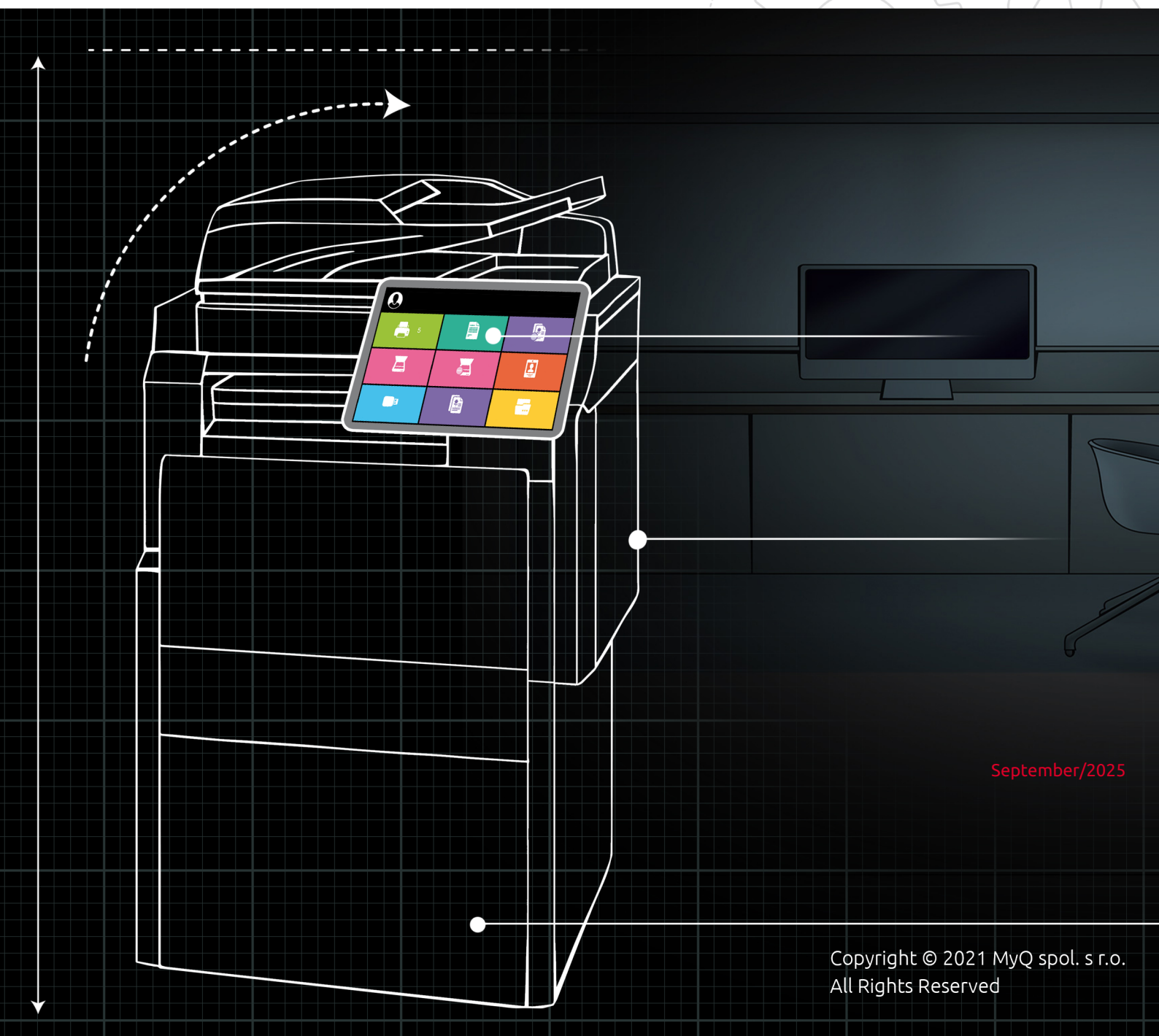


myQ X

Central Server 10.2



September/2025

Copyright © 2021 MyQ spol. s r.o.
All Rights Reserved

Table of Contents

1	Release Notes	9
1.1	What's New in 10.2	9
1.2	MyQ Central Server 10.2 (Patch 15)	10
1.3	MyQ Central Server 10.2 (Patch 14)	10
1.4	MyQ Central Server 10.2 (Patch 13)	11
1.5	MyQ Central Server 10.2 (Patch 12)	12
1.6	MyQ Central Server 10.2 (Patch 11)	13
1.7	MyQ Central Server 10.2 (Patch 10)	13
1.8	MyQ Central Server 10.2 (Patch 9)	14
1.9	MyQ Central Server 10.2 (Patch 3)	14
1.10	MyQ Central Server 10.2 (Patch 2)	15
1.11	MyQ Central Server 10.2 (Patch 1)	17
1.12	MyQ Central Server 10.2 RTM	19
1.13	MyQ Central Server 10.2 RC 4	19
1.14	MyQ Central Server 10.2 RC 3	23
1.15	MyQ Central Server 10.2 RC 2	24
1.16	MyQ Central Server 10.2 RC 1	25
1.17	MyQ Central Server 10.2 BETA 2.....	26
1.18	MyQ Central Server 10.2 BETA.....	26
1.19	Component Versions.....	28
2	Central Server and MS Cluster.....	34
2.1	About	34
2.2	System Requirements	34
2.3	Licenses	34
2.4	Setup.....	35
2.4.1	Installing MyQ on the server in the cluster (all nodes)	35
2.4.2	Setting services to manual startup (all nodes)	35
2.4.3	Creating the MyQ server MS Cluster role (Failover Cluster Manager)	36
2.4.4	Adding MyQ Resources (Failover Cluster Manager)	38
2.4.5	Setting Resources Dependencies (Failover Cluster Manager)	40
2.5	Additional Setup.....	43
2.5.1	Setting up the MyQ admin credentials (active node)	43
2.5.2	Setting the location of the data folder (all nodes)	43
2.5.3	Running MyQ in the MS Cluster environment.....	44
2.5.4	Starting the system (Failover Cluster Manager).....	44
2.5.5	Setting hostname of the MyQ server role	44
2.6	Configuration and Maintenance	46
2.6.1	Bringing the resources of the MS Cluster online (Failover Cluster Manager).....	46
2.6.2	Taking the MS Cluster resources offline (Failover Cluster Manager)	46
2.6.3	Restarting MyQ services via the MS Cluster (Failover Cluster Manager)	47

2.6.4	Changing the MyQ admin credentials (active node).....	47
2.7	Backup and Restore	48
2.7.1	Backing up the MyQ database on the MS Cluster	48
2.7.2	Restoring the MyQ database on the MS Cluster (all nodes)	48
2.7.3	Using Database Encryption	49
2.8	Upgrading MyQ.....	49
2.8.1	Necessary steps before the upgrade	49
2.8.2	Upgrading MyQ (all nodes)	49
2.9	Recommended Troubleshooting	50
3	System Requirements	51
3.1	MyQ Central Server mode with integrated Firebird database	51
3.1.1	Recommendations	51
3.2	MyQ Central Server mode with an external MS SQL database	52
3.2.1	Recommendations	52
3.2.2	Operating System	52
3.3	Additional software required	53
3.3.1	Storage sizing.....	53
3.3.2	Database	54
3.3.3	Web browser.....	54
3.3.4	Security.....	54
3.4	MyQ installation in Private Cloud	55
3.5	Main Communication Ports.....	55
3.5.1	Incoming Ports.....	55
3.5.2	Outgoing Ports	55
4	Installation	57
4.1	Central Server Database Setup	57
4.1.1	Embedded Database Configuration.....	58
4.1.2	MS SQL Server Configuration.....	58
4.1.3	Setting up the Embedded Database	58
4.1.4	Setting up an MS SQL Database.....	59
4.1.5	MS SQL Server Setup Example	64
4.2	Installation in Private Cloud.....	67
4.2.1	Environment Requirements.....	67
4.2.2	About MyQ in Private Cloud	68
4.3	OEM Migration.....	70
4.3.1	Prerequisites	70
4.3.2	Recommended Steps	70
4.3.3	Migrate to MyQ	70
4.4	Updating MyQ.....	71
5	MyQ Central Server Easy Config	73
5.1	Home.....	73
5.2	Services	74

5.3	Settings	75
5.3.1	Windows Services Account	75
5.3.2	Web Server Ports	76
5.3.3	Data Folder	76
5.3.4	Server Maintenance	78
5.4	Security	79
5.4.1	Changing Passwords on the Security Tab	79
5.4.2	Unlocking the MyQ Administrator account	79
5.4.3	Data Encryption	80
5.5	Database	80
5.5.1	Backing up MyQ data	81
5.5.2	Restoring MyQ Data	82
5.5.3	Database Connection Settings	82
5.6	Log	82
6	MyQ Central Web Interface	84
6.1	Accessing the MyQ Central Web Interface	84
6.2	Logging in as an administrator	85
6.3	Main Menu and Settings Menu	86
6.4	Home Dashboard	87
6.4.1	Quick Setup Guide	90
6.4.2	Generate Data for Support	91
6.5	MyQ Log	93
6.5.1	Opening the MyQ Log	93
6.5.2	Pausing/Refreshing the log	93
6.5.3	Filtering the log: selecting time period, verbosity of information, subsystem or context	93
6.5.4	My Searches	94
6.5.5	Exporting the log/Generating support data	95
6.5.6	Highlighting log messages	95
6.6	MyQ Audit Log	96
6.6.1	Opening the MyQ Audit Log	96
6.6.2	Filtering the Audit Log: selecting time period, user and type of event	97
6.6.3	Exporting the Audit Log	97
7	MyQ Central System Settings	99
7.1	General Settings	99
7.2	Personalization Settings	101
7.2.1	Application Personalization	102
7.3	Task Scheduler Settings	102
7.3.1	Running and setting task schedules	103
7.3.2	Providing rights for task schedules	104
7.4	Network Settings	105
7.4.1	General	106
7.4.2	Communication Security	106

7.4.3	Outgoing SMTP server	107
7.4.4	HTTP Proxy Server	109
7.4.5	Firewall.....	109
7.5	Connections Settings	109
7.5.1	Microsoft Exchange Online Setup	109
7.5.2	Gmail with OAuth2 Setup.....	113
7.5.3	Entra ID (Azure AD) with Microsoft Graph Setup	113
7.6	Authentication Servers Settings	122
7.6.1	Adding a new LDAP server:.....	122
7.6.2	Adding a new MS Azure Server:	123
7.6.3	Adding a new Radius server:.....	125
7.7	Printers Settings.....	125
7.8	Accounting Settings	126
7.9	Data Replication from Sites Settings	127
7.9.1	Replication Settings.....	127
7.9.2	Scheduling Replication.....	128
7.9.3	Resolving Replication Errors.....	128
7.10	External Reports.....	129
7.11	Log and Audit Settings.....	130
7.11.1	Management of Log Notifier Rules.....	131
7.12	REST API Apps.....	132
7.13	System Management Settings.....	133
7.13.1	Disk space checker	133
7.13.2	History	133
7.13.3	System Maintenance	134
8	Licenses	136
8.1	License Distribution to Site Servers	136
8.2	Adding Licenses	138
8.3	Activating Licenses	140
8.3.1	To manually activate a license:.....	140
8.3.2	Reactivating Licenses in Case of Hardware Change	141
8.4	Deleting Licenses	142
8.5	Extending Software Assurance Licenses.....	142
8.5.1	Manual activation.....	142
8.6	Migrating Old Licenses to MyQ X	143
8.6.1	Migration Process	144
8.7	VMHA License	145
9	Central and Site Administration	147
9.1	Sites Page	148
9.2	Editing a Site	148
9.3	Grouping Sites.....	149
9.4	Site Server Data Replication	150

9.5	Site Server Rights Management.....	151
9.6	Job Roaming	152
10	Users	154
10.1	List of Users.....	155
10.2	Adding and Deleting Users Manually	156
10.2.1	Adding Users	156
10.2.2	Deleting Users	156
10.3	Editing User Accounts	156
10.3.1	User information and settings.....	157
10.3.2	Adding users to and removing them from groups.....	158
10.3.3	Selecting user delegates	159
10.4	User Groups.....	160
10.5	Exporting Users	161
10.6	User Import and Synchronization	162
10.6.1	User Properties in MyQ.....	162
10.6.2	User Synchronization from LDAP Servers.....	163
10.6.3	User Synchronization from Entra ID with Microsoft Graph.....	173
10.6.4	User Synchronization from CSV Files	181
10.6.5	User Synchronization from Entra ID (Azure AD) with SLDAP	186
10.6.6	User Synchronization from Google Workspace	187
10.6.7	Using External Authentication Servers.....	189
10.6.8	Manual and Scheduled Synchronization Run	190
10.7	Users Settings	191
10.7.1	General Section	192
10.7.2	Account lockout section	192
10.7.3	PIN section.....	193
10.7.4	Password Complexity section	194
10.8	Rights.....	195
11	Credit	198
11.1	Activation and Setup	198
11.2	Manual Credit Recharge	199
11.2.1	Providing users with rights to recharge credit	200
11.2.2	Recharging credit on the Credit Statement tab	200
11.2.3	Recharging credit on the Users main tab.....	201
11.3	Recharging Credit via PayPal.....	202
11.3.1	Setting up PayPal Payments.....	202
11.3.2	Recharge User Credit with PayPal.....	203
11.4	Recharging Credit via SnapScan.....	203
11.4.1	Setting up the SnapScan payment option	204
11.4.2	Recharging credit via SnapScan on the user's account on the MyQ Web Interface.....	204
11.5	Recharging Credit via TouchNet uPay	205
11.5.1	Setting up TouchNet uPay	205

11.5.2	Recharging credit via TouchNet uPay on the user's account on the MyQ Web Interface	206
11.6	Recharging Credit by Vouchers	207
11.6.1	Setting the Voucher Format	207
11.6.2	Custom Logo for Credit Vouchers	208
11.6.3	Voucher Batches	208
11.6.4	Vouchers Usage Overview	209
11.7	Recharging Credit via External Payment Providers	210
12	Central Server Reports Management	211
12.1	Reports	211
12.1.1	Report Types	212
12.1.2	Reporting Sources	226
12.1.3	Report Values Description	227
12.1.4	Creating, Editing, and Cloning Reports	228
12.1.5	Generating Reports	234
13	Connection to BI tools	237
13.1	Embedded Database Connection Configuration	237
13.2	Creating Reports	239
13.2.1	Manual Reports Creation	239
13.2.2	Reports Creation via Template Import	242
13.2.3	Report Examples	243
13.2.4	Database Views Description	245
14	System Health Check	256
14.1	Using System Health Check	256
15	Uninstalling MyQ	258
16	Available languages	259
17	Business Contacts	262

MyQ Central Server 10.2

MyQ is a universal printing solution that provides a wide variety of services related to printing, copying, and scanning. All functions are integrated into a single unified system, which results in an easy and intuitive employment with minimal requirements for installation and system administration.

The main areas of application of the MyQ solution are monitoring, reporting and administration of printing devices; print, copy, and scan management, extended access to printing services via the MyQ X Mobile Client application and the MyQ Web Interface, and simplified operation of printing devices via MyQ Embedded terminals.

Here you can find all the information needed to install, configure, upgrade, and uninstall the MyQ Central Server.

All changes compared to the previous version are listed in the [release notes](#).

All changes compared to the previous version are listed in the release notes, available [online](#) and in [PDF](#).

1 Release Notes

MyQ Central Server 10.2

- Minimum required support date: **June 1, 2024**
- Minimum required version for upgrade: **8.2**

1.1 What's New in 10.2

- ✓ Find details of the improvements in MyQ 10.2 across our full range of solutions [here](#).

Version Highlights

Click to see a full list of new features available in version 10.2

- Added support for Integrated Windows Authentication (Windows single sign-on) for Web User Interface and MyQ Desktop Client 10.2, logging in environments where IWA is used can be enabled in Settings – User Authentication and MyQ Desktop Client's Configuration profiles.
- Entra ID (Azure AD) Joined devices are now supported for Job Authentication; a new option to Entra ID User Synchronization can automatically create compatible user aliases from concatenated Display names (for job submission from local accounts such as AzureAD\displayName).
- In addition to permanent PINs, you can now create temporary PINs with limited validity.
- Ukrainian was added as a new supported language to the MyQ Central Server.
- the widget "Updates" was added on the admin's Dashboard. When a new version of MyQ Central Server is released, administrators will see a notification in the MyQ Web Interface.
- System health check will now report Sites that have not been replicated for some time. This will help to prevent issues with long replication queues that could result in missing or inaccurate data in reports.
- Administrators can now see a list of errors which occurred during replications on the Replications settings page with help on how to resolve some of them.
- Option to group Sites on Central was added. It allows administrators to configure Job roaming only among Sites within a selected group. This helps to decrease traffic needed for Job roaming to work.
- New user's attribute "Alternate email" allows the administrator to add multiple email addresses to a user.
- Microsoft single sign-on (Sign in with Microsoft) can now be also used to log in to the Central Server, previously available only on the Print Server.
- MyQ Log interface was largely improved, it now allows saving commonly used filters and reusing them while searching or monitoring live logs.
- Added support for MyQ in IPv6 networks, IPv6 addresses can now be used across MyQ to configure authentication servers, SMTP, add printers, communicate with Site servers and more.

1.2 MyQ Central Server 10.2 (Patch 15)

3 September, 2025

Improvements

- Added status labels and a new *Last run result* column to the Task Scheduler overview.

Changes

- PHP updated to 8.3.24
- Apache updated to 2.4.65
- Firebird updated to 4.0.6
- OpenSSL updated to 3.3.4
- DotNetZip replaced by ProDotNetZip

Bug Fixes

- Incorrect column label in Environmental reports: changed *Total Pages* to *Equivalent A4 Sheets*.
- PIN validity parameter contained text that could not be translated.
- Scheduled tasks grid did not update in certain cases.
- Reports sent to the *All Users* group were also sent to deleted users.
- Error deleting old reports when running system maintenance.
- User accounts were incorrectly locked after failed/successful login attempts.
- Built-in *All Users* group could not be selected in Reports design after it was removed.
- Searching users could cause the page to hang under certain conditions.
- Toner level not displayed for some sites using replication.
- Installer provided an incorrect .NET download link.
- Pipe character in group name broke Entra ID synchronization.
- MyQ Central Server service could crash due to delayed start of SQL service after restart.
- Occasional backup failed when downloading XML files during backup process.
- Removed HTML tags from System Health Check *critical free space* email.

1.3 MyQ Central Server 10.2 (Patch 14)

16 July, 2025

Bug Fixes

- Entering invalid LDAP user synchronization credentials error was only displayed once.
- Deleting a MyQ user account does not clear the email, and new user accounts are blocked from using the same email.
- Logging in with username and password creates two log records.
- Pending emails block server upgrade.
- Canceling log in with Windows Authentication shows HTML code instead of rendered page.
- Not possible to define IP Include/Exclude for clients on Central Server.

1.4 MyQ Central Server 10.2 (Patch 13)

19 June 2025

Improvements

- **NEW FEATURE** **Kerberos is now supported for both Desktop Client and Web authentication**, enabling seamless Single Sign-On (SSO) in enterprise environments.
- **Microsoft Entra ID integration now includes OpenID Connect (OIDC) support**, providing enhanced security and identity verification capabilities. Existing Microsoft Entra ID authentication configurations will continue to work without any changes.
- **Outgoing emails are now generated as MIME multipart/alternative messages** that contain both an HTML and a plain-text version of the body. This ensures reliable parsing and improved delivery to systems that do not render or parse HTML effectively.
- Improved the installer to **detect PHP customization** and warn about potential incompatibility.
- Improved the **wording of server emails**, including the new PIN and PIN reset email.
- Improved the export of Windows certificates during system maintenance.
- Printer hostname/address now **supports up to 256 characters**.
- Improved error message in case of an issue during certificate import (invalid, wrong password) in Manual Certificate Management mode.
- Added IWA support for pre-Windows 2000 environments, where the domain name and NETBIOS name may be different. To enable support for this, add the following to the **General** section of `config.ini`, where `domain1` is the NETBIOS name, and `newdomain2.com` is the DNS name (multiple mappings supported).
 - `domainsMapping="domain1=newdomain2.com, domain2a=newdomain2.cz, domain2b=newdomain2.cz"`

Changes

- **Currency must now be entered in general settings** in order for payment providers to be saved.
- **Updated the expired license message** that appears when attempting to upgrade Central Server without a valid support license.
- Minor UI changes, such as wrapping long labels on **Sign in with Microsoft** login buttons.
- Updated PHP to 8.3.21.

Bug Fixes

- User synchronization from CSV can fail when user has an unsupported PIN.
- Printers whose IP address/hostname is too long, or with an empty IP address (such as printers created during Local Print Monitoring or created by customizations), can cause issues with replications to the Central Server.

- Unable to autcreate user (i.e. by receiving job via e-mail) from Site server 8.2.
 - Sites are moved to the All Sites group after their original group is deleted.
 - In the Environmental Report, user groups are not available when job privacy is enabled.
 - Customizations are removed during upgrade from Central Server 8.2 and 10.1.
 - Synchronizing users from Central Server to Site Server sometimes ends with message "Central Server database is not in sync. Deleting ID mapping" even when there is nothing to synchronize.
 - Memory usage is reported incorrectly in the user synchronization log.
 - HTML tags appear in system health check log and email body for some messages, instead of plain text only.
-

1.5 MyQ Central Server 10.2 (Patch 12)

06 May, 2025

Improvements

- Logging of PayPal connection issues related to network and certificates was improved.
- Increased the maximum length of the Token field in the database from 4,000 to 8,000 characters to accommodate longer values that previously could not be stored.

Changes

- Minimal support date raised to June 1, 2024. To upgrade to this or later versions, the support license must be valid at least until this date.

Bug Fixes

- The Central Server could crash during user synchronization to a Site Server when debug logging was enabled.
 - Resolved incorrect handling of health check error messages.
 - Toner levels were not replicated when using Central Server 10.2 with Site Server 8.2.
 - Replication counter history could enter a loop if the data gap exceeded one year.
 - Replication loop could occur when a Site Server was restored from an older backup that had already been replicated.
 - Addressed a synchronization failure with Entra ID users, which could result in the error "Undefined array key 0."
 - Resolved an issue where operations involving the Token table could overload the server.
 - Groups listed in User Properties → Groups tab disappeared when switching tabs.
-

1.6 MyQ Central Server 10.2 (Patch 11)

MyQ Central Server 10.2 has skipped Patch 11 to keep Central Server releases in tandem with Print Server releases. The next Central Server release will be Patch 12.

1.7 MyQ Central Server 10.2 (Patch 10)

18 March, 2025

Improvements

- [Managed Service Accounts](#) are now supported.
- Firebird DB can now use more system memory for caching.

Changes

- Updated Apache to 2.4.63.
- Phone numbers can contain any character.
- Updated OpenSSL to version 3.3.3.
- Updated PHP version to 8.3.17.
- Re-authorising Entra ID connection form no longer contains option to create user synchronisation as it could cause duplicates.
- Removed requesting POP3 scope in Microsoft Exchange Online.
- Update Firebird to 4.0.5.

Bug Fixes

- Text on 'Import CA Certificate' button missing.
- BETA User Reports are still available when Job Privacy is enabled.
- Error was generated after switching Certificates from Manual Certificate Management to Built-in Certificate Authority.
- CVE-2025-24374 twig - escaping is missing when using null coalesce operator.
- Using language code unsupported by MyQ but valid in URL will now default to English rather than give "requested resource could not be found" error.
- Upgrade hangs when certain database password character combinations are used.
- Missing category in downloaded report file name.
- Missing charts in some PDF reports i.e. Hourly Activity.
- Conversion failed when converting the varchar value to data type int when generating some report types.
- Renamed reports display only the report name without category.
- Failed email cannot be moved to failed folder in some cases because of identical file name which prevent other email from being sent.
- Operations with Token table can overload the server.
- It is not possible to login to Web UI using IWA (Integrated Windows Authentication).
- Token field in database extended from 4000 to 8000 characters, because of some cases, where 4000 characters were exceeded and could not be stored in database.
- System maintenance step "Cleaning the database" is extremely slow in 50GB DB.

1.8 MyQ Central Server 10.2 (Patch 9)

31 January, 2025



MyQ Central Server 10.2 Patch 4 has been renamed Patch 9 to keep Central Server releases in tandem with Print Server releases.

Improvements

- When maximum number of users or groups is listed in a drop down, it is now possible to load more.
- Improved performance of Web UI in case of huge database.
- Add "Load more items" command to Email selector for users/groups.
- Improved speed of user synchronization from Entra ID.
- Extend apache access_log by a request execution time.
- Added notification about expiration of server certificate.
- OpenSSL updated to version 3.2.2.
- PHP updated to version 8.3.16.

Bug Fixes

- Cannot change alignment of aggregate column.
- Loading of dashboard can fail in case of huge database.
- User can select "Me" and own username in reports.
- Manual/Offline activation is not possible.
- Renaming top parent user group can lead to replications issue in some cases.
- Incorrect name for Accounting Group dropdown in reports design.

1.9 MyQ Central Server 10.2 (Patch 3)

10 December, 2024

Security

- PHP updated to version 8.3.14 (addressing CVE-2024-11233, CVE-2024-11234, and CVE-2024-11236, CVE-2024-8932).
- Updated various components.

Improvements

- Added System health check and notification about soon-to-be-expired Secret Keys for Microsoft services connected in the Automatic mode of [Entra ID](#). Users who receive health check notifications will be reminded when these connectors are 30 days before expiration.,
- Added additional user attributes that can be [synchronized by importing a CSV file](#), including Department, Custom (1), Custom (2), and Custom (3). Skip header line option changed to No header line.
- Enhanced the Audit log to better track history, including operations like adding or removing PINs.

- Added summary [Environmental report](#), which are available when Job Privacy is enabled active.
- Added cost-related optional columns (B&W Cost and Color Cost) to multiple reports, including Groups, Printers, Projects, and Users categories.
- A more detailed error message is displayed when the connection to the authentication server fails (even without the debug mode).
- Unified column names between Print and Central Server reports.
- CSV file examples for importing CodeBook, Printers, Projects, Quota, and Users added in **ProgramData\MyQ\Data\Import** , these examples can be used as a basis for creating data for import.
- Small design update of the login screen, improved UI control for setting the [custom logo](#).
- The warning bar with license information (trial license, expiration) at the top of the page is now displayed only on the Home page, and not on all pages.

Bug Fixes

- Report General - Price list comparison, graph in preview, and PDF report might not display for large data sets.
- Anonymization doesn't remove the user's department and Custom field.
- Cannot generate the grid preview for a large number of columns in reports.
- Cannot run the newly added report: General – Day of the week.
- Credit debit request via REST API throws an error.
- Custom logo does not show in the upper right corner.
- Database password starting with a question mark caused Print Server services to stop or fail to start. This issue has been resolved, and a question mark is now supported.
- Entra ID sync options do not prevent saving with a misconfigured "Users to import" field.
- Entra ID synchronization fails if the "Ignore groups containing string" contains a forward slash.
- It is not possible to manage the Credit widget.
- MD5 Hashed PIN Import from CSV fails.
- Unable to save Report's chart settings.
- Panel with the anonymized user is still present, and fields are editable.
- Print Jobs category of Reports is missing copies.
- Reports Group summary rows show a dash instead of an empty string.
- Service might not stop correctly during server shutdown or reboot.
- The value of the Color Cost column in Printer reports is incorrect.
- Unable to save the Credit Statement grid as CSV.
- In reports, the date picker in the Advanced range does not have a maximum limit.
- The 'Recharge credit' option appears on the Web Interface's dashboard when only External Payment Providers are set. An error is displayed upon using it.

1.10 MyQ Central Server 10.2 (Patch 2)

4 October, 2024

Security

- Updated twig library to 3.14.0.

Improvements

- Prices are now rounded to a specific number of decimals according to what is configured in Settings – General; this setting was already used in PDF reports.
- PHP updated to version 8.3.12
- Added the option to select groups to use for user group memberships in Entra ID user synchronization (on the Groups tab). This does not affect the users that will be synchronized, but includes/excludes groups that these users can be members of.
- Smaller adjustments and fixes of inconsistencies in reports of the User category.
- Added user-related additional optional columns (Username, Full name) to Total summary reports.
- A new option has been added to the Entra ID sync feature, allowing administrators to synchronize groups under a parent group. This enhancement replicates the behavior of LDAP/CSV sync.
- You can now select multiple search results while holding the Ctrl/Command key in any multi-item selection widget (users, groups, printers, etc.).
- It is now possible to add ID cards with up to 32 characters, accommodating modern methods such as those generated by Apple Wallet.
- When the log is filtered, the Generate Support Data option reflects the date selected in the filter. The end date is pre-filled automatically based on the maximum amount for export, and the Type filter has been exchanged with Verbosity.
- Azure cloud service connections' Edit/Re-authorize flows were improved to prevent invalid configuration.
- The fields Notes and Email have been added to the Entra ID synchronization options and can be now also adjusted. By default, Email uses the "email" user properties; Notes does not use any default.
- Added additional user attributes that can be synchronized from Entra ID and LDAP. Those are: Department, Custom (1), Custom (2), and Custom (3), and they can be used to store more user-related information. These fields were also added to reports containing information about users.
- **REST API** When listing users, their groups can also be requested in the **users** endpoints.

Changes

- It is now not possible to remove columns that are used for grouping in reports. If those columns were removed, the reports might not be rendered optimally.

Bug Fixes

- Users cannot connect to cloud storage on the Site server in some cases and might encounter an "Invalid parameter" error.
- Report Meter reading via SNMP does not contain time in Start and End dates.
- During mass-generation of PINs for users, it was an infrequent occurrence that some users were not assigned a PIN. This happened because the system, in rare

cases, did not attempt to generate a new unique PIN after encountering a duplicate in the batch.

- Reports from the Groups category are missing "Single color copy".
- Sorting user reports "Daily summary" and "Day of Week" by username is not working properly
- Integrated Windows Authentication does not properly work in domain environments with more than two levels in the domain (e.g., "sub.company.com") when the full domain is filled in the Authentication Server's settings.
- When searching in groups on the Users page, the results also contain users.
- Charges recorded in the Audit log on site (i.e. change of user's PIN) done by a user with administrator rights are displayed on the Central Server as *admin; the user "system" is now used instead.
- The "Save as CSV" function on the Users page did not include ID Card and PIN information which helps to see whether users have PINs and ID Cards registered in the system.

1.11 MyQ Central Server 10.2 (Patch 1)

7 August, 2024

Improvements

- **NEW FEATURE** **MyQ Log interface** was largely improved, it now allows saving commonly used filters and reusing them while searching or monitoring live logs.
- Introduced the ability to **clone an existing report**, simplifying the process of creating multiple similar reports.
- **The user interface of User Synchronization improved.** Possible to run longer synchronization than 5 minutes not only via Task Scheduler but also from the User Synchronization page, the log is being shown in real-time, and it is possible to stop synchronization and save the log to the text file.
- The speed of synchronization from Entra ID improved, especially in cases when a particular group is filtered.
- Filter in LDAP synchronization source settings has been enhanced, raw filtering query can be used, and also objectClass can be changed to allow for more flexibility, e.g. by using a query such as (&(objectClass=person)(| (Attribute=Value)(Attribute=Value))). If some filter existed prior upgrade, it will be converted to the raw format.
- MS Visual C++ 2015-2022 Redistributable updated to 14.40.33810.
- Option to synchronize multiple ID cards and PIN from Entra ID by selecting multiple attributes or one attribute supporting multiple values.
- When creating a connector for Entra ID, it is now possible to also have the related Authentication Server and User Synchronization source created automatically when the "manual mode" is selected and the admin provides the app credentials manually.
- Apache updated to 2.4.62.

- PHP updated to 8.3.9.
- MS Visual C++ 2015-2022 Redistributable updated to 14.40.33810.

Changes

- Adjustments were made so that the MyQ Desktop Client 10.0 can also be used with a fresh installation of MyQ 10.2; previously, older MDC versions were supported only on upgraded installations.
- Adjustments to meet the new requirements for card payments that mandate additional cardholder information during credit recharge with GP Webpay. For customers using GP Webpay, upgrade is strongly recommended.

Bug Fixes

- When creating the SQL database, Window Authentication could have been attempted using a different account. The dialogue was also improved to suit the Windows authentication method better when it is selected.
 - The connection between the Central and Site servers when replicating data missed timeout, and it could block other sites from replicating when paused.
 - Multiple users with empty e-mail addresses trigger duplicate e-mail address warnings in System Health Check.
 - User Synchronization from CSV takes significantly longer compared to previous versions; the synchronization performance has been further optimized.
 - Users might not be correctly registered from the Recharge Terminal.
 - Upgrade from the previous Central Server versions with SQL database to the latest version 10.2 fails without secured connections.
 - Report "Print jobs – Daily summary" is missing Document type information.
 - Cascade deletion of rights in MS SQL database.
 - In some instances, the original document type (doc, pdf, etc.) of a print job may be incorrectly detected.
 - Installation of MyQ might fail when the prerequisite software required was already installed before the installation was started.
 - The Updates widget could incorrectly show "Update available" for the server even when this version is the one currently installed.
 - Inconsistency in default Accounting group when moving user into and out of group and switching accounting mode.
 - When generating Data for support, the data provided to our Support team does not contain the support validity date information.
 - When an HTTP proxy is used, users or admins might not be able to connect to services such as Microsoft Exchange Online, OneDrive for Business, or Sharepoint Online.
 - Scheduled reports are not sent via email if the recipient is a manually specified email address.
 - Central Server installed without the Firebird component causes MSSQL database creation to fail and server fails to start.
 - Scheduled report is generated and sent repeatedly to the same user when the user is a member of multiple user groups.
-

1.12 MyQ Central Server 10.2 RTM

13 June, 2024

Improvements

- Added a more flexible option for updating users synchronized from Entra ID onto the same users already existing in MyQ who were previously synchronized from AD; a personal number field that should store a unique identifier of the user in both sources can now be used in Entra ID to pair the user identities.
- PHP updated to version 8.3.7.
- SQL Database creation process and UI improved.

Changes

- After changing the PIN length in Settings, administrators can choose whether to generate new PINs only for users who already have a PIN or all users.
- SQL Server 2014 is no longer supported. Minimum supported version of SQL Server is 2016.

Bug Fixes

- A user with user right "Delete Cards" is not able to delete cards due to options in the dialogue available on their Web Interface being inactive.
- Configured connections (Settings – Connections) could have been invalidated during the upgrade in specific cases such as when the *admin account still used the default password "1234" (note: since MyQ 10.2 RC 4, the *admin does not have any default password set anymore) or when the admin account that created this connector later changed their MyQ password.
- Database upgrade between patches can fail in rare cases (The DELETE statement conflicted with the REFERENCE constraint "FK_ACE_TBLORMOBJECTS").
- Generating reports or report previews might fail with an error in some cases.
- Ineligible PIN could have been sent to users by email if those users were imported from CSV which was exported from older MyQ versions (and when Send PIN via email was enabled).
- PIN displayed by the user (i.e. when the user attempts to recover the PIN) is displayed without leading zeros. Example: PIN 0046 is displayed as 46.
- Rights for reports and its related scheduled settings are not inherited.
- When logging in with the Sign in with Microsoft option, accounts the user is already signed into with Microsoft might not have been detected and offered to be used.

1.13 MyQ Central Server 10.2 RC 4

17 May, 2024

Security

- Default password for the *admin account is not set for new MyQ installations anymore. Set the password manually in the Easy Config before heading to the

MyQ Web Admin Interface. If you are still using the default password at the time of the upgrade, you will be asked to create a new one in the Easy Config.

- Added option to enable/disable *admin account which leads to a new possibility to lock *admin account for login when required. It is recommended to assign specific users desired rights and prevent using a shared account for server administration. Added option to enforce or disable encryption when connecting to the SQL Server in the Easy Config's database configuration step.
- Improved logging of login events especially attempts to log in with invalid credentials.
- LDAP communication was not validating certificates.
- Limited access to data that could be considered sensitive when custom reports are used.
- Limited options for well-known clients to request certain operations on users via REST API.
- **REST API** Removed capability to change the authentication server of a user (LDAP) server.
- The access of the account for external reporting has been limited, some database tables with data that might be considered sensitive will not be accessible by default by this user.
- Unauthenticated Remote Code Execution Vulnerability fixed (resolves CVE-2024-28059 reported by Arseniy Sharoglazov).
- Scopes well-known clients (MyQ applications) can request were limited.
- Unsuccessful authentications are now limited for security reasons, by default, the client/device is blocked for 5 minutes if more than 5 invalid login attempts are registered in a span of 60 seconds; these periods can be manually adjusted.

Improvements

- **NEW FEATURE** Added support for [Integrated Windows Authentication](#) (Windows single sign-on) for Web User Interface and MyQ Desktop Client 10.2, logging in environments where IWA is used can be enabled in Settings – User Authentication and MyQ Desktop Client's Configuration profiles.
- **NEW FEATURE** Added support for MyQ in IPv6 networks, IPv6 addresses can now be used across MyQ to configure authentication servers, SMTP, add printers, communicate with Site servers and more.
- **NEW FEATURE** Entra ID (Azure AD) Joined devices are now supported for Job Authentication; a new option to Entra ID User Synchronization can automatically create compatible user aliases from concatenated Display names (for job submission from local accounts such as AzureAD\displayName).
- The connection processes for SharePoint Online and Entra ID were improved, administrators can use the [Automatic mode](#) when creating the connector which does not require creating an Azure application manually but uses a MyQ predefined Enterprise application instead.
- Added options that allow to automatically create a synchronization source and authentication server for Entra ID in the dialogue for adding a new Entra ID connector.
- To strengthen the security of user authentication, [manually and automatically generated PINs](#) are now subject to improved complexity standards; weak PINs (with subsequent numbers, etc.) cannot be manually set and are never

- automatically generated. It is recommended to always use the Generate PINs functionality instead of filling PINs manually.
- Default PIN length increased to 6 and minimum PIN length is now 4, resulting in improved security defaults for user authentication; for upgraded installations, if PIN is set to length below 4, it is automatically increased and will be used next time you generate new PINs.
 - Added options to [select the level of synchronization](#) for Groups in Entra ID sources; allowing for more flexibility such as choosing whether full synchronization should be performed or when synchronization should be skipped.
 - A warning when removing a trial license was added to inform that another trial license cannot be added in case there are accounted jobs from active user sessions existing in MyQ.
 - Added option to add an additional column "Project code" to [reports in the Projects category](#).
 - Columns Total, B&W, and Color renamed to Total, B&W, and Color parsed pages in certain reports to clarify that these reports show the number of pages as they arrived in MyQ and not the final printed and accounted pages.
 - Improved logging of user synchronization issues.
 - LDAP synchronization options are validated on saving to avoid duplicated Base DN's which could cause errors during user synchronization.
 - Name or Tenant Domain is displayed of Entra ID is displayed on the Connections page for better recognition when multiple tenants are used.
 - Password field for SMTP settings can accept up to 1024 characters instead of 40.
 - The design of the Azure-related connectors (Entra ID, OneDrive for Business, and SharePoint Online) was improved.
 - **REST API** Added option to soft-delete users.
 - **REST API** Enhanced options for user management by allowing you to set user group memberships.
 - Firebird upgraded to version 4.
 - .NET Runtime updated to version 8.
 - PHP updated to version 8.3.6.
 - OpenSSL updated to version 3.3.0.
 - OpenSSL updated to version 3.2.1.
 - Apache updated to version 2.4.59.

Changes

- Correction of project names "No project" and "Without project".
- Custom reports have to be signed; in case the installation uses custom reports, backup them before the upgrade to be able to request signing.
- Deleted sites are not displayed in "With issue" filter on Sites page.
- Lotus Domino has been repositioned to the legacy mode; upgraded installations will preserve Lotus Domino integration (it is recommended to test the integration before upgrading production environments), and new installations will not have the option to add a new Lotus Domino connection available by default.
- Security settings in Web Interface were renamed from SSL to TLS.

- The CASHNet payment provider has been deprecated; the upgrade will also remove the existing CASHNet payment provider, payment history data are preserved and moved under "External Payment Provider", and thus backup of payment history is recommended before the upgrade if CASHNet was used.
- The option to allow unsecure communication with Central Server was removed. This means SSL/TLS is always enforced in communication between Central and Sites.
- As part of excluding jobs moved by Job Scripting from the Expired and deleted jobs report, a new rejection reason can be seen for such jobs on the Jobs page.

Bug Fixes

- "Count it" on the Sites page might result in an error message being displayed.
- Cannot generate support data over midnight.
- Certificate validation could cause problems with connecting to Google Workspace.
- Certificates are not validated during connection to cloud services.
- Configured HTTP proxy is not used for connections to Entra ID and Gmail.
- Custom Help widget is not displayed on the Dashboard by default.
- Easy Config > Log > Subsystem filter: "Unselect all" is present even if all is already unselected.
- Installing PS and CS on one server causes error: Error occurred while trying to replace existing file, DeleteFile failed; code 5.
- Monthly report containing the Period column has months in incorrect order.
- Not possible to authenticate user against LDAP using LDAP authentication server with autoresolved address.
- Original jobs moved to different queue by job scripting are included in reports for expired and deleted jobs.
- Recharging credit via GP webpay - payment gateway is not loaded when the user's language is set to specific languages (FR, ES, RU).
- Replication from all Sites might be paused due to a replication problem with only one Site server.
- Report "Projects - User Session details" shows the user's Full name in the User name field.
- SMTP test error message contains incomplete information.
- Some groups might be considered different if they contain full-width and half-width characters in the name.
- The test of connection to Google Workspace in the authentication server settings which did not require credentials previously could have impacted user synchronization and caused problems with authentication to Google Workspace; The Test of connection will now also require user credentials filled in similarly to the synchronization source settings.
- Toner level on the Printers page might not be displayed in some cases.
- User group is not possible to be a delegate of its own to allow members of the group to be delegates of each other (i.e. members of the group "Marketing" cannot release documents on behalf of other members of this group).
- User synchronization from Entra ID can fail when a user is manually created on Print Server but the same user exists also in Entra ID.

- User synchronization from LDAP can cause error: Undefined array key "samaccountname" and fail.

1.14 MyQ Central Server 10.2 RC 3

13 December, 2023

Security

- Hashing of passwords enhanced.

Improvements

- **NEW FEATURE** In addition to permanent PINs, you can now [create temporary PINs with limited validity](#).
- **NEW FEATURE** [Ukrainian](#) was added as a new supported language to the [MyQ Central Server](#).
- Changed "Azure AD" to "Microsoft Entra ID" to correspond with MS naming.
- Optimizations of Entra ID synchronization via Microsoft Graph API connector that should prevent slowdowns and skipping users.
- Administrators can [create multiple Entra ID instances](#) to synchronize and authenticate users towards more than one tenant.
- Added new settings to [Entra ID synchronization source](#) that allow setting attributes to synchronize the users' Full name, and Language. New attributes are also available for Aliases, PINs, Cards, and Personal numbers. It is now also possible to manually type in a required Entra ID user attribute to be used for these values.
- Added additional options for [User synchronization from Microsoft Entra ID](#) (Ignore sync source, deactivate missing users, add new users).
- Added report ["Servers - User Rights"](#) that groups data per server name.
- New [permission Delete Cards added](#), allowing to give users or user groups option to be able to delete ID cards without them having access to other user management features.
- List of characters allowed to be used in project code expanded. Upgrade to this patch is required for the replication of projects from Sites to work correctly if any of the new characters is used.
- OpenSSL updated to version 3.1.3
- PHP updated to 8.2.12
- CURL upgraded to 8.4.0
- Apache updated to version 2.4.58.

Changes

- In newly created user synchronization sources using the Entra ID connector (Microsoft Graph), the User Principal Name is now used as the username. After upgrade, existing username settings are preserved. To transition from old attributes to User Principal Name, users should be synchronized, the synchronization source removed, and created again. Users are also always paired by Entra ID's unique Object ID.

Bug Fixes

- Checking uniqueness of user group names is not working properly.
- Custom Help widget not displayed for users and cannot be added.
- Database creation can fail in some cases on SQL Server 2022 ("Conversion failed when converting the nvarchar value 'oft'").
- Database upgrade can fail in some cases ("Error while try to execute Php script version: 10.2.7").
- Easy Config is missing Chinese Traditional and Chinese Simplified languages.
- Hiding the Price List column on the Printers page renders the Printers page inaccessible.
- Is it possible to add the same column multiple times on the Sites page.
- Not possible to add groups to Sites user synchronization.
- Replication can fail in some cases with error "Class "UserDto" does not exist".
- Replication of data can end with warning "Dependency not found" in some cases, causing differences in reports on Site Server and Central Server.
- The printer's toner level can be incorrect when the printer was on Site with a lower version than the Central Server.
- Toner level information on the Printers page is missing after upgrade from previous versions.
- User synchronization results page is not refreshed automatically when synchronization finishes.
- User with rights to edit Scheduled report cannot select an attachment file format other than PDF.
- Creating a PDF report may fail if a job containing some special characters is present.
- Error "-901 Implementation limit exceeded Too many values" can occur during replications to the Central Server, potentially due to a rare device-related error causing wrong user session data reported to the Site.

1.15 MyQ Central Server 10.2 RC 2

6 October, 2023

Improvements

- Firebird update to version 3.0.11.
- PHP updated to version 8.2.11.
- OpenSSL updated to version 3.1.3.
- Built-in Groups (All users, Managers, Unclassified) are internally moved to new hidden group "Built-in" to avoid conflicts with groups with the same name created by user synchronization.
- HTTPS is used for external links from the Web Interface.
- Added option to [synchronize "onPremisesSamAccountName" and "onPremisesDomainName" from Azure AD via MS Graph](#) and pairing by Object ID to allow update existing users whose usernames changed.
- Added option to define regular expression for user synchronization (LDAP and Azure AD) for Aliases, Cards, PINs and Personal numbers.
- Added option to [exclude specific user\(s\) from Reports](#).

Bug Fixes

- In Job privacy mode, user running a report is excluded when Exclude filter is not used.
- In Job privacy mode, Administrators and users with Manage reports rights can see only their own data in all reports, resulting in the inability to generate organization-wide reports for group accounting, projects, printers, and maintenance data.
- Users could lose some Cost Center assignments after user synchronization from Azure AD and LDAP.
- Change of user's Accounting Group is not propagated to Site server.
- In some cases, Central upgrade fails with the error "No user specified".
- Upgrade could fail in some cases (with error violation of PRIMARY or UNIQUE KEY constraint "PK_ACE" on table "ACE").
- Login to Central Server's Web Interface fails if the username contains an apostrophe.
- Some groups reports are not possible to save when only Accounting group filter is set with error "User may not be empty".
- Two groups with identical names are indistinguishable in reports.
- Synchronized users who are members of groups with identical names to MyQ built-in groups in the source, are wrongly assigned to these built-in groups due to conflicting names.
- User editing own profile on Site server changes user synchronization source on Central server resulting in warnings during user synchronization.
- User synchronization takes more time compared to previous MyQ versions.

1.16 MyQ Central Server 10.2 RC 1

28 July, 2023

Improvements

- Added unique session identifiers to replication data to prevent differences in accounting data between Sites and Central.
- PHP upgraded to version 8.2.8.
- Improved look of new HTML emails. Footer text in emails can now be translated.
- Added options for behavior of [PINs and Cards synchronization from LDAP](#) same way as in CSV synchronization.
- Administrators do not need to re-type an authorization code when connecting cloud services into MyQ. Authorization is now done automatically.

Bug Fixes

- Refresh token for Exchange Online expires due to inactivity in spite of the system is being actively used.
- It is possible to save empty email destination for Log Notifier rules.
- Missing Scan and Fax columns in report Projects – User Session details.

1.17 MyQ Central Server 10.2 BETA 2

29 June, 2023

Improvements

- **NEW FEATURE** Widget "Updates" was added on the admin's Dashboard. When a new version of MyQ Central Server is released, administrators will see a notification in the MyQ Web Interface.
- Added support for Romanian language.
- User rights changes are logged to Audit log.
- Certificates in PHP updated.
- PHP updated to v8.2.6.

Changes

- Removed support for GPC file format in Bulk credit recharge.
- Default time periods for clean-up of jobs, log, and user sessions, performed by System Maintenance, were adjusted.
- The default runtime of scheduled tasks was changed to prevent them from running at the same time.

Bug Fixes

- Received email opened in Outlook is missing line breaks.
- Some rows could be skipped during replication on a Site that had active user sessions. **LIMITATION**: Site 10.2 BETA is now not compatible with Central Server 10.2 BETA 2 due to differences in communication during replications. Upgrade of the Site to 10.2 BETA 2 is required.
- Firebird temporary folder size could grow during large replication.

1.18 MyQ Central Server 10.2 BETA

1 June, 2023

Security

- Domain credentials were stored in plain text in PHP session files, now fixed.
- Added missing security attribute for encrypted session cookie (CWE-614).

Improvements

- **NEW FEATURE** System health check will now report Sites that have not been replicated for some time. This will help to prevent issues with long replication queues that could result in missing or inaccurate data in reports.
- **NEW FEATURE** Administrators can now see a list of errors which occurred during replications on the [Replications settings](#) page with help on how to resolve some of them.
- **NEW FEATURE** Option to group Sites on Central was added. It allows administrators to configure Job roaming only among Sites within a selected group. This helps to decrease traffic needed for Job roaming to work.
- **NEW FEATURE** New user's attribute "[Alternate email](#)" allows the administrator to add multiple email addresses to a user.

- **NEW FEATURE** [Microsoft single sign-on](#) (Sign in with Microsoft) can now be also used to log in to the Central Server, previously available only on the Print Server.
- OpenSSL updated to version 3.1.0.
- PHP updated to version 8.2.5.
- Apache updated to version 2.4.57.
- Health check will warn the administrator if their database is using a page size of 8 KB instead of 16 KB which may affect the performance. Page size can be increased by backing up and restoring the database.
- The possibility to [export users](#) only from selected group(s) into CSV was added.
- More errors occurring during replications from Print Server will be now resolved automatically. This should prevent delays in replications and help with accuracy of Central reports.
- Purchased Assurance Plan is displayed on the Dashboard of the MyQ Web Interface.
- Possible to synchronize user's multiple email addresses. Attributes for email address need to be separated by semicolon and all the next email addresses are imported as alternate email address.
- If you modify settings in the MyQ Web Interface and forget to save them, MyQ will now remind you about that.
- Minimum TLS version configured for MyQ communication is visible on the Network page in Settings.
- The default minimum TLS version has been increased to version 1.2.
- You can now see the version of MyQ installed on your Site on the Sites page.
- Users no longer need to connect their personal cloud storage on each Site individually. Once the user connects their storage on the first Site, their access is distributed to the rest of the Sites, allowing them to scan to the cloud immediately. Note that after upgrading to 10.2, users will have to re-connect their storage once in order to be connected everywhere.
- Accessing Web UI over HTTP is redirected to HTTPS (except when accessing localhost).

Changes

- [Minimal supported version](#) of Windows Server is 2016.
- The following features were deprecated: SQL Server as user synchronization source, custom user synchronization source, schedulable external commands via Task Scheduler.
- Email addresses are now a unique property. More users should not have similar email addresses to prevent incorrect pairing of jobs received via email.
- User's scan storage now does not accept email addresses, only valid storage paths.
- Old License Keys are not supported anymore, they have been replaced by Installation Keys.

Bug fixes

- It is not possible to save addresses for site's clients IP range higher than 127.255.255.255 when using MSSQL database.
- Aliases are incorrectly escaped in exported users CSV file.

- Email that cannot be sent blocks all other emails from being sent.
- User selection boxes sometimes do not show build in groups ("All users", "Managers", "Unclassified" options).
- Some columns of some reports are showing no values.
- User synchronization - LDAP export to CSV after successful import is not working, causing Web Server Error.
- History deletion cannot delete old jobs from table Jobs in some cases because of foreign key.
- System maintenance's Database sweeping cannot be started when Print Server is installed on the same server as Central Server.

1.19 Component Versions

Expand the content to see the version list of used components for the above MyQ Central Server releases.

	Apa che	Apa che SSL	Fire bird	PH P	PH P SSL	C++ Run tim es
MyQ Central Server 10.2 (Patch 15)	2.4. 65	3.3. 2	WI- V4. 0.6	8.3. 24	3.0. 15	VC ++ 201 5-2 022 (vc 17) - 14. 40. 338 10
MyQ Central Server 10.2 (Patch 14)	2.4. 63	3.3. 2	WI- V4. 0.5. 314 0	8.3. 22	3.0. 15	VC ++ 201 5-2 022 (vc 17) - 14. 40. 338 10

	Apa che	Apa che SSL	Fire bird	PH P	PH P SSL	C++ Run tim es
MyQ Central Server 10.2 (Patch 13)	2.4. 63	3.3. 2	WI- V4. 0.5. 314 0	8.3. 21	3.0. 15	VC ++ 201 5-2 022 (vc 17) - 14. 40. 338 10
MyQ Central Server 10.2 (Patch 12)	2.4. 63	3.3. 2	WI- V4. 0.5. 314 0	8.3. 20	3.0. 15	VC ++ 201 5-2 022 (vc 17) - 14. 40. 338 10
MyQ Central Server 10.2 (Patch 10)	2.4. 63	3.3. 2	WI- V4. 0.5. 314 0	8.3. 17	3.0. 15	VC ++ 201 5-2 022 (vc 17) - 14. 40. 338 10

	Apa che	Apa che SSL	Fire bird	PH P	PH P SSL	C++ Run tim es
MyQ Central Server 10.2 (Patch 9)	2.4. 62	3.1. 6	WI- V4. 0.4. 301 0	8.3. 16	3.0. 15	VC ++ 201 5-2 022 (vc 17) - 14. 40. 338 10
MyQ Central Server 10.2 (Patch 3)	2.4. 62	3.1. 6	WI- V4. 0.4. 301 0	8.3. 14	3.0. 15	VC ++ 201 5-2 022 (vc 17) - 14. 40. 338 10
MyQ Central Server 10.2 (Patch 2)	2.4. 62	3.1. 6	WI- V4. 0.4. 301 0	8.3. 12	3.0. 15	VC ++ 201 5-2 022 (vc 17) - 14. 40. 338 10

	Apa che	Apa che SSL	Fire bird	PH P	PH P SSL	C++ Run tim es
MyQ Central Server 10.2 (Patch 1)	2.4. 62	3.1. 6	WI- V4. 0.4. 301 0	8.3. 9	3.0. 13	VC ++ 201 5-2 022 (vc 17) - 14. 40. 338 10
MyQ Central Server 10.2 RTM	2.4. 59	3.1. 5	WI- V4. 0.4. 301 0	8.3. 7	3.0. 13	VC ++ 201 5-2 022 (vc 17) - 14. 32. 313 26. 0
MyQ Central Server 10.2 RC 4	2.4. 59	3.1. 5	WI- V4. 0.4. 301 0	8.3. 6	3.0. 13	VC ++ 201 5-2 022 (vc 17) - 14. 32. 313 26. 0

	Apa che	Apa che SSL	Fire bird	PH P	PH P SSL	C++ Run tim es
MyQ Central Server 10.2 RC 3	2.4. 58	3.1. 3	WI- V3. 0.1 1.3 370 3	8.2. 12	3.0. 11	VC ++ 201 5-2 022 (vc 17) - 14. 32. 313 26. 0
MyQ Central Server 10.2 RC 2	2.4. 57	3.1. 0	WI- V3. 0.1 1.3 370 3	8.2. 11	3.0. 8	VC ++ 201 5-2 022 (vc 17) - 14. 32. 313 26. 0
MyQ Central Server 10.2 RC 1	2.4. 57	3.1. 0	WI- V3. 0.8. 335 35	8.2. 8	3.0. 8	VC ++ 201 5-2 022 (vc 17) - 14. 32. 313 26. 0

	Apa che	Apa che SSL	Fire bird	PH P	PH P SSL	C++ Run tim es
MyQ Central Server 10.2 BETA 2	2.4. 57	3.1. 0	WI- V3. 0.8. 335 35	8.2. 6	3.0. 8	VC ++ 201 5-2 022 (vc 17) - 14. 32. 313 26. 0
MyQ Central Server 10.2 BETA	2.4. 57	3.1. 0	WI- V3. 0.8. 335 35	8.2. 5	3.0. 8	VC ++ 201 5-2 022 (vc 17) - 14. 32. 313 26. 0

2 Central Server and MS Cluster

2.1 About

The MyQ MS Cluster high-availability solution consists of multiple nodes in the active/passive configuration with the MyQ server installed on each node. MS Cluster administrates the MyQ services and if the currently active node becomes unavailable, it switches to one of the available passive nodes.

2.2 System Requirements

The fully detailed MyQ Central Server system requirements can be found [here](#).

- Compatibility with Windows Servers

The MyQ MS Cluster solution is supported by the following Windows Server versions and editions:

Windows Server	Editions
Windows Server 2016	Standard, Datacenter
Windows Server 2019	Standard, Datacenter
Windows Server 2022	

- A prepared failover cluster with at least two nodes and storage for MyQ data is needed. Each node must meet the system requirements of the MyQ server and its components.
- The same time zone has to be set on each of the nodes.

 If the MyQ Desktop Client, MyQ Smart Job Manager or the MyQ Smart Print Services applications are to be used on the MyQ users workstations, the IP address or hostname of the cluster has to be set in the applications (not the IP address or hostname of the nodes).

2.3 Licenses

With the new MyQ X licensing model with **Installation Keys** used in MS Cluster, there is only one installation key needed. The HW code is taken from the whole cluster, not individual nodes, so the license is activated against the cluster's HW, and not a single node.

 With the old licensing model, when MS Cluster is used with the MyQ server, the amount of licenses needed depends on the number of nodes used, as the licenses need to be added and activated separately on each node.

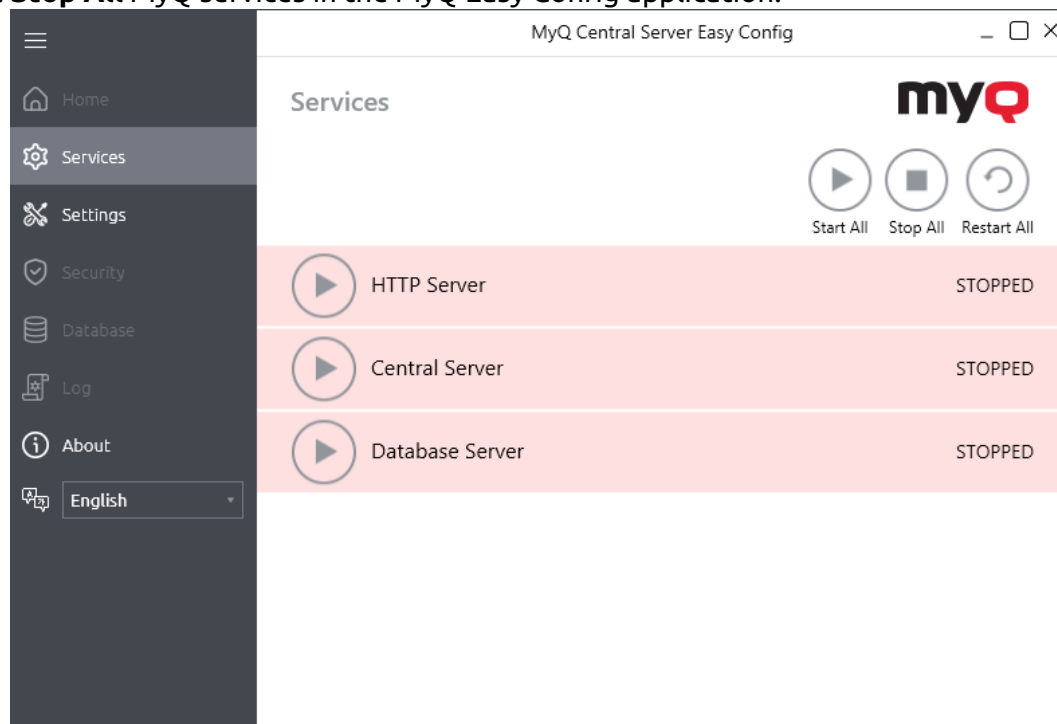
- MyQ server in Site mode - licenses are received from the Central server automatically every day or during MyQ service or Cluster Node restart.
- MyQ server in Standalone mode - needs an extra licenses set for each node; each licenses set must be activated only on one node.

2.4 Setup

2.4.1 Installing MyQ on the server in the cluster (all nodes)

On each cluster node, do the following:

1. Run the MyQ installation file and install MyQ (details can be found [here](#)).
2. Make sure that the time zone set on the MyQ server is the same as the time zone set on each node).
3. **Stop All** MyQ services in the MyQ Easy Config application.

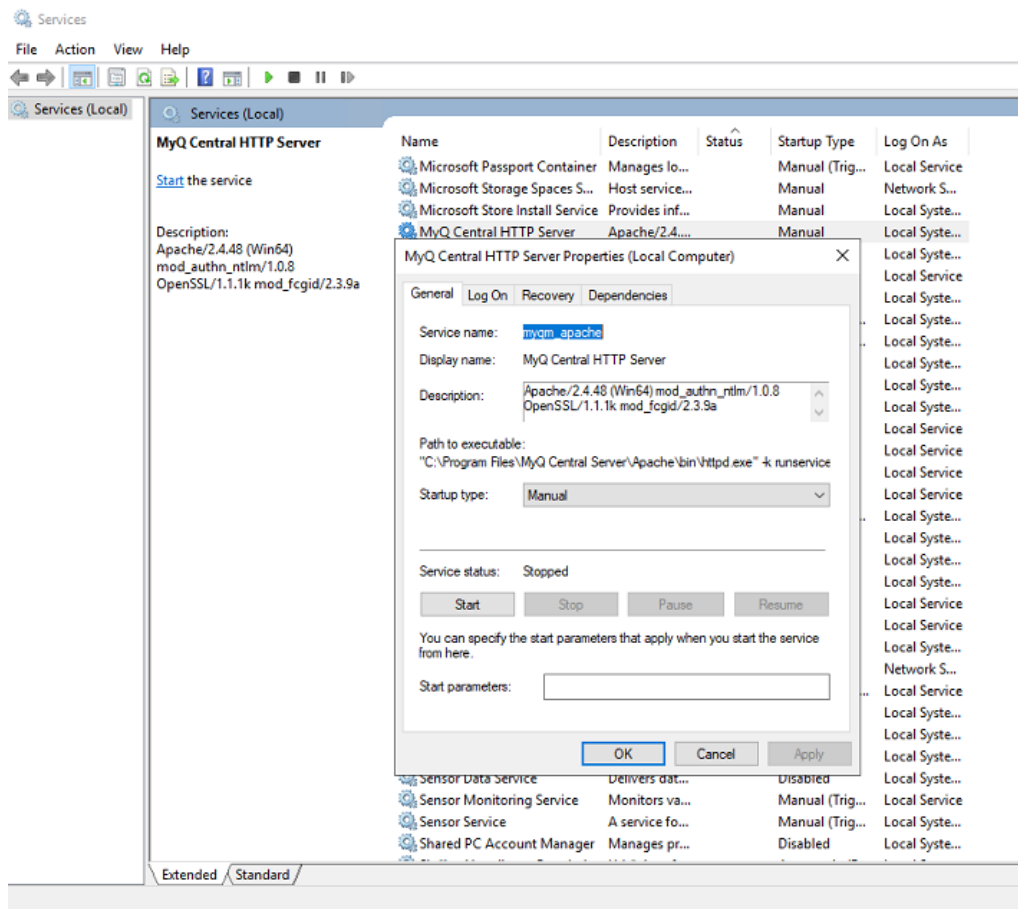


2.4.2 Setting services to manual startup (all nodes)

All services used by the MyQ server need to be set to manual startup, on every node.

The following services need to be changed this way:

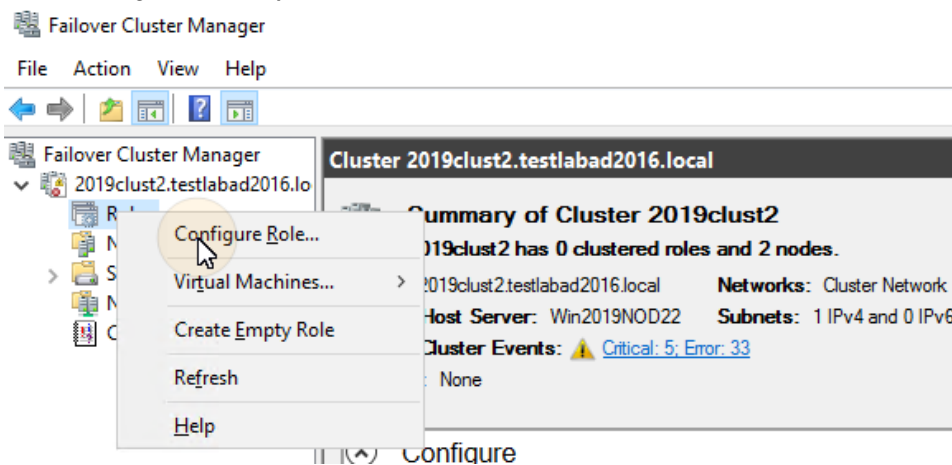
- MyQ Central HTTP Server
- Firebird Server - MasterInstance
- MyQ Central Server



2.4.3 Creating the MyQ server MS Cluster role (Failover Cluster Manager)

Open Failover Cluster Manager and do the following:

1. Right-click **Roles** and select **Configure Role** on the shortcut menu. The High Availability Wizard opens.



2. Click **Next**. The Select role tab opens.
3. On the tab, select **Other Server**, and click **Next**. The Client Access Point tab opens.
4. On the tab, type a new **Name** for the MyQ server cluster, for example *myq-server*, then enter an unoccupied IP address from the network to be used by the MyQ server role, and lastly click **Next**. The Select Storage tab opens. MyQ will use the hostname for communication with terminals, as the SMTP server in MFPs etc.

High Availability Wizard X

Client Access Point

Before You Begin
Select Role
Client Access Point
Select Storage
Select Resource Types
Confirmation
Configure High Availability
Summary

Type the name that clients will use when accessing this clustered role:

Name:

i The NetBIOS name is limited to 15 characters. One or more IPv4 addresses could not be configured automatically. For each network to be used, make sure the network is selected, and then type an address.

	Networks	Address
☒	10.14.4.0/23	10 . 14 . 4 . 176

5. On the tab, select the storage volumes that you want to use for the MyQ server.

High Availability Wizard X

Select Storage

Before You Begin
Select Role
Client Access Point
Select Storage
Select Resource Types
Confirmation
Configure High Availability
Summary

Select only the storage volumes that you want to assign to this clustered role.
You can assign additional storage to this clustered role after you complete this wizard.

Name	Status
☒ Cluster Disk 1	Online
☐ Cluster Disk 2	Online

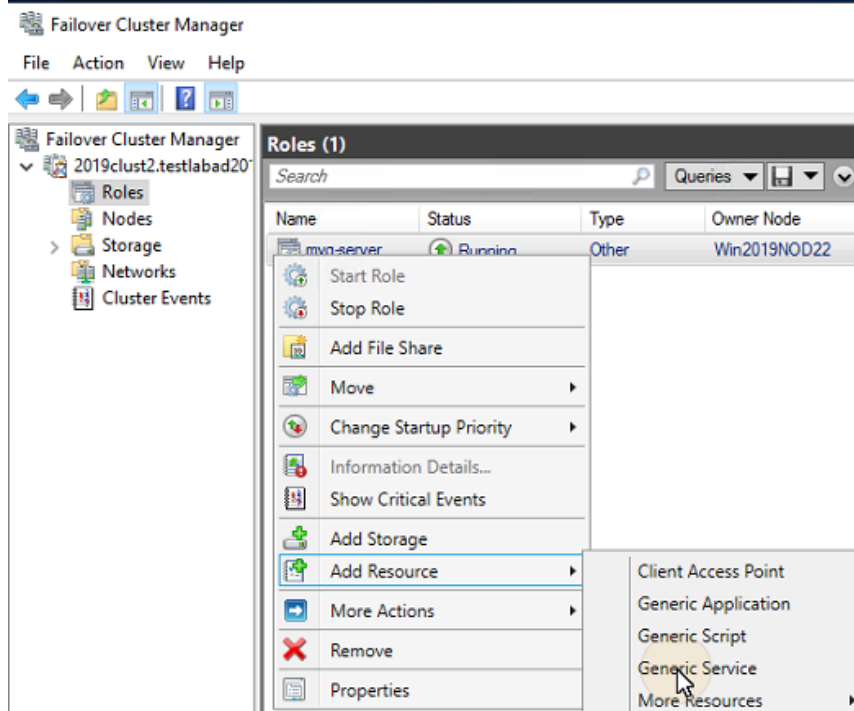
6. Click **Next** to finish the installation process.

2.4.4 Adding MyQ Resources (Failover Cluster Manager)

Once the MyQ server role is created and configured, MyQ resources need to be configured as well, in the **Roles** tab in Failover Cluster Manager.

Add the Firebird server - MasterInstance service to the MyQ server role:

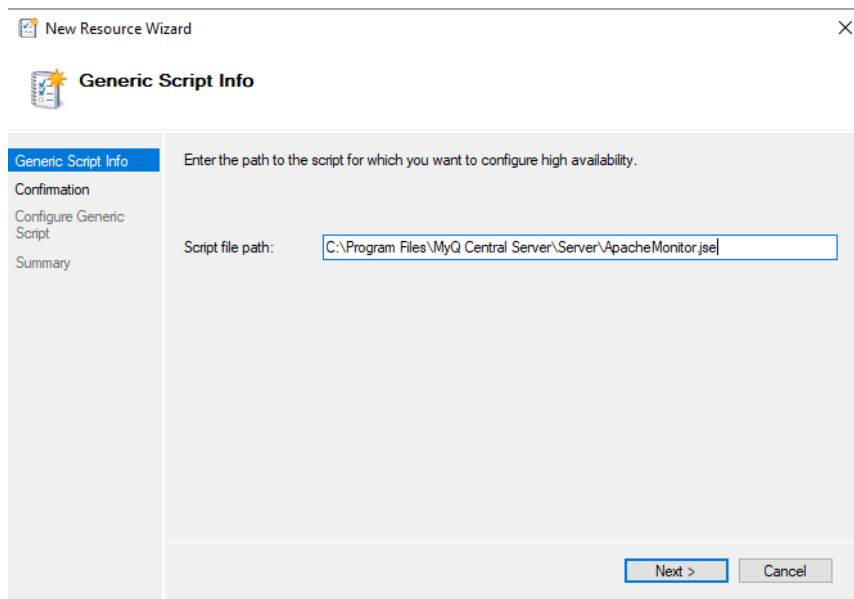
1. Right-click the MyQ server role, then click **Add resource** on the shortcut menu, and click **Generic Service**. The New Resource Wizard opens.



2. In the list of services, select **Firebird Server - MasterInstance**, and click **Next**.
3. On the **Confirmation** tab, click **Next** to create the service. The service is created and configured.
4. Click **Finish** to leave the setup.

Add the Apache Monitor script to the MyQ server role:

1. Right-click the MyQ server role, click **Add resource** on the shortcut menu, and click **Generic Script**. The New Resource Wizard opens.
2. Enter the path to the **ApacheMonitor.jse** script, located in the MyQ installation folder, and click **Next**. The Confirmation tab opens. The default path to the script is:
C:\Program Files\MyQ Central Server\Server\ApacheMonitor.jse

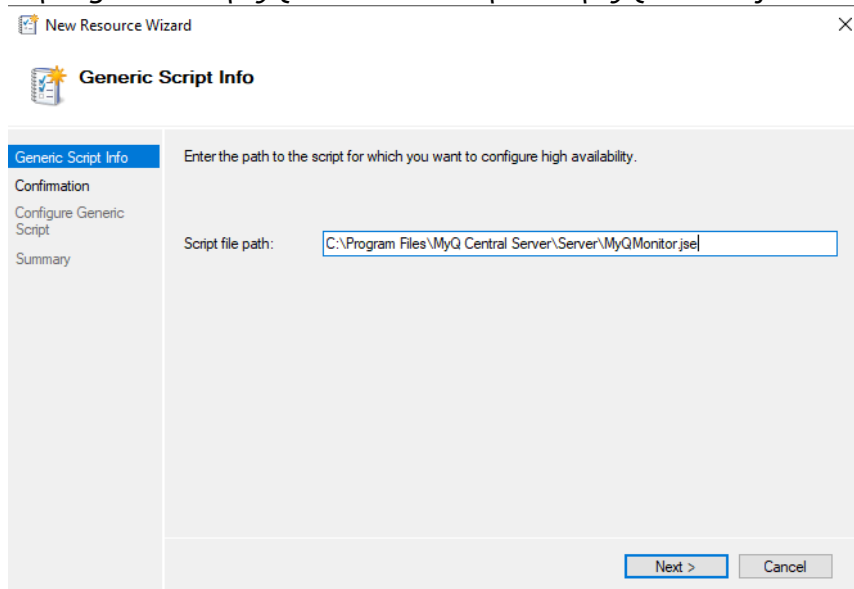


3. On the tab, click **Next** to create the service. The service is created and configured.
4. Click **Finish** to leave the setup.

Add the MyQ Monitor script to the MyQ server role:

1. Right-click the MyQ server role, click **Add resource** on the shortcut menu, and click **Generic Script**. The New Resource Wizard opens.
2. Enter the path to the **MyQMonitor.jse** script, located in the MyQ installation folder, and click **Next**. The Confirmation tab opens. The default path to the script is:

C:\Program Files\MyQ Central Server\Server\MyQMonitor.jse

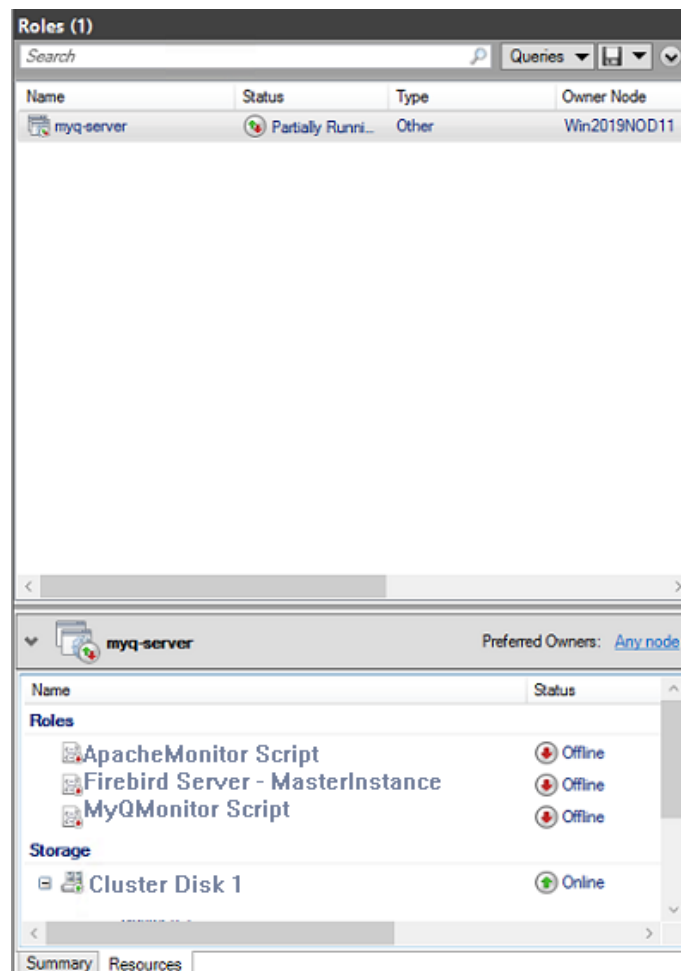


3. On the tab, click **Next** to create the service. The service is created and configured.
4. Click **Finish** to leave the setup.

 If you are using an MS SQL database instead of the Embedded database, you don't need to add the Firebird server - MasterInstance service to the MyQ server role. You should only add the Apache Monitor script, and the MyQ Monitor script.

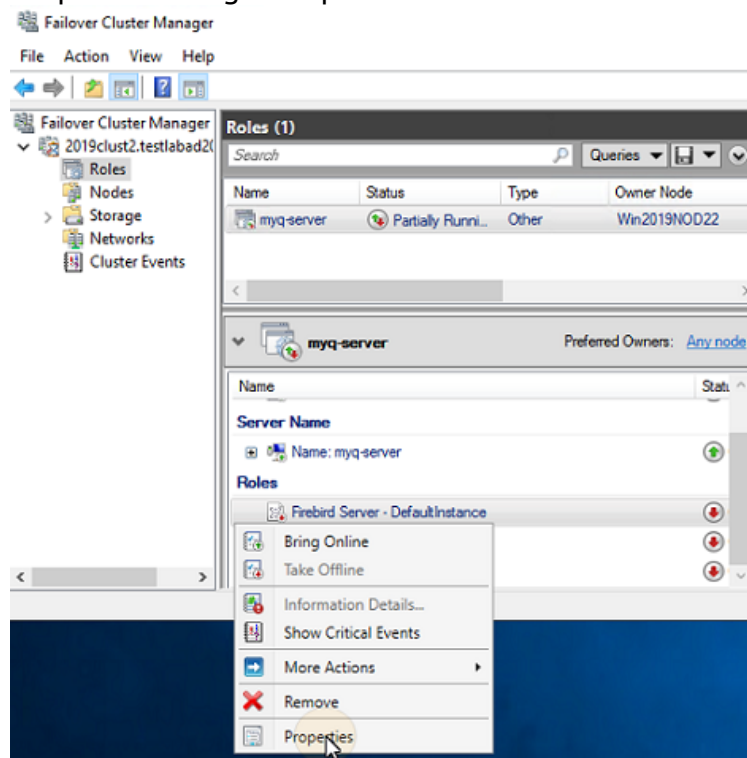
2.4.5 Setting Resources Dependencies (Failover Cluster Manager)

After adding the services and scripts to the MyQ server role, open the **Resources** tab of the MyQ server role at the bottom of the **Roles** tab and set the dependencies of the MyQ services and scripts.

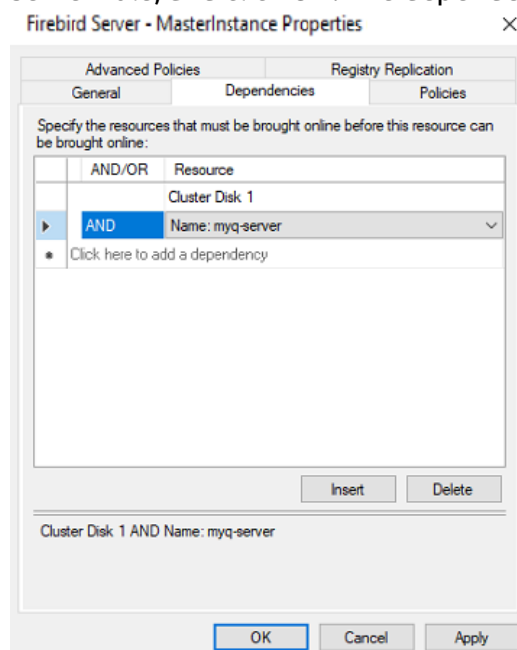


Set the **Firebird Server - MasterInstance** service dependency

1. In the list at the bottom of the tab, right-click **Firebird Server - MasterInstance**, and click **Properties**. The Firebird Server - MasterInstance Properties dialog box opens.



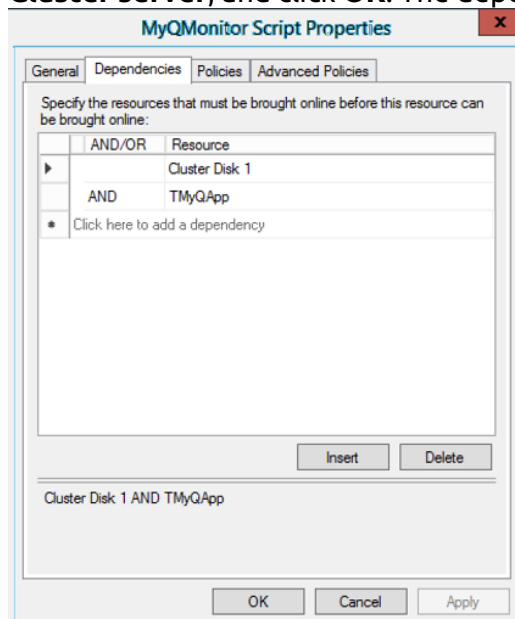
2. In the dialog box, open the **Dependencies** tab, add the shared disk drive (or NAS) where the system is supposed to work on, add the name of the MyQ server role, and click **OK**. The dependency is set.



- Setting the Firebird Server - MasterInstance service dependency is not needed if you are using an MS SQL database.**

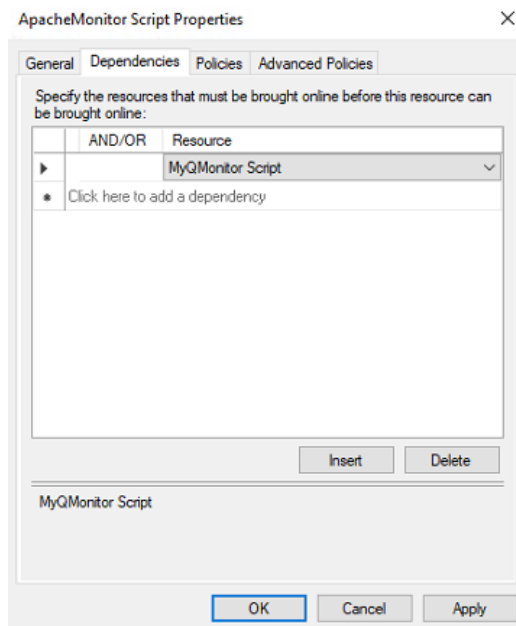
Set the MyQMonitor script dependency

1. In the list at the bottom of the tab, right-click **MyQMonitor Script**, and click **Properties**. The MyQMonitor Script Properties dialog box opens.
2. In the dialog box, open the **Dependencies** tab, add the **Cluster Disk** and the **Cluster server**, and click **OK**. The dependency is set.



Set the ApacheMonitor script dependency

1. In the list at the bottom of the tab, right-click **ApacheMonitor Script**, and click **Properties**. The ApacheMonitor Script Properties dialog box opens.
2. In the dialog box, open the **Dependencies** tab, add the **MyQMonitor Script**, and click **OK**. The dependency is set.



i To open the dependency report, right-click the MyQ server role on the **Roles** tab of the cluster in Failover Cluster Manager, click **More Actions**, and click **Show Dependency Report**.

2.5 Additional Setup

Even though the installation is finished, there are some additional steps needed to setup the environment before bringing the resources online.

2.5.1 Setting up the MyQ admin credentials (active node)

On the active node, open the MyQ Central Easy Config application:

1. On the **Services** tab, **Start All** services.
2. On the **Home** tab, set the **Server Administrator Account** password and the **Database Administrator Password** (if the passwords have been changed before, they can be changed again on the **Settings** tab).
3. On the **Services** tab, **Stop All** services, and close the MyQ Central Easy Config application.

2.5.2 Setting the location of the data folder (all nodes)

On each node of the cluster, you need to set the location of the **Data** folder, which requires access to the shared cluster disk, so the node has to be active. Therefore, you need to switch the active mode between all of the nodes (move the MyQ server role between the nodes).

To set the folder's location, open MyQ Central Easy Config on the currently active node and:

1. On the **Services** tab, **Start All** services.
2. On the **Settings** tab, under the **Data** folder, click **Change location**, and then define the path to the shared cluster disk. (For more information about how to do this, check [here](#)).
3. On the **Services** tab, **Stop All** services, and then close the MyQ Central Easy Config application.
4. In Failover Cluster Manager, move the MyQ server role to the next node and repeat the process.

2.5.3 Running MyQ in the MS Cluster environment

The following instructions have to be followed while MyQ runs in the MS Cluster:

- You should not start, stop or restart MyQ services while MyQ is controlled by the MS Cluster (cluster resources are online). The services should only be managed by Failover Cluster Manager.
- When switching to a different node, MyQ Central Easy Config should not be used on any node.
- When performing system maintenance (cluster resources are offline), but MyQ services are online on any node (activated manually), do not switch to a different node. By doing so, you risk corrupting the MyQ database.
- When switching to a different node, all services on the initial node are stopped by the MS Cluster.
- While MyQ runs in the cluster, the IP address of the MyQ server is the one that you have selected within the setup of the MyQ server role, and the hostname of the MyQ server is the one that you will set in the MyQ web administrator interface after you bring the resources of the MS Cluster online.
- It is strongly recommended to always keep the **Storage** and **Server Name** resources online. In case you need to take them offline, make sure that all MyQ services on the active node (the current owner of the MyQ server role) are stopped in the MyQ Central Easy Config application.
- After completing the setup (setup and additional setup) of the MyQ server role, and also after each crucial change on the cluster, it is recommended to test the cluster by moving the ownership of the MyQ server role between all nodes of the cluster.

2.5.4 Starting the system (Failover Cluster Manager)

To start the system, you have to bring the resources of the MS Cluster online. For information on how to do this, check [here](#).

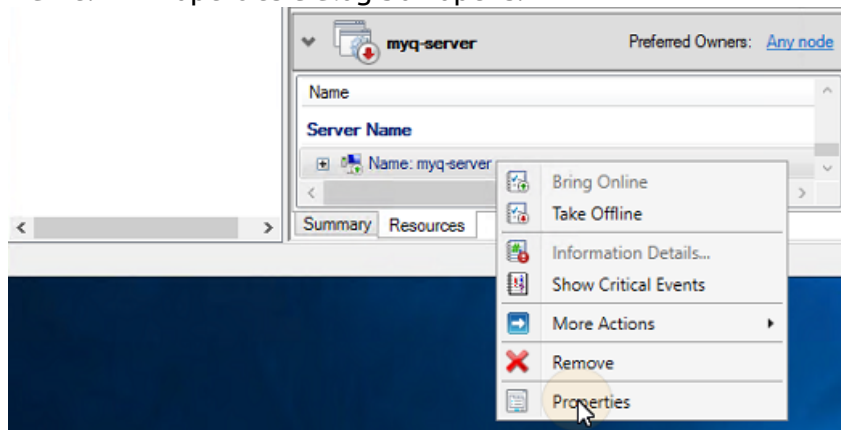
2.5.5 Setting hostname of the MyQ server role

On the **Resources** tab of the MyQ server role in Failover Cluster Manager, you can see (and change) the DNS Name of the MyQ server role. The **Full name** of the role

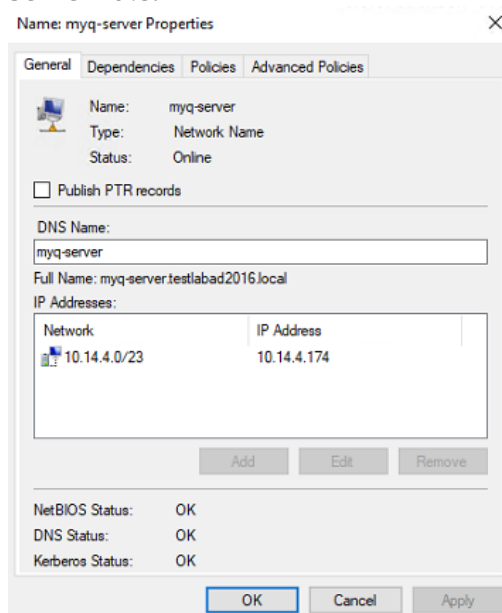
(DNS + domain) needs to be used as the server hostname and as the MyQ X Mobile Client server in MyQ.

To see or change the DNS name of the MyQ server role on the MS Cluster, do the following:

1. In the list at the bottom of the **Resources** tab of the MyQ server role, under **Server Name**, right-click the server's name, and then click **Properties**. The Name:*** Properties dialog box opens.



2. On the **General** tab, you can see (and change) the DNS Name of the MyQ server role.



To set the hostname of the MyQ server role on the MyQ cluster server, do the following:

1. On the **Network** settings tab of the MyQ web administrator interface of the MyQ cluster server, use the **Full name** (DNS + domain) of the MyQ server in the following setting:
 - a. **This server hostname** under **General**.
2. Then click **Save** at the bottom of the tab.

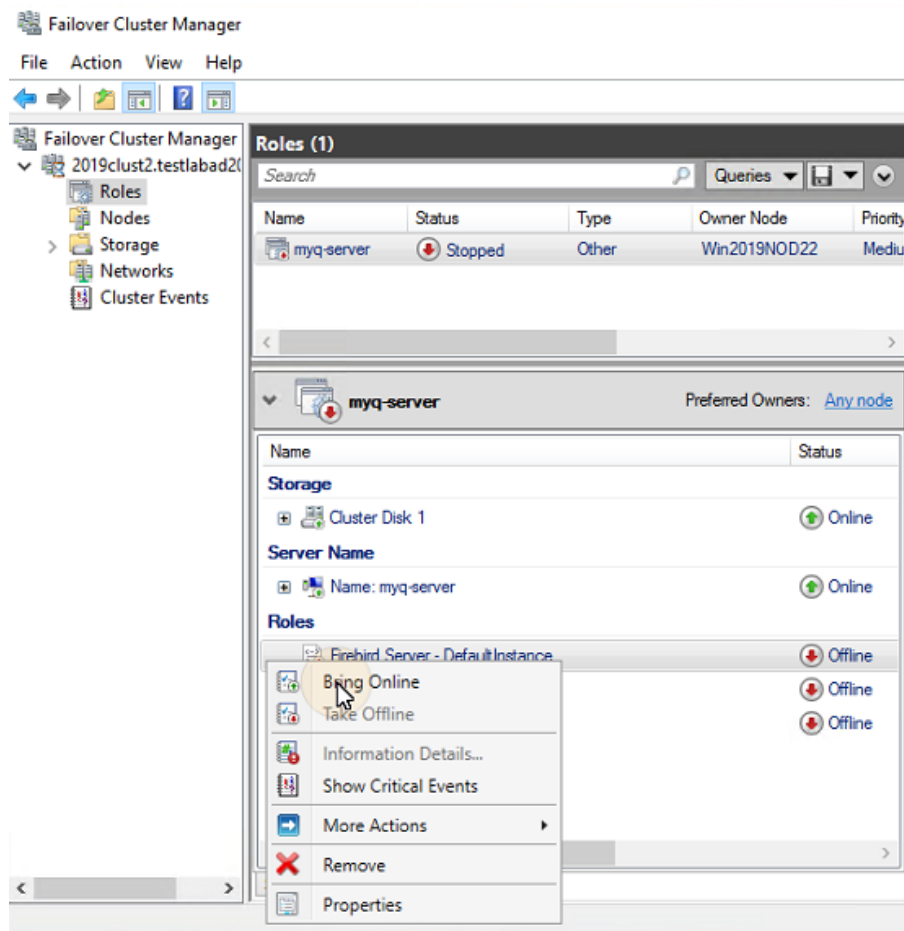
2.6 Configuration and Maintenance

The chapters below show additional configuration and maintenance steps.

2.6.1 Bringing the resources of the MS Cluster online (Failover Cluster Manager)

To start the system, you need to bring all the MS Cluster resources online - the **Firebird Server - MasterInstance** service, the **ApacheMonitor.jse** script, and the **MyQMonitor.jse** script.

To bring a service or script online, open the Failover Cluster Manager application, go to **Roles**, right-click the service or script, and click **Bring Online** on the shortcut menu.

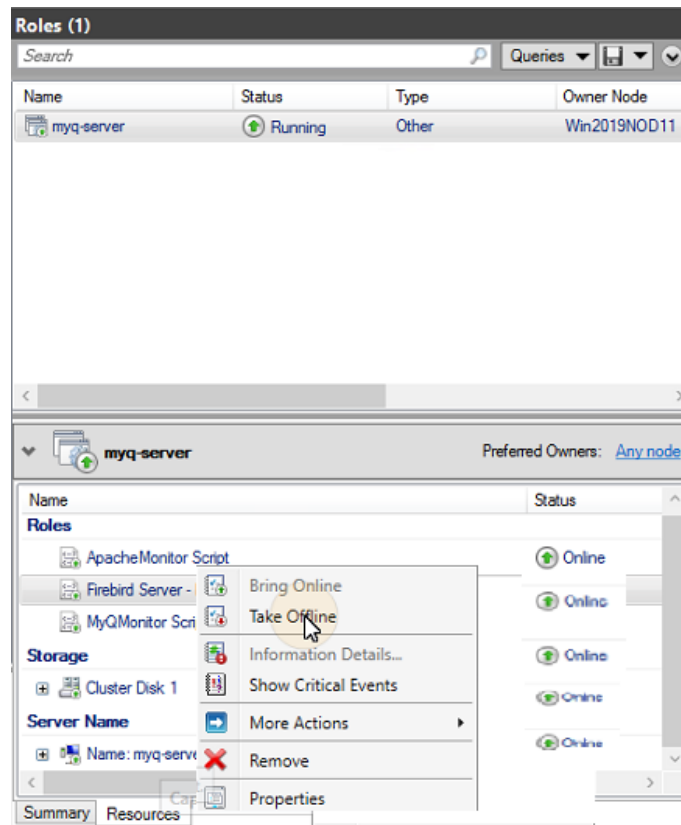


2.6.2 Taking the MS Cluster resources offline (Failover Cluster Manager)

To make sure that all the MS Cluster resources -except for **Storage** and **Server Name**- are offline, it is sufficient to take the **Firebird Server - MasterInstance** service offline; all of the scripts will be taken offline due to their dependency on this service.

 The **Storage** and **Server Name** resources must stay online.

To take the **Firebird Server - MasterInstance** service offline, open Failover Cluster Manager, go to **Roles**, right-click the **Firebird Server - MasterInstance** service, and click **Take Offline** on the shortcut menu.



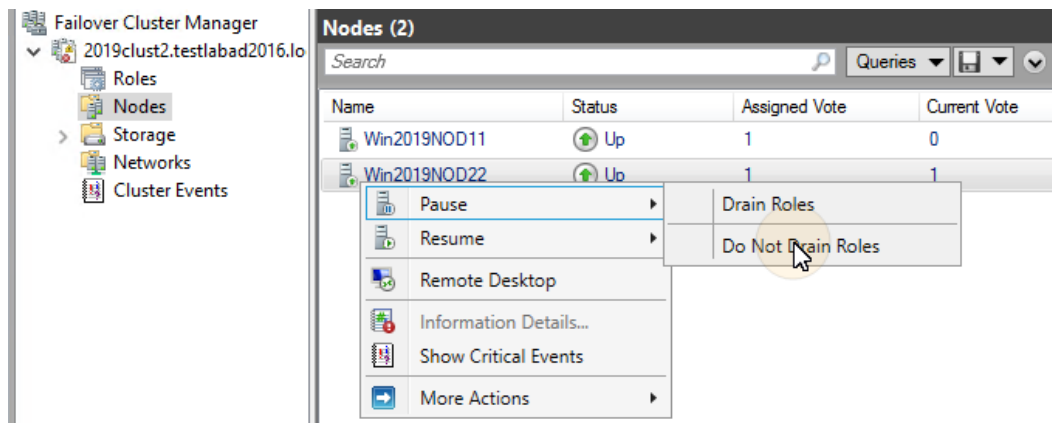
2.6.3 Restarting MyQ services via the MS Cluster (Failover Cluster Manager)

To restart MyQ services via the MS Cluster, take all the MS Cluster resources, except for **Storage** and **Server Name**, offline and then bring them online.

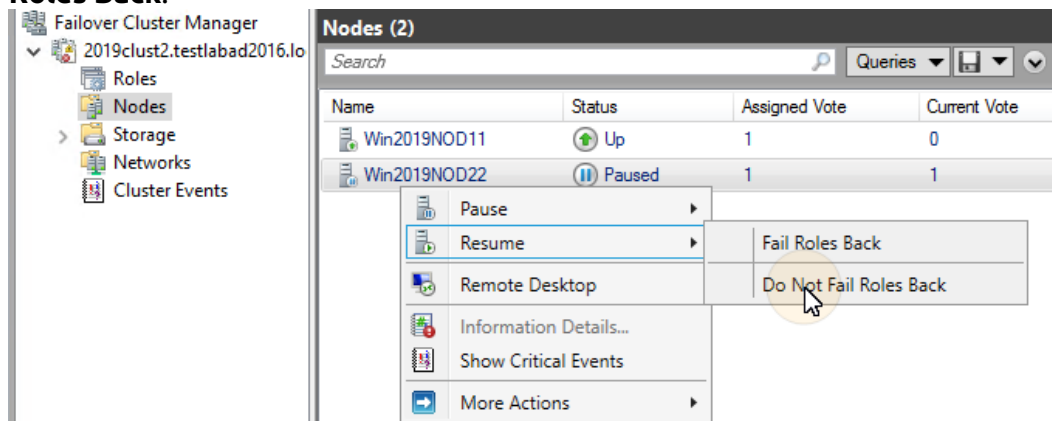
2.6.4 Changing the MyQ admin credentials (active node)

To change the **Server Administrator Account** and **Database Administrator** passwords, you need to do the following on the currently active node (the current owner of the MyQ server role):

1. Open the Failover Cluster Manager application.
2. Open the **Nodes** tab of the cluster, right-click the currently active node, right-click **Pause** on the shortcut menu, and click **Do Not Drain Roles**.



3. Take all the MS Cluster resources, except for **Storage** and **Server Name**, offline.
4. Open the MyQ Central Easy Config application, start all services, change the passwords, stop all services, and lastly close the application.
5. Bring the resources of the cluster online.
6. Open the **Nodes** tab of the cluster in Failover Cluster Manager, right-click the node, right-click **Resume** on the shortcut menu, and lastly click **Do Not Fail Roles Back**.



2.7 Backup and Restore

2.7.1 Backing up the MyQ database on the MS Cluster

The automatic and manual backup processes do not differ from the standard backup processes described in “[Backing up MyQ Data](#)”. The only setting that requires special attention is the backup destination folder. It is recommended to save the backup files on the shared cluster disk.

2.7.2 Restoring the MyQ database on the MS Cluster (all nodes)

Before restoring the MyQ database, MyQ has to be installed and set up on all the MS Cluster nodes.

Now you need to restore the MyQ database and settings on the active node of the Cluster (the current owner of the MyQ server role) via the following steps:

1. **Start All** services via MyQ Central Easy Config.
2. Open the **Database** tab in MyQ Central Easy Config.
3. In the **Main Database** section, click **Restore...**. Select the *database_*.zip* file, and click **Open**. If the backup is password protected, there is a prompt to provide the password. The database is restored and, if needed, upgraded as well.
4. Repeat the process for all the other nodes.

2.7.3 Using Database Encryption

If you are using the **Database Encryption** feature in MyQ Central Easy Config, it is necessary to perform the following steps after encrypting or restoring your database:

1. Stop all Cluster resources except for **Storage** and **Server Name**.
2. Open MyQ Central Easy Config on the active node and start all services.
3. Enable DB encryption.
4. **Stop All** services in MyQ Central Easy Config.
5. Copy the DB encryption key to all the other nodes. The key is located by default in
"C:\Program Files\MyQ Central Server\Firebird\plugins\keyholder.conf".
6. **Start All** MyQ services in MyQ Central Easy Config, and bring all the resources online via Failover Cluster Manager.

2.8 Upgrading MyQ

2.8.1 Necessary steps before the upgrade

Before starting the upgrade, make sure that you have an up-to-date and properly finished backup of the MyQ database. The database can be backed up either manually in MyQ Central Easy Config or automatically as a scheduled task in the MyQ web administrator interface. To make sure that the backup file is preserved, it is recommended to copy the database backup file to a different location.

2.8.2 Upgrading MyQ (all nodes)

The upgrade needs to be performed on each node of the cluster. To be able to upgrade MyQ on a node, you need to have access to the shared cluster disk, so the node has to be active. Therefore, you need to switch the active mode between all of the nodes (move the MyQ server role between the nodes).

Before upgrading MyQ on the nodes, take all the MS Cluster resources, except for Storage and **Server Name**, offline.

To upgrade MyQ on all nodes, start with the currently active node (the owner of the MyQ server role) and do the following:

1. **Start All** services via MyQ Central Easy Config.
2. Run the MyQ installation file.
3. Finish the installation process.
4. **Stop All** services via MyQ Central Easy Config, and then close the MyQ Central Easy Config application.
5. Move the MyQ server role to the next node and repeat all the steps.

After MyQ is upgraded on all the nodes, bring all the MS Cluster resources online.

 During the installation, you might encounter a warning message about a problem related to updating the MyQ database. In such cases, continue with the setup, as the problem does not impact the installation.

2.9 Recommended Troubleshooting

The MS Cluster solves issues on the currently active node which might affect the availability of the MyQ server, by switching to one of the available passive nodes.

Problems related to the MyQ server need to be treated manually. In case you encounter such problems, it is recommended to restart MyQ services in the Failover Cluster Manager application. If the problem persists, contact MyQ support.

In case the MS Cluster does not start, try taking all the MS Cluster resources, except for **Storage** and **Server Name**, offline, and then try to manually start MyQ services. If successful, it is likely that the problem is on the cluster side; otherwise the problem is probably related to the MyQ server, in which case contact MyQ support.

3 System Requirements



The operating system and other software require their own additional system resources. The system requirements described below are only for MyQ solution.

3.1 MyQ Central Server mode with integrated Firebird database

MyQ Central Server	1 - 10,000 users	10,001 - 50,000 users	50,001 - 100,000 users
Physical Core*	6	6	6
RAM	8GB	12GB	16GB

Valid for a typical deployment:

- Integrated Firebird database - installed automatically.
- Central Server features:
 - Data replication from site servers
 - User synchronization
 - License distribution
- Up to 500 Sites (See [\(10.2\) System Requirements](#) for site requirements.)
- Up to 30,000 printers total on MyQ Central Server.

3.1.1 Recommendations

- Install Windows updates out of the replication or user synchronization time.
- Always monitor the server performance during peak usage hours and adjust the settings accordingly.
- Changing the power plan of Windows Server in *Control Panel – Hardware – Power Options* from Balanced (the default setting) to **High performance** is recommended to utilize the maximum performance. This may help speed up database operations.



It is possible to install MyQ Central Server and MyQ Site Server on one Server, but it is recommended only for small installations (small Site Server). In this case, the HW requirements for both MyQ Central and MyQ Site Server need to be taken into account.

3.2 MyQ Central Server mode with an external MS SQL database

MyQ Central Server	1 - 10,000 users	10,001 - 50,000 users	50,001 - 100,000 users
Physical Core*	4	4	4
RAM	4GB	6GB	6GB

MS SQL server (database)	1 - 10,000 users	10,001 - 50,000 users	50,001 - 100,000 users
Physical Core*	6	6	6
RAM	12GB	24GB	32GB

*number of physical cores with 3,5GHz frequency (calculated with AMD Ryzen Threadripper 1920X 3,5GHz).

Valid for a typical deployment:

- External MS SQL database used.
- Central Server features:
 - Data replication from site servers
 - User synchronization
 - License distribution
- Up to 500 Sites (See [\(10.2\) System Requirements](#) for site requirements.)
- Up to 30,000 printers total on MyQ Central Server.

3.2.1 Recommendations

- Install Windows updates out of the replication or user synchronization time.
- Always monitor the server performance during peak usage hours and adjust the settings accordingly.
- Changing the power plan of Windows Server in *Control Panel – Hardware – Power Options* from Balanced (the default setting) to **High performance** is recommended to utilize the maximum performance. This may help speed up database operations.

3.2.2 Operating System

Windows Server 2016/ 2019/2022/2025, with all the latest updates; only 64bit OS supported.

Windows 8.1/10/11 **, with all the latest updates; only 64bit OS supported. Be aware that the EULA for Windows 10 and 11 limits the number of connections to 20 clients.

**For the trouble-free running of the machine, it is strongly recommended using a server operating system.

3.3 Additional software required

- [.NET Runtime 8](#)
- ASP .NET Core 8
- Windows Desktop Runtime 8

i Microsoft .NET Core 8 is installed automatically at the beginning of the MyQ installation. If installation fails, the installer can not proceed, and the installation is terminated. In such case, .NET Core 8 has to be installed prior to MyQ installation manually. Microsoft .NET Framework is not automatically installed and needs to be installed prior to running MyQ installation. We recommend enabling automatic .NET updates using Microsoft Update, learn how to do so [here](#).

Windows Server 2022 Core

If the Easy Config does not launch, it may be necessary to install [Server Core App Compatibility Feature on Demand in Windows Server](#). It can be installed from PowerShell as a Windows Update using this command:

```
Add-WindowsCapability -Online -Name
ServerCore.AppCompatibility~~~~0.0.1.0
```

Restart the server after installation is finished.

3.3.1 Storage sizing

The MyQ Central Server installation files are approximately 300MB.

Minimum 10GB dedicated disk for MyQ Data storage (jobs, main database and log database) is recommended; see the below tables for more details.

Data storage with integrated Firebird database (included users, replications):

	10k jobs	100k jobs	1M jobs
MYQ database	30MB	200MB	1,5GB
MYQLOG database	30MB	300MB	3GB

MyQ data folder storage counted for 1 year.

Data storage on external MS SQL database (include users, replications):

	10k jobs	100k jobs	1M jobs
MYQ database	500MB	700MB	7GB
MYQLOG database	1GB	1,5GB	3GB

MyQ data folder storage counted for 1 year.

Storage performance

- minimum 100 IOPS required.
- RAID data storage supported.

3.3.2 Database

- Microsoft SQL Server 2016 or newer.
 - Microsoft SQL Server 2017 or newer is recommended.
- On MS SQL Server older than 2017:
 - CLR must be enabled (<https://docs.microsoft.com/en-us/sql/relational-databases/clr-integration/clr-integration-enabling>).
 - User with owner privileges for Main and Log database.
- User (Server user/login) used to connect to the DB must have their default language set to *us_english*.

3.3.3 Web browser

- Microsoft Edge 91 or higher (Recommended)
- Google Chrome 91 or higher
- Mozilla Firefox 91 or higher
- Apple Safari 15 or higher
- Opera 82 or higher
- Internet Explorer and MS Edge Legacy are no longer supported

3.3.4 Security

DigiCert Global Root CA certificate (required for Installation Key license activation)

→ <https://www.digicert.com/kb/digicert-root-certificates.htm#roots>.

It should be included by default in the latest updated Windows versions.
Supported Public Key Infrastructure for asymmetric cryptography.



Limitations:

- To make sure that the MyQ system runs smoothly, you need to set an exception for MyQ in your antivirus setup.
- MyQ should not be installed on a Domain Controller.

3.4 MyQ installation in Private Cloud

MyQ can also be installed in Private Cloud. For requirements and further details, see [Installation in Private Cloud](#).

For the Print Server requirements, check the [MyQ Print Server](#) guide.

3.5 Main Communication Ports

If you need to adjust your firewall, it is recommended to allow MyQ processes in the firewall and not particular ports. If you allow particular ports, MyQ may stop working if:

1. you change port settings in MyQ, or
2. you upgrade to a newer version and the port specification has changed.

3.5.1 Incoming Ports

The server is listening on the following ports (does not include private ports):

Protocol	Port	Configurable	Description
TCP	8083	Yes (MyQ Easy Config)	HTTP protocol for accessing the MyQ Web interface and REST API.
TCP	8093	Yes (MyQ Easy Config)	HTTPS protocol for accessing the MyQ Web interface and REST API.

3.5.2 Outgoing Ports

The server is connecting to the following ports (does not include localhost connections):

Protocol	Port	Description
TCP	443	• License activation server. The MyQ license server address is license2.myq.cz. • Other enabled services from Settings → Connections (e.g., Microsoft Exchange Online).

You can also set up additional services that require further configuration and their port will often differ:

Protocol	Port	Default	Description
TCP	Custom	25/465/587	Connection to SMTP server for sending outgoing emails from MyQ.
TCP	Custom	389/636/1812	Connection to Authentication server(s) (LDAP, Radius, ...) for user authentication/synchronization.
TCP	Custom	8090/443	Site server(s) connection.
TCP	Custom	-	Connection to External credit account.



For a complete list of the ports used by Site servers, check [Main communication ports](#) in the MyQ Print Server guide.

4 Installation

- ✓ A comprehensive guide to installing and upgrading all MyQ components is available [here](#).

This topic shows you how to install the MyQ Central server and how to connect it to a database.

- ⓘ Before you start the installation, make sure your system is up to date and meets the requirements as described in [System Requirements](#).

MyQ Central server is installed simply by running the executable file and following the instructions of the installation wizard.

1. Download the latest available MyQ Central Server version from the MyQ Community portal (*MyQ Central Server X.X.X.X*).
2. Run the executable file. The Select Setup Language dialog box appears.
3. Select your language, and then click **OK**. The License Agreement dialog box appears. Select **I accept the agreement**, and click **Next**. The Accessibility mode dialog box appears.
4. Select between the *Standard* or *Enhanced* accessibility mode, and click **Next**. The Select Destination Location dialog box appears.
5. Select the folder where you wish to install MyQ Central server. The default path is:
C:\Program Files\MyQ Central Server.
6. Click **Next**. The Select Components dialog box opens.
7. If you want to use the MyQ Embedded database server, keep the **Embedded Database** option selected (default setting). If you want to use an MS SQL database server, you should clear the selection. Click **Next**. The Ready to Install window opens, with an overview of your selections.
8. Click **Install**. MyQ Central server is installed on your computer. Depending on the OS settings on the server, you might be asked to restart the computer. If you are asked to restart the computer, you need to do so in order to finish the installation. After the restart, the MyQ Central Server Easy Config application opens and you can continue with the setup there.

4.1 Central Server Database Setup

Within the installation of the MyQ Central Server, you can either use the Embedded (Firebird) database, or later set up a connection to your own MS SQL Server.

If you select to use the Embedded database, you can still choose between both options afterwards, while if you install the MyQ server without it, you have to use the MS SQL Server.

Unless you have already been using an MS SQL server within your company and want to connect MyQ to your MS SQL database, it is recommended to install and employ the Embedded Database.

4.1.1 Embedded Database Configuration

As the Embedded Database is fully integrated with the MyQ server, it does not require any further configuration.

4.1.2 MS SQL Server Configuration

To enable a connection to an MS SQL server, you need to make sure that the following options are set on there:

- Authentication has to be set to the **MS SQL Server and Windows Authentication** mode.
- A user account with the **public** fixed server role for access to the MS SQL Server; a user account with the **dbcreator** fixed server role, for creating the MyQ database. The default language of the user who creates the database must be set to **English (US)**.
- On MS SQL Server 2016 and older, the **common language runtime (CLR)** integration feature has to be enabled.
- **TCP/IP** protocol has to be enabled and the **IPAll** TCP Port has to be set to **1433**.
- A **TCP 1433** port inbound rule has to be created in the Firewall.

Once the MyQ Central server is installed, the MyQ Central Server Easy Config application opens and you are asked to select and set the MyQ database. The two following sections describe the setup of the database after the installation.

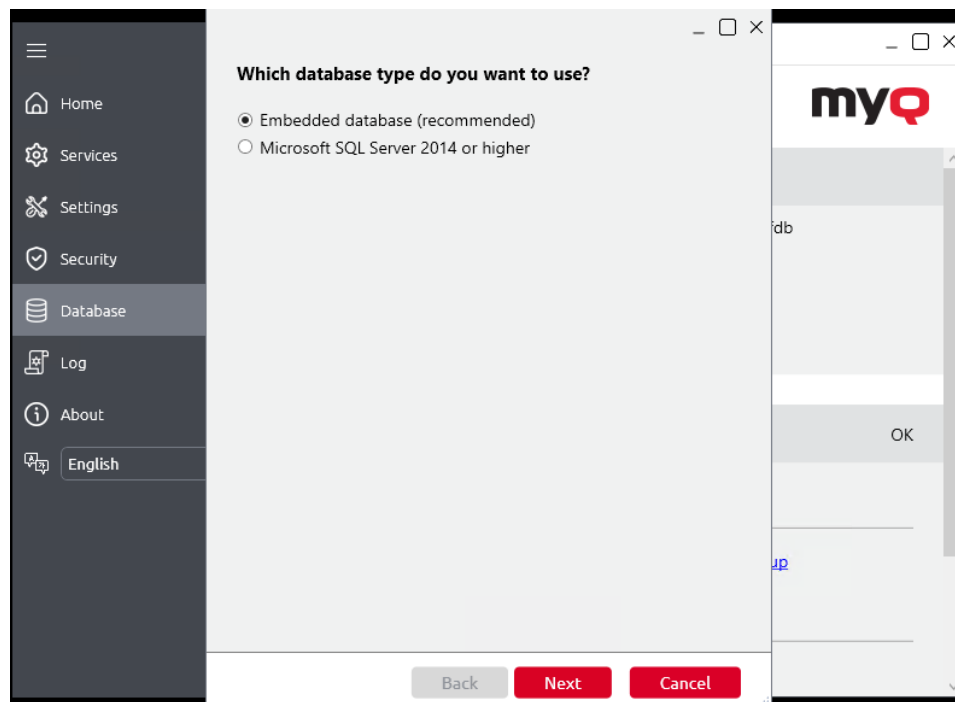


If you have deselected the **Embedded Database** option during the installation, the MyQ Embedded database option is no longer available on the MyQ server.

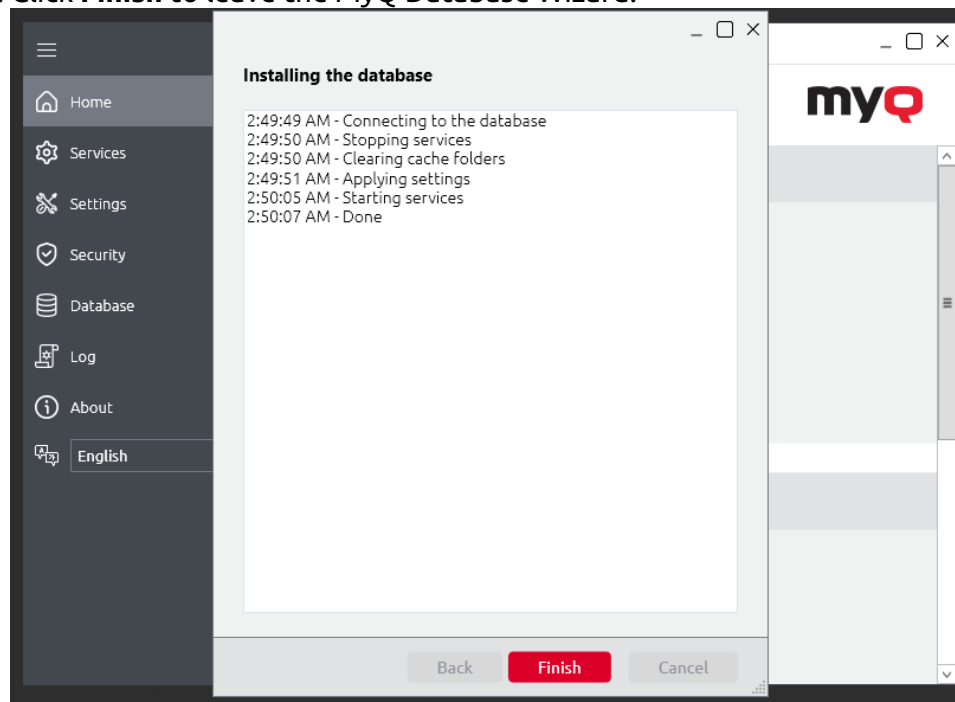
4.1.3 Setting up the Embedded Database

To set up the Embedded database:

1. Select the **Embedded Database (recommended)** option, and click **Next**. The database is installed and upgraded if needed.



2. Click **Finish** to leave the MyQ Database Wizard.



4.1.4 Setting up an MS SQL Database

To set up an MS SQL database:

1. Select the **Microsoft SQL Server 2016 or higher** option and click **Next**.

MyQ Central Server Installation

What type of database do you want to use?

☐ Embedded database (recommended)
☒ Microsoft SQL Server 2016 or higher

[Help](#)
Back
Next
Cancel

2. Fill in the setup fields with the following information:

MyQ Central Server Installation (1/4)

Provide the MS SQL Server connection information

Database server address:

mssql

Server port:

1433

☒ Secure connection

Authentication type:

☒ Windows Authentication

Username:

AD\Administrator

This account will be used to configure the database. To use a different account run MyQ Easy Config using that account.

☐ SQL Server Account

[Help](#)
Back
Next
Cancel

MyQ Central Server Installation (1/4)

Provide the MS SQL Server connection information

Database server address:

mssql

Server port:

1433

☒ Secure connection

Authentication type:

☐ Windows Authentication

☒ SQL Server Account

Username:

mssqluser

Password:

.....

[Help](#)
Back
Next
Cancel

1. **Database server address:** the IP address or the hostname of the MS SQL server.
 - a. **Server port:** TCP port used for communication with the MS SQL server; by default it is *1433*. In case of a Local database, the Server port field must be left empty.
 - b. **Username/Password:** Login credentials for accessing the MS SQL database management. The login account has to have the **public** fixed server role for access to the MS SQL database. You can alternatively use **Windows Authentication**.
2. Select the account the services will run under. This account must have the **Log on as a service** user right.

MyQ Central Server Installation (2/4) ×

Select the account under which the services will run

☒ Custom account

Account:

AD\gMSA-CSS Browse...

The account must have the "Log on as a service" user right.

Password:

[Help](#) Back Next Cancel

MyQ Central Server Installation (2/4) ×

Select the account under which the services will run

☒ Custom account

Account:

mssqluser@ad.fp.local Browse...

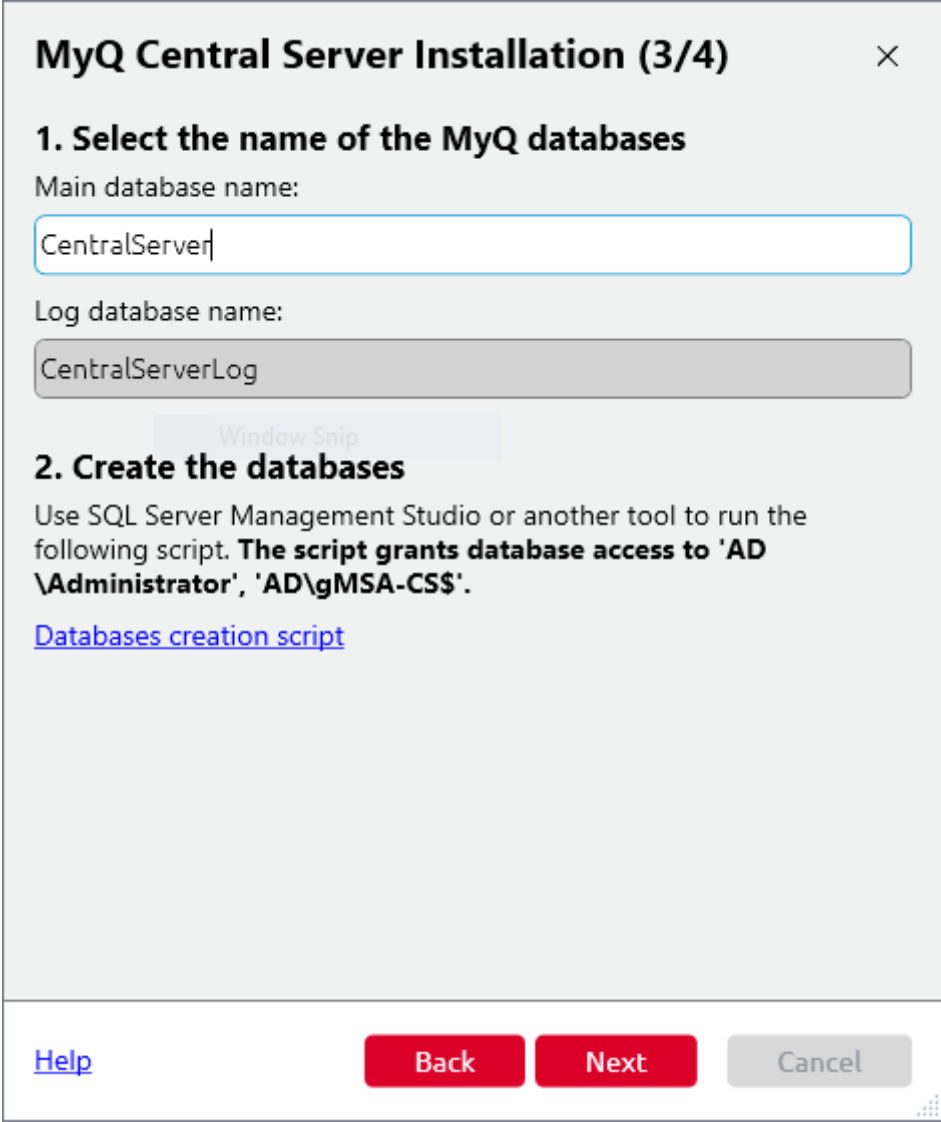
The account must have the "Log on as a service" user right.

Password:

.....

[Help](#) Back Next Cancel

3. Fill in the **Main database name** (name of the new MyQ MS SQL database for example *MyQDatabase*), the **Log database name** is automatically filled according to the Database name and run the **Databases creation script**.



MyQ Central Server Installation (3/4) ×

1. Select the name of the MyQ databases

Main database name:

CentralServer

Log database name:

CentralServerLog

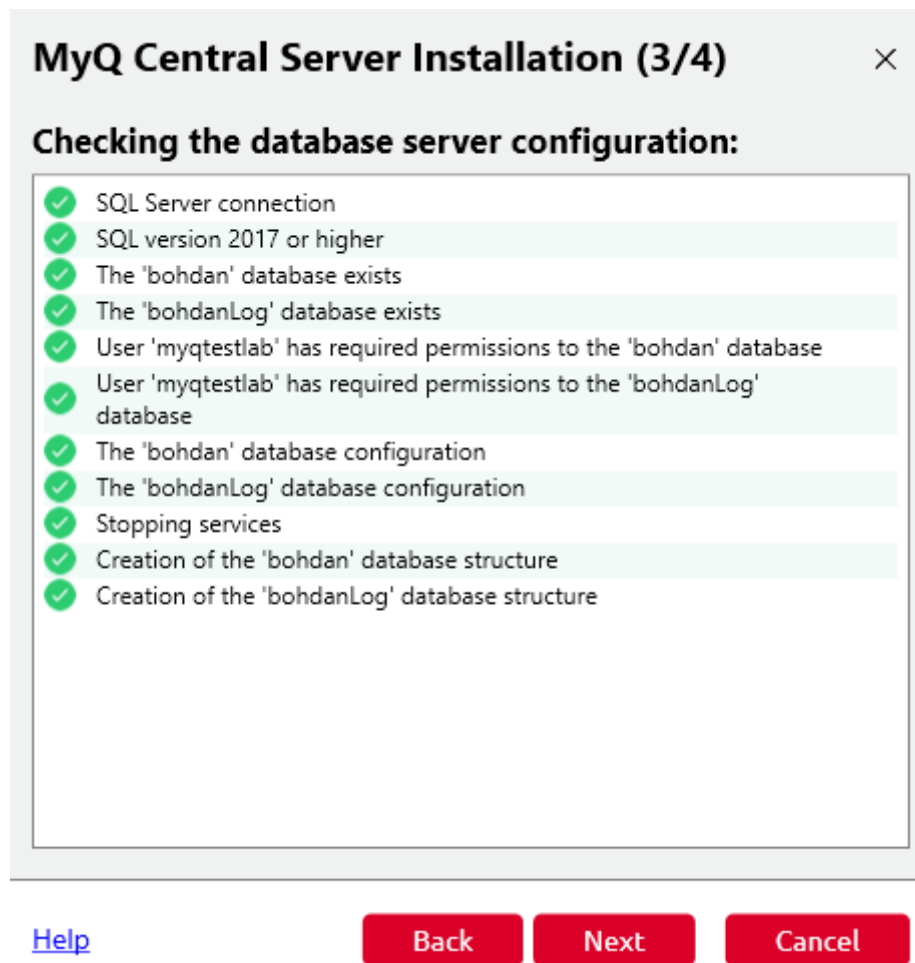
2. Create the databases

Use SQL Server Management Studio or another tool to run the following script. **The script grants database access to 'AD \Administrator', 'AD\gMSA-CSS'.**

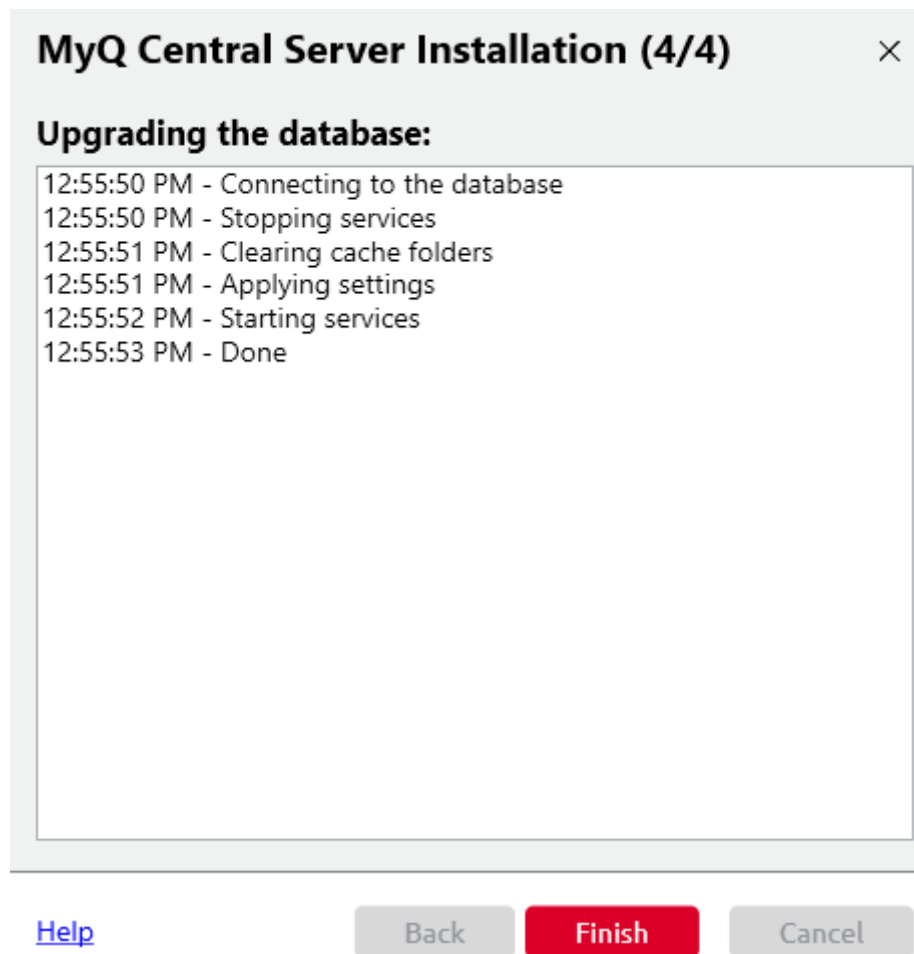
[Databases creation script](#)

[Help](#) **Back** **Next** Cancel

4. Once the databases are successfully created, click **Next** to continue. MyQ Central Server Easy Config will run the Database Prerequisites Check.



5. Click **Finish** to leave the MyQ Database Wizard.

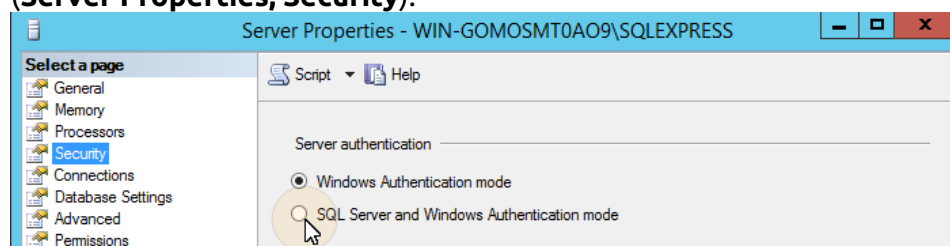


4.1.5 MS SQL Server Setup Example

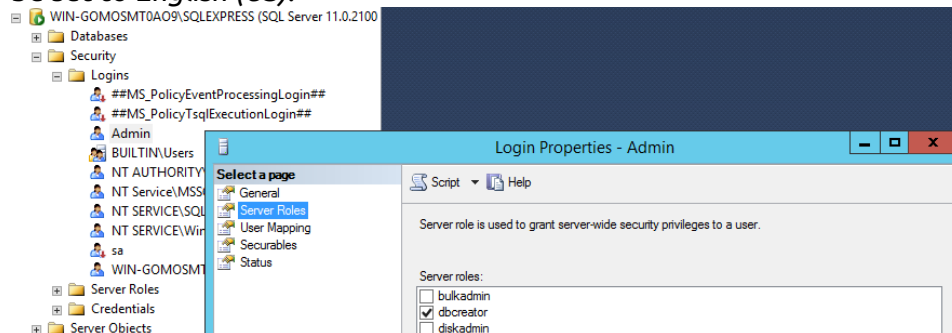
This is an example of an installation of a Microsoft SQL server and the setup necessary for its connection to the MyQ Central server.

To install and set up the MS SQL server:

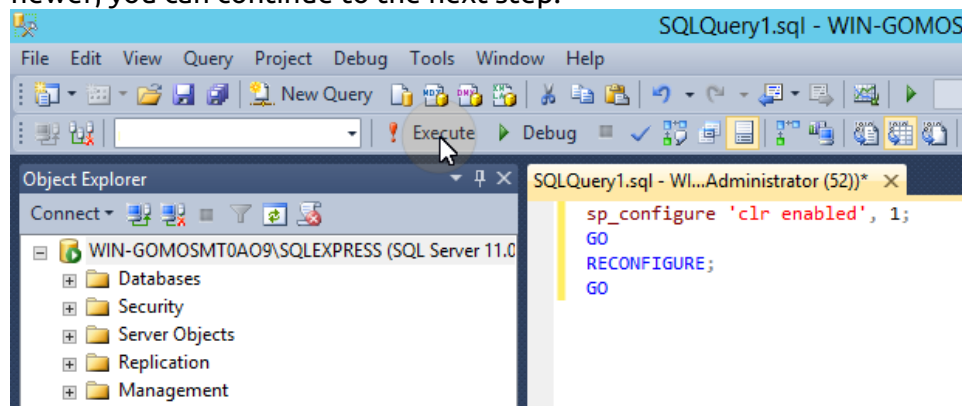
1. Install the MS SQL Server and the MS SQL Server Management Studio application.
2. Open the SQL Server Management Studio app (Windows Apps menu).
3. Change the **Server authentication** setting of the MS SQL Server from the *Windows Authentication mode* to *SQL Server and Windows Authentication mode* (**Server Properties, Security**).



4. Provide any user account (existing or new) with the **Database Creator** role. This account will be used to access the MS SQL server and manage the MyQ database there, which means that the MyQ administrator needs to know its credentials. The default language of the user who creates the database must be set to *English (US)*.



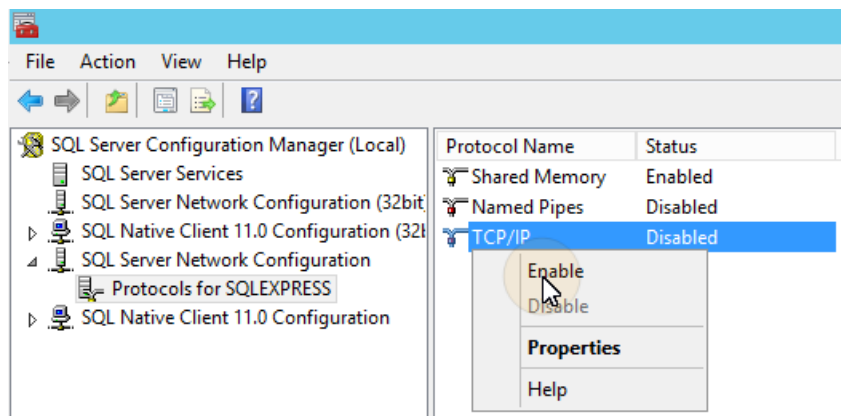
5. On MS SQL Server 2016 and older, you need to enable the common language runtime (CLR) integration feature. If you are using the MS SQL Server 2017 or newer, you can continue to the next step.



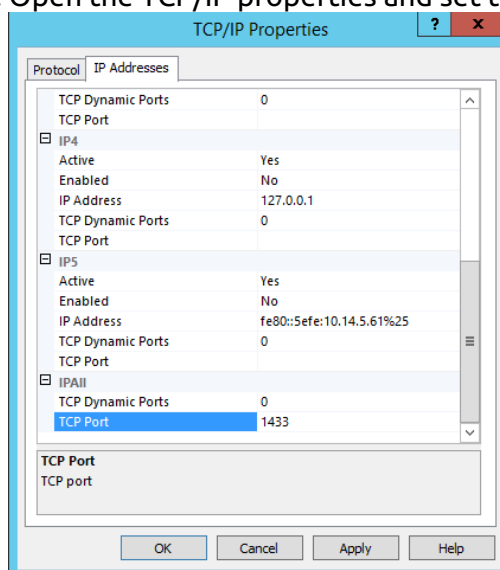
To enable the CLR, use the following script:

```
sp_configure 'clr enabled', 1;
GO
RECONFIGURE;
GO
```

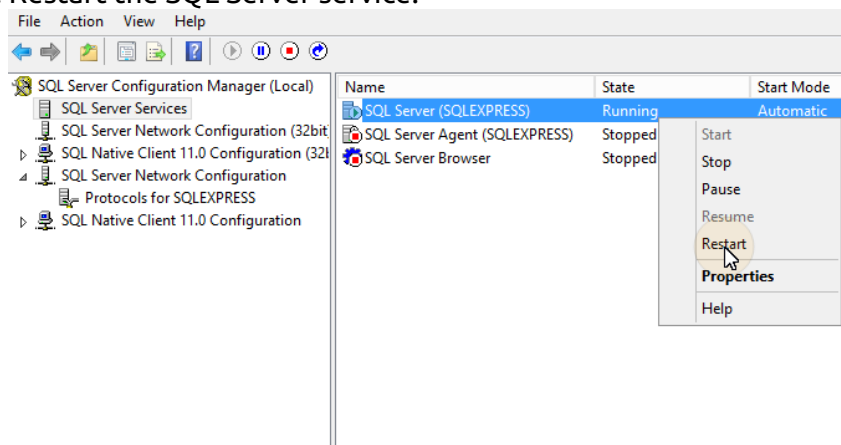
6. Leave the MS SQL Server Management Studio and open the SQL Server Configuration Manager app.
7. Enable the TCP/IP protocol.



8. Open the TCP/IP properties and set the **IPAll TCP Port** to 1433.

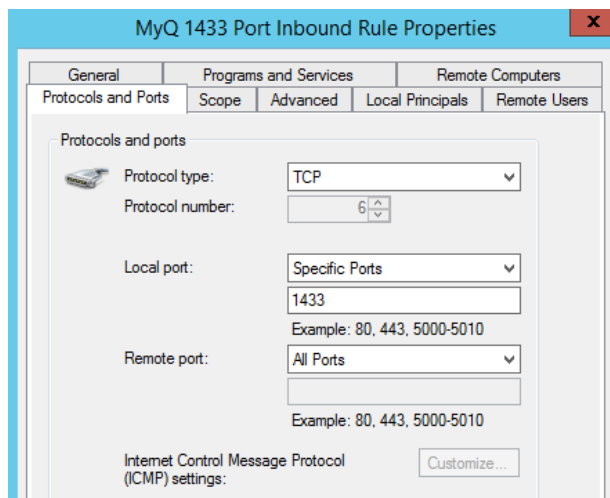


9. Restart the SQL Server service.



10. Leave the SQL Server Configuration Manager.

11. Create a TCP 1433 port inbound rule in Windows Firewall.



12. Exit the setup.

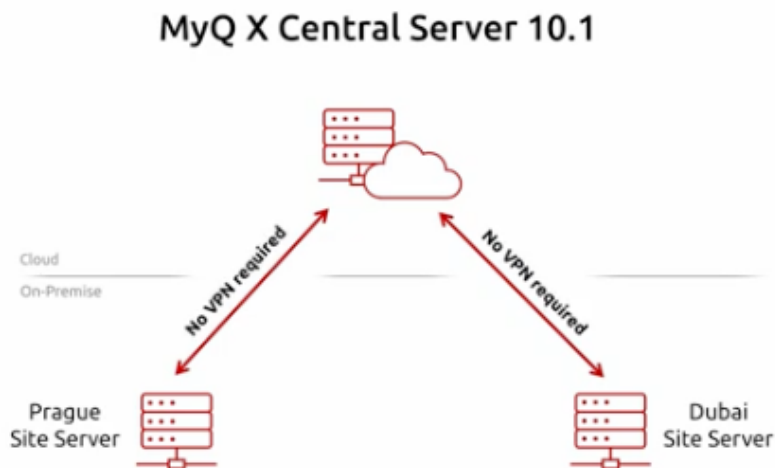
4.2 Installation in Private Cloud

MyQ Central Server can be installed and run, besides on-premise servers, also on an Azure Virtual Machine, with a VPN tunnel connecting the physical network and Azure's virtual network.

4.2.1 Environment Requirements

- The minimum recommended virtual machine is B4ms, with a dedicated (not system disk) standard HDD.
 - The recommended CPU, RAM and HDD resources are the same as a standard installation and can be found in [system requirements](#).
- It is required to open ports used by MyQ or make sure they are not blocked on Azure's Network security group.

✓ Since MyQ Central Server 10.1, communication with Sites does not require a VPN tunnel. Public IP address of the machine running the Central Server can be used.



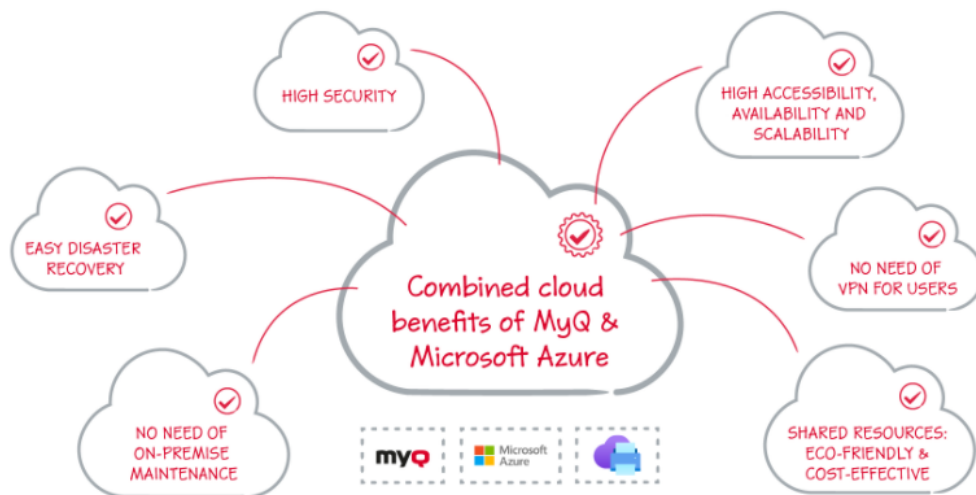
Once you set up the Azure virtual environment, follow the [Installation](#) instructions to install MyQ.

4.2.2 About MyQ in Private Cloud

Customers using Microsoft 365 as a private cloud hosting their internal systems can add MyQ to the list of IT services they no longer need to have installed on an on-premise server.

Part of the leased private cloud space can be dedicated to MyQ server(s), and MyQ running in Azure can make use of [Azure Active Directories](#).

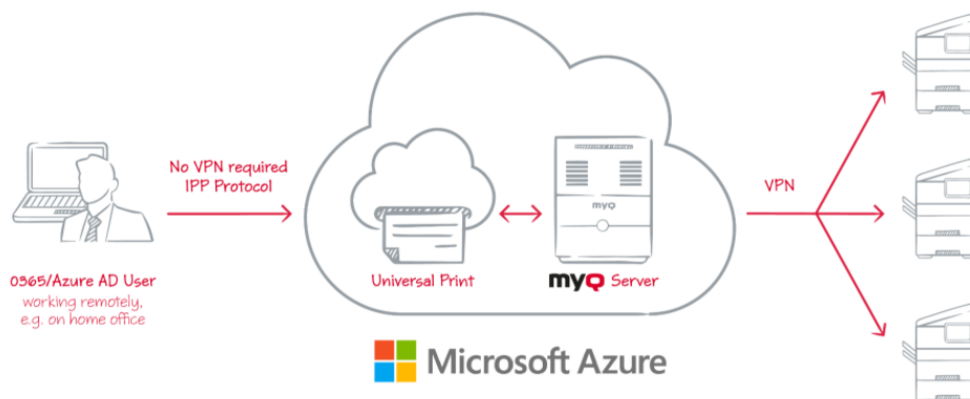
The single sign-on feature already used by users to access applications in the Microsoft cloud can also cover cloud printing with MyQ, without the need to use a VPN connection.



MS Universal Print is also fully integrated in MyQ, offering mobility, quick printer discovery, and no need for a VPN connection.

What is more, MyQ's Universal Print connector can work with older devices, so there's no need to invest into upgrading your fleet with more recent models which would natively support Universal Print.

For more information, see **Microsoft Universal Print** in the [MyQ Print Server guide](#).



- A VPN tunnel connecting the physical network and Azure's virtual network is also required when using Microsoft Universal Print. Thanks to this VPN tunnel, there is no need for a VPN connection from the client's side to the MyQ Server.

4.3 OEM Migration

Since **10.1 Patch 2** it is possible to restore KNM and aQrate databases in the MyQ installation, which allows to migrate all data from a KNM or aQrate installation into the MyQ installation. Other directions of migration are not possible.

4.3.1 Prerequisites

- Backup of a database from the current OEM installation, minimum version 8.2
- Installer of the MyQ Central Server (for multi-site installation, the installer of the MyQ Central Server)
- New MyQ license(s) of your choice to be activated in MyQ once the migration is complete



Contact MyQ Support for more information specific to the migration process of your installation.

4.3.2 Recommended Steps

Before you begin, we recommend you read our [Upgrading MyQ Guide](#).

General

- Use a backup created right before migration to achieve no data loss
- Once the migration process is complete, check the setting of the new MyQ installation – some settings that differ from the MyQ defaults are kept intact; see more information below in the Migration section

Multi-site installations

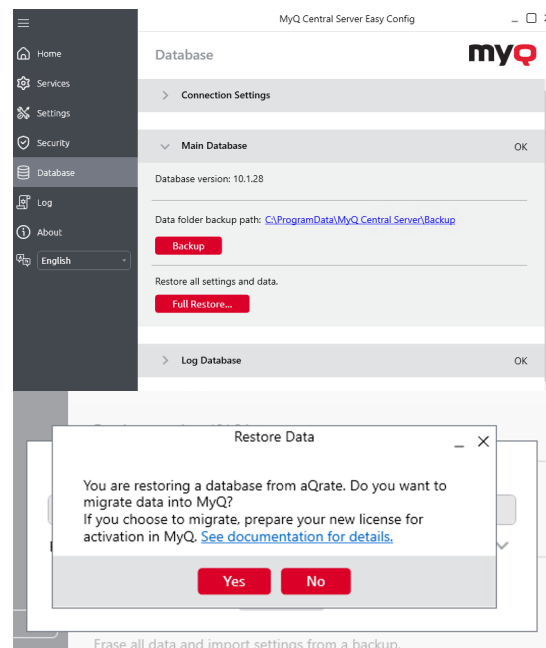
- Start with the Central Server migration and after the migration, insert the new MyQ license you had prepared prior to the migration
- Keep in mind that once the Central Server is migrated, the license recalculations on connected Site servers may end unsuccessfully; this conflict should be resolved by migrating the Site servers as soon as possible

4.3.3 Migrate to MyQ

Migration can be performed with the use of the standard Database Restore option in the Easy Config.

1. Back up the database in your current OEM installation
2. Set up a clean installation of the MyQ Central Server (**10.1 Patch 2** or above)
3. Go to **Easy Config > Database**, and click **Full Restore...**
4. Select the backup of your OEM installation
5. Confirm the migration process

The migration is started – see below for what data is migrated and further manual steps that are recommended before you can start using your MyQ installation.



Migration

Detailed feature specifications can be found in [Print Server](#). It behaves the same on Central Server except that the only settings which are relevant for Central Server are:

- Email templates, fewer than on Print Server;
- SMTP sender email;

4.4 Updating MyQ

- ✓ A comprehensive guide to updating all MyQ components is available [here](#).

The MyQ update to a higher version or reinstalling the same version is performed automatically after running the installation executable file.

Before a MyQ update on Windows Server 2016/2019/2022 (or on Windows 8.1/10/11), make sure that the latest Windows updates are downloaded and installed on the server.

When upgrading or updating MyQ, ensure all antivirus exclusions are made and that there are no running scan operations on the MyQ directories structure.

It is strongly recommend to backup your database before the update.

- ⚠ A direct upgrade to version 10.0 is only possible from version 8.2.

To update MyQ:

1. Run the MyQ software installation executable file. The Select Setup Language dialog box appears.

2. Select your language, and then click **Next**. The Setup dialog box appears. It informs you that there is an older version of MyQ and that the installer will start the update process.
3. Click **Yes**. The License Agreement dialog box appears.
4. Select **I accept the agreement** and click **Next**.
5. In the Ready to Install dialog, click **Install**. The rest of the update process is nearly identical to this of installing MyQ.



In older MyQ versions, it was possible to switch between a Standalone server, a Site server, or a Central server. This is no longer available, as the MyQ Print server and MyQ Central server are different products and use separate installers. If you have such a setup and plan to upgrade it to MyQ Central server 10.0, be advised that the upgrade will not be successful. This kind of upgrade and migration is only available between MyQ Central server 8.1 and MyQ Central server 8.2. Check [here](#) for further details.

5 MyQ Central Server Easy Config

The MyQ Central Easy Config application is the basic environment for setup of the essential parts of the MyQ Central server, such as the MyQ database and log.

It automatically opens during the installation of the server. Otherwise, you can find it on the Apps screen in Windows 8.1+, Windows Server 2016 and newer. After you open the application, you see its menu on the left side of the dialog box. From this menu, you can access the following settings:

- On the **Home** tab, you can quickly change the default passwords for access to the Server Administrator account and the Database Administrator account. You can generate data needed by MyQ Support, and you can also log in to the MyQ Web Administrator Interface from there.
- On the **Services** tab, you can control the run of the MyQ Central server's services.
- On the **Settings** tab, you can change both the Server administrator and the Database administrator passwords, setup the Windows Services account, unlock the Server administrator account, change file paths of the MyQ system data files, change the port of the web server and clean up your Cache and Temp folders.
- On the **Security** tab, you can enable/disable unsecure communication, and manage the MyQ DB, the Log DB, and jobs encryption.
- On the **Database** tab, you can change the type and settings of the MyQ database, and back up and restore your data.
- On the **Log** tab, you can overview all operations executed by the MyQ system.
- On the **About** tab, you can see the information about the current version of the MyQ Central server.

5.1 Home

Once you open the MyQ Easy Config application on the Home tab for the first time, you will be prompted to create a for the Database Administrator account, which is important for database security.

Database Administrator Account

This is the SYSDBA account used for accessing the Firebird database. It is strongly recommended to create a strong and secure password for this account.

The first time you open the application, on the **Home** tab, you can see the **Database Administrator Password** section. To create a password, type the new password, confirm the password, and then click **Save**.

MyQ Central Server Easy Config

Home

myQ

Database Administrator Password

Change the default password

Password:

Confirm password:

Save

MyQ Web Administrator

To setup the server go to the MyQ Web Administrator and login as *admin.

[MyQ Web Administrator](#)

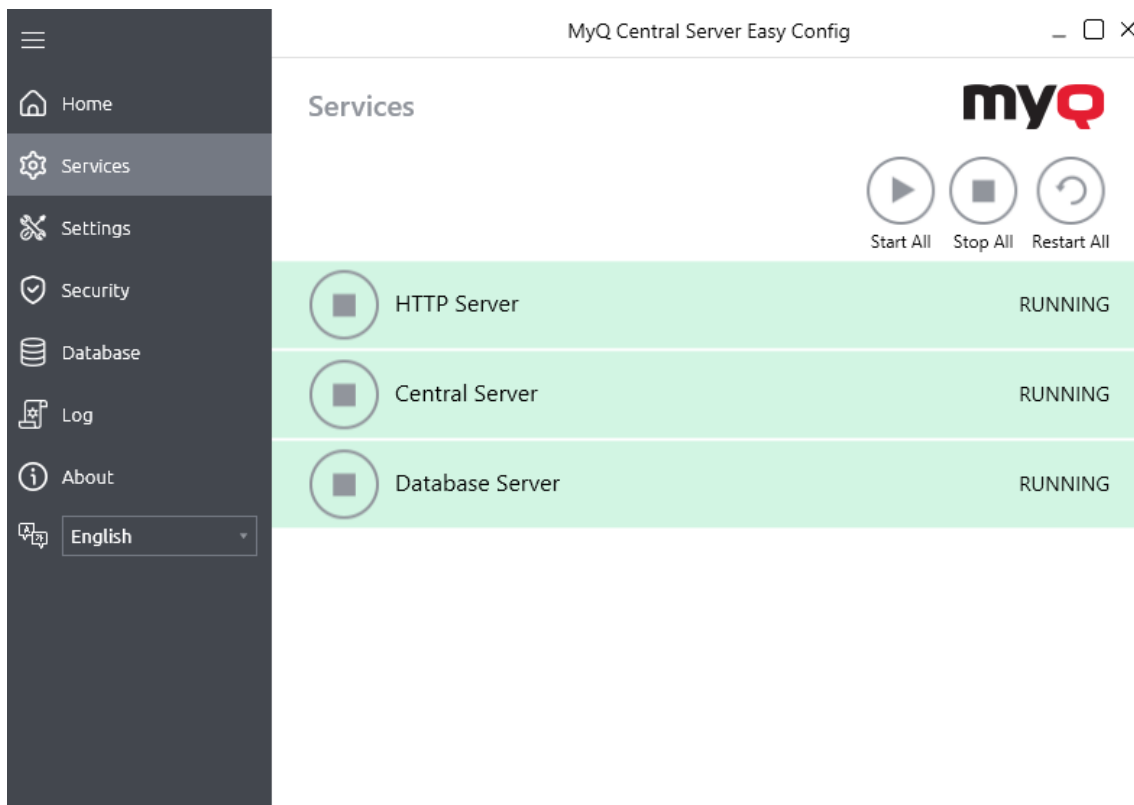
Data for Support

After you create the password, its initial setup section disappears from the **Home** tab.

Additional options are available on the **Home** tab to access the **MyQ Web Administrator** account, and generate **Data for Support**.

5.2 Services

On the **Services** tab you can stop, start, and restart the services of the MyQ Central server.



5.3 Settings

5.3.1 Windows Services Account

MyQ Services run, by default, under the *Local System* account, meaning the account that was used during the installation.

This can be changed in the **Settings** tab, in the **Windows Services Account** section:

- Under *Log on services as*, select **Custom account**.
- Click on **Browse**, select the user account to be used for MyQ services and click **OK**. The selected user account should have "Local administrator" rights or be a member of the Local Administrators Group. It should also already have rights to "Log on as service".
- Type the account's password and then confirm it in the next field.
- Click **Save**. MyQ Services are automatically stopped and restarted.

To change back to the default account, select **Local System account**, and click **Save**. MyQ Services are automatically stopped and restarted.

5.3.2 Web Server Ports

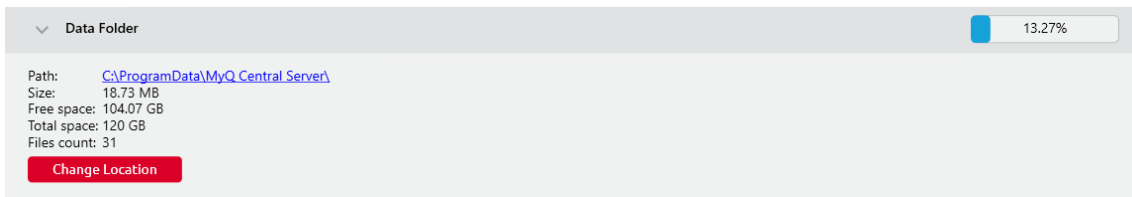
On the **Settings** tab, under **Web Server Ports**, you can change the ports for the connection to the MyQ Web server:

- **Port:** communication port for the MyQ HTTP server; the default value is *8083*.
- **Secure port (SSL):** communication port for the MyQ HTTPS server; the default value is *8093*.

Use the up/down arrows to select the new port, and click **Save** to apply the changes.

5.3.3 Data Folder

On the **Settings** tab, you can see the MyQ database folder location.



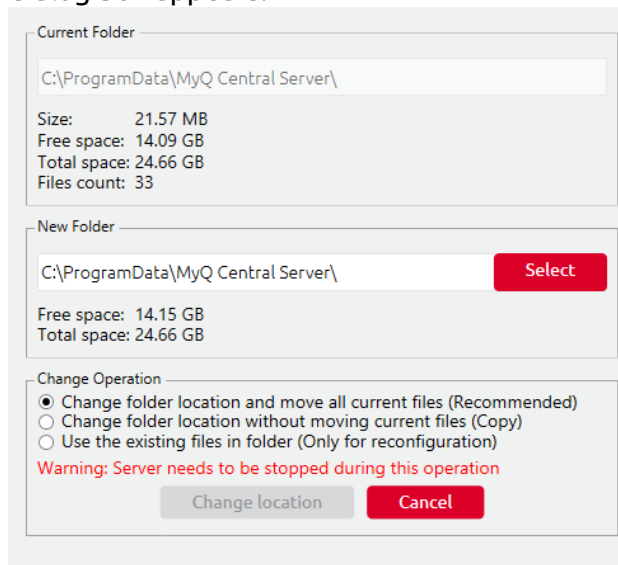
Depending on the type of the database, the Data folder either does, or does not contain the MyQ database: the MyQ Embedded database is part of the folder, whereas the SQL database is stored on the SQL server. Besides the MyQ database, the folder contains additional files with data used by the MyQ system, such as reports, certificates or the *config.ini* file.

The default folder path is:

C:\ProgramData\MyQ Central Server

Under normal circumstances, there is no need to change the location. In case you have to do it, for example when there is not enough space on the system disk, follow the instructions below:

1. On the **Settings** tab, in the respective section, click **Change Location**. The **Change folder location** dialog box appears.



2. In the dialog box, under **New folder**, enter the path to the new folder or click **Select** to browse and find the new folder location.
3. Under **Change Operation**, select the required method of existing data relocation, and then click **Change Location**. The folder is moved to the new location.



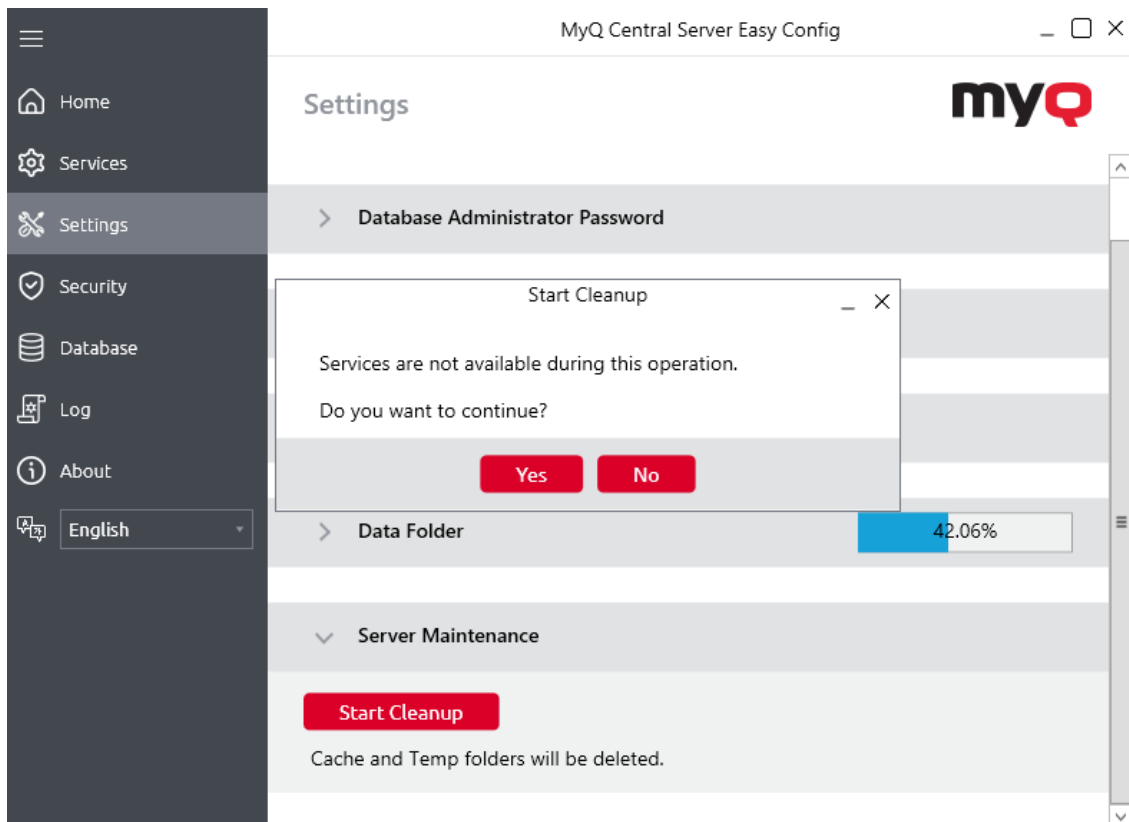
If you relocate your Data folder to a network drive, be aware that Apache or Firebird service cannot access network drives created by the Administrator or other users. The network drive needs to be created by the "**nt authority\system**" user. You can

do this using this guide: <https://stackoverflow.com/questions/182750/map-a-network-drive-to-be-used-by-a-service/4763324#4763324> or it should work when you mount the drive on Windows startup.

5.3.4 Server Maintenance

In the **Server Maintenance** section of the **Settings** tab, you can clean up your Cache and Temp folders. This might be necessary in cases when problems with the temporary files affect the MyQ system.

To delete the two folders, click **Start Cleanup**. A pop-up window informs you that services are not available during the cleanup. Click **Yes** to continue or **No** to cancel.



A busy indicator window lets you follow the cleanup process, and informs you when it ends.

5.4 Security

5.4.1 Changing Passwords on the Security Tab

As soon as you replace the default password, the section disappears from the **Home** tab and the password can no longer be changed there.

Server Administrator Account

This is the **admin* account which is used for the initial MyQ configuration. Once you create a password for this account, you can continue to the MyQ Web Interface, use it for logging in as the administrator, and start configuration. It is generally recommended to later disable this account once you have created dedicated administrator accounts.

Database Administrator Account

This is the *SYSDBA* account used for accessing the Firebird database. It is strongly recommended to create a strong and secure password for this account.



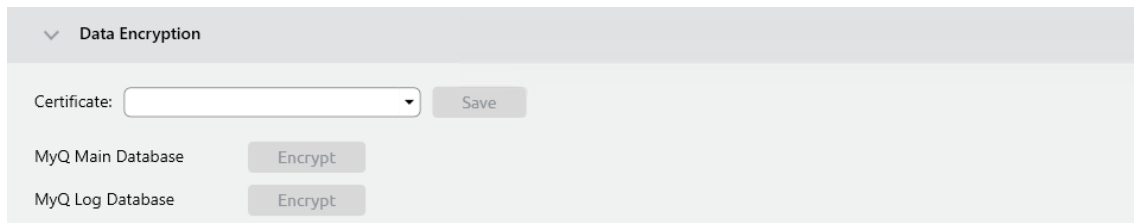
The MyQ database access user name is *SYSDBA* and its default password is *masterkey*.
The Server administrator user name is **admin* and its default password is *1234*.

5.4.2 Unlocking the MyQ Administrator account

After 5 consecutive failed login attempts to the MyQ administrator account, the account is locked.

The admin can see a warning that the *admin account is locked, and unlock it, in the **Server Administrator Account** section on the **Security** tab. Once they click **Unlock**, the account is unlocked.

5.4.3 Data Encryption



The screenshot shows the 'Data Encryption' section of the MyQ Central Server Easy Config interface. At the top, there is a 'Certificate' dropdown menu and a 'Save' button. Below this, there are two rows: 'MyQ Main Database' and 'MyQ Log Database'. Each row has an 'Encrypt' button next to it.

In the **Data Encryption** section, for better security, you can encrypt the main database, the log database, and print jobs using a certificate. MyQ does not provide these certificates. You should install and use your own. The certificate used for the encryption needs to have the “Encrypting File System” Enhanced Key Usage (EKU) and it must be located in one of the following computer certificate stores:

- Personal
- Trusted Publishers
- Third-Party Root Certification Authorities
- Other people

Once installed, it will be visible in the **Certificate** drop-down.

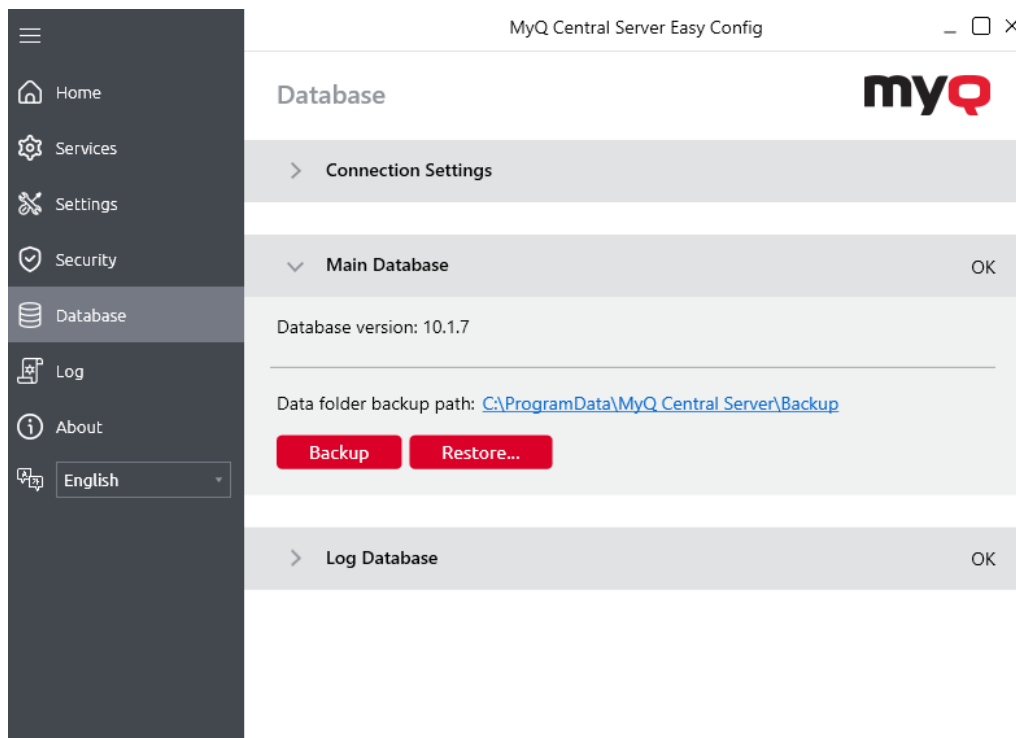
Click **Encrypt** next to **MyQ Main Database**, **MyQ Log Database**, or **Print jobs. Scan Jobs** are encrypted by default.

During the encryption, other services will not be available. A busy indicator will let you follow the encryption/decryption process:

After the encryption, the **Encrypt** button will change to **Decrypt** so you can reverse the action.

5.5 Database

On the **Database** tab, you can change the database connection settings, check the main and log database's status, and perform backup and recovery. You can also see information about the current version of the database, available updates, and also a warning in case there is a need for an upgrade.



5.5.1 Backing up MyQ data

To back up your MyQ data:

1. Open the **Database** tab.
2. In the **Main Database** section, click **Backup**.
3. Provide and confirm a password to protect the backup. If skipped, the backup will be created unprotected.

Backup Data

Provide a password to protect the backup:

•••••

Confirm the password:

•••••

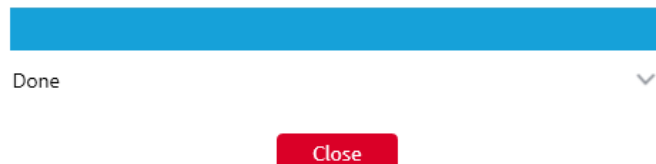
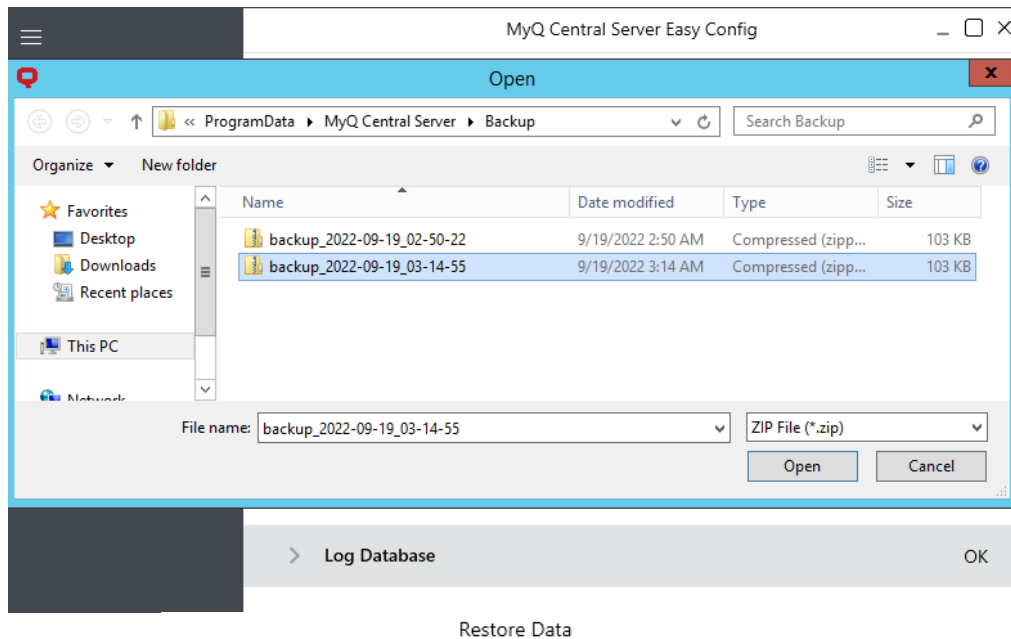
OK Cancel

4. A new backup file is created, called *backup_*.zip*. Depending on the database type, the *backup_*.zip* either does or does not contain the MyQ database file (MyQ.FDB): the MyQ Embedded database is part of the folder, whereas the SQL database is stored on the SQL server. Besides the MyQ database, the folder contains additional files with data used by the MyQ system, such as reports, certificates, the *metadata.backup* file or the *config.ini* file.

5.5.2 Restoring MyQ Data

To restore your MyQ data:

1. Open the **Database** tab.
2. In the **Main Database** section, click **Restore....** Select the *backup_*.zip* file to restore MyQ Data, and click **Open**. If the backup is password protected, there is a prompt to provide the password. The database is restored and, if needed, upgraded as well.



5.5.3 Database Connection Settings

In the Connection Settings section, you can view database information, such as the name, server address, server port, username, and password. If you click **Edit**, you can set up a new MyQ Embedded database or an SQL database. This change is only available if you selected the MyQ Embedded database during the installation.

5.6 Log

The **Log** tab of Easy Config allows you to view all operations being executed by the MyQ system. These can be filtered by **Field**, **Date**, **Type**, and **Subsystem**.

Home

Services

Settings

Security

Database

Log

About

English

Log

Auto-refresh: ☐

All Fields:

From:

To:

Type: ☒ Critical ☒ Error ☒ Warning ☒ Info ☒ Notice ☒ Debug ☒ Trace

Subsystem: ☐ CU ☐ EasyConfig ☐ General ☐ Kyocera Provider ☐ Platform ☐ Plug-in ☐ Replicator ☐ Scheduler ☐ Web Service ☐ WebUI

Unselect All

Apply

MyQ Central Server Easy Config

Log

Filters

Date and time

Subsystem

Context

Text

File

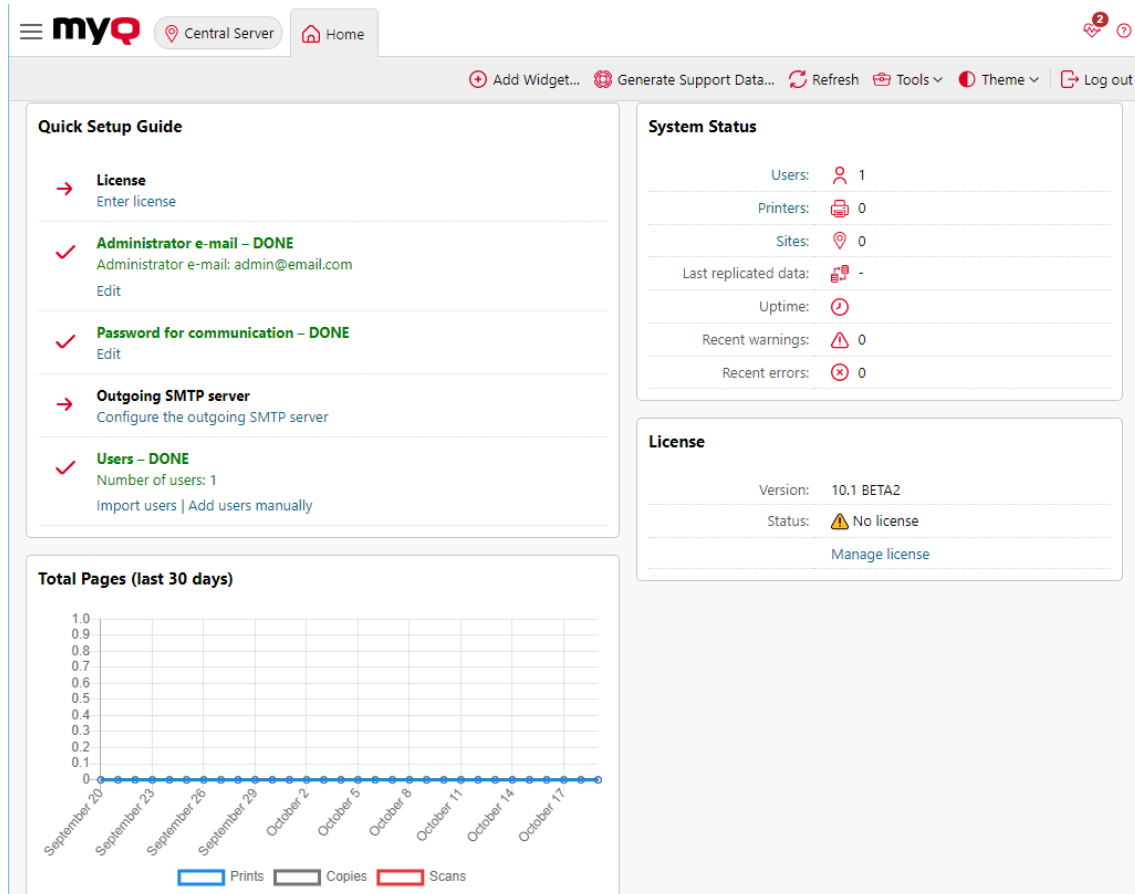
Line

Date and time	Subsystem	Context	Text	File	Line
3/6/2024 12:42:16 PM	Scheduler	Log backup, id=-69	Event raised name=tasks.queueEmpty.DB Mo		0
3/6/2024 12:42:16 PM	Scheduler	Log backup, id=-69	OUT MyQ\Schedule\SchedulerService:runSch	\\WsfPlatform\Plu	81
3/6/2024 12:42:16 PM	Scheduler	Log backup, id=-69	Scheduled task "Log backup" was finished.		0
3/6/2024 12:42:15 PM	EasyConfig	Database back-up	Database 'C:\ProgramData\MyQ Central Server	BackupRestore.cs	191
3/6/2024 12:42:15 PM	CU		OUT Services\EmailHandlerService:runEmailSi	\\WsfPlatform\Plu	81
3/6/2024 12:42:15 PM	CU		IN Services\EmailHandlerService:runEmailSen	\\WsfPlatform\Plu	39
3/6/2024 12:42:14 PM	Scheduler	Log backup, id=-69	Executing scheduled task: Log backup		0
3/6/2024 12:42:14 PM	Scheduler	Log backup, id=-69	IN MyQ\Schedule\SchedulerService:runSchec	\\WsfPlatform\Plu	39
3/6/2024 12:42:14 PM	Scheduler	Database and setting	OUT MyQ\Schedule\SchedulerService:runSch	\\WsfPlatform\Plu	81
3/6/2024 12:42:14 PM	Scheduler	Database and setting	Scheduled task "Database and settings backup		0
3/6/2024 12:42:14 PM	EasyConfig	Database back-up	Database 'C:\ProgramData\MyQ Central Server	BackupRestore.cs	191
3/6/2024 12:42:12 PM	Scheduler	Database and setting	Executing scheduled task: Database and setting		0
3/6/2024 12:42:12 PM	Scheduler	Database and setting	IN MyQ\Schedule\SchedulerService:runSchec	\\WsfPlatform\Plu	39
3/6/2024 12:42:12 PM	Scheduler	System maintenance	OUT MyQ\Schedule\SchedulerService:runSch	\\WsfPlatform\Plu	81
3/6/2024 12:42:12 PM	Scheduler	System maintenance	Scheduled task "System maintenance" was fini		0
3/6/2024 12:42:11 PM	Scheduler	System Health Check	OUT MyQ\Schedule\SchedulerService:runSch	\\WsfPlatform\Plu	81
3/6/2024 12:42:11 PM	Scheduler	System Health Check	System Health Check found issues which need		0
3/6/2024 12:42:11 PM	Platform	127.0.0.1:49808	OUT EventDispatcher:raiseEvent 6ms	\\WsfPlatform\Plu	81
3/6/2024 12:42:11 PM	Platform	127.0.0.1:49808	OUT Services\MessageSourceService:conEvent	\\WsfPlatform\Plu	81
3/6/2024 12:42:11 PM	Platform	127.0.0.1:49814	OUT Messages:send 0ms	\\WsfPlatform\Plu	81
3/6/2024 12:42:11 PM	Platform	127.0.0.1:49814	IN Messages:send	\\WsfPlatform\Plu	39
3/6/2024 12:42:11 PM	Platform	127.0.0.1:49808	IN Services\MessageSourceService:conEvent	\\WsfPlatform\Plu	39
3/6/2024 12:42:11 PM	Platform	127.0.0.1:49808	Event raised name=ServerHealth.changed		0
3/6/2024 12:42:11 PM	Platform	127.0.0.1:49808	IN EventDispatcher:raiseEvent	\\WsfPlatform\Plu	39
3/6/2024 12:42:11 PM	Scheduler	System health check	Default password is used for the Administrator		0
3/6/2024 12:42:11 PM	Scheduler	System health check	Default password is used for accessing the dat		0
3/6/2024 12:42:11 PM	Platform	127.0.0.1:49808	OUT Platform:getServicesByInterface 0ms	\\WsfPlatform\Plu	81
3/6/2024 12:42:11 PM	Platform	127.0.0.1:49808	IN Platform:getServicesByInterface	\\WsfPlatform\Plu	39
3/6/2024 12:42:11 PM	Platform	127.0.0.1:49808	OUT EasyConfigService:runHealthChecks 20	\\WsfPlatform\Plu	81
3/6/2024 12:42:11 PM	Platform	127.0.0.1:49808	IN EasyConfigService:runHealthChecks	\\WsfPlatform\Plu	36
3/6/2024 12:42:11 PM	Scheduler	Data replication from	Event raised name=tasks.queueEmpty.Replica		0
3/6/2024 12:42:11 PM	Scheduler	Data replication from	OUT MyQ\Schedule\SchedulerService:runSch	\\WsfPlatform\Plu	81

83

6 MyQ Central Web Interface

This topic describes the MyQ Central Web Interface where you manage most of MyQ functions. It shows you how to access the web interface and the two menus where you can access all settings and functions on the web interface: the **Main** menu, and the **Settings** menu. Furthermore, it describes the web interface's **Home** dashboard and shows you how to perform the initial MyQ setup. The last two sections introduce two MyQ logs: the **MyQ Log** and the **MyQ Audit Log**.



6.1 Accessing the MyQ Central Web Interface

To access the MyQ Central Web Interface, you need to open it in your web browser and log in as an administrator:

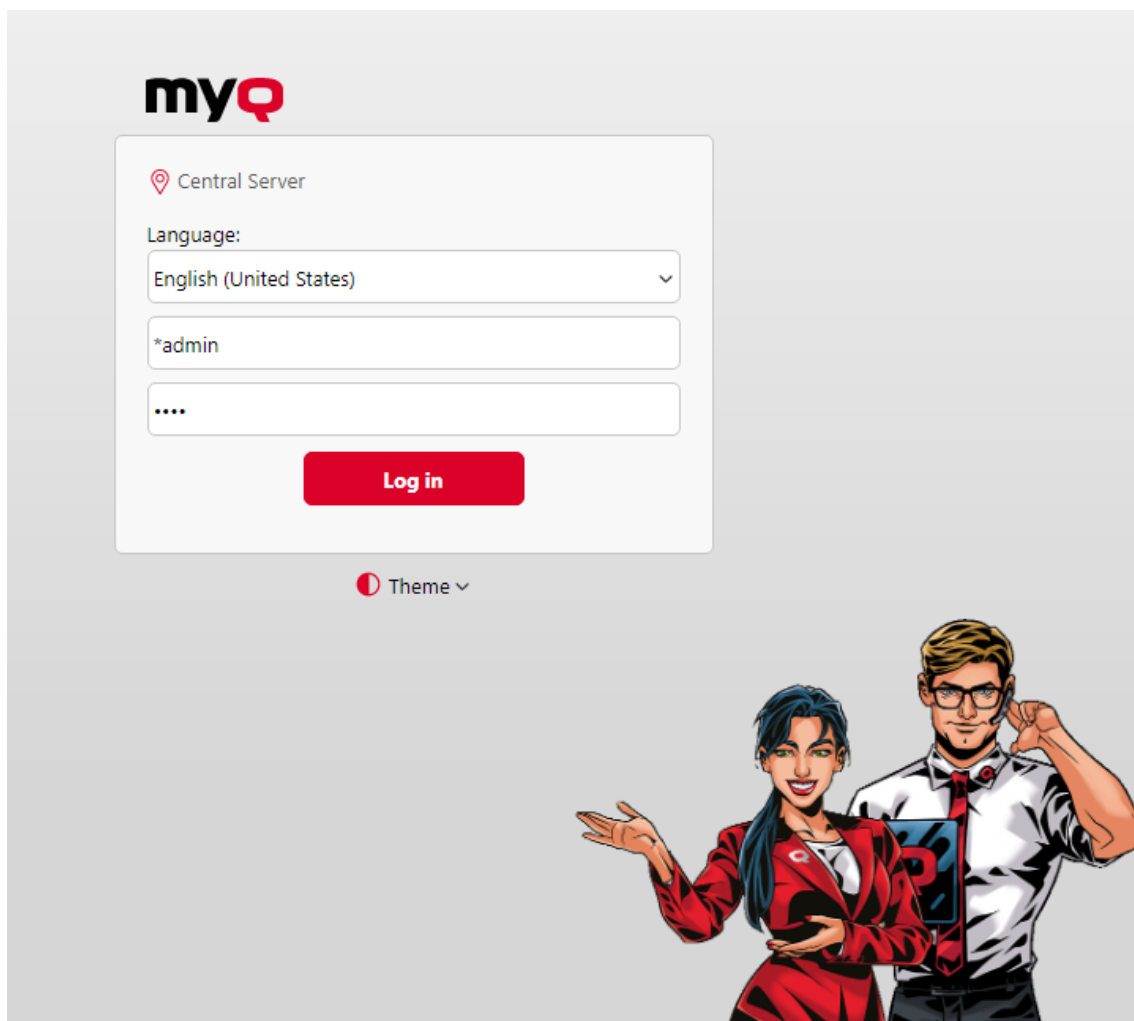
There are three ways to open the MyQ Central Web Interface:

1. Open your web browser, and then enter the web address in the form: `https://*MyQCentralserver*:8093`, where *MyQCentralserver* represents the IP address or the host name of your MyQ Central server, and *8093* is the default port for access to the server.

2. Log on to the interface from the MyQ Central Easy Config application, by clicking the *MyQ Web Administrator* link on the **Home** tab, in the **MyQ Web Administrator** section.
3. Open the MyQ Central Web Administrator application. You can find this application on the Apps screen in Windows 8.1+, Windows Server 2016 and newer.

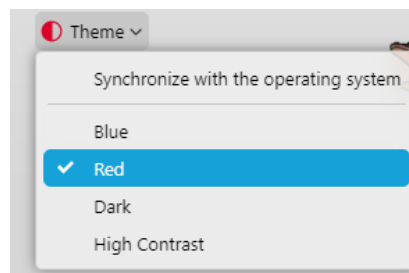
6.2 Logging in as an administrator

Enter the MyQ administrator name (**admin*) and the password that you have set in the MyQ Central Easy Config application, and then click **Log In**. If you have not changed the default password yet (not recommended), enter the default one: *1234*.



In the drop-down at the top of the login window, you can select your preferred language.

Before logging in, you can click **Theme** to choose the theme for the interface. The options are: *Synchronize with the operating system*, *Blue*, *Red (default)*, *Dark*, *High Contrast*.



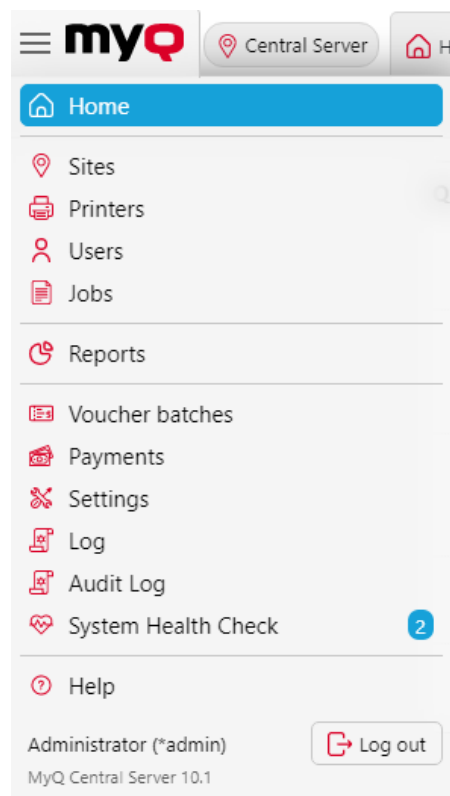
6.3 Main Menu and Settings Menu

There are two menus where you can access all the features and settings of the MyQ Central server: the **Main** (MyQ) menu and the **Settings** menu.

In this guide, all the tabs accessed from the Main menu, except for the **Home** screen and **Settings** menu, are called main tabs, as opposed to settings tabs that are accessed from the **Settings** menu.

Main menu

To open the **Main** menu, click the MyQ logo at the upper-left corner of the screen. From there, you can access the **Home dashboard**, the **Settings** menu, and a number of tabs where you can manage and use MyQ functions.



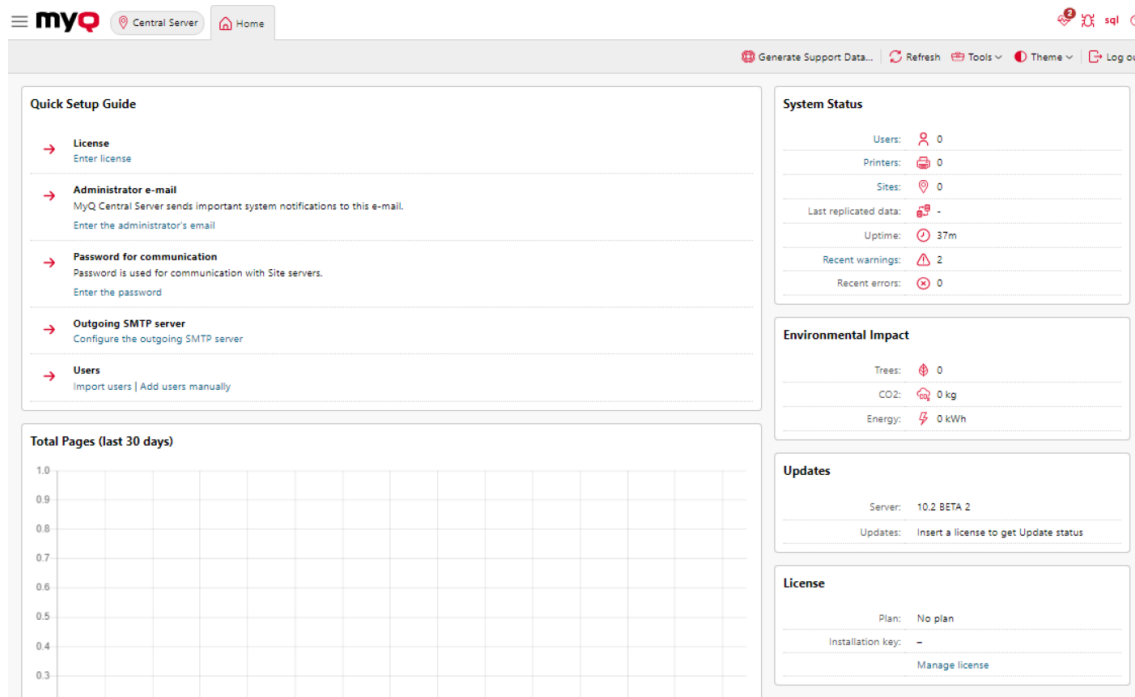
Settings menu

To open the **Settings** menu, click **Settings** on the **Main** menu.

The tabs that are accessed from the **Settings** menu serve for the global setup of the MyQ Central server.

6.4 Home Dashboard

On the **Home** dashboard, you can perform the initial MyQ setup. After the setup, you can use the dashboard to directly access MyQ key features, to display statistics and to generate data for support.



The dashboard is fully adjustable; it consists of multiple building blocks (widgets) that can be added and removed from the screen. You can use the blocks to customize both the layout and functionality of the dashboard.

By default, there are six widgets on the dashboard: **Quick Setup Guide**, **System Status**, **Environmental Impact**, **Total Pages (last 30 days)**, **Updates**, and **License**.

The **Quick Setup Guide** walks you through the initial MyQ setup.

In the **System Status** widget, you can see the following system status information:

Name	Description
Users	Number of active users. Clicking opens the Users page overview.

Name	Description
Printers	Number of printers where the status is not: Local, replicated or deleted. Cached every 15 seconds. Clicking opens the Printers page.
Sites	Number of active MyQ Site servers. Clicking opens the Sites page.
Last replicated data	Shows when data were last replicated.
Uptime	MyQ system uptime, in hours.
Recent warnings	Number of warning log messages over the last 24 hours. Cached every 60 seconds.
Recent errors	Number of error and critical log messages over the last 24 hours. Cached every 60 seconds.

The **Environmental Impact** widget shows your environmental impact in Trees, CO₂, and Energy.

1 tree = 8333 pages / 1 page = 12.7g of CO₂ / 1 page = 48Wh of energy / 1 recycled page = 32Wh of energy

In the **Total Pages (last 30 days)** widget, you can see a graph of the prints, copies, and scans in the last 30 days.

The **Updates** widget shows available updates for the MyQ installation and its components (terminal packages). To get the updates status, a valid license needs to be added to MyQ. Once a license is added, the MyQ administrator (or a user with the Manage settings rights) may see the following:

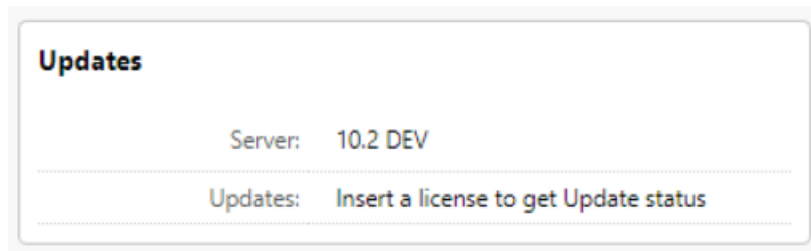
- **LATEST** - the currently installed version is the latest one
- **UPDATE AVAILABLE** - there is a newer version in this branch
 - e.g. *MyQ 10.1 patch 1* will show that *MyQ 10.1 patch 2* is available
 - e.g. *10.2 BETA* will show that *10.2 BETA 2* is available
 - e.g. *Terminal 8.2 patch 23* will show the latest patch released for that 8.2 Terminal
- **DEPRECATED** - this version is not being updated anymore, an upgrade path is recommended

- Shown currently only for Server components - Print and Central Server, not Terminal Packages.

In the event that a license has been installed, the update information may not be immediately downloaded and displayed in the widget. If there is no information about updates, the **"Check now"** button is displayed in the widget. The administrator can manually initiate the retrieval of update information using this button.

The **"Check now"** button is only displayed if a license is installed. Without a license, the widget displays the message *"Insert a license to get Update status"*.

If the server is offline or there are any errors, a warning is displayed on the widget.

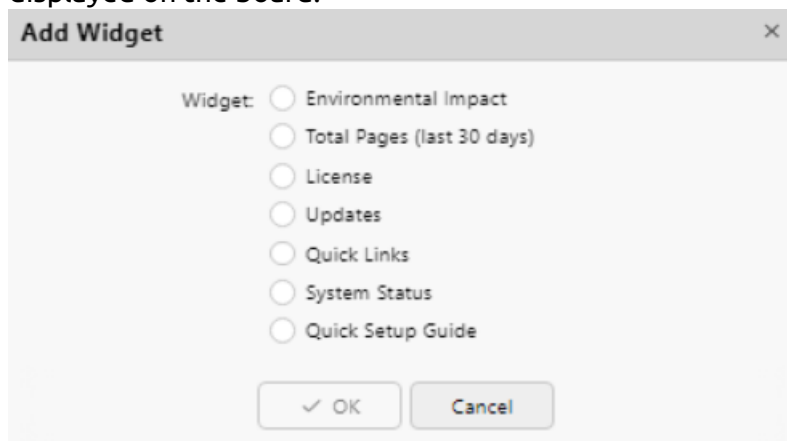


The **License** widget shows license information and can redirect you to the [License](#) settings tab.

Adding new widgets and moving widgets on the dashboard

To add a new widget:

1. Click **Tools** and then **Add Widget** at the top-right corner of the dashboard. The Add Widget pop-up window appears.
2. In the pop-up, select the widget, and then click **OK**. The new widget is displayed on the board.



To move widgets, drag and drop them on the board.

To delete widgets, click on the three dots at the top-right corner of the widget, and click **Remove**.

Select **Default layout** in the **Tools** menu, to restore the dashboard to its default layout.

Changing the theme

To change the MyQ Web Administrator's interface theme, click on **Theme** at the top-right corner of the dashboard. The available options are:

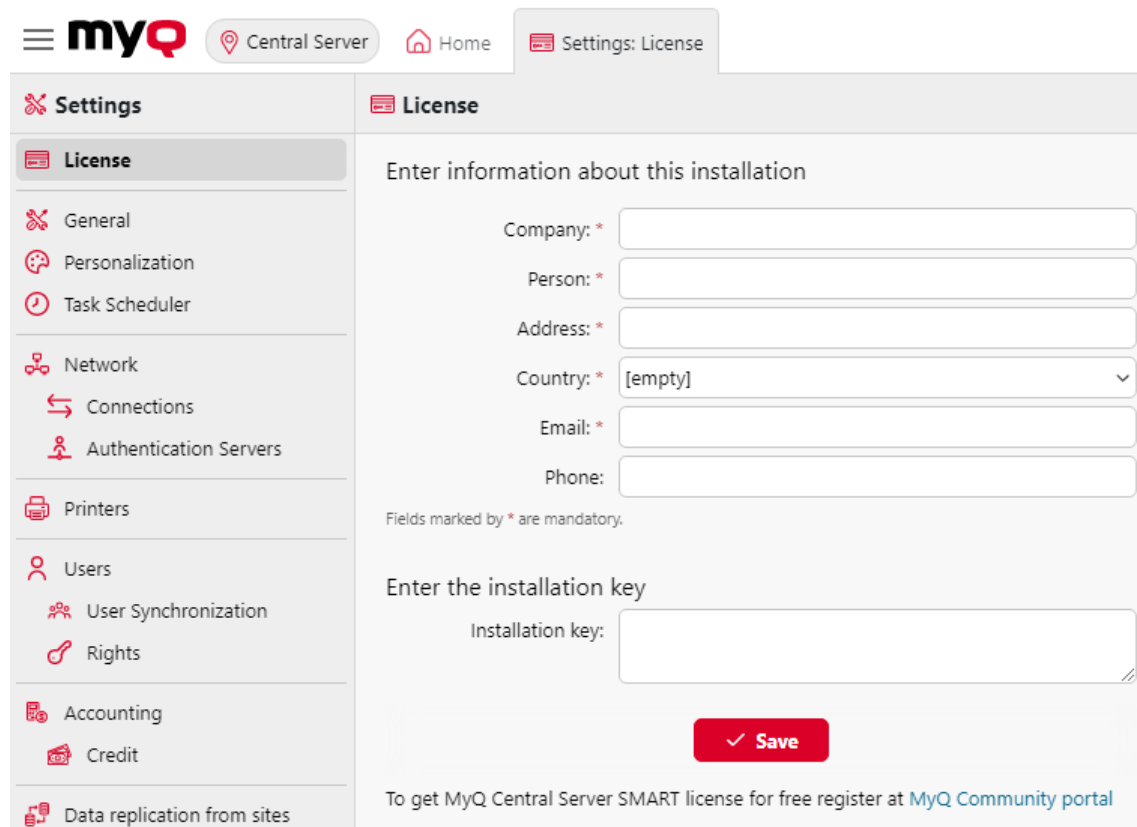
- Synchronize with the operating system
- Blue
- Red (default)
- Dark
- High Contrast

6.4.1 Quick Setup Guide

On the **Quick Setup Guide** widget, you can set the basic and most important features of the MyQ system:

License

Click **Enter License**. The **License** settings tab opens. You are asked to enter information about your installation and enter your installation key.



The screenshot shows the MyQ Central Web Interface. At the top, there is a navigation bar with the MyQ logo, a 'Central Server' button, a 'Home' button, and a 'Settings: License' button. Below this is a sidebar with a 'Settings' header and a list of settings categories: License, General, Personalization, Task Scheduler, Network, Connections, Authentication Servers, Printers, Users, User Synchronization, Rights, Accounting, Credit, and Data replication from sites. The main content area is titled 'License' and contains the following fields:

Enter information about this installation

Company: *

Person: *

Address: *

Country: *

Email: *

Phone:

Fields marked by * are mandatory.

Enter the installation key

Installation key:

To get MyQ Central Server SMART license for free register at [MyQ Community portal](#)

Administrator email

By clicking **Enter the administrator's email**, you open the **General** settings tab, where you can set the administrator email. Important system messages (disk space checker warnings, license expiration etc.) are automatically sent to this email.

Password for communication

To communicate with your site servers you must set a password. By clicking **Enter the password**, you open the **General** settings tab, where you can set the password for network communication, in the **Security** section.

Outgoing SMTP server

By clicking **Configure the outgoing SMTP server**, you open the **Network** settings tab, where you can set the outgoing SMTP server.

Users

- By clicking **Add users manually**, you open the **Users** main tab, where you can manually add users.
- By clicking **Import users**, you open the **User Synchronization** settings tab, where you can import users from LDAP servers, an MS Azure source or from a CSV file.

6.4.2 Generate Data for Support

In case you encounter a problem that requires help from the MyQ support team, you may be asked to provide more information about your MyQ system configuration, licenses, printer devices, terminals, etc. In such case, you need to generate a *MyQ-helpdesk.zip* file, which contains multiple files with all the necessary information, and send it to the MyQ support team.

The *.zip* file contains:

- the Logs folder with error logs from Apache and PHP,
- the MyQ log file *log_dateandtime.xlsx*,
- the Windows Event log,
- the *statsData.xml* file,
- and the *MyQ-helpdesk.xml* file with MyQ system information.

The MyQ log file corresponds to the MyQ log that can be displayed on the MyQ Central Web Interface or in the MyQ Central Easy Config application, and contains attachments with detailed information.

To generate the *MyQ-helpdesk.zip* file:

1. Click **Generate Support Data** on the bar at the top of the **Home** dashboard. The Generate Support Data dialog box appears.
2. In the dialog box, specify the **Day** and the exact **Time** span of the MyQ events to include in the *MyQ-helpdesk* file, and then click **Export**. The file is generated and saved to your *Downloads* folder.

Generate Support Data

Day: * 09/19/2022
mm/dd/yyyy

Time from: * 03:08 AM till: * 04:08 AM

✓ Export Cancel

Fields marked by * are mandatory.

You can also generate data for support in the MyQ Central Easy Config application. In the **Home** tab, under the **Data for Support** section, set the **Date** and **Time** for the data, and click **Generate**. The file is generated and you can select where to save it.

MyQ Central Server Easy Config

Home

Database Administrator Password

Server Administrator Account

MyQ Web Administrator

Data for Support

Day: 9/19/2022

Time: 2:54 AM - 3:54 AM

Generate

6.5 MyQ Log

In the MyQ Central server log, you can find information about all parts of the MyQ Central server: the MyQ Central server, MyQ Central Web UI, etc. Log messages are sorted into these types *Critical*, *Error*, *Warning*, *Info*, *Notice*, *Debug*, *Trace* and you can select the types that you want to be displayed.

You can also set the log to display only messages informing about specific MyQ subsystems, such as the Web UI, remote printer setup, user sessions on MyQ terminals, and also about a specific context, for example, direct printing or a specific printing device.

The log is updated in real time, but you can pause it by clicking **Watch live**, and filtering to show messages from a specific time period, such as yesterday, this week, last week, last X hours, last X weeks, etc.

The screenshot shows the MyQ Log interface. On the left is a sidebar with a search icon and filters: 'All Records', 'Errors', 'Errors and Warnings', 'My Searches', 'Admin Search', and 'Maintenance'. The main area displays a table of log records. The table has columns: Time, Type, Subsystem, Context, and Text. The records show various log messages, including 'Checking new direct print jobs', 'Event raised | name=tasks.queueEmpty.platform', 'OUT | PhpDaemon::recycle | 0ms', and 'IN | PhpDaemon::recycle'. At the bottom, there is a pagination bar with 'Count: Count it', 'Page: 1', and 'Items per page: 100'.

6.5.1 Opening the MyQ Log

On the MyQ Web User Interface, go to **MyQ, Log**, or on the **Home** dashboard, click **Log** on the **Quick links** widget.

6.5.2 Pausing/Refreshing the log

To pause or resume the real time run of the log, click **Watch live** on the bar at the top of the **Log** tab. To refresh the log to the current moment, click **Refresh** on the same bar.

6.5.3 Filtering the log: selecting time period, verbosity of information, subsystem or context

You can filter the log on the panel:

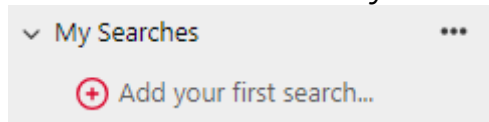
- After you pause the log, you can select the period in the **Date** combo box.
- In the **Verbosity** field you can select the type of log entries you want to view (*Critical, Info, Error*, etc.).
- In the **Subsystem** combo box, you can select/type one or more subsystems to be displayed in the log.
- In the **Context** text box, you can type the context you want to view.

After the filters are set, click **Search** to submit them.

6.5.4 My Searches

You can use **My Searches** to save filters and common searches for future use. Saved searches can be shared and organized into folders. It is also possible to share an entire folder of saved searches. To create a saved search:

1. Click **Add your first search** or use the context menu and select **Add search** (if saved searches have already been created).

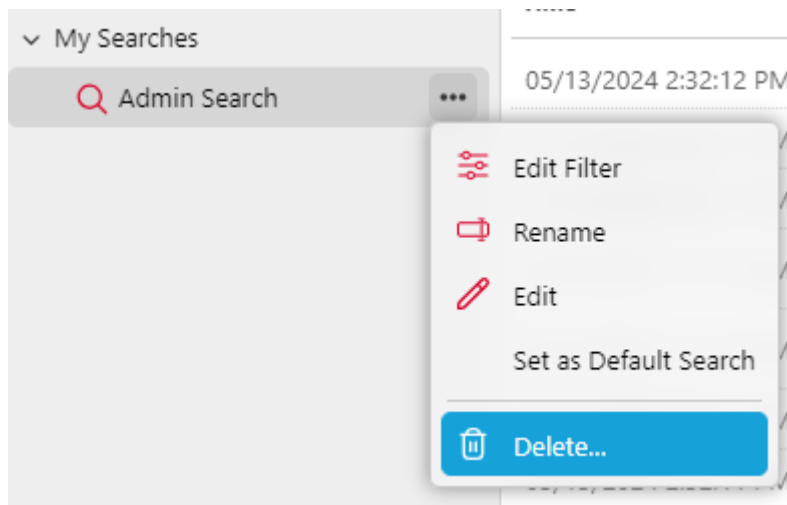


2. Enter a name for your search and edit the search filters as required, particular filters can be turned on or off using the + icon.

 A screenshot of the 'admin search' form. At the top, there's a search bar with 'admin search' and a dropdown arrow. To the right are 'Search' and 'Watch Live' buttons. Below the search bar are five filter fields: 'Full-text search:', 'Date:', 'Verbosity:', 'Subsystem:', and 'Context:'. Each field has a dropdown arrow. To the right of these fields is a '+' icon and a 'Search' button. Below the filters is a table with columns: 'Time', 'Type', 'Subsystem', 'Context', 'A...', and 'Text'. The table contains six rows of search results. A context menu is open over the 'Search' button, showing options: 'Context', 'Date', 'Full-text search', 'Subsystem', and 'Verbosity'.

Time	Type	Subsystem	Context	A...	Text
10/02/2024 10:16:19 AM	Trace	General	OUT Services\SitesStatusC		80ms
10/02/2024 10:16:19 AM	Trace	General	IN Services\SitesStatusCh		
10/02/2024 10:15:49 AM	Trace	General	OUT Services\SitesStatusC		19ms
10/02/2024 10:15:49 AM	Trace	General	IN Services\SitesStatusCh		
10/02/2024 10:15:42 AM	Trace	CLI	OUT Services\EmailHandlerService::runEmailSender		49ms
10/02/2024 10:15:42 AM	Trace	CLI	IN Services\EmailHandlerService::runEmailSender		

Once a search has been created the following options are available using the context menu next to the search name:

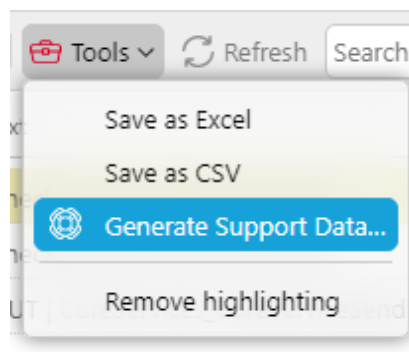


- **Edit Filter:** displays the filter editor for the search.
- **Rename:** allows the user to rename the search.
- **Edit:** opens advanced properties in the right panel including sharing options.
- **Set as Default Search:** sets the search as the default one.
- **Delete:** deletes the search.

6.5.5 Exporting the log/Generating support data

Click **Tools** on the bar at the top of the **Log** tab, and then select one of the following export options:

- **Save as Excel** — export the log as an Excel file.
- **Save as CSV** — export the log as a CSV file.
- **Generate Support Data** — generates a .zip file with multiple files for MyQ support.



When the log is filtered, the Generate Support Data option reflects the date selected in the filter, the end date is pre-filled automatically based on the maximum amount of data for export.

6.5.6 Highlighting log messages

You can highlight particular log messages. To do so, select the message that you want to highlight and then press the **SHIFT + SPACE** keyboard shortcut.

Time	Type	Subsystem	Context	A...	Text
09/13/2022 4:41:14 AM	Debug	Direct Print			Checking new direct print jobs
09/13/2022 4:41:11 AM	Debug	Direct Print			Checking new direct print jobs
09/13/2022 4:41:08 AM	Debug	Direct Print			Checking new direct print jobs
09/13/2022 4:41:05 AM	Debug	Direct Print			Checking new direct print jobs
09/13/2022 4:41:02 AM	Debug	Direct Print			Checking new direct print jobs
09/13/2022 4:40:59 AM	Debug	Direct Print			Checking new direct print jobs

To remove all highlights, click **Tools** on the bar at the top of the **Log** tab, and then click **Remove highlighting**.

6.6 MyQ Audit Log

In the **MyQ Audit Log**, you can view all the changes of MyQ settings, along with information about who made the changes, the time when they were made and which subsystem of MyQ was affected by them.

The screenshot shows the MyQ Central Web Interface with the **Audit Log** tab selected. On the left, there are filters for Date, User, and Type, with a **Search** button. The main area displays a table of audit events. The table has columns for Time, Type, Description, Context, User, and Subsystem. The events listed are:

Time	Type	Description	Context	User	Subsystem
09/19/2022 11:50:...	Settings were changed.		System		CLI
09/19/2022 11:50:...	Group All users was edited.		System		CLI
09/19/2022 4:08:4...	Settings were changed.		Administrator • "admin"		WebUI
09/19/2022 3:58:1...	Settings were changed.		Administrator • "admin"		WebUI

6.6.1 Opening the MyQ Audit Log

On the MyQ Web User Interface, click **MyQ**, and then click **Audit Log**. Example of the types of actions you can see in the **Audit Log**:

The screenshot shows the MyQ Central Web Interface with the **Audit Log** tab selected. On the left, there are filters for Date, User, and Type, with a **Search** button. The main area displays a table of audit events. The events listed are:

Time	Type	Description	Context	User	Subsystem
11/20/2024 10:22:06 AM	'Smith' user's rights were edited		Administrator • "admin"		Web Service
11/20/2024 10:19:45 AM	'Smith' user's rights were edited		Administrator • "admin"		Web Service
11/20/2024 10:19:33 AM	'Smith' user's rights were edited		Administrator • "admin"		Web Service
11/20/2024 10:19:10 AM	Card/PIN "****" was added to user 'Smith'	Smith	Administrator • "admin"		Web Service
11/20/2024 10:19:10 AM	User 'John' was created		Administrator • "admin"		Web Service
11/20/2024 10:10:07 AM	Settings were changed		Administrator • "admin"		CLI
11/20/2024 10:10:07 AM	Group 'All users' was edited		System		CLI

For actions related to user rights, you can open the log entry to see the details of the change.

Audit Log: 11/20/2024 10:22:06 AM
×

Description: 'Smith' user's rights were edited

ID: 143

Time: 11/20/2024 10:22:06 AM

User: Administrator • *admin

Subsystem: Web Service

Changes

Name	New value
Manage vouchers	Revoked
Read Jobs	Revoked

6.6.2 Filtering the Audit Log: selecting time period, user and type of event

The displayed data can be filtered by a time period, the user who made the changes and the type of the event.

To display additional information about a particular change, double-click the change. A panel with the detailed information opens on the right side of the **Audit Log** tab.

6.6.3 Exporting the Audit Log

You can export the **Audit Log** by clicking **Tools** and selecting **Export**. The log is instantly generated and downloaded.

You can also select **Schedule Export** to have the log regularly exported. The schedule's properties panel open to the right, where you can set its parameters.

 **Audit Log Export** ×

General Filters and parameters Rights

Enabled: * ☒

Name: *

Description:

▼ Schedule

Repetition: *

Day: * ☒ Monday
☐ Tuesday
☐ Wednesday
☐ Thursday
☐ Friday
☐ Saturday
☐ Sunday

Hours of run: *
hh:mm, hh, h:mm, hh am, hh p
For multiple values, separate with a comma or semicolon

> Notification

> Report

☒ **Save**

7 MyQ Central System Settings

This topic discusses basic system settings of the MyQ system. The settings are located on separate tabs, accessed from the Settings menu:

- On the [General](#) settings tab, you can set the administrator email, change regional settings, and other general settings.
- On the [Personalization](#) settings tab, you can add custom help links and custom logos to be used in various parts of the MyQ system.
- On the [Network](#) settings tab, you can modify network settings such as certificates, server ports, etc.
- On the [Authentication servers](#) settings tab, you can add LDAP and Radius servers for user authentication.
- On the [Printers](#) settings tab, you can set the duration of the temporary cards validity in hours.
- On the [Task scheduler](#) settings tab, you can add new task schedules, change their settings and run scheduled tasks.
- On the [Log & Audit](#) settings tab, you can set the Log notifier feature, which enables sending notifications about selected log events to the administrator and/or any number of MyQ users.
- On the [System management](#) settings tab, you can change settings of the MyQ history, set the maximum size of files that can be uploaded on the MyQ Web Interface, delete data from the MyQ database, and also reset MyQ components to apply settings previously made on other tabs.

7.1 General Settings

The **General** settings tab contains the **General**, **Security**, and **Job Privacy** sections.

myQ Central Server Home Settings: General

Settings

- License
- General**
- Personalization
- Task Scheduler
- Network
- Connections
- Authentication Servers
- Printers
- Users
- User Synchronization
- Rights
- Accounting
- Credit
- Data replication from sites
- Reports
- External Reports
- REST API Apps
- Log & Audit
- System Management

General

General

Administrator e-mail: *
 MyQ Central Server sends important system notifications to this e-mail

Time zone: Los Angeles (UTC-07:00 DST) ▼

Default language: * English (United Kingdom) ▼
 Default language is used 1) when user has no language set 2) for naming built-in users, groups, queues and other objects 3) for default text of e-mail notifications

Currency:
 3-letter currency code

Number of digits after the decimal point: * 5

Column delimiter in CSV: * ; ▼

Security

Password for communication: *
 Password is used for communication with Site servers.

Job Privacy

Job privacy feature limits access to sensitive job metadata for everyone but job owner and his/her delegates.
WARNING: Once enabled it cannot be disabled again!

Fields marked by * are mandatory.

In the **General** section, you can set the administrator email, time zone, default language, currency, and the column delimiter in CSV files.

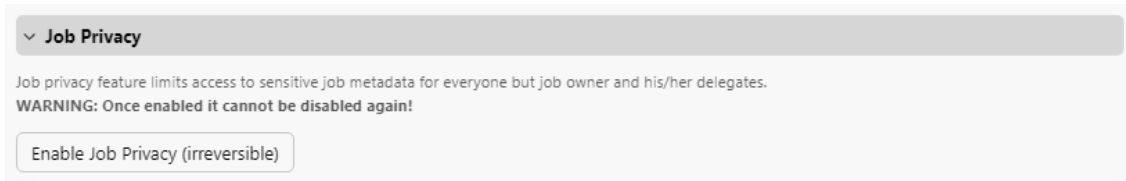
- **Administrator email:** The administrator email receives important system messages (disk space checker warnings, license expiration, etc.) automatically sent from MyQ.
- **Time zone:** For the proper functioning of the MyQ system, make sure that the time zone set here is the same as the time zone set in the Windows operating system. After changing the time zone, you will be asked to restart the web server.
- **Default Language:** The default language setting determines the language of all emails that are automatically sent from MyQ and the language used on all connected terminals and interactive readers.
- **Currency:** In the currency setting, you can enter the 3-letter currency code of the currency that you want to use in your pricelist.
 - The **Number of digits after the decimal point** option can be set from 0 to 5 (default is 2).
- **Column delimiter in CSV:** The column delimiter in CSV files setting determines the delimiter in source and destination files used for all the import and export operations to and from the CSV file format. The default value is based on the regional settings of your operating system.

In the **Security** section, you can set the **Password for communication** between the MyQ Central server and Site servers. The same password has to be set on your Site servers to ensure the communication between your Central server and Site servers.

In the **Job Privacy** section, you can enable the **Job privacy** feature. The Job privacy feature limits access to sensitive job metadata for everyone, except for the job owner and their delegates. If **Job Privacy** is enabled at your Central server, it will be automatically enabled on all the connected site servers.

 Once enabled, it cannot be disabled again!

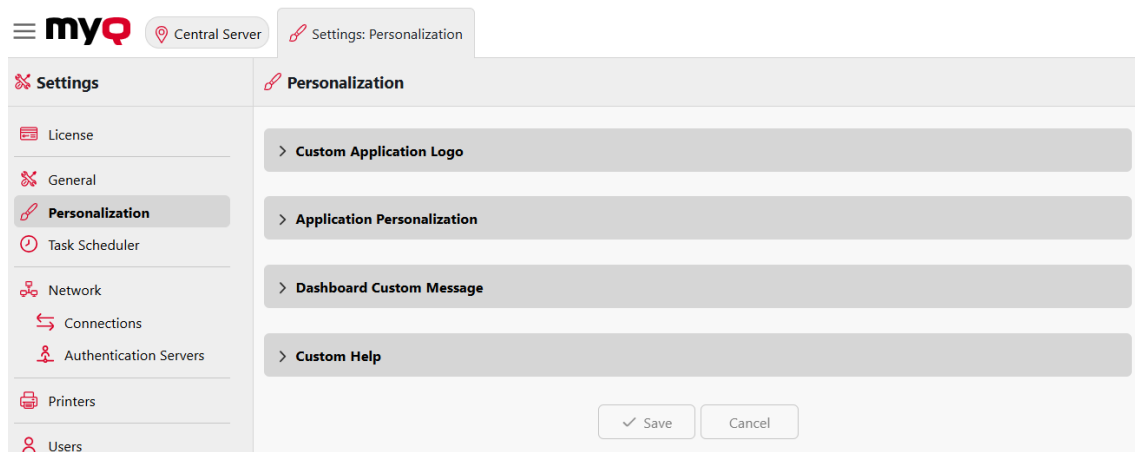
To use the feature, click on the **Enable Job Privacy (irreversible)** button.



In the confirmation pop-up, type your Server administrator password in the **Password** field, and click **Enable Job Privacy (irreversible)**.

7.2 Personalization Settings

On this tab, you can set a custom message to be shown on the Web accounts of MyQ users, add links to your own custom help, and custom application logos to be used in MyQ.



Custom application logo

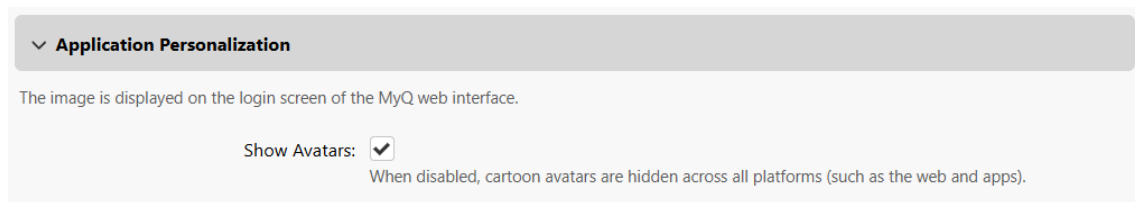
Here you can add your company's logo to be used in the MyQ system. The logo will appear on the upper right corner of the MyQ Web Interface, on MyQ credit vouchers, and on reports.

Supported picture formats are *JPG/JPEG/PNG/BMP* and the minimum size is *398px x 92px*.

To import a custom logo, click the **Custom Logo** field to browse your files, use the drop-down arrow and select **Paste** to select a file from your clipboard, or drag and drop a file onto the field, then select **Save** to save your changes. A preview of the new logo is displayed on the tab.

7.2.1 Application Personalization

Here you can enable or disable the MyQ branding avatars that are generally shown on login screens. Disabling this option will disable these avatars across all platforms (Desktop Clients, mobile application, etc.).



Dashboard custom message

Here you can enter a message to be displayed on the MyQ users web accounts. After you change the message, click **Save** at the bottom of the **Personalization** settings tab.

The `%admin%` parameter can be used to display the email address of the MyQ administrator within the message (the Administrator email set on the [General settings](#) tab).

Custom help

Here you can add a link to your own web based help that will be displayed as a widget on the user's MyQ home page.

To add a custom help link, enter the title and the link of your custom help, and then click **Save** at the bottom of the tab.

7.3 Task Scheduler Settings

The **Task Scheduler** settings tab serves as an interface for planning regular tasks in MyQ. There are seven predefined tasks:

System health check, History deletion, Data replication from sites, System maintenance, Database and settings backup, Log backup, and User Synchronization.

Apart from these, you can import projects from CSV files, and execute external commands.

Settings	Task Scheduler						
- Server Type - License - General - Personalization Task Scheduler - Network	Status	Name	Action	Period	Last run	Last run res...	Next run
	● Disabled	User Synchronization	User Synchronization	Daily	Never	Never	-
	○ Disabled	Printer Discovery	Printer Discovery	Daily	Never	Never	-
	● Ready	System Health Check	System Health Check	Minute	09/02/2025 3:07:00 PM	Finished	09/02/2025 3:12:00 PM
	● Ready	Database and settings backup	Backup	Daily	Never	Never	09/03/2025 2:45:00 AM
	● Ready	Log backup	Backup	Daily	Never	Never	09/03/2025 3:00:00 AM

7.3.1 Running and setting task schedules

To manually run a task schedule:

- Select the task schedule that you want to run.
- Click **Run** on the **Task Scheduler** toolbar.

Or

- Right-click the task schedule.
- Click **Run** on the shortcut menu.

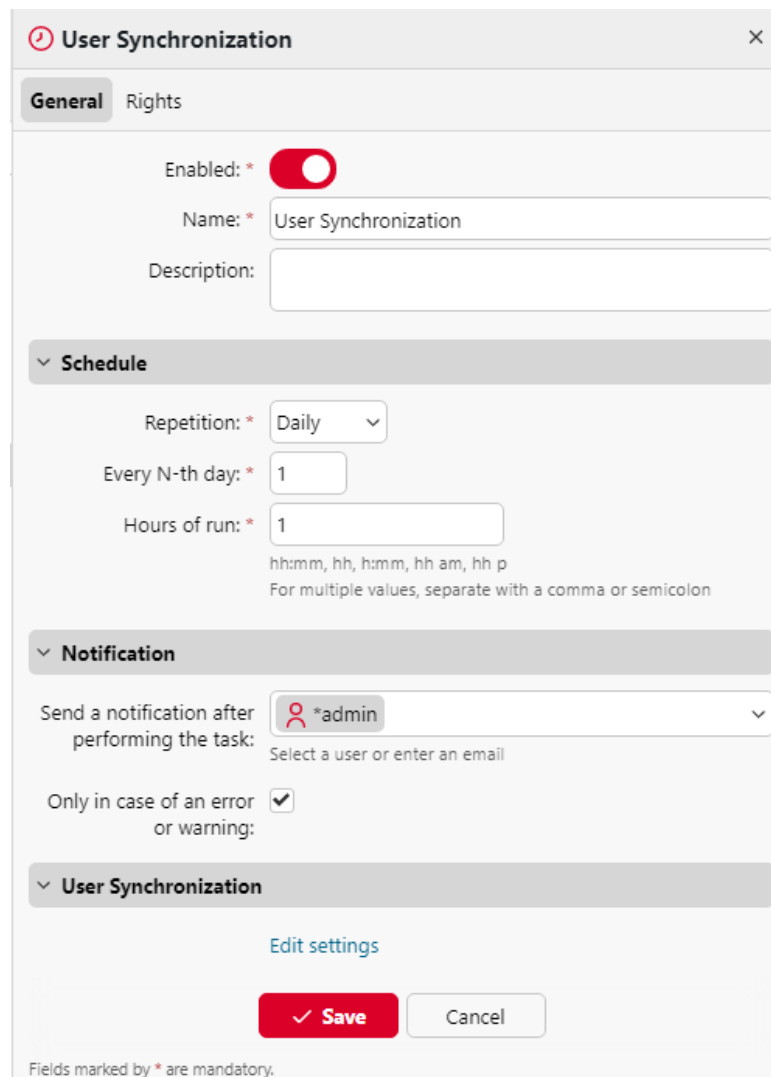
To set a task schedule:

Double-click the task schedule that you want to set (Or right-click it, and then click **Edit** in the actions shortcut menu). The respective task schedule properties panel opens on the right side of the screen.

The task schedule properties panel is divided into four sections:

- In the uppermost section, you can enable or disable the schedule, enter its **Name** and write its **Description**.
- In the **Schedule** section, you must set a period of **Repetition** for the task run and change the exact time of the task run start.
- In the **Notification** section, you can select to send an email notification. You must also choose if you want to send the notification every time or just in case of an error.
- The bottom section, if present, is particular to the type of task.

After you set the schedule, click **Save**.



User Synchronization [Close]

General Rights

Enabled: * ☒

Name: *

Description:

Schedule

Repetition: *

Every N-th day: *

Hours of run: *

hh:mm, hh, h:mm, hh am, hh p
For multiple values, separate with a comma or semicolon

Notification

Send a notification after performing the task:

Select a user or enter an email

Only in case of an error or warning: ☒

User Synchronization

[Edit settings](#)

Fields marked by * are mandatory.

7.3.2 Providing rights for task schedules

You can provide users with rights to change some task schedules settings themselves.

To provide users with rights to change settings of a task schedule:

1. Double-click the schedule that you want to set. The respective schedule properties panel opens on the right side of the screen.
2. On the bar on the upper-left corner of the panel, click **Rights**. The **Rights** tab opens.
3. Click **+Add user**. The Select user or group dialog box appears.
4. Select the user or the group of users that you want to provide with the rights, and then click **OK**.

Adding a new schedule:

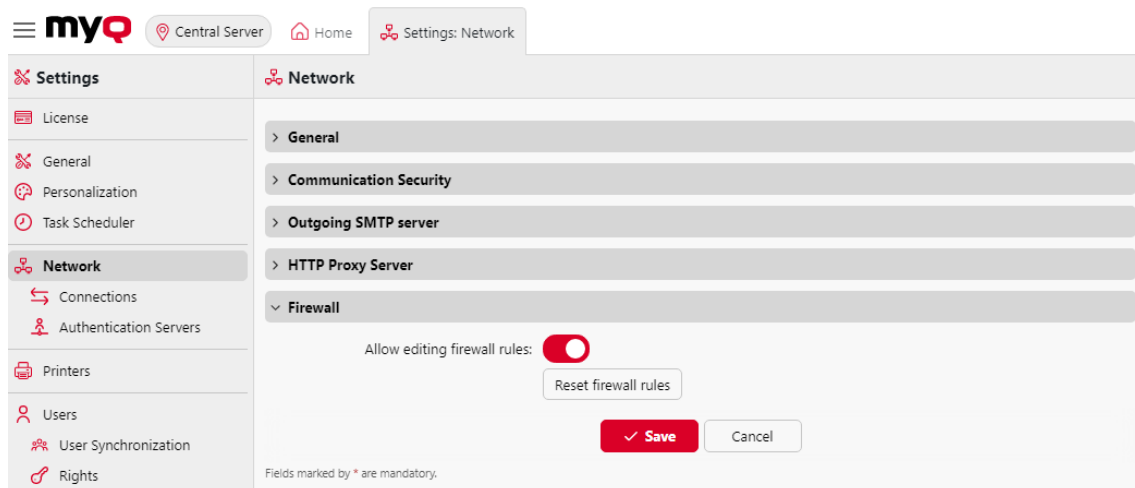
You can add two kinds of new schedules, related to reports: **Users export** and **Printers export**.

On the main ribbon, click **Add** and select **Users export** or **Printers export**. The task schedule properties panel opens on the right side of the screen and it is divided into four sections like the rest of the schedules. The last section, **Report**, is present only on these two schedules and contains the following settings:

- **Format** - Select the report's format from the list: *CSV, XLSX, ODS, XML*.
- **Language** - Select the report's language from the list.
- **All sites must be replicated** - If enabled, all sites are replicated and included in the report.
- **Send via email**
 - **Recipient** - Select the recipient from the list of users.
 - **Subject** - Type a subject for the email.
 - **Message** - Type the body of the email.
 - **Embed the report in the email body** - If enabled, the report is included in the email body.
 - **Maximum email size** - Set the maximum email size from 0 to 2047 MB. If the email exceeds the set size, a secure link to the document is included instead.
- **Save to a file**
 - **File** - Set the path where the file is stored. The default path is `%app%\Data\Export\Users_%datetime%.csv` where `%app%` is the MyQ Data folder and `%datetime%` is the current date and time.

7.4 Network Settings

On the **Network** settings tab, you can manage the network communication between the MyQ Central server and other parts of the MyQ solution. It is divided into the following sections: **General**, **Communication Security**, **Outgoing SMTP server**, **HTTP Proxy server**, and **Firewall**.



7.4.1 General

In this section, you can enter the hostname of the MyQ Central server. This hostname is used by external components of the MyQ system, such as the MyQ Replicator or Site servers, for communication with the MyQ Central server.

7.4.2 Communication Security

In this section, you can choose how your security certificates are managed.

MyQ offers three different certificate management modes:

1. **Built-in Certificate Authority** - This is the default mode for new installations. MyQ creates a self-signed CA certificate and uses it to sign server and client certificates. The public key of the CA certificate can be exported (click the **Export CA certificate** button) to install it to clients, so they trust MyQ server. It is possible to specify the **Subject Alternative Name (SAN)**, which is set as a comma separated list of domain names and/or IP addresses. In case the certificate is compromised, click the **Generate new CA certificate** button, to generate a new one.
2. **Company Certificate Authority** - Your company CA generates an intermediate CA certificate which MyQ uses to sign certificates for the server and clients. To generate an intermediate CA certificate click **Create CSR** to create a Certificate Signing Request (CSR), sign it by your CA and click **Finish CSR** to finish CSR by importing signed certificate. If the intermediate CA certificate does not contain a CA root certificate in its chain, the administrator is prompted to upload the public key of the CA root certificate as well (the **Import CA root certificate** button appears).
3. **Manual Certificate Management** - Provide a certificate for the MyQ Server. MyQ creates no certificates; all certificates are managed by you. Click **Import Server certificate** to upload it. The certificate can be uploaded in *PEM* (public + private key separately) or in *PFX* format. The *PFX* format may be password encrypted. This mode is recommended only for expert users.

Communication Security

MyQ Central Server secures communication with certificates which is an industry standard. Choose how certificates are managed.

Certificate authority mode: *

☒ **Built-in Certificate Authority**
Server and clients are secured by certificates generated by the built-in certificate authority (CA). The CA certificate is self-signed. Export the CA certificate and install it to clients so they trust MyQ Central Server. If the CA certificate is compromised, generate a new one. Server certificate will be regenerated automatically.

Generate new CA certificate
Export CA certificate

☐ **Company Certificate Authority**
Your company CA generates an intermediate CA certificate which MyQ Central Server uses to sign certificates for the server and clients. To generate an intermediate CA certificate create Certificate Signing Request (CSR), sign it by your CA and finish CSR by importing signed certificate. Server certificate will be regenerated automatically.

☐ **Manual Certificate Management**
Provide a certificate for the MyQ Central Server. MyQ Central Server creates no certificates, all certificates are managed by you.

Server alternative names:

Comma separated list of DNS names and/or IP addresses. To set new Subject Alternative Name (SAN) for MyQ Central Server generate new Server certificate. Server hostname is included automatically.

Generate new Server certificate

When upgrading an existing MyQ installation, the **Certificate Authority mode** is selected according to the existing server certificate:

- if the certificate is not CA, then the mode is set to **Manual Certificate Management**.
- if it was generated by MyQ before, then the mode is set to **Built-in Certificate Authority**.
- in other cases, the mode is set to **Company Certificate Authority**.

7.4.3 Outgoing SMTP server

To send email reports, send error messages to users, send automatically generated PIN to users, and forward scanned documents, you have to configure the email server where all the emails are forwarded to.

To configure the server, do the following:

Select a **Type** from *Classic SMTP Server*, *Microsoft Exchange Online* or *Gmail*.

For *Classic SMTP Server*:

1. Enter the server hostname or IP address in the **Server** text box. If the email server listens to other than the 25 TCP port, change the **Port** setting to the correct value.
2. Choose between the *Prefer StartTLS (default)*, *Implicit TLS*, and *Require StartTLS Security* options.
3. Optionally choose to **Validate certificate** or not.
4. If credentials are required, enter the **User** and **Password**.

5. Enter the address that you want to be displayed as the **Sender email** on PIN, alert and report messages.
6. After you enter the data, you can click **Test** to test the connection to the email server, and click **Save** to save your changes.

For *Microsoft Exchange Online*:

1. If you have already set up a Microsoft Exchange Online server in the **Connections** settings, the server is available in the **Connections** field drop-down. If not, you can click on the **Connections** field and then click **Add new** to add your Microsoft Exchange Online server connection. For more information, check [Microsoft Exchange Online Setup](#).

The screenshot shows the 'Outgoing SMTP Server' configuration form. Under the 'Type' section, 'Microsoft Exchange Online' is selected with a radio button. The 'Connections' field is a dropdown menu with 'Microsoft Exchange Online' selected. The 'User' field has a red plus icon and the text 'Add new...'. The 'Sender email' field is empty. A 'Test' button is at the bottom.

2. If credentials are required, enter the **User**.
3. Enter the address that you want to be displayed as the **Sender email** on PIN, alert and report messages.
4. After you enter the data, you can click **Test** to test the connection to the email server, and click **Save** to save your changes.

For *Gmail*:

1. If you have already set up a Gmail server in the **Connections** settings, the server is available in the **Connections** field drop-down. If not, you can click on the **Connections** field and then click **Add new** to add your Gmail server connection. For more information, check [Gmail with OAuth2 Setup](#).

The screenshot shows the 'Outgoing SMTP Server' configuration form. Under the 'Type' section, 'Gmail' is selected with a radio button. The 'Connections' field is a dropdown menu with 'Gmail' selected. The 'User' field has a red plus icon and the text 'Add new...'. The 'Sender email' field is empty. A 'Test' button is at the bottom.

2. If credentials are required, enter the **User**.
3. Enter the address that you want to be displayed as the **Sender email** on PIN, alert and report messages.
4. After you enter the data, you can click **Test** to test the connection to the email server, and click **Save** to save your changes.

7.4.4 HTTP Proxy Server

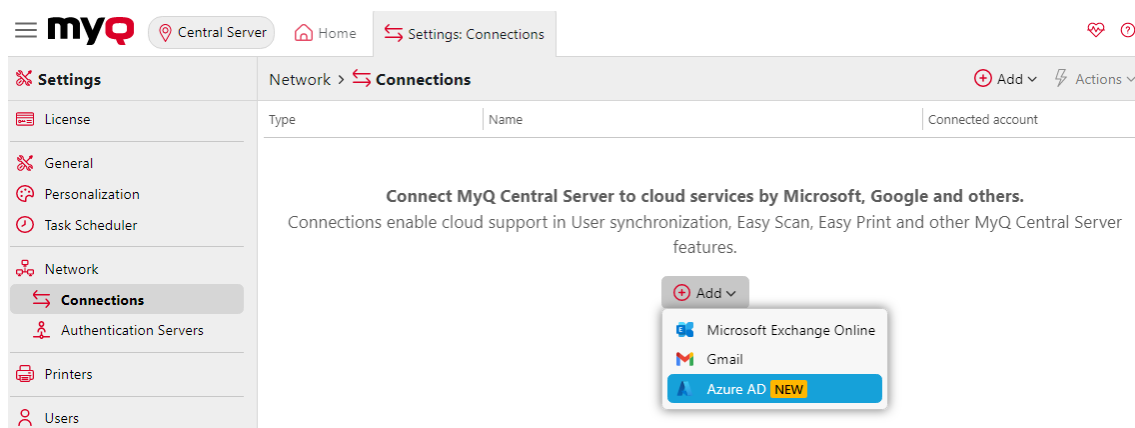
In this section, you can set up a MyQ Proxy server which can be used for activating a license. Mandatory fields are **Server** (name) and **Port**. After changing ports, restart all MyQ services.

7.4.5 Firewall

In this section, you can **Allow editing firewall rules** of the Microsoft Windows Firewall and you can also **Reset firewall rules**.

7.5 Connections Settings

On the **Connections** settings tab, you can connect MyQ to external cloud services.



Click **Add** and select one of the following available services:

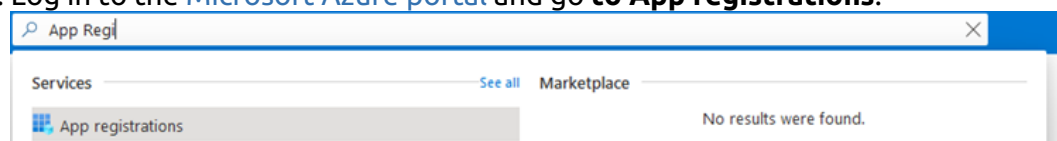
- Microsoft Exchange Online
- Gmail
- Entra ID (formerly Azure AD)

7.5.1 Microsoft Exchange Online Setup

It is first needed to set up Microsoft Exchange Online in Microsoft Azure, and then configure it in MyQ.

Microsoft Exchange Online setup in Microsoft Azure

1. Log in to the [Microsoft Azure portal](#) and go to **App registrations**.



2. Create a **New registration:****App registrations**

[+ New registration](#) [🌐 Endpoints](#) [🔧 Troubleshooting](#) [⬇ Download \(Preview\)](#) | [💙 Got feedback?](#)

3. Create an Azure application:

- Name** - The name for this application (this can be changed later). For example, *MS Exchange Online*. It is important to use the same name as the one used in MyQ under Connections.
- Supported account types** - Who can use this application or access this API? Select the *Accounts in this organizational directory only ({Tenant name} only - Single tenant)* option. Multitenant application can also be used if required, depending on the target audience of the application (what account will be used for authorization in MyQ).
- Redirect URI (optional)** - The authentication response is returned to this URL after successfully authenticating the user. Select the *Public client/native (mobile&desktop)* option from the drop-down and fill in <https://login.microsoftonline.com/common/oauth2/nativeclient> as the redirect URI.
- Click **Register**.

Register an application ...

* Name

The user-facing display name for this application (this can be changed later).

MS Exchange Online ✓

Supported account types

Who can use this application or access this API?

- ☐ Accounts in this organizational directory only (_____ only - Single tenant)
- ☒ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Public client/native (mobile ... ✓

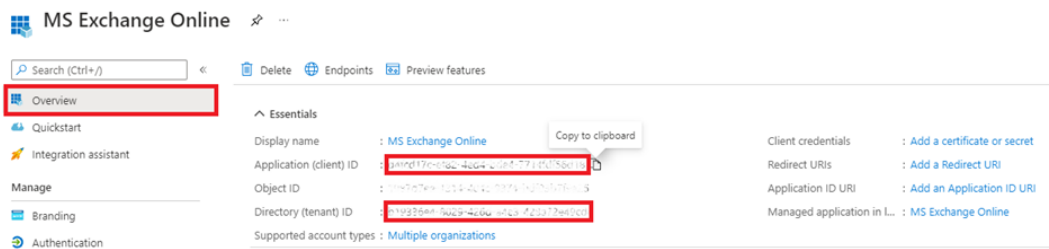
<https://login.microsoftonline.com/common/oauth2/nativeclient> ✓

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

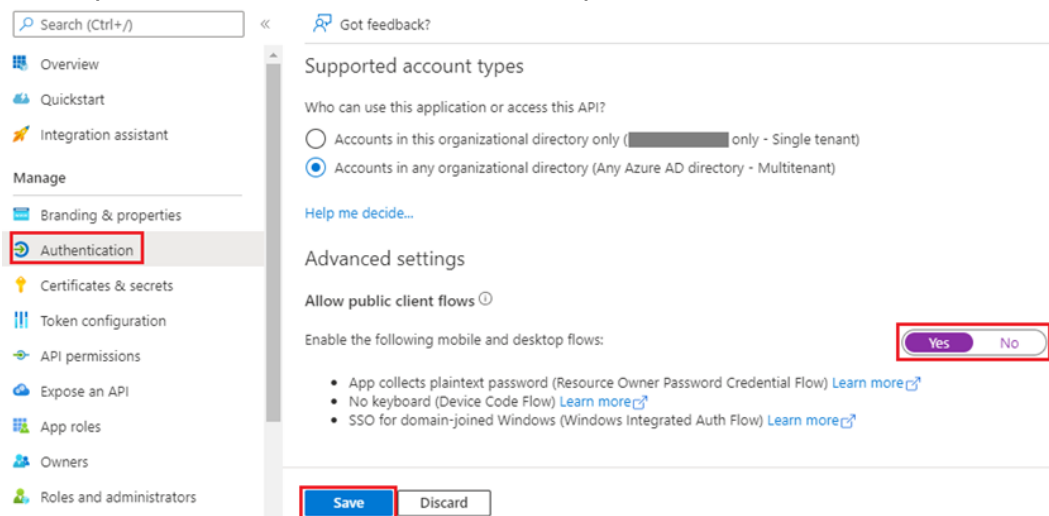
By proceeding, you agree to the [Microsoft Platform Policies](#) 

Register

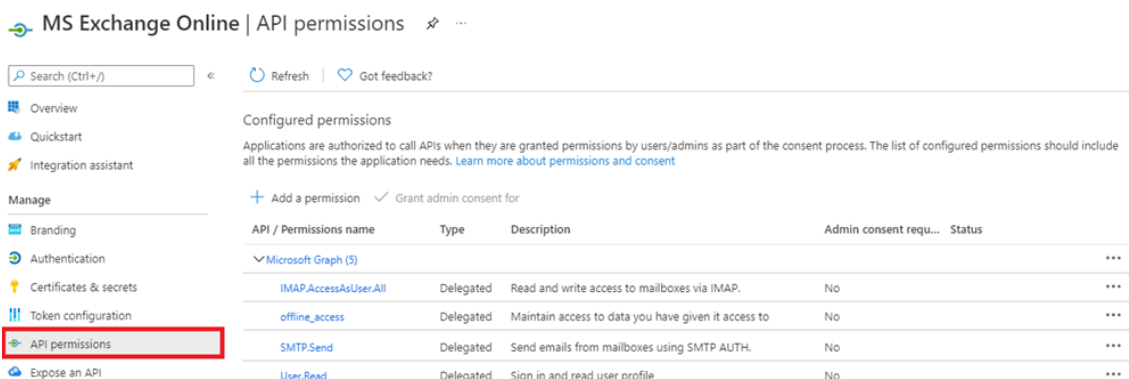
4. The new app overview page opens. Copy the **Application (client) ID** and the **Directory (tenant) ID**, as they are needed for the connection to MyQ.



5. On the left-hand menu, click **Authentication**. In Advanced settings, under Allow public client flows, select **Yes** next to Enable the following mobile and desktop flows, and then click **Save** at the top.

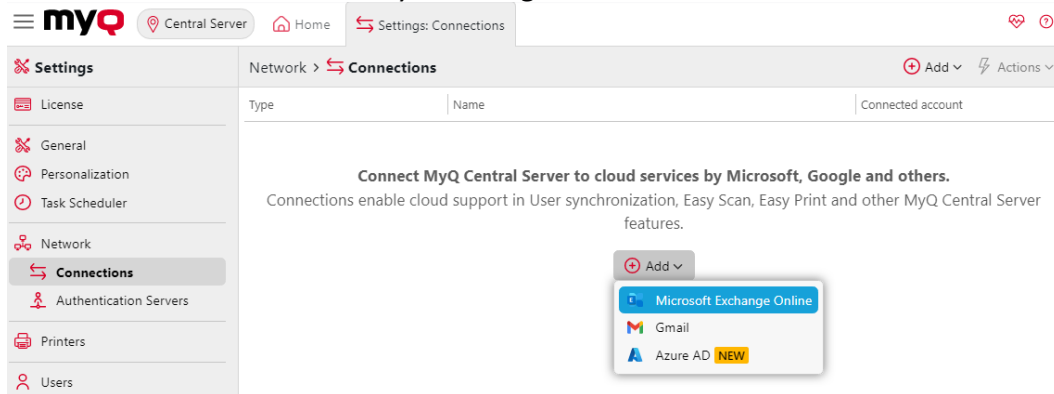


6. On the left-hand menu, click **API permissions** and add the additional permissions required for the correct functionality:
- Microsoft Graph: **offline_access** - Allows the app to see and update the data you gave it access to, even when you are not currently using the app. This does not give the app any additional permissions.
 - Microsoft Graph: **User.Read** - Sign in and read user profile.
 - Microsoft Graph: **IMAP.AccessAsUser.All** - Allows the app to read, update, create and delete email in your mailbox. Does not include permission to send mail.
 - Microsoft Graph: **SMTP.Send** - Allows the app to send emails on your behalf from your mailbox.



Microsoft Exchange Online setup in MyQ

1. Log in to the MyQ web administrator interface, and go to **MyQ, Settings, Connections**.
2. Click **+Add** and select *Microsoft Exchange Online*.



3. In the pop-up window, fill in the required fields:

- a. **Title** - Add the name you chose during App registration in MS Azure; for example, *MS Exchange Online*.
 - b. **Directory (tenant) ID** - The **Directory ID** you copied during the MS Azure setup.
 - c. **Application (client) ID** - The **Application ID** you copied during the MS Azure setup.
4. Click **OK**.
 5. After setting up the connection in MyQ, you are requested to confirm a **code** through the Microsoft website (<https://microsoft.com/devicelogin>). The code you need to confirm is shown in the pop-up window, just below the link to the Microsoft website. There is timeout for confirming the code (usually it is 15 minutes).



The email functionality will not work until the confirmation is successfully completed.

Confirmation must be completed by the Microsoft account that owns the email box (email address) which is used to connect to the exchange (**Sender email** in MyQ, Settings, **Network** tab).

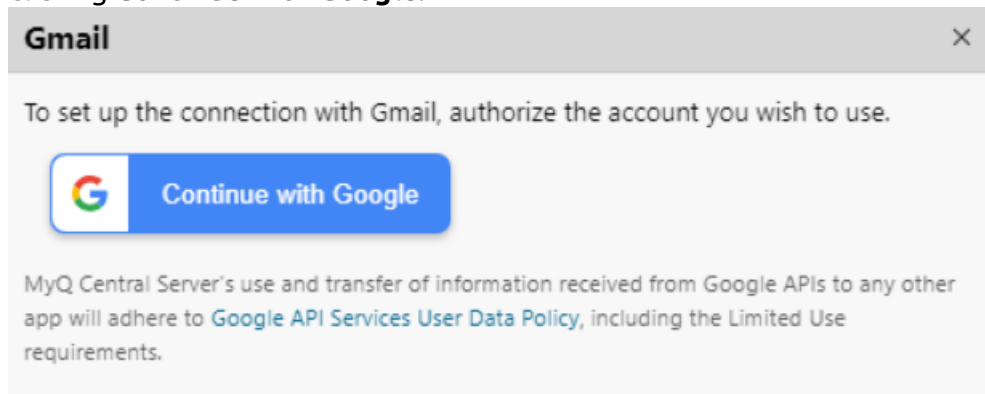
For example, if you use the sender email "print@somedomain.com", then you need to authenticate on the Microsoft website as this user during this step.

Microsoft Exchange Online is now connected to MyQ and is ready to be used in the **Network** settings tab as an Outgoing SMTP server.

7.5.2 Gmail with OAuth2 Setup

To configure Gmail with OAuth2 in MyQ:

1. Log in to the MyQ web administrator interface, and go to **MyQ, Settings, Connections**.
2. Click **+Add** and select *Gmail*.
3. In the pop-up window, you are requested to authorize the connection by clicking **Continue with Google**.



4. Sign in with your Gmail account and allow MyQ to have access to your account.

Gmail is now connected to MyQ and is ready to be used in the **Network** settings tab as an Outgoing SMTP server.

 MyQ's use and transfer of information received from Google APIs to any other app will adhere to [Google API Services User Data Policy](#), including the Limited Use requirements.

7.5.3 Entra ID (Azure AD) with Microsoft Graph Setup

Microsoft Entra ID, previously known as Azure Active Directory (Azure AD), is a cloud-based identity and access management solution. This article explains how to integrate Microsoft Entra ID with MyQ to provide user authentication and other services.

Create a Microsoft Entra ID Connection

1. Go to **MyQ > Settings > Connections**.
2. Click **Add** and select *Microsoft Entra ID* from the list.

Microsoft Entra ID

Title: *

Mode: ☒ **Create automatically**
 You have already configured the Azure application. Provide its credentials to connect MyQ Central Server to this application.

☐ **Create user synchronization**
 Automatically creates the user synchronization source for Entra ID. Adjust the options in User Synchronization before you start importing users.

☐ **Enable Sign in with Microsoft**
 Users can sign in with their work Microsoft account.

 **Continue with Microsoft**

☐ **Set up manually**
 You will sign in with an Azure administrator account and give MyQ Central Server consent to register an application with required permissions to access Microsoft Entra ID.

3. Enter a **Title** for your connection and select your preferred **Mode**:
 - **Create automatically**: MyQ X configures the Azure application required for accessing Entra ID user information.
 - **Set up manually**: Configure the Azure application manually. Select this option if you want to manage all aspects of the integration setup.
4. Proceed to the corresponding section below.

Create Automatically

This mode allows the administrator to have MyQ create the **Enterprise Application (Service Principal)** on their tenant and grant this application permissions to access Entra ID users.



Considerations

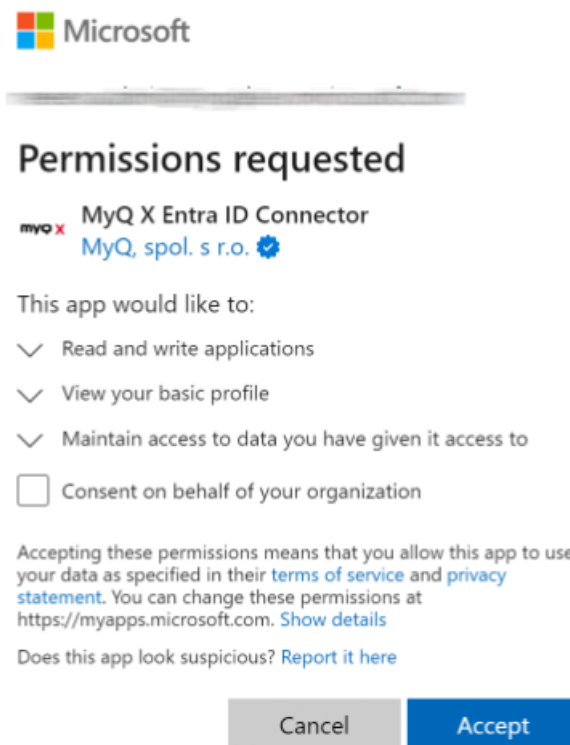
If you are hesitant to grant even temporary administrative access for the creation of a client secret, the automatic connection procedure to ODB will not be available for use. In such cases, it's advisable to manually create an application within your organization's Azure environment and configure the connection to MyQ X by yourself (mode **Set up manually**). This approach ensures that you maintain full control over the application's permissions and the security aspects of the connection, aligning with your organization's specific security policies and compliance requirements.

Prerequisites

- For creating the service principal on the customer's tenant, **Application Administrator** or **Cloud Application Administrator** roles are required.
- For granting admin consent to the service principal, the **Global Administrator** role is required.
- To finish all steps in the automatic setup, the **Global Administrator** role is required.

Steps to automatically set up the Microsoft Entra ID application

1. The administrator signs in with their Azure Administrator account. **MyQ X Entra ID Connector** service principal is created on the tenant.
2. The administrator grants the **delegated** permission to manage Azure applications.
 - a. Permissions requested in this step:
 - Application.ReadWrite.All** (to retrieve a Security key)
 - Directory.Read.All** (to read the default domain name in the connected tenant so that it can be displayed in MyQ).

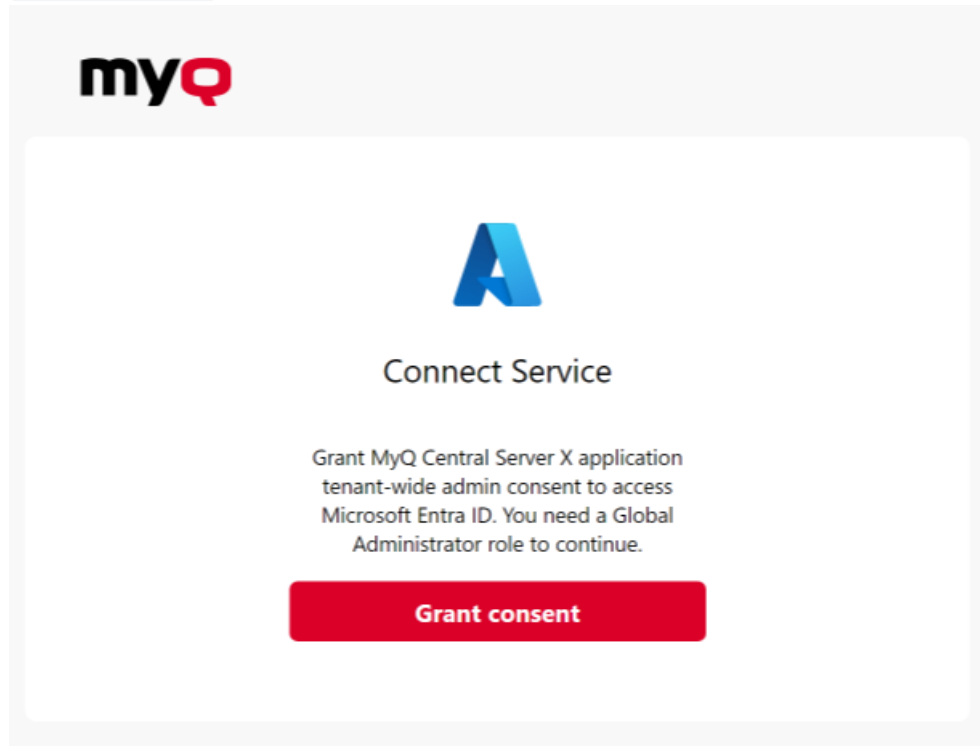


3. The administrator grants the **MyQ X Entra ID Connector** enterprise application **permissions to read Users and Groups** and grants **Admin consent**.

- Permissions requested in this step:

Group.Read.All

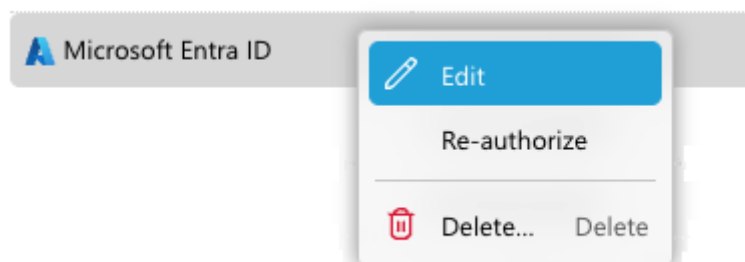
User.Read.All



4. Once the process is completed, the **Microsoft Entra ID** connector is saved, and the connection details are securely saved in MyQ.

Re-authorizing the Entra ID Connection

The automatic connection to Entra ID can be changed or switched to manual after it has been created. By right-clicking on the connection, the **Re-authorize** option will be available in the context menu.





Application Management

- The validity of the Secret is 2 years. Be sure to rotate the key when its expiration is due. You can do this with the Re-authorize option in MyQ. When the secret is within 30 days of expiry, MyQ will send a Health Check warning.
- Credentials for service principals are not visible in the Azure portal. They can be managed via PowerShell or Microsoft Graph API.
- In case you need to **revoke the app's access or currently used Secret**, you can simply delete the entire *MyQ X Entra ID Connector* enterprise application in Azure and create a new one with the Re-authorize option in MyQ.



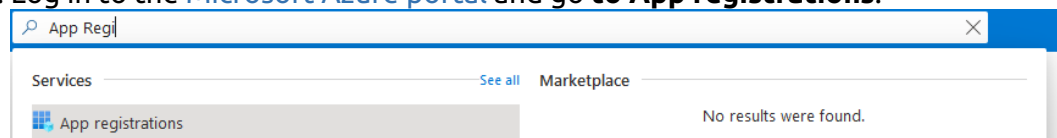
Additional information

- If the automatic setup is completed again, it does not create a new instance of the application on the tenant, but the current application is updated (e.g. new secret on the service principal on the tenant created). If the *MyQ X Entra ID Connector* application has been removed from Azure, it is created again.
- Service principal (enterprise application) is created on the tenant after Step 1 (without necessary permissions which are granted in Step 2). Step 2 can be finished later (by right-clicking the *MyQ X Entra ID Connector* and selecting *Re-authorize*).
- To better understand what MyQ is doing in this mode, Microsoft explains this method in their Developer documentation – [Understand user and admin consent](#) from the perspective of the application developer

Manual Setup

Microsoft Entra ID Application Configuration

1. Log in to the [Microsoft Azure portal](#) and go to **App registrations**.



2. Click **New registration** to create a new application or select an existing application.
3. If you are creating a new application, set the **Name** and in **Supported account types** select *Accounts in this organizational directory only ({Tenant name} only - Single tenant)* option if all your users are members of your tenant. Multitenant

application can also be used if required, depending on the target audience of the application.

4. You can skip the **Redirect URI** settings for now (described in step 7). Click **Register** to create the application.
5. From the application's Overview screen, go to **API Permissions** and select **Microsoft Graph API** and the required type of permission (**Delegated** or **Application**) as illustrated below.

- The following permissions are required:

- **Microsoft Graph \ Group.Read.All**
- **Microsoft Graph \ User.Read**
- **Microsoft Graph \ User.Read.All**

+ Add a permission ✓ Grant admin consent for Default Directory

API / Permissions n...	Type	Description	Admin consent req...	Status
Microsoft Graph (3)				
Group.Read.All	Application	Read all groups	Yes	✓ Granted for Default Directory
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for Default Directory
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for Default Directory

- Note that the system will also automatically request the following **OpenID Connect** scopes during user authentication to enable enhanced identity verification.
 - **openid** (allows sign-in and read basic user profile)
 - **email** (access to user's email address)
 - **profile** (access to user's basic profile information)
- 6. The status "*Granted for Default Directory*" needs to be set on all permissions that require them. All needed permissions can be added and configured with the buttons at the top of the list of permissions.

+ Add a permission ✓ Grant admin consent for Default Directory

Use "**Add a permission**" to add new permission.

Use "**Grant admin consent for Default Directory**" to set the status of the permission as "Granted for Default Directory".

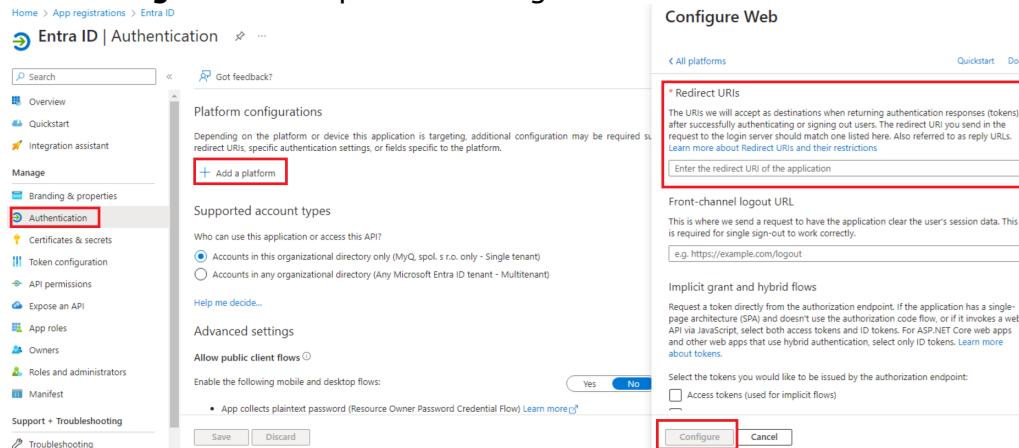
7. Go to **Authentication**, and under Platform configurations click **Add a platform**.
 - Select **Web**, and list all redirect URLs for your MS Entra ID application. For the actual URLs, use the hostname (and port) of your server in the following format:

https://{hostname:port}/auth
 - Additionally, click **Add a platform** and select **Single-page application**. Add the following redirect URL, ensuring that the trailing slash is included:

https://helper.myq.cz/openid/

All servers that use Entra ID sign-on must have a redirect defined in the Azure application. Make sure to perform this step for every print server and central server in your deployment.

- Click **Configure** for each platform configuration.



- In the application's overview page, save the **Application (client) ID** and the **Directory (tenant) ID**, as they are needed for the MyQ configuration.
- Click **Add a certificate or secret** next to **Client credentials** and complete the following steps:

Add a client secret

Description	Enter a description for this client secret
Expires	Custom
Start	Recommended: 180 days (6 months)
End	90 days (3 months)
	365 days (12 months)
	545 days (18 months)
	730 days (24 months)
	Custom

- Click **New client secret**.
- Add a **Description**.
- Set the expiration for the key.
- Click **Add**.
- Save the **client secret key Value**, because you need it for the configuration in MyQ and you cannot retrieve it later.

Configuration in MyQ

Go to **MyQ, Settings, Connections** to connect MyQ to Microsoft Entra ID. Click **Add** and select *Microsoft Entra ID* from the list. In the pop-up window, fill in the required information:

- **Title:** Add a title for the connection.
- **Tenant ID:** Add the Directory (tenant) ID you saved from Microsoft Entra.
- **Client ID:** Add the Application (client) ID you saved from Microsoft Entra.
- **Security key:** Add the (secret) **Value** you saved from Microsoft Entra.

Click **Save** and your Microsoft Entra ID connection is now complete.

Microsoft single sign-on

To use Microsoft single sign-on:

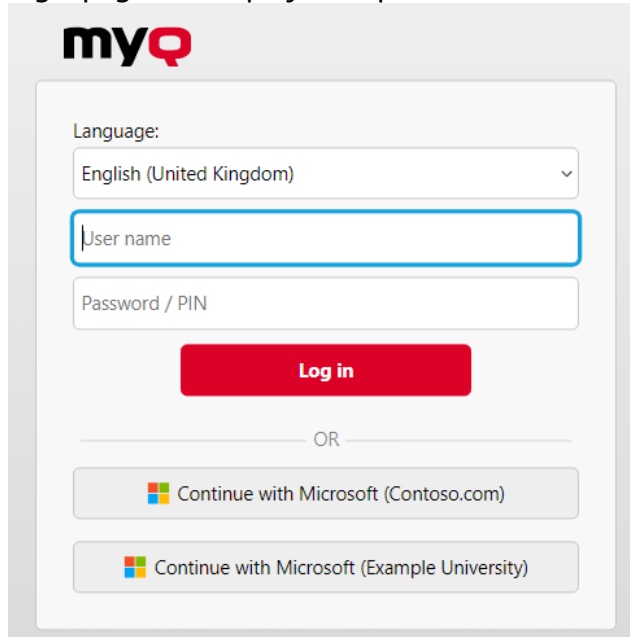
1. Enable "**Use as an authentication server**" in **Microsoft Entra ID synchronization source - Users tab** prior to synchronizing users or enable Microsoft Entra ID as an authentication server manually for selected users in their details on the **Users** main page.
2. In the Microsoft Entra ID authentication server settings, enable displaying the '**Sign in with Microsoft**' login method.

 When Microsoft single sign-on is enabled, the **Sign in with Microsoft** button is always displayed on the MyQ Web UI login page, but only users who use Microsoft Entra ID as their authentication server can use it to log in. Any attempt to use Microsoft single sign-on by a user who does not use the Microsoft Entra ID authentication system will end with an error.

What happens when a user tries to sign in with Microsoft in the MyQ Web UI:

- The user clicks the single sign-on button.
 - If the user is not signed in to Microsoft in the browser, they are forwarded to the Microsoft login page to sign in, and then logged into MyQ with the provided account.
 - If the user is signed into two Microsoft accounts, they are forwarded to the Microsoft login page and are given a choice to select the account to continue with.

- Logout in MyQ Web UI signs out the user only locally, not from Microsoft.
- In cases where multiple Entra ID authentication servers are configured, the login page will display multiple "Continue with Microsoft" buttons.



The screenshot shows the MyQ login interface. At the top is the 'myQ' logo. Below it is a 'Language:' dropdown menu set to 'English (United Kingdom)'. There are two input fields: 'User name' and 'Password / PIN'. A red 'Log in' button is positioned below the password field. Below the button is an 'OR' separator. Underneath are two buttons for Microsoft authentication: 'Continue with Microsoft (Contoso.com)' and 'Continue with Microsoft (Example University)'.



Limitations

- Users using Microsoft Entra ID authentication server cannot sign in on the MyQ Web User Interface with a PIN. However, they can use their PIN on the MyQ Embedded terminals and MyQ Desktop Client up to version 10.0.

Synchronization and authentication through Microsoft Entra ID with Microsoft Graph can now be used via the following steps:

1. [Adding a Microsoft Entra ID authentication server](#) in **MyQ, Settings, Authentication Servers.**
2. [Adding a Microsoft Entra ID synchronization source](#) in **MyQ, Settings, User Synchronization.**



Entra ID (Azure) Multi-Tenant Synchronization and Authentication

You can now use multiple Entra ID tenants in MyQ environments to synchronize and authenticate users. This is particularly useful in shared print infrastructure settings, such as those found in the public sector, where multiple organizations manage printers from a single location, while each uses its own Entra ID.

Follow one of the processes as described above but repeat it to set up multiple instances. Ensure that clear and unique naming is given to each tenant, which will allow users to identify which is relevant for their use.

7.6 Authentication Servers Settings

You will need to do configuration in **Settings – Authentication Servers** if you want to:

- Synchronize users from and/or have them authenticate towards an LDAP server, such as local Active Directory domain.
- Synchronize users from your Microsoft Entra ID, and use Sign in with Microsoft for the MyQ Web Interface, Mobile, and Desktop Clients.
- Authenticate users against a Radius server.

You can later assign the authentication server created here to be used by all synchronized users automatically when you are [creating the user synchronization source](#).

You also can control these settings for each user individually in their profile on [the Users page](#).

i If you only authenticate users against MyQ (ID cards, PINs, and passwords), and thus do not use any remote authentication servers, or need to integrate with another external authentication provider, see [User Authentication](#) for details.

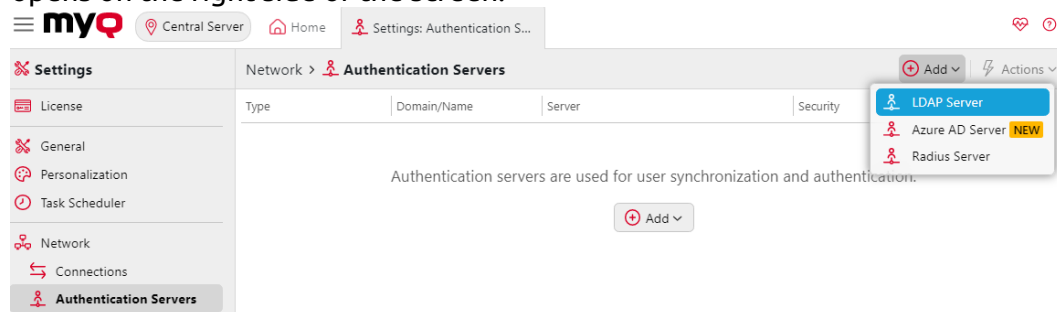


Limitations

Users using an LDAP, Microsoft Entra ID, or Radius authentication server cannot sign in on the MyQ Web User Interface with a PIN. However, they can use their PIN on the MyQ Embedded terminals and MyQ Desktop Client up to version 10.0.

7.6.1 Adding a new LDAP server:

1. Click **+Add** and select **LDAP Server**. The new LDAP server properties panel opens on the right side of the screen.



2. Enter the LDAP **Domain**.
3. Select the LDAP **Type** as *Active Directory* or, if required, one of the other LDAP options such as *Novell*, *OpenLDAP*, or *Lotus Domino*.

4. You should allow the LDAP connection to be secured by selecting the **Security** protocol you want to use.
 - a. For *Active Directory*, you must select **TLS** in the **Security** field.
5. Enter the **Server** hostname and the communication port.
 - a. For *Active Directory*, use the **Server** port **636** for secure communication with TLS. You can also leave the IP address or hostname empty if you do not know them. The server will then be automatically discovered.
6. If you have more addresses related to one LDAP server, you can add them by clicking **Add**.
7. Click **Save**. The LDAP server now appears on the list of servers.

LDAP Server: LocalAD [X]

Domain: * LocalAD

Type: * Active Directory ▾

Security: * TLS ▾

Server: acme.com 636 [X]

+ Add

Leave blank for automatic discovery of the Domain Controller for the domain

Test

✓ Save Cancel

7.6.2 Adding a new MS Azure Server:

1. Click **+Add** and select **Entra ID Server**. The new Entra ID server properties panel opens on the right side of the screen.
2. If you have already added Microsoft Entra ID in the **Connections** settings, the server appears on the list. If not, click **Add new**, add the Microsoft Entra ID connection first (follow the [guide for creating a new Entra ID connector](#)).

Microsoft Entra ID Server: Microsoft Entra ID

Name: * Microsoft Entra ID
Enter the Microsoft Entra ID domain name (e.g., 'ContosoAD') for the sign-in button, to distinguish if multiple domains are used.

Connection: * Microsoft Entra ID

Enable Sign in with Microsoft: ☐

Test

+ Add Cancel

Microsoft Entra ID Server: <no name>

Name: * Microsoft Entra ID
Enter the Microsoft Entra ID domain name (e.g., 'ContosoAD') for the sign-in button, to distinguish if multiple domains are used.

Connection: *
Add new...
Microsoft Entra ID

Enable Sign in with Microsoft: ☐

Test

+ Add Cancel

3. If you want your users to be able to log in on the MyQ Web UI via Microsoft single-sign-on, select the **Enable Sign in with Microsoft** checkbox.

myQ

Language: English (United States)

User name

Password / PIN

Log in

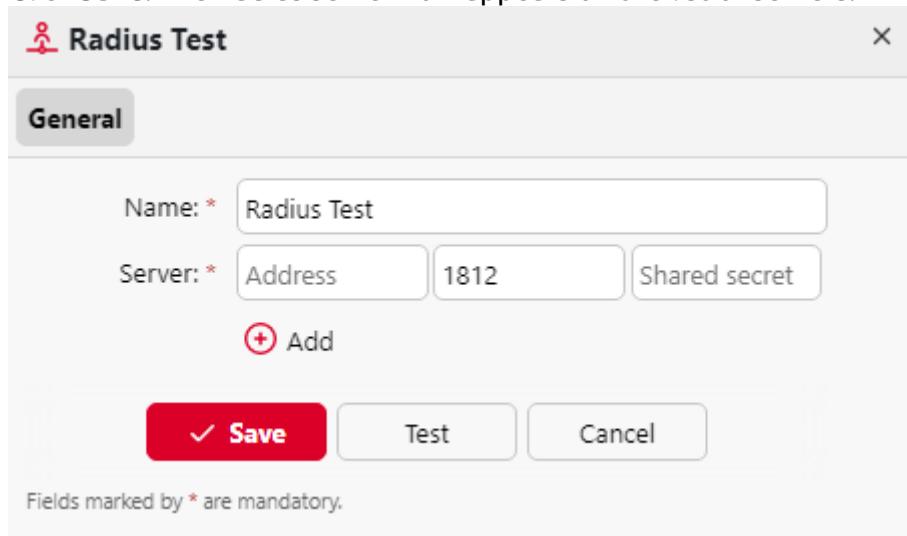
Sign in with Microsoft

Lost PIN • Theme

4. Click **Save**. The Entra ID Server now appears on the list of servers.

7.6.3 Adding a new Radius server:

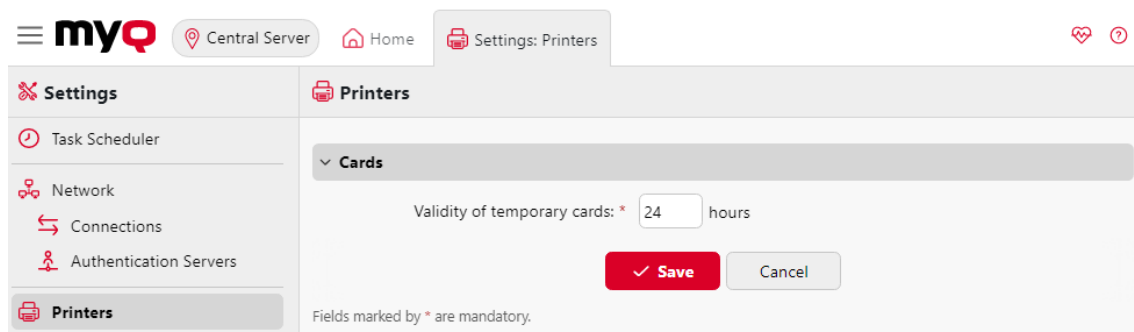
1. Click **+Add** and select **Radius server**. The new Radius server properties panel opens on the right side of the screen.
2. Enter the Radius server **Name**.
3. Enter the **Server** IP address or hostname, the communication port and the Shared secret.
4. If you have more addresses related to one Radius server, you can add them by clicking **Add**.
5. Click **Save**. The Radius server now appears on the list of servers.



i When an authentication server is renamed, a server with the old name will still appear in the Authentication server settings of a user profile, alongside the server with the new name. The old server is removed after the following user synchronization propagates changes.

7.7 Printers Settings

On the **Printers** settings tab, in the **Validity of temporary cards** field, you can set the duration of the temporary cards validity in hours. The default value is 24 hours.



7.8 Accounting Settings

In the **Accounting** settings tab, in the **General** section, the MyQ administrator selects the **Accounting mode** MyQ will be using:

- **Accounting Group** - This is selected by default. In this mode, all quotas are available and can be spent.
- **Cost Center** - In this mode, only the selected (cost center) payment account is spent.

It is possible to switch between the modes anytime.

Limitations:

- The **Cost Center** mode does not work on printers without a terminal.
- **The Cost Center mode can be used only with embedded terminal versions 8.2 or higher.**
- In the **Cost Center** mode, if a user has more than one account, the job is paused and the account must be selected via MyQ Desktop Client (v.8.2 or higher). If there is only one account, the account is assigned automatically.

The screenshot shows the MyQ Central System Settings interface. The top navigation bar includes 'Central Server', 'Home', and 'Settings: Accounting'. The left sidebar lists various settings categories: Authentication Servers, Printers, Users, User Synchronization, Rights, Accounting (selected), and Credit. The main content area is titled 'Accounting' and contains a 'General' section. Under 'General', the 'Accounting mode' is set to 'Accounting Group'. Below this, there is a detailed explanation: 'Accounting Group: Accounting group is selected automatically, all quotas are spent. Cost Center: Only selected payment account is spent. The Cost Center mode can be used only with embedded terminal versions 8.2 or higher.' At the bottom of the 'General' section, there are 'Save' and 'Cancel' buttons. A note at the bottom left states 'Fields marked by * are mandatory.'



If you use the **Cost Center** mode on embedded terminals with a version older than 8.2, the terminals activation fails. The following error message can be found in the log: *"Terminal is incompatible / reason=Terminal version must be at least 8.2 in cost center mode"*.

If you switch to the **Cost Center** mode on embedded terminals with a version older than 8.2, the following warning can be found in the log: *"This terminal is not supported in cost center accounting mode. Upgrade terminal at least to version 8.2"*. Switch to the **Accounting Group** mode or upgrade your embedded terminals to version 8.2 for the terminals to be successfully activated and work properly.

Comparison between Accounting Group and Cost Center

Accounting group	Cost center
Max 1 accounting group per user	Multiple cost centers can be assigned to a user

Accounting group	Cost center
If multiple quotas are assigned to a user, all of them are spent.	Only one quota is spent. If credit, or a cost center without quota is selected, no quota is used.
If credit or personal quota is selected, the job is still accounted to the accounting group	If credit or personal quota is used, no cost center is accounted.
Every job performed by user is accounted to their Accounting group	A job is accounted to the cost center only if selected, or if it is the only account the user has.

7.9 Data Replication from Sites Settings

7.9.1 Replication Settings



This option was added in MyQ Central Server 8.2 (Patch 6) and requires Sites running at least the MyQ Print Server 8.2 (Patch 7).

The administrators of the Central Server can select what data is to be replicated from Sites on the MyQ Central Server Web Admin Interface – **Settings, Data replication from sites** page.

Check the checkbox next to an option to enable the data replication and uncheck it to disable it (all options are selected by default). Click **Save** to apply any changes. The available options are:

- User sessions (non-editable)
- Printers (non-editable)
- Printer groups
- Printer events
- Price Lists
- Projects
- Jobs
- Toner replacements

myQ Central Server Home Settings: Data replication ...

Settings

- Authentication Servers
- Printers
- Users
- User Synchronization
- Rights
- Accounting
- Credit
- Data replication from sites**

Data replication from sites

Replicate data: *

- ☒ User sessions
- ☒ Printers
- ☒ Printer groups
- ☒ Printer events
- ☒ Price Lists
- ☒ Projects
- ☒ Jobs
- ☒ Toner replacements

Data to replicate from site servers

Save Cancel

Fields marked by * are mandatory.

Segmenting and excluding data

- When data are excluded from the replication settings, they are not replicated to the MyQ Central Server.
- If job-related data (*Jobs*, *Projects*) were skipped during replication, then including the data again doesn't lead to replication of already skipped data; only new data is replicated.
- If printer-related data (*Printer groups*, *Printer events*, *Price lists*, *Toner replacements*) were skipped during replication, then including the data again also replicates previously skipped data.
- If an older MyQ Print Server version is used with these settings unavailable, then segmentation settings on the MyQ Central Server don't take effect; all data is replicated.

7.9.2 Scheduling Replication

This data is then downloaded to the Central Server during a scheduled task which period can also be adjusted on the Central Server in **Settings – Task Scheduler**, task **Data replication from sites**. For details, see [Task Scheduler](#).

7.9.3 Resolving Replication Errors

Since MyQ Server 10.2, there is a new health check that checks if there are any non-replicable objects in replications older than the last 30 days, and alerts administrators by notifying them of how many sites are not properly replicated.

After the replication is finished, MyQ tries to resolve these errors automatically. If some errors were resolved automatically, the task will run to retry the failed replications for all sites with automatically resolved errors.

The **Replication errors** section lists any unresolved errors and where some can be resolved manually.

The list is empty

The listed errors can be filtered by site. The errors are grouped by site and missing dependency and its external ID. This means that, for example, user 'X' can block multiple websites and multiple objects dependent on it. Creating user 'X' manually can resolve all errors associated with this missing user. After manual resolution, it is possible to select the lines of errors that you have manually resolved or that you want to recheck and click on the **Resolved manually** button. This will start a retry failed replication with automatic error resolution for all affected sites with the selected errors, and once they're done you can refresh the list to check if any errors came back as unresolved.

7.10 External Reports

By default, the only access to the MyQ Firebird database is via the *SYSDBA* account. Since this account has full read/write rights, it is not secure to use it for accessing the database from 3rd party software (for example BI tools for reporting). A read-only access account is needed to avoid unintentional database corruption.

In the **External Reports** settings tab, the administrator can enable a **database read-only account** to be used with external reports.

Activating the **Enabled** switch automatically creates a read-only access account to the MyQ Firebird database with the following settings:

- **Account name:** *db_datareader*. This is the newly created read-only database user. The account name cannot be changed.
- **Password:** password for the *db_datareader* account, set by the administrator. A new password must be set every time when switching from the **Disabled** to **Enabled** state.
- **Confirm password:** confirmation of the above password.

Enabling the database read-only account automatically enables a Windows Firewall rule to allow incoming connections to the MyQ Firebird database. If disabled, the rule is deleted.

After restoring a backup using **MyQ Easy config**, the Windows Firewall rule and the *db_datareader*'s account password will be restored if the account state was **Enabled** when the backup was created. If the account state was **Disabled**, then the existing Windows Firewall rule will be deleted and the user account will be dropped in the restored Firebird database.

7.11 Log and Audit Settings

On this tab, you can set general settings for the MyQ Log, and the **Log notifier** feature, which enables sending notifications about selected log events to the administrator and/or any number of MyQ users. The notifications can be sent via email or they can be sent to Windows Event Viewer.

The screenshot shows the MyQ Central System Settings interface. The sidebar on the left lists various settings categories: Settings, Network, Connections, Authentication Servers, Printers, Users, User Synchronization, Rights, Accounting, Credit, Data replication from sites, Reports, External Reports, REST API Apps, and Log & Audit. The main area is titled 'Log & Audit' and contains three sections: General, History, and Log Notifier. The General section has a checkbox for 'Log debug level messages' which is checked. Below it, a note states: 'This will generate more information for troubleshooting purposes only. Note: Enabling this feature will impact performance.' The History section has a text box for 'Delete logs older than' set to 14 days. The Log Notifier section has a text box for 'Check new records in log every' set to 300 seconds. There are 'Save' and 'Cancel' buttons. Below these sections is a table for 'Log Notifier rules' with columns for Enabled, Rule name, Type, Subsystem, Context, and Text. The table is currently empty.

General – If you select the **Log debug level messages** option, the system will generate more information for troubleshooting. The information will be shown in the MyQ Log.

However, this feature will impact your system's performance. Therefore, we recommend you enable it only in case of a system malfunction or if it is requested by MyQ support.

History – Here you can set when the logs should be deleted (in days).

Log Notifier – The notifications and their destinations are both specified by log notifier rules. Here you can set the period after which the log is checked for new events in the **Check new records in log every: ... seconds** text box (300 by default).

7.11.1 Management of Log Notifier Rules

To add a new rule, click **+Add item** at the upper-left corner of the **Log Notifier rules** section. The properties panel of the new rule opens on the right side of the tab. On the tab, edit and save the rule.

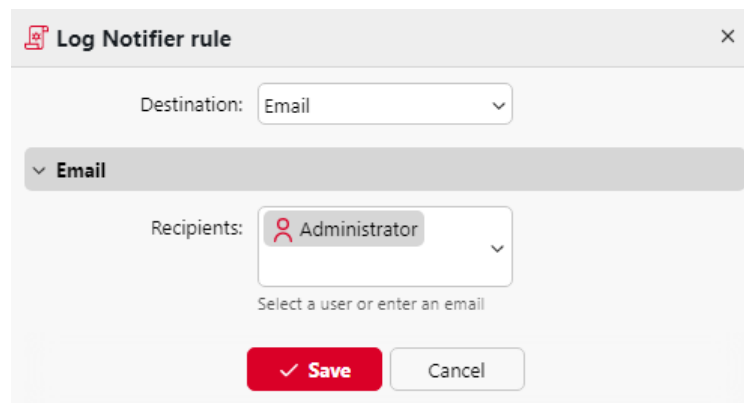
To open the editing options of a rule, double-click the rule (or right-click the rule, and then click **Edit** on the shortcut menu). The following settings can be changed:

The screenshot shows a 'Log Notifier rule' configuration window. It includes a toggle for 'Enabled', text input for 'Rule name' (marked with an asterisk), a dropdown for 'Type', a dropdown for 'Subsystem', and text input for 'Context' and 'Text' (all marked with an asterisk). Below the inputs are 'Save' and 'Cancel' buttons. A footer note indicates that fields marked with an asterisk are mandatory.

- **Enabled:** activate, deactivate the rule
- **Rule name:** name of the rule
- **Type:** the available event types - *Info, Warning, Error, Notice, Debug, Critical*
- **Subsystem:** subsystems of the MyQ application (*Terminal, SMTP Server, CLI, etc.*)
- **Context:** specific part of the subsystem
- **Text:** text of the log event message; you can use Regular expressions to search for specific patterns

After you set the notification rule, click **Save**. The rule is saved and you can select its destinations.

To add the destination, click **+Add item** under **Destinations**.



Log Notifier rule

Destination:

Email

Recipients:

Select a user or enter an email

You can select between two destination options: **E-mail** and **Windows Event Log**. If you select the **E-mail** destination, you need to add one or more recipients; you can either select them from the list of MyQ users in the **Recipients** drop-down or directly type the addresses there. After you set the destination, click **Save**. The new rule is displayed on the tab.

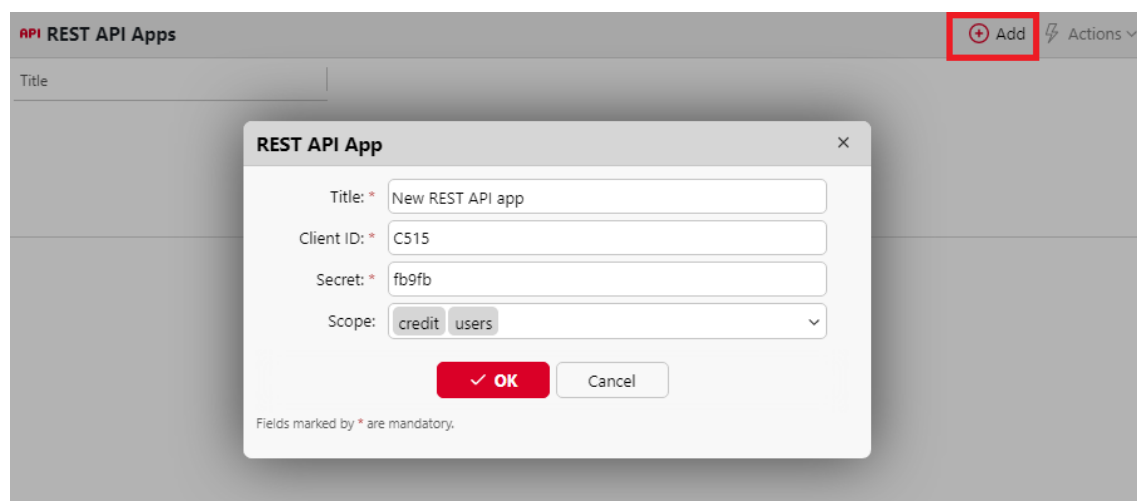
To enable/disable Log Notifier rules:

1. Right-click on the rule.
2. Select **Enabled** (or **Disabled**) on the shortcut menu.

7.12 REST API Apps

In **MyQ, Settings, REST API Apps**, you can add REST API applications.

Click **+Add** and fill in the **Title**, **Client ID**, **Secret**, and **Scope** of the application and click **OK**.



REST API Apps

Title:

Client ID:

Secret:

Scope:

Fields marked by * are mandatory.

7.13 System Management Settings

On the **System Management** settings tab, you can set warning levels for the disk space checker, change the settings of the MyQ history, and also do system maintenance.

The screenshot shows the MyQ Central System Settings interface. The top navigation bar includes a hamburger menu, the MyQ logo, and links for Central Server, Home, and Settings: System Manage... The sidebar on the left lists various settings categories: Settings, License, General, Personalization, Task Scheduler, Network, Connections, Authentication Servers, Printers, Users, User Synchronization, Rights, Accounting, Credit, Data replication from sites, Reports, External Reports, REST API Apps, Log, and System Management (which is highlighted). The main content area is titled 'System Management' and contains three sections: 'Disk space checker', 'History', and 'System maintenance'. The 'Disk space checker' section has input fields for 'Warning level: *' (2048 MB) and 'Critical level: *' (100 MB). The 'History' section has input fields for 'Delete history older than: *' (1460 days), 'Delete printer events older than: *' (90 days), 'Delete archived reports older than: *' (90 days), 'Close payment sessions older than: *' (24 hours), and 'Delete Audit log older than: *' (180 days). Each input field has a description of what the setting controls. At the bottom of the 'History' section are 'Save' and 'Cancel' buttons. The 'System maintenance' section has two expandable sections: 'Data deletion' and 'Advanced'. A note at the bottom of the 'History' section states 'Fields marked by * are mandatory.'

7.13.1 Disk space checker

In the Disk space checker section, you can set the **Warning level** and the **Critical level** (in MB) for the free disk space where the MyQ Central server is stored. Once one of these levels is reached, an email notification is sent to the MyQ administrator. If the critical level is reached, services are also stopped.

7.13.2 History

In the **History** section, you can change the periods after which data stored on the MyQ server is deleted. You can set time periods for the following data:

- **Delete history older than:** User sessions remain on the MyQ Central server for the period (in days) set here. Anything older deleted.
- **Delete printer events older than:** Printer events remain on the MyQ Central server for the period (in days) set here. Older ones are deleted.

- **Delete archived reports older than:** Reports are archived for the period (in days) set here. Older reports are deleted.
- **Close payment sessions older than:** Payment sessions remain on the MyQ Central server for the period (in hours) set here. Older ones are deleted.
- **Delete Audit log older than:** The audit log stores information about change in MyQ Central server for the period (in days) set here. Anything older is deleted.

To change the values, enter new values to the particular text box, and then click **Save**.

7.13.3 System Maintenance

In the **System maintenance** section, you can delete data from the MyQ database, and manage advanced options.

Data Deletion section

The delete/remove buttons perform the following actions. These actions cannot be undone. It is recommended you backup your data before performing any of them.

System maintenance

Data deletion

Users to delete: 0
 X Delete users without sessions
 Users with user sessions will not be deleted.

Deleted inactive users: 0
 X Permanently remove deleted users
 Deleted inactive users will be permanently removed. This action can not be undone.

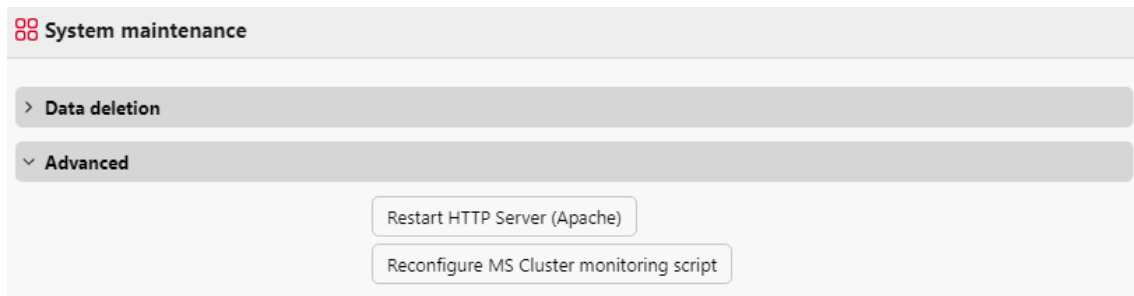
Inactive printers: 0
 X Remove printers without user session and events
 Only the printers without user session and events will be deleted. This action can not be undone.

Projects to delete: 0
 X Remove projects without user sessions
 Only the projects that never were used will be deleted. This action cannot be undone.

User data: User sessions, Jobs, Groups, Users
 X Delete user data
 This action can not be undone. We recommend that you make a backup.

- **Users to delete:** Deletes all users without user sessions.
- **Deleted inactive users:** Removes all inactive users from the MyQ database.
- **Inactive printers:** Removes all printers without a user session from the MyQ database.
- **Projects to delete:** Removes projects that were never used.
- **User data: User Sessions, Jobs, Groups, Users:** Removes all user related data from the MyQ database.

Advanced section



- Click the **Restart HTTP Server (Apache)** button, to restart the HTTP server.
- Click the **Reconfigure MS Cluster monitoring script** button to reconfigure the MS Cluster monitoring script.

8 Licenses

A MyQ Enterprise or MyQ Ultimate license is required. You can purchase the license with rights to a certain number of printers.

For information about the differences between the two types of licenses, see <http://myq-solution.com/products>.

The new MyQ X licensing model -in use since MyQ Server 8.0 (patch 4)-, introduced the use of an **Installation Key** per MyQ setup.

You can view your current license in the License Settings of you MyQ User Interface, or in the Licences widget shown on your dashboard. Three types of assurance plan are available, Standard, Premium, and Premium Plus. More information on assurance plans is available [here](#).

License	License	License
Plan: ENTERPRISE Status: ✓ Standard Assurance Plan. The support will expire on 31/12/2024. Embedded terminals: 0 of 11 0% Features: Virtual machine high availability Installation key: IKA00-6H2P0-2GDTG-52H09-LIKG0	Plan: ENTERPRISE Status: ✓ Premium Assurance Plan. The support will expire on 07/03/2025. Embedded terminals: 0 of 11 0% Features: Virtual machine high availability Installation key: IKA00-6H2P0-2GDTG-52H09-LIKG0	Plan: ENTERPRISE Status: ✓ Premium Plus Assurance Plan. The support will expire on 03/07/2025. Embedded terminals: 0 of 11 0% Features: Virtual machine high availability Installation key: IKA00-6H2P0-2GDTG-52H09-LIKG0

Compared to older editions, MyQ X offers a new price list with updated and new functionalities, one Installation key containing all the license information instead of multiple license keys, a fast and automated license ordering process, and a complete overview in the MyQ X Partner portal of all the products and their software assurance.

This chapter covers the following topics:

- [adding, activating and deleting licenses](#)
- [extending software assurance licenses](#)



The old licensing model (with license keys) is not supported in MyQ Server 10.2+. Upgrade to the new licensing model with Installation Keys is needed.

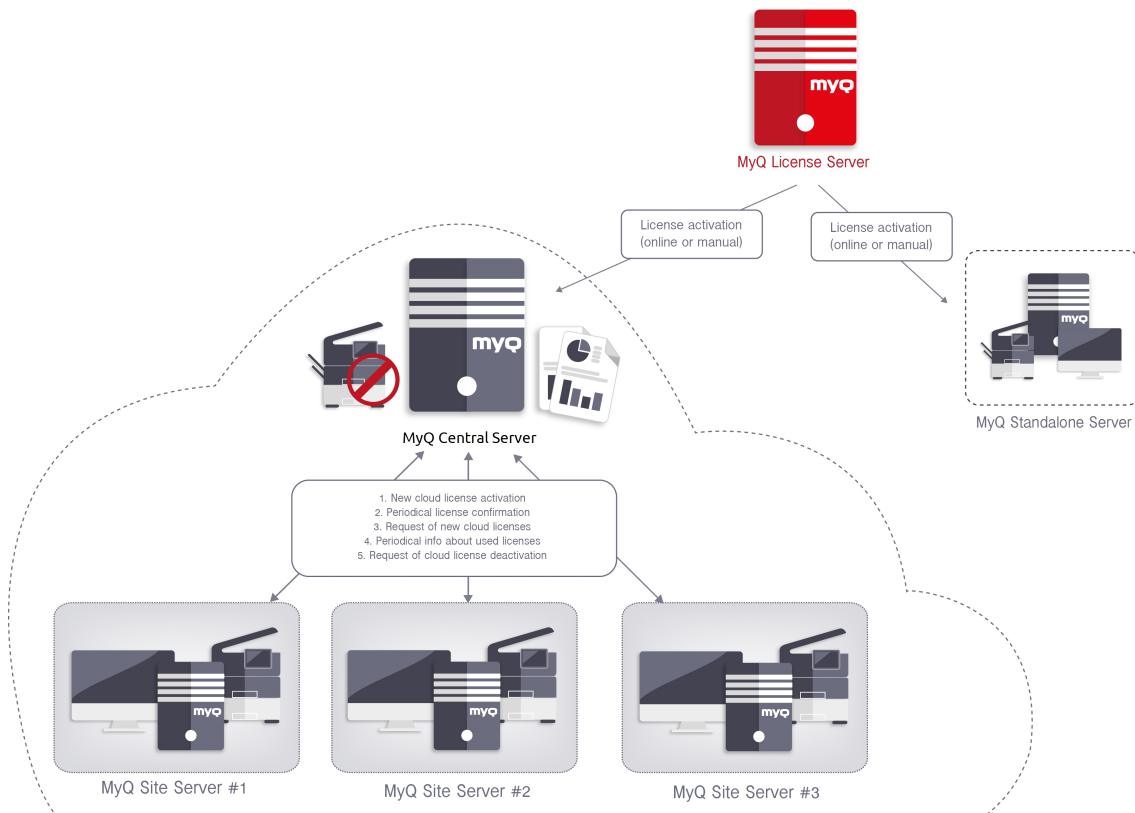
8.1 License Distribution to Site Servers

When using a MyQ Central Server, licenses are first added to the Central server and then distributed to Site servers; no licenses are added directly to Site servers. On each Site server, you set parameters of the Site licenses (exact number of embedded and embedded lite terminals that will be available on the Site server). The Central server generates corresponding Site server licenses (Embedded terminals, Embedded Lite terminals) and accordingly subtracts the number of items from its own licenses.

When you add licenses to the Central server, make sure that you cover the needs of all the Site servers that are used together with the Central server. For example, if you run two Site servers, one with 12 activated printing devices and one with 17 activated printing devices, you need to add and activate a license supporting at least 29 printing devices. If there are 23 embedded terminals used with these printing

devices, you need to add and activate a license supporting at least 23 embedded terminals, etc.

Non-MFPs printers are automatically assigned with an Embedded lite license (2x non-MFPs printers = 0,5 EMB lite + 0,5 EMB lite = 1xEMB license).



Once the installation key is added and activated on your Central Server setup, you can go to each Site server's MyQ web interface and allocate licenses. Go to **MyQ, Settings, Server type**, in the **Licenses** section, add the number of licenses for **Embedded terminals** and/or **Embedded Lite terminals** and click **Save**.

8.2 Adding Licenses

You can add new licenses either on the **Home** dashboard during the initial setup of MyQ, or any time on the **License** settings tab.

After activation, the license is linked with the hardware configuration of the server where MyQ is installed. If the configuration changes (for example, after you reinstall MyQ on a different server, or after you change any of the hardware components of the server), the license becomes invalid and you have to reactivate it within seven days.

The total number of devices allowed to be activated at the same time is equal to the number allowed by individual licenses (for example: a license allowing ten printing devices + a license allowing one printing device + a license allowing five printing devices = sixteen printing devices allowed to be activated).

Adding licenses on the Home dashboard

The first time you set up the system, you can add new licenses on the **Home** dashboard. In the **License** section, click **Enter License**. You are redirected to the **License** Settings tab, where you can add your license information.

Adding licenses on the License settings tab

On the **License** settings tab, you are asked to enter the following information about your installation:

- **Company** - Your company's name
- **Person** - Your full name (e.g. the MyQ administrator's name)
- **Address** - The company's address

- **Country** - Select the country from the drop-down
- **Email** - Your email address
- **Phone** - Your phone number (optional)

myQ Central Server Home Settings: License

Settings

- License**
- General
- Personalization
- Task Scheduler
- Network
 - Connections
 - Authentication Servers
- Printers
- Users
 - User Synchronization
 - Rights
- Accounting
 - Credit
- Data replication from sites

License

Enter information about this installation

Company: *

Person: *

Address: *

Country: * [empty]

Email: *

Phone:

Fields marked by * are mandatory.

Enter the installation key

Installation key:

To get MyQ Central Server SMART license for free register at [MyQ Community portal](#)

Then, enter your Installation keys in the **Enter the installation key** field and click **Save**, and then **Activate**.

- If you are connected to the internet and you have used an Installation key, your licenses are now added and activated.
- If you have used license keys, your licenses are added but need to be activated. Follow the activation steps below.
- If you want to manually activate your licenses, see the steps below.
- If you haven't purchased any license or installation keys yet, you can register in the MyQ Community portal and request for the free **MyQ SMART** license.

You can see the newly added licenses on the **License** settings tab, under **License**.

If you are using a subscription license, you can see when the subscription is expiring or when it is going to be automatically prolonged:

10 days before the expiration, a banner message appears on the interface, reminding you to prolong your subscription:

"Your subscription is about to expire soon, all services will stop in 10 day(s). Please prolong your subscription"

If you don't prolong it on time, your licenses will expire and MyQ will stop working. The following banner message is displayed: *"MyQ is not running: There is an issue with your license. Check details on the 'Settings > License' page."*

If the MyQ server cannot connect to the License server:

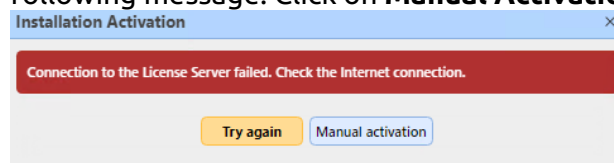
- After the first unsuccessful connection, the MyQ server starts displaying the alert banner *"MyQ server cannot connect to License server, subscription cannot be prolonged and all services will stop in X days. Check internet connection and try to connect manually"*. X = number of days until the expiration + 10.
- If the MyQ server can't connect to the License server for 10 subsequent days after the subscription has expired, the MyQ server will stop working and display the alert banner *"Server stopped working, because it cannot reach License server to update the subscription. Check internet connection and try to connect manually."*

8.3 Activating Licenses

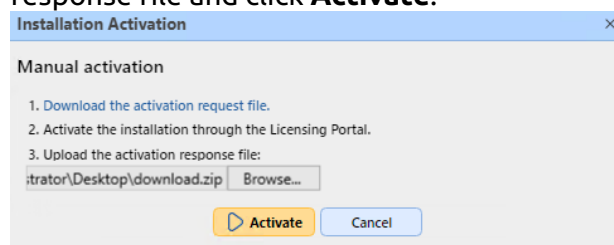
Installation Keys are automatically activated as soon as they are added (if connected to the Internet).

8.3.1 To manually activate a license:

1. Go to the MyQ Web Administrator interface, in **MyQ, Settings, Licenses**. Add your Installation Key and click **Next**. The online activation fails and you get the following message. Click on **Manual Activation**.



2. In the newly opened window, click on **Download the activation request file**.
3. Upload the file in the MyQ X Partner portal and download the activation response file.
4. Go back to the MyQ Web Administrator interface, upload the activation response file and click **Activate**.



8.3.2 Reactivating Licenses in Case of Hardware Change

When moving a MyQ installation from an old server to a new server, a Support task needs to be created with the MyQ License department (Support task - Type license issue) for license installation key reactivation

Steps:

1. Prepare the **new server** with a clean MyQ installation.
2. Create a backup of MyQ (MyQ Easy Config\Database\Backup) on the **old MyQ server**.
3. Restore the backup file from step 2 on the **new MyQ server** (MyQ Easy Config\Database\Restore).
4. With the Installation key now in MyQ Web UI\Settings\License on the **new MyQ server**, you should request for license installation keys activation in 10 days.
5. Generate the Helpdesk support file from the new MyQ server installation (MyQ Web UI\Log\Tools\Generate data for support).
6. Create a Support request (type License issue) for reactivating the installation key with attached Helpdesk support file on the **MyQ Helpdesk partner portal**.
7. When reactivation is confirmed in the task, activate the installation key in MyQ Web UI\Settings\License on the **new MyQ server**.

Notes:

- A valid Software Assurance is required for the period when these changes are made.
- In case of offline activation, provide the Helpdesk support file from the old MyQ server as well.
- Be sure that you are not using 2 MyQ servers with the same database at the same time.
- Licenses on the old MyQ server will no longer be activated (there is a 10 days period from deactivation).

When significant hardware changes are done on the MyQ server and MyQ installation key required activation in 10 days (MyQ Web UI\Settings\License), a Support task needs to be created with the License department (Support task - Type license issue) for license installation key

Steps:

1. Check MyQ Web UI\Settings\License in case any HW changes are done on MyQ server.
2. If the installation key in MyQ Web UI\Settings\License requires activation in 10 days or less, continue with the next steps.
3. Generate the Helpdesk support file (MyQ Web UI\Log\Tools\Generate data for support).

4. Create a Support request (type License issue) for reactivating the installation key with the Helpdesk support file attached on the **MyQ Helpdesk partner portal**.
5. When reactivation is confirmed in the task, activate the installation key in MyQ Web UI\Settings\License.

Notes:

- A valid Software Assurance is required for the period when these changes are made.

8.4 Deleting Licenses

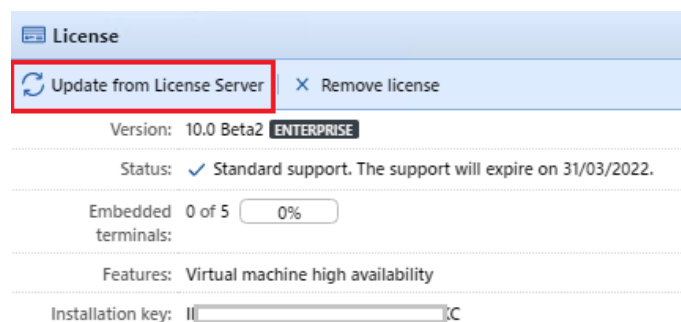
To delete a license:

1. Select the license that you want to delete.
2. On the **Licenses** settings tab, under **License**, click **Delete**.

8.5 Extending Software Assurance Licenses

You can extend the support period by assigning a support license to the particular main license. This can be done at any time, even before your current support period expires. In this case, the service is extended from the last day of validity of the current support.

You can order to prolong your support on the MyQ X Partner portal. Once your order is approved, go to the MyQ Web Administrator interface, in **MyQ, Settings, License** and click the **Update from License Server** button to update your prolonged Software Assurance license. If the new date is not displayed, refresh the web page.



8.5.1 Manual activation

1. Once your additional licenses order is approved, go to the MyQ Web Administrator interface, in **MyQ, Settings, License** and click the **Update from License Server** button. Since there is no network, you will be prompted to **Download** the activation request file.
2. After you download the file, go to the MyQ X Partner portal, under your Project, in the Installations tab. Click **Offline activation**.

3. In the pop-up window, upload the *offlineActivation.zip* file you downloaded from the MyQ Web Administrator interface and click **OK**. The activation response file is then automatically downloaded.
4. Go back to the MyQ Web Administrator interface, upload the activation response file and click **Activate**. Your additional licenses are added and activated.

8.6 Migrating Old Licenses to MyQ X

If you are using older MyQ editions, you must migrate your licenses to MyQ X, as the old licensing model is **not supported** in MyQ Server 10.2+.

Compared to older editions, MyQ X offers a new price list with updated and new functionalities, one Installation key containing all the license information instead of multiple license keys, a fast and automated license ordering process, and a complete overview in the MyQ X Partner portal of all the products and their software assurance.

Moreover, if you use embedded lite licenses, during the license migration to MyQ X, their price is halved (two embedded lite = one embedded license). If you have an odd number of embedded lite licenses, the total is rounded up, and then halved (eleven lite = twelve lite = six embedded licenses).

The software assurance expiration date is recalculated during the migration:

1. Expiration dates are converted to a real number and the average is computed.
(for example, you have 100 x Embedded (E) and 200 x Embedded Lite (EL) | so $100 \times \text{'expiration date' of (E)} + 200/2 \times \text{'expiration date' of (EL)} / \text{count of ((E) + (EL) / 2)}$)
2. The computed average is a real number and, converted back to the date format may produce, for example, 23h:56min - for this reason 1 day is added.
3. From the average corrected date, only the month + year are used, without day + time, and one month is added to the final date.

License Type	Pcs	Software Assurance Expiration	SA Days till Expiration (from today, 5.10.2020)	SA Days of all Pcs
Embedded	40	04.11.2020	30,00	1 200,00
Embedded	10	28.07.2021	296,00	2 960,00
Embedded	8	19.12.2021	440,00	3 520,00
Embedded	1	20.02.2022	503,00	503,00
TOTAL of Embeddeds	59			8 183,00
Lite	10	04.11.2020	30,00	300,00
Lite	1	19.12.2021	440,00	440,00
TOTAL of Lites	11			740,00
Round up to an even number of Pcs	12			807,27
Conversion of Lites to Embeddeds (2-in-1)	6			403,64
TOTAL Enterprise & Support	65	14.02.2021	132,10	8 586,64
FINAL Enterprise & Support	65	01.03.2021		

The prerequisites for license migration are:

- MyQ Print Server or MyQ Central Server 8.2 or higher installed (valid support required).

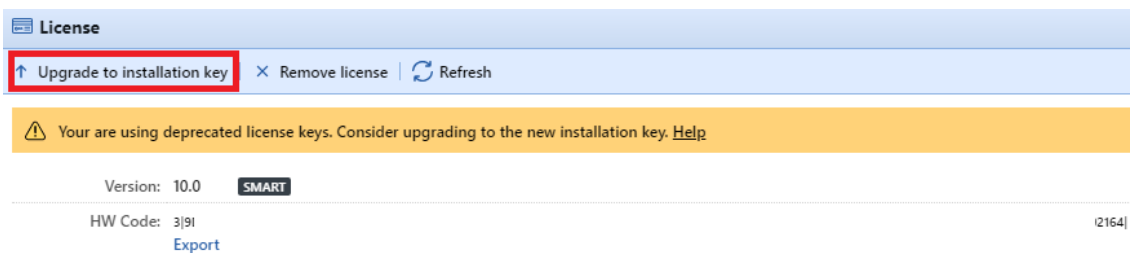
- Valid support required; support date for version 8.2 is 15 January 2021, but it is recommended having valid support all the time, especially when there are planned system changes and MyQ Helpdesk would be contacted.
- Access to the MyQ X Partner portal (Partner ID and password. If you do not have access, contact your Sales representative).

With the above prerequisites fulfilled, you can start the Migration Process.

8.6.1 Migration Process

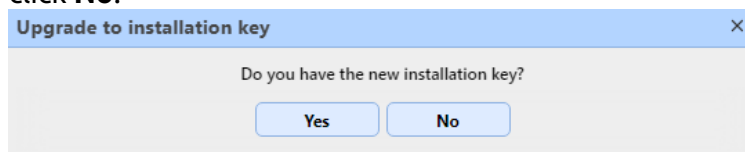
You can start the license migration process in the MyQ web administrator interface.

Go to **MyQ, Settings, License**. At the top bar, click **Upgrade to installation key**.

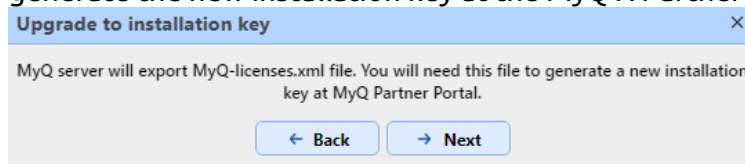


The Upgrade to installation key wizard starts, guiding you through the upgrade:

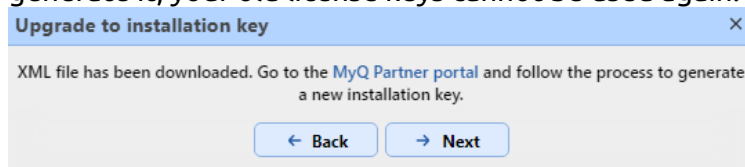
1. If you already have an Installation Key, click **Yes** and continue to step 4. If not, click **No**.



2. The MyQ server will now export the *MyQ-licenses.xml* file. You need this file to generate the new installation key at the MyQ X Partner Portal. Click **Next**.



3. The *MyQ-licenses.xml* file has been downloaded. Go to the [MyQ X Partner portal](#) and follow the process to generate a new installation key. Once you generate it, your old license keys cannot be used again.



4. Back in the MyQ web administrator interface, insert the installation key in the field, and click **Next**.

5. MyQ is contacting the License server to get the license information. In case you have no internet connection, click **Manual activation** to [manually activate the license](#).
6. Check the overview and if everything is correct, click **Activate**; otherwise, click **Cancel**.

7. Your license keys were successfully upgraded to an installation key and are now activated.

You can see your new licenses overview in the **License** settings tab.

 If the activation fails due to connection issues, or for any other issues with the migration, contact MyQ Support.

8.7 VMHA License

Normally, the hardware signature of the server hosting MyQ is occasionally verified to make sure that the license is still installed on the same server and isn't misused. In certain scenarios, the underlying hardware may change and so a license reset is required to re-activate the license. If the hardware changes often (which is common when the server is hosted in a virtual environment), the Virtual Machine High Availability (VMHA) feature may be required.

 The VMHA license is included free of charge in MyQ Enterprise and MyQ Ultimate plans. [Discover our licensing options](#) to find out more.



For the VHMA feature to function, a domain environment is mandatory - the server running MyQ must be a member of a domain. For MyQ installed in an MS Azure environment, a domain is not required. Changing the domain or migrating to a completely different server will still require a license reset.

To verify that the VHMA feature is available, go to **MyQ, Settings, License**.

With the new licensing model, with installation keys, VHMA is enabled by default in a Print Server or Central Server setting. If you are using Site servers, you have to enable the feature in each Site server.

9 Central and Site Administration

As opposed to the MyQ Print server standalone model, where all parts of the MyQ system run on one server, the MyQ Central/Sites model consists of one Central server and multiple site servers.

The Central server cannot be used as a print server and its options are restricted to its central management role. Therefore it is not possible to administer printing devices or print jobs there. The site servers work as the print servers and perform local management of printing devices and print jobs. Their function and management options are similar to those of a standalone server.

After you setup your Central server and add and activate your licenses, you should setup your Site servers as well. In a Site server's MyQ web interface, go to **MyQ, Settings, Server Type** and fill in the following information:

In the **Server Type** section, choose **Site server**. This can only be used within a MyQ Central server installation and the change is permanent. You cannot switch back to standalone mode afterwards.

myQ Home Settings: Server Type

Settings

- Server Type
- License
- General
- Personalization
- Task Scheduler
- Network
- Connections
- Authentication Servers
- SNMP
- Printers & Terminals
- Configuration Profiles
- Printer Discovery
- Terminal Actions
- Events
- Event Actions
- Users

Server Type

Standalone server: licensed separately.
Site server: Production MyQ server, licenses are allocated from the Central Server.

Server Type: * ☐ Standalone server ☒ Site server

Connection settings

Site name: *

Central Server address: *

Enable secure connection: ☒

Port: * 8093

Password for communication: *

Password is used for communication between Central server and Site servers.

Licenses

Embedded terminals: * 0

Embedded Lite terminals: * 0

Fields marked by * are mandatory.

In the **Connection settings** section:

- **Site name** - add a name for your site server.
- **Central Server address** - add the Central server's host name or IP address.
- **Enable secure connection** - enabled by default. The connection between the Central server and the site servers is secured.
- **Port** - 8093 by default.
- **Password for communication** - password used for the communication between the MyQ Central server and Site servers.

In the **Licenses** section:

- **Embedded terminals** - add the number of embedded terminal licenses to be used on this site (distributed by the Central server).
- **Embedded Lite terminals** - add the number of embedded lite terminal licenses to be used on this site (distributed by the Central server).

9.1 Sites Page

Once the site servers are connected to your Central server, you can manage them via the Central's server MyQ web interface, in **MyQ, Sites**.

The left-hand panel of the page contains a view of all the groupings of your sites as well as the default groups **All**, **With Issue**, and **Deleted**.

From the control panel you can select a site and **Edit** it, **Manage** its **Log**, **Printers**, **Settings**, and **Reports**, complete **Actions** such as **Duplicate settings** or **Replicate data**, and **Refresh** the info.

The main section of this page contains an overview of each of your sites, displaying:

- **Status**: the site status (**Unreachable**, **Unknown**, **Error**, **Ready**).
- **Name**: the site name.
- The number of embedded and embedded lite terminals.
- **Last downloaded data**: displays the date and time of the last successfully downloaded record of the site server data.
- **Download status**: shows the status of the last attempt to download site server data (**OK** or **Error**).
- **Last replicated data**: displays the date and time of the last successfully replicated record. Warnings are ignored. If an error occurred during the replication, the displayed date and time represents the last record replicated before the error.
- **Replication status**: shows the status of the last attempt to replicate site server data (**OK**, **Pending**, **Warning**, **Error**).
- **Version**: lists the version of MyQ the site is operating.

9.2 Editing a Site

In the **Sites** main page, select a Site server and click **Edit** on the main ribbon (or double-click or right-click and select **Edit** on the Site server) to modify it. The Site server's properties panel opens on the right side.

- In the **General** tab, you can view the Site's name, port, and if secure connection is enabled. You can also add a description for the Site server.
- In the **User Synchronization** tab, you can select the user groups that you want to synchronize.
- In the **Client** tab, you can add IP ranges for the client PCs that will be used with MyQ Desktop Client (mandatory if you are using the Central server API to obtain the server address for MDC. Check [here](#) for more information). You can also exclude IP ranges in this tab.
- On the **Rights** tab, you can manage user rights for the Site server.

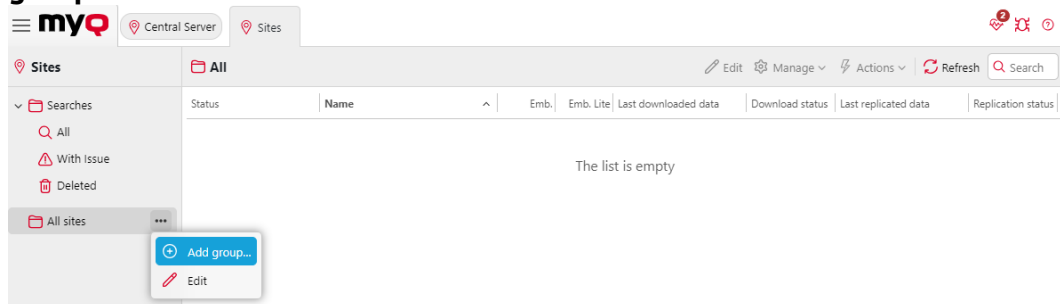
After any modification, click **Save**. Any changes are then distributed during the User Synchronization.

9.3 Grouping Sites

Sites can be grouped to correspond to regions, or your organization's needs.

To create a new site group:

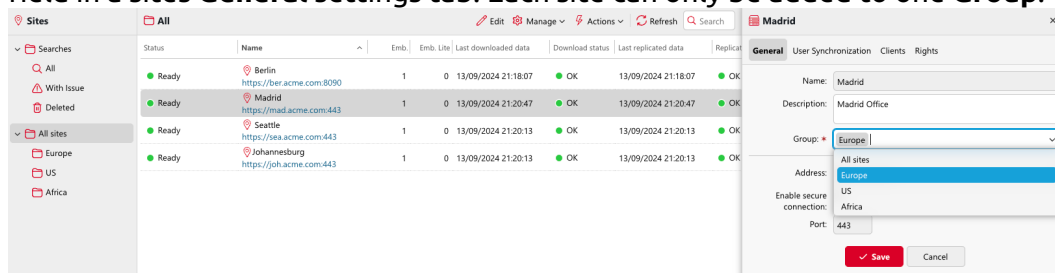
1. Navigate to **MyQ, Sites**, and using the action menu for **All sites**, select **Add group**.



2. Enter the group **Name** and enable or disable **Job Roaming** (if job roaming is enabled for **All sites** it will be enabled for any new group created by default).

The screenshot shows a dialog box titled 'Europe' with a close button (X). It contains a 'Name' field with a red asterisk and the text 'Europe'. Below it is a 'Job Roaming' checkbox, which is currently unchecked. At the bottom, there are two buttons: a red '+ Add' button and a grey 'Cancel' button.

3. Once you have created a group, sites can be moved into it using the **Group** field in a sites **General** settings tab. Each site can only be added to one **Group**.



It is possible to enable **Job Roaming** only for a specific group of sites. Sites then can only roam jobs to the rest of the Sites in the same group. Similarly, it is possible to enable **Job Roaming** for the group **All sites**, meaning despite any groups created, all sites will have **Job Roaming** enabled for all other sites.

i By default, **Job Roaming** is enabled for **All Sites**, this means that any site groups created also have **Job Roaming** enabled. However, **Job Roaming** can be disabled for all sites, and only allowed within particular groups. Doing so can optimize large installations by preventing the loading of unnecessary jobs from remote sites.

Use the actions menu for **All sites** and select edit, where you can enable or disable **Job Roaming**.

If **Job Roaming** for **All sites** is disabled, you can then enable/disable **Job Roaming** for other groups selectively, using the same edit menu. This may be used to enable Job roaming partially, only for selected sites. It allows a level of granularity for the Job roaming feature. For more information on this feature see [Job Roaming](#).

✓ Example: Group sites in one location
If you are running multiple print servers in one location due to a high number of devices or the performance requirements of your installation, you can group only local sites, allowing users to seamlessly release jobs at any release station, and forbid the release of jobs in this location from any other print server outside of your branch.

9.4 Site Server Data Replication

The data to be replicated can be adjusted in **Settings – Data replication from sites**. For further information, check [Data replication from sites Settings](#).

Data replication from sites is set as a scheduled task on the Central server. You can change the time and period of its run on the **Task Scheduler** settings tab.

In case you want to run the task outside of the schedule, you can do so on the **Sites** main tab.

The replication consists of two stages: at the first stage, the data are downloaded from the site server to a folder on the Central server, and at the second stage, they are uploaded to the Central server's database. Only data that are already uploaded to the database are included in the reports on the Central server.

On the **Sites** main tab, you can check the current state of replications for all site servers:

- The **Status** column gives you the following information:

- Ready
- Unknown, http 404
- Error; this can be an http 5xx or http 200 with body '0' error
- Unreachable, a timeout. As an admin you can set the timeout and the period in the *config.ini*.
- The **Last downloaded data** column displays date and time of the last successful download of the site server data.
- The **Download Status** column shows either OK or a red (error) icon.
- The **Last successfully replicated data** column shows if any error happened during the replication. The displayed date and time represent the last record replicated before the error.
- The **Replication status** shows you any of three colored icons:
 - OK - all the downloaded data were successfully replicated.
 - Pending - there are downloaded data waiting to be replicated.
 - Error - replication was not finished due to errors (not warnings!).

To manually run a replication of a site servers' data:

1. Open the **Sites** main tab (**MyQ, Sites**).
2. On the **Sites** main tab, select a Site, click **Actions** on the toolbar, and then click **Replicate data**.

Scheduled run of data replication from sites

By default, the data replication from sites is set to run once per day.

To change the **Data replication from sites** schedule, open the **Task Scheduler** settings tab (**MyQ, Settings, Task Scheduler**), and then double click the Data replication from sites schedule to open its properties panel, where it can be set. For more information, see [Task Scheduler](#).

 The statistical data on Site servers are stored for the period of time that is set on the **System Management** settings tab of the site server MyQ Web Interface, under **History**. To maintain the data, make sure that the time intervals between replications are shorter than these periods. Furthermore, the time periods for storing the data on Site servers should be long enough to avoid losing data, in case the scheduled replication is delayed, for example due to lost connection between the Central server and a Site server.

9.5 Site Server Rights Management

Once a Site server is connected to the Central server, the MyQ administrator can manage the user rights for that server. Any changes are then distributed during the User Synchronization. As soon as the changes are synchronized, the previous user rights settings in the Site server are overwritten and the new rights are read-only in the Site server's rights settings.

To manage a Site server's rights in the Central Server, go to **MyQ, Sites**, select the Site server and click **Edit** on the main ribbon (or double-click or right-click and select **Edit** on the Site server). The Site server's properties panel opens on the right side. Go to the **Rights** tab, click on **Add user** to select the user (or user group), and then assign rights to them.

There is also the option to copy these settings to another Site server. Select the Site server that you want to copy the settings to, and click **Actions - Duplicate settings** on the main ribbon (or right-click and **Duplicate settings**). On the Duplicate settings pop-up, select the **Source** of the settings from the drop-down, and in **Duplicate settings**, mark the checkbox next to the settings that you want to duplicate, *User Synchronization* and/or *Rights*. Click **OK** and the changes are copied to the selected Site server.

9.6 Job Roaming

The Job Roaming feature enables users to transfer their jobs from one location to another: jobs sent to one Site can be printed on printing devices at another Site.

The feature only works in the Central/Site mode, however, it does not have to be centrally managed; Job Roaming between two locations depends exclusively on the settings of the locations Site servers.

The print job is stored on the original Site server until the user logs in at another Site, where they download the job to the **Job Roaming** queue. Thanks to the fact that the files are not unnecessarily transferred between servers, this method guarantees the lowest possible network load.

On a Site's server MyQ web interface go to **MyQ, Settings, Jobs**. In the **Job roaming** section:

- **Allowed users** - Select from the list which users are allowed to use job roaming.
- **Manage queue for these jobs** - Click to open and manage the job roaming queue's properties.
- **Separate job list** - With this option, the remote jobs are displayed on a separate job list. This is optimal for 10+ servers and a slow network connection.
- **Shared job list** - With this option, the remote jobs are displayed on the same job list as the local jobs. This is optimal for up to 10 servers and a fast network connection.
 - **Print remote jobs with Print All** - This option is only available with a shared job list. If you select it, the **Print All** terminal action prints both local and remote jobs.

▼ **Job roaming**

Allowed users:  All users ▼

[Manage queue for these jobs](#)

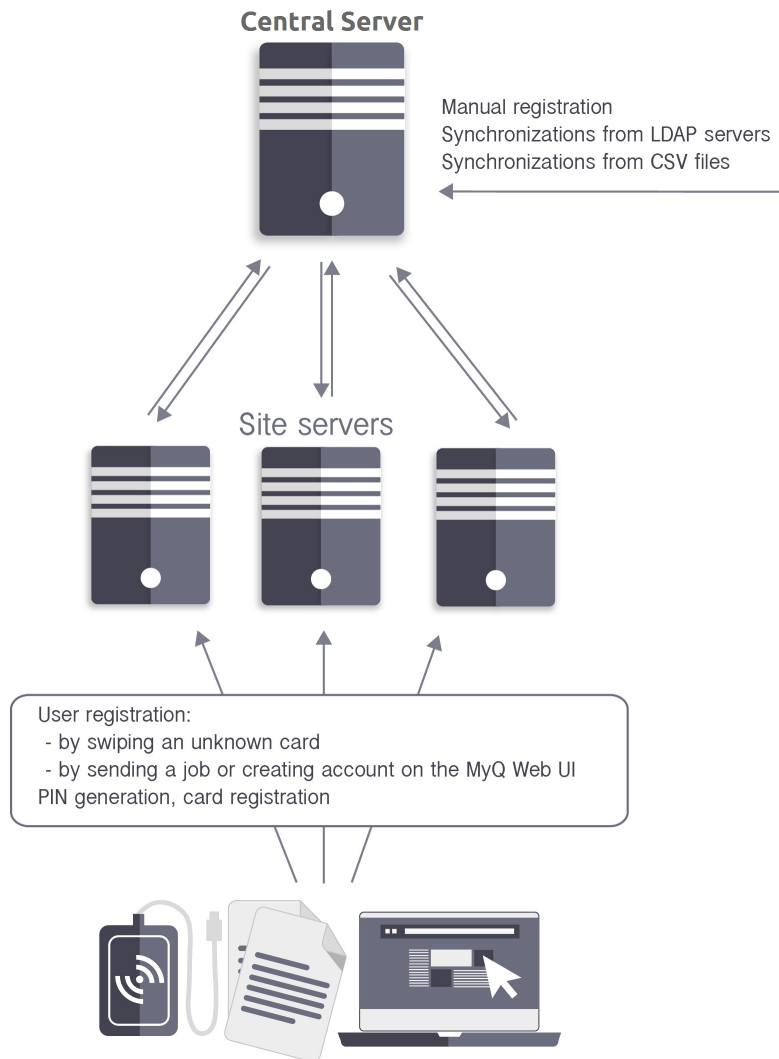
☒ **Separate job list**
Remote jobs are displayed on separate job list. Optimal for 10+ servers and slow network

☐ **Shared job list**
Remote jobs are displayed on one list with local jobs. Optimal for up to 10 servers and fast network

☐ **Print remote jobs within Print All**
Print All button will print local and remote jobs

10 Users

Each Site server connected to your MyQ Central server can synchronize users directly from the Central server and be almost entirely dependent on the changes made there, described below.



There are, however, a few exceptions:

- Users can register themselves by swiping an unknown ID card, on the Web user interface, by sending a job via LPR protocol, or by sending a job via email. The newly created user is automatically replicated to the Central server. If the connection to the Central server is working, the user is automatically added to the server database and also replicated to the Central server database. From there, the accounts are imported to all other sites using the Central server as a synchronization source during the scheduled process of synchronization. If there is no online connection to the Central server, the registration of the new user fails.

- Users that are already in the system can change their language and generate PIN on the Web User Interface. In addition, they can register their cards on MyQ terminals. Every such change has to be authorized by the Central server. If there is no connection to the Central server, the registration of the new PIN/card fails.
- The administrator can add a new card, and add or generate a new PIN for users that are already in the system. Every change has to be authorized by the Central server. If there is no connection to the Central server, the registration of the new PIN/card fails.

In the following sections, you can find information on user management options on the MyQ Central server:

- Overview, registration, adding, importing, synchronizing and deleting users: [List of users](#), [Manually adding and deleting users](#), [Users synchronization from LDAP servers](#).
- PIN generation: [Generating PIN](#)
- Individual users settings: [Editing user accounts](#), [Groups of users](#), [Exporting users](#)
- Special administrative rights: [Rights](#)

10.1 List of Users

On the **Users** main tab, you can see users and information about them. With the **All users** search option selected, you see a list of all the users that are currently in the system.

Apart from this search option, you can also choose from:

- **Unclassified** - select to display only the users that do not belong to any group
- **Managers** - select to display only group managers
- **Locked** - select to display users whose accounts have been locked
- **Deleted** - select to display only deleted users

Default system users

The database of every installation of MyQ contains five default system users. These users are used for administration of the MyQ system and cannot be deleted.

1. ***admin** - This is the MyQ administrator account. It is used for administration of the MyQ system on the Web Administrator User Interface.
2. ***api** - MyQ uses this account to connect to external applications.
3. ***fax** - All printed faxes are charged to this account.
4. ***system** - All the actions performed by the MyQ system are charged to the ***system** user.
5. ***unauthenticated** - If there are any printed, copied or scanned pages that for some reason cannot be assigned to concrete users, they are charged to this account. This can happen, for example, if the print server is not available and users print in an emergency, offline mode on a printing device. It can also

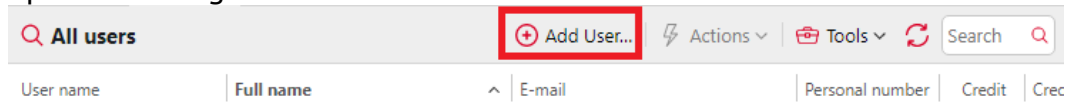
happen if someone prints directly on a printing device, bypassing the MyQ system. In such cases, you might need to check the printing device security settings.

10.2 Adding and Deleting Users Manually

10.2.1 Adding Users

To manually add a new user, follow these steps:

1. On the **Users** main tab, click **+Add User**. The properties panel of the new user opens on the right side of the screen.



2. On the panel, enter the username and full name of the user, and eventually set other data of the user account (see [User information and settings](#)), and then click **Save**.

10.2.2 Deleting Users

When you delete a user, they are removed from all groups (including **All users**) and are marked **Deleted**. They are not completely removed from the MyQ database and can be undeleted.

Deleting users

To delete a user:

1. On the **Users** main tab, select the users that you want to delete, and then click **Actions**. The Actions drop-down box appears.
2. In the **Actions** drop-down box, click **Delete**. You can find the deleted users under the **Deleted** search option.

Undeleting users

To undelete a user:

1. On the **Users** main tab, under searches, select the **Deleted** search option. The list of deleted users appears.
2. On the list, select the users that you want to undelete, and then click **Actions**. The **Actions** drop-down box appears.
3. Click **Undelete**.

10.3 Editing User Accounts

Each individual user has their own properties panel. To open the panel, double-click the user on the list on the **Users** main tab (or right-click the user, and then click **Edit**). The properties panel opens on the right side of the screen. The panel is divided into three tabs: **General**, **Groups**, and **Delegates**.

Carol Kai ×

General Groups Delegates

User name: * Carol Kai

Full name: * Carol Kai

Aliases: + Add

Cards: + Add

PIN: + Add + Generate PIN

E-mail:

Alternate email: + Add

Phone:

Personal number:

Default language: [empty] v

User's storage:

Folder for storing user's documents

Use authentication server: ☐

Authentication server: None v

Notes:

Synchronization source:

+ Add Cancel

10.3.1 User information and settings

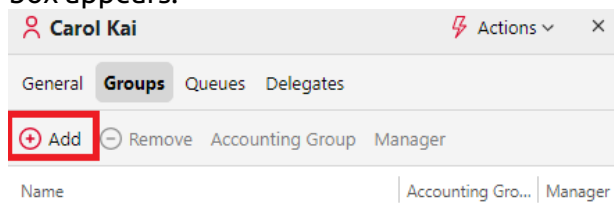
- **User name** - Here you can enter or change the user name. This entry is mandatory. It is unique and is used to identify the user. It is compared to the parameter obtained from the **User detection method**.
- **Aliases** - In addition to their user name, each user can have a number of aliases. MyQ treats the aliases as alternative user names.
- **Card** - Here you can set the number of the user's identification card. If the **Enable deleting all ID cards** option is enabled in **MyQ, Settings, Users**, the **Delete all ID cards** button is available here.
- **PIN** - Here you can manually create or automatically generate new PIN code for the user and remove existing ones. An unlimited number of PINs can be added.
- **Full name** - Here you can enter or change the user's full name. This entry is mandatory.
- **E-mail** - Here you can enter or change the user's email.
- **Alternate email** - Here you can add alternate email addresses for the user to be used as a scan destination.

- **Phone** - Here you can set the user's phone number
- **Personal number** - The personal number can be used as the user ID in MyQ. The primary ID is the **user name** property.
- **Default language** - Here you can select the language of the user's sessions on MyQ embedded terminals.
- **User's storage** - Here you can set the folder where scanned documents are saved.
- **Use authentication server** - If you select this option, an LDAP server is used for the user authentication. The user uses their LDAP credentials to authenticate to MyQ instead of having a password set in MyQ. Select the domain for the authentication on the setting below.
- **Authentication server** - Here you can select the LDAP domain for user authentication.

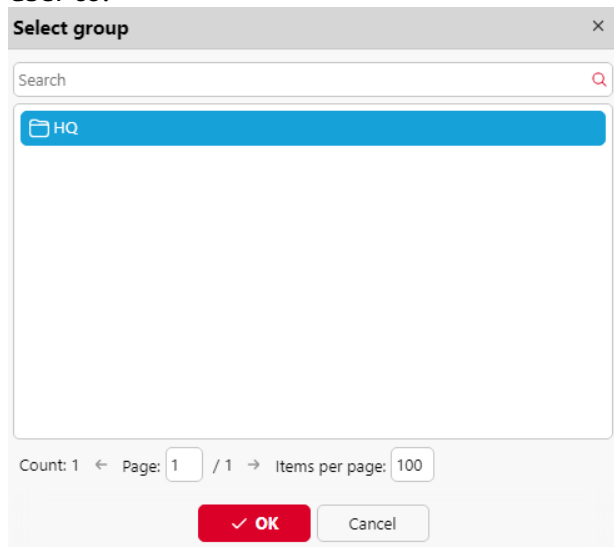
10.3.2 Adding users to and removing them from groups

To add a user to a group on the user properties panel, in the **Groups** tab:

1. On the bar at the top of the **Groups** tab, click **+Add**. The Select group dialog box appears.



2. In the Select group dialog box, select the groups where you want to add the user to.



3. Click **OK**.

A user can also be added to a group on the **Users** main tab using drag and drop. Drag the user and drop it on the group icon, on the groups tab on the left side of the screen.

Default group and Group manager options

On the bar at the top of the **Groups** tab, you can see two options: **Accounting Group** and **Manager**.

The **Accounting Group** is the group where the user is counted in reports and it is set to every user by default.

If you make a user the **Manager** of a certain group, the user can see jobs and reports of all the users from the group. To make the user a manager of a group, select the group and click **Manager**.

To remove a user from a group:

On the bar at the top of the **Groups** tab, click **–Remove**. The group disappears from the **Groups** tab.

To remove selected users from a group on the **Users** main tab, select the group there, select the users that you want to remove, click **Actions**, and then click **Remove from group** in the **Actions** drop-down.

10.3.3 Selecting user delegates

On the **Delegates** tab, you can select delegates (users or groups) who are able to print all of the delegating user jobs sent to a **Delegate** printing type of queue. The delegate will see the jobs on the embedded terminal. The print jobs are displayed in the form: (*Sending user**Name of the print job*).

Users need to have rights to a delegate printing type queue to be able to select delegates.

To select delegates:

On the bar at the top of the **Delegates** tab, in the **Delegates** combo box, enter the user (or the group of users), and then click **Save**. This way, you can add multiple users (or groups of users).

Carol Kai Actions ▾ ×

General Groups Queues **Delegates**

Delegates can print user's jobs sent to the delegated printing queue.

Delegates: HQ ▾

✓ Save Cancel

Tools

⚙ Show resultant delegates

To deselect delegates:

On the bar at the top of the **Delegates** tab, in the **Delegates** combo box, point to the user (or group of users) that you want to deselect, and then click the remove button (X) on the right side of the user (or group of users).

10.4 User Groups

On the **Users** main tab, you can create new user groups.

Creating user groups

To create a group, do the following:

1. On the group tab on the left side of the **Users** main tab, point on the group under which you want to create the new group. A drop-down box appears to the right.
2. On the drop-down box, click **+New Group**. The new group properties panel opens on the right side of the screen.
3. Enter a **Name** for the new group, and optionally add a **Description**.
4. Click **Save**.

To select delegates for the group:

1. Open the group properties panel by double-clicking on the group.
2. On the bar at the top of the **Delegates** tab of the group properties panel, in the **Delegates** combo box, enter or select the user (or the user group).
3. Click **Save**. This way you can add multiple users (or the user group).

To deselect delegates for the group:

On the bar at the top of the **Delegates** tab, in the **Delegates** combo box, point to the user (or user group) that you want to deselect, and then click the remove button (X) on the right side of the user (or user group).

Deleting user groups

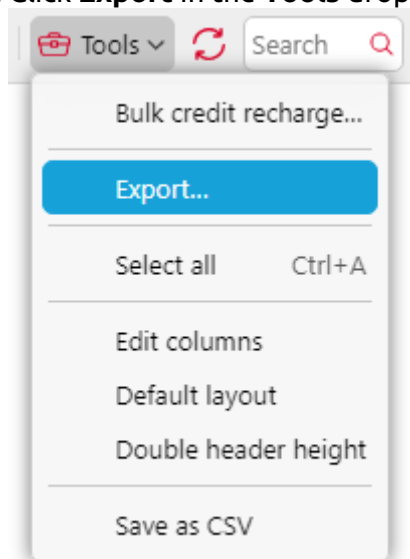
1. On the group tab on the left side of the **Users** main tab, right-click the group that you want to delete.
2. Click **Delete**.

10.5 Exporting Users

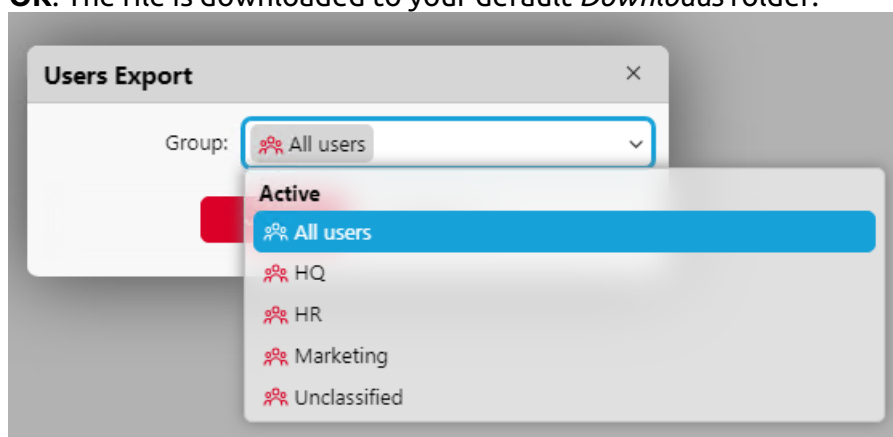
In case you need to export the complete list of MyQ users or a specific user group to a CSV file — for example if you want to use the CSV file for user synchronization — you can do so on the **Users** main tab of the MyQ Web Interface.

To export users:

1. Click **Tools** on the toolbar at the top of the **Users** main tab.
2. Click **Export** in the **Tools** drop-down.



3. In the pop-up window, select which user group you want to export, and click **OK**. The file is downloaded to your default *Downloads* folder.



10.6 User Import and Synchronization

User synchronization is a method of synchronizing user related data in the MyQ database with data in external sources, such as LDAP servers or CSV files. Importing new users is an optional part of the synchronization process. Within the synchronization setup, you can activate or deactivate the new users import; if you deactivate it, MyQ only updates accounts of users that already are in its database. To learn more about user synchronization, see [\(v1\) Synchronize Users](#) in the Deployment guide.

This topic provides detailed information about the synchronization. It fully describes the methods of import and synchronization available in MyQ, and presents two options of running the synchronizations:

- [User synchronization from LDAP servers](#)
- [User synchronization from Azure AD with Microsoft Graph](#)
- [User synchronization from CSV files](#)
- [Manual and scheduled synchronization run](#)
- [User synchronization from Azure AD with SLDAP](#)
- [User synchronization from Google Workspace](#)
- [Using external authentication servers](#)

 User passwords are not synchronized/stored in the MyQ Database in case of LDAP/Azure synchronizations.

10.6.1 User Properties in MyQ

- **User name:** Name of the user account in MyQ. In Active directory and Open LDAP, this property corresponds to the **samaccountname** user attribute on the LDAP server.
- **Full name:** This is the full name of the user. In Active directory and Open LDAP, this property corresponds to the **cn** user attribute on the LDAP server. Usually, it is the given name and the surname of the user.
- **Alias:** In addition to their user name, each user can have a number of aliases. MyQ treats aliases as alternative user names. You can use aliases, for example, if you need to enable one user to send jobs to MyQ from different OS accounts.
- **Card:** The number of the user's identification card. It can be either imported from LDAP or added to MyQ on the user's properties panel. Also, it can be registered by an administrator on a card reader connected to a USB slot or registered by the user on an embedded terminal.
- **PIN:** The MyQ personal identification number is used for access to MyQ Web Interface and MyQ terminals.
- **Personal number:** The personal number can be used as the user ID in MyQ. The primary ID is the user name property. If you select the **Pair by the personal number** property during the user synchronization, the personal number is used instead.
- **Email:** The user's primary email address.
- **Notes:** You can use this text box to enter additional notes concerning the user.

- **Language:** The language used on the user's MyQ Web Interface and their home screen on the embedded terminal.
- **Department:** this field can be used to indicate the user's department if needed.
- **User's storage:** You can select a folder or one or more email addresses where MyQ sends the user's scans. Depending on the scanning setup, scans can be sent here, to the user primary email set in the
- **Email** property text box, or to other sources defined in MyQ or entered by the scanning users.
- **Custom Properties:** attributes can be used to map any other relevant attributes that exist in your synchronization source.

 The properties listed above can be used in certain reports.

10.6.2 User Synchronization from LDAP Servers

An LDAP server contains a database that stores all user accounts, passwords and other user related data of an organization. On the **LDAP Synchronization** settings tab on the MyQ Web Interface, you can synchronize users directly from the server database.

MyQ can communicate with as much as five LDAP servers at the same time. It supports Active Directory, OpenLDAP, Novell, and Google Workspace. To synchronize the users, you need to add the synchronization source first, and then setup the synchronization. After the synchronization is set up, you can either run it manually on the **User Synchronization** settings tab or set it as a regular task on the **Task Scheduler** settings tab.

 The settings described here apply only to Active Directory, although the settings for OpenLDAP, Novell, and Google Workspace are similar.

 OpenLDAP, with its default settings, limits the number of returned entries and the maximum total time for a query. The default size limit is 500 entries and the default time limit is one hour. In case of a larger customer installation with OpenLDAP, you must adjust these limits appropriately in the OpenLDAP settings, otherwise the user sync will give incomplete results.

For more details see: <https://www.openldap.org/doc/admin24/limits.html>

Creating an LDAP Synchronization

Before creating the synchronization, you have to add the LDAP server to MyQ. You do this on the **Authentication Servers** settings tab (**MyQ, Settings, Authentication Servers**).

To create a new LDAP synchronization:

1. Add the new synchronization:
Under **User synchronization**, click **+Add**. A drop-down box appears. In the

General Tab

On the **General** tab, set the general properties of the synchronization: enable or disable the synchronization, select the LDAP server domain, enter user name and password for access to the server, eventually select to export the imported users to a CSV file. See the list below for a description of individual settings.

The screenshot shows the 'LDAP synchronization' settings in the MyQ application. The 'General' tab is active. The 'Enabled' toggle is turned on. Under 'Connection parameters', the 'LDAP Server' is set to 'LocalAD', 'User' is 'Admin', and 'Password' is masked. Under 'Export to CSV after successful import', the 'Enabled' checkbox is unchecked, and the 'File' path is '%app%\Data\Export\Users_LDAP_%datetime%.csv'. The 'Parameters' field shows '%app%', '%datetime%'. At the bottom, there are 'Save' and 'Cancel' buttons. A note at the bottom left states 'Fields marked by * are mandatory.'

- **Enabled:** Here you can enable or disable the synchronization.
- **LDAP Server:** Here you can select the domain that you want to synchronize from.
- **User:** Enter the user name for access to the LDAP domain server.
- **Password:** Enter the password for access to the LDAP domain server.
- **Enabled:** If you enable the **Export to CSV after successful import** option, MyQ creates a CSV file with the imported users after the synchronization.
- **File:** Add the path to the folder where you want to save the created file.

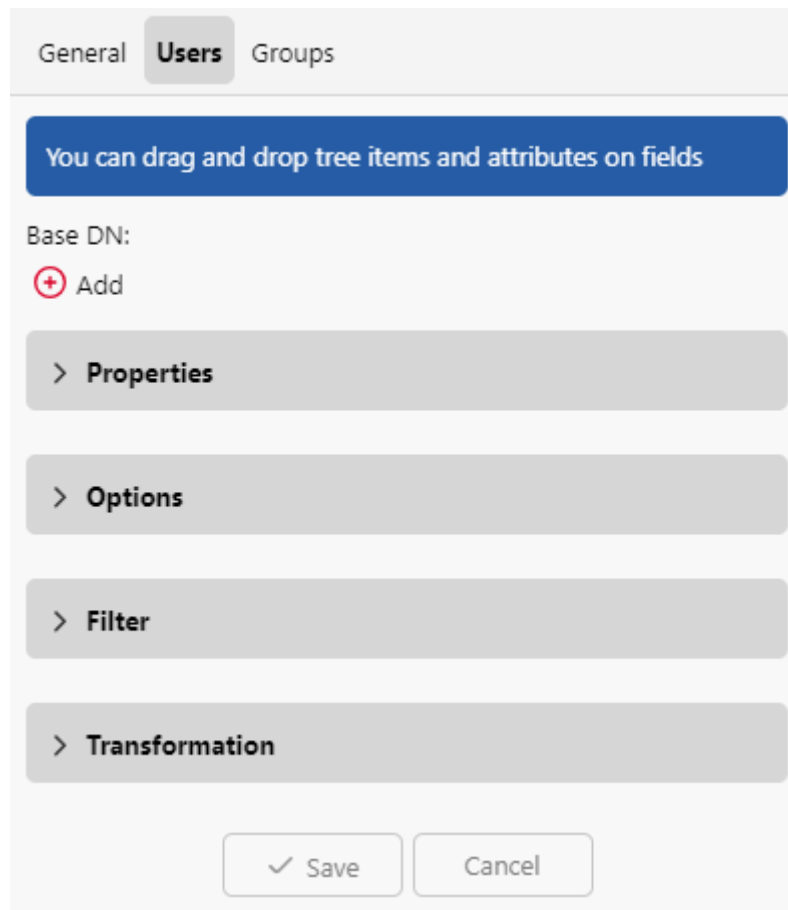
After you correctly set the connection parameters (LDAP server, username and password) and save the settings, the LDAP browser opens on the right side of the screen.

ⓘ In the **User** setting, a sub-domain user account with enough rights can also be used for authentication, but the sub-domain has to be specified in the username.

For example, the user *Administrator* connects to the *testAD.local* LDAP server, but their account is in the *cz.testAD.local* sub-domain. For successful authentication, the filled in username should be:
Administrator@cz.testAD.local

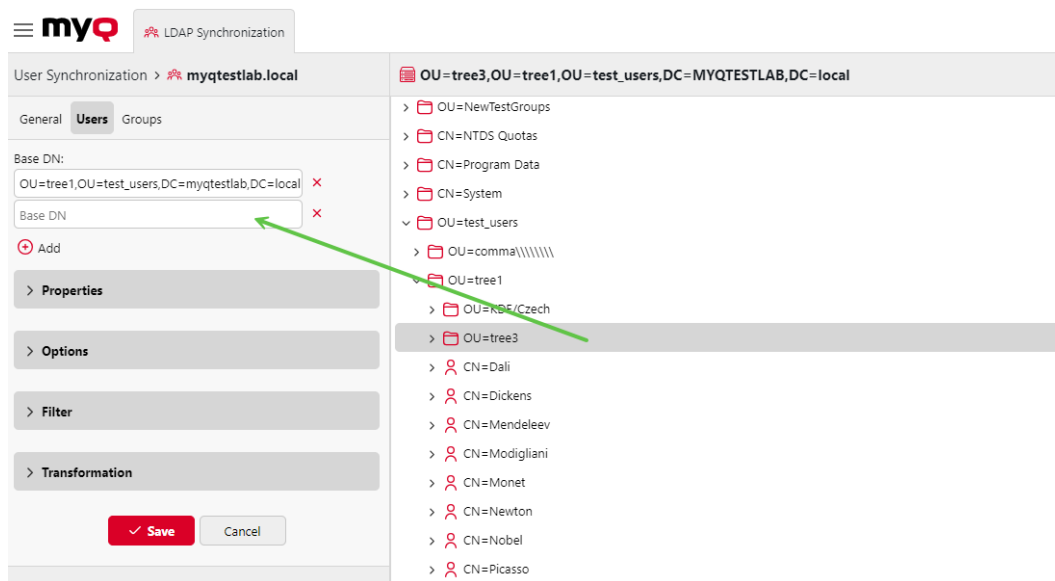
Users Tab

On the **Users** tab, pick one or more base DN's (distinguished names) from which you import the users. In addition, you can assign user attributes from the LDAP server to user properties in MyQ and select additional options concerning the synchronization.



The screenshot shows the 'Users' tab in a configuration window. At the top, there are three tabs: 'General', 'Users' (which is selected and highlighted), and 'Groups'. Below the tabs is a blue instruction bar that says 'You can drag and drop tree items and attributes on fields'. Underneath this, there is a 'Base DN:' label followed by a red circle with a plus sign and the word 'Add'. Below the 'Add' button are four expandable sections, each with a right-pointing chevron and a label: 'Properties', 'Options', 'Filter', and 'Transformation'. At the bottom of the form are two buttons: 'Save' (with a checkmark icon) and 'Cancel'.

- **Base DN:** Here you can pick the base domain or domains from which you import users. Click **+Add** to add a text box for the new base DN, and then drag a group from the database browser and drop it in the text box. You can add multiple domains this way.



- **Properties:** These are the properties of every individual user. MyQ will automatically find and assign the user's **SAM account name** to **user name**, **cn** to **full name** and **mail** to **Email** (this applies to Active directory and OpenLDAP only). The user name property is the only one that cannot be changed. To assign an attribute to a property, write the name of the attribute in the property text box or drag it from the attributes of any individual user and drop it in the text box. The following properties support adding multiple values to them, separated by a semicolon (;):
 - **Alias**
 - **PIN**
 - **Card**

For example, in the **Alias** property, you could add *alias1;alias2;alias3*.

The AD attribute name should not contain the semicolon (;) character. If a semicolon is part of the attribute's name, that attribute will not be synchronized in MyQ.

For the **Card** and **PIN** properties, the administrator can choose one of the following options:

1. **Do not synchronize:** This option will skip the synchronization of these values.
2. **Full synchronization:** This option will replace the existing values with the new values from LDAP, irrespective of whether the new value is empty or not.
3. **Synchronize if not empty:** This option will replace the existing values only if the new values from LDAP are not empty. It won't remove the existing values if the corresponding value in LDAP is empty.
4. **Add new:** This option will update the existing values by adding new values from LDAP, without replacing the existing ones.

For assigning default languages to users, you have to use an attribute from the LDAP server that has the language abbreviations as its values. For example, you can create and use an attribute called **lang** with the values *en* for English, *hr* for Croatian, etc.

- **Options:** For a description of the common synchronization options, see [User information and settings](#). The basic options that are common for both the synchronization from LDAP servers and for synchronization from CSV files are:
 - **Deactivate missing users:** If you select this option, MyQ deletes users that are imported from the current synchronization source and that are not in the source anymore. To delete users that were added from different sources, select the **Ignore synchronization source** option together with this option.
 - **Add new users:** If you select this option, MyQ adds new users from the current synchronization source. If you do not select it, MyQ updates the user accounts of the users who are already in MyQ, but does not add any new users.
 - **Convert user name to lowercase:** Unlike some other systems that do not differ between two words with the same letters but different cases (such as "Pear", "pear"), MyQ is case sensitive. You can use the **Convert user name to lowercase** option to prevent creating multiple accounts for one user.
 - **Use authentication server:** If you select this option and a user logs in by entering their username and password, the credentials are not authenticated against the MyQ database, but instead against an LDAP or Radius server. If you synchronize users via LDAP, the source LDAP server is automatically assigned as the authentication server. If you synchronize users via CSV, you can select the authentication server from the list of predefined authentication servers.
 - **Pair by the personal number:** If you select this option, MyQ identifies users by their personal number instead of their user names. This way you can keep track of a single user with different names in different sources or a user whose name has changed for some reason. For example, if this option is activated and a username in LDAP changes from *cat.stevens* to *yusuf.islam*, MyQ does not create a new user account, but recognizes the old user by their personal number.
 - **Ignore synchronization source:** If this option is not selected, MyQ recognizes two users from different synchronization sources as two different entities. This can cause conflicts during synchronizations from multiple sources. If it is selected, MyQ ignores the synchronization sources and treats all users the same, regardless of their synchronization source. For example, if you run a synchronization and MyQ would import/update a user that has been already added from a different synchronization source, it does not update the user. Instead, it shows the message *The name/alias "X" is already used by the user "X"* among the synchronization results. After you select the **Ignore synchronization source** option, the user is updated by the latest synchronization.
If you select this option together with the **Deactivate missing users** option, all users that were added from different sources and are not in the current synchronization source are deleted during the synchronization.
 - **Append the domain name to the username** (*username@domain.local*): With this option selected, the name of the domain can be retrieved from the MyQ username. The information about the domain may be needed for example, when scanning to users' home folders is used on an embedded terminal.

- **Filter:** You can filter the users import by specifying the values of attributes. Add the conditions in the form of [LDAP filter syntax](#). Users with a different value on this attribute are not accepted and are filtered out of the import. For example:

Search filter	Description
(objectClass=*)	All objects.
(&(objectCategory=person)(objectClass=user)(!(cn=andy)))	All user objects but "andy".
(sn=sm*)	All objects with a surname that starts with "sm".
(&(objectCategory=person)(objectClass=contact)((sn=Smith)(sn=Johnson)))	All contacts with a surname equal to "Smith" or "Johnson".

For attributes where the values are strings, such as the cn attribute, you can use the wildcard * symbol to search for substrings.

Filter:

(|(sn=Smith)(sn=Johnson))

(&(objectClass=organizationalPerson)(|(Attribute=Value)(Attribute=Value)))

- **Transformation:** this feature enables administrators to define regular expressions (RegEx) to transform user data during the synchronization process, details are available [here](#).

Groups Tab

On this tab, you can import groups and the group structure from the LDAP source. There are four different ways of specifying which groups are imported. You can use multiple different methods together and by each method, you can create different groups of users. You can also select to import the groups under an existing group in MyQ.

Settings > Users > User Synchronization >

LDAP synchronization

General Users **Groups**

You can drag and drop tree items and attributes on fields

☒ Make default

Import groups under this group:

- > Group stored in user's attribute
- > Group stored in user's DN
- > Tree group stored in user's DN
- > Group stored in user's memberOf attribute

- **Do not change default group:** A user can be a member of multiple groups but all their prints, copies and scans are accounted to only one group: the default (accounting) group of the user. If you select this option, the default group of the selected user does not change during the synchronization.
- **Import groups under this group:** You can select an existing group in MyQ under which you import the groups from the LDAP database.
- **Groups stored in user's attribute:**
 - **Attribute:** You can select this option if you want to use an attribute that defines groups in the LDAP database. To add it, type the name of the attribute in the property text box or drag the attribute from any individual user and drop it in the **Attribute** text box.

Attribute: ☒ Make default

> Group stored in user's DN

> Tree group stored in user's DN

> Group stored in user's memberOf attribute

Attribute	Value
accountExpires	9223372036854775807
badPasswordTime	0
badPwdCount	0
cn	Picasso
codePage	0
countryCode	0
dSCorePropagationData	20130910165104.0Z
dSCorePropagationData	16010101000000.0Z
displayName	Pablo Picasso

You can also create groups by combining multiple attributes. To create such groups, put each of the attributes between two percentage signs (%). For example, the combination of attributes `%attribute1%_%attribute2%`, imports a new group named `value1_value2`.

> Group stored in user's attribute

Attribute: ☒ Make default

Furthermore, you can create tree structures of groups by separating the attributes with vertical bars. For example, the combination of attributes `%attribute1%/%attribute2%`, imports a group `value1`, and its sub-group `value2`.

- **Make default:** If you select this option, the group becomes the default group of the imported user.
- **Group stored in user's DN:**
 - **OU component index:** Here you can select a group by its OU (organizational unit) index among the DN components. The index is counted from right to left: the first OU group from the right has index 1, the second from the right has index 2 and so on.

`CN=Picasso,OU=tree1,OU=test_users,DC=MYQTESTLAB,DC=local`

On the image above, there are two OU groups: `test_users` has index 1 (as it is the first OU group from the right), `tree1` has index 2. The other components are not OU and therefore have no index.

- **Make default:** If you select this option, the group becomes the default group of the imported user.

- **Tree group stored in user's DN:** Here you can import the whole tree structure of groups. You can restrict the import to any part of the structure by stripping the DN components from the left and from the right. In the respective text boxes, enter the amount of components to be striped from the left and from the right side. You have to strip at least one component from the left (the user CN component) and one component from the right (the right-most DC component).

 **CN=Fleming,OU=tree3,OU=tree1,OU=test_users,DC=MYQTESTLAB,DC=local**

On the image above, there are six components. If you strip one component from the left and one from the right, you import the following structure of groups: *MYQTESTLAB > test_users > tree1 > tree3*. By stripping components from the left, you remove the groups from the bottom to the top of the structure. By stripping components from the right, you remove the groups from the top to the bottom of the structure.

- **Make default:** If you select this option, the bottom group of the imported structure becomes the default group of the imported user.
- **Group stored in user's memberOf attribute:**
 - **Group base DN:** MyQ can import security and distribution groups stored in the user's **memberOf** attribute. The security groups are used to define access permissions granted to their members. Distribution groups can be used for sending emails to a group of users. To specify which groups should be taken into consideration during the import, you have to insert the groups base DN. MyQ imports only groups that are included in the base DN; other groups stored in the **memberOf** attribute are ignored. The group base DN does not have to be in the same organizational unit as the users base domain. If a user is member of more than one group on the LDAP server, all the groups are stored in the **memberOf** attribute. Therefore, the **Make default** option, which requires a single value, is not available for this method of import.
To add the groups base DN, drag it from the database browser and drop it in the **Group base DN** text box.
 - **Filter:** You can filter this import by specifying the values of attributes. Add the conditions in the form: *Attribute=Value*. Groups with a different value on this attribute are not accepted and are filtered out of the import. You can use the * symbol to search for substrings. The symbol can be appended from both sides. For example, if you add a *cn=*in** condition, only users whose common name attribute contains "in" are accepted. You can add one condition per row. Groups are accepted if they satisfy at least one condition.

▼ **Group stored in user's memberOf attribute**

Groups base DN:

Filter:

Attribute=Value
Attribute=Value

Import empty groups: ☐

Import tree of groups: ☐

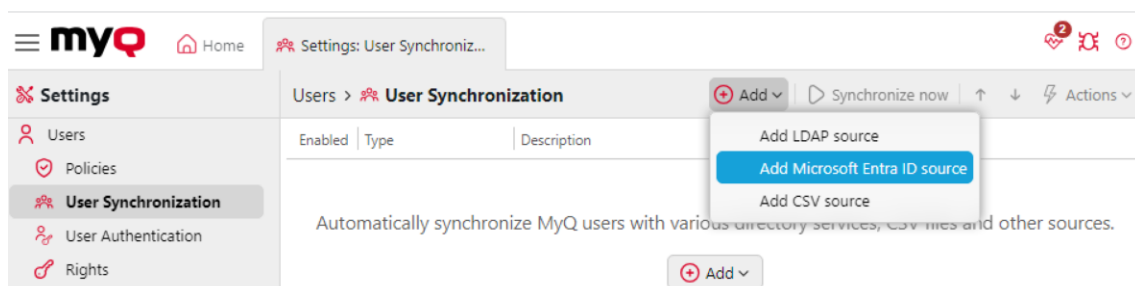
- **Import empty groups:** If you select this option, groups from the **Group base DN** are imported even if there is no user having them in their **memberOf** attribute.
- **Import tree of groups:** If you select this option, the whole tree structure is imported. Otherwise all groups are added separately; not as a part of a tree structure.

10.6.3 User Synchronization from Entra ID with Microsoft Graph

Microsoft Entra ID (formerly Azure AD) with Microsoft Graph is a service accessed from the Microsoft Azure Portal, it must be [enabled and configured](#) before it can be used to synchronize users to MyQ.

Add Microsoft Entra ID as a Source

Once the Microsoft Entra ID connection is established, go to **MyQ > Settings > User Synchronization**. Click **Add**, and then click **Add Microsoft Entra ID source**.



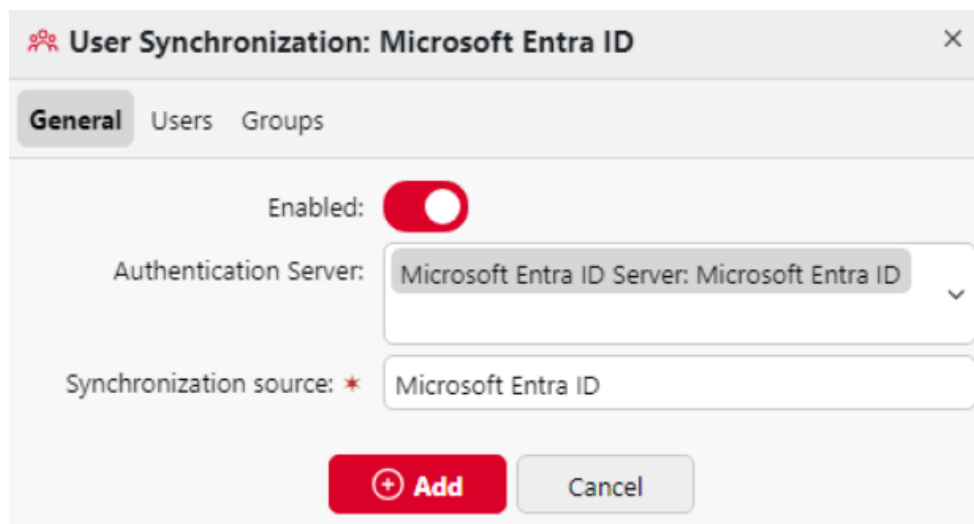
Once the source is established, configuration options allow you to edit how users are imported.

- In the **General** tab the **Authentication Server** and **Synchronization Source** can be set, and the synchronization can be enabled or disabled.
- In the **Users** tab, the users that should be imported can be selected, their properties can be set, and various other options can be enabled or disabled.
- In the **Groups** tab you can set rules not for which users to import (this is set in the **Users** tab), but how to group users that are imported, based on their grouping in your Entra ID source.

General Tab

This tab opens by default when you select **Add Microsoft Entra ID source**. The following options are available:

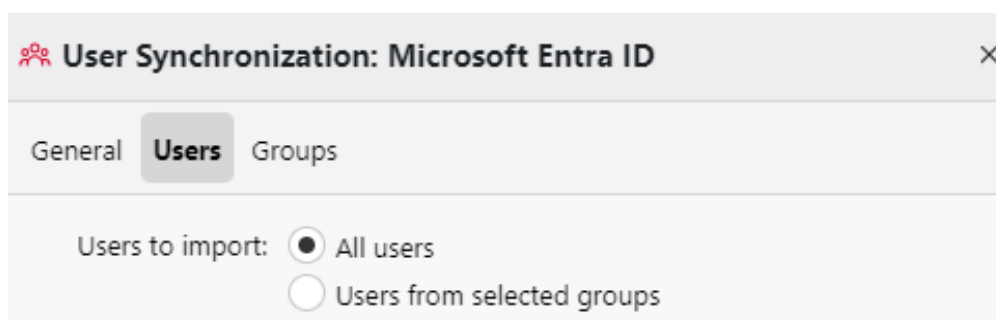
- **Enable:** use this toggle to enable or disable the user synchronization.
- **Authentication Server:** select the authentication server you wish to use. This server should already be connected and configured according to [these instructions](#). If multiple connections are established, you can select which to use for this user synchronization.
- **Synchronization Source:** give this particular user synchronization a name which allows it to be easily identified. This is especially important if you are using multiple Entra ID tenants, to differentiate between them.



The screenshot shows the 'User Synchronization: Microsoft Entra ID' dialog box with the 'General' tab selected. The 'Enabled' toggle is turned on. The 'Authentication Server' dropdown is set to 'Microsoft Entra ID Server: Microsoft Entra ID'. The 'Synchronization source' text field contains 'Microsoft Entra ID'. At the bottom, there are 'Add' and 'Cancel' buttons.

Users Tab

This tab allows you to select which **Users to import**, their **Properties**, and various **Options** for user synchronization.



The screenshot shows the 'User Synchronization: Microsoft Entra ID' dialog box with the 'Users' tab selected. The 'Users to import' section has two radio button options: 'All users' (which is selected) and 'Users from selected groups'.

▼ Properties

Full name: *

displayName

▼

Personal number:

▼

Email:

mail

▼

Notes:

▼

Language:

preferredLanguage

▼

Department:

department

▼

Alias:

▼

Card:

▼

PIN:

▼

Custom (1):

▼

Custom (2):

▼

Custom (3):

▼

▼ Options

☒ Deactivate missing users

☒ Add new users

☒ Use as authentication server

Users will be using their credentials from Microsoft Entra ID and can use the Sign in with Microsoft to log in.

☐ Pair by the personal number

☐ Ignore synchronization source

☐ Create a normalized alias from Display name

May be required for print from Entra ID Joined devices where users identify as AzureAD\displayName.

✓ Save

Cancel

Users to Import

This is where you can select which users you want to import from your Entra ID Tenant into MyQ. You can select from **All users** or **Users from selected groups**. In the latter option, the groups refer to existing user groups in your Entra ID source, you can choose to use these groups, ignore them, or organize them further in MyQ in the **Groups** tab.

Properties

In the **Properties** section, you can map user information from Microsoft Entra ID to the credentials in MyQ. A predefined selection of recommended values is provided. If the predefined value is not used, a manually typed custom attribute can replace it and synchronize a different [user attribute from Entra ID](#).

Property Name	Description	Predefined Attribute/s
Full name	Users' full name.	<code>displayName</code>
Personal number	User identification number.	<code>employeeId</code> or <code>extensionAttribute1</code> to <code>extensionAttribute15</code>
Email	Users' email.	<code>mail</code>
Notes	Relevant notes.	<code>extensionAttribute1</code> to <code>extensionAttribute15</code>
Language	Users preferred language.	<code>preferredLanguage</code>
Department	Users' department.	<code>department</code>

Property Name	Description	Predefined Attribute/s
Alias	An alternative name or username.	displayName , userPrincipalName , upnPrefix , mailNickname , onPremisesSamAccountName , onPremisesSamAccountName@onPremisesDomainName , and extensionAttribute1 to extensionAttribute15
Card	The users' ID card number.	employeeId or extensionAttribute1 to extensionAttribute15
PIN	The users' PIN.	employeeId or extensionAttribute1 to extensionAttribute15
Custom (1)	Custom attribute to assign to other relevant information.	extensionAttribute1 to extensionAttribute15
Custom (2)	Custom attribute to assign to other relevant information.	extensionAttribute1 to extensionAttribute15
Custom (3)	Custom attribute to assign to other relevant information.	extensionAttribute1 to extensionAttribute15

 For the **Alias** property, if the attribute `onPremisesSamAccountName@onPremisesDomainName` is used, the user's Alias after synchronization will be a combination of the user's Microsoft Entra ID attributes `onPremisesSamAccountName` and `onPremisesDomainName` in the format, for example, `user@myq.cz`.

Options

- **Deactivate Missing Users:** this option allows the system to automatically deactivate users in MyQ X who are no longer present in the Microsoft Entra ID source.
- **Add New Users:** when enabled, this feature automatically adds new users found in the Microsoft Entra ID source to MyQ X.
- **Use as authentication server:** if you plan to authenticate users towards Azure using Active Directory credentials and use the Microsoft single-sign-on option, select the **Use as authentication server** option and click **Save**.
- **Pair by the personal number:** check this box if you wish to update users based on their personal number. If the personal number option is checked, during re-synchronization, the system will look for the user by their personal number. If a match is found, the user details will be updated, otherwise, a new user will be created.

 Since MyQ Print Server 10.2 RC 4, the **Pair by the personal number** option is checked by default for all newly created synchronization sources and cannot be changed. Sources created in 10.1 after migration to 10.2 allow editing this option. Pairing Users by personal number is strongly recommended.

- **Ignore Synchronization Source:** this option provides the ability to selectively ignore certain aspects or data from the Microsoft Entra ID source during synchronization.
- **Create normalized alias from Display name:** this option means an additional alias is added to the user on top of those configured in the user attributes section, this alias takes the form of `AzureAD\concatatedDisplayName`. It allows proper recognition of users who print from Entra ID Joined devices.

 If two or more users have the same Full Name synced from Entra ID, a normalized Alias will be created only for the first user. There is no way to distinguish Job owners for this case in the ADD environment since the printer's driver provides only a concatenated user's Name and Surname.

Groups Tab

The **Groups** tab does not specify which user groups to import, but how they should be organized within MyQ. Which user groups are imported is controlled in **Users > Users to import**.

User Synchronization: Microsoft Entra ID

General Users **Groups**

Full synchronization

Select groups: Group-16 Group-17

Import groups under this group:

Ignore groups:

Ignore groups containing string:

Place each string on a new line. Matching is case insensitive.

✓ Save Cancel

The following options are available:

- **Select type of synchronization:** In a synchronization source, you can adjust the level of synchronization on the **Groups** tab. It is possible to select from the following levels:
 - **Full synchronization:** synchronize groups 1:1 as they are in the source, meaning users are both added to and removed from groups as in the source.
 - **Synchronize if not empty:** leave a user in at least one group even after they lose all memberships in the directory.
 - **Add new:** ensure that once a user is assigned to a group in MyQ, they do not lose this membership even after they are removed from a group in the source directory.
- **Select groups:** this allows you to select the groups that exist in your instance of Entra ID which you want to include as groups within MyQ.
- **Import groups under this group:** allows you to select an existing user group in MyQ to use as a parent group for any groups synchronized from this source.
- **Ignore groups:** select what Active Directory groups you do not want to use in this synchronization.
- **Ignore groups containing string:** fulfills the same function as **Ignore groups** allowing you to specify groups to be ignored according to a string they contain.



Group Synchronization - Example Scenario

Administrators have enhanced control over group memberships during Entra ID user synchronization. With the **Select groups** filter option in the Entra ID User Sync source settings, you can specify which group memberships are imported into MyQ without affecting the overall user synchronization process.

Example:

The Entra ID group structure is as follows:

- **All students:** 1,500 users
- **Class1A:** 1,000 users
- **Class1B:** 500 users

MyQ Settings:

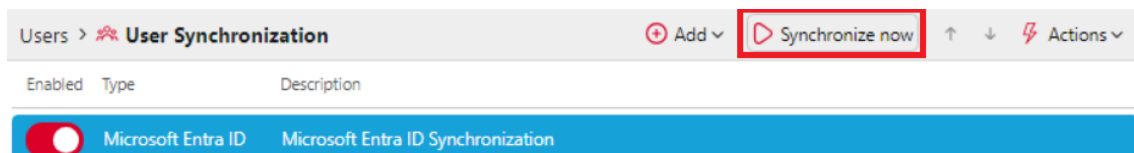
- In the **Users** tab under **Users to import** select **Users from selected groups** and specify the **All students** group to synchronize all 1,500 users.
- In the **Groups** tab under **Select groups**, select **Class1B** only.

Result:

- All 1,500 users are synchronized to MyQ.
- Only the 500 users in **Class1B** have their group membership applied in MyQ.
- The remaining 1,000 users are imported without any group membership.
- Users who are also members of **Class1A** do not have this membership applied in MyQ.

Synchronize Now

Users can be now synchronized by selecting your Microsoft Entra ID source from the list and clicking **Synchronize now**. It is also possible to schedule user synchronization using the [task scheduler](#).



Multi-Tenant Synchronization and Authentication

You can now use multiple Entra ID tenants in MyQ environments to synchronize and authenticate users. This is particularly useful in shared print infrastructure settings, such as those found in the public sector, where multiple organizations manage printers from a single location, while each uses its own Entra ID.

Follow the process as described below but repeat it to set up multiple instances. Ensure that clear and unique naming is given to each tenant, which will allow users to identify which is relevant for their use.

10.6.4 User Synchronization from CSV Files

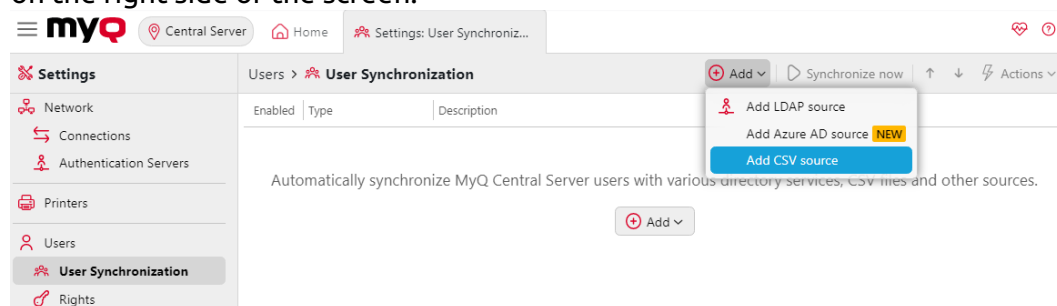
To synchronize users from a CSV file, you have to create a new CSV synchronization on the **User Synchronization** settings tab and on the synchronization properties panel, add the source file and set properties of the synchronization.

After the synchronization is set up, you can either manually run it on the **User Synchronization** settings tab or set it as a regular task on the **Task Scheduler** settings tab.

Creating a new CSV synchronization

To create a new synchronization:

1. On the bar at the top of the **User Synchronization** settings tab, click **Add**, and then click **Add CSV source**. The CSV synchronization properties panel appears on the right side of the screen.



2. **Set up the synchronization:** On the CSV synchronization properties panel, set the path to the **CSV file** and configure the synchronization. For information about the synchronization options, see "CSV synchronization setup options" below.

3. **Save** the setup.

CSV synchronization setup options

These are the CSV synchronization setup options:

- **Enabled:** Here you can enable or disable the synchronization.
- **CSV file:** Here you can set the path to the CSV file on the MyQ server.
- **Encoding:** Select the encoding that is used in the CSV file. The default value depends on the OS settings of the computer where you access the MyQ Web Interface on.
- **Column delimiter in CSV:** Select the delimiter that is used in the CSV file. If you select the **Default** option, MyQ scans for the delimiter set on the **Column delimiter in CSV** drop-down list box on the **General** settings tab.
- **No header line:** This option is *disabled* by default, meaning that the first row of the CSV will be read as a header row and columns will be imported based on their header value. If this option is *enabled*, the CSV should contain no header row, and columns will be imported based on their order (in order of appearance in the CSV File Syntax table below).
- **Import groups under this group:** Here you can select an existing group in MyQ under which you import the groups from the CSV file.
- **Synchronization source:** Here you can specify a different source than the CSV to be marked as the synchronization source by the MyQ system. For example, you can insert an LDAP server domain.
- **Ignore synchronization source:** If you select this option together with the **Deactivate missing users option**, all users that are not in the current synchronization source are deleted.
- **Use authentication server:** If you select this option, an LDAP or Radius server is used for the authentication of the imported users.
- **Authentication server:** Here you can select the LDAP or Radius domain for the user authentication.
- **Deactivate missing users:** If you select this option, MyQ deletes users that are imported from the current synchronization source and that are not in the source anymore. To delete users that were added from different sources, select the **Ignore synchronization source** option together with this option.
- **Add new users:** If you select this option, MyQ adds new users from the current synchronization source.
- **Pair users by personal number:** If you select this option, multiple accounts with a single personal number are paired.
- **Convert user name to lowercase:** If you select this option, all letters in user names are converted to lowercase.
- **Cards/PIN/Groups/Delegates:** In each of the mandatory drop-down boxes, you can select from these synchronization options for the respective parameter (Cards, PIN, Groups):
 - **Do not synchronize:** The value of the respective parameter in MyQ is not changed.
 - **Full synchronization:** The value of the respective parameter in MyQ is always replaced by the value in the CSV file. If the value in the source file is empty, the value in MyQ is erased.
 - **Synchronize if not empty:** If the respective field in the CSV file is not empty, the parameter value in MyQ is replaced by the value in the CSV file.

Otherwise, the parameter value remains unchanged. This is the default setting.

- **Add new:** If the parameter is already set in MyQ, it is not replaced. Only new values are added.

CSV File Syntax

In the table below, you can find information about individual fields of the CSV file.

A single word or a plain number can be put in the CSV fields as they are, while more complex strings, such as full name or email address, have to be bounded by quotes.

Column name	Mandatory	Description
FULLNAME	Yes	Name of the user in double quotation marks, for example " <i>Thomas Pineapple</i> ".
USERNAME_ALIASES	Yes	Login of the user and eventually their aliases. The login should be the same as the user's domain login name, for example <i>Tom</i> . When you import multiple aliases, separate them with commas, for example " <i>Tom,Tommy,Apple</i> ".
EMAIL	No	Email of the user, for example " <i>t.pinapple@domain.com</i> ".
CARDS	No	Number of the user's authentication card/chip. It has to be inserted in the form in which it is read by the card/chip reader, for example <i>7E9700C9</i> .

GROUPS	No	Here you can add user groups. You can import a whole branch of the groups tree structure. The groups on the imported branch have to be separated by vertical bars. If you want to import multiple groups (or groups tree branches), separate them by commas. For example, if you add two branches separated by a comma: "<i>Activities/Outdoor/Swimming,Activities/Outdoor/Birdwatching</i>", MyQ imports a single parent group <i>Activities</i> with a single child group <i>Outdoor</i>, with two child groups <i>Swimming</i> and <i>Birdwatching</i> (<i>Activities>Outdoor>Swimming,Birdwatching</i>). Commas and vertical bars cannot be used in group names as they are used as group delimiters.
CODE	No	The personal number of the user. The ID number must be unique for each user. This parameter is very useful when using multiple sync sources.
SCANSTORAGE	No	The folder or email where the user wants their scans to be sent to, for example "<i>\Users\Tommy</i>".
PIN	No	You can define one or more PINs to be assigned to users within the synchronization process. It is not absolutely necessary, as PINs may also be generated later within the setup of the user account. The PINs should be in the hashed MD5 format, for example <i>14BFA6BB14875E4</i>.
MANAGED_GROUPS	No	You can make the user the manager of a particular group by adding the group or path to the group here in the way in which you would import the group. If you want the user to be a manager of a child group, enter a whole branch ending with this group. For example, enter the branch "<i>Activities/Outdoor/Swimming</i>" to make the user a manager of the <i>Swimming</i> group. If there are no parents of the group in the group structure, enter just the group name, e.g. <i>Activities</i>. Commas and vertical bars cannot be used in group names as they are used as group delimiters.

AUTHSERVER	No	In this field you may define the domain for user authentication, for example <i>"testAD.local"</i> .
PHONE	No	The user's phone number, for example <i>080008020</i> .
LANG	No	Default language of the user, for example <i>en</i> .
PWD	No	If you want to use the MyQ password, insert the password in the hashed MD5 format, for example <i>18BFA6BB14875E8</i> . If you are using a different authentication server (i.e. LDAP server), you can leave it empty.
EXTID	No	EXTID is an internal MyQ parameter. This field has to be left empty.
DELEGATES	No	For each user, you can import any number of delegates. If you import multiple delegates, separate them with commas, for example <i>"Carol,Kohei,Eliot"</i> .
ALTERNATEEMAILS	No	Comma separated list of the user's alternate emails.
DEPARTMENT	No	User's department, for example <i>Marketing</i> .
CUSTOM1	No	User's "Custom 1" field from profile.
CUSTOM2	No	User's "Custom 2" field from profile.
CUSTOM3	No	User's "Custom 3" field from profile.

"FULLNAME"; "USERNAME_ALIASES"; "EMAIL"; "CARDS"; "GROUPS"; "CODE";
 "SCANSTORAGE"; "PIN"; "MANAGED_GROUPS"; "AUTHSERVER"; "PHONE";
 "LANG"; "PWD"; "EXTID"; "DELEGATES"

"Thomas Pineapple"; "Tom, Tommy, Apple"; "t.pineapple@domain.com";
 7E9700C9;"Imported Users, Activities|Outdoor|Swimming,
 Activities|Outdoor|Birdwatching";22212;"\\Users\Tomy";
 14BFA6BB14875E4;Birdwatching;testAD.local;080008020;en; 18BFA6BB14875E8; ;"Carol,Kohei,Eliot";

10.6.5 User Synchronization from Entra ID (Azure AD) with SLDAP

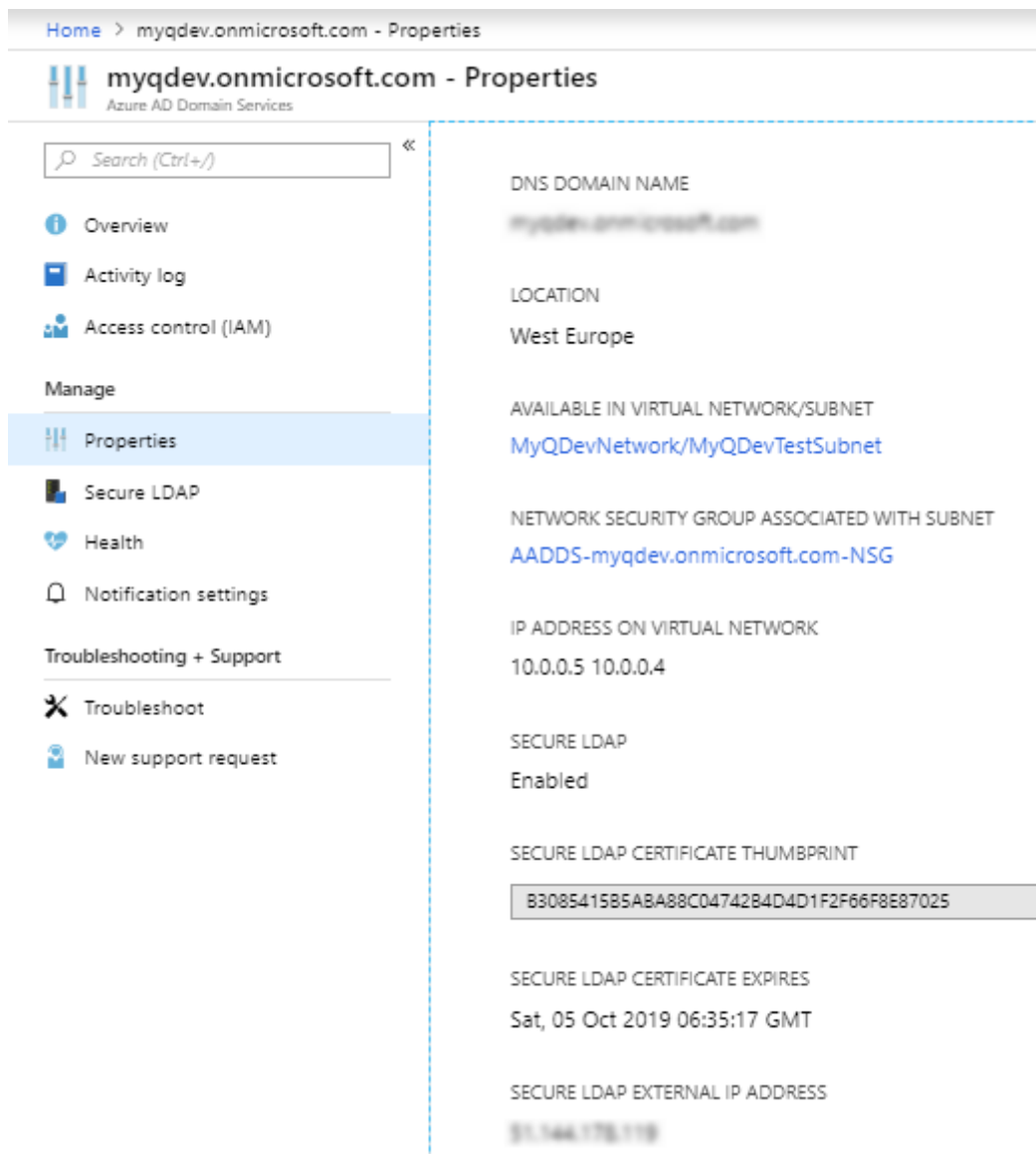
Entra ID (formerly Azure AD) with SLDAP is a service accessed from the Microsoft Azure Portal. It has to be enabled and configured in Azure Active Directory Domain Services.

The activation and setup of the service are described in the following Microsoft guides:

- To enable and configure Azure Active Directory Domain Services:
<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-create-instance>
- Configure Entra ID Domain Servers to use SLDAP:
<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-configure-ldaps>

After you activate the Entra ID, you need to add it to MyQ and set up the synchronization in the standard way (see [User Import and synchronization](#)). When setting up the **Authentication server** in MyQ, you need to make sure that the LDAP server parameters are set to the following values:

- **Domain** = *DNS DOMAIN NAME* of the Entra ID Domain
- **Security**: *SSL*
- **Server** = *SECURE LDAP EXTERNAL IP ADDRESS* of the Entra ID Domain



Home > myqdev.onmicrosoft.com - Properties

myqdev.onmicrosoft.com - Properties

Azure AD Domain Services

Search (Ctrl+J)

- Overview
- Activity log
- Access control (IAM)
- Manage
 - Properties**
 - Secure LDAP
 - Health
 - Notification settings
- Troubleshooting + Support
 - Troubleshoot
 - New support request

DNS DOMAIN NAME
myqdev.onmicrosoft.com

LOCATION
West Europe

AVAILABLE IN VIRTUAL NETWORK/SUBNET
MyQDevNetwork/MyQDevTestSubnet

NETWORK SECURITY GROUP ASSOCIATED WITH SUBNET
AADDs-myqdev.onmicrosoft.com-NSG

IP ADDRESS ON VIRTUAL NETWORK
10.0.0.5 10.0.0.4

SECURE LDAP
Enabled

SECURE LDAP CERTIFICATE THUMBPRINT
B3085415B5ABA88C04742B4D4D1F2F66F8E87025

SECURE LDAP CERTIFICATE EXPIRES
Sat, 05 Oct 2019 06:35:17 GMT

SECURE LDAP EXTERNAL IP ADDRESS
51.144.178.118

10.6.6 User Synchronization from Google Workspace

Google Workspace (previously named G-Suite), a set of cloud computing, productivity and collaboration tools, software and products developed by Google Cloud, can be used with MyQ Central Server (versions 8.0+). For setting up the connection to MyQ follow the short procedure below.

- Go to <https://support.google.com/a/answer/9048541?hl=en> to configure your Google Workspace Environment for working with MyQ as an LDAP Client.
 - Turn service status on or off
 - Edit access permissions
- Go to <https://support.google.com/a/answer/9048541#generate-certificateauthentication> to get a private key and a certificate.
 - Generate certificate authentication

- Generate access credentials.
The downloaded file is a **zip* file containing the private key and the certificate you need for connecting to MyQ.
- After the above procedure, you need to set up the user synchronization from Google Workspace in the standard way. When setting up the **Authentication server** in MyQ, you need to make sure that the LDAP server parameters are set to the following values:
 - **Domain** - add your Google Workspace domain; the name of the domain component must be used (for example, **dc=example,dc=com**)
 - **Type** - select *Google Workspace* from the drop-down
 - **Certificate** - click **Add** and browse to upload the downloaded certificate file (*.crt*)
 - **Private key** - click **Add** and browse to upload the downloaded private key file (*.key*)

 **LDAP Server: dc=example,dc=com** ×

Domain: *

Type: *

Security:

Server: ×

+ Add

Test

▼ **Certificate**

Google Workspace server requires a client certificate. [How to generate it](#)

Certificate:  Google_2026_10_03_38620.crt (1.22 KB)

Private key:  Google_2026_10_03_38620.key (1.66 KB)

✓ Save Cancel

 Find out more about Google Workspace's [Secure LDAP schema](#).

10.6.7 Using External Authentication Servers

In addition to the internal MyQ authentication methods (password, PIN or ID card), you can use two types of external authentication servers: LDAP and Radius.

With the two external methods, MyQ does not use the internal MyQ PIN or password for user authentication, but instead authenticates users against an LDAP or Radius server. After the user enters their credentials during the authentication, the credentials are sent to be verified directly by the external server. If there is no online connection with the LDAP or Radius server, users cannot log in.

To enable this method of authentication, you have to take two steps:

1. register the external authentication servers in MyQ
2. select to use them for user authentication

To register external authentication servers in MyQ, see [Authentication Servers Settings](#).

Selecting to use the registered external authentication servers for user authentication, can be done either automatically during the user import from an LDAP server or a CSV file, or manually on the properties panels of individual users.

Automatically selecting the external authentication option

Importing users from a CSV file

When you import users from a CSV file, you have two options of selecting the authentication server for the users:

1. You can select the **Use authentication server** option and select the server during the synchronization setup on the synchronization properties panel.
2. You can specify the **Authentication server** for a particular user in the **AUTHSERVER** field of the CSV file. If the field is not empty, its value has priority over the value selected on the properties panel.

For more information about importing users from CSV files, see [User synchronization from CSV files](#).

Importing users from an LDAP server

During the users import from an LDAP server, you can select the **Use authentication server option**, to use the current synchronization source server for users authentication. For information about importing users from LDAP servers, see [User synchronization from LDAP servers](#).

Unlike the **Use authentication server** setting for the import from a CSV file, which allows you to select the authentication server, the **Use authentication server** setting here gives you a single option — users will be authenticated against the LDAP server where they are imported from.

Manually selecting the external authentication option

To manually select the external authentication option

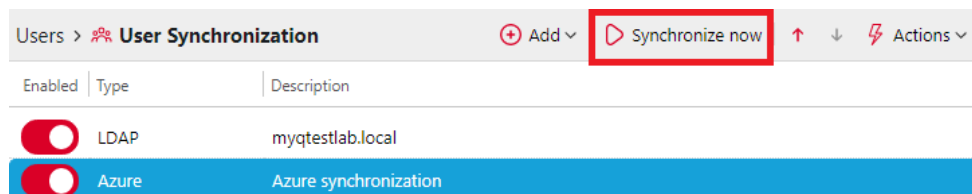
1. Open the **Users** main tab and double-click the user. The user's properties panel opens on the right side of the screen.
2. On the panel, select the **Use authentication server** option. The Authentication server setting becomes available.
3. On the Authentication server drop-down, select the server you want to use, and then click **Save** at the bottom of the panel.

10.6.8 Manual and Scheduled Synchronization Run

The synchronization can be manually run on the **User Synchronization** tab of the MyQ Web Interface, or it can be set as a scheduled task on the **Task Scheduler** tab.

Manual Synchronization Run

On the **User Synchronization** settings tab, select the synchronizations that you want to run, and then click **Synchronize now** on the bar at the top of the tab.



The **Synchronize Now** button will start the synchronization, unless another one is already running. In this case, an error message will be displayed.

Upon start, the **Synchronization Results** panel opens and displays the operation log live. The log tail is automatically monitored when the panel is scrolled to the bottom. A spinning wheel at the bottom of the log indicates that synchronization is in progress.

The **Cancel** button cancels the process. It may take some time until the synchronization is actually canceled.

The **Save** button downloads the synchronization log.



Synchronization Results - Running

```

GroupRoot12|SubGroupE: created
GroupRoot12|SubGroupE|SubGroup7: created
Group 3524: created
GroupRoot28|SubGroupW: created
GroupRoot28|SubGroupW|SubGroup4: created
Group 709: created
GroupRoot34|SubGroupJ: created
GroupRoot34|SubGroupJ|SubGroup0: created
Group 3751: created
GroupRoot2|SubGroupG|SubGroup2: created
Group 2977: created
GroupRoot18|SubGroupJ: created
GroupRoot18|SubGroupJ|SubGroup9: created
Group 3123: created
GroupRoot43|SubGroupL: created
GroupRoot43|SubGroupL|SubGroup8: created
Group 3825: created
GroupRoot25|SubGroupA|SubGroup0: created
Group 4304: created
GroupRoot26|SubGroupG: created
GroupRoot26|SubGroupG|SubGroup1: created
Group 208: created
GroupRoot25|SubGroupL: created
GroupRoot25|SubGroupL|SubGroup7: created
Group 72: created
GroupRoot5|SubGroupN: created
GroupRoot5|SubGroupN|SubGroup7: created
Group 3693: created
GroupRoot3|SubGroupQ: created
GroupRoot3|SubGroupQ|SubGroup1: created
Group 4353: created
GroupRoot38|SubGroupC: created
GroupRoot38|SubGroupC|SubGroup0: created

```

Scheduled Synchronization Run

On the **Task scheduler** settings tab, you can setup a scheduled run of the synchronization. For more information about this option, see [Task scheduler](#).

10.7 Users Settings

In the **Users** settings tab (**MyQ > Settings > Users**), the MyQ administrator can manage MyQ users **General** and **Lockout** settings. In the **User Authentication** tab, you can access MyQ users **PIN** options, the MyQ accounts **Password complexity**, and the MyQ **Account lockout** options.

10.7.1 General Section

The screenshot shows the MyQ web interface. At the top, there are tabs for 'Central Server', 'Home', and 'Settings: Users'. The left sidebar contains a 'Settings' menu with options: License, General, Personalization, Task Scheduler, Network, Connections, Authentication Servers, and Printers. The main content area is titled 'Users' and shows the 'General' section. It contains four settings, all with checkboxes that are currently unchecked:

- Enable Sign in with Windows Authentication:** Users are recognized from their Windows account and can sign in to MyQ Central Server without using a password.
- Enable user profile editing:** If enabled, user can change these properties: Full name, E-mail. Properties which can be changed always: Password, Default language.
- Show more info about user profile:** Widget 'User profile' will contain more information.
- Enable deleting all ID cards:**

- **Enable Sign in with Windows Authentication** - enabling this option means those using a Windows account correctly synchronized with MyQ will not need to enter their MyQ login details to access the web interface. You can learn more about Integrated Windows Authentication [here](#).
- **Enable user profile editing** - By default, all users can change their password and their default language on their MyQ Web accounts and on some embedded terminals, while the rest of their properties can be changed only by the administrator. If the **Enable user profile editing** option is enabled, users can also change their full name and email, and select their delegates.
- **Show more info about user profile** - If enabled, the User profile widget on the MyQ web interface will contain more information.
- **Enable deleting all ID cards** - If enabled, all ID cards can be deleted.

10.7.2 Account lockout section

In this section, the MyQ administrator can set the number of failed login **Attempts before lockout**, and the **Lockout time** (in minutes).

The screenshot shows the 'Account lockout' section of the MyQ interface. It contains two settings, both with asterisks indicating they are required:

- Attempts before lockout:** A text input field containing the value '5'.
- Lockout time:** A text input field containing the value '15', followed by the text 'minutes'.

10.7.3 PIN section

myQ Home Settings: User Authentication...

Settings

- Server Type
- License
- General
- Personalization
- Task Scheduler
- Network
 - Connections
 - SNMP
 - Authentication Servers
- Printers & Terminals
 - Configuration Profiles
 - Printer Discovery
 - Terminal Actions
 - Events
 - Event Actions
- MyQ Desktop Client
- Users**
 - Policies
 - User Synchronization
 - User Authentication**
 - Rights
- Accounting
 - Credit
 - Quota
 - Projects
 - Price Lists

Users > User Authentication

PIN

User can change PIN: ☒

Minimal PIN length: * 4

Send new PIN via email: ☐

Generate PIN for users created by synchronization or manual input: ☐ 'Send new PIN via email' will be automatically checked.

Temporary PINs

Generate PINs as temporary: ☒

Only for users in groups: * All users

Validity of temporary PINs: * 24 hours

Email with a new PIN

Subject: * MyQ: Your new PIN

Message: * Your new MyQ PIN is: %pin%
%validity%
Please contact the administrator at %admin% in case of further requests

Parameters: %pin%, %validity%, %username%, %realname%, %admin%.

[Revert values](#)

Email with the PIN reset code

Subject: * MyQ: PIN reset code

Message: * Hello %realname%,
Your PIN reset code is: %code%
Go to the MyQ website, click "Lost PIN" and enter the code.
Your MyQ
Please contact the administrator at %admin% in case of further requests

Parameters: %code%, %username%, %realname%, %admin%.

[Revert values](#)

With the **User can change PIN** option selected, the users can generate a new PIN on their account on the MyQ Web User interface, by clicking **Generate PIN** on the **Home** screen of their user account.

The **Minimal PIN length** option determines the mandatory minimum PIN length. The number can be set between 4 and 16. If the administrator creates the PIN manually, it cannot be shorter than the value set in this field. If the PIN is generated by the system, it cannot be shorter than the value in this field, and also cannot be shorter than the minimal value enforced by the number of users, described below.

The required minimal PIN length that depends on the number of MyQ users is:

- < 1000 — 4-digit PIN is required
- 1000 - 10 000 — 5-digit PIN is required
- 10 000 - 100 000 — 6-digit PIN is required

The required minimal length lowers the chance of randomly guessing the PIN. In addition, an algorithm disallows any PIN with a constant delta from one digit to the next. For example, the PIN 1111 has a constant delta of 0,0,0, so it is excluded from the automatic PIN generation process and will not be allowed as a manually created PIN.

If the administrator increases the **Minimal PIN length** value, a pop-up will prompt them to generate new PINs for all the active users. If the administrator chooses to

generate new PINs, the old PINs will be deleted and new PINs will be automatically sent via email to all the active users. Otherwise, the old, potentially shorter PINs will be kept.

With the **Generate PIN for users created in synchronization or manual input** option selected:

- A new PIN is generated for new, manually created users.
 - A manually created user without an email address will not receive the new PIN via email.
- During **User synchronization**, a new PIN is generated for every user that does not already have a PIN.
 - PINs are generated only for users with an email address. Users without an email address are skipped.

With the **Send new PIN via email** option selected, users are sent an email informing them about the new PIN every time a new PIN is generated. This is automatically checked if the above option (**Generate PIN for users created in synchronization or manual input**) is selected.

There are also email templates you can use for informing the users about their new PIN (**Email with a new PIN**) or for providing them with a reset code in case of a lost/forgotten PIN (**Email with the PIN reset code**). The template is editable and the values can be reset to their defaults if needed, by clicking **Revert values**.

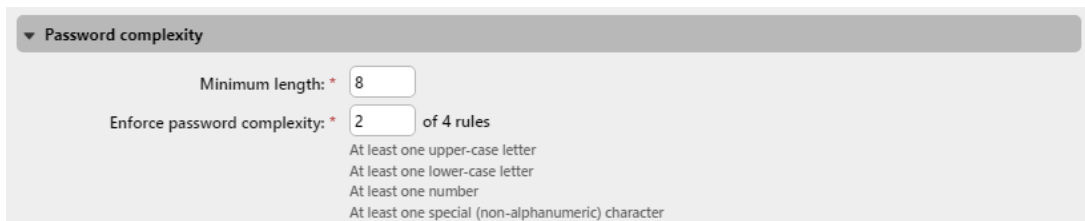
Temporary PIN section

With the option to **Generate PINs as temporary** selected for the user groups in the **Only for users in groups** field, the automatically generated PINs are always temporary. You can set the **Validity of temporary PINs** in hours (24 hours by default). Find out more about utilizing temporary PINs [here](#).

 When a Site that doesn't support temporary PINs (Print Server versions older than 10.2) is connected to Central Server 10.2, it's still possible to create temporary PINs on Central Server, but they will not be synchronized with Site. Persistent PINs still will be synchronized.

10.7.4 Password Complexity section

In this section, the MyQ administrator manages the password complexity of MyQ users accounts.



▼ Password complexity

Minimum length: * 8

Enforce password complexity: * 2 of 4 rules

At least one upper-case letter
 At least one lower-case letter
 At least one number
 At least one special (non-alphanumeric) character

- **Minimum length** - set the minimum character length for the password, in range 1-100 (8 by default).

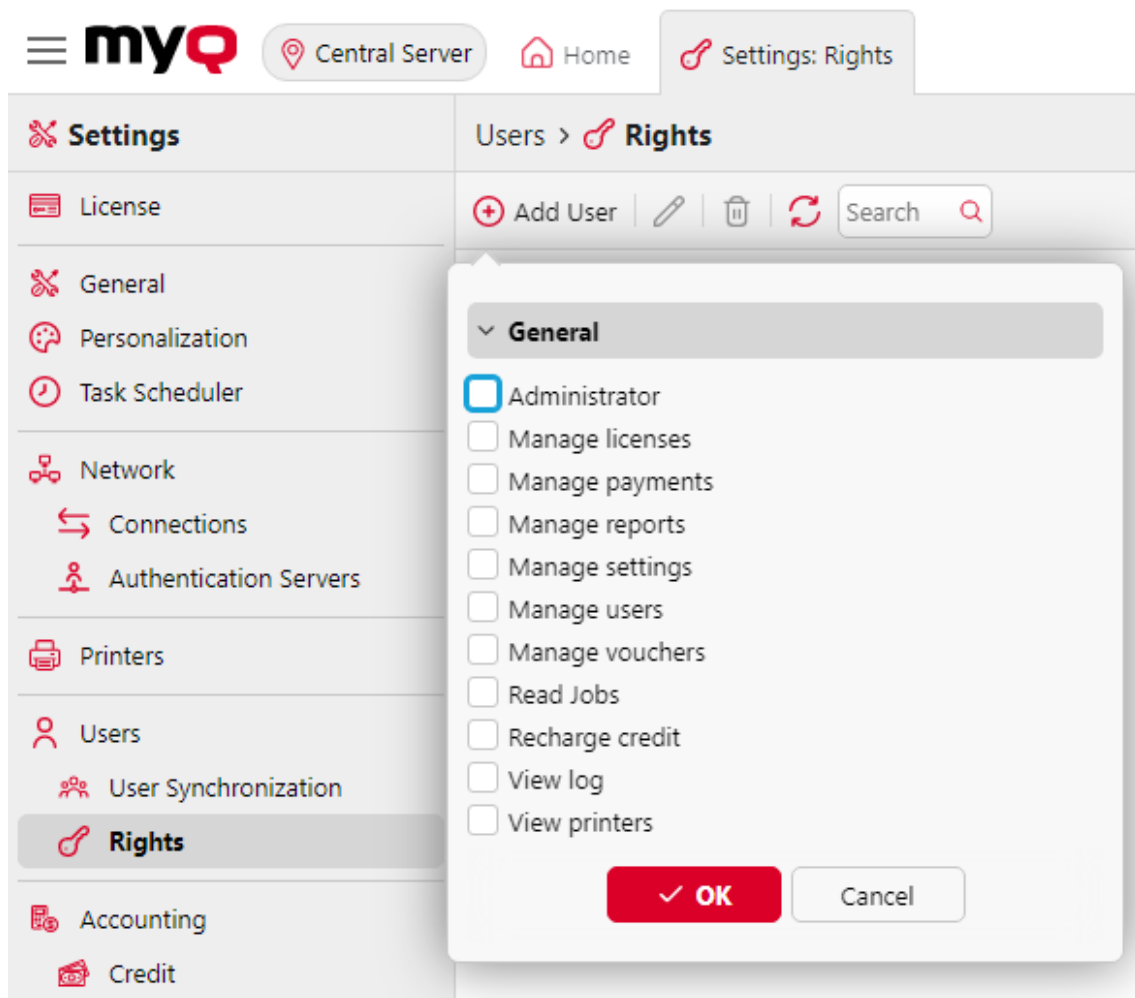
- **Enforce password complexity** - set how many of the four password complexity rules are to be enforced (2 by default):
 - At least one upper-case letter
 - At least one lower-case letter
 - At least one number
 - At least one special (non-alphanumeric) character

10.8 Rights

On the **Rights** settings tab, you can provide users or groups of users with administrator rights or provide them with rights to run one or more of the MyQ agendas: they can perform actions, change settings or see information that are inaccessible under a standard user account. On the tab, you can add users or groups and provide them with the rights.

To add a new user or a group of users to the list on the **Rights** settings tab:

1. On the **Rights** settings tab, click **+Add User**. The Select user or group dialog box appears.
2. In the dialog box, select the user (or group) and click **OK**.
3. Select the user (or group) rights.
4. Click **OK**. The user (or group) appears on the list on the **Rights** settings tab.



To edit a user's rights:

Double-click the user (or the group) on the list of users and groups on the **Rights** settings tab. The panel appears on the left side of the screen.

In the user rights panel, under the **General** section, you can change the user's rights. These rights are described below:

- **Administrator** - The user is provided with administrator (*admin) rights.
- **Manage licenses** - The user can view and manage MyQ licenses on the **License** settings tab.
- **Manage payments** - The user gets access to the **Payments** main tab.
- **Manage reports** - The user can manage all reports.
- **Manage settings** - The user gets access to management of all settings on the **Settings** tab of the MyQ Web interface except for the settings on the **Rights** tab.
- **Manage users** - The user gets access to the **Users** main tab, the **Users** settings tab and the **Policies** settings tab, can add users and change their settings and rights. The user also gets access to the **Accounting** settings tab, but cannot

change the settings. Access to the **Credit** settings tab is granted, but the user is only allowed to change Users and Groups.

- **Manage vouchers** - The user can get access to the **Voucher Batches** main tab.
- **Read Jobs** - The user can see other users' jobs.
- **Recharge credit** - The user gets access to the **Recharge credit** main tab.
- **View log** - The user can view the MyQ log.
- **View printers** - The user gets access to the **Printers** main tab, to monitor printers.
- **Delete Cards** - If granted, the user has the **Delete all ID cards** button available on their User profile widget in the MyQ web UI and they are able to delete all their ID cards.

11 Credit

With the credit accounting feature activated, users can copy, print, and scan only if they have enough credit on their account in MyQ. Printing is allowed only for print jobs that do not exceed the credit, and copying is terminated immediately after the credit is exceeded. The credit system can be restricted to selected users and groups.

Users can view the current amount of credit on their accounts on the MyQ Web Interface and in the MyQ mobile application. If a printing device is equipped with an embedded terminal or a reader with an LCD display, the logged users check the current state of their credit there and are allowed to select only those jobs that do not exceed their credit.

Based on the setup and properties of the printing environment, a variety of recharge methods may be employed. The MyQ administrator can manage the credit on the MyQ Web Interface, and also provide the users with the option to recharge the credit themselves on embedded terminals, on recharging terminals, in the MyQ mobile application, via recharging vouchers, or via a third-party payment method.

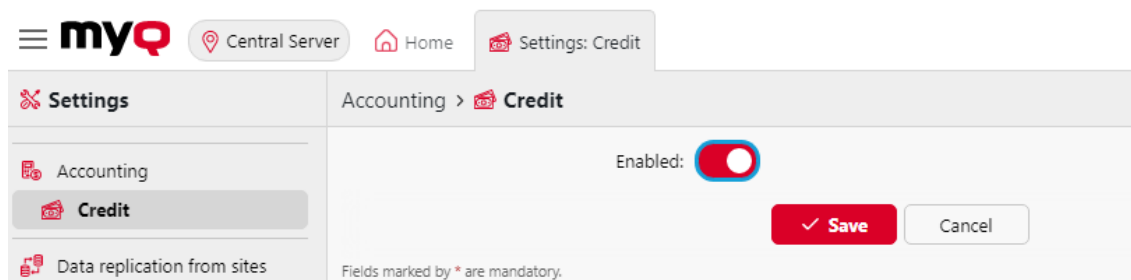
The MyQ Administrator (and authorized MyQ users) can also reset the credit to a specific amount on the MyQ Web Interface.

11.1 Activation and Setup

The activation and setup of credit accounting is managed on the **Credit** settings tab (**MyQ, Settings, Credit**).

To set up credit accounting:

On the **Credit** settings tab, set credit accounting to **Enabled** and click **Save**:



Activate credit for a user or for a group of users:

- Under **Users and Groups**, click **+Add item**. A new item appears on the list of users and groups on the **Credit** settings tab. Select a **Name** (user or group) from the drop-down.
- Click **OK** to save the settings.

Users and Groups + Add item Edit Trash Refresh

Name

+ Managers Name

OK Cancel

Enable/disable methods of payment for credit recharge

Available payment methods:

- External Payment Providers
- PayPal
- SnapScan
- TouchNet uPay
- Voucher
- GP webpay

To enable any of these options (if disabled), select it in the **Payment providers** section, and then click **Enabled** on the bar at the top of the section (or right-click the item, and then click **Enabled** on the shortcut menu).

⚙️ Payment providers Edit ● Enabled		
Enabled	Name	Type
☐ Disabled	CASHNet	Credit recharge
☒ Enabled	External Payment Providers	Credit recharge
☐ Disabled	PayPal	Credit recharge
☐ Disabled	SnapScan	Credit recharge
☐ Disabled	TouchNet uPay	Credit recharge
☒ Enabled	Voucher	Credit recharge
☐ Disabled	WebPay	Credit recharge

11.2 Manual Credit Recharge

The administrator (and users authorized to recharge credit) can manually recharge the credit of each user to a specific value. This can be done either on the **Credit Statement** main tab, or on the **Users** main tab in the MyQ Web administrator interface.

On the **Credit Statement tab**, you first open the credit recharge action, and subsequently select the users and groups to recharge credit.

On the **Users tab**, first select the users or group, and then recharge their credit.

Users' credit can be reduced by entering a negative number in the recharge credit dialog box. By entering *-100*, the credit is decreased by 100.

11.2.1 Providing users with rights to recharge credit

By default, the only person who can recharge credit is the administrator. However, the administrator can authorize a MyQ user to recharge credit as well. The user needs to be provided with the rights to access the credit settings and to recharge credit. This is done on the **Rights** settings tab of the MyQ Web Interface.

To authorize a user to recharge credit on the **Credit Statement** tab, you need to provide them with the right to **Recharge credit**.

To authorize a user to recharge credit on the **Users** tab, you need to provide them with the right to **Recharge credit**, and the right to **Manage Users**.

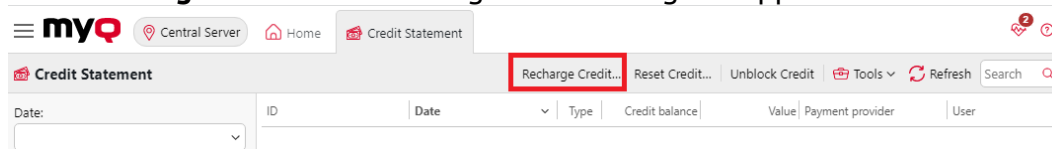
The authorized user can then recharge credit on their MyQ Web interface in the same way as the MyQ administrator.

11.2.2 Recharging credit on the Credit Statement tab

On the **Credit Statement** tab, you can overview the changes in the credit balance of MyQ users, and also recharge credit to users and groups. To open the tab on the MyQ Web administrator interface, go to **MyQ, Credit Statement**.

To recharge credit to users or groups:

1. Click **Recharge Credit**. The Recharge Credit dialog box appears on the tab.



2. In the dialog box, either **Enter the card ID** of a user card, or select the **User or group** to recharge the credit to, then **Enter amount** to be recharged, and lastly click **Recharge credit**.

You can also **Reset Credit** and **Unblock Credit** to users or groups, by clicking the relevant button, selecting the user or group, and the credit amount.

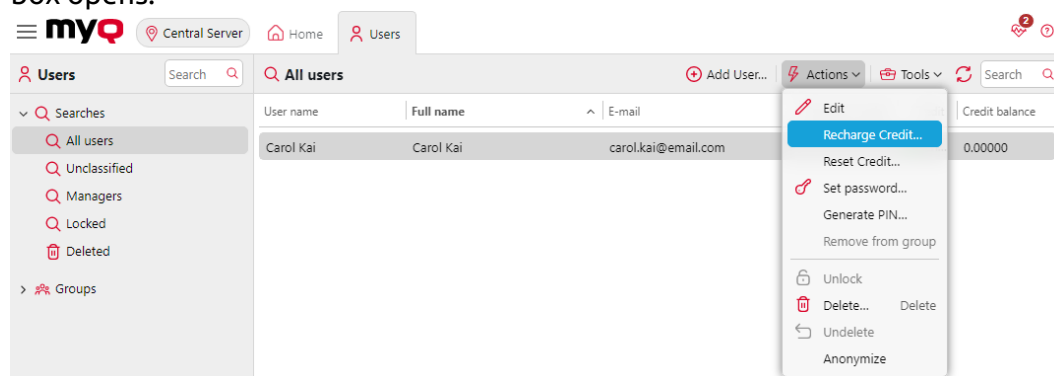
Depending on the administrator and device settings, when the server blocks credit on the account, it temporarily decreases the available balance until the user session finishes. This prevents spending the same credit multiple times resulting in a negative balance. Credit may also be blocked when there is a server or account failure while the user's session is active.

11.2.3 Recharging credit on the Users main tab

To open the **Users** main tab on the MyQ Web administrator interface, go to **MyQ, Users**.

To recharge credit to selected users:

1. Select the users.
2. Click **Actions**.
3. Click **Recharge Credit** in the **Actions** drop-down. The Recharge Credit dialog box opens.

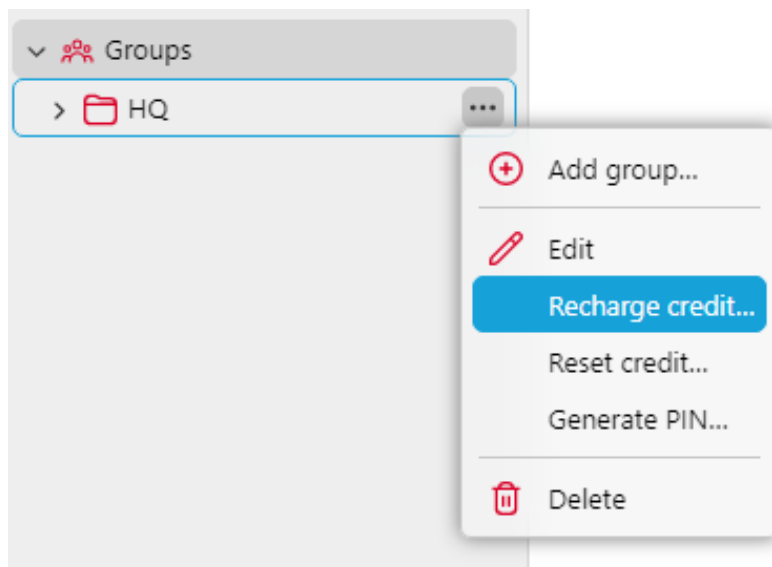


4. **Enter amount** to be recharged, and then click **Recharge credit**. The credit is increased by the specified amount.

The 'Recharge credit' dialog box is shown. It has a title bar with a close button. Inside, there is a 'User or group:' label followed by a dropdown menu showing 'Carol Kai'. Below that is an 'Enter amount: *' label followed by a text input field containing '50'. A note below the input field says 'Credit can be decreased by using a negative number.' At the bottom, there are two buttons: a red button with a checkmark and the text 'Recharge credit', and a white button with the text 'Cancel'. At the very bottom, a small note says 'Fields marked by * are mandatory.'

To recharge credit to a group of users:

1. In the panel on the left side of the **Users** main tab, right-click the group, and select **Recharge credit**. The Recharge Credit dialog box appears.



2. In the dialog box, **Enter amount** to be recharged and click **Recharge Credit**. The credit is increased by the specified amount.

11.3 Recharging Credit via PayPal

If you have a PayPal Business account, you can let users recharge credit with their PayPal accounts from the MyQ Web Interface.

- Users should always send payments in the currency that is set on the MyQ server. Payments in other currencies require approval by the PayPal account admin, and credit must be added in MyQ manually.

11.3.1 Setting up PayPal Payments

To integrate PayPal with MyQ, you first create a new App in your organization's PayPal Business account. Then you set up PayPal as a payment option in the MyQ server settings.

Create a new App in the PayPal Developer Environment

1. Log in to the PayPal developer portal (<https://developer.paypal.com/>) with your PayPal Business account.
2. On the **Dashboard**, under **MyApps & Credentials**, create a new REST API app.
3. In the App properties, select **Live** and remember (copy) the app **Client ID** and **Secret**. MyQ uses this information to register your PayPal account.

Set up PayPal Payments in MyQ

1. Go to **MyQ, Settings, Credit**.
2. Under **Payment providers**, double-click the **PayPal** payment provider. The **PayPal** properties panel opens.

3. Type the minimum amount that users must pay when they buy credit.
4. Enter the **Client ID** and **Secret** (Security key) of your PayPal App.

The image shows two side-by-side screenshots. The left screenshot is a table titled 'LIVE API CREDENTIALS' with columns 'Created' and 'Secret'. It lists a PayPal account with a 'Client ID' and a 'Secret' (Security key). The right screenshot is a 'PayPal' configuration dialog box. It has fields for 'Currency' (USD), 'Minimal amount' (1.000), 'Client ID', 'Security key', and 'Mode' (LIVE). Green arrows point from the 'Client ID' and 'Secret' in the table to the corresponding fields in the dialog box. The dialog box also has 'Save' and 'Cancel' buttons.

5. (Optional, recommended) To verify your integration with a PayPal sandbox account, set the **Mode** to *SANDBOX*.
6. To go live with PayPal integration, set **Mode** to *LIVE*, and click **Save**.

11.3.2 Recharge User Credit with PayPal

To update their credit with PayPal, the user completes these steps in the MyQ Web Interface.

1. Log in to the MyQ Web Interface.
2. Go to **Credit** and click **Recharge Credit**.
3. Select **PayPal** as the payment provider and type how much credit to recharge.
4. Click **Recharge Credit**.

PayPal opens in a new window where the user completes the payment. PayPal then redirects the user back to MyQ, where a **Payment successful** dialog box appears.

 If you encounter errors with payment provider integration:

- **Check DNS settings** - Ensure your hostname resolves correctly from external DNS servers.
- **Verify redirection is not blocked** - Ensure that redirects between the payment provider and your server are not being blocked by firewalls, security settings, or network configurations.

11.4 Recharging Credit via SnapScan

With the **SnapScan** app, users can pay for their MyQ credit via a QR code displayed in the app on their mobile phones.

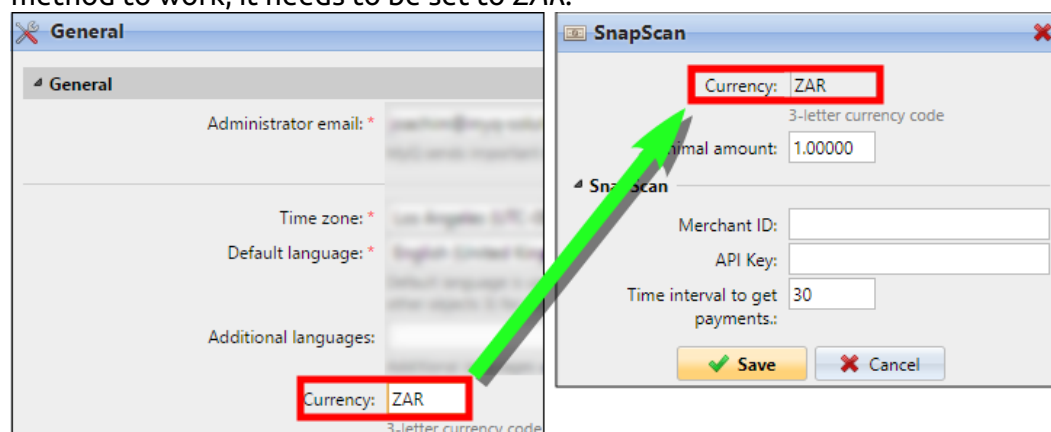
To be able to connect **SnapScan** to MyQ, you need to create a **Merchant SnapScan Account** and obtain the **Merchant Account API**. Within the setup of the connection on the MyQ Web Interface, you must enter the **Merchant ID** and the **API key** of the account.

As **SnapScan** is a South African service, users need to use a phone with a South African Mobile number (+27) to be able to scan the QR code and pay for the credit.

11.4.1 Setting up the SnapScan payment option

To set up the SnapScan payment option on the MyQ Web Interface:

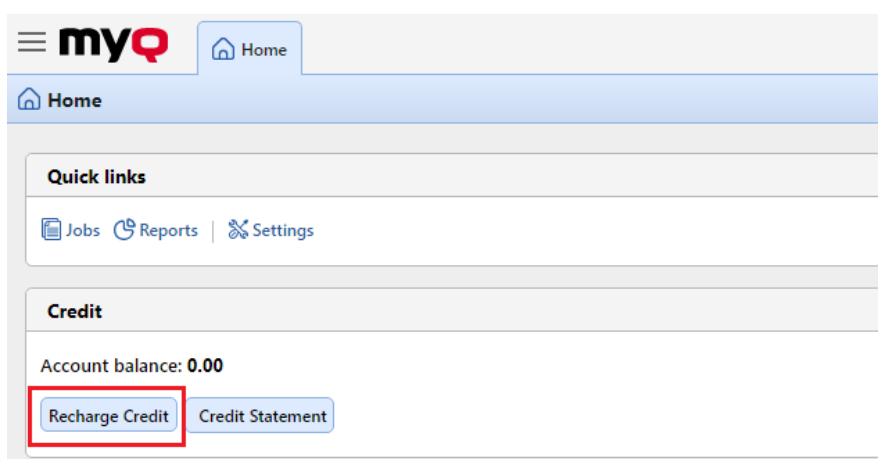
1. Open the **Credit** settings tab (**MyQ, Settings, Credit**).
2. On the tab, under **Payment providers**, double-click the **SnapScan** payment provider. The **SnapScan** properties panel opens on the right side of the tab.
3. The value of the **Currency** setting corresponds to the currency set on the **General** settings tab of the MyQ Web Interface. For the SnapScan payment method to work, it needs to be set to **ZAR**.



4. Type the **Minimal amount** of money that has to be paid when a user buys the credit.
5. Enter the **Merchant ID**(Company Name) and the **API key** provided by SnapScan.
6. Set the **Time interval to get payments** (in seconds), and click **Save**. The **Time interval to get payments** setting limits the time for the recharge action; if MyQ does not receive confirmation of the payment within the interval, the credit recharge is canceled. If the payment is successful but MyQ does not receive the response within the time limit, the user has to contact the MyQ administrator, who can manually recharge the credit.

11.4.2 Recharging credit via SnapScan on the user's account on the MyQ Web Interface

First of all, the user needs to log in to their account on the MyQ Web Interface. To recharge the credit there, the user has to click **Recharge credit** under **Credit**. The Recharge credit dialog appears.



In the dialog box, the user has to select the **SnapScan** payment provider, **enter the amount** of credit that they want to buy, and then click **Recharge Credit**.

A window with the SnapScan payment options opens in the web browser; the rest of the steps correspond to the standard SnapScan payment process.

After the payment is successfully sent to MyQ, the **Payment successful** dialog box appears.

- SnapScan tries to connect to the MyQ server via the hostname or IP address that is set on the **Network** settings tab of the MyQ Web Interface. In case a hostname is set on the tab and paying users receive the "*This site can't be reached / XYZ's server DNS address could not be found. / DNS_PROBE_FINISHED_NXDOMAIN*" message, try to replace the hostname with the IP address of your server.

11.5 Recharging Credit via TouchNet uPay

With partner driven recurring payments, the TouchNet Ready Partner application is the recurring engine controlling when payments take place, as well as the amount of each payment. The TouchNet Ready Partner's application links the user to the uPay payment pages where the user enters their payment information. This can be either a credit card or a bank account. This solution is widely used on American campuses for making payments.

11.5.1 Setting up TouchNet uPay

To use this option in MyQ you must be a partner of TouchNet.

MyQ only supports SSL, so your MyQ application must use a secure port. The default is **8093**.

You also need to copy the following information **Client ID**, **API Key** and **uPay Site ID**.

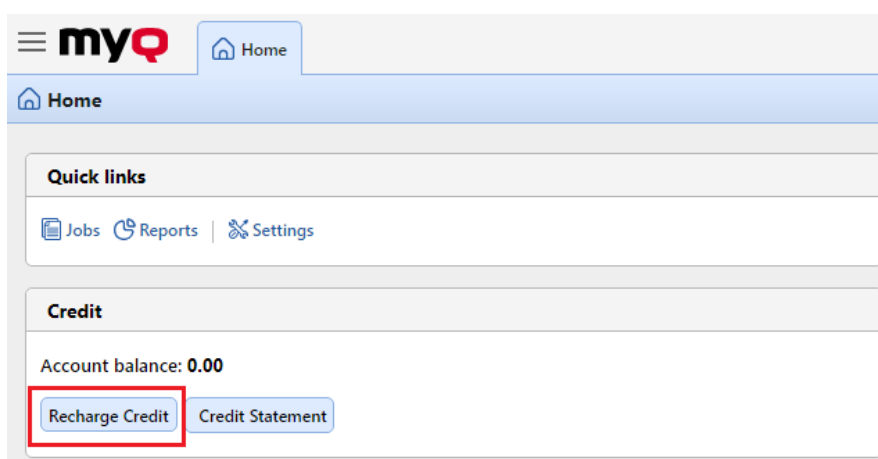
To setup TouchNet uPay in MyQ:

1. Open the **Credit** settings tab (**MyQ, Settings, Credit**).

2. On the tab, under **Payment providers**, double-click the **TouchNet uPay** payment provider. The **TouchNet uPay** properties panel opens on the right side of the tab.
3. The value of the **Currency** setting corresponds to the currency set on the **General** settings tab on the MyQ Web Interface. TouchNet uPay uses USD as currency.
4. Type the **Minimal amount** that users will have to pay when they buy credit. Leaving it blank will accept every payment.
5. Enter the information you got from TouchNet into the mandatory fields **Client ID**, **API Key** and **uPay Site ID**.
6. Use **TEST** as **Mode** when you are not yet in production, otherwise use **PRODUCTION**.
7. Click **Save** to store your settings.

11.5.2 Recharging credit via TouchNet uPay on the user's account on the MyQ Web Interface

First of all, the user needs to log in to their account on the MyQ Web Interface. To recharge the credit there, the user has to click **Recharge credit** under **Credit**. The Recharge credit dialog appears.



In the dialog box, the user has to select the **TouchNet uPay** payment provider, enter the amount of credit that they want to buy, and then click **Recharge Credit**.

A window with the TouchNet uPay payment options opens in the web browser; the rest of the steps correspond to the standard TouchNet uPay payment process.

After the payment is successfully sent to MyQ, the **Payment successful** dialog box appears.

i TouchNet uPay tries to connect to the MyQ server via the hostname or IP address that is set on the **Network** settings tab of the MyQ Web Interface. In case a hostname is set on the tab and paying users receive the "This site can't

be reached / XYZ's server DNS address could not be found. / DNS_PROBE_FINISHED_NXDOMAIN" message, try to replace the hostname with the IP address of your server.

11.6 Recharging Credit by Vouchers

The MyQ administrator (and users authorized to manage vouchers) can generate and print any number of vouchers of a defined value to be distributed to users.

The vouchers can be sold to MyQ users through any standard distribution channel. Once the user has the credit voucher, they can recharge their credit on their account on the MyQ Web Interface, on embedded terminals, on MyQ TerminalPro terminals and in the MyQ mobile application.

All generated and used vouchers are logged in the MyQ database. The information about which voucher was used and for which user can be accessed on the MyQ Web administrator interface. This ensures full control and transparency and enables the administrator to prevent possible misuse.

To enable users to manage vouchers on the **Voucher Batches** main tab, provide them with the **Manage Vouchers** rights. For more information about rights and how to provide them, see [Rights](#).

11.6.1 Setting the Voucher Format

Before the vouchers are generated, it is necessary to set the format of the voucher unique code and define the text printed on the voucher. These parameters can be set and modified on the **Credit** settings tab, under **Payment providers**. Double-click the **Voucher** item (or select the item and click **Edit**) to open the **Voucher** properties panel.

The unique code format can be defined by creating a **Voucher code mask** – a predefined code template consisting of zeroes and lower case a's. Zeroes are substituted by numbers and a's are substituted by upper case letters or numbers. For example, the *00a0000aaa* mask will generate numbers such as *86D9841POE*, *03E8976E67*, etc.

Always set the code format adequate to the number of users and the frequency of the voucher generation process, to ensure a sufficient variety of codes. If the amount of the currently valid codes is large and the variety not sufficient, the chance of randomly guessing the valid code number is high and the credit system can be easily bypassed.

The text entered in the **Voucher-custom lines 1 and 2** fields is displayed on the printed vouchers. You can enter, for example, the name of your company and additional information.

Do not forget to set the currency on the **General** settings tab, if you have not set it earlier. The currency on the printed voucher is the same as the one set in MyQ.

11.6.2 Custom Logo for Credit Vouchers

If you want to use your own logo on MyQ credit vouchers instead of the default MyQ logo, you can import the new logo on the [Personalization](#) settings tab in the MyQ Web Administrator Interface.

The file with the logo has to be in the *JPG*, *JPEG*, *PNG* or the *BMP* format; the recommended size of the logo is *398px x 92px*.

To import the logo:

1. On the MyQ Web administrator interface, open the **Personalization** settings tab. (**MyQ, Settings, Personalization**).
2. On the tab, under **Custom application logo**, click **+Add**, browse and upload the file with the logo, and lastly click **Save** at the bottom of the tab. A preview of the new logo is displayed on the tab.

11.6.3 Voucher Batches

Vouchers can be generated on the **Voucher Batches** tab of the MyQ Web Interface. To open this tab, go to **MyQ, Voucher Batches**.

To generate new vouchers:

1. On the bar at top of the **Voucher Batches** tab, click **+Add**. The New Voucher Batch dialog box appears.

2. In the dialog box, enter the number of vouchers to be generated in the **Count** field, the **Price** of the vouchers in the batch, add the validity period in the **Valid till** field, and then click **OK**.

Count: *

Price: *

Valid till:

📅

mm/dd/yyyy

✓ OK

Cancel

Fields marked by * are mandatory.

The new voucher batch record is displayed in the voucher batches list. You can overview all of the vouchers by double-clicking this record.

Managing Voucher Batches

Voucher batches can be filtered by serial number, date, creator, price and expire date. From the **Voucher Batches** main tab, you can export the list of voucher batches to a CSV, and display and print vouchers included in particular batches.

myQ

Central Server

Home

Voucher batches

Voucher batches

Add

Open

Print vouchers

Save as CSV

Refresh

Voucher batch:

Created:

Created by:

Price:

Expire date:

Search

Serial n...	Created	Created by	Price	Valid till	Count	Remaining	Used
Today							
3	09/20/2022 2:40:28 AM	Administrator	10.00000	11/01/2022	3	3	
2	09/20/2022 2:40:15 AM	Administrator	20.00000	11/01/2022	5	5	0%
1	09/20/2022 2:39:54 AM	Administrator	100.00000	11/03/2022	80	80	0%

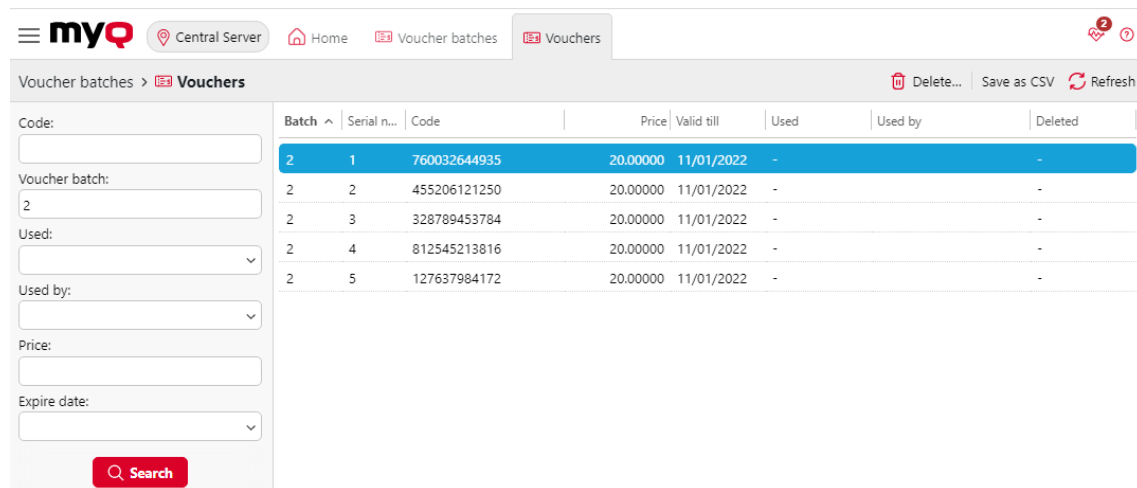
11.6.4 Vouchers Usage Overview

To open the table of all the vouchers generated in one batch, double-click the batch on the **Voucher Batches** main tab (or select the batch, and then click **Open** on the bar at the top of the tab).

In the table, you can see records of all of the generated vouchers with information such its unique code, price, validity, the current status of the voucher usage, etc. If the number of records is too high to be displayed clearly, you can filter them by using filters on the left side. Vouchers can be filtered by code, voucher batch, price, etc.

To delete a voucher, select it in the table and click **Delete** on the bar at the top of the tab. When a voucher is deleted, the code on the voucher becomes invalid.

Click **Save as CSV** to download a CSV file with the vouchers usage overview.



Voucher batches > **Vouchers** Delete... Save as CSV Refresh

Code:

Voucher batch:

Used:

Used by:

Price:

Expire date:

Batch	Serial n...	Code	Price	Valid till	Used	Used by	Deleted
2	1	760032644935	20.00000	11/01/2022	-		-
2	2	455206121250	20.00000	11/01/2022	-		-
2	3	328789453784	20.00000	11/01/2022	-		-
2	4	812545213816	20.00000	11/01/2022	-		-
2	5	127637984172	20.00000	11/01/2022	-		-

11.7 Recharging Credit via External Payment Providers

The external payment provider option is used for managing credit via a Recharge Terminal.

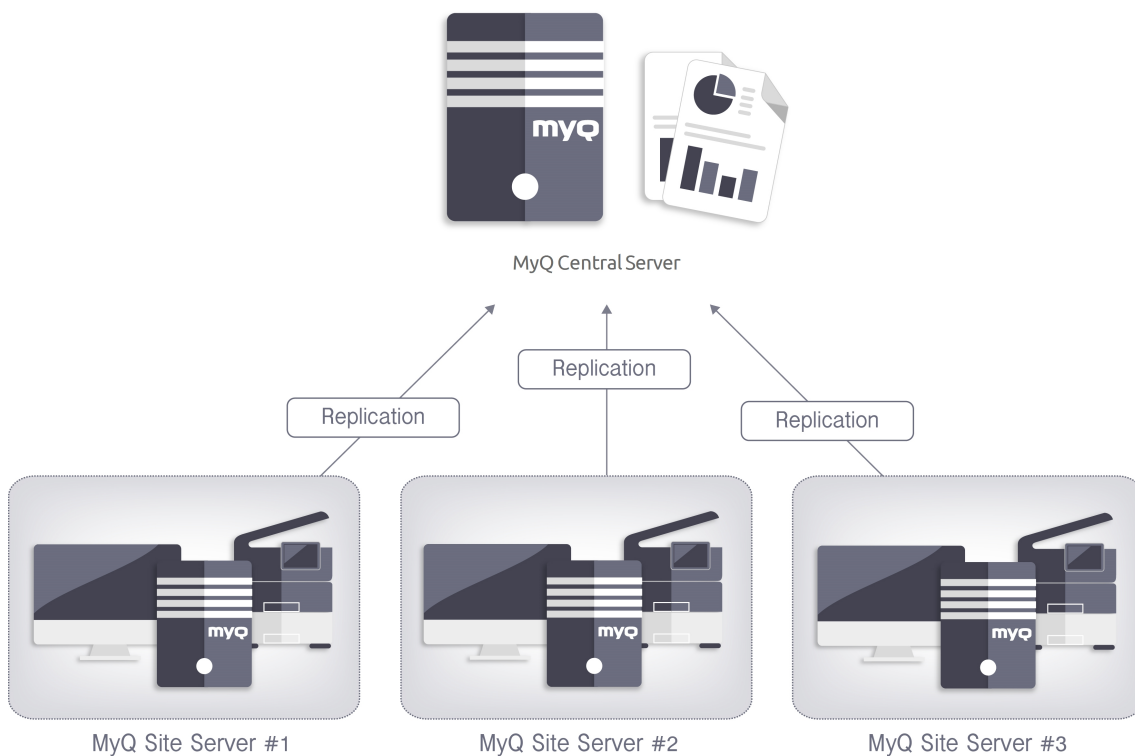
For information on how to set it up, please check the *MyQ Recharge Terminal Guide*.

If a Recharge Terminal is used, you can view the transaction info in **MyQ, Payments**.

12 Central Server Reports Management

On the MyQ Central server, you can create and run reports which include all sorts of information that are downloaded from the site servers and stored on the Embedded or MS SQL database. Running reports on the Central server is useful, especially if you have several branch offices and want to access overall statistics.

The process of downloading data from site servers and storing them on the MyQ Central server's database is called **Replication**. It is essential for central reporting, as all site servers that are included in reports have to be fully replicated to ensure that the data in the reports are correct and up-to-date.



12.1 Reports

In the MyQ web interface, on the **Reports** main tab (**MyQ, Reports**), you can create and generate reports with a variety of data concerning your printing environment. The reports can be related to users, printing devices, print jobs, etc.

The screenshot shows the MyQ web interface. The top navigation bar includes 'myQ', 'Central Server', 'Home', and 'Reports'. The 'Reports' section is active, showing a list of reports under 'My reports'. The table below lists the reports:

Status	Run at	Report	Files	Run by
Today				
✓	09/20/2022 2:45:5...	My monthly summary	XLSX	Administrator
✓	09/20/2022 2:45:4...	My sessions	CSV	Administrator
✓	09/20/2022 2:45:4...	My daily summary	PDF	Administrator

Reports in MyQ are divided into two main categories: **My reports** and **Shared reports**. **My reports** show users reports created by themselves, while **Shared reports** show them reports created by the administrator or by other users.

There are three default reports: **My daily summary**, **My sessions** and **My monthly summary**. These are displayed in the **My reports** folder of the MyQ administrator, who can modify them, delete them or change their design. For all the other users, the default reports are displayed in the **Shared reports** folder and cannot be changed in any way.

In addition to the three default reports, the administrator can create an unlimited number of reports and sort them into sub-folders of the **My reports** folder. Users can create their own reports but they are limited to use only certain report types depending on the rights granted by the administrator.

Each report can be directly displayed on the web interface and saved in any of the following formats: *PDF*, *CSV*, *XML*, *XLSX* and *ODS*. The reports can be automatically generated and stored in a predefined folder. There is no data limitation for the generated report, it includes all the data from the specified period.

All the reports have the MyQ logo displayed by default, but it can be replaced by your company's logo. To upload a custom logo go to **MyQ, Settings, Personalization**. In the **Custom application logo** section, click **+Add** next to **Custom logo** and upload your own file (supported formats - *JPG*, *JPEG*, *PNG*, *BMP* and recommended size - *398px x 92px*).

12.1.1 Report Types

When you are creating reports on the **Reports** main tab, you can choose from a large number of built-in report types that are sorted into multiple categories. Some of the types are included in more categories (for example, *Groups: Daily Summary*, *Print Jobs: Daily Summary*, etc.), while some of the types are particular to only one category (for example, *Device Alerts in Alerts Maintenance* or *Credit Balance in Credit*). You can overview all of the report types on the **Reports** settings tab (in **MyQ, Settings, Reports**).

The screenshot displays the MyQ Central Server Reports Management interface. The sidebar on the left lists various settings categories, with 'Reports' currently selected. The main panel shows a table of built-in reports, organized into four categories: Alerts & maintenance, Credit, Environmental, and General. Each report entry includes its type (Built-in), name, and category.

Type	Name	Category
Alerts & maintenance		
Built-in	Counter analysis	Alerts & maintenance
Built-in	Event history	Alerts & maintenance
Built-in	Toner replacement	Alerts & maintenance
Built-in	Top N alerts summary	Alerts & maintenance
Credit		
Built-in	Credit balance	Credit
Built-in	Credit operations	Credit
Environmental		
Built-in	Expired & deleted jobs	Environmental
Built-in	Printers	Environmental
Built-in	User groups	Environmental
Built-in	Users	Environmental
General		
Built-in	Day of Week	General
Built-in	Hourly activity	General
Built-in	Monthly statistics	General
Built-in	Pricelist comparison	General
Built-in	Weekly statistics	General

Providing users with rights to use a report

The administrator can run all the built-in reports and provide other users and groups with rights to run them as well. In **MyQ, Settings, Reports**, right-click on a report and click **Edit**. On the **General** tab, in the **Permission for running the report** field, choose users and groups from the list and click **Save**.

Add custom reports

You can also add custom report types developed by the MyQ development team. To do so, just click **+Add**, upload the custom report definition file, select users or groups to access it, and click **OK**. For more information about custom report types, contact MyQ support.

Report Categories

- **Alerts and Maintenance** - These reports provide information about device alerts and unusual changes on device counters.
- **Credit** - These reports contain information concerning credit, for example the remaining credit of selected users.
- **Environmental** - These reports inform about the environmental impact of printing. They show how many trees needed to be harvested, how much energy was spent and how much carbon dioxide was emitted during the production of

the paper used for printing and copying within your company's printing environment. Data sources vary in their estimations. MyQ calculations in the report are based on the following data estimates:

- **Carbon dioxide for paper production:** 12,7 gram per paper sheet
- **Energy used for production:** 48 Wh per paper sheet or 32Wh for a recycled paper sheet
- **Trees:** 8333 paper sheets are counted as 1 tree.
- **General** - These reports provide general information about the MyQ system, such as total counters statistics and printing peaks or comparison of price lists used for printers.
- **Groups** - These reports inform about groups of users. They can contain information about membership, printed pages, weekly stats etc.
- **Print Jobs** - These reports contain information about jobs printed in MyQ, such as the list of all expired and deleted jobs over a certain period.
- **Printers** - These reports inform about all the printing devices in the MyQ system (both local and network). Generated reports can contain graphs of the device usage, daily, weekly and monthly counters, etc.
- **Projects** - These reports contain information regarding projects and project accounting in MyQ, such as daily summary of projects or projects assigned to selected users over a certain period.
- **Users** - These reports can contain various information about users. They can concern their print jobs, credit statements, printed pages etc.

Alerts and Maintenance Reports

The following reports are included in the **Alerts and Maintenance** category:

Counter Analysis

This report shows the page counts per session, covering B&W pages, color pages, total pages, and scans by the user. It shows sessions where the counters reached or exceeded the predefined value.



The report is not available when Job Privacy is enabled.

Event History

This report shows the occurrence of predefined device errors and alerts. It only shows alerts that are turned on in **Settings > Events** in the MyQ Web UI.

Toner Replacement

This report shows the toner usage, the date the toner was installed or replaced, and the pages printed for each toner container.

The number displayed in the Toner replacement report in the Pages printed and Total counters columns depends on the toner it relates to:

- **Pages printed** - The number of pages printed with the replaced toner. Only color pages for color toners (CMY) and all pages for black toners (K) are considered.

- **Total counters** - Total counters of the printer related to the replaced toner. Color pages for color toners (CMY) and all pages for black toners (K) are considered.

Top N Alerts Summary

This report shows the most common errors and alerts. The number of alerts shown can be customized.

 Charts are available for this report.

Credit Reports

The following reports are included in the **Credit** category:

Credit Balance

This report shows the current Credit balance.

Credit Operations

This report shows a list of credit transactions (top-up and spent).

Environmental Reports

 The information in these reports is based on the following data:
1 tree = 8333 pages / 1 page = 12.7g of CO2 / 1 page = 48Wh of energy / 1 recycled page = 32Wh of energy

The following reports are included in the **Environmental** category:

Expired and Deleted Jobs

This report shows a list of expired/deleted jobs and the environmental impact of not printing them. They are sorted by print queue.

 When Job Privacy is enabled, this report can be used but will exclude user-specific information.

Printers

This report shows the environmental impact of each printer.

User Groups

This report shows the environmental impact of each User Group.

Users

This report shows the environmental impact of each User.

 The report is not available when Job Privacy is enabled.

General Reports

The following reports are included in the **General** category:

Day of the Week

This report shows the output volume by day of the week.

Charts are available for this report.

Hourly Activity

This report shows the output volume by time of day.

Charts are available for this report.

Monthly Statistics

This report shows the output volume by month.

Charts are available for this report.

Price List Comparison

This report shows the price lists applied to various printer groups.

Weekly Statistics

This report shows the output volume by week.

 Charts are available for this report.

Groups Reports

The following reports are included in the **Groups** category:

Counters by Function and Duplex(BETA)

This report shows counters per group by print/copy, color, and duplex.

The function field refers to whether a page was printed or copied.



Reports marked as BETA only contain data from Embedded Terminals running MyQ 8+. If some of your Embedded Terminals run earlier versions of MyQ, their data will not be included in the report.

 The report is not available when Job Privacy is enabled.

Counters by Function and Paper Format(BETA)

This report shows counters per group by print/copy, color, and paper format.

The function field refers to whether a page was printed or copied.

 Reports marked as BETA only contain data from Embedded Terminals running MyQ 8+. If some of your Embedded Terminals run earlier versions of MyQ, their data will not be included in the report.

 The report is not available when Job Privacy is enabled.

Counters by Function Paper Format and Duplex(BETA)

This report shows counters per group by color, duplex, and paper format.

The function field refers to whether a page was printed or copied.

 Reports marked as BETA only contain data from Embedded Terminals running MyQ 8+. If some of your Embedded Terminals run earlier versions of MyQ, their data will not be included in the report.

 The report is not available when Job Privacy is enabled.

Daily Summary

This report shows a summary of the daily output by group.

Day of the Week

This report shows a summary of the daily output based on the day of the week by group.

Monthly Summary

This report shows a summary of the monthly output by group.

 This report supports aggregated columns.

Top N

This report shows the groups sorted by largest output volume.
Charts are available for this report.

 It will show the top 5 by default, but this can be changed in the **Design** section of the report, under **Filters and Parameters**, by changing the number for **N**.

Total Summary

This report shows the total output volume per group for a predefined period.

 This report supports aggregated columns.

 The report is not available when Job Privacy is enabled.

User Group Membership

This report shows the list of members of the group and their membership options.

 The report is not available when Job Privacy is enabled.

Print Jobs Reports

 Reports in this category should not be used for accounting purposes. Print Job reports display print jobs either as received by MyQ (for devices without an embedded terminal) or they reflect the printing parameters selected on the embedded terminal, rather than the final printed outcome.

The following reports are included in the **Print Jobs** category:

Daily Summary

This report shows the list of print jobs printed by user on a daily basis.

 The report is not available when Job Privacy is enabled.

Expired and Deleted Jobs

This report shows the list of expired and deleted jobs.

 This report supports aggregated columns.

 The report is not available when Job Privacy is enabled.

Printed Jobs Summary

This report shows the list of all the print jobs printed by the user for a predefined period.

 The report is not available when Job Privacy is enabled.

Printers Reports

The following reports are included in the **Printers** category:

Counters by Function and Duplex(BETA)

This report shows counters per device by print/copy, color, and duplex. The function field refers to whether a page was printed or copied.

 Reports marked as BETA only contain data from Embedded Terminals running MyQ 8+. If some of your Embedded Terminals run earlier versions of MyQ, their data will not be included in the report.

 The report is not available when Job Privacy is enabled.

Counters by Function and Paper Format(BETA)

This report shows counters per device by print/copy, color, and paper format.

The function field refers to whether a page was printed or copied.

 Reports marked as BETA only contain data from Embedded Terminals running MyQ 8+. If some of your Embedded Terminals run earlier versions of MyQ, their data will not be included in the report.

 The report is not available when Job Privacy is enabled.

Counters by Function Paper Format and Duplex(BETA)

This report shows counters per device by color, duplex, and paper format.

The function field refers to whether a page was printed or copied.

 Reports marked as BETA only contain data from Embedded Terminals running MyQ 8+. If some of your Embedded Terminals run earlier versions of MyQ, their data will not be included in the report.

 The report is not available when Job Privacy is enabled.

Daily Summary

This report shows the list of print jobs printed by device on a daily basis.

 This report supports aggregated columns.

Day of the Week

This report shows a summary of the daily output based on the day of the week by device.

 This report supports aggregated columns.

Meter Reading via SNMP

This report shows the device's total output volume.

 This report (unlike the rest of MyQ reports) includes accounting data of the jobs bypassing MyQ server.

Monthly Summary

This report shows a summary of the monthly output by device.

Top N

This report shows the printers sorted by largest output volume.

 Charts are available for this report.

Total Summary

This report shows the total output volume per printer for a predefined period.

 This report supports aggregated columns.

 The report is not available when Job Privacy is enabled.

Projects Reports

The following reports are included in the **Projects** category:

Counters by Function and Duplex(BETA)

This report shows counters per project by print/copy, color, and duplex. The function field refers to whether a page was printed or copied.

 Reports marked as BETA only contain data from Embedded Terminals running MyQ 8+. If some of your Embedded Terminals run earlier versions of MyQ, their data will not be included in the report.

 The report is not available when Job Privacy is enabled.

Counters by Function and Paper Format(BETA)

This report shows counters per project by print/copy, color, and paper format. The function field refers to whether a page was printed or copied.

 Reports marked as BETA only contain data from Embedded Terminals running MyQ 8+. If some of your Embedded Terminals run earlier versions of MyQ, their data will not be included in the report.

 The report is not available when Job Privacy is enabled.

Counters by Function Paper Format and Duplex(BETA)

This report shows counters per project by color, duplex, and paper format.

The function field refers to whether a page was printed or copied.

 Reports marked as BETA only contain data from Embedded Terminals running MyQ 8+. If some of your Embedded Terminals run earlier versions of MyQ, their data will not be included in the report.

 The report is not available when Job Privacy is enabled.

Daily Summary

This report shows the list of print jobs printed by project on a daily basis.

 This report supports aggregated columns.

Day of the Week

This report shows a summary of the daily output based on the day of the week by project.

 This report supports aggregated columns.

Monthly Summary

This report shows a summary of the monthly output by project.

 This report supports aggregated columns.

Print Jobs per Project

This report shows the list of print jobs assigned to each project.

 The report is not available when Job Privacy is enabled.

Project Groups Total Summary

This report shows the total output volume per project for a predefined period.

Projects per User

This report shows the output volume per user and project. The data is grouped by user.

 This report supports aggregated columns.

 The report is not available when Job Privacy is enabled.

Top N

This report shows the projects sorted by largest output volume.

 Charts are available for this report.

User Project Assignment

This report shows the list of projects assigned to each user.

 The report is not available when Job Privacy is enabled.

Users per Project

This report shows the members of each project.

 This report supports aggregated columns.

User Session Details

This report shows the list of all the user's interactions on the device sorted by project.

 This report supports aggregated columns.

 The report is not available when Job Privacy is enabled.

Users Reports

The following reports are included in the **Users** category:

Counters by Function and Duplex(BETA)

This report shows counters per user by print/copy, color, and duplex. The function field refers to whether a page was printed or copied.

 Reports marked as BETA only contain data from Embedded Terminals running MyQ 8+. If some of your Embedded Terminals run earlier versions of MyQ, their data will not be included in the report.

 The report is not available when Job Privacy is enabled.

Counters by Function and Paper Format(BETA)

This report shows counters per user by print/copy, color, and paper format.

The function field refers to whether a page was printed or copied.

 Reports marked as BETA only contain data from Embedded Terminals running MyQ 8+. If some of your Embedded Terminals run earlier versions of MyQ, their data will not be included in the report.

 The report is not available when Job Privacy is enabled.

Counters by function paper format and duplex(BETA)

This report shows counters per user by color, duplex, and paper format.

The function field refers to whether a page was printed or copied.

 Reports marked as BETA only contain data from Embedded Terminals running MyQ 8+. If some of your Embedded Terminals run earlier versions of MyQ, their data will not be included in the report.

 The report is not available when Job Privacy is enabled.

Daily Summary

This report shows the list of print jobs printed by user on a daily basis.

 The report is not available when Job Privacy is enabled.

Day of the Week

This report shows a summary of the daily output based on the day of the week by user.

 The report is not available when Job Privacy is enabled.

Monthly Summary

This report shows a summary of the monthly output by user.

 The report is not available when Job Privacy is enabled.

Session Details

This report shows the list of all user's interactions on the device.

 The report is not available when Job Privacy is enabled.

Top N

This report shows the users, sorted by largest output volume.

Charts are available for this report.

 The report is not available when Job Privacy is enabled.

Total Summary

This report shows the total output volume per user for a predefined period.

 The report is not available when Job Privacy is enabled.

User Rights

This report shows the list of users with enhanced access rights.

 The report is not available when Job Privacy is enabled.

Servers – User Rights

This report shows the rights assigned to users for each site server.

Creating New Aggregated Columns

For some types of reports, you can create any number of custom aggregated (summary) columns. An aggregated column can display either the sum or the average of a selection of any number of other columns available for the type.

To create a new aggregated column for a report:

1. Go to **MyQ, Reports**. On the list of reports on the right side, select the report and click **Edit** on the ribbon (or right-click, edit). The report properties panel opens on the right side of the screen.
2. Go to the **Design** tab on the properties panel.
3. In the **Table** section, click **+Add** and select **+Add aggregated column**. The properties panel of the new column opens.

myQ Home Reports Monthly summary

Reports > Monthly summary

General **Design** ✓ Save Preview

Options

Orientation: Portrait

Show filters in the final report: ☐

Filters and parameters

User: All users

Accounting Group:

Printer: All printers

Period: * Last 3 month(s)

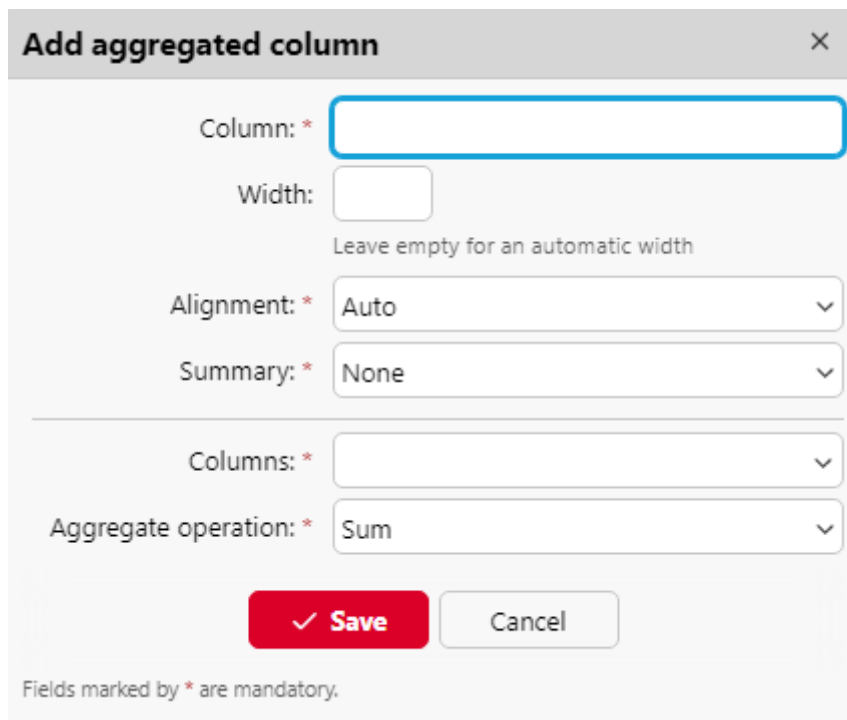
Fields marked by * are mandatory.

Table

+ Add

Column	Width	Order	Aggregate
Group	Auto	Auto	No
Period	Auto	Auto	No
B&W pages	Auto	Auto	Sum
Color pages	Auto	Auto	Sum
Total	Auto	Auto	Sum
Scans	Auto	Auto	Sum
Total price	Auto	Auto	Sum

4. In the panel, set the columns properties, select the **Aggregate operation** you want to use (*Sum* or *Average*), and click **Save**. The new aggregated column is listed with the other table columns, and you can double-click on it to edit it.



Add aggregated column [X]

Column: *

Width:
Leave empty for an automatic width

Alignment: *

Summary: *

Columns: *

Aggregate operation: *

Fields marked by * are mandatory.

Supported types of reports for aggregated columns

The aggregated (summary) columns can be created for the following types of reports:

- From the **Groups** category: Monthly summary
- From the **Print jobs** category: Expired and deleted jobs
- From the **Printers** category: Daily summary, Day of the week, Meter reading via SNMP
- From the **Projects** category: Daily summary, Day of the week, Monthly summary, Project groups total summary, Projects per user, Users per project.

12.1.2 Reporting Sources

Accounting in MyQ depends on the MyQ server version, the MyQ embedded terminal version and the printing device. MyQ 8.0+ currently uses the user-session architecture. The values in every report are based on user sessions (except for the **Meter reading via SNMP** printers report, described below).

- Counters are calculated in the following way:
 - B&W pages = B&W prints + B&W copies + Fax
 - Color pages = Color prints + Color copies + Single color copy
 - Total Pages = B&W pages + Color pages
 - Total prints = B&W prints + Color prints
 - Total copies = B&W copies + Color copies
- Price related columns include discounts.
- Any printers monitored via MyQ Desktop Client are included in the reports.
- Any non-MyQ users activity (*unauthenticated) is included in the reports.

- MyQ does not track deleted printers. If a deleted printer is later added and activated in MyQ, the reports will not include any activity during the time the device was deleted.
- If a printer is deactivated but not deleted, the reports include information about the period it was inactive only after it is reactivated. In that case, after the reactivation, all the activity is accounted to users not authenticated in a single session. The reports cannot include printers' data while they are deactivated.
- When an embedded terminal is installed on the printing device, accounting is also done for any direct/tandem print queues of the device.
- When an embedded terminal is not installed or a device is used with a MyQ Hardware terminal, accounting is done via SNMP by the MyQ Print Server (depends on provided data via SNMP from the device).

Values calculation in the Meter reading via SNMP printers report

The values in this report are based on counters read directly from the printers.

- Any printers monitored via MyQ Desktop Client are **not** included in the reports.
- The highest and lowest values are compared for a selected period and printer/group of printers.
- The total value displayed in the report is the summary of all the subtotal values, without *Pages printed* while the device was deactivated.

12.1.3 Report Values Description

Description of values in the reports' default and additional columns and how they are accounted.

These values are accounted as page counts in the following way: 2 clicks for the A3/ Ledger page format and 1 click for the rest (A4 etc.); in case of Duplex, it is 4 clicks for the A3 / Ledger format and 2 clicks for the rest (A4 etc.). L formats are coverage counters.

- B&W prints
- B&W copies
- Color prints
- Color copies
- Single color copy
- Total prints
- Total copies
- Fax
- Color pages (L1)
- Color cost (L1)
- Color pages (L2)
- Color cost (L2)
- Color pages (L3)
- Color cost (L3)
- Print color pages (L1)
- Copy color pages (L1)

 If discounts are used, they are not applied to all "cost" values in reports, e.g. *Color cost (L1)*, *Color cost (L2)* or *Color cost (L3)*. However, *Total cost*, *Color cost* do reflect discounts.

These values are accounted as paper sheets in the following way : 1x A3 / 1x A4 etc.

- A4 paper
- A3 paper
- A5 paper
- B4 paper
- B5 paper
- Other paper
- Folio paper
- Ledger paper
- Legal paper
- Letter paper
- Statement paper
- Rest of the paper formats

These values are accounted as paper sheets as well, however, when a printing device is used without an installed Embedded terminal, this counter is specified via SNMP and depends on the counter used from the printing device.

- Simplex
- Duplex

 Terminals version 7 and lower might have reported Duplex values differently depending on the vendor – either as the number of images (e.g. 1 page printed duplex as Duplex=2) or the number of sheets (Duplex=1). Since Terminals 8.2, these values are unified as the number of sheets. The combination of data from older Terminals with Terminals 8.2 in Reports may cause an inconsistency in the Duplex values.

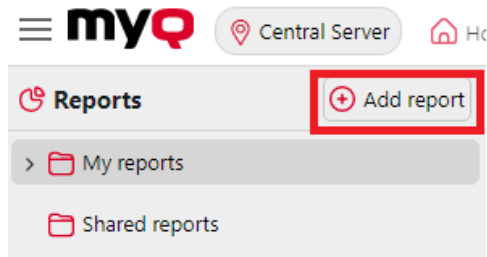
A job printed in 1x A3 monochrome sheet, on both sides in duplex mode, on a device where an Embedded terminal is installed, is accounted in MyQ as 1x A3 paper + 4x print monochrome and 1x duplex. In the MyQ log it will look like this:

PM=4, A3=1, Duplex=1

12.1.4 Creating, Editing, and Cloning Reports

You can create a new report in a few steps:

1. At the top-right corner of the **Reports** main tab, click **+Add report**. The Add report dialog box appears.



2. In the box, select the type of the new report and the folder to place it, and then click **OK**. The editing panel of the new report opens. On the panel, edit and save the report or simply close the panel to save the report without changes.

 The screenshot shows a modal dialog box titled 'Add report' with a close button (X) in the top right corner. Inside the dialog, there are two dropdown menus. The first is labeled 'Type: *' and has 'Groups - Daily summary' selected. The second is labeled 'Folder:' and has 'My reports' selected. Below the dropdowns are two buttons: a red button with a checkmark and the text 'OK', and a white button with the text 'Cancel'. At the bottom left of the dialog, there is a small note: 'Fields marked by * are mandatory.'

Editing a report

1. On the **General** tab of the report's editing tab, you can change the report's **Name**, add a **Description**, select **Sharing** rights, meaning the users or groups who will have the rights to **Run** the report and those who will have the rights to **Edit** the report. You can also click **Schedule** to set its scheduled run. Once done, click **Design** to open the Design tab of the report.

Reports > **Daily summary**

General | Design | Save | Preview

General

Name: *

Description:

Sharing

You can always run and edit this report.

Run:

Edit:

Scheduled run

This report is not scheduled.

Fields marked by * are mandatory.

2. On the **Design** tab, you can set the report's layout, select the items (Users, Printers, etc.) to be included in the report, add or remove columns and change their order.

Options

- **Orientation:** Select either the **Portrait**, or the **Landscape** orientation.

Options

Orientation:

Show filters in the final report: ☐

- **Show filters in the final report:** Mark the checkbox if you want filters to be visible in the final report.

Filters and parameters

Available filters and parameters differ depending on the report type. These are the main parameters available for most of the standard reports types:

Filters and parameters

Site:

User: All users

Group:

Printer: All printers

Period: * Last 7 day(s)

Exclude data

User:

- **Site:** Select the sites to be included in the report.
- **User:** Select the users to be included in the report. If you select the **Me** option and share this report with all users, each user can only see just the data that concern themselves; this way you can make personalized reports for each user.
- **Accounting Group:** Select the accounting groups of users to be included in the report.
- **Printer:** Select the printers to be included in the report.
- **Period:** Select the time period to be covered by the report.
- **Exclude data - User:** Select the users to be excluded from the report (only available in reports where *User* is one of the filters used).

Table

Here you can enable and disable the table option.

Table Add				
Column	Width	Alignment	Summary	Aggregate
Group	Auto	Left	None	No
Date	Auto	Auto	None	No
B&W pages	Auto	Auto	Sum	No
Color pages	Auto	Auto	Sum	No
Total	Auto	Auto	Sum	No
Scans	Auto	Auto	Sum	No
Total price	Auto	Auto	Sum	No

You can also add and remove columns to the table, edit them and change their order. For each column, you can change the width, alignment and the type of summary that will be shown on the final (bottom) row (Sum, Average or None).

To add a new column, click **+Add**. To open the editing options of an existing column, double-click it (or select it, and then click **Edit**). To remove a column, select it and

click **X**. To move a column up or down the order, select it, and then use the up/down arrows.

Period	B&W pages	Color Pages	Total	Scans	Total price
2017-3	5,621	9,189	14,810	5,506	\$5,440.000
2017-4	1,211	569	1,780	1,234	\$7,072.000
Period	B&W pages	Color Pages	Total	Scans	Total price
	6,832	9,758	16,590	6,740	\$12,512.000

Some reports do not include the option to use tables and their data can be displayed only in the chart form.

Chart

Here you can enable and disable the chart option.

Chart

Pie chart

Doughnut chart

Bar chart

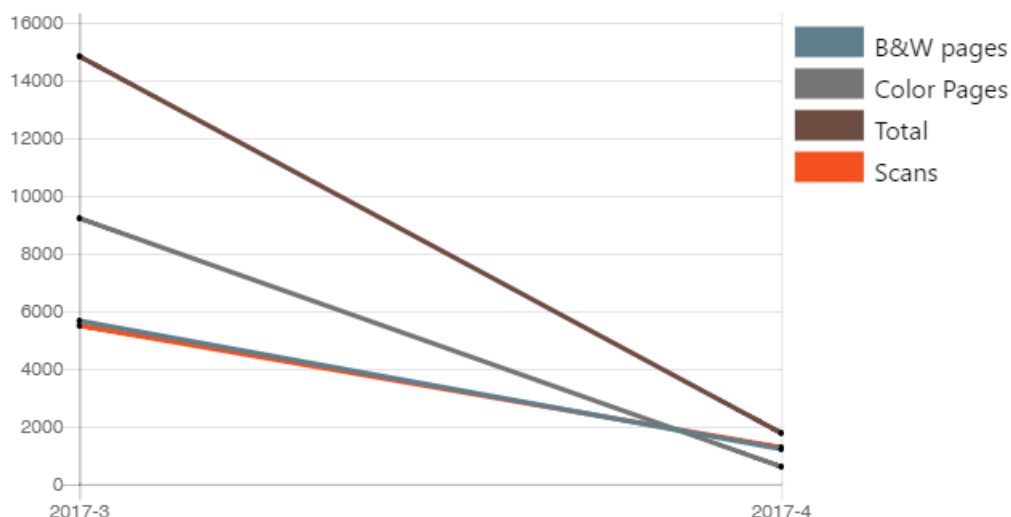
Type: Bar chart

☒

You can also select from the **Bar**, **Pie** and **Doughnut** chart types. Furthermore, you can add and remove data types to be shown on the chart and select colors for each data type (depending on the report type).

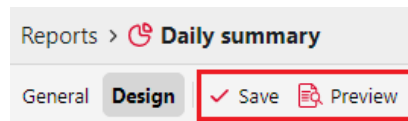
To add a data type, click **+Add**. To open editing options of a data type, double-click it (or select it, and then click **Edit**). To remove a data type, select it and click **X**. To move a data type up or down the order, select it, and then use the up/down arrows.

Some reports do not include the option to use charts and their data can be displayed only in the table form.



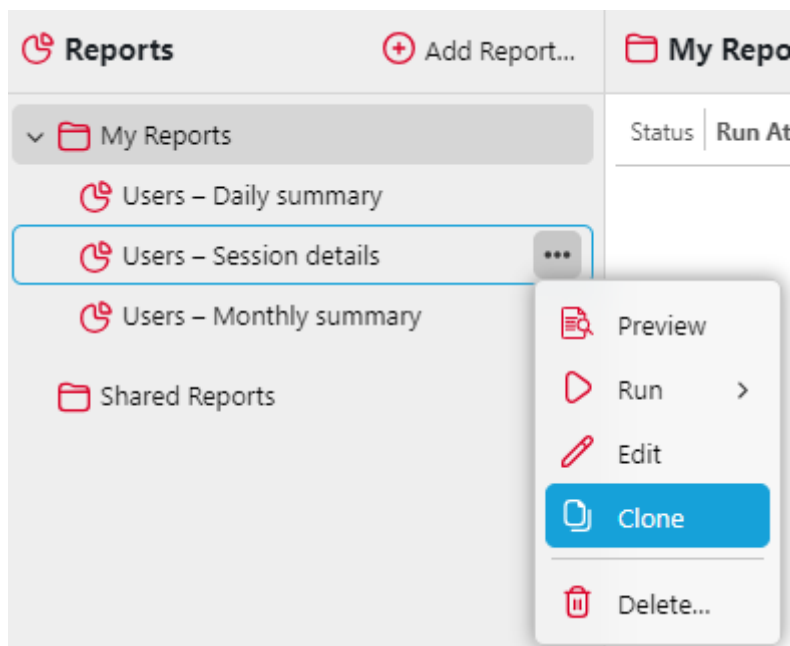
Designing your own reports can be a bit tricky, since it always depends on many factors - amount of data included (columns), length of column names and values, report orientation etc. To get the best result, you can click **Preview** anytime during

the report's creation to check what the new design will look like. Only after you are satisfied with the layout, click **Save** to save the report.



Cloning Reports

Any user can clone an existing report that they have access to, this copies the settings of the existing report and saves it with a modified title, for example, the clone of **Users - Session details** is automatically named **Users - Session details (1)**.



To clone a report, right-click its title or use its context menu and select **Clone**. The edit report options for the newly cloned report open automatically. Users can then change the title of the report or edit any other relevant settings and click **Save**. If a user does not edit any of the new report's settings, the clone is already automatically saved.

Reports >  (Edit) Users – Session details (1)

General | Design |  Preview

▼ **General**

Name: *

Description:

▼ **Sharing**

You can always run and edit this report.

Run:  All users ▼

Edit: ▼

▼ **Scheduled run**

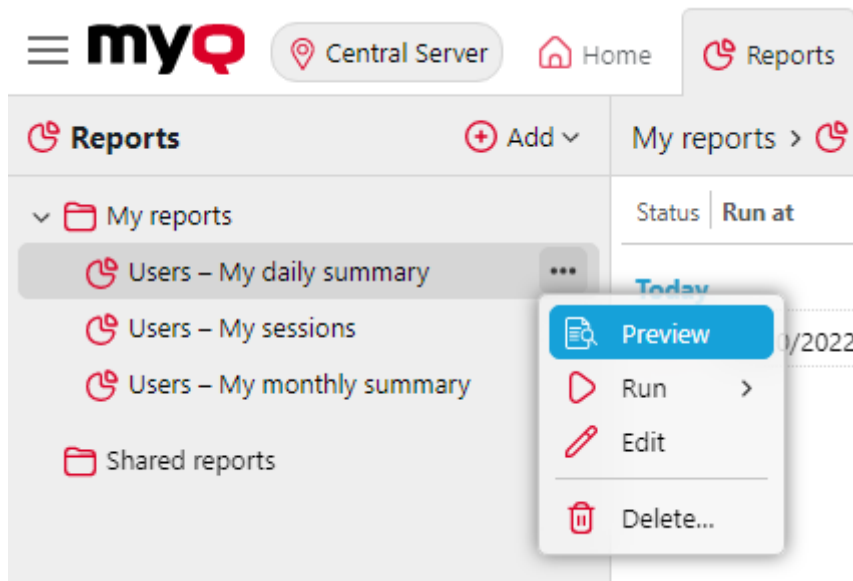
This report is not scheduled.

If the source folder of the report was not created by the user, a clone will be created in the My Reports folder.

12.1.5 Generating Reports

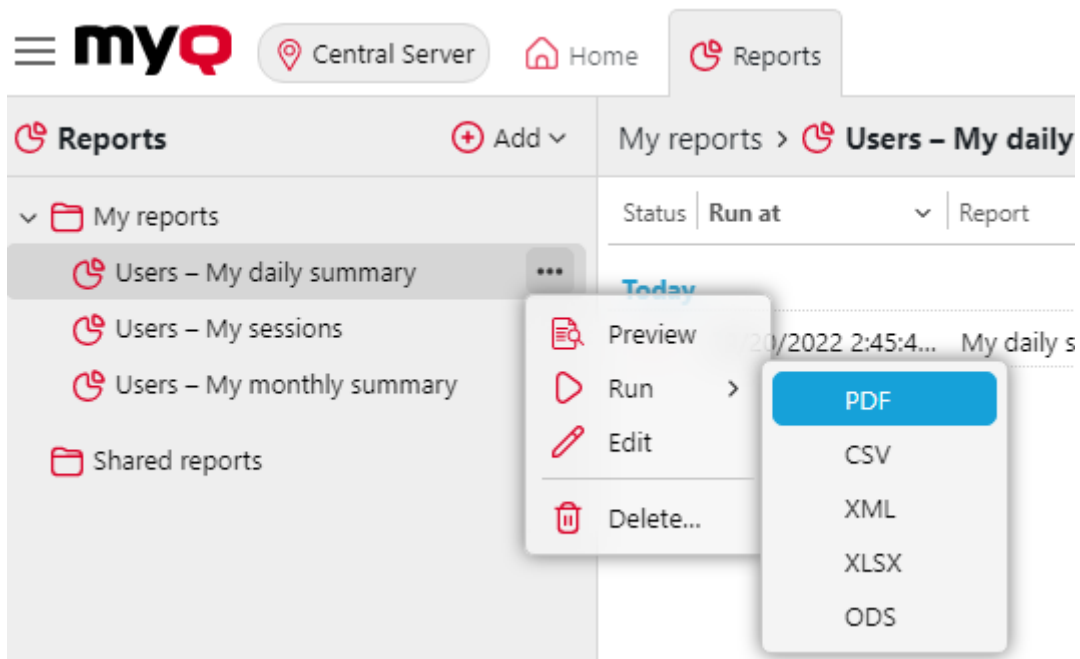
To preview a report

Select the report and click **Preview** (or right-click it and click **Preview** on its shortcut menu). The report is shown in HTML format and the number of included data is limited. You can switch between Graphical view and Grid view.



To run a report

Select the report and click **Run**. (Or right-click it and click **Run** on its shortcut menu). The report runs in the specified format (*PDF, CSV, XML, XLSX* or *ODS*) with no data limitation.



To export the displayed report

After the report is generated, click on the report's format link in the file column to download it.

My reports				
Status	Run at	Report	Files	Run by
Today				
✓	09/15/2022 5:14:1...	My monthly summary	ODS	Administrator
✓	09/15/2022 5:14:0...	My sessions	XLSX	Administrator
✓	09/15/2022 5:13:5...	My daily summary	CSV	Administrator
✓	09/15/2022 4:38:1...	My monthly summary	PDF	Administrator
✓	09/15/2022 4:37:5...	My sessions	PDF	Administrator
✓	09/15/2022 4:37:4...	My daily summary	PDF	Administrator

13 Connection to BI tools

Starting from version 8.1(patch 2), MyQ Central Server exposes data to be analyzed with external BI tools (Business Intelligence tools).

The below information refers to the setup and use of Power BI by Microsoft, along with a MyQ setup.

For further information about Power BI, visit:

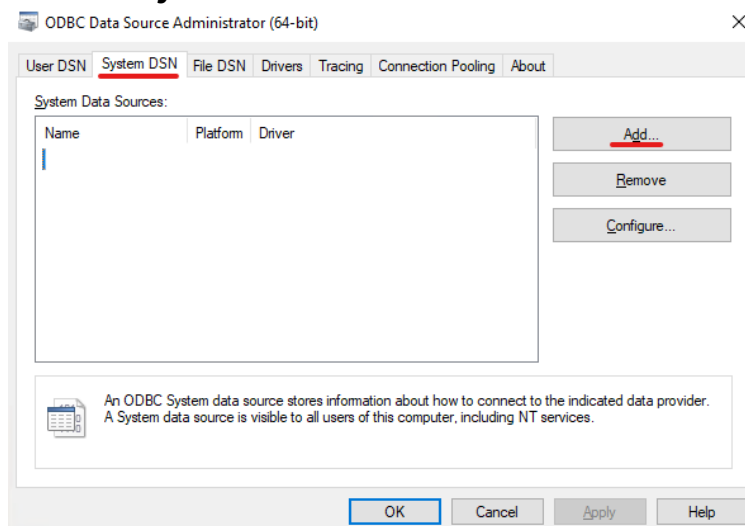
<https://docs.microsoft.com/en-us/power-bi/fundamentals/desktop-getting-started>

13.1 Embedded Database Connection Configuration

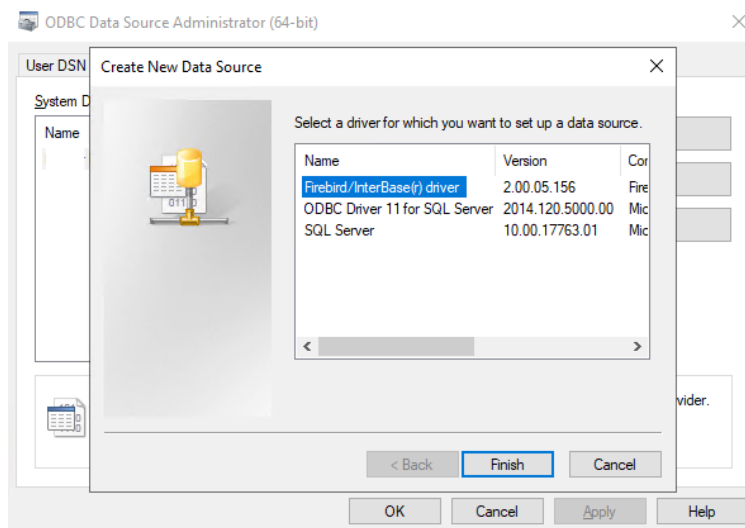
Power BI can access the MyQ Embedded Database via ODBC. In order to create an ODBC data source:

P Power BI will only let you connect to a ODBC data source that is available on the local PC it is running within. Your data source should be created on the same PC that Power BI desktop run.

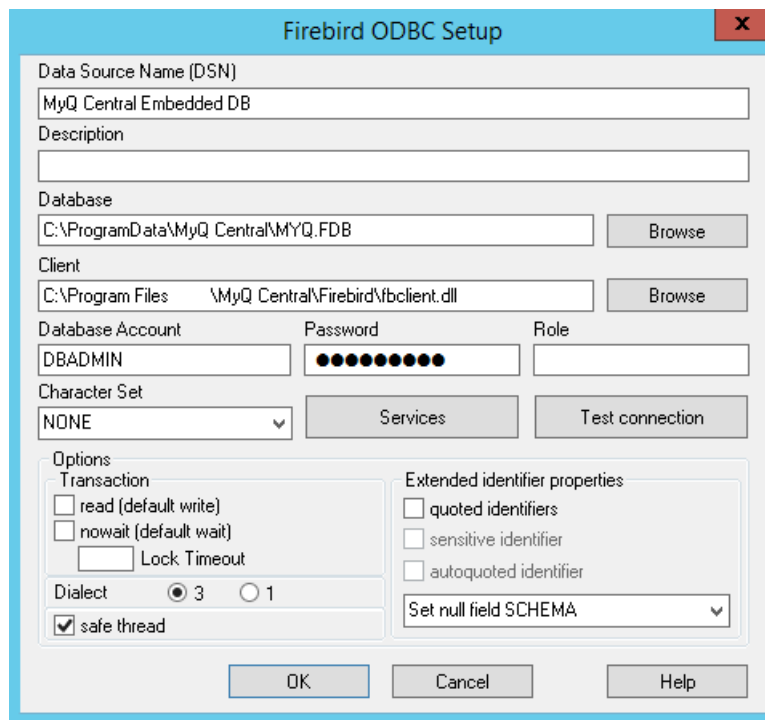
1. Download and install the latest ODBC driver for Firebird from:
<https://firebirdsql.org/en/odbc-driver/>
2. Once installed, open the **ODBC Data Sources** application from the Windows Apps menu.
3. Go to the **System DSN** tab and click **Add**.



4. In the Create New Data Source window, select *Firebird/InterBase(r) driver* and click **Finish**.



5. In the Firebird ODBC Setup tab, enter the connection details:
 - a. **Data Source Name (DSN):** Add a name as an identifier for the connection
 - b. **Database:** Add the path to your database file (C:\ProgramData\MyQCentral\MYQ.FDB by default)
 - c. **Client:** Add the path to the Firebird library client used for the connection. It is recommended to use the MyQ Central Server client, found in C:\Program Files\MyQ Central\Firebird\fbclient.dll by default
 - d. **Database Account:** Add the Database Account user name. The default one is SYSDBA, but it is highly recommended not to use the default database account, but enable and use the **database read-only account** available in the [External Reports](#) settings tab
 - e. **Password:** Add the Database Account password. In case you are using the default database account (not recommended) and you haven't changed the password in MyQ Central Easy Config, the default one is *masterkey*.
 - f. The rest of the fields can be left unchanged. Click **Test Connection** and if successful, click **OK**.



13.2 Creating Reports

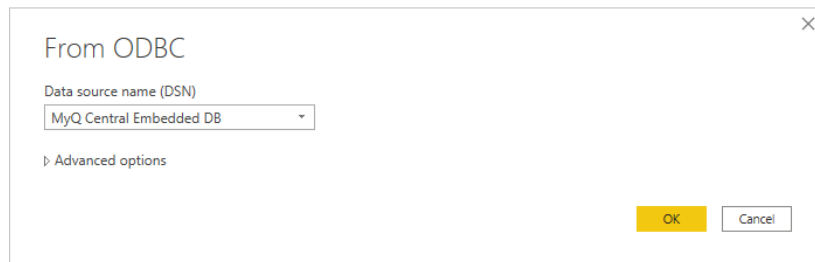
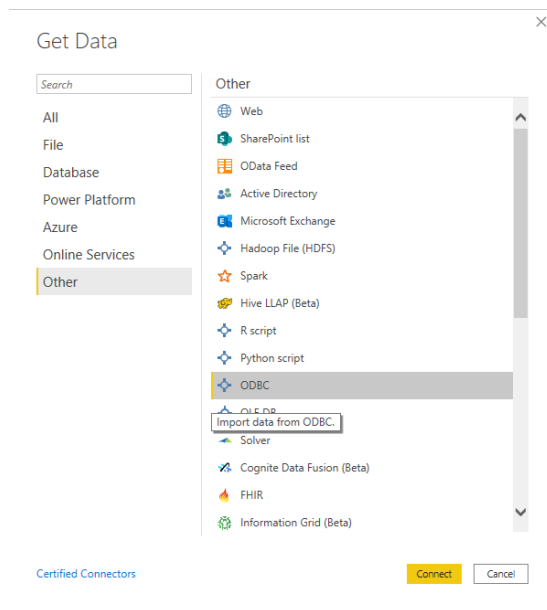
Reports can be created according to each customer's specific requirements. It is possible to create the reports manually, or use the Power BI template created by MyQ and available in the MyQ Community, in order to generate reports quickly.

- [Manual reports creation](#)
- [Reports creation via template import](#)
- [Report examples](#)
- [Database Views description](#)

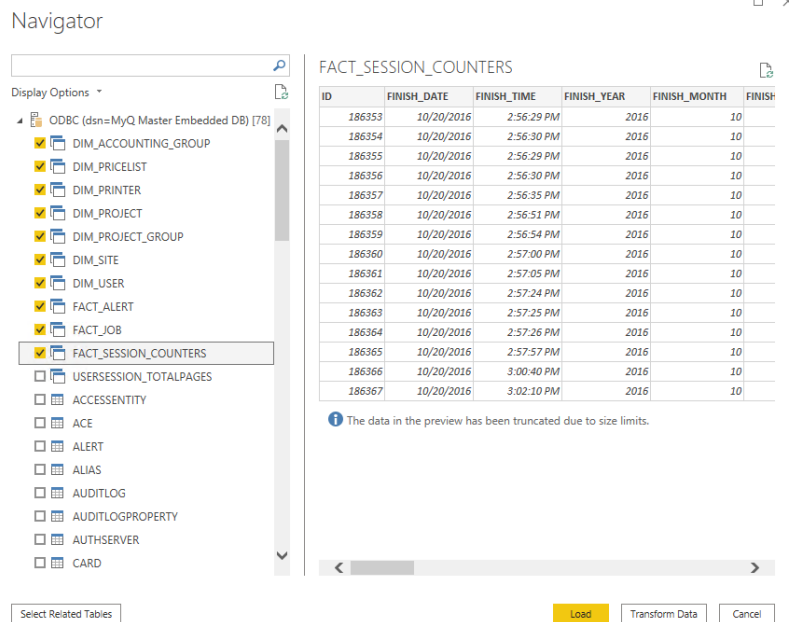
13.2.1 Manual Reports Creation

To manually create the reports, open Power BI and:

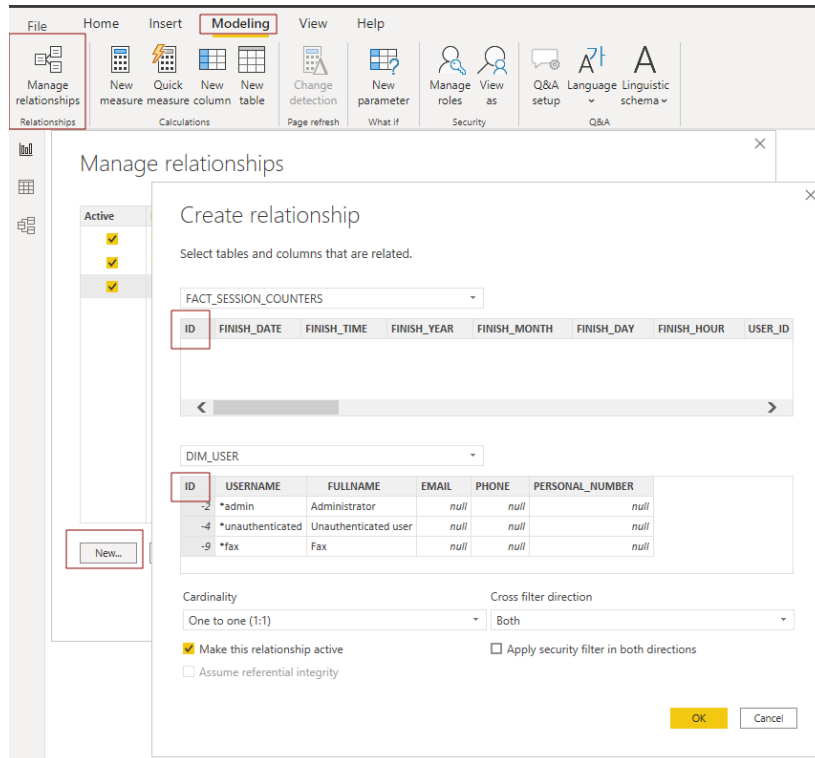
1. Establish the connection to your database:
 - a. For direct connection (**only for MS SQL servers**), click **Get data, SQL Server** and add the server and database name.
 - b. For ODBC, click **Get data, More....** In the new window, select **Other**, click on **ODBC** on the list, and click **Connect**. In the new prompt, select the Data source name (DSN) you created in the ODBC Data Sources app and click **OK**.



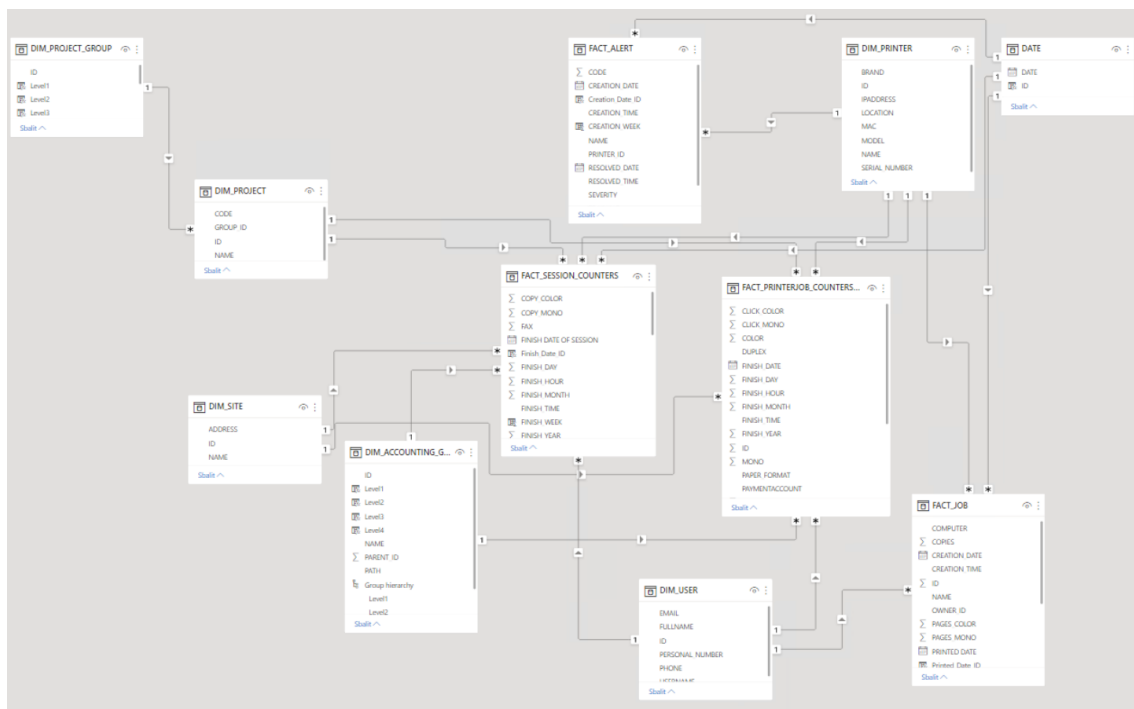
2. In the Navigator window, select all the options with the **DIM_** and **FACT_** prefixes and click **Load** (see [Database Views description](#)).



3. Power BI loads the data, however the relationships between them must be created manually, since Power BI cannot extract them:
 - a. Go to the Modeling menu and click on **Manage relationships**
 - b. Click **New...** and create the relationships between the views, selecting the IDs in each of them. Click **OK** once done.



4. Your model has been created and you can add visualizations to the report.



13.2.2 Reports Creation via Template Import

There are two template versions, one to be used with an Embedded database and one to be used with an SQL server. An ODBC DSN for either an SQL Server or Firebird must be configured before using the template.

- ODBC template

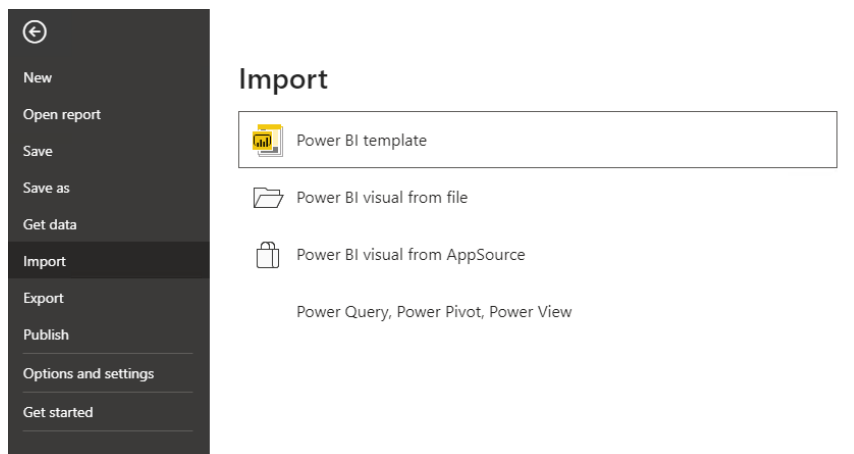


- SQL template



To import the template provided by MyQ , open Power BI and:

1. Open the **File** menu, select **Import**, and click on **Power BI template**. Find and open the correct template according to your database.



2. Establish the connection to your database:
 - a. For direct connection to an MS SQL server, add the **SQL Server** and **Database name** and click **Load**.

- b. For ODBC, add the **Data source name (DSN)** you created in the ODBC Data Sources app and click **Load**.

3. Power BI imports the data. The reports can be edited; the changes are saved in a different file so the template can be reused.

13.2.3 Report Examples

The examples below were generated using the MyQ templates.

Print date range

6/7/20186/14/2018



SAVINGS

PRINTED JOBS IN COLOR

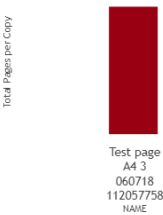
PRINTED JOBS IN B&W

1984
Total pages

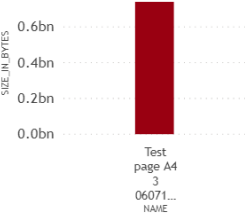
247

55

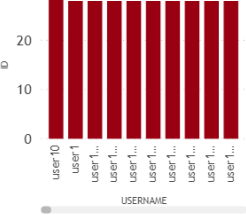
TOP JOBS BY TOTAL PAGES



TOP JOBS BY SIZE



TOP USERS BY NUMBER OF JOBS PRINTED

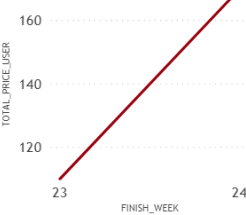


Date range

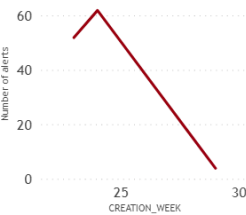
6/7/20186/14/2018



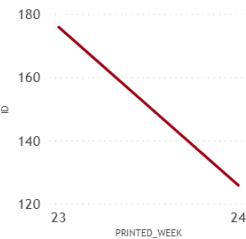
TOTAL COST PER WEEK



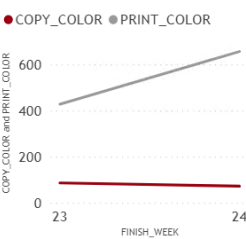
NUMBER OF ALERTS PER WEEK



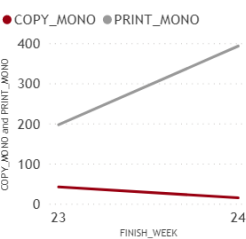
NUMBER OF JOBS PRINTED PER WEEK

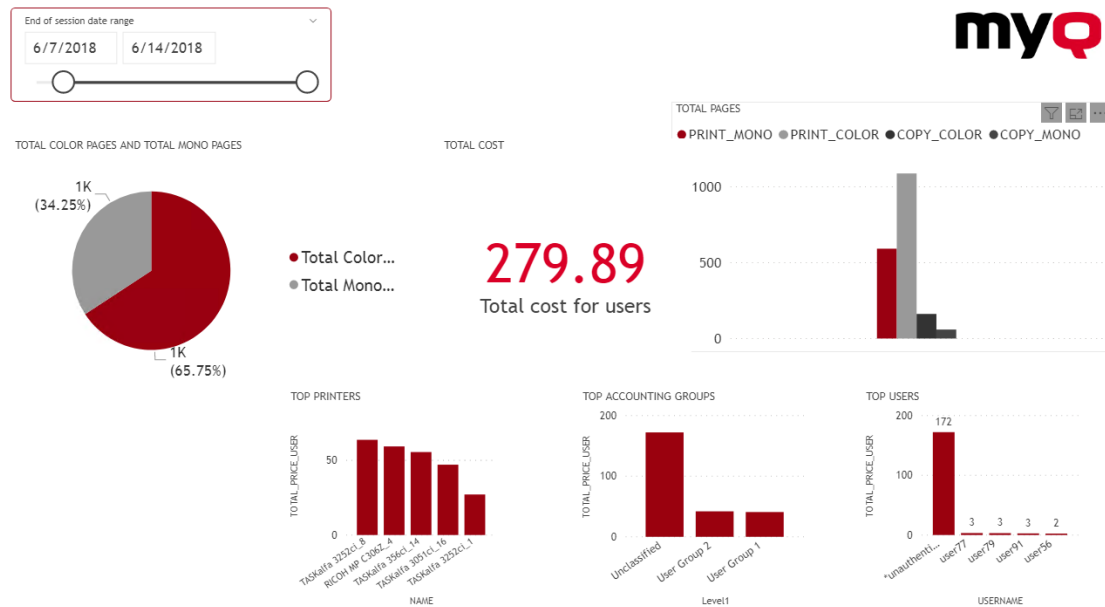


COLOR PAGES PER WEEK



MONO PAGES PER WEEK





13.2.4 Database Views Description

There are two groups of views; **dimensions** and **facts**. The fact views contain measures, numeric data which can be used in calculations for reports. The dimension views contain descriptive information used for the measures in the facts. Dimension views have the **dim_** prefix and fact views have the **fact_** prefix.

The IDs in the views are internal MyQ IDs and can be used to establish relationships between views.

Printer Dimension (dim_PRINTER_V2) - Information about the printer

Field Name	Description
ID	Printer ID
Name	Printer name
IP_Address	Printer IP address
MAC	Printer MAC address
Brand	Printer brand
Model	Printer model

Field Name	Description
Location	Printer location
Serial_Number	Printer serial number
ASSET_NUMBER	Printer asset number
CONTACT	Printer contact info
NOTES	Printer notes (memo text)
MODE	Printer mode. Values: 1 = Offline , 2 = Online , 8 = Local
IS_COLOR	Color printing. Values: 1 = Color print available , 0 = Monochrome print only
IS_COPIER	Copier function. Values: 1 = Copier , 0 = Copier function is not available
IS_A3	A3 paper format support. Values: 1 = A3 format is supported , 0 = No A3 format support
COPIER_COLOR_COUNTER	Total counter of color copies
COPIER_MONO_COUNTER	Total counter of monochrome copies
PRINTER_COLOR_COUNTER	Total counter of printed color pages
PRINTER_MONO_COUNTER	Total counter of printed monochrome pages

Field Name	Description
SCANNER_COUNTER	Total counter of scanned pages
FAX_COUNTER	Total counter of fax pages

User Dimension (dim_User) - Information about the user

Field Name	Description
ID	User ID
USERNAME	MyQ username
FULLNAME	User's name and surname
EMAIL	User's email
PHONE	User's phone number
PERSONAL_NUMBER	User's MyQ personal number
CREDIT	Credit amount (null - if credit is disabled for user)
LANGUAGE	User language
NOTES	Notes (memo text) to users account

Printer Events Fact (fact_PRINTER_EVENTS) - Information about printer events.

Field name	Description
Name	Name of the event
Type	Type of the event (alert or tonerLevel or totalCounter or tonerReplacement)

Field name	Description
Created	Date and time in which the event was created
Closed	Date and time in which the event was closed
Data	Data of the event (JSON example: <pre>{ "TONER_K.LEVEL": "8", "EVENT.TONER.INFO": "TK-8305Y", "TONER_C.LEVEL": "6", "TONER_K.INFO": "TK-8305K", "TONER_C.INFO": "TK-8305C", "TONER_M.INFO": "TK-8305M", "TONER_M.LEVEL": "0", "TONER_Y.INFO": "TK-8305Y", "TONER_Y.LEVEL": "6", "SUPPLY.INFO": "TK-8305C;TK-8305M;TK-8305Y;TK-8305K", "EVENT.TONER.LEVEL": "6" }</pre>)
Printer_Id	ID of the printer where the event was raised

Toner replacements (fact_TONER_REPLACEMENTS) - It provides certain data about printer toners that have been replaced and currently installed. This view combines the results of **V_TONERS_REPLACED** and **V_TONERS_INSTALLED** into one view.

V_TONERS_REPLACED

Field name	Description
Name	Name of the toner
Type	Type of the toner (cyan or magenta or yellow or black)
Installed	Date and time in which the toner was installed
Replaced	Date and time in which the toner was replaced
Counters	Total number of pages printed with the toner type of the toner until the toner was replaced

Field name	Description
Period	Number of days from the toner installation to the toner replacement
Pages	Number of pages printed by the toner
Printer_Id	ID of the printer where the toner was installed

V_TONERS_INSTALLED

Field name	Description
Name	Name of the toner
Type	Type of the toner (cyan or magenta or yellow or black)
Installed	Date and time in which the toner was installed
Replaced	NULL
Counters	Total number of pages printed with the toner type since the toner type installation
Period	Number of days since the toner installation
Pages	Number of pages printed by the toner
Printer_Id	ID of the printer where the toner was installed

Printer jobs counter fact (fact_PRINTERJOB_COUNTERS_V3) - Information about printer jobs counters

Field name	Description
PRINTERJOB_ID	Printer job Id
USER_ID	User Id

Field name	Description
USER_GROUP_ID	Group of users
PRINTER_ID	Printer Id
PROJECT_ID	Project Id (-56 for jobs without project)
SITE_ID	Site id
TYPE	Job type. Values: print , copy , scan , faxRx (Incoming fax -print), faxTx (Outgoing fax - scan)
PAYMENTACCOUNT	Payment Account. Values Credit , Quota , Cost Center
FINISH_DATE	Date when job was finished
FINISH_TIME	Time when job was finished
FINISH_YEAR	Year when job was finished
FINISH_MONTH	Month when job was finished
FINISH_DAY	Day of a month when job was finished
FINISH_HOUR	Hour when job was finished
PAPER_FORMAT	Paper format
DUPLEX	Duplex print. Values: Yes , No
SHEETS	Used sheets of paper
MONO	Monochrome print job

Field name	Description
COLOR	Color print job
SINGLE	Single color print job
PRICE	Job price
CLICK_MONO	Click mono
CLICK_COLOR	Click color
SESSION_ID	User session id
JOB_ID	Job id (Reference to user's job)

Job Fact (fact_job) - Information about print jobs

Field Name	Description
ID	Job ID
SESSION_ID	Session ID
NAME	Job name
OWNER_ID	Job owner ID
PRINTER_ID	Printer ID where the job was printed. Null if not printed
COMPUTER	Computer name or address where the job was sent from
SIZE_IN_BYTES	Job size in bytes
PAGES_MONO	Number of pages in black and white
PAGES_COLOR	Number of pages in color

Field Name	Description
DUPLEX	Duplex print. Values: 1 = Duplex , 0 = Simplex
COPIES	Number of copies
STATE	Job state. Values: Ready , Printed , Expired or deleted
PRINTED_DATE	Date when the job was printed
PRINTED_TIME	Time when the job was printed
CREATION_DATE	Date when the job was created
CREATION_TIME	Time when the job was created

Session Fact (FACT_SESSION_COUNTERS) - Information about sessions

Field Name	Description
ID	User session ID
FINISH_DATE	Date when session was finished
FINISH_TIME	Time when session was finished
FINISH_YEAR	Year when session was finished
FINISH_MONTH	Month when session was finished
FINISH_DAY	Day when session was finished
FINISH_HOUR	Hour when session was finished
USER_ID	User ID

Field Name	Description
PRINTER_ID	Printer id
PROJECT_ID	Project id
USER_GROUP_ID	User group id
TOTAL_PRICE_USER	Total price for the user
TOTAL_PRICE_ADMIN	Total price for the admin
TOTAL_PAGES	Total number of pages
PRINT_MONO	Printed pages in black and white
PRINT_COLOR	Printed pages in color
COPY_MONO	Copied pages in black and white
COPY_COLOR	Copied pages in color
COPY_SINGLECOLOR	Copied pages in single color
FAX	Faxed pages
SCAN	Scanned pages
PAPERA4	Pages in A4 paper format
PAPERA3	Pages in A3 paper format
PAPER_A5	Pages in A5 paper format
PAPER_B4	Pages in B4 paper format
PAPER_B5	Pages in B5 paper format

Field Name	Description
PAPER_FOLIO	Pages in folio paper format
PAPER_LEDGER	Pages in ledger paper format
PAPER_STATEMENT	Pages in statement paper format
PAPEROTHER	Pages in other paper format

Session Environmental Impact Fact (FACT_SESSION_ENV_IMPACT) - Information about sessions' environmental impact

Field Name	Description
ID	User session ID
CREATION_DATE	Date of the session creation
FINISHDATE	Date when session was finished
TOTAL_A4	Converted to A4 paper size units total pages amount
USER_ID	User ID
GROUP_ID	User group id
PRINTER_ID	Printer id
TOTAL_TREES	Approximate amount of trees used per session
TOTAL_CO2_GRAMS	Approximate amount of CO2 was produced per session (in gram units)
TOTAL_ENERGY_WH	Approximate amount of Energy consumed per session (in watt-hour units)

Field Name	Description
TOTAL_ENERGY_WH_RECYCLED	Estimated approximate amount of Energy will be consumed to recycle used amount of paper per session (in watt-hour units)

Printer Job Environmental Impact Fact (FACT_PRINTERJOB_ENV_IMPACT)

-Information about printer job's environmental impact

Field Name	Description
ID	Printer Job counter Id
PRINTERJOB_ID	Printer Job Id
TOTAL_TREES	Approximate amount of trees used per session
TOTAL_CO2_GRAMS	Approximate amount of CO2 was produced per session (in gram units)
TOTAL_ENERGY_WH	Approximate amount of Energy consumed per session (in watt-hour units)
TOTAL_ENERGY_WH_RECYCLED	Estimated approximate amount of Energy will be consumed to recycle used amount of paper per session (in watt-hour units)



There is a limitation that even if you are using a Job Privacy license, the data in the database are not changed by this feature and are still readable.

14 System Health Check

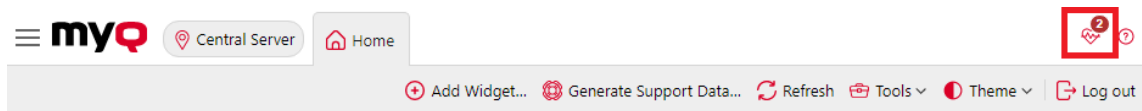
This option presents you with an overview of error messages with the level of severity added after some registered checks are done. The errors concern database health, disk space availability, PIN length settings and time zone configuration, etc. They are listed in the table below.

Code	Severity	Description
101	High	Main database health is not good; multiple messages can appear in the log
102	High	Log database health is not good; multiple messages can appear in the log
103	Medium	PIN length needs to be increased
104	High	Disk space is on warning level
105	Critical	Disk space is on critical level
106	High	Time zones misconfiguration
109	High	License subscription is going to expire
110	High	License Subscription expired
111	High	Contacting license server failed
112	High	HW code mismatch
113	High	License activation required
114	High	License expires soon

When the error message has a **Critical** severity, the administrator gets an email. Every error message with a **Low** severity is logged in the MyQ main log.

14.1 Using System Health Check

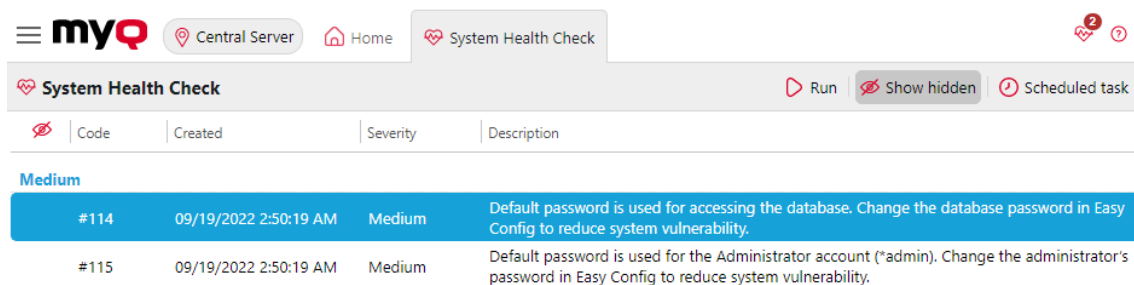
To access the system health check overview go to **MyQ, System Health Check**, or click on the system health check button on the top-right side of the window.



Click **Run** to trigger the System health check **Task schedule** to perform a check.

Click **Show hidden** to view any hidden checks on the list.

Click **Scheduled task** to open the System Health Check task in Task Scheduler, where you can view and modify it.



15 Uninstalling MyQ

To uninstall MyQ:

1. Run **unins000.exe**. You can find this file in your MyQ program folder (the default folder is: *C:\Program Files\MyQ Central Server*). The MyQ Uninstall dialog box appears.
2. Click **Yes**.

All parts of MyQ will be uninstalled except for the **Data Folder**. You can delete the folder manually. In case you install MyQ again, the installation program will ask if you want to use the old database files or replace them with new files.

16 Available languages

Language	Abbreviation
Arabic (Saudi Arabia)	ar
Bosnian (Bosnia & Herzegovina)	bs
Bulgarian (Bulgaria)	bg
Chinese (China)	zh-CN
Chinese (Taiwan)	zh-TW
Croatian (Croatia)	hr
Czech (Czech Republic)	cs
Danish (Denmark)	da
Dutch (Belgium)	nl-BE
Dutch (The Netherlands)	nl
English (United Kingdom)	en
English (United States)	en-US
Estonian (Estonia)	et
Finnish (Finland)	fi
French (France)	fr
German (Germany)	de
Greek (Greece)	el
Hungarian (Hungary)	hu

Language	Abbreviation
Icelandic (Iceland)	is
Italian (Italy)	it
Japanese (Japan)	ja
Korean (South Korea)	ko
Latvian (Latvia)	lv
Lithuanian (Lithuania)	lt
Malay (Malaysia)	ms
Norwegian Nynorsk (Norway)	no
Polish (Poland)	pl
Portuguese (Brazil)	pt-BR
Portuguese (Portugal)	pt
Romanian (Romania)	ro
Russian (Russia)	ru
Serbian (Serbia)	sr
Slovak (Slovakia)	sk
Slovenian (Slovenia)	sl
Spanish (Spain)	es
Spanish (United States)	es-US
Swedish (Sweden)	sv

Language	Abbreviation
Thai (Thailand)	th
Turkish (Turkey)	tr
Ukrainian (Ukraine)	ua-UA
Vietnamese (Vietnam)	vn
Welsh (Wales)	cy

17 Business Contacts

MyQ® Manufacturer	MyQ® spol. s r.o. Harfa Business Center, Ceskomoravska 2532/19b, 190 00 Prague 9, Czech Republic ID no. 615 06 133 MyQ® spol. s r.o. is registered in the Commercial Register at the Municipal Court in Prague, file no. C 29842 (hereinafter as "MyQ®")
Business information	http://www.myq-solution.com info@myq-solution.com
Technical support	support@myq-solution.com
Notice	MANUFACTURER WILL NOT BE LIABLE FOR ANY LOSS OR DAMAGE CAUSED BY INSTALLATION OR OPERATION OF THE SOFTWARE AND HARDWARE PARTS OF THE MyQ® PRINTING SOLUTION. This manual, its content, design and structure are protected by copyright. Copying or other reproduction of all or part of this guide, or any copyrightable subject matter without the prior written consent of MyQ® is prohibited and can be punishable. MyQ® is not responsible for the content of this manual, particularly regarding its integrity, currency and commercial occupancy. All the material published here is exclusively of informative character. This manual is subject to change without notification. MyQ® is not obliged to make these changes periodically nor announce them, and is not responsible for currently published information to be compatible with the latest version of the MyQ® printing solution.
Trademarks	"MyQ®", including its logos, is a registered trademark of MyQ®. Any use of trademarks of MyQ® including its logos without the prior written consent of MyQ® Company is prohibited. The trademark and product name are protected by MyQ® and/or its local affiliates.