupported algorithm *VALUE_0* .

Explanation:
PKCS11Impl is not a supported algorithm for symmetric keys. A supported algortihm is AES.

System action:
Make sure to have symmetric keys with AES algorithm and size 32 bytes to support LTO drives.

Administrator response:
Make sure to have symmetric keys with AES algorithm and size 32 bytes to support LTO drives.

CTGKS0036E AES key size is *VALUE_0* bytes. Only 32 bytes keys are supported.

Explanation:
Supported algorithm is AES with 32 byte size.

System action:
symmetricKeySet needs to have valid AES keys. Make sure that 32 byte AES symmetric keys exist in the keystore.

Administrator response:
Add 32 byte size AES keys using the graphical user interface or command line interface to support LTO drives.

CTGKS0037E Internal Error:Crypto not initialized. ErrorCode=0xEE0F.

Explanation:
Internal error. Crypto class is not initialized. key server cannot serve the keys. ErrorCode is 0xEE0F.

System action:
Make sure the keystore type is supported by IBM Security Guardium Key Lifecycle Manager.

Administrator response:
Check logs for more information. Try to restart IBM Security Guardium Key Lifecycle Manager and retry the operation.

CTGKS0038E Vendor ID *VALUE_0* error. ErrorCode=0xEE02.

Explanation:
This OEM vendor is not supported by IBM.

System action:
Contact IBM Support.

Administrator response:
Contact IBM Support.

CTGKS0039E Drive with device serial number *VALUE_0* and WWN *VALUE_1* not found.

Explanation:
This drive is not found in the database and cannot be served keys.

System action:
No keys are served.

Administrator response:
Set the device.AutoPendingAutoDiscovery attribute to a value of 1 for the device group. Then, try the operation again.

CTGKS0040E Socket timed out.

Explanation:
Socket time out occurred. It may not be an error. If there are no other errors, no action is necessary.

System action:
Socket timed out.

Administrator response:
If there are no other errors, no action is necessary.

CTGKS0041E Bad ASC and ASCQ received.

Explanation:
Message processing failed. The drive sent bad ASC and ASQ codes.

System action:
Cannot serve the keys to this device.

Administrator response:
Check the logs for more information. Retry the operation with valid values of ASC and ASCQ.

CTGKS0042E Unexpected payload.

Explanation:
Message processing failed. The drive sent a message out of order.

System action:
Cannot serve the keys to this device.

Administrator response:
Check the logs for more information.

CTGKS0043E Drive certificate type not provided.

Explanation:
Message processing failed. The drive did not send certificate type and cannot be validated.

System action:

Cannot serve the keys to this device.

Administrator response:
Check the logs for more information.

CTGKS0044E No drive certificate provided.

Explanation:
Message processing failed. The drive did not send any certificate and cannot be validated.

System action:
Cannot serve the keys to this device.

Administrator response:
Check the logs for more information.

CTGKS0045E Unsupported drive certificate type.

Explanation:
Message processing failed. The drive provided a certificate type that is not valid.

System action:
Cannot serve the keys to this device.

Administrator response:
Check the logs for more information.

CTGKS0046E Drive certificate not signed properly.

Explanation:
Message processing failed. The drive certificate needs to be signed by trusted party.

System action:
Cannot serve the keys to this device.

Administrator response:
Check the logs for more information.

CTGKS0047E Unexpected DSK count: 0

Explanation:
Message processing failed. The drive did not send any certificates.

System action:
Cannot serve the keys to this device.

Administrator response:
Check the logs for more information.

CTGKS0048E No signature in DSK.

Explanation:
Message processing failed. Signature is missing in drive certificate.

System action:
Cannot serve the keys to this device.

Administrator response:
Check the logs for more information.

CTGKS0049E Cannot verify signature on DSK.

Explanation:
Message processing failed. Drive certificate signature cannot be verified.

System action:
Cannot serve the keys to this device.

Administrator response:
Check the logs for more information.

CTGKS0050E No label expected in UKI with ukiType 0x1931 but label was received.

Explanation:
Message processing fails.

System action:
Cannot serve the keys to this device.

Administrator response:
Check the logs for more information.

CTGKS0051E Expected uki 0x1930 or 0x1931. Uki received is *VALUE_0*

Explanation:
Message processing fails.

System action:
Cannot serve the keys to this device.

Administrator response:
Check the logs for more information.

CTGKS0052E Could not choose the key from the specified key group.

Explanation:
Message processing failed. Could not find valid key from the specified key group or key group is not specified. chooseDKI() returned null alias

System action:
Cannot serve the keys to this device.

Administrator response:
Check the logs for more information. Add valid symmetric keys to the default key group and retry the operation.

CTGKS0053E Keystore did not return SecretKey corresponding to DKI *VALUE_0*

Explanation:
Internal Error: Message processing failed. Could not find valid symmetric key from the keystore for the specified key.

System action:
The specified key cannot be served to this device.

Administrator response:
Check the logs for more information. Make sure key pointed to by this DKI exists in the keystore and retry the operation.

CTGKS0054E Cannot retrieve certificate with label *VALUE_0*

Explanation:
Message processing failed. Cannot retrieve certificate with this alias from the keystore.

System action:
Cannot serve the keys to this device.

Administrator response:
Make sure this certificate exists in the keystore. Check logs for more information.

CTGKS0055E Cannot obtain SKI from the certificate.

Explanation:
Message processing failed. Cannot obtain SKI from the provided certificate.

System action:
Cannot serve the keys to this device.

Administrator response:
Check the logs for more information.

CTGKS0056E Certificate with alias *VALUE_0* does not exist in the keystore or is incorrect.

Explanation:
Message processing failed. Certificate either does not exist or is not valid. That is, the certificate might have been expired or compromised.

System action:
Cannot serve the keys to this device.

Administrator response:
Use the command line interface to make sure the certificate with this alias is active and not expired or compromised. Check the logs for more information.

CTGKS0057E Certificate alias is null.

Explanation:
Message processing failed. Drive did not send certificate alias.

System action:
Check the logs for more information.

Administrator response:
Use the command line interface to make sure the certificate is active and not expired. Check the logs for more information.

CTGKS0058E No private key found.

Explanation:
Message processing failed. No private key found to decrypt the DK.

System action:
The key cannot served to this device.

Administrator response:
Check the logs for more information. Make sure keystore contains keys for provided aliases and retry the operation.

CTGKS0059E Unknown payload type received.

Explanation:
Message processing failed. Unknown payload type received, the message cannot be parsed.

System action:
Cannot serve the keys to the device.

Administrator response:
Use the command line interface to make sure the certificate is active and not expired. Check the logs for more information.

CTGKS0060E DKI *VALUE_0* not found in the keystore.

Explanation:
Message processing failed. DKI not found in the keystore.

System action:
Cannot serve the leys to the device.

Administrator response:
Make sure the symmetric key with this alias exists in the keystore. Check the logs for more information.

CTGKS0061E eedkuki is null

Explanation:
Message processing failed. eedkuki is null.

System action:
Cannot serve the leys to the device.

Administrator response:
Check the logs for more information.

CTGKS0062E Cannot retrieve key data.

Explanation:
Message processing failed. DK cannot be decrypted.

System action:
Cannot serve the keys to the device.

Administrator response:
Check the logs for more information.

CTGKS0063E Action value *VALUE_0* is incorrect.

Explanation:
Message processing failed. Action value incorrect, error in parsing the message.

System action:
Cannot serve the keys to the device.

Administrator response:
Check the logs for more information.

CTGKS0064E IBM Security Guardium Key Lifecycle Manager Truststore does not exist.

Explanation:
The truststore file tklmTruststore.jceks does not exist.

System action:
The software cannot validate device certificates or serve keys.

Administrator response:
If IBM Security Guardium Key Lifecycle Manager installed successfully, the tklmTruststore.jceks file should exist. If the file does not exist, contact IBM Support.

CTGKS0065E IBM Security Guardium Key Lifecycle Manager Truststore cannot be loaded.

Explanation:
The IBM Security Guardium Key Lifecycle Manager Truststore file tklmTruststore.jceks cannot be loaded.

System action:
Device certificates cannot be validated. Keys cannot be served.

Administrator response:
Make sure that the file exists and that the password of the file has not been changed. Check the logs for more information. If that does not help, call IBM Support.

CTGKS0066E symmetricKeySet is incorrect.

Explanation:
Configuration property symmetricKeySet cannot be validated. LTO drives cannot be served.

System action:
If symmetrickeySet points to a key group, then make sure the group has at least one AES or DESede key depending on whether the zOSCompatibility flag is off or on. If symmetricKeySet points to a key alias, then make sure the alias exists in the keystore and is valid.

Administrator response:
Refer to the product documentation on how to create key groups and symmetric keys.

CTGKS0067E No keys available in key group *VALUE_0*.

Explanation:
All the keys from this key group are already served to drives and no more unique keys are available to serve to the LTO drive.

System action:
With stopRoundRobinKeyGrps flag on, the keys from the key group can be used only once. There are no more keys available to serve to the LTO drive. Drive write fails with error 0XEE34.

Administrator response:
Refer to the product documentation on how to create key groups and symmetric keys. Add more keys to this key group and retry the operation.

CTGKS0068E Server parameters not initialized.

Explanation:
key server is not able to read the keystore password from the database and server parameters cannot be initialized.

System action:
IBM Security Guardium Key Lifecycle Manager will not be able to serve keys to devices.

Administrator response:
Make sure keystore is properly configured in the IBM Security Guardium Key Lifecycle Manager server and the internal property tklm.encryption.password is present in the SKLMConfig.properties file. Refer to the logs for more information. Correct the problem and restart the server.

CTGKS0069E Client certificate chain not received.

Explanation:
TLS connection fails because the server did not receive any certificate from a client to be able to authenticate that client. This error can happen only if clientAuthentication is set to 2 (required) in SKLMConfig.properties file for key server. Note that for KMIP protocol, clientAuthentication is always set to required.

System action:
TLS handshake fails and TLS connection cannot be established.

Administrator response:
Make sure client is configured to send a certificate to IBM Security Guardium Key Lifecycle Manager that IBM Security Guardium Key Lifecycle Manager can trust. These trusted TLSClient certificates can be listed with the tklmCertList command. Refer to the logs for more information. Correct the problem and restart the server.

CTGKS0070E Server does not trust the client certificate.

Explanation:
Client authentication fails because the server does not trust the certificate sent by the client. This error can happen only if clientAuthentication is set to 2 (required) in the SKLMConfig.properties file for key server. Note that for KMIP protocol, clientAuthentication is always set to required.

System action:
TLS handshake fails and TLS connection cannot be established.

Administrator response:
Make sure client is configured to send a certificate to IBM Security Guardium Key Lifecycle Manager that it can trust. These trusted TLSClient certificates can be listed with the tklmCertList command. Refer to the logs for more information. Correct the problem and restart the server.

CTGKS0071E **No SSLServer certificate with alias *VALUE_0* found in the database.**

Explanation

Date	Change description
10 Feb 2021	Corrected instances of 'TLSServer' to 'SSLServer'. Refreshed only the English language content.
08 Dec 2020	Initial version.

Explanation:
The TLS certificate specified by **`config.keystore.ssl.certalias`** in the `SKLMConfig.properties` file is not found in the database or is not marked as the SSLServer certificate.

System action:
TLS handshake fails and TLS connection cannot be established.

Administrator response:
Make sure the TLS server certificate is configured and exists in the database by listing it with tklmCertList command. Once the correct TLS server is configured then restart the server. Refer to the logs for more information.

CTGKS0072E **Certificate alias length cannot exceed 256 characters.**

Explanation:
Certificate alias exceeded 256 characters in length.

System action:
Certificate creation fails.

Administrator response:
Check the logs for more information.

CTGKS0073E **Attribute *VALUE_0* is not supported for device group *VALUE_1* .**

Explanation:
Attribute is not supported for the specified device group.

System action:
The operation fails.

Administrator response:
Check the logs for more information.

CTGKS0074E **Message signature does not verify.**

Explanation:
Message signature cannot be verified. Message processing failed. key server cannot serve the keys.

System action:
Cannot serve the keys to this device.

Administrator response:
Check the logs for more information. Try to restart IBM Security Guardium Key Lifecycle Manager and retry the operation.

CTGKS0075E **Message type not *VALUE_0* .**

Explanation:
Received wrong message type for the message, message cannot be parsed. Message processing failed. key server cannot serve the keys.

System action:
Cannot serve the keys to this device.

Administrator response:
Check the logs for more information. Try to restart IBM Security Guardium Key Lifecycle Manager and retry the operation.

CTGKS0076E **DKI length not 12 bytes or data key length not 32 bytes in KADDescriptor.**

Explanation:
Message processing failed. key server cannot serve the keys.

System action:
Cannot serve the keys to this device.

Administrator response:
Check the logs for more information. Try to restart IBM Security Guardium Key Lifecycle Manager and retry the operation.

CTGKS0077E **Audit or Configuration objects are null.**

Explanation:
Internal error. Audit or Configuration objects are not initialized for the object being used.

System action:
The system cannot process the message.

Administrator response:
Refer to the logs for more information.

CTGKS0078E **Keystore not found in the database.**

Explanation:
The keystore is not found in the database.

System action:

The system cannot initialize and function properly.

Administrator response:
Make sure the database server is up and running. Refer to the logs for more information.

CTGKS0079E Unknown message type *VALUE_0*.

Explanation:
Message processing failed. Unknown message type received, cannot parse the message.

System action:
Cannot serve the keys to this device.

Administrator response:
Check the logs for more information. Retry the operation with valid values of message type.

CTGKS0080E Cannot update device labels or type for this device *VALUE_0*.

Explanation:
Message processing failed. Internal error occurred while updating device metadata.

System action:
The device metadata will not be updated in the database.

Administrator response:
Check the logs for more information. Retry the operation with valid values of message type.

CTGKS0081E audit not initilized.

Explanation:
The files that are specified for audit output might be specified as read-only.

System action:
Initialization fails.

Administrator response:
Specify that the audit output files are writable. Then, try the operation again.

CTGKS0124E Migration fails. The file or directory {0} does not exist.

Explanation:
The migration program accesses files from the previous and new IBM Security Guardium Key Lifecycle Manager directory. One of the critical files or the directory cannot be accessed.

System action:
The migration program fails.

Administrator response:
Verify that the file or directory exists and has the appropriate read and write permissions. Run the migration program again.

CTGKS0125E Migration fails. The specified argument {0} is not a directory.

Explanation:
The argument specified must be a directory where Tivoli Integrated Portal is installed.

System action:
The migration program fails.

Administrator response:
Specify a valid directory where Tivoli Integrated Portal is installed. Run the migration again.

CTGKS0126E Migration fails. The file {0} could not be read. The exception {1} occurred.

Explanation:
Before starting the migration process, the migration program reads the configuration file to verify that all the critical information needed to migrate the previous IBM Security Guardium Key Lifecycle Manager is available and correct. This file could not be read.

System action:
The migration program fails.

Administrator response:
Verify that the file exists and has correct read permissions. This file might have been removed. If the file does not exist, restore the backed up version of IBM Security Guardium Key Lifecycle Manager. Run the migration program again.

CTGKS0127E Migration fails. The property file {0} is missing the required property {1}.

Explanation:
Before starting the migration process, the migration program reads the configuration file to verify that all the critical information needed to migrate the previous IBM Security Guardium Key Lifecycle Manager is available and correct. One of the required properties is missing.

System action:
The migration program fails.

Administrator response:
The required property might have been removed. add the property with the correct value or restore the backed up version of IBM Security Guardium Key Lifecycle Manager. Run the migration program again.

CTGKS0128E Migration fails. The value {0} is not a valid value for the configuration parameter {1}.

Explanation:
Before starting the migration process, the migration program reads the configuration file to verify that all the critical information needed to migrate the previous IBM Security Guardium Key Lifecycle Manager is available and correct. One of the required properties has an incorrect value.

System action:
The migration program fails.

Administrator response:
The required property might have been modified. Either set the property to the correct value or restore the backed up version of IBM Security Guardium Key Lifecycle Manager. Run the migration program again.

CTGKS0129E **Migration fails. IBM Security Guardium Key Lifecycle Manager could not validate the previous Tivoli Integrated Portal Administrator password. The password might be incorrect or the server might not be running.**

Explanation:
Before starting the migration process, the migration program validates the Tivoli Integrated Portal Administrator password. The Tivoli Integrated Portal password is required to start and stop the Tivoli Integrated Portal server and to undeploy the previous IBM Security Guardium Key Lifecycle Manager.

System action:
The migration program fails.

Administrator response:
Verify that Tivoli Integrated Portal Server is running and the password is correct. Place quote marks around the password if necessary. Run the migration program again.

CTGKS0130E **Migration fails. IBM Security Guardium Key Lifecycle Manager could not validate the database administrator password. The password might be incorrect or the database server might not be running.**

Explanation:
Before starting the migration process, the migration program validates the database administrator password. The password is required to migrate the database schema and the data.

System action:
The migration program fails.

Administrator response:
Verify that the database server is running and the password specified is correct. Run the migration program again.

CTGKS0131E **Migration fails. The database schema could not be migrated to the latest version of IBM Security Guardium Key Lifecycle Manager.**

Explanation:
Before starting the migration process, the migration program validates that the database schema is at the earlier level of IBM Security Guardium Key Lifecycle Manager.

System action:
The migration program fails.

Administrator response:
Verify that the database server is running and the correct version ofIBM Security Guardium Key Lifecycle Manager is installed. Run the migration program again.

CTGKS0132E **Migration fails. IBM Security Guardium Key Lifecycle Manager could not validate the new Tivoli Integrated Portal Administrator password. The password might be incorrect or the server might not be running.**

Explanation:
Before starting the migration process, the migration program validates the Tivoli Integrated Portal Administrator password. The Tivoli Integrated Portal password is required to start and stop the new Tivoli Integrated Portal server.

System action:
The migration program fails.

Administrator response:
Verify that the new Tivoli Integrated Portal Server is running and the specified password is correct. Place quote marks around the password if necessary. Run the migration program again.

CTGKS0133E **Migration fails. IBM Security Guardium Key Lifecycle Manager could not validate the new IBM Security Guardium Key Lifecycle Manager Administrator password. The password might be incorrect or the server might not be running.**

Explanation:
Before starting the migration process, the migration program validates the Tivoli Integrated Portal Administrator password. The Tivoli Integrated Portal password is required to migrate the previously scheduled rollover tasks.

System action:
The migration program fails.

Administrator response:
Verify that the new Tivoli Integrated Portal Server is running and the specified password is correct. Place quote marks around the password if necessary. Run the migration program again.

CTGKS0134E **Migration fails. The IBM Security Guardium Key Lifecycle Manager**

database password contains characters that are other than [a-z,A-Z,0-9].

Explanation:
Before starting the migration process, the migration program validates that the database administrator password contains only allowable characters.

System action:
The migration program fails.

Administrator response:
Verify that the database password contains only characters [a-z,A-Z,0-9]. Change the password to include only characters[a-z,A-Z,0-9] using tools that the operating system provides and run the migration again. After successful migration, you might change the database password as documented in the IBM Security Guardium Key Lifecycle Manager Installation Guide.

CTGKS0135E Migration fails. IBM Security Guardium Key Lifecycle Manager cannot verify that schema is at the appropriate level before migration starts. The database server might not be running.

Explanation:
Before starting the migration process, the migration program validates that the database schema is at the correct level.

System action:
The migration program fails.

Administrator response:
Verify that the database server is running. Run the migration program again.

CTGKS0136E Migration fails. IBM Security Guardium Key Lifecycle Manager cannot migrate the key groups. The database server might not be running, the transaction log might be full, or an unexpected database error occurred.

Explanation:
The migration program migrates the existing groups to assign device groups to each of the key groups.

System action:
The migration program fails.

Administrator response:
Verify that the database server is running and transaction log is not full. The database exception might provide additional information about the problem. Correct the condition and run the migration program again. If the problem persists, contact IBM Support.

CTGKS0137E Migration fails. IBM Security Guardium Key Lifecycle Manager cannot migrate the keys. The database server might not be running, the transaction log might be full or an unexpected database error occurred.

Explanation:
The migration program migrates the existing keys to assign device groups to each of the keys and other data transformations needed to make the keys work with the latest version of IBM Security Guardium Key Lifecycle Manager.

System action:
The migration program fails.

Administrator response:
Verify that the database server is running and transaction log is not full. The database exception may provide additional information about the problem. Correct the condition and run the migration program again. If the problem persists, contact IBM Support.

CTGKS0138E Migration fails. IBM Security Guardium Key Lifecycle Manager cannot migrate the certificates. The database server might not be running, the transaction log might be full, or an unexpected database error occurred.

Explanation:
The migration program migrates the existing certificates to assign device groups to each of the certificates and other data transformations needed to make the certificates work with the latest version of IBM Security Guardium Key Lifecycle Manager.

System action:
The migration program fails.

Administrator response:
Verify that the database server is running and transaction log is not full. The database exception may provide additional information about the problem. Correct the condition and run the migration program again. If the problem persists, contact IBM Support.

CTGKS0139E Migration fails. IBM Security Guardium Key Lifecycle Manager cannot migrate the device attributes. The database server might not be running or an unexpected database error occurred.

Explanation:
The migration program sets the device attributes on how to handle unknown DS8000 and LTO drives based on the properties in the SKLMConfig.properties file.

System action:
The migration program fails.

Administrator response:
Verify that the database server is running.
The database exception may provide additional information about the problem. Correct the condition that caused the error and run the migration program again. If the problem persists, contact IBM Support.

CTGKS0140E Migration fails. IBM Security Guardium Key Lifecycle Manager cannot migrate the device audit data. The server might not be running, the transaction log might be full, or an unexpected database error occurred.

Explanation:
The migration program migrates the existing device audit metadata to assign device groups to each of the audit records.

System action:
The migration program fails.

Administrator response:
Verify that the database server is running and the transaction log is not full. The database exception may provide additional information about the problem. Correct the condition and run the migration program again. If the problem persists, contact IBM Support.

CTGKS0141E Migration fails. IBM Security Guardium Key Lifecycle Manager cannot migrate the scheduled tasks. The exception {0} occurred. The database server might not be running, an unexpected database error occurred, or the Tivoli Integrated Portal server might not be running.

Explanation:
The migration program migrates the existing scheduled rollover tasks to assign device groups to each of the tasks.

System action:
The migration program fails.

Administrator response:
Verify that the database server and the Tivoli Integrated Portal server are running. The database exception may provide additional information about the problem. Correct the condition and run the migration program again. If the problem persists, contact IBM Support.

CTGKS0142E Migration fails. You must be running Encryption Key Manager Version 2.1 before migrating to IBM Security Guardium Key Lifecycle Manager.

Explanation:
The migration program verifies that Encryption Key Manager Version 2.1 is installed. The properties TransportListener.ssl.keystore.password.obfuscated and config.keystore.password.obfuscated must be set in the KeyManagerConfig.properties file.

System action:
The migration program fails.

Administrator response:
Verify that Encryption Key Manager Version 2.1 is installed. If you are running an earlier version of Encryption Key Manager, upgrade to Version 2.1 and run the migration again.

CTGKS0143E Server parameters not initialized.

Explanation:
The key group cannot be deleted because server parameters are not initialized.

System action:
The delete key group operation fails.

Administrator response:
The key group cannot be deleted because server parameters are not initialized.

CTGKS0146E The message type is not as expected: *VALUE_0* .

Explanation:
The message type is not as expected.

System action:
The operation fails

Administrator response:
Examine the exception message, and then try the operation again.

CTGKS0147E Message OEM shared secret does not verify.

Explanation:
Message OEM shared secret does not verify.

System action:
The operation fails.

Administrator response:
Make sure the OEM shared secret is correct, and try again.

CTGKS0148W Warning: The migration to IBM Security Guardium Key Lifecycle Manager was successful. However, the migration could not remove the {0}component of IBM Security Guardium Key Lifecycle Manager Version 1 from Tivoli Integrated Portal

Server. For steps to manually remove remaining components of IBM Security Guardium Key Lifecycle Manager Version 1 from Tivoli IntegratedPortal Server, see the Installing section of the product documentation in the IBM Knowledge Center.

Explanation:
The migration program, after successfully migrating to IBM Security Guardium Key Lifecycle Manager Version 2, removes IBM Security Guardium Key Lifecycle Manager Version 1 from Tivoli Integrated Portal server. The components are the graphical user interface, data sources, and application. The process could not remove all the components of IBM Security Guardium Key Lifecycle Manager Version 1.

System action:
The migration program succeeds with a warning.

Administrator response:
Verify that the IBM Security Guardium Key Lifecycle Manager Version 2 is functioning correctly. Refer to the IBM Security Guardium Key Lifecycle Manager Version 2 Installation Guide for steps to remove the remaining components of IBM Security Guardium Key Lifecycle Manager Version 1 from Tivoli Integrated Portal Server.

CTGKS0149E **Migration fails. IBM Security Guardium Key Lifecycle Manager could not validate the previous Tivoli Integrated Portal Administrator password. Possible reasons: specified password is incorrect or the server is not running.**

Explanation:
Before starting the migration process, the migration program validates the Tivoli Integrated Portal Administrator password. The Tivoli Integrated Portal password is required to start and stop the Tivoli Integrated Portal server and to undeploy the previous IBM Security Guardium Key Lifecycle Manager.

System action:
The migration program fails.

Administrator response:
Verify that Tivoli Integrated Portal Server is running and the password specified is correct. Run the migration program again.

CTGKS0150E **Usage: migratetklm db_administrator_pwd v1_tipadmin_pwd v2_tipadmin_pwd v2_tklmadmin_pwd\n where \n db_administrator_pwd - IBM Security Guardium Key Lifecycle Manager Version 1 database administrator password.\n v1_tipadmin_pwd - Tivoli Integrated Portal Server Administrator password for IBM Security Guardium Key Lifecycle Manager Version 1\n v2_tipadmin_pwd - Tivoli Integrated Portal Server Administrator password for IBM Security Guardium Key Lifecycle Manager Version 2\n v2_tklmadmin_pwd - IBM Security Guardium Key Lifecycle Manager Version 2, Administrator password.**

Explanation:
The migration program was started with an incorrect number of arguments. Either specify all the required passwords as arguments or start the program without any arguments. You will be prompted for the passwords when the program starts.

System action:
The migration program fails.

Administrator response:
Start the migration program either specifying all the passwords or without any passwords.

CTGKS0155E **Migration fails. The following exception occurred: {0}**

Explanation:
While performing a migration step, an exception occurred. The migration program immediately prints an error message indicating the correct action.

System action:
The migration program fails.

Administrator response:
Perform the action that the message provides.

CTGKS0158W **Partially removed IBM Security Guardium Key Lifecycle Manager Version 1 files. However, you might remove the rest of the files manually.**

Explanation:
The migration could not remove all files in IBM Security Guardium Key Lifecycle Manager Version 1.

System action:
Migration succeeds.

Administrator response:
Remove the remainder of the files from IBM Security Guardium Key Lifecycle Manager Version 1 after moving audit logs to another location.

CTGKS0160E Migration fails. Refer to the SKLM_HOME/migration/migrate.log file to identify causes of failure and recovery steps.

Explanation:
Migration fails.

System action:
Migration fails.

Administrator response:
Perform the recovery step identified by one or more earlier error messages in the migrate.log file.

CTGKS0163E Migration fails. The database schema version could not be set to 2.0 to indicate successful database schema and data migration during the previous migration attempts.

Explanation:
At the end of migration, the migration program sets the version to 2.0 in the database to indicate that the schema has been upgraded to the latest level. It also drops the migration-related table from the database.

System action:
Migration fails.

Administrator response:
The database server might have stopped. Start the database server and run the migration again.

CTGKS0164E Migration fails. The database instance or database could not be migrated to the latest version of Db2.

Explanation:
The migration program migrates the database instance and database to the latest version of Db2. This process failed.

System action:
Migration fails.

Administrator response:
There might be low disk space or an unexpected error. Run the migration program again. If the problem persists, contact IBM Support.

CTGKS0165E Migration fails. The migration program cannot copy either the user keystore or the IBM Security Guardium Key Lifecycle Manager internal keystore to the new location under the IBM Security Guardium Key Lifecycle Manager Version 2 folder.

Explanation:
The migration program copies the user and internal keystores to the IBM Security Guardium Key Lifecycle Manager Version 2 location.

System action:
Migration fails.

Administrator response:
There might be incorrect permissions for the keystore files in IBM Security Guardium Key Lifecycle Manager Version 1 or the target folder does not have correct permissions. Verify that both the source and target directories have correct permissions for copying. Run the migration program again. If the problem persists, contact IBM Support.

CTGKS0168E Migration fails. The user key store {0} cannot be not migrated successfully.

Explanation:
The migration program copies the user keystore from IBM Security Guardium Key Lifecycle Manager Version 1 to Version 2. This operation did not succeed.

System action:
Migration fails.

Administrator response:
Verify that permissions for the user keystore have the correct read permissions in IBM Security Guardium Key Lifecycle Manager Version 1 and the directory in Version 2 where user keystore would have been copied has the correct write permissions.

CTGKS0171E Migration fails. IBM Security Guardium Key Lifecycle Manager cannot migrate the devices.

Explanation:
The migration program migrates the existing devices to assign the original device type to each of the devices to be consistent with the latest version of IBM Security Guardium Key Lifecycle Manager.

System action:
The migration program fails.

Administrator response:
Verify that the database server is running and transaction log is not full. The database exception may provide additional information about the problem. Correct the condition and run the migration program again. If the problem persists, contact IBM Support.

CTGKS0173E Migration fails. The migration program cannot migrate the rollover task because of an internal error. Contact IBM Support.

Explanation:
The migration program fails.

System action:
The migration program fails.

Administrator response:
Send the migrate.log to IBM Support.

CTGKS0180E Migration fails. IBM Security Guardium Key Lifecycle Manager cannot add missing public keys. The database server might not be running, the transaction log might be full, or an unexpected database error occurred.

Explanation:
The migration program fails to add missing public keys to those public/private keypairs that were imported.

System action:
The migration program fails.

Administrator response:
Verify that the database server is running and transaction log is not full. The database exception might provide additional information about the problem. Correct the condition and run the migration program again. If the problem persists, contact IBM Support.

CTGKS0183E Migration fails. The migration program fails to create a unique database entry for each alias when a key or certificate has multiple aliases. The database server might not be running, the transaction log might be full, or an unexpected database error occurred.

Explanation:
The migration program fails to create a unique database entry for each alias when a key or certificate has multiple aliases.

System action:
The migration program fails.

Administrator response:
Verify that the database server is running and transaction log is not full. The database exception may provide additional information about the problem. Correct the condition and run the migration program again. If the problem persists, contact IBM Support.

CTGKS0191E The migration program failed to execute a batch file or a shell script.

Explanation:
The migration program executes one or more shell scripts or batch files during migration. An error occurred.

System action:
The migration program fails.

Administrator response:
One or more batch files or shell scripts may not have correct permissions. Contact IBM support if problem persists.

CTGKS0500E Unsupported Value received in *VALUE_0* for *VALUE_1* field.

Explanation:
The message from the client has an unsupported value in the given field.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information.

CTGKS0501E Cannot skip bytes, not enough bytes.

Explanation:
The message does not have enough bytes left and cannot skip the bytes to read the whole message.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information.

CTGKS0503E Integrity check failed.

Explanation:
The EncryptedPayload cannot be verified because it failed the integrity check.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information.

CTGKS0504E No value provided in *VALUE_0* for *VALUE_1* field.

Explanation:
The message from the client did not provide the value in the given field.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information.

CTGKS0505E Not enough cryptographic algorithm descriptors in UTCryptographicAlgorithmsPayload.

Explanation:
The UTCryptographicAlgorithmsPayload does not have enough cryptographic algorithm descriptors. The expected number of descriptors is 2.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information.

CTGKS0506E Not enough bytes in SPHeader. Number of bytes received are *VALUE_0* , expected number of bytes in SPHeader is 16.

Explanation:
Not enough bytes in SPHeader in SPINCommand received.

System action:
IBM Security Guardium Key Lifecycle Manager

System action:
cannot process the message for the client.

Administrator response:
Check the logs for more information.

CTGKS0507E More than one *VALUE_0* in the *VALUE_1* message.

Explanation:
More than one payload received in the message as indicated. Expected to receive only one.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information.

CTGKS0508E Not enough bytes in SPHeader. Number of bytes received are *VALUE_0* , expected number of bytes in SPHeader is 16.

Explanation:
Not enough bytes in SPHeader in SPOUTCommand received.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information and resend the request.

CTGKS0509E DS_SAI value is larger than 4 bytes. Value received is *VALUE_0* .

Explanation:
DS_SAI value cannot exceed 4 bytes.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information to correct the problem and try sending the request again.

CTGKS0510E Encryption key and/or algorithm is not set.

Explanation:
Encryption key and/or algorithm is not set. It needs to be set to AES_CBC. Cannot proceed.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information to correct the problem and try sending the request again.

CTGKS0511E Ac_SAI field mismatch. Value received from the device is *VALUE_0* .

Explanation:
AC_SAI field does not match with the one that is sent to the device.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information to correct the problem and try sending the request again.

CTGKS0512E UTCryptographicAlgorithmsPayload present in SPINKeyExchangeResponse.

Explanation:
UTCryptographicAlgorithmsPayload not expected in SPINKeyExchangeResponse.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information to correct the problem and try sending the request again.

CTGKS0513E Bad certificate request data.

Explanation:
Bad certificate request data received in SPINKeyExchangeResponse.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:

Check the logs for more information to correct the problem and try sending the request again.

CTGKS0514E IKEV2SERVER certificate not found.

Explanation:
IKEV2SERVER certificate not configured on the IBM Security Guardium Key Lifecycle Manager server.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Ensure that the IKEV2SEREVR certificate is configured on the server using the graphical user interface or by running the tklmListConfig command. Check that it is marked trusted and not expired. Check the logs for more information to correct the problem and try sending the request again.

CTGKS0515E No certificate request received from drive.

Explanation:
Certificate request payload is required in SPINKeyExchangeResponse.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information to correct the problem and try sending the request again.

CTGKS0516E Illegal certificate encoding *VALUE_0* received in *VALUE_1* .

Explanation:
Illegal certificate encoding received. Only X509 encoding is supported.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information to correct the problem and try sending the request again.

CTGKS0517E IKEV2CLIENT certificate not valid.

Explanation:
IKEV2CLIENT certificate configured on the IBM Security Guardium Key Lifecycle Manager server but does not seem to be valid.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Ensure that the IKEV2CLIENT certificate is marked trusted and not expired. Check the audit logs for more information to correct the problem and try sending the request again.

CTGKS0518E Identification sent by the device cannot be verified.

Explanation:
Idenitification payload send by a client has a server ID that does not match ID in the certificate in SPINAuthenticationResponse. Identification check failed.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information to correct the problem and try sending the request again.

CTGKS0519E UTCryptographicAlgorithmsPayload in SPINAuthenticationResponse differs from that in SPOUTAuthentication.

Explanation:
UTCryptographicAlgorithmsPayload in SPINAuthenticationResponse received from the device has to match the UTCryptographicAlgorithmsPayload sent in SPOUTAuthentication.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information to correct the problem and try sending the request again.

CTGKS0520E Authentication of authentication payload failed.

Explanation:
Signature cannot be verified in SPINAuthenticationResponse. Authentication check failed.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information to correct the problem and try sending the request again.

CTGKS0522E Nonce minimum length *VALUE_0* is greater than Nonce maximum length allowed which is *VALUE_1* .

Explanation:
Nonce minimum length cannot be greater than the maximum length allowed.

System action:

IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information to correct the problem and try sending the request again.

CTGKS0523E Cannot get public keys for trusted certificates.

Explanation:
Cannot get public keys for trusted certificates configured in IBM Security Guardium Key Lifecycle Manager. Cannot build SPOUTKeyExchange.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information to correct the problem and try sending the request again.

CTGKS0524E Wrong message received. At this state *VALUE_0* the message expected is *VALUE_1* .

Explanation:
IBM Security Guardium Key Lifecycle Manager received a message out of order.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information to correct the problem and try sending the request again.

CTGKS0525E CCS timeout occurred. The timer started at *VALUE_0* and the current timestamp is *VALUE_1* .

Explanation:
IBM Security Guardium Key Lifecycle Manager requires the next message to be received within CCS timeout period. The CCS timeout value is configured in SKLMConfig.properties file by config.keystore.IKEV2SERVER.CCSTimeout property name or 5 minutes by default.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Make sure the configured CCS timeout has a suitable value. Check the logs for more information to correct the problem and try sending the request again.

CTGKS0526E Payload not encrypted.

Explanation:
Payload in SPINAuthenticationResponse and SPOUTAuthentication are required to be encrypted.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information to correct the problem and try sending the request again.

CTGKS0527E No private key found to sign the certificate.

Explanation:
No private key found to sign the certificate.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information to correct the problem and try sending the request again.

CTGKS0528E IKEv2Server alias is not defined.

Explanation:
IKEv2Server alias needs to be configured.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Configure the IKEv2Server alias using the graphical user interface by going to Advanced Configuration > Server certificate. Check the logs for more information to correct the problem and try sending the request again.

CTGKS0529E Identification payload is not properly encoded.

Explanation:
Identification payload is not properly encoded.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information to correct the problem and try sending the request again.

CTGKS0530E Point coordinates do not match field size.

Explanation:
Point coordinates do not match field size. Cannot generate ECPrivateKey.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information to correct the problem and try sending the request again.

CTGKS0531E Only uncompressed point format supported.

Explanation:
Only uncompressed point format supported. Cannot generate ECPrivateKey.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information to correct the problem and try sending the request again.

CTGKS0532E Point does not match field size.

Explanation:
Point does not match field size. Cannot generate ECPrivateKey.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information to correct the problem and try sending the request again.

CTGKS0533E *VALUE_0* not set.

Explanation:
Internal error. The value of the given field is not set.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information to correct the problem and try sending the request again.

CTGKS0534E One or more key lengths is zero.

Explanation:
Internal error. One of the key lengths is not set.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information to correct the problem and try sending the request again.

CTGKS0535E Private key is larger than D-H modulus.

Explanation:
Internal error. Cannot generate D-H private key.

System action:
IBM Security Guardium Key Lifecycle Manager cannot process the message for the client.

Administrator response:
Check the logs for more information to correct the problem and try sending the request again.

CTGKS0536E The alias *VALUE_0* does not identify a certificate in the keystore.

Explanation:
Either the alias does not exist in the keystore, or it does not refer to a certificate.

System action:
The operation fails.

Administrator response:
Specify a valid alias, and try the operation again.

CTGKS0560E Data structure length is incorrect.

Explanation:
Data structure length is incorrect.

System action:
The operation fails.

Administrator response:
Correct the data structure, and try the operation again.

CTGKS0561E Response code is incorrect.

Explanation:
Response code is incorrect.

System action:
The operation fails.

Administrator response:
Try the operation again.

CTGKS0562E Expecting page code *VALUE_0* .

Explanation:
Unexpected page code.

System action:
The operation fails.

Administrator response:
Examine the error message, and then try again.

CTGKS0563E The routing structure type is not as expected: *VALUE_0* .

Explanation:
The routing structure type is not as expected.

System action:
The operation fails.

Administrator response:
Examine the exception message, and then try again.

CTGKS0564E Expecting page code *VALUE_0* .

Explanation:
Unexpected page code.

System action:
The operation fails.

Administrator response:
Examine the error message, and then try again.

CTGKS0565E Unknown signature type.

Explanation:
The signature type is unknown.

System action:
The operation fails.

Administrator response:
Check the signature type, and then try again.

CTGKS0566E Message has been tampered with.

Explanation:
Message has been tampered with.

System action:
The operation fails.

Administrator response:
Make sure the message is correct, and try again.

CTGKM9002E The administrator ID must be eight characters or less.

Explanation:
The user ID is restricted to a maximum length of eight characters.

System action:
Installation cannot continue until you correct the error.

User response:
Select a different user ID that is eight characters or less.

CTGKM9003E The administrator ID must begin with an alphabetic character.

Explanation

The user ID must start with a letter.

Additionally, the user ID can only use alphabetical characters, numeric characters, and the underscore (A-Z, a-z, 0–9, and _).

System action:
Installation cannot continue until you correct the error.

User response:
Select a different user ID that starts with a letter.

CTGKM9004E The administrator ID cannot begin with: ibm, sql, or sys.

Explanation:
The administrator user ID cannot start with ibm, sql, or sys.

System action:
Installation cannot continue until you correct the error.

User response:
Select a different user ID that does not start with one of the restricted strings.

CTGKM9005E The administrator ID cannot be: db2, users, admins, guests, public, private, properties, local, or root.

Explanation:
Db2 reserved keywords cannot be used as an administrator user ID.

System action:
Installation cannot continue until you correct the error.

User response:
Select a different user ID that is not a Db2 keyword.

CTGKM9006E The administrator ID is a required field.

Explanation:
You must specify an administrator user ID.

System action:
Installation cannot continue until you enter a value in the field.

User response:
Enter a user ID in the Administrator ID field.

CTGKM9007E The password is a required field.

Explanation:
You must specify a password.

System action:
Installation cannot continue until you enter a value in the field.

User response:
Enter a password for the user ID.

CTGKM9010E The password confirmation field is required.

Explanation:
You must specify a password.

System action:
Installation cannot continue until you enter a value in the field.

User response:
Enter a password for the user ID.

CTGKM9011E The database home is a required field.

Explanation:
You must specify the database home directory.

System action:
Installation cannot continue until you enter a value in the field.

User response:
Enter the directory in which to store the database files.

CTGKM9012E The database name is a required field.

Explanation:
You must specify a name for the database.

System action:
Installation cannot continue until you enter a value in the field.

User response:
Enter a name for the database.

CTGKM9037E The port number must be a positive integer among 9443, 9080, or between 1024 and 65536.

System action:
Installation cannot continue until you correct the error.

User response:
Enter a port number that is among 9443, 9080, or between 1024 and 65536.

CTGKM9038E The port is a required field.

Explanation:
You must specify a port.

System action:
Installation cannot continue until you enter a value in the field.

User response:
Enter a port number.

CTGKM9041E The password and password confirmation fields do not match. Reenter matching passwords for these two fields.

Explanation:
The passwords in both fields must match.

System action:
Installation cannot continue until you correct the error.

User response:
Re-enter the values in the fields.

CTGKM9042I Passwords cannot contain spaces.

Explanation:
Passwords can only contain alphanumeric characters and the underscore (a-z, A-Z, 0–9, and _).

System action:
Installation cannot continue until you correct the error.

User response:
Enter a different password that conforms to the rules.

CTGKM9044I The Administrator ID cannot be an SQL reserved word.

Explanation:
The Administrator ID cannot be an SQL reserved word.

System action:
Installation cannot continue until you correct the error.

User response:
Enter a different value for the Administrator ID.

CTGKM9049I The Windows Db2 DB Home field must be a drive letter [A-Z] followed by a colon.

Explanation:
On Windows systems, you must select the drive on which to install the IBM Security Guardium Key Lifecycle Manager database. A Windows drive indicator is a letter, following by a colon (:). For example, C:.

System action:
Installation cannot continue until you correct the error.

User response:
Enter a correctly formatted drive letter.

CTGKM9050E The DB Name must be 8 characters or less.

Explanation:
The DB Name must be 8 characters or less.

System action:
Installation cannot continue until you correct the error.

User response:
Select a different name.

CTGKM9050I The Windows Db2 DB Home field must be a drive letter that can be written to.

Explanation:
The drive must be writable for installation to proceed.

System action:
Installation cannot continue until you correct the error.

User response:
Use the operating system utilities to make the drive writable, or select a different drive.

CTGKM9051E The DB Name cannot contain special characters.

Explanation:
The name contains one or more incorrect characters.

User response:
Reenter the name and try again.

CTGKM9052E The DB Name must begin with an alphabetic character.

Explanation:
The DB Name can only use alphabetical characters, numeric characters, and the underscore (A-Z, a-z, 0–9, and _).

System action:

Installation cannot continue until you correct the error.

User response:
Select a different name.

CTGKM9053E The DB2 version currently selected for use is not supported. The supported version is 11.1 and above.

Explanation:
Guardium Key Lifecycle Manager requires a supported version of Db2.

System action:
The installation task fails.

User response:
Obtain a supported version of Db2. Try again.

CTGKM9054E The location specified is not a valid DB2 installation directory

Explanation:
The specified directory does not contain the existing DB2 installation.

User response:
Select a valid DB2 installation directory.

CTGKM9055E The user name/password fields cannot have more than {0} characters.

Explanation:
The value you specified exceeds the maximum length.

System action:
Installation cannot continue until you correct the error.

User response:
Specify a value that does not exceed the limit. Then, try the operation again.

CTGKM9056E Password and the confirmation does not match for {0}.

Explanation:
The Password and Confirm Password fields must have the same value.

System action:
Installation cannot continue until you correct the error.

User response:
Specify the same value for the Password and Confirm Password fields, and try the operation again.

CTGKM9057E The Application Server Administrator Confirm Password field is empty.

Explanation:
User has not specified the password confirmation value.

System action:
Installation cannot continue until you correct the error.

User response:
Enter a value in the Confirm Password field. Try again.

CTGKM9058E The Application Server Administrator User field is empty or invalid.

Explanation:
This message is displayed when the Application Server Administrator User field is empty or invalid.

System action:
Installation cannot continue until you correct the error.

User response:
Specify a correct value and try again.

CTGKM9059E The IBM Security Guardium Key Lifecycle Manager Administrator User field is empty.

Explanation:
This message is displayed when the IBM Security Guardium Key Lifecycle Manager Administrator User field is empty or invalid.

System action:
Installation cannot continue until you correct the error.

User response:
Specify a correct value and try again.

CTGKM9060E The user name field cannot contain any special characters.

Explanation:
The user name contains one or more incorrect characters.

System action:
Installation cannot continue until you correct the error.

User response:
Reenter the user name with valid characters and try again.

CTGKM9061E The port specified is already in use.

Explanation:
The port number that is entered must be available for use. The port number is already in use.

System action:
Installation cannot continue until you correct the error.

User response:
Select another port number. Ensure that the specified port number is available.

CTGKM9062E The IBM Security Guardium Key Lifecycle Manager Administrator Password field is empty.

Explanation:

This message is displayed when the IBM Security Guardium Key Lifecycle Manager Administrator Password field is empty or invalid.

System action:
Installation cannot continue until you correct the error.

User response:
Specify a correct value and try again.

CTGKM9063E The Application Server Administrator Password field is empty or invalid.

Explanation:
This message is displayed when the Application Server Administrator Password field is empty or invalid.

System action:
Installation cannot continue until you correct the error.

User response:
Specify a correct value and try again.

CTGKM9064E The Encryption Key Manager Property File field is empty.

Explanation:
This message is displayed when the Encryption Key Manager Property File field is empty.

System action:
Installation cannot continue until you correct the error.

User response:
Specify a value.

CTGKM9065E The IBM Security Guardium Key Lifecycle Manager Administrator Confirm Password field is empty.

Explanation:
User has not specified the password confirmation value.

System action:
Installation cannot continue until you correct the error.

User response:
Specify a value and try again.

CTGKM9066E IBM Security Guardium Key Lifecycle Manager Application Port Number is empty.

Explanation:
This message is displayed when the IBM Security Guardium Key Lifecycle Manager Application Port Number field is empty.

System action:
Installation cannot continue until you correct the error.

User response:
Specify a value and try again.

CTGKM9067E The password for Database Administrator field is empty.

Explanation:
This message is displayed when the password field for Database Administrator field is empty.

System action:
Installation cannot continue until you correct the error.

User response:
Specify a value and try again.

CTGKM9068E The password for keystore is empty.

Explanation:
You must specify a password for the keystore.

User response:
Specify a password for the keystore and try again.

CTGKM9069E The user name {0} or password is not valid.

Explanation:
The operation requires a valid user name and password.

System action:
The operation fails.

User response:
Specify a valid user name and password. Then, try again.

CTGKM9070E The credentials could not be validated at the moment.

Explanation:
The specified credentials might be incorrect.

System action:
Installation cannot continue until you correct the error.

User response:
Refer to the WebSphere Application Server logs for more information and correct the problem.

CTGKM9071E The WebSphere Application Server instance could not be started.

Explanation:
The WebSphere Application Server instance could not be started.

System action:
Installation cannot continue until you correct the error.

User response:
Refer to the WebSphere Application Server logs for more information and correct the problem.

CTGKM9072E The DB2 installation details file {0} cannot be found.

Explanation:
The DB2 instance data file was not found.

System action:
Installation cannot continue until you correct the error.

User response

Ensure that the following files exist.

Windows systems
The `db2srcit.txt` file under the following directories:

- `C:\sklmtemp`
- `C:\sklm41properties`

Linux and AIX® systems
Check for the missing properties in the `db2unix.srcit` file under the following directories:

- `/sklmtemp`
- `/root/sklm41properties`

CTGKM9073E DB2InstallResponseUpdater requires minimum {0} parameters. Only had {1} parameters.

Explanation:
The installer is not passing in the correct parameters for a binary which it is trying to execute. This is an internal error which cannot be resolved by the Installation Manager.

System action:
The installation fails.

User response:
Identify the package that has the issue by looking at the installation history. In Installation Manager, click **File** > **Installation History**. In console mode, enter S on the main menu to select "View Installation History". Contact IBM customer support.

CTGKM9074E File {0} does not exist.

Explanation:
A binary which the installer is executing is attempting to access a file which does not exist. This is an internal error which cannot be resolved by the Installation Manager.

System action:
The installation fails.

User response:
Identify the package that has the issue by looking at the installation history. In Installation Manager, click **File** > **Installation History**. In console mode, enter S on the main menu to select "View Installation History". Contact IBM customer support.

CTGKM9075E File {0} is not writable.

Explanation:
A binary which the installer is executing is attempting to modify a read-only file. This is an internal error which cannot be resolved by the Installation Manager.

System action:
The installation fails.

User response:
Identify the package that has the issue by looking at the installation history. In Installation Manager, click **File** > **Installation History**. In console mode, enter S on the main menu to select "View Installation History". Contact IBM customer support.

CTGKM9076E The specified path for existing DB2 installation is not valid.

Explanation:
The specified path for existing DB2 installation is incorrect.

System action:
Installation cannot continue until you correct the error.

User response:
Specify the correct path. Then, try again.

CTGKM9077E The response file object is null.

Explanation:
You must specify the response file.

User response:
Specify a value. Then, try again.

CTGKM9078E {0} requires {1} parameters. Only had {2} parameters.

Explanation:
The installer is not passing in the correct parameters for a binary which it is trying to execute. This is an internal error which cannot be resolved by the Installation Manager.

System action:
The installation fails.

User response:
Identify the package that has the issue by looking at the installation history. In Installation Manager, click **File** > **Installation History**. In console mode, enter S on the main menu to select "View Installation History". Contact IBM customer support.

CTGKM9079E The file/folder specified by the path {0} does not exist on the file system.

Explanation:
A binary which the installer is executing is attempting to access a file which does not exist. This is an internal error which cannot be resolved by the Installation Manager.

System action:

The installation fails.

User response:
Identify the package that has the issue by looking at the installation history. In Installation Manager, click **File** > **Installation History**. In console mode, enter S on the main menu to select "View Installation History". Contact IBM customer support.

CTGKM9080E IBM Tivoli Key Lifecycle Manager server version {0} has been detected on the system. This version cannot be upgraded to v2.6. To continue with the installation, upgrade IBM Tivoli Key Lifecycle Manager to version {1}.

Explanation:
The installation fails.

System action:
Installation cannot continue until you correct the error.

User response:
Upgrade IBM Tivoli Key Lifecycle Manager to the supported version.

CTGKM9081E Error while executing the command {0}

Explanation:
There was a problem when running the specified command.

System action:
The installation fails.

User response:
Check the Installation Manager log files and take necessary corrective actions. Then, try again.

CTGKM9082E Cannot find a running process for the server.

Explanation:
There was a problem when trying to stop WebSphere Application Server.

System action:
The installation fails.

User response:
Manually start the server and try again.

CTGKM9083E Unable to determine the install location for WebSphere Application Server v9.

Explanation:
The Installer could not identify the location of WebSphere Application Server, version 9.0.

System action:
The installation fails.

User response:
Uninstall Installation Manager and rerun the installation process.

CTGKM9084E Invalid DB2 installation details file. Cannot find an entry for {0}.

Explanation:
The details present in the DB2 instance data file is incorrect.

System action:
The installation fails.

User response

Windows systems
Check for the missing properties in the `db2srcit.txt` file under the following directories:

- `C:\sklmtemp`
- `C:\sklm41properties`

Linux and AIX systems
Check for the missing properties in the `db2unix.srcit` file under the following directories:

- `/sklmtemp`
- `/root/sklm41properties`

CTGKM9085E The DB2 installation details file {0} cannot be found.

Explanation:
The DB2 instance data file was not found.

System action:
Installation cannot continue until you correct the error.

User response

Ensure that the following files exist.

Windows systems
The `db2srcit.txt` file under the following directories:

- `C:\sklmtemp`
- `C:\sklm41properties`

Linux and AIX systems
Check for the missing properties in the `db2unix.srcit` file under the following directories:

- `/sklmtemp`
- `/root/sklm41properties`

CTGKM9086E No WebSphere Application Server installation found in the registry.

Explanation:

Instance of the WebSphere Application Server, version 8.5 was not found in the install registry.

System action:
Installation cannot continue until you correct the error.

User response:
Uninstall Installation Manager and rerun the installation program.

CTGKM9087E Could not load data from the ports definition file {0}.

Explanation:
The ports definition file for the WebSphere Application Server could not be read.

System action:
Installation cannot continue until you correct the error.

User response:
Clean up any existing installation and rerun the installation program.

CTGKM9088E The ports definition file {0} does not contain the required keys - {1}.

Explanation:
Details in the ports definition file is incorrect.

System action:
Installation cannot continue until you correct the error.

User response:
Clean up any existing installation and rerun the installation program.

CTGKM9089E Could not get the key store file location.

Explanation:
Keystore location was not found.

System action:
Installation fails.

User response:
Make sure that the Tivoli Key Lifecycle Manager database is up and running and rerun the installation program.

CTGKM9090E IBM DB2 and IBM WebSphere Application Server offerings must be selected for IBM Security Guardium Key Lifecycle Manager installation to proceed. Go back to the previous screen and select IBM DB2 V11.1 and IBM WebSphere Application Server V9.0 offerings.

Explanation:
The details that you specified are incorrect.

User response:
Specify the correct values.

CTGKM9091E IBM DB2 and IBM WebSphere Application Server offerings associated with IBM Security Guardium Key Lifecycle Manager must be selected for IBM Security Guardium Key Lifecycle Manager uninstallation to proceed. Go back to the previous screen and select IBM DB2 V11.1 and IBM WebSphere Application Server V9.0 offerings.

Explanation:
The details that you specified are incorrect.

System action:
Uninstallation cannot continue until you correct the error.

User response:
Specify the correct values.

CTGKM9092E One or more prerequisites failed to meet the requirements. The report is given below.

Explanation:
The prerequisite requirements for the installation are not met. All prerequisites must be satisfied for the installation.

System action:
Installation cannot continue until you correct the error.

User response:
Take corrective actions to meet the requirements. Then, try again.

CTGKM9093E None of the drives on the system has the required space ({0}) to install the product.

Explanation:
The minimum space to install the product is not available in the system.

System action:
Installation cannot continue until you correct the error.

User response:
Increase the amount of space available on the specified drive to the minimum required. Then, try again.

CTGKM9094E Unable to read the prerequisite scanner results.

Explanation:
The prerequisite output file was not found after Prerequisite Scanner is run.

System action:
Installation cannot continue until you correct the error.

User response:

Rerun the installation without deleting any files from the system.

CTGKM9095E The password does not meet the operating system password policy requirements. Check the minimum password length and password complexity requirements.

Explanation:
The password the you specified violates the password rules.

System action:
The password is not updated on the server.

User response:
Check the minimum password length, password complexity and password history requirements.

CTGKM9096E The credentials provided for WebSphere Application Server Administrator is not valid.

Explanation:
Incorrect credentials are specified for the WebSphere Application Server administrator.

System action:
Installation cannot continue until you correct the error.

User response:
Specify the correct user name and password for WebSphere Application Server administrator. Then, try again.

CTGKM9099E WebSphere Administrator credentials are required to proceed with uninstallation.

Explanation:
The user name or password for WebSphere Application Server is not specified or incorrect.

User response:
Specify the correct user name and password for the WebSphere Application Server administrator and then try again.

CTGKM9100E DB2 installation details file {0} cannot be found

Explanation:
The DB2 instance data file was not found.

System action:
Installation cannot continue until you correct the error.

User response

Ensure that the following files exist.

Windows systems
The `db2srcit.txt` file under the following directories:

- `C:\sklmtemp`
- `C:\sklm41properties`

Linux and AIX systems
Check for the missing properties in the `db2unix.srcit` file under the following directories:

- `/sklmtemp`
- `/root/sklm41properties`

CTGKM9101E The path "<Variable formatSpec="{0}">VALUE_0</Variable>" is either on a network file system or not writable. Select a local file system path for installation.

Explanation:
The installation is attempted on a location that is not on the local hard disk of the system.

System action:
Installation cannot continue until you correct the error.

User response:
Change the installation path and specify a local path on the system.

CTGKM9102E The path "<Variable formatSpec="{0}">VALUE_0</Variable>" is either on a network drive or not writable. Select a local drive for installation.

Explanation:
The installation is attempted on a location that is not on the local hard disk of the system.

System action:
Installation cannot continue until you correct the error.

User response:
Change the installation path and specify a local path on the system.

CTGKM9103E Unable to find the location of prerequisite scanner tool.

Explanation:
Location of Prerequisite Scanner was not found.

System action:
Installation cannot continue until you correct the error.

User response:
Rerun the installation without deleting any files from the system.

CTGKM9104E Required permission is not available on {0} to perform the installation.

Explanation:

You might not have the read, write, and execute permissions to the installation directories.

System action:
Installation cannot continue until you correct the error.

User response:
Verify permissions to the installation directories for performing installation of each component of IBM Security Guardium Key Lifecycle Manager and try the installation again.

CTGKM9105E Java TEMP location and environment variable TEMP location are different. The location paths must be same.

Explanation:
Java temporary directory location and the TEMP environment variable location might not be same.

System action:
Installation cannot continue until you correct the error.

User response:
Ensure that the location paths for Java temporary directory and the TEMP environment variable are same.

CTGKM9106E Error in uninstalling IBM Security Guardium Key Lifecycle Manager. Check the installer log files for details.

System action:
You cannot uninstall until you correct the error.

User response:
Take corrective actions and try again.

CTGKM9107E {0} environment variable not set OR is null, please set the environment variable to proceed further.

Explanation:
The `TEMP` (Windows) or `TMPDIR` (Linux) environment variable is not set or empty.

System action:
Installation cannot continue until you correct the error.

User response:
Ensure that the environment variable value is set to a valid temporary directory, for example `TMPDIR=/tmp`.

CTGKM9108E The port FCM_PORT_NUMBER {0} that is required for DB2 installation is in use. Release the port to continue with the installation.

System action:
Installation cannot continue until you correct the error.

User response:
Release the port by stopping the application, which is using this port. Then, try the installation again.

CTGKM9109E Port number {0} is in conflict with `FCM_PORT_NUMBER` value. Choose a different port and try again.

System action:
Installation cannot continue until you correct the error.

User response:
Specify a valid port, which does not cause a port conflict. Then, try the installation again.

CTGKM9110W IBM Security Guardium Key Lifecycle Manager is being installed on an unsupported operating system.

User response:
Ensure you are running on a supported operating system. For a list of supported operating systems, see the IBM Security Guardium Key Lifecycle Manager product documentation in IBM Knowledge Center.

CTGKM9111W The product installer cannot detect the operating system on the host.

User response:
Ensure you are running on a supported operating system. For a list of supported operating systems, see the IBM Security Guardium Key Lifecycle Manager product documentation in IBM Knowledge Center.

CTGKM9112E You must specify different port numbers.

Explanation:
Port numbers that are mentioned on the form must not be the same.

System action:
Installation cannot continue until you correct the error.

User response:
Ensure that the port numbers are different and try the installation again.

CTGKM9113E The port {0} is in conflict with DB2 port. Choose a different port to proceed with the installation.

Explanation:
Selected value for the port is in conflict with the DB2 port.

System action:
Installation cannot continue until you correct the error.

User response:
Specify a free port and try the installation again.

CTGKM9114E Ports 1441, 5696, 3801 are reserved for other services.

Specify a different port to continue with the installation.

Explanation:
Selected value for the port is reserved for another service.

System action:
Installation cannot continue until you correct the error.

User response:
Check to ensure that the port value is not reserved for any other services.

CTGKM9115E Unable to create the port definition property file.

Explanation:
Unable to modify the `portsDef.props` file with the port number settings for WebSphere Application Server profile creation.

System action:
Installation cannot continue until you correct the error.

User response

Check for the following information and try the installation:

- Check that you have the read, write, and execute permission to the TEMP (Windows) and $HOME (Linux) location.
- Ensure that the property file with the same name does not exist.
- Ensure that the file is not in use by another program.

CTGKM9116E The password must be different from the user name. Specify a different password.

Explanation:
A password cannot be the same as your user name or user ID.

System action:
Installation cannot continue until you correct the error.

User response:
Enter a different password that conforms to the rules and try again.

CTGKM9117E The version detected is not supported for IBM Security Guardium Key Lifecycle Manager inline migration.

User response:
Ensure that you are migrating a supported version. For a list of supported versions for inline migration, see the IBM Security Guardium Key Lifecycle Manager product documentation in IBM Knowledge Center.

KMIP messages

These are the KMIP error messages.

CTGKP0001E Check failed. Nothing to return in response.

Explanation:
Internal error. Cannot return response for Check operation.

System action:
Cannot process the KMIP message.

Administrator response:
Check the audit logs. Correct the problem and retry the operation.

CTGKP0002E Check failed, no unique identifier to return in the response.

Explanation:
Internal error. Cannot return response for the Check operation.

System action:
Cannot process the KMIP message.

Administrator response:
Check the audit logs. Correct the problem and retry the operation.

CTGKP0003E Field *VALUE_0* not specified.

Explanation:
Field is not specified in the KMIP message that was received.

System action:
Cannot process the message.

Administrator response:
Correct the input and retry the operation.

CTGKP0004E Structure *VALUE_0* is empty.

Explanation:
Field is expected to have a valid value in the KMIP message that was received.

System action:
Cannot process the message.

Administrator response:
Correct the input and retry the operation.

CTGKP0005E Structure *VALUE_0* is null.

Explanation:
Structure is not specified in the KMIP message that was received.

System action:
Cannot process the message.

Administrator response:
Correct the input and retry the operation.

CTGKP0006E Header tag is neither Response nor Request. The tag is *VALUE_0*.

Explanation:
Incorrect tag received in the KMIP message header.

System action:
Cannot process the message.

Administrator response:
Correct the input and retry the operation.

CTGKP0007E Protocol Version : major: *VALUE_0* , minor *VALUE_0* is not supported.

Explanation:
Incorrect protocol version received in the KMIP message header.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0008E Message is neither Response nor Request. The message tag is *VALUE_0*.

Explanation:
Cannot parse the message. An incorrect KMIP message tag was received.

System action:
Cannot process the message.

Administrator response:
Correct the input and retry the operation.

CTGKP0009E Message is not a single structure. Type of message object is *VALUE_0*.

Explanation:
Cannot parse the message. Received an incorrect KMIP message type.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0010E Message that was received is null.

Explanation:
Nothing to parse. Received no KMIP message.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0011E Vendor extension tag value is incorrect.

Explanation:
Cannot parse the KMIP message. Received an incorrect tag value.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0012E Operation is pending but no asynchronous correlation value was specified.

Explanation:
Cannot proceed. Received no asynchronous correlation value in the KMIP message.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0014E Following values must all be specified: *VALUE_0*.

Explanation:
Cannot proceed. Required values are missing in the message.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0015E Following value must be specified: *VALUE_0*.

Explanation:
Cannot proceed. A required value is missing in the KMIP message.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0016E Parsed object is null.

Explanation:
Cannot proceed. No object is in the KMIP message payload.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0101E **Attribute name *VALUE_0* not recognized.**

Explanation:
Cannot parse. An unrecognized attribute name is in the KMIP message.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0102E **Attribute value of attribute *VALUE_0* is not a single field.**

Explanation:
Cannot parse. Received multiple values for single-valued attribute in a KMIP message.

System action:
The requested operation fails.

Administrator response:
See the KMIP specification for details. Correct the input and retry the operation.

CTGKP0103E **Attribute value *VALUE_0* is not of type *VALUE_1*.**

Explanation:
Cannot parse. The data type of the attribute value is incorrect.

System action:
The requested operation fails.

Administrator response:
See the KMIP specification for more information. Correct the input and retry the operation.

CTGKP0105E ***VALUE_0* for attribute *VALUE_1* is not of type *VALUE_2*.**

Explanation:
Cannot parse. The data type of the attribute value is incorrect. See the KMIP specification for more information.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0106E **KMIPDataStructure is not a primitive attribute.**

Explanation:
Cannot parse. The data type of the attribute is incorrect.

System action:
The requested operation fails.

Administrator response:
See the KMIP specification for more information. Correct the input and retry the operation.

CTGKP0107E **At least one field must be specified for ObtainUsageAllocation.**

Explanation:
All fields cannot be null for ObtainUsageAllocation operation. Incorrect parameters were received.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0108E **Either bytes or object values must be specified.**

Explanation:
Combination of input parameters received for obtaining Usage Allocation operation is incorrect. Either bytes or object values must be specified.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0301E **No credential structure found inside the authentication structure.**

Explanation:
Unexpected error. Asked for credential but the authentication structure did not contain credentials. This might occur because of incorrect input parameters.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP0302E **Cryptographic algorithm not specified and not contained within key value.**

Explanation:
Cannot parse the message. Cryptographic algorithm cannot be determined.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0303E **Cryptographic length not specified and not contained within key value.**

Explanation:

Cannot parse the message. Cryptographic length cannot be determined.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0304E Key value received but key format type not defined.

Explanation:
Cannot parse the message. The required value for key format attribute is not specified.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0305E Data type *VALUE_0* not valid for field key value.

Explanation:
Cannot parse the message. An incorrect type for key value is specified. Expected OCTET_STRING data type.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0306E Tag value for the field *VALUE_0* is incorrect.

Explanation:
Cannot parse the message. A tag value is not correct for the specified field.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0307E Vendor extension key value *VALUE_0* not supported.

Explanation:
Cannot parse the message. The value for the specified field is not correct.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0308E Transparent key format type *VALUE_0* not recognized.

Explanation:
Cannot parse the message. The value for the specified field is not correct.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0309E One of the following must be present: (Private Exponent), (P and Q) or (Prime Exponent P and Prime Exponent Q).

Explanation:
Cannot parse the message. The value for the RSA private key is not correct.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0310E Value not valid for the parameter *VALUE_0*, received *VALUE_1*.

Explanation:
The parameter value in the message is either not specified or not valid.

System action:
The requested operation failed.

Administrator response:
Correct the input and retry the operation.

CTGKP0311E Transparent symmetric key not specified.

Explanation:
The parameter value in the request is not specified or not valid.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0401E End of file reached. No more bytes to read.

Explanation:
Cannot read the message completely. No more bytes are available.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP0402E Error reading *VALUE_0* bytes.

Explanation:
Cannot read the message completely because the expected number of bytes cannot be read.

System action:

The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP0403E Number of bytes to read *VALUE_0* is more than maximum size *VALUE_1*.

Explanation:
Cannot read the message because the value for bytes is not valid.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0404E Tried to skip *VALUE_0* bytes, could only skip *VALUE_1*.

Explanation:
Cannot read the message because there are not enough bytes to skip.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0405E Maximum level of nesting reached *VALUE_0*.

Explanation:
Cannot parse the message. Reached the maximum level of nesting.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0406E Unknown type *VALUE_0*.

Explanation:
Cannot parse the message because an object in the message is an unknown type.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0407E For the object *VALUE_0*, received length of *VALUE_1* that is not valid.

Explanation:
Cannot parse the message. The length of the data type is not valid for the specified object type.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0408E Structure length *VALUE_0* is not a multiple of 8.

Explanation:
Cannot parse the message because the length of the structure is not a multiple of 8.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0409E Structure length *VALUE_0* is a negative number.

Explanation:
Cannot parse the message because the length of the structure is not a valid number. Expected a positive number that is a multiple of 8.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0410E Padding length *VALUE_0* bytes is more than maximum size *VALUE_1* bytes.

Explanation:
Cannot parse the message because padding length received is not valid.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0411E *VALUE_0* length of *VALUE_1* bytes is more than maximum size *VALUE_2* bytes.

Explanation:
Cannot parse the message because the length of the object in the message is not valid.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0601E KMIPDataTypeObject is null.

Explanation:
Internal error. Cannot encode the message, received null value for KMIPDataTypeObject.

System action:
The requested operation fails.

Administrator response:

Check the audit logs. Correct the input and retry the operation.

CTGKP0602E Structure length *VALUE_0* is not a multiple of *VALUE_1* .

Explanation:
Cannot encode the message. The length of the structure is not valid.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0603E Unknown type *VALUE_0*.

Explanation:
Cannot encode the message. The type of the object in the message is unknown.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0701E KLMAdapter classname is null.

Explanation:
Internal error. KLMAdapter classname should be set with installation.

System action:
The requested operation fails.

Administrator response:
Try restarting the server. If the probem continues, you might need to contact IBM Support.

CTGKP0702E Only request messages can be processed.

Explanation:
Received the message with a type other than request.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation

CTGKP0703E The method processBatchItem returned null.

Explanation:
Internal error. Cannot proceed because an unexpected error ocurred.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry.

CTGKP0704E Cannot authenticate the client.

Explanation:
Did not receive a client certificate for authentication. The client certificate is required to be sent on TLS communication on operations other than Query.

System action:
The request fails.

Administrator response:
Make sure a client sends a certificate that IBM Security Guardium Key Lifecycle Manager trusts and retry the request.

CTGKP0801E Certificate type *VALUE_0* not supported.

Explanation:
Cannot proceed because a value in the message is not valid.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry.

CTGKP0802E Key representation not supported.

Explanation:
Cannot proceed because a value in the message is not valid.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry.

CTGKP0803E Could not create managed object.

Explanation:
Cannot proceed. An internal error occurred.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry.

CTGKP0804E Key format type must be opaque for secret data objects. Value not valid: *VALUE_0*

Explanation:
Cannot proceed. A value in the message is not valid.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry.

CTGKP0805E Template must have at least one attribute.

Explanation:
Cannot proceed. The template must have at least one attribute.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry.

CTGKP0901E Error constructing KMIP Attribute object. Exception is: *VALUE_0*

Explanation:
Cannot proceed. An internal error occurred.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry.

CTGKP0902E Error getting KMIPConfig object.

Explanation:
Cannot proceed. An internal error occurred.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry.

CTGKP0903E Error in KMIP Attribute object. Exception is: *VALUE_0*

Explanation:
Cannot proceed. An internal error occurred.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry.

CTGKP0904E Unique identifier of the *VALUE_0* is null.

Explanation:
Cannot proceed. An unexpected error occurred.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry.

CTGKP0905E Must specify either Common Key Specification, or both Private and Public Key Specifications.

Explanation:
Cannot proceed. The input is not valid.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry.

CTGKP0906E More than two unique identifiers specified.

Explanation:
Cannot proceed. Received a value that is not valid.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry.

CTGKP0907E No templates or attributes specified.

Explanation:
Cannot process this message. This operation requires either a template name or at least one attribute.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry.

CTGKP0908E *VALUE_0* payloads do not exist.

Explanation:
Cannot proceed. An unexpected error occurred.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry.

CTGKP0909E Unable to create KMIP message object.

Explanation:
Cannot proceed. An unexpected error occurred.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry.

CTGKP0910E At most, two unique identifiers can be specified.

Explanation:
Cannot proceed. Received a value that is not valid.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry.

CTGKP0911E Error in KMIP Attribute object. Exception is *VALUE_0*

Explanation:
Cannot proceed. Received a value that is not valid.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the problem and retry.

CTGKP0912E No attribute names returned.

Explanation:
Cannot proceed. An internal error occurred.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the problem and retry.

CTGKP0913E At least one attribute name must be requested.

Explanation:
Cannot proceed. The input is not valid.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry.

CTGKP0914E Error in ManagedObject.

Explanation:
Internal error. Received null or not valid value for ManagedObject.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0915E Object tag does not match the type of cryptographic object returned.

Explanation:
Internal error. The tag does not match the type of the object returned.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0916E Either byte or object count must be specified.

Explanation:
Cannot process the GetUsageAllocation request. Specify either byte or object count.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0917E No attributes specified for Locate request.

Explanation:
Cannot process Locate request. Specify at least one attribute.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0918E Error constructing KMIP Attribute object. Exception is *VALUE_0*.

Explanation:
Internal error. Cannot process the request.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP0919E No attributes specified on *VALUE_0*.

Explanation:
Cannot process the request. Specify at least one attribute.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0920E Multiple values for field *VALUE_0* received.

Explanation:
Cannot process the request. Received multiple values of the field. However, the field is single-valued.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0921E Unrecognized field *VALUE_0*.

Explanation:
Cannot process the request. The field is not recognized.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0922E Received null object in a Put request.

Explanation:
Cannot process the Put request. There must be an object in the message.

System action:
The requested operation fails.

Administrator response:

Correct the input and retry the operation.

CTGKP0923E Replaced unique identifier must be specified if Put function is Replace.

Explanation:
Cannot process the Put request.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP0924E Error constructing managed object. Error is *VALUE_0*.

Explanation:
Cannot process the Put request. The input is not valid.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP0925E Error constructing KMIP Attribute Object. Error is *VALUE_0*.

Explanation:
Cannot process the request. An internal error occurred.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP0926E *VALUE_0* not specified.

Explanation:
Cannot process the Put request. One of the required fields is not specified.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP0927E All Query functions are null.

Explanation:
Cannot process the Query request. Specify at least one Query function.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP0928E Unique Identifier of the object is null.

Explanation:
Internal error. Could not get a response to send back to the client. Cannot process the request.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry the operation. If the problem persists, call IBM Support.

CTGKP0929E If Revocation Reason is Compromised, Compromise OccurrenceDate must be specified.

Explanation:
Cannot process the request. The input is not valid.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP0930E Compromise Occurrence Date not specified and Revocation Reason is Compromised.

Explanation:
Internal error. Cannot process the request. The input might not be valid.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP0931E Error in constructing date-time object while processing *VALUE_0*. Error is *VALUE_0*

Explanation:
Cannot process the request because one of the KMIP attributes cannot be constructed from the specified input.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP0932E Error in Revoke request fields. Error is *VALUE_0*

Explanation:
Cannot process the request. The input is not valid.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP0933E Certificates and Unique Identifiers are both null, nothing to validate.

Explanation:
Cannot process the request. The input is not valid.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP0934E Error constructing KMIP Certificate object. Error is *VALUE_0*

Explanation:
Cannot process the request. The input is not valid.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP0935E Certificates and Unique Identifiers are both null.

Explanation:
Cannot process the request. The input is not valid.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP1001E *VALUE_0* is null.

Explanation:
Internal error occurred. One of the required objects is null. TLS initialization failed.

System action:
KMIP TLS Listener is not available to accept KMIP requests.

Administrator response:
Check the audit logs. If you intend to use KMIP, ensure that your TLS configuration properties are defined properly and that the KMIP TLS port does not conflict with the port numbers that other applications use. If the problem persists, call IBM Support.

CTGKP1005E Error initializing KMIP Servlet.

Explanation:
Internal error occurred. There is a problem in initialization.

System action:
Server is not able to accept KMIP requests.

Administrator response:
Check the audit logs. Correct the problem and retry. If the problem persists, call IBM Support.

CTGKP1007E KMIP is supported on TLS protocol only.

Explanation:
KMIP supports TLS protocol only. Http(s) is not supprted.

System action:
The request fails.

Administrator response:
Retry sending the request using TLS protocol.

CTGKP2001E Element size *VALUE_0* bytes is larger than maximum size *VALUE_1* bytes.

Explanation:
Cannot parse the message. The size is not valid.

System action:
Cannot process the request.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP2002E Unable to read the response.

Explanation:
Cannot send the response to the client. An internal error occurred.

System action:
Cannot process the request.

Administrator response:
Check the audit logs. Correct the problem and retry. If the problem persists, call IBM Support.

CTGKP2003E Byte array to send as a response message is null.

Explanation:
Cannot send the response to the client. An internal error occurred.

System action:
Cannot process the request.

Administrator response:
Check the audit logs. Correct the problem and retry. If the problem persists, call IBM Support.

CTGKP2004E Unable to connect to server. Error is *VALUE_0*

Explanation:

Cannot connect to the server.

System action:
Cannot send the request to the server.

Administrator response:
Check the audit logs. Make sure the hostname and the port number of the server is correctly specified and retry. If the problem persists, call IBM Support.

CTGKP3001E Multiple values for *VALUE_0* field received.

Explanation:
Multiple values received for the field, which is not a multi-valued attribute. Specify a single value for this field.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP3002E Message is null.

Explanation:
Cannot parse the message. The input is not valid.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP3003E Message is not a response. Message is *VALUE_0*

Explanation:
Cannot parse the message. The message type is not valid.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP3004E No payload in batch item.

Explanation:
Cannot parse the message. The input is not valid.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP3005E More than one batch item in the message.

Explanation:
Cannot process the message. The input is not valid.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP3006E Field in *VALUE_0* is unknown *VALUE_1*.

Explanation:
Cannot parse object. Received an unrecognized field.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP3007E Can only get response payload from response messages.

Explanation:
Internal error. Tried to get response payload from a request message.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Take appropriate action and retry.

CTGKP3008E Result status is pending but there are no batch items in the message *VALUE_0*.

Explanation:
Internal error. The result status is not correct when no batch items remain.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Take appropriate action and retry.

CTGKP3009E The result status is unknown in this message *VALUE_0*.

Explanation:
Internal error. The result status is not correct. Cannot send the response to the client.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Take appropriate action and retry.

CTGKP3010E Error reading result status from this response *VALUE_0*.

Explanation:
Internal error. The result status is not correct when no batch items remain. Cannot send the response to the client.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Take appropriate action and retry.

CTGKP3011E No batch items in the message.

Explanation:
Cannot process the message. Received no batch items.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Take appropriate action and retry.

CTGKP3012E The result status cannot be recognized.

Explanation:
Internal error. Received a result status that is not valid. Cannot send the response to the client.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Take appropriate action and retry.

CTGKP3013E Error occurred while creating KMIPCheckException. Error is *VALUE_0*.

Explanation:
Internal error occurred. Cannot process KMIP Check operation.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Take appropriate action and retry.

CTGKP3014E Operation failed. Error is *VALUE_0*.

Explanation:
Internal error occurred.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Take appropriate action and retry.

CTGKP3015E The result status cannot be recognized.

Explanation:
Internal error. Cannot send the response to the client because the result status is not correct.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Take appropriate action and retry.

CTGKP3016E Cryptographic algorithm is null.

Explanation:
No value for the cryptographic algorithm in the message.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP3017E Year must be 4 characters.

Explanation:
Cannot process the message. The value for the year field is not valid.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP3018E Month must be between 1 and 12.

Explanation:
Cannot process the message. The value for the month field is not valid.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP3019E Day must be between 1 and 31.

Explanation:
Cannot process the message. The value for the day field is not valid.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP3020E Hour must be between 0 and 24.

Explanation:
Cannot process the message. The value for the hour field is not valid.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP3021E Minute must be between 0 and 59.

Explanation:
Cannot process the message. The value for the minute field is not valid.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP3022E Second must be between 0 and 59.

Explanation:
Cannot process the message. The value for the second field is not valid.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP3023E Unknown cryptographic algorithm *VALUE_0*

Explanation:
Cannot process the message. A cryptographic algorithm parameter that is not valid.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP3024E Unsupported key format *VALUE_0*

Explanation:
Cannot process the message. The key format parameter is not valid.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP3025E Wrapping method *VALUE_0* is not supported.

Explanation:
Cannot process the message. The wrapping method in the message is not supported.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP3026E The MAC/Signature verification failed.

Explanation:
Cannot process the message. The signature verification failed.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP3027E Block cipher mode *VALUE_0* only supported for AES algorithm.

Explanation:
Cannot process the message. The block cipher mode is not valid.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP3028E Block cipher mode is null.

Explanation:
Cannot process the message. The block cipher mode is missing in the message.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP3029E Block cipher mode *VALUE_0* only supported for algorithm *VALUE_1*.

Explanation:
The block cipher mode in the message is not supported for this algorithm.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP3030E The key value type *VALUE_0* of the encryption key is not supported.

Explanation:
Cannot process the message. The input is not valid.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP3031E The wrapping key itself cannot already be wrapped.

Explanation:
Cannot process the message. The wrapping key is not valid.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP3032E Unique Identifier mismatch: query does not match response.

Explanation:

Internal error. The unique identifier in the query and response do not match.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP3033E No Last Changed Date attribute for specified cryptographic object.

Explanation:
Operation fails because the specified cryptogrpahic object does not have the last changed date attribute.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP3034E Parameter *VALUE_0* is not a Boolean value.

Explanation:
Cannot process the message. Specify the parameter as a Boolean value.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP3035E Parameter *VALUE_0* not defined.

Explanation:
Cannot process the message because the parameter is not specified.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP3036E Parameter *VALUE_0* is empty.

Explanation:
Cannot process the message because the parameter is not specified.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP4001E Zero or more than one attributes in container.

Explanation:
Internal error. Cannot get single-valued attribute because there are zero or more than one attribute present in the container.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP4002E Template name cannot be null.

Explanation:
Cannot process the message. An unexpected error occurred.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP4003E Error adding *VALUE_0* attribute. Error is *VALUE_1*.

Explanation:
Cannot process the message. An internal error occurred.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP4004E The index can only be set when there is exactly one attribute in the container.

Explanation:
Cannot process the message. An unexpected error occurred.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP4005E No index specified for *VALUE_0* attribute value and index zero already used.

Explanation:
Cannot process the message. The parameters in the message are incorrect.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP4006E This method cannot be batched with other requests.

Explanation:

Cannot process the message. The input is not valid.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP4007E Length of Wrapping Key ID array must be the same as the array for unique identifiers.

Explanation:
Cannot process the message. An internal error occurred.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP4008E List of unique identifiers is null.

Explanation:
Cannot process the message. The input parameter is not valid.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Correct the input and retry the operation.

CTGKP4009E Response was asynchronous although the Asynchronous Indicator is false.

Explanation:
Cannot process the message. The input parameter is not valid.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP4010E Thread.sleep() interrupted. Error is *VALUE_0*

Explanation:
Cannot process the message. An internal error occurred.

System action:
The requested operation fails.

Administrator response:
Check the audit logs. Take appropriate action and retry. If the problem persists, call IBM Support.

CTGKP4011E No templates or attributes specified.

Explanation:
Cannot process a message. The input parameter is not valid.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP4012E Attribute name is null.

Explanation:
Cannot process a message. The input is not valid.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP4013E Attribute value is null.

Explanation:
Cannot process a message. An internal error occurred.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP4014E Unexpected response payload received.

Explanation:
Cannot process a message. An internal error occurred.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP4015E Error parsing returned object in the response.

Explanation:
Cannot process a message. An internal error occurred.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP4016E Error getting attributes from the response.

Explanation:
Cannot process a message. An internal error occurred.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP4017E No attributes in the message.

Explanation:
Cannot process a message. An internal error occurred.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP4018E Unique identifier in the response does not match the one in the request.

Explanation:
Cannot process a message. An internal error occurred.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP4019E Asynchronous correlation value does not match. Result was *VALUE_0*.

Explanation:
Cannot process a message. An internal error occurred.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP4020E Error encoding request message *VALUE_0*.

Explanation:
Cannot process a message. An internal error occurred.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP4021E Reply is not a KMIP response.

Explanation:
Cannot process a message. An internal error occurred.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP4022E The response is empty even though batching is not used.

Explanation:
Cannot process a message. An internal error occurred.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP4023E Error while wrapping object. Error is *VALUE_0*.

Explanation:
Cannot process a message. An internal error occurred.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP4024E Error while unwrapping object. Error is *VALUE_0*.

Explanation:
Cannot process a message. An internal error occurred.

System action:
The requested operation fails.

Administrator response:
Correct the input and retry the operation.

CTGKP4025E Error connecting to the remote server. Error is *VALUE_0*.

Explanation:
Cannot process a message, unexpected error occurred.

System action:
The requested operation fails.

Administrator response:
Ensure that the remote server is up and running.

Index