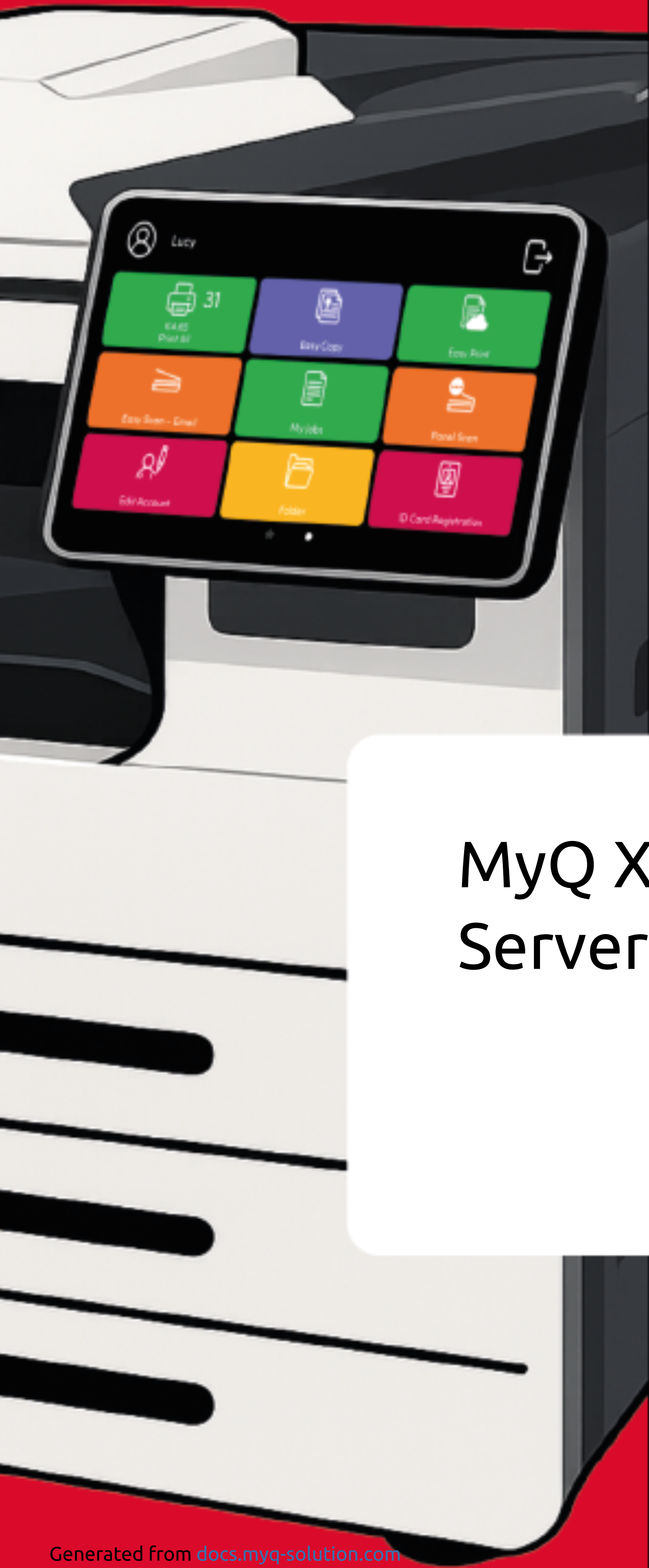


MyQ X Server 10.3 Central Server

Generated from docs.myq-solution.com
September/2026

ENGLISH

Table of Contents

MyQ Central Server 10.3 RC

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.

1 What's New in 10.3

Here's an overview of the new features included in MyQ 10.3 Print and Central Server.

1.1 Release Stations

A **Release Station** is a new browser-based kiosk application for secure job release on printers that don't have an embedded terminal. Use a Release Station to provide self-service printing solution, as a single device kiosk or a common printing room.

- Release Stations run in browser kiosk mode (for example, Microsoft Edge kiosk mode on Windows).
- Users log in to a Release Station using a PIN, ID card, or account credentials, then select a printer and release their queued jobs. Unknown ID card registration is supported.
- Each printer assigned to one or more Release Stations consumes an **Embedded Lite** license.
- Supports credit and quota accounting. Cost Centers accounting mode is not supported.

See also: (10.3) Release Stations

1.2 MyQ Scan Review

MyQ Scan Review works with the Easy Scan terminal action to create a document review workflow which supports replacement scanning processes. It enables organizations to capture paper documents, review scanned images, and maintain an auditable record of the scanning process before hard copies are archived.

Scan Review is a separately installed service that connects to an instance of Print Server. Specified MyQ users can then submit documents for review using the Easy Scan terminal action, and log into Scan Review directly to review and approve documents.

Features:

- Intended for organizations that must comply with regulatory requirements for trustworthy digitization, including Germany's TR-RESISCAN guidelines.
- Document queues can be configured with specific reviewers, destinations, protection levels and transfer note details.
- Reviewers can inspect scanned documents, search their contents, view metadata and approve or reject submissions.

- Approved documents can be delivered to local or network folders or SFTP servers.
- An audit log records relevant actions and can be searched and filtered by criteria such as user, document, date, queue and protection level.
- Each device set up with a Scan Review terminal action consumes an **Embedded Ultimate** license.

See also: (10.3) MyQ Scan Review

1.3 MyQ Document Processor (MDP)

MyQ Document Processor works with Easy Scan to process scanned documents and then forward them to the configured scan destination.

MyQ Document Processor is a separately installed service that connects to an instance of Print Server. Create an OCR Profile that uses MDP and assign it in Easy Scan Processing options of your terminal action.

Features:

- OCR processing with output formats including PDF, PDF/A, DOCX, XLSX, PPTX, and TXT.
- Split scanned documents by:
  - page interval
  - barcode/QR code separator page
  - matching barcode/QR code value
- Automatic blank page removal, with paper profile selection for accurate detection.

See also: (10.3) MyQ Document Processor

1.4 Delta Synchronization for Microsoft Entra ID

MyQ now supports delta (incremental) synchronization for Microsoft Entra ID sources using the Microsoft Graph API. When enabled, MyQ checks Entra ID for changes - new users, updated attributes, disabled or deleted accounts, group renames, and membership changes - since the last delta run, and applies only those changes. This allows the synchronization to run every few minutes instead of once a day, so changes in Entra ID reach MyQ much faster.

To enable this feature, open the Entra ID sync source in **MyQ > Settings > User Synchronization**, go to the **General** tab, and select **Enable delta synchronization**. Then enable the new **User Delta Synchronization** scheduled task (default interval:

10 minutes) to process all sources that have this option enabled. The existing full synchronization continues to run on its daily schedule and acts as a safety net.

See also: Synchronize Users from Microsoft Entra ID (see page 231)

1.5 IPP Pass-Through Mode for WPP-Compatible Queues

MyQ Print Server can now propagate the full set of IPP capabilities from the target printer to the MyQ queue. When a queue uses IPP pass-through, users printing over IPP or in Windows Protected Print (WPP) environments can access advanced print options, such as detailed stapling and punching combinations and tray selection, directly from the print dialog. This feature is supported for direct queues and pull print queues using IPP/IPPS output. For pull print queues, you can select which printer's capabilities are used as the source.

See also: (10.3) Jobs via IPPS

1.6 Require Authentication for IPPS Jobs

Added **Require authentication** option in **MyQ > Settings > Jobs > Jobs via IPPS**. When enabled, the IPP server enforces authentication for all IPP and IPPS print jobs and rejects unauthenticated requests. Enabling this option requires MyQ Desktop Client 10.2 patch 13 or later for Windows and patch 7 or later for macOS. Operating systems that do not support IPP authentication will not be able to print when this option is enabled.

See also: (10.3) Jobs via IPPS

2 Latest Release Notes

- Minimum support date: 1 February, 2026
- Minimum required version for upgrade: **10.2 Patch 24**

2.1 **MyQ Central Server 10.3 RC**

14 September, 2026

2.2 Security

- Improved security for CSV exports.
- Communication patterns unified with Print Server, the HTTP Proxy (Traefik) is now in use.
- A new helper is used for cloud connections.

2.2.1 Improvements

- Optimized the speed of long running database queries under certain conditions.
- Added the new Delta synchronization option for Entra ID, and a new scheduled task for lightweight, frequent synchronization.

2.2.2 Changes

- The EULA has been updated. You can view it during installation or upgrade.
- Modified Traefik rules to prevent server overload in case of too many MDC connections.
- Connections to Sites now require 10.2 or later.
- Removed option to set unsecure HTTP port.
- Updated Apache to 2.4.68.
- Updated Firebird to 4.0.7.
- Updated Microsoft Playwright to 1.62.0.
- Updated OpenSSL to 3.5.7.
- Updated PHP to 8.3.31.
- Updated Traefik to 3.6.19.

2.2.3 Bug Fixes

- Adding new delegates can cause user synchronization errors.
- Apache reports errors about missing environment variables to Event log.
- Creation of default backup folder fails during installation.

- Database sweep cannot complete on big databases in some cases because of too short timeout.
- Delegate removal was not reflected in user sync in some cases.
- Exporting users to CSV during user synchronization exports outdated users.
- Incorrect font scaling in generated PDF reports.
- Reordering synchronization sources can fail when the list of sources contains a combination of LDAP and CSV sources.
- Under certain conditions and with certain certificates the Web UI fails to load, with the message "ERR_SSL_PROTOCOL_ERROR".
- When the Printer Provisioning Profiles license package has been purchased multiple times, the displayed number of profiles was incorrect.

2.3 Component Versions

	Apache	Apache SSL	Firebird	PHP	PHP SSL	C++ Runtimes	Traefik
MyQ Central Server 10.3 RC	2.4.68	3.6.2	WI-V4.0.7.3271	8.5.9	3.5.7	VC++ 2015-2022 (**vc17**) - 14.40.33810	3.7.11

3 Licenses

When you become a MyQ customer, you select a license plan and a Software Assurance plan, and purchase the required number of licenses. Licenses are assigned to devices but can be transferred between them. Your licensing and Software Assurance are managed through a single **Installation Key**.

To activate a new installation, add your contact details and Installation Key in **MyQ > Settings > License**. See License Settings (see page 14).

3.1 License Plans

Your license plan defines your MyQ X edition and commercial model.

From MyQ X 10.3, the ULTIMATE license plan is retired. Customers with the legacy ULTIMATE license plan are automatically migrated to the ENTERPRISE plan with the corresponding number of Embedded licenses.

License Plan	Description
SMART	Free for commercial use after registration in the MyQ Community. Does not cover Embedded Terminals or support cases.
ENTERPRISE (Subscription)	Full MyQ X feature set. Renewed periodically, with Software Assurance included.
ENTERPRISE (Perpetual)	Full MyQ X feature set with no license renewal. Software Assurance is purchased separately.
ENTERPRISE for Government / Education	Enterprise editions for government and education customers.
Trial and NFR	A time-limited license plan for evaluation or demonstration, arranged through your MyQ Supplier.

ULTIMATE (Legacy)	Enterprise, plus support for the External Workflow (ScannerVision) terminal action. From 10.3, this license plan is no longer available. This license tier is automatically migrated to ENTERPRISE with the corresponding number of Embedded licenses.

3.2 Licenses

Licenses determine how many devices and provisioning profiles you can activate. You cannot exceed the available license count. When you deactivate a device, its license becomes available to use on another device.

Devices used for monitoring only are unlimited, but the server must have at least one Embedded or Embedded Lite activation available. Single-function printers consume one Embedded Lite activation.

License	What It Activates
Embedded	The MyQ X Embedded Terminal on one multi-function printer, including Smart Workflows (ScannerVision).
Embedded Lite	Any Embedded Lite terminal or device assigned to a Release Station. An Embedded Lite license consumes half of one Embedded license; the License widget shows this as fractional usage (for example, 0.5 of 52).
Embedded Ultimate	All Embedded features, plus Scan Review.
Printer Provisioning Profile	A single printer provisioning profile, which lets you deploy one or more printers (queues) to client workstations. Additional profiles let you deploy printers to different groups of users or computers.

3.3 Software Assurance

Software Assurance allows you to upgrade your MyQ system, open support cases with the MyQ support team, and more. Standard, Premium, and Premium Plus plans are available.

- Subscription licenses include Standard Software Assurance by default. To upgrade to a higher plan, contact your MyQ supplier.
- For perpetual licenses, Software Assurance must be purchased separately through your MyQ supplier.

The **License** widget shows your current Software Assurance plan and expiration date.

3.4 Installation Key

Each MyQ X deployment uses one Installation Key, whether it consists of a standalone Print Server or a Central Server with multiple Site Servers. The key is issued through the MyQ Community directly or through your MyQ supplier, and contains information about your:

- license plan
- licenses
- software assurance plan

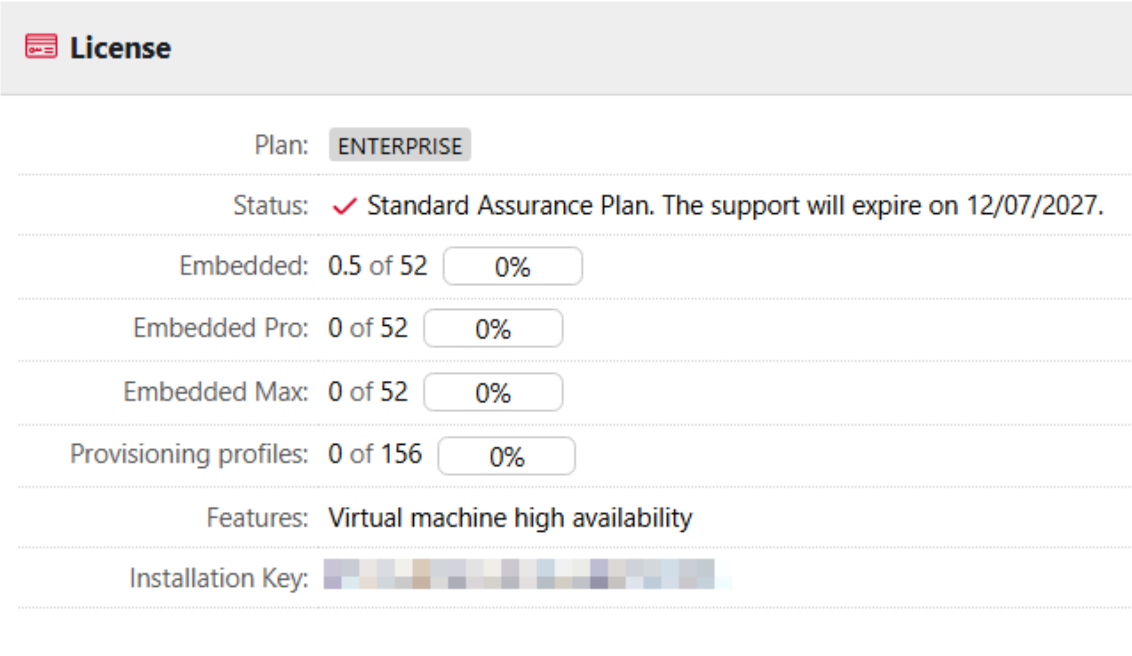
New licenses and software assurance extensions or upgrades are added to the existing Installation Key and synchronized to your MyQ installation.

See also:

- https://www.myq-solution.com/en/myq-x#myq-x-plans
- https://www.myq-solution.com/en/software-assurance
- License Settings (see page 14)
- (10.3) Release Stations
- (10.3) Configure ScannerVision

3.5 License Settings

Go to **MyQ > Settings > License** to activate and manage your Installation Key. The **License** widget on the **Home** tab summarizes your license plan, software assurance status, and license usage.



3.5.1 Adding Your Installation Key

You can add the Installation Key from the **Quick Start** widget or the **License** settings tab.

1. Enter your company and contact information.
2. Enter the Installation Key and click **Save**.
3. Click **Activate**.

3.5.2 Activation and Hardware Binding

Activation binds your installation key to the server's hardware configuration. If the hardware signature changes, reactivate the installation key within 10 days.

The **Virtual Machine High Availability (VMHA)** feature allows expected hardware-signature changes in virtual environments without requiring reactivation. VMHA is included with Enterprise licenses and is enabled by default.

VMHA requires the MyQ server to be a domain member, except in Microsoft Azure environments.

3.5.3 Updating Your License

After purchasing licenses or a Software Assurance plan extension or upgrade, click **Update from License Server**. Refresh the page if the changes are not displayed. For a server without internet access, use Manual Activation.

3.5.4 Expiration

The **License** settings tab displays the expiration or renewal date of your license plan. MyQ warns you before an expiring subscription impacts server operation.

3.5.5 Removing a License

Click **Remove license** on the **License** settings tab and confirm the action.

See also:

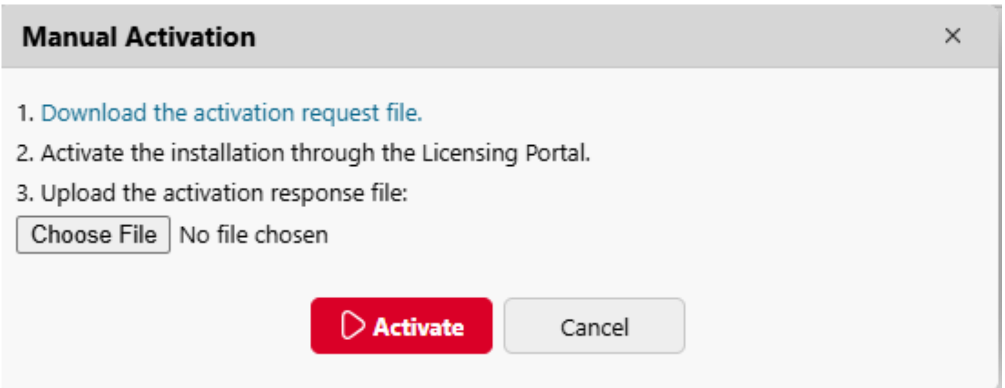
- Manual Activation (see page 16)
- Moving Licenses to New Hardware (see page 19)
- Troubleshooting Licenses (see page 20)

3.6 Manual Activation

If your MyQ server cannot connect to the MyQ License Server, for example in air-gapped deployments, use manual activation to add a new Installation Key, and every time you need to apply purchased licenses and software assurance extensions or upgrades.

To activate manually:

1. On the **License** settings tab, add your Installation Key (or click **Update from License Server** for an existing one), and click **Activate.**
2. When the connection to the License Server fails, select **Manual activation**.



3. Click **Download the activation request file** and save the file.
4. On a computer with internet access, sign in to the MyQ Community portal.
5. Open the relevant **Project**, go to the **Installations** tab and click **Offline activation.**

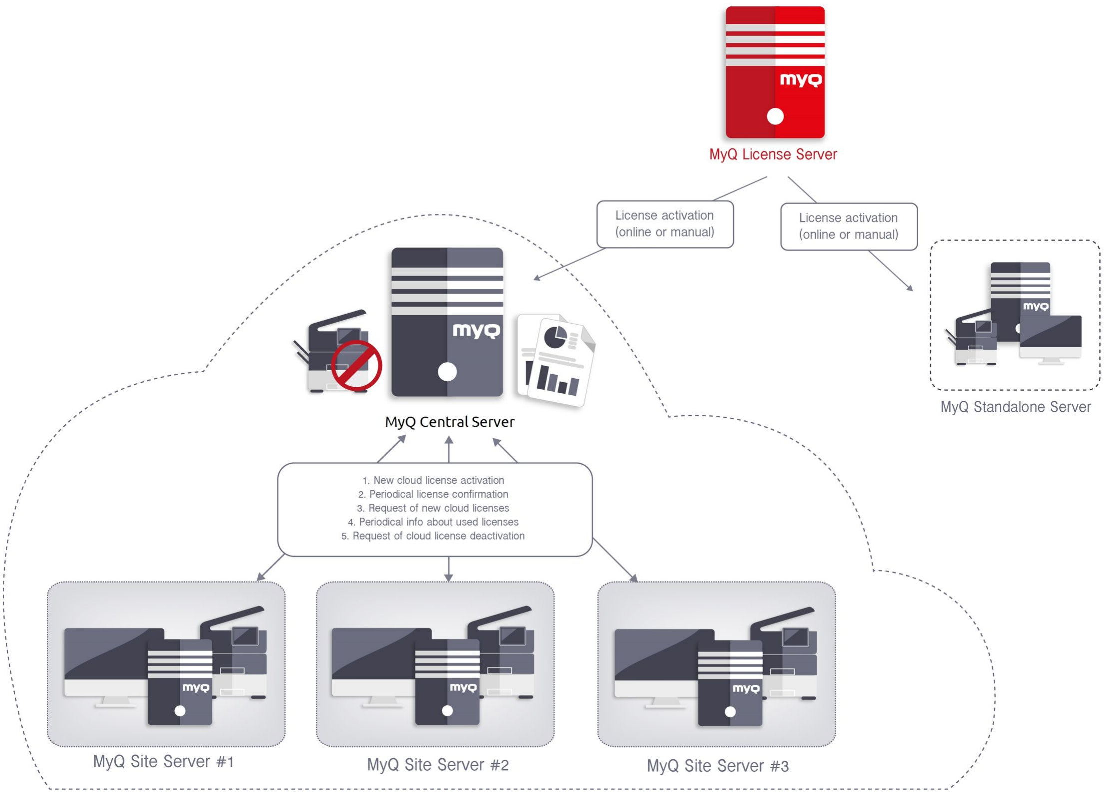
6. Upload the activation request file. The activation response file is downloaded automatically.
7. In the MyQ Web Administrator interface, upload the activation response file and click **Activate**.

Your license is now activated, and any newly purchased items are applied.

3.7 Distributing Licenses to Sites

In a Central Server deployment, activate the Installation Key on the Central Server only.

Licenses are then claimed from the Central Server by Site servers from the total provided by the installation key.



Then on each Site Server you specify the number of licenses that you want to provide to the Site. The amounts are deducted from the Central Server pool. If you remove licenses from a Site, they are restored to the pool. The balance of licenses in Central Server reflects current allocations to Site servers. If a license was claimed by a Site server but has not been assigned to a printer yet, it is counted as active from the Central Server perspective.

Embedded Lite does not have a separate central pool; an Embedded Lite consumes half of one Embedded license.

3.7.1 Planning the License Pool

The Installation Key must cover the combined allocations of all Site Servers.

Include all required Embedded, Embedded Lite, Embedded Ultimate, and Printer Provisioning Profile capacity when planning the deployment.

After purchasing additional capacity:

1. Update the Installation Key on the Central Server.
2. Adjust the Site Server allocations as needed.

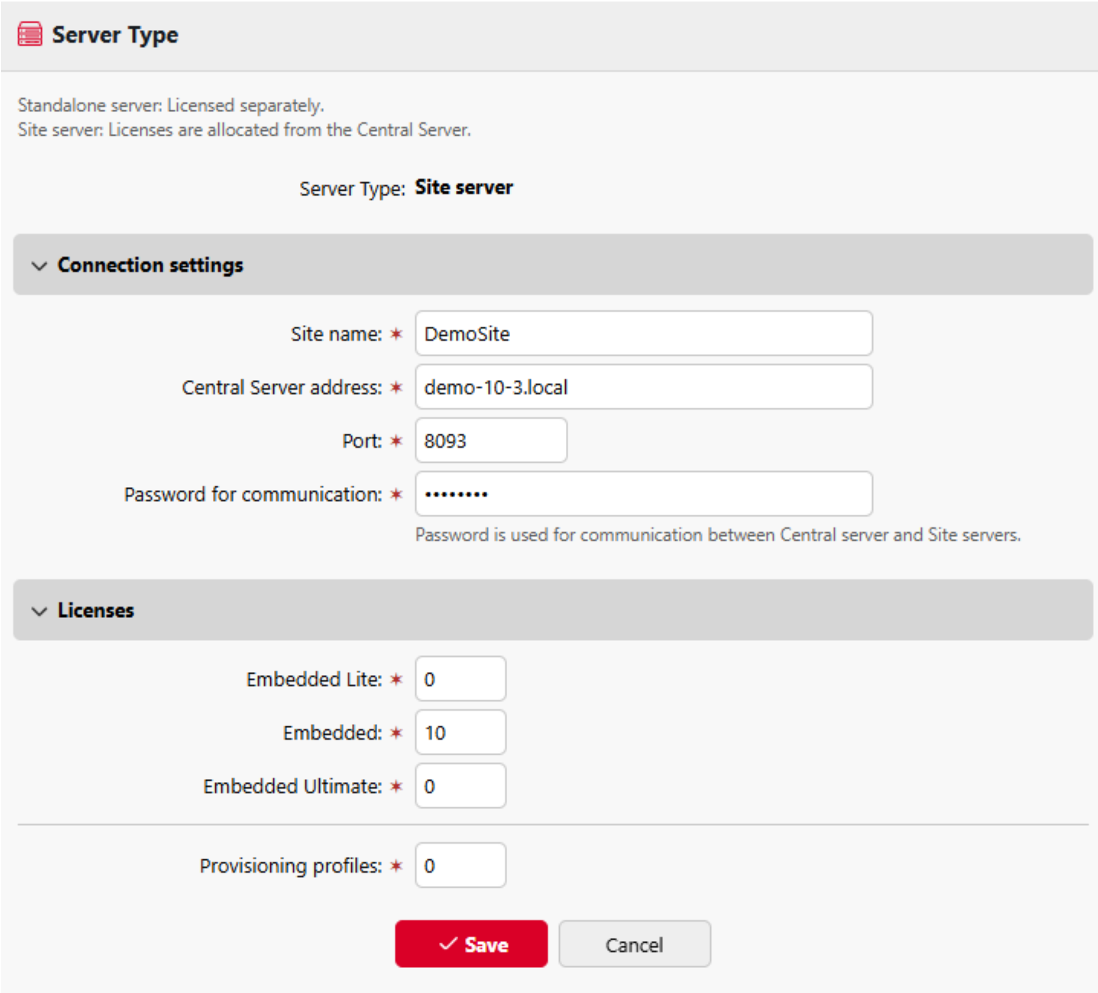
3.7.2 Allocating Licenses to a Site Server

Once your Installation Key is added and activated on the Central Server, log in to each Site Server and allocate the licenses it needs:

1. On the **Site Server**, go to **MyQ > Settings > Server Type.**
2. In the **Licenses** section, enter the number of licenses that you want to allocate to the Site:
   - **Embedded Lite**
   - **Embedded**
   - **Embedded Ultimate**
   - **Provisioning profiles**
3. Click **Save**.

   The Central Server subtracts the allocated licenses from its own pool.

If the requested allocation exceeds the available pool, the available amount is shown. Reduce the allocation or update the Installation Key before trying again.



See also:

- Licenses (see page 12)
- License Settings (see page 14)
- (10.3) Server Type Settings

3.8 Moving Licenses to New Hardware

Migrating MyQ to a different server requires license reactivation. Valid Software Assurance is required for migration.

Follow the standard server migration procedure to install MyQ on the new server and restore the database backup from the old server. You must activate the license on the new server within 10 days.

> ⚠ Never run the old and new MyQ servers with the same database at the same time.

After restoring the database:

1. On the old server, stop all MyQ services and set their startup type to **Disabled**. This prevents the server from attempting to reactivate after a restart.
2. On the new server, generate a Helpdesk support file in **MyQ > Log > Tools > Generate data for support**.
3. For an offline deployment, generate a support file on the old server as well.
4. In the MyQ Helpdesk partner portal, create a **License issue** support request and attach the support file or files.
5. After the reactivation request is approved, go to **MyQ > Settings > License** on the new server and activate the Installation Key.

The license on the old server is deactivated within 10 days.

3.9 Troubleshooting Licenses

License issues appear on the **License** settings tab or in an alert banner. Use the displayed message to identify the required action.

Status message	Action
The support expired on <date>.	Renew your Software Assurance through your MyQ Partner.
There were issues while connecting to the License Server.	Check the server's internet connection, and try again.
Your subscription is about to expire soon, all services will stop in 10 day(s).	Renew the subscription before the displayed deadline.
MyQ is not running: There is an issue with your license.	Check the details on the **License** settings tab, and contact your MyQ Partner if the license has expired.

Status message	Action
MyQ server cannot connect to License server, subscription cannot be prolonged and all services will stop in X days.	Restore the connection to the MyQ License Server, and click **Update from License Server**. For an offline server, use Offline Activation.
Server stopped working, because it cannot reach License server to update the subscription.	Restore the connection and click **Update from License Server**. For an offline server, use Offline Activation.
The hardware code has changed and the license must be reactivated. The server will stop working in 10 days.	Click **Update from License Server**. If this occurs repeatedly in a virtual environment, verify that VMHA is enabled.
The hardware code has changed and the license must be reactivated.	Click **Update from License Server**. If reactivation fails, contact MyQ support.

3.9.1 Central Server Deployments

Issue	Action
The license allocation cannot be saved on a Site Server.	The requested allocation exceeds the available Central Server pool. Reduce the allocation, or add the required capacity to the Installation Key and click **Update from License Server** on the Central Server before trying again.
An Embedded Lite allocation error reports the available Embedded count.	Embedded Lite is drawn from the Embedded pool; two Embedded Lite allocations consume one Embedded license. Reduce the Embedded Lite allocation or add Embedded capacity.
New licenses are not available for Site allocation.	Click **Update from License Server** on the Central Server, and then update the allocation on the Site Server.

See also:

- License Settings (see page 14)
- Manual Activation (see page 16)
- Moving Licenses to New Hardware (see page 19)

4 System Requirements

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

The estimates for Physical Core requirements below are based on AMD Ryzen Threadripper 1920X 3.5 GHz.

4.1 MyQ Central Server mode with integrated Firebird database

Users	1 - 10,000	10,001 - 50,000	50,001 - 100,000
Physical Core	6	6	6
RAM	8 GB	12 GB	16 GB

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
- Up to 30,000 printers total on MyQ Central Server.

4.2 MyQ Central Server mode with an external MS SQL database

MyQ Central Server

Users	1 - 10,000	10,001 - 50,000	50,001 - 100,000
Physical Core	4	4	4
RAM	4 GB	6 GB	6 GB

MS SQL Server

Users	1 - 10,000	10,001 - 50,000	50,001 - 100,000

Physical Core	6	6	6
RAM	12 GB	24 GB	32 GB

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
- Up to 30,000 printers total on MyQ Central Server.

4.2.1 Recommendations

- Install Windows updates during off-peak hours, and not during replication or user synchronization.
- Monitor server performance during peak usage hours and adjust the settings accordingly.
- For maximum performance, change the Windows Server power plan from Balanced (default) to High Performance (in *Control Panel – Hardware – Power Options)*. This may help speed up database operations.

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

4.2.2 Operating System

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

4.3 Additional Software Requirements

4.3.1 Microsoft .NET

.NET Framework 4.8 must be installed manually before running the MyQ installer.

.NET 8 is installed automatically during MyQ installation. If it fails to install, the MyQ installation cannot proceed. Install .NET 8 manually before retrying, with these components:

- .NET 8 Runtime
- http://ASP.NET Core 8
- .NET Desktop Runtime 8

We recommend enabling automatic .NET updates via Microsoft Update.

More information

- https://dotnet.microsoft.com/en-us/download
- https://devblogs.microsoft.com/dotnet/server-operating-systems-auto-updates/

4.3.2 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[1]. 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.

4.3.3 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

1. https://docs.microsoft.com/en-us/windows-server/get-started/server-core-app-compatibility-feature-on-demand

WebSocket notifications only work with valid certificates in some browsers. Some MyQ features may have limited functionality without them, and it's recommended to have them valid and installed on all client devices.

4.3.4 Storage

The MyQ Central Server installation files are approximately 300MB.

Minimum 10 GB 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):

Jobs	10,000	100,000	1,000,000
MYQ database	30 MB	200 MB	1.5 GB
MYQLOG database	30 MB	300 MB	3 GB

MyQ data folder storage counted for one year.

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

Jobs	10,000	100,000	1,000,000
MYQ database	500 MB	700 MB	7 GB
MYQLOG database	1 GB	1.5 GB	3 GB

MyQ data folder storage counted for one year.

4.3.5 Storage performance

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

4.3.6 MyQ Desktop Client Capacity (Patch 25+)

In a Central-Site deployment, the Central Server can assign clients to sites based on IP ranges.

On the minimum hardware, MyQ Central Server supports up to 50,000 MDC client logins within a one-hour window, with each site server able to handle up to 10,000 connections.

4.3.7 **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*.

4.3.8 Security

DigiCert Global Root CA certificate (required for Installation Key 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.

4.4 MyQ installation in Private Cloud

MyQ can also be installed in Private Cloud. For details, see Install MyQ in Private Cloud (see page 69).

4.5 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.

4.5.1 Incoming Ports

The server is listening on the following ports (private ports are not included):

Transport 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.

4.5.2 Outgoing Ports

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

Transport 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:

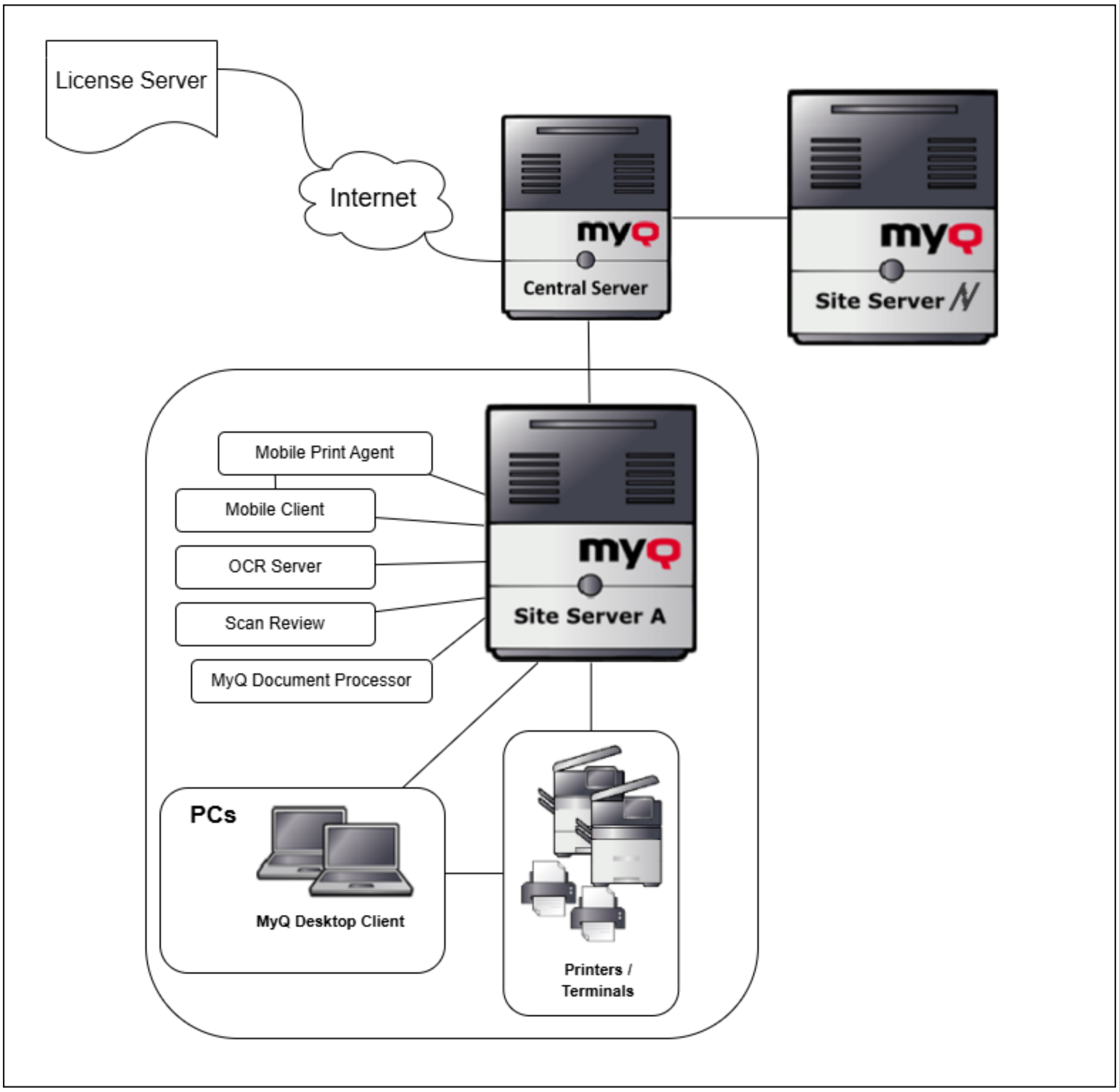
Transport Protocol	Port	Default	Description
TCP	Custom	**25/465/587**	Connection to SMTP server for sending outgoing emails from MyQ.
TCP	Custom	**389/636/1812**	Connection to Authentication server(s) (LDAP, Radius, ...) for user authentication/synchronization.
TCP	Custom	**8093**	Site server(s) connection.
TCP	Custom	**-**	Connection to External credit account.

4.6 Components Overview

MyQ X is a distributed system consisting of servers, client applications, embedded terminal packages, and supporting services. Use the diagram below to identify the components required for your deployment.

Consider how users will print, scan, authenticate, release jobs, use mobile devices, and access MyQ services. The components you need depend on your deployment model, printer fleet, authentication requirements, scan workflows, mobile printing, reporting, and availability requirements.

This page provides a planning-level overview of the main MyQ components. For installation, configuration, ports, and detailed requirements, see the relevant MyQ Server and component documentation.



1 MyQ Server Architecture

4.6.1 Core Server Components

Print Server / Site Server

Print Server is the core MyQ X component. It manages print, scan, and device operations, including printers, queues, jobs, users, embedded terminal communication, reporting data, and local system configuration.

Every MyQ X deployment requires at least one Print Server. Consider whether one Print Server is sufficient or whether the environment requires multiple Print Servers for scale, location-based printing, local resilience, or separate administration.

A **Site Server** is the same component operating as part of a Central/Site deployment. It is connected to a Central Server while continuing to handle local print, scan, and device operations at its site.

Central Server

Central Server is used in Central/Site deployments with multiple Site Servers. It provides central licensing, consolidated reporting, user distribution, and selected shared configuration for connected Site Servers.

Use Central Server when multiple locations or Print Servers require shared reporting, administration, user distribution, or coordinated management.

Central Server does not replace local Site Server administration. Site Servers still require local setup, monitoring, maintenance, backup planning, and site-specific configuration.

4.6.2 User-Facing Components

Embedded Terminals

Embedded terminals are applications installed on supported multifunction devices. They let users authenticate and access supported MyQ functions directly from the device panel, including print release, copying, scanning, and other terminal actions.

Use embedded terminals when users require secure access to device functions, authenticated print release, user-specific scan workflows, or accounting directly at the device.

Available functions and behavior depend on the device vendor and model, terminal package, license, configuration, and MyQ version.

MyQ Desktop Client

MyQ Desktop Client is installed on user workstations. Depending on its configuration, it can provide user authentication, job metadata collection, project or cost-center selection, local printer monitoring, client spooling, fallback printing, and other workstation-side printing features.

Use MyQ Desktop Client when printing must be controlled or enriched on the user workstation, particularly for project accounting, client spooling, fallback printing, local printer monitoring, or prompts before job submission.

MyQ X Mobile Client

MyQ X Mobile Client gives users access to selected MyQ functions from mobile devices.

Use MyQ X Mobile Client when users need features such as mobile printing or interaction with their print environment without using a workstation.

4.6.3 Supporting Components

Mobile Print Agent

Mobile Print Agent supports mobile printing through protocols such as AirPrint and Mopria. It is typically deployed where mobile devices need to discover printers or MyQ queues on the local network, such as a Wi-Fi segment used by mobile users.

Use Mobile Print Agent to provide AirPrint or Mopria printing from iOS, macOS, or Android devices.

MyQ Document Processor

MyQ Document Processor is a supporting service that performs document-processing operations for MyQ scan workflows. It processes jobs received from MyQ X and returns the resulting documents for delivery to their configured destinations.

Use MyQ Document Processor for scan workflows that require supported document-processing functions, including OCR and conversion to searchable document formats.

Document processing can require significant CPU, memory, and storage resources. Consider installing MyQ Document Processor on a separate machine, particularly in environments with frequent scanning or large documents.

MyQ Scan Review

MyQ Scan Review adds a review and approval stage to Easy Scan workflows. Users scan documents at a device as usual, after which authorized reviewers can inspect the scanned images and record the result of the review before the paper originals are archived.

Use Scan Review when the organization requires a documented and auditable replacement-scanning process. It is intended to support compliance workflows such as those based on Germany's TR-RESISCAN guidelines.

Scan Review requires additional planning for reviewer access, workflow responsibilities, metadata, document retention, and integration with the organization's archiving process. It supports the review workflow but does not by itself constitute a complete compliant archiving solution.

OCR Server (Deprecated)

OCR Server is a legacy supporting component used to perform optical character recognition in scan workflows, enabling output such as searchable PDFs and recognized text.

OCR Server is deprecated. For new deployments, use MyQ Document Processor where it supports the required document-processing workflow. Existing deployments should consider migration requirements when planning an upgrade.

Because OCR processing can require significant resources, OCR Server may need to run on a separate machine.

External Systems and Integrations

Depending on the deployment model and enabled features, MyQ X may depend on external systems such as identity providers, directory services, mail servers, cloud storage providers, licensing services, reporting tools, backup locations, monitoring systems, or BI tools.

Plan these dependencies early because they can affect authentication, user synchronization, scanning, notifications, reporting, firewall rules, certificates, availability, and support ownership.

See also:

- (10.3) MyQ X Server
- (10.2) MyQ Desktop Client
- (10.3) MyQ Scan Review
- (10.3) MyQ Document Processor
- (10.2) MyQ X Mobile Client
- (3.4) MyQ OCR Server
- (1.3) Mobile Print Agent

4.7 Network Architecture

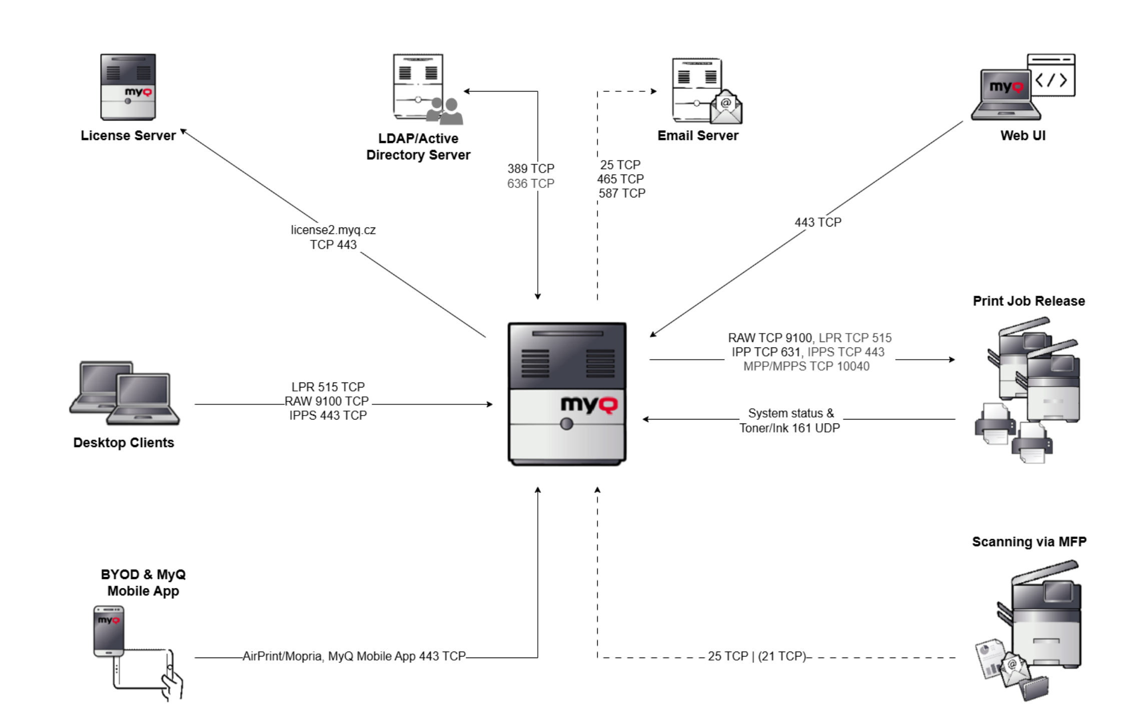
Network planning starts with identifying which MyQ components, clients, devices, and external services must communicate in your deployment. Focus on the paths used for printing, scan reception and delivery, authentication, administration, reporting, licensing, and any enabled integrations.

Use the diagrams below as a reference map before completing the checklist. Focus on the connections that apply to your environment, especially traffic that crosses sites, network zones, or external services.

⚠ These diagrams are planning references, not a comprehensive port matrix. The current port, protocols and version-specific defaults are in the MyQ X Server guide:

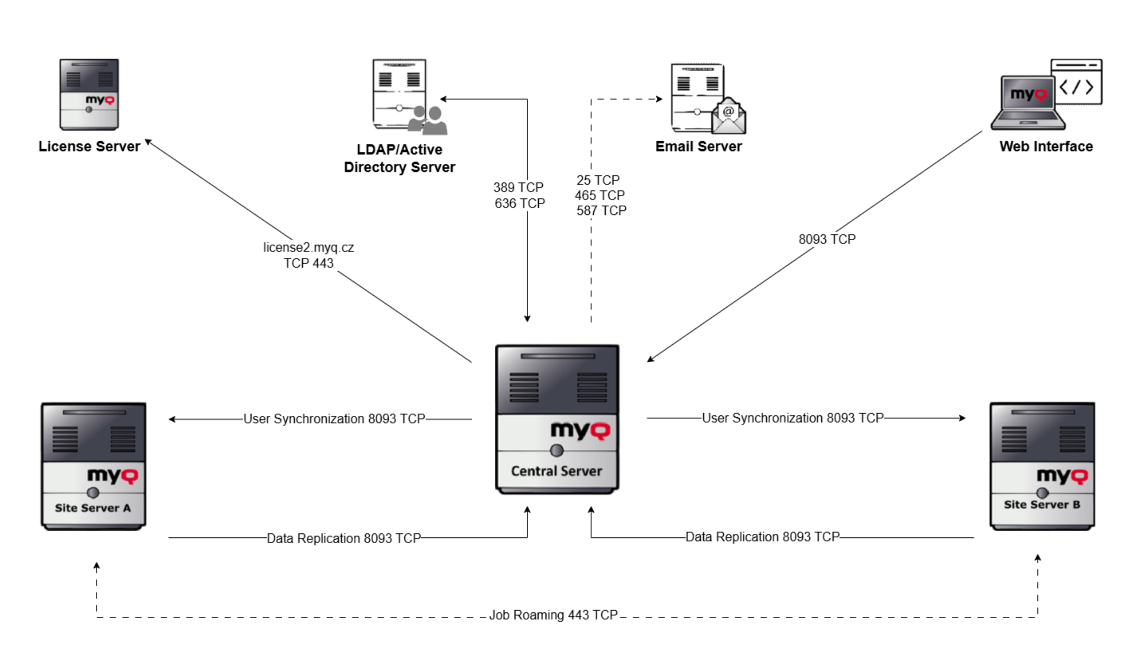
- (10.3) Main Communication Ports

4.7.1 Standalone Print Server



2 Print Server

4.7.2 Central/Site Environment



3 Central Server

4.7.3 Network Planning Checklist

Before deployment, confirm the main network paths that MyQ depends on.

1. **Server placement and site topology**

   Decide where each Print Server, Site Server, Central Server, OCR Server, and Mobile Print Agent will run. Place services close enough to users, printers, and required scan destinations to avoid unnecessary WAN dependency, especially where large print jobs or scan files would otherwise cross slow or unreliable links.
2. **Client, mobile, and user access**

   Confirm how users and workstations connect to MyQ, including MyQ Desktop Client, MyQ X Mobile Client, AirPrint, Mopria, and Mobile Print Agent where used. Consider users who move between sites and need access to jobs, printers, or cloud storage from different locations.
3. **Printer and embedded terminal communication**

   Confirm that MyQ servers can reach printers for monitoring, configuration, and print delivery. Also confirm the scan paths used in your deployment, including how scans are received from devices and how MyQ delivers scans to email, folders, cloud storage, FTP servers, or other configured destinations. Embedded terminals must be able to communicate with the required MyQ server, and any vendor-specific terminal requirements should be checked before rollout.
4. **Central, site, and identity communication**

   Confirm reliable communication between Central Server and Site Servers, including DNS, routing, certificates, and firewall rules. In cloud and hybrid deployments, this does not necessarily require a VPN between the Central Server and Site Servers; check the current cloud deployment and port requirements for the selected model. Also confirm access to the user sources and authentication services used in your deployment, such as LDAP/LDAPS directories, Microsoft Entra ID, Google Workspace Secure LDAP, RADIUS, or other configured authentication providers.
5. **External services, mail, scan, storage, and certificates**

   Confirm access to the external services used in your deployment, such as mail servers, scan destinations, cloud storage, licensing services, Microsoft or Google endpoints, remote backup locations, and monitoring systems. Define stable DNS names and certificate requirements before production, rather than relying on temporary hostnames or IP addresses.

6. **WAN resilience and rollout validation**
   Identify sites with slow, weak, or unstable links and decide whether they need a local Site Server, Client Spooling, Device Spooling, Offline Login, or another fallback option. Verify each fallback option against the relevant MyQ X Server, Desktop Client, and embedded terminal documentation before rollout. Before rollout, test the paths used in your deployment, such as printing, scan reception and delivery, authentication, embedded terminal login, mobile printing, reporting, remote backups, and expected behavior during network restrictions or outages.

5 Installation

This section describes 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 (see page 23).

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

1. Download the latest available MyQ X Central Server version from the MyQ Community portal (*MyQ X 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.

5.1 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.

5.1.1 Embedded Database Configuration

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

5.1.2 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.

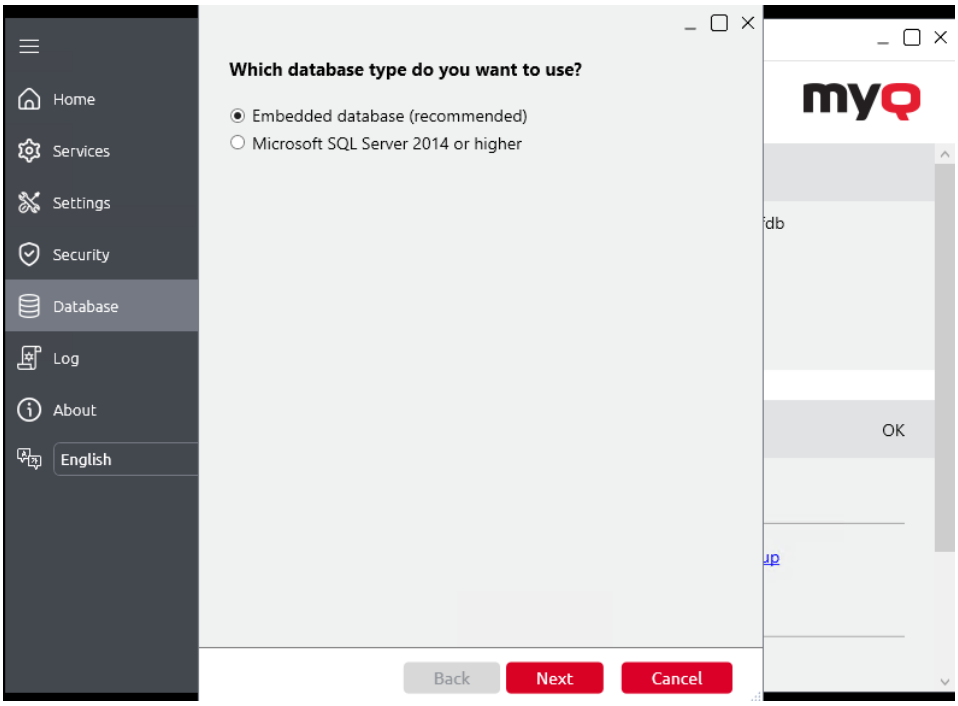
Once the MyQ Central server is installed, the MyQ Central Server Easy Config application opens and you are asked to select and set the MyQ database. The two following sections describe the setup of the database after the installation.

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

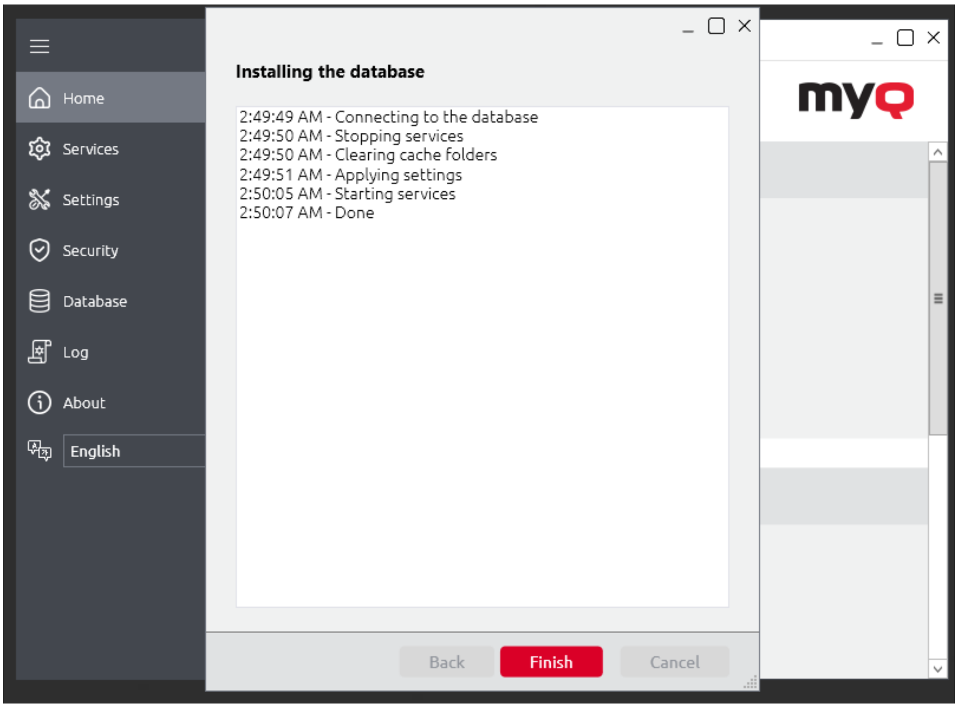
5.1.3 Setting up the Embedded Database

To set up the Embedded database:

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



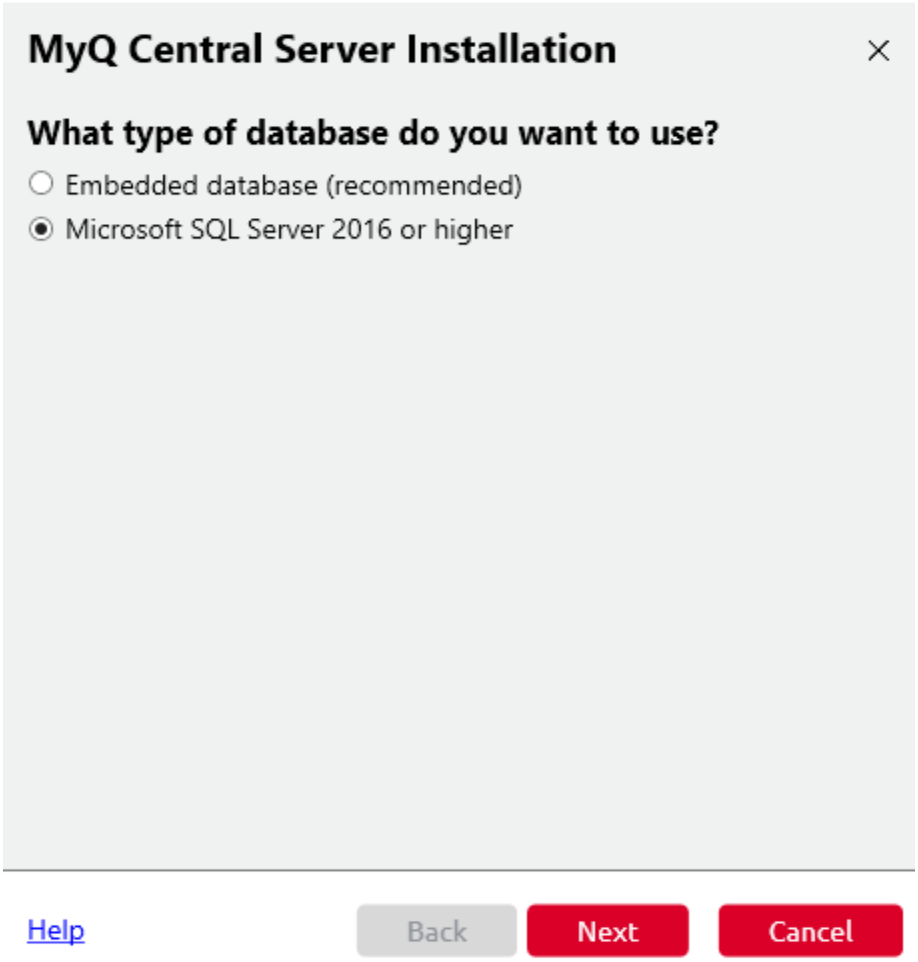
2. Click **Finish** to leave the MyQ Database Wizard.



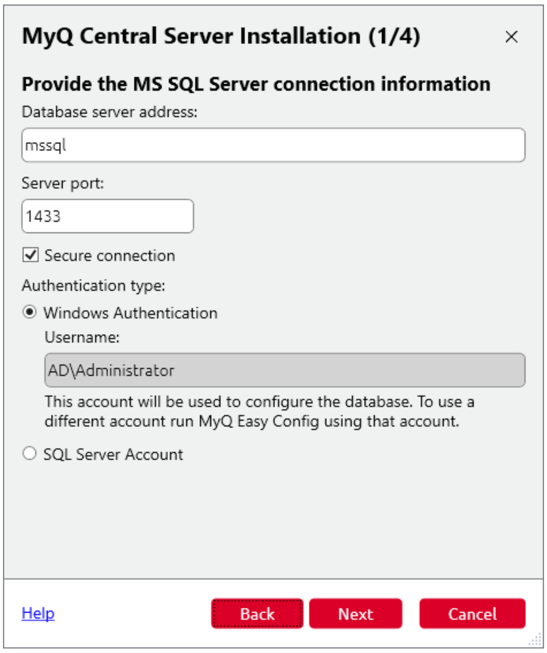
5.1.4 Setting up an MS SQL Database

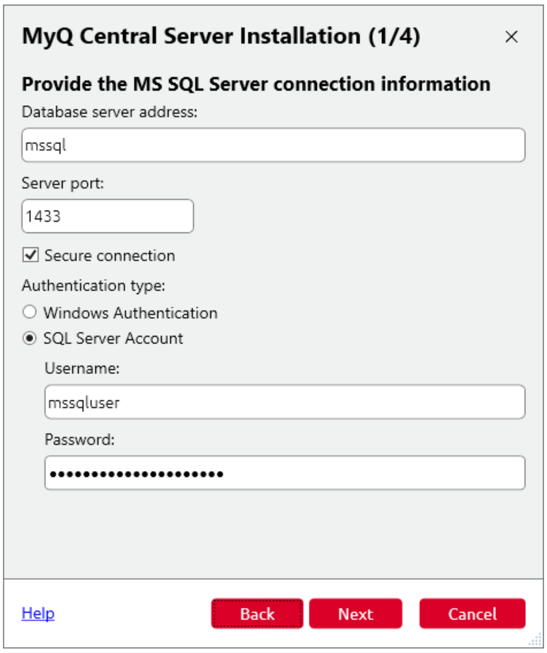
To set up an MS SQL database:

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

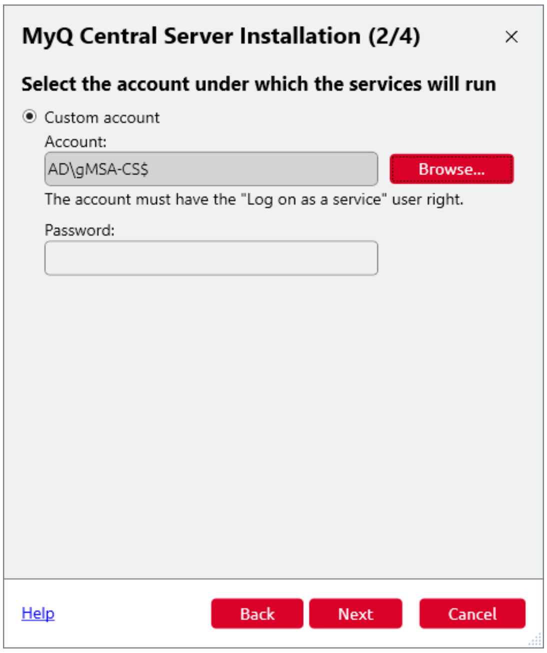


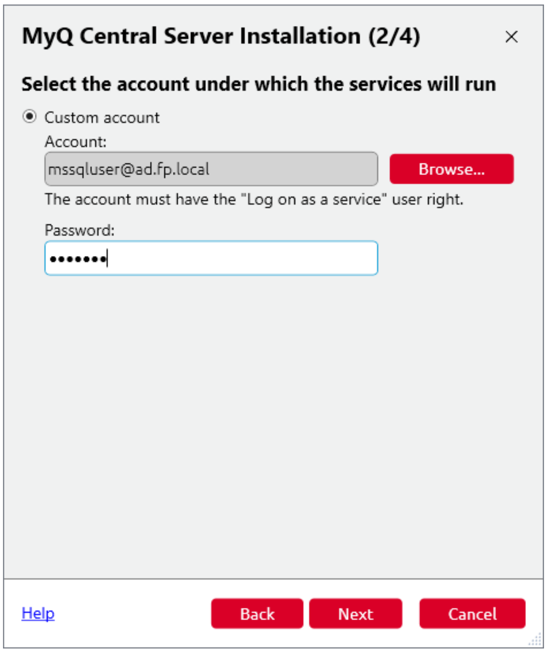
2. Fill in the setup fields with the following information:



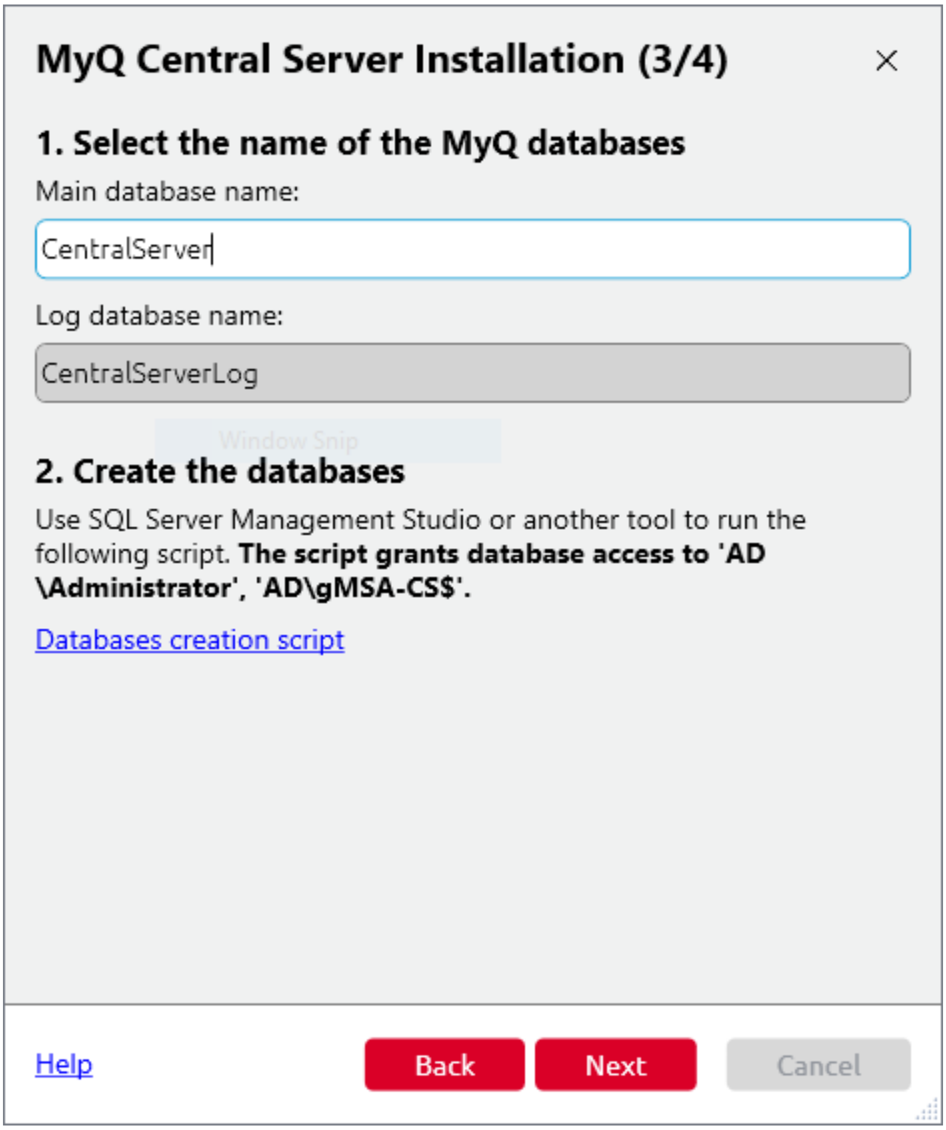


1. **Database server address**: the IP address or the hostname of the MS SQL server.
    a. **Server port**: TCP port used for communication with the MS SQL server; by default it is *1433*. In case of a Local database, the Server port field must be left empty.
    b. **Username/Password**: Login credentials 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.

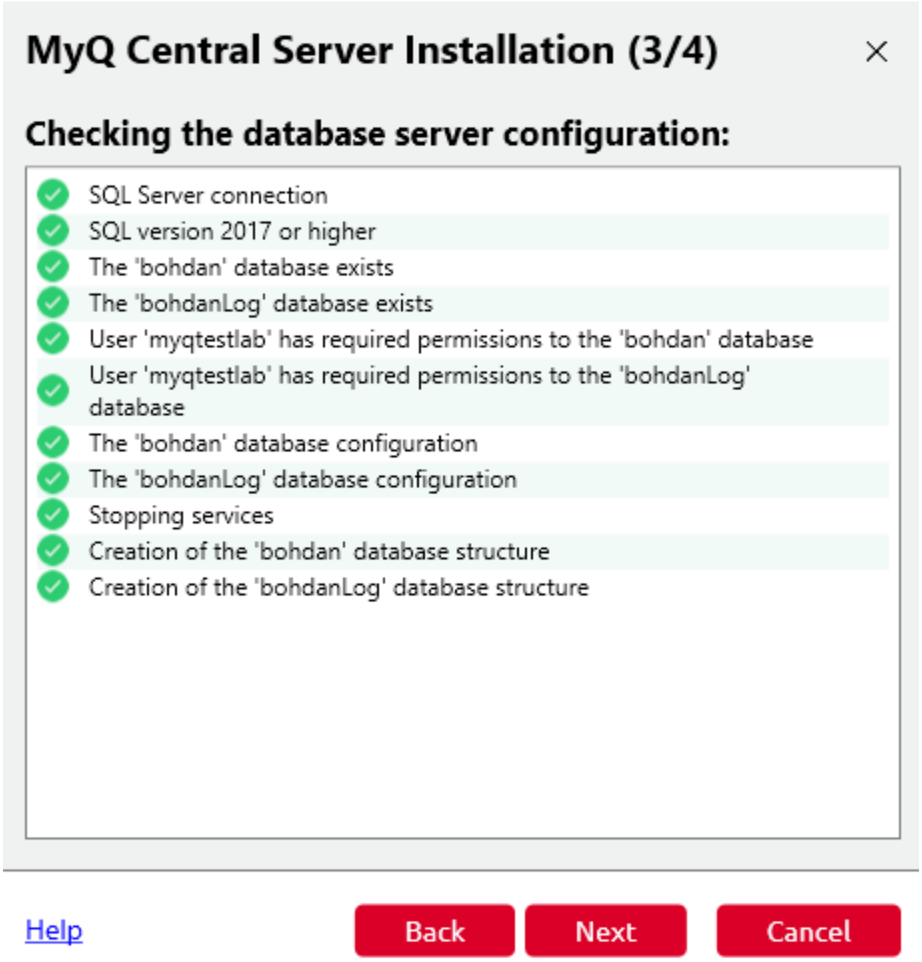




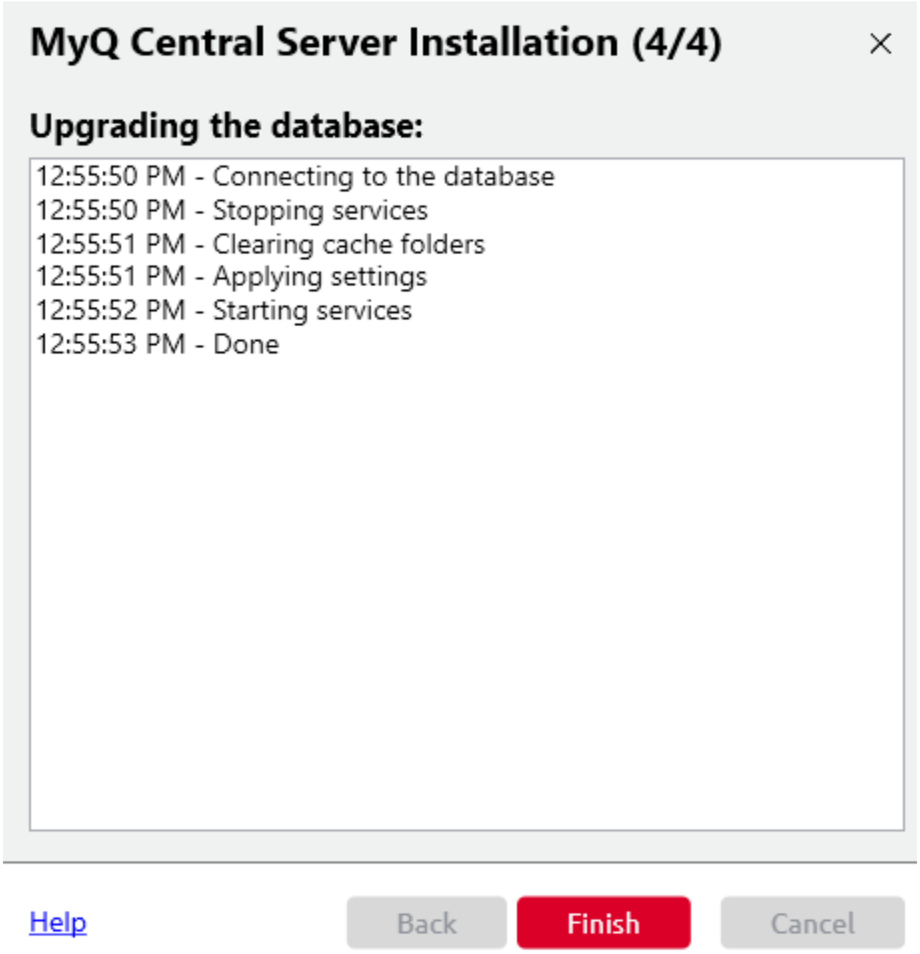
3. Fill in the **Main database name** (name of the new MyQ MS SQL database for example *MyQDatabase*), the **Log database name** is automatically filled according to the Database name and run the **Databases creation script**.



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.

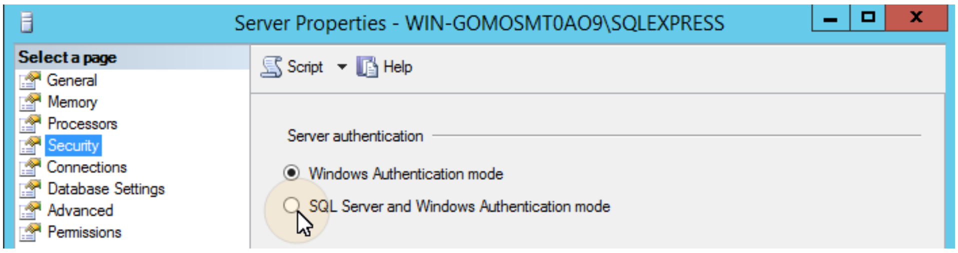


5.1.5 MS SQL Server Setup Example

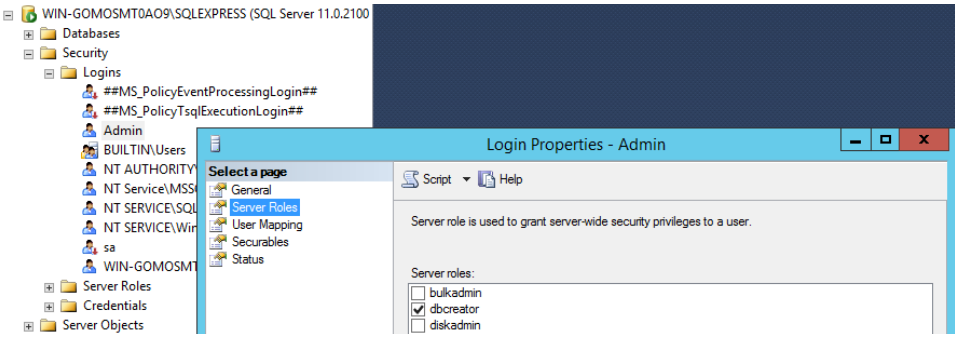
This is an example of an installation of a Microsoft SQL server and the setup necessary for its connection to the MyQ Central server.

To install and set up the MS SQL server:

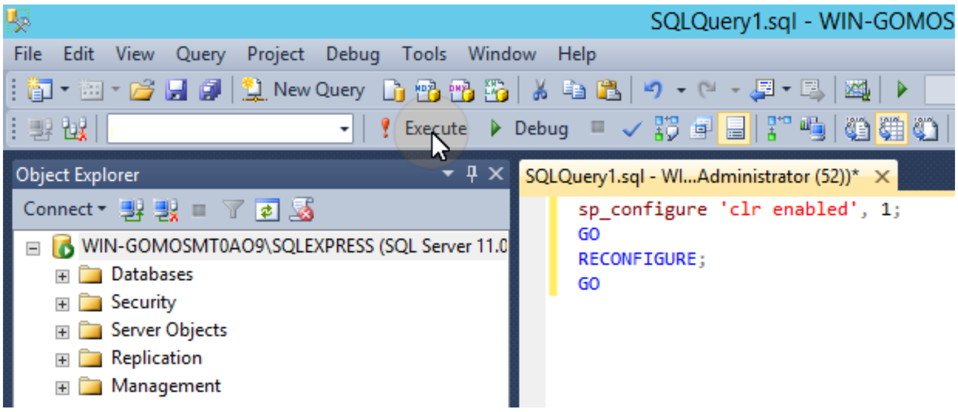
1. Install the MS SQL Server and the MS SQL Server Management Studio application.
2. Open the SQL Server Management Studio app (Windows Apps menu).
3. Change the **Server authentication** setting of the MS SQL Server from the *Windows Authentication mode* to *SQL Server and Windows Authentication mode*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



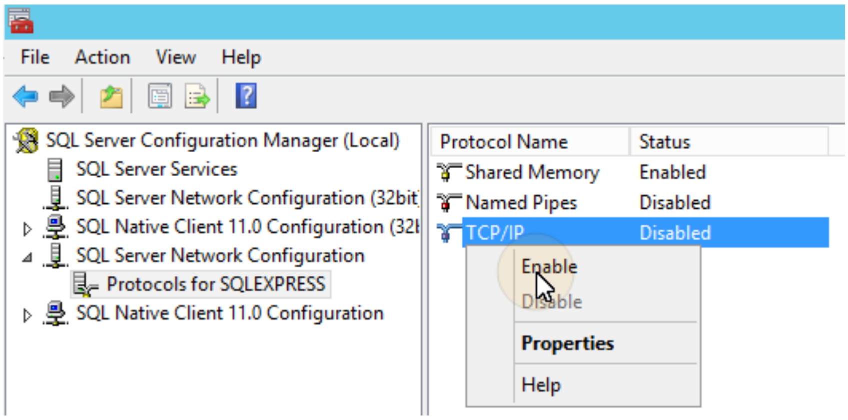
5. On MS SQL Server 2016 and older, you need to enable the common language runtime (CLR) integration feature. If you are using the MS SQL Server 2017 or newer, you can continue to the next step.



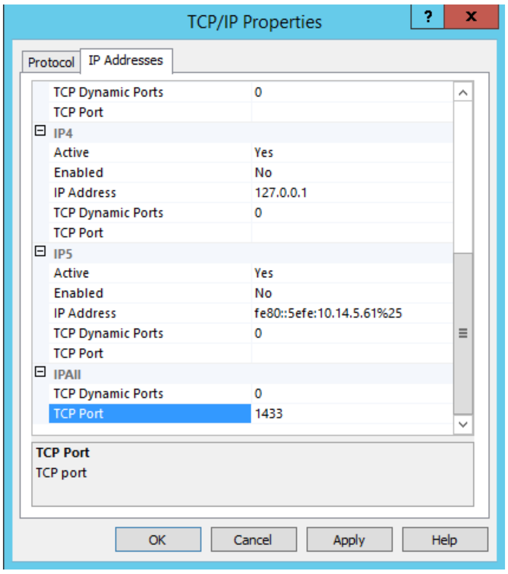
To enable the CLR, use the following script:

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

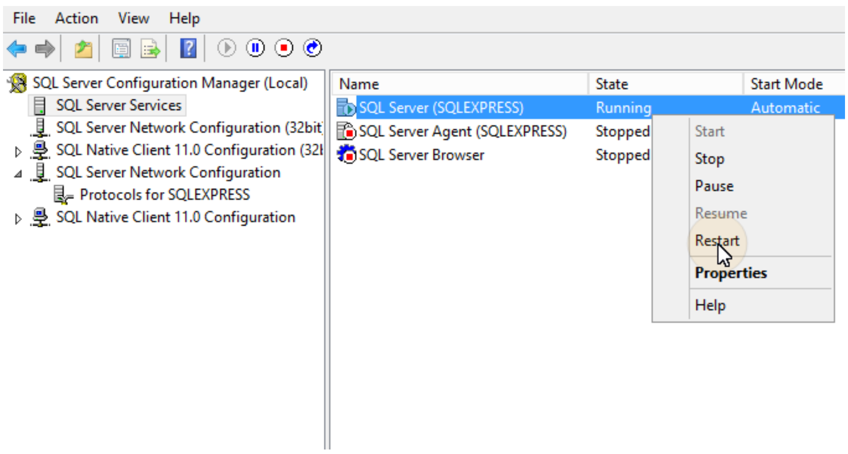
6. Leave the MS SQL Server Management Studio and open the SQL Server Configuration Manager app.
7. Enable the TCP/IP protocol.



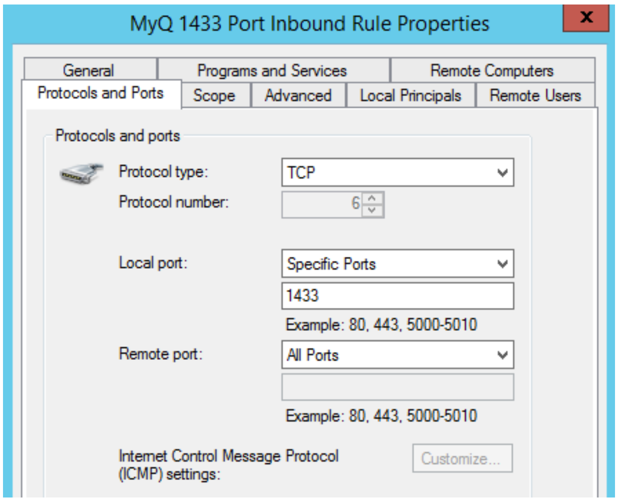
8. Open the TCP/IP properties and set the **IPAll TCP Port** to *1433*.



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.

5.2 Upgrading to MyQ 10.3

Planning your upgrade from 10.2 Patch 24+ to 10.3 ahead will help minimize the impact on operations and prevent emergency troubleshooting. Perform the upgrade during a scheduled maintenance window in your off-peak hours.

You can upgrade from 10.2 Patch 24 and later. To upgrade from an earlier version, you must first upgrade to 10.2 Patch 24, and then to 10.3.

Your MyQ provider can perform the upgrade for you or assist you with the procedure. This will minimize the downtime of your printing and document processing services.

5.2.1 Prepare For Upgrade

Before upgrading, verify that your server meets the hardware and software requirements, including free storage requirements, and that you have an active Software Assurance plan. Make sure that the additional packages or applications that are used in the your environment are available and are compatible with MyQ X 10.3.

5.2.2 Check Software Assurance Validity

The minimum support requirement is the Standard Software Assurance plan, with validity to date stated in the release notes**.** You must have a valid software assurance plan before you upgrade.

To check the validity of your software assurance plan, go to **MyQ > Settings > License**. If your plan has expired, purchase and activate the new plan and then perform the upgrade.

5.2.3 Free Storage Requirements

During the upgrade process, migration of the data and log databases can require significantly more storage space. Verify that both the system volume (which stores temporary files) and the application data volume have at least four times the storage space available than the total size of the data and log databases.

> We strongly recommend using an SSD hard drive for the installation of both the program and data parts of the application.

To view your current storage usage, check the size of your application data folder. The default location is `C:\ProgramData\MyQ`, or view the location in **Easy Config > Settings > Data folder**.

The database files are **MYQ.fdb** and **MYQLOG.fdb**.

When a MS SQL database is used, the SQL Server handles the temporary databases, which reduces the space requirements. However, we still recommend having at least 2-3 times the size of the SQL database of free storage on the disk.

> Running out of storage during an upgrade can break your MyQ server and may make the host operating system unstable.

5.2.4 Customizations and Custom Reports

If any customizations are running in the current installation, such as customized reports, scripts, or anything else that is not included in the standard setup, contact MyQ support first to verify whether they are compatible with version 10.3.

After finishing the upgrade, verify the MyQ Main Log to observe any errors and warnings, including those about incompatible customizations, and also test the customized functionality yourself.

5.2.5 Order of Component Upgrades

In a Central-Site configuration, always upgrade the Central Server before the Site Servers. Older Site Server versions continue to work with a newer Central Server, so sites can be upgraded gradually.

Upgrade MyQ components, as they apply to your environment, in the following order:

1. **Central Server**
2. **Print Server** (Standalone and Site Servers)
3. **Other server applications** – e.g. Mobile Print Agent, MyQ Document Processor, Scan Review.
4. **Client applications** – Desktop Client, Mobile Client, etc.

Always upgrade server components before client applications. Newer servers remain backward compatible with older clients and Site Servers, but the reverse is not guaranteed – upgrading clients before servers may cause issues due to backend changes such as REST API updates or new compatibility requirements.

5.2.6 Replace Helper URL in Manually Connected Cloud Services

MyQ X 10.3 uses a new helper URL for cloud services.

If your organization has registered applications in third-party cloud services that are configured in **Manual** mode (in **MyQ > Settings > Network > Connections**), you must update those registered applications with the new helper URL (`helper2.myq-solution.com`) before upgrading to ensure uninterrupted service.

5.2.7 Migrate Custom Traefik Rules

MyQ X 10.3 upgrades the bundled Traefik reverse proxy from c2.x to v3.6.x. The MyQ configuration is migrated automatically, but custom rules must be migrated manually.

These rules are in the file `traefik.custom.rules.yaml` in your application data folder (default location is `C:\ProgramData\MyQ\`). If that file is absent or empty, no action is needed. If you maintain custom rules, you must modify them to use Traefik v3 syntax before upgrading. For more information, see Migrate Custom Traefik Rules (see page 53).

See also:

- Latest Release Notes (see page 10)
- System Requirements (see page 23)
- Easy Config Database Tab (see page 104)
- (10.3) Supported Terminals and Applications
- Supported Products
- MyQ Product End-of-Life Policy[2]

5.2.8 Important Changes in 10.3

MyQ X 10.3 has important changes compared to previous versions. These changes include added, remove, and changed features of the system. Read this article carefully to understand the impact of such changes before you upgrade.

For details about new features, see What's New in 10.3 (see page 7)

Important Changes

ULTIMATE License Plan replaced by ENTERPRISE

MyQ X 10.3 introduces changes to the licensing model:

- The **ULTIMATE license plan** has been retired**.** During upgrade to 10.3, customers on this plan are migrated to **ENTERPRISE** with the corresponding number of Embedded licenses. The External Workflow (ScannerVision) feature is now included in the Embedded license.
- **The Embedded Ultimate** license is introduced. This license is assigned per device, and enables all Embedded features, plus **Scan Review** support.

License Assignment to Devices

Prior to MyQ X 10.3, licenses were assigned to devices silently and automatically. Now, you must assign a license to a printer according to its usage. Go to **MyQ > Printers > Action - Edit Printer > Licenses** and assign a license to a printer:

2. https://www.myq-solution.com/product-support-end-of-life-policy

- Embedded
- Embedded Lite
- Embedded Ultimate

See also: Licenses (see page 12)

OCR Profiles

MyQ X 10.3 introduces Hot Folder and MyQ Document Processor OCR profile types. You can now use both types of profile with difference Easy Scan actions at the same time.

During upgrade, 10.2 OCR profiles are migrated as follows:

- **Custom OCR Server → Hot Folder**
- **MyQ OCR Server** -> **MyQ Document Processor**
  If a profile's output format is not compatible with MDP, the profile is deleted, and any Easy Scan actions that used it are reset to the **Default** format.

Review your OCR profiles and Easy Scan actions after upgrading to confirm that all profiles were converted correctly and that no actions were unexpectedly reset.

See also: (10.3) OCR Profiles

Cloud Connector Helper URL

Before MyQ X 10.3, the cloud helper application for OAuth token exchange was hosted at `helper.myq.cz`.

Starting with 10.3, a new cloud helper application is used, hosted at `helper2.myq-solution.com`. This applies to all OEM variants (MyQ, KNM, aQrate).

Action required if you use Manual-mode Connections:

If your organization has registered applications in cloud services that are configured in **Manual** mode (in **MyQ > Settings > Network > Connections**), you must update those registered applications to add the new helper URL (`helper2.myq-solution.com`) before or after upgrading.

Connections configured in automatic mode are updated by MyQ and do not require manual action.

Traefik Upgrade - Migrate Custom Rules

MyQ X 10.3 includes **Traefik v3.6.x**, replacing the previous v2.x. If your environment uses custom Traefik rules, you must migrate the YAML file from v2 to v3 syntax.

See also: Migrate Custom Traefik Rules (see page 53)

Removed Features

OCR Server

Support for the standalone MyQ OCR Server was removed in 10.3. The feature is replaced by MyQ Document Processor (MDP), and existing **MyQ OCR Server** profiles are converted to **MyQ Document Processor** profiles.

Removed Terminal Support

10.3 removes support for the following legacy terminals:

- Recharge Terminal
- TerminalPro
- TCPCONV2 (including NET2USB Converter V2)
- Android Terminal

As alternatives, use native embedded terminals, the Release Station app, the Network Authentication Terminal, Embedded Lite terminals and job release via the MyQ X Mobile Client.

Terminal Manager is deprecated, and the legacy terminal RPC interface (`WebService_Terminal`) is disabled (since 10.2 patch 23). Installations that have these legacy devices in the database keep working (auto-detected), but no new deployments of this hardware/software are supported.

Migrate Custom Traefik Rules

MyQ X 10.3 includes an upgrade of the Traefik reverse proxy. MyQ's own configuration is migrated automatically. If you have custom rules, you need to edit your rules file to use v3 syntax.

This page is relevant only if you have a non-empty `traefik.custom.rules.yaml` file (default location `C:\ProgramData\MyQ\`).

Steps to Prepare Your Custom Rules File

1. Open `traefik.custom.rules.yaml`.
2. Review every router rule, middleware definition, and TLS option against the official Traefik v3 migration guide: Traefik V3 Migration Documentation[3]
3. Apply the required changes and save the file.

3. https://doc.traefik.io/traefik/migrate/v2-to-v3/

4. Run the MyQ upgrade.

Common v2-to-v3 Changes

The list below covers the most common changes. It is not exhaustive – cross-check your file against the official Traefik v3 migration guide for the complete set.

v2 syntax	v3 replacement
`ipWhiteList` middleware	`ipAllowList`
`Host("a", "b")` (multi-value matchers)	`Host("a") || Host("b")` (single-value with OR)
`Headers(...)` / `HeadersRegexp(...)`	`Header(...)` / `HeaderRegexp(...)`
`HostHeader(...)`	`Host(...)`
`PathPrefix("/foo", "/bar")`	`PathPrefix("/foo") || PathPrefix("/bar")`
`PathPrefix` with regular expressions	`PathRegexp("...")`
Path placeholders `{name}` inside matchers	`PathRegexp("...")` with a Go regex
`sslRedirect`, `sslTemporaryRedirect`, `sslHost`, `sslForceHost` headers options	`redirectScheme` middleware
`featurePolicy` headers option	`permissionsPolicy`
`stripPrefix` option `forceSlash`	Removed - no replacement
`tls.options.default.preferServerCipherSuites`	Removed - no replacement needed
`tls.caOptional` option	Removed - no replacement

When combining multiple matchers, note the v3 precedence rules: the NOT operator binds tighter than AND, which binds tighter than OR.

Traefik v3 can still process v2 rule syntax when `core.defaultRuleSyntax` is set to `v2` or when v2 syntax is configured for an individual router. This compatibility mode is deprecated and is expected to be removed in the next major Traefik version. Existing v2 rules may therefore continue to work temporarily, but they should be migrated to v3 syntax.

After Upgrading

Check `C:\ProgramData\MyQ\Logs\traefik.log` for the following errors, which indicate remaining v2 syntax in your custom rules file:

- `error while parsing rule`
- `headers configuration not valid`
- `unknown middleware`

If any appear, correct the relevant entries and restart Traefik.

See also:

- Traefik V3 Migration Documentation[4]

5.2.9 Run a Test Upgrade

Testing an upgrade in an isolated environment is the safest way to validate the upgrade process **without risking production downtime**. This is recommended for all MyQ deployments, and especially for large environments, Central–Site deployments, and High Availability (HA) setups.

The most common upgrade issues occur during **database upgrade**. The most reliable verification is to run the upgrade on a restored copy of the production database in isolation from your production network.

Use this procedure to:

- verify that the MyQ upgrade completes successfully.
- validate that MyQ services start correctly after the upgrade.
- confirm that core system data and settings remain consistent.
- collect usable troubleshooting documentation for MyQ Support if an upgrade fails.

4. https://doc.traefik.io/traefik/migrate/v2-to-v3/

This article applies to upgrades of MyQ X Print Server and MyQ X Central server.

Prerequisites

Required Access

- local admin access to the production server
- local admin access to the test server
- access to the MyQ installer for:
  - the production version (current)
  - the target version (upgrade target)

Test server requirements

- separate server or VM (recommended)
- a network adapter must be present (services may not start otherwise)

Recommended minimum resources

- CPU: 4 cores
- RAM: 8 GB
- storage: SSD recommended

You can use a test server with fewer resources than production, because it does not serve real users.

License

A separate license is not required.

Set Up Test Environment

Important!
Your test environment must be isolated from your organization's network and the internet.

An isolated test environment ensures that during the test upgrade, your system is blocked from:

- sending emails and notifications
- connecting to embedded terminals
- running directory synchronization
- interacting with real users or jobs

However, the environment still needs a network adapter and an IP address. We recommend that you use an internal-only network, for example, a Hyper-V “Internal Switch”.

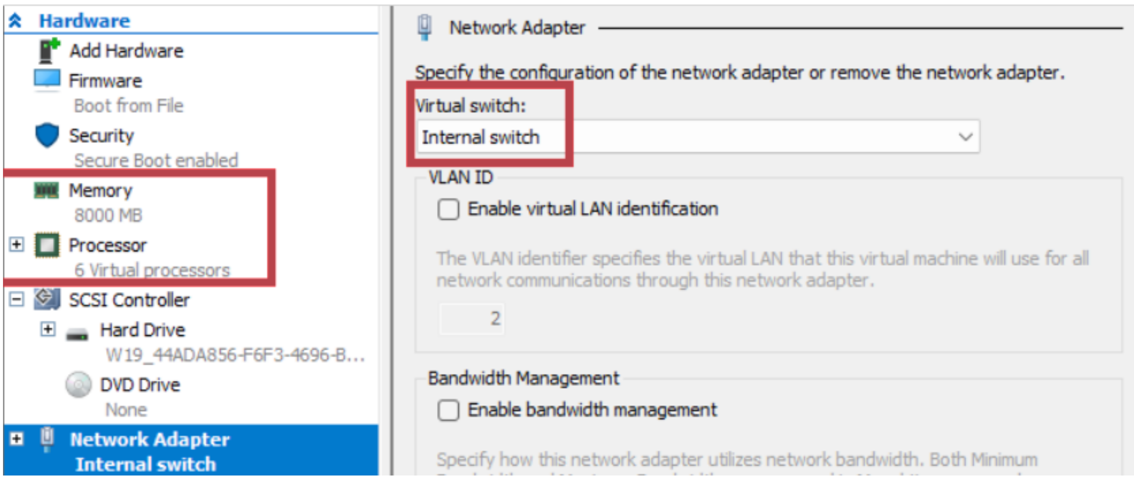
Prepare an Isolated Test Environment

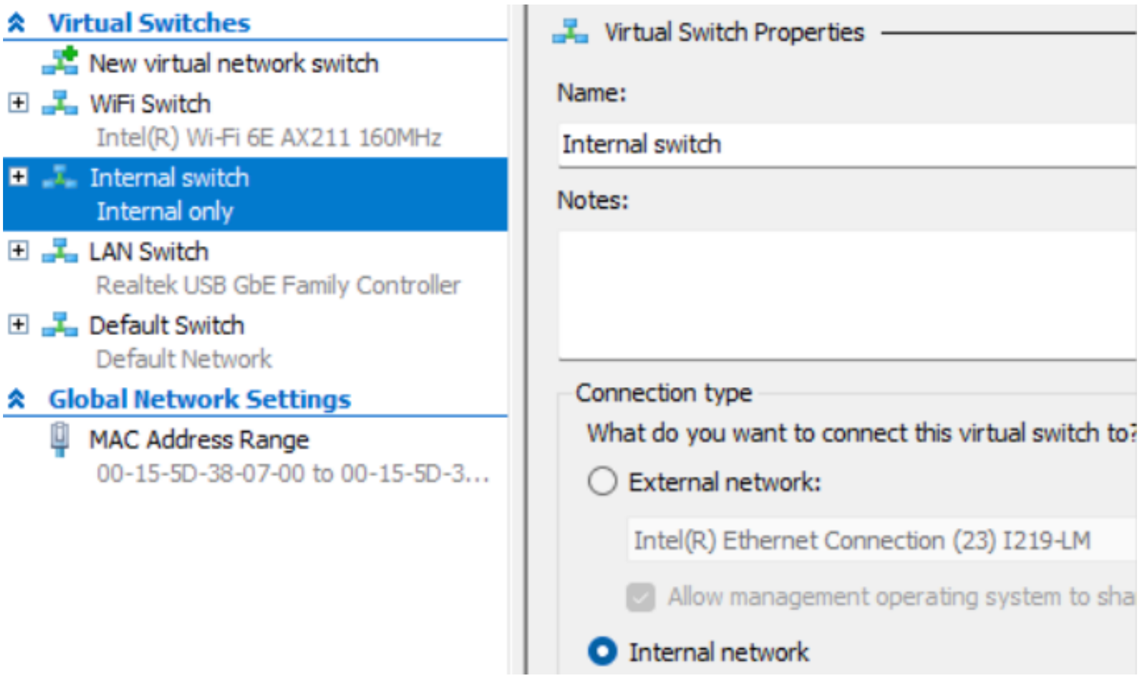
Follow these steps to create an isolated virtual server using Windows Hyper-V Manager.

> Alternatively, you can run an identical copy of your MyQ system in a network-isolated container. In that case, you must ensure that the container is not able to connect to any external network. With this set up, you do not need to copy job files or perform a data backup and restore – you can simply run the upgrade and check the results.

1. Create a test VM (recommended) or prepare a separate physical server.
2. Configure networking so that:
   - the VM has an IP address
   - the VM has no access outside the isolated network.
3. Set the hostname to match the production server hostname.

Example VM configuration with an internal switch:





Install the Production MyQ Version

You need the installer for the MyQ version in your production system. If you do not have the same version, contact MyQ Support.

Then, on the test server:

1. Install the production MyQ version.
2. Use the production installation setup:
    - same installation path
    - same drive letter
3. **Important!** Do not install the target upgrade version yet.

Back Up and Copy Data from Production to the Test Server

Create a full backup of the production server and transfer it to the test server. The backup contains all production data **except print job files**, which must be copied separately.

Default locations

- Backup directory: `C:\ProgramData\MyQ\Backup`
- Job files directory: `C:\ProgramData\MyQ\Jobs`

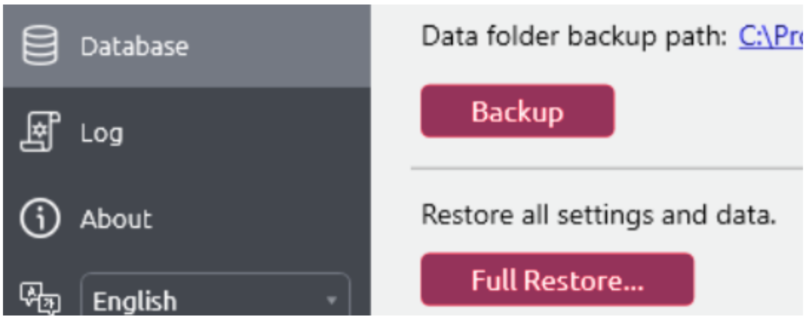
Steps

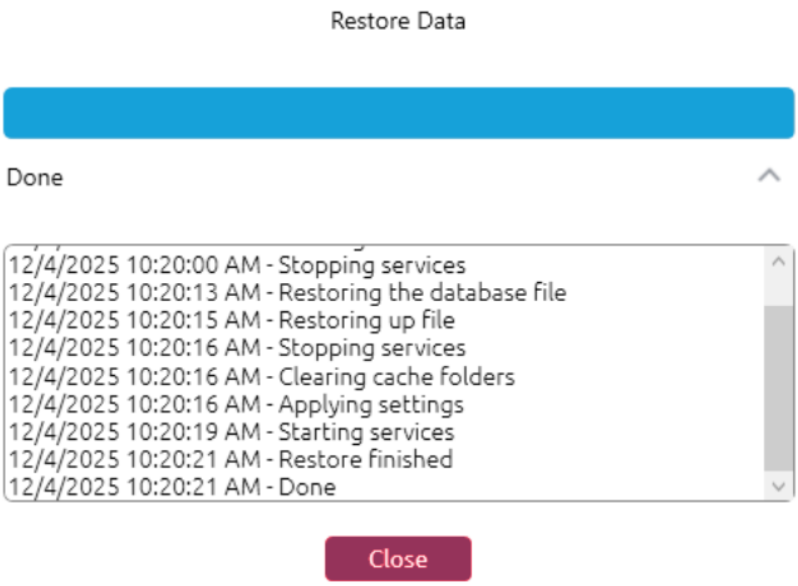
1. On the production server, create a full backup.
   The backup is saved as a `.zip` file in the backup directory. Note that for large deployments, backup creation may take up to an hour.
2. Copy the backup `.zip` file to the test server.
3. Copy the contents of the job files directory from the production server to the corresponding location on the test server.

Restore the Backup on the Test Server

On the test server:

1. Open **Easy Config**.
2. Go to the **Database** tab.
3. Select **Full Restore**.
4. Select the backup `.zip` file.
5. Run the restore.
6. Verify restore completion and service startup.





Run the Upgrade on the Test Server

On the test server:

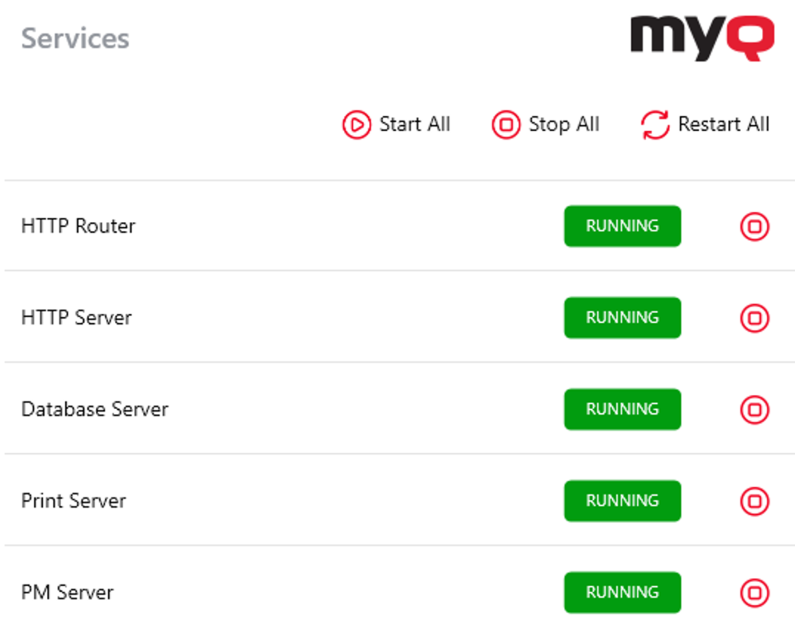
1. Run the installer for the target MyQ version.
2. Follow the standard upgrade procedure.

Post-Upgrade Verification

After the upgrade completes, verify minimum functionality.

> ⚠ In an isolated environment, warnings related to connectivity may appear (for example, notifications, device connections, or user synchronization). This is expected and you can safely ignore these warnings.

Verification	Expected result
Upgrade completion	Installer and Easy Config finish without error.
Services	Required MyQ services are running.
Web UI	MyQ Web UI opens successfully.
Data sanity	Key settings and data appear correct.



Next steps

If the test upgrade succeeds, proceed with the production upgrade.

If the test upgrade fails, stop and do not upgrade production. Contact MyQ Support, and provide:

- log files from the test server
- the production backup `.zip`

See also:

- Important Changes in 10.3 (see page 51)
- Generate Support Data (see page 117)

5.2.10 Perform the Upgrade

Perform the following steps during the scheduled maintenance window to upgrade MyQ X Server to version 10.3.

To run the upgrade, the logged-in user must have Local Administrator access.

Step 1. Disable MyQ Scheduled Tasks

At the beginning of the upgrade process, you should disable all scheduled tasks. This prevents any long-running tasks from interrupting the upgrade.

Go to **MyQ > Settings > Task Scheduler**, right-click all the tasks, and click **Enabled** to disable the given tasks.

For scheduled tasks that cannot be disabled, change the next scheduled run time.

Step 2. Stop Services

The installer attempts to stop all services. However, we recommend that you stop component services manually. This ensures that no users are logged in, and no tasks are in progress during the upgrade.

Go to **Easy Config > Services tab** and select **Stop All Services**. This may take a few minutes while the system waits for running tasks to finish correctly. Do not force-stop processes using Task Manager, as this may leave some tasks in an unfinished-state.

Step 3. Start the Database Server

For a successful upgrade of your system and database, your database service should be running.

If you are using the MyQ-provided Firebird DB, go to **Easy Config > Services** and manually start the Database Server service.

For installations using MS SQL, log in to the database server, open Windows Services and verify that the relevant SQL Server service has the status `Running`.

Step 4. Create a Backup/Recovery Point

The best time to back up the database is when all services have been stopped.

If your server is hosted on a VM, creating a snapshot is the most effective way to back up your system and date. If for any reason you need to rollback or abandon the upgrade, simply restore the VM to the snapshot.

Alternatively, to create a backup manually go to **Easy Config > Database tab** and select **Backup**. Store the backup in a secure location.

For Print Server, you must backup the Jobs folder manually. Copy the contents of the Jobs folder (by default `C:\ProgramData\MyQ\Jobs)` to a separate volume.

Step 5. Run the Upgrade

Close Easy Config, and run the MyQ X 10.3 executable to start the installation/ upgrade wizard.

1. Choose the language of the installation wizard and click OK.
2. The installer detects your current system. Click **Yes** to continue with the upgrade.
3. Accept the **License Agreement** and click **Next**.
4. (Optional) Choose whether to:
    - **Start services after installation** (default: Yes, recommended)
    - **Back up the database** (default: No)
      Creates a backup similar to Easy Config. This is typically not necessary if you created a backup already. **Note:** This option is sometimes force-enabled, for example if an update needs to modify the database engine.
    - **Clear the log** (default: Yes)
      (Recommended) This speeds up the upgrade process, and old log data is available in the backup if needed.
5. Click **Install**. The wizard completes the installation.

   After the wizard finishes, you have the option to complete the upgrade in **Easy Config**. This process will take time, especially with larger databases. Do not forcibly end this process.

⚠ If you are prompted to restart the system, first check if Easy Config is running.
If Easy Config is not running, proceed with the system restart.
If Easy Config is running, it may be performing a database upgrade. A restart will interrupt this process and may corrupt the database. Wait for Easy Config to finish, and then restart the system.

Step 6. Verify the Upgrade

1. When the database upgrade is complete, Easy Config opens on the **Home** tab.
2. Check **Easy Config > Services** to verify that all services are running.
3. Go to **Easy Config > Database** and expand Main Database and Log Database. Verify that the tatus for both is **OK**.
4. Go to **Easy Config > About** and confirm that the new version is displayed.
5. Launch the **MyQ Web Interface** and perform the following checks:

a. Go to **MyQ > Log** and search the logs for error messages.

b. Go to **MyQ > Settings > Licenses** and check that the license information is correct.

c. Go to **MyQ > Settings > User Synchronization** and confirm that your synchronizations are in place and correct.

d. In a Central-Site environment, go to **MyQ > Sites** and verify that the site status is **Ready**, and the replication status is **OK**.

e. Go to **MyQ > Settings > Scheduled Tasks** and check that scheduled reports generation is as expected.

Step 7. Perform Post-Upgrade Steps

Go to to **MyQ > Settings > Task Scheduler**, re-enable all tasks that you disabled, restore any schedules you temporarily changed, and verify the next run time of synchronization, replication, backup, maintenance, and report tasks.

See also:

- Upgrading to MyQ 10.3 (see page 48)
- Roll Back an Upgrade (see page 64)
- Troubleshooting Upgrades (see page 66)

5.2.11 Roll Back an Upgrade

Use this procedure if an upgrade to 10.3 fails or if critical problems prevent the upgraded system from returning to production.

You must have a backup or virtual-machine snapshot created before the upgrade. To roll back Print Server, you must also have a copy of the Jobs folder.

Rollback restores the system to its state before the upgrade. It is not an in-place downgrade: do not run a 10.2 installer over a 10.3 installation or attempt to use a database that has already been migrated to 10.3.

Before you Begin

Make sure that you have:

- The pre-upgrade database and settings backup
- If your deployment uses MS SQL, a backup of the MS SQL database, or snapshot of the VM where it runs.
- The installer for the exact MyQ X 10.2 patch that was installed before the upgrade.
- A copy of the Print Server Jobs folder, if applicable.
- Local Administrator access to the system where MyQ X is installed.
- (Recommended) A VM snapshot or checkpoint created from your MyQ Server VM before the upgrade.

> ⚠ **Central-Site Considerations**
> If you are rolling back a Central Server, first roll back all Site Servers. If only one site needs to be rolled back, other sites and the central server can remain on 10.3.

Option 1: Restore a Virtual-Machine (VM) Snapshot

Use this method when a snapshot was created immediately before the upgrade.

1. Shut down the MyQ server VM.
2. Restore the pre-upgrade snapshot. If you use MS SQL, restore your database or the VM where it runs.
3. Start the VM where your MyQ Server runs.
4. Open **Easy Config** and verify that:
   - Verify that all required services are running.
   - The Main Database and Log Database statuses are **OK**.
   - The expected MyQ X 10.2 version is displayed on the **About** tab.
5. Continue with **Verify the Rollback**.

Option 2: Reinstall MyQ X 10.2 and Restore the Backup

Use this method when a VM snapshot is not available.

1. Stop all MyQ services.
2. Uninstall MyQ X 10.3 and restart the system.
3. Manually delete any remaining files in `C:\ProgramData\MyQ` and `C:\Program Files\MyQ` and restart the system again.

4. Install the exact MyQ X 10.2 patch that was installed before the upgrade.
   Use the same installation path, application-data path, and drive letters as the original installation.
5. Go to **Easy Config > Database** and restore the backup created before the upgrade.
6. (MS SQL) Restore the database backups (main and log database) on the MS SQL server.
7. (Print Server) Restore the backed-up contents of the Jobs folder to its original location.
8. Start all MyQ services.

Verify the Rollback

After restoring the system:

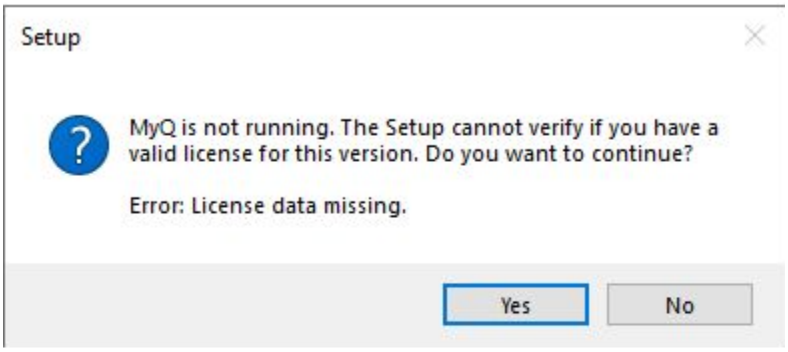
1. Open **Easy Config** and verify that all required services are running.
2. Verify that the Main Database and Log Database statuses are **OK**.
3. Confirm that the expected MyQ X 10.2 version is displayed.
4. In the MyQ Web Interface, go to **MyQ > Log** and check for errors.
5. Verify:
   - Licenses
   - User synchronization
   - Scheduled tasks
   - Central-Site connection and replication, if used
   - Printer and terminal connectivity
6. Submit and release a test print job.
7. Perform a test scan, if scanning is used.

> If the rollback cannot be completed successfully, stop further recovery attempts and contact MyQ Support. Provide the installer logs, MyQ support data, the source and target versions, and details of the backup or snapshot used.

5.2.12 Troubleshooting Upgrades

Setup Cannot Verify License

If a site server has an invalid license, such as after restoring a backup to a new server but before obtaining a new license from the Central Server, the following dialog appears:



This is to be expected because the license is not valid. Click **Yes** to continue with the upgrade. The site server will request a new license from the Central Server after the upgrade and continue normal operation.

How to Verify Services are Not Running

When services are stopped, verify all the processes are stopped using the Task Manager and the Details tab. Technically, some stuck processes may be still running and blocking the files, even though the related service is stopped.

> In this state, only the following processes should be running:
> - Firebird.exe
> - MyQ EasyConfig.exe

Make sure that **none** of the processes or related services in the table below is running.

Process/Service	Description	Component(s)
CanonTerminal.exe	Canon terminals service	Print Server
HPProTerminal.exe	HP Pro terminals service	Print Server
httpd.exe	Apache HTTP Server	Print and Central Server
Kmum.Server.exe	Kyocera-related service	Print Server
MyQ.exe	MyQ X Print Server application	Print Server

Process/Service	Description	Component(s)
MyQBrotherTerminal.exe	Brother terminals service	Print Server
MyQCentral.exe	MyQ X Central Server Application	Central Server
MyQEpsonTerminal.exe	Epson terminals service	Print Server
MyQFujifilmTerminal.exe	Fujifilm terminals service	Print Server
MyQHPTerminal.exe	HP terminals service	Print Server
MyQJobProcessor.exe	MyQ Job Processor	Print Server
MyQKatunTerminal.exe	Katun terminals service	Print Server
MyQKyoceraTerminal.exe	Kyocera terminals service	Print Server
MyQLexmarkTerminal.exe	Lexmark terminals service	Print Server
MyQRicohTerminal.exe	Ricoh terminals service	Print Server
MyQSharpTerminal.exe	Sharp terminals service	Print Server
MyQSvc.exe	Supporting service for the MyQ server	Print Server
MyQToshibaTerminal.exe	Toshiba terminals service	Print Server
MyQXeroxTerminal.exe	Xerox terminals service	Print Server

Process/Service	Description	Component(s)
nssm.exe	The non-sucking service manager	Print and Central Server
php-cgi.exe	Common Gateway Interface	Print and Central Server
php.exe	Command line interface (CLI)	Print and Central Server
rotatelogs.exe	Apache HTTP Server rotate logs program	Print and Central Server
traefik.exe	HTTP reverse proxy	Print and Central Server

If any of these processes is running despite all the services being stopped, then it is most likely a stuck process and will block the correct execution of the upgrade installation wizard. If this happens, reboot the server. Then go to **Easy Config > Services** and select **Stop All Services**, verify that no processes are running, and try the upgrade again.

5.3 Install MyQ in Private Cloud

As an alternative to using on-premises servers, the MyQ Server can be installed and run on an Azure Virtual Machine, with a VPN tunnel connecting the physical network and Azure's virtual network, using site-to-site VPN via Amazon Web Service (AWS), or using a Google Compute Engine Instance in Google Cloud.

See also:

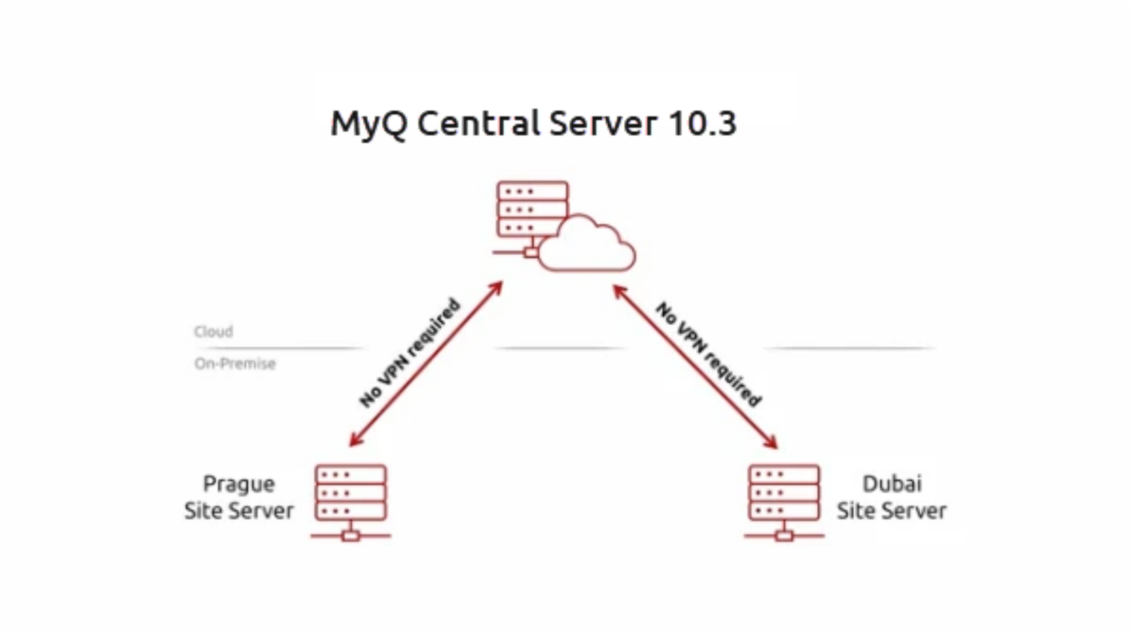
- MyQ in Cloud
- (v2) Deployment in the Cloud

5.3.1 Private Cloud in Azure

Environment Requirements

- The minimum recommended virtual machine is B4ms, with a dedicated (non-system disk) standard HDD. The recommended CPU, RAM, and HDD resources are the same as a standard installation.
- VPN tunnel (100mbps line is recommended) connecting the physical network and Azure's virtual network where the MyQ Server is installed.
- Outgoing communication on ports used by MyQ must be allowed on Azure's Network security group.
- The geolocation of the cloud server should be as physically close as possible.
- The ping response from printers to the cloud server should be within 750ms (max 1 second, can be adjusted in `config.ini`).

Communication with Sites does not require a VPN tunnel. The public IP address of the machine running the Central Server.



Once you set up the Azure virtual environment, follow the installation instructions to install MyQ.

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.

See also:

- System Requirements (see page 23)
- Main Communication Ports (see page 27)
- Installation (see page 37)
- Configure ExpressRoute and S2S VPN coexisting connections with Azure PowerShell[5]

5.3.2 Private Cloud in AWS

Environment Requirements

- **Amazon EC2 Instance:** MyQ Server(s) can be installed on an AWS EC2 instance. The instance should meet the standard system requirements for MyQ X installations, which include sufficient CPU, RAM, and storage.
- **AWS VPC Setup:** Create an AWS Virtual Private Cloud (VPC) with necessary resources like subnets, route tables, and gateways.
- **Site-to-Site VPN:** A site-to-site VPN tunnel is mandatory to connect your on-premises network with the AWS VPC. This VPN allows MyQ X to access resources on the local network. The setup process involves creating a customer gateway, a virtual private gateway, and configuring routing and security groups on AWS.

See also:

- System Requirements (see page 23)
- AWS VPC guide[6]
- AWS Site-to-Site VPN documentation[7]
- AWS Customer Gateway guide[8]
- AWS Virtual Private Gateway guide[9]
- AWS Route Table Configuration[10]

5. https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/vpn#architecture
6. https://docs.aws.amazon.com/vpc/latest/userguide/create-vpc.html#create-vpc-and-other-resources
7. https://docs.aws.amazon.com/vpn/latest/s2svpn/SetUpVPNConnections.html
8. https://docs.aws.amazon.com/vpn/latest/s2svpn/SetUpVPNConnections.html#vpn-create-cgw

- AWS Security Group guide[11]

When connecting your AWS VPC to your on-premises network via a site-to-site VPN connection it is assumed that the target on-premises network has resources like a DNS server, a DHCP server, a network switch, or router, an internet gateway, a physical or virtual firewall, etc. Other resources like a domain, a domain controller, a file server, an SMTP server, etc. are optional.

Getting started with AWS Site-to-site VPN

- **Create a Customer Gateway:** Represent your on-premises network's VPN device in AWS. This involves entering the static IP address of the device and selecting appropriate routing options.
- **Create a Virtual Private Gateway:** This is the VPN gateway on the AWS side. After creation, attach it to your VPC.
- **Configure Routing:** Update your VPC's route table to direct traffic through the VPN connection to your on-premises network.
- **Update Security Groups:** Modify the security group associated with your EC2 instance to allow necessary inbound and outbound traffic.
- **Create the VPN Connection:** Establish the VPN connection between your AWS VPC and your on-premises network by configuring the necessary tunnels.
- **Download Configuration File:** Download the configuration file provided by AWS to set up your customer gateway device.
- **Configure Your Customer Gateway Device:** Follow the instructions in the configuration file to complete the VPN setup on your on-premises gateway device.

5.3.3 Private Cloud Using Google Cloud

Environment Requirements

- **Google Compute Engine Instance**: MyQ Server can be installed on a Google Cloud Compute Engine virtual machine. The instance must meet the standard system requirements for MyQ X installations, including sufficient CPU, RAM, and storage.

9. https://docs.aws.amazon.com/vpn/latest/s2svpn/SetUpVPNConnections.html#vpn-create-target-gateway
10. https://docs.aws.amazon.com/vpn/latest/s2svpn/SetUpVPNConnections.html#vpn-configure-route-tables
11. https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

- **Site-to-Site VPN**: A site-to-site VPN tunnel is required to securely connect the on-premises network to the Google Cloud Virtual Private Cloud (VPC). This ensures encrypted communication using IPsec.
- **VPC Network**: A custom or default VPC network is needed to host the MyQ server. The VPC enables connectivity between resources like subnets and gateways within Google Cloud.
- **Latency Considerations**: Select a region close to the on-premises network to minimize latency. All resources should ideally be in the same region.

See also:

- System Requirements (see page 23)
- Compute Engine Overview[12]
- Cloud VPN Overview[13]
- VPC Networks Documentation[14]
- Google Cloud Console[15]
- Quick Start: Create and Manage VPC Networks[16]
- Classic VPN Topologies[17]
- HA VPN Topologies[18]
- Compute Engine Documentation[19]

GCP Setup Steps

1. **Create a Project**:
    - Organize resources by creating a new project or using an existing one in Google Cloud.
2. **Set Up a VPC Network**:
    - Create a custom VPC with subnets and appropriate IP ranges not overlapping with the on-premises network.
3. **Configure VPN**:
    - Use Classic VPN or HA VPN to establish IPsec tunnels between the on-premises network and the VPC.
    - Configure IKEv2 with pre-shared keys and set up routing options (e.g., route-based or policy-based). Refer to for details.

12. https://cloud.google.com/compute/docs/overview
13. https://cloud.google.com/network-connectivity/docs/vpn
14. https://cloud.google.com/vpc/docs/vpc
15. https://console.cloud.google.com/
16. https://docs.cloud.google.com/vpc/docs/create-modify-vpc-networks
17. https://docs.cloud.google.com/network-connectivity/docs/vpn/concepts/classic-topologies
18. https://docs.cloud.google.com/network-connectivity/docs/vpn/concepts/topologies
19. https://cloud.google.com/compute/docs/instances

4. **Create a Compute Engine VM Instance**:
   - Select machine specifications based on MyQ system requirements (e.g., 8 vCPUs, 8 GB RAM). Additional storage for MyQ data should be separate from the OS disk for better performance and resiliency.
5. **Network Configuration**:
   - Assign internal IP addresses from the VPC subnet range.
   - External IP addresses are optional but can be used temporarily for internet access during setup.

Once the environment is set up, follow MyQ installation instructions to deploy the server on the VM.

5.4 Migrate from OEM to MyQ

You can restore KNM and aQrate databases in the MyQ installation, which allows migrating all data from a KNM or aQrate installation into the MyQ installation. Other directions of migration are not possible.

5.4.1 Prerequisites

- Backup of a database from the current OEM installation, minimum version 10.2 patch 24.
- Installer of the MyQ Print Server (for standalone mode)
- Installer of the MyQ Central Server (for central-site installations)
- 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.

5.4.2 Recommended steps

Before you begin, we recommend that you review our upgrade guidance. See Upgrading to MyQ 10.3 (see page 48).

General

- Use a backup created immediately before migration to achieve no data loss
- Once the migration process is complete, check the settings 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 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

Licenses

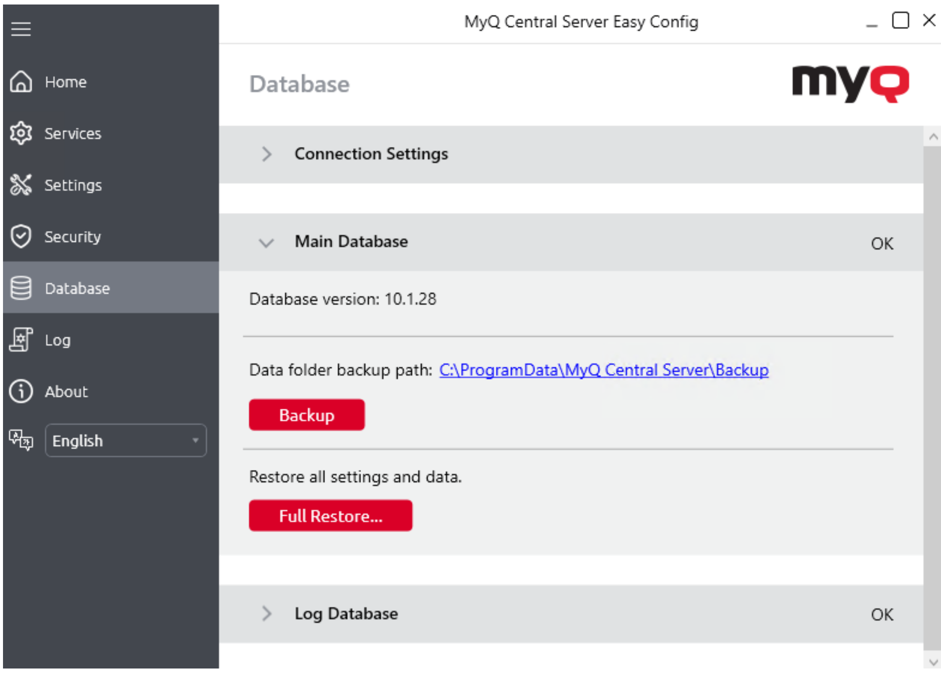
Since MyQ and other brands have different licenses, the license is lost when the database is restored. A new MyQ license must be activated instead of the previous KNM/aQrate one.

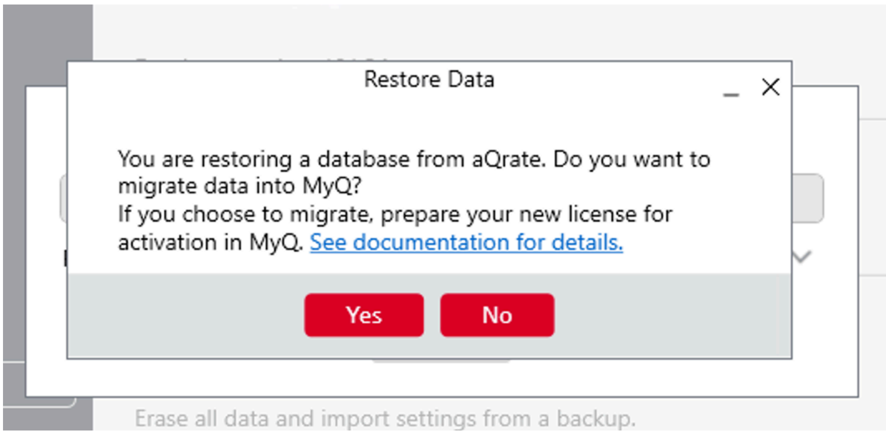
5.4.3 Migrate to MyQ

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 (`10.2 Patch 24` 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

Migration process on Central Server is similar to Print Server except that the only settings which are relevant for Central Server are:

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

5.5 Updating MyQ

To benefit from the latest improvements, bug fixes, and security updates, keep your installation up to date with the latest patch releases.

To update your MyQ Server 10.3 system, download the latest installation executable file from the MyQ Community and run it on the server, with local administrator access. The update process starts automatically.

5.5.1 Before you Start

- make sure that the latest Windows updates are installed on the server.
- ensure all antivirus exclusions are made and that there are no running scan operations on the MyQ directories structure.
- back up your current database.

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.

5.6 MyQ and MS Cluster

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 administers the MyQ services and if the currently active node becomes unavailable, it switches to one of the available passive nodes.

5.6.1 Compatibility with Windows Servers

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

Windows Server	Editions
Windows Server 2025	Standard, Datacenter
Windows Server 2022	Standard, Datacenter

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

- 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).

5.6.2 Licenses

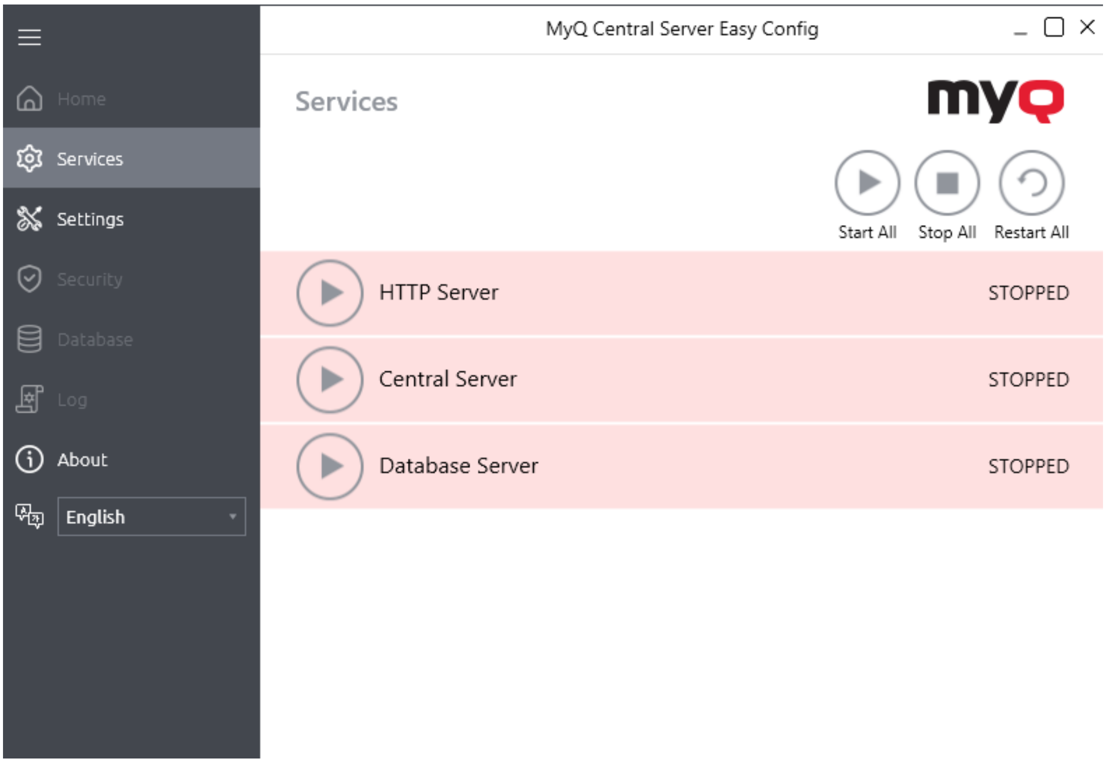
Only one installation key is needed to use MyQ in a MS Cluster. The HW code is taken from the whole cluster, not individual nodes, so the license is activated against the cluster's HW, and not a single node.

5.6.3 Deploy in MS Cluster

Installing MyQ Server in the cluster (all nodes)

On each cluster node, do the following:

1. Run the MyQ installation file and install MyQ.
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.

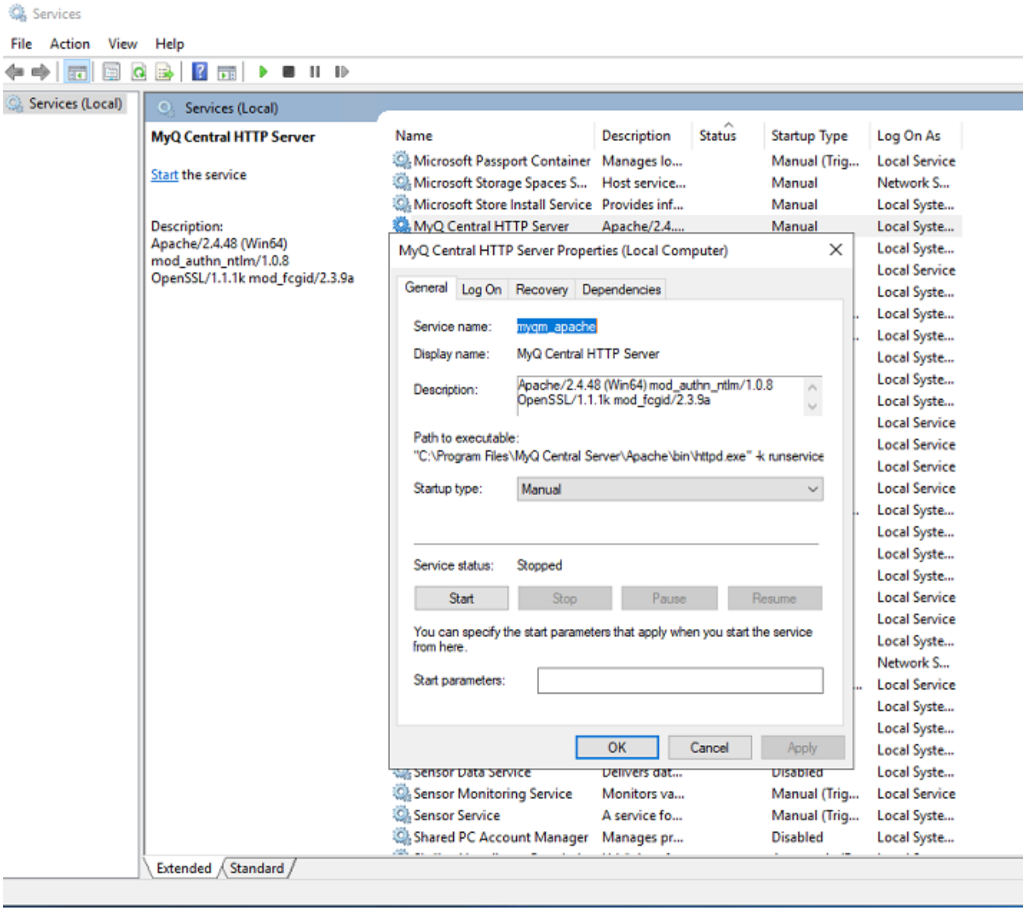


Setting services to manual startup (all nodes)

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:

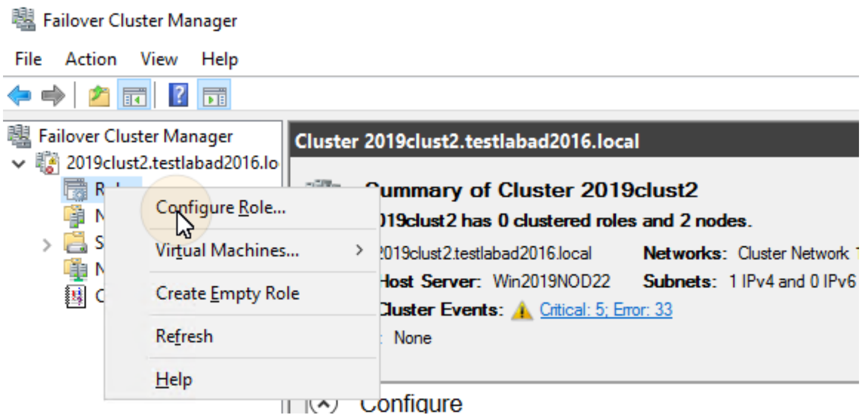
- MyQ Central HTTP Server
- Firebird Server - MasterInstance
- MyQ Central Server



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

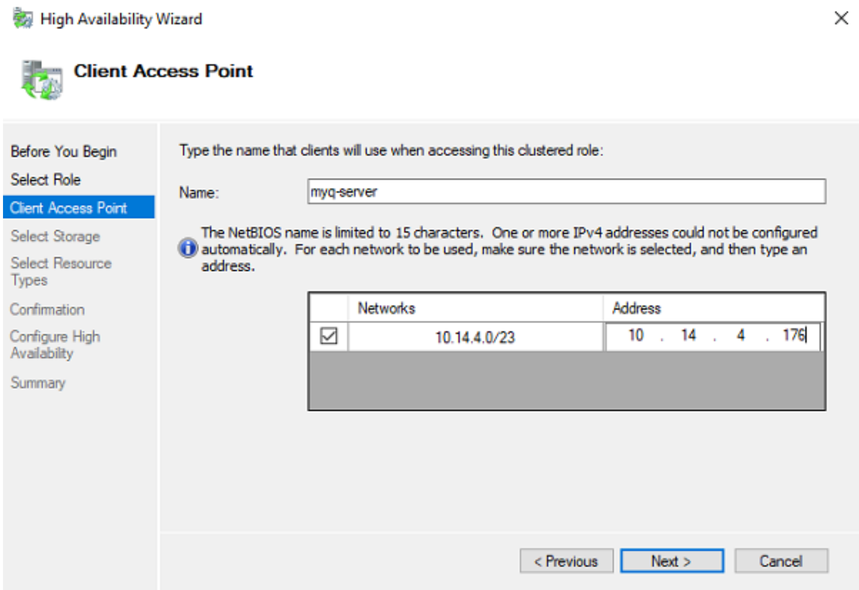
Open Failover Cluster Manager and do the following:

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

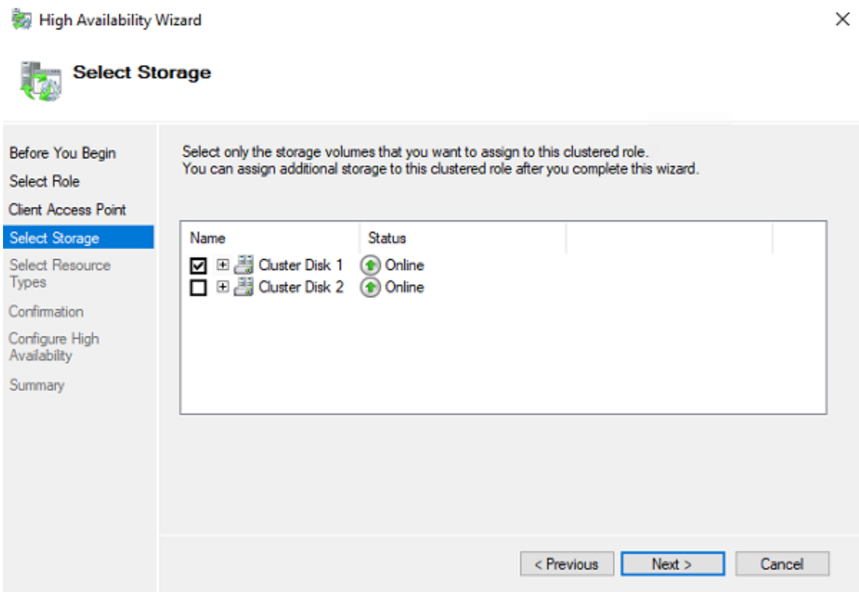


2. Click **Next**. The Select role tab opens.

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.



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



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

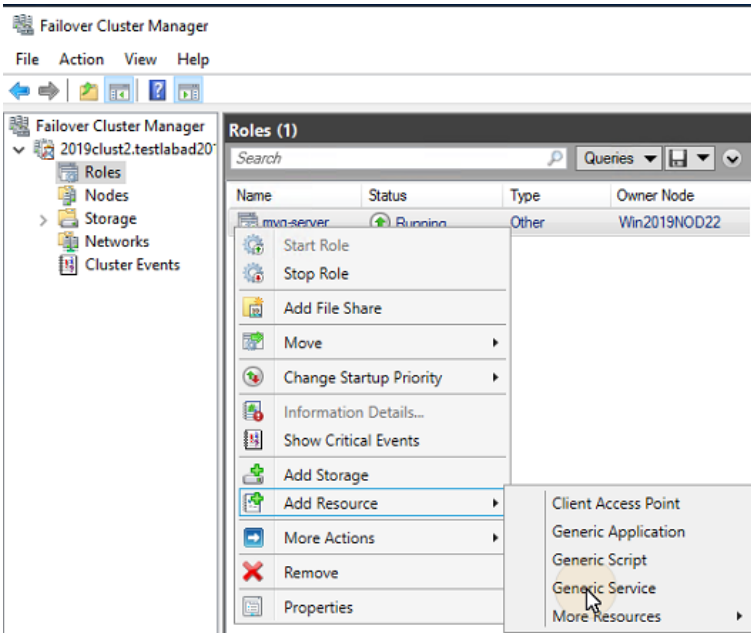
Adding MyQ Resources (Failover Cluster Manager)

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.

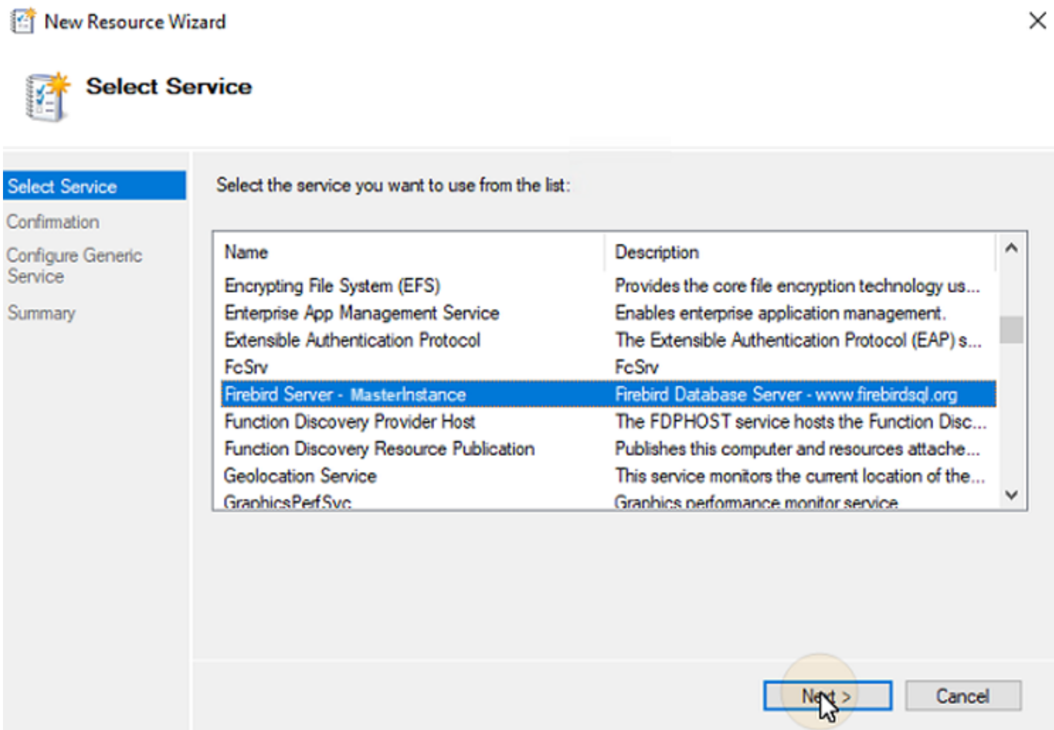
> If you are using an MS SQL database instead of the Embedded database, you don't need to add the Firebird Server - MasterInstance service to the MyQ server role. You should only add the Apache Monitor script, and the MyQ Monitor script.

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:

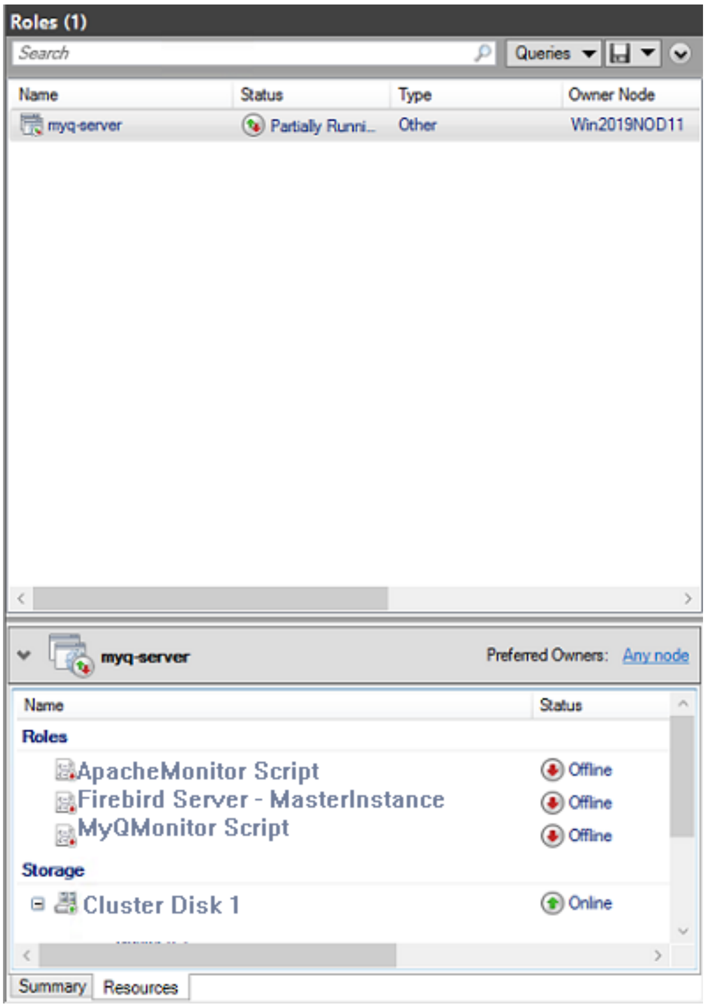
1. Right-click the MyQ server role, click **Add resource** on the shortcut menu, and click **Generic Script**. The New Resource Wizard opens.
2. Enter the path to the **MyQMonitor.jse** script, located in the MyQ installation folder, and click **Next**. The Confirmation tab opens. The default path to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

Setting Resources Dependencies (Failover Cluster Manager)

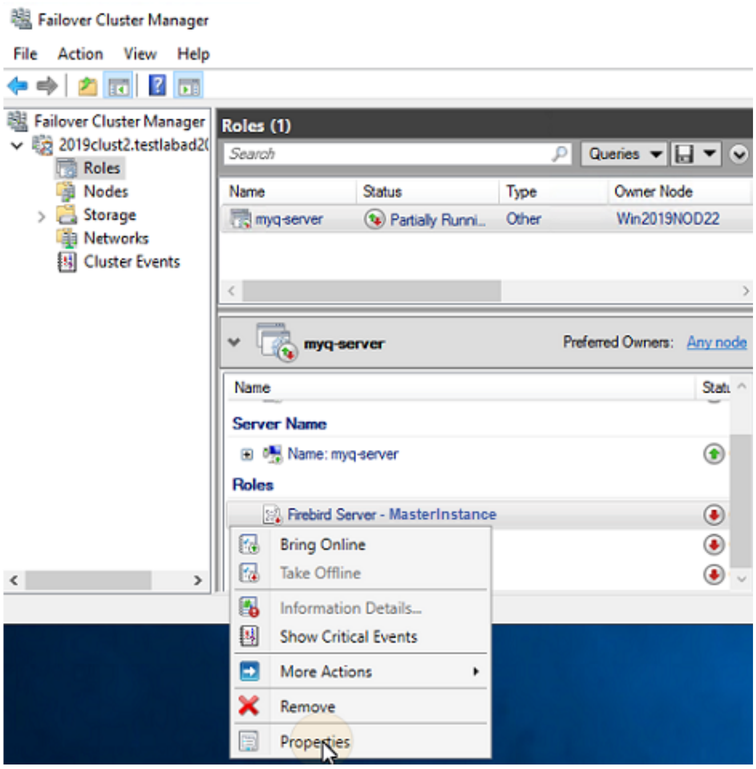
After adding the services and scripts to the MyQ server role, open the **Resources** tab of the MyQ server role at the bottom of the **Roles** tab and set the dependencies of the MyQ services and scripts.



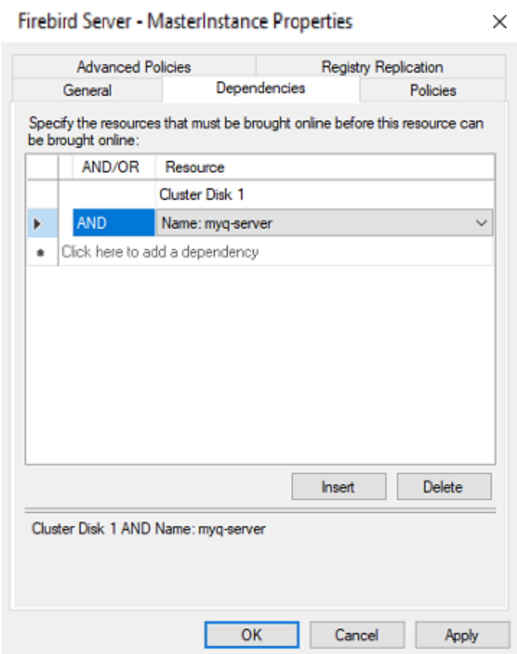
Set the Firebird Server - MasterInstance service dependency

This step is not needed if you are using an MS SQL database.

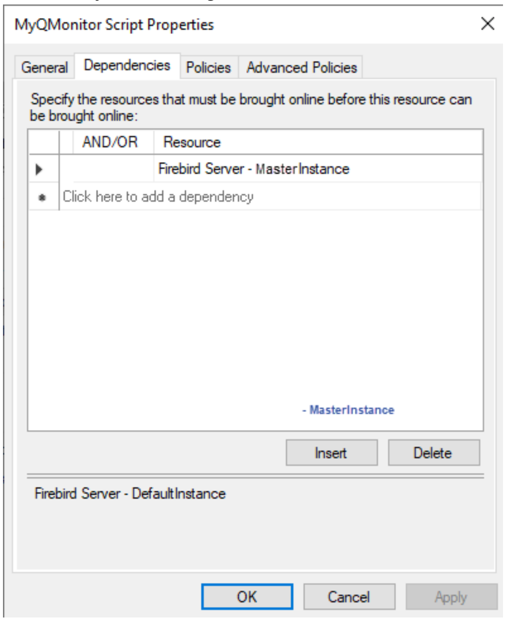
1. In the list at the bottom of the tab, right-click **Firebird Server - MasterInstance**, and click **Properties**. The Firebird Server - MasterInstance Properties dialog box opens.

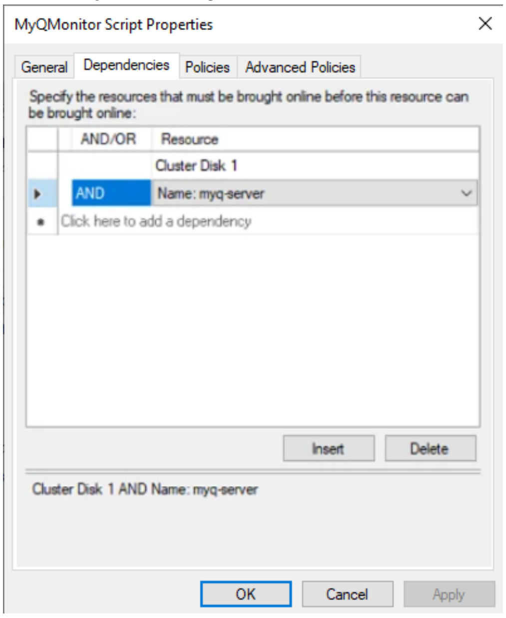


2. In the dialog box, open the **Dependencies** tab, add the shared disk drive (or NAS) where the system is supposed to work on, add the name of the MyQ server role, and click **OK**. The dependency is set.



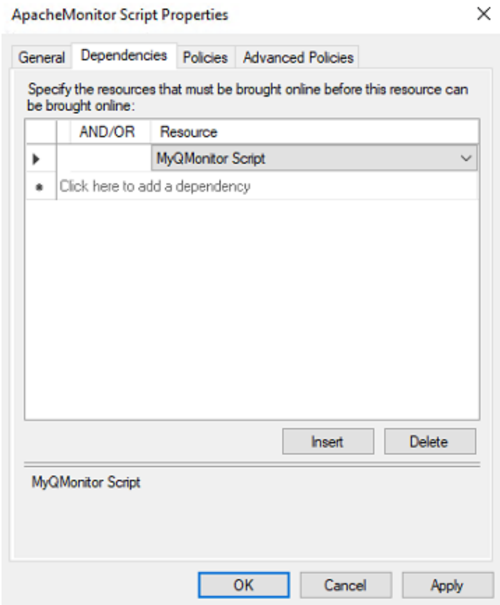
Set the MyQMonitor script dependency

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.
   - If you are using Firebird - MasterInstance, insert it as a dependency for the MyQMonitor Script, and click **OK**.
     The dependency is set.
     

   - If you are using MS SQL, add the **Cluster Disk** and **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.



To view 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**.

5.6.4 Additional MS Cluster Setup

After installing MyQ on your nodes and setting up resource dependencies, perform these post-installation steps before bringing the resources online.

Set Up 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.

Set the Data Folder Location (All Nodes)

On each node of the cluster, you msut 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 folders 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 both the **Data** folder and the **Jobs** folder, click **Change location**, and then define the path to the shared cluster disk.
3. On the **Services** tab, **Stop All** services, and then close the MyQ Easy Config application.
4. In Failover Cluster Manager, move the MyQ server role to the next node and repeat the process.

Important Considerations when Running MyQ in MS Cluster

- Do not start, stop, or restart MyQ services while MyQ is controlled by the MS Cluster (cluster resources are online). The services should be managed only 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), with MyQ services are online on any node (activated manually), do not switch to a different node. If you switch to a different node you may corrupt your 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.

Starting the System (Failover Cluster Manager)

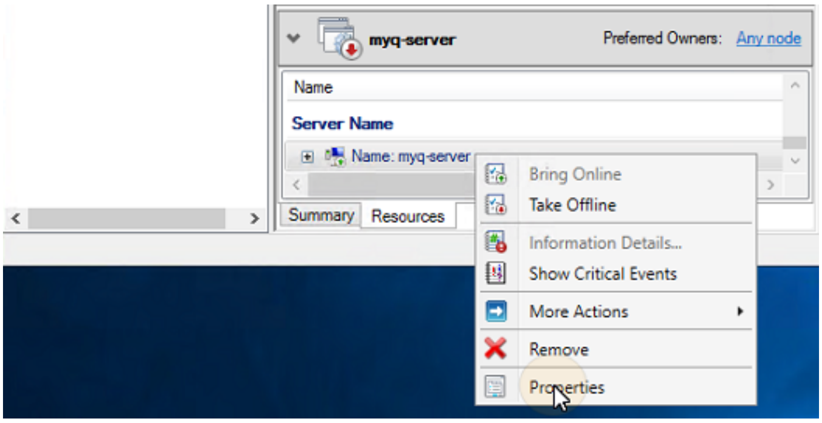
To start the system, bring the resources of the MS Cluster online. For information on how to do this, see Running in MS Cluster (see page 90).

Set the Hostname of the MyQ Server Role

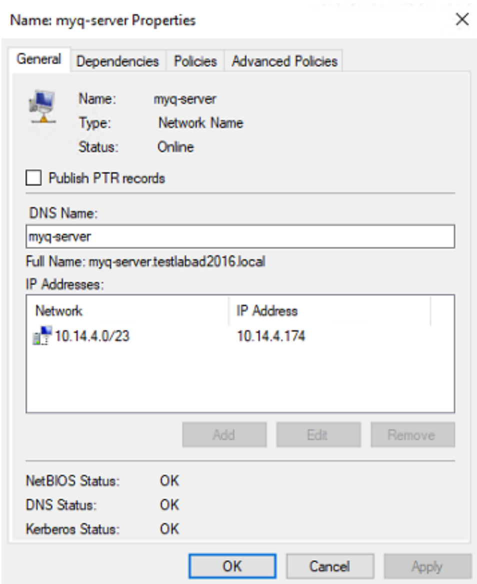
On the **Resources** tab of the MyQ server role in Failover Cluster Manager, you can view (and change) the DNS Name of the MyQ server role. You must use the **Full name** of the role (DNS + domain) as the server hostname and as the MyQ X Mobile Client server in MyQ.

To view 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:

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.

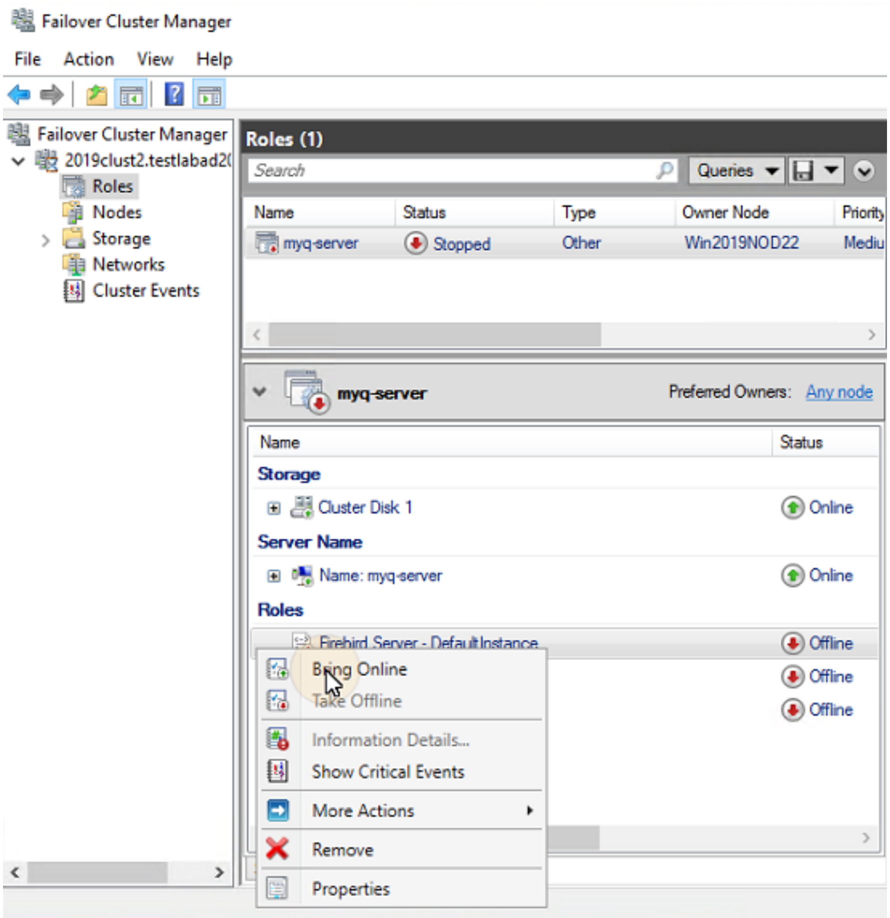
5.6.5 Running in MS Cluster

This page describes additional configuration and maintenance steps, and troubleshooting information.

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.

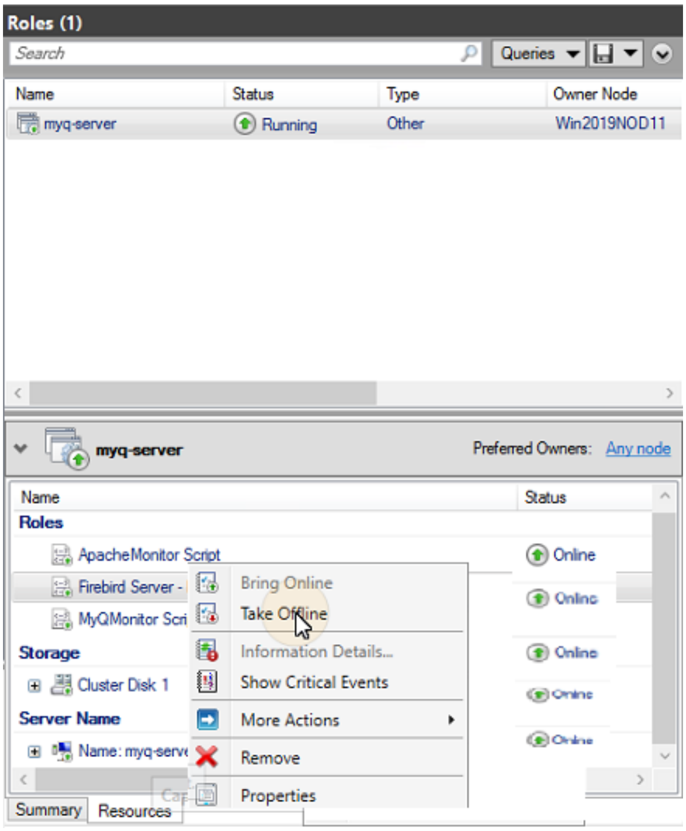


Taking the MS Cluster resources offline (Failover Cluster Manager)

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.



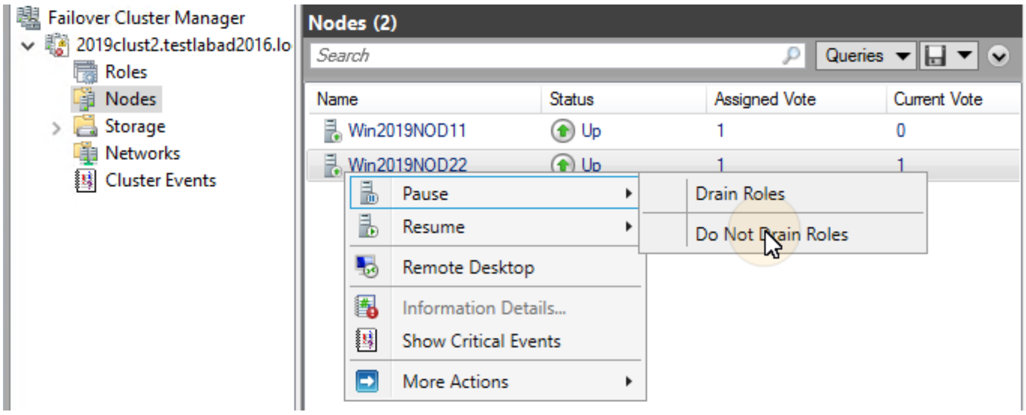
Restarting MyQ services via the MS Cluster (Failover Cluster Manager)

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.

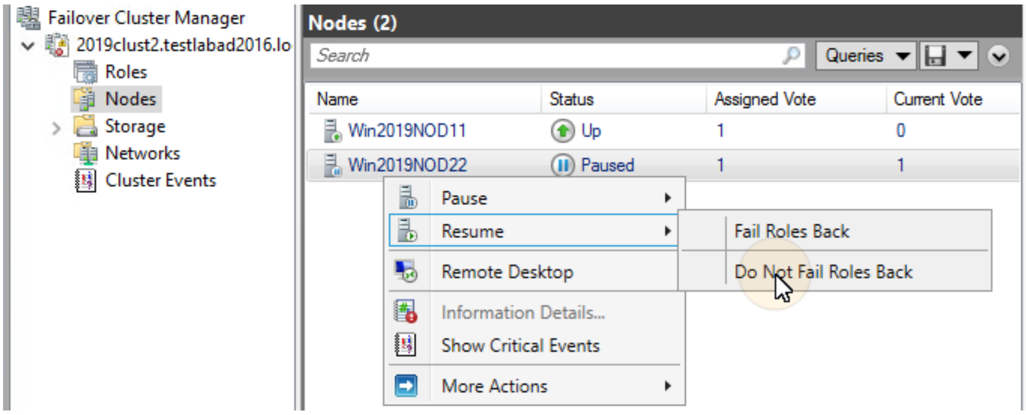
Changing the MyQ admin credentials (active node)

To change the **Web 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**.



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.

5.6.6 Backup and Restore in MS Cluster

Backing Up the MyQ Database in a MS Cluster

The automatic and manual backup processes do not differ from the standard backup processes described in Easy Config Database Tab. 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. See Easy Config Database Tab (see page 104)

Restoring the MyQ Database on a MS Cluster (all nodes)

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

Then restore the MyQ database and settings on the active node of the cluster (the current owner of the MyQ server role):

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.

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.

5.6.7 Updating MyQ in MS Cluster

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.

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.

Upgrading Terminal Packages in a Cluster

To upgrade terminal packages within a cluster, first open Failover Cluster Manager and take the TerminalsMonitor script offline. Then, go to **MyQ > Settings > Printers & Terminals** and perform the upgrade. When the terminal packages have been upgraded, bring the TerminalsMonitor script online again in Failover Cluster Manager.

5.7 Uninstall 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.

6 MyQ Easy Config

The MyQ Central Easy Config application is the basic environment for the setup of essential parts of the MyQ 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.

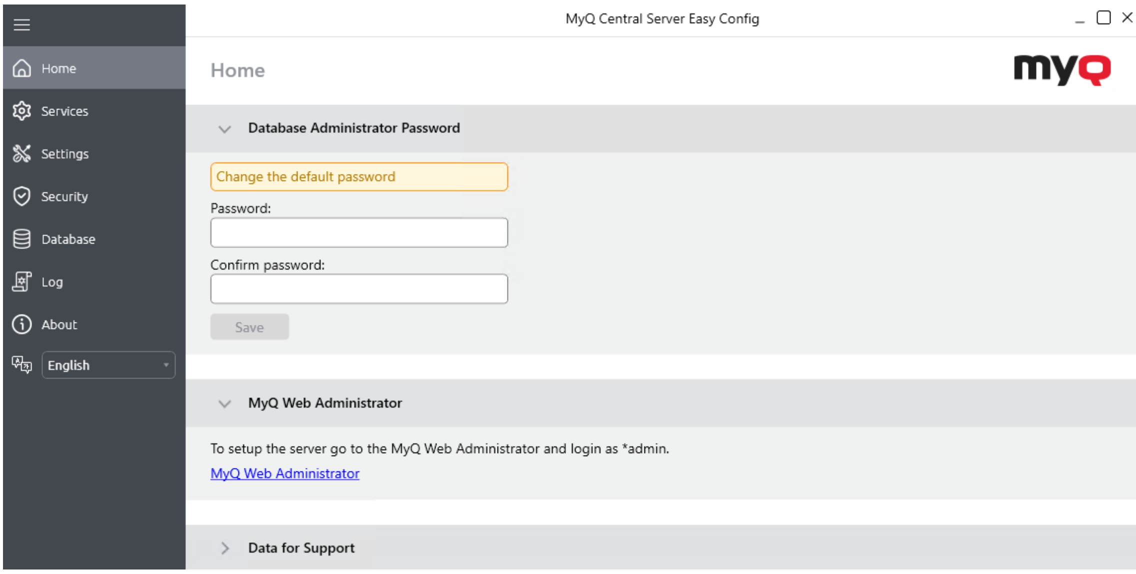
6.1 Easy Config Home Tab

Once you open the MyQ Easy Config application on the Home tab for the first time, you will be prompted to create a password 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 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**.

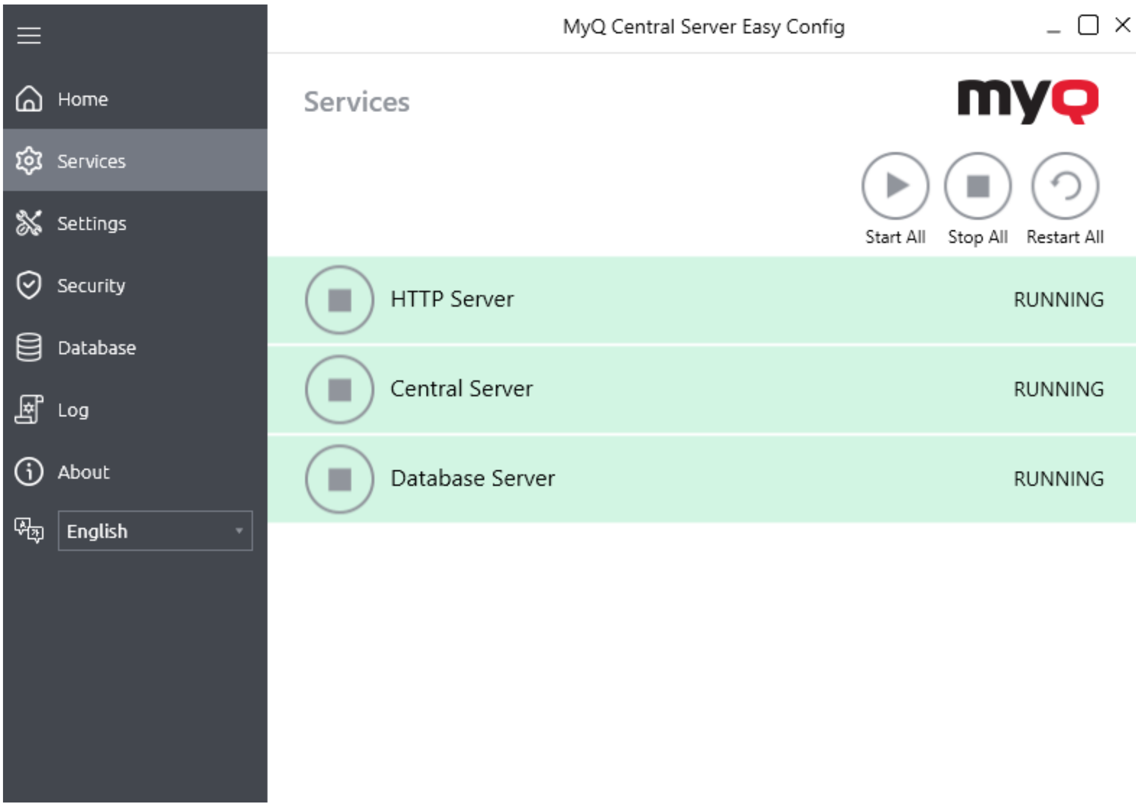


> After you change credentials for the first time, its initial setup section disappears from the **Home** tab. Passwords can be later changed from the **Security** tab.

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

6.2 Easy Config Services Tab

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



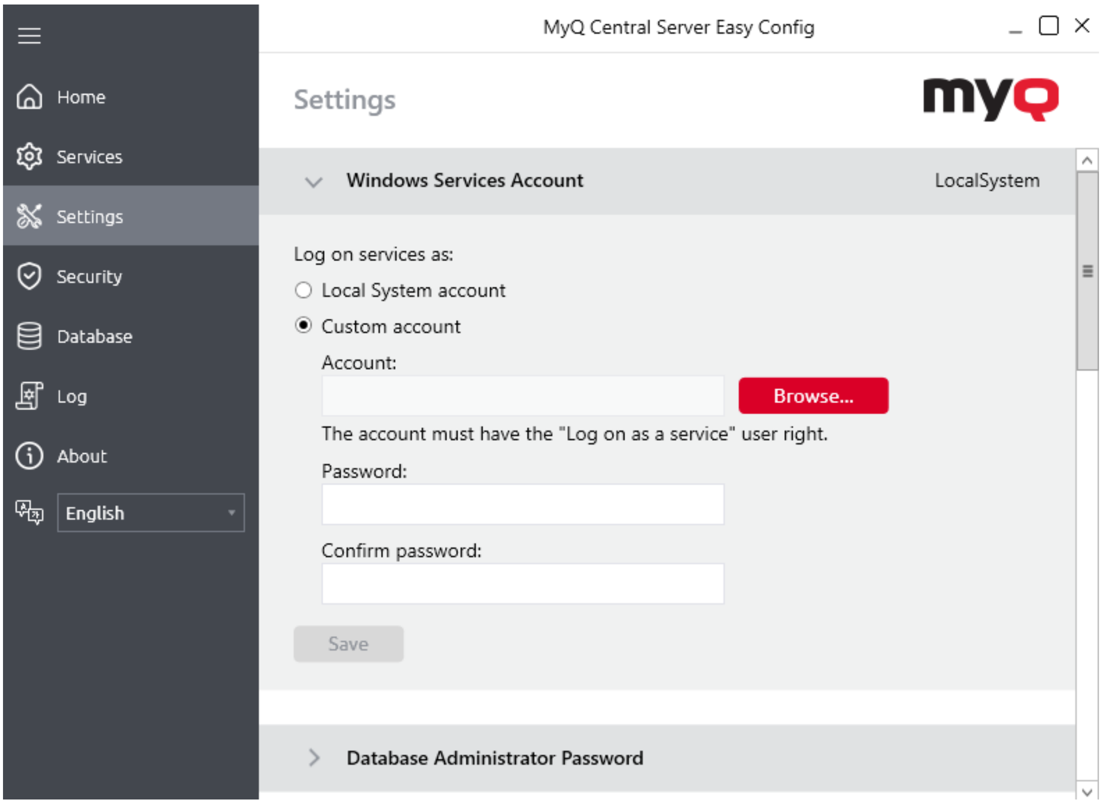
6.3 Easy Config Settings Tab

6.3.1 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.



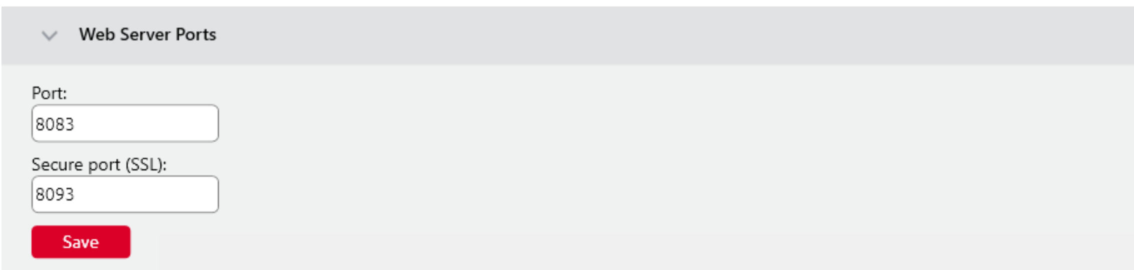
To change back to the default account, select **Local System account**, and click **Save**. MyQ Services are automatically stopped and restarted.

6.3.2 Web Server Ports

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

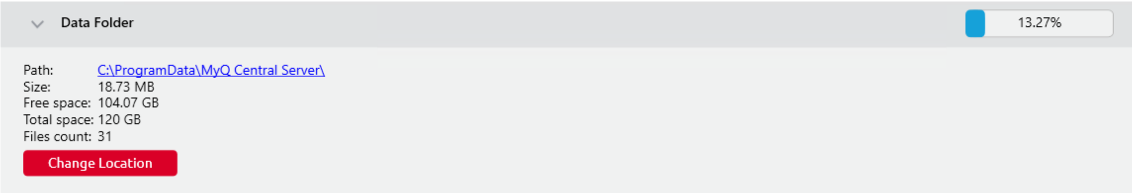
- **Port**: communication port for the MyQ HTTP server; the default value is *8083*.
- **Secure port (SSL)**: communication port for the MyQ HTTPS server; the default value is *8093*.

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



6.3.3 Data Folder

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

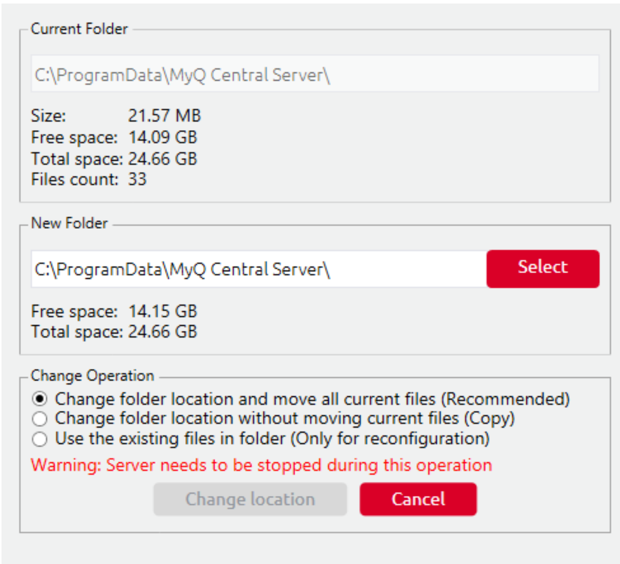


Depending on the type of the database, the Data folder either does, or does not contain the MyQ database: the MyQ Embedded database is part of the folder, whereas the SQL database is stored on the SQL server. Besides the MyQ database, the folder contains additional files with data used by the MyQ system, 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 and Jobs 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. See Map a network drive to be used by a service[20].

6.3.4 Server Maintenance

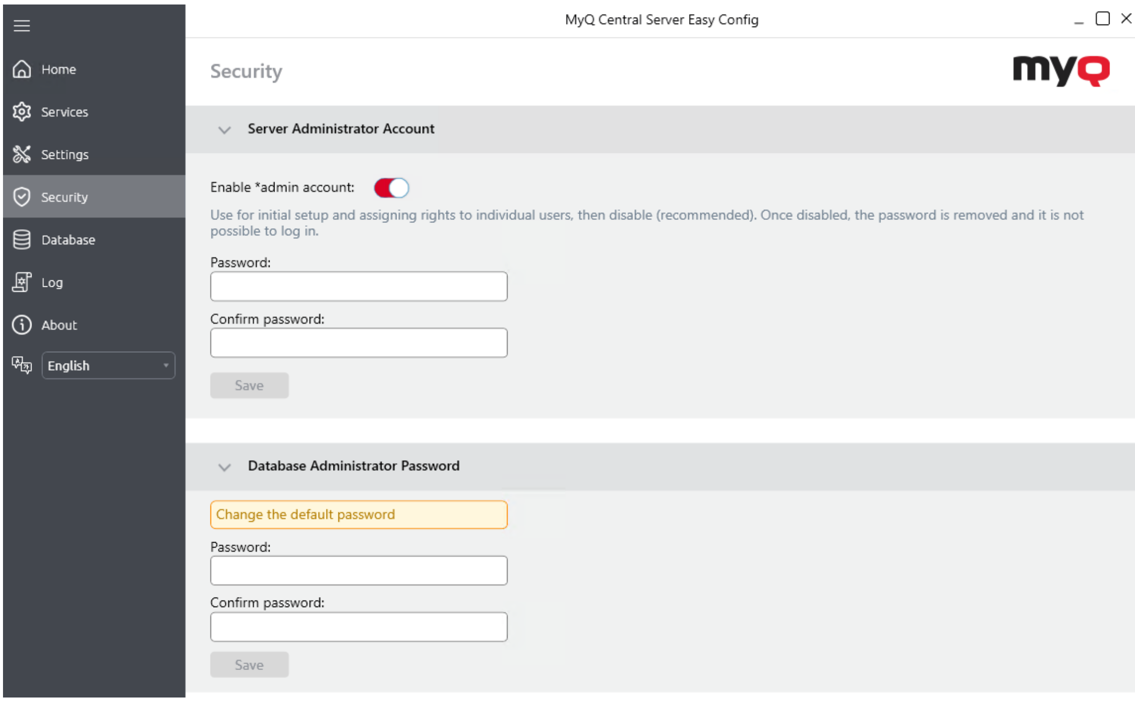
In the **Server Maintenance** section of the **Settings** tab, you can clean up your Cache and Temp folders. This might be necessary in cases where problems with the temporary files affect the MyQ system.

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.

20. https://stackoverflow.com/questions/182750/map-a-network-drive-to-be-used-by-a-service/4763324#4763324

6.4 Easy Config Security Tab

6.4.1 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 used for the initial MyQ configuration. Once you create a password for this account, you can continue to the MyQ Web Interface, use `*admin` to log in as the administrator and start the configuration. It is generally recommended to disable this account once you have created dedicated administrator accounts, you can do so on the **Security** tab.

Database Administrator Account

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

> The MyQ database access username is *SYSDBA* and its default password is *masterkey*.

6.4.2 Unlocking the MyQ Administrator account

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

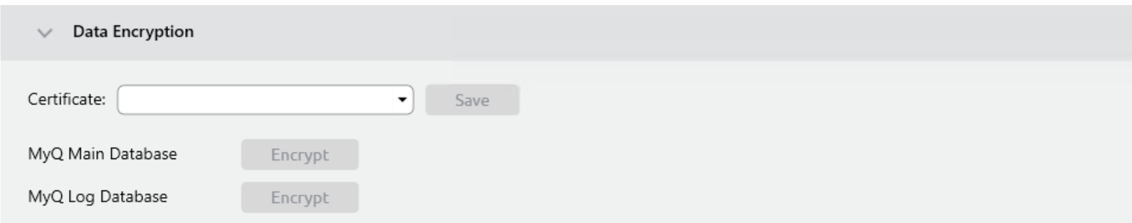
The admin can see a warning that the *admin account is locked, and unlock it, in the **Server Administrator Account** section on the **Security** tab. Once they click **Unlock**, the account is unlocked.

6.4.3 Data Encryption

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.



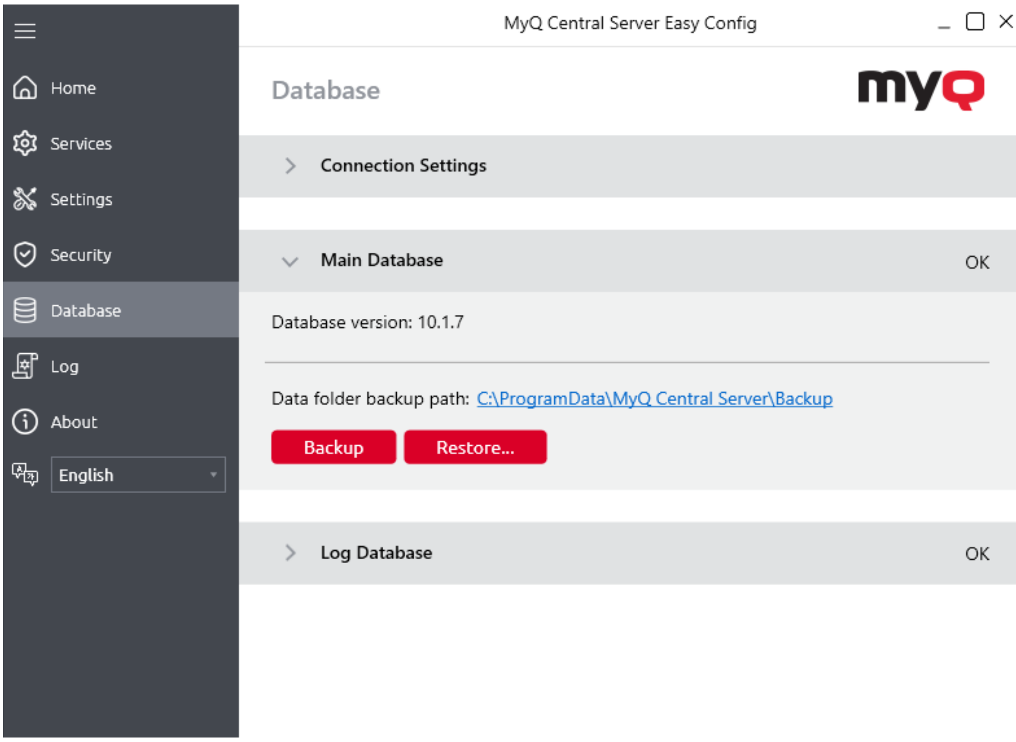
Click **Encrypt** next to **MyQ Main Database**, **MyQ Log Database**, or **Print jobs**. **Scan Jobs** are encrypted by default.

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.

6.5 Easy Config Database Tab

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.



6.5.1 Backing up MyQ data

To back up your MyQ data:

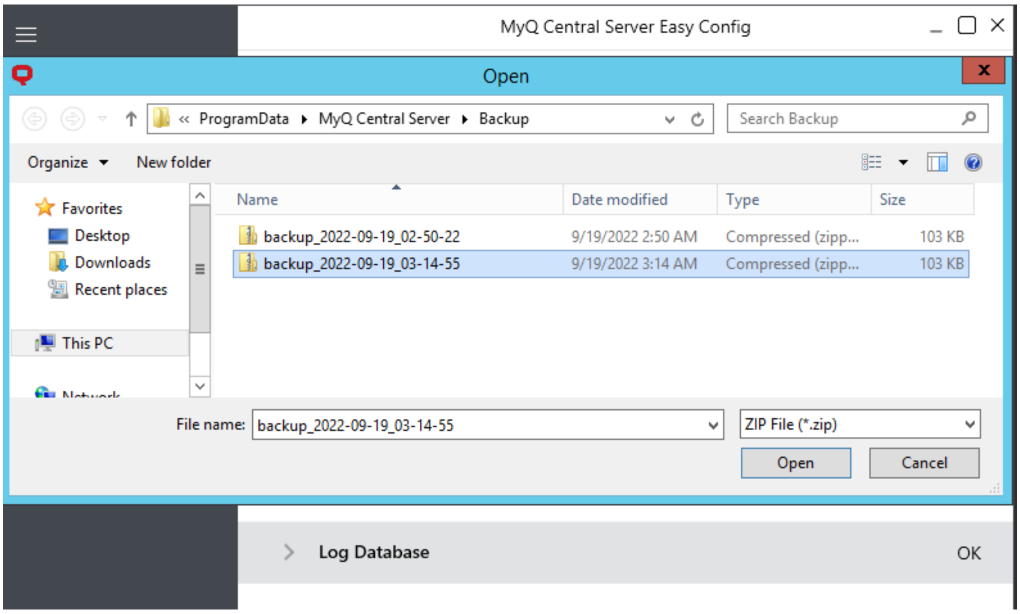
1. Open the **Database** tab.
2. In the **Main Database** section, click **Backup**.
3. Provide and confirm a password to protect the backup. If skipped, the backup will be created unprotected.
4. A new backup file is created, called *database_*.zip*.

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.

6.5.2 Restoring MyQ Data

To restore your MyQ data:

1. Open the **Database** tab.
2. In the **Main Database** section, click **Full Restore...**. Select the *database_*.zip* file and click **Open**. If the backup is password protected, you will be prompted to provide the password. The database is restored and, if needed, upgraded as well.

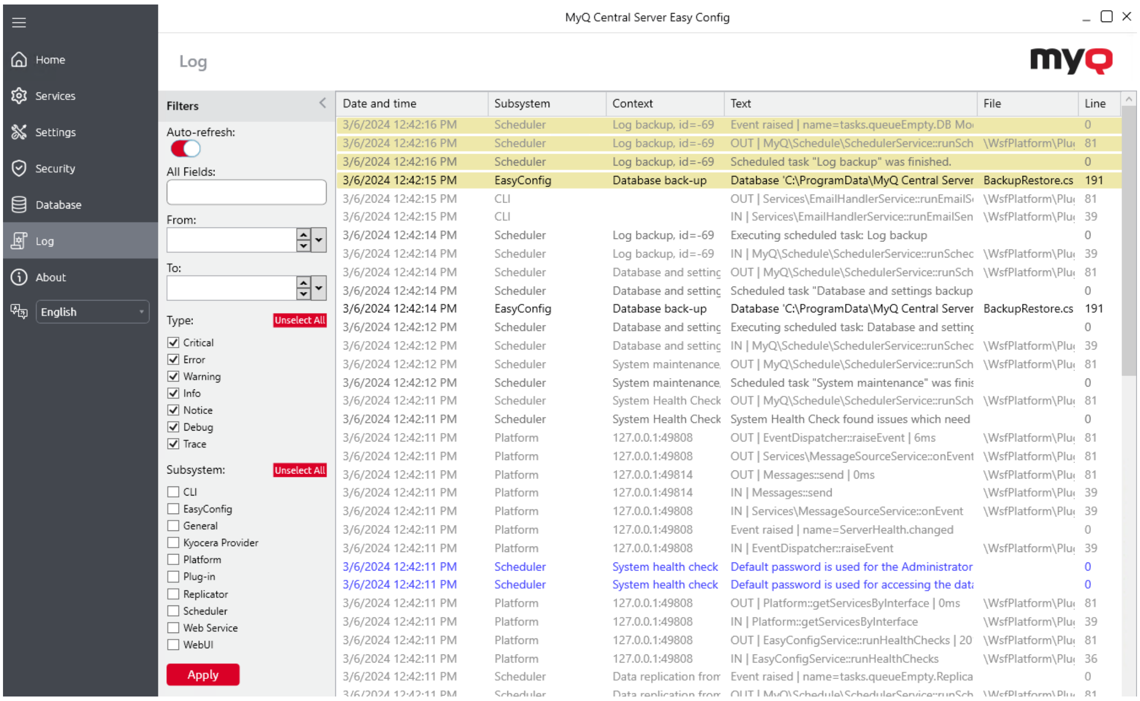


6.5.3 Database Connection Settings

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.

6.6 Easy Config Log Tab

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**.


MyQ Central Server Easy Config
Home
Services
Settings
Security
Database
Log
About
English
Log
myQ
Filters
Auto-refresh:
All Fields:
From:
To:
Type:
Unselect All
Critical
Error
Warning
Info
Notice
Debug
Trace
Subsystem:
Unselect All
CLI
EasyConfig
General
Kyocera Provider
Platform
Plug-in
Replicator
Scheduler
Web Service
WebUI
Apply
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 CLI OUT | Services\EmailHandlerService::runEmailS \WsfPlatform\Plu 81
3/6/2024 12:42:15 PM CLI 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 settinc OUT | MyQ\Schedule\SchedulerService::runSch \WsfPlatform\Plu 81
3/6/2024 12:42:14 PM Scheduler Database and settinc 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 settinc Executing scheduled task: Database and settinc 0
3/6/2024 12:42:12 PM Scheduler Database and settinc 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 finis 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::onEvent \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::onEvent \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

7 MyQ Web Interface

The MyQ Web Interface is the central access point for both administrators and users.

Administrators use the interface to configure and manage the MyQ system. Standard users have access to a limited set of self-service features, such as managing their account and PIN, viewing their jobs, uploading files for printing, checking their credit or quota status, and accessing reports available to them.

Additional administrative features can be delegated to selected users or groups through access rights. This allows organizations to grant controlled access to specific functions, such as managing printers, jobs, users, reports, or credit, without providing full administrator privileges.

This section explains how to access the MyQ Web Interface and introduces its main navigation, Home dashboard, initial setup options, and system logs.

7.1 Accessing the MyQ Web Interface

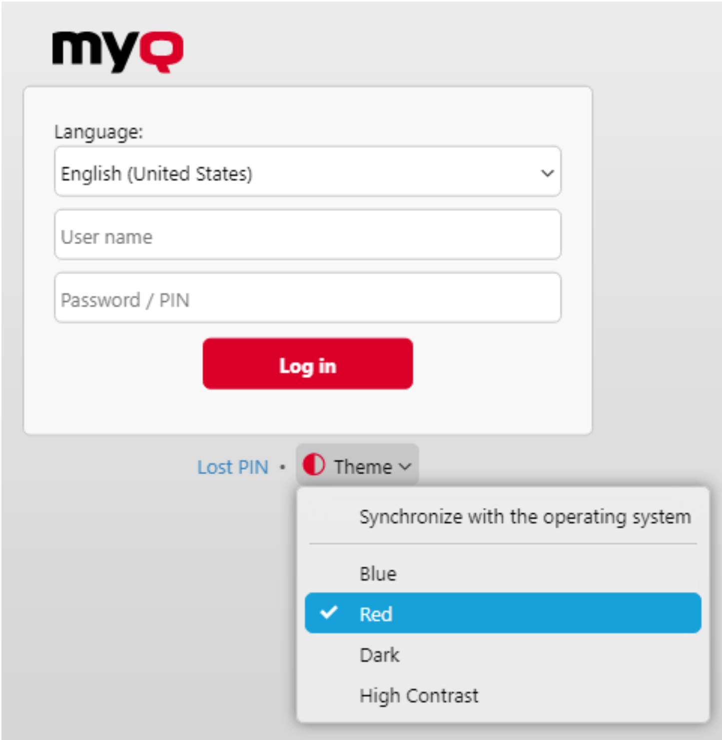
To access the MyQ Web Interface, open it in a supported web browser and log in with your MyQ account. The available menus and features depend on the rights assigned to your account.

- Open your web browser, and then enter the web address:
  `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.
- From the MyQ Central Easy Config **Home** tab, click the **MyQ Web Administrator** link in the **MyQ Web Administrator** section.
- Open the MyQ Central Web Administrator application. You can find this application on the Apps screen in these and later versions: Windows 10, Windows Server 2019.

7.2 Log In as an Administrator

Enter the MyQ administrator name (**admin*) and the password that you have set in the MyQ 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*.

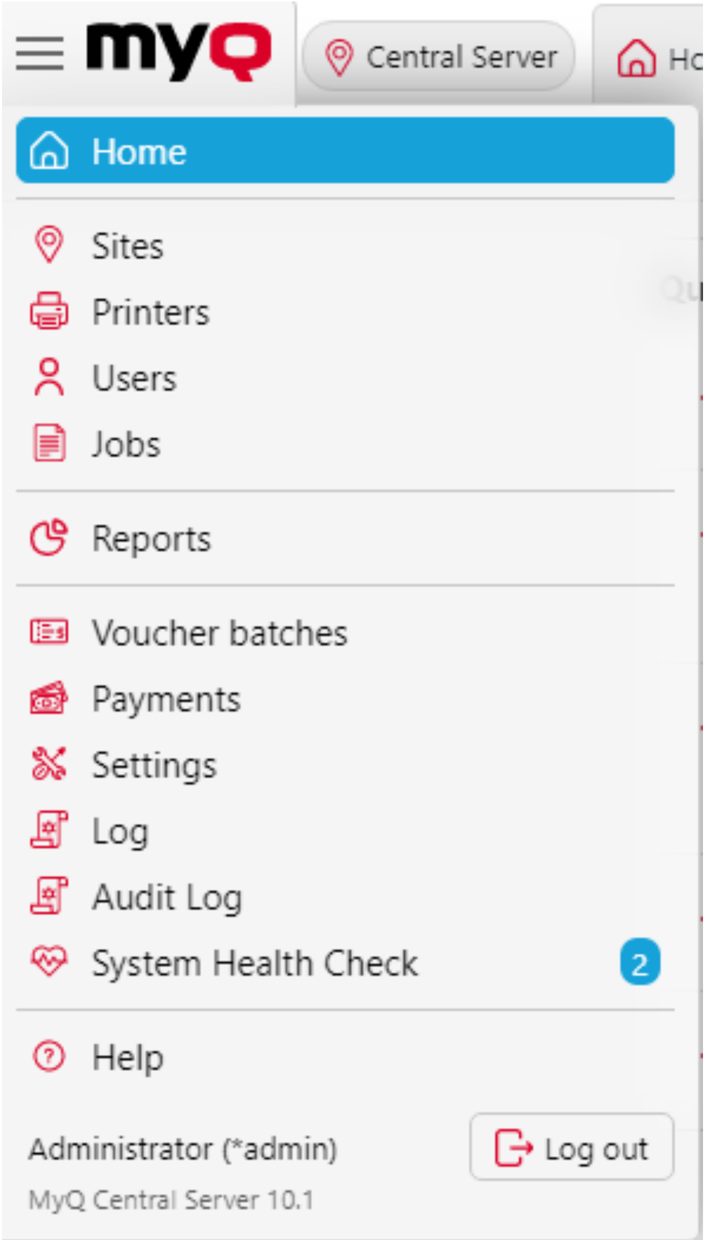
7.3 Main Menu and Settings Menu

There are two menus where you can access all the features and settings of the MyQ 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.



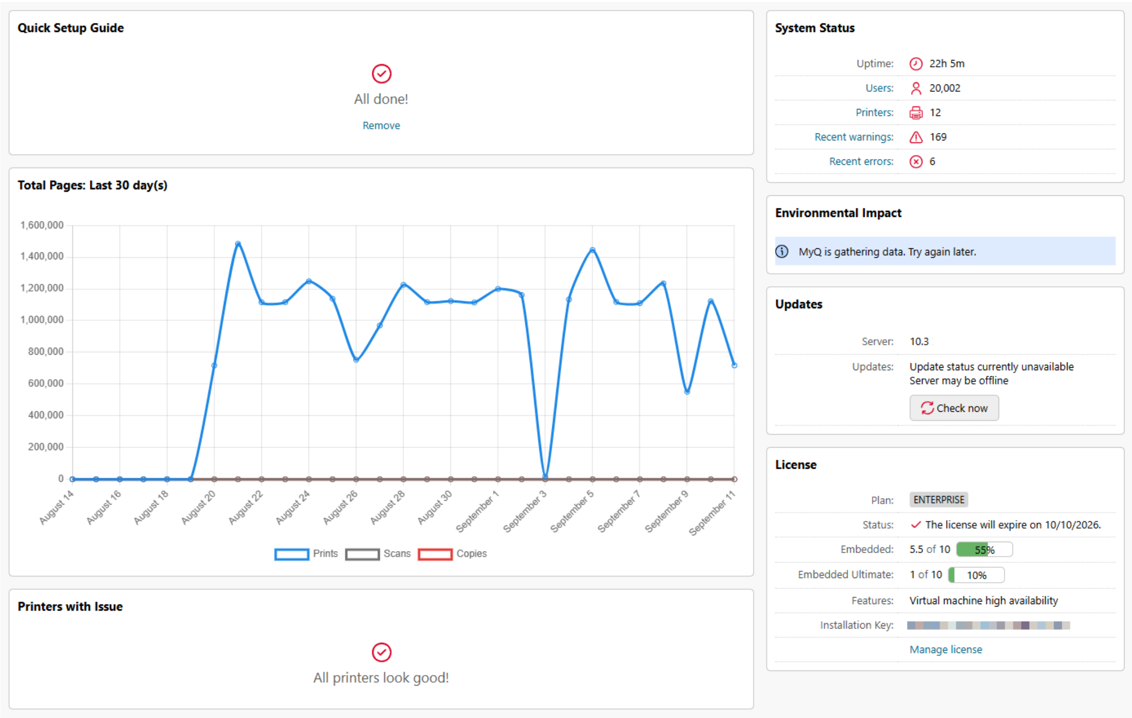
Settings menu

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 server.

7.4 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, display statistics, and generate support data.



The dashboard is customizable. It consists of adjustable 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.

The following widgets are supported. Widgets with an asterisk are displayed in the default layout.

- Environmental impact *
- Total Pages: Last 30 day(s) *
- License *
- Updates *
- Quick Links
- System Status *
- Quick Setup Guide *

System Status

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

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

Total Pages: Last 30 day(s)

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

Environmental Impact

Environmental Impact shows estimates of your environmental impact in Trees, CO_2, and Energy. The calculations are use these assumptions:

- 1 tree = 8333 pages
- 1 page = 12.7g of CO_2
- 1 page = 48Wh of energy
- 1 recycled page = 32Wh of energy

Updates

The **Updates** widget shows available updates for the MyQ installation and its components (terminal packages). To get the updates status, your installation key must be activated with a valid license. 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

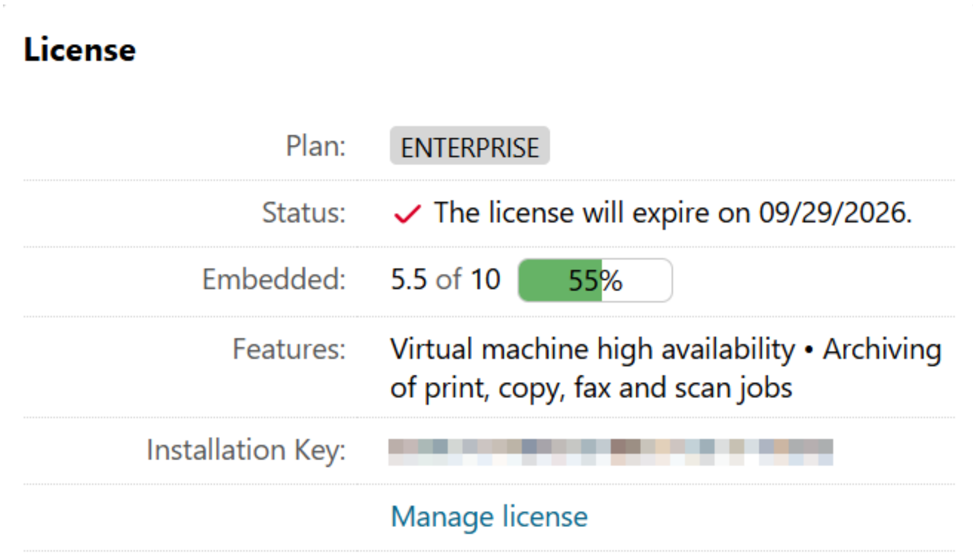
- **DEPRECATED** - this version is not being updated anymore, an upgrade path is recommended
  - Shown currently only for Server components - Print and Central Server, not Terminal Packages.

If no update information appears, click "**Check now**". This button is displayed only 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.

License

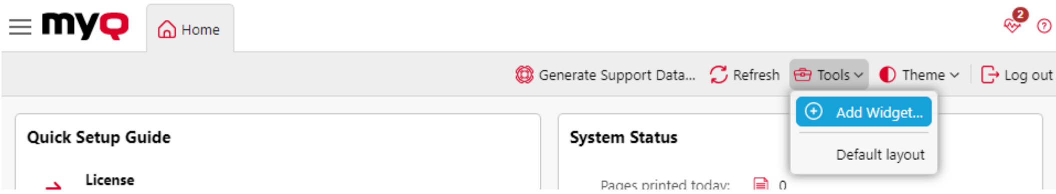
The **License** widget shows information about your license plan, software assurance status, license usage, features and your installation key. Click **Manage license** to open the **License** settings tab.



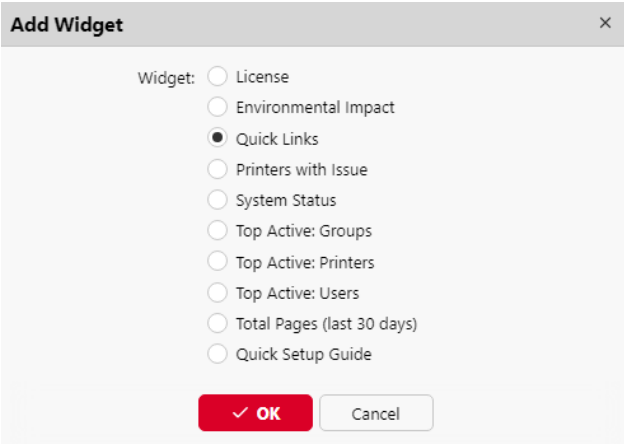
7.4.1 Customize the Dashboard

To add a new widget:

1. Click **Tools** at the top-right corner of the dashboard, and then click **Add Widget**. 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.

7.4.2 Change the Theme

To change the MyQ Web UI 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

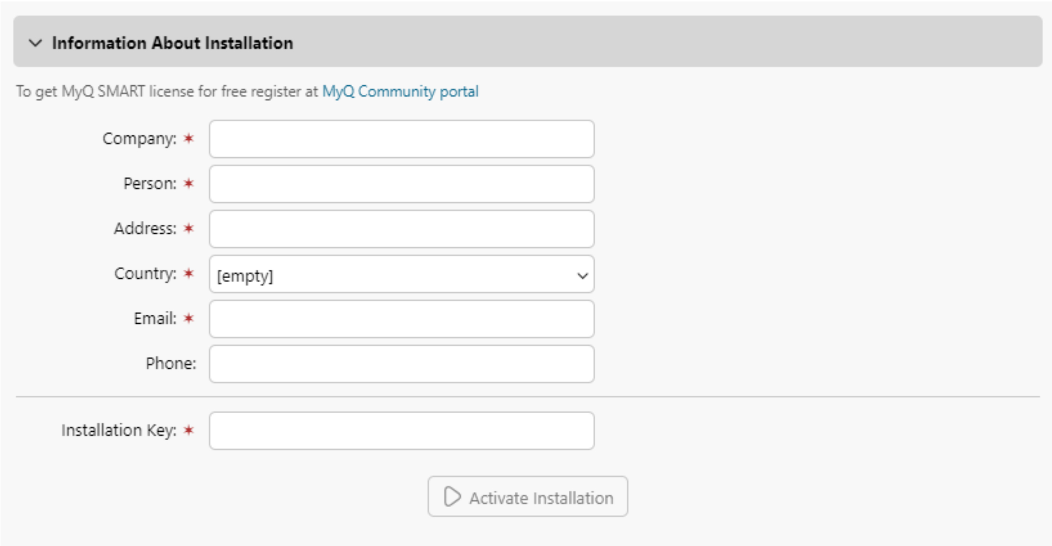
7.4.3 Quick Setup Guide

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

License

In this section you can provide information about your installation, and activate your installation key.

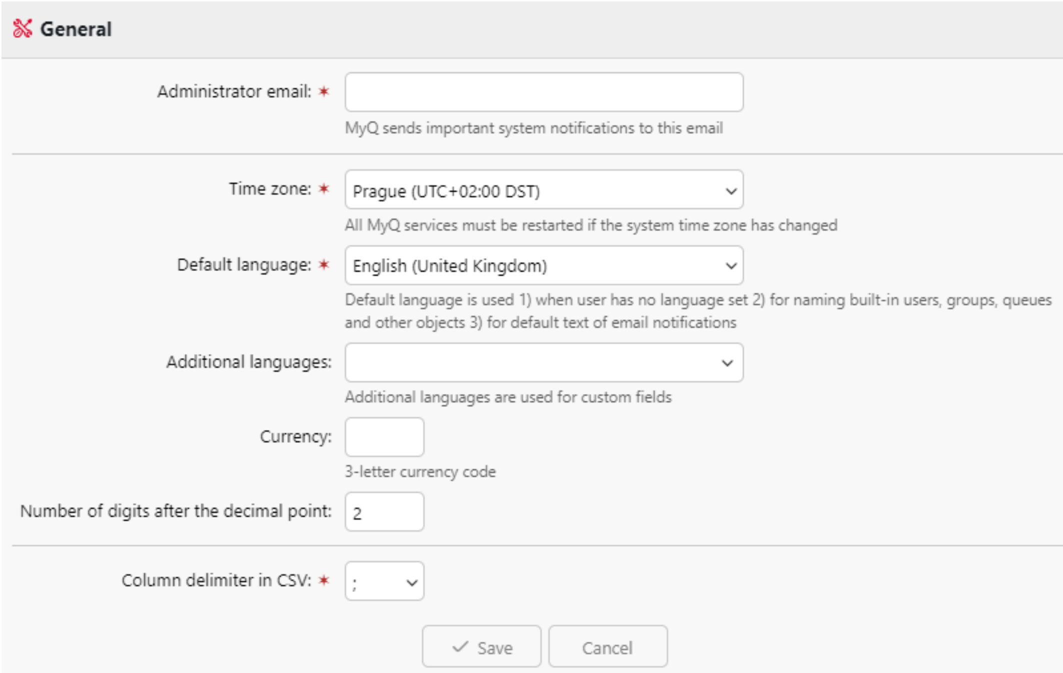
1. Click **Enter License**. The **License** settings tab opens. You are asked to enter the following information about your installation:



2. Enter your **installation key**.
3. Click **Activate Installation**.

You can also register in the MyQ Community portal and request a free **MyQ SMART** license.

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 **Users synchronization** settings tab, where you can import users from the MyQ Central server, from LDAP servers, or from a CSV file.

7.4.4 Generate Support Data

If you encounter a problem that requires help from the MyQ support team, providing detailed information about your MyQ system configuration, licenses, printer devices, terminals, etc., can be helpful in resolving your issue. You can generate a `MyQ-helpdesk_%datetime%.zip` file and send it to the MyQ support team.

Support ZIP File Contents

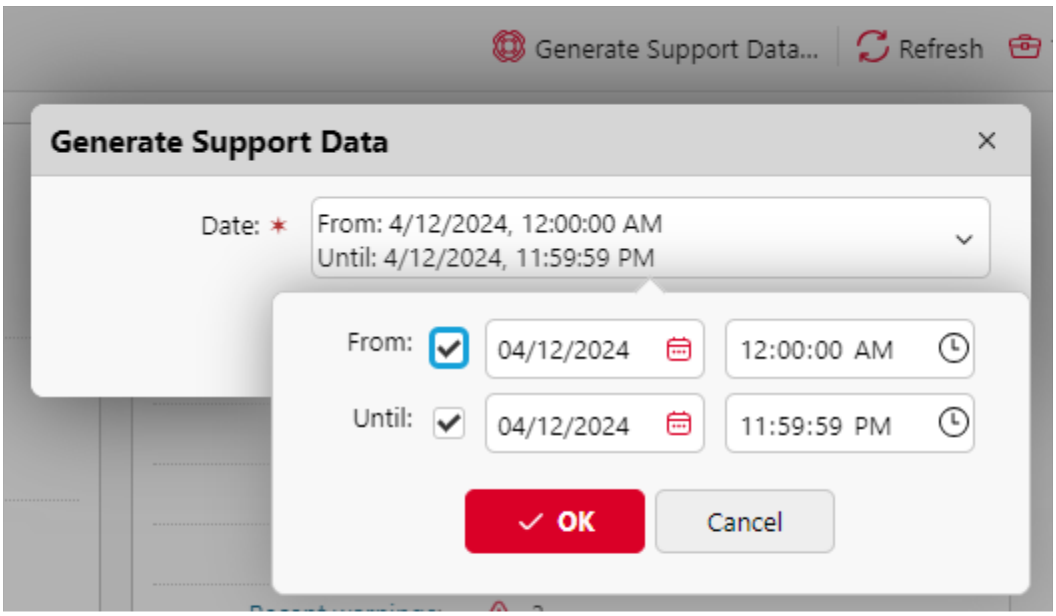
The *.zip* file contains:

- MyQ log file `log_%datetime%.xlsx`
- `MyQ-helpdesk.xml`
  This XML file contains necessary information about the MyQ configuration.
- the Logs directory, with error logs from Apache and PHP
- Windows Event log
- `The file statsData.xml`

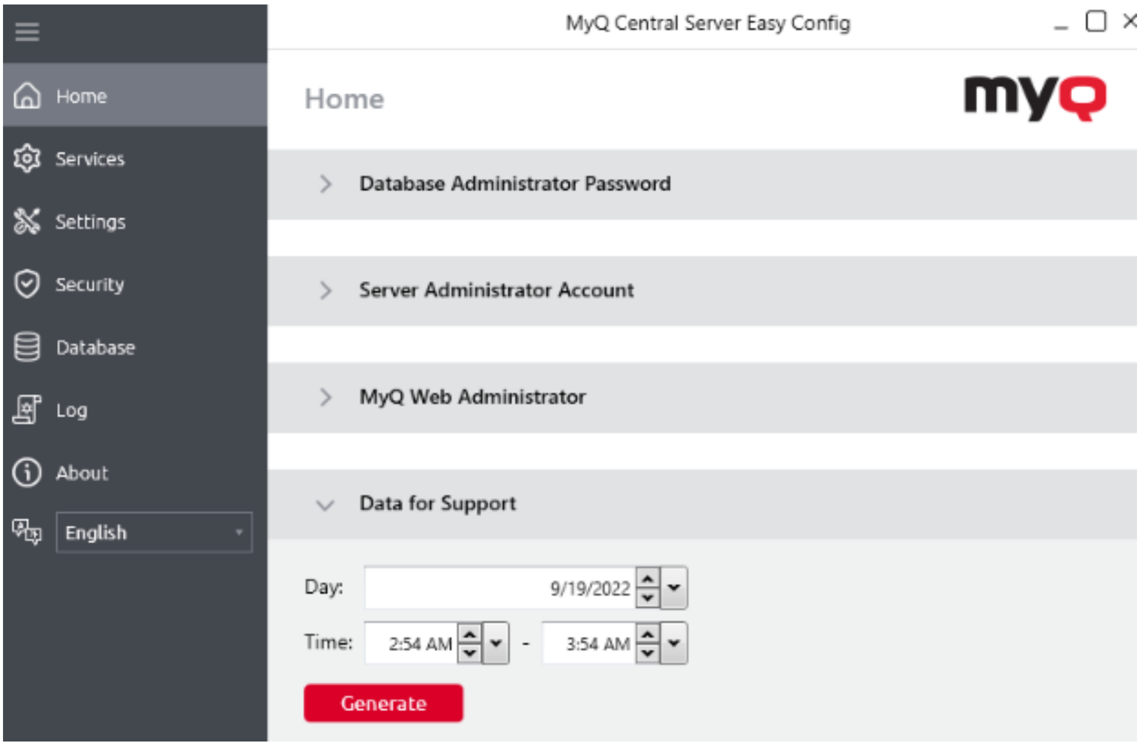
The MyQ log file corresponds to the MyQ log that can be displayed on the MyQ Web Interface or in the MyQ Easy Config application.

How to Generate Support Data

1. Click **Generate Support Data** at the top of the **Home** dashboard.
2. Specify the **Date** range of the MyQ events to include in the *MyQ-helpdesk* file, and click **OK**.
3. Click **Export**. The file is generated and saved to your *Downloads* folder.



You can also generate data for support in Easy Config. On 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.

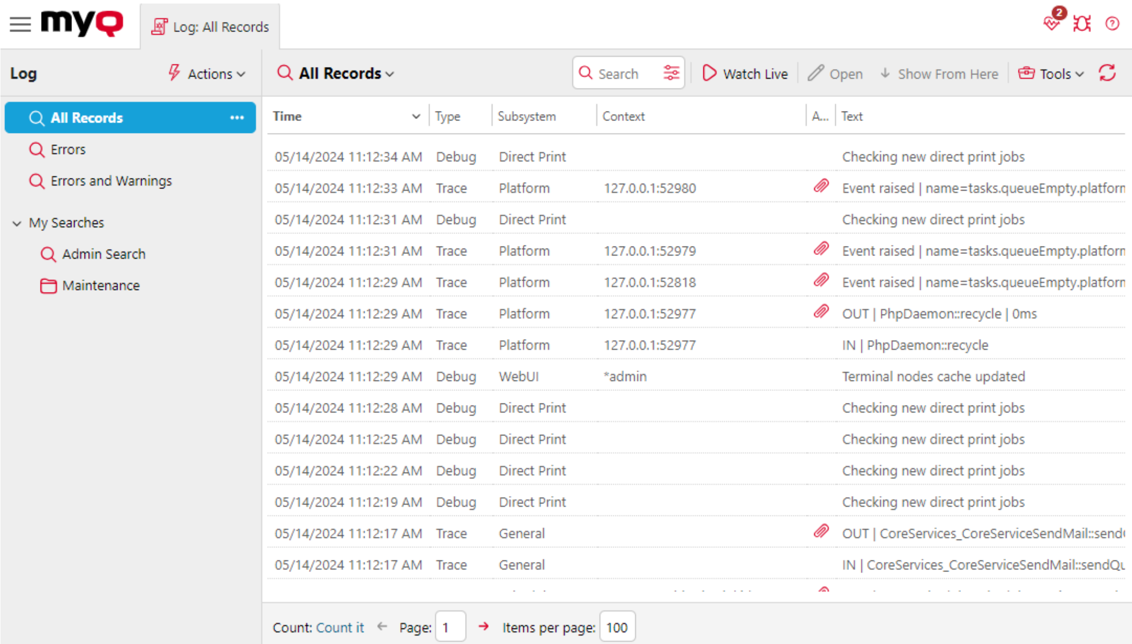


7.5 MyQ Log

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.



7.5.1 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.

7.5.2 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.

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

You can filter the log on the panel:

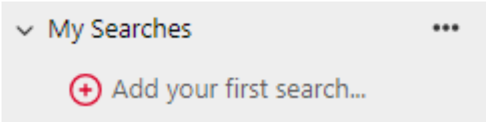
- After you pause the log, you can select the period in the **Date** combo box.
- In the **Verbosity** field you can select the type of log entries you want to view (*Critical, Info, Error*, etc.).
- In the **Subsystem** combo box, you can select/type one or more subsystems to be displayed in the log.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

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

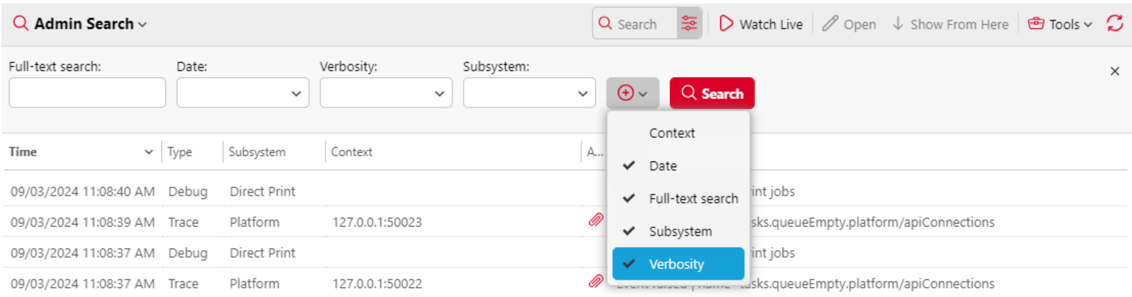
7.5.4 My Searches

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:

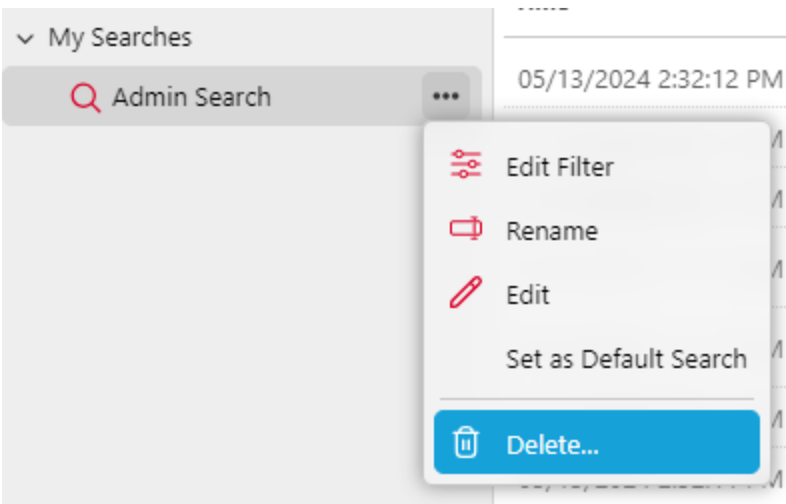
1. Click **Add your first search** or use the context menu and select **Add search** (if saved searches have already been created.



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.



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



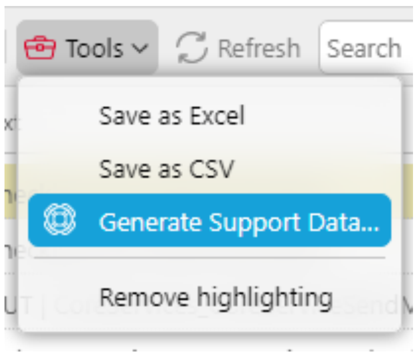
- **Edit Filter:** displays the filter editor for the search.
- **Rename:** allows the user to rename the search.

- **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.

7.5.5 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.

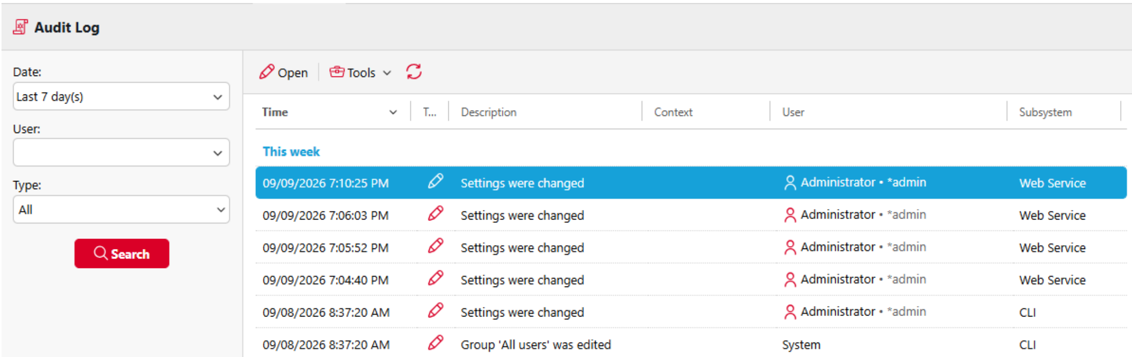
7.5.6 Highlighting log messages

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.

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

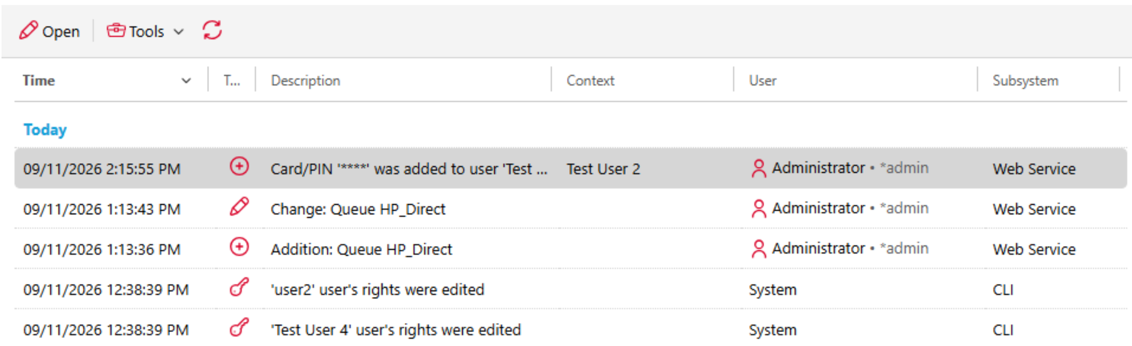
7.6 MyQ Audit Log

In the **MyQ Audit Log**, you can view all changes to 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.

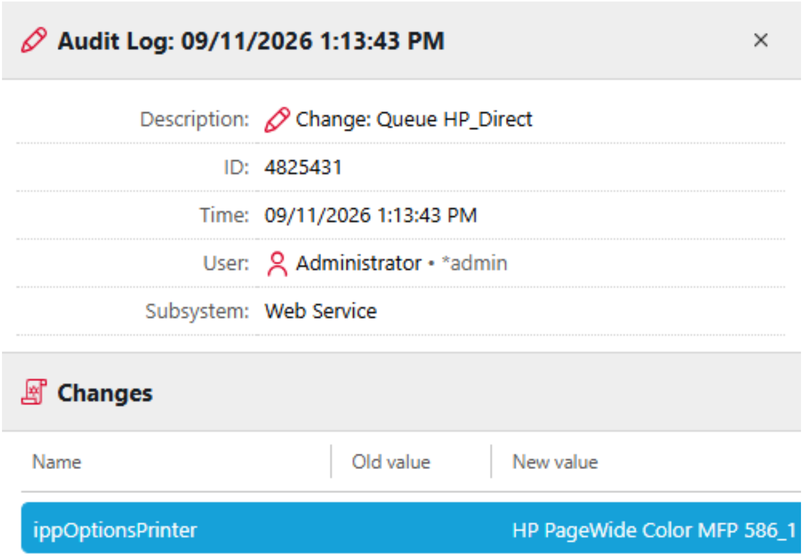


7.6.1 Opening the MyQ Audit Log

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**:



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



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

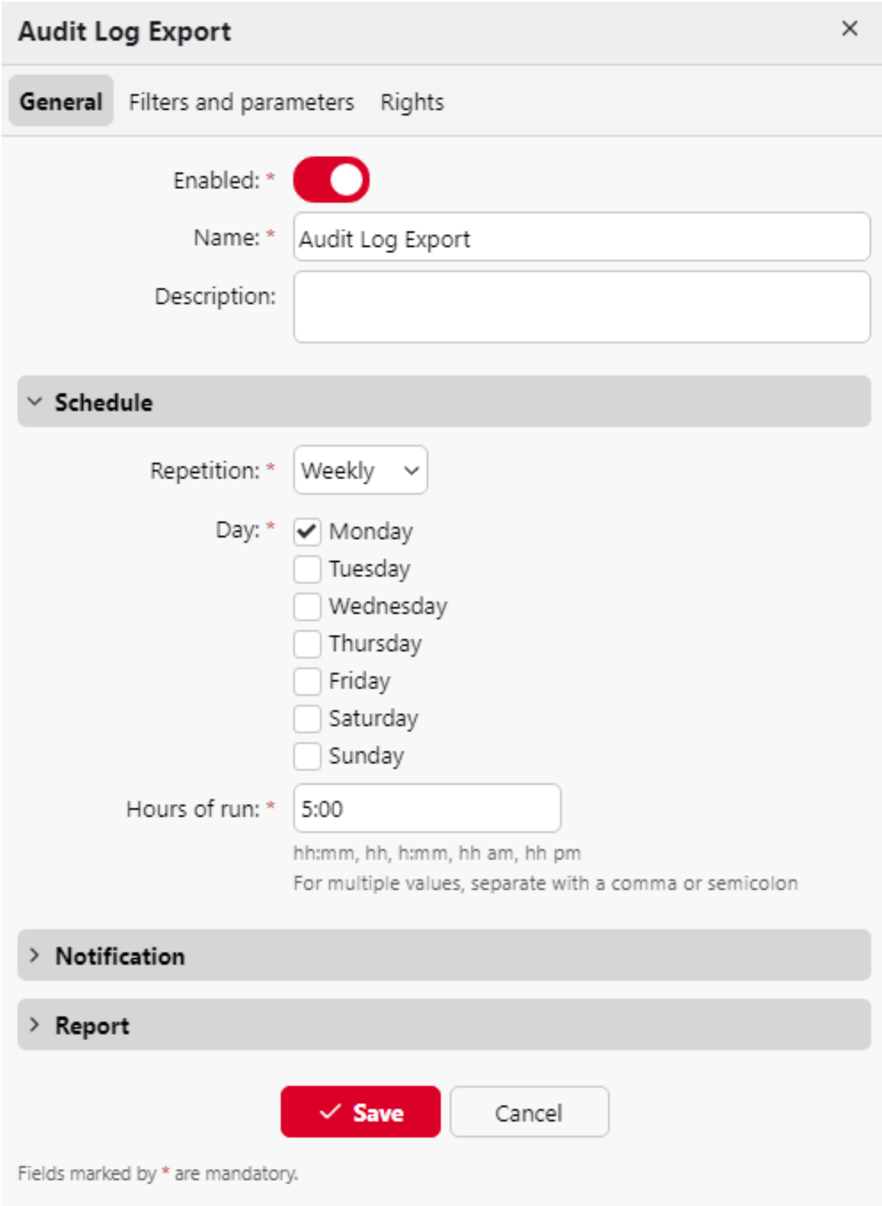
The displayed data can be filtered by a time period, the user who made the changes and the type of the event.

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.

7.6.3 Exporting the Audit Log

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

You can also click **Schedule Export** to have the log regularly exported as scheduled task. The schedule properties panel opens to the right, where you can set the parameters of the task.


Audit Log Export
General
Filters and parameters
Rights
Enabled: *
Name: *
Audit Log Export
Description:
Schedule
Repetition: *
Weekly
Day: *
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sunday
Hours of run: *
5:00
hh:mm, hh, h:mm, hh am, hh pm
For multiple values, separate with a comma or semicolon
Notification
Report
Save
Cancel
Fields marked by * are mandatory.

8 Central & Site Administration

MyQ Central Server centrally manages environments with multiple Site Servers, which handle local printing devices and jobs.

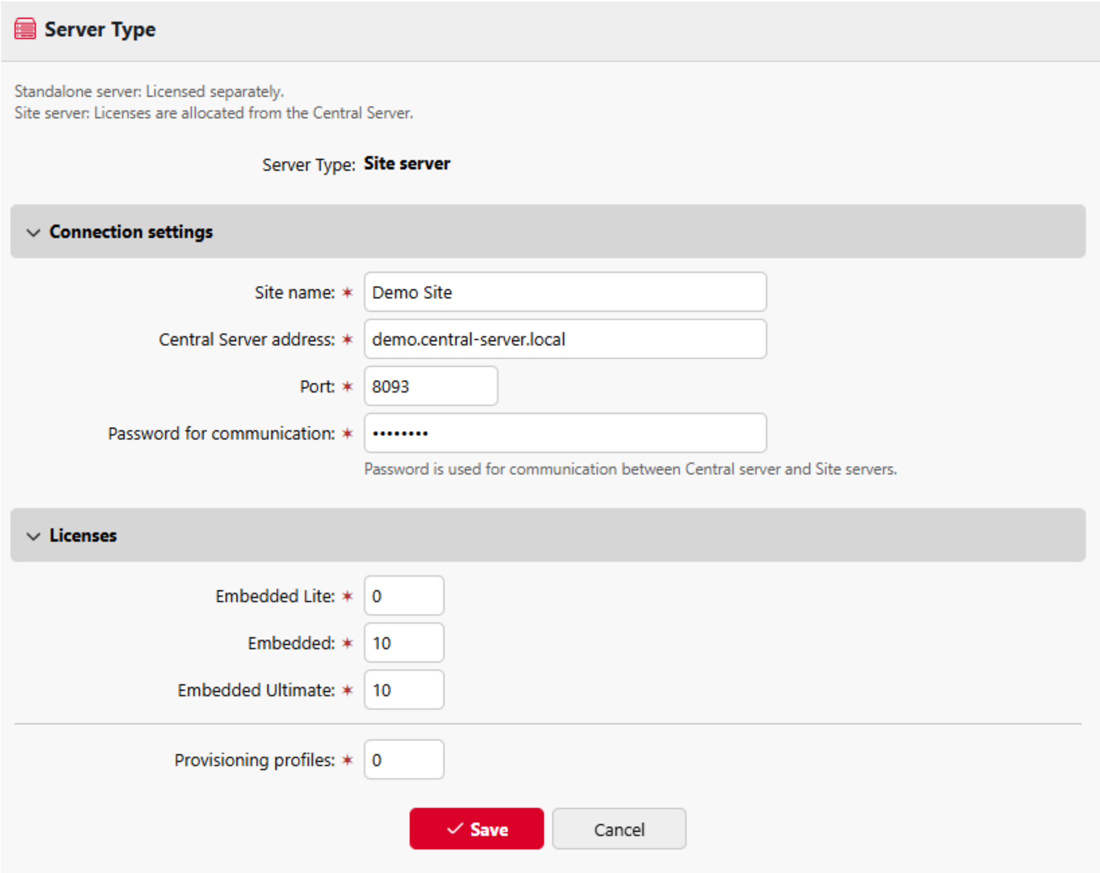
The Site Servers work as print servers and perform local management of printing devices and print jobs. Their function and management options are similar to those of a standalone server.

To create a Central-Site configuration, follow these general steps:

1. On the Central Server, go to **MyQ > Settings > Licenses** and activate your license key. Then go to **MyQ > Settings > General** and set a password for communication.
2. On each Site server, go to **MyQ > Settings > Server Type** and change the Server Type to Site server. Then configure the connection settings and licenses, and click **Save**.

If you have configured the connection successfully, after a few moments the new Site appears in **MyQ Central Server > Sites**.

8.1 Convert a Standalone Server to a Site 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.

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.
- **Port** - *8093* by default.
- **Password for communication** - enter password used by the Site Server to communicate with the Central Server. Set this password in **MyQ Central Server > Settings > General**.

In the **Licenses** section, add the number of each license to reserve from the Central Server.

- **Embedded Lite**
- **Embedded**
- **Embedded Ultimate**
- **Provisioning Profiles**

8.2 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.

8.3 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. You can also exclude IP ranges in this tab.
- On the **Rights** tab, you can manage user rights for the Site server.

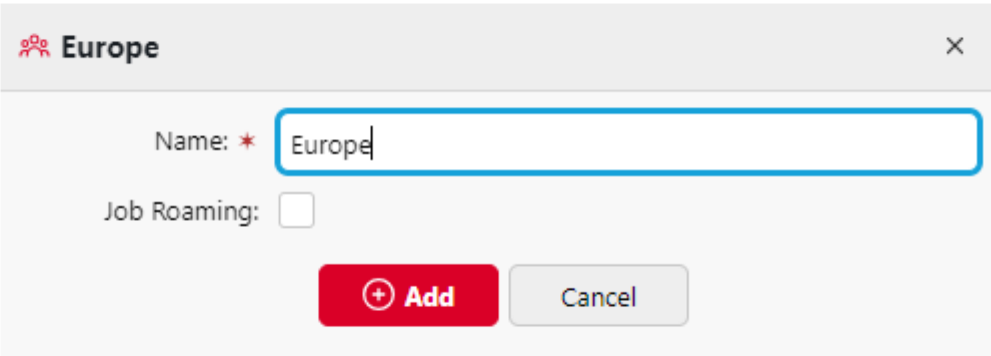
After any modification, click **Save**. Any changes are then distributed during the User Synchronization.

8.4 Grouping Sites

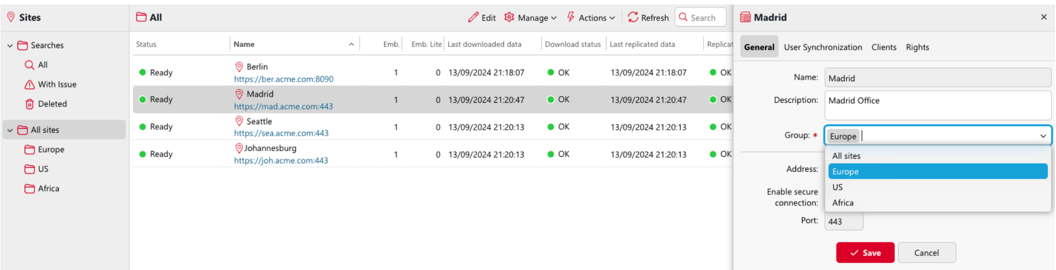
Sites can be grouped to correspond to regions, or your organization's needs.

To create a new site group:

1. On MyQ Central Server, go to **MyQ > Sites**. Click **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).



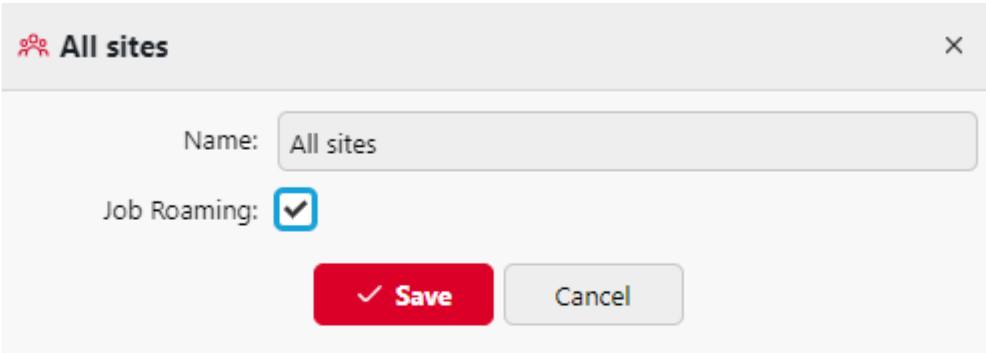
3. Once you have created a group, sites can be moved into it using the **Group** field in a sites **General** settings tab. Each site can only be added to one **Group**.



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.

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.

See also: Job Roaming (see page 132)

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.

8.5 Site Server Data Replication

To configure how data is replicated from Sites and troubleshoot replication errors, go to **MyQ > Settings > Data Replication from Sites**.

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. Go to **MyQ > Sites**.
2. 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.

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.

See also:

- Task Scheduler Settings (see page 141)
- Data Replication Settings (see page 164)

8.6 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.

8.7 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.

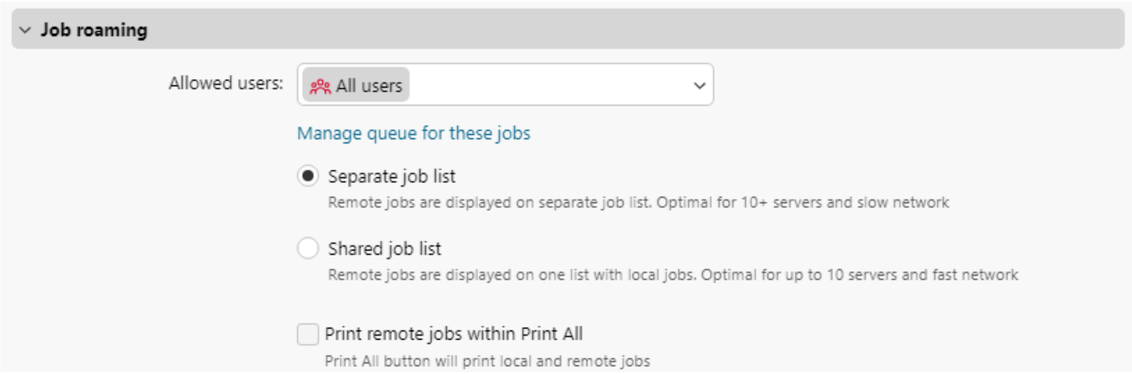
While this feature works in Central/Site mode only, it does not have to be centrally managed – Job Roaming between two locations depends exclusively on the settings of the locations Site servers.

> **Security changes in Patch 24**
> Starting with Print Server 10.2 patch 24, Job Roaming uses site-to-site authentication to protect the channel used for cross-site job transfer. This change is not backward compatible and requires all sites to be updated to maintain full Job Roaming functionality.
> See also: (10.2) Upgrading to Patch 24 or later - Job Roaming Authentication Change

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 WebUI go to **MyQ, Settings, Jobs**. In the **Job roaming** section, the following options are available:

- **Allowed users**
  Specify which users are allowed to use job roaming.
- **Manage queue for these jobs**
  Click to open and manage the properties of the job roaming queue.
- **Separate job list**
  Display remote print jobs on a separate job list. Use this option if you have 10 or more servers and a slow network connection.
- **Shared job list**
  Display remote print jobs on the same job list as local jobs. Use this option if you have up to 10 servers and a fast network connection.
  - **Print remote jobs with Print All**
    Select this option to enable **Print All** terminal action to print both local and remote jobs. This option is available with a shared job list only.


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

9 MyQ System Settings

This topic introduces the MyQ system settings. To access the settings below, go to **MyQ > Settings.**

9.1 License

On the License settings tab, you can view your installation key, add, activate refresh and remove licenses, and manage software assurance plans.

9.2 General

On the General settings tab, you can set the administrator email, change regional settings, and other general settings.

9.3 Personalization

On the Personalization settings tab, you can add custom help links and custom logos to be used in various parts of the MyQ system.

9.4 Task Scheduler

On the Task scheduler settings tab, you can add new task schedules, change their settings and run scheduled tasks.

9.5 Network

On the Network settings tab, you can modify network settings such as certificates, server ports, etc.

9.5.1 Connections

On the Connections Settings tab, you connect MyQ to external cloud services such as Gmail, Microsoft Entra applications, Microsoft Exchange Online.

9.5.2 Authentication Servers

On the Authentication servers settings tab, you can add LDAP, Microsoft Entra ID and Radius servers for user authentication.

9.6 Printers

On the Printers settings tab, you can control the duration of temporary cards validity in hours.

9.7 Users

On the Users settings tab, you can configure general user account options (enable user profile editing, show more info in the user profile widget, enable personal queues settings, delegate changes, and deleting all ID cards), set up new user registration (via the Web Interface, job submission, or email), and configure timeout and account lockout settings.

9.7.1 User Synchronization

On the User Synchronization settings tab, you can import and synchronize users from LDAP servers, Microsoft Entra ID, Google Workspace, and other sources, and configure their properties.

9.7.2 Rights

On the Rights settings tab, you can give users or groups of users administrator rights, or rights to run specific MyQ agendas (managing printers, users, jobs, reports, and more).

9.8 Accounting

On the Accounting settings tab, you can set the accounting mode (Accounting Group or Cost Center) and the payment account priority for terminals and queues that don't support account selection.

9.8.1 Credit

On the Credit settings tab, you can activate credit-based accounting, where users can print, copy, and scan only while they have sufficient credit, and configure recharge methods.

9.9 Data Replication From Sites

On the Data Replication from Sites settings tab, Central server administrators can choose which data types (jobs, projects, printer groups, printer events, price lists, and more) get replicated from Site servers.

9.10 Reports

On the Reports main tab, you can create, generate, and schedule reports on users, printing devices, and print jobs, exportable as PDF, CSV, XML, XLSX, or ODS.

9.11 External Reports

On the External Reports settings tab, you can enable a read-only database account for external BI tools and reporting software to safely query the MyQ database.

9.12 REST API Apps

On the REST API Apps settings tab, you can register applications for access to the MyQ REST API, each with a title, scope, client ID, and secret.

9.13 Log

On the Log 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.

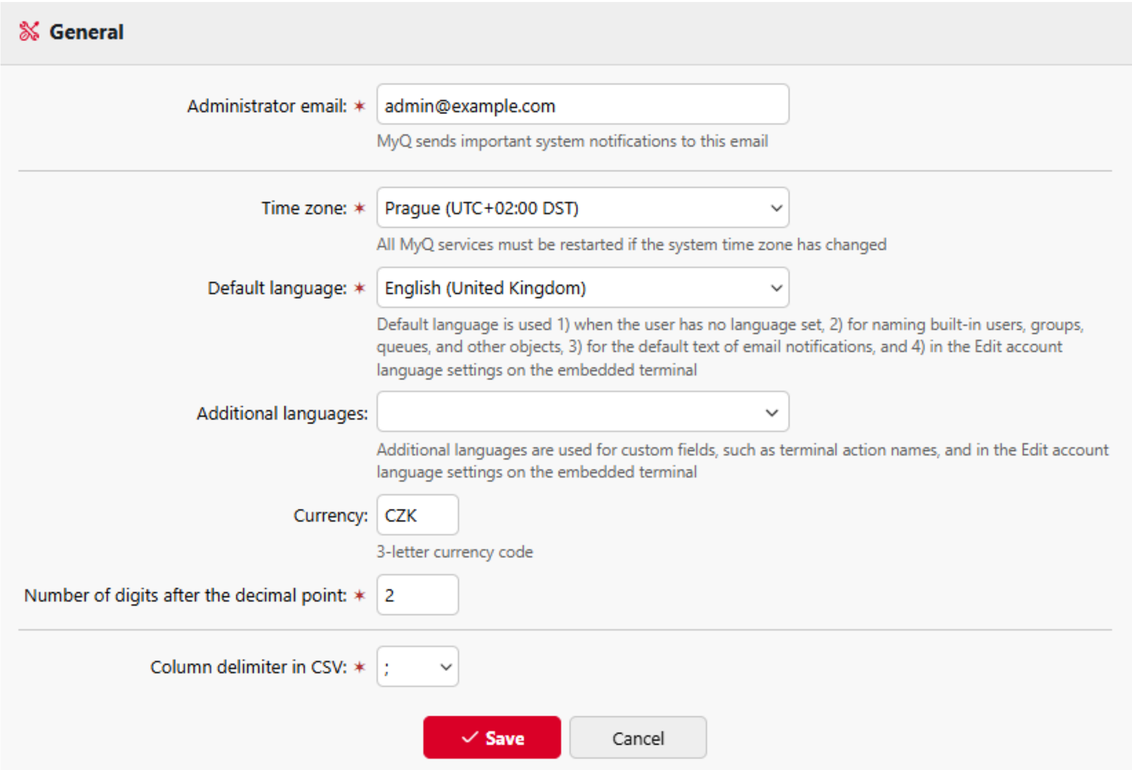
9.14 System Management

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.

9.15 General Settings

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

9.15.1 General



- **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. See Available languages (see page 325).
- **Currency**: In the currency setting, 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.

9.15.2 Security

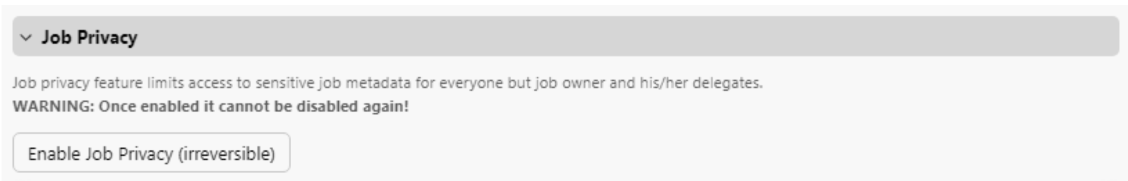
In the **Security** section, you can set the Central Server **Password for communication**. You must enter the same password on each Site Server, in **MyQ > Settings > Server Type**.

9.15.3 Job Privacy

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, Job Privacy cannot be disabled!

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

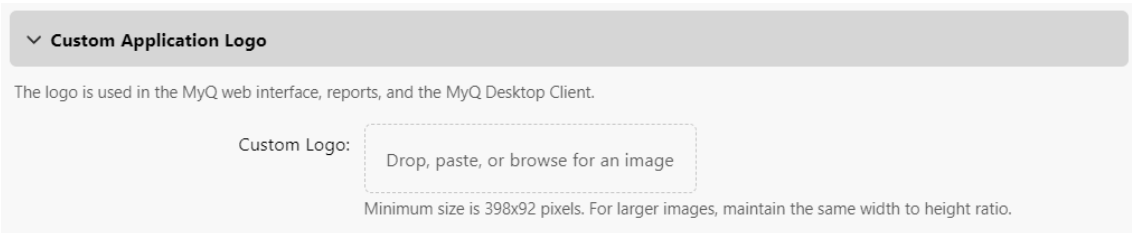


In the confirmation pop-up, type your Server administrator password in the **Password** field, and click **Enable Job Privacy (irreversible)**.

9.16 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.

9.16.1 Custom Application Logo



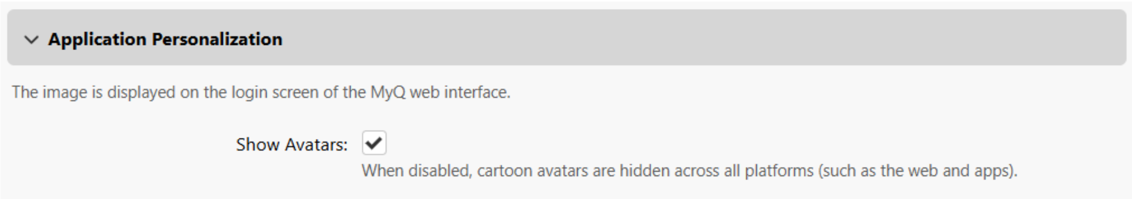
Here you can add your company's logo to be used in the MyQ system. The logo will appear on the upper right corner of the MyQ Web Interface, on MyQ credit vouchers, and on reports.

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.

9.16.2 Application Personalization

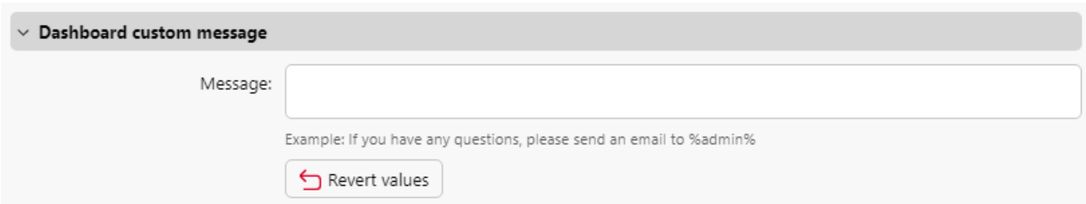
Here you can enable or disable the MyQ branding avatars that are generally shown on login screens, currently on the Web Interface. Disabling this option will disable these avatars across all platforms (Desktop Clients, mobile application, etc.).



9.16.3 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.

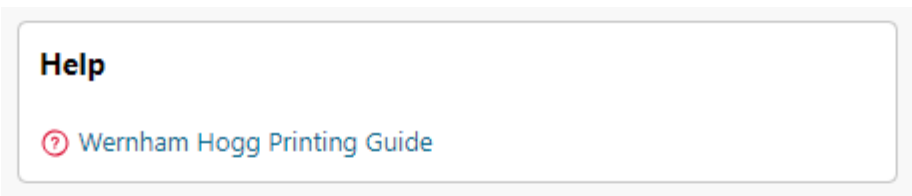
The *%admin%* parameter can be used to display the email address of the MyQ administrator within the message (the Administrator email set on the General settings tab).



9.16.4 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.

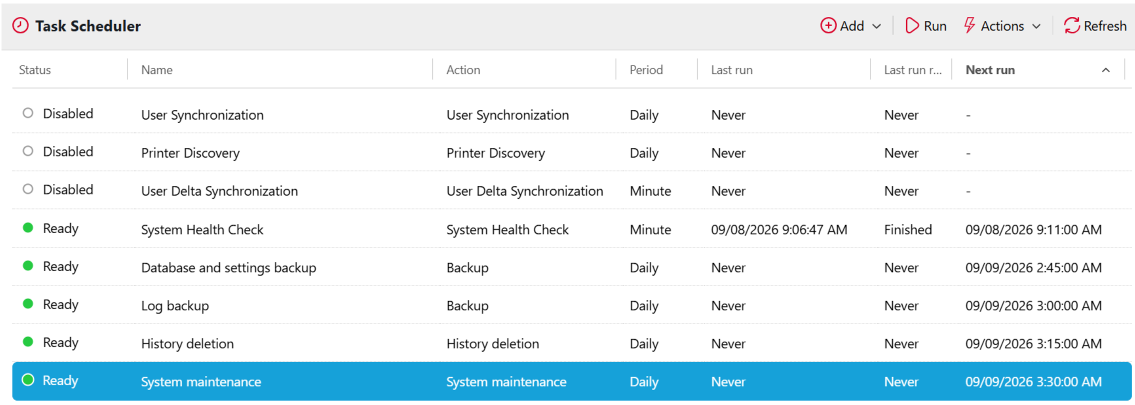


9.17 Task Scheduler Settings

The **Task Scheduler** settings tab serves as an interface for planning regular tasks in MyQ, and includes the following predefined tasks:

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

In addition, you can import projects from CSV files, and execute external commands.



Status	Name	Action	Period	Last run	Last run r...	Next run
Disabled	User Synchronization	User Synchronization	Daily	Never	Never	-
Disabled	Printer Discovery	Printer Discovery	Daily	Never	Never	-
Disabled	User Delta Synchronization	User Delta Synchronization	Minute	Never	Never	-
Ready	System Health Check	System Health Check	Minute	09/08/2026 9:06:47 AM	Finished	09/08/2026 9:11:00 AM
Ready	Database and settings backup	Backup	Daily	Never	Never	09/09/2026 2:45:00 AM
Ready	Log backup	Backup	Daily	Never	Never	09/09/2026 3:00:00 AM
Ready	History deletion	History deletion	Daily	Never	Never	09/09/2026 3:15:00 AM
Ready	System maintenance	System maintenance	Daily	Never	Never	09/09/2026 3:30:00 AM

9.17.1 Running and setting task schedules

To manually run a task schedule:

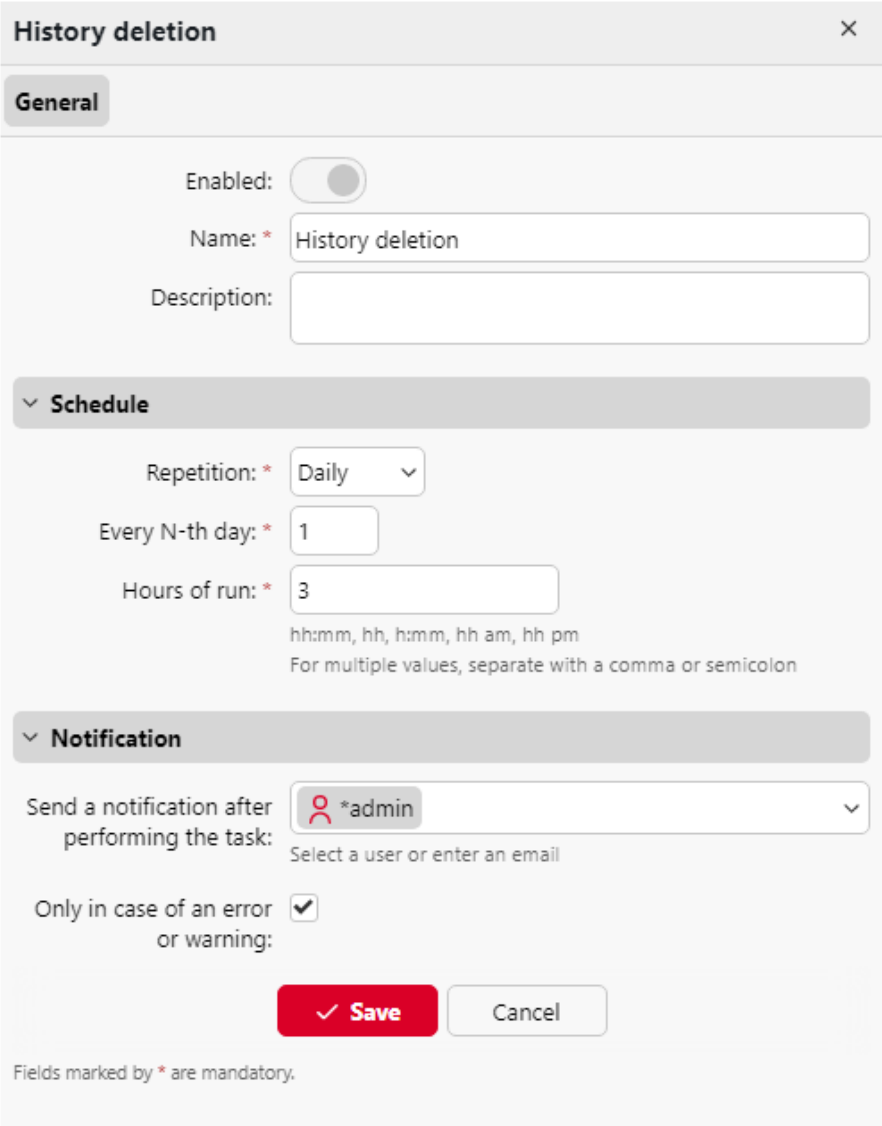
- Select the task schedule that you want to run.
- Click **Run** on the **Task Scheduler** toolbar.

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 opt to enable email notifications. 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, contains task-specific parameters. These include filenames, email distribution, and backup lifetime settings.

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

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.

9.17.2 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**.

9.18 Network Settings

On the **Network** settings tab, you can manage the network communication between the MyQ 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 Management.

9.18.1 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.

9.18.2 Certificates

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 **Export CA certificate**) to install it to clients, so they trust MyQ server.
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

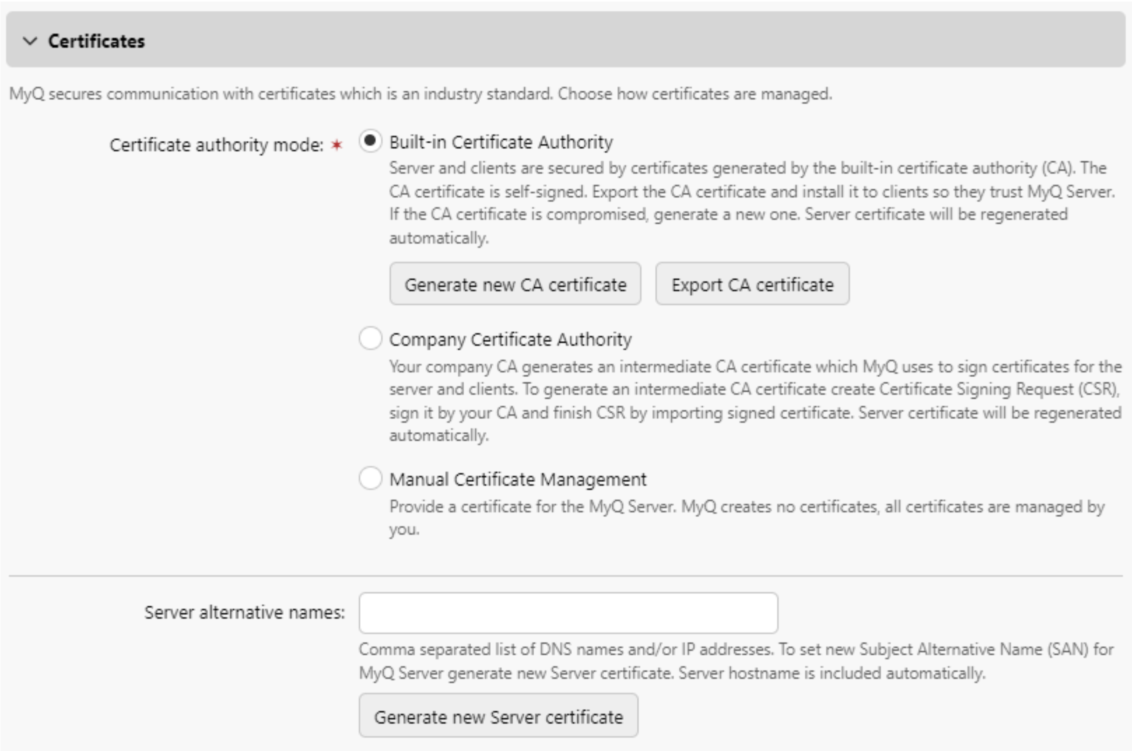
(CSR), sign it by your CA and click **Finish CSR** to finish CSR by importing signed certificate. If the intermediate CA certificate does not contain a CA root certificate in its chain, the administrator is prompted to upload the public key of the CA root certificate as well (the **Import CA root certificate** 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.

Use the **Server alternative names** field to specify additional DNS names and/or IP addresses to
include in the certificate's **Subject Alternative Name (SAN)** extension, entered as a comma-separated list. The server hostname is included automatically.

> **Important**!
> Any IP address or hostname that devices or the MyQ Desktop Client (MDC) use to connect to the server must be listed here. If a client connects by IP address and that IP is not included, certificate validation will fail and the client will be unable to authenticate. This applies to both Device Configuration Profiles and MDC configurations that reference the server by IP. As a best practice, populate this field during initial installation, before enrolling devices or deploying MDC.

After editing the **Server alternative names** field, click **Generate new Server certificate** to
apply the changes.



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**.

9.18.3 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 emails are forwarded.
To configure the server, do the following:

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

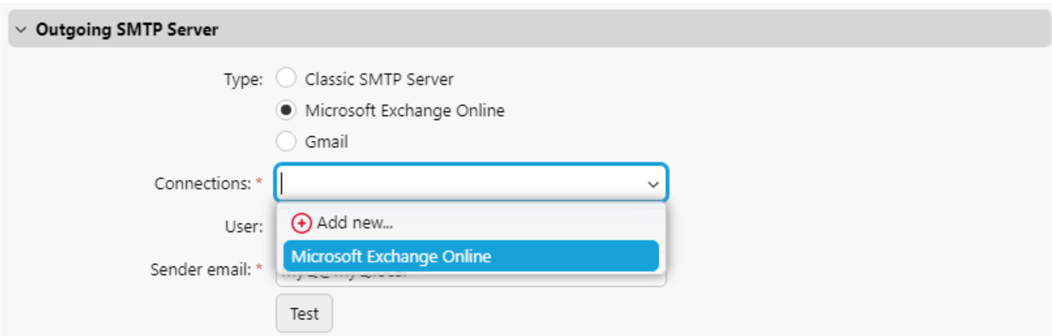
Classic SMTP Server

1. Enter the server hostname or IP address in the **Server** text box. If the email server listens to a port other than the 25 TCP port, change the **Port** setting to the correct value.

2. Choose one of the available **Security** options.
    a. **Prefer StartTLS** - allows even unencrypted communication (default)
    b. **Implicit TLS** - allows only full encryption
    c. **Require StartTLS** - allows for the handshake to be unencrypted then switches to encrypted
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** for 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.

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. See Connect to Microsoft Exchange Online (see page 154)

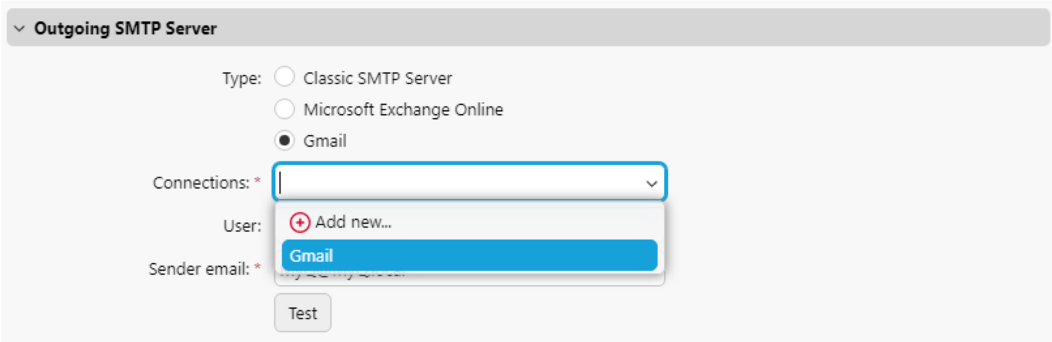


2. If credentials are required, enter the **User**.
3. Enter the address that you want to be displayed as the **Sender email** for PIN, alert and report messages.
4. After you enter the data, you can click **Test** to test the connection to the email server and click **Save** to save your changes.

Gmail

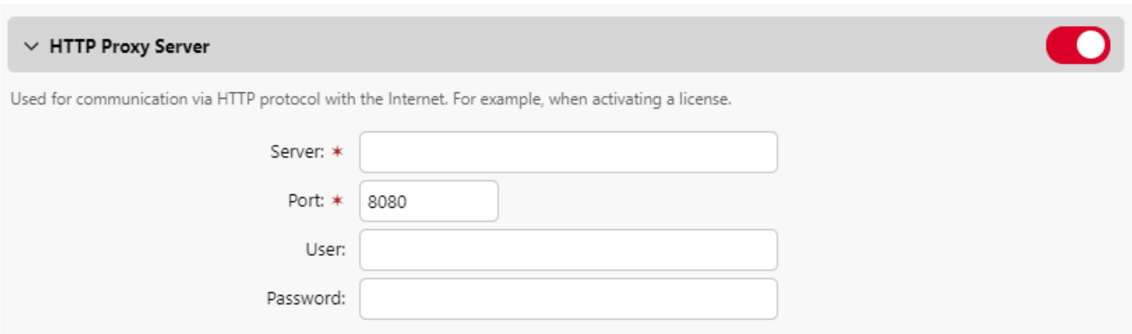
1. If you have already set up a Gmail server in the **Connections** settings, the server is available in the **Connections** field drop-down. If not, you can click on the **Connections**

field and then click **Add new** to add your Gmail server connection. See Connect to Gmail with OAuth2 (see page 149)



2. If credentials are required, enter the **User**.
3. Enter the address that you want to be displayed as the **Sender email** for 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.

9.18.4 HTTP Proxy Server



In this section, you can choose whether to enable and 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.

Supported/Unsupported HTTP Proxy Services

Supported Services

- Microsoft Azure Entra ID
- Microsoft OneDrive for Business
- Microsoft OneDrive Personal
- Microsoft SharePoint Online

- Microsoft Exchange Online
- Gmail
- Google Drive
- Dropbox
- Box
- Amazon S3
- License Server Communication

Unsupported Services ❌

- Microsoft Exchange (Local)
- Payment Providers
- Site → Central Communication
- Central → Site Communication
- Site → Terminals Communication

9.18.5 Firewall Management

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

9.18.6 Connections Settings

In **MyQ > Settings > Network > Connections**, you can connect MyQ to external cloud services.

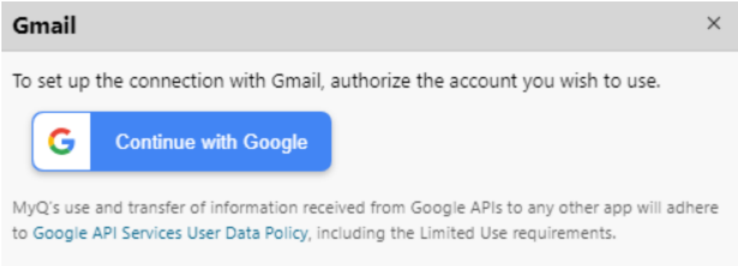
Click **Add** and select one of the following available services:

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

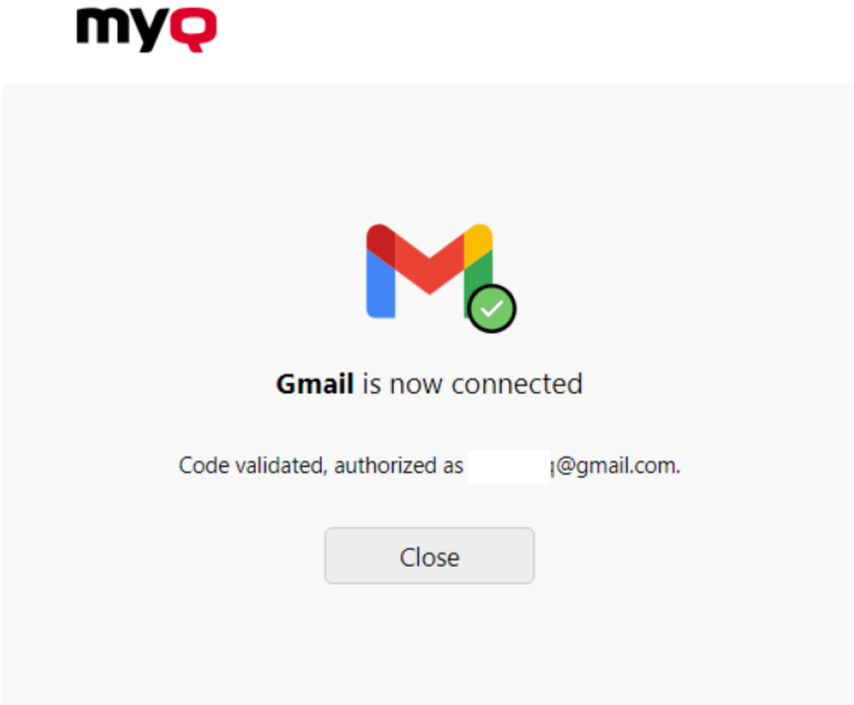
Connect to Gmail with OAuth2

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 uses and transfers information received from Google APIs to any other app in adherence with Google API Services User Data Policy, including the Limited Use requirements. See Google API Services User Data Policy[21].

21. http://redirect.myq.cz/?id=myqServer.googleSecurityPolicy&version=10.2&l=en-us

Connect to Microsoft Entra ID (Graph API)

Connect MyQ X to Microsoft Entra ID to synchronize users and groups and to authenticate MyQ users with their Microsoft identity. The connection can be used for:

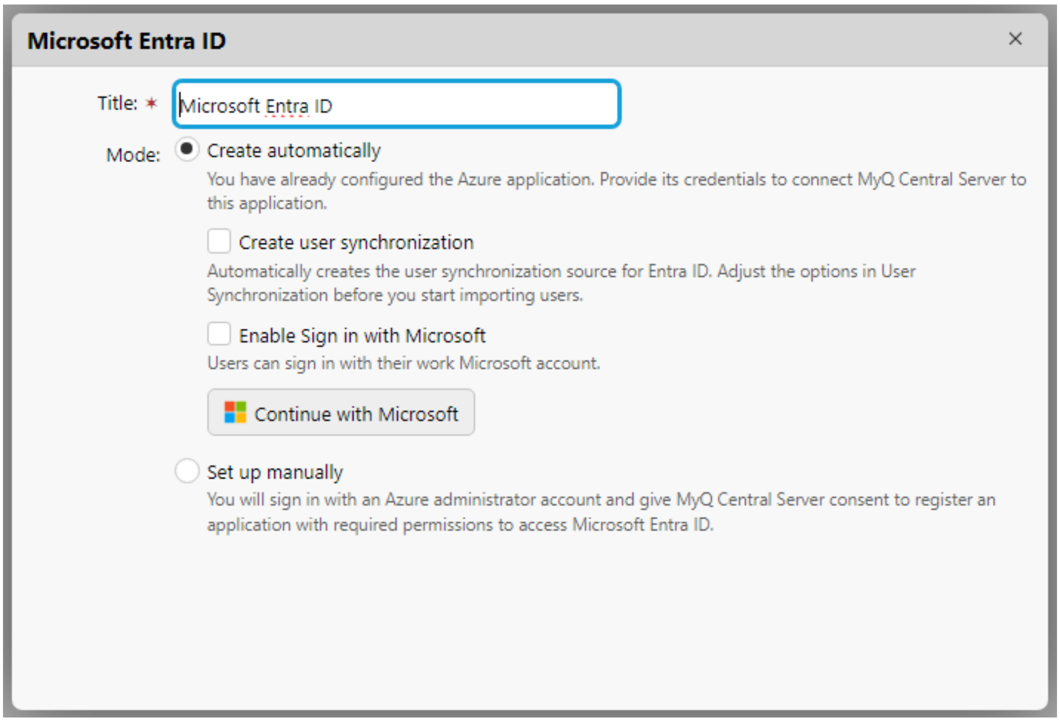
- synchronizing users and groups from Microsoft Entra ID
- authenticating users against Microsoft Entra ID
- Sign in with Microsoft
- Seamless SSO with MyQ Desktop Client

You can create the required Microsoft application automatically from MyQ, or connect MyQ to an application registration that you manage manually.

Microsoft Entra ID, OneDrive for Business, and SharePoint Online can use the same manually registered application. If you plan to use these integrations together, configure the application with the combined permissions required by them.

Create a Microsoft Entra ID Connection

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



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 the connection automatically

During setup, sign in with a Microsoft account that can grant the permissions required to create and configure the connector application.

Permission	API	Type	Purpose
`Application.ReadWrite.All`	Microsoft Graph	Delegated	Create or update the connector application credential.
`Directory.Read.All`	Microsoft Graph	Delegated	Read tenant information, including the default domain name.

MyQ creates the connector application and configures it with the runtime permissions required for the selected integration. Complete the Microsoft authorization process and save the connection.

You can also create the corresponding user synchronization source and enable **Sign in with Microsoft** during setup.

Connect a manually registered application

Select **Set up manually** if your organization manages Microsoft Entra application registrations directly.

Before configuring MyQ, register a Microsoft Entra application for MyQ X, and configure the application with the required API permissions.

For an Entra ID-only integration, configure the permissions identified for **Microsoft Entra ID**. If the same application is also used for OneDrive for Business or SharePoint Online, add the permissions required by those integrations.

Grant administrator consent where required.

Required Permissions

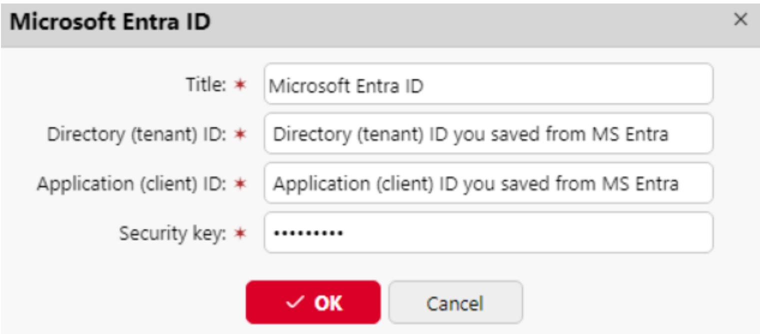
Permission	API	Type	Purpose
`Group.Read.All`	Microsoft Graph	Application	Read groups and group membership.

Permission	API	Type	Purpose
`User.Read.All`	Microsoft Graph	Application	Read users.
`User.Read`	Microsoft Graph	Delegated	Sign in and read the signed-in user's profile.

Then enter the following values from the application registration in MyQ:

- **Application (client) ID**
- **Directory (tenant) ID**
- **Client secret**

Save the connection.



Configure user synchronization

Creating the Entra ID connection does not itself import users.

To synchronize users and groups, create a **Microsoft Entra ID** synchronization source in **MyQ > Settings > User Synchronization** and select the connection you created.

See also: Synchronize Users from Microsoft Entra ID (see page 231)

Configure authentication

To authenticate users with Microsoft Entra ID, configure the corresponding authentication server and associate it with the Entra ID connection.

Depending on your environment, you can also configure:

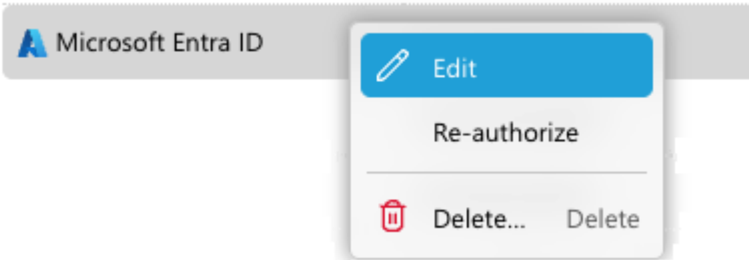
- **Sign in with Microsoft**
- **Seamless SSO** for MyQ Desktop Client

The required authentication scopes and redirect URIs are listed separately.

See also: (v2) Microsoft Entra Application Reference

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.



Multiple Microsoft Entra tenants

MyQ can connect to multiple Microsoft Entra tenants. Create a separate connection for each tenant and assign the appropriate synchronization source and authentication configuration to each connection.

Next Steps

You are now ready to configure synchronization and authentication through Microsoft Entra ID with Microsoft Graph.

See also:

- (10.3) Configure Microsoft Entra ID Authentication
- Synchronize Users from Microsoft Entra ID (see page 231)

Connect to Microsoft Exchange Online

Connect MyQ X to Microsoft Exchange Online to use an Exchange Online mailbox for MyQ email services.

The connection can be used for:

- sending MyQ system email through Exchange Online
- sending scanned documents by email
- receiving print jobs through **Jobs via Email**

Microsoft Exchange Online requires a dedicated Microsoft Entra application registration. Do not reuse the application registration used for Microsoft Entra ID, OneDrive for Business, or SharePoint Online.

> ⚠ If MyQ will send email through Exchange Online, **SMTP AUTH** must be enabled for the Exchange Online tenant and for the mailbox used by MyQ. If SMTP AUTH is disabled, MyQ cannot send email through the connection.
> For information about enabling SMTP AUTH, see the Microsoft Exchange Online documentation.

Configure the Microsoft application

Configure the dedicated application registration for Microsoft Exchange Online as described in (v2) Set up Microsoft Exchange Online.

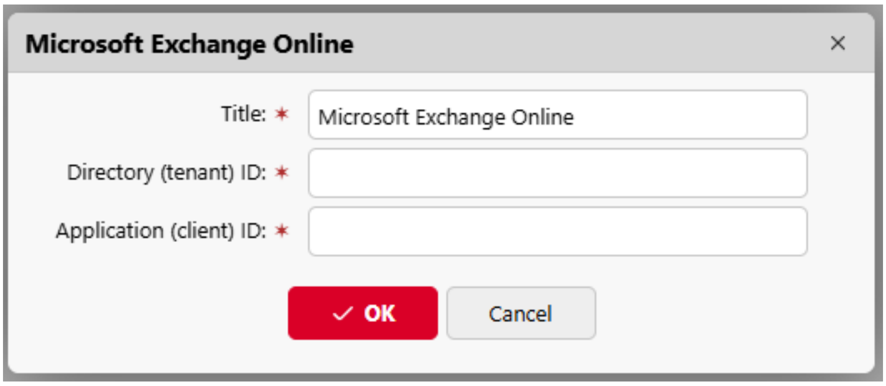
The application uses delegated permissions and is authorized by the Microsoft account of the mailbox that MyQ will use.

No client secret is required.

Permission	**API**	**Type**	**Purpose**
`User.Read`	Microsoft Graph	Delegated	Sign in and read the mailbox user's profile.
`IMAP.AccessAsUser.All`	Microsoft Graph	Delegated	Read, update, create, and delete email in the user's mailbox. This permission does not include sending mail.
`SMTP.Send`	Microsoft Graph	Delegated	Send email from the user's mailbox.

Create the Exchange Online connection

Go to **MyQ > Settings > Connections**, click **Add**, and select **Microsoft Exchange Online**.



Enter:

- **Title** – a name for the connection.
- **Directory (tenant) ID** – the tenant ID of the Microsoft Entra application.
- **Application (client) ID** – the client ID of the Microsoft Entra application.

Save the connection. Next, authorize the mailbox user.

Authorize the mailbox user

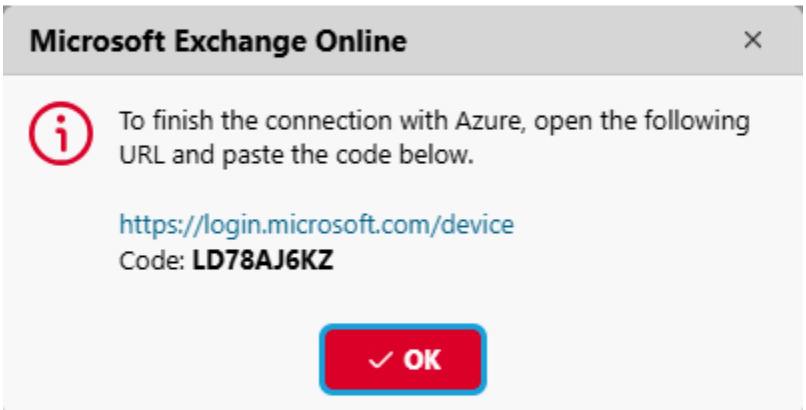
After the connection is created, MyQ displays a Microsoft device authorization code and a link to the Microsoft sign-in page. Open the link and enter the displayed code.

Sign in with the **Microsoft account that owns the mailbox MyQ will use**.

For example, if MyQ will send email from `print@example.com`, authorize the connection by signing in as `print@example.com`.

After successful authorization, Microsoft Exchange Online is connected to MyQ.

> ⚠ The connection cannot be used until this authorization is completed. The authorization code is valid for a limited time.



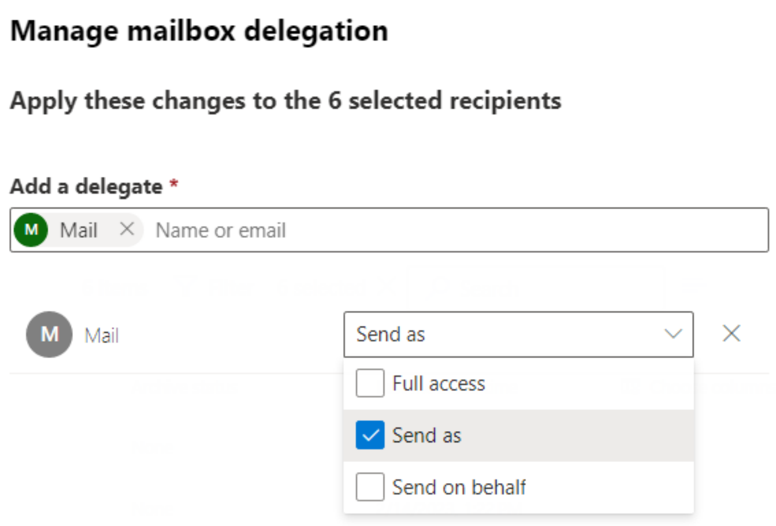
Microsoft Exchange Online is now connected to MyQ and is ready to be used in the **Network** settings tab as an Outgoing SMTP server.

Send scan as the logged-in user

If you have configured **MyQ > Settings > Scanning & OCR - Default settings of an email with scan - Sender**, the mailbox authenticated in MyQ has to have a *Send As* permission for all users.

If you select to send emails as the default sender, this change is not required.

1. Log in to Exchange admin center[22].
2. Go to Mailboxes, select all users.
3. Click on **Mailbox delegation**.
4. Select the mailbox that was authenticated in MyQ when the MS Exchange Online connector was created (visible in **MyQ > Settings > Connections**).
5. Choose **Send as** permission.



6. Click Save.

Your selected mailbox for outgoing emails has now been assigned the rights to send scanned documents on behalf of the user who scanned them.

22. https://admin.exchange.microsoft.com/

9.18.7 Authentication Servers Settings

MyQ can integrate with your domain directory to synchronize users and groups, and enable authentication. This ensures that your current users and groups can interact with MyQ embedded terminals, web interface, and clients with their domain identity.

The following authentication methods are supported:

- LDAP Server
  - Active Directory
  - Google Workspace
  - OpenLDAP
  - Novell
- Microsoft Entra ID
- Radius Server

In **MyQ > Settings > Authentication Servers** you can configure the following:

- Synchronize users from and/or have them authenticate towards an LDAP server, such as a 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.
- Synchronize and authenticate users and groups from Google Workspace with Secure LDAP.

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.

Notes

- 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 (10.3) User Authentication.
- On embedded terminals using the username + password login screen, and when printing via AirPrint, users linked to an external authentication server can authenticate with either their external account password or their MyQ PIN. MyQ checks the entered value locally first: if it matches the user's PIN, authentication succeeds without contacting the external server. If it does not match a PIN, it is forwarded to the external server as a password.

- Users linked to an LDAP, Microsoft Entra ID, or Radius authentication server cannot sign in on the MyQ Web User Interface with a PIN. They must use their external account password (or Sign in with Microsoft for Entra ID accounts) on the Web UI.

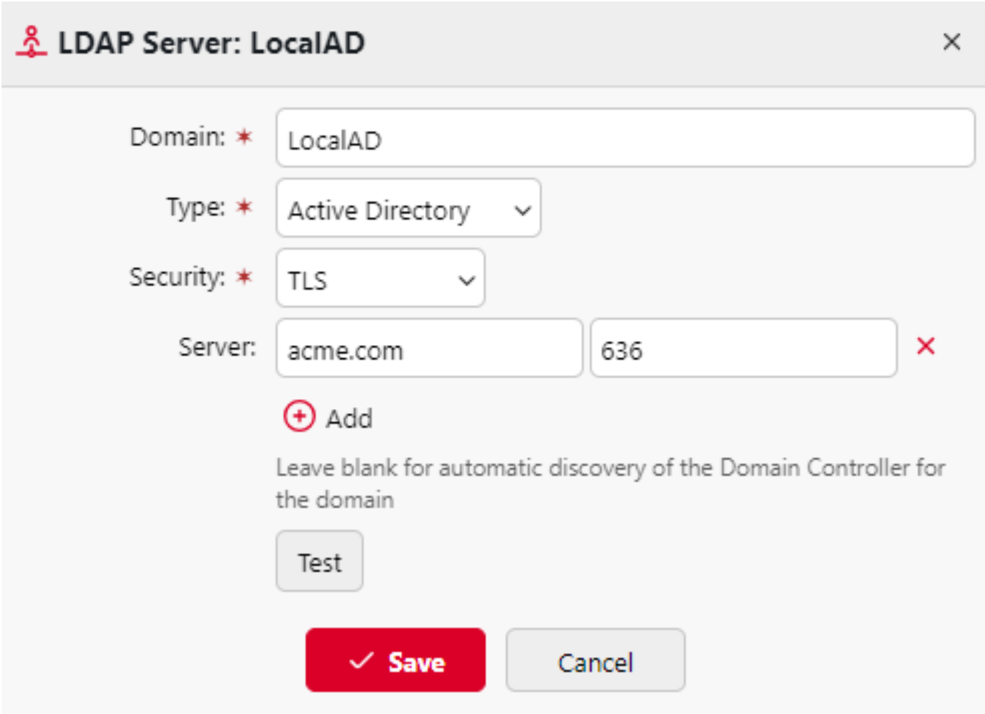
Add an LDAP Server

1. Go to **MyQ > Settings > Authentication Servers**, click **+Add**, and select **LDAP Server**.

   The LDAP server properties panel opens.

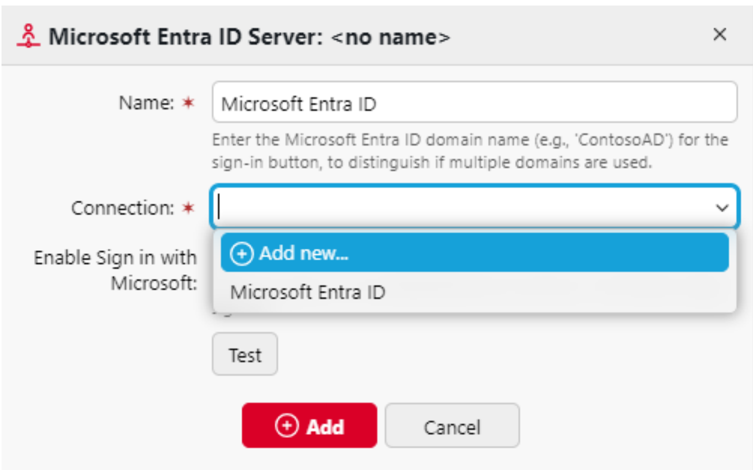
2. Enter the **LDAP domain** in LDAP format (for example, `dc=example,dc=com`).
3. Under **Type**, select the appropriate LDAP server:
   - **Active Directory**, or
   - another supported option such as **Novell**, **OpenLDAP**, or **Google Workspace**.
4. Configure the **security settings**:
   - Select the security protocol for the LDAP connection.
   - For **Active Directory**, you must select **TLS**.
5. Configure the **server connection**:
   - Enter the **server hostname** and **port**.
   - For **Active Directory with TLS**, use port **636**.
   - If the hostname or IP address is unknown, you can leave it empty to allow automatic server discovery.
   - To define multiple addresses for the same LDAP server, click **Add**.
6. *(Google Workspace only)*

   When **Google Workspace** is selected:
   - Default values for **Security**, **Server**, and **Port** are filled in automatically.
   - In the **Certificate** section, click **Add** and upload the certificate file (`.crt`) and private key file (`.key`) obtained from the Google Admin console.
7. Click **Save** to add the LDAP server.
8. *(Optional)* Click **Test** to verify the connection, and enter the LDAP client username and password when prompted.



Add Microsoft Entra ID Server

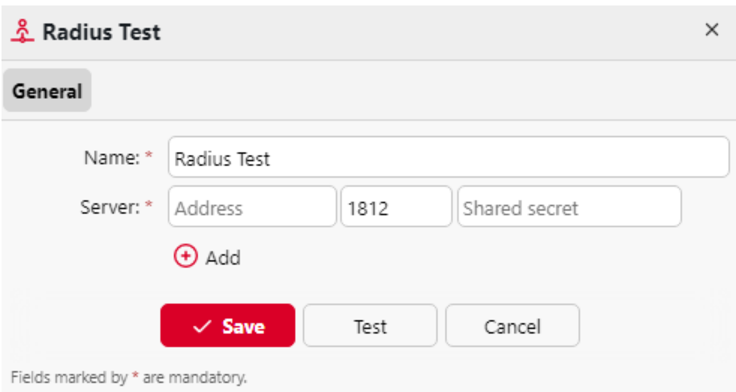
1. Click **+Add** and select **Microsoft Entra ID Server**. The new Microsoft Entra ID server properties panel opens on the right side of the screen.
2. If you have already added Microsoft Entra ID in the **Connections** settings, the server appears on the list. If not, click **Add new**. See Connect to Microsoft Entra ID (Graph API) (see page 151).



3. Check the **Enable Sign in with Microsoft** checkbox if you want to allow users the login method Sign in with Microsoft.
4. Click **Save**. The Microsoft Entra ID Server now appears on the list of servers.

Add a 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.



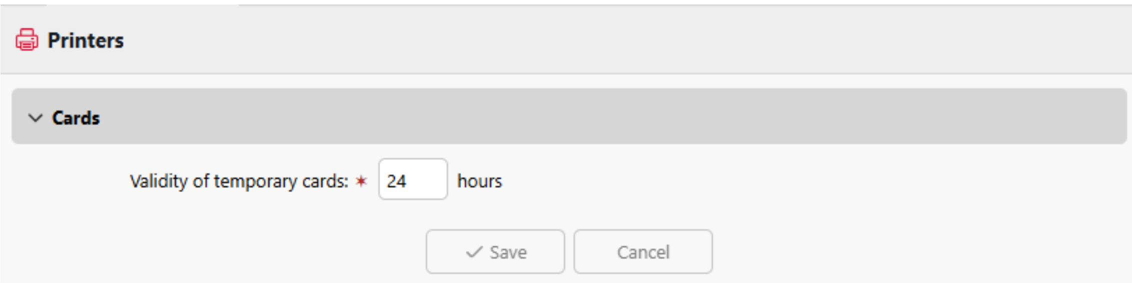
When an authentication server is renamed, a server with the old name will still appear in the Authentication server settings of a user profile, alongside the server with the new name. The old server is removed after the following user synchronization propagates changes.

See also:

- Authenticate Users from LDAP or RADIUS (see page 245)
- (10.3) Configure Microsoft Entra ID Authentication

9.19 Printers Settings

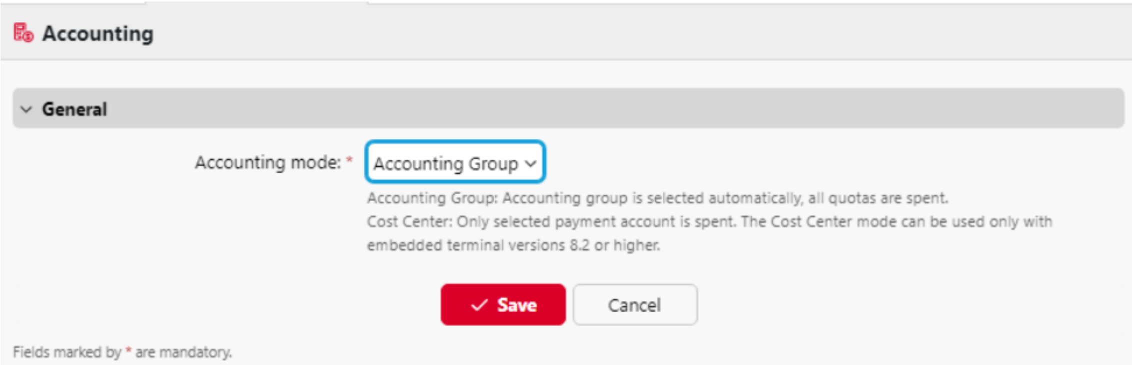
On the **Printers** settings tab, in the **Validity of temporary cards** field, you can set the duration of the temporary cards validity in hours. The default value is *24* hours.



9.20 Accounting Settings

In the **Accounting** settings tab, in the **General** section, the MyQ administrator can set 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.



Limitations:

- **Cost Center** mode does not work on printers without a terminal.
- **Cost Center mode can be used only with embedded terminal versions 8.2 or higher.**
- In **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.

> ⚠ 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. If you choose to switch, your terminals need to be re-activated. This can be done automatically by clicking **OK** in the Apply Settings pop-up, or manually on each device.

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

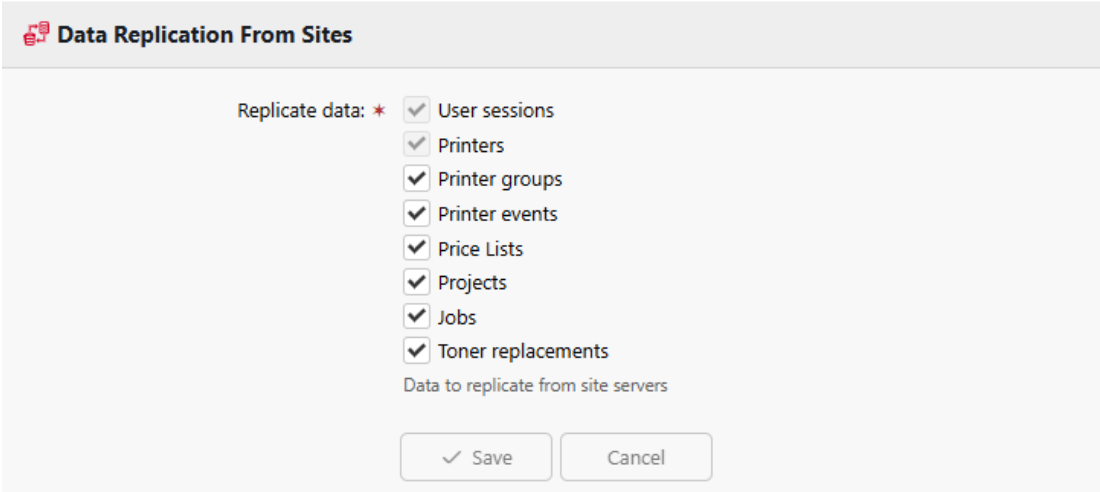
Accounting group	Cost center
If multiple quotas are assigned to a user, all of them are spent.	Only one quota is spent. If credit, or a cost center without quota is selected, no quota is used.
If credit or personal quota is selected, the job is still accounted to the accounting group	If credit or personal 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.

9.21 Data Replication Settings

The administrators of the Central Server can select what data is to be replicated from Sites in **MyQ > Settings > Data replication from sites**.

Select 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



9.21.1 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.

9.21.2 Scheduling Replication

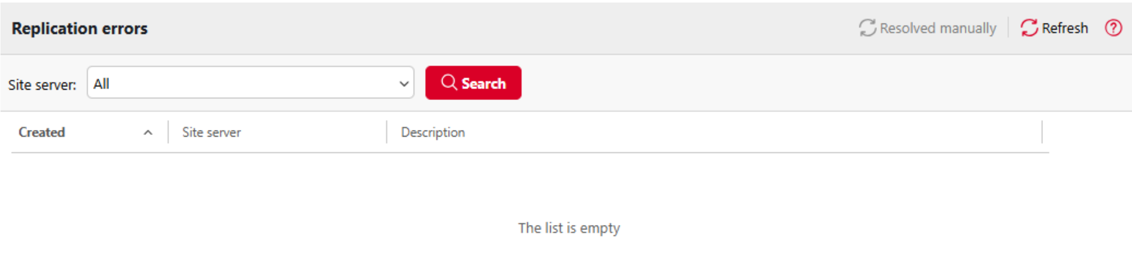
This data is then downloaded to the Central Server during a scheduled task which period can also be adjusted on the Central Server in **Settings** – **Task Scheduler**, task **Data replication from sites**.

9.21.3 Resolving Replication Errors

The Replication Errors health check identifies any non-replicable objects in replications older than 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 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.

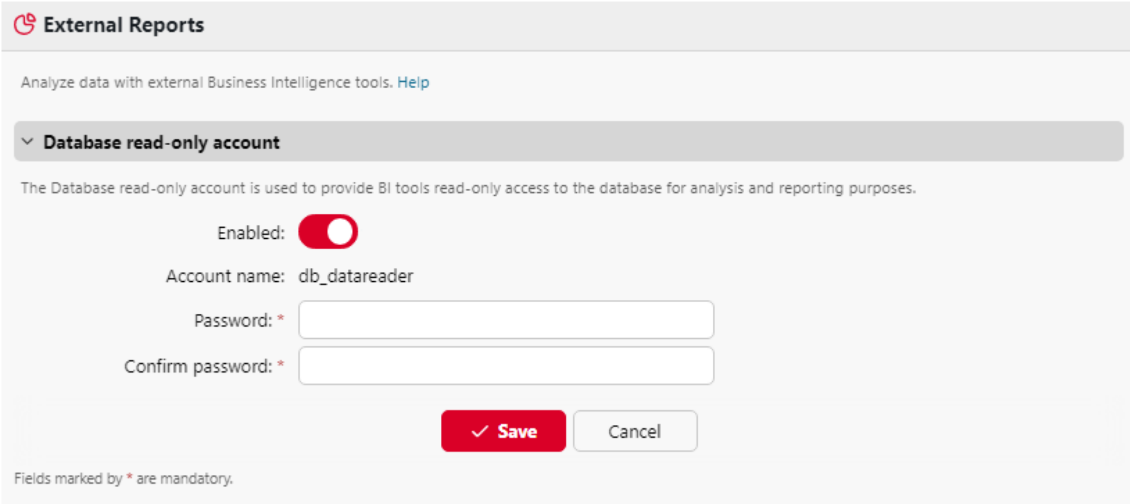
See also:

- Site Server Data Replication (see page 129)
- Task Scheduler Settings (see page 141)

9.22 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:

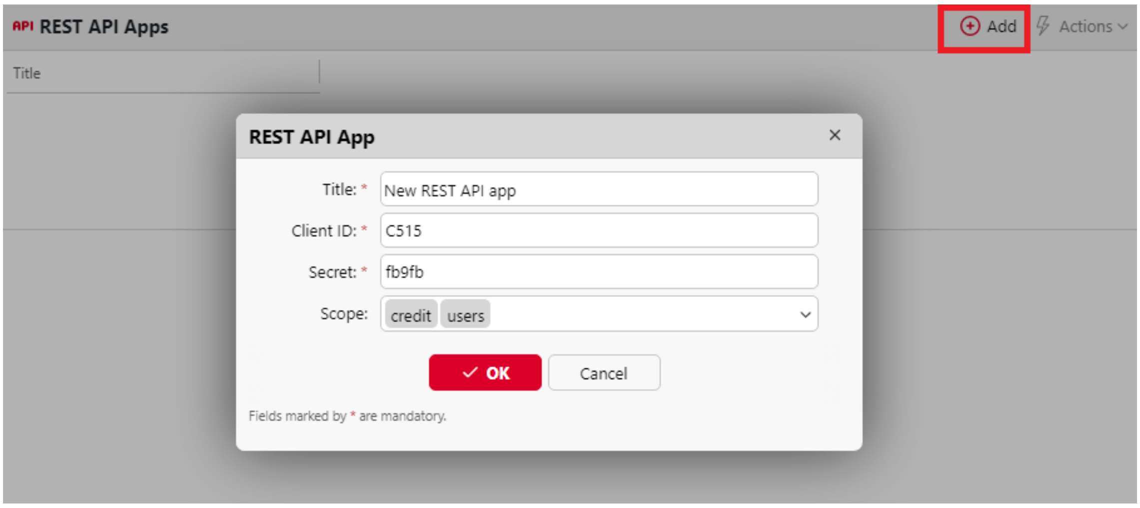
- **Account name**: *db_datareader*. This is the newly created read-only database user. The account name cannot be changed.
- **Password**: password for the *db_datareader* account, set by the administrator. A new password must be set every time when switching from the **Disabled** to **Enabled** state.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

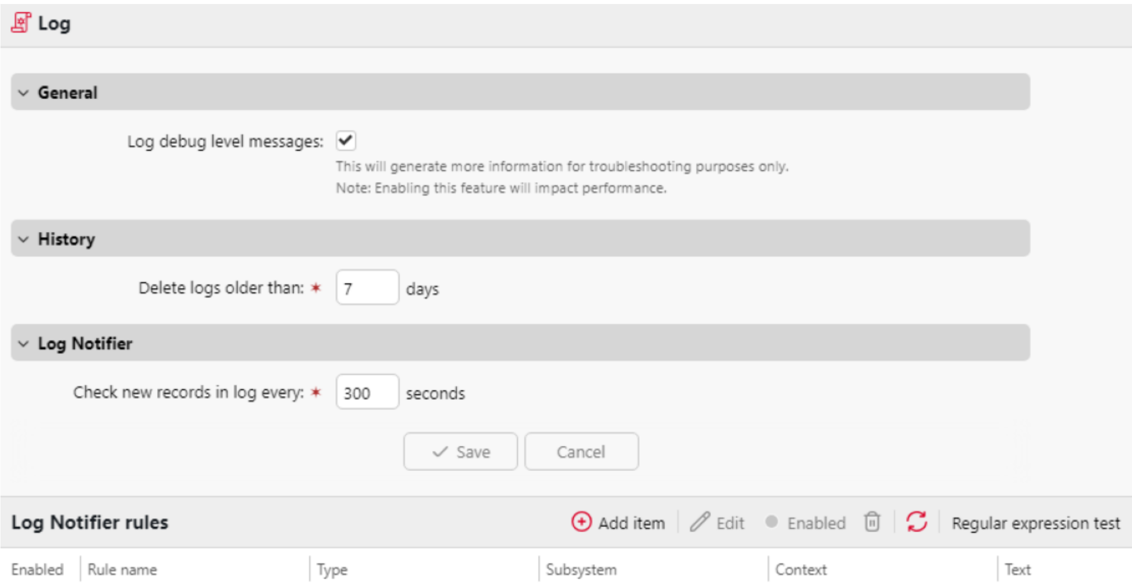
9.23 REST API Apps

In the **REST API Apps** settings tab you can add applications to MyQ by clicking **+Add** and filling in the **Title** and **Scope**. The **Client ID** and **Secret** fields should be used for the application's configuration.



9.24 Log Settings

On this 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. The notifications can be sent via email or they can be sent to Windows Event Viewer.



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 to enable it only in case of a system malfunction or if it is requested by MyQ support.

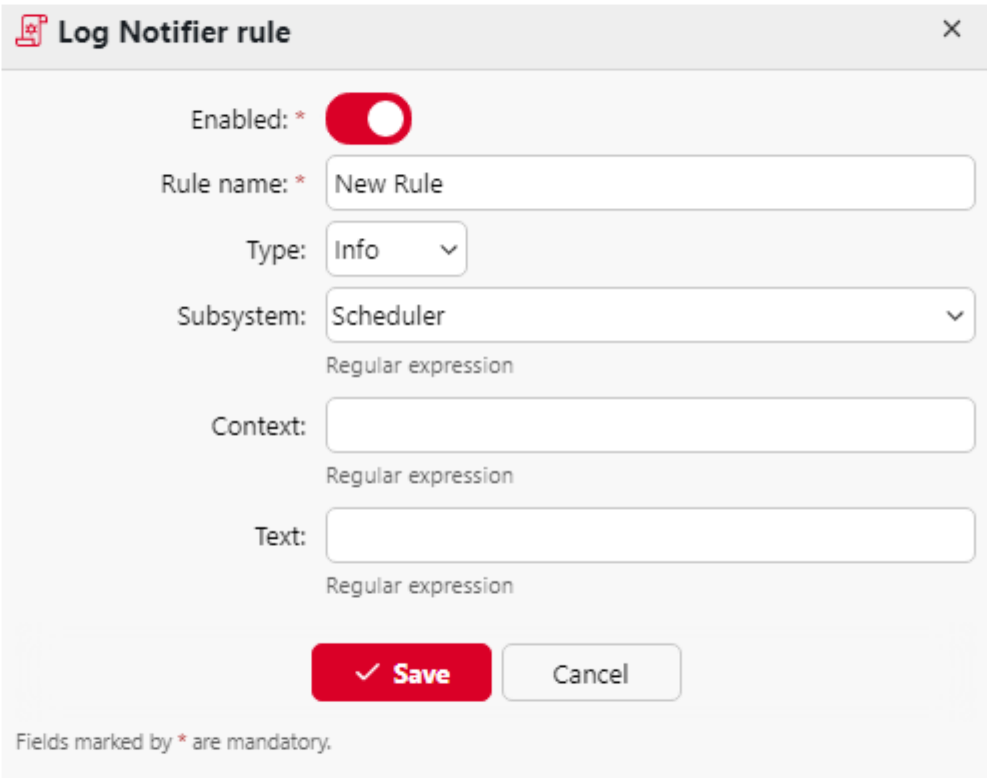
History – Here you can set when the logs should be deleted (in days).

Log Notifier – The notifications and their destinations are both specified by log notifier rules.

Under **Log Notifier**, 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).

9.24.1 Management of the Log Notifier Rules

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



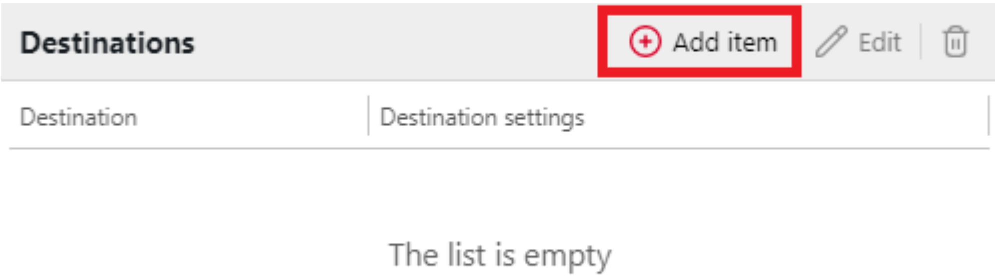
To open the editing options of a rule, double-click the rule (or right-click the rule, and then click **Edit** on the shortcut menu). The following settings can be changed:

- **Enabled**: activate, deactivate the rule.

- **Rule name**: name of the rule.
- **Type**: the available event types are: *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 rule, click **Save**. The rule is saved and you can select its destinations.

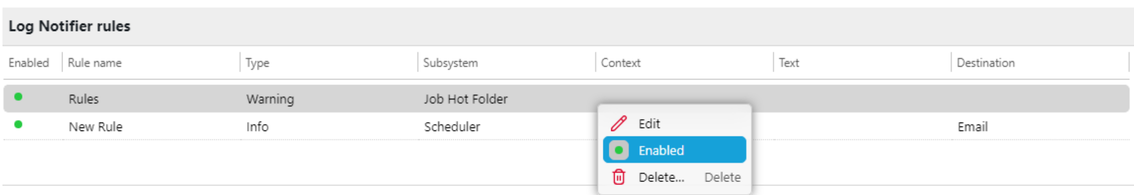
To add the destination, click **+Add item** under **Destinations**.



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.

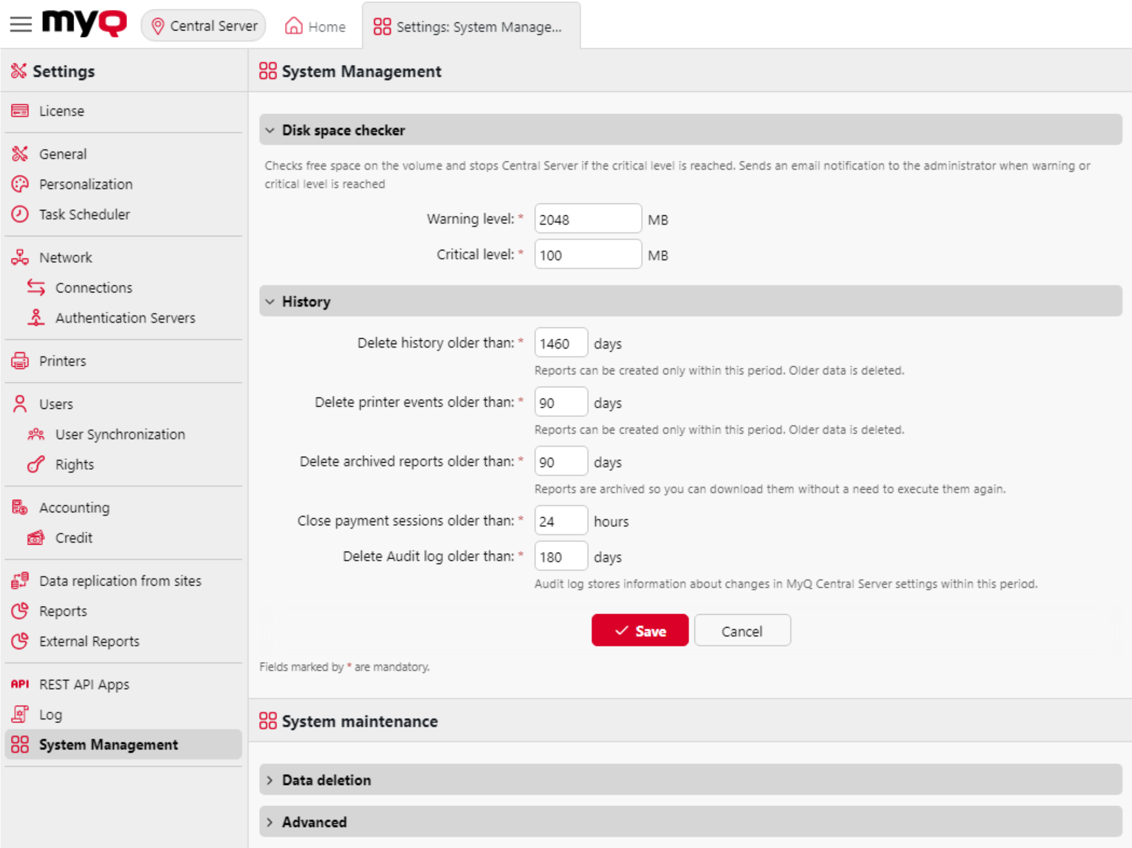
To enable/disable Log Notifier rules:

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



9.25 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.



9.25.1 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.

9.25.2 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.

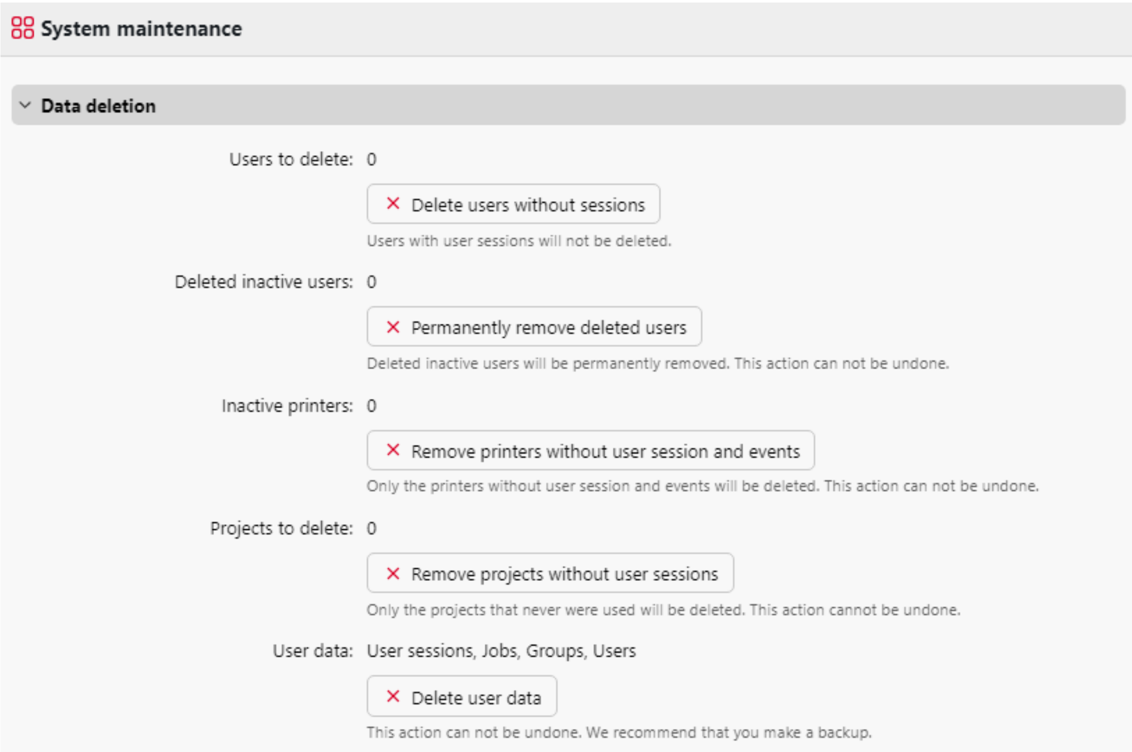
To change the values, enter new values to the particular text box, and then click **Save**.

9.25.3 System Maintenance

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

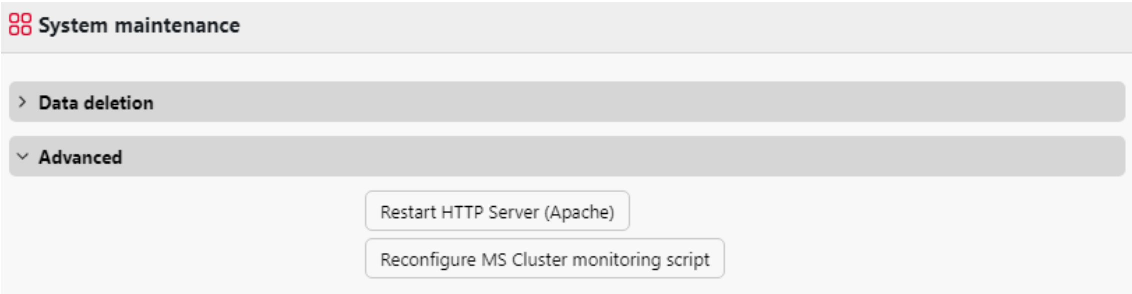
Data Deletion section

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.



- **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.

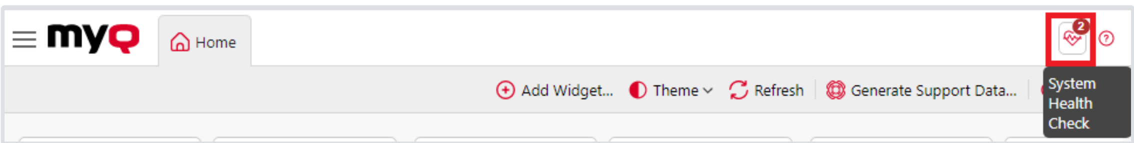
9.25.4 System Health Check

MyQ performs registered checks which can return error messages and their level of severity, these can be viewed in System Health Check. The errors concern database health, disk space availability, PIN length settings, time zone configuration, etc.

Every error message is logged in the MyQ main log.

When the error message has a **Critical** severity, the related MyQ service is stopped, and the administrator gets an email notification about it.

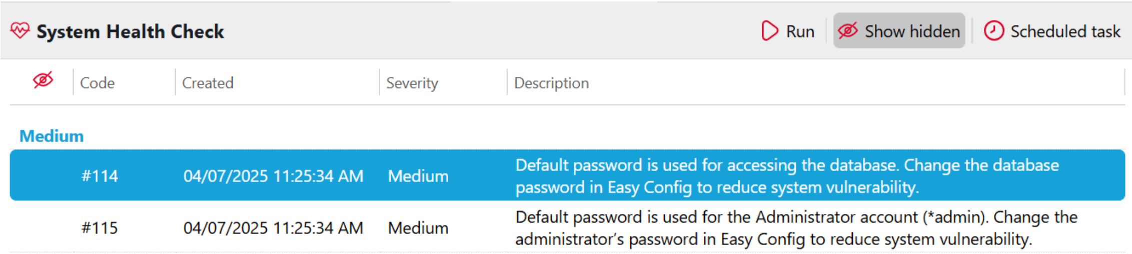
To access the system health check overview, log in as admin to MyQ and go to **MyQ > System Health Check** or click on the system health check button on the top-right side of the window.



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.



Error Codes

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.

Error codes and their severity 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

9.25.5 MyQ Server Processes and Services

MyQ Print Server runs several services and supporting processes. During troubleshooting, you may need to identify these processes in Windows Services, Task Manager, logs, firewall rules, or performance monitoring tools.

Main Components and Services

Print Server

Handles core MyQ server logic, print job reception, job processing coordination, notifications, and communication with other MyQ components.

HTTP Router

Acts as the reverse proxy for incoming HTTP and HTTPS traffic and handles TLS termination.

HTTP Server

Hosts the MyQ Web Interface and REST API.

Database Server

Stores MyQ system data.

Job Processor

Processes and parses print jobs. It runs separately from the main Print Server process to reduce the impact of job-processing failures.

Terminal Packages

Provide vendor-specific embedded terminal functionality and communication with supported devices.

PM Server

Provides Kyocera-specific device configuration and embedded terminal installation functionality.

Data folder

MyQ stores application data, databases, logs, jobs, and other runtime data in the MyQ data folder. The default location is:

`C:\ProgramData\MyQ`

In production environments, storage location, capacity, performance, backup, and access permissions should be planned carefully.

Executable Names

Friendly name	Executable name	Alternative name
HTTP Router	traefik.exe	Traefik
HTTP Server	httpd.exe	Apache
Database Server	firebird.exe	Firebird
Print Server	myq.exe	
Kyocera Provider	knum.server.exe	PM Server
Terminal Package	MyQ*Terminal.exe	Vendor terminal package
Job Processor	MyQJobProcessor.exe	

9.25.6 Windows Server Performance Monitor

If you experience issues such as high CPU utilization, slow disk or network, or out-of-memory errors, the Windows Server application Performance Monitor can help you gather useful system information.

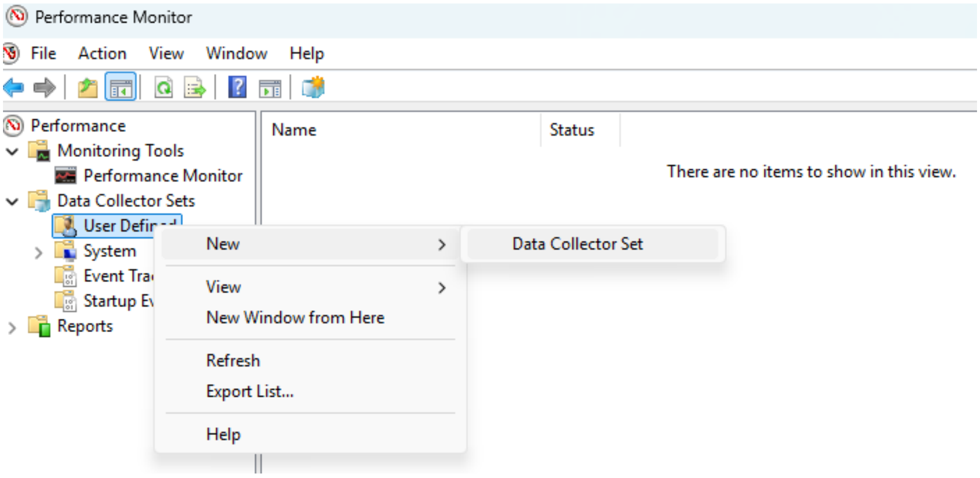
Performance Monitor is a Microsoft Management Console (MMC) snap-in that you can use to obtain system performance information. You can use this tool to:

- Analyze the performance effects that applications and services have on a computer.
- Obtain an overview of system performance.
- Collect detailed information for troubleshooting.

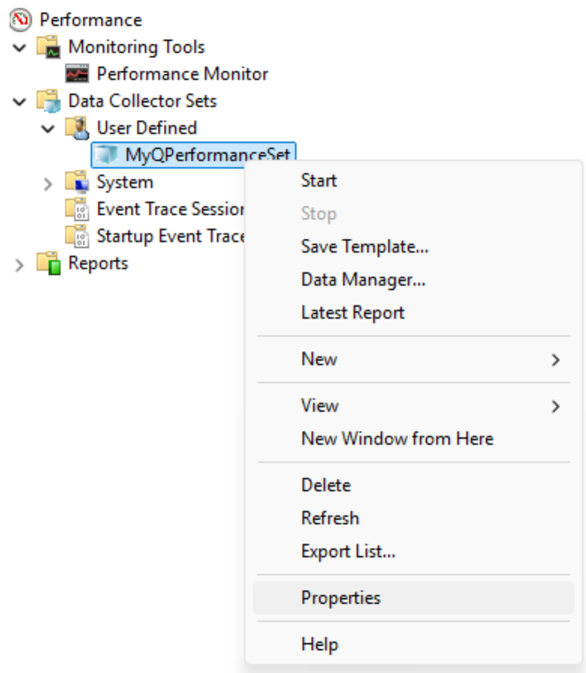
Sharing Performance Monitor reports with MyQ Support can help us resolve your issue faster.
We strongly recommend to use the **System Diagnostics** data collector template**.** This template selects objects and counters that report the status of hardware resources, system response times, and processes on the local computer, along with system information and configuration data.

Run **System Diagnostics Using the Template Data Collector**:

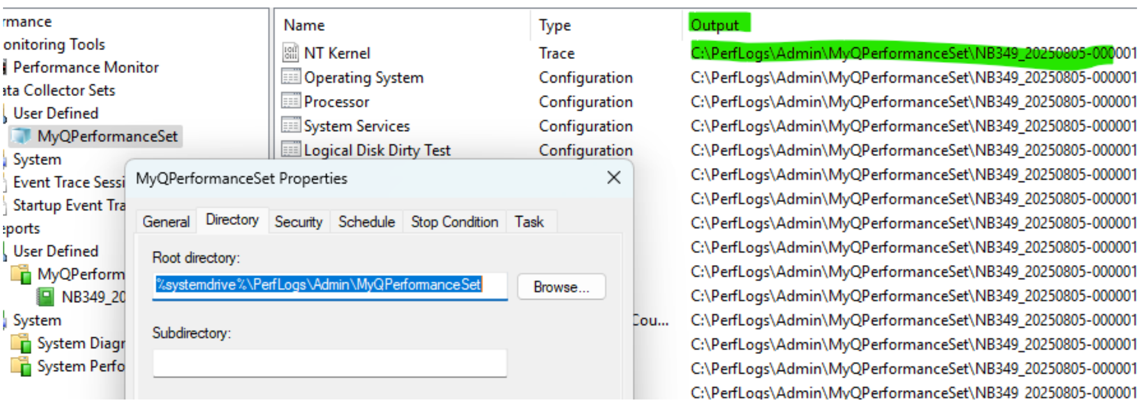
1. Log in as an administrator to the Windows Server where your MyQ server runs.
2. On the Windows taskbar, select **Start > Run**.
3. In the **Run** dialog box, type `perfmon`, and then click **OK**.
4. In **Performance Monitor**:
    a. In the panel on the left, expand **Data Collector Sets**.
    b. Right-click **User-Defined** and select **New > Data Collector Set**.



    c. In the first **Create new Data Collector Set** wizard dialog box:
        i. In the **Name** field type any descriptive name.
        ii. Select **Create from a template (Recommended)**.
        iii. Click **Next**.
    d. In the second **Create new Data Collector Set** wizard dialog box:
        i. Select **System Diagnostics**.
        ii. Click **Finish**.
5. (Recommended) Change the properties of this user-defined data set. In particular, consider adjusting the **Schedule** and **Stop Condition,** to control the capture period and duration. Right-click the name, select **Properties**, and adjust as needed.
6. To start gathering performance information go to your data set, right-click the name and click **Start**.



7. To stop gathering performance information, go to your data set again, right-click the name, and click **Stop**.
8. To review the logged performance information, open Windows Explorer and locate and double-click the .blg file indicated in the Output column in the Performance Monitor.



Performance Monitor opens showing the collected data.

Gather all of the Output files (`.blg, .xml, .etl, .log, .xsl, .xml, .html`) and send them to the *MyQ Support*.

> We recommend to create a ZIP file from the directory where these files are located.

Monitor VMs Running Windows Server

Server virtualization is widely used practice, and many organizations have migrated some or all their server workloads to virtual machines (VMs) that are running virtualization servers.

From a monitoring perspective, it's important to remember that servers running as guest VMs consume resources in the same way as physical host–server computers.

In addition to monitoring guest VMs, always remember that you must monitor the host that runs them.

For more information about performance monitoring and tuning, see:

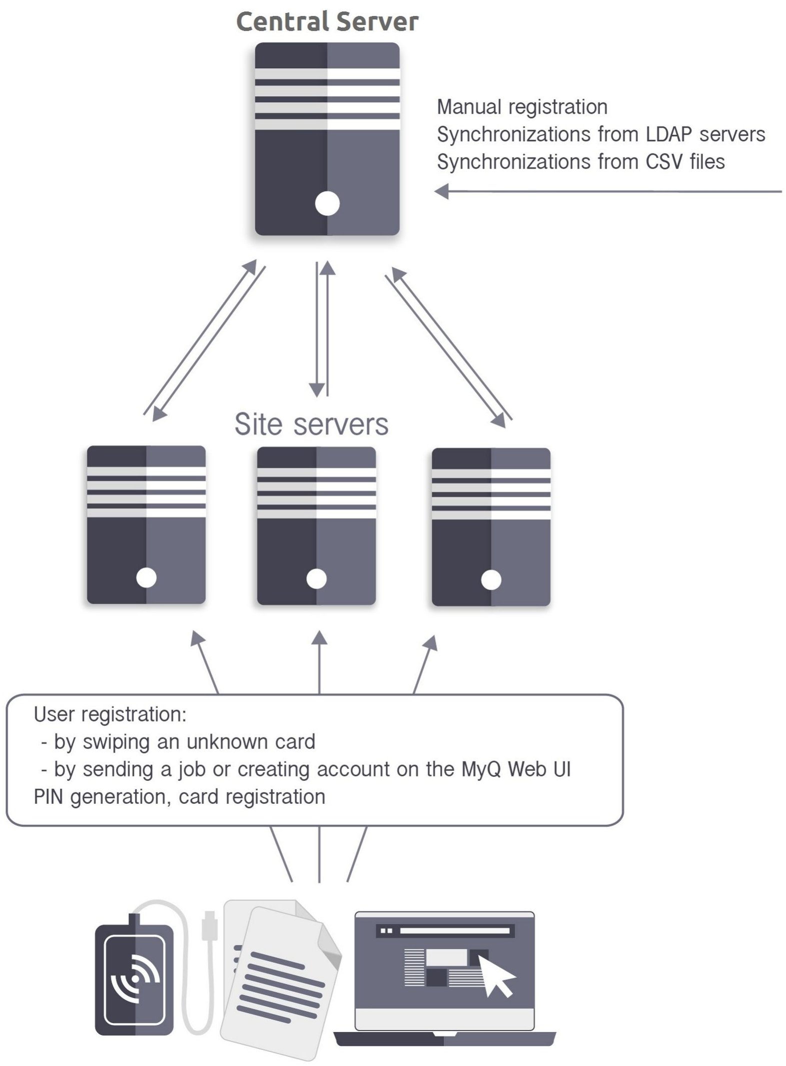
- Server Hardware Performance Considerations[23]
- Monitor Windows Server performance[24]

23. https://learn.microsoft.com/en-us/windows-server/administration/performance-tuning/hardware/
24. https://learn.microsoft.com/en-us/training/modules/monitor-windows-server-performance/

10 Users

This section describes how to set up and manage user accounts in MyQ. It covers adding, importing, synchronizing, and deleting users, user authentication, managing user and group settings, and more.

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.

See also:

- Users Settings (see page 192)
- User Synchronization (see page 199)
- (10.3) Automatic User Registration
- (10.3) User Authentication
- Data Privacy and Anonymization (see page 251)

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

10.1 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. ***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.
5. ***system** - All the actions performed by the MyQ system are charged to the ***system** user.

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, set other data of the user account as required, and then click **Save**.

See also: Editing User Accounts (see page 183)

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 restored.

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.

Restoring users

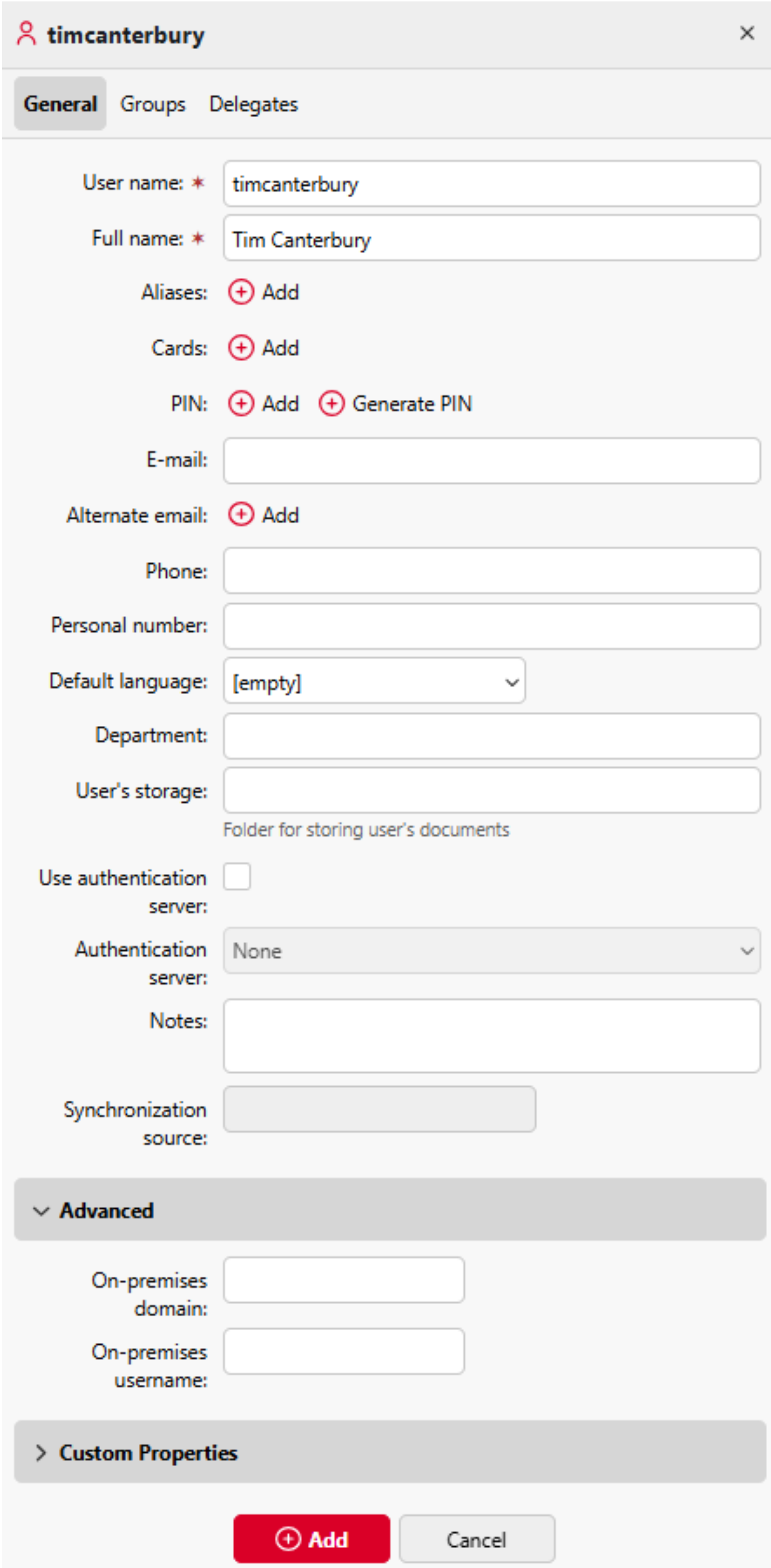
To restore a user:

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 restore, and then click **Actions**. The **Actions** drop-down box appears.
3. Click **Restore**.

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**.


timcanterbury
General
Groups
Delegates
User name: *
timcanterbury
Full name: *
Tim Canterbury
Aliases:
Add
Cards:
Add
PIN:
Add
Generate PIN
E-mail:
Alternate email:
Add
Phone:
Personal number:
Default language:
[empty]
Department:
User's storage:
Folder for storing user's documents
Use authentication server:
Authentication server:
None
Notes:
Synchronization source:
Advanced
On-premises domain:
On-premises username:
Custom Properties
Add
Cancel

10.3.1 General User Properties

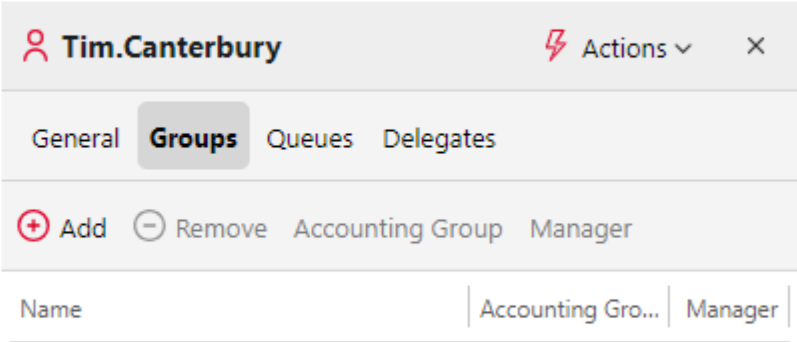
Property	Description
User name	Unique identifier used to identify and authenticate the user. Must be unique across all accounts in the installation. MyQ compares this value against the identifier extracted from incoming print jobs to match jobs to users.
Full name	Display name shown in the MyQ Web Interface, on terminal screens, and in reports. Typically first name and surname. In Active directory and Open LDAP, this property corresponds to the `cn` user attribute on the LDAP server.
Aliases	Alternative usernames that allow the same user to log in or send jobs using different identifiers – for example, a UPN alongside a `sAMAccountName`, or an email address. An unlimited number of aliases can be added. MyQ matches incoming jobs against both the username and all aliases.
Cards	ID card number used for login at embedded terminals. Can be set manually, imported during synchronization, or registered by the user at the terminal. Multiple cards can be assigned to one account.
PIN	Personal identification number for access to the MyQ Web Interface and terminals. Multiple PINs can be assigned. PINs can be Persistent (never expire) or Temporary (expire after a defined period). Automatically generated PINs are recommended for security.
Email	Primary email address. Used for PIN delivery, scan-to-email, and system notifications.
Alternate emails	Additional email addresses that can be used as scan destinations.
Phone	Contact phone number. Informational only – not used by MyQ for any automated function.

Property	Description
Personal number	Optional secondary identifier. Can be used in place of the username when pairing users across synchronization sources, or as a stable identifier during username changes.
Default language	Language used for the user's Web Interface and terminal screen.
Department	Optional organizational field. Can be populated manually or via synchronization. Used in reports and for grouping.
User's storage	Default destination for scanned documents – a folder path, email address, or other configured target. Used by Easy Scan and Easy Print terminal actions.
Use authentication server	When enabled, the user's credentials are validated against an external directory service (LDAP or RADIUS) rather than the MyQ database.
Authentication server	The external server used for credential validation when Use authentication server is enabled.
Notes	Internal free-text field for administrator notes about the account. Not visible to the user.
Synchronization source	Identifies which synchronization source imported this account. Used by MyQ to determine which source is responsible for updating the account on subsequent syncs.
Advanced	Displays the synchronized on-premises domain and username for hybrid Entra ID users. Both values can be edited manually but are overwritten on the next Entra ID synchronization.
Custom (1–3)	Three additional fields available for mapping any other attributes from a synchronization source that do not correspond to a standard MyQ property.

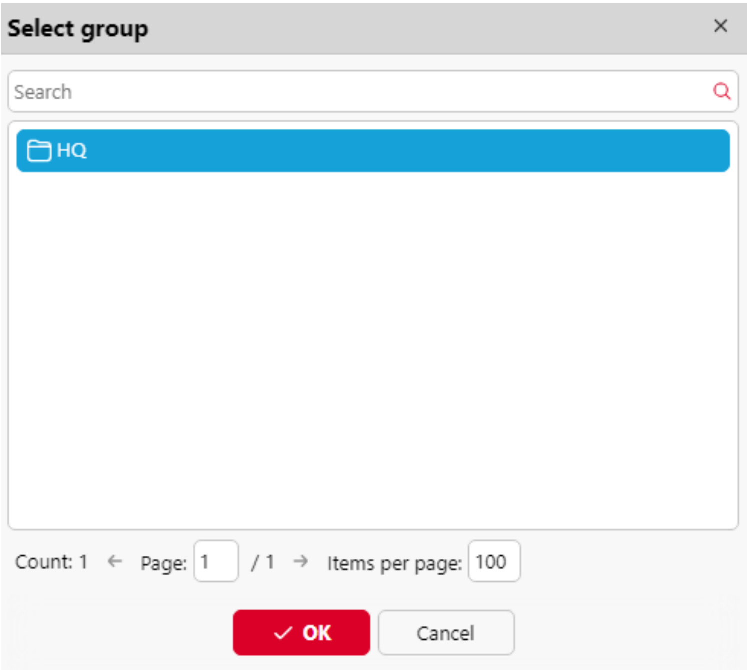
10.3.2 Adding Users to and Deleting Users from Groups

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** 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. If this group contains subgroups, the user inherits the Manager role also for all these subgroups. 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 box.

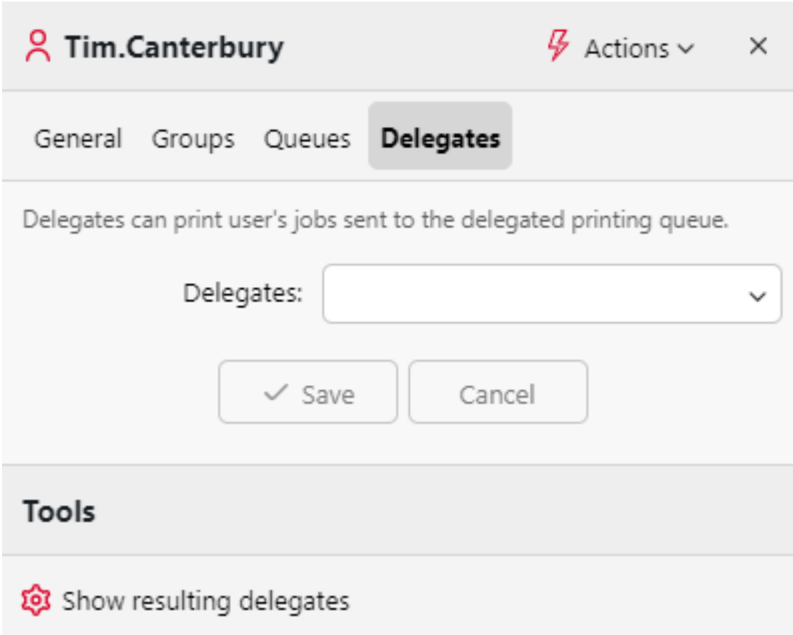
10.3.3 Selecting User Delegates

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.

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).

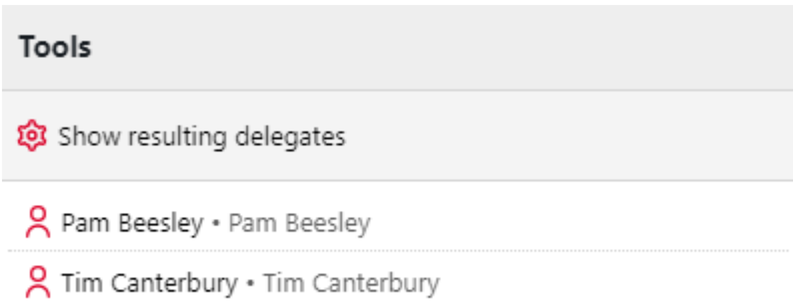


Deselect delegates

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).

Show resulting delegates

You can use the **Show resulting delegates** tool to show you each delegate for a specified user. This is helpful if you have added one or more user groups as delegates for a user, and will show each user who is now a delegate as a result of adding their user group.



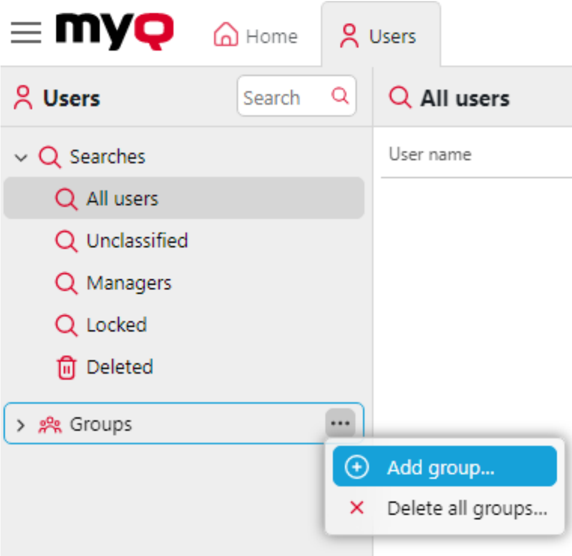
10.4 User Groups

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

10.4.1 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 **+Add Group**. The new group properties panel opens on the right side of the screen.



3. Enter a name for the new group.
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).

10.4.2 Deleting User Groups

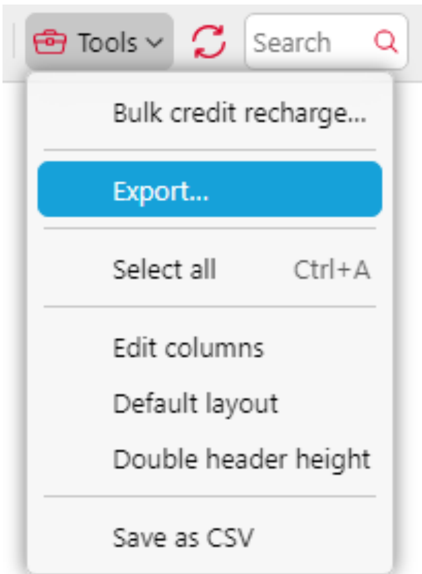
1. On the group tab on the left side of the **Users** main tab, right-click the group that you want to delete.
2. Click **Delete**.

10.5 Exporting Users

In case you need to export the list of MyQ users 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 the list of users:

1. Click **Tools** on the toolbar at the top of the **Users** main tab.
2. Click **Export** in the **Tools** drop-down. The Users Export dialog box appears.
3. In the dialog box, select the group you want to export and click **OK**. The file is downloaded to your default *Downloads* folder.

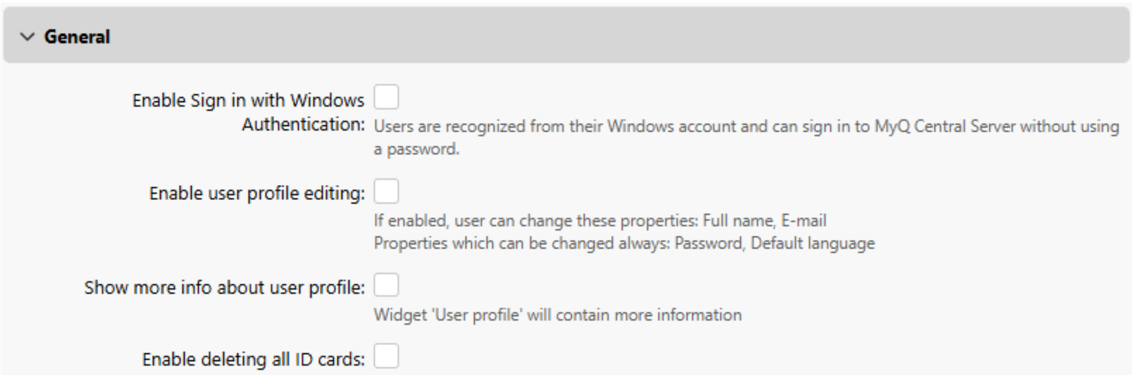


You can also export all the users by selecting **Save as CSV** in **Tools**.

10.6 Users Settings

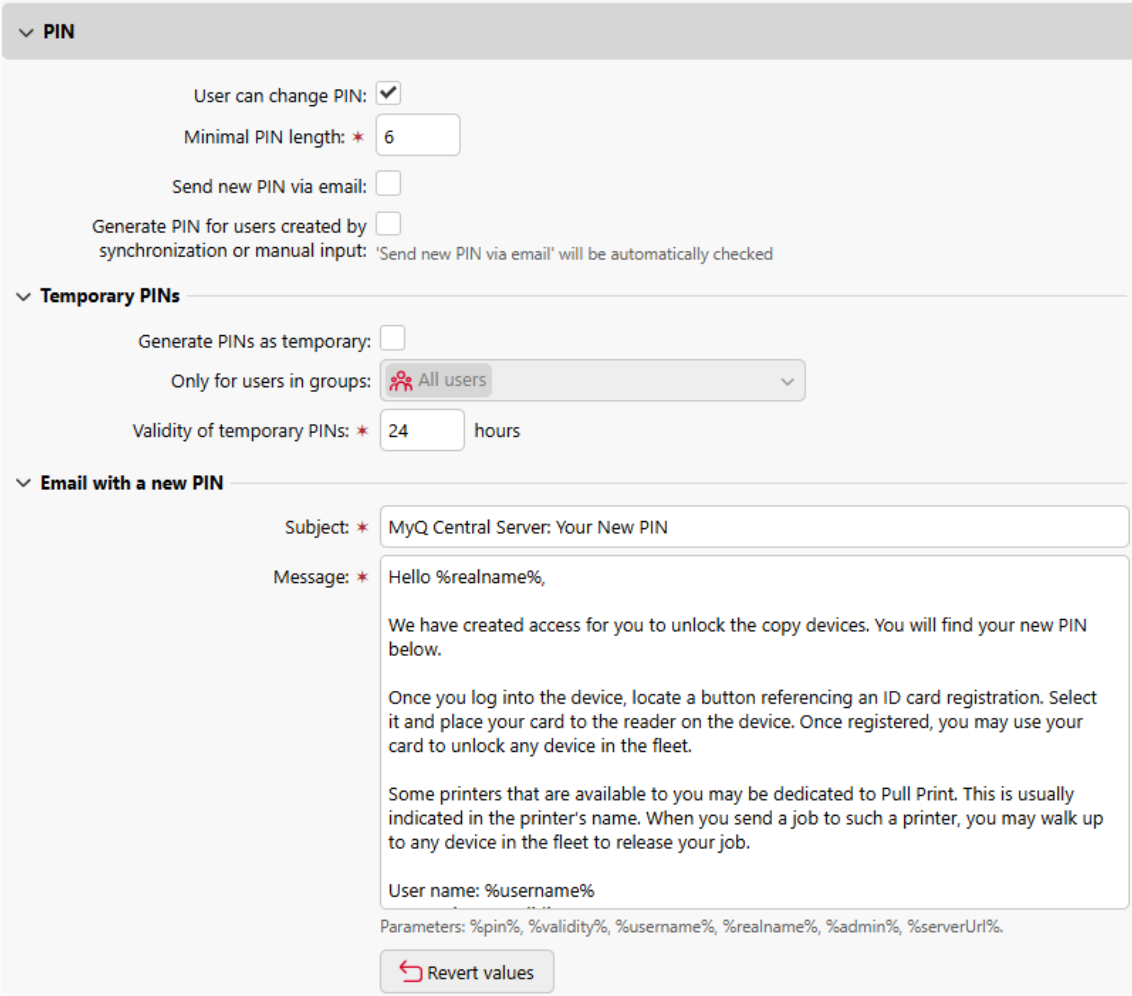
In the **Users** settings tab (**MyQ > Settings > Users**), you manage MyQ users' **General settings, PIN** and **Password complexity** requirements**, Web Interface Session Timeout** settings, and **Account lockout** settings.

10.6.1 **General Settings**



- **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.
- **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.

10.6.2 PIN



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.

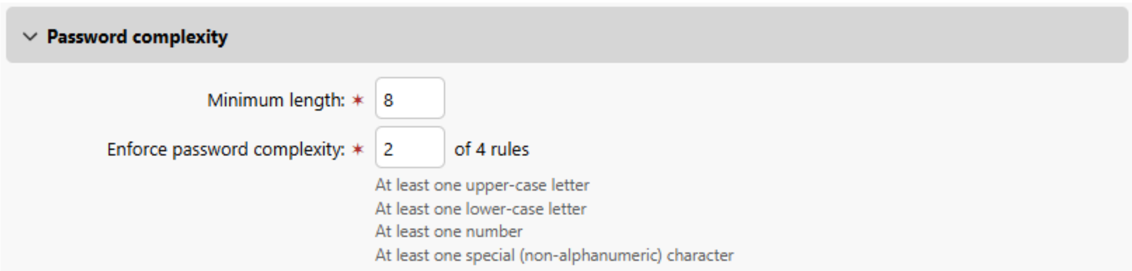
There are also email templates you can use for informing the users about their new PIN (**Email with a new PIN**) or for providing them with a reset code in case of a lost/ forgotten PIN (**Email with the PIN reset code**). The template is editable and the values can be reset to their defaults if needed, by clicking **Revert values**.

Temporary PIN

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).

> ⚠ 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.

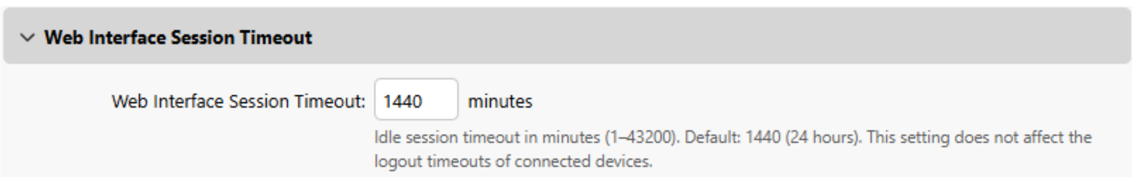
10.6.3 Password complexity



Manage password complexity requirements for MyQ user accounts.

- **Minimum length** – set the minimum character length for passwords
  - **Range**: 1 – 100
  - **Default**: 8
- **Enforce password complexity** – set how many of the password complexity rules (**default**: 2) you want to enforce:
  - At least one upper-case letter
  - At least one lower-case letter
  - At least one number
  - At least one special (non-alphanumeric) character

10.6.4 Web Interface Session Timeout

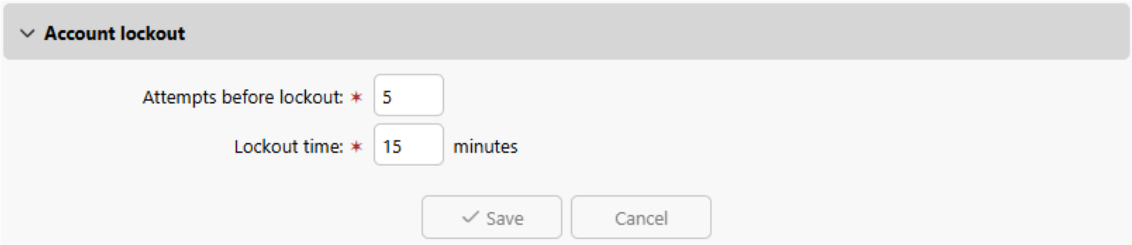


Set the idle timeout duration for web sessions, in minutes. If a user session is inactive for longer than the configured period, the session expires and the user must log in again. Changes take effect immediately for new requests without requiring a server restart.

- **Range:** 1 to 43,200 minutes (up to 30 days)

- **Default:** 1,440 minutes (24 hours)

10.6.5 Account lockout



Configure the maximum failed login attempts before a user is locked out, and the duration of the lockout time.

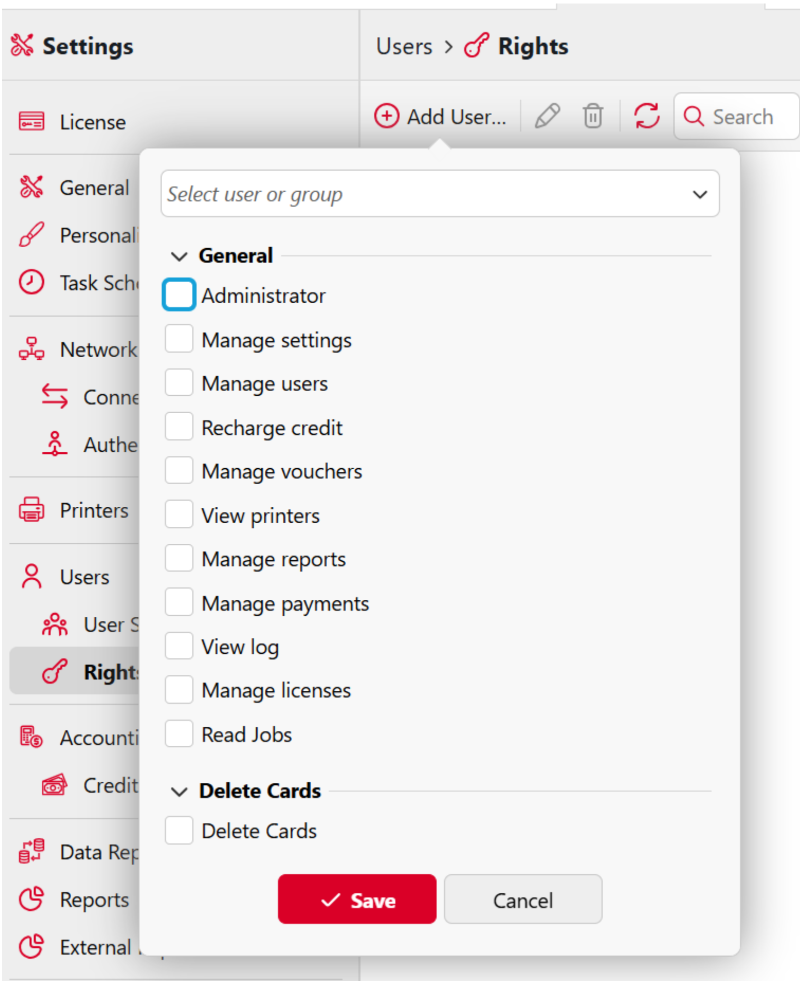
- **Attempts before lockout**
  Number of failed login attempts before user is locked out.
  - **Range**: 1 – 100
  - **Default**: 5
- **Lockout time**
  Period, in minutes, that a user must wait before they can attempt to log in again.
  - **Range**: 1 – 144,000
  - **Default**: 15

10.6.6 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.

From the toolbar at the top, you can:

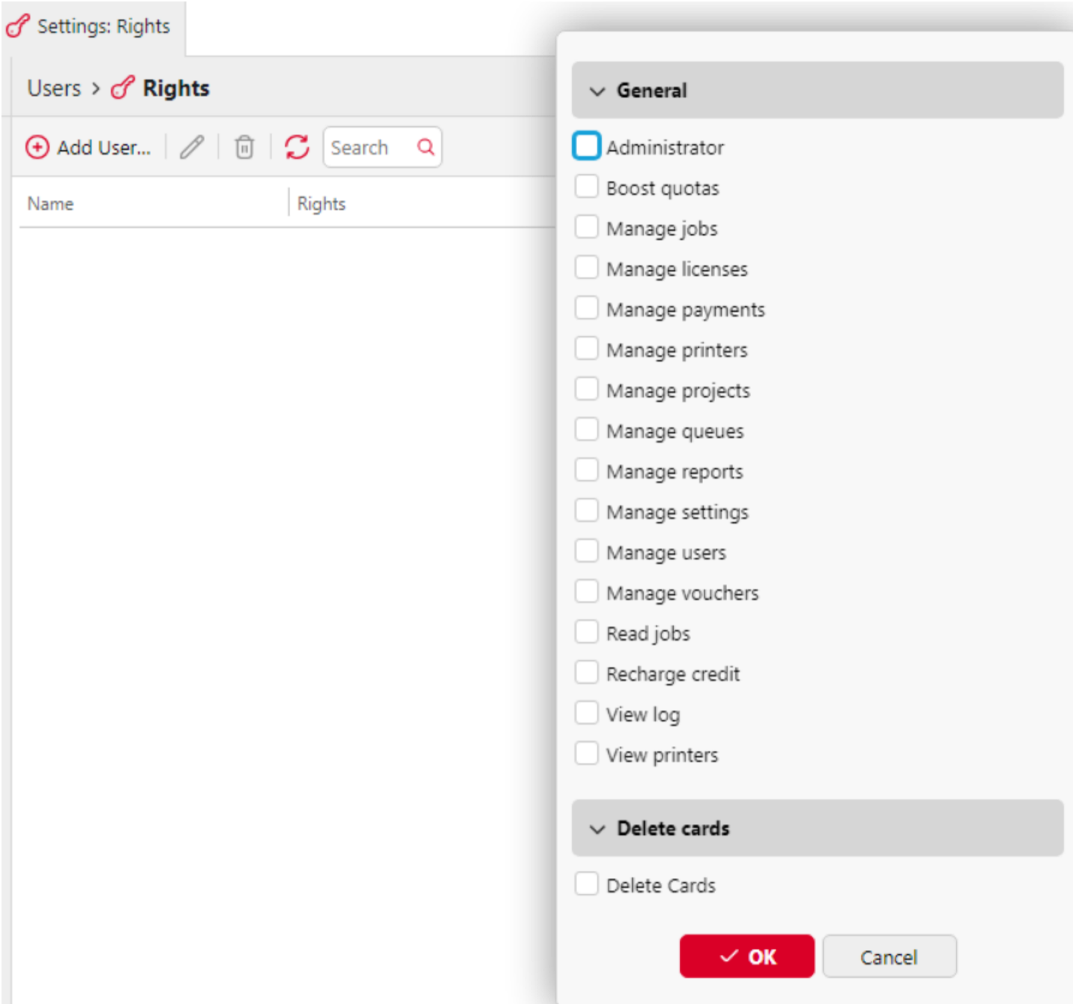
- **Add user** - add a new user or group with assigned rights.
- **Edit** - edit an existing user or group with assigned rights.
- **Delete** - delete a user or group with assigned rights.
- **Refresh** - refresh the list of users and groups.
- **Search** - search for a user or group with assigned rights. You can either use user names or rights for filtering your search results.



Providing Users and Groups with Rights

To add a new user or a group of users to the list on the **Rights** settings tab:

1. Click **+Add User**. The Select user or group dialog box appears.
2. In the dialog box, select the user (or group) and click **OK**. The rights panel opens.
3. Select the user (or group) rights.
4. Click **OK**. The user (or group) appears on the list on the **Rights** settings tab along with the assigned rights.



Editing Users' Rights

To open the user rights properties panel (or the group rights panel), 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 assign rights concerning the general run of MyQ. 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 able to delete all their ID cards.

10.7 User Synchronization

User synchronization is a method of importing and periodically synchronizing user-related data in the MyQ database with data in external sources, such as Microsoft Entra ID, 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.

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

> User passwords are not synchronized/stored in the MyQ Database in case of LDAP/MS Entra ID synchronizations.

10.7.1 Which Properties Can Be Synchronized

When MyQ synchronizes users from a directory service or CSV file, it maps source attributes to MyQ user properties. Not all user properties can be populated by synchronization, and not all properties behave the same way across sync sources. This page summarizes which properties can be synchronized, their constraints, and the default attribute mappings for each source type.

MyQ Property	Syncable	Constraints
User name	Yes	**Fixed per source type** – always `sAMAccountName` for LDAP/AD, always `userPrincipalName` for Entra ID (Graph API). Cannot be changed in sync source settings.
Full name	Yes	No constraints.
Aliases	Yes	Multiple values accepted, comma-separated. Used to match jobs sent with identifiers other than the username.
Personal number	Yes	Must be unique per user. Used for pairing users across sources.
Email	Yes	No constraints.
Alternate emails	Yes	Multiple values accepted, comma-separated.
Phone	No	Must be set manually.
Department	Yes	No constraints.
Cards	Yes	Sync mode configurable: Do not synchronize / Full synchronization / Synchronize if not empty / Add new. Multiple values accepted, comma-separated.
PIN	Yes	Sync mode configurable: same options as Cards. In CSV, PIN values must be in hashed MD5 format. Multiple values accepted, comma-separated.
Default language	Yes	Value must be a supported language abbreviation, for example `en`, `hr`.
User's storage	Yes	No constraints.
Notes	Yes	No constraints.

MyQ Property	Syncable	Constraints
Custom (1-3)	Yes	Available for Entra ID (Graph API) and CSV sources. Map any attribute not covered by standard properties.
Use authentication server	Yes	Set at the sync source level – applies to all users imported by that source. Not mapped per user.
Synchronization source	Automatic	Set by MyQ based on the sync source name. Not configurable per user via sync.
Advanced (on-premises identity)	Automatic	Populated automatically for hybrid Entra ID users from `onPremisesSamAccountName` and `onPremisesDomainName`. No configuration required.

10.7.2 Default Attribute Mappings by Source

Where a default mapping exists, MyQ applies it automatically. Properties with no default must be configured explicitly in the sync source settings.

Active Directory (LDAP)

MyQ Property	Default AD Attribute	Notes
User name	`sAMAccountName`	Fixed.
Full name	`cn`	
Email	`mail`	
All other properties	*(none)*	Must be configured explicitly.

Commonly configured explicitly:

MyQ Property	Recommended AD Attribute	Notes
Alias	`userPrincipalName`	Map here if job detection returns UPN.
Alias	`mailNickname` or `mail`	Map here if job detection returns email-format identifiers.

MyQ Property	Recommended AD Attribute	Notes
Personal number	`employeeId`	Useful for pairing across sources.
User's storage	`HomeDrive`	Enables Easy Print from / Easy Scan to user's home folder.
Card, PIN	Custom or `extensionAttribute`	Review confidential attribute protection before enabling.

Microsoft Entra ID (Graph API)

MyQ Property	Default Attribute	Notes
User name	`userPrincipalName`	Fixed.
Full name	`displayName`	
Email	`mail`	
Language	`preferredLanguage`	
Department	`department`	
All other properties	*(none)*	Must be configured explicitly.

Available attributes for explicit mapping include `employeeId`, `mailNickname`, `upnPrefix`, `onPremisesSamAccountName`, `onPremisesDomainName`, and `extensionAttribute1` through `extensionAttribute15`. Any Entra ID user resource attribute can also be typed manually if not listed in the dropdown.

OpenLDAP

MyQ Property	Default Attribute	Notes
User name	`uid`	Fixed.
Full name	`cn`	
Email	`mail`	

MyQ Property	Default Attribute	Notes
All other properties	*(none)*	Must be configured explicitly. Schema varies by installation – verify attribute names in your directory.

Novell eDirectory

No default mappings. All properties must be configured explicitly. Use the LDAP browser in the sync source General tab to identify attribute names in your directory.

Google Workspace (Secure LDAP)

MyQ Property	Typical Attribute	Notes
User name	`uid`	
Full name	`cn`	
Email	`mail`	
All other properties	*(none)*	Verify attribute names against your directory using the LDAP browser.

CSV

All properties are mapped by column name (or column position if no header row).

10.7.3 Sync Mode Options for Cards and PIN

The following sync modes apply to Cards and PIN properties across all source types that support them.

Mode	Behavior
Do not synchronize	Existing values in MyQ are not changed.
Full synchronization	Existing values are replaced with values from the source, including replacement with empty if the source value is empty.

Mode	Behavior
Synchronize if not empty	Existing values are replaced only if the source value is not empty. Default for CSV.
Add new	New values from the source are added without replacing existing ones.

See also:

- Editing User Accounts (see page 183)
- Available languages (see page 325)
- Transform User Data with RegEx (see page 246)
- Run and Schedule User Synchronization (see page 249)

10.7.4 Synchronize Users from LDAP

MyQ X can synchronize users from any LDAP-compatible directory service. Supported sources include Active Directory, OpenLDAP, Novell, Google Workspace, and Microsoft Entra ID Domain Services (via LDAPS). MyQ can communicate with up to five LDAP servers simultaneously.

This article describes the settings common to all LDAP synchronization sources. For directory preparation and source-specific requirements, see:

- (v2) Prepare for LDAP User Synchronization
- Synchronize Users from Active Directory (see page 219)
- Synchronize Users from Google Workspace (see page 223)
- Synchronize Users from Entra Domain Services (see page 228)

OpenLDAP and Novell use the common LDAP configuration described here. Lotus Domino synchronization is supported only for legacy deployments and must be explicitly enabled.

For Microsoft Entra ID synchronization through Microsoft Graph, see Synchronize Users from Microsoft Entra ID (see page 231).

Prerequisites

Before creating the synchronization source:

- Prepare the directory scope, attribute mappings, groups, directory account, and network connection.
- Configure the LDAP server under **MyQ > Settings > Authentication Servers**.
- Verify that MyQ can connect to the LDAP server.
- For LDAPS, verify that the directory certificate is trusted by the MyQ server.

LDAPS is recommended because it protects directory credentials and data in transit. It commonly uses TCP port `636`. Use another security mode or port only when it is supported by the directory and permitted by your organization's security policy.

For preparation guidance, see (v2) Prepare for LDAP User Synchronization.

Create an LDAP Synchronization Source

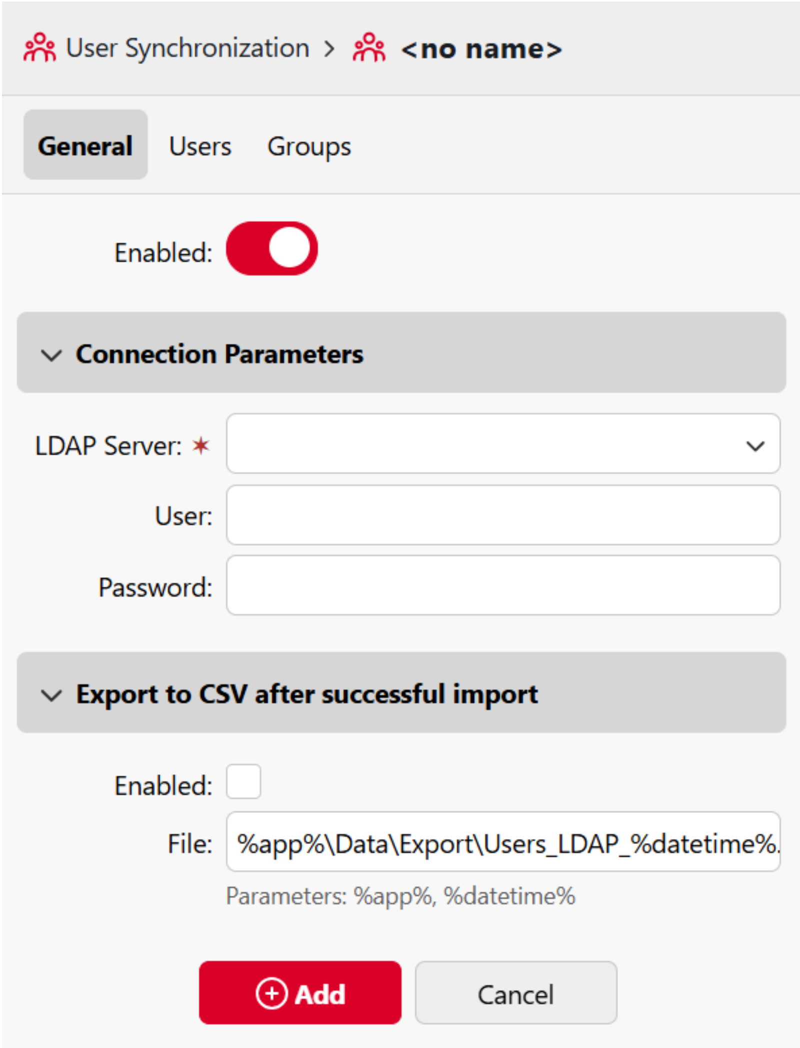
1. Go to **MyQ > Settings > User Synchronization**.
2. Click **+Add**.
3. Select **Add LDAP source**.

The LDAP synchronization properties panel opens.

4. Configure the synchronization on the **General**, **Users**, and **Groups** tabs.
5. Save the settings on each tab after making changes.

After it is saved, the source appears in the synchronization-source list.

General Tab



Use the **General** tab to select the LDAP server and provide the account MyQ uses to query it.

Setting	Description
Enabled	Enable or disable this synchronization source.
LDAP Server	Select the LDAP server added as an authentication server.
User	Username for access to the LDAP server.
Password	Password for the service account.

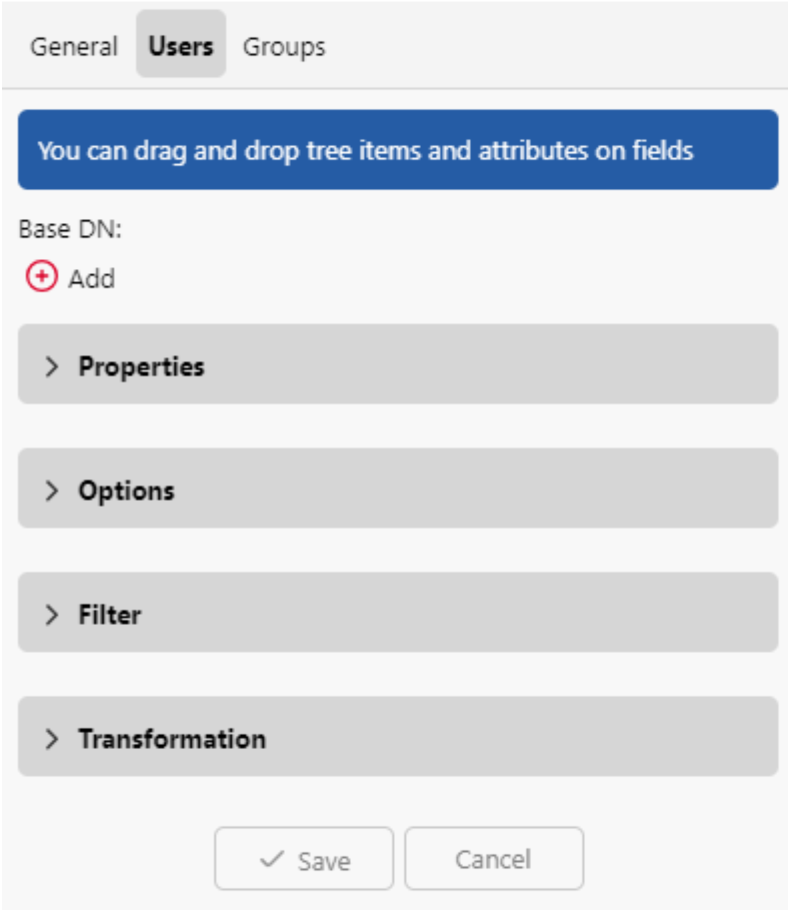
Setting	Description
Export to CSV after successful import	When enabled, MyQ writes a CSV file of imported users after each sync run.
File	File path using `%app%` and `%datetime%` parameters, for example `%app%\Data\Export\Users_LDAP_%datetime%.csv`.

Use a username format accepted by the directory. If the account belongs to a subdomain, a domain-qualified username may be required. For example:

```
Administrator@cz.example.local
```

After valid connection parameters are saved, the LDAP browser opens on the right side of the panel. Use it to browse the directory and drag directory objects or attributes into fields on the **Users** and **Groups** tabs.

Users Tab



Use the **Users** tab to define which users are imported, map directory attributes to MyQ properties, and control how existing MyQ users are updated.

Base DN

Add one or more Base DNs from which MyQ should search for users.

To add a Base DN:

1. Click **+Add**.
2. Enter the distinguished name, or drag the required directory object from the LDAP browser into the field.

For example:

```
OU=Prague,DC=example,DC=com
```

Multiple Base DNs can be used to import users from separate organizational units or directory branches.

The correct Base DN depends on the directory structure and LDAP server. In configurations where searches must begin at the directory root, the Base DN can be left empty.

Properties

Map LDAP attributes to MyQ user properties. To assign an attribute, type its name in the property field or drag it from the LDAP browser and drop it in. Where a default mapping exists, it is applied automatically – the Username property is the only one that cannot be changed.

MyQ property	Default mapping	Notes
Username	`sAMAccountName` for Active Directory	The username mapping is determined by the LDAP source type and cannot be changed.
Full name	`cn` for Active Directory and OpenLDAP	
Email	`mail` for Active Directory and OpenLDAP	
Alias	None	Accepts multiple comma-separated values.
Personal number	None	Can be used to pair an imported identity with an existing MyQ user.
Card	None	Accepts multiple comma-separated values. Synchronization behavior is configurable.
PIN	None	Accepts multiple comma-separated values. Synchronization behavior is configurable.

MyQ property	Default mapping	Notes
Language	None	Map an attribute containing supported language abbreviations, such as `en` or `de`.
User storage	None	Storage destination associated with the user.
Notes	None	

The **Alias**, **Card**, and **PIN** properties support multiple values separated by commas. For example:

```
alias1,alias2,alias3
```

Attribute names containing semicolons, such as `email;x-private`, are supported from Print Server 10.2 patch 24. In earlier versions, a semicolon in an attribute name can prevent that attribute from being synchronized.

Using semicolons to separate multiple values is deprecated from patch 24. Use commas instead.

Card and PIN Synchronization

For the **Card** and **PIN** properties, select how synchronization affects values already stored in MyQ.

Mode	Behavior
Do not synchronize	Does not change existing values in MyQ.
Full synchronization	Replaces existing values with the directory values. Existing values are removed if the corresponding directory value is empty.
Synchronize if not empty	Replaces existing values only when the directory provides a value. Existing values remain when the directory value is empty.
Add new	Adds new directory values without replacing or removing existing values.

Choose the mode according to whether the directory or MyQ is authoritative for cards and PINs.

Options

Option	Description
Deactivate missing users	Deactivates users previously imported from this source when they are no longer present in the synchronization results.
Add new users	Imports new directory users. When disabled, synchronization updates matching MyQ users but does not create accounts.
Convert user name to lowercase	Converts imported usernames to lowercase, preventing separate MyQ accounts from being created solely because of differences in letter case.
Use authentication server	Assigns the source LDAP server as the authentication server for synchronized users. Username and password authentication is then performed against LDAP instead of the MyQ database.
Pair by the personal number	Uses a synchronized personal number to associate a directory identity with an existing MyQ account. This allows the existing account to be retained when its username changes.
Ignore synchronization source	Allows this source to consider and update matching users regardless of which source originally created or imported them.
Append the domain name to the username	Stores usernames in a domain-qualified form such as `username@domain.local`. Use this where domains contain overlapping usernames or a domain-qualified identity is required by other features.

Pair by the Personal Number

Use **Pair by the personal number** when a stable personal number should identify the same person after their username changes.

For example, if the directory username changes from `cat.stevens` to `yusuf.islam`, MyQ can update the existing account instead of creating another account, provided both identities have the same unique personal number.

Before enabling this option, confirm that personal numbers are:

- Populated for all relevant users
- Unique across the synchronization scope
- Stable throughout the user's lifecycle
- Never reassigned to another person

Ignore Synchronization Source

By default, a synchronization source updates users associated with that source. If another source already owns a matching username or alias, MyQ can report a conflict instead of updating that user.

Enable **Ignore synchronization source** when the current synchronization should update matching users regardless of their original synchronization source.

This can be useful during migrations or when several sources intentionally manage the same user population. However, it changes the scope of users that the synchronization can affect.

> ⚠ Use **Ignore synchronization source** with **Deactivate missing users** only when the current LDAP source is authoritative for all affected users. With both options enabled, users imported or created through other sources can be deactivated when they are absent from the current LDAP results.

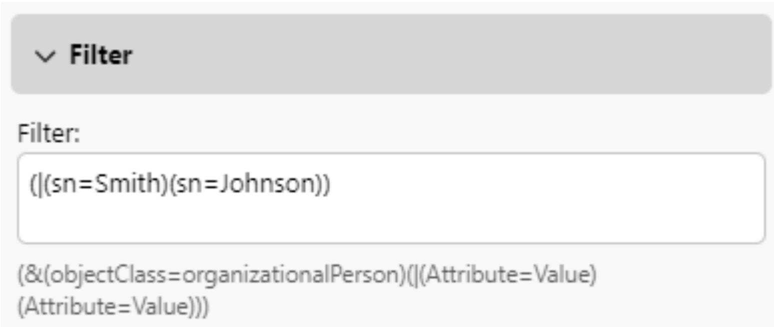
Filter

Use an LDAP filter to restrict which directory objects are imported. If the field is empty, MyQ applies the default filter for the selected LDAP source type.

Example filter	Matches
`(objectClass=*)`	All objects.
`(&(objectCategory=person)(objectClass=user)(!(cn=andy)))`	All user objects except `andy`.
`(sn=sm*)`	All objects with a surname starting with `sm`.

Example filter	Matches
`(&(objectCategory=person)(objectClass=contact)((sn=Smith)(sn=Johnson)))`	Contact objects whose surname is `Smith` or `Johnson`.

The `*` wildcard can be used with string-valued attributes. Distinguished-name attributes such as `memberOf` do not support partial wildcard matching and must be matched using the complete value.



For example:

```
(memberOf=CN=Print Users,OU=Groups,DC=example,DC=com)
```

Escape Special Characters

When a special character forms part of an attribute value rather than LDAP filter syntax, escape it as follows:

Character	Escaped form
`\`	`\5c`
`;`	`\3b`
`*`	`\2a`
`(`	`\28`
`)`	`\29`
`Null`	`\00`

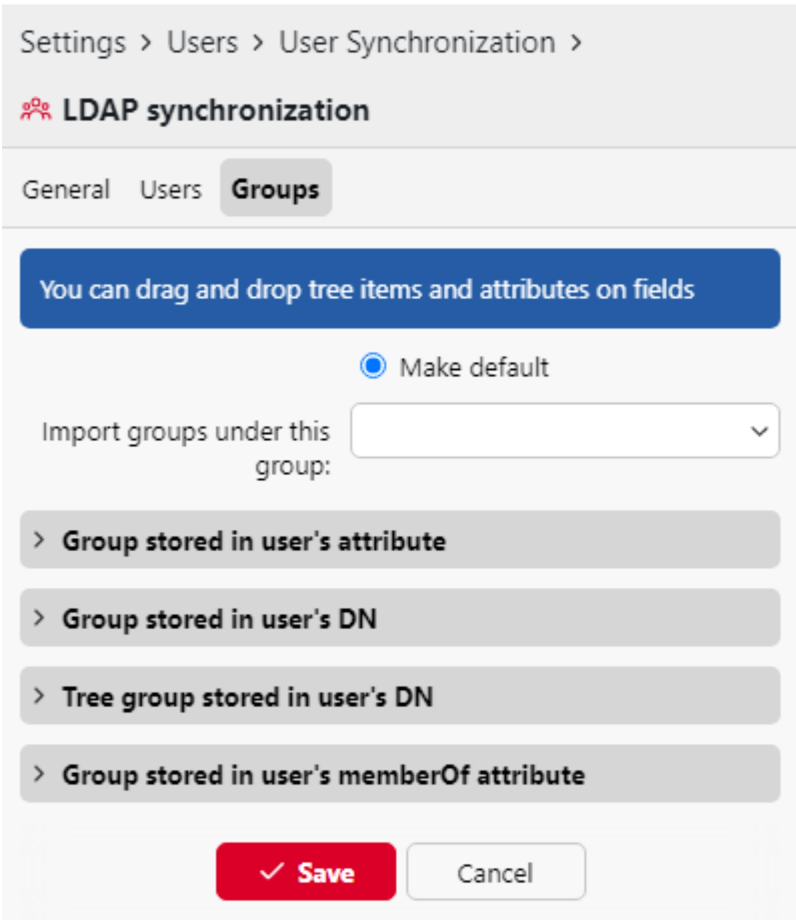
Transformation

A regular expression transformation can parse or reformat directory values before MyQ stores them.

Use transformations when, for example:

- Several identifiers are stored in one attribute.
- A prefix or suffix must be removed.
- A source value must be divided into separate MyQ properties.
- An identifier must be normalized into the format used for job detection or authentication.

Groups Tab



Use the **Groups** tab to import directory groups and define how they are represented in MyQ.

The **Groups** tab determines group structure and membership. It does not determine which users are imported; user scope is configured on the **Users** tab.

General Group Settings

Setting	Description
Do not change default group	Prevents synchronization from changing a user’s existing default accounting group.
Import groups under this group	Places all groups imported by this source beneath a selected MyQ group.
Synchronization level	Determines how changes to directory group membership affect existing MyQ memberships.

A user can belong to multiple groups, but only one group can be their default accounting group. Print, copy, and scan activity is accounted to this group where group-based accounting is used.

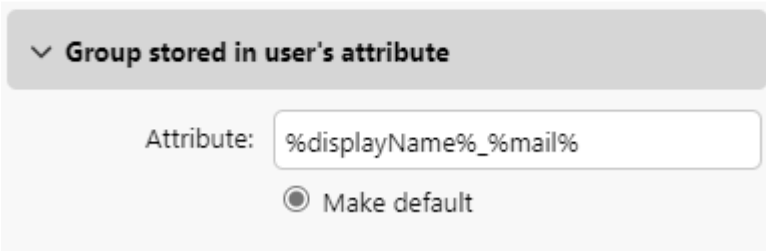
Group Synchronization Level

Level	Behavior
Full synchronization	Group membership in MyQ follows the directory. Users are added to and removed from groups as directory membership changes.
Synchronize if not empty	Synchronizes directory memberships while preventing the user from being left without any group.
Add new	Adds new directory memberships. Memberships removed from the directory remain in MyQ.

Groups Stored in a User Attribute

Use this method when a user attribute contains the group name or values from which the group name should be created.

Enter the attribute name or drag it from the LDAP browser.



Multiple attributes can be combined. For example:

```
%attribute1%_%attribute2%
```

If the attributes contain `Prague` and `Sales`, MyQ creates the group:

```
Prague_Sales
```

Use vertical bars to create a hierarchy:

```
%attribute1%|%attribute2%
```

This produces:

```
Prague > Sales
```

Enable **Make default** to make the resulting group the user's default accounting group.

Group Stored in the User DN

Use this method to derive one group from an organizational-unit component in the user's distinguished name.

For example:

```
CN=Anna Novak,OU=Sales,OU=Prague,DC=example,DC=com
```

OU components are counted from right to left:

OU component	Index
`Prague`	1
`Sales`	2

To import `Sales` as the group, set **OU component index** to `2`.

Enable **Make default** to make the imported group the user's default accounting group.

Tree Group Stored in the User DN

Use this method to reproduce an organizational-unit hierarchy from the user's distinguished name.

For example:

```
CN=Anna Novak,OU=Sales,OU=Prague,DC=example,DC=com
```

To derive the hierarchy:

```
Prague > Sales
```

remove:

- The user component from the left: `CN=Anna Novak`
- The domain components from the right: `DC=example,DC=com`

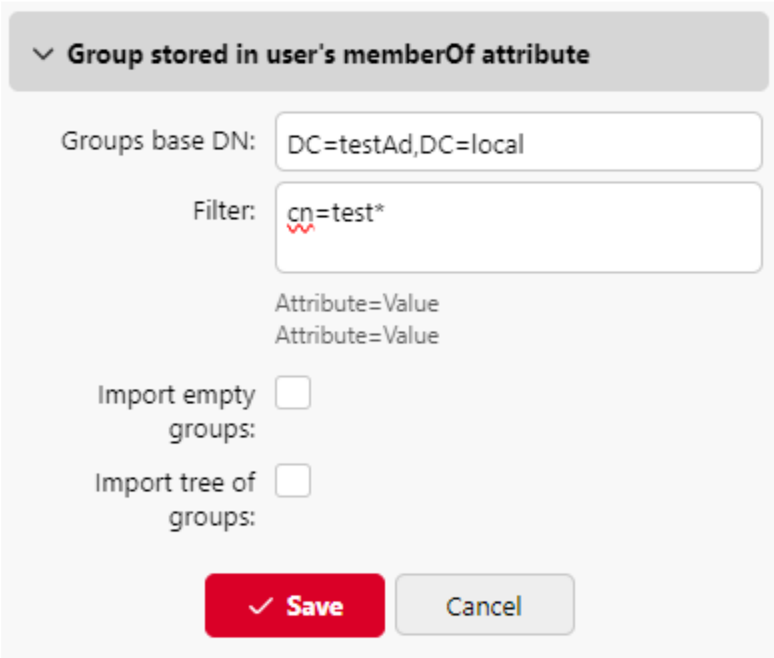
Configure **Strip from left** and **Strip from right** according to the number of components that must be excluded.

At least one component must be stripped from each side.

Enable **Make default** to make the lowest group in the imported hierarchy the user's default accounting group. In this example, the default group would be `Sales`.

Groups Stored in the `memberOf` Attribute

Use this method to import security or distribution groups referenced by the user's `memberOf` attribute.



Specify a **Groups Base DN** to restrict which groups are considered. MyQ ignores groups outside this Base DN.

The Groups Base DN does not need to belong to the same organizational unit as the Users Base DN.

Because `memberOf` can contain several groups, **Make default** is not available for this method.

Configure the following options where required:

Option	Description
Filter	Restricts imported groups using `Attribute=Value` conditions. Enter one condition per line. A group is accepted if it satisfies at least one condition. The `*` wildcard is supported.
Import empty groups	Imports groups from the Groups Base DN even when no synchronized user references them through `memberOf`.
Import tree of groups	Preserves the directory's parent-child group structure. When disabled, groups are imported as separate, flat groups.

For example:

```
cn=*Print*
```

This accepts groups whose common name contains `Print`.

Run and Validate the Synchronization

Run the source manually before scheduling it.

1. Use a restricted Base DN or filter for the initial test where possible.
2. Keep **Deactivate missing users** disabled.
3. Run the synchronization.
4. Review its log and reported conflicts.
5. Verify the imported users, properties, groups, group memberships, and default accounting groups.
6. Test job ownership and user authentication where applicable.
7. Expand the scope only after the results are correct.
8. Enable user deactivation only after confirming which accounts it will affect.
9. Schedule recurring synchronization.

See also:

- Authentication Servers Settings (see page 158)
- Available languages (see page 325)
- Editing User Accounts (see page 183)
- Run and Schedule User Synchronization (see page 249)
- Transform User Data with RegEx (see page 246)

Synchronize Users from Active Directory

MyQ X synchronizes users from Active Directory (AD) using the LDAP protocol. The synchronization imports user accounts and group memberships, keeps them current as the directory changes, and maps the directory attributes that job authentication and terminal login depend on.

Guidance on when to use this source is provided in the Deployment guide. See (v2) User Synchronization.

See also: Synchronize Users from LDAP (see page 204)

Prerequisites

- An Active Directory domain controller reachable from the MyQ server over LDAPS (port 636 recommended) or LDAP (port 389).
- A service account in AD with read-only access scoped to the organizational units you intend to sync. No write access or elevated domain privileges are required.
- If using LDAPS (recommended) the issuing root CA certificate must be installed in the Windows certificate store on the MyQ server so that it can verify the AD certificate. In managed environments this may already be handled by Group Policy.
- DNS correctly resolves the AD domain from the MyQ server.

Key Considerations

Test job detection before configuring sync. MyQ always maps `sAMAccountName` to the username field for LDAP-synced users – this cannot be changed. If your job detection returns a different value, most commonly `userPrincipalName` in environments with Entra ID-joined or hybrid-joined devices, the match will fail unless that value is also present as an alias. Send a test job from an account that does not yet exist in MyQ and check the discard log entry (`Job discarded. User "x" not found.`) – the quoted value is exactly what your sync must place in the username or alias field. See (v2) Understanding Job Detection.

Multi-value fields require transformation. Some environments store multiple identifiers – an ID card number and a personal number, for example – in a single AD attribute separated by a delimiter. MyQ supports regex transformation in the sync source settings to parse these values. See Transform User Data with RegEx (see page 246) .

Multi-domain environments require domain appending. If users from multiple AD domains are synchronized into the same MyQ installation, the same `sAMAccountName` can exist in more than one domain. Enable **Append the domain name to the username** in each LDAP sync source to produce unique usernames in the format `username@domain`. For job authentication to work correctly, the domain must also be present in the print job. See (v2) Multi-domain and Multi-tenant Environments.

Schema extension is irreversible. If you plan to use custom schema extension attributes to protect sensitive values such as card numbers or PINs, test the schema change in a lab environment before applying it to production. Custom attributes added to the AD schema cannot be removed.

Configure the Authentication Server

Go to **MyQ > Settings > Authentication Servers** and add a new LDAP server for the AD domain. Set **Security** to **SSL** and the port to **636**.

If a sub-domain service account is used, specify the sub-domain in the username field. For example, if the account `Administrator` resides in `cz.testAD.local` but connects to `testAD.local`, enter `Administrator@cz.testAD.local`.

See also: Authentication Servers Settings (see page 158)

Configure the Synchronization Source

Go to **Settings > User Synchronization**, click **+Add**, and select **Add LDAP source**.

For the full configuration reference, see Synchronize Users from LDAP (see page 204). The following covers what is specific to Active Directory.

Default Attribute Mapping

MyQ applies these default mappings automatically for Active Directory sources. All other properties have no default and must be configured explicitly.

MyQ Property	Default AD Attribute
Username	`sAMAccountName`
Full name	`cn`
Email	`mail`

Properties commonly configured explicitly for AD:

MyQ Property	AD Attribute	Notes
Alias	`userPrincipalName`	Map here if job detection returns UPN rather than `sAMAccountName`.

MyQ Property	AD Attribute	Notes
Alias	`mailNickname` or `mail`	Map here if job detection returns email-format identifiers.
Personal number	`employeeId`	Useful for pairing users across sync sources, including during AD-to-Entra ID migration.
Card	Custom or `extensionAttribute`	Review confidential attribute protection before enabling – see Security Considerations.
PIN	Custom or `extensionAttribute`	Same consideration as Card.
User's storage	`HomeDrive`	Enables Easy Print from and Easy Scan to the user's home folder on embedded terminals.

Run and Schedule Synchronization

To run synchronization immediately, go to **MyQ > Settings > User Synchronization**, select the source, and click **Synchronize now**. If configured correctly, synced users and groups appear under **MyQ > Users**.

To synchronize automatically on a schedule, go to **MyQ > Settings > Task Scheduler** and configure the User Synchronization task.

Security Considerations

Use LDAPS

All LDAP communication between MyQ and AD should use LDAPS (LDAP over SSL/TLS) or StartTLS. Plain LDAP transmits credentials and directory data in cleartext. LDAPS can be enforced in the Authentication Server settings in MyQ.

Protect Sensitive Directory Attributes

Standard AD attributes are readable by any authenticated domain user by default. If ID card numbers, PINs, or other sensitive identifiers are stored in AD and will be synced to MyQ, mark those attributes as confidential before enabling the sync.

Confidential attributes restrict read access to specified trustee accounts – the service account used by MyQ for synchronization would be granted trustee access.

For stronger protection, store sensitive values in custom schema extension attributes rather than standard attributes. Custom attributes are less predictable to enumerate and can also be flagged as confidential.

Apply Least Privilege to the Sync Service Account

The service account used for LDAP synchronization should have read-only access scoped to the organizational units being synced. If confidential attributes are used, the service account must be explicitly granted trustee access to those attributes only.

See also:

- Synchronize Users from LDAP (see page 204)
- Authentication Servers Settings (see page 158)
- Run and Schedule User Synchronization (see page 249)

- (v2) Multi-domain and Multi-tenant Environments
- (v2) Transition from Active Directory to Entra ID

Synchronize Users from Google Workspace

MyQ X synchronizes users from Google Workspace using Google's Secure LDAP service, which provides read-only access to the Google directory over LDAPS. The synchronization imports user accounts and group memberships and maps directory attributes to MyQ user properties.

Guidance on when to use this source is provided in the Deployment guide. See (v2) User Synchronization.

See also: Synchronize Users from LDAP (see page 204).

Prerequisites

- Super Admin privileges in Google Workspace.
- A Google Workspace subscription that supports the Secure LDAP service.
- The MyQ server must be able to establish outbound LDAPS connections (TCP 636) to Google.
- Familiarity with which users or groups MyQ should be allowed to access.

Key Considerations

Each MyQ server instance requires its own LDAP client certificate. Google issues a unique certificate per LDAP client. If you run multiple MyQ servers – for example, a Central Server and Site Servers – each must have its own client registered in Google Admin with its own certificate and credentials.

Certificates expire and must be renewed. Google Workspace LDAP client certificates have an expiry date. Plan certificate renewal into your operational calendar. When a certificate expires, synchronization will fail until a new certificate is generated and uploaded to MyQ.

Access permission changes can take up to 24 hours to take effect. When you modify LDAP client access permissions in Google Admin Console, the changes are not immediate. Account for this delay during initial setup and testing – if sync is not returning expected results shortly after a permission change, wait and retry before troubleshooting further.

The client certificate must be in PEM format. MyQ requires the client certificate in PEM format (Base64-encoded, with `BEGIN CERTIFICATE` headers). If the certificate downloaded from Google Admin is in binary DER format, convert it before uploading to MyQ, for example using OpenSSL: `openssl x509 -inform der -in certificate.der -out certificate.pem`

Do not protect the private key with a password. MyQ cannot use a password-protected private key. When generating credentials in Google Admin, leave the private key unprotected.

Configure the LDAP Client in Google Admin

This step is performed entirely in the Google Admin Console. It produces the client certificate, private key, and LDAP credentials that MyQ needs to connect.

1. Sign in to the Google Admin Console with a Super Admin account.
2. Go to **Apps > LDAP** and click **Add Client**.
3. Enter a name for the client (required) and an optional description. Click **Continue**.
4. On the LDAP client page, click **Access Permissions** and configure the following:

   Verify user credentials – enables user authentication via MyQ. Set to all users or to specified organizational units.

Read user information – enables MyQ to read user attributes. Set to all users or to specified organizational units, then enable access to:

- System Attributes
- Public Custom Attributes
- Private Custom Attributes

Read group information – allows MyQ to read directory group membership. Set to **On**.

5. Click **Add LDAP Client** and wait while the client is provisioned and a certificate is generated. This may take a few minutes.
6. Download the generated certificate package. The ZIP file contains:
   - The client certificate (`.crt` or `.pem`)
   - The private key (`.key`)

   Store these files securely. If the certificate is in DER format, convert it to PEM before proceeding.
7. Click **Continue to Client Details**.
8. Click **Access Credentials**, then click **Generate New Credentials**. The generated username and password are displayed once only – store them securely before leaving this screen.
9. Return to the LDAP client details page and set the **Service Status** to **ON for everyone**. Click **Save**.

Google Workspace is now configured with MyQ as an LDAP client.

Configure the Authentication Server in MyQ

Go to **MyQ > Settings > Authentication Servers** and add a new LDAP server for Google Workspace.

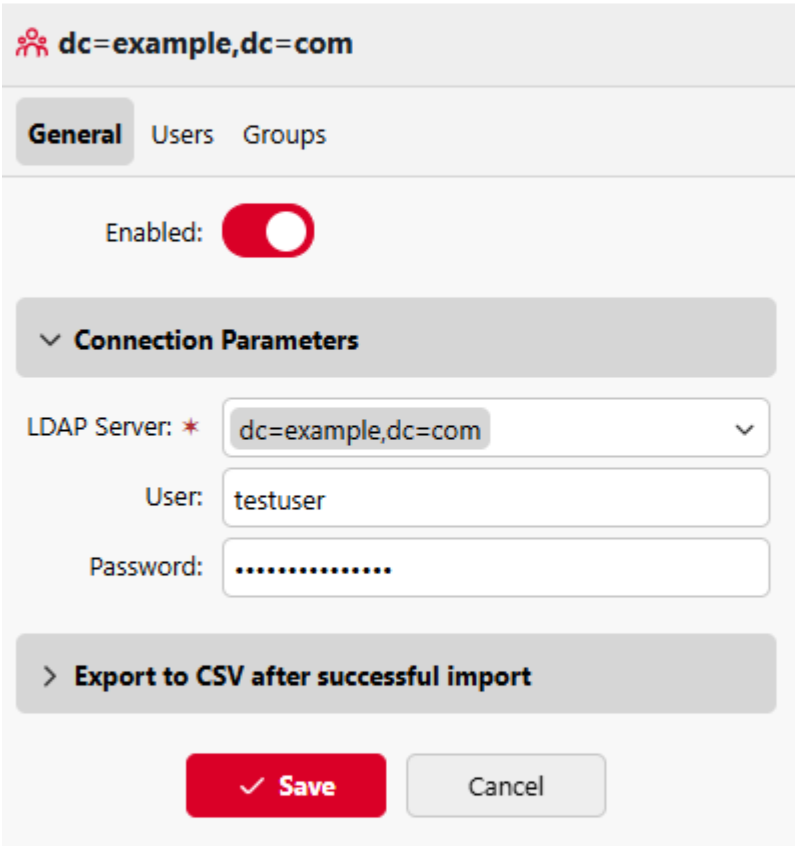
Setting	Value
Security	SSL
Port	636
Server	`ldap.google.com`
User	The username generated in Google Admin (Step 1)
Password	The password generated in Google Admin (Step 1)

Setting	Value
Client certificate	Upload the `.crt` or `.pem` file downloaded from Google Admin
Private key	Upload the `.key` file downloaded from Google Admin

---

Configure the Synchronization Source

Go to **MyQ > Settings > User Synchronization**, click **+Add**, and select **Add LDAP source**.



The following covers what is specific to Google Workspace.

Base DN

The Base DN for Google Workspace uses the domain components of your Google Workspace domain. For example, for the domain `example.com`:

`dc=example,dc=com`

Default Attribute Mapping

Google Workspace exposes a standard LDAP schema. The following mappings are typical for most Google Workspace directories, but confirm attribute names against your actual directory using the LDAP browser in the General tab.

MyQ Property	Typical Google Workspace Attribute
Username	`uid`
Full name	`cn`
Email	`mail`
Alias	*(none – configure explicitly if needed)*
Personal number	*(none – configure explicitly if needed)*

Run and Schedule Synchronization

To run synchronization immediately, go to **MyQ > Settings > User Synchronization**, select the source, and click **Synchronize now**. If configured correctly, synced users and groups appear under **MyQ > Users**.

To synchronize automatically on a schedule, go to **MyQ > Settings > Task Scheduler** and configure the User Synchronization task.

Security Considerations

LDAPS Is Mandatory

Google's Secure LDAP service only operates over LDAPS – plain LDAP is not supported. Ensure the MyQ server can reach `ldap.google.com` on TCP 636 and that no firewall rule blocks outbound connections on that port.

Protect Client Certificates and Credentials

The client certificate, private key, and generated credentials provide read access to your Google directory. Store them securely and limit access to the MyQ server and its administrators. Rotate credentials if they are exposed.

Apply Least Privilege via Access Permissions

In Google Admin, scope the LDAP client's access permissions to only the organizational units MyQ needs to read. Granting access to all users when sync only covers a subset of the organization is unnecessary exposure.

See also:

- Synchronize Users from LDAP (see page 204)
- Authentication Servers Settings (see page 158)
- Run and Schedule User Synchronization (see page 249)
- Manage LDAP Clients – Google Workspace Admin Help[25]
- Secure LDAP Schema – Google Workspace[26]

Synchronize Users from Entra Domain Services

MyQ X can synchronize users from Microsoft Entra ID using LDAPS, via the Entra ID Domain Services managed domain service. This method uses the same LDAP synchronization source as Active Directory and other LDAP directories – the difference is in how the Entra ID Domain Services instance is configured in Azure before MyQ connects to it.

Guidance on when to use this source is provided in the Deployment guide. See (v2) User Synchronization.

For the full LDAP sync source configuration reference, see Synchronize Users from LDAP (see page 204).

Prerequisites

- Microsoft Entra ID Domain Services enabled and configured in your Azure subscription. This is a paid Microsoft add-on – it is not included in standard Entra ID licensing.
- Secure LDAP (LDAPS) enabled on the Entra ID Domain Services instance.
- The Secure LDAP external IP address of the Entra ID Domain Services instance.
- The DNS domain name of the Entra ID Domain Services instance.
- The issuing root CA certificate installed in the Windows certificate store on the MyQ server.

---

25. https://support.google.com/a/answer/9048516
26. https://support.google.com/a/answer/9188164

Key Considerations

Setup is performed in Azure before configuring MyQ. The Entra ID Domain Services instance and its LDAPS configuration must be fully operational before adding the authentication server in MyQ. The Microsoft setup guides below cover both steps.

Connection parameters differ from standard AD. When adding the LDAP authentication server in MyQ, use the Entra ID Domain Services-specific values rather than a local AD domain controller address – see Configure the Authentication Server in MyQ, below.

Configure Entra ID Domain Services in Azure

Study the following Microsoft guides before proceeding to MyQ configuration:

1. Enable and configure Azure Active Directory Domain Services[27]
2. Configure Entra ID Domain Services to use Secure LDAP[28]

Once both steps are complete, note the following values from the Entra ID Domain Services Properties page in the Azure portal – you will need them in MyQ:

Value	Where to find it
DNS domain name	Properties page, **DNS DOMAIN NAME** field
Secure LDAP external IP address	Properties page, **SECURE LDAP EXTERNAL IP ADDRESS** field

---

Configure the Authentication Server in MyQ

Go to **MyQ > Settings > Authentication Servers** and add a new LDAP server using the following parameters:

Setting	Value
Domain	DNS domain name of the Entra ID Domain Services instance
Security	SSL

27. https://docs.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-create-instance

28. https://docs.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-configure-ldaps

Setting	Value
Server	Secure LDAP external IP address of the Entra ID Domain Services instance
Port	636

Configure the Synchronization Source

Go to **MyQ > Settings > User Synchronization**, click **+Add**, and select **Add LDAP source**. Select the authentication server you created.

The attribute mapping and options for Entra ID Domain Services follow the same conventions as Active Directory, since Entra ID Domain Services exposes a Windows Server AD-compatible schema.

Run and Schedule Synchronization

To run synchronization immediately, go to **MyQ > Settings > User Synchronization**, select the source, and click **Synchronize now**. If configured correctly, synced users and groups appear under **MyQ > Users**.

To synchronize automatically on a schedule, go to **MyQ > Settings > Task Scheduler** and configure the User Synchronization task.

See also:

- Authentication Servers Settings (see page 158)
- Run and Schedule User Synchronization (see page 249)
- Enable and configure Azure Active Directory Domain Services – Microsoft Learn[29]
- Configure Secure LDAP for Entra ID Domain Services – Microsoft Learn[30]

29. https://docs.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-create-instance
30. https://docs.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-configure-ldaps

10.7.5 Synchronize Users from Microsoft Entra ID

Synchronize users from Microsoft Entra ID to create and maintain MyQ users and groups.

Prerequisites

Plan your synchronization source, user identities, authoritative-source behavior, and multi-tenant environments, then register a Microsoft Entra ID application, and then create a Microsoft Entra ID connection in MyQ.

See also:

- (v2) User Synchronization
- (v2) Manual App Registrations
- Connect to Microsoft Entra ID (Graph API) (see page 151)

Add Microsoft Entra ID as a Synchronization Source

Go to **MyQ > Settings > User Synchronization**.

Click **Add** and select **Add Microsoft Entra ID source**.

Configure the synchronization source on the following tabs:

- **General**: select the Entra connection and identify the synchronization source.
- **Users**: select which users to synchronize, map their properties, and configure user lifecycle options.
- **Groups**: configure which Entra group memberships are represented in MyQ and how they are maintained.

General Tab

Configure the synchronization source:

- **Enable**: enable or disable the synchronization source.
- **Authentication Server:** select the Microsoft Entra ID connection used to access the tenant.
- **Synchronization Source:** enter a descriptive name for the source.

Use clear and unique names if you synchronize users from multiple Entra tenants.

Users Tab

On the **Users** tab, select which Entra users to synchronize, map their properties to MyQ, and configure how MyQ handles changes detected during synchronization.

Users to Import

Select one of the following:

- **All users**: synchronize all users in the tenant.
- **Users from selected groups:** synchronize users who are members of at least one selected Entra group.
- **Users from groups containing a string:** synchronize users belonging to groups whose names contain one of the specified strings. Enter each string on a separate line. Matching is case-insensitive.

> ⚠ Filtering users by strings in group names can increase synchronization time significantly.

User Properties

Map Microsoft Entra attributes to MyQ user properties.

MyQ property	Available Entra attributes
Full name	`displayName`
Personal number	`employeeId`, `extensionAttribute1` – `extensionAttribute15`
Email	`mail`
Notes	`extensionAttribute1` – `extensionAttribute15`
Language	`preferredLanguage`
Department	`department`
Alias	`displayName`, `userPrincipalName`, `upnPrefix`, `mailNickname`, `onPremisesSamAccountName`, `onPremisesDomainName`, `extensionAttribute1` – `extensionAttribute15`

MyQ property	Available Entra attributes
Card	`employeeId`, `extensionAttribute1` – `extensionAttribute15`
PIN	`employeeId`, `extensionAttribute1` – `extensionAttribute15`
Custom 1–3	`extensionAttribute1` – `extensionAttribute15`

You can also enter a supported custom Entra attribute instead of selecting one of the predefined attributes.

The user's Entra **UPN is always used as the MyQ username** and cannot be remapped.

For the **Alias** property, you can use `onPremisesSamAccountName@onPremisesDomainName` to combine the two attributes into an alias such as `user@company.com`.

User Synchronization Options

Configure how MyQ handles synchronized users.

- **Deactivate Missing Users:** Automatically deactivate users in MyQ that are no longer present in the synchronization scope.
  Use this option when Entra ID controls the lifecycle of the synchronized MyQ users.
- **Add New Users:** Automatically create MyQ users that are found in the synchronization scope but do not yet exist in MyQ.
- **Use as authentication server:** Assign the selected Microsoft Entra ID connection as the authentication server for synchronized users.
  Enable this when users synchronized from this source should also authenticate against Microsoft Entra ID.
- **Pair by the personal number:** Match synchronized identities to existing MyQ users by personal number. When a matching personal number is found, MyQ updates the existing user instead of creating another account.
  Pairing by personal number is enabled by default for synchronization sources created in current MyQ X versions and is strongly recommended.
- **Ignore Synchronization Source:** Use this option to control whether the synchronization source associated with a user is considered when processing synchronization changes.
- **Enable delta synchronization**: periodically check for changes since the last delta run and apply only those changes - new users, updated users, disabled or

deleted users, group renames, and membership changes. This option requires the User Delta Synchronization scheduled task to be enabled.

Create a Normalized Alias from Display Name

Enable **Create normalized alias from Display name** to add an additional alias that can be used to identify jobs submitted from Entra ID joined devices.

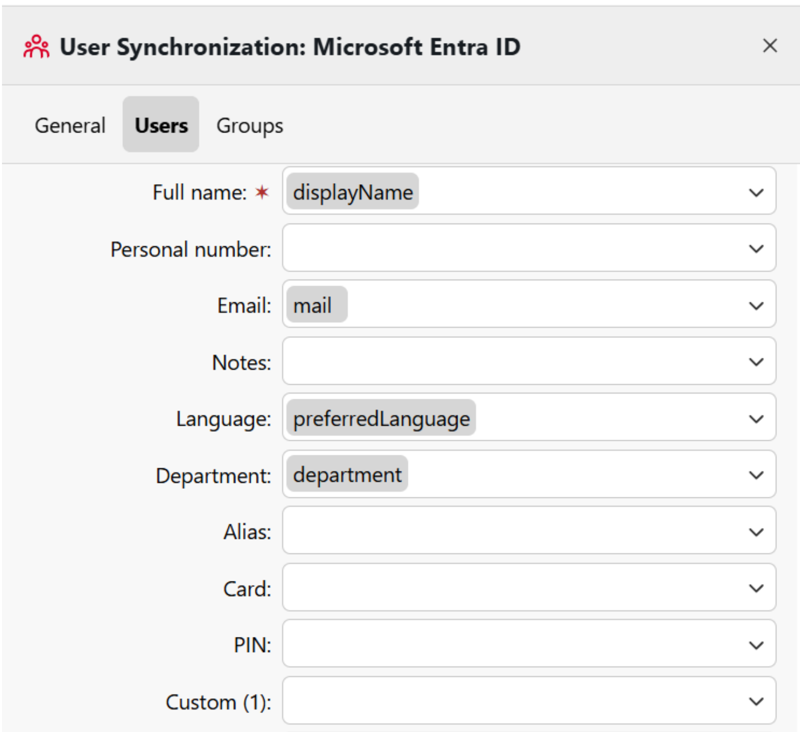
The alias is generated from the user's Entra display name in the form expected from supported Windows print-job identities.

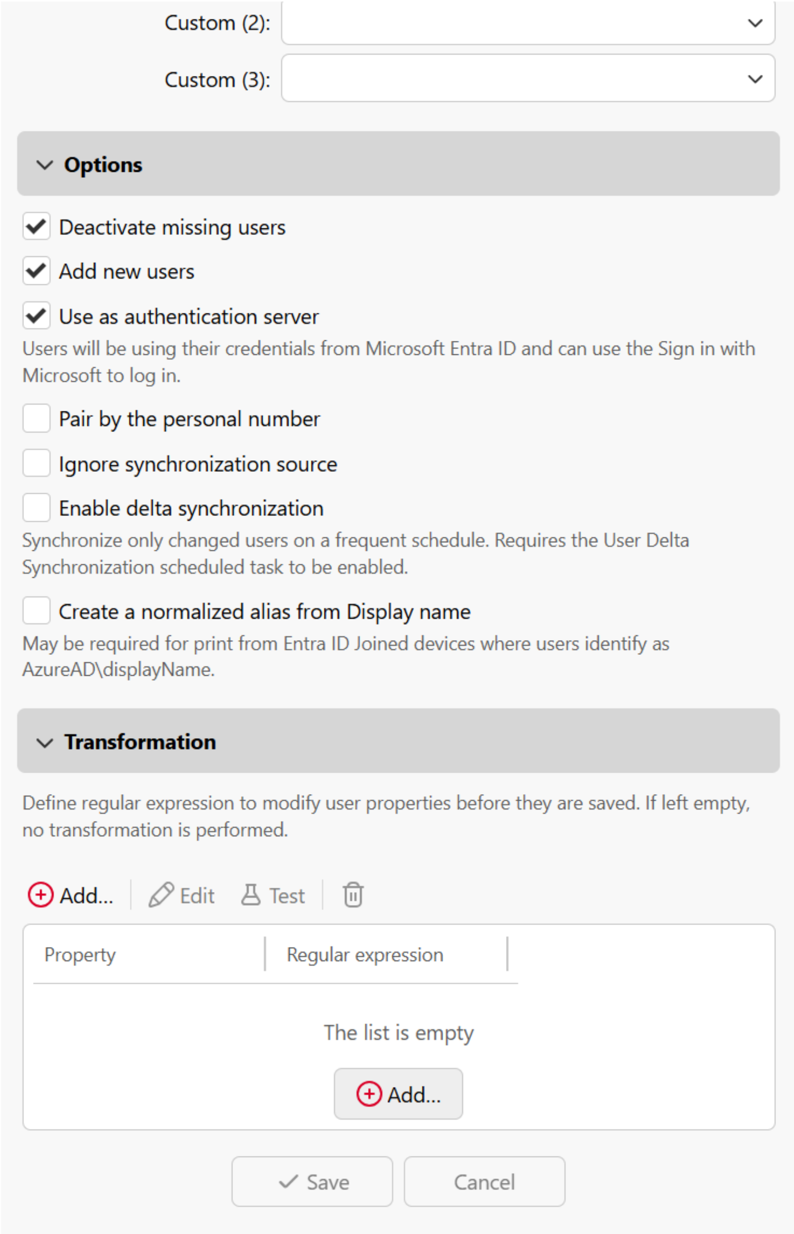
This alias is added in addition to any aliases configured through the property mappings.

> **Limitation**
> If multiple synchronized users have the same display name, the normalized alias can be assigned only to the first matching user. In this case, MyQ cannot reliably distinguish the users from the concatenated name supplied with the print job.

Transformation

Regex transformation rules can be applied to user attributes during sync to parse or reformat values before they are stored in MyQ.





Groups Tab

The **Groups** tab controls how Entra group memberships are represented in MyQ. It does **not** determine which users are imported. User selection is configured separately, on the **Users Tab** in **Users to import**.

Synchronization Type

Select how MyQ handles changes to group membership:

- **Full synchronization**: MyQ group membership follows Entra ID. Users are added to and removed from groups to match the source.
- **Synchronize if not empty:** synchronize group membership while preventing a user from being left without any group membership.
- **Add new**: add memberships found in Entra ID, but do not remove existing MyQ memberships when users are later removed from the corresponding Entra group.

Select Groups

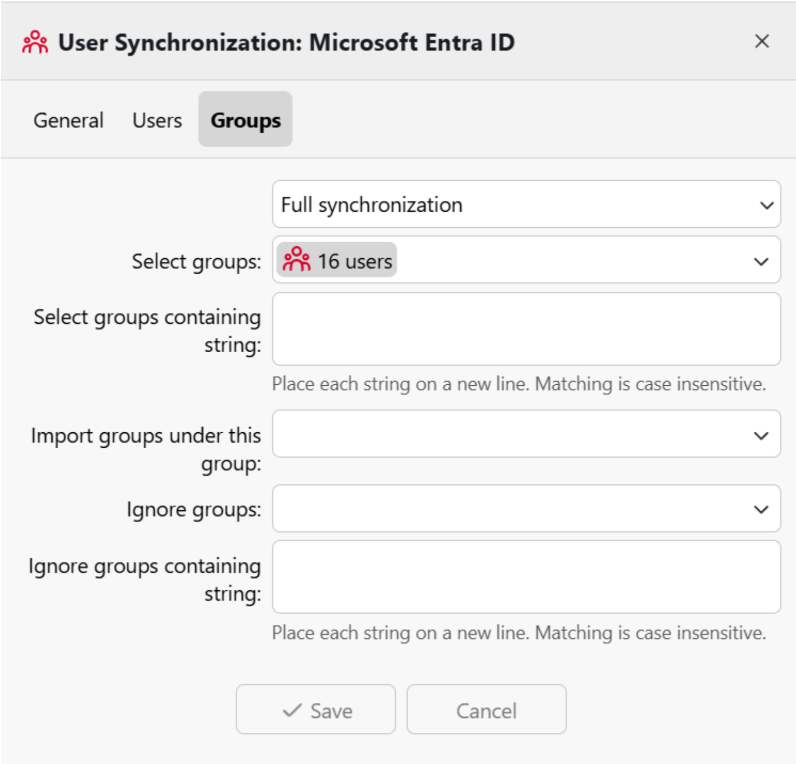
Use the group filters to determine which Entra group memberships should be created in MyQ:

- **Select groups:** select individual Entra groups.
- **Select groups containing string**: include groups whose names match the specified strings.
- **Import groups under this group:** place synchronized groups beneath an existing MyQ parent group.
- **Ignore groups:** exclude selected groups.
- **Ignore groups containing string:** exclude groups whose names contain specified strings.

User Selection and Group Synchronization

The groups used to select **which users are synchronized** do not have to be the same groups whose memberships are created in MyQ.

> Example – assume Entra ID contains:
>
> - **All students -** 1,500 users
> - **Class1A** - 1,000 users
> - **Class1B -** 500 users
>
> To synchronize all students but create only the `Class1B` membership in MyQ:
>
> 1. On the **Users** tab, select **Users from selected groups** and select `All students`.
> 2. On the **Groups** tab, select only `Class1B`.
>
> All 1,500 users are synchronized, but only the 500 members of `Class1B` receive that group membership in MyQ.
> This allows the **user synchronization scope** and the **MyQ group structure** to be controlled independently.



Delta Synchronization

Delta synchronization is an incremental mode that supplements the regular full synchronization. Instead of re-reading the entire Entra ID directory, each delta run asks Microsoft Entra ID only for what has changed since the previous run. Because very little data is transferred, the delta task can run every few minutes, so changes in Entra ID reach MyQ much faster than with a daily full sync alone.

Delta synchronization does not replace full synchronization. The regular full synchronization continues to run on its own schedule (typically daily) and acts as a safety net that reconciles anything the delta runs could not cover.

> Enabling the checkbox alone does not trigger an immediate delta run. Changes are picked up when the User Delta Synchronization scheduled task next runs.

Run the Synchronization

To run synchronization immediately, go to **MyQ > Settings > User Synchronization**, select the source, and click **Synchronize now**. If configured correctly, synced users and groups appear under **MyQ > Users**.

To synchronize automatically on a schedule, go to **MyQ > Settings > Task Scheduler** and configure the User Synchronization task.

Synchronize Multiple Entra Tenants

To synchronize users from multiple Microsoft Entra tenants, create a separate Entra connection and synchronization source for each tenant. Give each connection and synchronization source a clear, unique name so that administrators can identify the corresponding tenant.

Each source can have its own:

- synchronization scope
- property mappings
- group configuration
- user lifecycle options
- authentication settings

On-Premises Identity for Hybrid Entra ID Users

In hybrid environments where Entra users have corresponding on-premises Active Directory identities, MyQ automatically imports the following attributes when they are available:

Entra attribute	MyQ property
`onPremisesSamAccountName`	On-premises username
`onPremisesDomainName`	On-premises domain

No additional attribute mapping is required.

The values are available in the user's **Advanced** properties. If they are edited manually, the next Entra synchronization overwrites the manual values.

If either attribute is unavailable for a user, MyQ records this in the synchronization log.

On-Premises Windows Identity

When both on-premises attributes are available, MyQ can construct a Windows identity for operations that must be performed as the user's on-premises account.

The NetBIOS domain is derived from the first label of the synchronized DNS domain:

On-premises identity	Result
Domain `acme.com`, user `smith`	`acme\smith`
Domain `abc.alphabet.com`, user `smith`	`abc\smith`

MyQ uses this identity for supported on-premises file operations that are configured to run as the logged-in user.

If MyQ cannot construct the on-premises identity:

- if the **On-premises domain** is unavailable, MyQ falls back to authentication-server domain resolution;
- if the **On-premises username** is unavailable, MyQ falls back to the user's MyQ username.

A warning is written to the log when a fallback is used.

Cloud-only Entra users without these attributes are unaffected.

See also:

- (v2) User Synchronization
- (v2) Manual App Registrations
- Connect to Microsoft Entra ID (Graph API) (see page 151)
- Run and Schedule User Synchronization (see page 249)
- Transform User Data with RegEx (see page 246)

10.7.6 Synchronize Users from CSV

MyQ X can import and synchronize users from a CSV file.

Guidance on when to use this source is provided in the Deployment guide. See (v2) User Synchronization.

Prerequisites

- A CSV file accessible from the MyQ server, formatted according to the syntax described in this article.
- If authenticating users against an external server rather than the MyQ database, an LDAP or RADIUS authentication server configured in MyQ at **MyQ > Settings > Authentication Servers**.

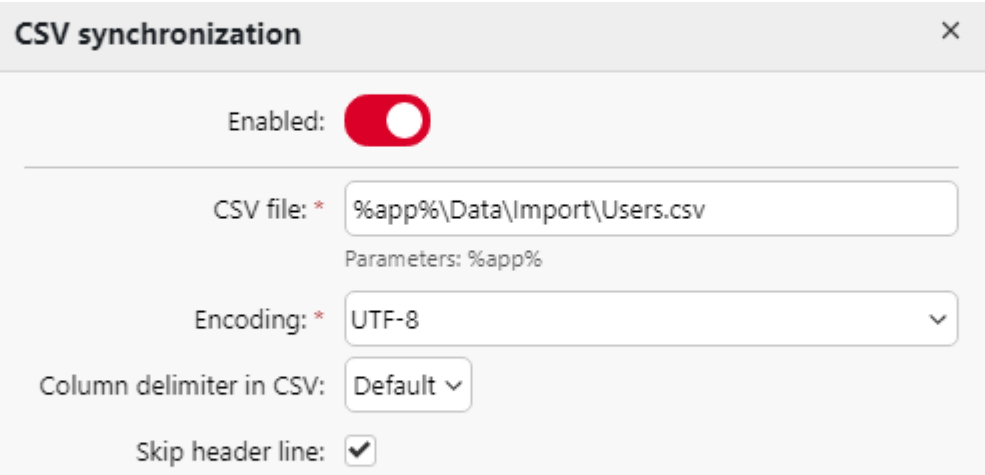
Key Considerations

CSV is not a live directory. Unlike LDAP or Entra ID synchronization, CSV sync reflects only the contents of the file at the time the sync runs. If users are added or removed from the organization, the CSV file must be updated manually before the next sync.

Column order matters only when there is no header row. By default, MyQ reads column names from the first row of the CSV and maps them regardless of order. If the **No header line** option is enabled, columns are mapped by their position in the file, in the order listed in the CSV File Syntax table below.

A sample CSV file is available at `C:\ProgramData\MyQ\Data\Import\Users_example.csv`. Populate it with your data and import it directly, or use it as a formatting reference.

Create a CSV Synchronization Source



1. Go to **MyQ > Settings > User Synchronization** and click **+Add**.
2. Select **Add CSV source**. The CSV synchronization properties panel opens.
3. Set the path to the CSV file in the **CSV file** field and configure the synchronization options.
4. Click **Save**.

Configuration Options

Setting	Description
Enabled	Enable or disable this synchronization source.
CSV file	Path to the CSV file on the MyQ server. Use `%app%` as a parameter for the MyQ application directory, for example `%app%\Data\Import\Users.csv`.
Encoding	Character encoding of the CSV file. The default depends on the OS settings of the computer where you access the MyQ Web Interface.
Column delimiter in CSV	Delimiter used in the CSV file. If set to **Default**, MyQ uses the delimiter configured on the General settings tab.
No header line	When disabled (default), the first row is read as a header row and columns are mapped by name. When enabled, the CSV must contain no header row and columns are mapped by position.
Import groups under this group	Places all imported groups as children of an existing MyQ group.
Synchronization source	Assigns a custom source name to users imported from this file. Useful when using CSV to update users originally imported from an LDAP source – set this to match the LDAP source name, or enable Ignore synchronization source.
Ignore synchronization source	When enabled, this source considers all users in MyQ regardless of which source imported them. When disabled, the source only updates users it originally imported.
Use authentication server	Authenticates imported users against an LDAP or RADIUS server rather than the MyQ database.
Authentication server	The LDAP or RADIUS server to use for authentication when Use authentication server is enabled.

Setting	Description
Deactivate missing users	Deactivates users imported from this source who are no longer present in the CSV file. Combine with Ignore synchronization source to also deactivate users from other sources.
Add new users	Imports new users from the CSV file. If disabled, only existing MyQ accounts are updated.
Pair users by personal number	Matches users by personal number rather than username during re-sync. Useful when updating users whose usernames will change – for example, during an AD-to-Entra ID migration.
Convert user name to lowercase	Prevents duplicate accounts caused by case differences in usernames.
Cards	Sync mode for card values: **Do not synchronize**, **Full synchronization**, **Synchronize if not empty** (default), or **Add new**.
PIN	Sync mode for PIN values: same options as Cards.
Groups	Sync mode for group memberships: same options as Cards.
Delegates	Sync mode for delegate assignments: same options as Cards.

CSV File Syntax

Column names are case-sensitive. Columns can appear in any order when a header row is present. Simple values (single words, plain numbers) can be written as-is; values containing spaces, commas, or special characters must be enclosed in double quotation marks.

Column	Required	Description
`FULLNAME`	Yes	User's full name. Enclose in double quotes, for example `"Thomas Pineapple"`.
`USERNAME_ALIASES`	Yes	Login name and optional aliases. The login should match the user's domain login name. Separate multiple aliases with commas, for example `"Tom,Tommy,Apple"`.
`EMAIL`	No	User's primary email address, for example `"t.pineapple@domain.com"`.
`CARDS`	No	ID card number in the format read by the card reader, for example `7E9700C9`.
`GROUPS`	No	Group or group tree branch. Separate levels with vertical bars and multiple groups with commas, for example `"Activities
`CODE`	No	Personal number. Must be unique per user. Used for pairing users across sync sources.
`SCANSTORAGE`	No	Folder path or email address for scan delivery, for example `"\\Users\Tommy"`.
`PIN`	No	One or more PINs. Must be in hashed MD5 format, for example `14BFA6BB14875E4`.
`MANAGED_GROUPS`	No	Groups the user manages. Use the same path syntax as GROUPS. For example, `"Activities
`AUTHSERVER`	No	Domain for user authentication, for example `"testAD.local"`.
`PHONE`	No	User's phone number, for example `080008020`.
`LANG`	No	Default language abbreviation, for example `en`.

Column	Required	Description
`PWD`	No	MyQ password in hashed MD5 format, for example `18BFA6BB14875E8`. Leave empty if using an external authentication server.
`EXTID`	No	Internal MyQ parameter. Must be left empty.
`DELEGATES`	No	Delegates who can print on behalf of this user. Separate multiple delegates with commas, for example `"Carol,Kohei,Eliot"`.
`ALTERNATEEMAILS`	No	Comma-separated list of alternate email addresses.
`DEPARTMENT`	No	User's department, for example `Marketing`.
`CUSTOM1`	No	Custom field 1 from the user profile.
`CUSTOM2`	No	Custom field 2 from the user profile.
`CUSTOM3`	No	Custom field 3 from the user profile.

Example CSV:

```
"FULLNAME";"USERNAME_ALIASES";"EMAIL";"CARDS";"GROUPS";"CODE";"SCANSTORAGE
";"PIN";"MANAGED_GROUPS";"AUTHSERVER";"PHONE";"LANG";"PWD";"EXTID";"DELEGA
TES"
"Thomas
Pineapple";"Tom,Tommy,Apple";"t.pineapple@domain.com";7E9700C9;"Activities
|Outdoor|Swimming,Activities|Outdoor|Birdwatching";22212;"\
\Users\Tomy";14BFA6BB14875E4;Birdwatching;testAD.local;080008020;en;18BFA6
BB14875E8;;"Carol,Kohei,Eliot"
```

Run and Schedule Synchronization

To run synchronization immediately, go to **MyQ > Settings > User Synchronization**, select the source, and click **Synchronize now**. If configured correctly, synced users and groups appear under **MyQ > Users**.

To synchronize automatically on a schedule, go to **MyQ > Settings > Task Scheduler** and configure the User Synchronization task.

See also:

- User Synchronization (see page 199)
- Authentication Servers Settings (see page 158)
- Run and Schedule User Synchronization (see page 249)

10.7.7 Authenticate Users from LDAP or RADIUS

This page covers authenticating user credentials against LDAP or RADIUS servers. For information about using your own connector via API, see (10.3) External Authentication via API Connector.

With these external authentication 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.

This authentication method requires an online connection to your LDAP or RADIUS server.

Enable Authentication via LDAP or RADIUS Server

1. Register your LDAP or RADIUS authentication server. Do this in **MyQ > Settings > Authentication Servers**.
2. Select to use your server for user authentication. You can do this either automatically during the user import from an LDAP server or a CSV file, or manually on the properties panels of individual users.

Set Authentication Server During User Import from CSV

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.

Set Authentication Server During User Import from an LDAP Server

During the user import from an LDAP server, you can select the **Use authentication server option**, to use the current synchronization source server for users authentication.

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.

Set External Authentication Server Manually in User Properties

To manually select the external authentication option:

1. Open the **Users** main tab and double-click the user. The user properties panel opens.
2. 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 click **Save.**

See also:

- Authentication Servers Settings (see page 158)
- Synchronize Users from CSV (see page 239)
- Synchronize Users from LDAP (see page 204)
- (10.3) External Authentication via API Connector

10.7.8 Transform User Data with RegEx

Regular expressions provide a powerful way to manipulate user data during synchronization. Administrators can use this feature to ensure that the imported data into MyQ is precisely in the format and content they desire. Always test your regular expressions before applying them to real data to avoid unexpected results.

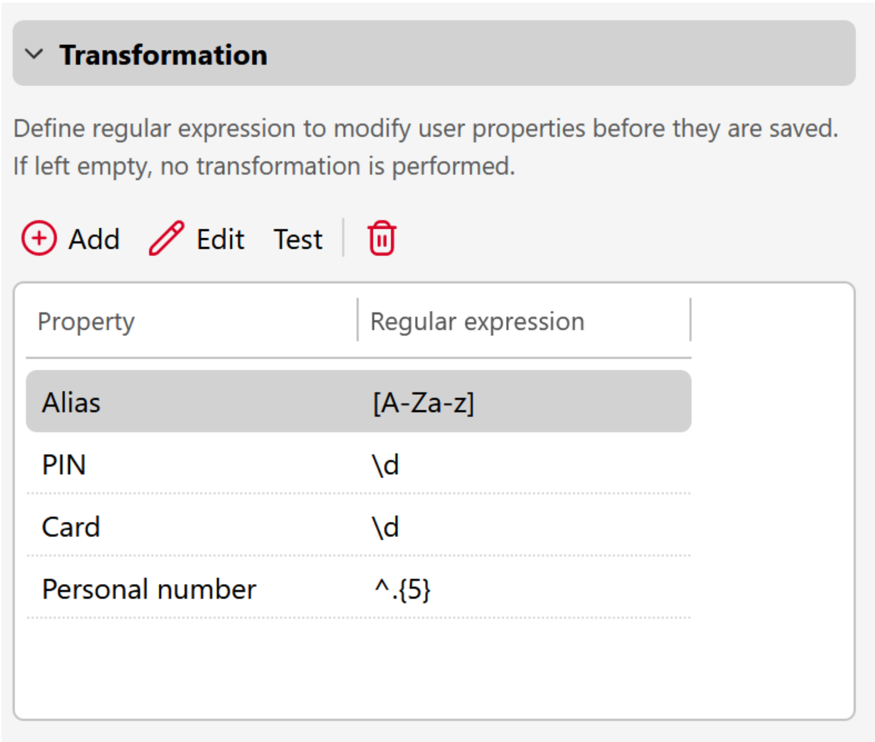
This feature is supported for LDAP and Entra ID synchronization sources only.

Use RegEx Transformation for User Synchronization:

1. Go to **MyQ**, **Settings**, **User Synchronization**.

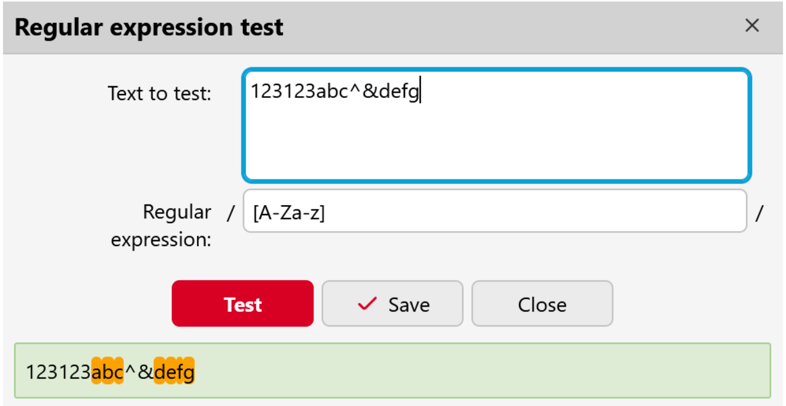
   Depending on your setup, double-click either on your LDAP or Entra ID Synchronization for the synchronization settings to open on the right.

2. In the **Users** tab, scroll down and expand **Transformation**.



3. You can add and configure the following supported user properties:
   - Alias
   - Card
   - PIN
   - Personal number
   - Click **Add** and for each property, input your desired regular expression in the provided field to modify the respective user property.

4. Click **Test** to check your regular expression**.** A regular expression test dialogue opens.
   - Type a string you want to test in **Text to test.**
   - Enter your regular expression.
   - Click **Test**.
     The post-transformation output appears. Use this feature to help ensure that the expression works as intended before applying it to actual user data.



RegEx Examples

Scenario: Remove any non-digit characters from PINs.

- **RegEx**: `\d`

If the PIN is '12a3b4', the transformed value will be '1234'.

If the source string contains no digit characters, the output value will be empty. Only characters matched by RegEx will be copied to the output.

Scenario: Remove all characters except the alphabetical ones from card numbers.

- **RegEx**: `[A-Za-z]`

For a Card number '1234-5678', this will transform it to '12345678'.

If the source string contains no alphabetical characters, the output value will be empty. Only characters matched by RegEx will be copied to the output.

Scenario: Only keep the first 5 characters of the personal number.

- **RegEx**: `^.{5}`

For a Personal number '1234567890', this will transform it to '12345'.

If the source string's length is less than 5 characters, the output value will be empty. Only characters matched by RegEx will be copied to the output.

Scenario: Only keep the last 3 characters of the personal number.

- **RegEx**: `.{3}$`

For a Personal number '1234567890', this will transform it to '890'.

If the source string's length is less than 3 characters, the output value will be empty. Only characters matched by RegEx will be copied to the output.

10.7.9 Run and Schedule User Synchronization

User synchronization in MyQ X does not run continuously. It runs on demand or on a schedule that you configure. This page describes how to trigger a synchronization run manually and how to set up automatic scheduled runs.

Run Synchronization Manually

1. Go to **Settings > User Synchronization**.
2. Select one or more synchronization sources from the list.
3. Click **Synchronize now** on the toolbar.

If another synchronization is already running, the **Synchronize now** button is unavailable and an error message is displayed. Wait for the running sync to complete before starting another.

The **Synchronization Results** panel opens automatically and displays the operation log in real time. The log tail follows automatically when the panel is scrolled to the bottom. A spinner at the bottom of the log indicates synchronization is in progress.

These options are available:

- **Cancel**: Stops the synchronization. The process may take a moment to halt after clicking.
- **Save**: Downloads the synchronization log as a file.

Schedule Synchronization

To run synchronization automatically on a recurring schedule, configure a task in the Task Scheduler.

1. Go to **Settings > Task Scheduler**.
2. Locate or create the **User Synchronization** task.
3. Set the schedule – frequency, time, and which sync sources to include.

For most environments, a daily scheduled sync is sufficient. If Entra ID is your single authoritative user source and you have **Deactivate missing users** and **Add new users** enabled, ensure the schedule runs frequently enough that joiners and leavers are reflected in MyQ within your acceptable time window.

If you have enabled **delta synchronization** on an Entra ID (Microsoft Graph) sync source, a second scheduled task - **User Delta Synchronization** - runs those sources incrementally on a frequent interval (every 10 minutes by default). This task processes only changes that occurred since the last delta run and keeps MyQ current with Entra ID between full synchronization runs.

If you use CSV as a supplementary sync source alongside an LDAP or Entra ID source, schedule the CSV sync to run after the primary sync completes – typically 30 minutes later – so that it operates on the most current user data.

Reading the Synchronization Log

The synchronization log records the outcome for every user and group processed during the run. Key log entries to look for:

Entry	Meaning
`created`	A new user or group was added to MyQ.
`updated`	An existing user or group was updated.
`deactivated`	A user was deactivated because they were no longer present in the source (requires Deactivate missing users enabled).
`Match via LOGIN`	An existing user was matched and updated by username.
`Match via PERSONAL NUMBER`	An existing user was matched and updated by personal number (requires Pair by personal number enabled).
`Job discarded. User "x" not found.`	A print job arrived for a username that does not exist in MyQ. The quoted value is what the sync must place in the username or alias field for jobs to authenticate.

If a sync completes without error but the user count is lower than expected, check whether query limits apply – this is particularly common with OpenLDAP sources. By default, OpenLDAP limits both the number of entries returned and the maximum time per query (500 entries, one hour). For larger installations, increase these limits in your OpenLDAP server configuration – otherwise the synchronization returns incomplete results.

See also: Task Scheduler Settings (see page 141)

10.8 Data Privacy and Anonymization

Except for the data shown in MyQ reports, everything stored in MyQ is necessary for the functioning of the system. The data can be accessed only by people with administrator rights in MyQ and are not processed by the system or disclosed to third parties. As to the information shown in MyQ reports, it is fully under the control of the MyQ administrator, who can provide certain users with rights to view information related to other users or groups.

MyQ users can access their personal data within the MyQ system and upon their request, the MyQ administrator can erase the data by anonymizing the user. The following sections show how the users can access the data and how to anonymize the users.

These options are closely related to the General Data Protection Regulation (GDPR), which aims to protect the personal data of EU citizens. For more information about how the GDPR is implemented in MyQ, contact MyQ Support.

10.8.1 Providing Users with their Personal Data

On their MyQ Web accounts, MyQ users can see the **User profile** widget with the personal information stored in MyQ.

On their Web account, MyQ users can generate reports related to their activity within MyQ, such as printing, copying and scanning to see what information is available in these reports.

Users may also contact the MyQ administrator with a request to provide them with the data.

The MyQ administrator can create a custom dashboard message informing all users about the data protection options and include the admin email contact via the **%admin%** parameter.

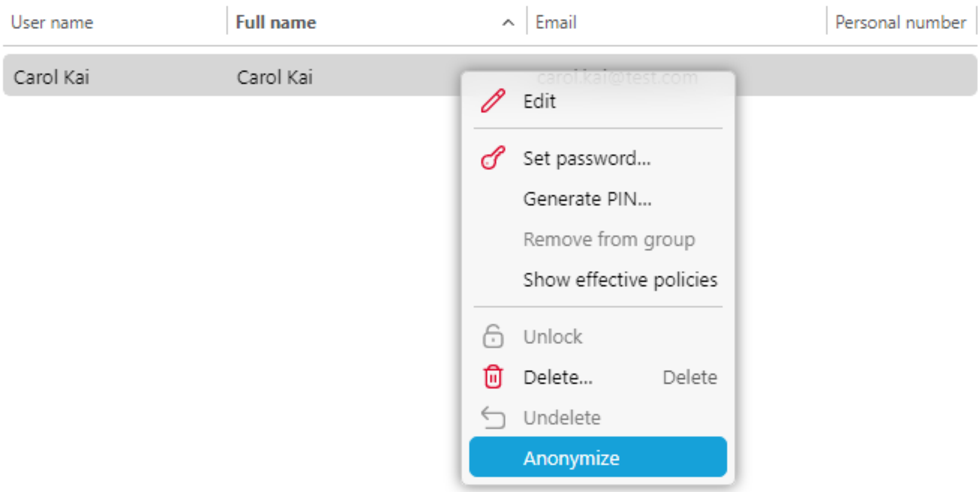
10.8.2 Anonymizing Users

After the anonymization, the user is completely removed from the system and replaced by a randomly generated name in all of the relevant MyQ reports.

After a user is anonymized, all of their personal data (including username and email) are permanently erased from the system and cannot be retrieved.

To anonymize a user:

On the **Users** main tab of the MyQ Web Interface, select the users that you want to anonymize, then click **Actions** (or select the users, and then right-click any of them), and finally click **Anonymize**.



See also: Reports (see page 274)

11 Accounting

MyQ X offers three accounting mechanisms for tracking, limiting, and charging for print, copy, and scan services: credit, quotas, and project accounting. They can be used independently or in combination, and all three build on price lists, which define the cost of each device operation.

11.1 Credit Accounting

With credit accounting, users can print, copy, and scan only if they have sufficient credit on their MyQ account. Printing is allowed only for jobs that do not exceed the current balance. Credit can be recharged by the administrator (or authorized users) on the MyQ Web Interface, or by users themselves via vouchers, recharging terminals, the MyQ mobile application, or third-party payment providers such as PayPal, Stripe, GP webpay, and SnapScan.

See Credit (see page 254).

11.2 Quota Accounting

Quotas set limits on the usage of print services over a defined period. A quota can limit the number of printed, copied, or scanned pages, or set an overall cost limit based on price list prices. Users receive an email warning when they approach their limit, and further operations can be disabled once the limit is reached. Quotas can be applied to individual users, group members, or accounting groups, and can be temporarily boosted when needed.

See (10.3) Quotas.

11.3 Project Accounting

Project accounting lets users assign print, copy, and scan jobs to particular projects, distributing costs among projects for internal charging. It also serves as an independent level of accounting alongside devices, users, and groups. Projects can be created manually or imported from CSV files, and jobs can be assigned in the web interface, embedded terminals and other client applications.

See (10.3) Projects.

11.4 Price Lists

Price lists assess the price of each printing device operation and are attached to devices through configuration profiles. They are required for all monetary accounting: credit, cost-based quotas, and project cost distribution. Discounts (or price increases) can be applied per user or group on top of any price list.

See (10.3) Using Price Lists.

11.5 Common Prerequisites

Before setting up any accounting method, check the following:

- **Job parser**: Both credit and quota accounting require the Job parser to obtain print job metadata (number of pages, color, etc.). To enable it, go to **Settings > Jobs**.
- **Currency**: Monetary accounting and all payment providers use the currency set on the General settings tab (**MyQ > Settings > General**). Set the currency before generating vouchers or configuring payment providers.
- **Price lists:** Credit accounting and cost-based quotas require a price list assigned to each device via its configuration profile.

11.6 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 current credit, and copying is terminated after credit is exceeded, although there can be an overflow of a few pages. 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.

11.6.1 Credit Refund

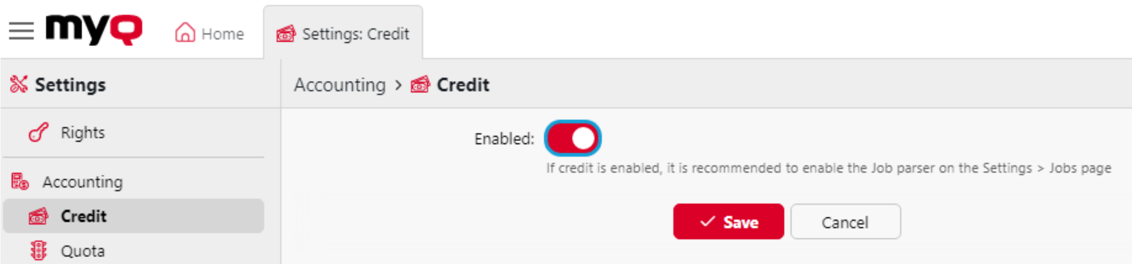
Direct credit refund from MyQ is not supported. If you need to reverse a transaction using any of the supported payment providers, you must then manually adjust the user's credit balance in MyQ. This can be done by users with Administrator and Recharge credit roles.

11.6.2 Activating and Setting Up Credit

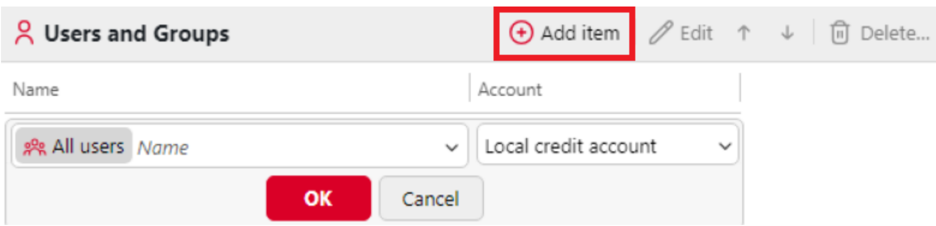
The activation and setup of credit accounting is managed on the **Credit** settings tab (**MyQ > Settings > Credit**).

To set up credit accounting:

Enable credit accounting on the **Credit** settings tab:



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** from the drop-down list.
  - Select an **Account** from the drop-down list. The available options are:
    - Local credit account

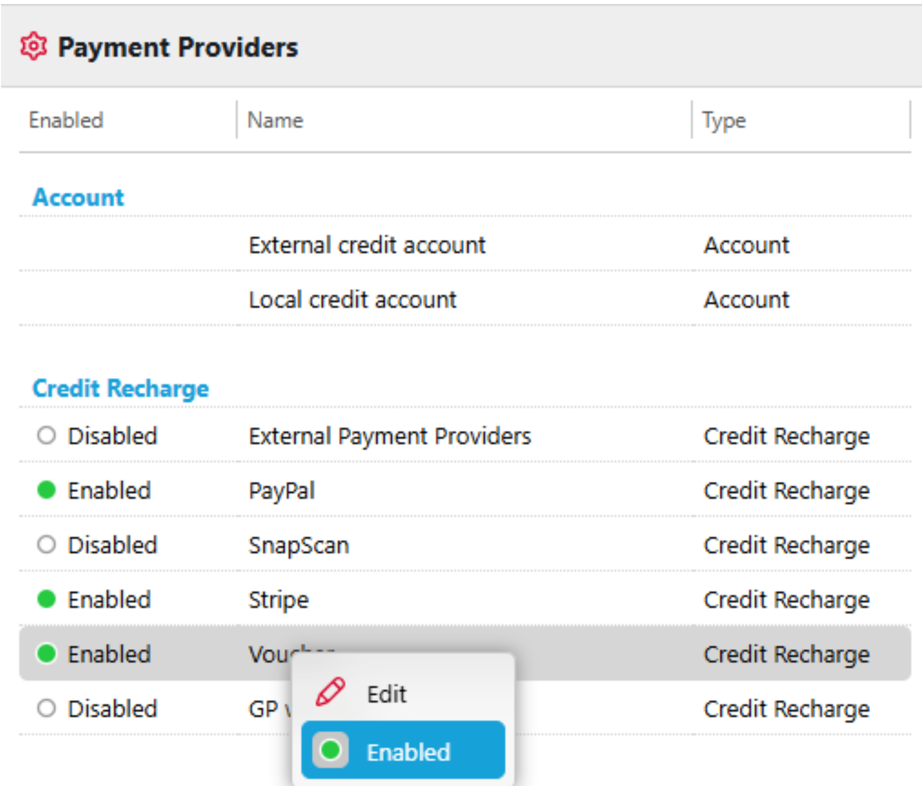
- External credit account
- Click **OK** to save the settings.

Enable/disable payment methods for credit recharge

Available payment methods:

- External Payment Providers
- PayPal
- SnapScan
- Stripe
- 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).



11.6.3 Recharging Credit Manually

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.

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**.

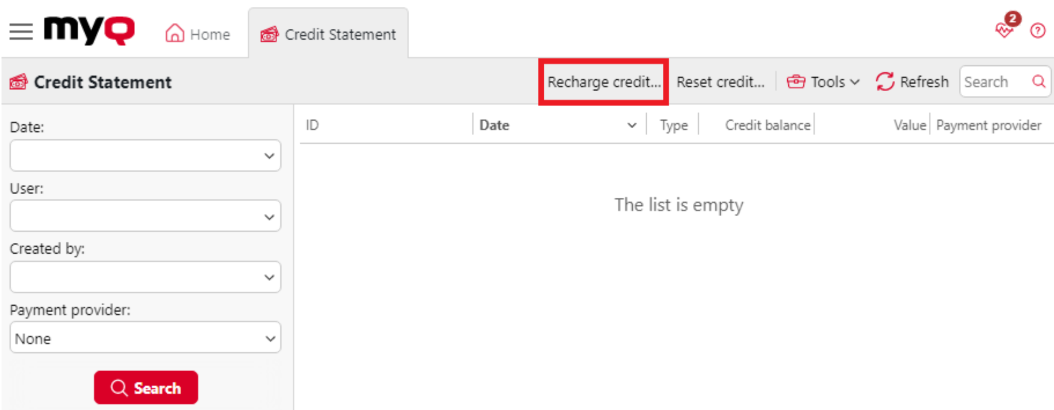
The authorized user can then recharge credit on their MyQ Web interface in the same way as the MyQ administrator.

Recharging Credit on the Credit Statement Tab

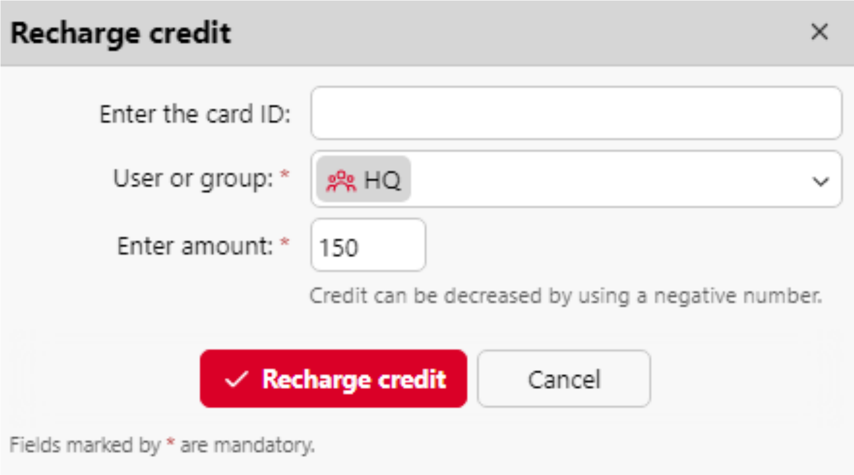
On the **Credit Statement** tab, you can overview the changes in the credit balance of MyQ users, and also recharge credit to users and groups. To open the tab on the MyQ Web administrator interface, go to **MyQ, Credit Statement**.

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**.

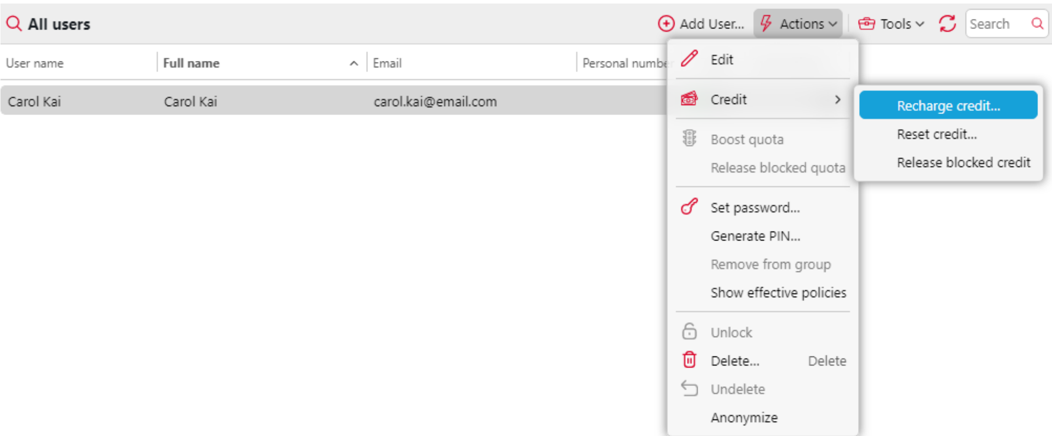


Recharging Credit on the Users Main Tab

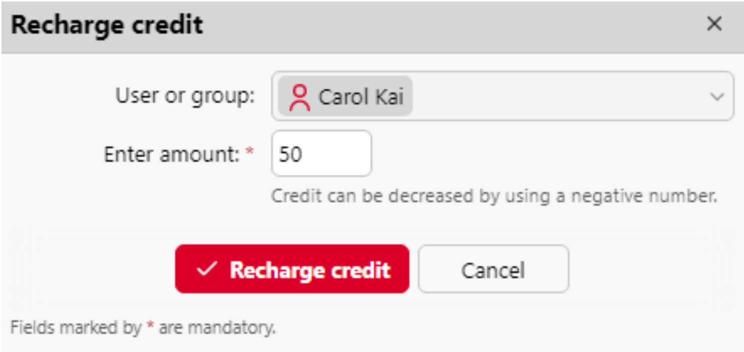
To open the **Users** main tab on the MyQ Web administrator interface, go to **MyQ, Users**.

To recharge credit to selected users:

1. Select the users.
2. Click **Actions**.
3. Hover over **Credit** and click **Recharge credit** in the **Actions** drop-down. The Recharge credit dialog box opens.

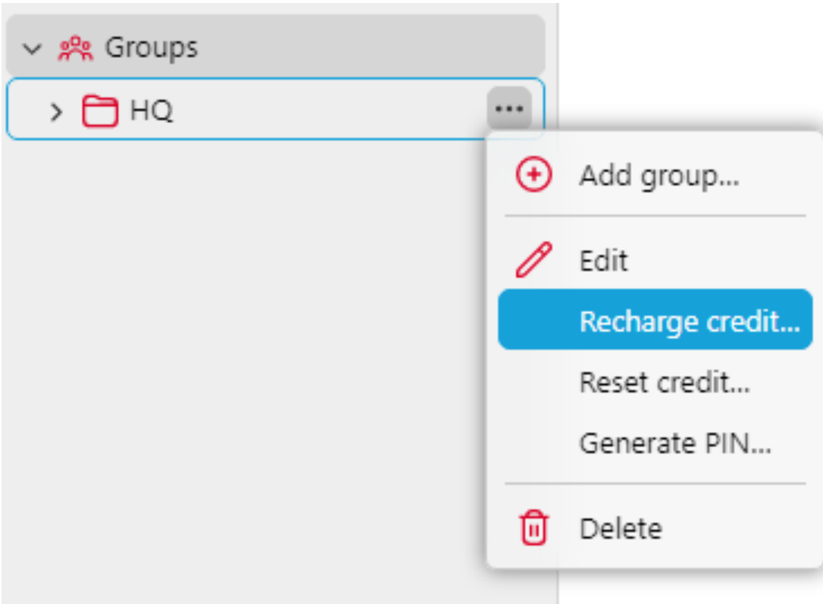


4. **Enter amount** to be recharged, and then click **Recharge credit**. The credit is increased by the specified amount.



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.

11.6.4 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**.

11.6.5 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.

More Information:

- Rights (see page 196)

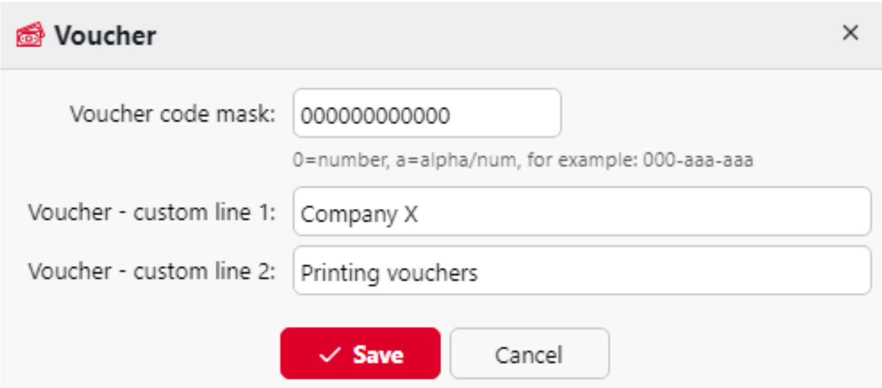
Setting the Voucher Format

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**. Select **Voucher** and mark it as **Enabled**. Then, 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.

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:

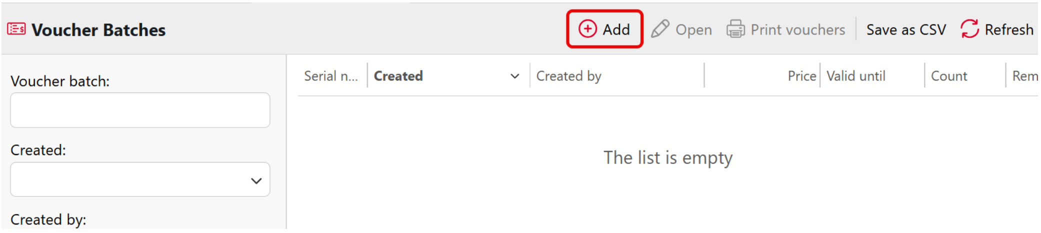
1. On the MyQ Web administrator interface, open the **Personalization** settings tab. (**MyQ, Settings, Personalization**).
2. On the tab, under **Custom application logo**, click **+Add**, browse and upload the file with the logo, and lastly click **Save** at the bottom of the tab. A preview of the new logo is displayed on the tab.

Voucher Batches

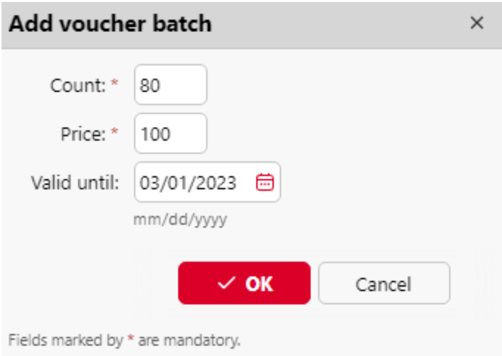
Vouchers can be generated on the **Voucher Batches** tab of the MyQ Web Interface. To open this tab, go to **MyQ, Voucher Batches**.

To generate new vouchers:

1. On the bar at top of the **Voucher Batches** tab, click **+Add**. The Add voucher batch dialog box appears.



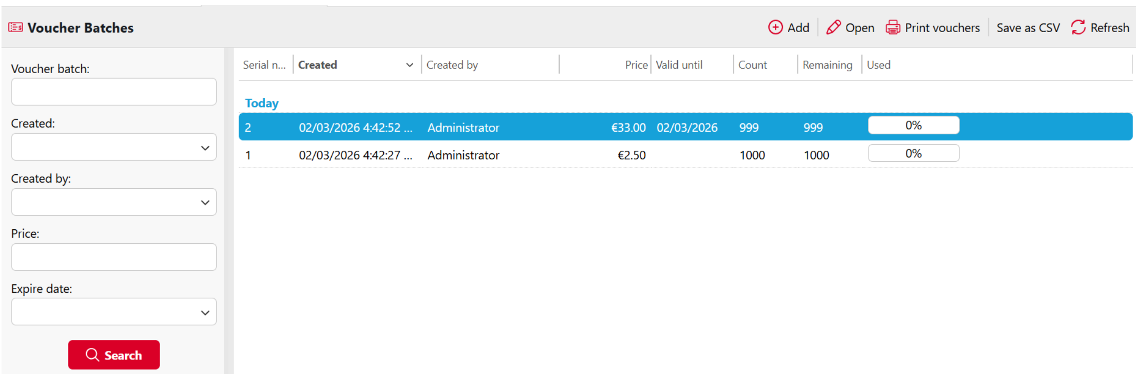
2. In the dialog box, enter the number of vouchers to be generated in the **Count** field, the **Price** of the vouchers, add the validity period in the **Valid until** field, and then click **OK**.



The new voucher batch record is displayed in the voucher batches list. You can overview all of the vouchers by double-clicking a record.

Managing Voucher Batches

Voucher batches can be filtered by serial number, date, creator, price, expiry date, etc. 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.



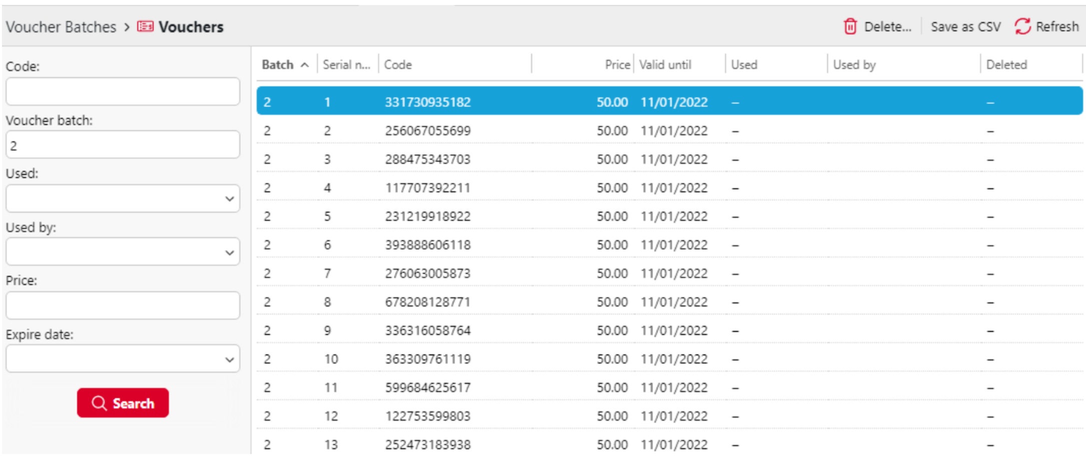
Vouchers Usage Overview

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 as the 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 on 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.



11.6.6 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.

Setting up PayPal Payments

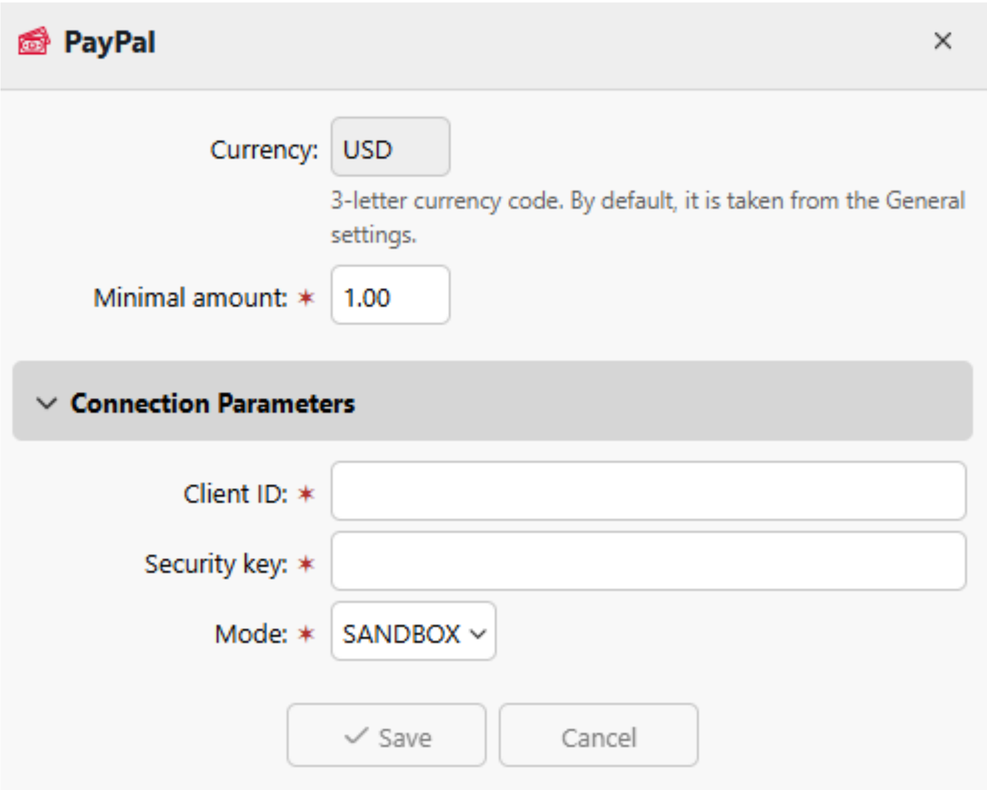
To integrate PayPal with MyQ, you first create a new App in your organization's PayPal Business account. Then you set up PayPal as a payment option in the MyQ server settings.

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.



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**.

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.

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.

Setting up PayPal Payments

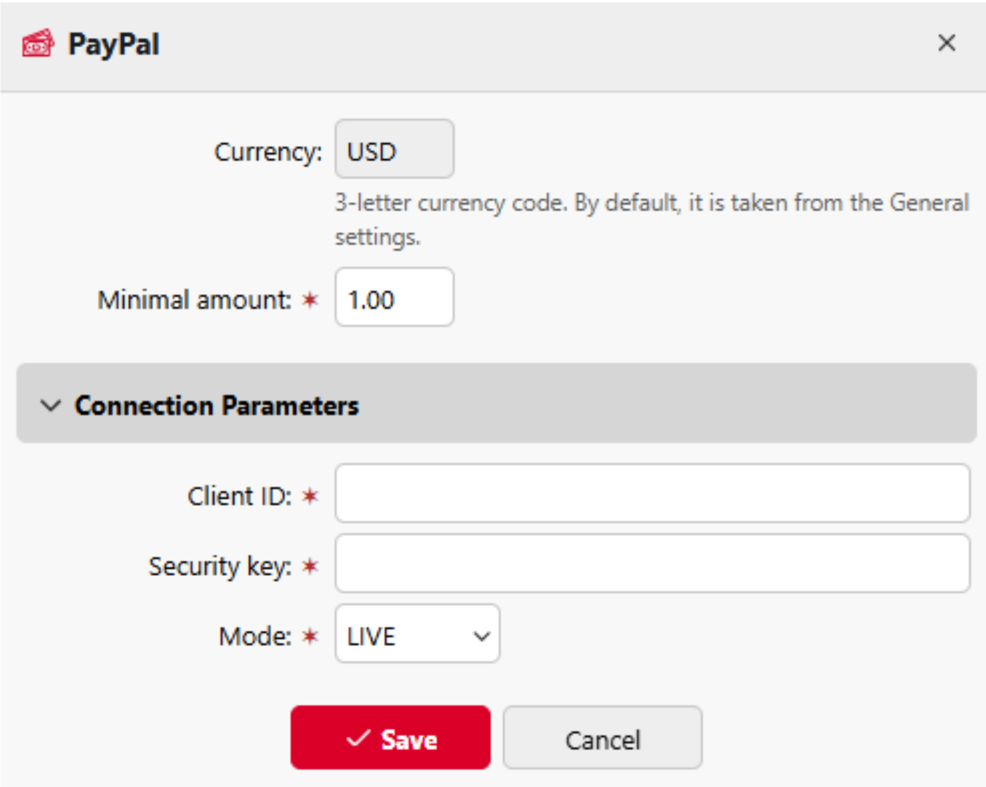
To integrate PayPal with MyQ, you first create a new App in your organization's PayPal Business account. Then you set up PayPal as a payment option in the MyQ server settings.

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.



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**.

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.

11.6.7 Recharging Credit via GP Webpay

The GP webpay payment gate enables customers to directly pay for their credit via a payment card or via a digital wallet.

Setting up GP Webpay

You need to have a GP webpay account, get a public and a private key; the public key has to be uploaded to the GP webpay server, and the private one needs to be uploaded to MyQ. Also, you need to remember/copy the password of the private key. You can either use your own keys (for more information, see https://developers.mygp.global/en/p/webpay/) or use the GP webpay tools to create new ones.

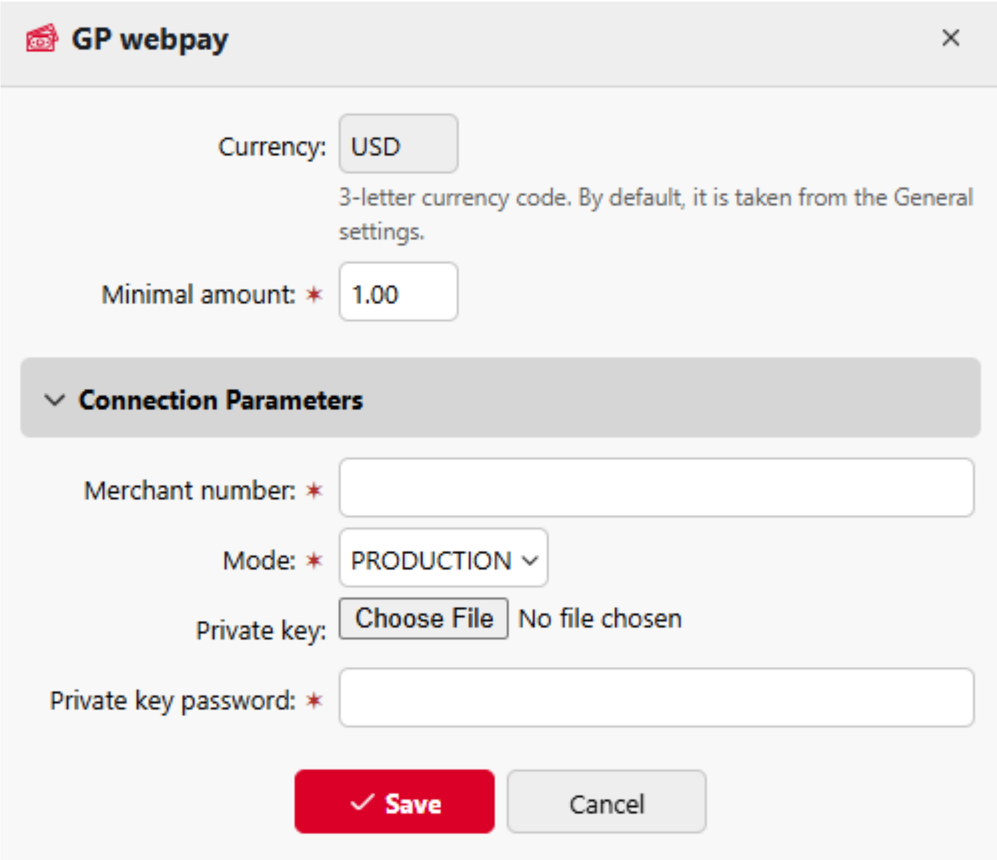
MyQ needs the following data:

- **Merchant number**: The Merchant number can be found on the GP webpay portal, under **Key management**.
- **Private key**: The private key can be generated on the GP webpay portal, under **Key Management**. It can be in the *.key*, *.pem* or *.crt* format.

- **Private key password**: The private key password is the password that is provided to GP webpay during private key generation, or the passphrase used to create the private key manually.

Setting up the GP webpay payment option on the MyQ Web Interface

1. Open the **Credit** settings tab (**MyQ, Settings, Credit**).
2. On the tab, under **Payment providers**, right-click the **GP webpay** payment provider, and then click **Edit** on the shortcut menu. The **GP webpay** 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.
4. Type the **minimal amount** that users will have to pay when they will buy credit.
5. Enter the **Merchant number** of the REST API app into the **Merchant number** text box and set the **MODE** to *PRODUCTION*.
6. Upload the **Private key** from GP webpay (click **Choose File**, select the file, and then click **Open**), enter the **Private key password** provided during generating of the private key, and then click **Save**.

User Credit Recharge

Users will find a **Recharge credit** option on the homepage of the web interface. Clicking opens a dialogue box where the user can select the **GP webpay** payment provider, enter the amount of credit that they want to buy, and then click **Recharge Credit**.

A window with the **GP webpay** payment options opens in the web browser; the rest of the steps correspond to the standard GP webpay payment process.

After the payment is successfully sent to MyQ, the **Payment successful** dialog box appears.

> GP webpay 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.

11.6.8 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.

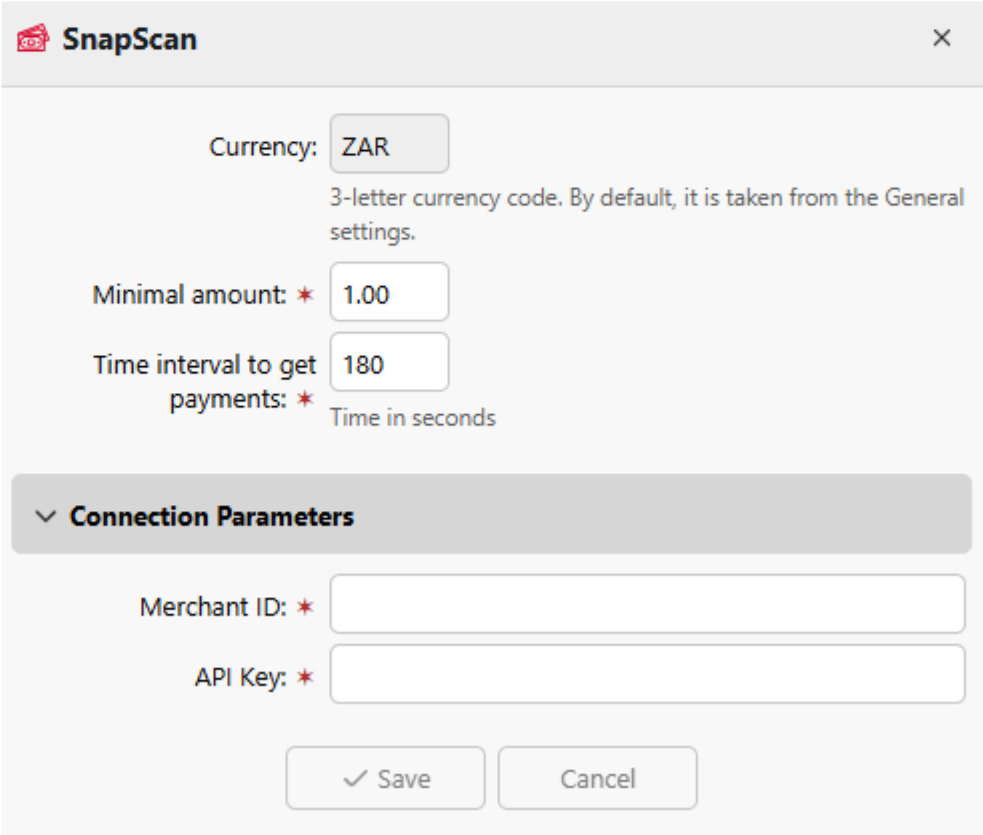
As **SnapScan** is a South African service, users need to use a phone with a South African Mobile number (*+27*) to be able to scan the QR code and pay for the credit.

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.
7. Restart MyQ services using Easy Config for your changes to take effect.

User Credit Recharge

Users will find a **Recharge credit** option on the homepage of the web interface. Clicking opens a dialogue box where the user can 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.

11.6.9 Recharging Credit via Stripe

Stripe is a payment provider that supports a range of payment methods, including credit cards, debit cards, and bank transfers. You configure and manage these from your Stripe dashboard.

With an activated Stripe account, you can allow users to recharge their MyQ credit via Stripe payments directly from the MyQ Web Interface.

To avoid currency conversion fees, ensure that the 3-letter currency code set in **MyQ > Settings > General** is also included among your settlement currencies in Stripe.

Setting up Stripe Payments

To set up Stripe as a payment provider in MyQ, you simply need to enter your Stripe secret key in MyQ. You do not need to create any special product catalog items – payments from MyQ are automatically processed in Stripe as **MyQ Credit.**

While you can use the default Stripe secret key (either for your test or live environments), we recommend generating a unique restricted key for each Print Server instance. Restricted keys are more secure because permissions must be granted explicitly. Using a separate key per instance enables you to revoke or rotate a single key without affecting others, and limits the impact if a key is compromised.

Use a Stripe test key to validate MyQ integration. When you are ready, generate a restricted key from your live Stripe environment and set it in MyQ.

For more information, see the following resources in the Stripe documentation:

- https://docs.stripe.com/get-started
- https://docs.stripe.com/payments/payment-methods/overview
- https://docs.stripe.com/keys

Create a Restricted Key in Stripe

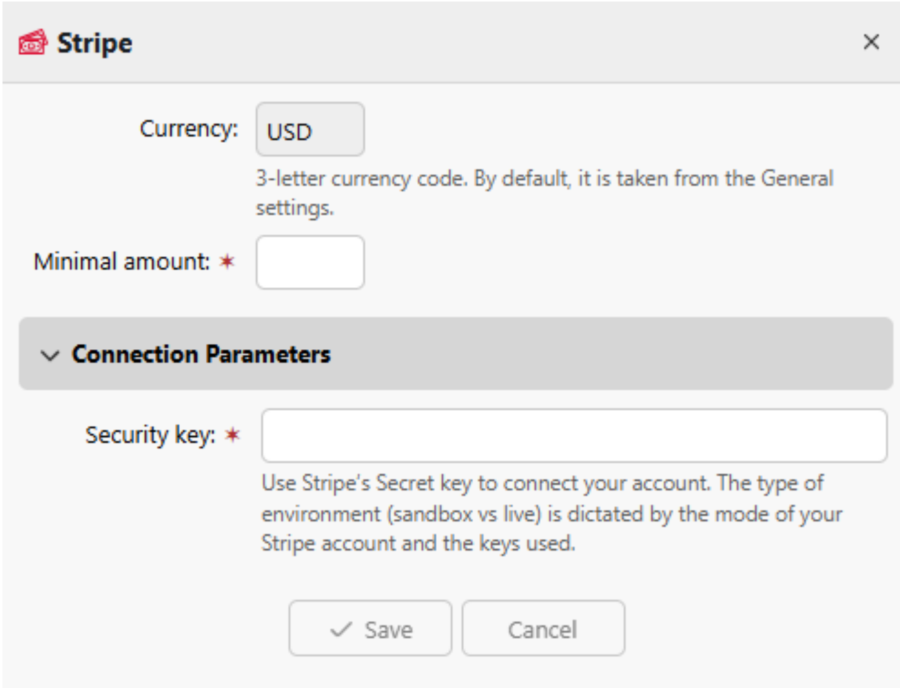
You generate a restricted key in your Stripe Dashboard.

1. Log in to your Stripe account at https://dashboard.stripe.com/ and select the environment that you want to use with MyQ.
2. Go to the **API keys** page in the Developers section of your Stripe Dashboard.
3. In the **Restricted keys** section, click **+ Create restricted key**.
4. Choose **Building your own integration** and click **Continue.**
5. Enter a descriptive **Key name** (for example, “MyQ Integration”).
6. Set the following permissions to `Write`:
   - Payment Intents
   - Checkout Sessions
7. Ensure all other permissions are set to `None`.
8. Click **Create key**.
9. Copy the token for your key.

   You will need this token when you configure Stripe in MyQ.

Configure Stripe in MyQ

1. Log in to the Web UI as an administrator, and go to **Settings > Accounting > Credit**.
2. Under *Payment providers*, double-click **Stripe**.
3. Enter the minimum amount of credit that a user can buy.
4. Enter your Stripe secret key in full (or the token for your restricted key) in the **Security key** field, and click **Save**.



Recharge User Credit with Stripe

To update their credit with Stripe, the user completes these steps in the MyQ Web Interface.

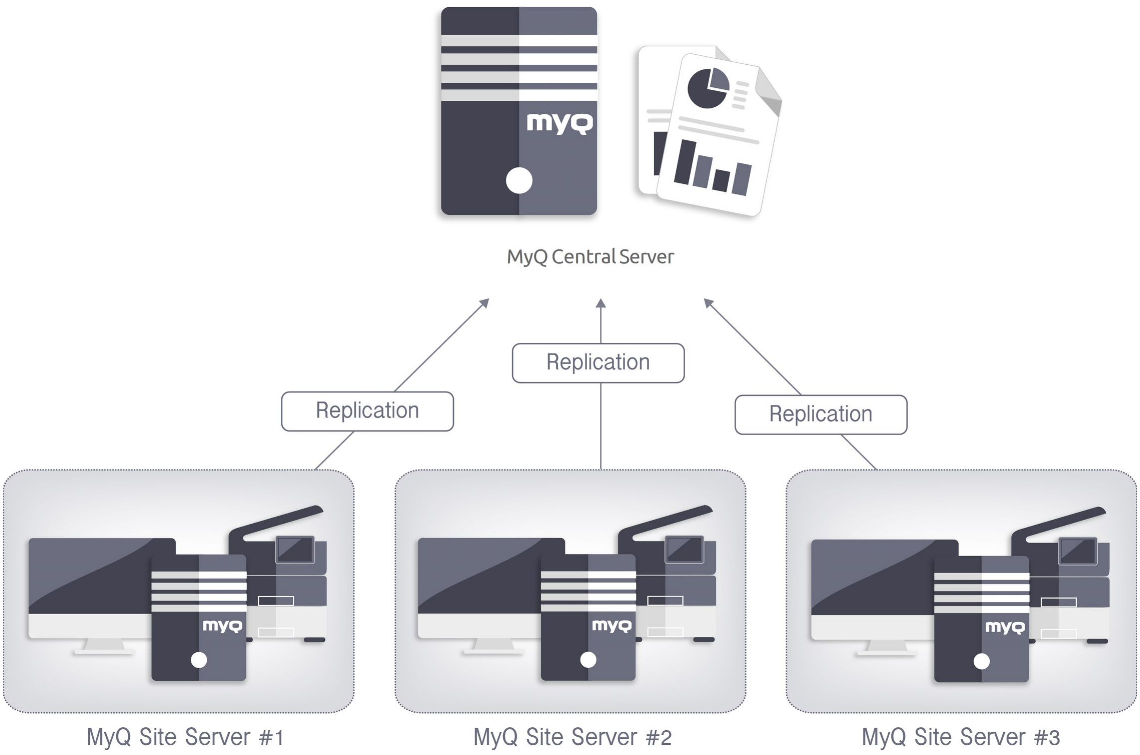
1. Log in to the MyQ Web Interface.
2. Go to **Credit** and click **Recharge Credit**.
3. Select *Stripe* as the payment provider and enter the desired amount of credit to purchase.
4. Click **Recharge Credit**.

   A Stripe checkout window opens, where you complete your payment. After successful payment, you are directed to the confirmation page. The credit will be automatically added to your account.
5. If the new credit balance is not shown, refresh MyQ in your browser.

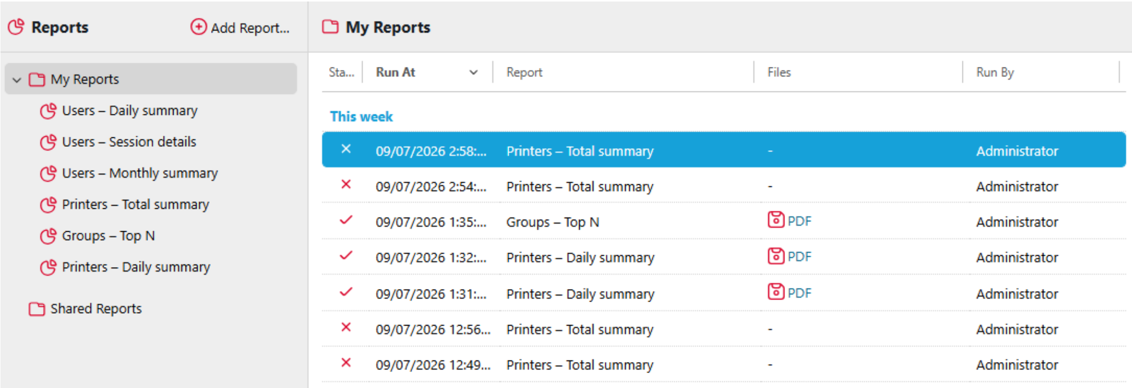
12 Reports

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.



Go to **MyQ > Reports** to generate and view reports with a variety of data concerning your printing environment. The reports can be related to users, printing devices, print jobs, etc.



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.

The default reports 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.

- **Daily summary**
- **Session details**
- **Monthly summary**

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 viewed in the web interface and saved in any of the following formats:

- PDF
- CSV
- XML
- XLSX
- 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 Granting Users 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**.

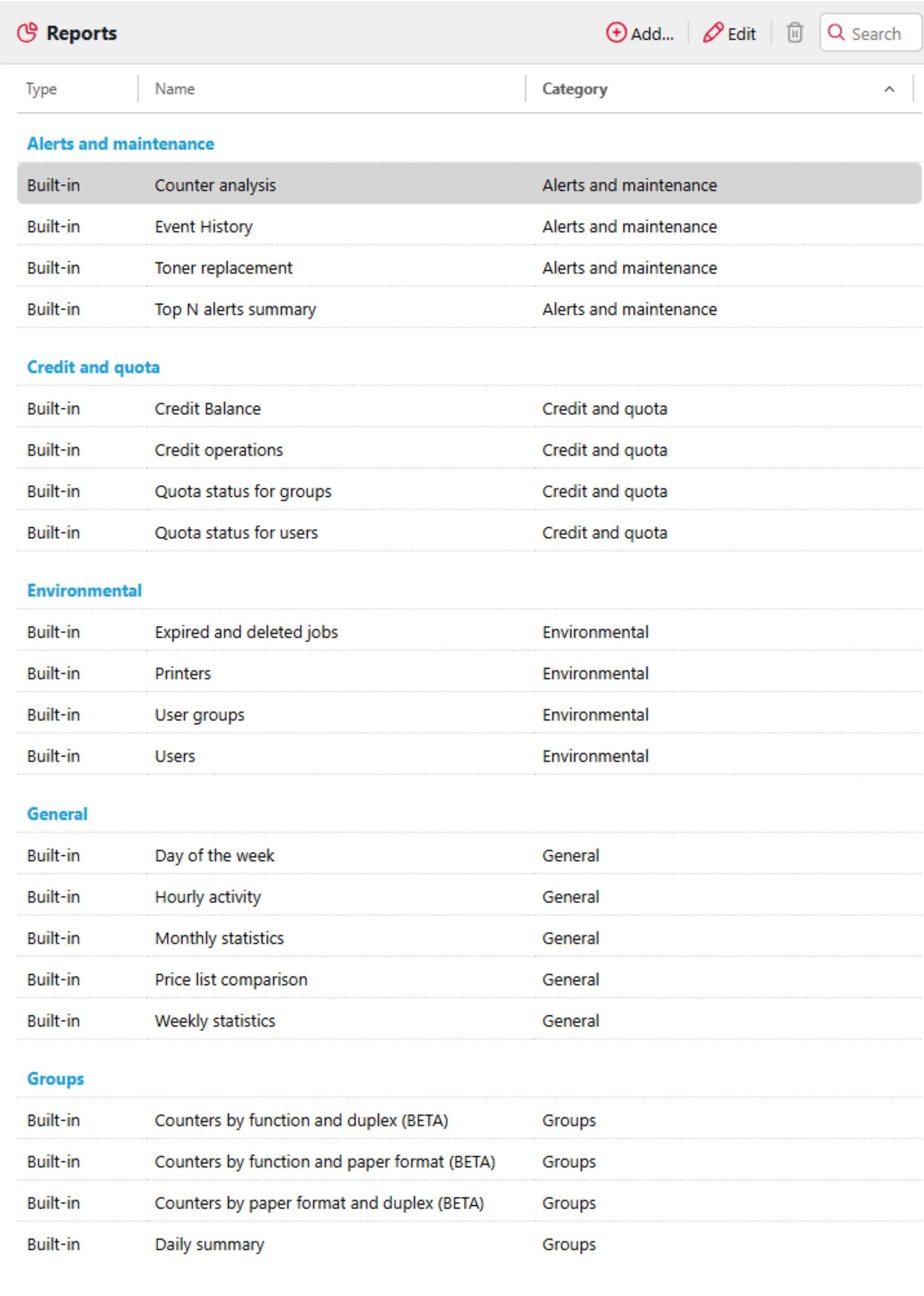
You can also add custom report types developed by the MyQ development team. To do so, just click **+Add**, upload the custom report definition file, select users or groups to access it, and click **OK.** For more information about custom report types, please contact MyQ support.

See also: Personalization Settings (see page 138)

12.2 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 & Quota*).

To see an overview all of the report types and categories, go to **MyQ > Settings > Reports**.



Type	Name	Category
Alerts and maintenance		
Built-in	Counter analysis	Alerts and maintenance
Built-in	Event History	Alerts and maintenance
Built-in	Toner replacement	Alerts and maintenance
Built-in	Top N alerts summary	Alerts and maintenance
Credit and quota		
Built-in	Credit Balance	Credit and quota
Built-in	Credit operations	Credit and quota
Built-in	Quota status for groups	Credit and quota
Built-in	Quota status for users	Credit and quota
Environmental		
Built-in	Expired and deleted jobs	Environmental
Built-in	Printers	Environmental
Built-in	User groups	Environmental
Built-in	Users	Environmental
General		
Built-in	Day of the week	General
Built-in	Hourly activity	General
Built-in	Monthly statistics	General
Built-in	Price list comparison	General
Built-in	Weekly statistics	General
Groups		
Built-in	Counters by function and duplex (BETA)	Groups
Built-in	Counters by function and paper format (BETA)	Groups
Built-in	Counters by paper format and duplex (BETA)	Groups
Built-in	Daily summary	Groups

12.2.1 **Granting Users 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**.

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, please contact MyQ support.

12.2.2 Report Categories

12.2.3 Alerts and Maintenance Reports

Alerts and Maintenance reports provide information about device alerts and unusual changes on device counters.

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.

12.2.4 Environmental Reports

Environmental reports provide information about the environmental impact of printing. They show estimates of environmental impact, in terms of how many tree-equivalents would be consumed, how much energy was used 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.

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.

12.2.5 General Reports

General reports provide an overview of your MyQ system, such as total counters statistics and printing peaks or comparisons of price lists used for printers.

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.

12.2.6 Groups Reports

Groups reports contain information about group membership, printed pages, weekly stats etc.

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.

12.2.7 Print Jobs Reports

Print Jobs reports contain information about jobs printed in MyQ, such as the list of all expired and deleted jobs over a certain period.

> Do not use Print Jobs reports for accounting purposes. Print Jobs 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.

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.

Favorite Jobs

This report shows the list of user's favorite jobs.

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.

12.2.8 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.

12.2.9 Projects Reports

Projects 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.

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.

12.2.10 Users Reports

Users reports can contain various information about users, print jobs, credit statements, printed pages, and more.

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.

12.3 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.

12.4 Creating Reports

12.4.1 Creating Reports

1. In **MyQ > Reports**, click **+Add report**. The Add report dialog box appears.
2. Select the type of the new report and the folder to place it, and click **OK**. The report is saved, and opens in edit mode on the Design tab.

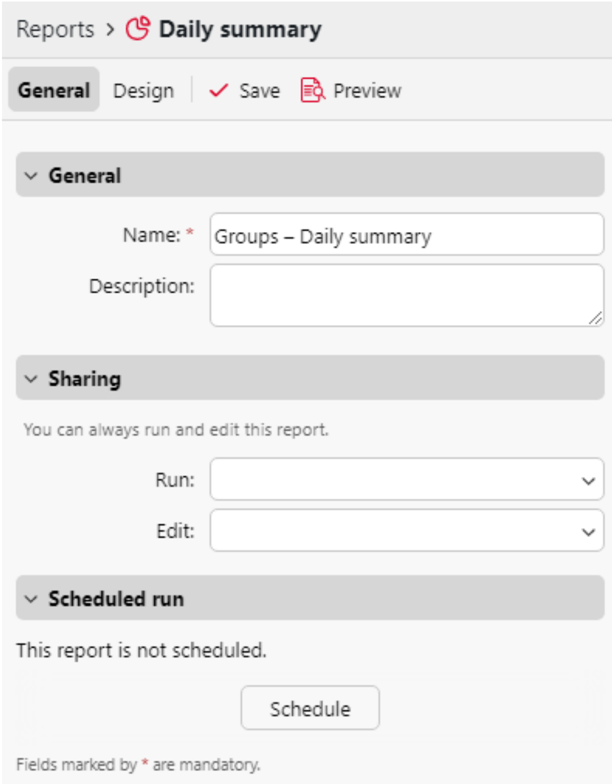
12.4.2 Editing a Report

To edit a report, go to **MyQ > Reports**, click the three-dot menu for the report you want to schedule, and select **Edit**. The report opens in edit mode.

General Tab

On the General tab of the report editor, you can configure these options:

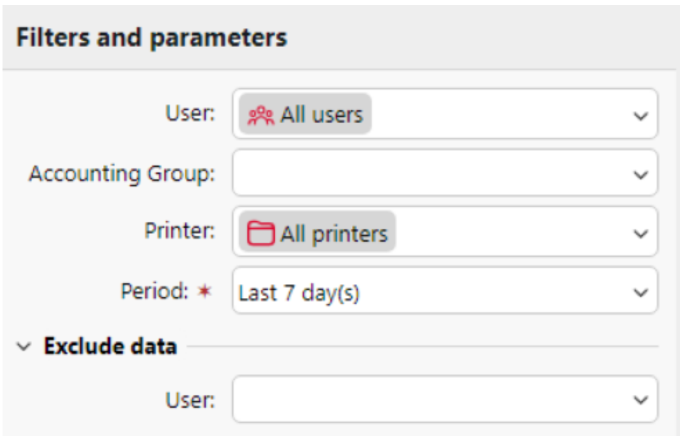
- **Name:** customize the report name.
- **Description**: add an optional description for the report.
- **Sharing**: specify what users or groups can **Run** and **Edit** the report.
- **Schedule run**: Define a scheduled task to run the report at regular intervals.



Design Tab

Filters and parameters

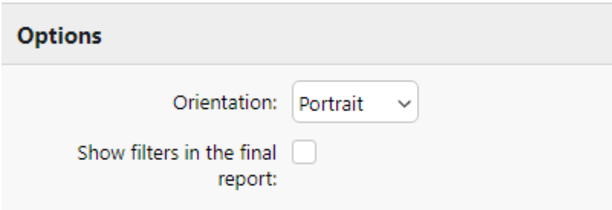
Available filters and parameters differ depending on the report type. These are the main parameters available for most of the standard reports types:



- **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).

Options

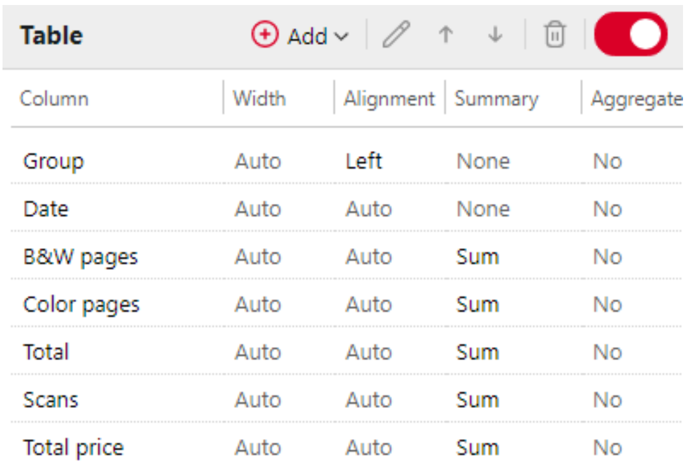
- **Orientation**: Select either the **Portrait**, or the **Landscape** orientation.



- **Show filters in the final report**: Mark the checkbox if you want filters to be visible in the final report.

Table

Here you can enable and disable the table option.



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).

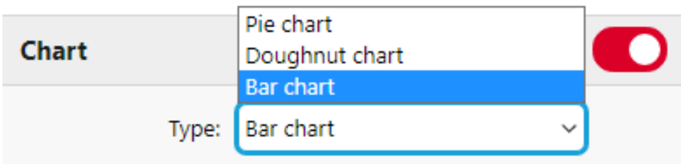
To add a new column, click **+Add**. To open the editing options of an existing column, double-click it (or select it, and then click **Edit**). To remove a column, select it and click **X**. To move a column up or down the order, select it, and then use the up/down arrows.

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

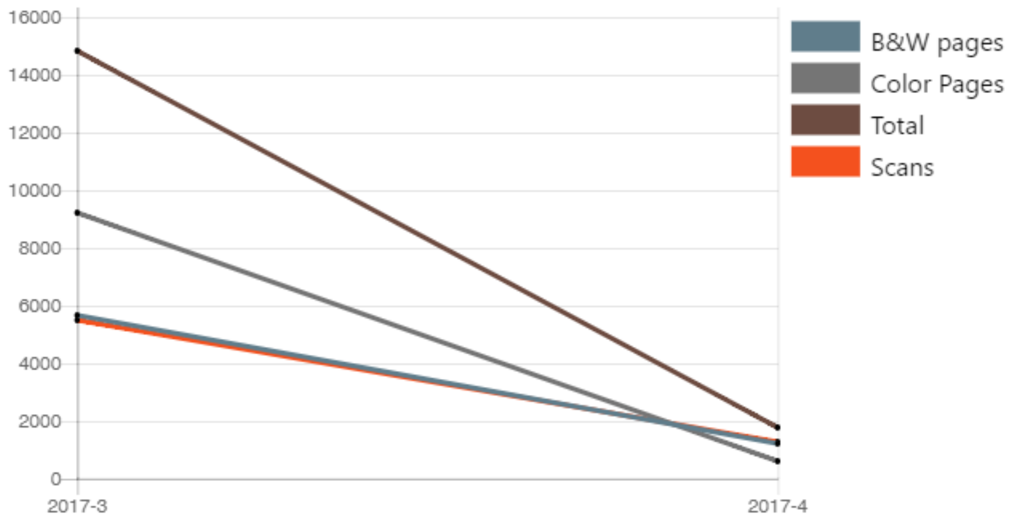
Here you can enable and disable the chart option.



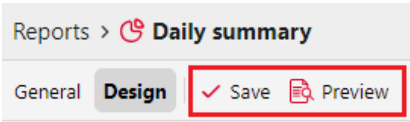
You can also select from the **Bar, Pie** and **Doughnut** chart types. Furthermore, you can add and remove data types to be shown on the chart and select colors for each data type (depending on the report type).

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.

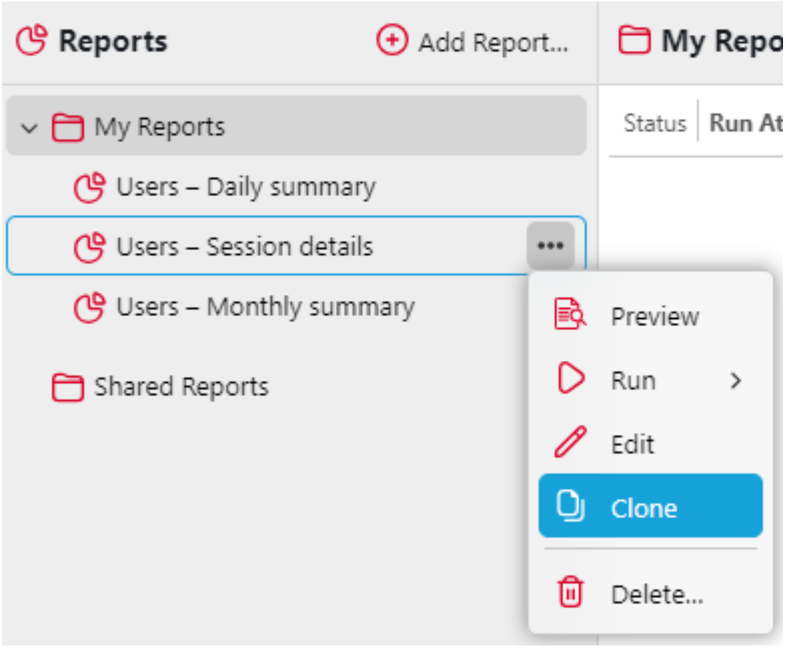


Designing your own reports can be a bit tricky, since it always depends on many factors - amount of data included (columns), length of column names and values, report orientation etc. To get the best result, you can click **Preview** anytime during the report's creation to check what the new design will look like. Only after you are satisfied with the layout, click **Save** to save the report.

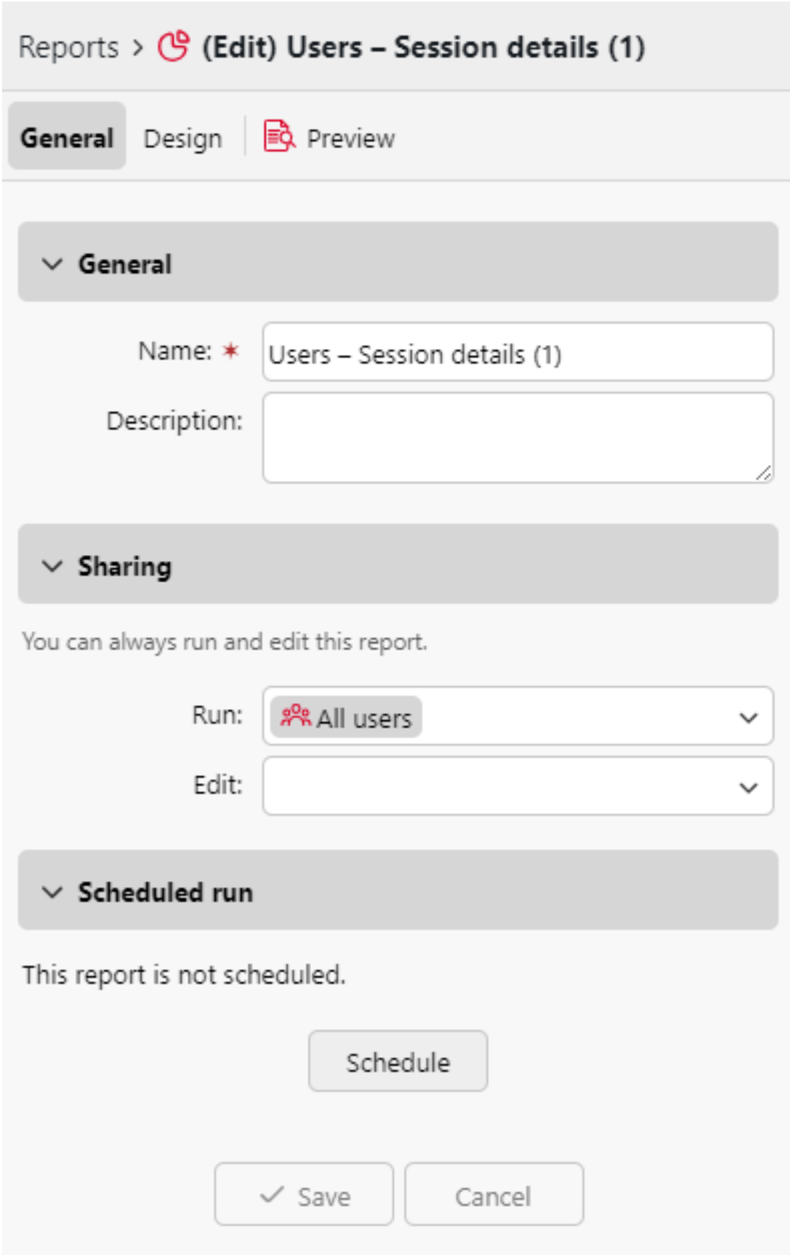


12.4.3 Cloning Reports

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.



If the source folder of the report was not created by the user, a clone will be created in the My Reports folder.

12.5 Running Reports

Reports can be run on-demand or scheduled to run automatically at specified intervals. This section describes both approaches.

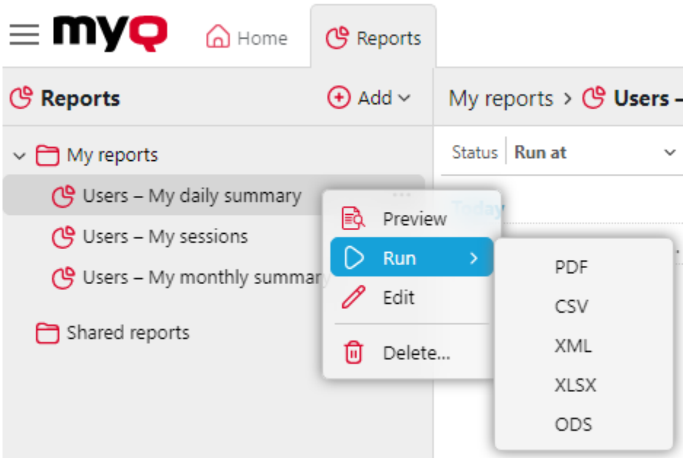
12.5.1 Running Reports On-Demand

Preview a report

Select the report and click **Preview**. The report is shown in HTML format, with a limited subset of data included. You can switch between Graphical and Grid views.

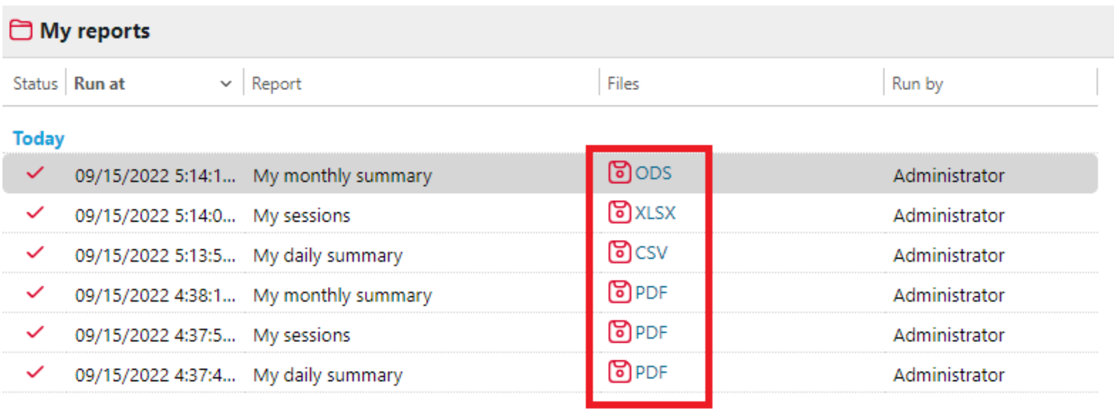
Run a report

Right-click the report and click **Run**. The report runs in the specified format (*PDF*, *CSV*, *XML*, *XLSX* or *ODS*) with no data limitation.



Export the displayed report

After the report is generated, click on the report's format link in the Files column to download it.

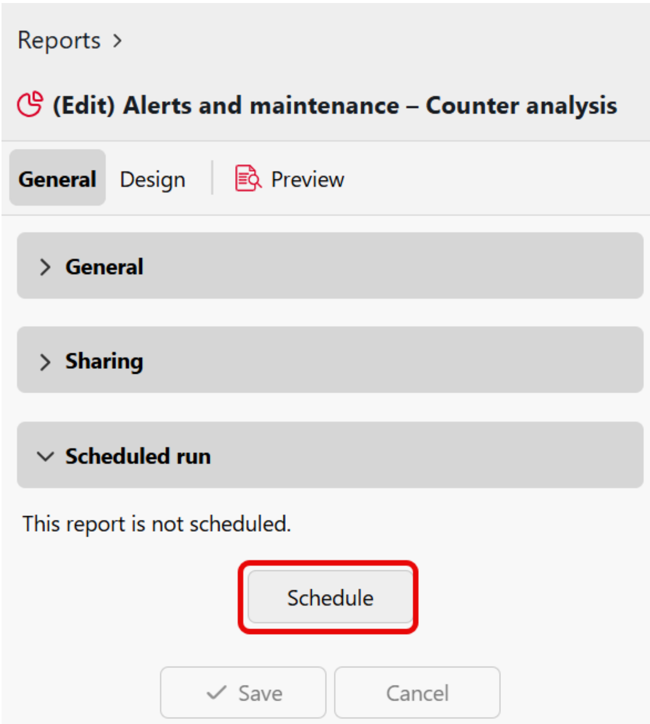


12.5.2 Scheduling Reports

You can schedule reports to run automatically at regular intervals. Scheduled reports are generated in the background and can be sent via email to specified recipients.

Schedule a report

1. In **MyQ > Reports**, click the three-dot menu for the report you want to schedule.
2. Click **Edit**. The report opens in edit mode.
3. On the **General** tab, in the **Scheduled run** section, click **Schedule**. The scheduled task editor opens.



4. Configure the scheduling options to your needs.
5. After configuring the schedule, click **Add** to create the scheduled task, or **Save** if editing an existing schedule.

Managing Scheduled Reports

Scheduled reports appear in the **Task Scheduler** settings tab (**MyQ > Settings > Task Scheduler**) alongside other system tasks. The Action column shows "Scheduled Report" for these tasks.

From the Task Scheduler, you can:

- **View status**: See whether the task is Ready, Disabled, or Running.

- **Check run history**: View the Last run time, Last run result, and Next run time.
- **Run manually**: Select the task and click **Run** to execute it immediately.
- **Edit**: Double-click the task to modify its schedule or settings, and toggle the task on or off without deleting it.
- **Delete:** Delete the scheduled report task. This removes the schedule from the defined report, but does not delete the report.

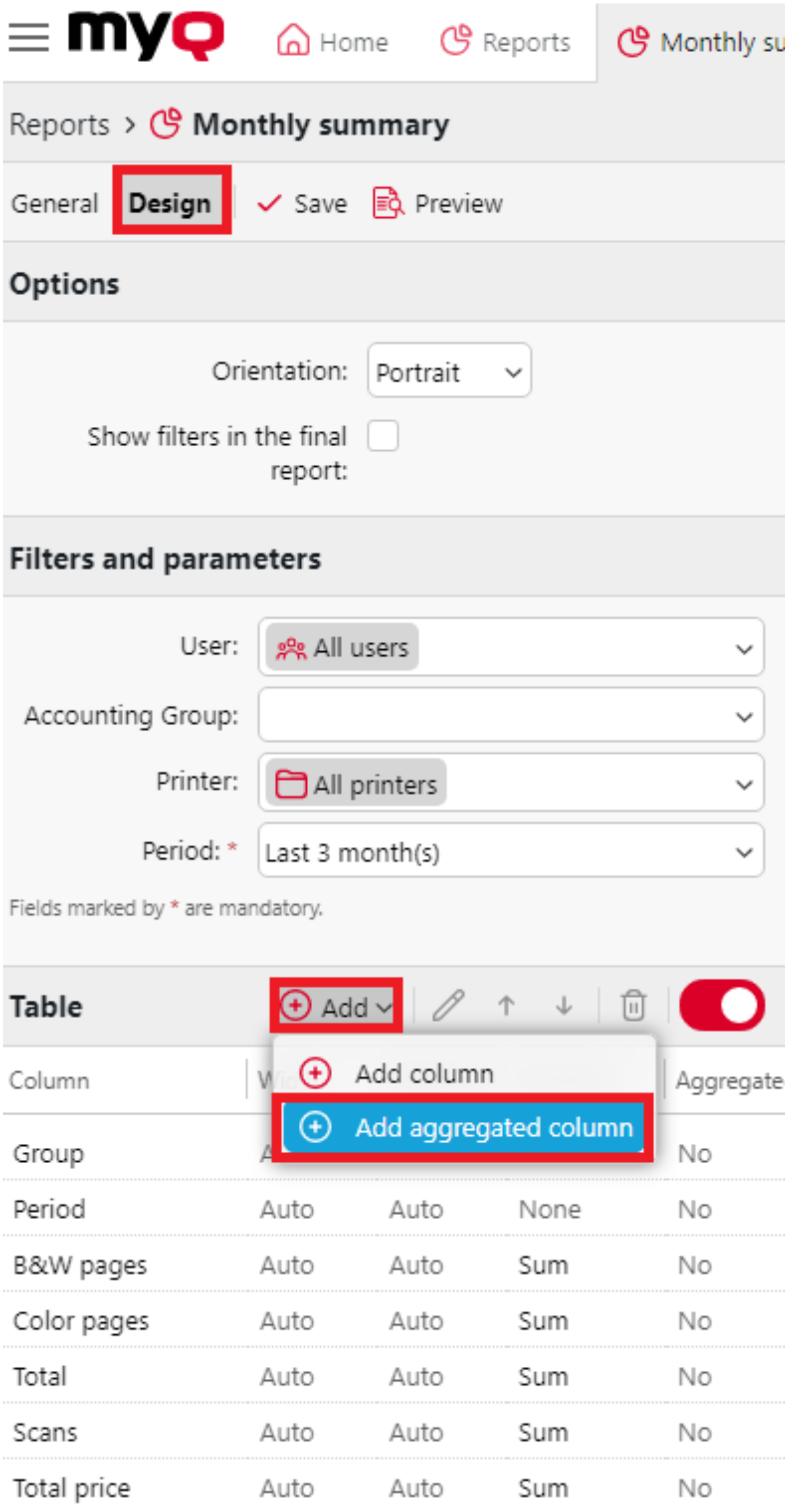
See also: Task Scheduler Settings (see page 141)

12.6 Aggregated Columns in Reports

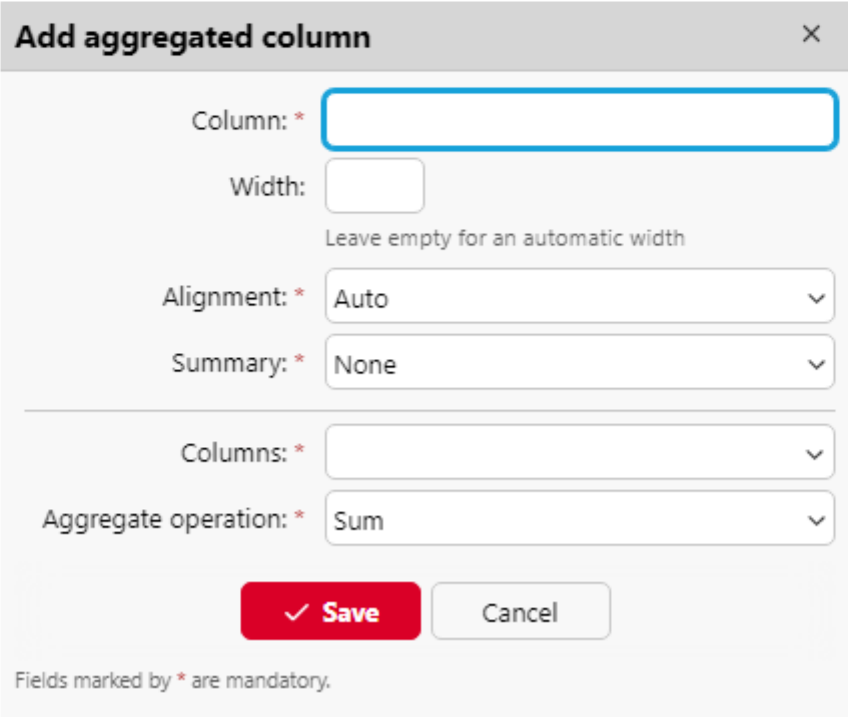
For some types of reports, you can create any number of custom aggregated (summary) columns. An aggregated column can display either the sum or the average of a selection of any number of other columns available for the type.

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 a new window.
2. Go to the **Design** tab on the properties panel.
3. In the **Table** section, click **+Add**, and select **+Add aggregated column** from the list. The properties panel of the new column opens.



4. In the panel, set the properties, select the **Aggregate operation** you want to use (*Sum* or *Average*), and click **Save**. The new column is listed with the other table columns, and you can double-click on it to edit it.



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, Total summary
- From the **Print jobs** category: Expired and deleted jobs
- From the **Printers** category: Daily summary, Day of the week, Meter reading via SNMP, Total summary
- From the **Projects** category: Daily summary, Day of the week, Monthly summary, Project groups total summary, Projects per user, Users per project.

12.7 Counts and Sheets in Reports

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

12.8 Connect to Power 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.

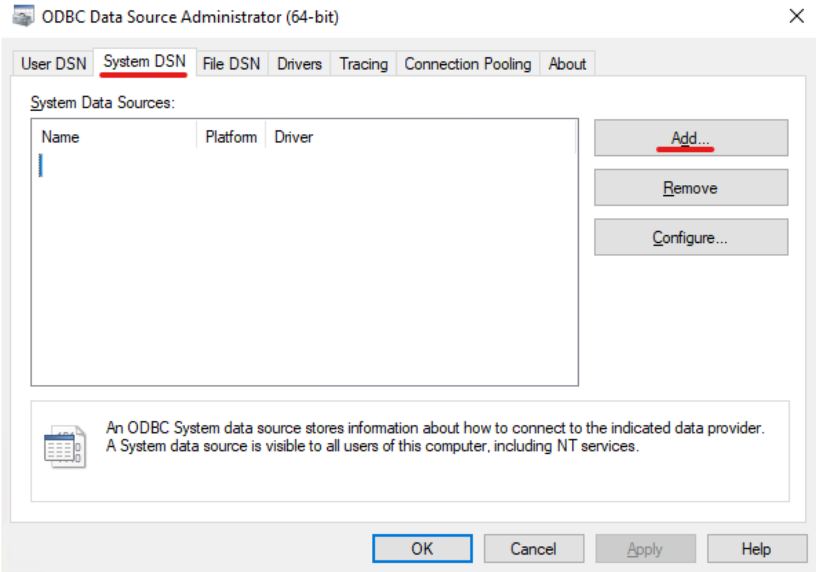
For further information about Power BI, visit:
https://docs.microsoft.com/en-us/power-bi/fundamentals/desktop-getting-started

12.8.1 Configure Power BI Embedded DB

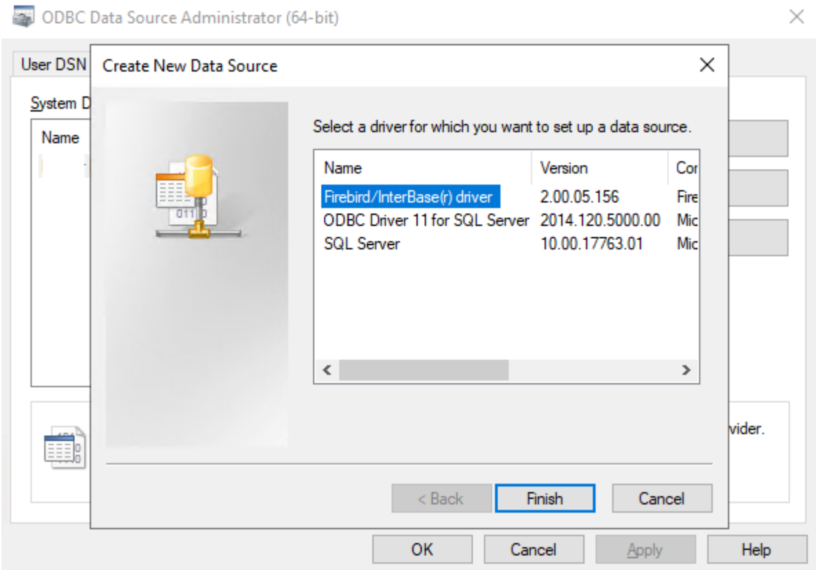
Power BI can access the MyQ Embedded Database via ODBC. In order to create an ODBC data source:

> 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 from the list below. Click Test connection, and if successful, click OK.

- **Data Source Name (DSN)**: Add a name as an identifier for the connection
- **Database**: Add the path to your database file (*C:\ProgramData\MyQCentral\MYQ.FDB* by default)
- **Client**: Add the path to the Firebird library client used for the connection. It is recommenced to use the MyQ Central Server client, found in *C:\Program Files\MyQ Central\Firebird\fbclient.dll* by default
- **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

- **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*.

12.8.2 Creating Power BI Reports

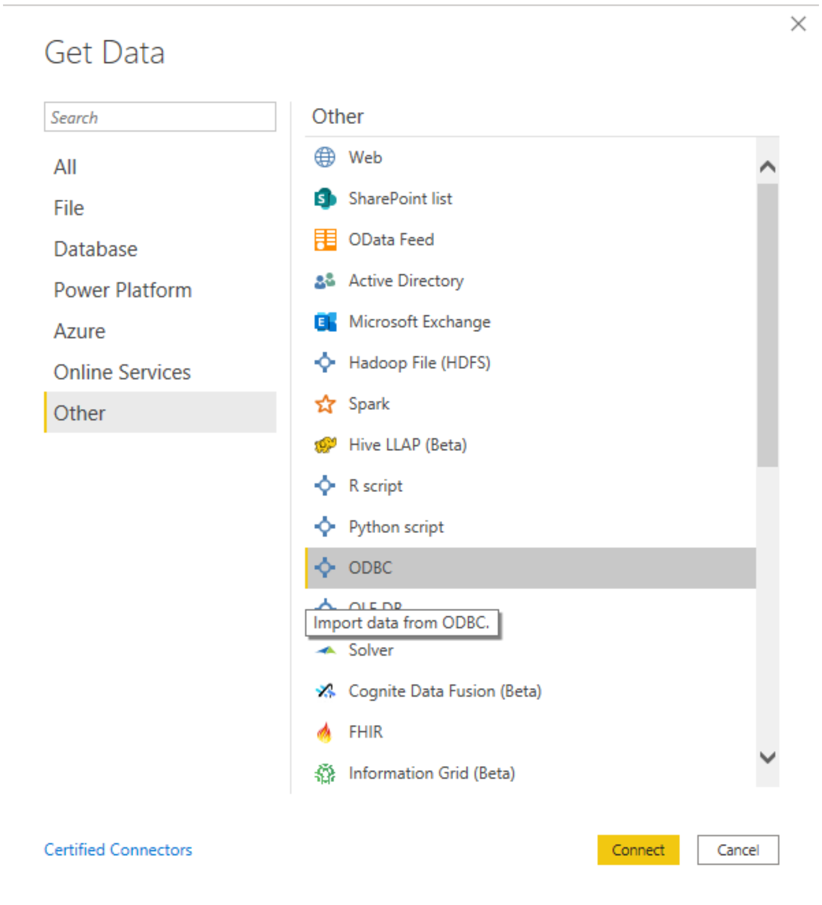
Reports can be created according to each customer's specific requirements. It is possible to create the reports manually, or use the Power BI template created by MyQ in order to generate reports quickly.

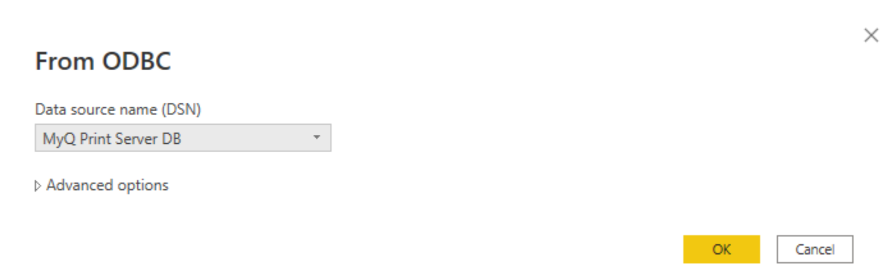
- Manual reports creation (see page 308)
- Reports creation via template import (see page 312)
- Report examples (see page 313)
- Database Views description (see page 315)

Create Power BI Reports Manually

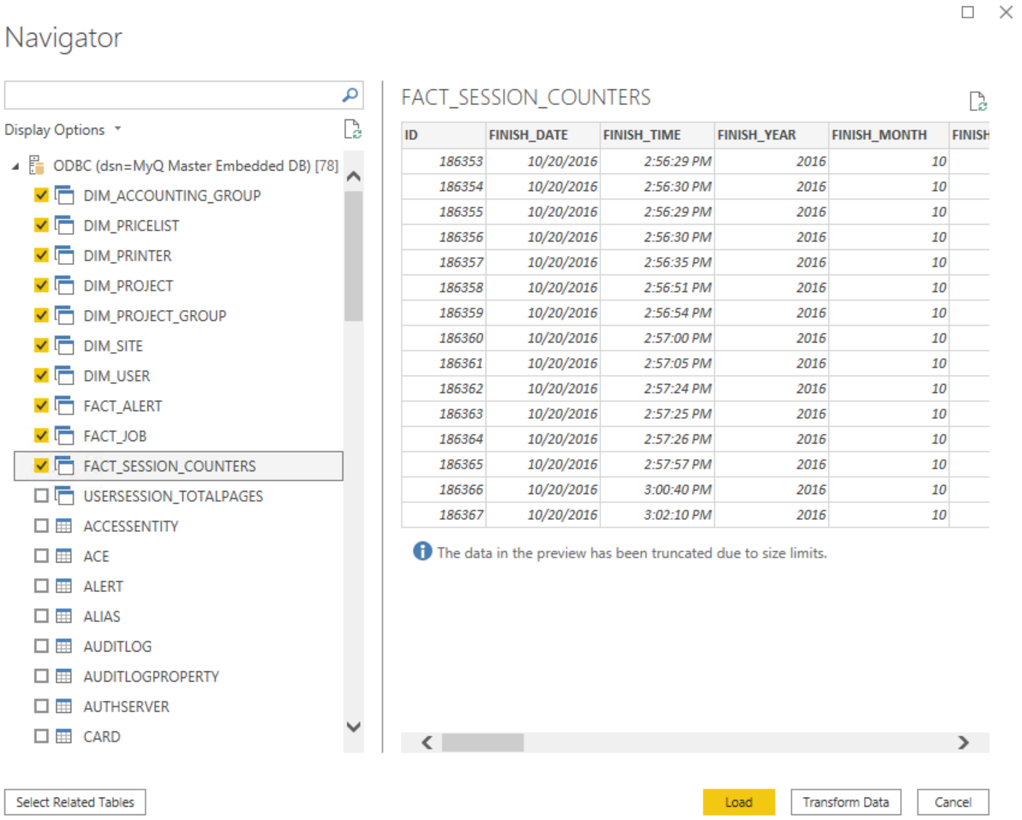
To manually create the reports, open Power BI and:

1. Establish the connection to your database:
    a. 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**.

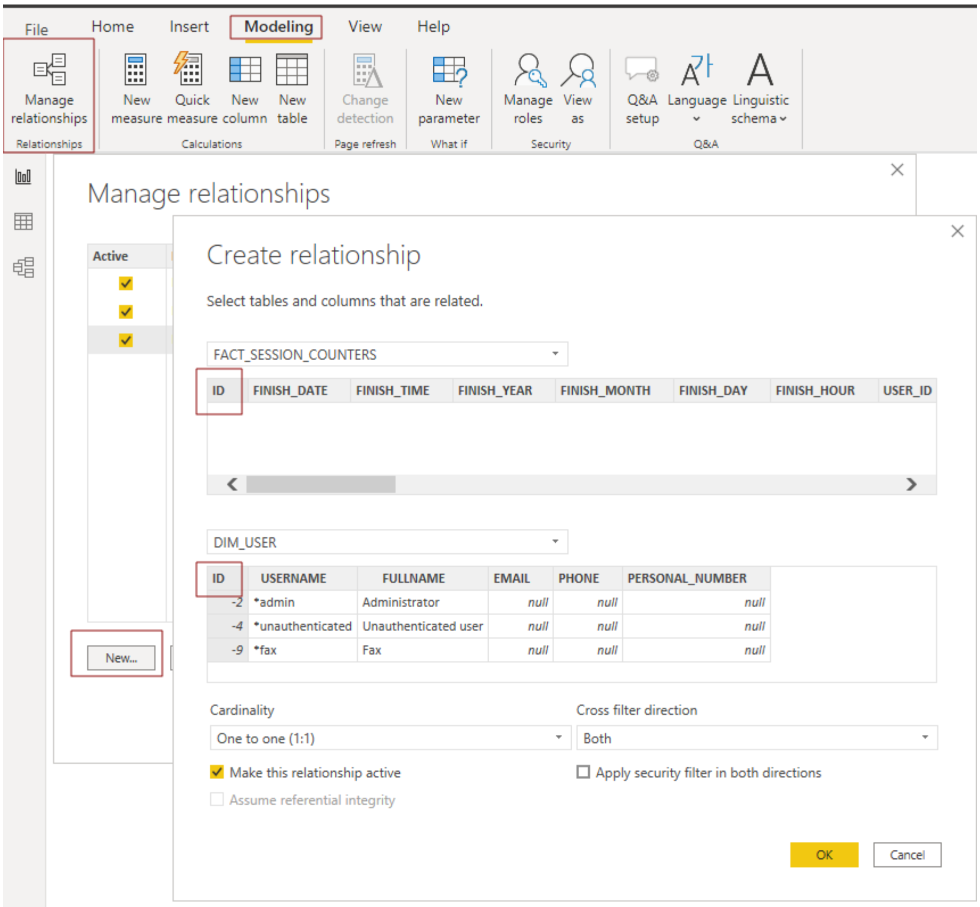




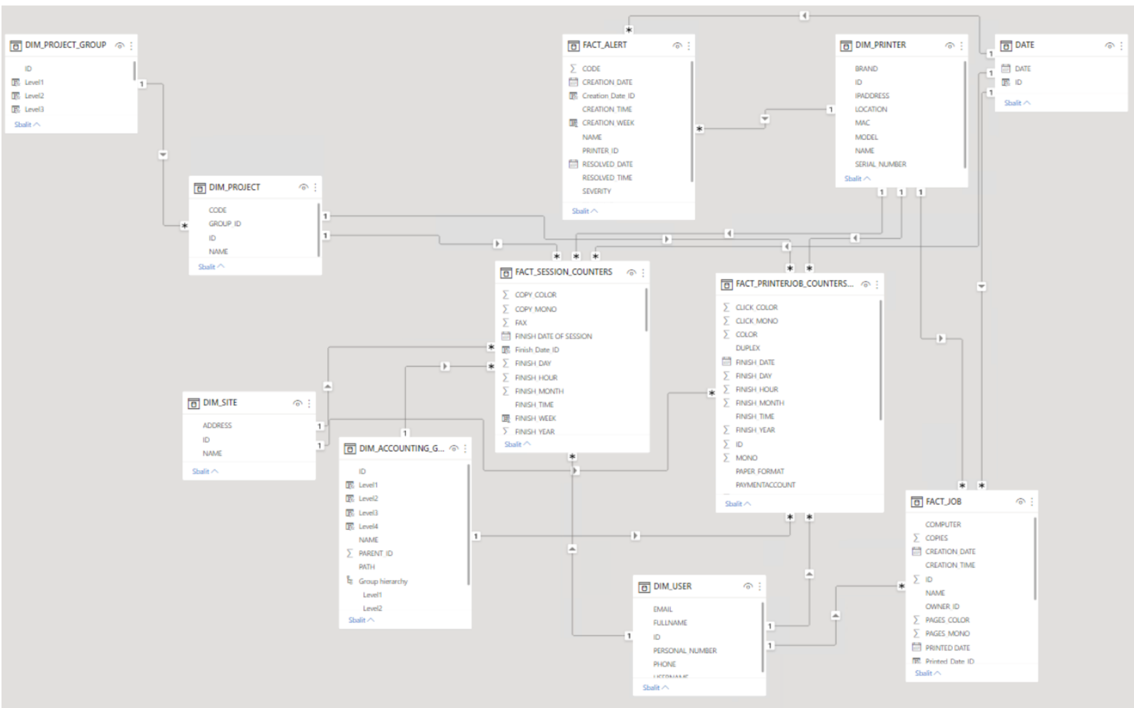
2. In the Navigator window, select all the options with the **DIM_** and **FACT_** prefixes and click **Load** (see Database Views description (see page 315)).



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.



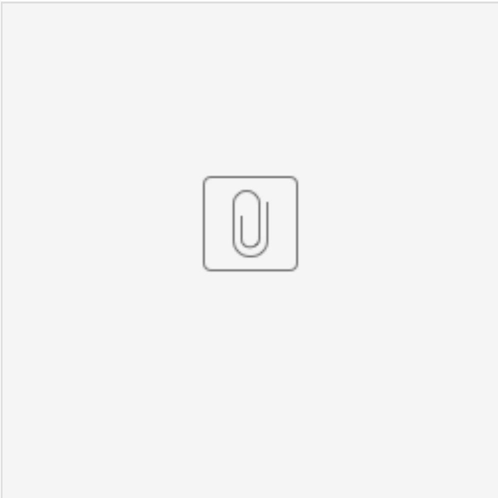
4. Your model has been created and you can add visualizations to the report.



Create Power BI Reports 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.

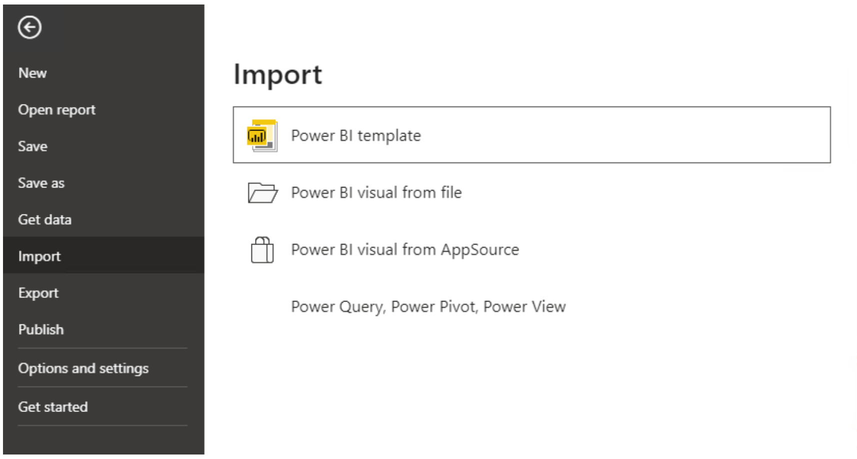
ODBC template



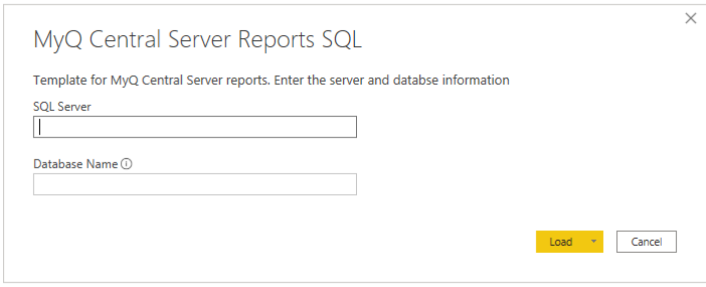
SQL template

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**.

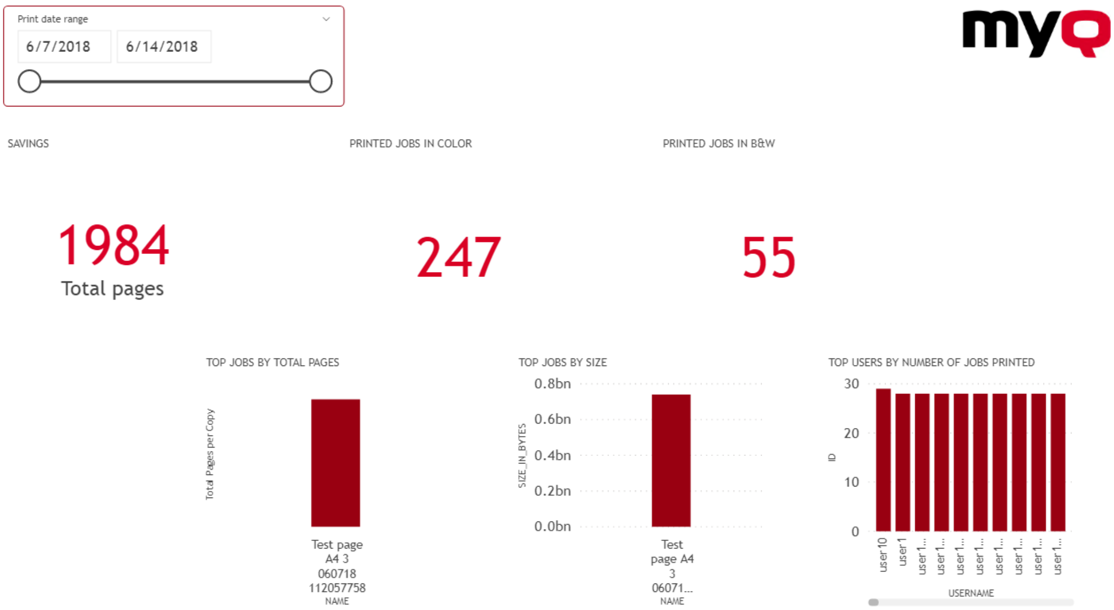


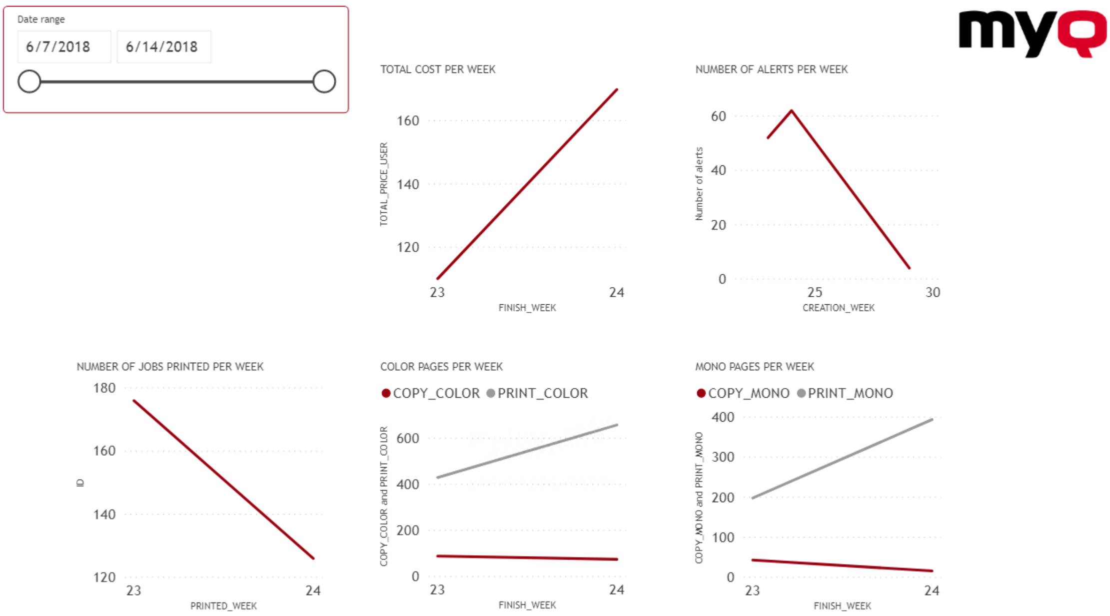
   b. For ODBC, add the **Data source name (DSN)** you created in the ODBC Data Sources app and click **Load**.

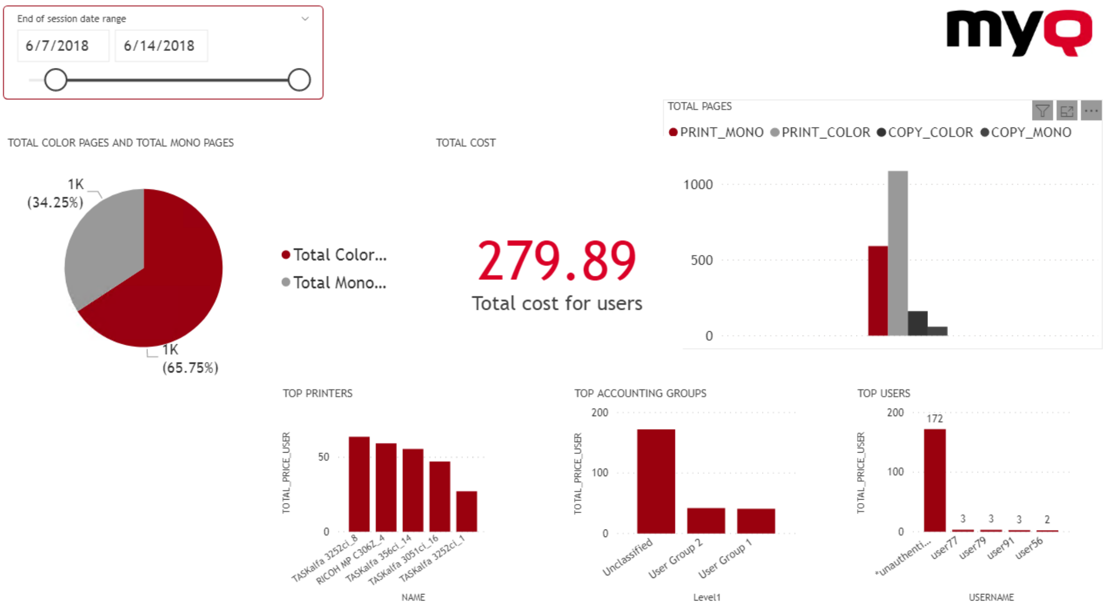
3. Power BI imports the data. The reports can be edited; the changes are saved in a different file so the template can be reused.

Sample Power BI Reports

The examples below were generated using the MyQ template.


Print date range
6/7/2018
6/14/2018
SAVINGS
PRINTED JOBS IN COLOR
PRINTED JOBS IN B&W
1984
Total pages
247
55
TOP JOBS BY TOTAL PAGES
Total Pages per Copy
Test page A4 3 060718 112057758
NAME
TOP JOBS BY SIZE
0.8bn
0.6bn
0.4bn
0.2bn
0.0bn
SIZE_IN_BYTES
Test page A4 3 06071...
NAME
TOP USERS BY NUMBER OF JOBS PRINTED
30
20
10
0
ID
user10
user1
user1...
USERNAME


Date range
6/7/2018
6/14/2018
TOTAL COST PER WEEK
160
140
120
TOTAL_PRICE_USER
23
24
FINISH_WEEK
NUMBER OF ALERTS PER WEEK
60
40
20
0
Number of alerts
25
30
CREATION_WEEK
NUMBER OF JOBS PRINTED PER WEEK
180
160
140
120
ID
23
24
PRINTED_WEEK
COLOR PAGES PER WEEK
COPY_COLOR
PRINT_COLOR
600
400
200
0
COPY_COLOR and PRINT_COLOR
23
24
FINISH_WEEK
MONO PAGES PER WEEK
COPY_MONO
PRINT_MONO
400
300
200
100
0
COPY_MONO and PRINT_MONO
23
24
FINISH_WEEK



DB Views and Dimensions

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
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`)
Created	Date and time in which the event was created
Closed	Date and time in which the event was closed

Field name	Description
Data	Data of the event (JSON example: `{"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"}`)
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
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
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)

Field name	Description
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
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

Field Name	Description
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
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

Field Name	Description
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
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_Counters) - 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)
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)

Limitation
Even if a Job Privacy license is activated, the data in the database is still readable.

13 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`
Icelandic (Iceland)	`is`
Italian (Italy)	`it`

Language	Abbreviation
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`
Thai (Thailand)	`th`
Turkish (Turkey)	`tr`
Ukrainian (Ukraine)	`ua-UA`
Vietnamese (Vietnam)	`vn`

Language	Abbreviation
Welsh (Wales)	`cy`

14 Release History

14.1 MyQ X Server RC

14.1.1 **MyQ Central Server 10.3 RC**

14 September, 2026

14.1.2 Security

- Improved security for CSV exports.
- Communication patterns unified with Print Server, the HTTP Proxy (Traefik) is now in use.
- A new helper is used for cloud connections.

Improvements

- Optimized the speed of long running database queries under certain conditions.
- Added the new Delta synchronization option for Entra ID, and a new scheduled task for lightweight, frequent synchronization.

Changes

- The EULA has been updated. You can view it during installation or upgrade.
- Modified Traefik rules to prevent server overload in case of too many MDC connections.
- Connections to Sites now require 10.2 or later.
- Removed option to set unsecure HTTP port.
- Updated Apache to 2.4.68.
- Updated Firebird to 4.0.7.
- Updated Microsoft Playwright to 1.62.0.
- Updated OpenSSL to 3.5.7.
- Updated PHP to 8.3.31.
- Updated Traefik to 3.6.19.

Bug Fixes

- Adding new delegates can cause user synchronization errors.
- Apache reports errors about missing environment variables to Event log.
- Creation of default backup folder fails during installation.

- Database sweep cannot complete on big databases in some cases because of too short timeout.
- Delegate removal was not reflected in user sync in some cases.
- Exporting users to CSV during user synchronization exports outdated users.
- Incorrect font scaling in generated PDF reports.
- Reordering synchronization sources can fail when the list of sources contains a combination of LDAP and CSV sources.
- Under certain conditions and with certain certificates the Web UI fails to load, with the message "ERR_SSL_PROTOCOL_ERROR".
- When the Printer Provisioning Profiles license package has been purchased multiple times, the displayed number of profiles was incorrect.

15 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[31]
Technical support	support@myq-solution.com[32]
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.

31. mailto:info@myq-solution.com
32. mailto:support@myq-solution.com

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.

myQ X

SAVE TIME WITH PERSONALIZED PRINT SOLUTIONS

MyQ X is an award-winning on-premise or private cloud print management solution trusted by millions of users.

info@myq-solution.com

myq-solution.com

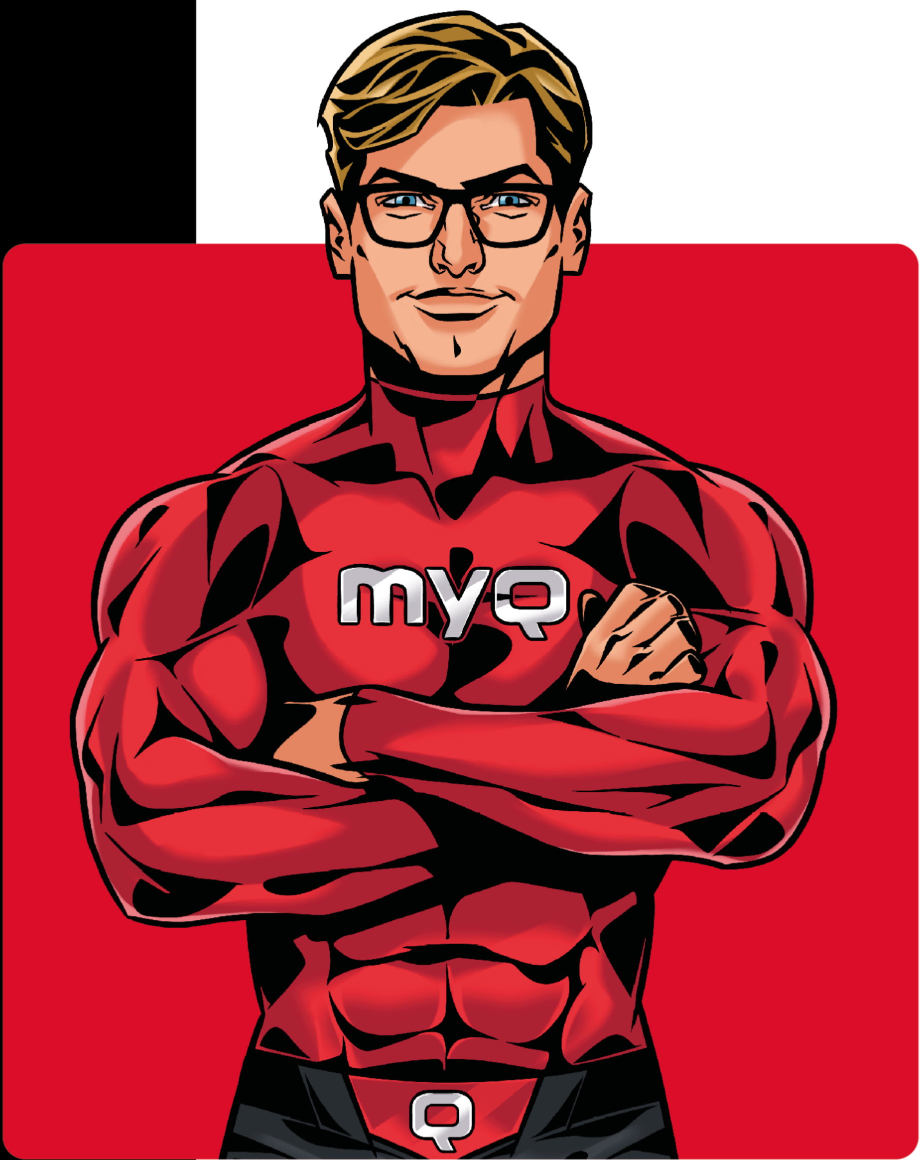
50+ million
Trusted users

1+ million
Active devices

26+
Brands supported

1000+
Certified partners

Operating in **140+** countries



Awarded and certified

BuyersLab PLATINUM TESTED SOLUTION 2023

BuyersLab PLATINUM TESTED SOLUTION 2022

BuyersLab PLATINUM TESTED SOLUTION 2021

TÜV SÜD ISO 9001 ISO 14001 ISO/IEC 27001