QGrip
Backup Encryption

GRIP ON SQL

2024-04-16

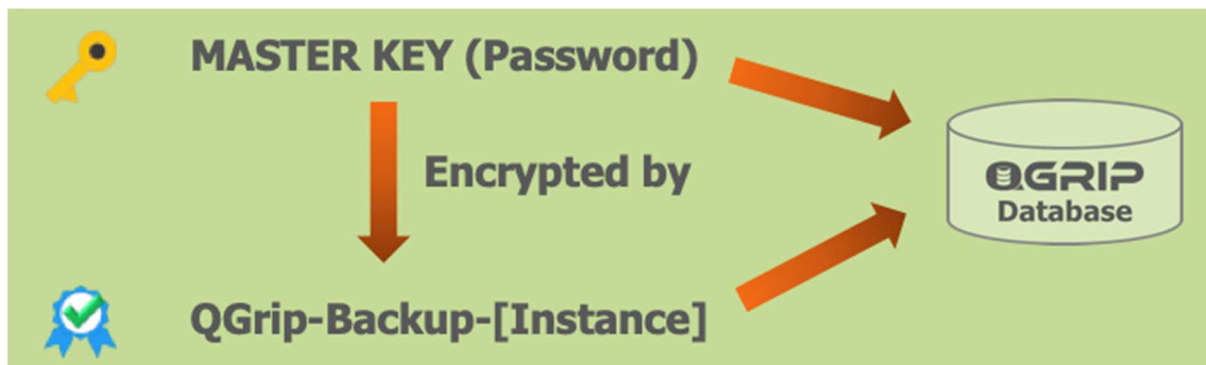Contents

1 Introduction

Pre-request

Doc-Tab	Title
Infra	Encryption (Keys and Certificates)

QGrip offers an easy way to Encrypt the Database and Log backups.

When the backups run with the backup option 'Encrypt', QGrip will automatically create a certificate [QGrip-Backup-INSTANCENAME-YYYYMMDD-hhmmss] on the SQL Server Instance if it does not already exist or if the existing Certificate is about to expire.
The certificate is ENCRYPTED_BY_MASTER_KEY.
If necessary, the MASTER KEY will be created as well.
MASTER KEY and Certificate will be Imported to the QGrip database to ensure availability.

QGrip will create separate certificates for each SQL Server Instance using Encryption.

When the backup is made, the QGrip internal CertificateID is saved together with the Backup record in the QGrip database.

When a database with QGrip encrypted backup files is restored or cloned, the Certificate will automatically and temporarily be created on the Destination Instance.

QGrip must be able to manage encryption objects like symmetric keys and certificates and the QGrip System Account must be added to the local Administrators group on all Backup Share servers as described in the document mentioned here above.

2 Enable QGrip Backup Encryption
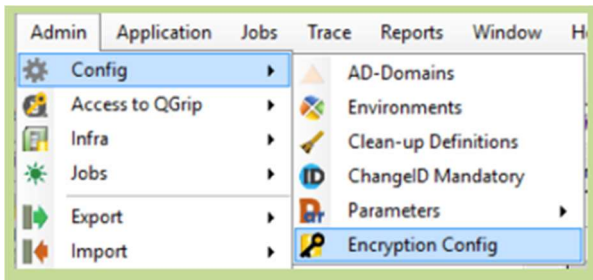
Before you enable 'QGrip Backup Encryption', make sure you have read the Document above and that all steps for enable 'Symmetric Keys and Certificates' have been executed correctly. QGrip will not be able to check that everything has been configured correctly and missed steps will result in run time errors.
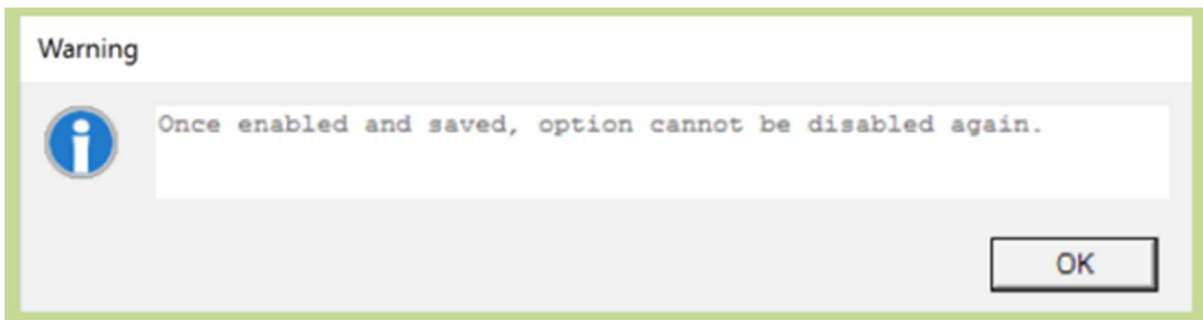
2.1 Encryption Config
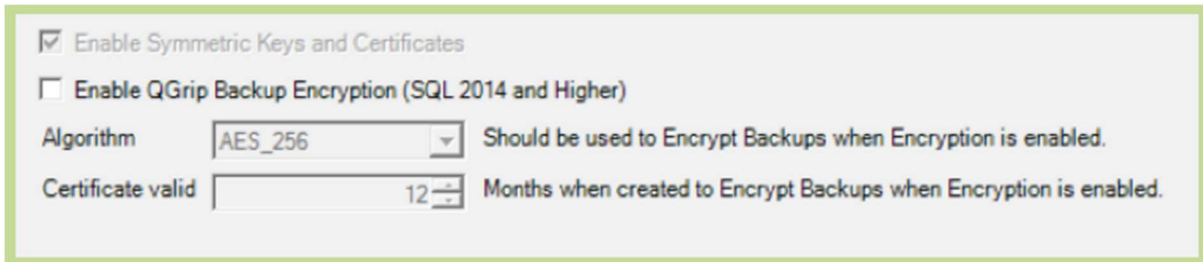
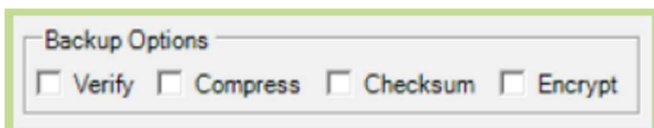Open the Encryption Config in QGrip (Admin->Config->Encryption Config).

Check the 'Enable QGrip Backup Encryption' checkbox.

Once the option has been enabled and saved, it cannot be disabled again.

Choose Algorithm and the number of months the 'Grip Backup Certificate' should be valid.

The Backup Option 'Encrypt' will now be visible for SQL Server instances of version 2014 or higher.