Encryption

Symmetric Keys, Certificates & TDE

GRIP ON SQL

2024-11-23

Contents

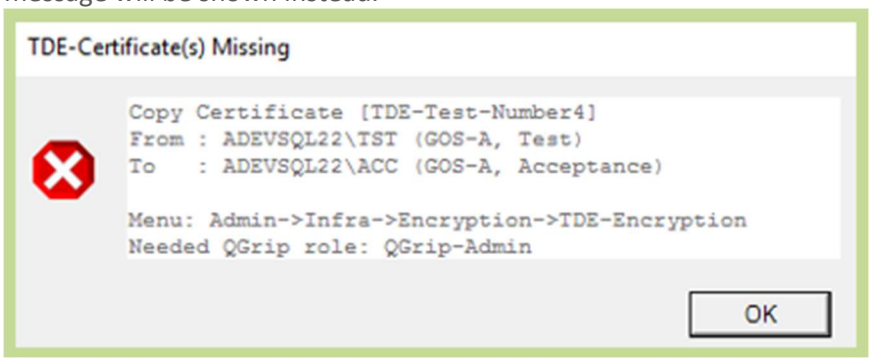
1 Introduction

QGrip can be used to manage encryption objects like symmetric keys and certificates. QGrip also makes it really easy to administer databases protected by TDE (Transparent Data Encryption).

Symmetric Keys of type MASTER KEY and certificates 'encrypted by master key' can easily be created, copied and dropped using the QGrip-UI.

QGrip Backup Encryption
When 'Symmetric Keys and Certificates' has been enabled and configured, you can enable QGrip Backup Encryption which makes it really easy to encrypt your backup files. QGrip will administer the MASTER KEYs and used Certificates and make sure they are created whenever needed for a restore or clone.

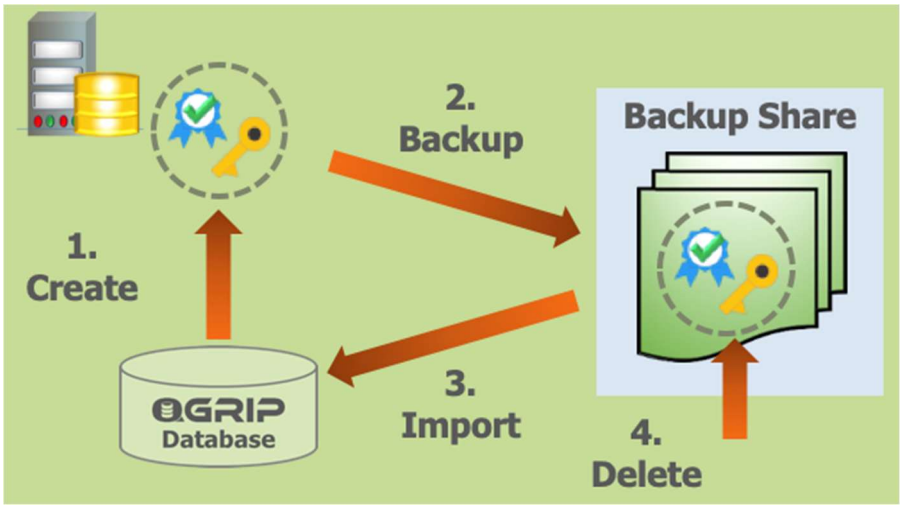
TDE Databases
When 'Symmetric Keys and Certificates' has been enabled and configured, QGrip will make it easier to administer TDE protected databases. QGrip will administer the MASTER KEYs and used TDE-Certificates and will tell the user which TDE-Certificate(s) need to be copied prior to a restore or clone. The missing TDE-Certificates will not automatically be created/copied by QGrip but an error message will be shown instead.



The missing TDE-Certificates can easily be Copied to the destination Instances using the QGrip-UI.

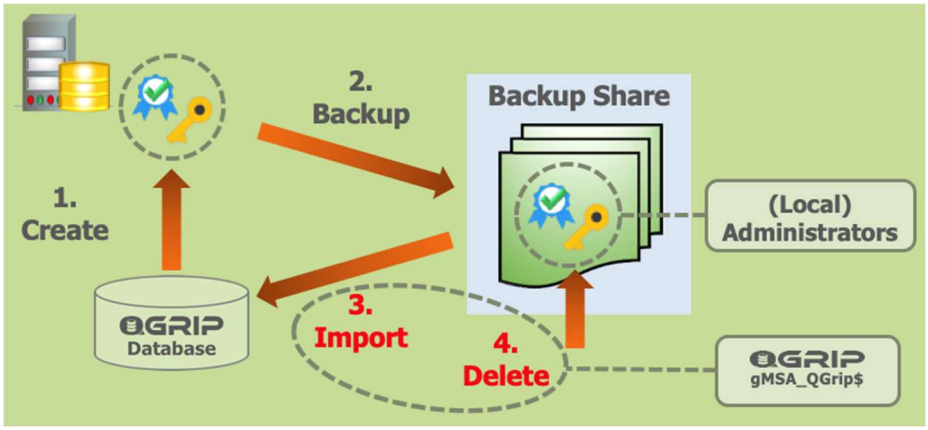
But there is a price to pay: the QGrip System Account must be added to the local Administrators group on all Backup Share servers as explained in the next section.

2 Why member Administrators group?

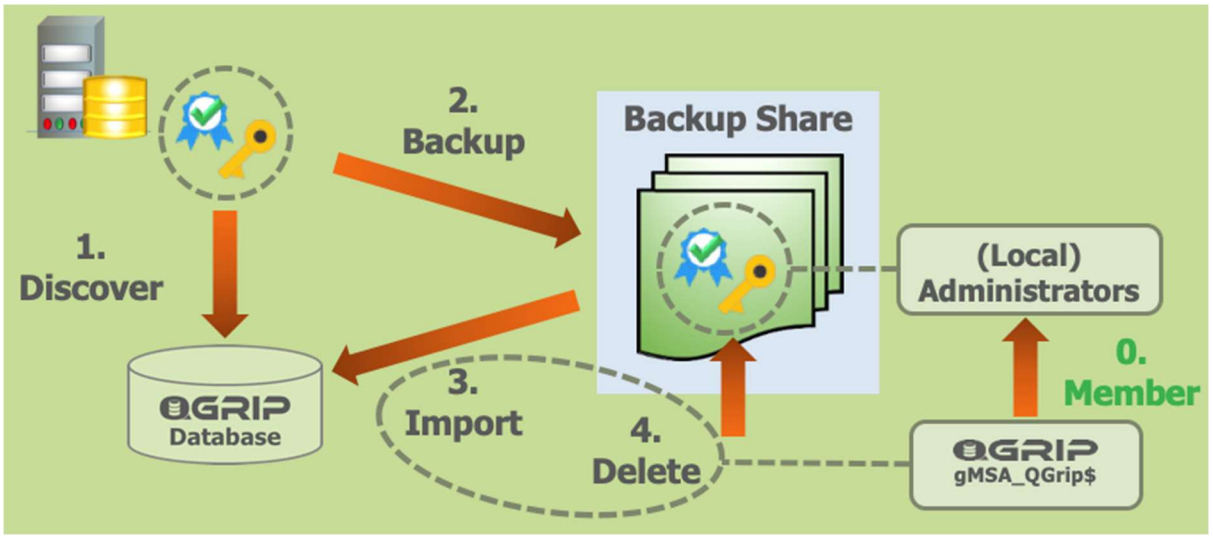


The process when Symmetric Keys and Certificates are created is as follows:

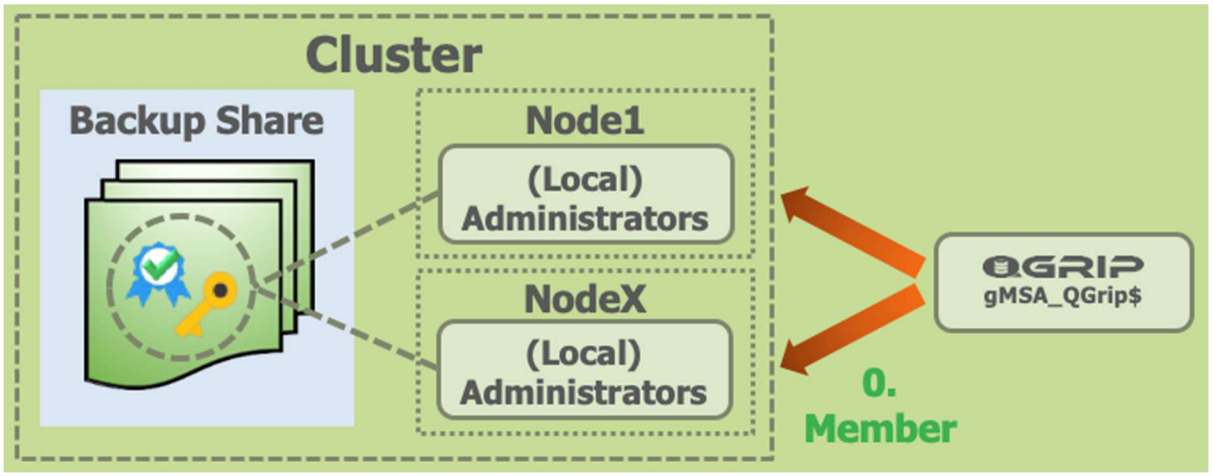
1. Create the objects on the Instance.
2. Backup the object to a file on the backup share.
3. Import the object file into the QGrip database.
4. Delete the file from the backup share.



The problem is that when SQL Server creates the backup file (2.), only the current DB Engine account and the (local) Administrators group are given permissions on the file. When QGrip tries to Import and/or Delete the file, the action will fail.

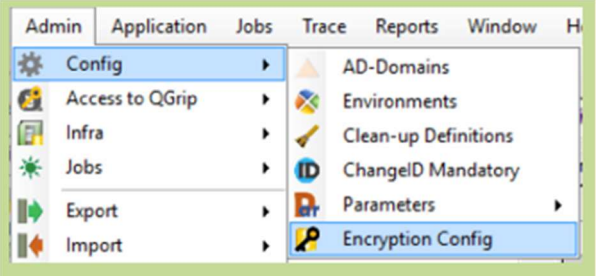


To automatically let QGrip import and delete these files from the backup share, the QGrip System Account must be added to the (local) Administrators group on all Backup Share servers.



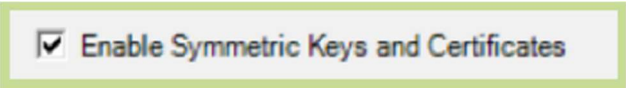
If the Backup Share is on a failover cluster, the QGrip System Account must be added as a member on all nodes in the cluster to prevent issues in case of a failover.

3 Enable Symmetric Keys, Certificates and TDE

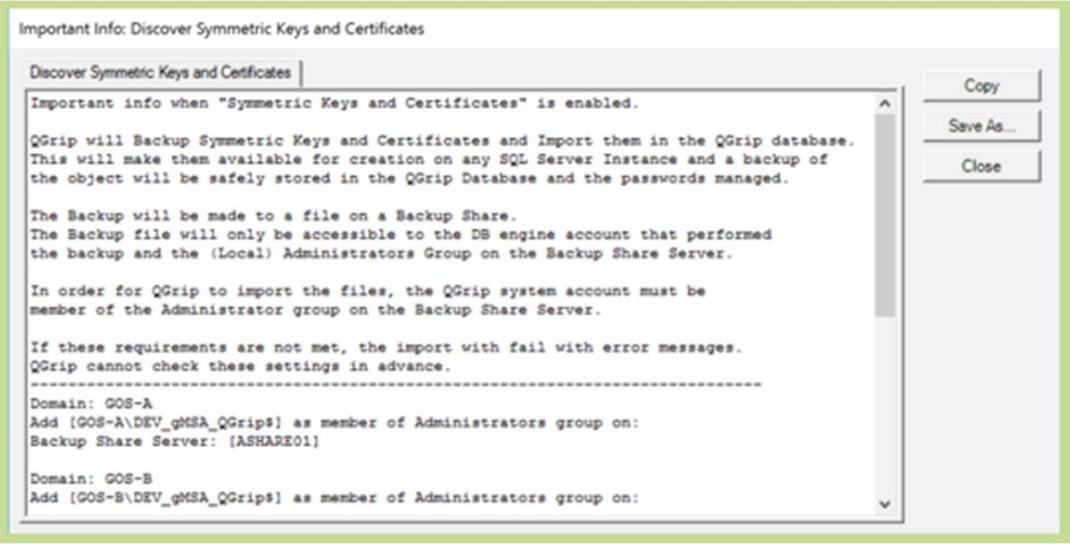


QGrip will not only look at Symmetric Keys and Certificates created via QGrip, already existing objects will be collected during the Discover process. To enable and configure, follow the steps in this section.

3.1 Encryption Config



Open the Encryption Config in QGrip (Admin->Config->Encryption Config) and check the 'Enable Symmetric Keys and Certificates' checkbox.



A popup with instructions will appear. Read it carefully. The instructions are the same as in this section but the names of all backup share servers are also listed.

Schedule the frequency of the Accessibility job that will run to check that the 'QGrip System Accounts' are Local Administrators on the Backup Share Servers.

3.2 Add QGrip System Account as member Administrator Groups

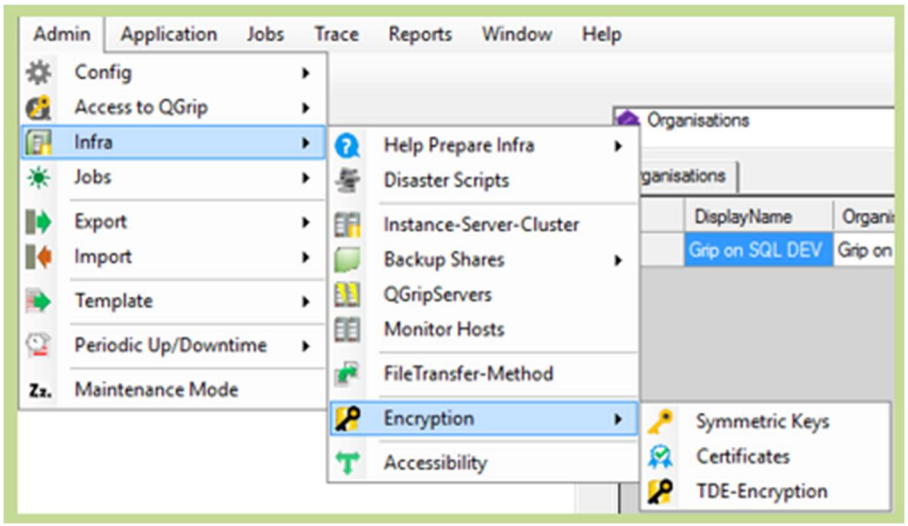
For each Backup Share Server listed in the popup in the last section, add the QGrip System Account to the local Administrators group on the server.

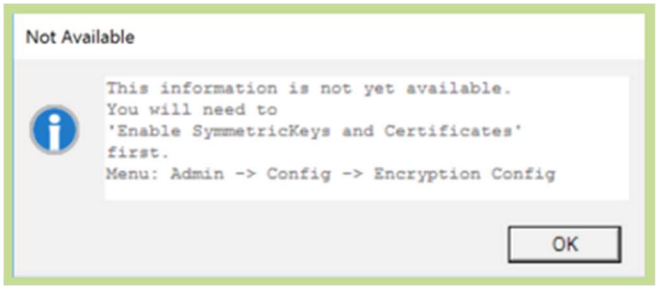
A detailed description of how you manually can add a member to the local Administrators group can be found in the Appendix:

- Add member: Local Administrator Group

Group Policies
If your organisation is using policies for the (Local) Administrators Groups, make sure that the QGrip System Account is added to the group Policy. Remember that the QGrip System Account is gMSA (Group Managed Service Account) and some Active Directory features do not apply to gMSA accounts.

4 Encryption

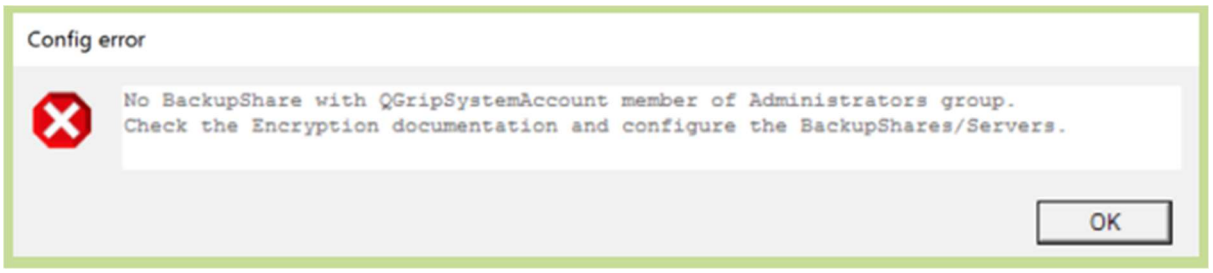




The Symmetric Keys, Certificate and TDE-Encryption module will not be available as long as it has not yet been enabled.

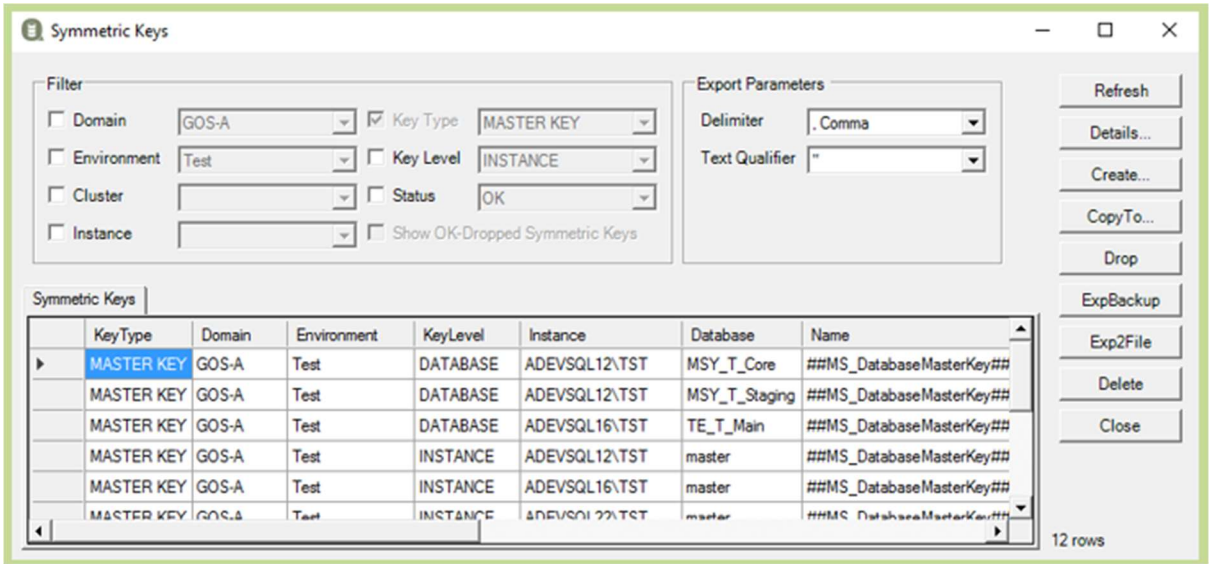
Temporary Status:
Queued For CopyTo
Queued For Create
Queued For Drop
Queued For Backup
Queued For Verify-Password

All actions done on Symmetric Keys, Certificates, TDE-Certificates and TDE-Databases are done via the RemoteJob Queue with as Job Type 'SymmetricKey', 'Certificate' and 'TDEDatabase'. When a request has been placed on the Queue to be executed, the object will get a Temporary Status. As long as it has that status, the object cannot be changed in the QGrip-UI. When your request, let say Create Symmetric Key has been processed, you will receive a personal message.



If you try to start an action and there is no Backup Share available for Backup/Import, you will receive the error message above.

5 Symmetric Keys

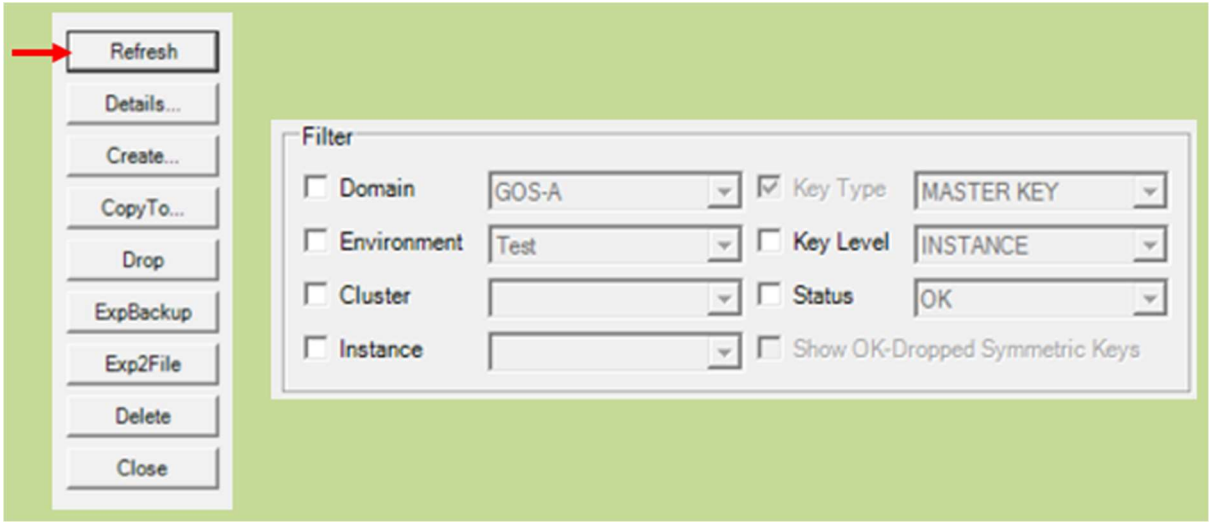


The Symmetric Keys main window is compact with a lot of different buttons that will be explained here below.

The status of a Symmetric Key depends on the availability of information and if QGrip is able to backup and import the Key to QGrip.

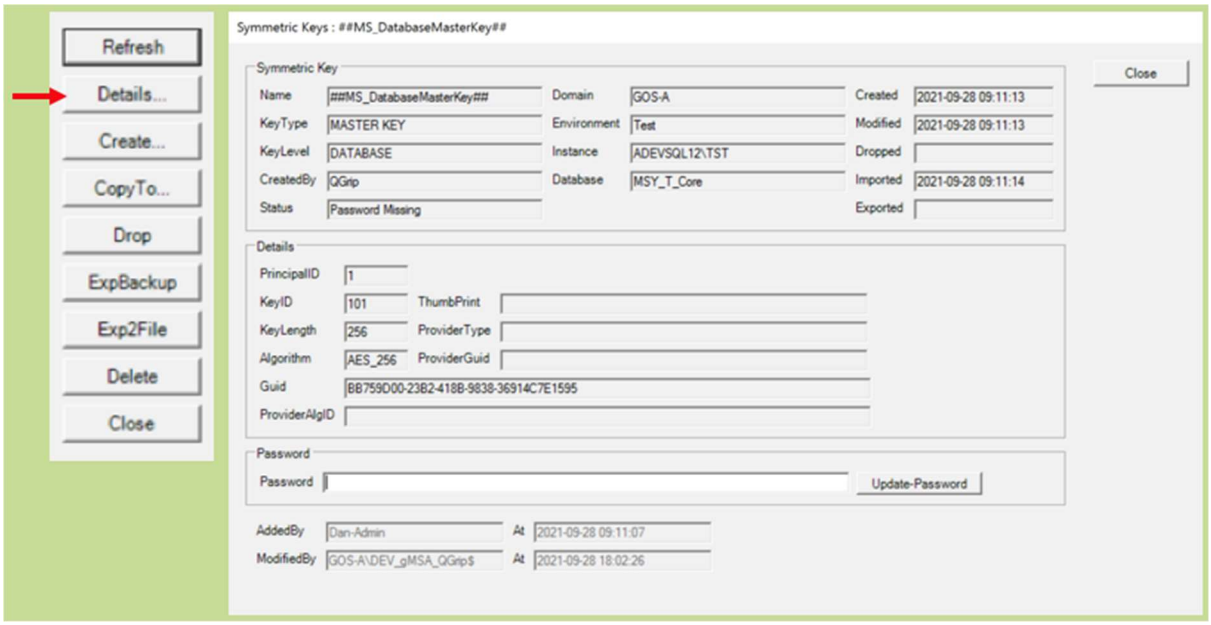
Status	Remark
Password Missing	As long as the password is missing, QGrip will not be able to backup and import the Symmetric Key (file) to QGrip.
Import Missing	Password is available but Backup/Import fails because of missing Authorisation on the Backup Share server (QGrip System Account member of Administrators group)
OK	Password is available and import to QGrip completed.
OK-Dropped	Password is available and import to QGrip completed but the Symmetric Key has been dropped on the Instance.

5.1 Symmetric Key: Refresh



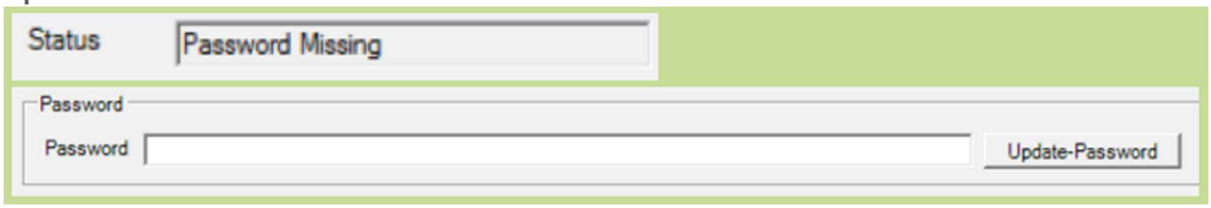
When the Refresh button is pushed, the data in the tab page will be refreshed according to the setting in the Filter. There is no automatic refresh when the filter is changed.

5.2 Symmetric Key: Details



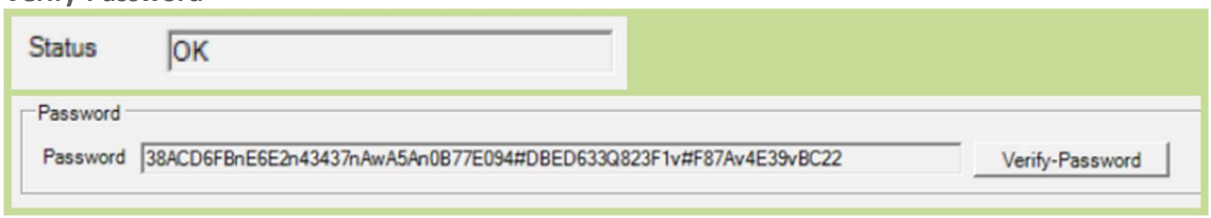
When the Details button is pushed, the details of the current row in the tab page will be shown.

Update-Password



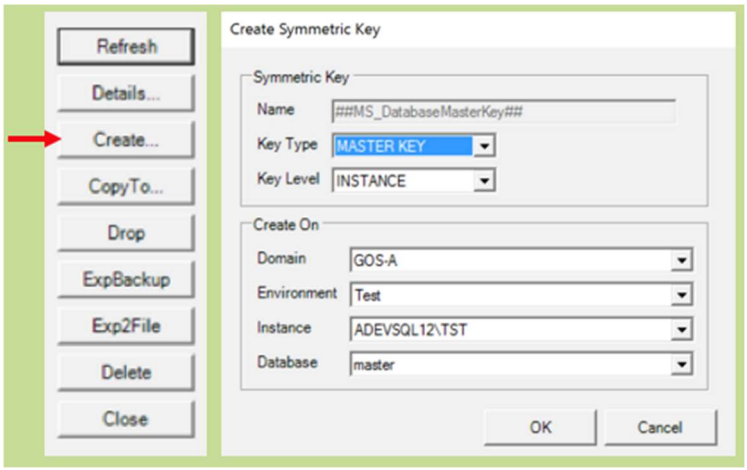
If the status of the Symmetric Key is 'Password Missing' you can add the password if you have it and hit the 'Update-Password' button. QGrip will save the password its database and push a 'Verify-Password' job on the Queue. If the password you entered is incorrect, the status will go back to 'Password Missing'. If it is correct, a backup and import of the Symmetric Key will be done and the status changed to 'OK'.

Verify-Password



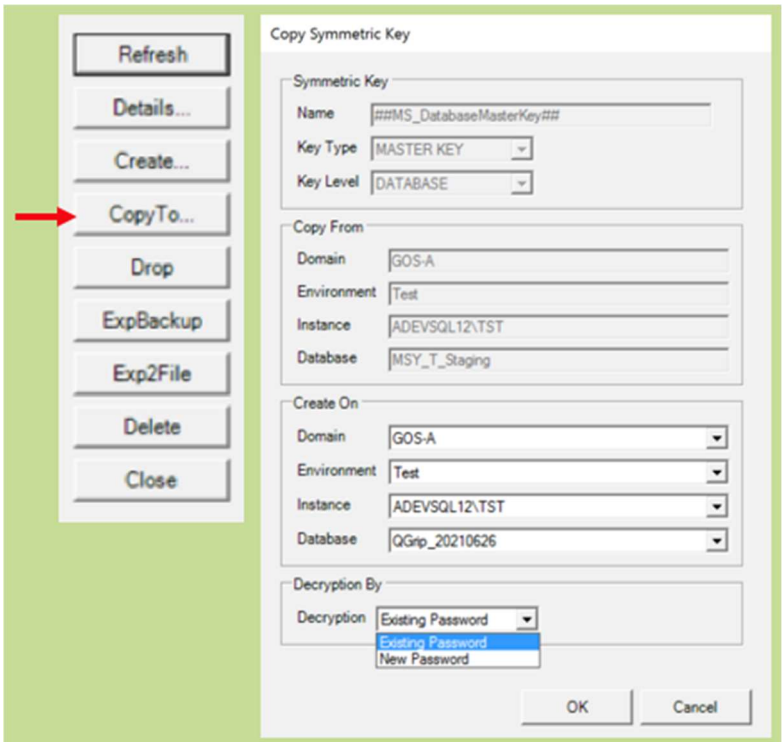
If the status of the Symmetric Key is 'OK' you can hit the 'Verify-Password' button to check that the password is still correct. If the password is incorrect, the Symmetric Key will get the status 'Password Missing'. The backup/import of the key have now also been removed as they are no longer valid and the backup/import useless.

5.3 Symmetric Key: Create



With the Create button, you can create a new Symmetric Key (of type MASTER KEY). Depending on the Key Level (INSTANCE/DATABASE) it can be created on a user database or in the master. A password of length 64 will be generated for the key and saved in the QGrip database.

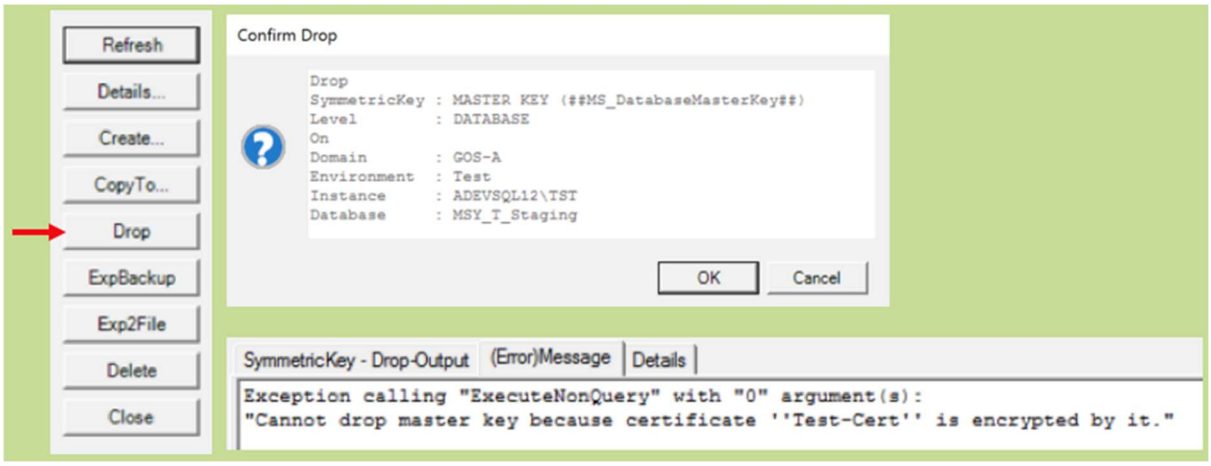
5.4 Symmetric Key: CopyTo



With the CopyTo button, you can copy an existing Symmetric Key to another database. You will only be able to copy Key Level to the same Key Level (master -> master or user database -> user database). You have the option to choose Decryption by Existing or New Password. If New Password is chosen, a password of length 64 will be generated.

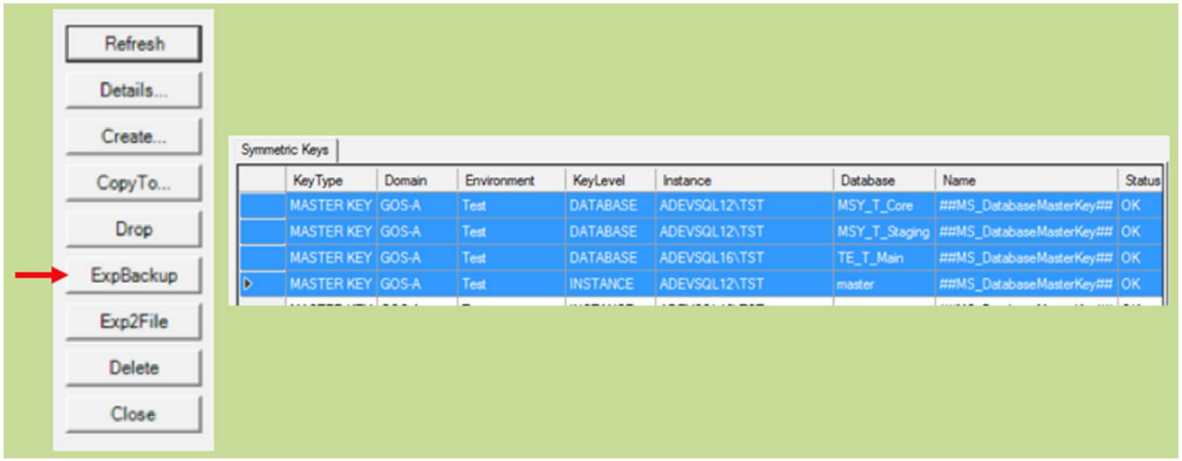
5.5 Symmetric Key: Drop

The difference between Drop and Delete is that Drop will drop the Symmetric Key on the Instance. The Symmetric Key info, including Backup/Import will still remain in the QGrip database.

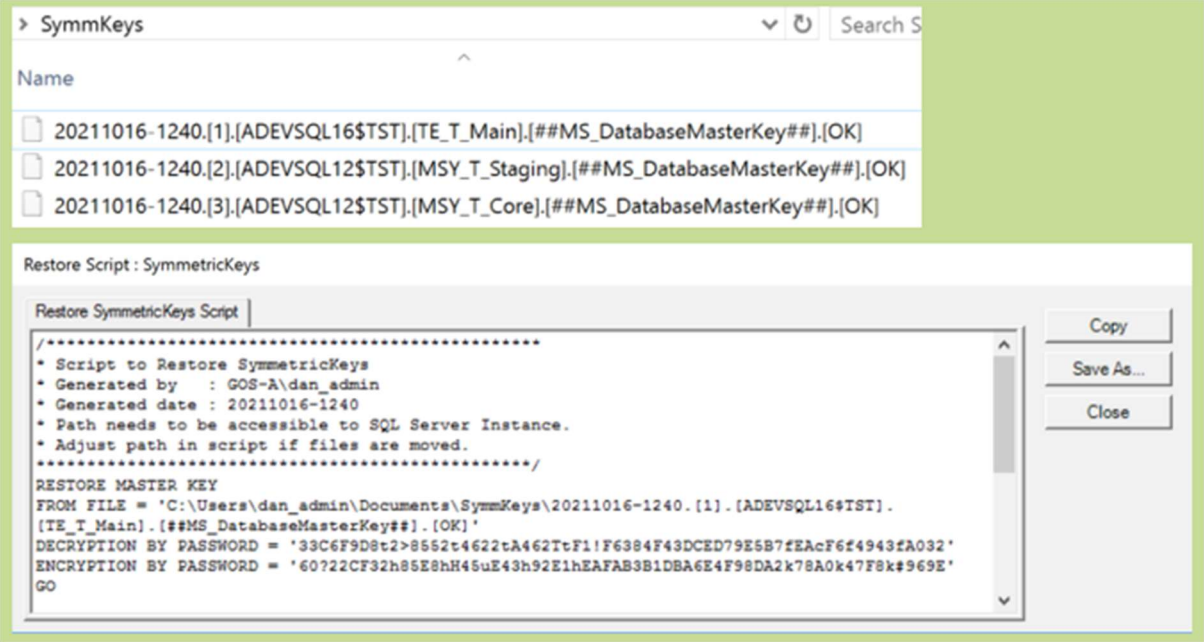


Drop the Symmetric Key related to the current row in the tab-page on the remote Instance. The information in QGrip will remain but the Symmetric Key will get the status: OK-Dropped
It is possible that the drop fails if the Symmetric Key has been used for encryption of other objects. In that case, the status will not change and no alterations will be made to the Symmetric Key.

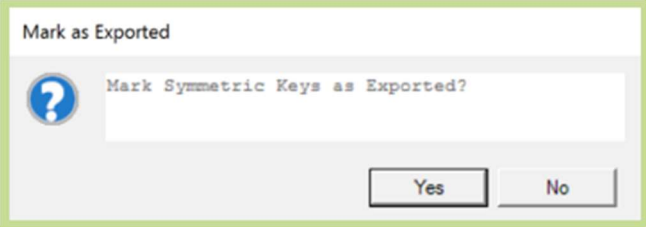
5.6 Symmetric Key: ExpBackup



To export Backups Imported to QGrip, select the Symmetric Keys in the tab-page and hit the ExpBackup button. The status of the Symmetric Keys must be ‘OK’ or OK-Dropped’. You will be asked to select to save a file. We advise you to create a new directory because as all the files will be saved there.

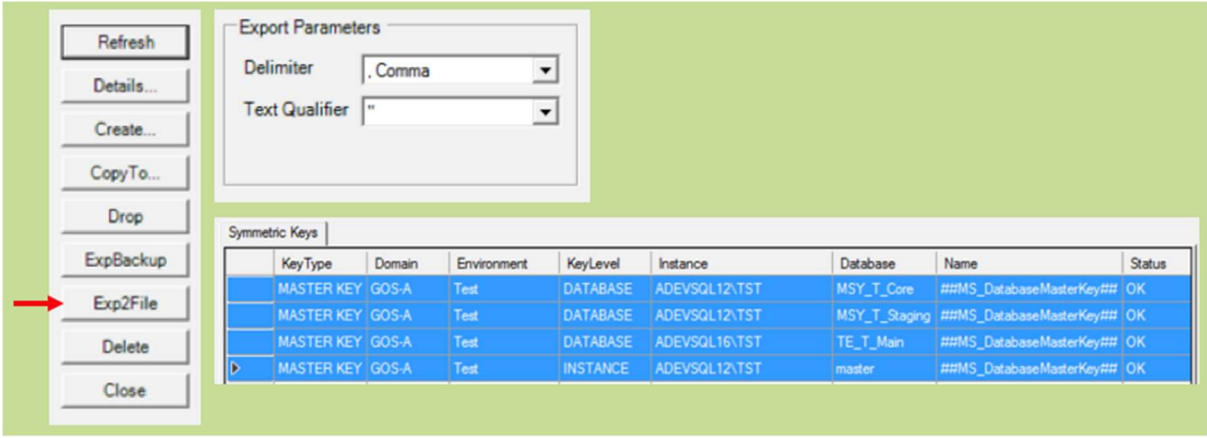


The files to (re-)create the Symmetric Keys have been placed in the directory. A popup with a script to create the objects will be shown. This popup will contain passwords and you should pay attention to where you save it.



You will receive a question if you want to mark the Symmetric Keys as exported or not. This is important for the Delete that will be explained in one of the following sections. Only records with status ‘OK-Dropped’ and ‘Marked as Exported’ can be deleted from the QGrip administration.

5.7 Symmetric Key: Exp2File

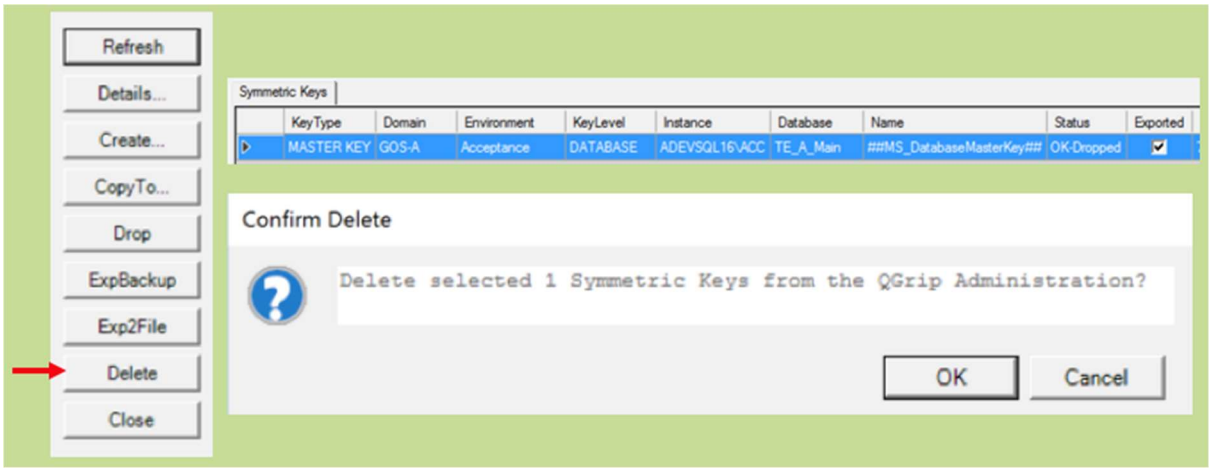


The difference between ‘ExpBackup’ and ‘Exp2File’ is that ‘Exp2File’ saves the selected rows in the tab-page to a csv-file, including the Symmetric Key passwords. The ‘Export Parameters’ will be used

to configure the file. The file will contain passwords and you should pay attention to where you save it.

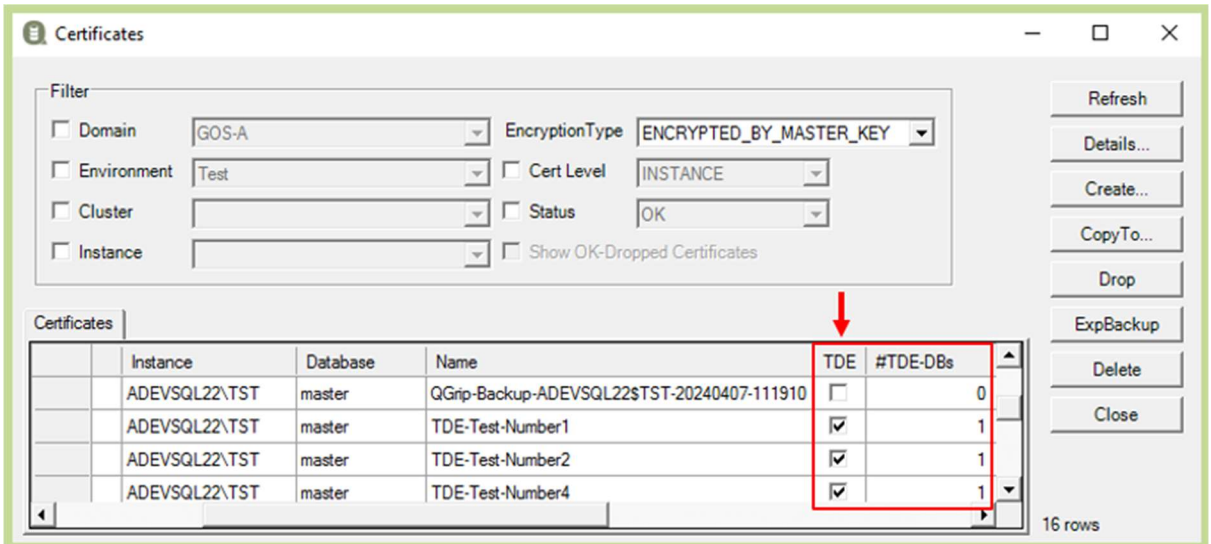
5.8 Symmetric Key: Delete

The difference between Delete and Drop is that Delete will delete the Symmetric Key from the QGrip administration. Delete is only possible if the Symmetric Key has status 'OK-Dropped' and has been marked as 'Exported'.

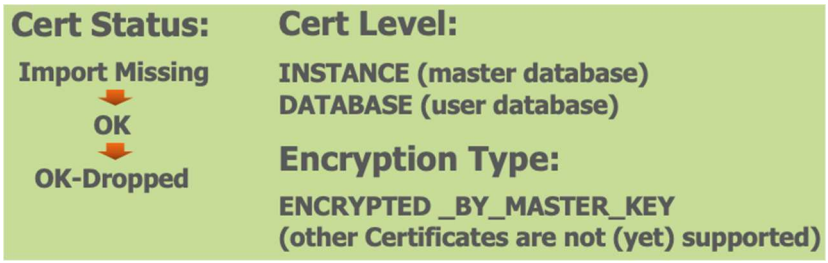


Select the Symmetric Keys you want to delete from the QGrip administration and hit Delete. QGrip will check that the records have the right status and that they have been marked as 'Exported'.

6 Certificates



The Certificates main window is compact with a lot of different buttons that will be explained here below.



The status of a Certificate depends on the availability of information and if QGrip is able to backup and import the Certificate to QGrip. QGrip will only allow 'Actions' on Certificates that have encryption type 'ENCRYPTED_BY_MASTER_KEY'. If another Encryption type is selected in the filter, the action buttons will be disabled.

Status	Remark
Import Missing	Certificate is available but Backup/Import fails because of missing Authorisation on the Backup Share server (QGrip System Account member of Administrators group). If the Cert Level is DATABASE and the Password of the Symmetric Key (MASTER KEY) is not in QGrip, the status will also be Import Missing.
OK	Password is available and import to QGrip completed.
OK-Dropped	Import to QGrip completed but the Certificate has been dropped on the Instance.

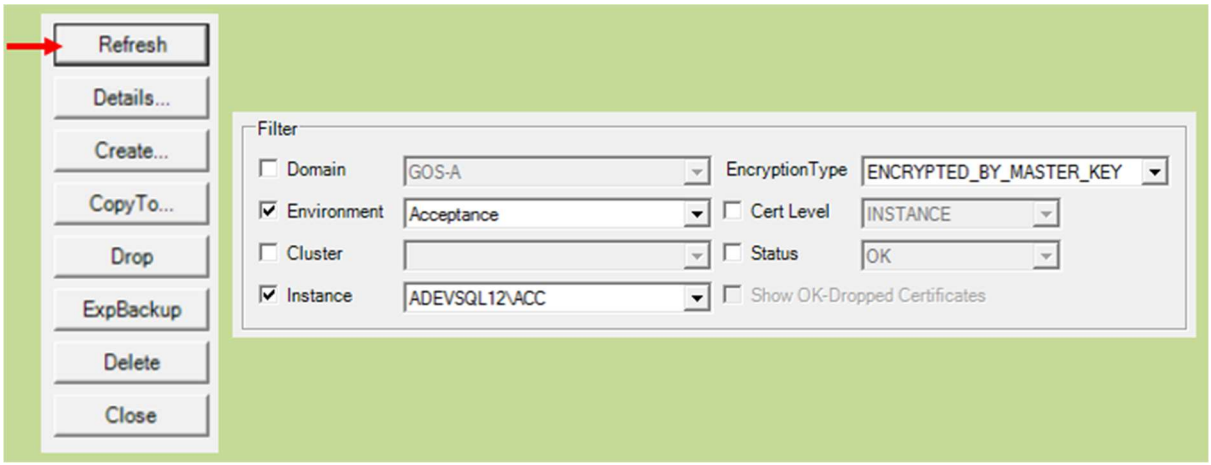
Symmetric Key Automatically created

Whenever needed, if a certificate is created or copied to a new Instance/Database, QGrip will automatically create the needed Symmetric Key (MASTER KEY) to complete the request.

TDE Certificates

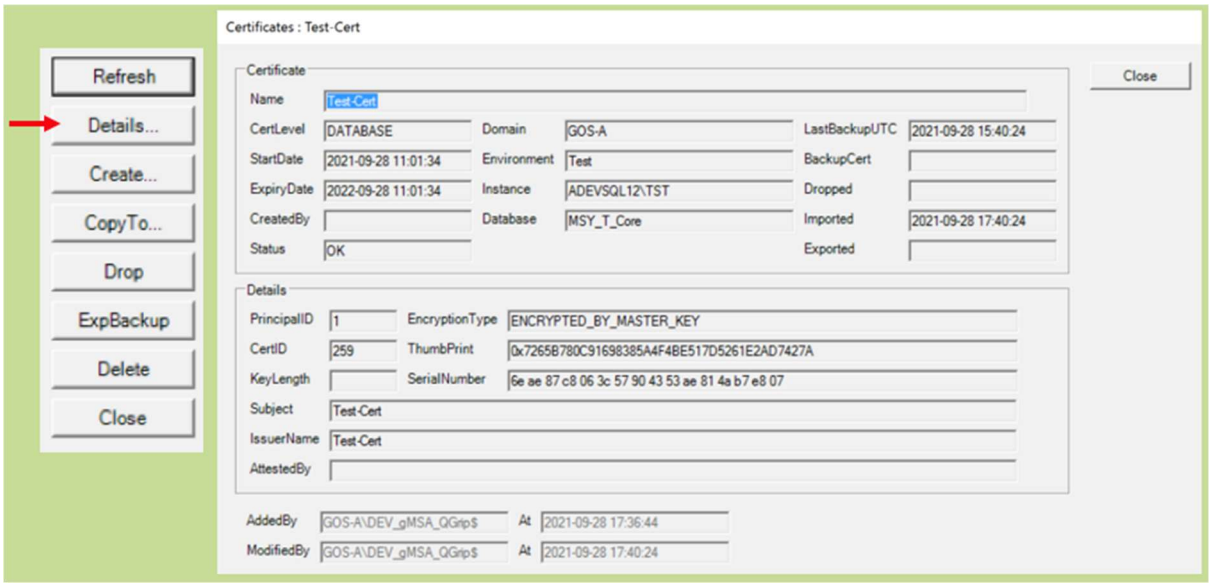
The column TDE indicates if a Certificate is (a potential) TDE Certificate. The TDE certificates are show in the Certificate window above but should only be edited in TDE-Encryption window described in the next section.

6.1 Certificate: Refresh



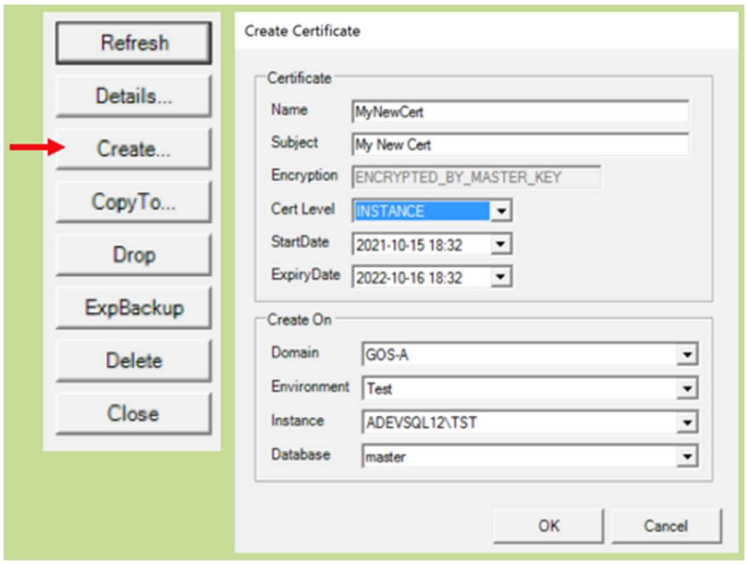
When the Refresh button is pushed, the data in the tab page will be refreshed according to the setting in the Filter. There is no automatic refresh when the filter is changed.

6.2 Certificate: Details



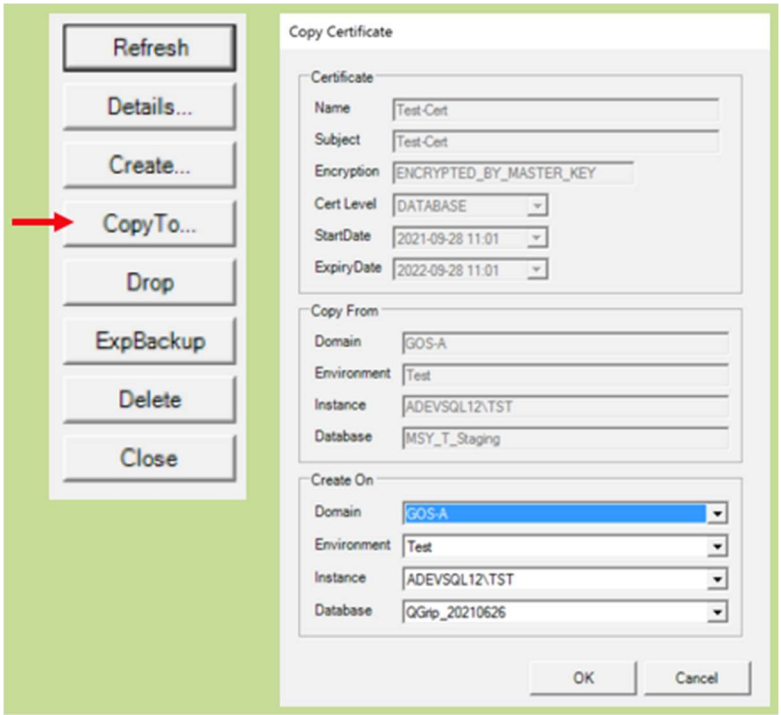
When the Details button is pushed, the details of the current row in the tab page will be shown.

6.3 Certificate: Create



With the Create button, you can create a new Certificate. Depending on the Key Level (INSTANCE/DATABASE) it can be created on a user database or in the master. You will need to enter a name and subject. The Start Date is automatically set to yesterday. This is to prevent warnings as certificates are using UTC time.
TDE-Certificates MUST be created in the TDE-Encryption window and not in the Certificates window!

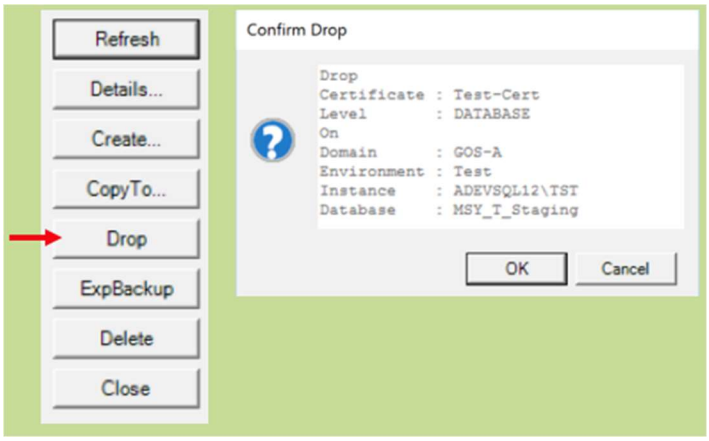
6.4 Certificate: CopyTo



With the CopyTo button, you can copy an existing Certificate to another database. You will only be able to copy Cert Level to the same Cert Level (master -> master or user database -> user database).

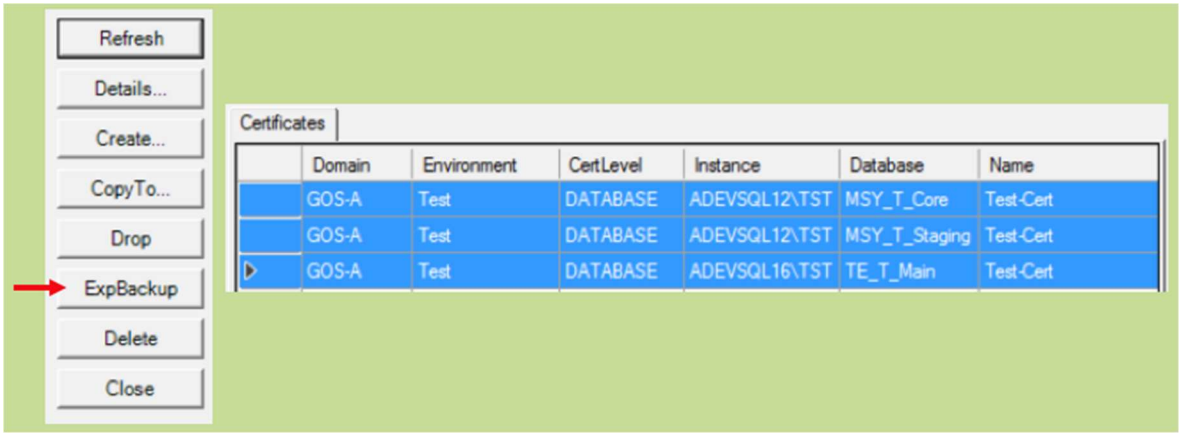
6.5 Certificate: Drop

The difference between Drop and Delete is that Drop will drop the Certificate on the remote Instance. The Certificate info, including Backup/Import will still remain in the QGrip database.



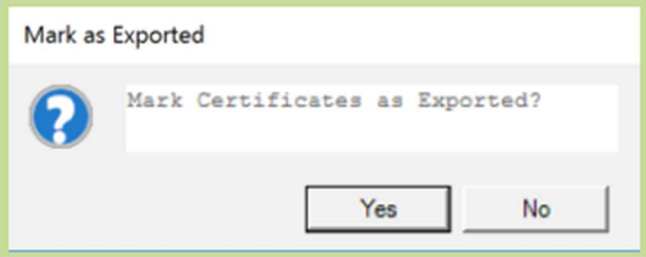
Drop the Certificate related to the current row in the tab-page on the remote Instance. The information in QGrip will remain but the Certificate will get the status: OK-Dropped
It is possible that the drop fails if the Certificate has been used for encryption of other objects. In that case, the status will not change and no alterations will be made to the Certificate.

6.6 Certificate: ExpBackup



To export Backups Imported to QGrip, select the Certificates in the tab-page and hit the ExpBackup button. The status of the Certificates must be 'OK' or OK-Dropped'. You will be asked to select to save a file. We advise you to create a new directory because as all the files will be saved there.

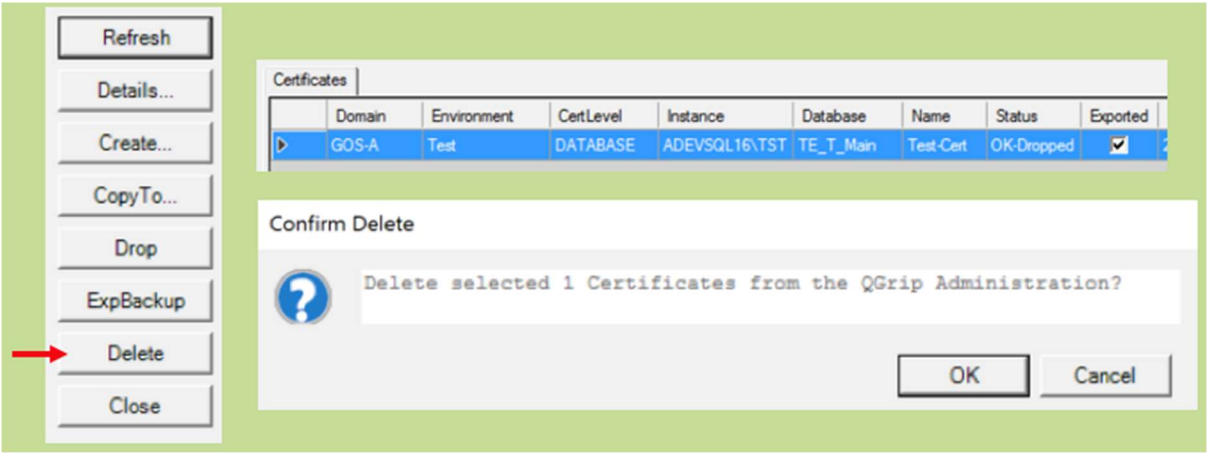
The files to (re-)create the Certificates have been placed in the directory. A popup with a script to create the objects will be shown. This popup will contain passwords and you should pay attention to where you save it.



You will receive a question if you want to mark the Certificates as exported or not. This is important for the delete that will be explained in the following sections. Only records with status ‘OK-Dropped’ and ‘Marked as Exported’ can be deleted from the QGrip administration.

6.7 Certificate: Delete

The difference between Delete and Drop is that Delete will delete the Certificate from the QGrip administration. Delete is only possible if the Certificate has status ‘OK-Dropped’ and has been marked as ‘Exported’.



Select the Certificates you want to delete from the QGrip administration and hit Delete. QGrip will check that the records have the right status and that they have been marked as 'Exported'.

7 TDE-Encryption in QGrip

QGrip makes it easy to implement TDE (Transparent Data Encryption) to protect the databases and will make sure that the TDE-Certificates are saved in the QGrip database. Use QGrip to Copy an existing TDE-Certificate to other Instance(s) whenever needed.
QGrip will also keep track of backup files that have been encrypted by a TDE-Certificate and will prevent that the TDE-Certificate is dropped (using QGrip) as long as It might be needed.
It is not possible to Delete a TDE-Certificate from the QGrip administration as long as it has not yet been Exported to a file that can be used to recreate it.

The terminology used in QGrip is somewhat different compared to the one used in the SQL Server documentation. This will be explained in this section.

7.1 Enable TDE

Implementing TDE protected Databases using QGrip.

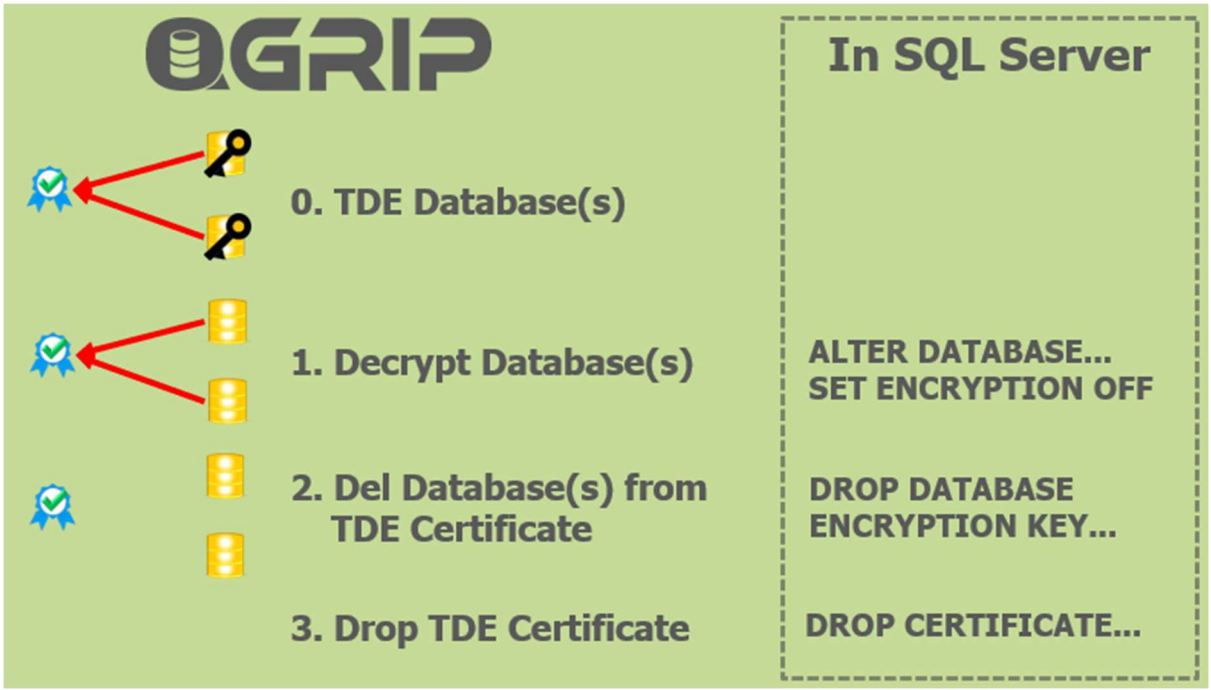
1. Create TDE Certificate
When a TDE Certificate is created using QGrip, the Master Key on the Instance is automatically created if it is not yet present. The password is generated and saved in the QGrip database together with the create statement assuring that the Master key can be recreated whenever needed.
If the instance where the TDE-Certificate is created is part of an Always On cluster, QGrip will create the Certificate on the selected Instance and then copy the Certificate to all other nodes in the Cluster.

2. Add Database(s) to TDE Certificate [Enable]
The Database Encryption key is created using the TDE-Certificate. The Encryption Algorithm needs to be selected in the step. QGrip supports AES_128, AES_192 and AES_256.
TDE will be Enabled for the Database but the database is not yet Encrypted.

3. Encrypt Database(s) [Encrypt]
Databases can be Encrypted using QGrip, but handle with care. If the database is large, it might take some time. If the encryption process needs to be paused, you will need to do it with a SQL Statement on the Instance, QGrip does not support it.

Step 2 and Step 3 can be combined as one action in QGrip; [Enable+Encrypt]

7.2 Disable TDE



Removing TDE protection on Databases using QGrip.

1. Decrypt Database(s) [Decrypt]
Databases can be Decrypted using QGrip, but handle with care. If the database is large, it might take some time. If the decryption process needs to be paused, you will need to do it with a SQL Statement on the Instance, QGrip does not support it.

2. Del Database(s) from TDE Certificate [Disable]
The Database Encryption key using the TDE Certificate is dropped.

3. Drop TDE Certificate
When a TDE Certificate is no longer used, it can be dropped. This should be done using QGrip because extra checks will be performed to make sure the Certificate does not protect backup files and might be needed for database restores/clones.

Step 1 and Step 2 can be combined as one action in QGrip; [Decrypt+Disable]

7.3 TDE and Always on Clusters

Create TDE Certificate
If a TDE Certificate is Created on an Instance using QGrip, QGrip will check if the Instance is part of an Always on Cluster, and automatically copy the TDE Certificate to all other nodes in the Cluster.

Copy TDE Certificate
If a TDE Certificate is Copied To an Instance using QGrip, QGrip will check if the Instance is part of an Always on Cluster, and automatically copy the TDE Certificate to all nodes in the Cluster.

Add Database(s) to TDE Certificate [Enable]
When you add a database running in an Always on cluster to a TDE Certificate [Enable], the database does not need to be Primary on the selected Instance. QGrip will determine where the Primary is running and perform the actions on that Instance/Database.

Del Database(s) from TDE Certificate [Disable]
When you delete a database running in an Always on cluster to from a TDE Certificate [Disable], the database does not need to be Primary on the selected Instance. QGrip will determine where the Primary is running and perform the actions on that Instance/Database.

[Encrypt] + [Decrypt]
When you Encrypt or Decrypt a database running in an Always on cluster, the database does not need to be Primary on the selected Instance. QGrip will determine where the Primary is running and perform the actions on that Instance/Database.

Export/Drop/Delete TDE Certificates
If you need to Export, Drop the Certificate on an Instance or Delete it from the QGrip Administration, the actions will NOT automatically be performed on all Instances in an Always On Cluster. These actions need to be done by selecting the TDE Certificates on ALL instances in the Always On Cluster.

7.4 Strategy before Implementing TDE

Before you start using TDE, you should decide on a strategy and decide for a naming convention for the TDE-Certificates. Not only based on the current situation but considering what the situation will look like in a few years. Keep in mind that if you clone TDE-Database(s), the TDE-Certificate from the Source Instance/Cluster will be needed on the Destination Instance/Cluster.

TDE Certificate	Certificate Name	Pros	Cons

Per Organisation	TDE-<OrgName>	Very easy.	Not very safe
Per Application	TDE-<AppName>	Easy & Safe	1 certificate per App
Per Application/Environment	TDE-<AppName><Env>	Safe	(*) Laborious
Per Instance and Per Always on Cluster	TDE-<InstanceName> TDE-<ClusterName>	Very Safe	(*) Laborious
Per DTAP Environment	TDE-<Develop> TDE-<Test> TDE-<Acceptance> TDE-<Production>	1 Cert per DTAP Environment	(*)Laborious
Per Database	TDE-<DatabaseName>	Very Safe	(*) Laborious

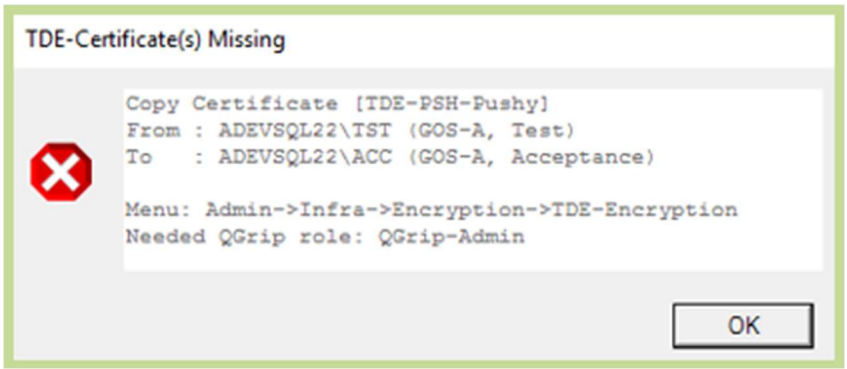
The table above contains some suggested strategies with pros and cons.

(*) Laborious
When a database is cloned to a Destination where the Source TDE-Certificate does not exist, these extra actions will be needed for the clone to succeed and to the maintain the chosen Strategy and keep your SQL Server environments consistent and clean. QGrip will NOT do this automatically but the steps should be performed manually, using QGrip.

1. Copy Source TDE-Certificate to Destination (temporarily)
2. Clone the database to Destination
3. Decrypt + Disable Encryption on the cloned database on Destination (using Source TDE-Certificate temporarily created)
4. Enable + Encrypt the cloned database on Destination (using Permanent Destination TDE-Certificate)
5. Drop the temporarily created source TDE-Certificate on the Destination. This cannot be done immediately as the TDE-Certificate has been used in the backup taken straight after the Clone.

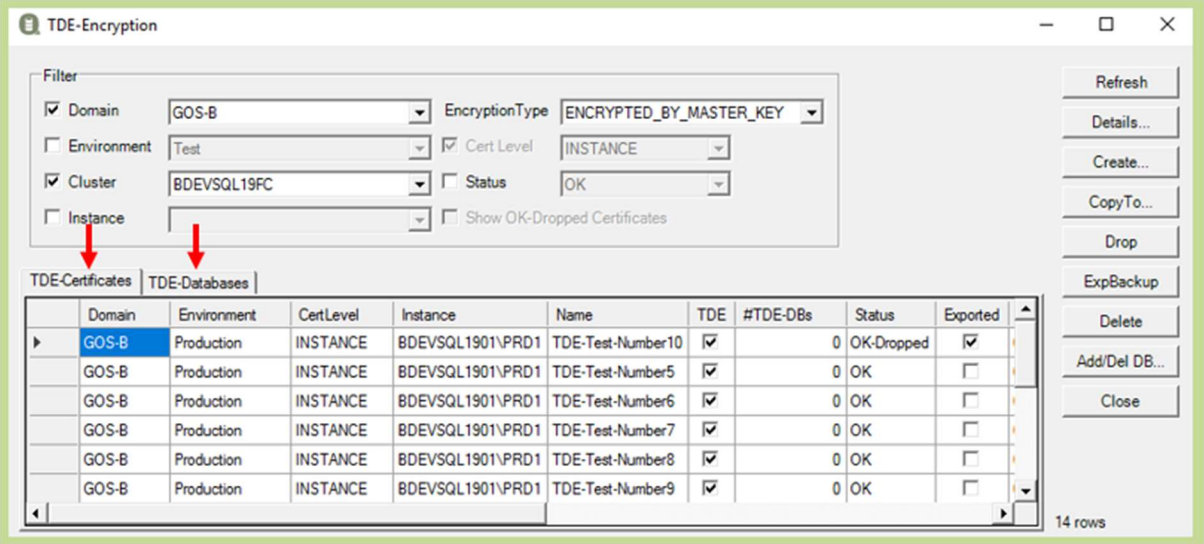
Advise
One TDE-Certificate per Application is straight forward, relatively safe and without extra manual actions when databases are being moved around.

7.5 Restore + Clone TDE-Databases

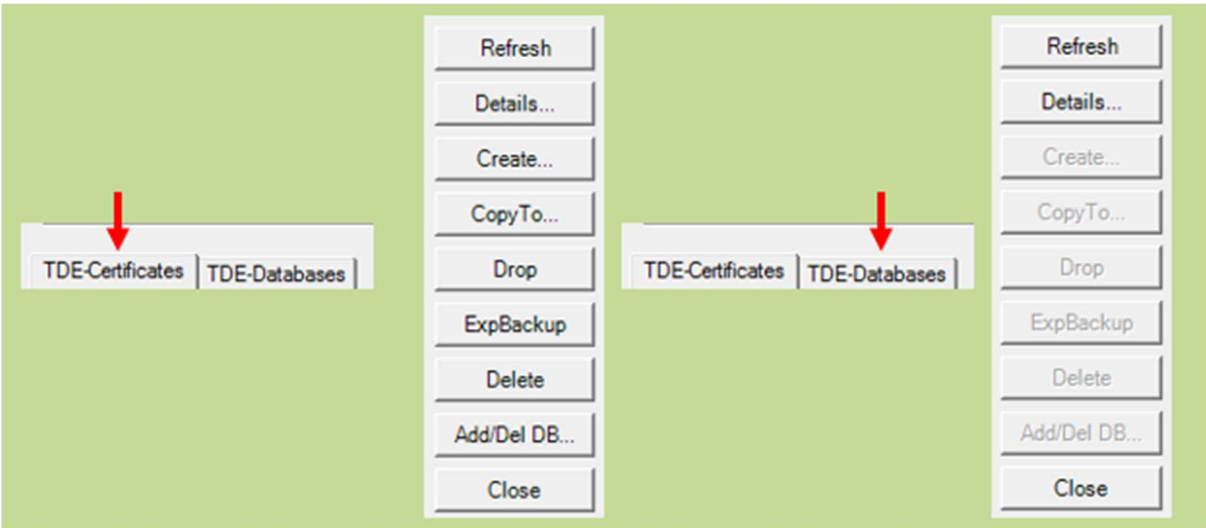


If you try to Clone a TDE-database to an Instance or Always On Cluster, where the needed TDE-Certificate is missing, you will receive an Error with instructions on what needs to be done.

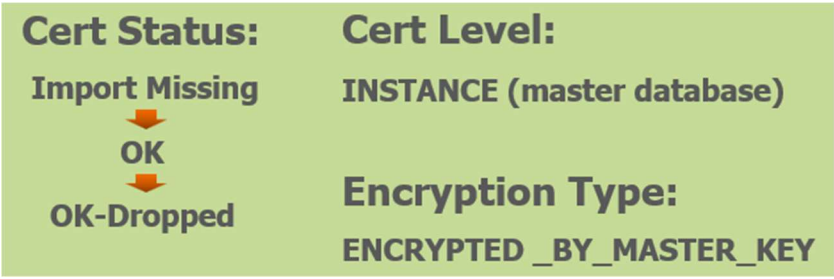
8 TDE-Encryption



The TDE-Encryption main window is compact with a lot of different buttons that will be explained here below. The window has 2 tab pages: TDE-Certificates and TDE-Databases.



Depending on the selected tab page, the action buttons will be enabled/disabled.



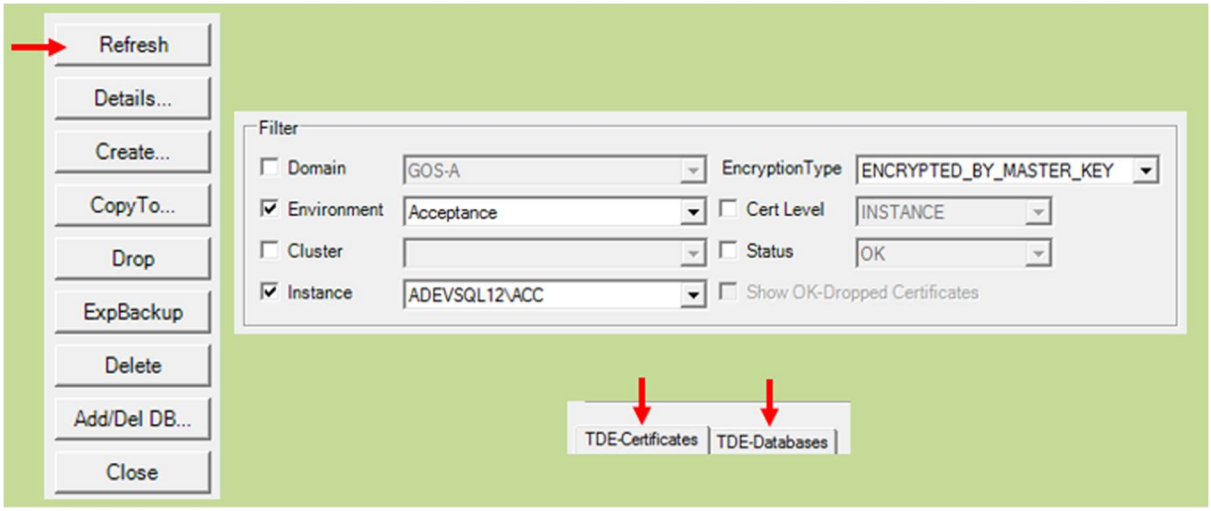
The status of a TDE-Certificate depends on the availability of information and if QGrip is able to backup and import the Certificate to QGrip.

Status	Remark

Import Missing	TDE-Certificate is available but Backup/Import fails because of missing Authorisation on the Backup Share server (QGrip System Account member of Administrators group).
OK	Import to QGrip completed.
OK-Dropped	Import to QGrip completed but the TDE-Certificate has been dropped on the Instance.

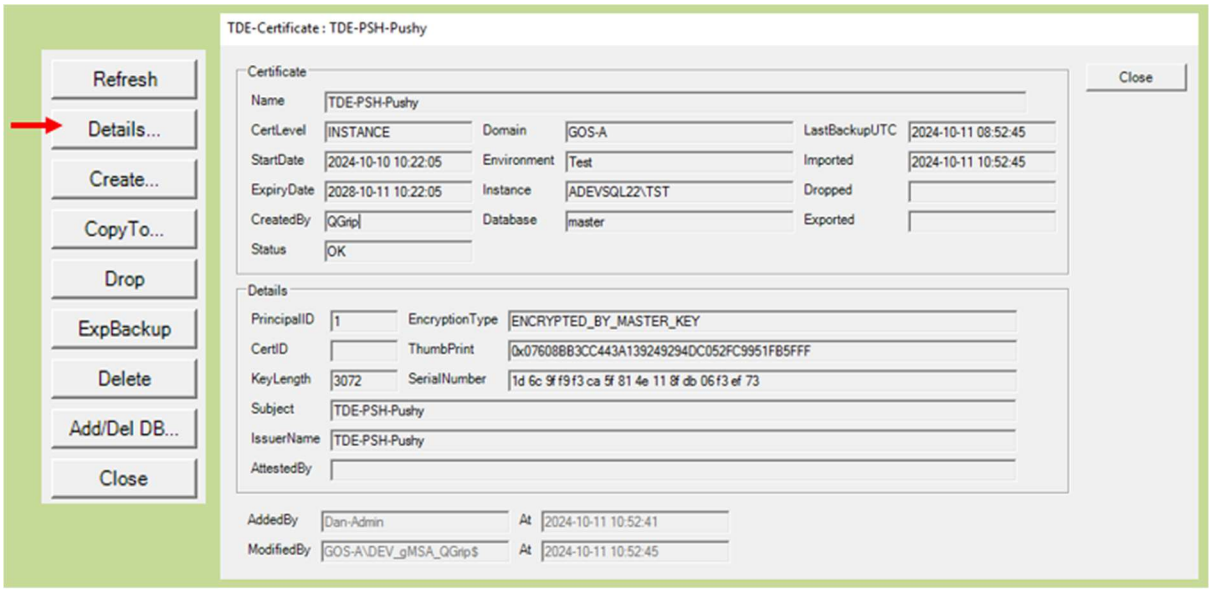
Symmetric Key Automatically created
Whenever needed, if a TDE-Certificate is created or copied to a another Instance, QGrip will automatically create the needed Symmetric Key (MASTER KEY) to complete the request.

8.1 TDE-Certificate: Refresh



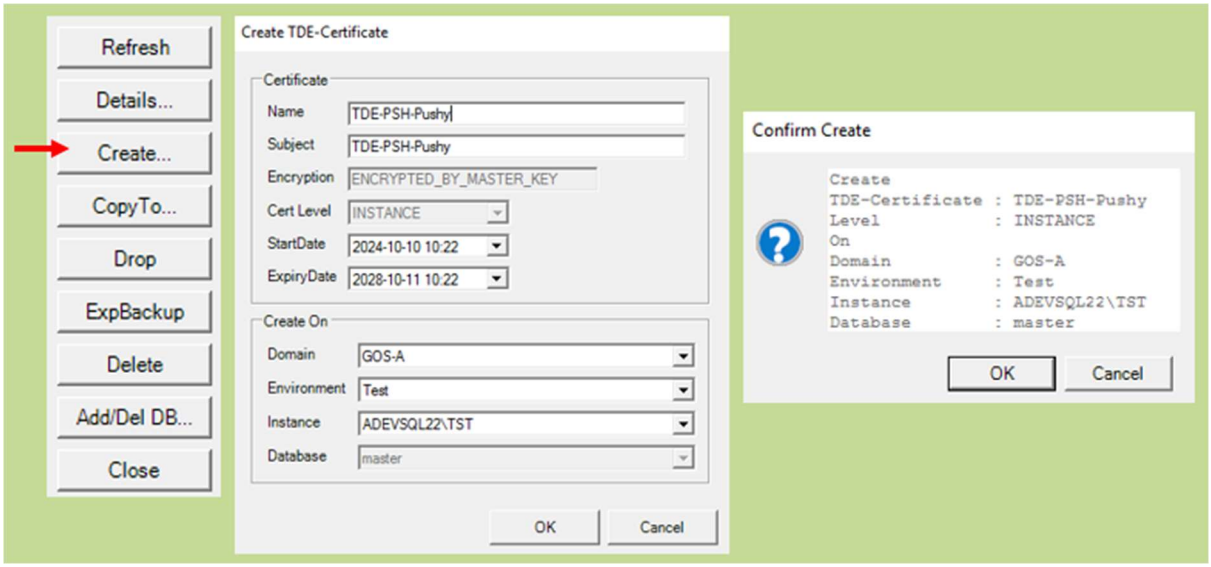
When the Refresh button is pushed, the data in both tab pages (TDE-Certificates and TDE-Databases) will be refreshed according to the setting in the Filter. There is no automatic refresh when the filter is changed.

8.2 TDE-Certificate: Details



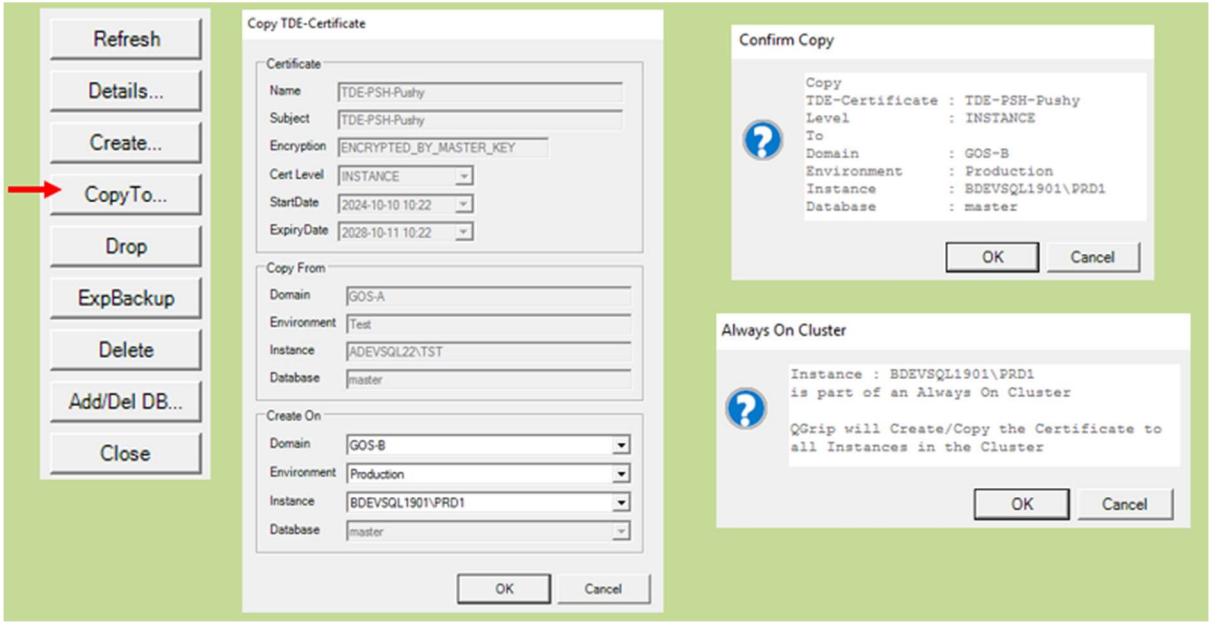
When the Details button is pushed, the details of the current row in the tab page TDE-Certificates will be shown.

8.3 TDE-Certificate: Create



With the Create button, you can create a new Certificate. You will need to enter a name and subject. The Start Date is automatically set to yesterday. This is to prevent warnings as certificates are using UTC time.
If the instance where the TDE-Certificate is created, is part of an Always On cluster, QGrip will create the TDE-Certificate on the selected Instance and then copy the TDE-Certificate to all other nodes in the Cluster.
TDE-Certificates MUST be created in the TDE-Encryption window and not in the Certificates window!

8.4 TDE-Certificate: Copy To

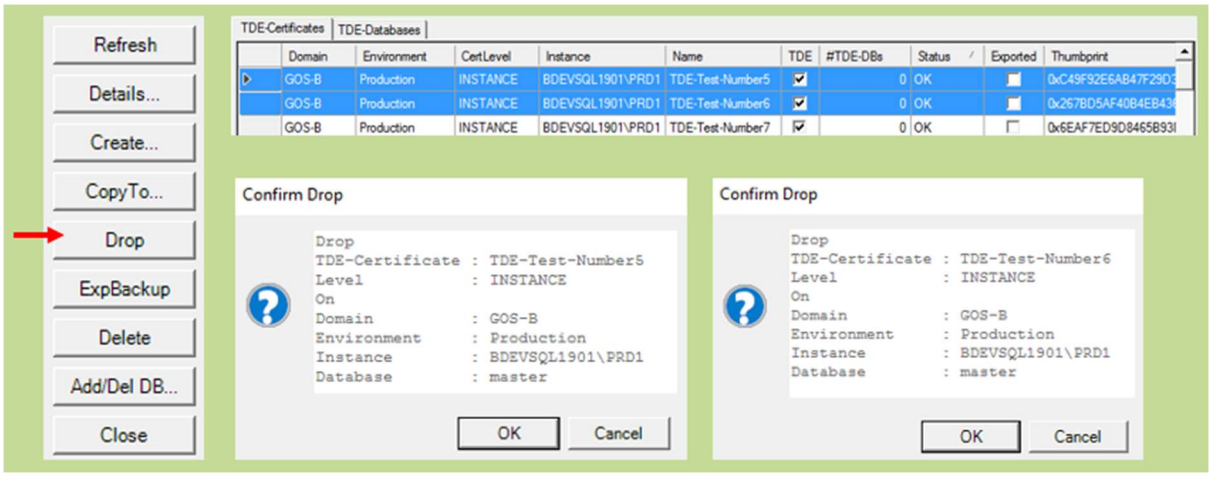


Select the TDE-Certificate that you want to Copy To another Instance and press [CopyTo…].

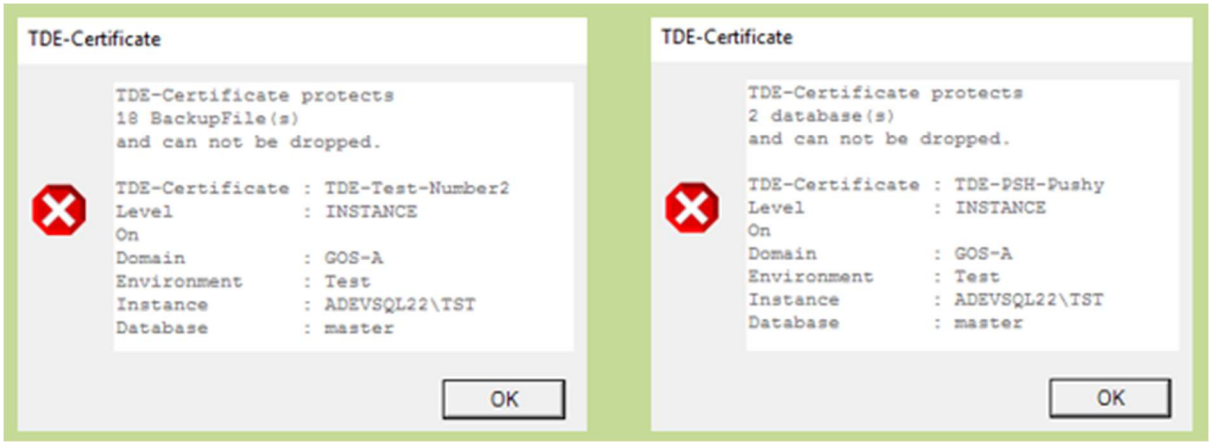
Select the Destination Instance and Press OK.
If the destination Instance is part of an Always On Cluster, QGrip will copy the TDE-Certificate to all Instances in the Cluster.

8.5 TDE-Certificate: Drop

The difference between Drop and Delete is that Drop will drop the TDE-Certificate on the remote Instance. The Certificate info, including Backup/Import will still remain in the QGrip database.

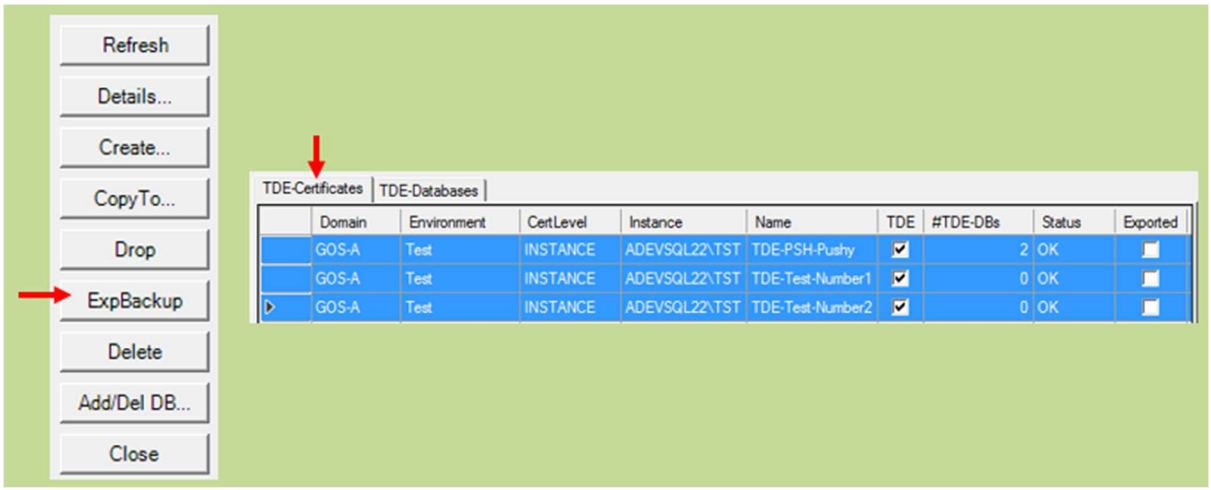


Select the rows with the TDE-Certificates you want to drop on the Instance(s) and press [Drop].
Drop the Certificate related to the current row in the tab-page on the remote Instance. The information in QGrip will remain but the Certificate will get the status: OK-Dropped

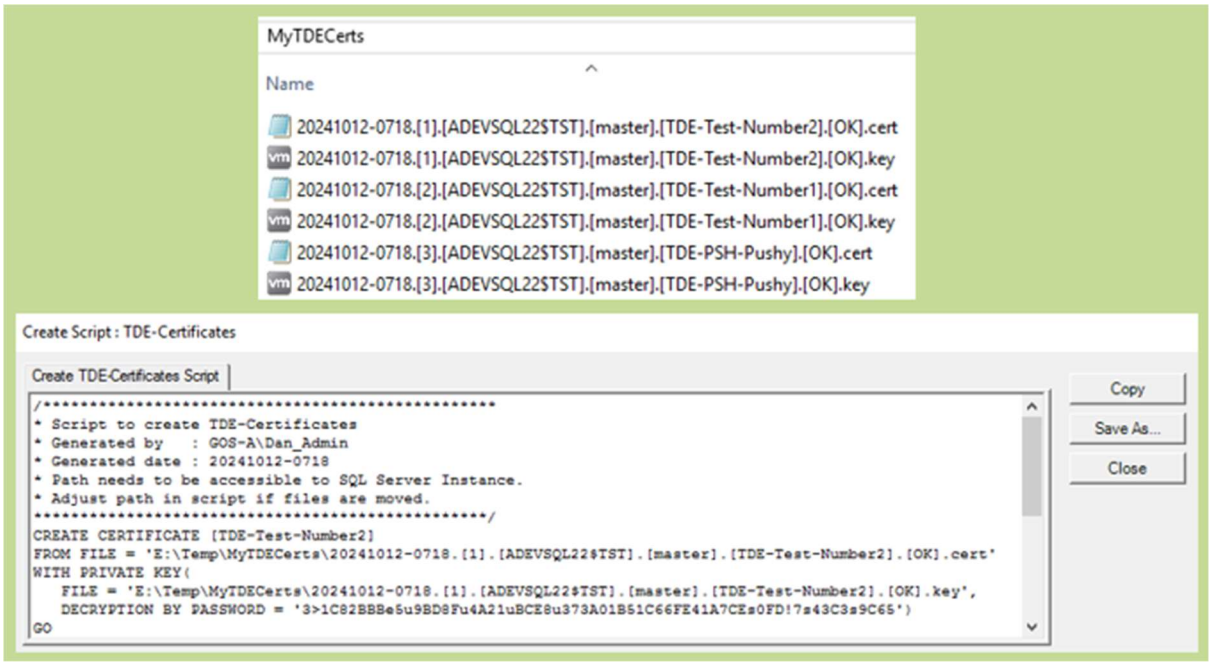


QGrip will check its own administration and show an Error if the TDE-Certificate cannot be dropped.

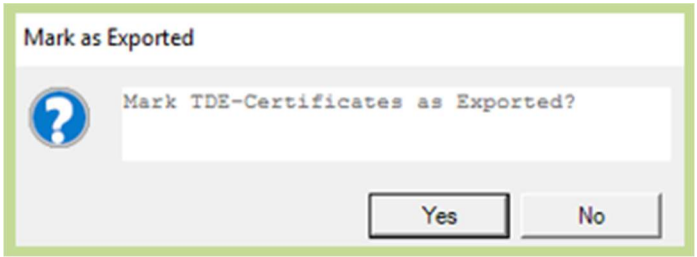
8.6 TDE-Certificate: ExpBackup



To export Backups Imported to QGrip, select the TDE-Certificates in the tab-page and hit the ExpBackup button. The status of the TDE-Certificates must be 'OK' or OK-Dropped'. You will be asked to select to save a file. We advise you to create a new directory because as all the files (2 per TDE-Certificate) will be saved there.



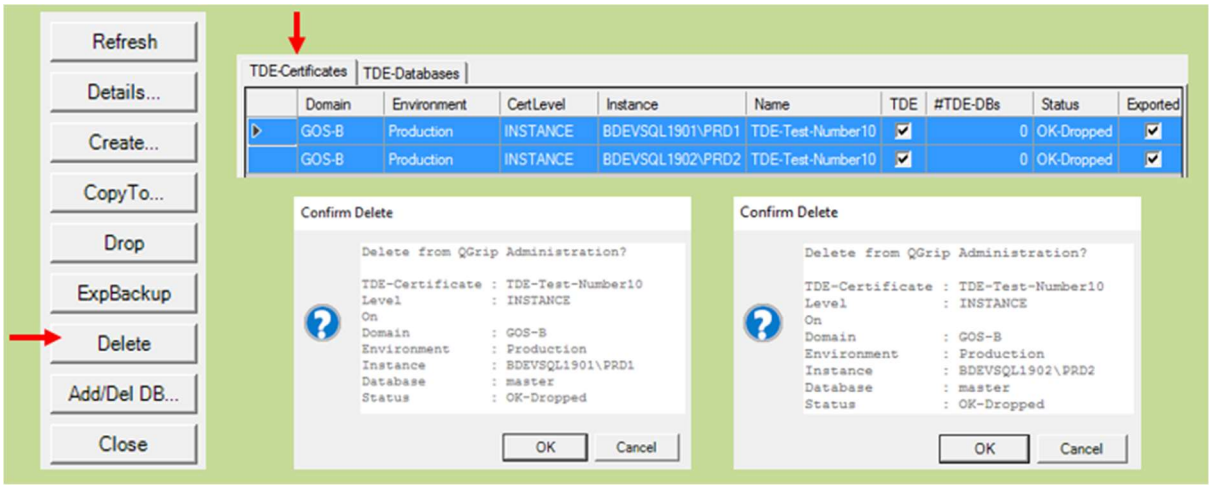
The files to (re-)create the TDE-Certificates have been placed in the directory. A popup with a script to create the objects will be shown. This popup will contain passwords and you should pay attention to where you save it.



You will receive a question if you want to mark the TDE-Certificates as exported or not. This is important for the delete that will be explained in the following sections. Only records with status 'OK-Dropped' and 'Marked as Exported' can be deleted from the QGrip administration.

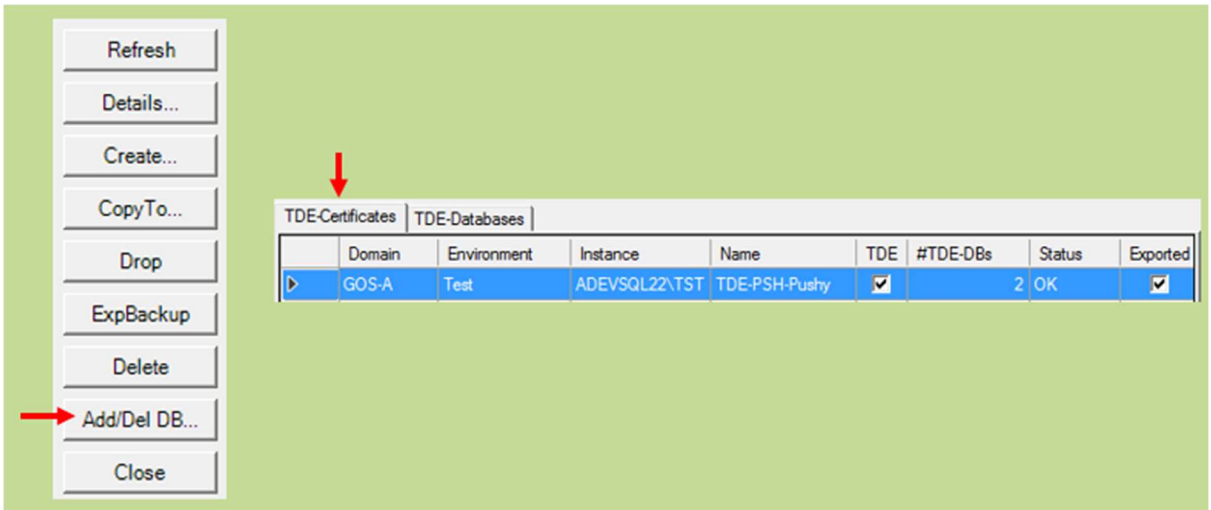
8.7 TDE-Certificate: Delete

The difference between Delete and Drop is that Delete will delete the TDE-Certificate from the QGrip administration. Delete is only possible when the TDE-Certificate has status 'OK-Dropped' and has been marked as 'Exported'.



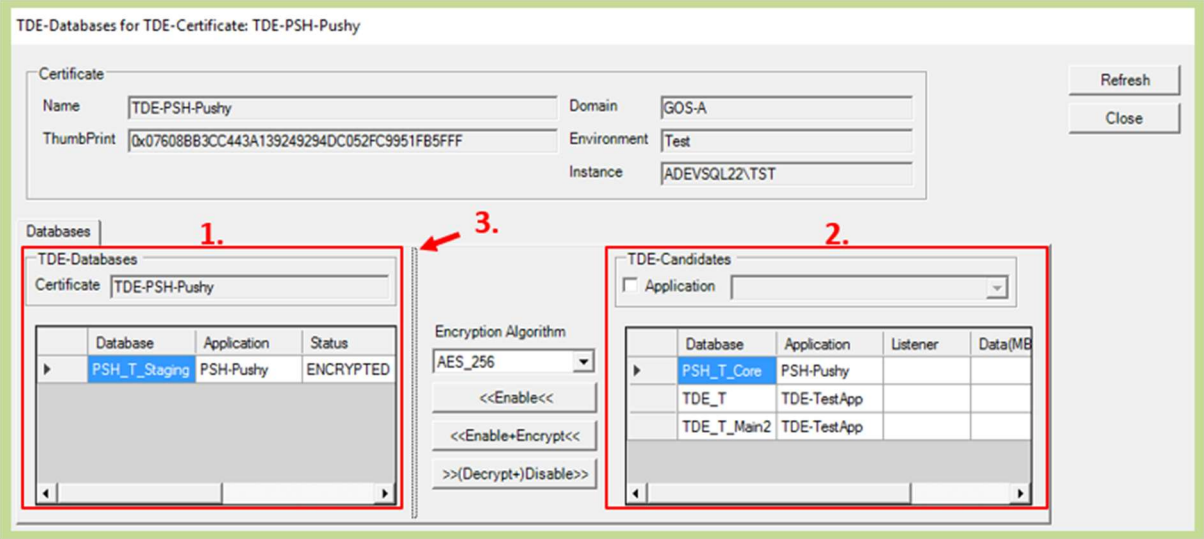
Select the TDE-Certificates you want to delete from the QGrip administration and hit Delete. QGrip will check that the records have the right status and that they have been marked as 'Exported'. You will need to confirm the Delete for each TDE-Certificate separately.

8.8 TDE-Certificate: Add/Del DB



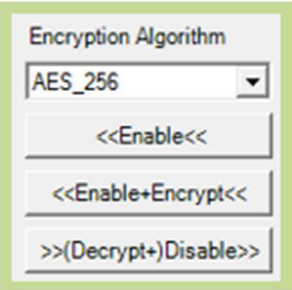
To Edit (Add or Delete) Databases protected by a TDE-Certificate, select the TDE-Certificate and hit the [Add/Del DB…] button.

Add: Create an Encryption Key on a Database using the TDE-Certificate; **Enable** TDE
Del: Drop the Encryption Key on a TDE-Database protected by the TDE-Certificate; **Disable** TDE

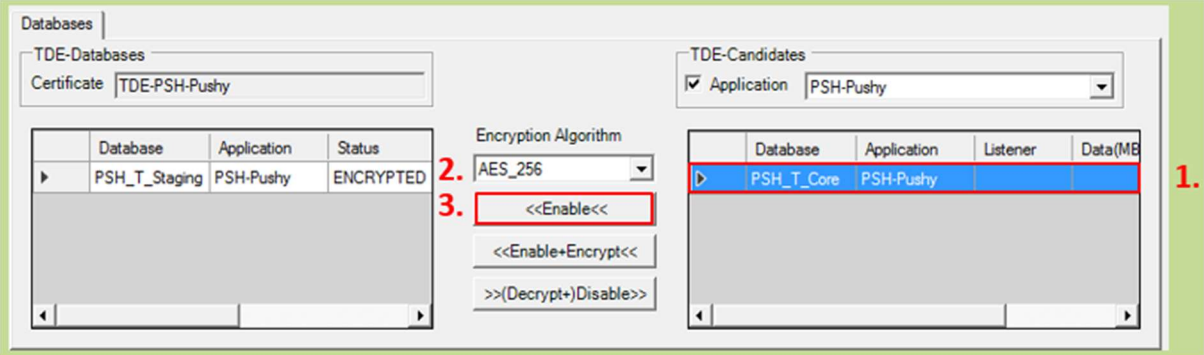


In the 'TDE-Databases for TDE-Certificate' window, you can Add/Enable or Del/Disable TDE for Databases using the TDE-Certificate for TDE protection.

1. Contains the TDE-Databases already protected by the TDE-Certificate.
2. Contains TDE-Candidates, Databases on the Instance that are not yet protected by a TDE-Certificate. The list can be filtered by selecting a specific Application.
3. Drag the splitter to change the size of the TDE-Databases panel

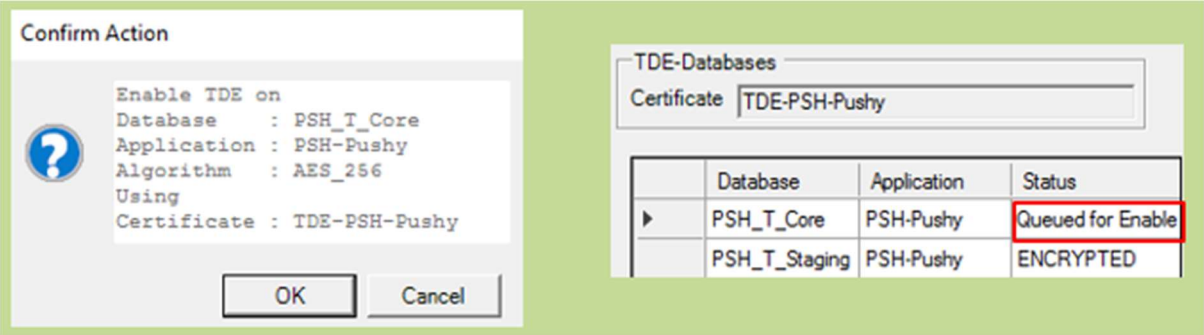


Encryption Algorithm:	Select the Encryption Algorithm that should be used when creating the Database encryption key [Enable]; AES_256, AES_192 or AES_128
Enable:	Create Database encryption key on selected database using the current TDE-Certificate.
Enable+Encrypt:	Create Database encryption key on selected database using the current TDE-Certificate and Encrypt the Database immediately.
(Decrypt)+Disable:	Drop Database encryption key on selected database protected by the current TDE-Certificate. If the Database is Encrypted, it will be Decrypted first.

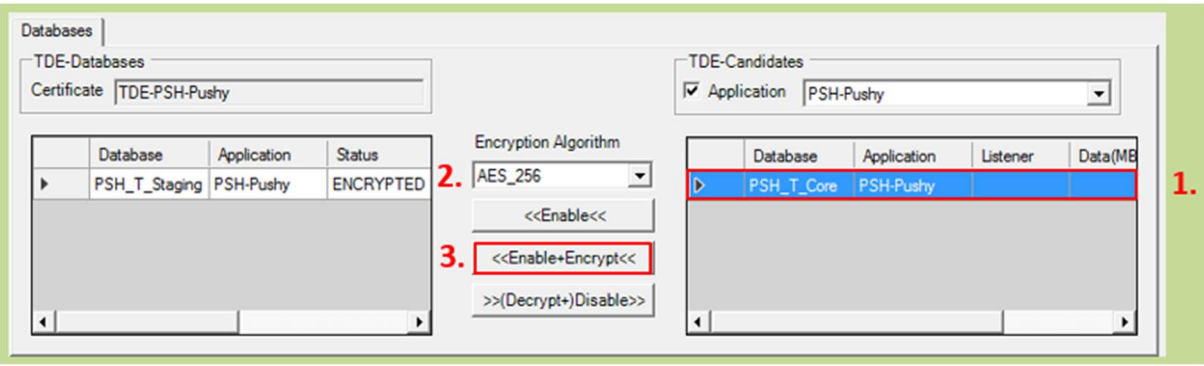


Enable:

1. Select the Rows with the databases in the TDE-Candidates Panel
2. Choose Encryption Algorithm
3. Hit the [Enable] button

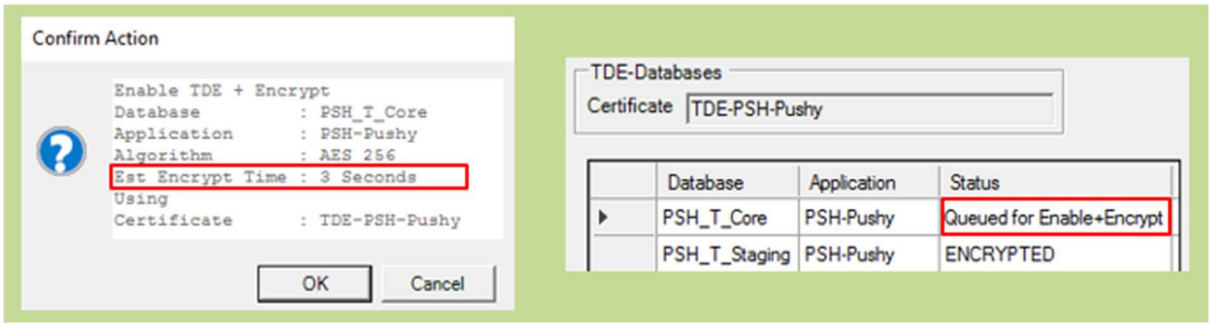


- You will need to Confirm the Action for each database separately.
- The Database Row will be moved to the TDE-Databases Panel with Status 'Queued for Enable'.
- Push [Refresh] to update the view.

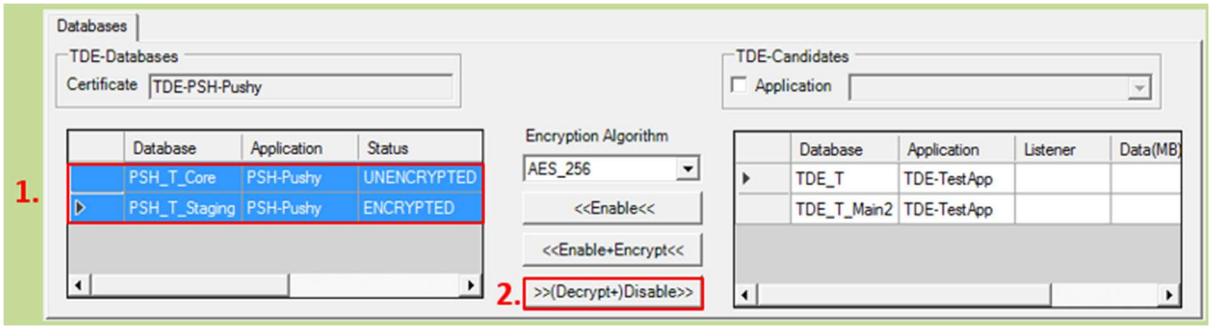


Enable+Encrypt:

1. Select the Rows with the databases in the TDE-Candidates Panel
2. Choose Encryption Algorithm
3. Hit the [Enable+Encrypt] button

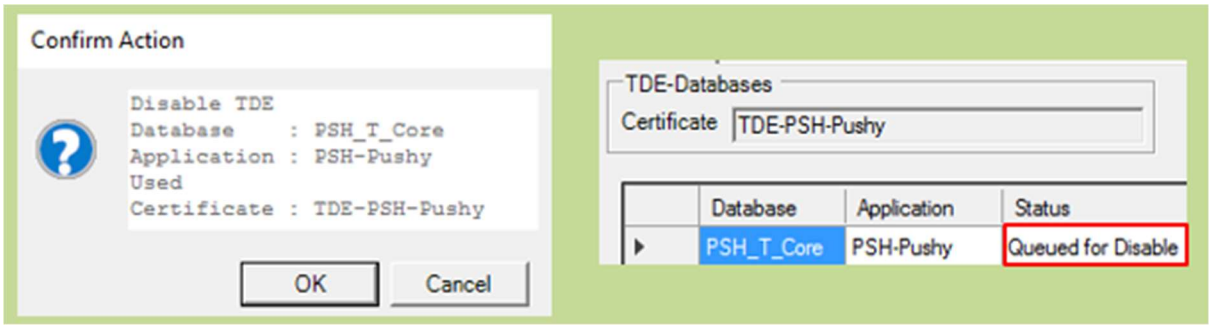


- You will need to Confirm the Action for each database separately.
- QGrip will Calculate an 'Estimated Encrypt Time' based on the size of the database and former Encrypt actions done using QGrip. If there is not enough history in QGrip, 'No estimate possible' will be shown.
- The Database Row will be moved to the TDE-Databases Panel with Status 'Queued for Enable+Encrypt'.
- Push [Refresh] to update the view.



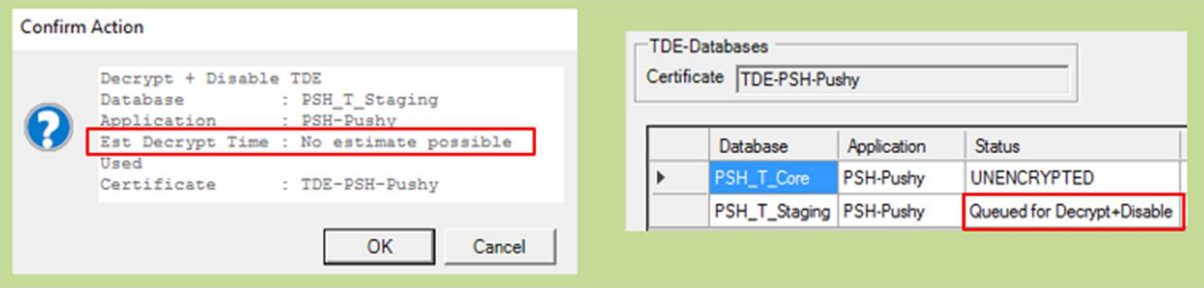
(Decrypt+)Disable:

1. Select the Rows with the TDE-databases in the TDE-Databases Panel
2. Hit the [(Decrypt+)Disable] button



Disable: TDE-Database Status: UNENCRYPTED

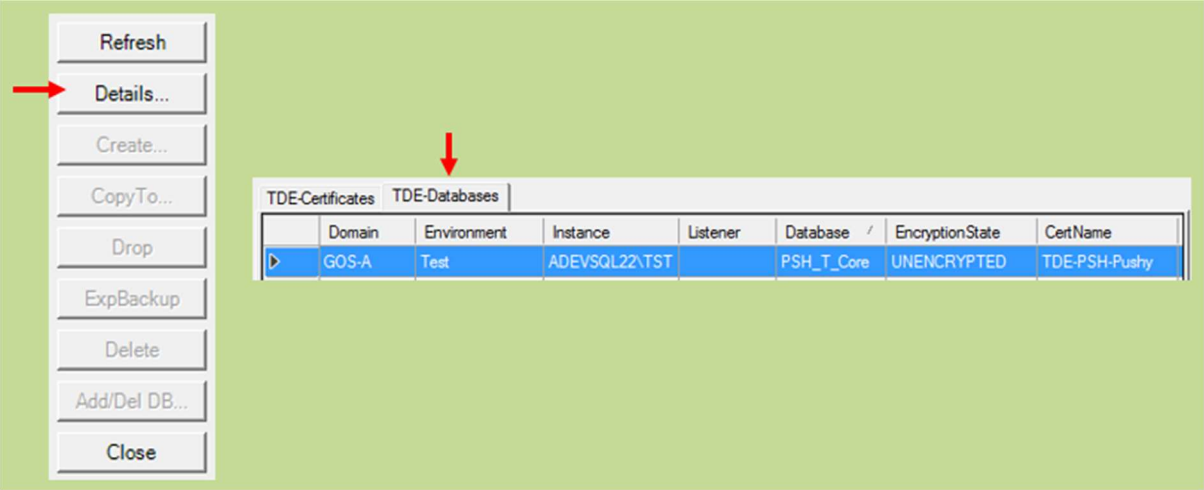
- You will need to Confirm the Action for each database separately.
- The status in the TDE-Databases Panel will be set to 'Queued for Disable'.
- Push [Refresh] to update the view. When QGrip has finished with Disable, the database will be moved to the TDE-Candidates Panel.



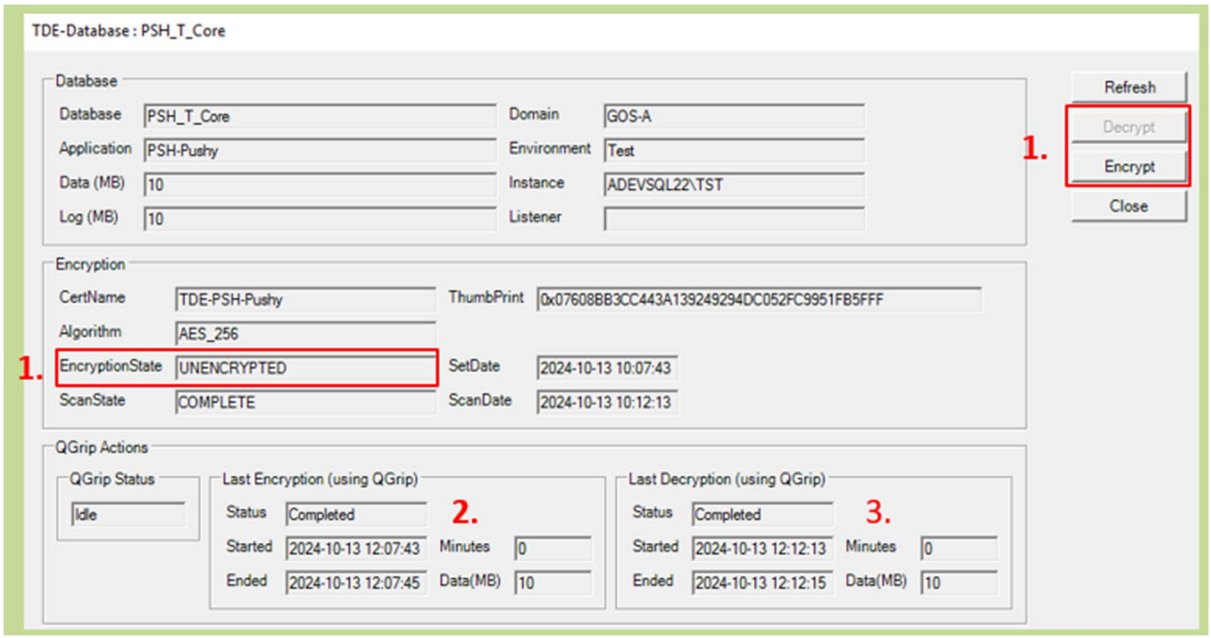
Decrypt+Disable: TDE-Database Status: ENCRYPTED

- You will need to Confirm the Action for each database separately.
- QGrip will Calculate an 'Estimated Decrypt Time' based on the size of the database and former Decrypt actions done using QGrip. If there is not enough history in QGrip, 'No estimate possible' will be shown.
- The status in the TDE-Databases Panel will be set to 'Queued for Decrypt+Disable.
- Push [Refresh] to update the view. When QGrip has finished with Decrypt and Disable, the database will be moved to the TDE-Candidates Panel.

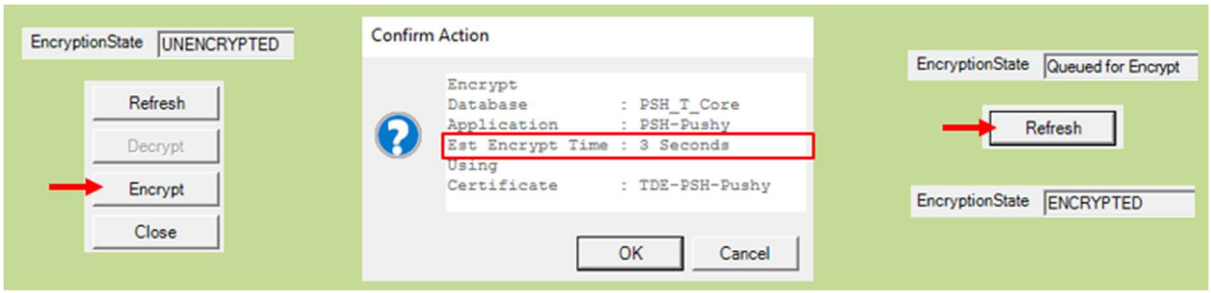
8.9 TDE-Database: Details (Encrypt + Decrypt)



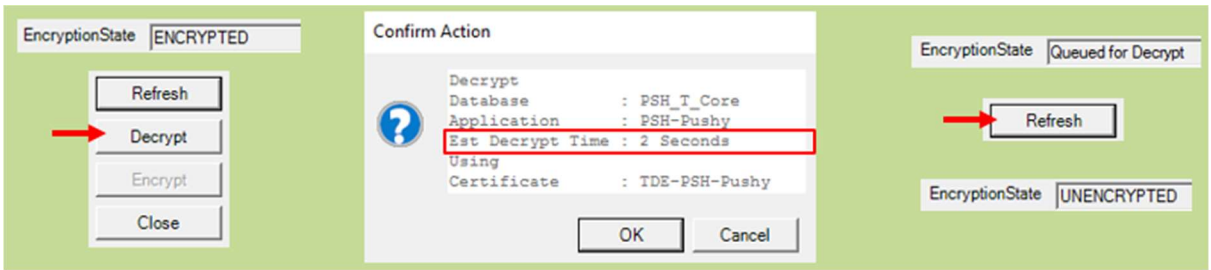
In the TDE-Databases tab-page, select the Row with the TDE-Database and hit [Details].



1. The buttons [Decrypt] and [Encrypt] will be Enabled/Disable depending on the 'Encryption State' value:
   UNENCRYPTED -> [Encrypt] is Enabled
   ENCRYPTED -> [Decrypt] is Enabled
   Any other value, both buttons will be Disabled.
2. Shows the details of the Last Encryption action of the TDE-Database using QGrip. If the Status is 'Interrupted', QGrip could not finalise the Encryption. The Encryption process has probably been Paused manually on the Instance.
3. Shows the details of the Last Decryption action of the TDE-Database using QGrip. If the Status is 'Interrupted', QGrip could not finalise the Decryption. The Decryption process has probably been Paused manually on the Instance.



Encrypt:
If the 'Encryption State' of the TDE-Database is UNENCRYPTED, hit [Encrypt] button, Confirm the Encrypt action. The 'Encryption State' will be set to 'Queued for Encrypt'. Hit [Refresh] button to see when 'Encryption State' changes into ENCRYPTED.



Decrypt:
If the 'Encryption State' of the TDE-Database is ENCRYPTED, hit [Decrypt] button, Confirm the Decrypt action. The 'Encryption State' will be set to 'Queued for Decrypt'. Hit [Refresh] button to see when 'Encryption State' changes into UNENCRYPTED.

9 Always On: Symmetric Keys & Certificates

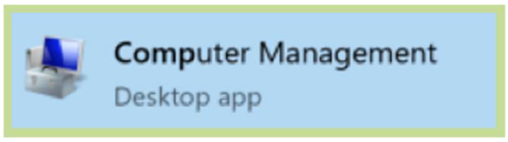
You might have noticed that there is no distinction made with DB Host type Instance/Listener in the Symmetric Keys and Certificates windows above and that is on purpose. Whenever you manipulate (Create, CopyTo, Drop or Backup) a Symmetric Key or Certificate of a database being part of an availability group on an Always On cluster, the action will automatically be performed for the databases in all replicas.

Passwords used for Symmetric Keys as well as File Passwords and Import files will be identical.

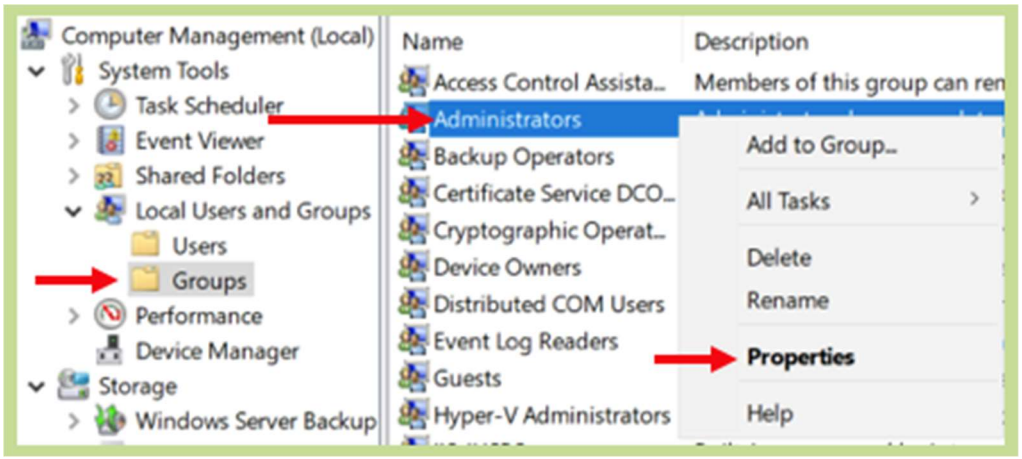
10 Appendix

10.1 Add member: Local Administrator Group

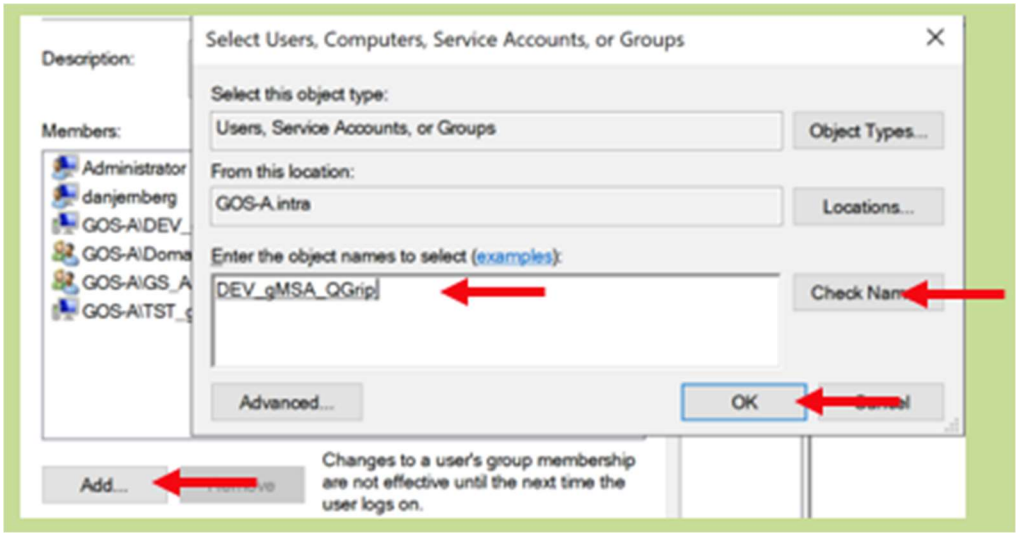
Required Authorisation
Local Administrator on the Machine



Open Computer Management application.



Locate the Administrators group and open the Properties.



Click on the Add… button, enter the name of the QGrip System Account, press Check Names and finally OK.