

Encryption

Symmetric Keys, Certificates & TDE



2025-01-12



Contents

1	Introduction4							
2	١	Why member Administrators group?5						
3	E	Enable Symmetric Keys, Certificates and TDE7						
	3.1	Encryption Config7						
	3.2	Add QGrip System Account as member Administrator Groups7						
4	E	Encryption						
5	9	Symmetric Keys9						
	5.1	Symmetric Key: Refresh10						
	5.2	Symmetric Key: Details						
	5.3	Symmetric Key: Create11						
	5.4	Symmetric Key: CopyTo12						
	5.5	5 Symmetric Key: Drop						
	5.6	5 Symmetric Key: ExpBackup13						
	5.7	Symmetric Key: Exp2File14						
	5.8	Symmetric Key: Delete15						
6	(Certificates15						
	6.1	Certificate: Refresh						
	6.2	2 Certificate: Details						
	6.3	Certificate: Create17						
	6.4	Certificate: CopyTo						
	6.5	6 Certificate: Drop						
	6.6	6 Certificate: ExpBackup19						
	6.7	Certificate: Delete						
7	-	TDE-Encryption in QGrip21						
	7.1	Enable TDE21						
	7.2	2 Disable TDE						
	7.3	3 TDE and Always on Clusters23						
	7.4	Strategy before Implementing TDE23						
	7.5	Restore + Clone TDE-Databases						
8	-	TDE-Encryption25						
	8.1	TDE-Certificate: Refresh26						
	8.2	2 TDE-Certificate: Details						
	8.3	3 TDE-Certificate: Create						
	8.4	TDE-Certificate: Copy To27						



8.5	TDE-Certificate: Drop	28
8.6	TDE-Certificate: ExpBackup	28
8.7	TDE-Certificate: Delete	30
8.8	TDE-Certificate: Add/Del DB	30
8.9	TDE-Database: Details (Encrypt + Decrypt)	34
9 Alw	vays On: Symmetric Keys & Certificates	36
10	Appendix	37
10.1	Add member: Local Administrator Group	37

OGRIP

ENCRYPTION KEYS/CERTIFICATES/TDE

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.

TDE-Certificate(s) Missing							
Copy Certificate [TDE-Test-Number4] From : ADEVSQL22\TST (GOS-A, Test) To : ADEVSQL22\ACC (GOS-A, Acceptance) Menu: Admin->Infra->Encryption->TDE-Encryption Needed QGrip role: QGrip-Admin OK							

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 <u>all nodes</u> 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

Enable Symmetric Keys and Certificates

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.

Enable Symmetric Keys and Certificates							
Check every	1 📩 Days 💌	That QGrip System Accounts are Local Administrators on the Backup Share Servers.					
		(Admin->Infra->Accessibility: QGripAccount-IsLocalAdmin)					

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.

lip Powntime Mode	- - - - - - - - - -	 2 5 6 6 6 7 7 8 8 7 8 8 9 9	Help Prepare Infra Disaster Scripts Instance-Server-Cluster Backup Shares QGripServers Monitor Hosts	•	ganis	ations Displa Grip or	ns nyName n SQL DEV	Organ
Powntime Mode	> > > > > > > >	2 5 11 11 11	Help Prepare Infra Disaster Scripts Instance-Server-Cluster Backup Shares QGripServers Monitor Hosts	•	ganis	ations Displa Grip or	ns nyName n SQL DEV	Organ
Powntime Mode	• • • •	2 冬 日日 日日 日日	Help Prepare Infra Disaster Scripts Instance-Server-Cluster Backup Shares QGripServers Monitor Hosts	•	ganis	ations Displa Grip or	yName	Organ Grip o
owntime Mode	> > > >		Disaster Scripts Instance-Server-Cluster Backup Shares QGripServers Monitor Hosts	,	ganis	Displa Grip or	yName	Organ Grip o
owntime Mode	> > >		Instance-Server-Cluster Backup Shares QGripServers Monitor Hosts	,		Displa Grip or	yName	Organ Grip or
owntime Mode	> > >		Backup Shares QGripServers Monitor Hosts	,		Grip or	n SQL DEV	Grip or
owntime Mode	•	80	QGripServers Monitor Hosts					
owntime Mode	•	88	Monitor Hosts					
Mode	-		Monitor Hosts					
		*	FileTransfer-Method					
		8	Encryption	•	1	Symr	metric Keys	
	ľ	-	Accessibility		0	Certi	ficates	
	L	•	rice sharing		2	TDE-	Encryption	
					1			
Cormation . need to Symmetric min -> Co	is n :Keys onfig	ot y and ->	vet available. 1 Certificates' Encryption Config					
1	formation 1 need to Symmetric imin -> Co	formation is n l need to SymmetricKeys imin -> Config	formation is not y l need to SymmetricKeys and imin -> Config ->	formation is not yet available. l need to SymmetricKeys and Certificates' dmin -> Config -> Encryption Config OK	formation is not yet available. 1 need to SymmetricKeys and Certificates' dmin -> Config -> Encryption Config OK	formation is not yet available. 1 need to SymmetricKeys and Certificates' dmin -> Config -> Encryption Config OK	formation is not yet available. 1 need to SymmetricKeys and Certificates' dmin -> Config -> Encryption Config OK	formation is not yet available. 1 need to SymmetricKeys and Certificates' dmin -> Config -> Encryption Config

4 Encryption

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

8



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.

Config e	rror
⊗	No BackupShare with QGripSystemAccount member of Administrators group. Check the Encryption documentation and configure the BackupShares/Servers.
	ОК

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

O. Sy	mmetric Keys							-		×
	ter Domain G Environment T Cluster T Instance T	GOS-A Test		Key Type MAX Key Level INS Status OK Show OK-Droppe	STER KEY V TANCE V Standard Symmetric Keys	Export Paramet Delimiter Text Qualifier	ers . Comma 💌		Refresh Details Create CopyTo. Drop	n
Symn	KeyType	Domain	Environment	Keyl evel	Instance	Database	Name	ן ור	ExpBack	up
•	MASTER KEY	GOS-A	Test	DATABASE	ADEVSQL12\TST	MSY T Core	##MS DatabaseMasterKey##	1.	Exp2File	e
	MASTER KEY	GOS-A	Test	DATABASE	ADEVSQL12\TST	MSY_T_Staging	##MS_DatabaseMasterKey##		Delete	
								-11	Class	1
	MASTER KEY	GOS-A	Test	DATABASE	ADEVSQL16\TST	TE_T_Main	##MS_DatabaseMasterKey##		Close	
	MASTER KEY MASTER KEY	GOS-A GOS-A	Test Test	INSTANCE	ADEVSQL16\TST ADEVSQL12\TST	master	##MS_DatabaseMasterKey## ##MS_DatabaseMasterKey##		Close	
	MASTER KEY MASTER KEY MASTER KEY	GOS-A GOS-A GOS-A	Test Test Test	INSTANCE INSTANCE	ADEVSQL16\TST ADEVSQL12\TST ADEVSQL16\TST	master master	##MS_DatabaseMasterKey## ##MS_DatabaseMasterKey## ##MS_DatabaseMasterKey##		Close	

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



Key Status:	Key Level:
Password Missing	INSTANCE (master database) DATABASE (user database)
OK	Кеу Туре:
OK-Dropped	MASTER KEY (other Symmetric Keys are not (yet) supported)

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)
ОК	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

Refresh						
Details						
Create	Filter					
CopyTo	C Domain	GOS-A	~ 17	Кеу Туре	MASTER KEY	Ψ
Drop	Environment	Test		Key Level	INSTANCE	Ŧ
ExpBackup	Cluster			Status	ОК	Ψ
- Suc25ile	Instance		- -	Show OK-D	ropped Symmetric	Keys
Exp2File		'				
Delete						
Close						

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

Details	Name	##MS_DatabaseMasterKey##	Domain	GOS-A	Created	2021-09-28 09:11:13	_
	KeyType	MASTER KEY	Environment	Test	Modified	2021-09-28 09:11:13	
Create	KeyLevel	DATABASE	Instance	ADEVSQL12\TST	Dropped		
CopyTo	CreatedBy	QGrip	Database	MSY_T_Core	Imported	2021-09-28 09:11:14	
	Status	Password Missing	1		Exported		
ExpBackup	PrincipalID KeyID	1 101 ThumbPrint					
Exp2File	KeyLength	256 ProviderType					
Delete	Algorithm Guid	Algorithm AES_256 ProviderGuid Guid BB759D00-2382-4188-9838-36914C7E1595					
Close	ProviderAlg	pID D					
	Password	1			Update	-Password	

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

Update-Password

Status	Password Missing	
Password		
Password		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

Status	ОК		
Password Password	38ACD6FBnE6E2n43437nAwA5An0B77E094#DBED633Q8	323F1v#F87Av4E39vBC22	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



Refresh	Create Symmetric Key
Details	Symmetric Key Name ###MS_DatabaseMasterKey###
Create	Key Type MASTER KEY
CopyTo	Key Level INSTANCE
Drop	Create On
ExpBackup	Domain GOS-A
Exp2File	Instance ADEVSQL12\TST
Delete	Database master
Close	OK Cancel

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

Refresh Details Create	Copy Symmetric Key Symmetric Key Name ###MS_DatabaseMasterKey### Key Type MASTER KEY Key Level DATABASE
СоруТо	Copy From
Drop	Domain GOS-A
ExpBackup	Environment Test Instance ADEVSQL12\TST
Exp2File	Database MSY_T_Staging
	Create On
Delete	Domain GOS-A
Close	Environment Test
	Instance ADEVSQL12\TST
	Database QGrip_20210626
	Decryption By Decryption Edisting Password Edisting Password New Password New Password
	OK Cancel

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.



ENCRYPTION

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

Refresh Details									
Create	Symm	etric Keys							
CopyTo		КеуТуре	Domain	Environment	KeyLevel	Instance	Database	Name	Status
		MASTER KEY	GOS-A	Test	DATABASE	ADEVSQL12\TST	MSY_T_Core	##MS_DatabaseMasterKey##	ОК
Drop		MASTER KEY	GOS-A	Test	DATABASE	ADEVSQL12\TST	MSY_T_Staging	##MS_DatabaseMasterKey##	ОК
		MASTER KEY	GOS-A	Test	DATABASE	ADEVSQL16\TST	TE_T_Main	##MS_DatabaseMasterKey##	ОК
ExpBackup	▶	MASTER KEY	GOS-A	Test	INSTANCE	ADEVSQL12\TST	master	##MS_DatabaseMasterKey##	ОК
Exp2File				-				······	•
Delete									
Close									

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.



> SymmKeys → ♂ ♂ Search S		
Name		
20211016-1240.[1].[ADEVSQL16\$TST].[TE_T_Main].[##MS_DatabaseMasterKey##].[OK] 20211016-1240.[2].[ADEVSQL12\$TST].[MSY_T_Staging].[##MS_DatabaseMasterKey##].[OK] 20211016-1240.[3].[ADEVSQL12\$TST].[MSY_T_Core].[##MS_DatabaseMasterKey##].[OK]		
Restore Script : SymmetricKeys		
Restore SymmetricKeys Script /****** * Script to Restore SymmetricKeys Generated by : GOS-A\dan_admin Generated date : 20211016-1240 * Path needs to be accessible to SQL Server Instance. * Adjust path in script if files are moved. ************************************	*	Copy Save As Close

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.

Mark as	Exported	d				
?	Mark	Symmetric	Keys	85	Exported?	
					Yes	No

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

Refresh Details Create CopyTo	Export Param Delimiter Text Qualifie	eters . Comma r "	•					
ExoBackup	Symmetric Keys	Demain	Environment	Keyleyel	Instance	Database	Name	Ortur
Chronenap	MASTER	Domain	Environment	DATABASE	ADEVISOL 12) TET	Used T Care	Name	Status
Exp2File	MASTER	ET GUSA	Test	DATABASE	ADEVSQL12(151	MST_T_Core	##m5_UatabaseMasterNey##	UK
	MASTER K	EY GOS-A	Test	DATABASE	ADEVSQL12\TST	MSY_T_Staging	##MS_DatabaseMasterKey##	ОК
Delete	MASTER K	EY GOS-A	Test	DATABASE	ADEVSQL16\TST	TE_T_Main	##MS_DatabaseMasterKey##	ОК
	MASTER K	EY GOS-A	Test	INSTANCE	ADEVSQL12\TST	master	##MS_DatabaseMasterKey##	ОК
Close								

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'.

	Refresh										
	Details	Symmet	tric Keys								
	Cruste		KeyType	Domain	Environment	KeyLevel	Instance	Database	Name	Status	Exported
-	Create	Þ	MASTER KEY	GOS-A	Acceptance	DATABASE	ADEVSQL16\ACC	TE_A_Main	##MS_DatabaseMasterKey##	OK-Dropped	
	CopyTo										
	Drop	Con	firm Dele	te							
	ExpBackup	6	Del	lete	selected	1 Symmet:	ric Keys :	from the	e QGrip Adminis	tratio	n?
	Exp2File										
-	Delete								ОК	Cance	
-	Close										

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

Certificates						-		×
Filter							Refrest	h
Domain	GOS-A		EncryptionType	ENCRYPTED_BY_MAS	TER_KEY		Details.	
Environment	Test		Cert Level	INSTANCE			Create	
Cluster			Status		<u>-</u>		CopyTo.	
Instance	I		Show OK-Dro	opped Certificates			Drop	
Certificates					↓ I		ExpBack	up
Instance	•	Database	Name		TDE #TDE-DBs	-	Delete	
ADEVSG	L22\TST	master	QGrip-Backup-ADEVSQL22	\$TST-20240407-111910		0		
ADEVSO	L22\TST	master	TDE-Test-Number1			1 -	Close	
ADEVSO	L22\TST	master	TDE-Test-Number2			1		
ADEVS0	L22\TST	master	TDE-Test-Number4		V		6 rows	

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



Cert Status:	Cert Level:
Import Missing OK	INSTANCE (master database) DATABASE (user database)
OK-Dropped	Encryption Type: ENCRYPTED _BY_MASTER_KEY (other Certificates are not (yet) supported

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.
ОК	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

+	CopyTo	TDE-Certificate
TDE #TDE-DBs	Drop	TDE-Certificates can only be
	ExpBackup	Copied to in the IDE-Encryption window
I I ■ 1	Delete	OK

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



_	Refresh						
	Details						
	Create	Filter	GOS-A	~	EncryptionType	ENCRYPTED BY MASTER	KEY 🔻
	CopyTo	Freironment	Acceptance	-	Cert Level	INSTANCE 👻	
	Drop	Cluster		-	Status	OK 💌	
	ExpBackup	✓ Instance	ADEVSQL12\ACC	-	Show OK-Dr	opped Certificates	
	Delete						
	Close						

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

Tioneon	Name	Test-Cert					
Details	CertLevel	DATABASE	Domain	GOS-A	LastBackupUTC	2021-09-28 15:40:24	
<u> </u>	StartDate	2021-09-28 11:01:34	Environment	Test	BackupCert		
Create	ExpiryDate	2022-09-28 11:01:34	Instance	ADEVSQL12\TST	Dropped		
CopyTo	CreatedBy		Database	MSY_T_Core	Imported	2021-09-28 17:40:24	
	Status	ок			Exported		
Drop	Details						- -
ExpBackup	PrincipalID	1 Encrypti	onType ENCRYP	TED_BY_MASTER_KEY			
	CertID	259 ThumbP	rint 0x72658	780C91698385A4F4BE517D526	1E2AD7427A		
Delete	KeyLength	SerialNu	mber 6e ae 87	7 c8 06 3c 57 90 43 53 ae 81 4a i	o7 e8 07		
Close	Subject	Test-Cert					
	IssuerName	e Test-Cert					
	AttestedBy						

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

6.3 Certificate: Create



Refresh	Create Certificate
Details	Certificate Name MyNewCert
Create	Subject My New Cert Encryption ENCRYPTED BY MASTER KEY
CopyTo	Cert Level INSTANCE
Drop	StartDate 2021-10-15 18:32 ExpiryDate 2022-10-16 18:32
ExpBackup	Create On
Delete	Domain GOS-A 💌
Close	Environment Test
	Database master
	OK Cancel

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

Refresh	Copy Certificate	•	
	Certificate		
Details	Name	Test-Cert	
Constra	Subject	Test-Cert	
Create	Encryption	ENCRYPTED_BY_MASTER_KEY	
ConvTo	Cert Level	DATABASE 👻	
	StartDate	2021-09-28 11:01 💌	
Drop	ExpiryDate	2022-09-28 11:01 💌	
	Copy From		
ExpBackup	Domain	GOS-A	
	Environment	Test	
Delete	Instance	ADEVSQL12\TST	
Close	Database	MSY_T_Staging	
Close	Create On		
	Domain	GOS-A	•
	Environment	Test	•
	Instance	ADEVSQL12\TST	•
	Database	QGrp_20210626	•
		ок	Cancel

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.

	Refresh	Confirm Drop
	Details	Drop Certificate : Test-Cert Larea - DETABLER
	Create	On Domain : GOS-A
	CopyTo	Environment : Test Instance : ADEVSQL12\TST Database : MSY_T_Staging
-	Drop	
	ExpBackup	OK Cancel
	Delete	
	Close	

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

[Refresh							
	Details							
	Create	Certific	cates					
			Domain	Environment	CertLevel	Instance	Database	Name
	CopyTo		GOS-A	Test	DATABASE	ADEVSQL12\TST	MSY_T_Core	Test-Cert
	Drop		GOS-A	Test	DATABASE	ADEVSQL12\TST	MSY_T_Staging	Test-Cert
	EveRackup	▶	GOS-A	Test	DATABASE	ADEVSQL16\TST	TE_T_Main	Test-Cert
-	Схроаскор							
	Delete							
	Close							

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.



	> Certs > Name	
Create Script : Certificates Create Certificates Script		Copy Save As
Generated by : GOS-A\dam_ad Generated date : 20211016-183 Path needs to be accessible t Adjust path in script if file CREATE CERTIFICATE (Test-Cert) FROM FILE = 'C:\Users\dam_admin WITH PRIVATE KEY(FILE = 'C:\Users\dam_admin\D	min 8 9 9 sQL Server Instance. 5 are moved. ************************************	Close
DECRYPTION BY PASSWORD = '71	121yDF6FnC3E3n442Bn88CCn8DC67DC84A469892ENEC57Eg2547g46E7gAABA*)	~

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.

Mark as Exported				
?	Mark Certificates as Exported?			
	Yes No			

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'.

Refresh									
Details	Certifi	icates							
		Domain	Environment	CertLevel	Instance	Database	Name	Status	Exported
Create	Þ	GOS-A	Test	DATABASE	ADEVSQL16\TST	TE_T_Main	Test-Cert	OK-Dropped	
CopyTo									
Drop	Con	firm Delete	•						
ExpBackup	6	Dele	te selecte	d 1 Certi	ficates from	n the QGr	ip Admi	lnistrati	on?
Delete							OK		Cancel
									Januer

ENCOUDTION

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></orgname>	Very easy.	Not very safe
Per Application	TDE- <appname></appname>	Easy & Safe	1 certificate per App
Per Application/Environment	TDE- <appname><env></env></appname>	Safe	(*) Laborious
Per Instance and	TDE- <instancename></instancename>	Very Safe	(*) Laborious
Per Always on Cluster	TDE- <clustername></clustername>		
Per DTAP Environment	TDE- <develop></develop>	1 Cert per	(*)Laborious
	TDE- <test></test>	DTAP	
	TDE- <acceptance></acceptance>	Environment	
	TDE- <production></production>		
Per Database	TDE- <databasename></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

TDE-Cer	rtificate(s) Missing
⊗	Copy Certificate [TDE-PSH-Pushy] From : ADEVSQL22\TST (GOS-A, Test) To : ADEVSQL22\ACC (GOS-A, Acceptance) Menu: Admin->Infra->Encryption->TDE-Encryption Needed QGrip role: QGrip-Admin
	ОК

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

g it	E-Encryption									-	. 🗆	×
Filt	er										Refres	h
~	Domain	GOS-B		 EncryptionType 	ENCRYPTED_BY_	MASTE	R_KEY -				Details.	
Г	Environment	Test		👻 🗹 Cert Level	INSTANCE	Ψ.					Create	
☑	Cluster	BDEVSQL19FC			ОК	Ŧ					Create.	
Г	Instance			Show OK-D	ropped Certificates						CopyTo)
		· •									Drop	
	1	-										
TDE	Certificates T	DE-Databases									ExpBack	up
TDE4	Certificates T	DE-Databases Environment	CertLevel	Instance	Name	TDE	#TDE-DBs	Status	Exported		ExpBack	up
IDE4	Certificates T[Domain GOS-B	DE-Databases Environment Production	CertLevel	Instance BDEVSQL1901\PRD1	Name TDE-Test-Number10	TDE V	#TDE-DBs	Status OK-Dropped	Exported		ExpBack Delete	sup
TDE4	Certificates T[Domain GOS-B GOS-B	DE-Databases Environment Production Production	CertLevel INSTANCE INSTANCE	Instance BDEVSQL1901\PRD1 BDEVSQL1901\PRD1	Name TDE-Test-Number10 TDE-Test-Number5	TDE V	#TDE-DBs 0	Status OK-Dropped OK	Exported		ExpBack Delete Add/Del D	oB
rde4	Certificates T[Domain GOS-B GOS-B GOS-B	DE-Databases Environment Production Production Production	CertLevel INSTANCE INSTANCE INSTANCE	Instance BDEVSQL1901\PRD1 BDEVSQL1901\PRD1 BDEVSQL1901\PRD1	Name TDE-Test-Number10 TDE-Test-Number5 TDE-Test-Number6	TDE V V	#TDE-DBs 0 0	Status OK-Dropped OK OK	Exported		ExpBack Delete Add/Del D Close	o B
TDE4	Certificates T[Domain GOS-B GOS-B GOS-B GOS-B	DE-Databases Environment Production Production Production Production	CertLevel INSTANCE INSTANCE INSTANCE INSTANCE	Instance BDEVSQL1901\PRD1 BDEVSQL1901\PRD1 BDEVSQL1901\PRD1 BDEVSQL1901\PRD1	Name TDE-Test-Number10 TDE-Test-Number5 TDE-Test-Number6 TDE-Test-Number7	TDE 2 2 2 2 2 2	#TDE-DBs 0 0 0 0	Status OK-Dropped OK OK OK	Exported		ExpBack Delete Add/Del D Close	ob B
TDE4	Certificates Tr Domain GOS-B GOS-B GOS-B GOS-B GOS-B GOS-B	DE-Databases DE-Databases Production	CertLevel INSTANCE INSTANCE INSTANCE INSTANCE INSTANCE	Instance BDEVSQL1901\PRD1 BDEVSQL1901\PRD1 BDEVSQL1901\PRD1 BDEVSQL1901\PRD1 BDEVSQL1901\PRD1	Name TDE-Test-Number10 TDE-Test-Number5 TDE-Test-Number6 TDE-Test-Number7 TDE-Test-Number8	TDE V V V V V V V V	#TDE-DBs 0 0 0 0 0	Status OK-Dropped OK OK OK OK	Exported		ExpBack Delete Add/Del D Close	B
TDE-	Certificates TT Domain GOS-B GOS-B GOS-B GOS-B GOS-B GOS-B GOS-B	DE-Databases DE-Databases Production Producti Production Production Production Producti	CertLevel INSTANCE INSTANCE INSTANCE INSTANCE INSTANCE INSTANCE	Instance BDEVSQL1901\PRD1 BDEVSQL1901\PRD1 BDEVSQL1901\PRD1 BDEVSQL1901\PRD1 BDEVSQL1901\PRD1 BDEVSQL1901\PRD1 BDEVSQL1901\PRD1 BDEVSQL1901\PRD1	Name TDE-Test-Number10 TDE-Test-Number5 TDE-Test-Number6 TDE-Test-Number7 TDE-Test-Number8 TDE-Test-Number9	TDE V V V V V V V V	#TDE-DBs 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Status OK-Dropped OK OK OK OK	Exported		ExpBack Delete Add/Del D Close	DB

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.

	Refresh		Refresh
	Details		Details
	Create		Create
	CopyTo		CopyTo
TDE-Certificates TDE-Databases	Drop	TDE-Certificates TDE-Databases	Drop
	ExpBackup		ExpBackup
	Delete		Delete
	Add/Del DB		Add/Del DB
	Close		Close

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

Cert Status:	Cert Level:
Import Missing	INSTANCE (master database)
OK-Dropped	Encryption Type:
on propped	ENCRYPTED _BY_MASTER_KEY

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).
ОК	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

_	Refresh	
	Details	
	Create	Filter GOS-A FincryptionType ENCRYPTED_BY_MASTER_KEY
	CopyTo	Environment Acceptance Cert Level INSTANCE
	Drop	Cluster J Status OK J
	ExpBackup	Instance ADEVSQL12\ACC Image: Show OK-Dropped Certificates
	Delete	
	Add/Del DB	TDE-Certificates TDE-Databases
	Close	

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

		TDE-Certificate	: TDE-PSH-Pushy					
Ref	fresh	Certificate	TDE-PSH-Pushy					Close
> Deta	ails	CertLevel	INSTANCE	Domain	GOS-A	LastBackupUTC	2024-10-11 08:52:45	
Cre	ate	StartDate ExpiryDate	2024-10-10 10:22:05	Environment Instance	Test ADEVSQL22\TST	Imported Dropped	2024-10-11 10:52:45	
Cop	yTo	CreatedBy Status	QGrip	Database	master	Exported		
D	rop	Details	,					
ExpB	ackup	PrincipalID CertID	1 Encryption ThumbPrint	Type ENCRYP	PTED_BY_MASTER_KEY BB3CC443A139249294DC052FC9951FB	SFFF		
De	lete	KeyLength	3072 SerialNumb	er 1d 6c 9f	f9 f3 ca 5f 81 4e 11 8f db 06 f3 ef 73			
Add/D	el DB	Subject IssuerName	TDE-PSH-Pushy TDE-PSH-Pushy					
Cl	ose	AttestedBy						
		AddedBy ModifiedBy	Dan-Admin GOS-A\DEV_gMSA_QGnp	At 20 \$ At 20	24-10-11 10:52:41 24-10-11 10:52:45			

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

ØGRIP

Refresh	Create TDE-Certificate
Details	Certificate Name TDE-PSH-Pushy
Create	Subject TDE-PSH-Pushy Confirm Create
CopyTo	Create TDE-Certificate : TDE-PSH-Pushy Level : INSTANCE
Drop	StartDate 2024-10-10 10:22 On ExpiryDate 2028-10-11 10:22 On
ExpBackup	Create On Database : master
Delete	Domain GOS-A Environment Test OK Cancel
Add/Del DB	Instance ADEVSQL22\TST
Close	Database master
	OK Cancel

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

Refresh	Copy TDE-Certificate	Confirm Copy
Details	Certificate Name TDE-PSH-Puthy Subject TDE-PSH-Puthy	Copy TDE-Certificate : TDE-PSH-Pushy Level : INSTANCE
Create	Encryption ENCRYPTED_BY_MASTER_KEY	To Domain : GOS-B
СоруТо	Cert Level INISTANCE Imit StartDate 2024-10-10 10:22 Imit	Environment : Production Instance : BDEVSQL1901\PRD1 Database : master
Drop	ExpiryDate 2028-10-11 10-22	OK Cancel
ExpBackup	Domain GOS-A	
Delete	Instance ADEVSQL22\TST	Always On Cluster
Add/Del DB	Database master	Instance : BDEVSQL1901\PRD1 is part of an Always On Cluster Ofrin will Create/Copy the Cattificate to
Close	Domain GOS-B	all Instances in the Cluster
	Environment Production Instance BDEVSQL1901\PRD1 Database master	OK Cancel
	OK Cancel	

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

ØGRIP

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

TDE-Certificate	TDE-Certificate				
TDE-Certificate protects 18 BackupFile(s) and can not be dropped. TDE-Certificate : TDE-Test-Number2 Level : INSTANCE On Domain : GOS-A Environment : Test Instance : ADEVSQL22\TST Database : master	TDE-Certificate protects 2 database(s) and can not be dropped. TDE-Certificate : TDE-DSH-Pushy Level : INSTANCE On Domain : GOS-A Environment : Test Instance : ADEVSQL22\TST Database : master				
ок	ок				

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

8.6 TDE-Certificate: ExpBackup



Refresh											
Details											
Create		1									
CopyTo TDE-Certificates TDE-Databases											
		Domain	Environment	CertLevel	Instance	Name	TDE	#TDE-DBs	Status	Exported	
Drop		GOS-A	Test	INSTANCE	ADEVSQL22\TST	TDE-PSH-Pushy			ок		
		GOS-A	Test	INSTANCE	ADEVSQL22\TST	TDE-Test-Number1	•		ОК		
ExpBackup	Þ	GOS-A	Test	INSTANCE	ADEVSQL22\TST	TDE-Test-Number2			ок		
Delete											
Add/Del DB											
Close											

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.

	MyTDECerts		
	Name		
	20241012-0718.[1].[ADEVSQL22\$TST].[master].[TDE-Test-Number2].[OK].cert 20241012-0718.[1].[ADEVSQL22\$TST].[master].[TDE-Test-Number2].[OK].key 20241012-0718.[2].[ADEVSQL22\$TST].[master].[TDE-Test-Number1].[OK].cert		
	20241012-0718.[2].[ADEVSQL22\$TST].[master].[TDE-Test-Number1].[OK].key		
	20241012-0718.[3].[ADEVSQL22\$TST].[master].[TDE-PSH-Pushy].[OK].cert		
	20241012-0718.[3].[ADEVSQL22\$TST].[master].[TDE-PSH-Pushy].[OK].key		
Create Script : TDE-Certificates			
Create TDE-Certificates Script			Com
<pre>/************************************</pre>	Certificates \\Dan_Admin 1012-0718 ssible to SQL Server Instance. if files are moved.).cert' key',	Close

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

ØGRIP

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'.

	Refresh		Ļ										
	Dataila	TDE-C	ertificates	TDE-Databases									
	Detalls		Domain	Environment	CertLevel	Instance		Name		TDE	#TDE-DBs	Status	Exported
	Create	Þ	GOS-B	Production	INSTANCE	BDEVSQL190	1\PRD	1 TDE-Te	st-Number10			0 OK-Dropped	
			GOS-B	Production	INSTANCE	BDEVSQL190	2\PRD	2 TDE-Te	st-Number10			0 OK-Dropped	
	CopyTo		Confirm	Valata				Confirm	Delete				
	Drop		Continue	Delete from QGrij	p Administrat	tion?	Delete from OGrip Administratio					tration?	
	ExpBackup		0	TDE-Certificate Level On	: TDE-Test-Nu : INSTANCE	umber10		0	TDE-Certi Level	ficat	e : TDE-Tes : INSTANC	t-Number10	
-	Delete		Ø	Domain Environment Instance	GOS-B Production BDEVSQL1901	L\PRD1		Ø	Domain Environme	nt	: GOS-B : Product:	ion	
	Add/Del DB			Database Status	Master OK-Dropped				Database Status		: master : OK-Drop	ped	
	Close				ОК	Cancel					ОК	Cancel	

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.

	Refresh													
	Details													
	Create		L I											
	CopyTo	TDE-Ce	ertificates	TDE	E-Databases									
	Drop		Domain		Environment	j.	nstance	Name	TDE	#TDE-DBs		Status	E	Exported
		▶	GOS-A		Test	A	DEVSQL22\TST	TDE-PSH-Pushy			2	ОК		
	ExpBackup													
	Delete													
-	Add/Del DB													
	Close													

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



TDE-Databases for TDE-Certificate: TDE-PSH-Pushy Certificate Name TDE-PSH-Pushy ThumbPrint Dx076088B3CC443A139249294DC052FC99	Doma 51FB5FFF Envir Instar	e ADEVSQL22\TST	Refresh Close
Databases 1. TDE-Databases Certificate TDE-PSH-Pushy Database Application Status PSH_T_Staging PSH-Pushy ENCRYPTED	3. Encryption Algorithm AES_256 < <enable<< <<enable<< td=""> <<enable+encrypt<< td=""> >>(Decrypt+)Disable>></enable+encrypt<<></enable<<></enable<< 	Z. TDE-Candidates Application Database Application Listener PSH_T_Core PSH-Pushy TDE_T TDE-TestApp TDE_T_Main2 TDE-TestApp tDE_T_Main2 TDE-TestApp	Deta(MB

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	
AES_256 -	
< <enable<<< td=""><td></td></enable<<<>	
< <enable+encrypt<<< td=""><td></td></enable+encrypt<<<>	
>>(Decrypt+)Disable>>	

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.



Databas TDE-I Certific	ees Databases cate TDE-PSH-Pu	shy				TDE-	Candidates	Pushy		•
•	Database PSH_T_Staging	Application PSH-Pushy	Status ENCRYPTED	2. 3.	Encryption Algorithm AES_256 </td <td>Þ</td> <td>Database PSH_T_Core</td> <td>Application PSH-Pushy</td> <td>Listener</td> <td>Data (MB</td>	Þ	Database PSH_T_Core	Application PSH-Pushy	Listener	Data (MB
•			•		< <enable+encrypt<<>>(Decrypt+)Disable>></enable+encrypt<<>	٩				•

Enable:

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

Confirm	Action	TOP D			
0	Enable TDE on Database : PSH_T_Core Application : PSH-Pushy	Certific	atabases ate TDE-PSH-Pu	shy	
	Algorithm : AES_256 Using		Database	Application	Status
	Certificate : TDE-PSH-Pushy	<u>۲</u>	PSH_T_Core	PSH-Pushy	Queued for Enable
			PSH_T_Staging	PSH-Pushy	ENCRYPTED
	OK Cancel				

- 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.

DE-I	cate TDE-PSH-Pu	shy				App	olication P	SH-Pushy		•
	Database	Application	Status]_	Encryption Algorithm		Database	Application	Listener	Data(MB
	PSH_T_Staging	PSH-Pushy	ENCRYPTED	2.	AES_256	▶	PSH_T_C	ore PSH-Pushy		
					< <enable<<< td=""><td></td><td></td><td></td><td></td><td></td></enable<<<>					
				3.	< <enable+encrypt<<< td=""><td></td><td></td><td></td><td></td><td></td></enable+encrypt<<<>					

Enable+Encrypt:

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



Confirm	Action					
0	Enable TDE + Encrypt Database : PSH_T_Core Application : PSH-Pushy Algorithm : AES 256	C	DE-Data ertificate	bases TDE-PSH-Pu	shy	
	Est Encrypt Time : 3 Seconds	Γ	(Database	Application	Status
	Certificate : TDE-PSH-Pushy		P	SH_T_Core	PSH-Pushy	Queued for Enable+Encrypt
			P	SH_T_Staging	PSH-Pushy	ENCRYPTED
	OK Cancel					

- 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.

	Databas TDE-D Certific	es Databases cate TDE-PSH-Pu	shy			TDE-	Candidates			Y
		Database	Application	Status	Encryption Algorithm		Database	Application	Listener	Data(MB)
1.	Þ	PSH_T_Core PSH_T_Staging	PSH-Pushy PSH-Pushy	ENCRYPTED	<=Enable<<		TDE_T TDE_T_Main2	TDE-TestApp TDE-TestApp		
	•			Þ	< <enable+encrypt<< 2.="">>(Decrypt+)Disable>></enable+encrypt<<>	4				×

(Decrypt+)Disable:

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

Confirm	Action								
?	Disable TDE Database : PSH_T_Core Application : PSH-Pushy Used		Certificate TDE-PSH-Pushy						
	Certificate : TDE-PSH-Pushy			Database	Application	Status			
			•	PSH_T_Core	PSH-Pushy	Queued for Disable			
	OK Cancel								

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.



onnin	Action		TDE	-Databases		
0	Decrypt + Disab Database Application	le TDE : PSH_T_Staging : PSH-Pushy	Certi	ficate TDE-PSH-Pu	ishy	
9	Est Decrypt Tim	e : No estimate possible		Database	Application	Status
	Certificate	: TDE-PSH-Pushy	Þ.	PSH_T_Core	PSH-Pushy	UNENCRYPTED
				PSH_T_Staging	PSH-Pushy	Queued for Decrypt+Disab

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)

	Refresh								
-	Details								
	Create			4					
	CopyTo	TD	E-Certificates TD	E-Databases					
	Dree		Domain	Environment	Instance	Listener	Database /	Encryption State	CertName
	Drop	Þ	GOS-A	Test	ADEVSQL22\TST		PSH_T_Core	UNENCRYPTED	TDE-PSH-Pushy
	ExpBackup								
	Delete								
	Add/Del DB								
	Close								

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



Destaura			0		Refresh
Database	PSH_T_Core		Domain	JGOS-A	Decrypt
Application	PSH-Pushy		Environment	Test	L. Encrypt
Data (MB)	10		Instance	ADEVSQL22\TST	
Log (MB)	10		Listener		Close
Encryptions ScanState	State UNENCRYPTED COMPLETE	SetDate ScanDa	2024-10-1 te 2024-10-1	13 10:07:43 13 10:12:13	

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.

EncryptionState UNENCRYPTED	Confirm Action	
Refresh	Encrypt Database : PSH_T_Core Application : PSH-Pushy	EncryptionState Queued for Encrypt
Encrypt	Using Certificate : TDE-PSH-Pushy EncryptionState	EncryptionState ENCRYPTED
Close	OK Cancel	

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.

EncryptionState ENCRYPTED	Confirm Action	EncryptionState Queued for Decrypt
Refresh	Decrypt Database : PSH_T_Core	,
Decrypt	Application : PSH-Pushy Est Decrypt Time : 2 Seconds	Refresh
Encrypt	Certificate : TDE-PSH-Pushy	EncryptionState UNENCRYPTED
Close	OK Cancel	



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.

Description:	Select Users, Computers, Service Accounts, or Groups	×
	Select this object type:	
Members:	Users, Service Accounts, or Groups	Object Types
🛃 Administrator	From this location:	
Anjemberg	GOS-A intra	Locations
& GOS-AlDoma & GOS-AlGS_A ₩ GOS-AlTST_¢	Enter the object names to select (examples): DEV_gMSA_QGrip	Check Name
	Advanced	ок 🗧 Салан
Add	Changes to a user's group membership are not effective until the next time the user loos on.	

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