



Access to QGrip

GRIP ON SOL

2024-04-16

Contents

1	Introduction	3
2	QGrip Login	3
3	QGrip Login versus QGrip-User	3
4	User Login - Preferred	5
5	QGrip-User - Authorisation	5
6	Extra security measures	6

1 Introduction

Access to QGrip is built up by 3 different layers:

- QGrip Login (Login on QGrip DB Host)
- QGrip-User (User in QGrip)
- Teams & Authorisation (Authorisation within QGrip)

Teams & Authorisation is described in detail in separate document.

2 QGrip Login

- **User Login**
 - AD-Group, AD-User
 - QGrip users using QGrip UI
- **Export Login**
 - AD-Group, AD-User, SQL Login
 - Export CMDDB
- **Monitor Login**
 - AD-Group, AD-User, SQL Login
 - External Monitoring
- **QGripSQLInstall**
 - SQL Login
 - Temp for Install QGrip Server Multiple Domain. Delete after use!

There are 4 types of QGrip Logins. Only the User Login is described in this document.

Use QGrip UI

Admin->Access to QGrip->QGrip Logins

- **Only for QGrip-Admin**
- **Job via QGrip Servers**
- **Password in Password Safe**
 - If applicable
- **On all Replicas**
 - If AlwaysOn

The QGrip logins should all be created using the QGrip-UI.

3 QGrip Login versus QGrip-User

QGrip Login

- Access to QGrip DB Host
 - Instance (Stand Alone)
 - All Replicas (AlwaysOn)

QGrip User

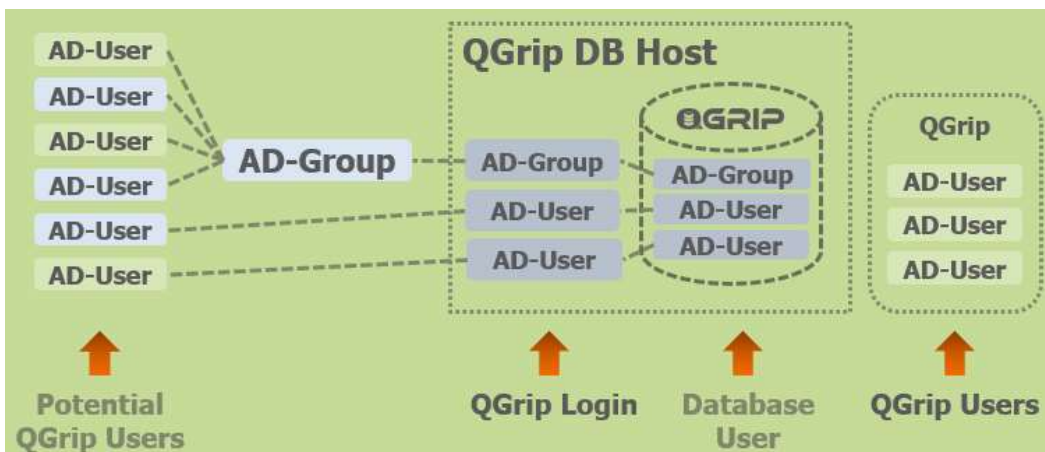
- Added as QGrip user in QGrip Administration

The QGrip Login is the login on Instance level and should preferably be a Windows Group.
The QGrip-User Windows User is a member of that Windows Group.

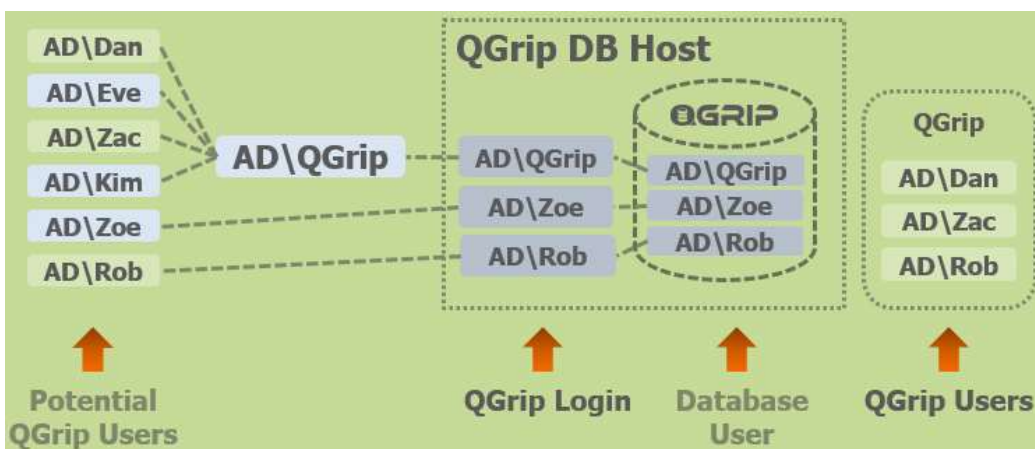
Become QGrip User

- After first login via QGrip UI
- or
- Added by QGrip Admin in advance

An AD-User can have access to QGrip via and AD-Group but will not become a QGrip-User until after first time login via the QGrip-UI or when added as QGrip-User in advance by the QGrip-Admin.

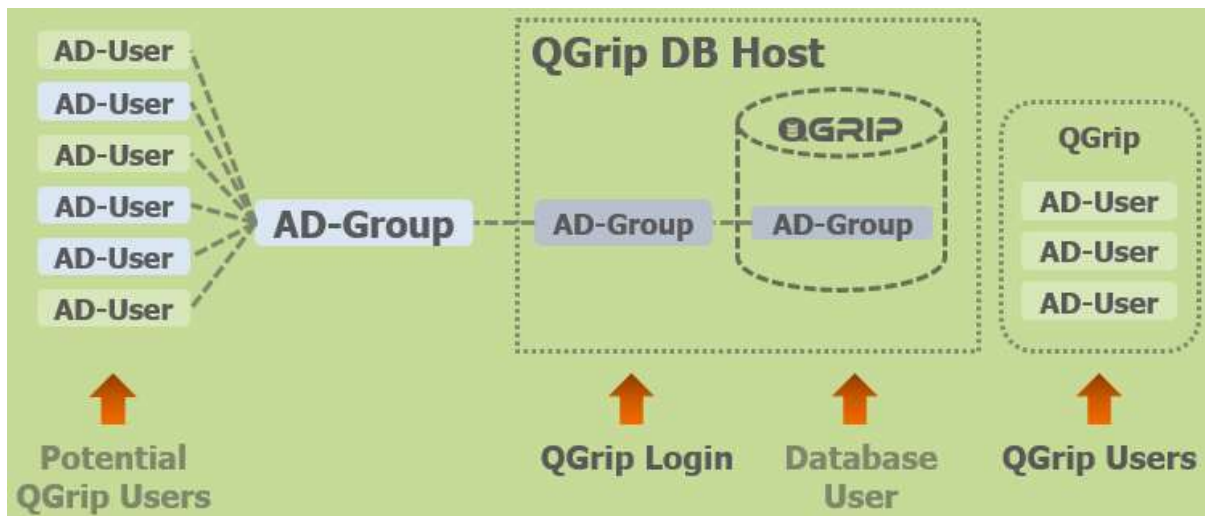


The blue AD-Users have not yet used the QGrip-UI and are not yet QGrip Users.



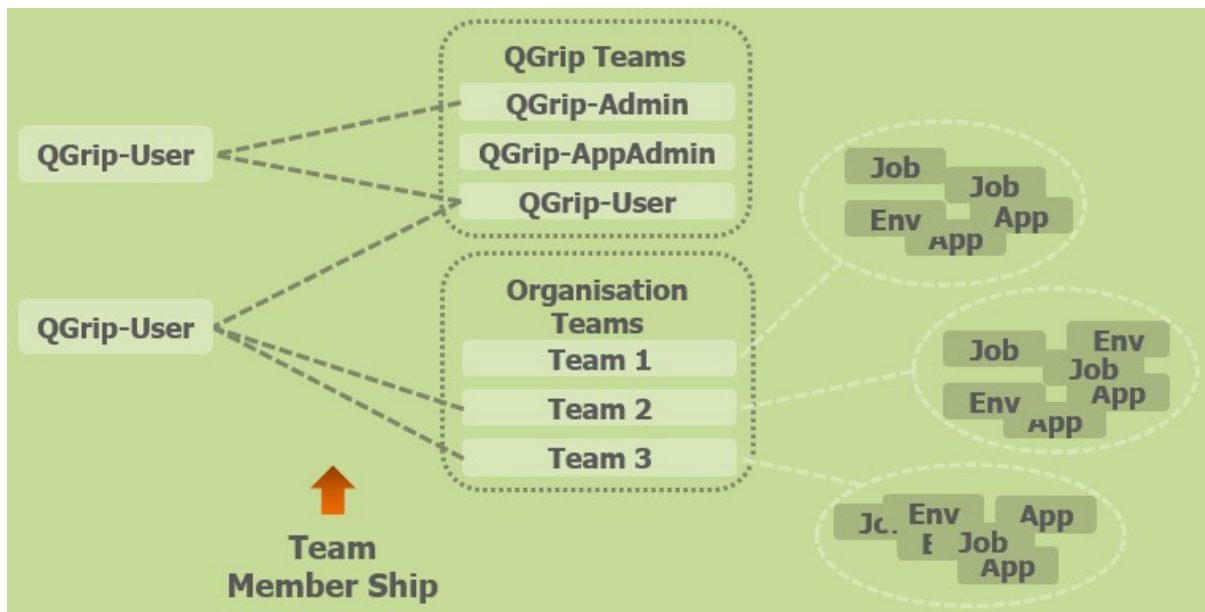
In the example above, AD\Eve, AD\Kim and AD\Zoe are not (yet) QGrip Users.

4 User Login - Preferred



The best option is to have one AD-Group with all QGrip Users where users can simply be added and removed at AD level.

5 QGrip-User - Authorisation



What the different QGrip users are authorised to do within QGrip depend on Team member ship.

The QGrip teams are fixed teams that do always exist. It is possible to change some of the authorisations within the QGrip teams except the QGrip-User team. The QGrip-User team will remain a team without any privileges that every QGrip-User is member of.

The Organisation Teams must be created before they can be used.

The QGrip-User can apply for Team membership using the QGrip-UI. The request must be approved by a QGrip-User with approval authorisation.

6 Extra security measures

The QGrip-Users are automatically database users on the QGrip database. To prevent a QGrip-User from performing unauthorised actions on the database using SQL Server Management Studio or another tool, the following controls are embedded:

- Only enabled to execute Stored Procedure and some functions (no tables).
- Stored procedures, Functions and triggers are encrypted.
- Extra Authorisation check in Stored procedures.

When the QGrip-UI is used, a secret key is generated and used for invoking certain actions. Attempts to invoke these actions with the wrong key will blacklist the user.