Active Directory Synchronization

1 Contents

1 Preface

This document describes steps necessary to set up a synchronization with Active Directory Services

2 Prerequisites

In order to set up a synchronization with Active Directory Services the following requirements have to be met:

- QEF and QEF Admin Console are installed and accessible;

3 Active Directory synchronization

QEF provides an ability to register AD users and groups and later use Windows credentials to be authenticated in QEF or its modules from both, On-Premise and Azure AD services.

Authentication of AD users is supported in two formats:
User Principal Name (UPN) - user@domain.com
SAM Account name (SAM) - domain\user or domain.com\user

Despite support of two formats, all AD users and groups created in QEF are displayed in UPN formant.

Data used from On-Premise AD to create and update users in QEF:

User attribute in AD	User property
objectGUID	Identifier
objectCategory	Type of LDAP object
userAccountControl	Is disabled
msDS-UserAccountDisabled (if userAccountControl undefined)	Is disabled
isDeleted	Is deleted
userPrincipalName	Login
sAMAccountName (if userPrincipalName undefined)	Login
givenName	First name
sn	Last name
description	Description
uSNChanged	Type of change
primaryGroupId	First part of identifier of primary group
memberOf	Member of
objectSid	Second part of identifier of primary group

Data used from On-Premise AD to create and update groups in QEF:

Group attribute in AD	Group property
objectGUID	Identifier
objectCategory	Type of LDAP object
isDeleted	Is deleted
name	Name
sAMAccountName (if name undefined)	Name
description	Description
uSNChanged	Type of change
member	Members
primaryGroupToken	Identifier of primary group

Data used from Azure AD to create and update users in QEF:

User attribute in AD	User property
ObjectId	Identifier
AccountEnabled	Is disabled
UserPrincipalName	Login
GivenName	First name
Surname	Last name
MemberOf	Member of

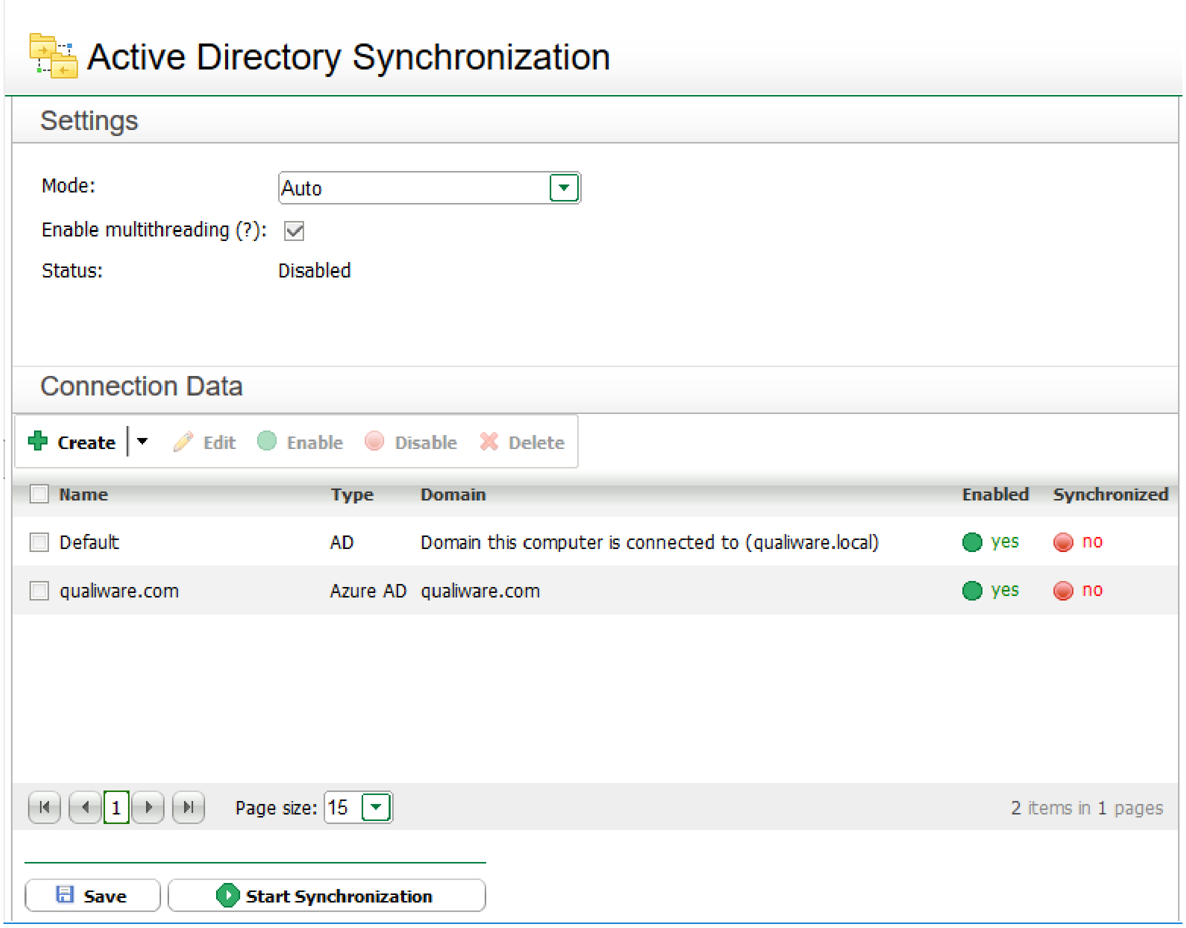
Data used from Azure AD to create and update groups in QEF:

Group attribute in AD	Group property
ObjectId	Identifier
Display Name	Name
Description	Description
Members	Members

N.B. QEF can authenticate an AD user only when synchronization is on despite user exists in QEF.

Active Directory synchronization settings are split into synchronization settings and list of connection data.

Settings include:



Active Directory Synchronization

Settings

Mode:	Auto
Enable multithreading (?):	☑
Status:	Disabled

Connection Data

□ Name	Type	Domain	Enabled	Synchronized
□ Default	AD	Domain this computer is connected to (qualiware.local)	● yes	● no
□ qualiware.com	Azure AD	qualiware.com	● yes	● no

Page size: 15

2 items in 1 pages

Mode:

- Auto - Synchronization is done once when it is started and when there are any changes in Active Directory (changes in Azure AD are tracked by polling differential queries).

- Manual - Synchronization is done once when it is started. Synchronization can be requested explicitly.

- Recurrent - Synchronization is done once when it is started and at specified time. Additionally, synchronization can be requested explicitly.

Enable multithreading – whether to use parallelism in membership resolving and persisting data to QEF DB. Can cause high load of AD and DB servers.

List of **Connection Data** specifies On-Premise AD servers or Azure AD tenants QEF synchronizes with.

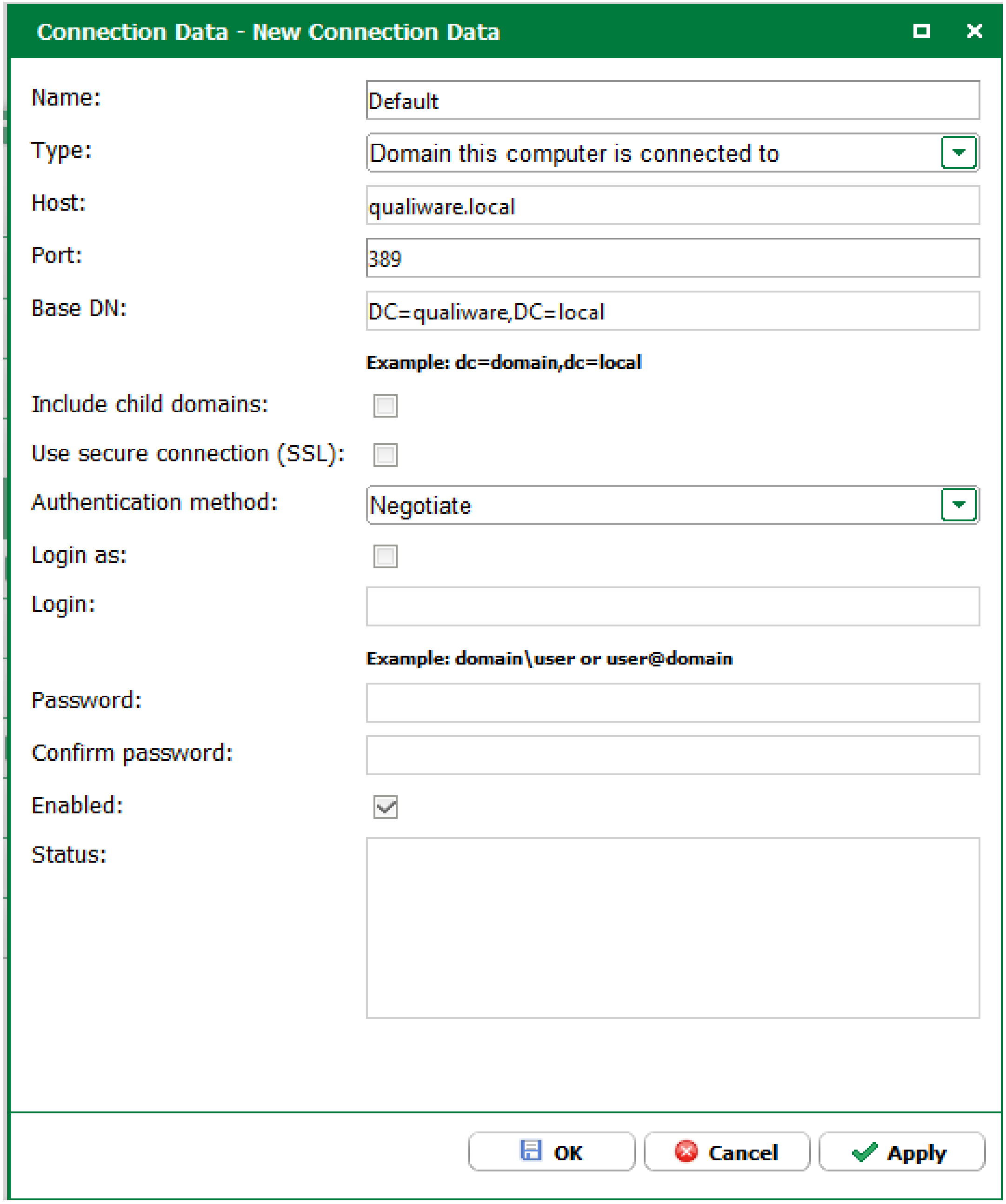
The current status of synchronization is displayed in a separate field. Additionally, each connection data displays its own synchronization status.

To start synchronization, click **Start synchronization*** button.
To stop it click **Stop synchronization** button.
Delete Users and Groups button removes all synchronized AD users and groups**.

** If QEF database contains users and groups from another domain they will be automatically removed.*
*** After user click the button only synchronized AD users will be deleted. All local users and groups will be preserved.*

3.1 On-Premise AD connection data

Below is the form for On-Premise AD connection data:



Connection Data - New Connection Data

Name:	Default
Type:	Domain this computer is connected to
Host:	qualiware.local
Port:	389
Base DN:	DC=qualiware,DC=local Example: dc=domain,dc=local
Include child domains:	☐
Use secure connection (SSL):	☐
Authentication method:	Negotiate
Login as:	☐
Login:	 Example: domain\user or user@domain
Password:	
Confirm password:	
Enabled:	☑
Status:	

Type:

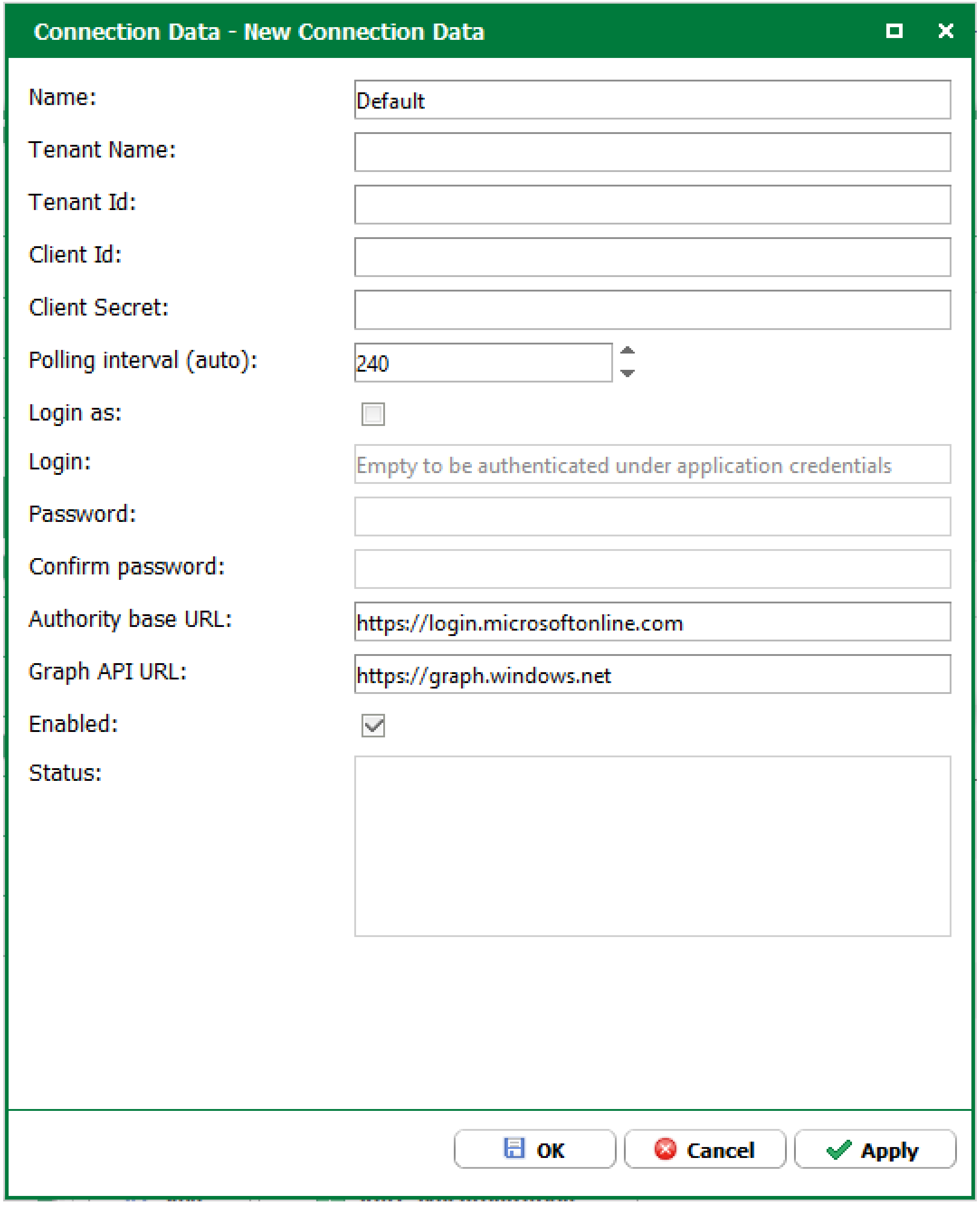
- **Domain this computer is connected to** (PCDomain) - Synchronize with a domain the computer running QEF process belongs to.

- **Domain the current user is connected to** (UserDomain) - Synchronize with a domain the account QEF process is run under belongs to.
- **Generic LDAP server** (Custom) - User can manually specify connection string to an LDAP server.

Host – DNS name or IP address of an AD server to connect to.
Port – Port of an AD server to connect to.
Base DN – Distinguishing Name of a container to synchronize with. Only whole domain (DC) or OrganizationalUnit (OU) are supported.
Include child domains - Synchronize with child domains or not.
Use secure connection (SSL) – Whether to establish a secure connection or not.
Authentication method – Which method to use: Negotiate or Simple.
Login as – Whether to use explicit user-defined credentials to connect to Active Directory server with.
Login – Explicit user-defined credentials to connect to Active Directory server with. Only login in full UPN or SAM format is valid.
Enabled - enable or disable synchronization with Active Directory server.
Status - Synchronization status when it is started.

3.2 Azure AD connection data

Below is the form for Azure AD connection data:



Connection Data - New Connection Data

Name:	Default
Tenant Name:	
Tenant Id:	
Client Id:	
Client Secret:	
Polling interval (auto):	240
Login as:	□
Login:	Empty to be authenticated under application credentials
Password:	
Confirm password:	
Authority base URL:	https://login.microsoftonline.com
Graph API URL:	https://graph.windows.net
Enabled:	☑
Status:	

Tenant Name – The name of a tenant in Azure AD to synchronize with. Optional.
Tenant Id – The identifier (GUID) of a tenant in Azure AD to synchronize with. Required.
Client Id – The identifier (GUID) of QEF registered as client application in Azure AD. Required.
Client Secret – Secret key string issued by Azure AD if QEF is registered as web application. Optional.

Polling interval (auto) – Defines an interval for Auto mode to poll Azure AD with (differential queries).
Login as – Whether to use explicit user-defined credentials to connect to Azure AD with. Used if QEF is registered as native application in Azure AD.
Login – Explicit user-defined credentials to connect to Azure AD with. Only login in full UPN format is valid.
Authority base URL – URL of Azure AD services provider. Gets filled with Microsoft cloud default.
Graph API URL – URL of graph API RESTful service in Azure AD. Gets filled with Microsoft cloud default.
Enabled - enable or disable synchronization with Active Directory server.
Status - Synchronization status when it is started.

4 Advanced Setup

General considerations to set up a synchronization not with a whole domain but only some its part(s) (OUs) do the following.

- Choose minimal container with needed objects. Choose more than one if necessary.
- Sometimes users and groups are placed in different OUs. In such a case if membership is important synchronize with both OUs, users and groups.
- Synchronization with different domains is supported.
- To enable maximum level of verbosity set LdapLogEnabled parameter to true on QEF Configuration tab in QEF Console. Log written into [QEF Working Directory]\LdapLog.