Password Safe

&

Connect Info

GRIP ON SQL

2024-04-16

Contents

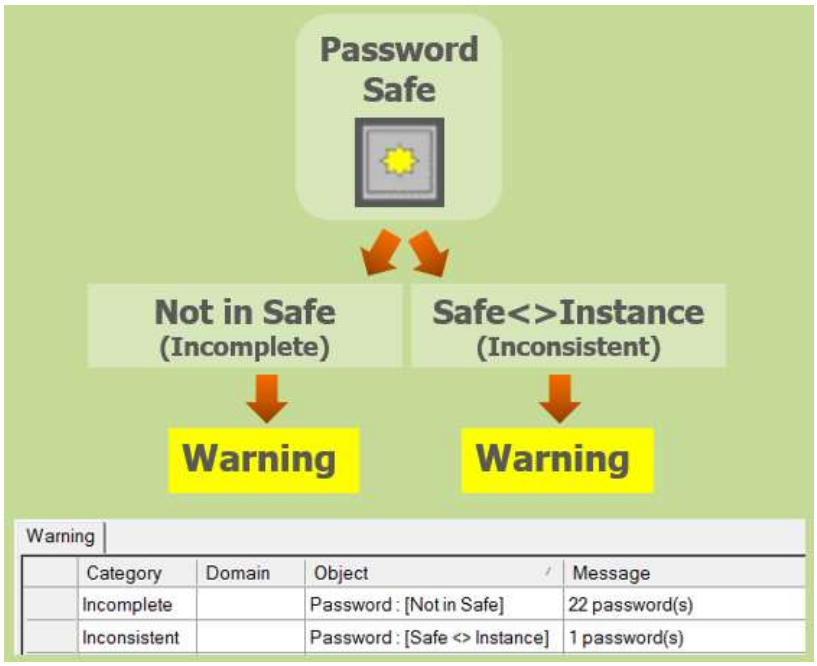
1 Password Safe 3
2 Password Warnings 3
3 Password Changes 4
3.1 QGrip-UI – Password & Scope 5
3.2 QGrip-UI – Actions 5
4 QGrip-UI – Password Safe 6
5 Password Security 8
5.1 Authorisation 8
5.2 Communication 8
5.3 Verify Password Job 8
5.4 Max Length Password 9
6 Connect Info 9

1 Password Safe

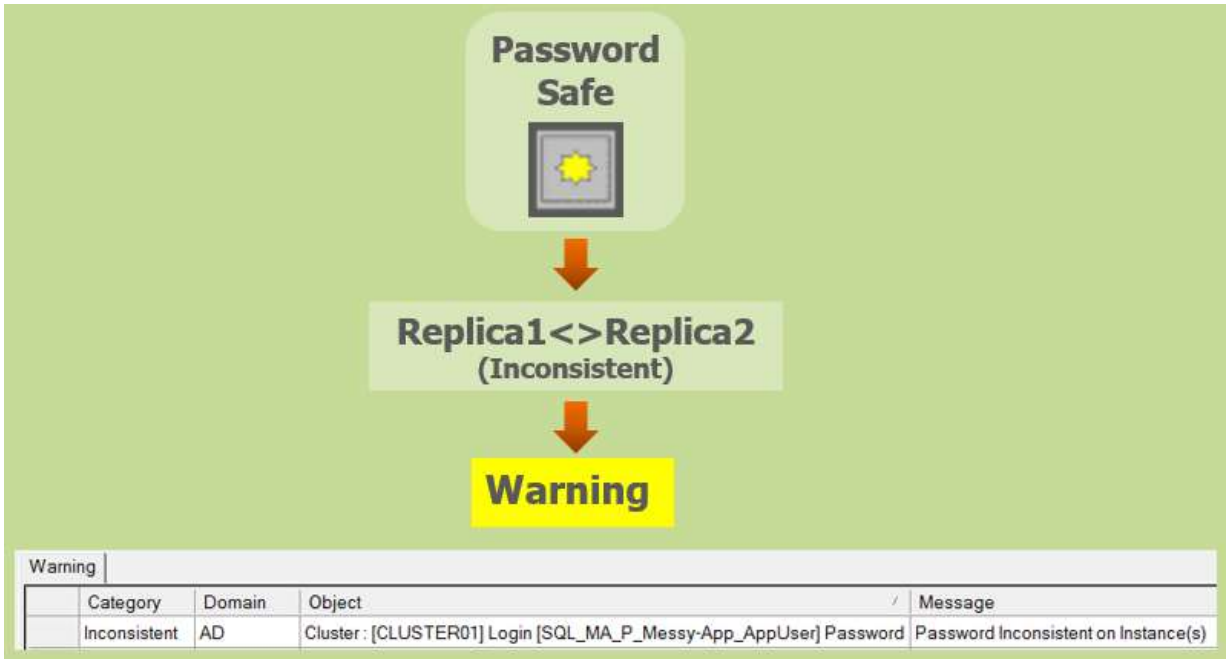
QGrip comes with a Password Safe. The aim is that the Password Safe contains all SQL Login passwords. When you start using QGrip, it is important to take the time to add all the passwords of existing SQL logins to the Safe.

A password has status; ‘OK’, ‘Not in Safe’ and ‘Safe <> Instance’.

2 Password Warnings

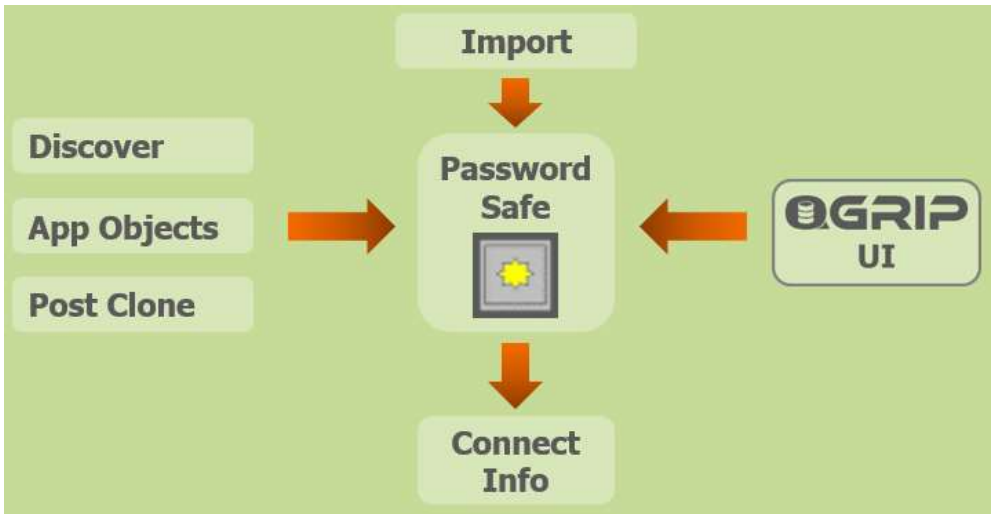


Missing or incorrect passwords can be a threat to continuity and are being checked regularly. Warnings are generated if there are password issues.



On an AlwaysOn cluster, the consistency of the passwords on the different replicas is also checked to prevent password issues after a failover. The 'sa' account (or renamed equivalent) is excepted from this check.

3 Password Changes



- The **Import** module can be used to add missing passwords to the Password Safe.
- The **Discover** job add and removes logins from the password safe and checks if passwords have been changed on the Instance and not in the Password safe.
- **App Objects** and **Post Clone** scripts add Login and correct password to the safe.
- The **QGrip-UI** is used to add missing password and change password in the safe and on the Instance.
- **Connect Info** gets its information from the Password Safe.

3.1 QGrip-UI – Password & Scope

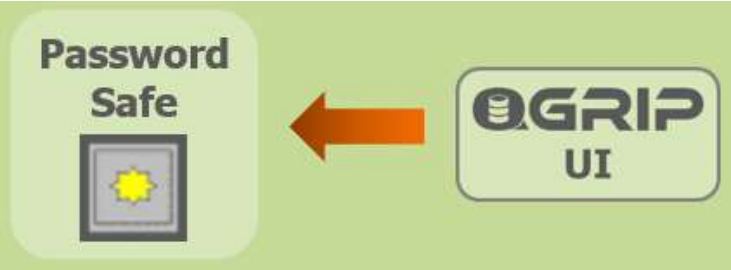
Password

-New Password	Manually entered password by User
-Generated Password	QGrip generates a random password
-Existing Password	The current password in the Password safe

Scope

-Safe	Save password in Password Safe
-Verify	Verify password by login job from QGrip Server
-Instance	Change the password on the Instance

3.2 QGrip-UI – Actions



The actions that can be done on the Logins/Passwords in the Password Safe depend on the Password status.

OK
Password
-New Password
-Generated Password
Scope
-Safe + Instance

It is only possible to change passwords on the Instances if the password status is OK. Password change can either be done with a manually entered password or QGrip can generate it.

Safe <> Instance	Not in Safe
Password	**Password**
-New Password	-New Password
Scope	**Scope**
-Safe + Verify	-Safe + Verify

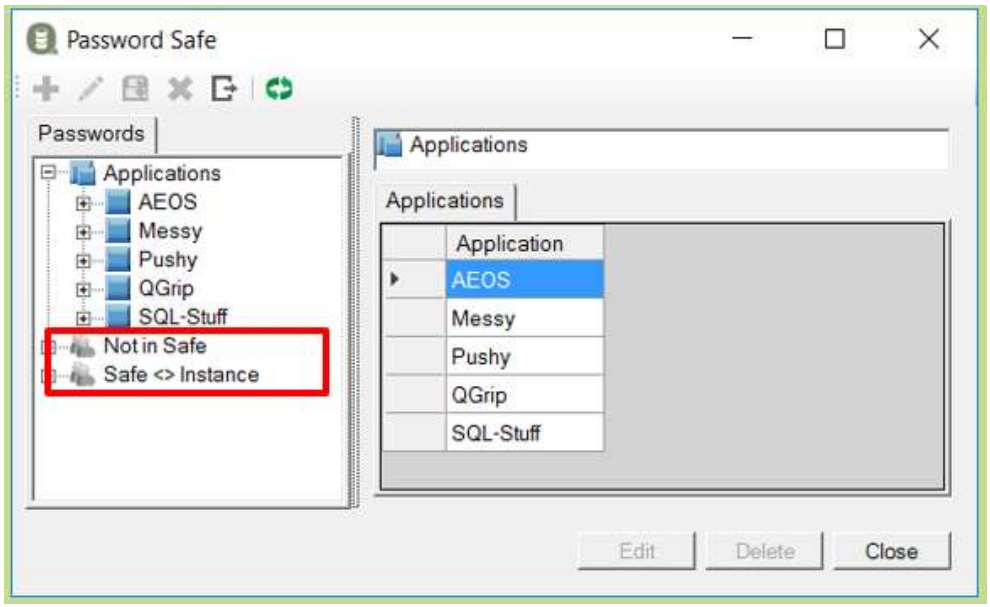
If the password in the Safe is not correct or missing, the only option is to manually enter a valid password, save it in the Safe and let QGrip verify it to see if it is correct.

Safe <> Instance
Password
-Existing Password
Scope
-Verify

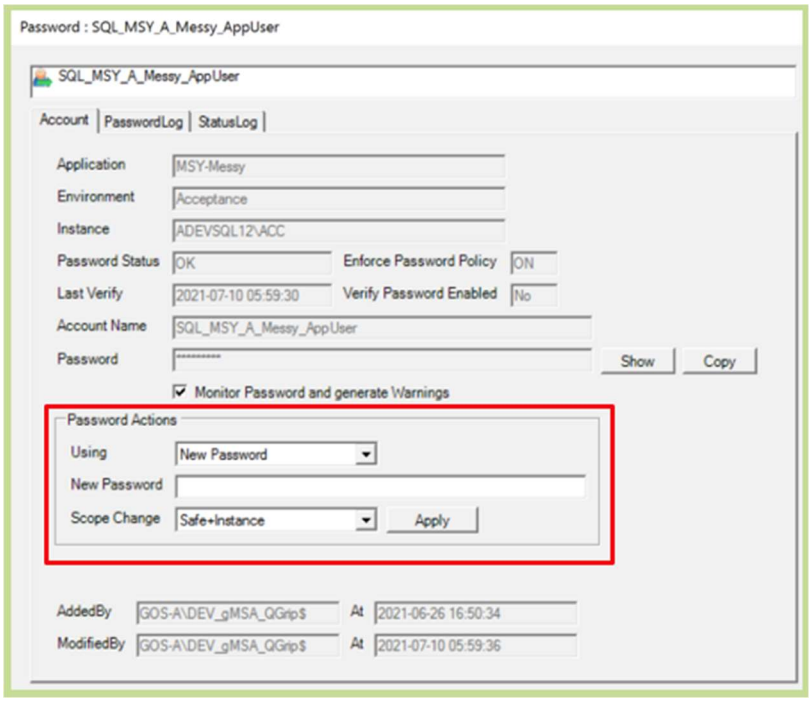
If there is a password in the Safe, you can let QGrip verify it to see if it is valid.

Verify Password
The QGrip Server picks up the Encrypted password and tries to Connect to the Instance using Login/Password. If it fails, password verification for that Login will be blocked for 60 minutes. This is to prevent hacking and lock out of the Login. The QGrip Admin will receive an Error message for each failed Verify Password jobs.

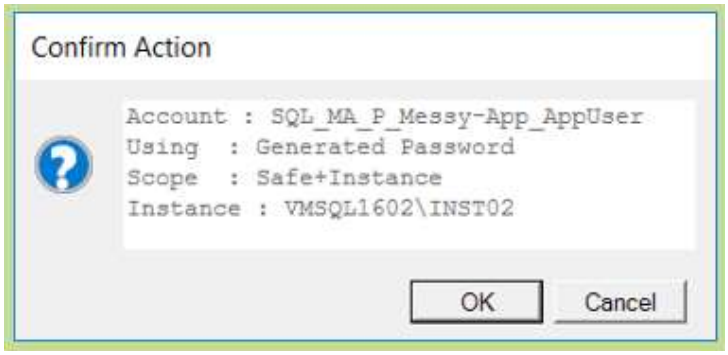
4 QGrip-UI – Password Safe



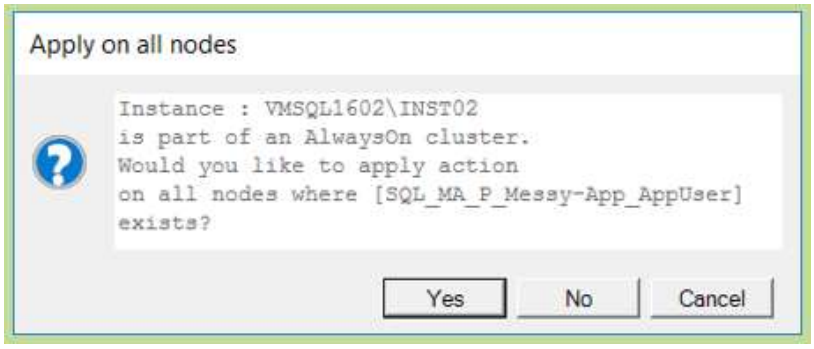
Incomplete/Inconsistent passwords can easily be found in the extra containers. A separate container, No Password Monitoring, will also be shown for Passwords that have been excluded from Monitoring.



Password actions are done in the Edit window of an account. Only valid actions will be available. Choose your options and press Apply.



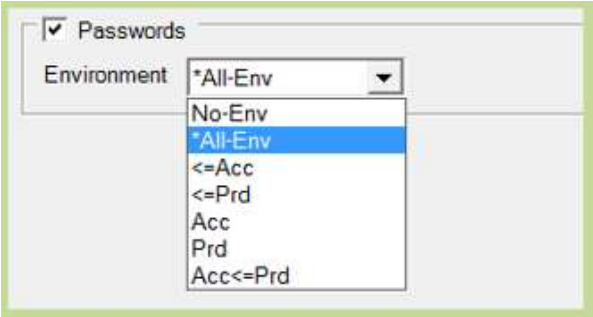
Confirmation is always needed. Personal message will be issued when actions has completed.



If the requested action is on an Account on an AlwaysOn cluster, you will be asked if the actions should be done on all nodes/replicas.

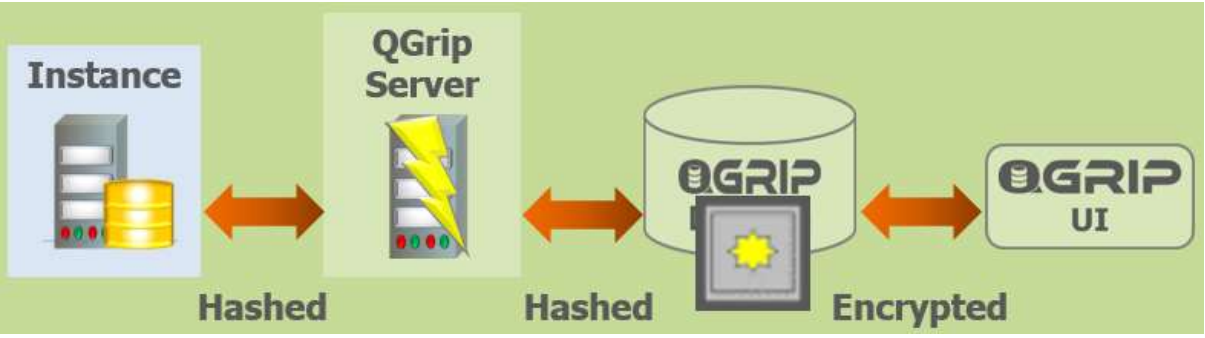
5 Password Security

5.1 Authorisation



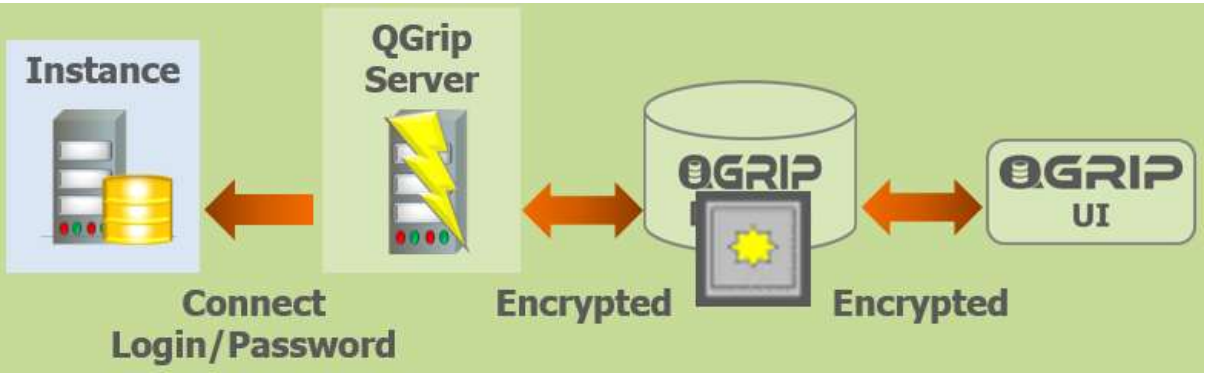
QGrip Users will only be able to see passwords for the applications and environments they have been authorised for. The Passwords are encrypted in the Database and can only be decrypted by the QGrip executables (QGrip-UI / QGrip worker processes)**.** Whenever a QGrip User is authorised for passwords, he is regarded as responsible, and can also change the passwords on the Instance via the QGrip-UI.

5.2 Communication



Passwords are never sent as plain text over the network. Between Instance, QGrip Server and QGrip Database, the Hashed password is used. Between the QGrip-UI and the QGrip Database a transport Encryption is used that changes continuously. The transport Encryption is different to the Password table encryption in the database.

5.3 Verify Password Job



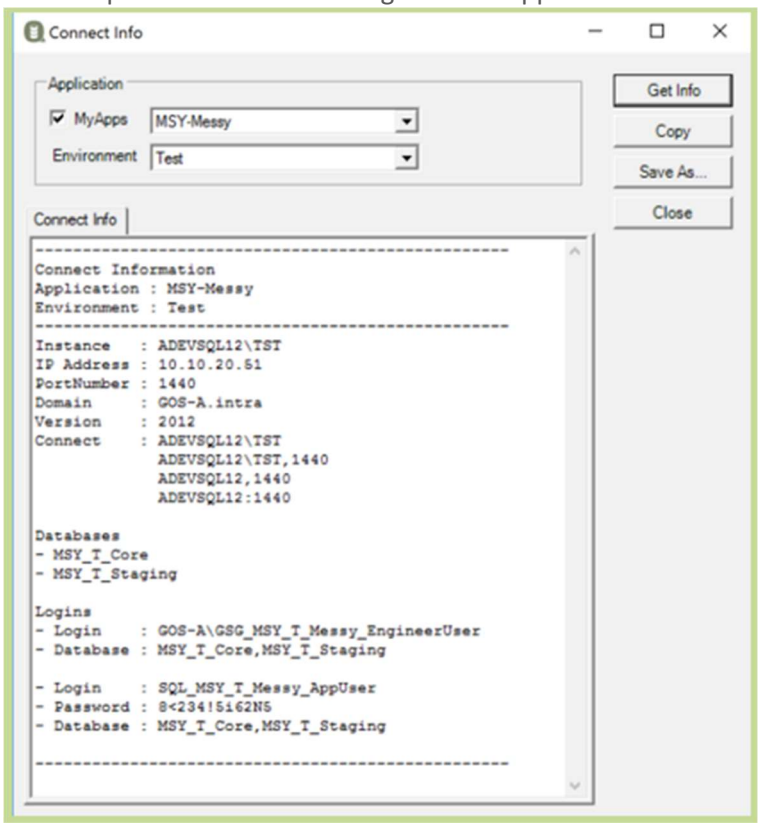
The QGrip Servers picks up the Encrypted password and tries to Connect to the Instance using Login/Password. If it fails, password verification for that Login will be blocked for 24 hours. This is to prevent hacking and lock out of the Login. The QGrip Admin will receive an Error message for failed Verify Password jobs.

5.4 Max Length Password

The max length passwords that QGrip can handle is 120.

6 Connect Info

The Connect Info uses the content of the Password safe. The Connect Info can be used to share connect parameters with colleagues and suppliers.



Select Application and Environment and Press 'Get Info'. AD logins will also be included.
If a password is not valid, you will receive a warning but the information will still be provided (without the missing password).