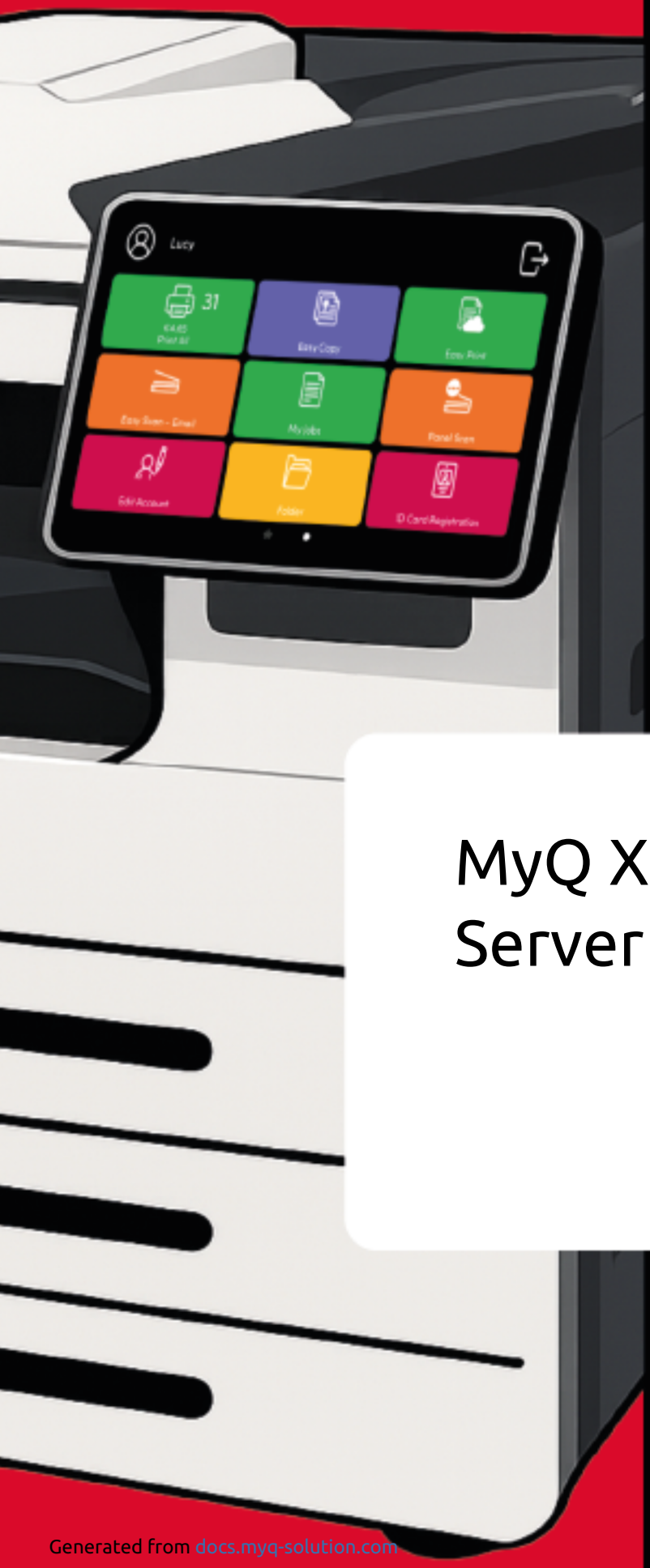


MyQ X Server 10.3 Print Server

Generated from docs.myq-solution.com
November/2026
Copyright © 2026 MyQ spol. s r.o. All Rights Reserved

ENGLISH

Table of Contents

1 What's New in 10.3 8
1.1 Release Stations 8
1.2 MyQ Scan Review 8
1.3 MyQ Document Processor 9
1.4 IPP Pass-Through Mode for WPP-Compatible Queues 9
1.5 Delta Synchronization for Microsoft Entra ID 10
1.6 Require Authentication for IPPS Jobs 10
1.7 Other Important Changes 10
1.8 Removed Features 12
2 Latest Release Notes 13
2.1 MyQ Server 10.3 13
2.2 Version Highlights 13
2.3 MyQ Print Server 10.3 RTM 13
2.4 Component Versions 14
3 Licenses 16
3.1 License Plans 16
3.2 Licenses 17
3.3 Software Assurance 18
3.4 Installation Key 18
3.5 License Settings 18
3.6 Manual Activation 20
3.7 Moving Licenses to New Hardware 21
3.8 Troubleshooting Licenses 22
4 System Requirements 24
4.1 MyQ Print Server – Standalone Mode 24
4.2 MyQ Print Server – Site Mode (Central Server & Site Servers Architecture) 25
4.3 Additional Software Requirements 26
4.4 MyQ Installation in Private Cloud 29
4.5 Main Communication Ports 29
4.6 Components Overview 41
4.7 Supported Terminals and Applications 46
4.8 Network Architecture 47
4.9 Embedded Terminal Features 50

5 Installation 97
5.1 Upgrading to MyQ 10.3 97
5.2 Install MyQ in Private Cloud 117
5.3 Migrate from OEM to MyQ 121
5.4 Updating MyQ 125
5.5 MyQ and MS Cluster 126
5.6 Uninstall MyQ 142
6 MyQ Easy Config 144
6.1 Easy Config Home 144
6.2 Easy Config Services 146
6.3 Easy Config Settings 148
6.4 Easy Config Security 150
6.5 Easy Config Database 154
6.6 Easy Config Log 157
7 MyQ Web Interface 159
7.1 Accessing the MyQ Web Interface 159
7.2 Log In as an Administrator 159
7.3 Main Menu and Settings Menu 160
7.4 Home Dashboard 163
7.5 MyQ Log 170
7.6 MyQ Audit Log 173
8 MyQ System Settings 175
8.1 Server Type 175
8.2 License 175
8.3 Sites 175
8.4 General 175
8.5 Personalization 175
8.6 Task Scheduler 175
8.7 Network 175
8.8 Printers & Terminals 176
8.9 MyQ Desktop Client 177
8.10 Printer Provisioning 177
8.11 Print Drivers 177
8.12 Users 177
8.13 Accounting 178

8.14 Jobs 179
8.15 Scanning & OCR 179
8.16 Code Books 179
8.17 Reports 179
8.18 External Reports 179
8.19 REST API Apps 179
8.20 Log 179
8.21 System Management 180
8.22 Server Type Settings 180
8.23 General Settings 181
8.24 Personalization Settings 182
8.25 Task Scheduler Settings 191
8.26 Network Settings 193
8.27 MyQ Desktop Client Settings 240
8.28 Print Driver Settings 246
8.29 Accounting Settings 249
8.30 External Reports 252
8.31 REST API Apps 253
8.32 Log Settings 253
8.33 System Management Settings 256
9 Printers 300
9.1 Printers Tab 300
9.2 Printers and Terminals Settings 301
9.3 Configuration Profiles 310
9.4 Adding Printing Devices 314
9.5 Terminal Actions 322
9.6 Release Stations 401
9.7 Managing Printers 414
9.8 Monitoring Network Printers in Offline Mode 421
9.9 Monitoring Local Printers 422
9.10 Printer Events 423
10 Users 429
10.1 Default System Users 429
10.2 Adding and Deleting Users Manually 430
10.3 Editing User Accounts 431

10.4 User Groups 438
10.5 Exporting Users 439
10.6 Automatic User Registration 440
10.7 Users Settings 442
10.8 User Synchronization 453
10.9 User Authentication 507
10.10 Data Privacy and Anonymization 530
11 Queues 532
11.1 Default Queues 532
11.2 Queue Types 533
11.3 Adding, Copying, and Deleting Queues 535
11.4 Editing Queues 536
11.5 Online/Offline Queues 539
11.6 Personal Queues 540
11.7 Advanced Queue Options 542
11.8 User Detection Methods 576
11.9 Binary Find & Replace 580
12 Jobs 583
12.1 Working with the Jobs List 583
12.2 Job Statuses 583
12.3 Jobs Settings 584
12.4 Editing & Deleting Jobs 587
12.5 Set Up Office Document Processing 588
12.6 Notifications on Job Receiving Errors 589
12.7 Job Parser 590
12.8 Jobs via LPR Protocol 592
12.9 Jobs via IPPS 595
12.10 Jobs via Email 601
12.11 Jobs via Web 604
12.12 Job Preview 606
12.13 Job Archiving 606
12.14 Job Privacy 608
12.15 Watermark Collections 608
13 Scanning & OCR 614
13.1 Using Document Processor 614

13.2 OCR Profiles 620
13.3 Code Books 624
13.4 Scan to Me 633
14 Accounting 637
14.1 Prerequisites 637
14.2 Credit Accounting 637
14.3 Quota Accounting 637
14.4 Project Accounting 638
14.5 Price Lists 638
14.6 Credit 638
14.7 Quotas 654
14.8 Projects 668
14.9 Price Lists 674
15 Reports 680
15.1 Granting Users Rights to Use a Report 681
15.2 Report Types 681
15.3 Reporting Sources 692
15.4 Creating Reports 693
15.5 Running Reports 697
15.6 Aggregated Columns in Reports 698
15.7 Counts and Sheets in Reports 699
15.8 Connect to Power BI Tools 701
16 Available Languages 718
17 Release History 721
17.1 MyQ X 10.3 RTM 721
17.2 MyQ X 10.3 RC 722
18 Business Contacts 725

MyQ Print Server 10.3

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 print management system, how to set up the system through the MyQ Web Administrator Interface, activate licenses, and set print ports. Furthermore, you can learn how to maintain the MyQ system, acquire its statistical data, and monitor the print environment.

This guide is also available for download. See (10.3) Guides in PDF.

1 What's New in 10.3

Here’s an overview of the new features included in MyQ version 10.3.

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 a 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: Release Stations (see page 401)

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

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

Document Processor is a separately installed service that connects to an instance of Print Server. Create an OCR Profile that uses Document Processor 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 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: Jobs via IPPS (see page 595)

1.5 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 485)

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: Jobs via IPPS (see page 595)

1.7 Other Important Changes

1.7.1 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.

1.7.2 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:

- Embedded
- Embedded Lite
- Embedded Ultimate

See also: Licenses (see page 16)

1.7.3 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 different 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 Document Processor, 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: OCR Profiles (see page 620)

1.7.4 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`.

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.

1.7.5 Traefik Upgrade - Migrate Custom Rules

MyQ X 10.3 includes **Traefik v3**, replacing the previous v2. 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 103)

1.8 Removed Features

1.8.1 OCR Server

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

1.8.2 Removed Terminal Support

10.3 removes support for the following legacy terminals:

- HW-11-T
- 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.

2 Latest Release Notes

2.1 MyQ Server 10.3

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

2.2 Version Highlights

Click to see the new features in 10.3

- Release Stations: Release jobs securely on printers without an embedded terminal, using a browser-based kiosk.
- MyQ Scan Review: Review, approve and audit scanned documents before the paper originals are archived. Designed for trustworthy digitization requirements such as TR-RESISCAN.
- MyQ Document Processor: Apply OCR, split documents by page interval or barcode, and remove blank pages from Easy Scan jobs.
- Delta synchronization for Microsoft Entra ID: Sync only what has changed, every few minutes, so Entra ID changes reach MyQ much faster.
- IPP pass-through for WPP: Give users advanced finishing and tray options from the print dialog in Windows Protected Print environments.
- Require authentication for IPPS jobs: Reject unauthenticated IPP and IPPS print jobs.

See also: What's New in 10.3 (see page 8)

2.3 MyQ Print Server 10.3 RTM

26 October, 2026

2.3.1 Changes

- Increased the minimum required Software Assurance date to 1 March, 2026. To upgrade to 10.3, your Software Assurance must be valid until at least that date.
- Updated OpenSSL to 3.5.8
- Updated PHP to 8.5.12
- Updated Traefik to 3.7.13

2.3.2 Bug Fixes

- Jobs printed with the HP Universal PCL driver with multiple copies and stapling are stapled together instead of each copy stapled separately.
- Jobs printed with the Ricoh PS driver are always printed in duplex, even when 2-sided printing is turned off in the driver.
- Booklet and stapling options are lost from jobs printed with the Fiery driver.
- Gmail connection used as an outgoing SMTP server fails with an authentication error.
- Enabling **Jobs via MS Universal Print** on a queue fails with the error "Duplicate attribute name in IPP message", and the printer is not available in Windows.
- Scan functions, such as Scan to Me, fail on devices with an Embedded Lite license with the error "Printer has no license for scanning".

2.3.3 Device Certifications

- Added support for Canon imageFORCE C3026.
- Added support for Epson AM-C10000.
- Added support for Epson DS-71000.
- Added support for HP LaserJet MFP X53052.
- Added support for HP Color LaserJet MFP X77823 and X77830, HP LaserJet MFP X72826 and X72831, HP Color LaserJet Enterprise MFP 4801 and X47635, with embedded terminal.
- Added support for HP LaserJet Enterprise 5501 and 6500, HP Color LaserJet Enterprise 4701 and X45135.
- Added support for Ricoh P C300W.

2.4 Component Versions

	Apache	**Apache SSL**	**Server SSL**	**Firebird**	**PHP**	**PHP SSL**	**C++ Runtimes**	**Traefik**	**MAKO**
MyQ Print Server 10.3 RTM	2.4.68	3.6.2	3.5.7	WI-V4.0.7.3271	8.5.12	3.5.7	VC++ 2015-2022 (**vc17**) - 14.44.35112.1	3.7.11	8.4

MyQ Print Server 10.3 RC	2.4.68	3.6.2	3.5.7	WI-V4.0.7.3271	8.5.9	3.5.7	VC++ 2015-2022 (**vc17**) - 14.44.35112.1	3.7.11	8.4

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 18).

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 devices (print-only, scan-only, or copy-only) 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 single-function device, Embedded Lite terminal or Release Station device. 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 (including on scanner-only devices).
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.

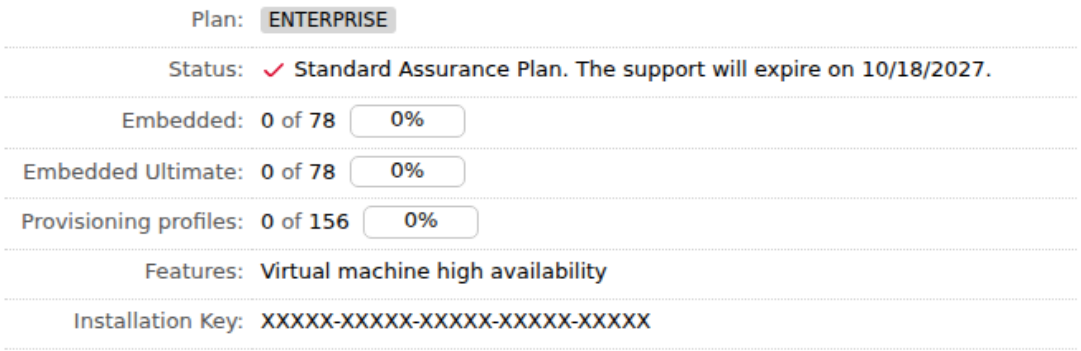
See also:

- https://www.myq-solution.com/en/myq-x#myq-x-plans
- https://www.myq-solution.com/en/software-assurance
- License Settings (see page 18)
- Release Stations (see page 401)
- Configure ScannerVision (see page 224)

3.5 License Settings

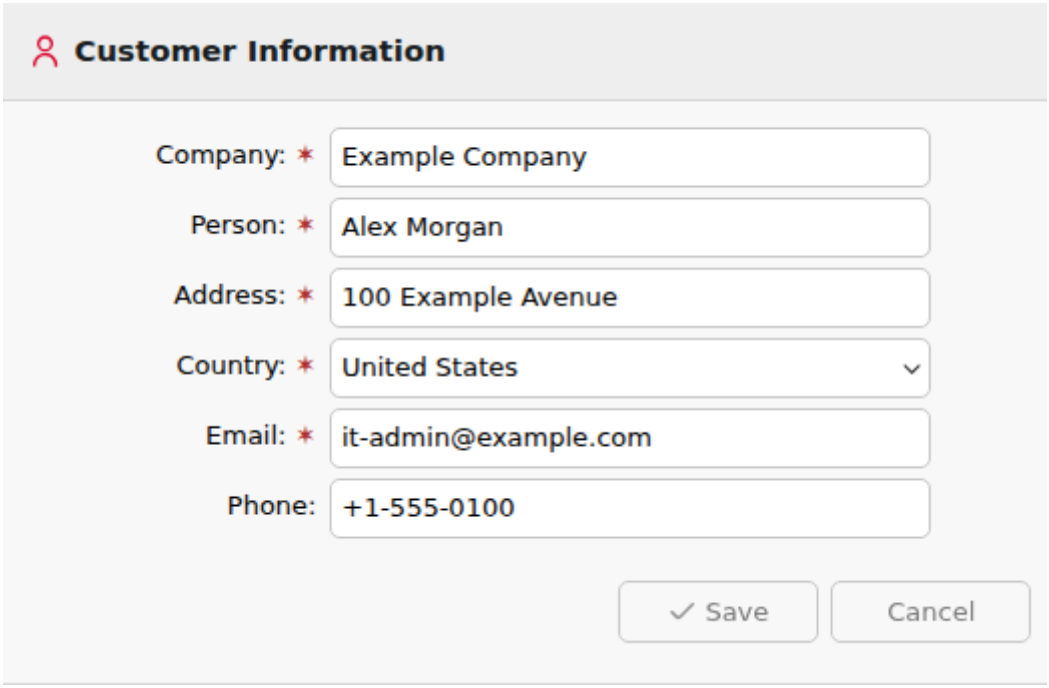
Go to **MyQ > Settings > License** to activate and manage your Installation Key.

When you have an activated license, 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 20)
- Moving Licenses to New Hardware (see page 21)
- Troubleshooting Licenses (see page 22)

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 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.

3.8 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.
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.

See also:

- License Settings (see page 18)
- Manual Activation (see page 20)

- Moving Licenses to New Hardware (see page 21)

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 Print Server – Standalone Mode

4.1.1 MyQ Print Server Hardware Requirements – Up to 600 Devices

Devices	1-10	11-100	101-300	301-600
Physical Core*	3	4	6	8
RAM	6 GB	8 GB	12 GB	14 GB
Storage space	30 GB	33 GB - 350 GB	380 GB - 1TB	1.4 TB - 2TB

* When using the Credit/Quota feature, 1 additional physical core is recommended.

Valid for a typical use case:

- Print job spooling via Windows spooler or directly to MyQ print queue
- Integrated Firebird database – installed automatically
- Activated Job Parser
- Activated Job Archiving
- High number of Office documents printed via email/web/mobile
- Use of MyQ Desktop Client (MDC) or
    - Use of MyQ Smart Job Manager (SJM)
    - Use of MyQ Smart Print Services (SPS)
- Watermarks used in queues
- Heavy usage of MyQ API
- 170 users per device (up to 100,000 users total)
- Heavy printing
- 30% active user sessions at once
- Embedded terminal installed on all devices

4.2 MyQ Print Server – Site Mode (Central Server & Site Servers Architecture)

4.2.1 Site Servers Hardware Requirements

Devices	1-10	11-100	101-300	301-600	601 - 30,000
Physical Core	5	6	8	10	10
RAM	6 GB	8 GB	12 GB	14 GB	14 GB
Minimum number of servers	1x Central server 1x Site server	1x Central server 1x Site server	1x Central server 1x Site server	1x Central server 1x Site server	1x Central server More Site servers with max 600 devices each
Storage space	30 GB	33 GB - 350 GB	380 GB - 1TB	1,4T - 2 TB	2 TB per 600 devices

4.2.2 Valid for a Typical Use Case

- Print job spooling via Windows spooler or directly to MyQ print queue
- Integrated Firebird database – installed automatically
- Activated Job Parser
- Activated Credit Accounting
- Activated Quota
- Activated Job Archiving
- High number of Office documents printed via email/web/mobile
- Use of MyQ Desktop Client (MDC) or
    - Use of MyQ Smart Job Manager (SJM)
    - Use of MyQ Smart Print Services (SPS)
- Watermarks used in queues
- Heavy usage of MyQ API
- 170 users per device (up to 100,000 users total)
- Heavy printing
- 30% active user sessions at once
- Embedded terminal installed on all devices
- User synchronization from Central Server
- Data replication to Central Server

4.2.3 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.

4.2.4 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
- 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

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 Print Server installation files are approximately 700 MB.

The annual printing volume for 1 printer is approximately 10,000 jobs; it is possible to multiply this value for the particular number of printers.

Jobs	**10,000**	**100,000**	**1,000,000**
Data folder size (jobs, main DB, log DB)	35 GB	300 GB	3.5 TB

Counted for jobs with 2.9 MB size.

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

By default, jobs are deleted every 7 days.

The Job archiving feature needs additional free space in data storage due to used configuration.

A dedicated disk for MyQ Data storage (jobs, main database and log database) is recommended.

During upgrades of the MyQ Print Server system, the actual size of the MyQ installation on the server (including MyQ database) may temporarily grow up to four times.
The size of the MyQ database depends on the size and complexity of your printing environment (number of users, printing devices, sent jobs etc.).

4.3.5 Storage Performance

- minimum 100 IOPS required.
- RAID data storage supported.
- for systems with a large number of direct queues, it is strongly recommended using SSD.

4.3.6 MyQ Desktop Client

If there are 100 - 1,000 or more client computers using MyQ Desktop Client (MDC) (or MyQ Smart Job Manager (SJM) and/or MyQ Smart Print Services (SPS)), the MyQ Print Server requires 2+ physical cores just for the MyQ Desktop Client operations. The recommended configuration may vary according to the system load.

4.3.7 Recommended Number of Users and Groups

Users: up to 100,000 (30,000 - 60,000 per one synchronizing line). Depends on the length and number of fields for synchronization.
Groups: up to 40,000/10 tree levels (group in group in group). Each user can be in up to 50 groups.

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 117).

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.

Terminal packages may use additional ports. Check the particular terminal package specification for details.

4.5.1 Printer Status

Make sure to create an exception that allows ICMP Echo Requests/Replies (Ping) through your Windows Firewall, as MyQ uses it by default to check the printer status.

4.5.2 Incoming Ports

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

Transport Protocol	Port	Configurable	Description
TCP	**21**	Yes (WebUI)	FTP protocol for receiving scans(1). The server runs in passive mode only and each data connection runs over a dynamic port in the range 49152-65535.
TCP	**25**	Yes (WebUI)	SMTP over StartTLS(2) for Scan Management function, receiving email notifications from printers, and for receiving emails with jobs.
TCP	**443**	Yes (Easy Config)	HTTPS protocol for: • Accessing MyQ web interface. • Mobile printing (AirPrint/Mopria; printing URL `/ipp-airPrint/<queue name>`). • IPPS printing. • Communication with Embedded terminals. • Job roaming among MyQ servers. Before MyQ X 10.2, this port was 8090. Its use is enabled for upgraded installations only.
TCP	**515**	Yes (WebUI)	LPR protocol for print job transmission to the MyQ server.
TCP	**587**	Yes (WebUI)	SMTPS protocol. Used in the same scenarios as SMTP.
TCP	**9100**	Yes (WebUI)	RAW protocol(3) for print job transmission to the MyQ server.

- (1) FTP ports might not be required for newer embedded terminals (the majority of the latest 8.2+ terminals except for Epson) where scanning can be performed over HTTP. The dependency in certain situations is based on the particular device models within your organization. Since MyQ 10.2 Print Server, the FTP server can be also completely turned off in the *Settings – Network* section of the MyQ Web Admin Interface.
- (2) Regarding the requirements for SMTP ports, the MyQ SMTP Server can be turned off in MyQ Print Server's *Settings – Network,* and these incoming ports closed as well since MyQ 10.2. This is possible if you do not intend to use MyQ

Print Server as an SMTP server in your MFDs to redirect email communication from the device for the Scan to Me[2] feature on the device's native panel.

- (3) RAW ports are required only when queues using them exist. RAW reception for a queue is configured in *Queues – queue's detail – Job Receiving – Jobs via RAW protocol*.

PM Server

Transport Protocol	Port	Configurable	Description
TCP	**631**	No	Port for Mobile print via IPP.
TCP	**717**	No	Port for Mobile print via IPPS.
TCP	**9090, 9091**	No	Necessary for remote setup of Kyocera embedded terminals.
TCP	**9092**	No	Felica reader
TCP	**9093**	Yes (WebUI)	Authentication / Authorization.
TCP	**9094**	No	Driver access, mobile access.
TCP	**9095**	Yes (WebUI)	Spooler service.
TCP	**9097**	Yes (WebUI)	Log information event.
TCP	**9098**	Yes (WebUI)	Job status event.
TCP	**9099**	Yes (WebUI)	Thrift access.
TCP	**9101**	No	User session service.

4.5.3 Outgoing Ports

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

2. https://docs.myq-solution.com/en/print-server/10.2/scan-to-me

Transport Protocol	Port	Description
TCP	**443**	HTTPS port for: • License activation server. The MyQ license server address is `http://license2.myq.cz/`. • Other enabled services from Settings→External Systems (Microsoft Universal Print, One Drive, ...)
TCP	**515**	LPR protocol for print job transmission from MyQ to printing devices.
TCP	**631**	IPP protocol for print job transmission from MyQ to printing devices.
TCP	**9100**	Raw protocol for print job transmission from MyQ to printing devices.
TCP	**10040**	MPP/MPPS protocol for print job transmission from MyQ to printing devices.

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

Transport Protocol	Port	Default	Description
TCP	Custom	**110**	Connection to email server via POP3 protocol for receiving jobs via email.
TCP	Custom	**143/993**	Connection to email server via IMAP/IMAPS protocol for receiving jobs via email.
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**	Connection to MyQ Central Server.

Transport Protocol	Port	Default	Description
UDP	Custom	**161**	SNMP protocol for communication with printing devices. Answer from printer is returned on a dynamic port.
TCP	Custom	**-**	Connection to External credit account.

- As for outgoing SMTP ports, port 587 is used for email transmission via Microsoft Exchange Online or Gmail (in Settings – Connections); in the case of the Classic SMTP Server method, the connection and port are configured in Settings – Network.

MyQ can connect to dynamic ports in the following contexts:

Transport Protocol	Port	Description
UDP	Dynamic	Communication with MDC (Former SJM and SPS). The port range is 49152 - 65535. Not required with MDC 10.2+.

4.5.4 Embedded Packages Ports

Kyocera	
If SSL is on, it's used for the following events:	Events are notified internally to the embedded application. No network communication is used.
MyQ Server (Protocol: Port - Description)	• HTTPS: 443 (default), configurable in MyQ Easy Config. HTTP on port 8090 is deprecated. • SMTP: 25 (default), configurable in **MyQ > Settings > Network > SMTP**. Used for Panel Scan to email.

Package **(Protocol: Port - Description)**	• Port is randomly selected during installation based on the available unused ports, within the range 8081 - 8381. Port is used only for internal communication (local host). • TCP: (OUT) 11108 - TCP link to device. Send request to Printers. **Kyocera 8.0+** A random TCP port is opened on each package service start/ restart, to be used for receiving scans over FTP. The package then tries to configure the Windows firewall to open the port for outside connections.
Printer **(Protocol: Port - Description)**	• TCP: (IN/OUT) 11108 - TCP link to device. Usage: Receive requests from Package. • TCP: (IN) 10040 - Usage: Use printer as a proxy for TCP communication. • UDP: (IN) 11108 in - UDP Link to device. Multipurpose. It dispatches all the received UDP packages. Usage: Receive requests to get local jobs. • UDP: (OUT) 11108 - Send broadcast to printers. GetJobs (Local Spooling) • TCP: (IN/OUT_ 10030 - TCP link to device. Usage: Receive requests or responses from other devices. • TCP: (IN) 10010 - Usage: Receive raw data of print jobs for local direct print job. • TCP: (IN) 10011 - Usage: Receive raw data of print jobs for local hold job. • TCP: (IN) 10013 - Usage: Receive raw data of print jobs for local delegate job. • TCP: (IN) 10020 - Usage: Receive raw data of print jobs for local LPR jobs. • TCP: (IN) 10012 - Usage: Receive raw data of print jobs for local Pull Print jobs. **Note**: Other ports used by the printer (common for all printers. Eg. 9100 for RAW printing, etc.).

- Pay attention to the Incoming Ports section, specifically the **PM Server** since it is an essential component for configuring Kyocera devices remotely, communicating with Kyocera or Kyocera Lite embedded terminals, and providing Kyocera-specific features supported by the vendor's print drivers.

HP	
If SSL is on, it's used for the following events:	All types of events go through SSL.
MyQ Server (Protocol: Port - Description)	• HTTPS: 443 (default), configurable in MyQ Easy Config. HTTP on port 8090 is deprecated. • SMTP: 25 (default), configurable in **MyQ > Settings > Network > SMTP**. Used for Panel Scan to email.
Package (Protocol: Port - Description)	• Port is randomly selected during installation based on the available unused ports, within the range 8081 - 8381. Port is used only for internal communication (local host).
Printer (Protocol: Port - Description)	• (OUT) 57627 - non SSL. • (OUT) 7627 - SSL.
Toshiba	
If SSL is on, it's used for the following events:	All types of events go through SSL.
MyQ Server (Protocol: Port - Description)	• HTTPS: 443 (default), configurable in MyQ Easy Config. HTTP on port 8090 is deprecated. • SMTP: 25 (default), configurable in **MyQ > Settings > Network > SMTP**. Used for Panel Scan to email.
Package (Protocol: Port - Description)	• Port is randomly selected during installation based on the available unused ports, within the range 8081 - 8381. Port is used only for internal communication (local host).

Printer (Protocol: Port - Description)	• (OUT) 49629, 50083 - non SSL. • (OUT) 49630, 50083 - SSL.
Xerox	
If SSL is on, it's used for the following events:	Always SSL
MyQ Server (Protocol: Port - Description)	• HTTPS: 443 (default), configurable in MyQ Easy Config. HTTP on port 8090 is deprecated. • SMTP: 25 (default), configurable in **MyQ > Settings > Network > SMTP**. Used for Panel Scan to email.
Package (Protocol: Port - Description)	• Port is randomly selected during installation based on the available unused ports, within the range 8081 - 8381. Port is used only for internal communication (local host).
Printer (Protocol: Port - Description)	• HTTPS: (OUT) 443 - secure connection • SNMP: (OUT) 161 - Used to set up the configuration of the printer.
Canon	
If SSL is on, it's used for the following events:	Events are notified internally to the embedded application. No network communication is used.
MyQ Server (Protocol: Port - Description)	• HTTPS: 443 (default), configurable in MyQ Easy Config. HTTP on port 8090 is deprecated. • SMTP: 25 (default), configurable in **MyQ > Settings > Network > SMTP**. Used for Panel Scan to email.

Package **(Protocol: Port - Description)**	• Port is randomly selected during installation based on the available unused ports, within the range 8081 - 8381. Port is used only for internal communication (local host). • TCP: (OUT) 11108 - TCP link to device. Send request to Printers.
Printer **(Protocol: Port - Description)**	• TCP: 11108 - TCP link to device. Usage: Receive requests from Package. • TCP: 10040 - Usage: Use printer as a proxy for TCP communication. **Note**: Other ports used by the printer (common for all printers. Eg 9100 for raw printing, etc.).
Ricoh	
If SSL is on, it's used for the following events:	Events are notified internally to the embedded application. No network communication is used.

Package **(Protocol: Port - Description)**	• Port is randomly selected during installation based on the available unused ports, within the range 8081 - 8381. Port is used only for internal communication (local host). • TCP: 49109 - sends live application logs from the device. • TCP: 11108 - TCP link to device. Usage: Receive requests from Package. • TCP: 10040 - Usage: Use printer as a proxy for TCP communication. • UDP: 11108 in - UDP Link to device. Multipurpose. It dispatches all the received UDP packages. Usage: Receive requests to get local jobs. • UDP: 11108 out - Send broadcast to printers. GetJobs (Local Spooling) • TCP: 10030 - TCP link to device. Usage: Receive requests or responses from other devices. • TCP: 10010 - Usage: Receive raw data of print jobs for local direct print job. • TCP: 10011 - Usage: Receive raw data of print jobs for local hold job. • TCP: 10013 - Usage: Receive raw data of print jobs for local delegate job. • TCP: 10020 - Usage: Receive raw data of print jobs for local LPR jobs. • TCP: 10012 - Usage: Receive raw data of print jobs for local Pull Print jobs. **Note**: Other ports used by the printer (common for all printers. Eg 9100 for raw printing, etc.).
Sharp	
If SSL is on, it's used for the following events:	All types of events go through SSL.
MyQ Server **(Protocol: Port - Description)**	• HTTPS: 443 (default), configurable in MyQ Easy Config. HTTP on port 8090 is deprecated. • SMTP: 25 (default), configurable in **MyQ > Settings > Network > SMTP**. Used for Panel Scan to email.

Package **(Protocol: Port - Description)**	• Port is randomly selected during installation based on the available unused ports, within the range 8081 - 8381. Port is used only for internal communication (local host).
Printer **(Protocol: Port - Description)**	Any port from the <0-65535> range. Default: • (OUT) 10080 - non SSL • (OUT) 10443 - SSL
Epson	
If SSL is on, it's used for the following events:	All types of events go through SSL.
MyQ Server **(Protocol: Port - Description)**	• HTTPS: 443 (default), configurable in MyQ Easy Config. HTTP on port 8090 is deprecated. • SMTP: 25 (default), configurable in **MyQ > Settings > Network > SMTP**. Used for Panel Scan to email.
Package **(Protocol: Port - Description)**	• Port is randomly selected during installation based on the available unused ports, within the range 8081 - 8381. Port is used only for internal communication (local host).
Printer **(Protocol: Port - Description)**	• (OUT) 80 - non SSL • (OUT) 443 - SSL

- Pay attention to the Incoming Ports section, specifically the **FTP server** since only selected Epson devices support scanning over HTTPS, and that support is limited, thus using FTP might be required.

Lexmark	
If SSL is on, it's used for the following events:	All communication goes through a secured connection.
MyQ Server (Protocol: Port - Description)	• HTTPS: 443 (default), configurable in MyQ Easy Config. HTTP on port 8090 is deprecated. • SMTP: 25 (default), configurable in **MyQ > Settings > Network > SMTP**. Used for Panel Scan to email.
Package (Protocol: Port - Description)	• Port is randomly selected during installation based on the available unused ports, within the range 8081 - 8381. Port is used only for internal communication (local host). • TCP: (OUT) 11108 - TCP link to device. Send request to Printers.
Printer (Protocol: Port - Description)	• TCP: 11108 - TCP link to device. Usage: Receive requests from Package. **Note**: Other ports used by the printer (common for all printers. E.g. 9100 for raw printing, etc.).
Fujifilm	
If SSL is on, it's used for the following events:	All communication goes through a secured connection.
MyQ Server (Protocol: Port - Description)	• HTTPS: 443 (default), configurable in MyQ Easy Config. HTTP on port 8090 is deprecated. • SMTP: 25 (default), configurable in **MyQ > Settings > Network > SMTP**. Used for Panel Scan to email.
Package (Protocol: Port - Description)	• Port is randomly selected during installation based on the available unused ports, within the range 8081 - 8381. Port is used only for internal communication (local host).

Printer **(Protocol: Port - Description)**	• (OUT) 443 - secure connection
KATUN	
If SSL is on, it's used for the following events:	All communication goes through a secured connection.
MyQ Server **(Protocol: Port - Description)**	• HTTPS: 443 (default), configurable in MyQ Easy Config. HTTP on port 8090 is deprecated. • SMTP: 25 (default), configurable in **MyQ > Settings > Network > SMTP**. Used for Panel Scan to email.
Package **(Protocol: Port - Description)**	• Port is randomly selected during installation based on the available unused ports, within the range 8081 - 8381. Port is used only for internal communication (local host).
Printer **(Protocol: Port - Description)**	• (OUT) 443 - secure connection

Some of the above-mentioned ports can be changed in cases of conflicts with other applications.

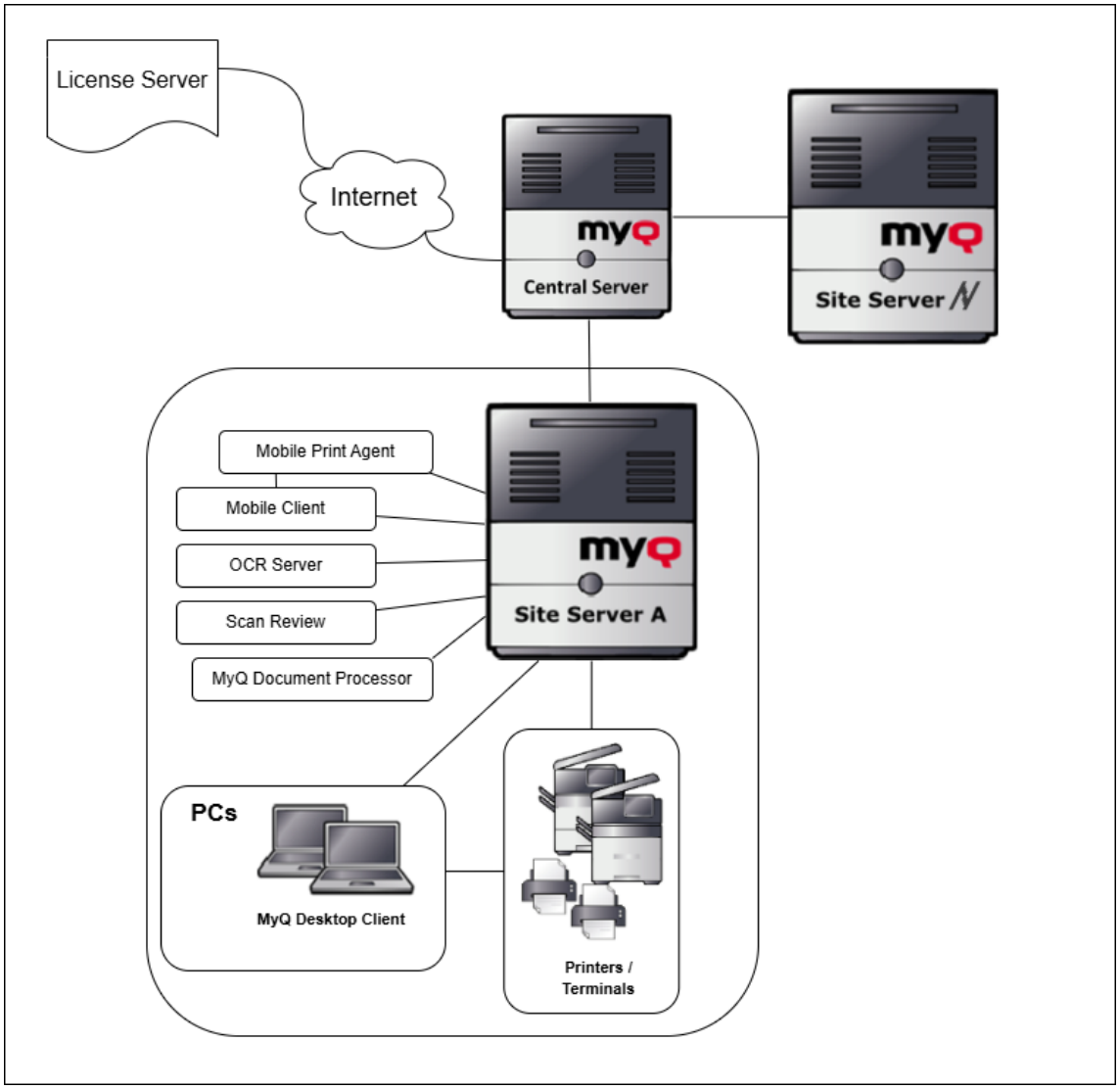
Conflicts of the communication ports with other software will be indicated by the error message **Windows socket error 10048**.

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
- (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 Supported Terminals and Applications

MyQ X 10.3 supports the following embedded terminals and applications.

4.7.1 Embedded Terminals

Device	Embedded Terminal Version				
Brother	10.2				
Canon		10.1	8.2 (EoL)		
Epson	10.2	10.1 (EoL)			
HP	10.2	10.1 (EoL)			
Fujifilm	10.2				
KATUN	10.2				
Kyocera	10.2	10.1 (EoL)	8.2		
Kyocera Lite				8.1	
Lexmark		10.1		8.1 (EoL)	
Ricoh		10.1	8.2 (EoL)		
Sharp	10.2	10.1 (EoL)			
Sharp Luna		10.1		8.1 (EoL)	
Toshiba			8.2		
Xerox	10.2				7.6 (EoL)

4.7.2 Applications

Name	Version
MyQ X Chromebook Client	10.2 RC 2
MyQ Desktop Client	10.2+
MyQ Document Processor	1.0
MyQ X Mobile Client	10.2
MyQ X Mobile Print Agent	1.3
MyQ Theme Editor	1.0
Scan Review	1.0
ScannerVision	9.1+

4.8 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.

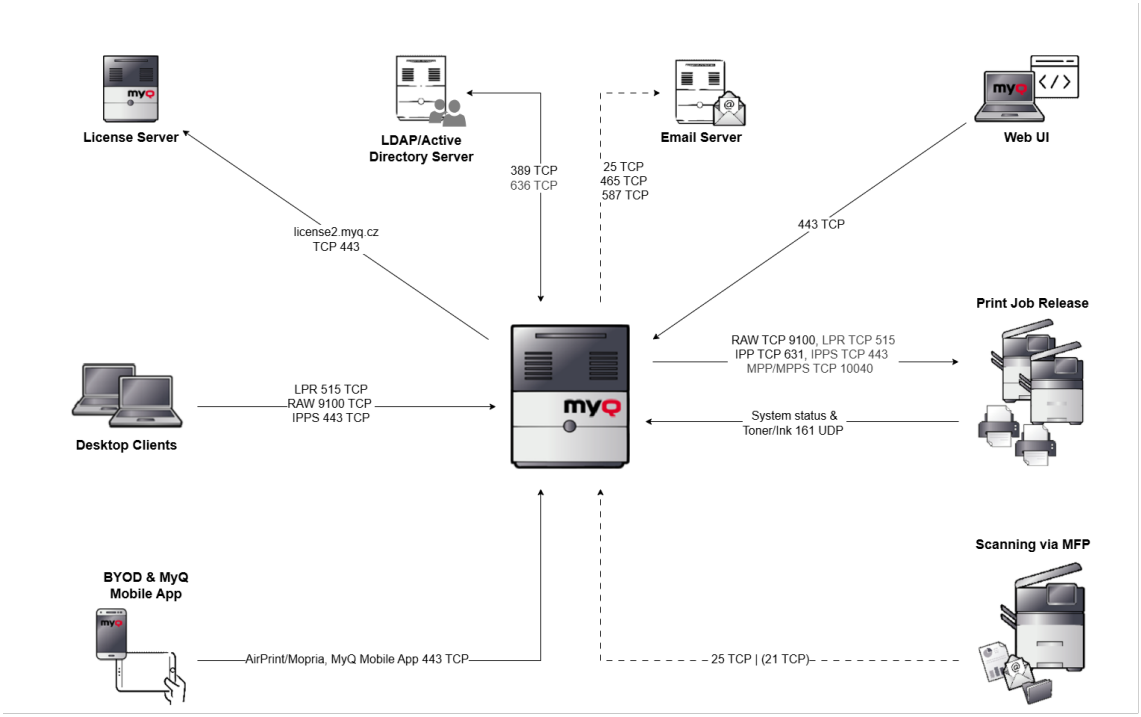
Use the diagrams below as a reference map before completing the checklist. Focus on the connections that apply to your environment, especially traffic that crosses sites, network zones, or external services.



For the current port, protocols and version-specific defaults, see the MyQ X Server guide:

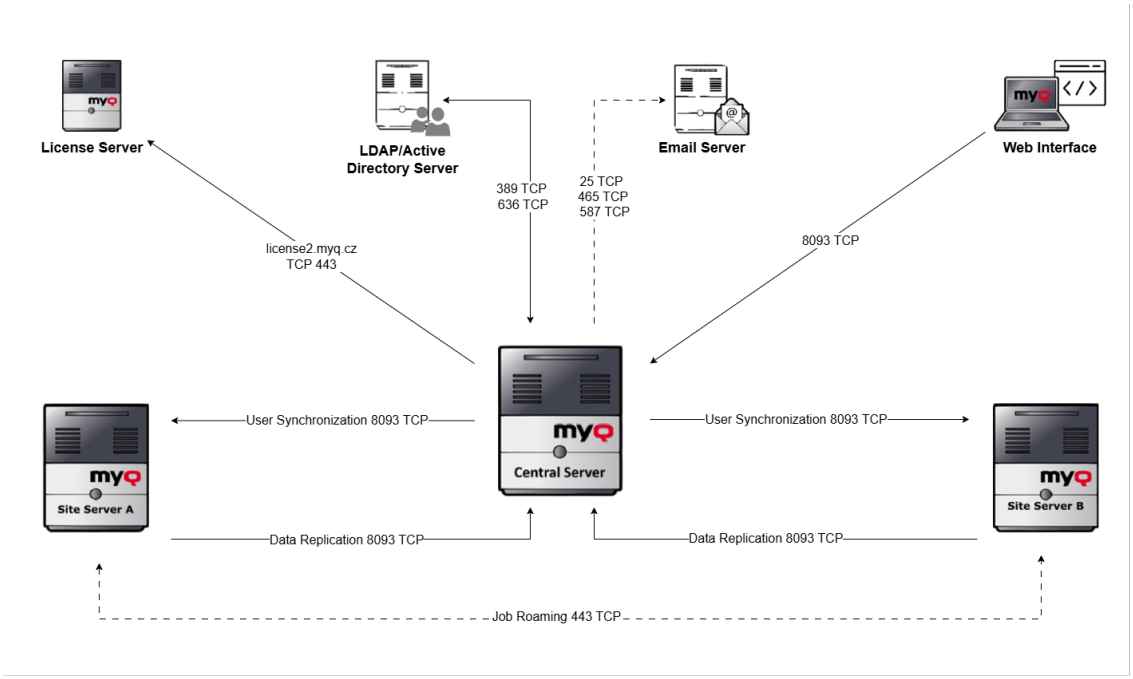
- (10.3) Main Communication Ports

4.8.1 Standalone Print Server



2 Print Server

4.8.2 Central/Site Environment



3 Central Server

4.8.3 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.

4.9 Embedded Terminal Features

The following information is subject to change without notice as we are constantly improving our software. Please contact your MyQ Certified Partner or Account Manager for the latest information about version compatibility.

- 4.9.1 Brother (see page 50)
- 4.9.2 Canon (see page 54)
- 4.9.3 Epson (see page 57)
- 4.9.4 Fujifilm (see page 60)
- 4.9.5 HP (see page 64)
- 4.9.6 Katun (see page 67)
- 4.9.7 Kyocera (see page 71)
- 4.9.8 Lexmark (see page 74)
- 4.9.9 Ricoh (see page 77)
- 4.9.10 Sharp (see page 80)
- 4.9.11 Toshiba (see page 83)
- 4.9.12 Triumph Adler (see page 86)
- 4.9.13 UTAX (see page 89)
- 4.9.14 Xerox (see page 93)

4.9.1 Brother

Feature	Function	10.2
Deployment & Administration		

Feature	Function	10.2
	Automated Printer Discovery and Remote Installation	✅
	Device Status Monitoring	✅
Authentication		
	ID Card / Username & Password / PIN	✅
	QR Code Login with MyQ X Mobile Client	❌
	Guest Login	❌
	ID Card Registration	✅
	NEW Unknown Card Registration	✅
Accounting		
	Print Accounting	✅
	Offline Accounting	❌
	Per Job Accounting *	❌
	Panel (Scan, Copy, Print) Accounting	✅
	Accounting of USB Devices (MyQ Desktop Client)	❌
	Projects*	✅
	Cost Centers*	✅
	Credit (Pre-paid & Top-up)*	✅
	Quota*	✅
Printing		
	Print All after Login	❌
	Job Select / Delete / Favorite / History	✅

Feature	Function	10.2
	Adjustable Print Options on the Device	✓
	Job Preview	✗
	USB Drive Print and Scan	✓
	Cancel Jobs After Logout	✗
	Client Spooling (MyQ Desktop Client)	✓
Finishing Options		
	Staple & Punch	✗
	Adjustable Staple & Punch on the Device	✗
Job Submission		
	Easy Print (Driverless Print from Cloud or Network Drives)	✗
	Folder Browsing	✗
	Email / Web Upload / Hot Folder	✓
	AirPrint / Mopria / Mobile Client	✓
	Universal Print by Microsoft	✓
	RAW/LPR/IPP(S)	✓
Scanning		
	Device Scan to Me (Email, Folder) *	✓
	Easy Scan including Adjustable Scan Options *	✓
	Scan to Email / Folder / FTP / Secure Link *	✓
	Scan to Cloud (including OneDrive for Business, SharePoint Online) *	✓
	Folder Browsing	✗

Feature	Function	10.2
	Advanced Scanning including Custom Parameters, Codebooks, and Metadata	✗
	OCR (PDF, TXT, other **)	✓
	Skip Blank Pages	✓
	Advanced Workflows & Document Processing (ScannerVision)	✗
Copying		
	Easy Copy incl. Adjustable Copy Options - implemented as Scan & Print	✗
	Easy Copy of ID cards	✗
	Skip Blank Pages	✗
Personalization		
	Easy Actions (Scan) *	✓
	NEW Favorite Actions (from supported Terminal Actions)	✗
	Web UI WCAG 2.1 level AA	✓ Web UI
	Multi Language Support	✓
	Embedded Themes & Custom Logo, Icons	✗
Extra Features		
	Guest Scan, Copy, Print	✗
	Print Job & Scan Archiving	✓
	Offline Login	✗
	Device Spooling	✗

- *** Limitations can be found in documentation**

4.9.2 Canon

Feature	Function	10.1
Deployment & Administration		
	Automated Printer Discovery *	✔
	Device Status Monitoring	✔
Authentication		
	ID Card / Username & Password / PIN with Two-Factor	✔
	QR Code Login with MyQ X Mobile Client	✔
	Guest Login	✔
	ID Card Registration	✔
Accounting		
	Print Accounting	✔
	Offline Accounting	✔
	Per Job Accounting	✔
	Panel (Scan, Copy, Print) Accounting	✔
	Accounting of USB Devices (MyQ Desktop Client)	✔
	Projects	✔
	Cost Centers	✔
	Credit (Pre-paid & Top-up)	✔
	Quota	✔

Feature	Function	10.1
Printing		
	Print All after Login	✅
	Job Select / Delete / Favorite / History	✅
	Adjustable Print Options on the Device	✅
	Job Preview	✅
	USB Drive Print and Scan	Manual only
	Cancel Jobs After Logout	✅
	Client Spooling (MyQ Desktop Client)	✅
Finishing Options		
	Staple & Punch	✅
	Adjustable Staple & Punch on the Device	✅
Job Submission		
	Canon CPCA Support	✅
	Easy Print (Driverless Print from Cloud or Network Drives)	✅
	Folder Browsing	✅
	Email / Web Upload / Hot Folder	✅
	AirPrint / Mopria / Mobile Client	✅
	Universal Print by Microsoft	✅
	RAW/LPR/IPP(S)	✅
Scanning		
	Device Scan to Me (Email, Folder)	✅

Feature	Function	10.1
	Easy Scan including Adjustable Scan Options	✓
	Scan to Email / Folder / FTP / Secure Link	✓
	Scan to Cloud (including OneDrive for Business, SharePoint Online)	✓
	Folder Browsing	✓
	Advanced Scanning including Custom Parameters, Codebooks, and Metadata	✓
	OCR (PDF, TXT)	✓
	Skip Blank Pages	✗
	Advanced Workflows & Document Processing (ScannerVision)	✗
Copying		
	Easy Copy including Adjustable Copy Options	✓
	Easy Copy of ID cards	✓
	Skip Blank Pages	✗
Personalization		
	Easy Actions (Print, Scan, Copy, Fax)	✓
	Web UI WCAG 2.1 level AA	✓ Web UI
	Multi Language Support	✓
	Embedded Themes & Custom Logo, Icons	✓
Extra Features		
	CPCA Print Driver Support	✓
	Guest Scan, Copy, Fax	✓

Feature	Function	10.1
	Print, Scan Archiving	✓
	Offline Login	✓
	Device Spooling	✗

- *** Remote installation is not available.**

4.9.3 Epson

Feature	Function	10.1	10.2
Deployment & Administration			
	Automated Printer Discovery and Remote Installation	✓	✓
	Device Status Monitoring	✓	✓
Authentication			
	ID Card / Username & Password / PIN with Two-Factor	✓	✓
	QR Code Login with MyQ X Mobile Client	✓	✓
	Guest Login	✓	✓
	ID Card Registration	✓	✓
	NEW Unknown Card Registration	✗	✓
Accounting			
	Print Accounting	✓	✓
	Offline Accounting	✗	✗
	Per Job Accounting	✓	✓

Feature	Function	10.1	10.2
	Panel (Scan, Copy, Print) Accounting	✓	✓
	Accounting of USB Devices (MyQ Desktop Client)	✓	✓
	Projects	✓	✓
	Cost Centers	✓	✓
	Credit (Pre-paid & Top-up)	✓	✓
	Quota	✓	✓
Printing			
	Print All after Login	✓	✓
	Job Select / Delete / Favorite / History	✓	✓
	Adjustable Print Options on the Device	✓	✓
	Job Preview	✓	✓
	USB Drive Print and Scan	✓	✓
	Cancel Jobs After Logout	✗	✗
	Client Spooling (MyQ Desktop Client)	✓	✓
Job Submission			
	Easy Print (Driverless Print from Cloud or Network Drives)	✓	✓
	Folder Browsing	✓	✓
	Email / Web Upload / Hot Folder	✓	✓
	AirPrint / Mopria / Mobile Client	✓	✓
	Universal Print by Microsoft	✓	✓

Feature	Function	10.1	10.2
	RAW/LPR/IPP(S)	✓	✓
Scanning			
	Device Scan to Me (Email, Folder)	✓	✓
	Easy Scan including Adjustable Scan Options	✓	✓
	Scan to Email / Folder / FTP / Secure Link	✓	✓
	Scan to Cloud (including OneDrive for Business, SharePoint Online)	✓	✓
	Folder Browsing	✓	✓
	Advanced Scanning including Custom Parameters, Codebooks, and Metadata	✓	✓
	OCR (PDF, TXT)	✓	✓
	Skip Blank Pages *	✓	✓
	Advanced Workflows & Document Processing (ScannerVision)	✗	✗ **
Copying			
	Easy Copy including Adjustable Copy Options	✗	✗
	Easy Copy of ID cards	✗	✗
	Skip Blank Pages	✗	✗
Personalization			
	Easy Actions (Print, Scan)	✓	✓

Feature	Function	10.1	10.2
	NEW Favorite Actions (from supported Terminal Actions)	✗	✓
	Web UI WCAG 2.1 level AA	✓ Web UI	✓ Web UI
	Multi Language Support	✓	✓
	Embedded Themes & Custom Logo, Icons	✓	✓
Extra Features			
	Guest Scan & Copy	✓	✓
	Embedded Terminal for Standalone Epson Scanners	✓	✓
	Print, Scan Archiving	✓	✓
	Offline Login	✗	✗
	Device Spooling	✗	✗
	EJL + ESC/Page-Color and Remote + ESC/P-R Print Driver Support	✓	✓
	EPSON Workforce Enterprise AM-C 4000/5000/6000	✓	✓

- *** Only models with firmware supporting the functionality.**
- **** Will be included in the future patches.**

4.9.4 Fujifilm

Feature	Function	10.2
Deployment & Administration		
	Automated Printer Discovery and Remote Installation	✓

Feature	Function	10.2
	Device Status Monitoring	✅
Authentication		
	ID Card / Username & Password / PIN with Two-Factor	✅
	QR Code Login with MyQ X Mobile Client	✅
	Guest Login	✅
	ID Card Registration	✅
	NEW Unknown Card Registration	✅
Accounting		
	Print Accounting	✅
	Offline Accounting	❌
	Per Job Accounting	✅
	Panel (Scan, Copy, Print) Accounting	✅
	Accounting of USB Devices (MyQ Desktop Client)	❌
	Projects	✅
	Cost Centers	✅
	Credit (Pre-paid & Top-up)	✅
	Quota	✅
Printing		
	Print All after Login	✅
	Job Select / Delete / Favorite / History	✅
	Adjustable Print Options on the Device	✅

Feature	Function	10.2
	Job Preview	✓
	USB Drive Print and Scan	✓
	Cancel Jobs After Logout	✗
	Client Spooling (MyQ Desktop Client)	✓
Finishing Options		
	Staple & Punch	✗
	Adjustable Staple & Punch on the Device	✗
Job Submission		
	Easy Print (Driverless Print from Cloud or Network Drives)	✓
	Folder Browsing	✓
	Email / Web Upload / Hot Folder	✓
	AirPrint / Mopria / Mobile Client	✓
	Universal Print by Microsoft	✓
	RAW/LPR/IPP(S)	✓
Scanning		
	Device Scan to Me (Email, Folder)	✓
	Easy Scan including Adjustable Scan Options	✓
	Scan to Email / Folder / FTP / Secure Link	✓
	Scan to Cloud (including OneDrive for Business, SharePoint Online)	✓
	Folder Browsing	✓

Feature	Function	10.2
	Advanced Scanning including Custom Parameters, Codebooks, and Metadata	✅
	OCR (PDF, TXT, other *)	✅
	Skip Blank Pages	✅
	Advanced Workflows & Document Processing (ScannerVision)	✅
Copying		
	Easy Copy incl. Adjustable Copy Options - implemented as Scan & Print	✅
	Easy Copy of ID cards	❌
	Skip Blank Pages	✅
Personalization		
	Easy Actions (Print, Scan, Copy (Scan&Print))	✅
	NEW Favorite Actions (from supported Terminal Actions)	✅
	Web UI WCAG 2.1 level AA	✅ Web UI
	Multi Language Support	✅
	Embedded Themes & Custom Logo, Icons	✅
Extra Features		
	Guest Scan, Copy, Print	✅
	Print Job & Scan Archiving	✅
	Offline Login	❌
	Device Spooling	❌

- *** Additional formats are supported for OCR with Advanced Workflows (ScannerVision).**
- **** Will be included in the future patches.**

4.9.5 HP

Feature	Function	10.1	10.2
Deployment & Administration			
	Automated Printer Discovery and Remote Installation	✓	✓
	Device Status Monitoring	✓	✓
Authentication			
	ID Card / Username & Password / PIN with Two-Factor	✓	✓
	QR Code Login with MyQ X Mobile Client	✓	✓
	Guest Login	✓	✓
	ID Card Registration	✓	✓
	NEW Unknown Card Registration	✗	✓
Accounting			
	Print Accounting	✓	✓
	Offline Accounting	✗	✗
	Per Job Accounting	✓	✓
	Panel (Scan, Copy, Print) Accounting	✓	✓
	Accounting of USB Devices (MyQ Desktop Client)	✓	✓

Feature	Function	10.1	10.2
	Projects	✓	✓
	Cost Centers	✓	✓
	Credit (Pre-paid & Top-up)	✓	✓
	Quota	✓	✓
Printing			
	Print All after Login	✓	✓
	Job Select / Delete / Favorite / History	✓	✓
	Adjustable Print Options on the Device	✓	✓
	Job Preview	✓	✓
	USB Drive Print and Scan	✓	✓
	Cancel Jobs After Logout	✗	✗
	Client Spooling (MyQ Desktop Client)	✓	✓
Finishing Options			
	Staple & Punch	✓	✓
	Adjustable Staple & Punch on the Device	✓	✓
Job Submission			
	Easy Print (Driverless Print from Cloud or Network Drives)	✓	✓
	Folder Browsing	✓	✓
	Email / Web Upload / Hot Folder	✓	✓
	AirPrint / Mopria / Mobile Client	✓	✓
	Universal Print by Microsoft	✓	✓

Feature	Function	10.1	10.2
	RAW/LPR/IPP(S)	✓	✓
Scanning			
	Device Scan to Me (Email, Folder)	✓	✓
	Easy Scan including Adjustable Scan Options	✓	✓
	Scan to Email / Folder / FTP / Secure Link	✓	✓
	Scan to Cloud (including OneDrive for Business, SharePoint Online)	✓	✓
	Folder Browsing	✓	✓
	Advanced Scanning including Custom Parameters, Codebooks, and Metadata	✓	✓
	OCR (PDF, TXT, other *)	✓	✓
	Skip Blank Pages	✓	✓
	Advanced Workflows & Document Processing (ScannerVision)	✓	✓
Copying			
	Easy Copy including Adjustable Copy Options	✓	✓
	Easy Copy of ID cards	✗	✗
	Skip Blank Pages	✗	✗
Personalization			
	Easy Actions (Print, Scan, Copy, Fax)	✓	✓
	NEW Favorite Actions (from supported Terminal Actions)	✗	✓

Feature	Function	10.1	10.2
	Web UI WCAG 2.1 level AA	✅ Web UI	✅ Web UI
	Multi Language Support	✅	✅
	Embedded Themes & Custom Logo, Icons	✅	✅
Extra Features			
	Embedded Terminal for Standalone HP Scanners	✅	✅
	Guest Scan, Copy, Fax	✅	✅
	Print, Scan Archiving	✅	✅
	Offline Login	❌	❌
	Device Spooling	❌	❌

- *** Additional formats are supported for OCR with Advanced Workflows (ScannerVision).**
- **** Will be included in future patches.**

4.9.6 Katun

Feature	Function	10.2
Deployment & Administration		
	Automated Printer Discovery and Remote Installation	✅
	Device Status Monitoring	✅
Authentication		
	ID Card / Username & Password / PIN with Two-Factor	✅
	QR Code Login with MyQ X Mobile Client	✅

Feature	Function	10.2
	Guest Login	✓
	ID Card Registration	✓
	NEW Unknown Card Registration	✓
Accounting		
	Print Accounting	✓
	Offline Accounting	✗
	Per Job Accounting	✓
	Panel (Scan, Copy, Print) Accounting	✓
	Accounting of USB Devices (MyQ Desktop Client)	✗
	Projects	✓
	Cost Centers	✓
	Credit (Pre-paid & Top-up)	✓
	Quota	✓
Printing		
	Print All after Login	✓
	Job Select / Delete / Favorite / History	✓
	Adjustable Print Options on the Device	✓
	Job Preview	✓
	USB Drive Print and Scan	✓
	Cancel Jobs After Logout	✗
	Client Spooling (MyQ Desktop Client)	✓
Finishing Options		

Feature	Function	10.2
	Staple & Punch	✗
	Adjustable Staple & Punch on the Device	✗
Job Submission		
	Easy Print (Driverless Print from Cloud or Network Drives)	✓
	Folder Browsing	✓
	Email / Web Upload / Hot Folder	✓
	AirPrint / Mopria / Mobile Client	✓
	Universal Print by Microsoft	✓
	RAW/LPR/IPP(S)	✓
Scanning		
	Device Scan to Me (Email, Folder)	✓
	Easy Scan including Adjustable Scan Options	✓
	Scan to Email / Folder / FTP / Secure Link	✓
	Scan to Cloud (including OneDrive for Business, SharePoint Online)	✓
	Folder Browsing	✓
	Advanced Scanning including Custom Parameters, Codebooks, and Metadata	✓
	OCR (PDF, TXT, other)	✓
	Skip Blank Pages	✓
	Advanced Workflows & Document Processing (ScannerVision)	✓

Feature	Function	10.2
Copying		
	Easy Copy incl. Adjustable Copy Options - implemented as Scan & Print	✅
	Easy Copy of ID cards	❌
	Skip Blank Pages	✅
Personalization		
	Easy Actions (Print, Scan)	✅
	NEW Favorite Actions (from supported Terminal Actions)	✅
	Web UI WCAG 2.1 level AA	✅ Web UI
	Multi Language Support	✅
	Embedded Themes & Custom Logo ****, Icons	✅
Extra Features		
	Guest Scan, Copy, Print	✅
	Print Job & Scan Archiving	✅
	Offline Login	❌
	Device Spooling	❌

- *** Additional formats are supported for OCR with Advanced Workflows (ScannerVision).**
- **** Will be included in the future patches**

4.9.7 Kyocera

Feature	Function	10.1	10.2
Deployment & Administration			
	Automated Printer Discovery and Remote Installation	✓	✓
	Device Status Monitoring	✓	✓
Authentication			
	ID Card / Username & Password / PIN with Two-Factor	✓	✓
	QR Code Login with MyQ X Mobile Client	✓	✓
	Guest Login	✓	✓
	ID Card Registration	✓	✓
	NEW Unknown Card Registration	✗	✓
Accounting			
	Print Accounting	✓	✓
	Offline Accounting	✓	✓
	Per Job Accounting	✓	✓
	Panel (Scan, Copy, Print) Accounting	✓	✓
	Accounting of USB Devices (MyQ Desktop Client)	✓	✓
	Projects	✓	✓
	Cost Centers	✓	✓
	Credit (Pre-paid & Top-up)	✓	✓

Feature	Function	10.1	10.2
	Quota	✓	✓
Printing			
	Print All after Login	✓	✓
	Job Select / Delete / Favorite / History	✓	✓
	Adjustable Print Options on the Device	✓	✓
	Job Preview	✓	✓
	USB Drive Print and Scan	✓	✓
	Discard Jobs After Logout	✓	✓
	Client Spooling (MyQ Desktop Client)	✓	✓
Finishing Options			
	Staple & Punch	✓	✓
	Adjustable Staple & Punch on the Device	✓	✓
Job Submission			
	Easy Print (Driverless Print from Cloud or Network Drives)	✓	✓
	Folder Browsing	✓	✓
	Email / Web Upload / Hot Folder	✓	✓
	AirPrint / Mopria / Mobile Client	✓	✓
	Universal Print by Microsoft	✓	✓
	RAW/LPR/IPP(S)	✓	✓
Scanning			
	Device Scan to Me (Email, Folder)	✓	✓

Feature	Function	10.1	10.2
	Easy Scan including Adjustable Scan Options	✓	✓
	Scan to Email / Folder / FTP / Secure Link	✓	✓
	Scan to Cloud (including OneDrive for Business, SharePoint Online)	✓	✓
	Folder Browsing	✓	✓
	Advanced Scanning including Custom Parameters, Codebooks, and Metadata	✓	✓
	OCR (PDF, TXT, other *)	✓	✓
	Skip Blank Pages	✓	✓
	Advanced Workflows & Document Processing (ScannerVision)	✓	✓
Copying			
	Easy Copy incl. Adjustable Copy Options	✓	✓
	Easy Copy of ID cards	✓	✓
	Skip Blank Pages	✓	✓
Personalization			
	Easy Actions (Print, Scan, Copy, Fax)	✓	✓
	NEW Favorite Actions (from supported Terminal Actions)	✗	✓
	Web UI WCAG 2.1 level AA	✓ Web UI	✓ Web UI
	Multi Language Support	✓	✓
	Embedded Themes & Custom Logo, Icons	✓	✓
Extra Features			

Feature	Function	10.1	10.2
	Guest Scan, Copy, Fax	✅	✅
	Print, Scan, Fax and Copy Archiving ***	✅	✅
	Offline Login	✅	✅
	Device Spooling	✅	✅

- *** Additional formats are supported for OCR with Advanced Workflows (ScannerVision).**
- ** **Will be arriving in next patches.**
- *** **Depending on the machine model and firmware.**

4.9.8 Lexmark

Feature	Function	10.1
Deployment & Administration		
	Automated Printer Discovery and Remote Installation	✅
	Device Status Monitoring	✅
Authentication		
	ID Card / Username & Password / PIN with Two-Factor	✅
	QR Code Login with MyQ X Mobile Client	✅
	Guest Login	❌
	ID Card Registration	✅
Accounting		
	Print Accounting	✅
	Per Job Accounting	✅

Feature	Function	10.1
	Panel (Scan, Copy, Print) Accounting	✅
	Accounting of USB Devices (MyQ Desktop Client)	✅
	Projects	✅
	Cost Centers	✅
	Credit (Pre-paid & Top-up)	✅
	Quota	✅
Printing		
	Print All after Login	✅
	Job Select / Delete / Favorite / History	✅
	Adjustable Print Options on the Device	✅
	Job Preview	✅
	USB Drive Print and Scan	✅
	Cancel Jobs After Logout	✅ (10.1.6+)
	Client Spooling (MyQ Desktop Client)	✅
Job Submission		
	Easy Print (Driverless Print from Cloud or Network Drives)	✅
	Folder Browsing (Easy Print)	✅
	Email / Web Upload / Hot Folder	✅
	AirPrint / Mopria / Mobile Client	✅
	Universal Print by Microsoft	✅
	RAW/LPR/IPP(S)	✅

Feature	Function	10.1
Scanning		
	Device Scan to Me (Email, Folder)	✅
	Easy Scan including Adjustable Scan Options	✅
	Scan to Email / Folder / FTP / Secure Link	✅
	Scan to Cloud (including OneDrive for Business, SharePoint Online)	✅
	Folder Browsing	✅
	Advanced Scanning including Custom Parameters, Codebooks, and Metadata	✅
	OCR (PDF, TXT)	✅
	Skip Blank Pages	✅
	Advanced Workflows & Document Processing (ScannerVision)	✅
Copying		
	Easy Copy including Adjustable Copy Options - implemented as Scan & Print	✅
	Easy Copy of ID cards	❌
	Skip Blank Pages	❌
Personalization		
	Easy Actions (Print, Scan, Copy(Scan&Print))	Scan, Copy, Print only
	Web UI WCAG 2.1 level AA	✅ Web UI
	Multi Language Support	✅
	Embedded Themes & Custom Logo, Icons	✅

Feature	Function	10.1
Extra Features		
	Guest Scan, Copy, Fax	✗
	Print Archiving	✗

4.9.9 Ricoh

Feature	Function	10.1
Deployment & Administration		
	Automated Printer Discovery and Remote Installation	✓
	Device Status Monitoring	✓
Authentication		
	ID Card / Username & Password / PIN with Two-Factor	✓
	QR Code Login with MyQ X Mobile Client	✓
	Guest Login	✓
	ID Card Registration	✓
Accounting		
	Print Accounting	✓
	Offline Accounting	✓
	Per Job Accounting	✓
	Panel (Scan, Copy, Print) Accounting	✓

Feature	Function	10.1
	Accounting of USB Devices (MyQ Desktop Client)	✔
	Projects	✔
	Cost Centers	✔
	Credit (Pre-paid & Top-up)	✔
	Quota	✔
Printing		
	Print All after Login	✔
	Job Select / Delete / Favorite / History	✔
	Adjustable Print Options on the Device	✔
	Job Preview	✔
	USB Drive Print and Scan	Panel USB
	Cancel Jobs After Logout	✔
	Client Spooling (MyQ Desktop Client)	✔
Finishing Options		
	Staple & Punch	✔
	Adjustable Staple & Punch on the Device	✔
Job Submission		
	Easy Print (Driverless Print from Cloud or Network Drives)	✔
	Folder Browsing	✔
	Email / Web Upload / Hot Folder	✔
	AirPrint / Mopria / Mobile Client	✔

Feature	Function	10.1
	Universal Print by Microsoft	✅
	RAW/LPR/IPP(S)	✅
Scanning		
	Device Scan to Me (Email, Folder)	✅
	Easy Scan including Adjustable Scan Options	✅
	Scan to Email / Folder / FTP / Secure Link	✅
	Scan to Cloud (including OneDrive for Business, SharePoint Online)	✅
	Folder Browsing	✅
	Advanced Scanning including Custom Parameters, Codebooks, and Metadata	✅
	OCR (PDF, TXT)	✅
	Skip Blank Pages	✅
	Advanced Workflows & Document Processing (ScannerVision)	❌
Copying		
	Easy Copy including Adjustable Copy Options	✅
	Easy Copy of ID cards	✅
	Skip Blank Pages	❌
Personalization		
	Easy Actions (Print, Scan, Copy, Fax)	✅
	Web UI WCAG 2.1 level AA	✅ Web UI
	Multi Language Support	✅

Feature	Function	10.1
	Embedded Themes & Custom Logo, Icons	✓
Extra Features		
	Guest Scan, Copy, Fax	✓
	Print, Scan Archiving	✓
	Offline Login (Ricoh Smart SDK platform)	✓
	Device Spooling (Ricoh Smart SDK platform)	✓

4.9.10 Sharp

Feature	Function	10.1	10.2
Deployment & Administration			
	Automated Printer Discovery and Remote Installation	✓	✓
	Device Status Monitoring	✓	✓
Authentication			
	ID Card / Username & Password / PIN with Two-Factor *	✓	✓
	QR Code Login with MyQ X Mobile Client	✓	✓
	Guest Login	✓	✓
	ID Card Registration	✓	✓
	NEW Unknown Card Registration	✗	✓
Accounting			
	Print Accounting	✓	✓
	Per Job Accounting	✓	✓

Feature	Function	10.1	10.2
	Panel (Scan, Copy, Print) Accounting	✓	✓
	Accounting of USB Devices (MyQ Desktop Client)	✓	✓
	Projects	✓	✓
	Cost Centers	✓	✓
	Credit (Pre-paid & Top-up)	✓	✓
	Quota	✓	✓
	Offline Accounting	✗	✗
Printing			
	Print All after Login	✓	✓
	Job Select / Delete / Favorite / History	✓	✓
	Adjustable Print Options on the Device	✓	✓
	Job Preview	✓	✓
	USB Drive Print and Scan	Panel only	Panel only
	Cancel Jobs After Logout	✗	✗
	Client Spooling (MyQ Desktop Client)	✓	✓
Job Submission			
	Easy Print (Driverless Print from Cloud or Network Drives) *	✓	✓
	Folder Browsing *	✓	✓
	Email / Web Upload / Hot Folder	✓	✓
	AirPrint / Mopria / Mobile Client	✓	✓

Feature	Function	10.1	10.2
	Universal Print by Microsoft	✓	✓
	RAW/LPR/IPP(S)	✓	✓
Scanning			
	Device Scan to Me (Email, Folder) *	✓	✓
	Easy Scan including Adjustable Scan Options *	✓	✓
	Scan to Email / Folder / FTP / Secure Link *	✓	✓
	Scan to Cloud (including OneDrive for Business, SharePoint Online) *	✓	✓
	Folder Browsing *	✓	✓
	Advanced Scanning including Custom Parameters, Codebooks, and Metadata *	✓	✓
	OCR (PDF, TXT) *	✓	✓
	Skip Blank Pages *	✓	✓
	Advanced Workflows & Document Processing (ScannerVision)	✗	✗
Copying			
	Easy Copy including Adjustable Copy Options *	✓	✓
	Easy Copy of ID cards *	✓	✓
	Skip Blank Pages	✗	✗
Personalization			
	Easy Actions (Print, Scan, Copy, Fax) *	✓	✓

Feature	Function	10.1	10.2
	Web UI WCAG 2.1 level AA	✅ Web UI	✅ Web UI
	Multi Language Support	✅	✅
	Embedded Themes & Custom Logo, Icons	✅	✅
	NEW Favorite Actions (from supported Terminal Actions)	❌	✅
Extra Features			
	Print, Scan Archiving	✅	✅
	Embedded Terminal for Sharp Luna Models **	✅	❌
	Offline Login	❌	❌
	Device Spooling	❌	❌

- *** Requires AMX 2 Module.**
- **** See more details in the Sharp documentation.**

4.9.11 Toshiba

Feature	Function	8.2
Deployment & Administration		
	Automated Printer Discovery and Remote Installation	✅
	Device Status Monitoring	✅
Authentication		
	ID Card / Username & Password / PIN with Two-Factor	✅

Feature	Function	8.2
	QR Code Login with MyQ X Mobile Client	✓
	Guest Login	✓
	ID Card Registration	✓
Accounting		
	Print Accounting	✓
	Offline Accounting	✗
	Per Job Accounting	✓
	Panel (Scan, Copy, Print) Accounting	✓
	Accounting of USB Devices (MyQ Desktop Client)	✓
	Projects	✓
	Cost Centers	✓
	Credit (Pre-paid & Top-up)	✓
	Quota	✓
Printing		
	Print All after Login	✓
	Job Select / Delete / Favorite / History	✓
	Adjustable Print Options on the Device	✓
	USB Drive Print and Scan	Panel only
	Discard Jobs After Logout	✗
	Client Spooling (MyQ Desktop Client)	✓
Job Submission		

Feature	Function	8.2
	Email / Web Upload / Hot Folder	✓
	AirPrint / Mopria / Mobile Client	✓
	Universal Print by Microsoft	✓
	RAW/LPR/IPP(S)	✓
Scanning		
	Device Scan to Me (Email, Folder)	✓
	Easy Scan including Adjustable Scan Options	✓
	Scan to Email / Folder / FTP / Secure Link	✓
	Scan to Cloud (including OneDrive for Business, SharePoint Online)	✓
	Advanced Scanning including Custom Parameters, Codebooks, and Metadata	✓
	OCR (PDF, TXT)	✓
	Skip Blank Pages	✗
	Advanced Workflows & Document Processing (ScannerVision)	✗
Copying		
	Easy Copy including Adjustable Copy Options	✗
	Easy Copy of ID cards	✗
	Skip Blank Pages	✗
Personalization		
	Easy Actions (Scan)	Scan Only ✓

Feature	Function	8.2
	Web UI WCAG 2.1 level AA	✓ Web UI
	Multi Language Support	✓
	Embedded Themes & Custom Logo, Icons	✓

4.9.12 Triumph Adler

Feature	Function	10.1	10.2
Deployment & Administration			
	Automated Printer Discovery and Remote Installation	✓	✓
	Device Status Monitoring	✓	✓
Authentication			
	ID Card / Username & Password / PIN with Two-Factor	✓	✓
	QR Code Login with MyQ X Mobile Client	✓	✓
	Guest Login	✓	✓
	ID Card Registration	✓	✓
	NEW Unknown Card Registration	✗	✓
Accounting			
	Print Accounting	✓	✓
	Offline Accounting	✓	✓
	Per Job Accounting	✓	✓

Feature	Function	10.1	10.2
	Panel (Scan, Copy, Print) Accounting	✓	✓
	Accounting of USB Devices (MyQ Desktop Client)	✓	✓
	Projects	✓	✓
	Cost Centers	✓	✓
	Credit (Pre-paid & Top-up)	✓	✓
	Quota	✓	✓
Printing			
	Print All after Login	✓	✓
	Job Select / Delete / Favorite / History	✓	✓
	Adjustable Print Options on the Device	✓	✓
	Job Preview	✓	✓
	USB Drive Print and Scan	✓	✓
	Discard Jobs After Logout	✓	✓
	Client Spooling (MyQ Desktop Client)	✓	✓
Finishing Options			
	Staple & Punch	✓	✓
	Adjustable Staple & Punch on the Device	✓	✓
Job Submission			
	Easy Print (Driverless Print from Cloud or Network Drives)	✓	✓
	Folder Browsing	✓	✓
	Email / Web Upload / Hot Folder	✓	✓

Feature	Function	10.1	10.2
	AirPrint / Mopria / Mobile Client	✓	✓
	Universal Print by Microsoft	✓	✓
	RAW/LPR/IPP(S)	✓	✓
Scanning			
	Device Scan to Me (Email, Folder)	✓	✓
	Easy Scan including Adjustable Scan Options	✓	✓
	Scan to Email / Folder / FTP / Secure Link	✓	✓
	Scan to Cloud (including OneDrive for Business, SharePoint Online)	✓	✓
	Folder Browsing	✓	✓
	Advanced Scanning including Custom Parameters, Codebooks, and Metadata	✓	✓
	OCR (PDF, TXT, other *)	✓	✓
	Skip Blank Pages	✓	✓
	Advanced Workflows & Document Processing (ScannerVision)	✓	✓
Copying			
	Easy Copy incl. Adjustable Copy Options	✓	✓
	Easy Copy of ID cards	✓	✓
	Skip Blank Pages	✓	✓
Personalization			
	Easy Actions (Print, Scan, Copy, Fax)	✓	✓

Feature	Function	10.1	10.2
	NEW Favorite Actions (from supported Terminal Actions)	✗	✓
	Web UI WCAG 2.1 level AA	✓ Web UI	✓ Web UI
	Multi Language Support	✓	✓
	Embedded Themes & Custom Logo, Icons	✓	✓
Extra Features			
	Guest Scan, Copy, Fax	✓	✓
	Print, Scan, Fax and Copy Archiving ***	✓	✓
	Offline Login	✓	✓
	Device Spooling	✓	✓

- *** Additional formats are supported for OCR with Advanced Workflows (ScannerVision).**
- ** **Will be arriving in next patches.**
- *** **Depending on the machine model and firmware.**

4.9.13 UTAX

Feature	Function	10.1	10.2
Deployment & Administration			
	Automated Printer Discovery and Remote Installation	✓	✓
	Device Status Monitoring	✓	✓
Authentication			

Feature	Function	10.1	10.2
	ID Card / Username & Password / PIN with Two-Factor	✓	✓
	QR Code Login with MyQ X Mobile Client	✓	✓
	Guest Login	✓	✓
	ID Card Registration	✓	✓
	NEW Unknown Card Registration	✗	✓
Accounting			
	Print Accounting	✓	✓
	Offline Accounting	✓	✓
	Per Job Accounting	✓	✓
	Panel (Scan, Copy, Print) Accounting	✓	✓
	Accounting of USB Devices (MyQ Desktop Client)	✓	✓
	Projects	✓	✓
	Cost Centers	✓	✓
	Credit (Pre-paid & Top-up)	✓	✓
	Quota	✓	✓
Printing			
	Print All after Login	✓	✓
	Job Select / Delete / Favorite / History	✓	✓
	Adjustable Print Options on the Device	✓	✓
	Job Preview	✓	✓
	USB Drive Print and Scan	✓	✓

Feature	Function	10.1	10.2
	Discard Jobs After Logout	✓	✓
	Client Spooling (MyQ Desktop Client)	✓	✓
Finishing Options			
	Staple & Punch	✓	✓
	Adjustable Staple & Punch on the Device	✓	✓
Job Submission			
	Easy Print (Driverless Print from Cloud or Network Drives)	✓	✓
	Folder Browsing	✓	✓
	Email / Web Upload / Hot Folder	✓	✓
	AirPrint / Mopria / Mobile Client	✓	✓
	Universal Print by Microsoft	✓	✓
	RAW/LPR/IPP(S)	✓	✓
Scanning			
	Device Scan to Me (Email, Folder)	✓	✓
	Easy Scan including Adjustable Scan Options	✓	✓
	Scan to Email / Folder / FTP / Secure Link	✓	✓
	Scan to Cloud (including OneDrive for Business, SharePoint Online)	✓	✓
	Folder Browsing	✓	✓
	Advanced Scanning including Custom Parameters, Codebooks, and Metadata	✓	✓
	OCR (PDF, TXT, other *)	✓	✓

Feature	Function	10.1	10.2
	Skip Blank Pages	✓	✓
	Advanced Workflows & Document Processing (ScannerVision)	✓	✓
Copying			
	Easy Copy incl. Adjustable Copy Options	✓	✓
	Easy Copy of ID cards	✓	✓
	Skip Blank Pages	✓	✓
Personalization			
	Easy Actions (Print, Scan, Copy, Fax)	✓	✓
	NEW Favorite Actions (from supported Terminal Actions)	✗	✓
	Web UI WCAG 2.1 level AA	✓ Web UI	✓ Web UI
	Multi Language Support	✓	✓
	Embedded Themes & Custom Logo, Icons	✓	✓
Extra Features			
	Guest Scan, Copy, Fax	✓	✓
	Print, Scan, Fax and Copy Archiving ***	✓	✓
	Offline Login	✓	✓
	Device Spooling	✓	✓

- *** Additional formats are supported for OCR with Advanced Workflows (ScannerVision).**
- ** **Will be arriving in next patches.**
- *** **Depending on the machine model and firmware.**

4.9.14 Xerox

Feature	Function	7.6	10.2
Deployment & Administration			
	Automated Printer Discovery and Remote Installation	✓	✓
	Device Status Monitoring	✓	✓
Authentication			
	ID Card / Username & Password / PIN with Two-Factor	✓	✓
	QR Code Login with MyQ X Mobile Client *	✓	✓
	Guest Login	✗	✓
	ID Card Registration	✓	✓
	NEW Unknown Card Registration	✗	✓
Accounting			
	Print Accounting	✓	✓
	Offline Accounting	✗	✗
	Per Job Accounting	✓	✓
	Panel (Scan, Copy, Print) Accounting	✓	✓
	Accounting of USB Devices (MyQ Desktop Client)	✓	✓
	Projects	✓	✓
	Cost Centers	✗	✓
	Credit (Pre-paid & Top-up)	✓	✓

Feature	Function	7.6	10.2
	Quota	✓	✓
Printing			
	Print All after Login **	✗	✓
	Job Select / Delete / Favorite / History	✓	✓
	Adjustable Print Options on the Device	✓	✓
	Job Preview	✗	✓
	USB Drive Print and Scan	✗	✓
	Cancel Jobs After Logout	✗	✗
	Client Spooling (MyQ Desktop Client)	✓	✓
Finishing Options			
	Staple & Punch	✗	✓
	Adjustable Staple & Punch on the Device	✗	✗
Job Submission			
	Easy Print (Driverless Print from Cloud or Network Drives)	✗	✓
	Folder Browsing	✗	✓
	Email / Web Upload / Hot Folder	✓	✓
	AirPrint / Mopria / Mobile Client	✓	✓
	Universal Print by Microsoft	✓	✓
	RAW/LPR/IPP(S)	✓	✓
Scanning			

Feature	Function	7.6	10.2
	Device Scan to Me (Email, Folder)	✓	✓
	Easy Scan including Adjustable Scan Options	✗	✓
	Scan to Email / Folder / FTP / Secure Link	✓	✓
	Scan to Cloud (including OneDrive for Business, SharePoint Online)	✗	✓
	Folder Browsing	✗	✓
	Advanced Scanning including Custom Parameters, Codebooks, and Metadata	✓	✓
	OCR (PDF, TXT, other ***)	✓	✓
	Skip Blank Pages	✗	✗
	Advanced Workflows & Document Processing (ScannerVision)	✗	✗ ****
Copying			
	Easy Copy incl. Adjustable Copy Options	✓	✓
	Easy Copy of ID cards	✗	✗
	Skip Blank Pages	✗	✗
Personalization			
	Easy Actions (Print, Scan, Copy)	✓ ******	✓
	NEW Favorite Actions (from supported Terminal Actions)	✗	✓
	Web UI WCAG 2.1 level AA	✓ Web UI	✓ Web UI

Feature	Function	7.6	10.2
	Multi Language Support	✓	✓
	Embedded Themes & Custom Logo *****, Icons	✓	✓
Extra Features			
	Guest Scan, Copy, Print	✗	✓
	Print Job & Scan Archiving	✗	✓
	Offline Login	✗	✗
	Device Spooling	✗	✗

- *** QR Code needs to be printed and placed on the machine**
- **** No checkbox is available on this login screen so this feature must be enabled on the server and is always applied when turned on.**
- ***** MyQ X OCR Server**
- ****** Will be included in the future patches.**
- ***** **The classic MyQ X login screen is not present on Xerox, the custom logo appears on selected screens.**
- ****** **Version 7.6 supports Scan and Copy Easy Actions only.**

5 Installation

This section shows you how to install the MyQ print management system.

Before you start the installation, make sure your system is up to date and meets the requirements as described in System Requirements (see page 24).

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

1. Download the latest available version of MyQ X Print Server from the MyQ Community portal.
2. Run the executable file. The **Select Setup Language** dialog box appears.
3. Select your language and click **OK**. The Select Destination Location dialog box appears.
4. Select the folder where you wish to install MyQ. The default path is: *C:\Program Files\MyQ*.
5. Click **Install**. MyQ is installed on the server.
6. Click **Finish**. 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 Easy Config application opens and the MyQ database is upgraded. If not, you can run the MyQ Easy Config application directly by keeping the **Finish installation in MyQ Easy Config** option selected.

5.1 Upgrading to MyQ 10.3

Planning your upgrade 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.

Minimum Requirements

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

If you run an earlier version, upgrade to the minimum required version first, 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.

5.1.1 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.

5.1.2 Check Software Assurance Validity

The minimum support requirement is the Standard Software Assurance plan, valid until at least the minimum support date listed above. 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.

5.1.3 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**.

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

5.1.4 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.

5.1.5 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.

5.1.6 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.

5.1.7 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 103).

See also:

- Latest Release Notes (see page 13)
- System Requirements (see page 24)
- Easy Config Database (see page 154)
- Supported Terminals and Applications (see page 46)
- Supported Products
- MyQ Product End-of-Life Policy[3]

5.1.8 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 8)

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.

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

- **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:

- Embedded
- Embedded Lite
- Embedded Ultimate

See also: Licenses (see page 16)

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 different 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 Document Processor, 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: OCR Profiles (see page 620)

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`.

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**, replacing the previous v2. 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 103)

Removed Features

OCR Server

Support for the standalone MyQ OCR Server was removed in 10.3. The feature is replaced by MyQ Document Processor, 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:

- HW-11-T
- 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[4]
3. Apply the required changes and save the file.
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

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

v2 syntax	v3 replacement
`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[5]

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

5.1.9 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.



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.

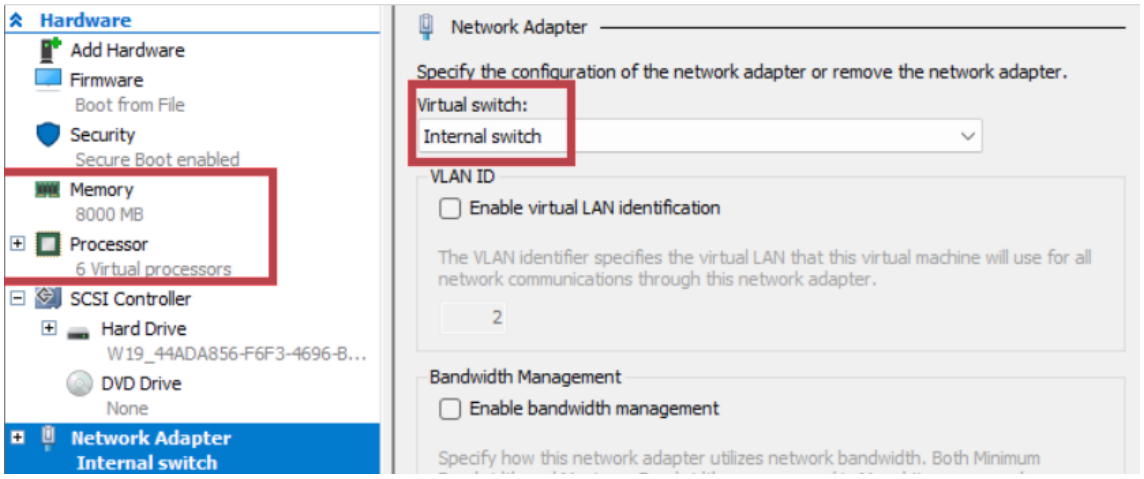
Alternatively, you can run an identical copy of your MyQ system in a network-isolated container. In that case, you must ensure that the container is not able to connect to any external network. With this set up, you do not need to copy job files or perform a data backup and restore – you can simply run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

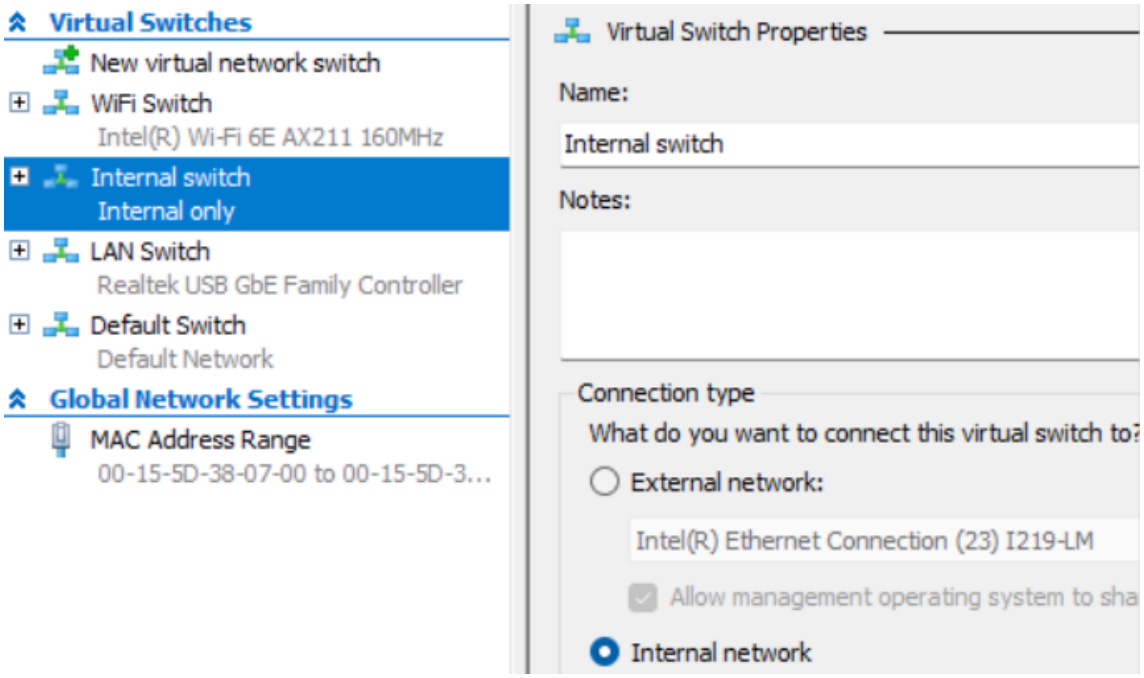
1. Create a test VM (recommended) or prepare a separate physical server.
2. Configure networking so that:

- 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`

> ℹ **See also:**
>
> - Important Changes in 10.3 (see page 100)
> - Generate Support Data (see page 168)

5.1.10 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 97)
- Roll Back an Upgrade (see page 112)
- Troubleshooting Upgrades (see page 115)

5.1.11 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.

Prerequisites

- 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.

5.1.12 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 Setup dialog shows the following message:

```
MyQ is not running. The Setup cannot verify if you have a valid license
for this version. Do you want to continue?

Error: License data missing.
```

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.

5.2 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:
- (v2) Deployment in the Cloud

5.2.1 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`).

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 24)
- Main Communication Ports (see page 29)
- Installation (see page 97)
- Configure ExpressRoute and S2S VPN coexisting connections with Azure PowerShell[6]

5.2.2 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.

6. https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/vpn#architecture

See also:

- System Requirements (see page 24)
- AWS VPC guide[7]
- AWS Site-to-Site VPN documentation[8]
- AWS Customer Gateway guide[9]
- AWS Virtual Private Gateway guide[10]
- AWS Route Table Configuration[11]
- AWS Security Group guide[12]

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.

---

7. https://docs.aws.amazon.com/vpc/latest/userguide/create-vpc.html#create-vpc-and-other-resources
8. https://docs.aws.amazon.com/vpn/latest/s2svpn/SetUpVPNConnections.html
9. https://docs.aws.amazon.com/vpn/latest/s2svpn/SetUpVPNConnections.html#vpn-create-cgw
10. https://docs.aws.amazon.com/vpn/latest/s2svpn/SetUpVPNConnections.html#vpn-create-target-gateway
11. https://docs.aws.amazon.com/vpn/latest/s2svpn/SetUpVPNConnections.html#vpn-configure-route-tables
12. https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

5.2.3 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.
- **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 24)
- Compute Engine Overview[13]
- Cloud VPN Overview[14]
- VPC Networks Documentation[15]
- Google Cloud Console[16]
- Quick Start: Create and Manage VPC Networks[17]
- Classic VPN Topologies[18]
- HA VPN Topologies[19]
- Compute Engine Documentation[20]

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**:

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

- 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.
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.

5.3 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.

5.3.1 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.

5.3.2 Recommended Steps

Before you begin, we recommend that you review our upgrade guidance. See Upgrading to MyQ 10.3 (see page 97).

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.

5.3.3 Migrate to MyQ

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

1. Back up the database in your current OEM installation
2. Set up a clean installation of the MyQ Print 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 details of what data is migrated and further manual steps that are recommended before you can start using your MyQ installation.

Data Migration

All data except some settings are migrated without any changes. Database restore runs as usual, after the restore is finished and all following database upgrades are completed, the corresponding settings are updated.

Settings Migration

Settings are migrated with some transformation due to differences in OEM brands.

User Policies

KNM and aQrate default user policies and permissions are more extensive than the MyQ defaults.

KNM/aQrate default policies & permissions

- **Keep job for reprint:** Yes
- **Color:** Do not change
- **Duplex:** Do not change
- **Staple:** Do not change
- **Punch:** Do not change
- **Toner saving:** Do not change
- **Force A3/B4 to A4 format:** No (KX Driver and Kyocera Mobile Print only)
- **Force B&W printing and page limit in MS Outlook:** No (KX Driver only)
- **Force multiple pages per sheet:** No (KX Driver and Kyocera Mobile Print only)
- **Display Quick Print tab only:** No (KX Driver only)
- **Change Keep job for reprint:** Deny
- **Change color:** Allow
- **Change duplex:** Allow
- **Change staple:** Allow
- **Change punch:** Allow
- **Change toner saving:** Allow
- **Change copies:** Allow
- **Change page range:** Allow

During the migration to MyQ, extra policies are removed and respectively one missing policy is added with its default value selected. Other policies and their values are not changed during the migration.

MyQ default policies & permissions

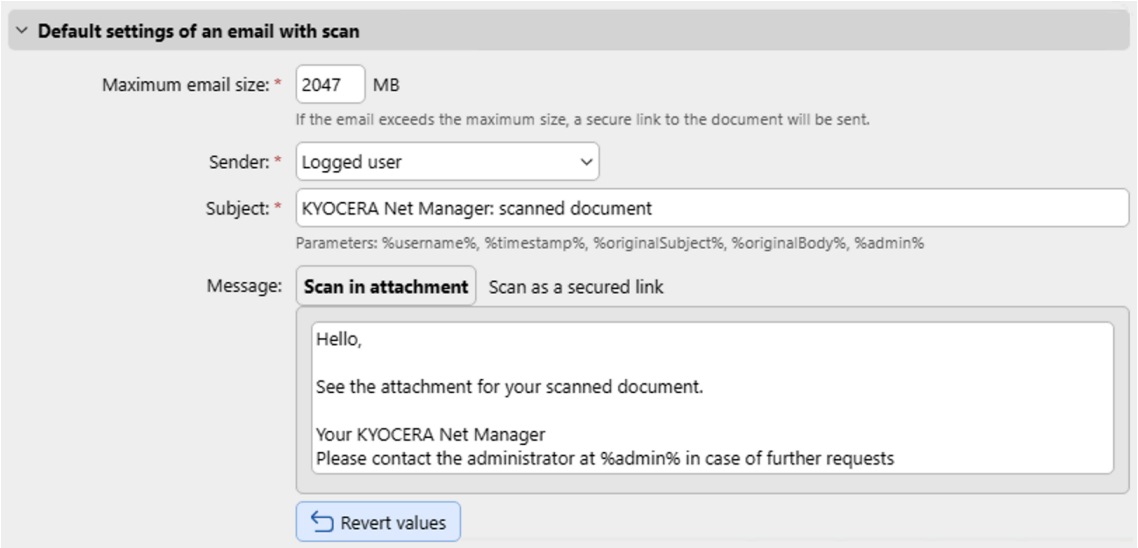
- **Keep job for reprint:** Yes
- **Color:** Do not change
- **Duplex:** Do not change
- **Staple:** Do not change
- **Punch:** Do not change
- **Toner saving:** Do not change
- **Change Keep job for reprint:** Deny
- **Change color:** Allow
- **Change duplex:** Allow
- **Change staple:** Allow

- **Change punch:** Allow
- **Change toner saving:** Allow
- **Change copies:** Allow
- **Change page range:** Allow

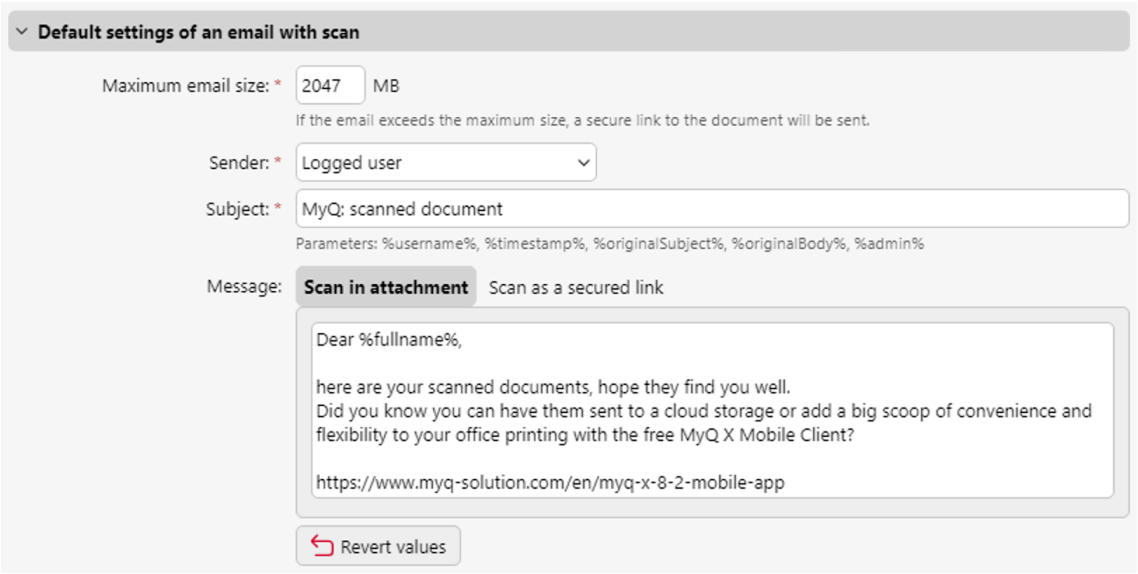
Email Templates

Email templates such as quota notification emails, scanning emails, users pin emails, etc., by default contain OEM brands. During migration all email templates are not changed, except brands are replaced with `MyQ`. So if there were custom email templates in KNM / aQrate, they are preserved on migration, only brands are switched.

By default all email templates do not differ between brands, the only exception is the email template of scan with attachment, which has a different body in MyQ and KNM / aQrate, see screenshots. Since we preserve custom templates on migration and we don't reset email templates to their defaults, it is recommended that customers reset templates to their defaults using the *"Revert values"* buttons in email templates settings and customize them after if needed.



4 KYOCERA Net Manager – emails with scan



5 MyQ – emails with scan

SMTP Sender Email

Settings → Network → Outgoing SMTP Server → Sender email - by default, its value respectively is `MyQ@MyQ.local` or `KNM@KNM.local` or `aQrate@aQrate.local`. If the default value is recognized during the migration, then it's replaced with MyQ's default value. Otherwise, the value is not changed.

5.3.4 Site Name (Central-Site Environments)

Settings → Server Type → Site server → Site name - it may have the OEM brand name as its default value. In this case, it is replaced with `MyQ` during migration; otherwise, it's not changed.

5.4 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.

5.4.1 Prerequisites

- The latest Windows updates are installed on the server.
- All antivirus exclusions are set, and no scans are running on the MyQ directory structure.

- You have a backup of your current database.

> **Limitation:**
> Before an update, go to MyQ Easy Config and set the database password to the default "*masterkey*". Once the update is complete, change the password again.

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 Select Additional tasks dialog appears.
4. Select if you want a MyQ Easy Config shortcut to be created and click **Next**. The rest of the update process is nearly identical to this of installing MyQ.

5.5 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.

5.5.1 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 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 your setup includes embedded terminals, make sure that the required .NET framework version installed in each cluster node. If not, the embedded terminal installation will fail. Further information can be found in the related MyQ Embedded terminal manuals.

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).

5.5.2 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.

5.5.3 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.

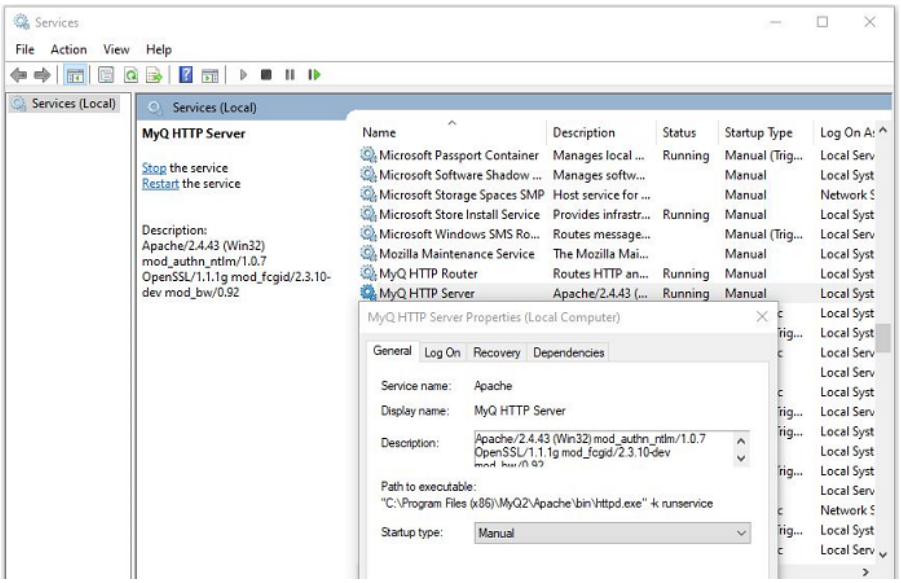
Setting Services to Manual Startup (All Nodes)

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 HTTP Server
- MyQ HTTP Router
- Firebird Server - DefaultInstance
- MyQ Print Server

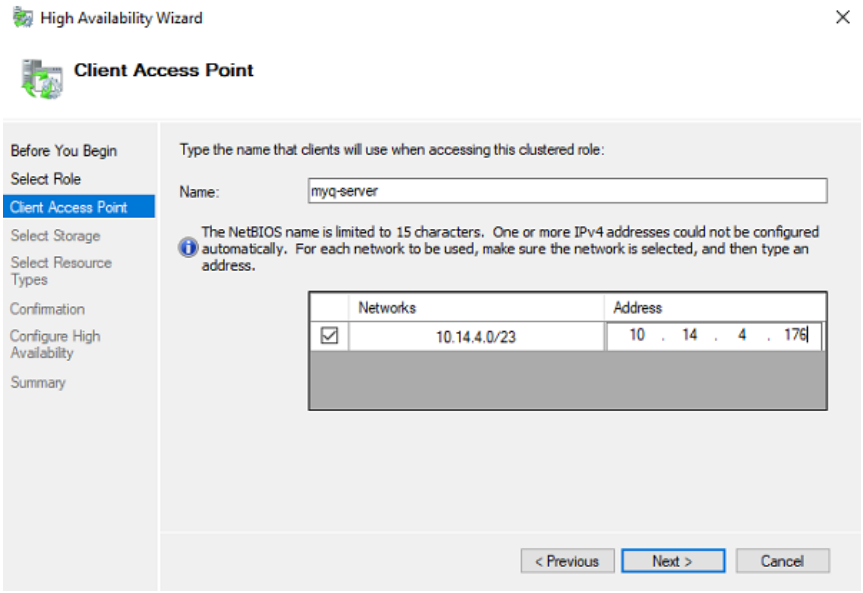
- MyQ Svc (not available in version 8.1+)
- PM Server
- Brand Terminals (only if embedded terminals are used)



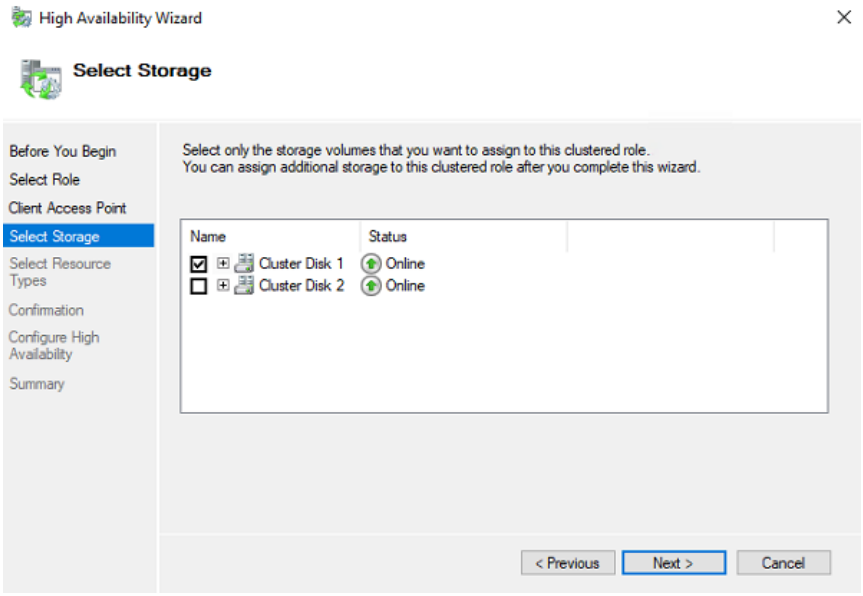
Creating the MyQ Server MS Cluster Role (Failover Cluster Manager)

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.

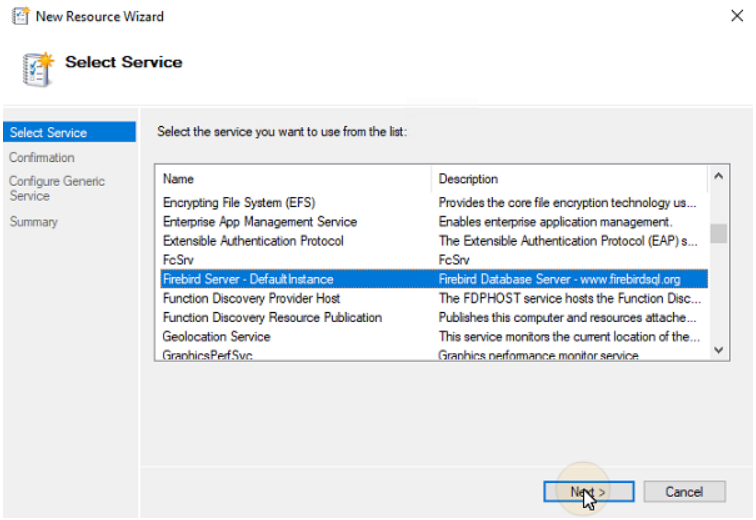
Adding MyQ Resources (Failover Cluster Manager)

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.

Add the Firebird Server – DefaultInstance 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 - DefaultInstance`, 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\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

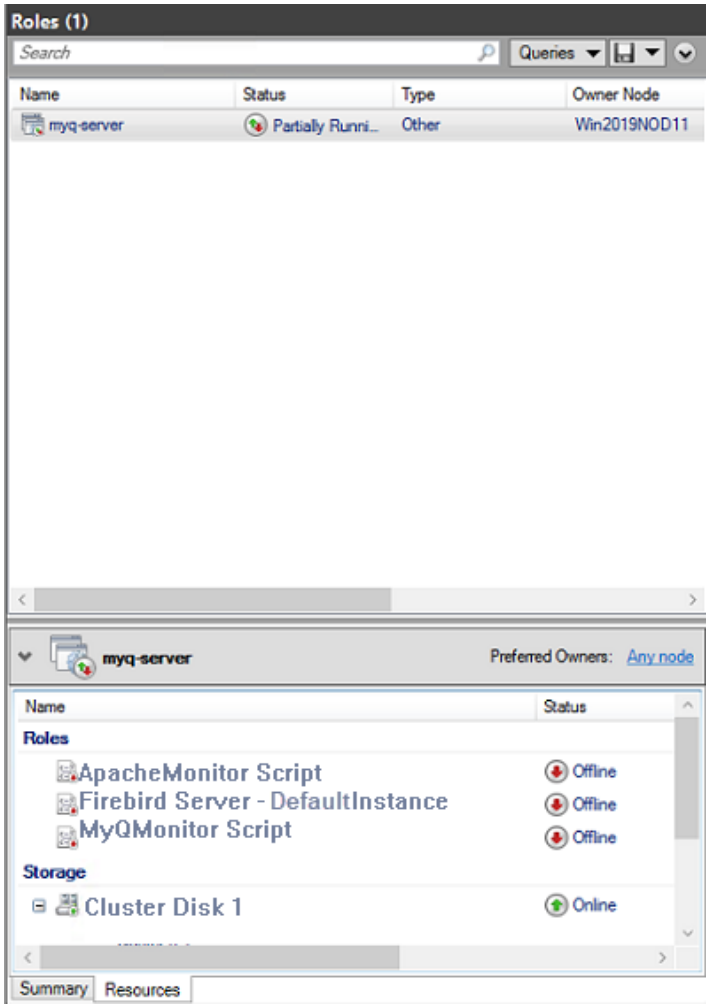
1. Right-click the MyQ server role, click **Add resource** on the shortcut menu, and click **Generic Script**. The New Resource Wizard opens.
2. Enter the path to the **MyQMonitor.jse** script, located in the MyQ installation folder, and click **Next**. The Confirmation tab opens. The default path to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

Add the TerminalsMonitor.jse Script to the Cluster (Embedded Terminals Only)

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

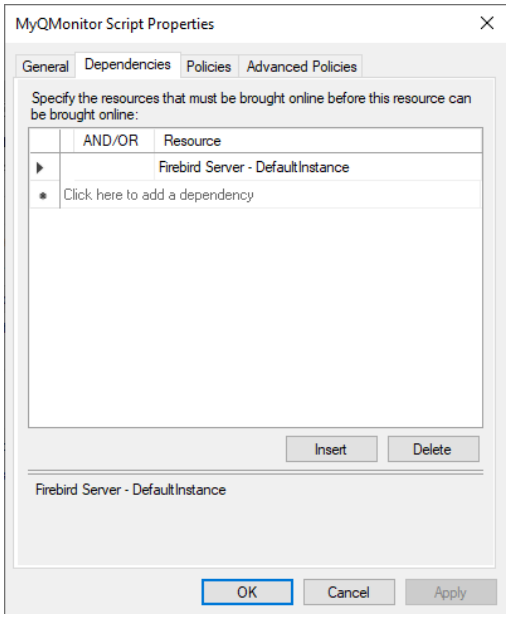
Setting Resources Dependencies (Failover Cluster Manager)

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.



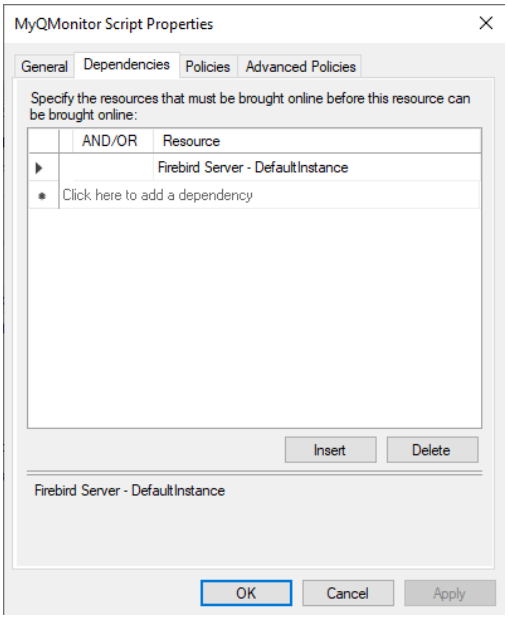
Set the Firebird Server - DefaultInstance Service Dependency

1. In the list at the bottom of the tab, right-click **Firebird Server - DefaultInstance**, and click **Properties**. The Firebird Server - DefaultInstance 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

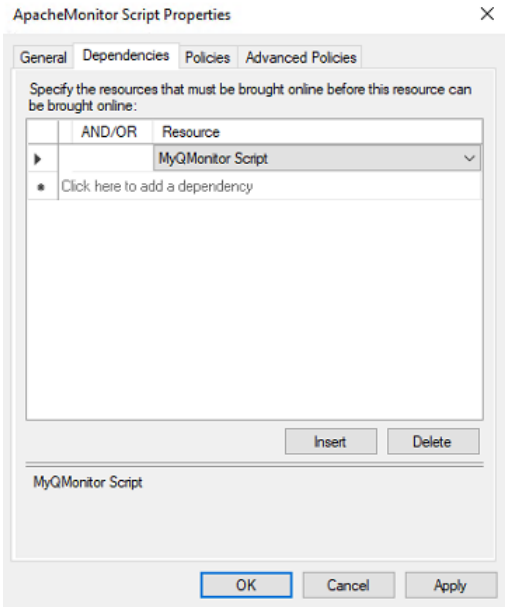
1. In the list at the bottom of the tab, right-click **MyQMonitor Script**, and click **Properties**. The MyQMonitor Script Properties dialog box opens.
2. In the dialog box, open the **Dependencies** tab, add the **Firebird Server - DefaultInstance**, and click **OK**. The dependency is set.



Set the ApacheMonitor Script Dependency

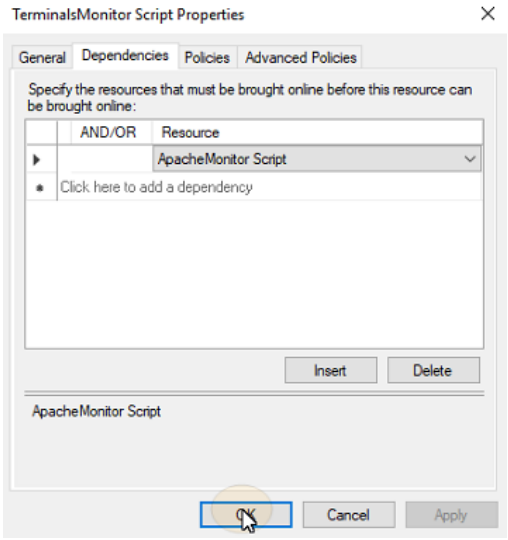
1. In the list at the bottom of the tab, right-click **ApacheMonitor Script**, and click **Properties**. The ApacheMonitor Script Properties dialog box opens.

2. In the dialog box, open the **Dependencies** tab, add the **MyQMonitor Script**, and click **OK**. The dependency is set.



Set the TerminalsMonitor Script Dependency (Embedded Terminals Only)

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

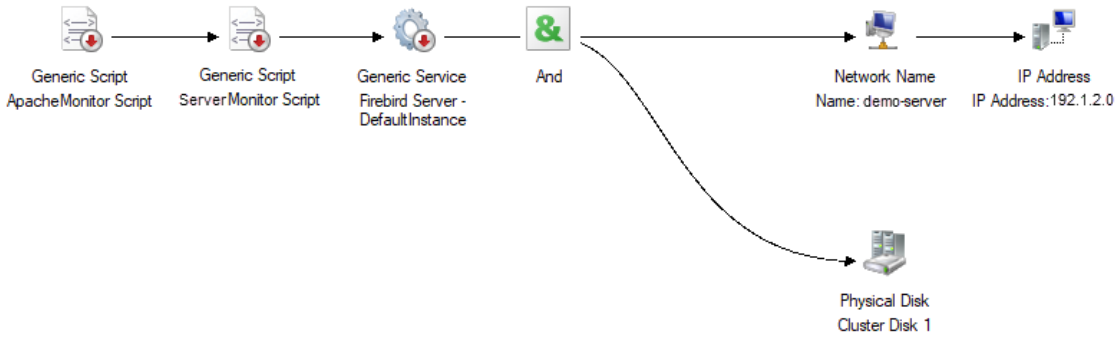


Once you upload an Embedded terminal installation package on the MyQ web administrator interface of the MyQ cluster server, the cluster uses the script to distribute the package among all the other nodes.

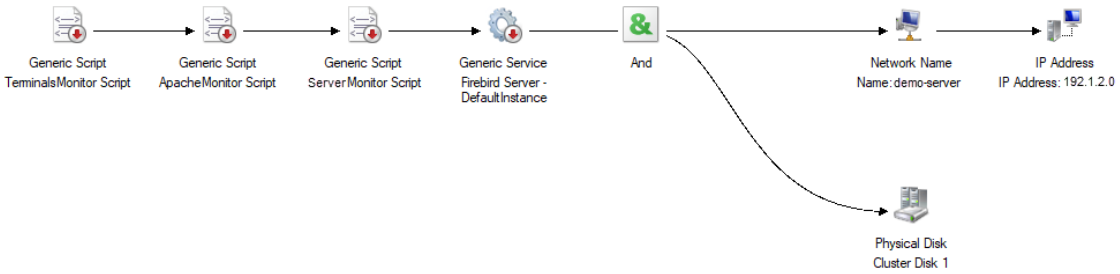
To view the dependency report, right-click the MyQ server role on the **Roles** tab of the cluster in Failover Cluster Manager, click **More Actions**, and click **Show Dependency Report**.

Viewing MS Cluster Dependency Reports

To make sure that the dependencies are set correctly, you can check if the dependency report of the MyQ server role corresponds to the below graphs:



6 Dependency graph of the cluster on the MyQ server



7 Dependency graph of the cluster with embedded terminal on the MyQ server

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

5.5.4 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 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 Easy Config application.

Set the Data Folder Location (All Nodes)

On each node of the cluster, you msut set the location of the **Data** folderand the Jobs folder, which require 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 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 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 Easy Config application.
- After completing the setup (setup and additional setup) of the MyQ server role (and all Embedded terminals, if used), 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)

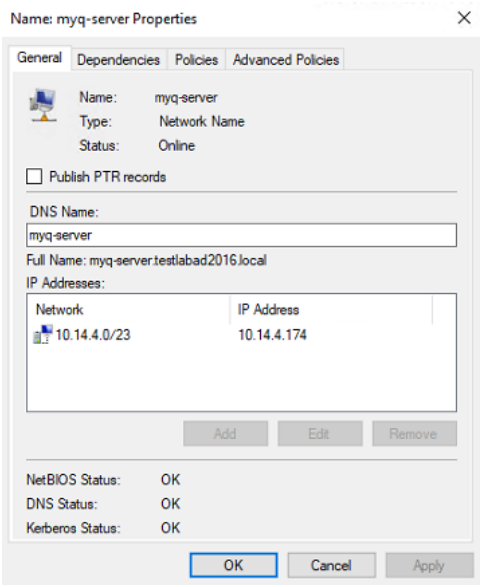
To start the system, bring the resources of the MS Cluster online. For information on how to do this, see Running in MS Cluster (see page 138).

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:

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 both of the following settings:
    a. **This server hostname** under **General**.
    b. **Server** under **MyQ X Mobile Client**.
2. Then click **Save** at the bottom of the tab.

5.5.5 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 - DefaultInstance** service, the **ApacheMonitor.jse** script, the **MyQMonitor.jse** script and the **Terminal Monitor** script (only if embedded terminals are used).

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

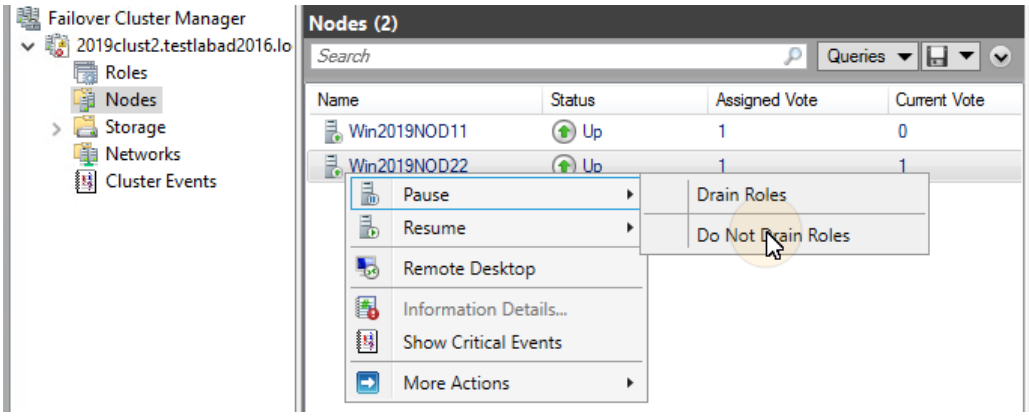
Restarting MyQ Services via the MS Cluster (Failover Cluster Manager)

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)

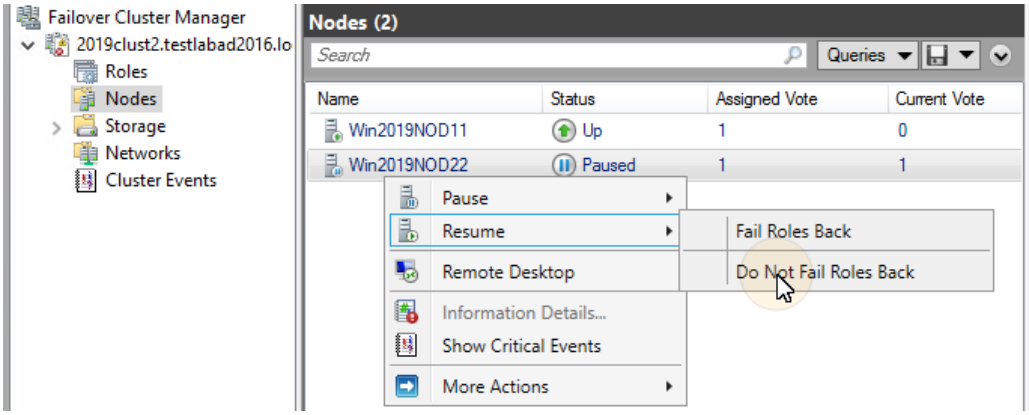
To change the **Web Administrator Account** and **Database Administrator** passwords, you need to do the following on the currently active node (the current owner of the MyQ server role):

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 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.

5.5.6 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 (see page 154)

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

5.5.7 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 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 Easy Config.
2. Run the MyQ installation file.
3. Finish the installation process.
4. **Stop All** services via MyQ Easy Config, and then close the MyQ 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.

5.6 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*). The MyQ Uninstall dialog box appears.
2. Click **Yes**.

All parts of MyQ will be uninstalled except for the **Data Folder** and its **Job Folder**. You can delete these folders 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

Use Easy Config to manage your MyQ and MyQ Central Server environment, and for essential operations such as port configuration, backup and restore, and log analysis.

You can find Easy Config from the Start menu and on the Apps screen in Windows 8.1+, Windows Server 2016 and later. Easy Config can also open as part of a system installation.

Easy Config opens with the following features:

- **Home:**
  - change the default passwords for Server and Database admin accounts
  - generate support data
  - access the MyQ Web Administrator Interface
- **Services:** start, stop and restart services
- **Settings:**
  - change the default passwords for Server and Database admin accounts
  - set up Windows Services account
  - unlock the Server Admin account
  - change file paths of the MyQ system data files
  - change the web port
  - clean up cache and temp
- **Security:**
  - enable and disable unsecure communication
  - manage the MyQ DB and Log DB
  - manage job encryption
- **Database:**
  - change the type and settings of the MyQ database
  - back up and restore data
- **Log:** monitor all operations executed by the MyQ system.
- **About:** view information about the MyQ system.

6.1 Easy Config Home

When you first open Easy Config, you will be prompted to create passwords for the Server Administrator and Database Administrator account.

6.1.1 **Server Administrator Account**

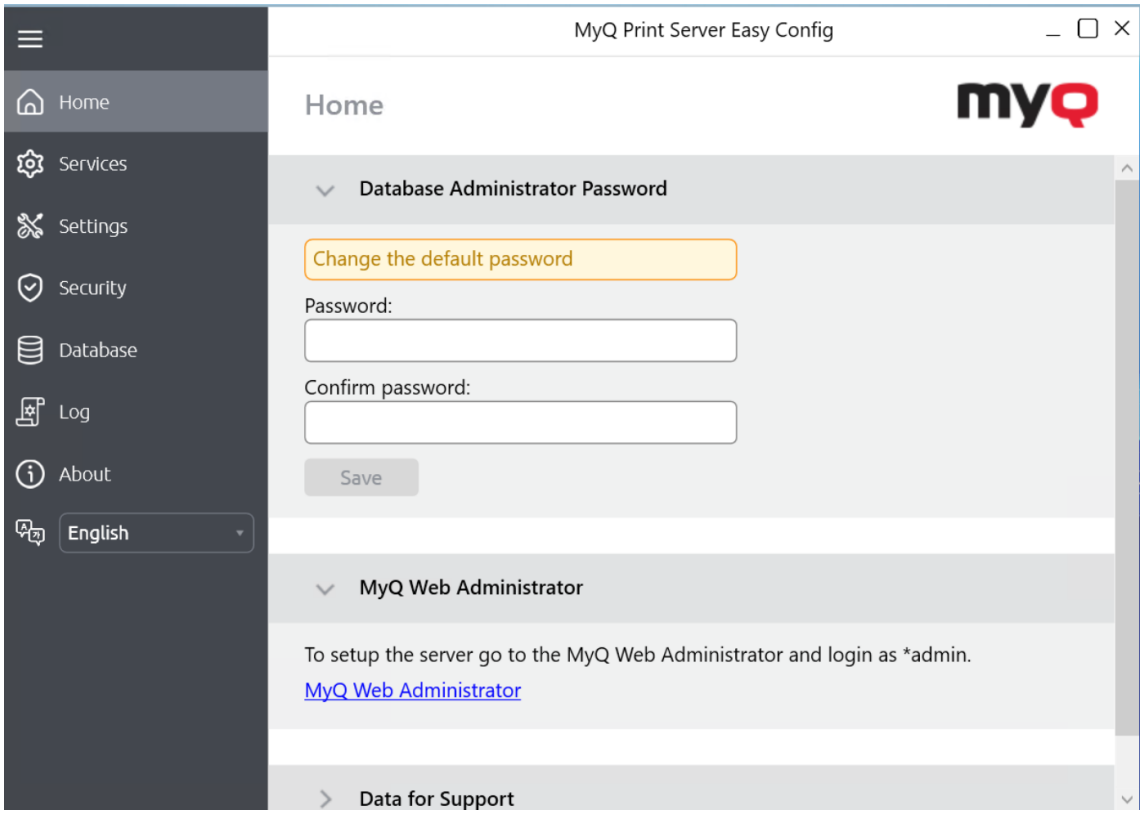
This is the `*admin` account used for the initial MyQ configuration. Once you create a password for this account, you can continue to the MyQ Web Interface, use `*admin` to log in as the administrator and start the configuration. It is generally

recommended to disable this account once you have created dedicated administrator accounts, you can do so on the **Security** tab.

6.1.2 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.

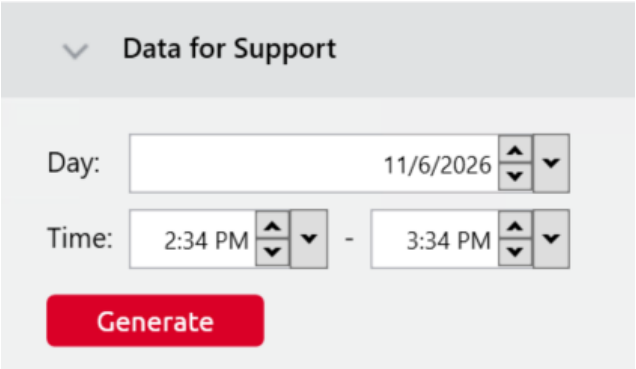
6.1.3 MyQ Web Administrator

This link is the MyQ Server log in page. The *admin account is a special administrator for setting up a new environment, with access to all settings and features.

Log in with the *admin account to set up your environment. Later, when you have configured user import and synchronization and allocated rights to users, you should disable the *admin account.

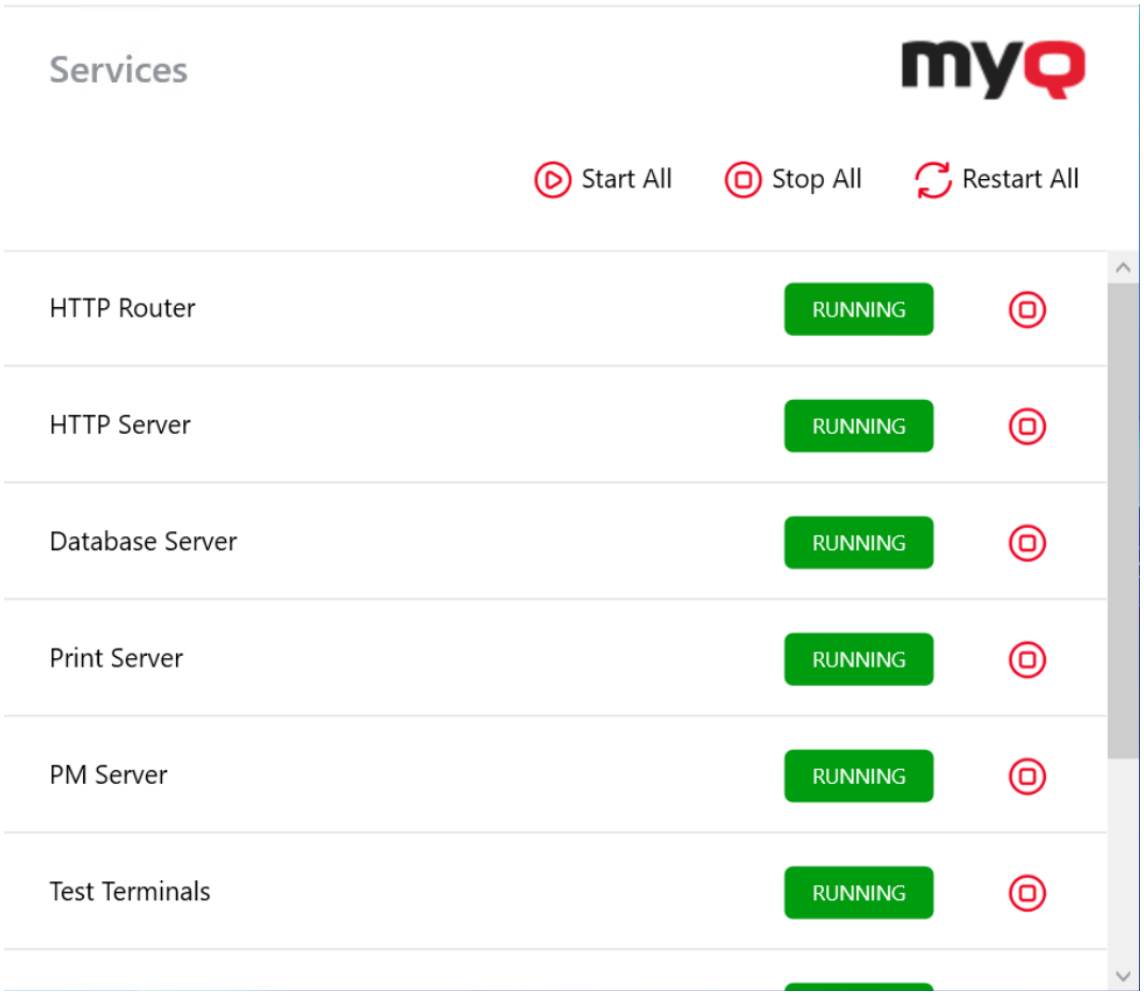
6.1.4 Generate Support Data

You can use Easy Config to generate data to share with support when troubleshooting issues. 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.

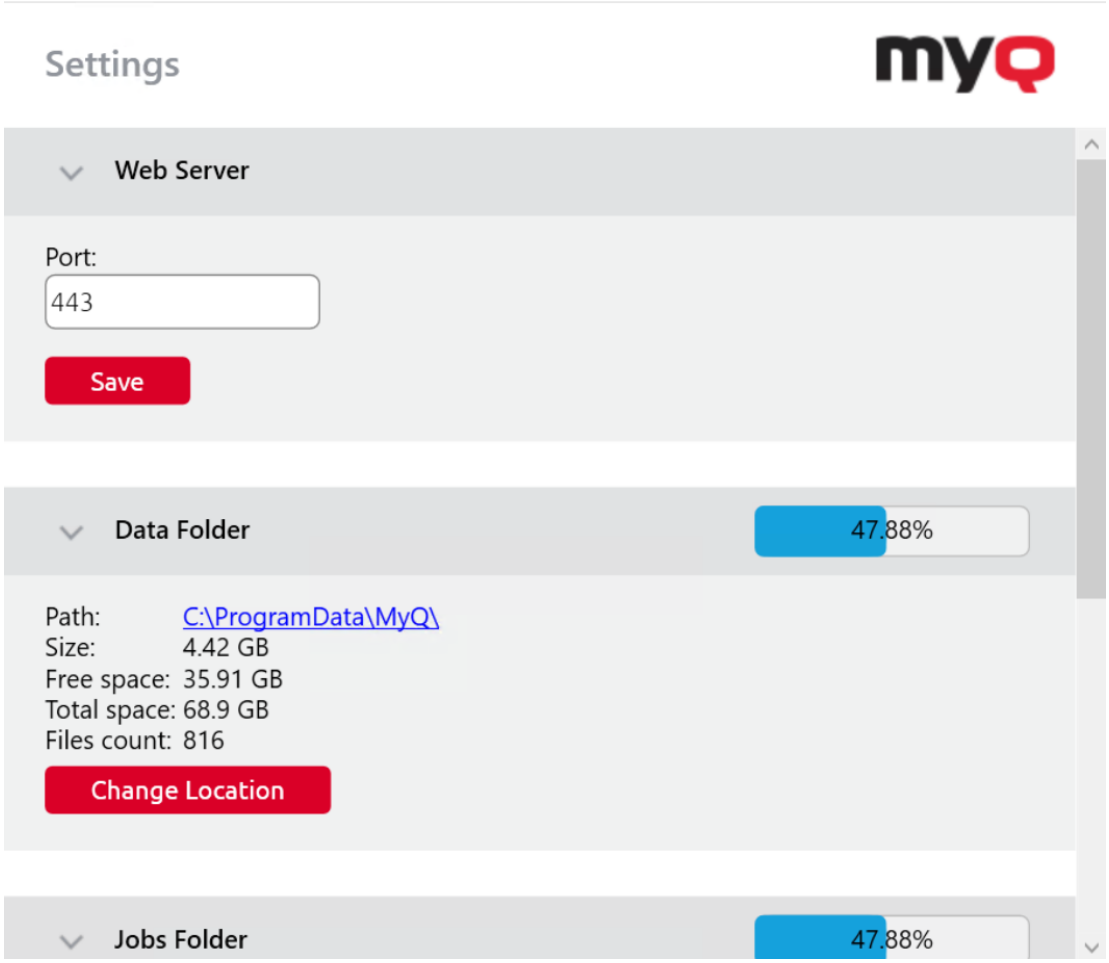


6.2 Easy Config Services

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


Services
myq
Start All
Stop All
Restart All
HTTP Router
RUNNING
HTTP Server
RUNNING
Database Server
RUNNING
Print Server
RUNNING
PM Server
RUNNING
Test Terminals
RUNNING

6.3 Easy Config Settings



6.3.1 Web Server Ports

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

- **Port**: communication port for the MyQ HTTP server; the default value is *443*.

6.3.2 Data and Jobs Folders

On the **Settings** tab, you can see the folder locations of MyQ database and MyQ print jobs. The default folders are:

- `C:\ProgramData\MyQ\` - database
- `C:\ProgramData\MyQ\Jobs` - print jobs

Under normal circumstances, there is no need to change these locations. 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 the browser icon and find the folder location.
3. Under **Change Operation**, select the required method of existing data relocation, and then click **Change location**. Keep in mind that the server needs to be stopped during the change. 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[21].

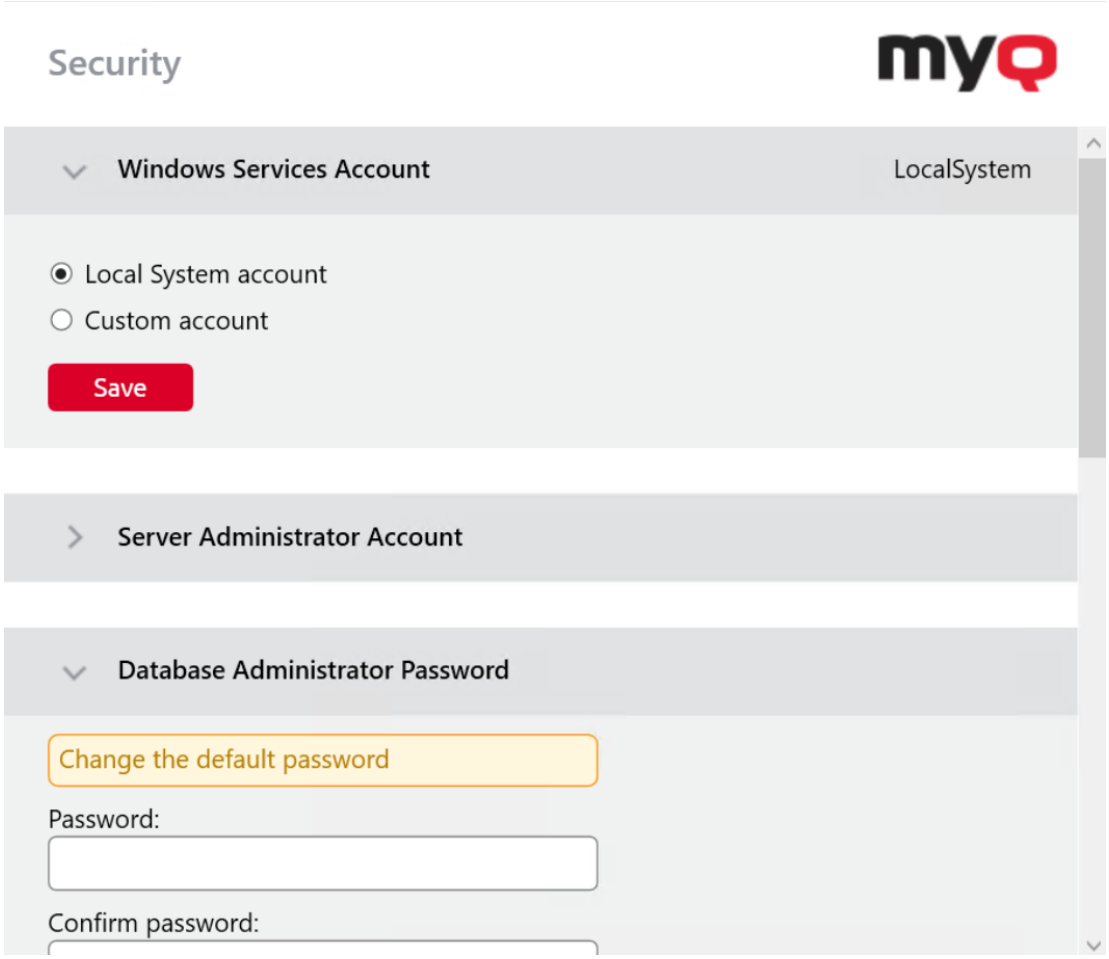
6.3.3 Server Maintenance

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.

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

6.4 Easy Config Security



6.4.1 Windows Services Account

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

Requirements for a Custom Service Account

Local System has implicit access to local resources that a custom account (domain user or gMSA) does not. Before switching the Windows Services Account, grant the target account the following:

- *NTFS – Modify* on the MyQ Data folder (`C:\ProgramData\MyQ` by default) and on `C:\Program Files\MyQ`. Without it, Firebird cannot open its security database and every login fails (`Error occurred during login`), and `firebird.log` is not writable.

- *Registry – Full Control / Write* on `HKLM\SOFTWARE\WOW6432Node\JANUS`. Without this, Print Server fails at boot with a code 5 error, and the service terminates *with Win32 error 1 ("Incorrect function", Event ID 7023)*.
- *If a server certificate is installed in the Windows Certificate Store* (e.g., for HTTPS): grant the account *Read* access to the certificate's private key.

If the *HP Embedded Terminal* is used: reserve the HTTP.sys URL for the account, otherwise MyQHPTerminal.exe will fail to start. Run:

```
netsh http add urlacl url=http://+:8130/ user=<account>
```

Grant permissions before changing the account!
If a service fails to start mid-change, Easy Config reports a generic *Request failed* error and closes, leaving services assigned to the new account without the access they need. Recovering from this requires applying the missing permissions manually and then restarting the affected services yourself – Easy Config will not retry this automatically.

Switch to a Custom Account

You can change the account 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 Windows services and click **OK**. The selected user account should have "Local administrator" rights or be a member of the Local Administrators Group. You can also select a gMSA account, in which case a password is not required. 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.

6.4.2 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*.

6.4.3 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.

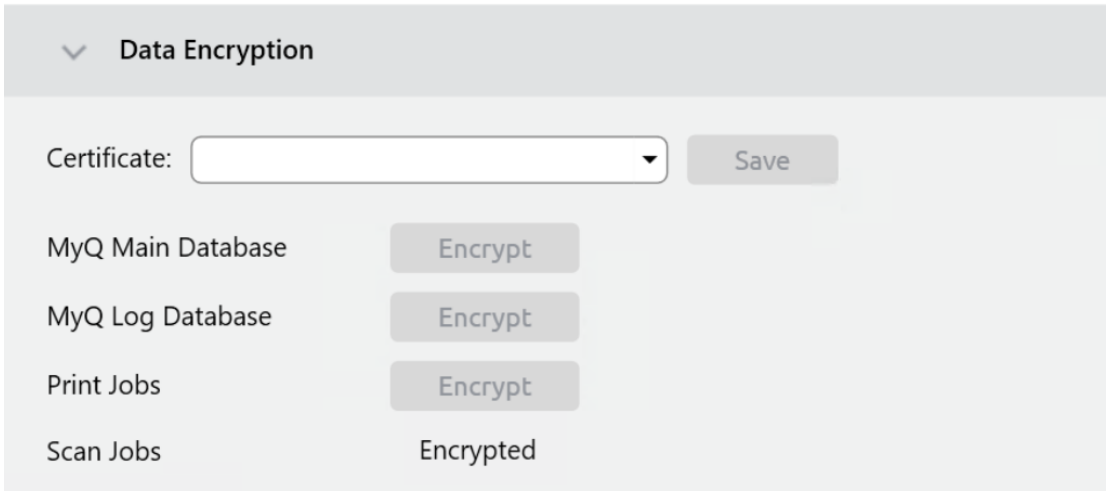
6.4.4 Data Encryption

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:

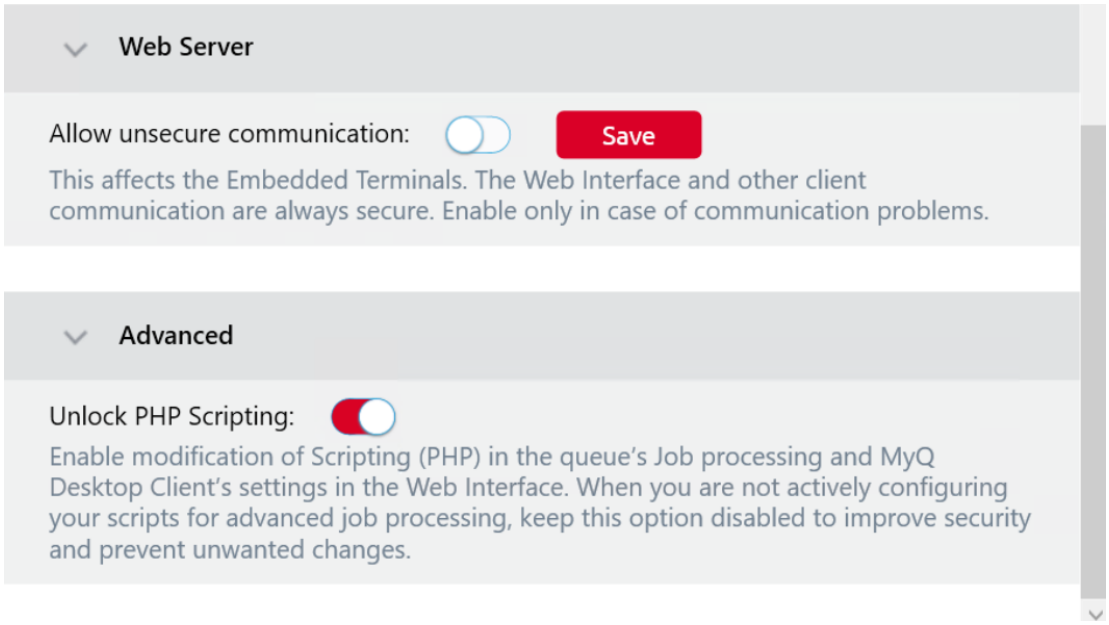
After the encryption, the **Encrypt** button will change to **Decrypt** so you can reverse the action.

6.4.5 Web Server

In the **Web Server** section, you should enable **Allow unsecure communication** only in case of communication problems.

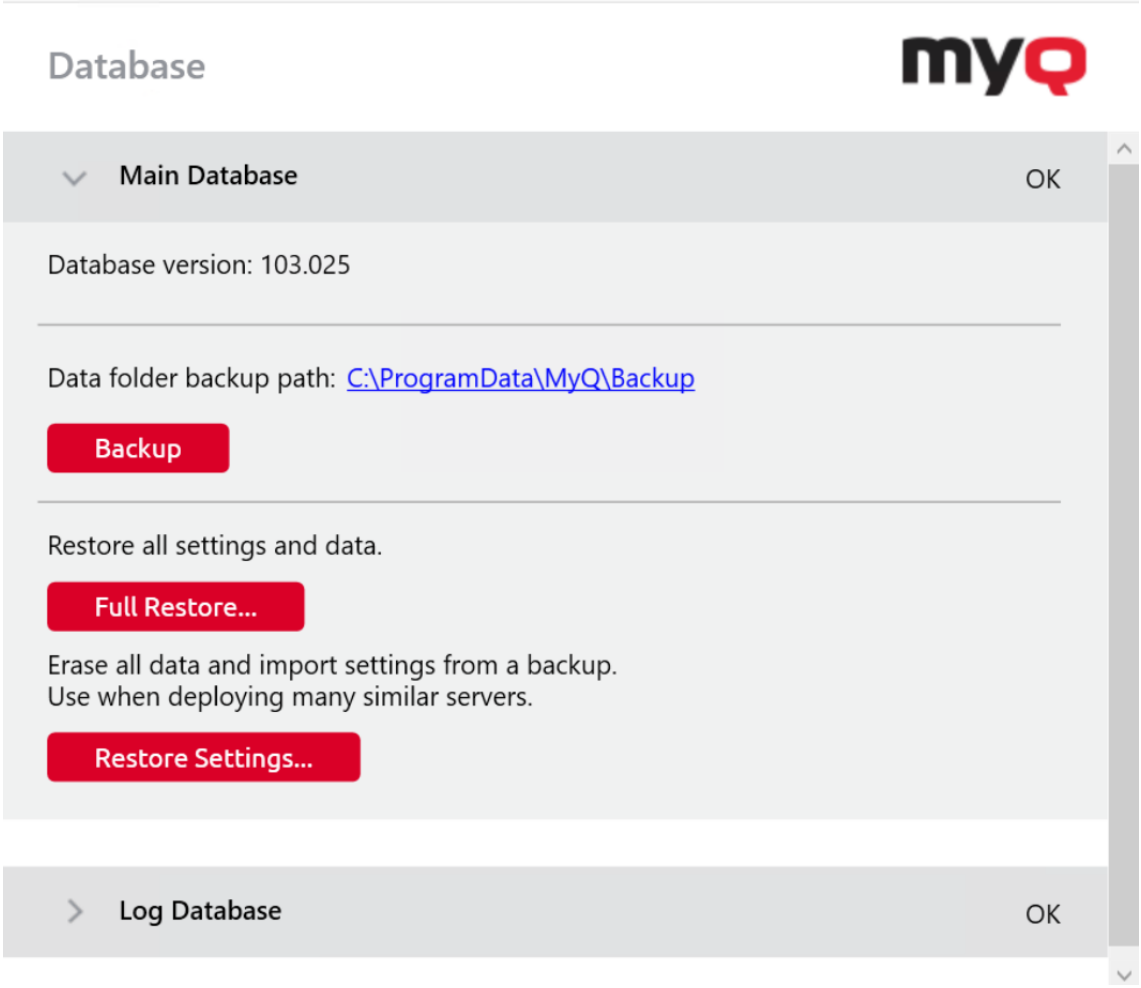
6.4.6 Unlocking PHP Scripting

In the **Advanced** section you can enable or disable the modification of PHP job scripting in the Web Interface, by default this option is disabled.



6.5 Easy Config Database

On the **Database** tab, you can check the main and log database's status, perform backup and recovery, and import settings from a different MyQ installation. You can also see information about the current version of the database, available updates, and also a warning if 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*.

The file contains the MyQ database and additional files with data used by the MyQ system, such as reports, certificates, or the *config.ini* file.

Print jobs (by default in C:\ProgramData\MyQ\Jobs) are not part of the backup, due to their size.

If required (especially favorite jobs could be required by users after restoring MyQ on the new server), they must be copied and backed up manually or using 3rd-party software.

6.5.2 Restoring MyQ Data

If you had manually backed up print jobs, then when restoring a backup, it is necessary to first copy the print jobs to the Jobs folder and then restore the MyQ backup using MyQ Easy Config.

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 Importing Settings from Another MyQ Installation

This feature simplifies large-scale deployments as it allows using one MyQ installation as a "template" to set up more installations without the need to manually configure most of the settings.

Creating a database template basics

- Use groups for any assignment such as Rights, Policies, etc. User and Printer groups are kept in contrast with specific users or printers.
- Create a standard backup (**Database** – **Backup**) in the source installation.

What the import does

During the import, the database is restored in the normal way, but the following data are changed:

- deleted users (groups are kept),
- deleted printers (groups are kept),
- deleted accounting data,
- deleted jobs,
- deleted payments, credit events,
- deleted vouchers and voucher batches,

- deleted quota boosts and quota periods,
- deleted reports execution history,
- deleted audit log records,
- deleted sites,
- new installation UUID,
- updated hostname,
- updated server name (if Site),
- non-archived price lists get new UUIDs,
- licenses are removed.

⚠ If assignments to specific users or printers exist in the backup that is being restored, the database is restored fully, and the cleanup of unnecessary data will not begin. In such cases, examine the logs and modify assignments in the source installation before creating a new backup.

To import settings from a different MyQ installation:

1. Open the **Database** tab.
2. In the **Main Database** section, click **Restore Settings...**. Select your "template" backup *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.

6.5.4 Embedded Terminals

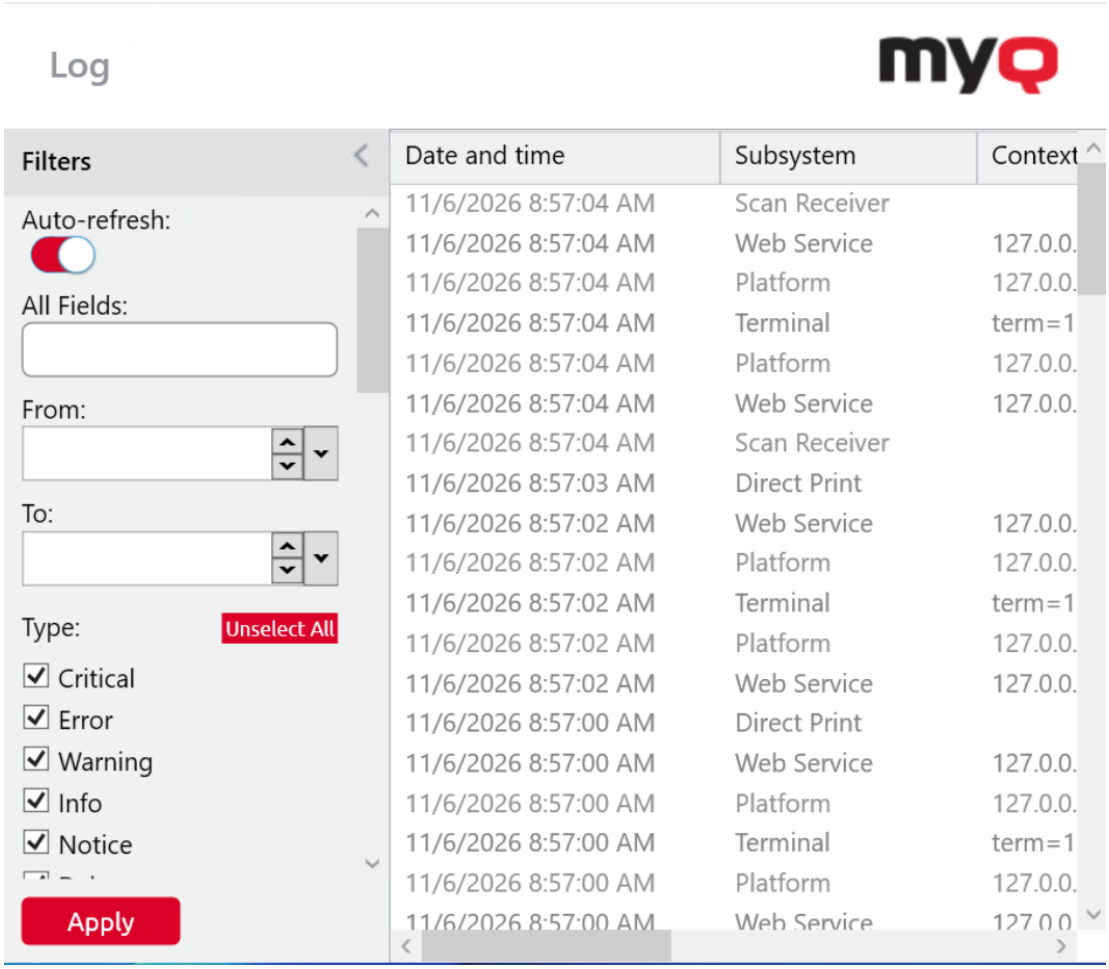
While restoring the database, MyQ checks terminal packages in the database and file system and synchronizes their state:

- Packages marked for uninstallation before services were stopped are **uninstalled**.
- Packages in the file system but missing in the database are **uninstalled**.
- Packages in the database but missing in the file system are **installed**.

Package synchronization may take some time, meaning printers may not become immediately available.

6.6 Easy Config Log

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


Log
myQ
Filters
Auto-refresh:
All Fields:
From:
To:
Type:
Unselect All
Critical
Error
Warning
Info
Notice
Apply
Date and time
Subsystem
Context
11/6/2026 8:57:04 AM Scan Receiver
11/6/2026 8:57:04 AM Web Service 127.0.0.
11/6/2026 8:57:04 AM Platform 127.0.0.
11/6/2026 8:57:04 AM Terminal term=1
11/6/2026 8:57:04 AM Platform 127.0.0.
11/6/2026 8:57:04 AM Web Service 127.0.0.
11/6/2026 8:57:04 AM Scan Receiver
11/6/2026 8:57:03 AM Direct Print
11/6/2026 8:57:02 AM Web Service 127.0.0.
11/6/2026 8:57:02 AM Platform 127.0.0.
11/6/2026 8:57:02 AM Terminal term=1
11/6/2026 8:57:02 AM Platform 127.0.0.
11/6/2026 8:57:02 AM Web Service 127.0.0.
11/6/2026 8:57:00 AM Direct Print
11/6/2026 8:57:00 AM Web Service 127.0.0.
11/6/2026 8:57:00 AM Platform 127.0.0.
11/6/2026 8:57:00 AM Terminal term=1
11/6/2026 8:57:00 AM Platform 127.0.0.

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.

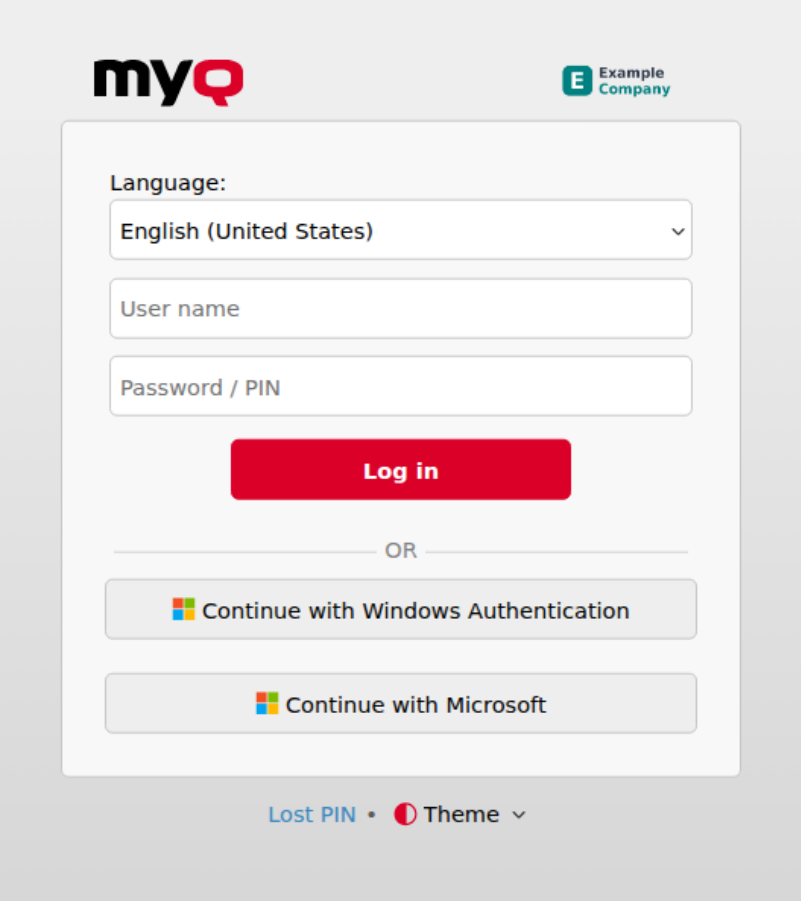
7.1 Accessing the MyQ Web Interface

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 enter the web address:
  `https://hostname:port`
  where `hostname` represents the IP address or the hostname of your MyQ Print Server and `port` is the configured access port (default: 443).
- From the MyQ Easy Config **Home** tab, click the **MyQ Web Administrator** link in the **MyQ Web Administrator** section.
- Open the MyQ 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*.



8 Login screen

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*.

Click **Lost PIN** and you are taken to a window where you can either enter your email in order to receive a PIN reset code or if you already have the code, you can type it and reset your PIN.

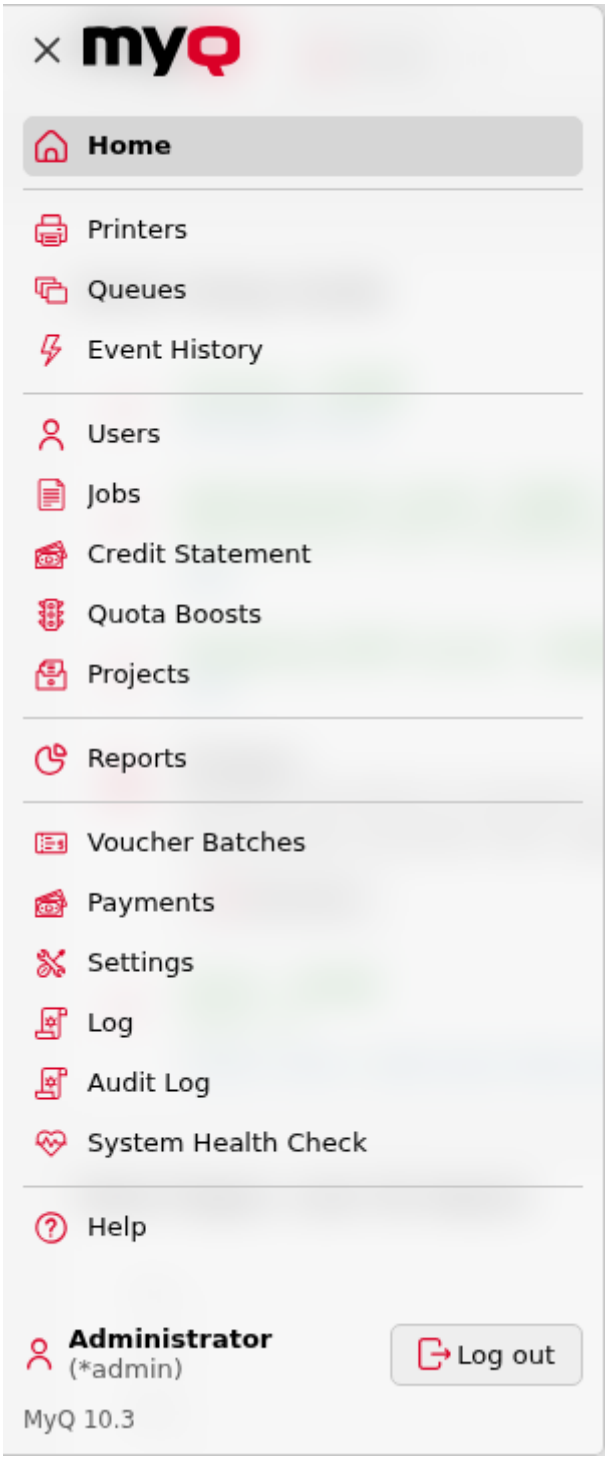
7.3 Main Menu and Settings Menu

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.



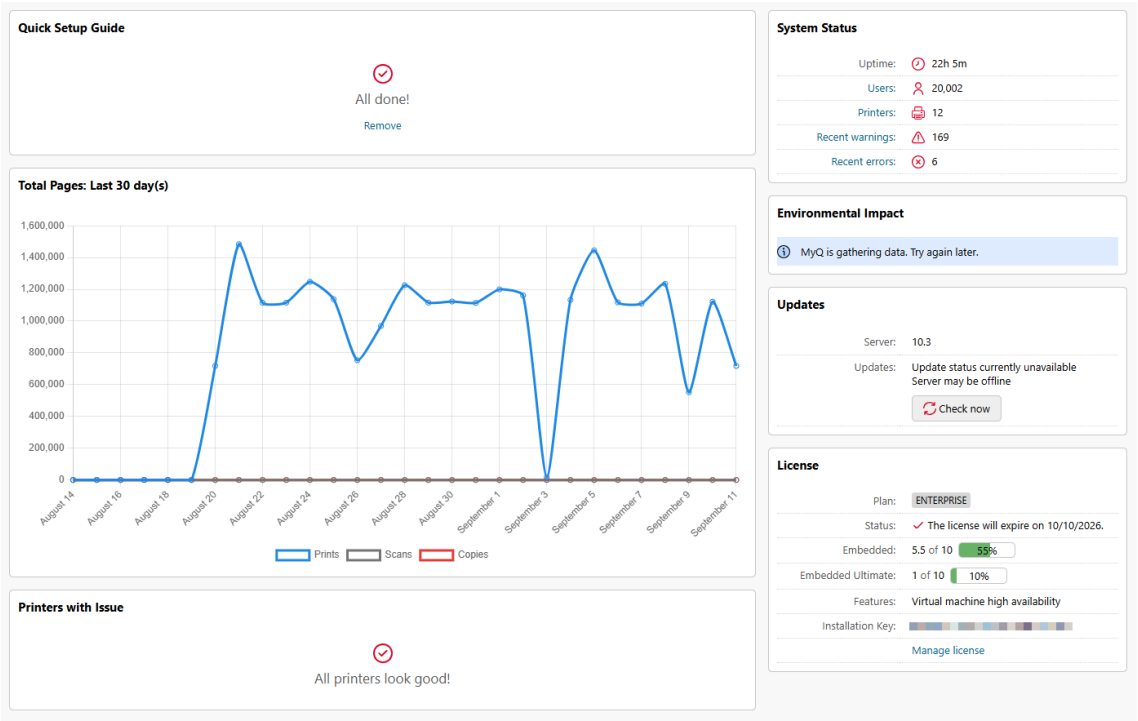
Settings menu

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
- Printers with Issue

- System Status *
- Top Active: Groups
- Top Active: Printers
- Top Active: Users
- Quick Setup Guide *

System Status

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

Name	Description
Pages printed today	Number of printed pages over the last 24 hours. Cached every 60 seconds.
Pages copied today	Number of copied pages over the last 24 hours. Cached every 60 seconds.
Pages scanned today	Number of scanned pages over the last 24 hours. Cached every 60 seconds.
Uptime	MyQ system uptime, in hours.
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.
Recent warnings	Number of warning log messages over the last 24 hours. Cached every 30 seconds.
Recent errors	Number of error and critical log messages over the last 24 hours. Cached every 30 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.

Printers with Issue

Printers with Issue shows unreachable active printers and active printers with unresolved alerts. You can also see these issues in the **Issues** column, in the **Printers** overview (**MyQ > Printers**).

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.

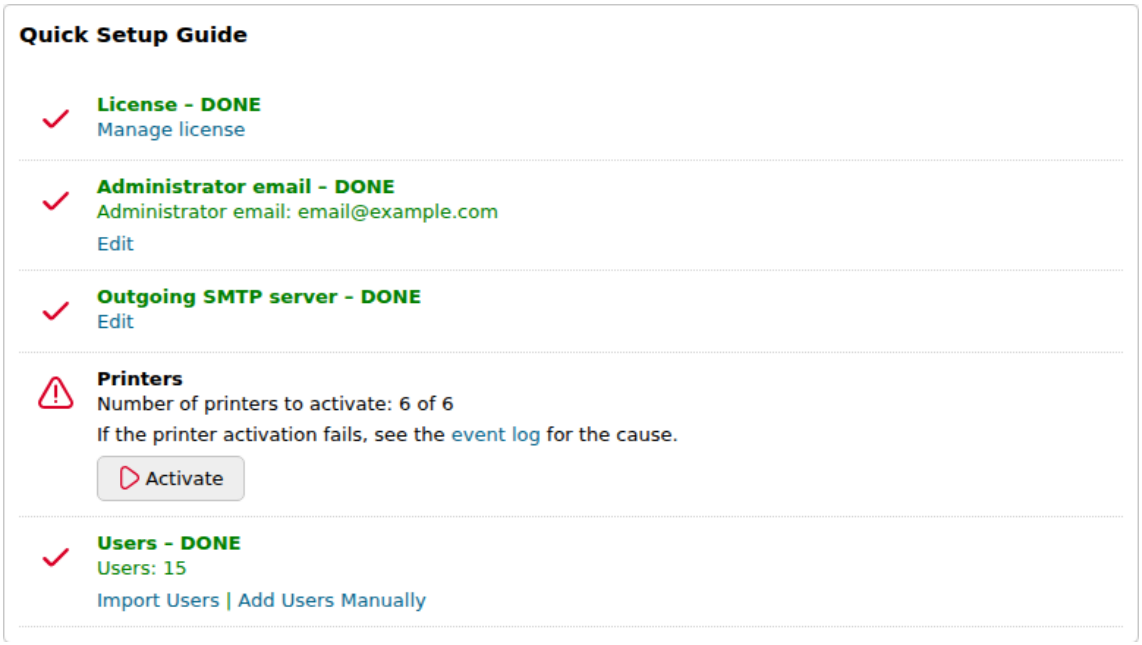
7.4.2 Change the Theme

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 information about your company.
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.

Outgoing SMTP Server

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

Printers

Adding printers:

- By clicking **Discover Printers**, you open the **Printer Discovery** settings tab, where you can discover and add printing devices.
- By clicking **Add printers manually**, you open the **Printers** main tab, where you can manually add printing devices.

Activating added printers:

Click **Activate** to activate all the added printing devices.

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.
- `myq.exe` dump files
- Logs and PM Server directories from the MyQ data folder
- Windows Event Logs, including the Application and System channels only. The included events are of Critical, Error, and Warning severity.
- The files `statsData.xml`, `config.ini`, and `traefik.custom.rules.yaml`
- Printers directory containing logs from supported devices

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

Generate Support Data in the Web UI

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. (Optional, Print Server only) Select up to 5 printers from which to include device logs.
4. Click **Export**. The .ZIP file is generated and saved to your Downloads folder.

Export Logs from Printers

When generating support data on Print Server, you can optionally include device logs from up to 5 printers. In the **Generate Support Data** dialog, select the printers whose device logs you want to include in the export.

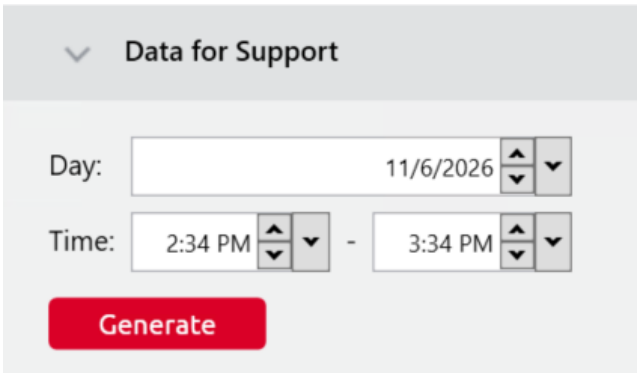
Device logs are available from Kyocera, Canon, Ricoh and Lexmark devices, with an embedded terminal installed.

Notes:

- The date range filter does not apply to printer device logs – the full device log is included.
- Exporting printer logs is only available from the MyQ Web Interface. This option is not available in Easy Config.

Generate Support Data with Easy Config

You can use Easy Config to generate data to share with support when troubleshooting issues. 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.

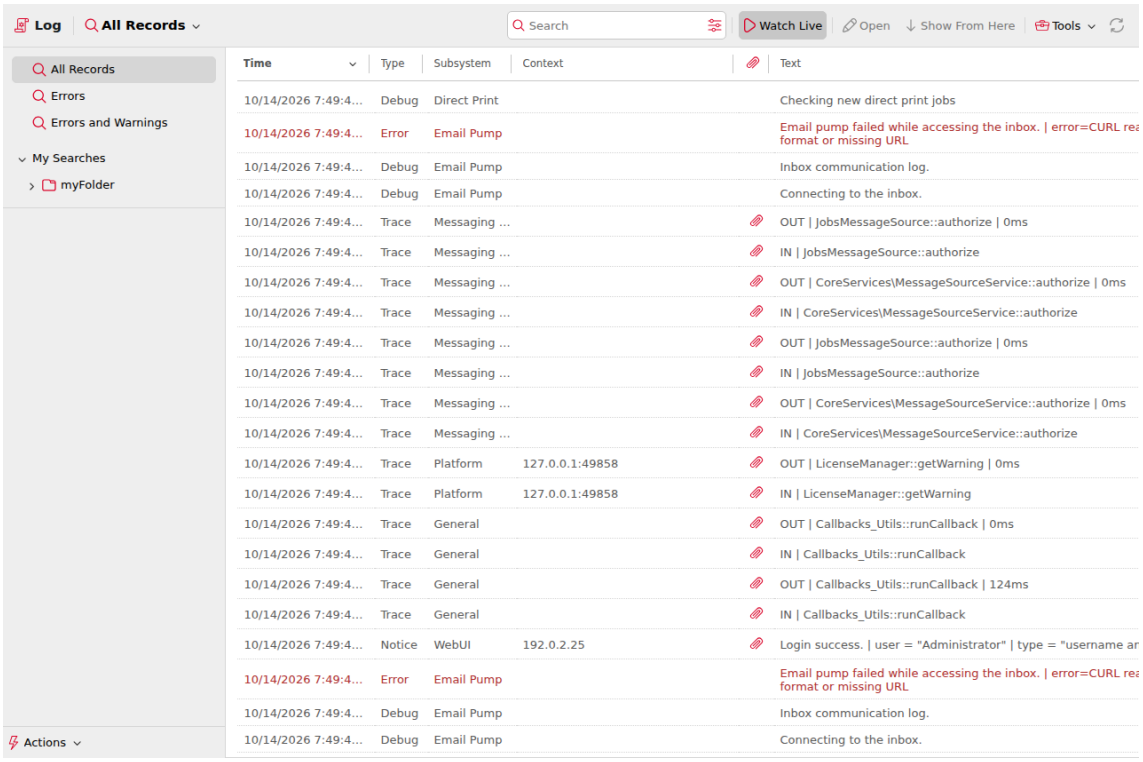


7.5 MyQ Log

In the MyQ server log, you can find information about all parts of the MyQ server: the MyQ server, MyQ 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:

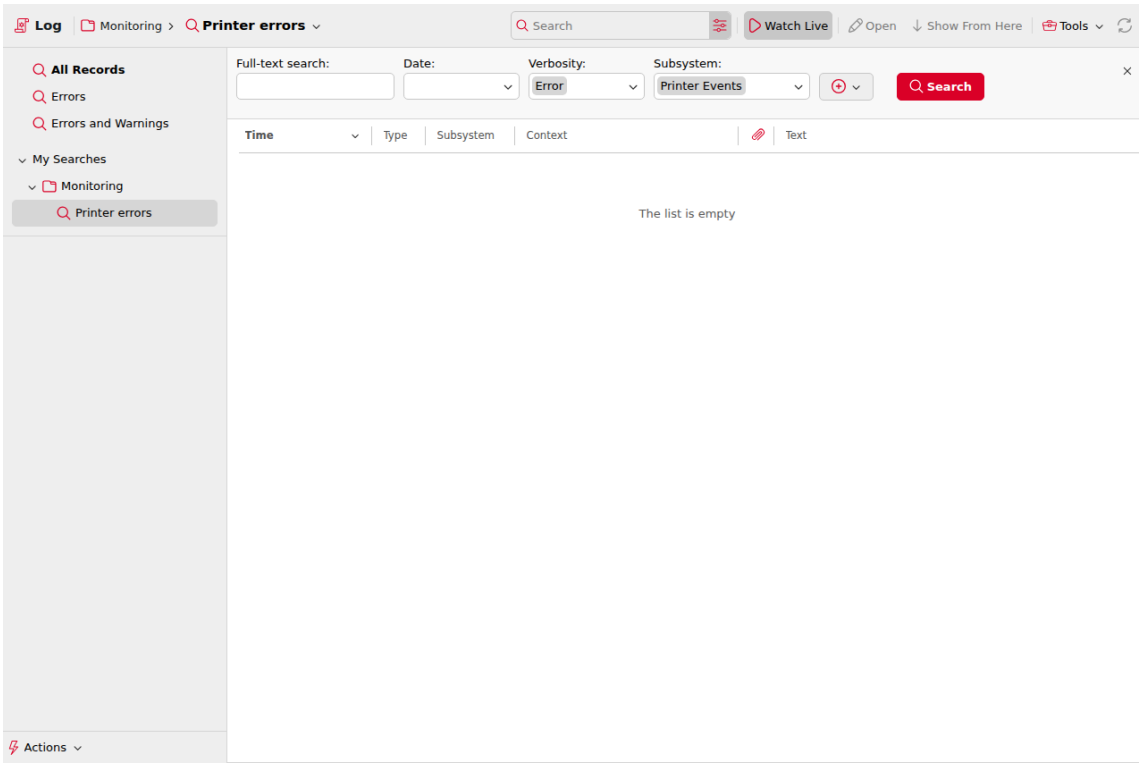
- After you pause the log, you can select the period in the **Date** combo box.
- In the **Verbosity** field you can select the type of log entries you want to view (*Critical, Info, Error*, etc.).
- In the **Subsystem** combo box, you can select/type one or more subsystems to be displayed in the log.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

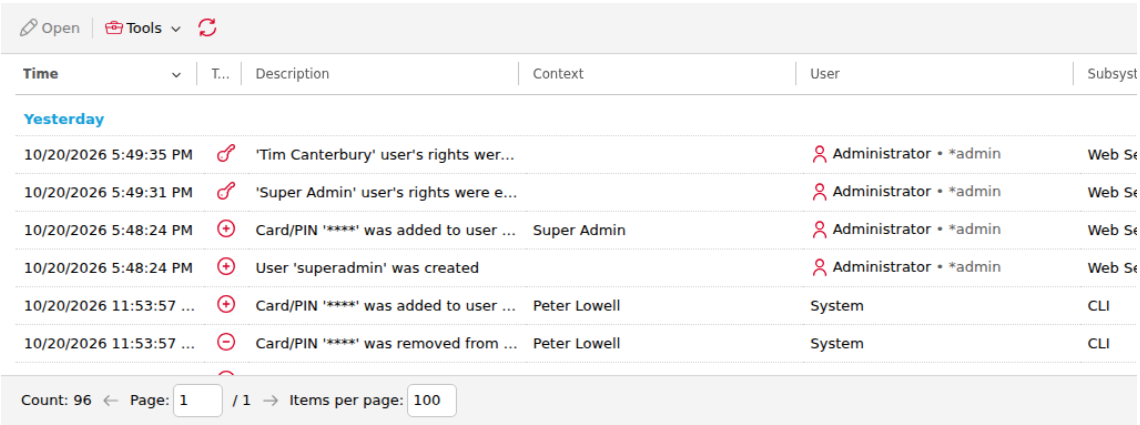
To remove all highlights, click **Tools** on the bar at the top of the **Log** tab, and then click **Remove highlighting**.

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, go to **MyQ > Audit Log**. Here is an 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.

8 MyQ System Settings

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

8.1 Server Type

On the Server Type settings tab, you can set whether the server runs as a Standalone server or a Site server, and, for a Site server, configure its connection to the Central server (site name, Central server address, port, and communication password).

8.2 License

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

8.3 Sites

On the Sites main tab, you can view and manage all Site servers connected to the Central server, group sites by region or organizational need, and monitor the status of data replication from each site.

8.4 General

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

8.5 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.

8.6 Task Scheduler

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

8.7 Network

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

8.7.1 Connections

On the Connections Settings tab, you connect MyQ to external cloud services such as Amazon S3, Gmail, Microsoft Entra applications, MyQ Scan Review, MyQ Document Processor, RightFax, and others.

8.7.2 SNMP

On the SNMP settings tab, you can create and manage SNMP v1, v2c, and v3 profiles, and assign them to printing devices for secure device communication.

8.7.3 Authentication Servers

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

8.8 Printers & Terminals

On the Printers & Terminals settings tab, you can manage terminal packages and configure embedded terminal behavior, divided into General, MyQ X Mobile Client, Device Spooling, Offline Login, and Terminal packages sections.

8.8.1 Configuration Profiles

On the Configuration Profiles settings tab, you can create profiles that bundle terminal type, login methods, price list, and network settings, and attach them to printers for embedded terminal setup.

8.8.2 Printer Discovery

On the Printer Discovery settings tab, you can create and run discoveries that search a defined IP range for network printing devices and add the ones you want into MyQ.

8.8.3 Terminal Actions

On the Terminal Actions settings tab, you can configure the layout and behavior of the embedded terminal's action buttons (Print, Copy, Scan, Fax, and others).

8.8.4 Release Stations

On the Release Stations settings tab, you can define and configure kiosk-based shared printing services.

8.8.5 Events

On the Events settings tab, you can define printer alert events (based on printing device alerts) that trigger notifications or terminal actions.

8.8.6 Event Actions

On the Event Actions settings tab, you can configure what happens when a printer event fires: an email notification to selected people, or termination of the user's session on the device's embedded terminal.

8.9 MyQ Desktop Client

On the MyQ Desktop Client settings tab, you can configure MDC settings and deployment, including configuration profiles assigned to specific locations and the print queues installed on client computers.

8.10 Printer Provisioning

On the Printer Provisioning settings tab, you can create Printer Provisioning Profiles that deploy print queues, drivers, and default settings to Desktop Client users based on IP range, hostname, user, or user group.

8.11 Print Drivers

On the Print Drivers settings tab, you can manage print driver sets captured by the Desktop Client, for use with Legacy Printer Provisioning.

8.12 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.

8.12.1 Policies

On the Policies settings tab, you can create print job policies and printer policies that control default job settings, user permissions, and access to printing device functions like copy, scan, and fax.

8.12.2 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.

8.12.3 User Authentication

On the User Authentication settings tab, you can manage how users authenticate to MyQ, including ID card management, PIN generation, password complexity, and external authentication servers.

8.12.4 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).

8.13 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.

8.13.1 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.

8.13.2 Quota

On the Quota settings tab, you can set limits on printed, copied, or scanned pages, or on the overall cost of print services, per user or group.

8.13.3 Projects

On the Projects settings tab, you can activate project accounting so print, copy, and scan jobs can be assigned to projects and their costs distributed accordingly.

8.13.4 Price Lists

On the Price Lists settings tab, you can create price lists and attach them to configuration profiles to assess the cost of each print, copy, scan, and fax operation.

8.14 Jobs

On the Jobs settings tab, you can configure global print job settings, including the job parser, job archiving, job previews, and notifications for refused jobs.

8.15 Scanning & OCR

On the Scanning & OCR settings tab, you can configure Scan to Me, set up OCR profiles that use either the MyQ Document Processor or a third-party application.

8.16 Code Books

On the Code Books settings tab, you can add code books and code lists (LDAP source, internal code list, MS Exchange address book, and fax phonebooks) for use in scan profiles.

8.17 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.

8.18 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.

8.19 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.

8.20 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.

8.21 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.

8.22 Server Type Settings

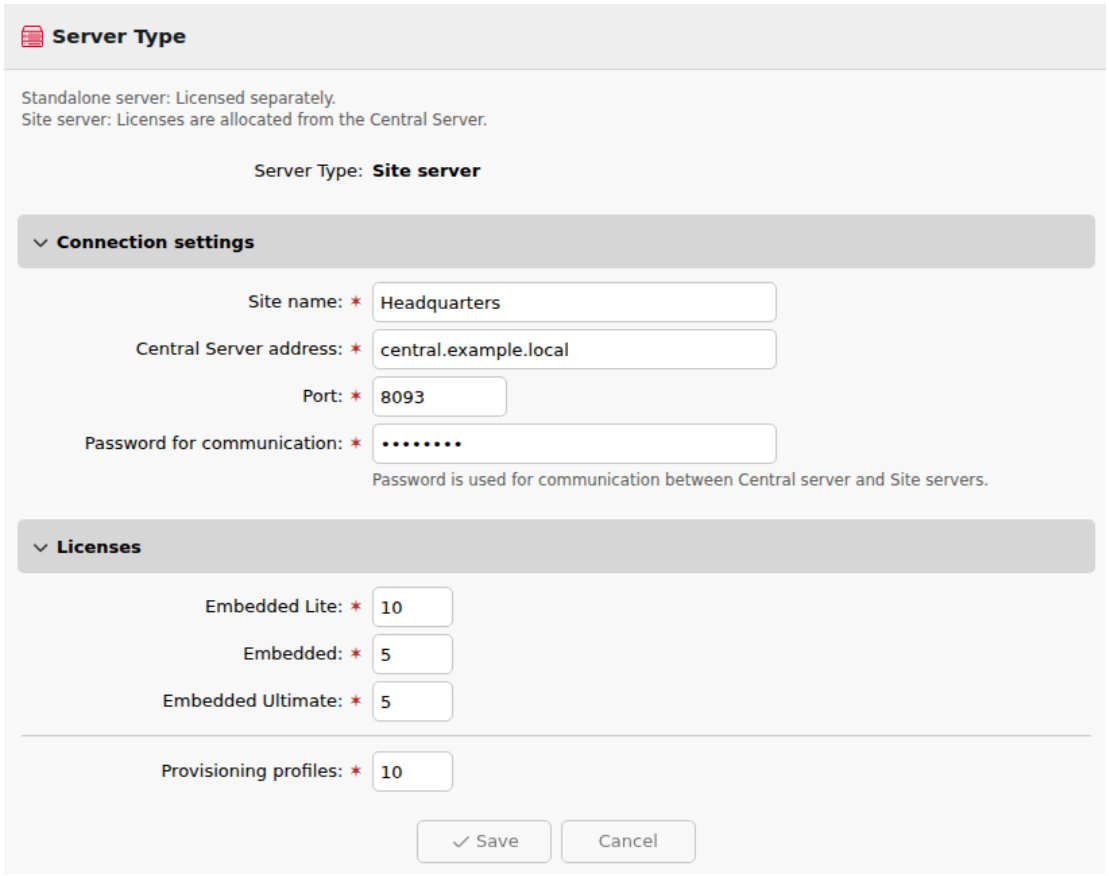
In **MyQ > Settings > Server Type**, the MyQ administrator can change the server from standalone to site. By default, all installations start as a standalone server. If you plan to use a single MyQ installation as your Print Server, do not change the server type.

To configure your installation as a site server, change the server type to **Site server**, and configure the site to connect to your Central Server.

1. **Site name**: choose a name to identify your site server.
2. **Central Server address:** the Central Server hostname or IP address.
3. **Port**: the Central Server incoming port (default: *8093*).
4. **Password for communication** - password used for the communication between the MyQ Central server and Site servers. Set the password on the Central Server in **MyQ > Settings > General**.

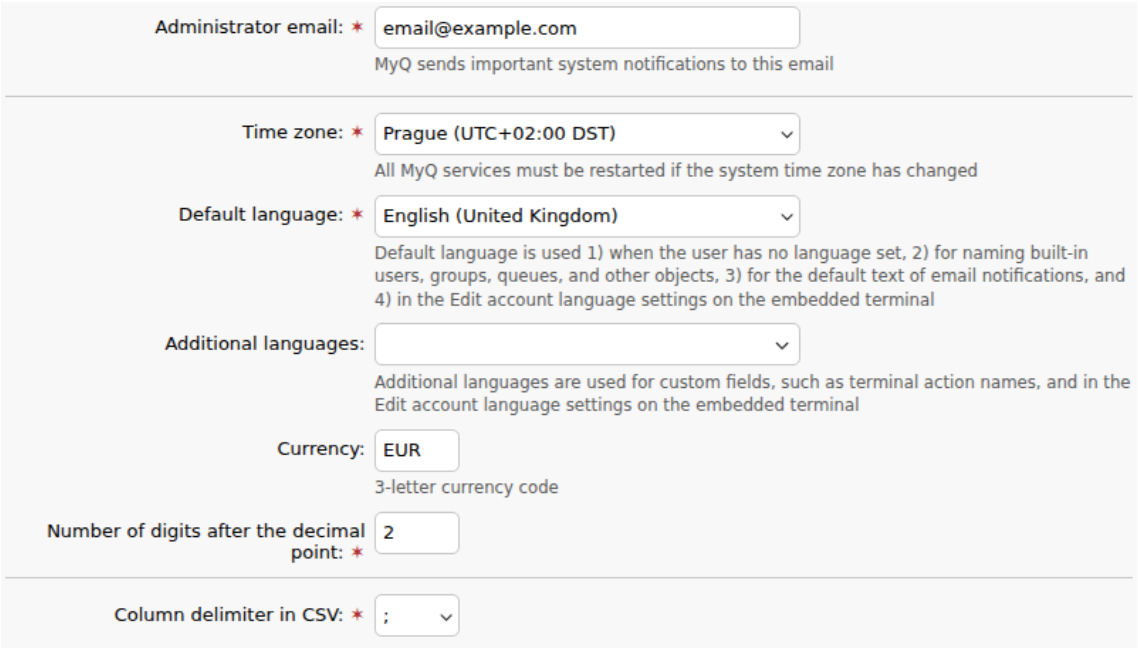
Next, enter the licenses that the Site Server should claim from your Central Server.

- **Embedded Lite** terminals or release stations
- **Embedded** terminals
- **Embedded Ultimate** terminals to use with MyQ Scan Review
- **Provisioning profiles**



8.23 General Settings

In the **General** settings tab. you can set the administrator email, time zone, default and additional languages, currency, and the column delimiter in CSV files.



- **Administrator email**: The administrator email receives important system messages (disk space checker warnings, license expiration, etc.) automatically sent from MyQ.
- **Time zone**: For the proper functioning of the MyQ system, make sure that the time zone set here is the same as the time zone set in the Windows operating system. After changing the time zone, you will be asked to restart the web server.
- **Default Language**: The default language setting determines the language of all emails that are automatically sent from MyQ and the language used on all connected terminals and interactive readers. See Available Languages (see page 718).
- **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.

8.24 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, add custom application logos to be used in

MyQ, on MyQ terminals, and in MyQ Desktop Client, and personalize your terminals with the available themes.

8.24.1 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.

8.24.2 Application Personalization

Here you can enable or disable the 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.).

8.24.3 Terminal Personalization

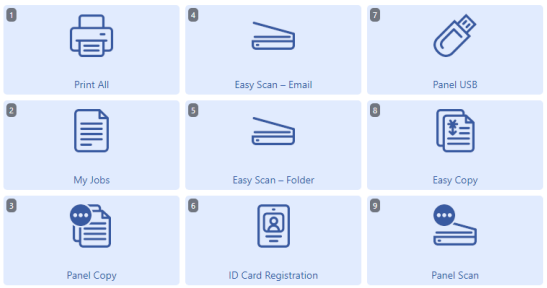
Here you can add your company's logo to be used on all your MyQ embedded terminals.

Supported formats are *JPG/JPEG/PNG/BMP* and the recommended size is *340px* x *92px*.

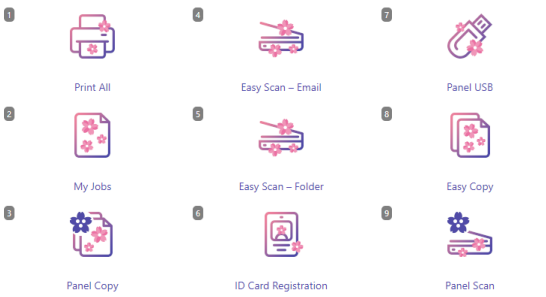
To import the custom logo, click **+Add**, **Browse** for the file and **Open** it, and then click **Save** at the bottom of the tab. A preview of the new logo is displayed on the tab.

To change the theme, select one of the available themes, and then click **Save**.

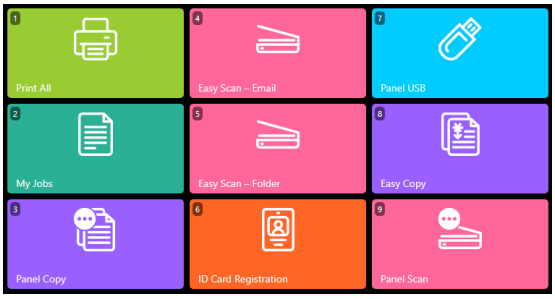
Blue Ice



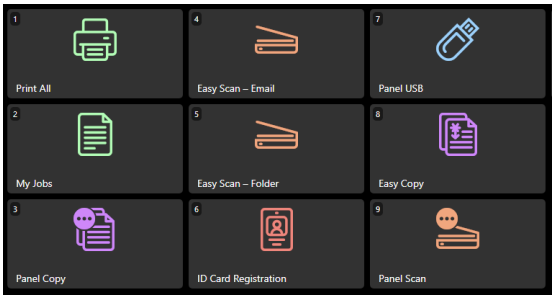
Cherry Blossom



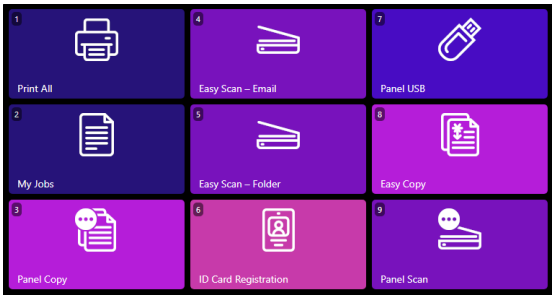
Classic



Colored Rays



Purple Peace



Spring Touch (Default)



You can also click **Manage and Customize Themes** to view all the built in themes and create your own. For more information, see Terminal Theme Editor (see page 185).

8.24.4 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).

8.24.5 Custom Help

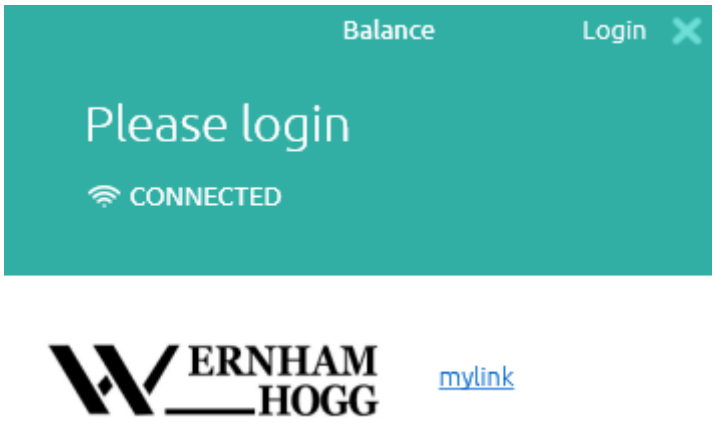
Here you can add a link to your own web-based help that will be displayed as a widget on the user's MyQ home page.

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.

8.24.6 Custom Link in the MyQ Desktop Client

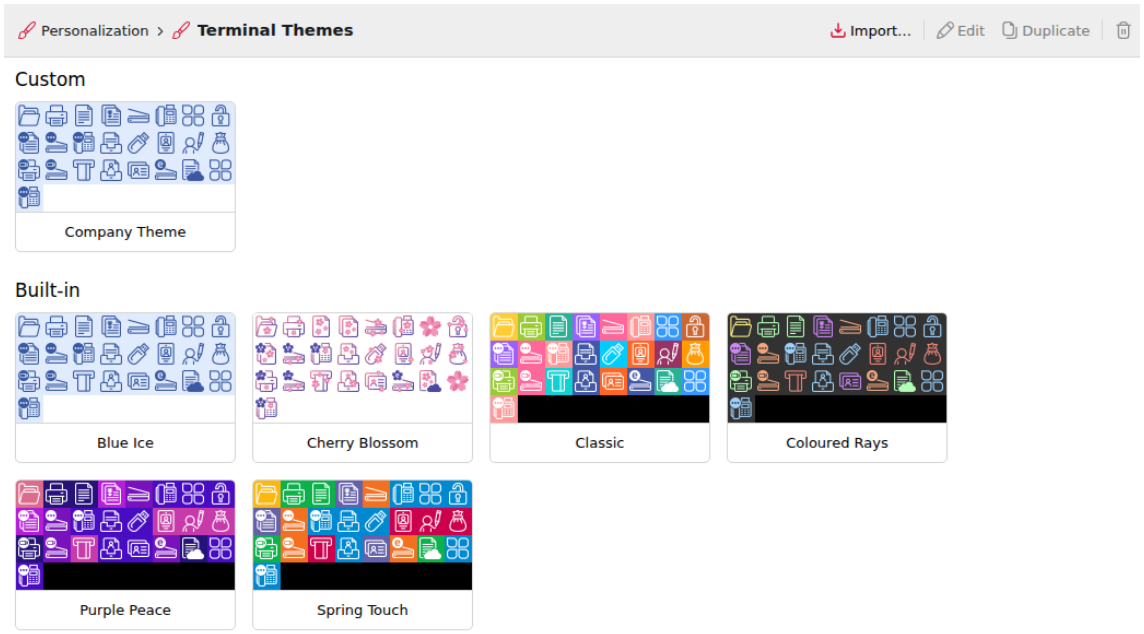
Here you can add a link to your own web-based help (weblink, network path or local path) that will be displayed in the MyQ Desktop Client.

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



8.24.7 Terminal Theme Editor

In **MyQ > Settings > Personalization** under **Terminal Personalization** it is possible to **Manage and Customize Themes** used on your Embedded Terminals. The theme affects the titles, colors, and icons used for your terminal actions.



From the **Terminal Themes** page header you can:

- **Import**: This option allows you to import a theme created using **MyQ Theme Editor**.
- **Edit**: This option allows you to view each element of a built-in theme or edit any of your custom themes.
- **Duplicate** (trash icon): This option allows you to duplicate a custom or built-in theme. The duplicate of a built-in theme is created as a custom theme and is editable.
- **Delete**: This option allows you to delete a built-in theme.

Built-In Themes

The following built-in themes are contained in the **Terminal Themes** and cannot be deleted or edited:

- Blue Ice
- Cherry Blossom
- Classic
- Colored Rays
- Purple Peace
- Spring Touch

Select a built-in theme and click **Edit** or simply double-click the theme. A side panel opens where the themes details can be viewed but not edited.

Select a built-in theme and click **Duplicate** to create an identical custom theme. This custom theme can then be edited.

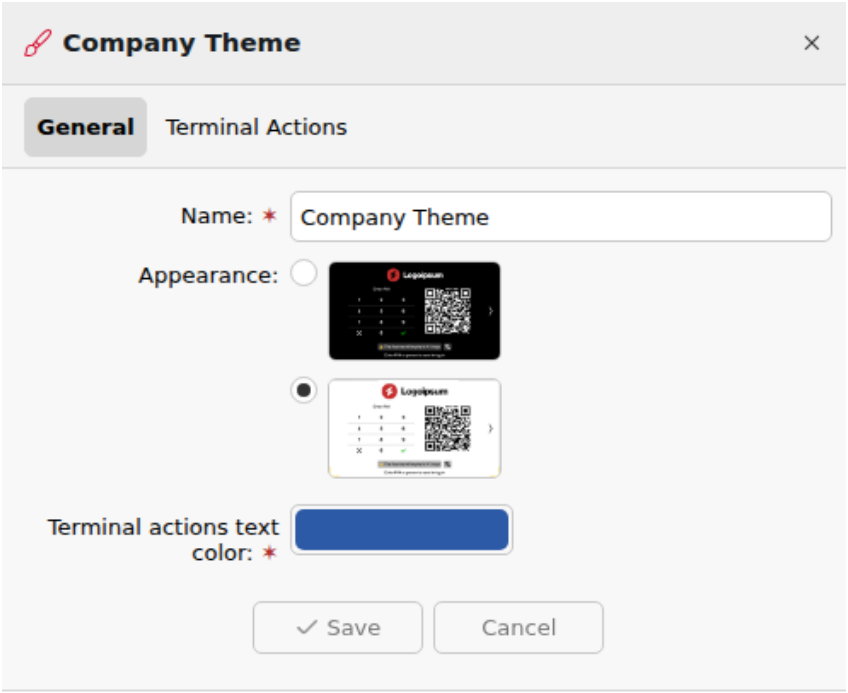
Editing Custom Themes

> Editing the terminal action nodes of a theme here sets the default appearance for a terminal action of that type, however, specific terminal action nodes can be customized further. See .
>
> For example, in the terminal theme editor you can create a theme where, by default, **Easy Scan** actions are green and have a scanner icon. However, after creating an **Easy Scan** action to **Scan to Dropbox**, that action node can be edited in Terminal Actions Settings to display a Dropbox logo and appear blue.

Once a custom theme has been created via duplication or import, simply select that theme and click **Edit**, or double-click the theme to open the editing panel.

General Tab

On the **General** tab you can edit:

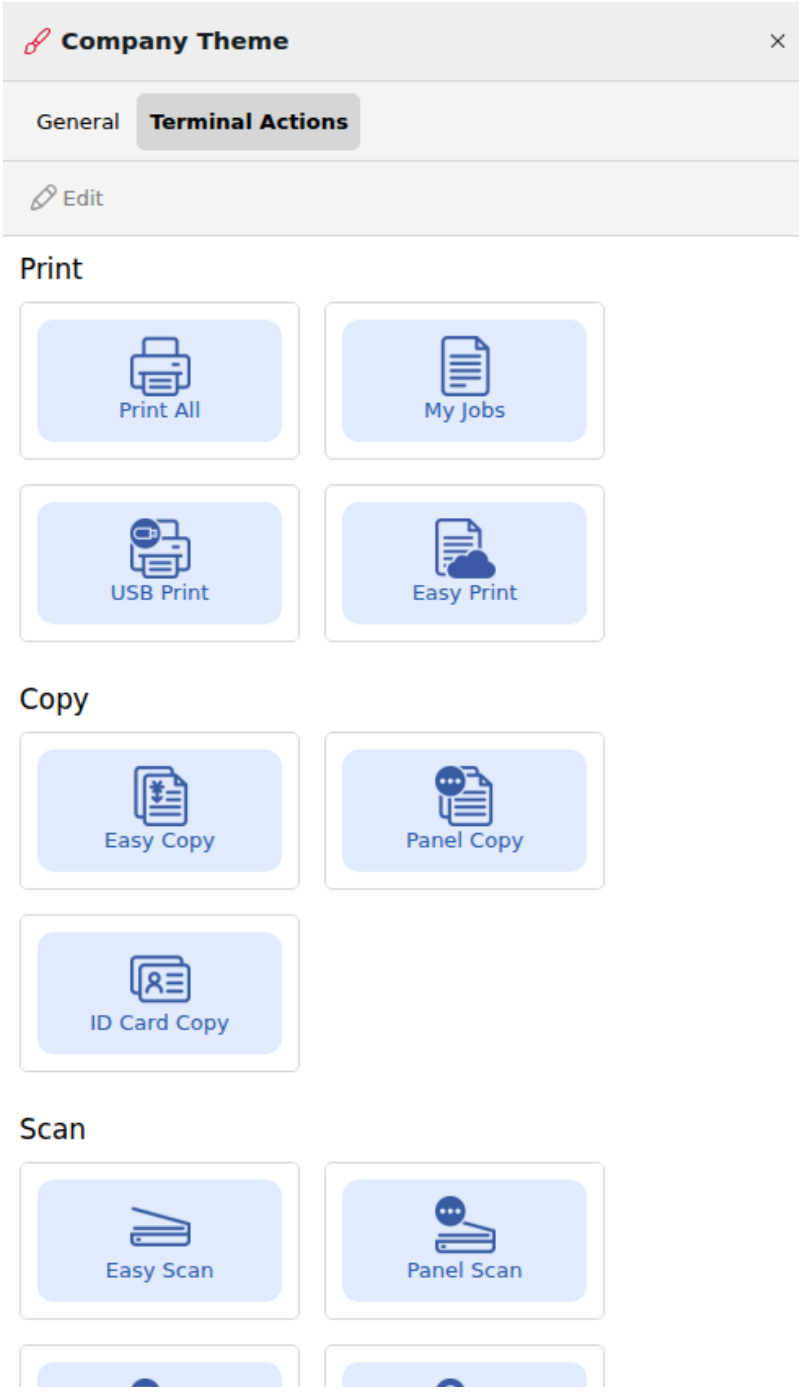


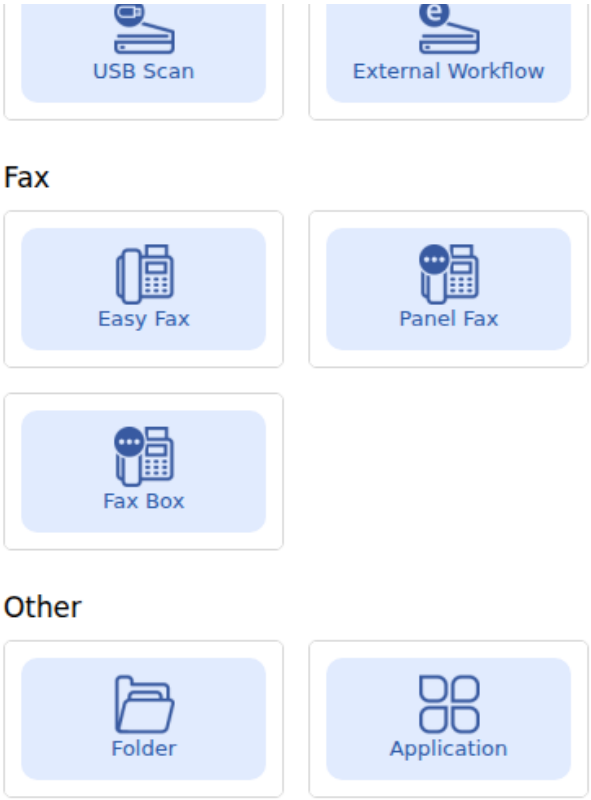
- **Name**: the name of your custom theme.
- **Appearance**: choose black or white as the background color of your theme.
- **Terminal actions text color**: select the color of text for the names of your terminal actions. Ensure this color will be visible against the background color of your terminal action icons.

Click **Save** to save your changes.

Terminal Actions Tab

On this tab you can alter the appearance of your terminal actions. All possible terminal actions are listed on this tab, even ones which might not be set to display on your Embedded Terminals (which can be edited in **MyQ**>**Settings**>**Printers & Terminals**>**Terminal Actions**).





To edit the appearance of a terminal action, select the action and click **Edit** or simply double-click the terminal action.

The editing menu opens with the following options:

- **Name**: displays the name of the selected terminal action, the name cannot be edited here but can be changed in **MyQ**>**Settings**>**Printers & Terminals**>**Terminal Actions**. Names changed in the **Terminal Actions** settings will not be reflected here but will be shown on the embedded terminal.
- **Color**: allows you to change the background color of the terminal action icon. If you use a custom terminal action icon, the background color may not be visible.
- **Icon**: allows you to change the icon displayed for this terminal action. You can either **Browse for a file** on your device, drag and drop an image file onto the selector, or **Paste** a file from your clipboard. File types .jpg, .png, .gif, and .bmp can be used. The selected image will be re-sized automatically, and if it contains transparent space, the selected icon **Color** will be visible in the transparent parts of the image.

Click **Save** to save your changes and **Back** to return to the previous menu and select another terminal action to edit.

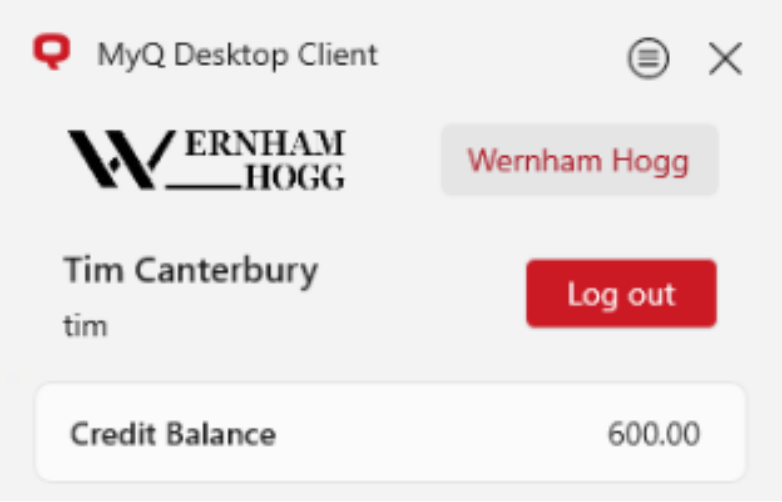
8.24.8 Personalize Desktop Client

For many organizations, the MyQ Desktop Client (MDC) is the main connection between your users and your printing environment. For this reason, we have created the MDC with a series of customizable options so that it reflects your company branding, and can direct users to helpful resources.

Set Up a Company Logo

Similarly to personalizing the Embedded Terminals, a configured custom logo can be used by the MyQ Desktop Client to show your organization's branding.

When no custom logo is used, the default logo of MyQ is used instead.



Recommendations for Custom Logos

- Supported formats: JPG/JPEG/PNG/BMP. Transparent backgrounds are recommended for PNG images.
- Recommended size: 398px x 92px

Custom Links

A custom link can be displayed in the Desktop Client. This helps you to direct users to a page with useful information they might need.

The link is configured in **Settings > Personalization > Custom link in the MyQ Desktop Client**.

Recommendations for Custom Links

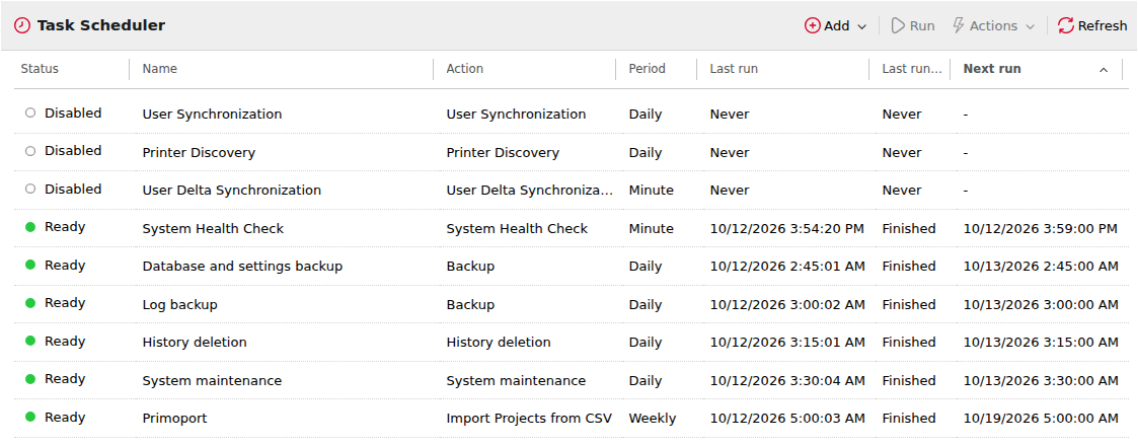
- You can set the link to point to the MyQ Web Interface so that users have easy access to it.
- It might be useful to propagate a link to your intranet or a dedicated page with news, announcements, resources, help links, links to our End-User Guide, or any other content.
- Ideally, the title should not exceed 25 characters, but if it does, it will be split into multiple rows.

8.25 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 Printer Discovery.

In addition, you can import projects or codebooks from CSV files, add scheduled reports, and export users or printers.



Status	Name	Action	Period	Last run	Last run...	Next run
Disabled	User Synchronization	User Synchronization	Daily	Never	Never	-
Disabled	Printer Discovery	Printer Discovery	Daily	Never	Never	-
Disabled	User Delta Synchronization	User Delta Synchroniza...	Minute	Never	Never	-
Ready	System Health Check	System Health Check	Minute	10/12/2026 3:54:20 PM	Finished	10/12/2026 3:59:00 PM
Ready	Database and settings backup	Backup	Daily	10/12/2026 2:45:01 AM	Finished	10/13/2026 2:45:00 AM
Ready	Log backup	Backup	Daily	10/12/2026 3:00:02 AM	Finished	10/13/2026 3:00:00 AM
Ready	History deletion	History deletion	Daily	10/12/2026 3:15:01 AM	Finished	10/13/2026 3:15:00 AM
Ready	System maintenance	System maintenance	Daily	10/12/2026 3:30:04 AM	Finished	10/13/2026 3:30:00 AM
Ready	Primoport	Import Projects from CSV	Weekly	10/12/2026 5:00:03 AM	Finished	10/19/2026 5:00:00 AM

8.25.1 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**.

8.25.2 Creating a Task Schedule

In addition to the seven predefined tasks, you can click **Add** and create any of the following scheduled tasks:

- **Scheduled Report** - redirects to **Reports** where any report can be edited and scheduled. See Reports (see page 680)
- **Import Projects from CSV**
- **Import Code Book from CSV**
- **Users Export** - an additional settings tab for settings **Filters and Parameters** is available.
- **Printers Export**- an additional settings tab for settings **Filters and Parameters** is available.



You can create multiple versions of any of these tasks.

8.25.3 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**.

8.25.4 Automatic Database and Log Backup

There are two automatic backup tasks on the **Task Scheduler** tab. The database and settings backup and the log backup. The backup process is automatic. The files are compressed and saved to the **Backup** folder.

Backup settings

- **Destination folder**: The folder that stores the backup data.
- **Backup Password**: Password-protect the backup. If this field is left empty, the created backup is unprotected.
- **Confirm Password**: Confirm the above password.
- **Delete backup after ___ days**: The days after which the data are deleted from MyQ.

8.26 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, Certificates, Outgoing SMTP Server, MyQ SMTP Server, MyQ FTP Server, MyQ X Mobile Client, HTTP Proxy Server, Firewall Management, and PM Server.

8.26.1 General

In this section, you can view the current **Minimum TLS version (1.2)** that affects MyQ communications (HTTP proxy, SMTP, IPPS, LPR). You can modify the security settings in the `config.ini` file if you want to change this setting.

In the **This server hostname** field, you should enter the hostname of the MyQ Print server. This hostname is used by external components of the MyQ system, such as embedded terminals or MyQ Desktop Client, for communication with the MyQ server.

During remote setup, the server hostname should be a valid hostname or IP address. A licenses update might change the hostname to myq.local. Then the remote setup will fail and result in an error message.

8.26.2 Certificates

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

MyQ offers three different certificate management modes:

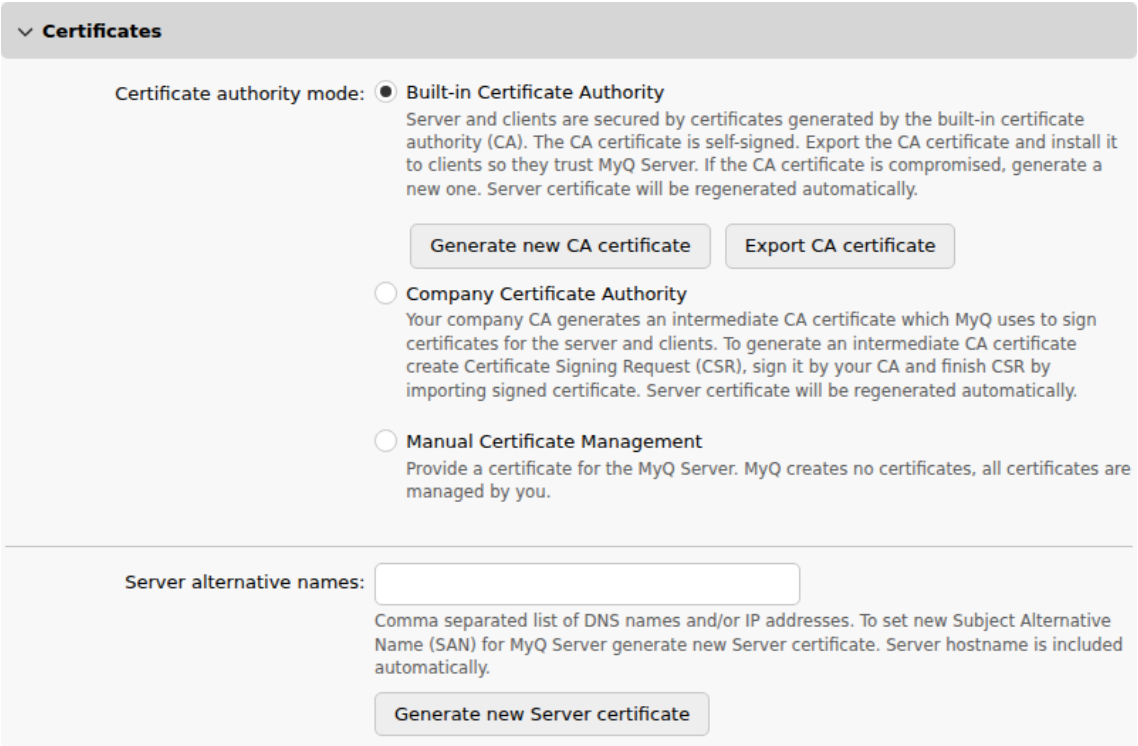
1. **Built-in Certificate Authority** - This is the default mode for new installations. MyQ creates a self-signed CA certificate and uses it to sign server and client certificates. The public key of the CA certificate can be exported (click **Export CA certificate**) to install it to clients, so they 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**.

8.26.3 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 217)
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 (see page 200)
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.

8.26.4 MyQ SMTP Server

In this section you can view and modify the SMTP server settings.

- **SMTP (STARTTLS)** - Enable when using unsecure communication or secure communication over STARTTLS. Port *25* by default.
- **SMTPS(SSL/TLS)** - Enable when using secure communication over SSL/TLS. Port *587* by default.

If scanning to MyQ is enabled, set the port shown here in the device's SMTP settings.

8.26.5 MyQ FTP Server

In this section, you can set the **FTP server port** that terminals use when sending scan jobs to MyQ over the FTP protocol. The FTP port is *21* by default, and the range is *0 to 65535.* If you click the **Generate new password** button, there is a confirmation pop-up informing that if a new password is generated, all the terminals need to be reconfigured.

8.26.6 MyQ X Mobile Client

In this section, you can set the server hostname or IP address and the communication port for using the MyQ X Mobile Client application and MyQ Print Agent. They may differ from the general settings because mobile devices connect via Wi-Fi.

Choose **Use the same settings as on the LAN (*hostname:port*)** to use the same settings as the MyQ server (default) or choose **Use custom settings** and add the **Server** and **Secure port (SSL)** you want to use.

8.26.7 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)
- Universal Print
- Payment Providers
- Site → Central Communication
- Central → Site Communication
- Site → Terminals Communication

8.26.8 Firewall Management

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

8.26.9 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:

- Amazon S3
- eGoldFax
- External Storage API

- Gmail
- Microsoft Entra ID
- Microsoft Exchange Online
- Microsoft Universal Print
- MyQ Document Processor
- MyQ Scan Review
- OneDrive for Business
- RightFax
- SharePoint Online

Connect to External Storage API

The **External Storage API** connection allows the integration of external applications that act as an API gateway into MyQ, to add support for new cloud or network storages.

Example usage

1. A third-party application uses their own storage.
2. An API gateway is developed and installed on a server.
3. In MyQ, a connector is created and pointed at this application.
4. The API gateway understands and maps API calls from one service (MyQ) to the other (e.g. remote file storage).

Connection details

To configure an external storage MyQ:

1. Log in to the MyQ web administrator interface, and go to **MyQ > Settings > Connections**.
2. Click **+Add** and select *External Storage API*.
3. In the pop-up window, fill in the required information, and click **OK**:
    a. **Title** - a title for your external storage.
    b. **URL** - URL where the application is listening
    c. **Login** - the username used for authentication
    d. **Password** - the password used for authentication

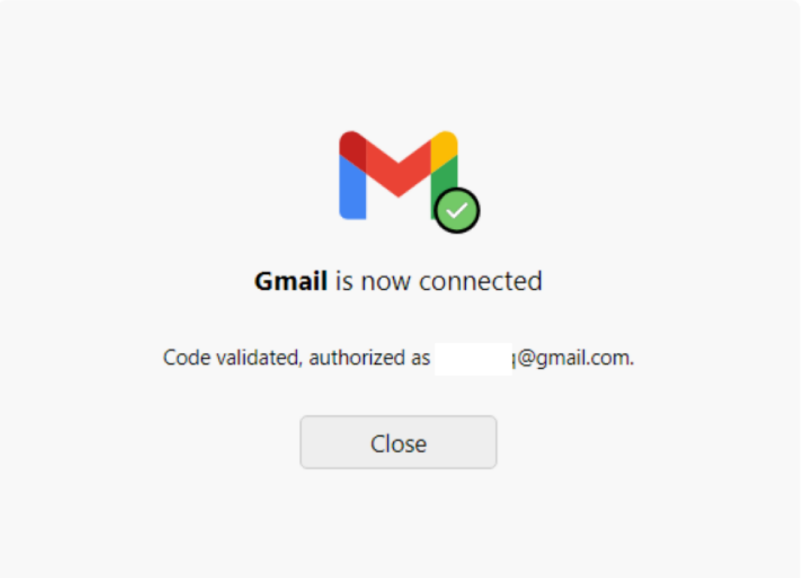
Your newly added external storage can now be used as a destination in the Easy Scan and Easy Print terminal actions, when setting up these actions you can enable or disable the option for users to delete files in storage from the terminal.

Connect to Gmail

To send email from MyQ using Gmail, create a connection. MyQ connects to Gmail using OAuth 2.0, so MyQ doesn't need to store your Google account password.

Create a Gmail Connection in MyQ

1. Go to **MyQ > Settings > Connections**.
2. Click **+Add** and select *Gmail*.
3. In the pop-up window, click **Continue with Google**.
4. Sign in with your Gmail account and authorize MyQ.



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

Gmail can also be configured in the Jobs settings tab, under Jobs via Email as a POP3 or IMAP 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[22].

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

Connect to MyQ Document Processor

MyQ Document Processor is a separate MyQ service that handles advanced document processing for Easy Scan jobs, including OCR, page splitting, and blank page removal. We recommend that you install Document Processor on a different machine from your Print Server system.

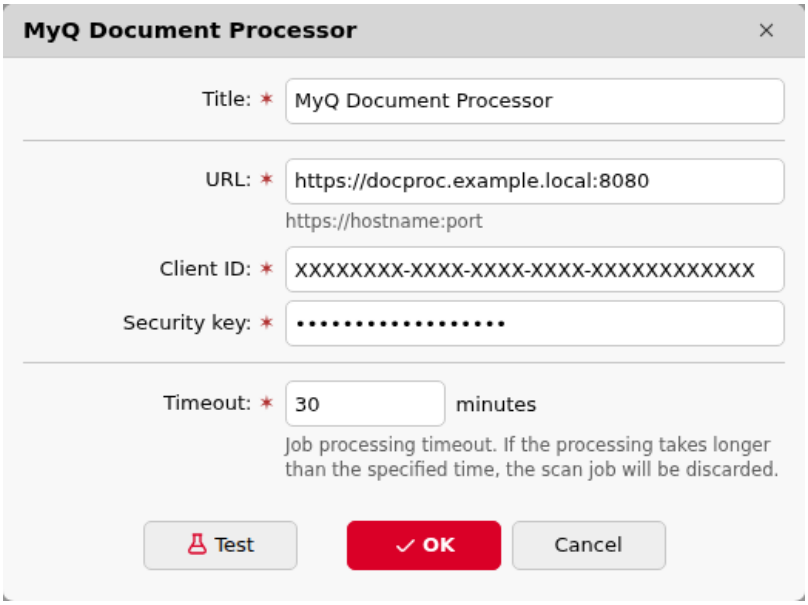
If multiple Document Processor connections are configured, MyQ selects one at random for each job.

Prerequisites

- MyQ Document Processor is installed and configured.
- The Print Server machine trusts the Document Processor machine.
- You have the following values from the Document Processor server:
  - Hostname and port
  - Client ID
  - Secret

Add a MyQ Document Processor Connection

1. Go to **MyQ > Settings > Connections** and click **Add**.
2. Select **MyQ Document Processor**.
3. Configure the following fields:
   - **Title**: enter a name for the Document Processor connection.
   - **URL**: the hostname and port of the Document Processor server. For example: `https://docprocessor:8080`
   - **Client ID**: the client number configured in the Document Processor server
   - **Security key**: the secret that correspond to the client ID.
   - **Timeout:** The job processing timeout. If processing takes longer than this value, the scan job is discarded. Default: 30 minutes.
4. Click **Test** to verify the connection, then click **OK**.



Important: You must use the server hostname in the URL. IP addresses are not supported.

See also:

- OCR Profiles (see page 620)
- Using Document Processor (see page 614)
- (10.3) MyQ Document Processor

Connect to Microsoft Entra ID

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

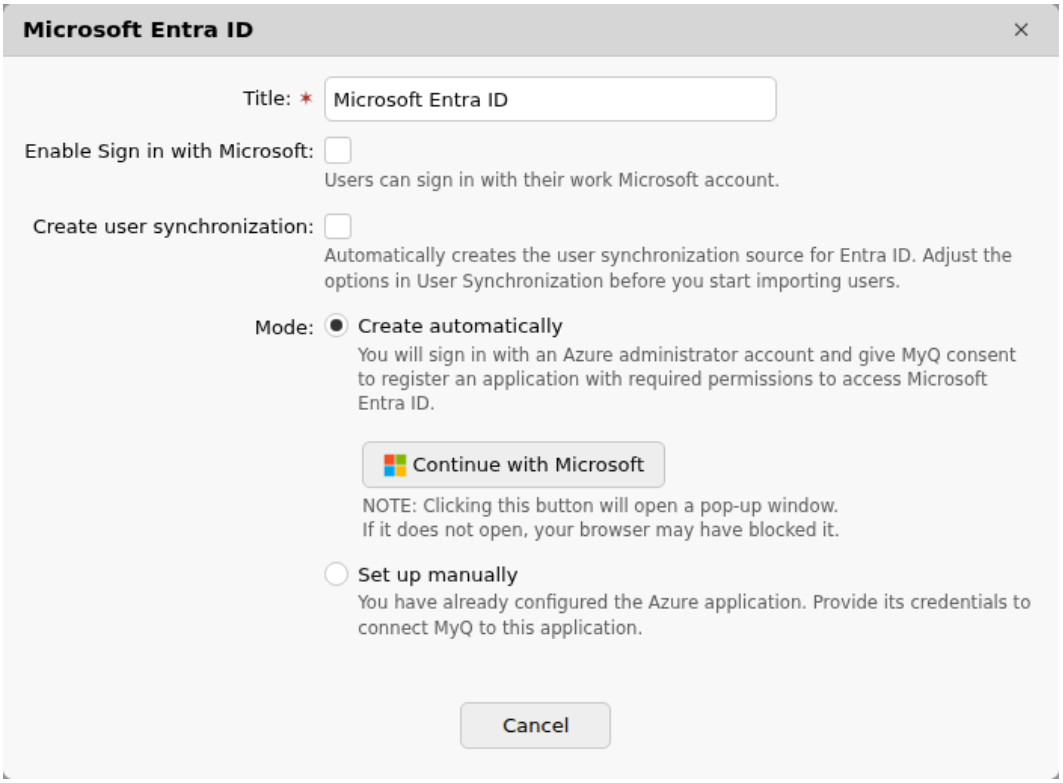
- synchronizing users and groups from Microsoft Entra ID
- authenticating users against Microsoft Entra ID
- Sign in with Microsoft
- Seamless SSO with MyQ Desktop Client

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 Entra application required for accessing Entra ID user information.
   - **Set up manually***:* Configure the Entra application manually. Select this option if you want to manage all aspects of the integration setup.
4. Proceed to the corresponding section below.

Create Automatically

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

Automatic setup applies the following temporary permissions:

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.

See also: (v2) Automatic Microsoft Entra App Registration

Set Up Manually

Select **Set up manually** if your organization manages Microsoft Entra application registrations directly. You can use the same application registration for Microsoft Entra ID, OneDrive for Business, and SharePoint Online, or a dedicated application for each service. The shared application must contain the permissions required by all integrations that use it.

See (v2) Manual Microsoft Entra App Registration.

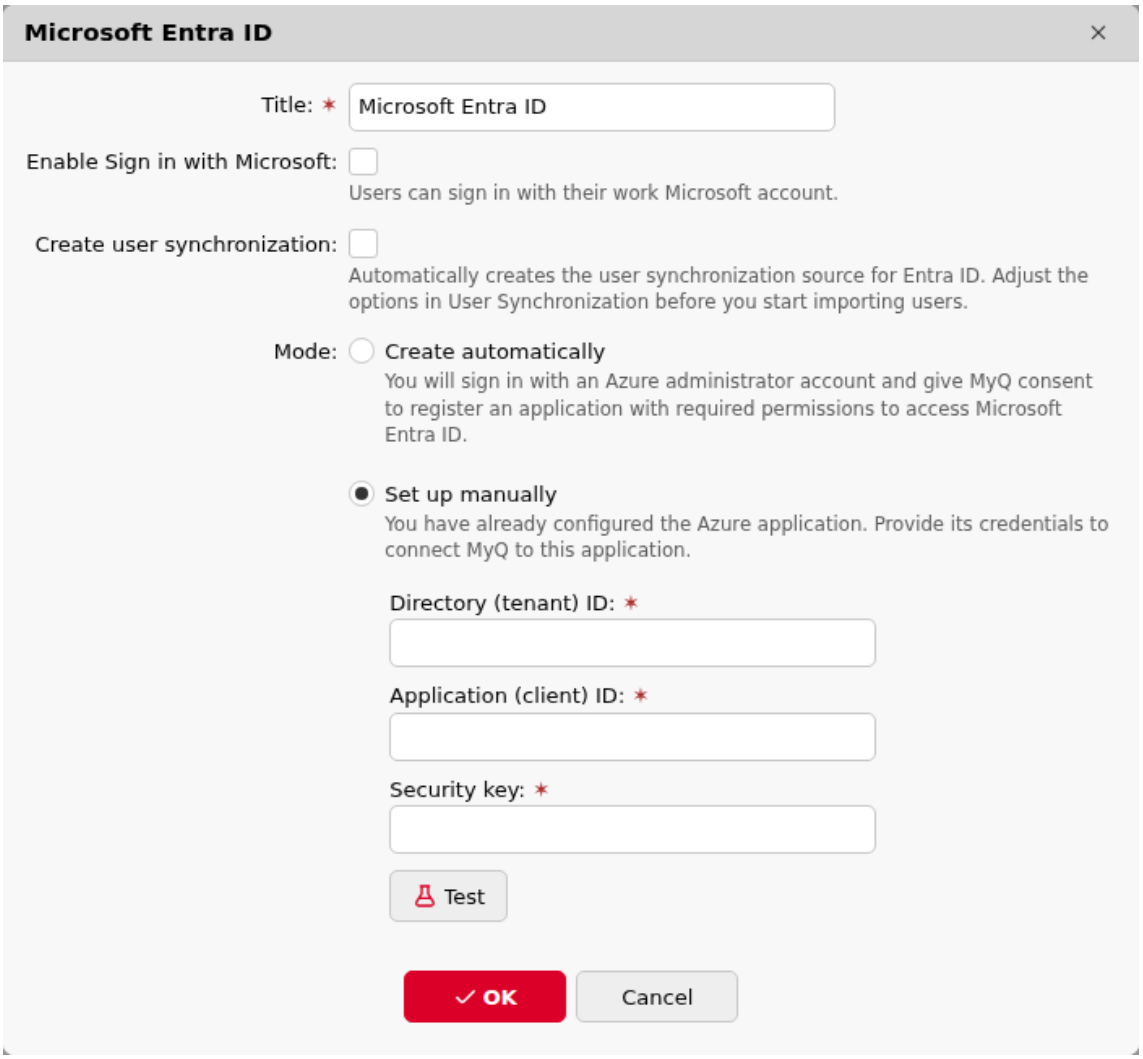
Microsoft Entra ID requires the following runtime permissions:

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

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

Then enter your Microsoft Entra app information into MyQ and save the connection.

- **Title**: a title for the connection.
- **Directory (tenant) ID:** the directory ID of your Entra app.
- **Application (client) ID**: the application ID of your Entra app.
- **Security key:** the Entra app client secret.



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 485)

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 use:

- **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 App Reference

Re-authorizing the Entra ID Connection

Use the **Re-authorize** option to repeat the Microsoft authorization process for an existing connection.

Reauthorization can:

- complete administrator consent that was not granted during the initial setup
- create a new client secret
- recreate a deleted enterprise application
- change the connection between automatic and manual configuration

Reauthorization updates the existing enterprise application when it is still present. It does not create a duplicate.

To re-authorize, right-click on the connection. This opens the create connection dialog. You can repeat all the steps to create a new secret for the existing connection.

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:

- Configure Microsoft Entra ID Authentication (see page 519)
- Synchronize Users from Microsoft Entra ID (see page 485)

Connect to OneDrive for Business

Connect MyQ to OneDrive for Business to make users' storage available to supported MyQ workflows. OneDrive for Business can use the same Microsoft Entra application registration as Microsoft Entra ID and SharePoint Online. You can also use a dedicated application registration.

Before configuring OneDrive for Business, synchronize the users who will use the integration from Microsoft Entra ID. MyQ uses their Microsoft Entra object IDs to associate MyQ users with their OneDrive accounts.

Users created manually or synchronized from sources other than Entra ID will not have access to the OneDrive for Business destination.

See also:

- Connect to Microsoft Entra ID (see page 202)
- Synchronize Users from Microsoft Entra ID (see page 485)

Choose the OneDrive Access Model

MyQ can access OneDrive for Business either using application permissions or on behalf of individual Microsoft users.

Application-Wide Access

With application-wide access, MyQ can access users' OneDrive storage without requiring each user to authorize the connection.

MyQ pairs each synchronized user with their OneDrive using the user's Microsoft Entra object ID. Automatic setup uses this access model. You can also configure it with a manually registered application.

Use application-wide access when users should be able to use OneDrive through MyQ without individually connecting their Microsoft accounts.

Individual User Access

With individual user access, each user authorizes MyQ to access their OneDrive. MyQ then accesses OneDrive on behalf of the signed-in user using delegated Microsoft permissions.

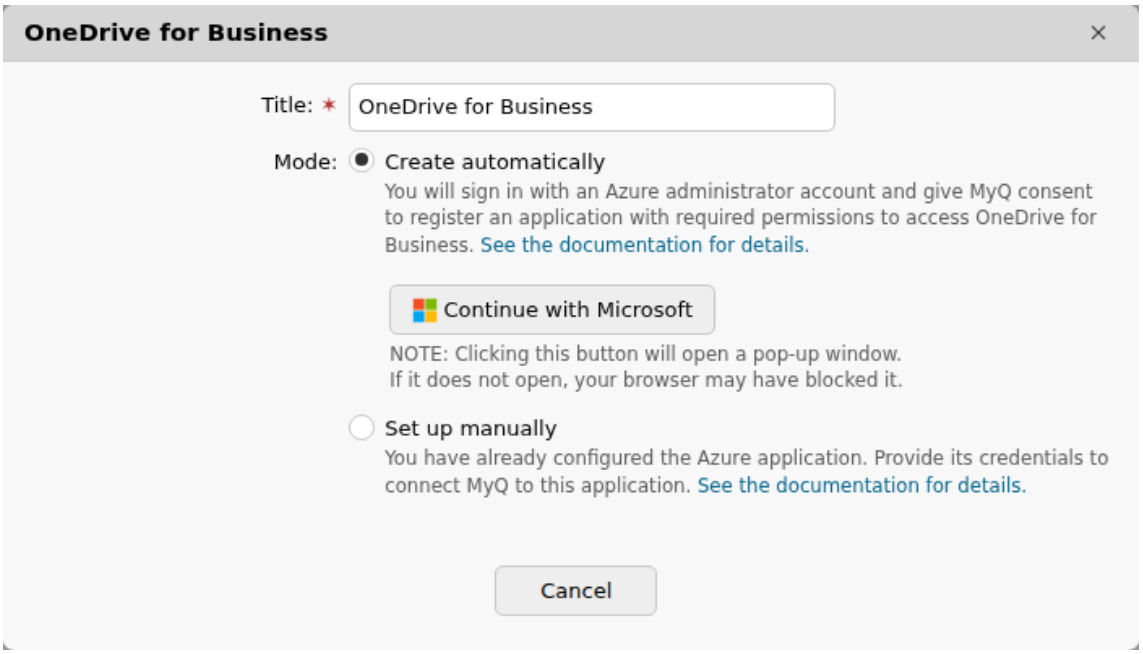
Users connect their OneDrive account from the **Cloud Storage** widget in the MyQ Web Interface. Use this model when users should explicitly authorize MyQ to access their OneDrive storage.

Add the OneDrive for Business Connection

Go to **MyQ > Settings > Connections**, click **Add**, and select **OneDrive for Business**.

Enter a **Title** for the connection and select:

- **Create automatically**
- **Set up manually**



Create Automatically

Select **Create automatically** to let MyQ create and configure the required Microsoft application.

Sign in with a Microsoft administrator account and authorize MyQ to create the connector application.

Automatic setup applies the following temporary permissions:

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.

Complete the Microsoft authorization process and save the connection.

MyQ configures application-wide access. Users synchronized from Microsoft Entra ID are automatically associated with their OneDrive for Business accounts and do not need to authorize it individually.

Set Up Manually

Select **Set up manually** if your organization manages Microsoft Entra application registrations directly. You can use the same application registration for Microsoft Entra ID, OneDrive for Business, and SharePoint Online, or a dedicated application for each service. The shared application must contain the permissions required by all integrations that use it.

See (v2) Manual Microsoft Entra App Registration.

OneDrive for Business requires the following runtime permissions:

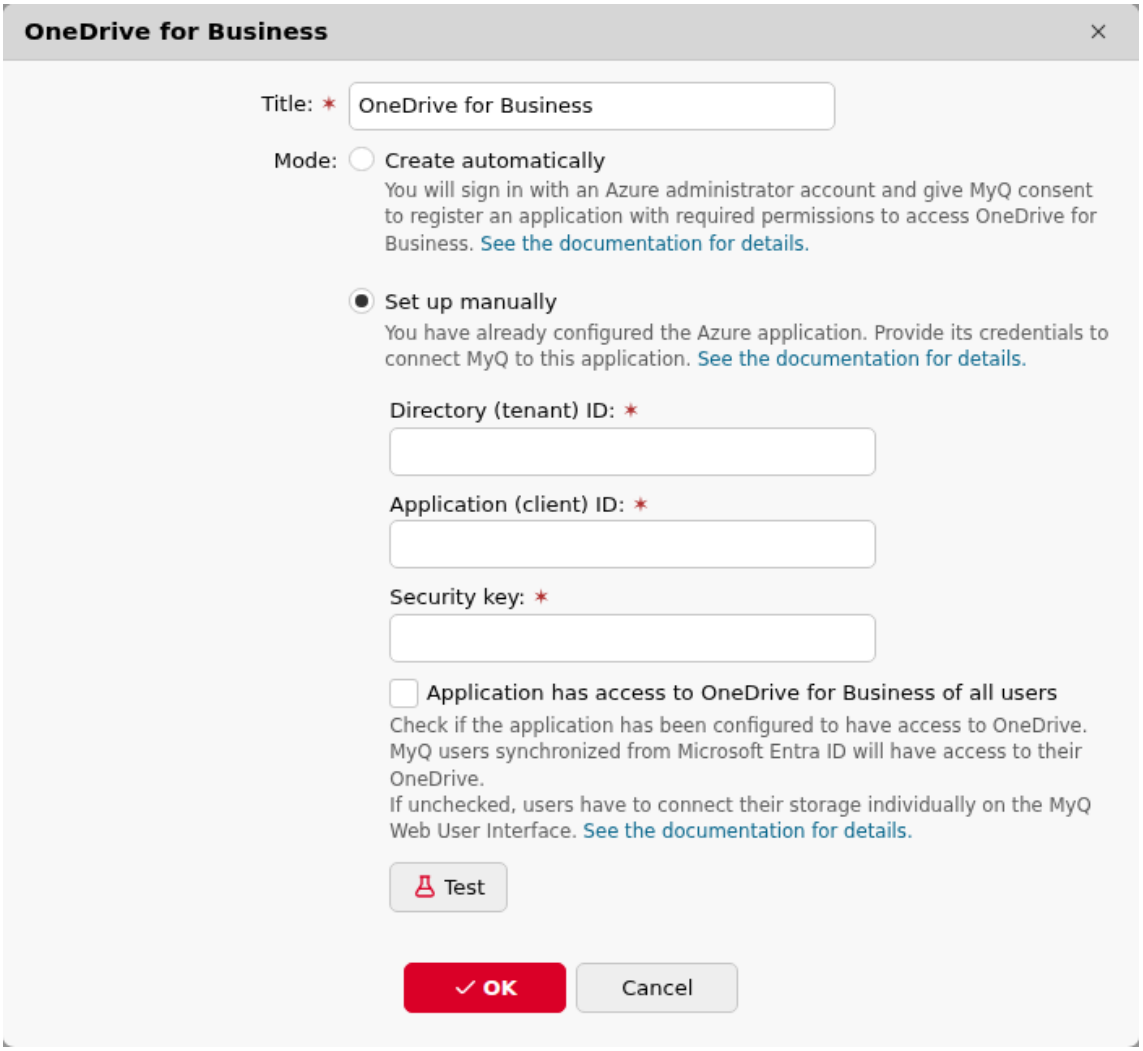
Permission	API	Type	Purpose
`Files.ReadWrite`	Microsoft Graph	Delegated	Read and write files available to the signed-in user.

Permission	API	Type	Purpose
`User.Read`	Microsoft Graph	Delegated	Identify the signed-in user.
`Files.ReadWrite.All`	Microsoft Graph	Application	Access users' files without individual user authorization.

Enter the application details in MyQ:

- **Title:** type a title for the connection.
- **Directory (tenant) ID:** the directory ID of your Entra app.
- **Application (client) ID**: the application ID of your Entra app.
- **Security key:** the Entra app client secret.
- **Application has access to OneDrive for Business of all users:** select this option to use application-wide access. If this option is disabled, users must connect their OneDrive account themselves.

Save the connection.



Re-authorizing the OneDrive for Business Connection

Use the **Re-authorize** option to repeat the Microsoft authorization process for an existing connection.

Reauthorization can:

- complete administrator consent that was not granted during the initial setup
- create a new client secret
- recreate a deleted enterprise application
- change the connection between automatic and manual configuration

Reauthorization updates the existing enterprise application when it is still present. It does not create a duplicate.

To re-authorize, right-click on the connection. This opens the create connection dialog. You can repeat all the steps to create a new secret for the existing connection.

Pairing Users with Their OneDrive

If you used Automatic mode or selected **Application has access to OneDrive Business of all users** in the manual setup, users do not need to do anything to connect their OneDrive accounts. Users are paired with their OneDrive storage via their unique user ID (UUID). These are automatically imported only with the Entra ID user's synchronization into MyQ. The UUID is synchronized from Central to Sites during user sync when Central users are synchronized with Entra ID. This process enables users at a Site to be automatically connected to their storage.

Next Steps

When a OneDrive for Business connection is configured, you can set it as a source or destination for printing and scanning.

See also:

- Scan to OneDrive for Business (see page 360)
- Print from OneDrive for Business (see page 389)

Connect to SharePoint Online

Connect MyQ X to SharePoint Online to make SharePoint cloud storage available to supported MyQ scan and print workflows.

SharePoint Online can use the same Microsoft Entra application registration as Microsoft Entra ID and OneDrive for Business, or a dedicated application registration.

Choose the SharePoint Access Model

MyQ supports two ways of accessing SharePoint Online.

Application-Wide Access

With application-wide access, MyQ accesses SharePoint using permissions granted to the application rather than the permissions of individual users.

MyQ users do not need to have Microsoft accounts or be synchronized from Microsoft Entra ID.

> ⚠ **Important:** All MyQ users using this connection receive the same SharePoint access granted to the application. Individual Microsoft or SharePoint permissions are not applied, so users may be able to access files that they could not access with their own Microsoft account.

Use this model only when uniform, centrally managed SharePoint access is appropriate for the users who can access the MyQ workflow.

Individual User Access

With application-wide access disabled, each user must connect their SharePoint Online storage from the MyQ Web Interface using their Microsoft account.

After the user signs in, MyQ stores an access token for that user. SharePoint operations are then performed on behalf of the individual user, and access to sites and files follows the permissions assigned to their Microsoft account. This provides more granular access control and preserves the organization's existing SharePoint Online permissions.

Use this model when access through MyQ should follow the permissions of individual Microsoft users.

Add the SharePoint Online Connection

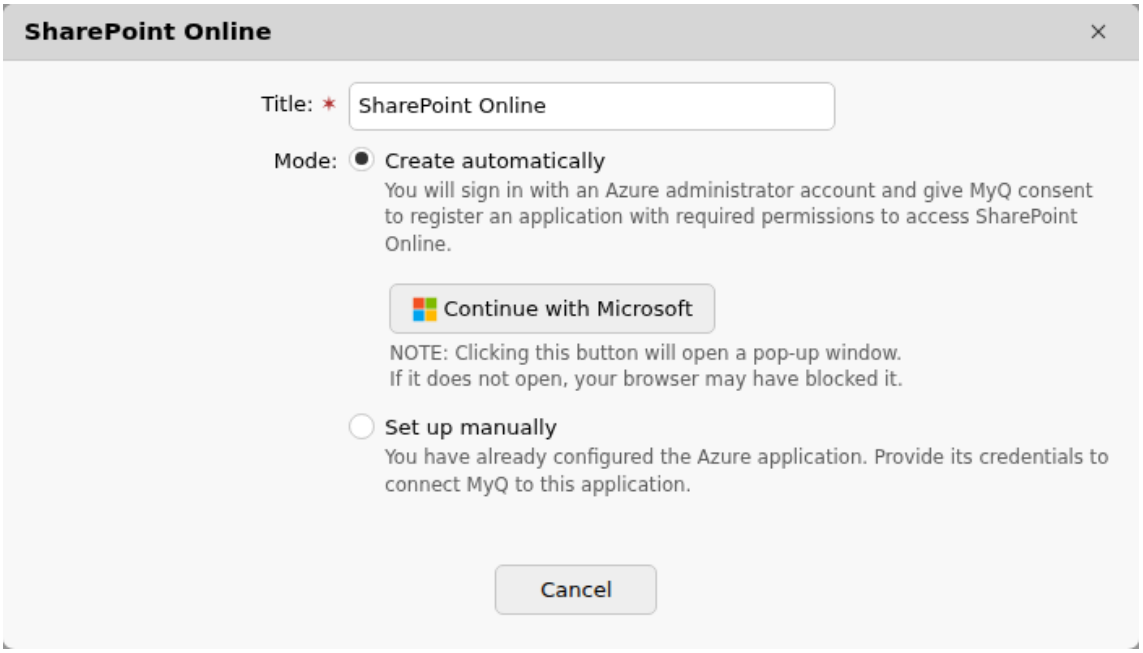
Go to **MyQ > Settings > Connections**, click **Add**, and select **SharePoint Online**.

Enter a **Title** for the connection and choose how the Microsoft application is configured:

- **Create automatically**
- **Set up manually**

Create Automatically

Select **Create automatically** to let MyQ create and configure the required enterprise application in your Microsoft Entra tenant.



Follow the Microsoft authorization process and then save the connection.

Automatic setup configures application-wide access to SharePoint Online. Individual users do not need to connect their Microsoft accounts to MyQ.

See also: (v2) Automatic Microsoft Entra App Registration

Set Up Manually

Select **Set up manually** if your organization manages Microsoft Entra application registrations directly. You can use the same application registration for Microsoft Entra ID, OneDrive for Business, and SharePoint Online, or a dedicated application for each service. The shared application must contain the permissions required by all integrations that use it.

See (v2) Manual Microsoft Entra App Registration.

SharePoint Online requires the following permissions:

Microsoft Entra ID requires the following runtime permissions:

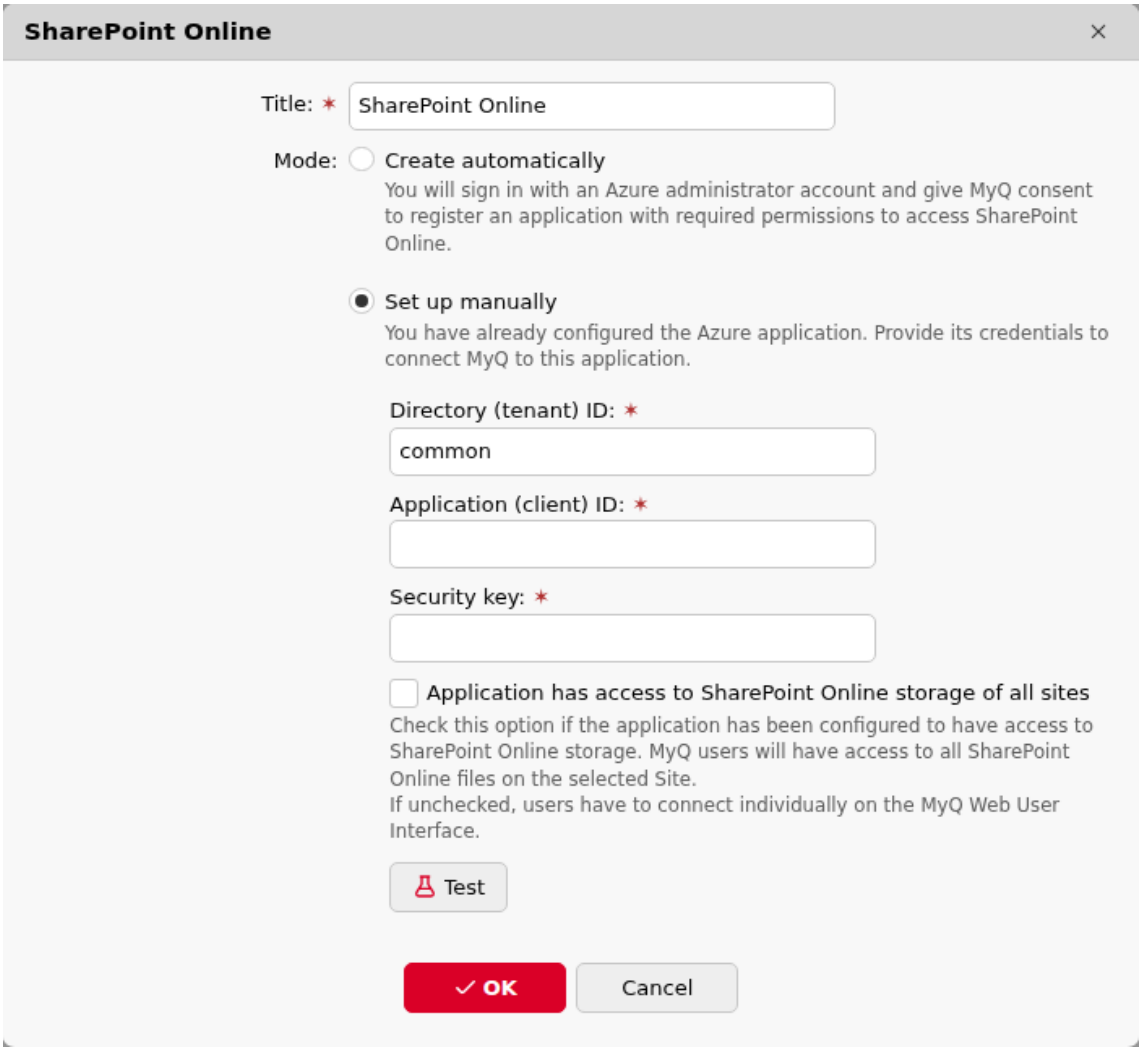
Permission	API	Type	Purpose
`Group.Read.All`	Microsoft Graph	Application	Read groups and group membership.
`User.Read.All`	Microsoft Graph	Application	Read users.

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

Enter the following details in MyQ:

- **Title**: enter a title for the connection.
- **Directory (tenant) ID:** the directory ID of your Entra app. In most cases, the **Directory (tenant) ID** can remain set to `common`.
- **Application (client) ID**: the application ID of your Entra app.
- **Security key:** the Entra app client secret.
- **Application has access to SharePoint Online storage of all sites:** select this option for application-wide access. If this option is disabled, users must connect their SharePoint Online account themselves.

Save the connection.



Re-authorize the SharePoint Online Connection

Use the **Re-authorize** option to repeat the Microsoft authorization process for an existing connection.

Reauthorization can:

- complete administrator consent that was not granted during the initial setup
- create a new client secret
- recreate a deleted enterprise application
- change the connection between automatic and manual configuration

Reauthorization updates the existing enterprise application when it is still present. It does not create a duplicate.

To re-authorize, right-click on the connection. This opens the create connection dialog. You can repeat all the steps to create a new secret for the existing connection.

Next Steps

When a SharePoint Online connection is configured, you can set it as an Easy Print source or Easy Scan destination in terminal actions.

One connection can support multiple terminal actions. In the terminal action settings, you can control the storage with the following options: all available SharePoint sites (multi-site) a single site, only sites followed by the user, folder browsing, or a specific folder within a site.

See also:

- Terminal Actions (see page 322)
- Scan to SharePoint Online (see page 364)
- Print from SharePoint Online (see page 390)

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.

Microsoft Exchange Online requires the following runtime permissions:

Permission	API	Type	Purpose
`User.Read`	Microsoft Graph	Delegated	Sign in and read the mailbox user's profile. Required for authentication.
`IMAP.AccessAsUser.All`	Microsoft Graph	Delegated	Read, update, create, and delete email in the user's mailbox. Required for Jobs via Email using IMAP. Does not include sending email.
`SMTP.Send`	Microsoft Graph	Delegated	Send email from the user's mailbox. Required for outgoing mail.

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, and in the **Jobs** settings tab, in Jobs via Email as a POP3 or IMAP server.

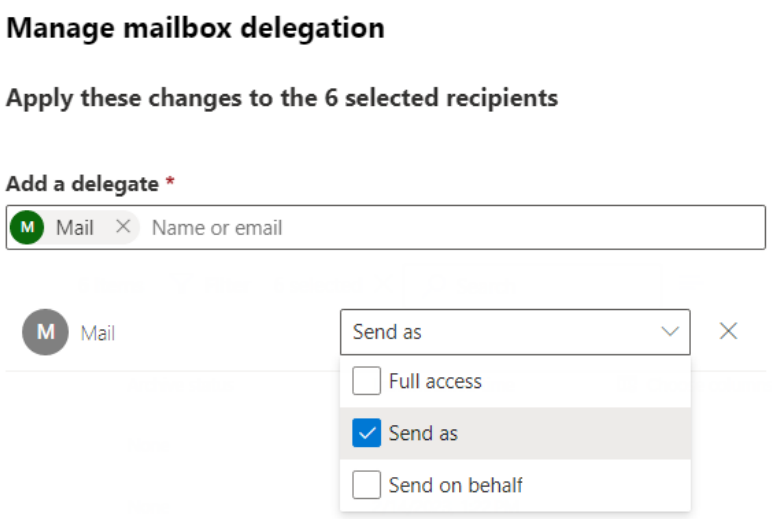
Send Scan as the Logged-In User

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[23].
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.

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



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.

Connect to Microsoft Universal Print

Microsoft Universal Print is a cloud-based print service from Microsoft. MyQ integrates with Universal Print by registering virtual printers in Azure that map to MyQ queues. Jobs submitted via Universal Print are downloaded by MyQ periodically and processed as standard print jobs.

Prerequisites

- An application is registered in Azure with the appropriate permissions. You need its Directory (tenant) ID and Application (client) ID to create the connection in MyQ.
- You have a Microsoft account with a Universal Print license assigned. You use it to finish the connection.

See also: (v2) Set up Microsoft Universal Print

Set Up a Microsoft Universal Print Connection

1. Go to **MyQ > Settings > Connections**.
2. Click **+Add** and select **Microsoft Universal Print**.
3. Fill in the required fields:

- **Title**: enter a name for this connection, for example `Universal Print`.
- **Directory (tenant) ID**: the value from your Azure application.
- **Application (client) ID**: the value from your Azure application.

4. Click **OK**.
5. Copy the code from the pop-up window, click the provided URL, enter the code, and follow the on-screen instructions to authorize the connection.

The authorization code expires after 15 minutes. If it is not confirmed in time, an error appears in the **Issues** column in the **Queues** section when a user next attempts to create a printer. MyQ generates a new code at the next attempt.

To use this connection with a queue, go to **MyQ > Queues** and open a queue for editing. On the **Job Receiving** tab, set **Jobs via MS Universal Print** to **Enabled,** and click **Save**.

After a few minutes the queue appears as a virtual printer in Microsoft Universal Print.

Connect to MyQ Smart Workflows

In order to create a MyQ Smart Workflow you need to install and configure the ScannerVision server to work with the MyQ server.

ScannerVision is a solution to automate document workflows, by capturing, processing, and storing scanned documents. This may include bar code reading, recognizing texts with the help of Optical Character Recognition (OCR), or converting documents to another format. Storage possibilities include a network folder, a database, cloud storage or storing as an e-mail attachment.

ScannerVision extends the features of MyQ by allowing the user to perform a customized and personalized scan workflow, and can utilize the user's credentials to access the storage where the scanned document will be placed, making not only secure printing possible, but also secure scanning.

Prerequisites

- 1 MyQ Embedded license
- 1 ScannerVision license
- Two servers setup (one for the MyQ server, one for the ScannerVision server). In case of a MyQ Central Server setup, one server can be used.
- ScannerVision server 9.1+
  - EMB Kyocera 7.5.9
  - EMB Kyocera 8.1.1+

- EMB HP Enterprise 8.1.1+ (supported in exploded mode as well)

ScannerVision Manual



Embedded Terminal Guides

- MyQ Brother Embedded
- MyQ Canon Embedded
- MyQ Epson Embedded
- MyQ Fujifilm Embedded
- MyQ HP Embedded
- MyQ KATUN Embedded
- MyQ Kyocera Embedded
- MyQ Kyocera Embedded Lite
- MyQ Lexmark Embedded
- MyQ Ricoh SmartSDK Embedded
- MyQ Sharp Embedded
- MyQ Sharp Luna Embedded
- MyQ Toshiba Embedded
- MyQ Xerox Embedded

Install ScannerVision Server

.NET Framework 4.8 has to be installed on the server before installing ScannerVision. If it is not installed, open Server Manager and install it.

To install the ScannerVision server:

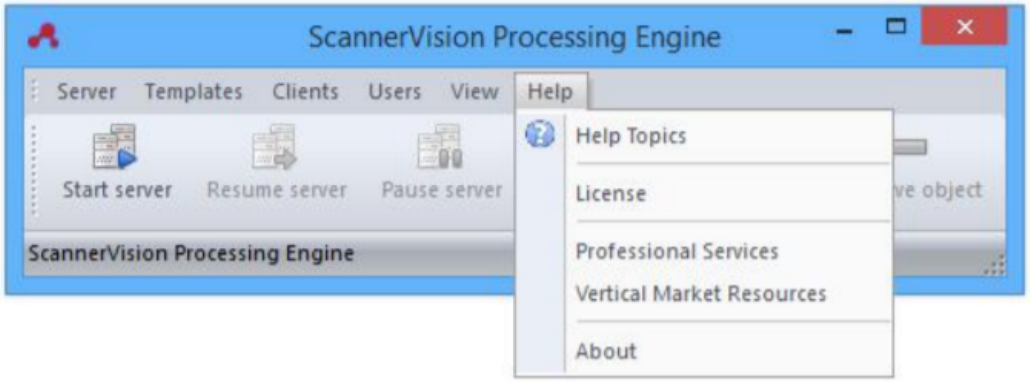
1. Run the ScannerVision installer.
2. Follow the installation wizard's instructions and install the server.

3. Activate the product.

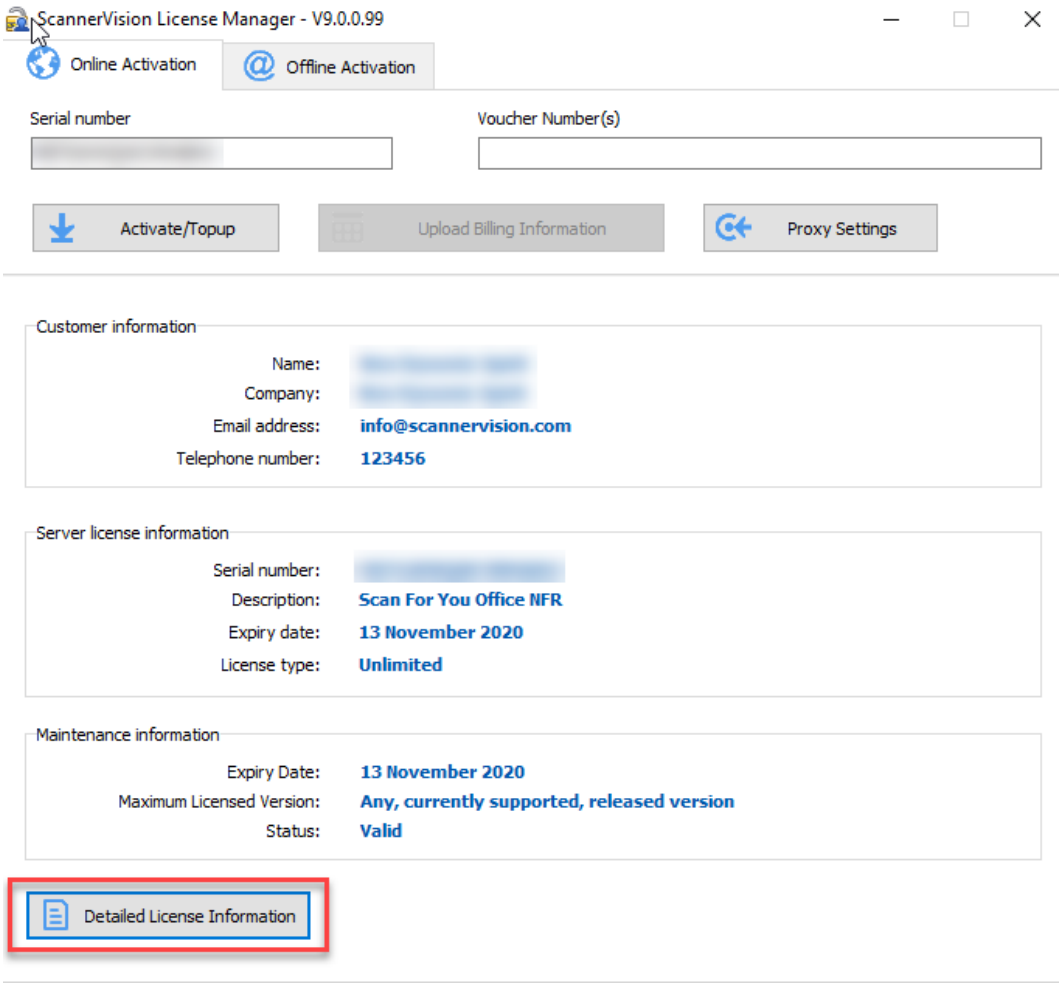
License Check

Once the ScannerVision server is installed and activated, verify the license information:

1. Open the ScannerVision Processing Engine user interface application.
2. On the top menu, click **Help, License**.



3. ScannerVision License Manager opens. Click **Detailed License Information**.



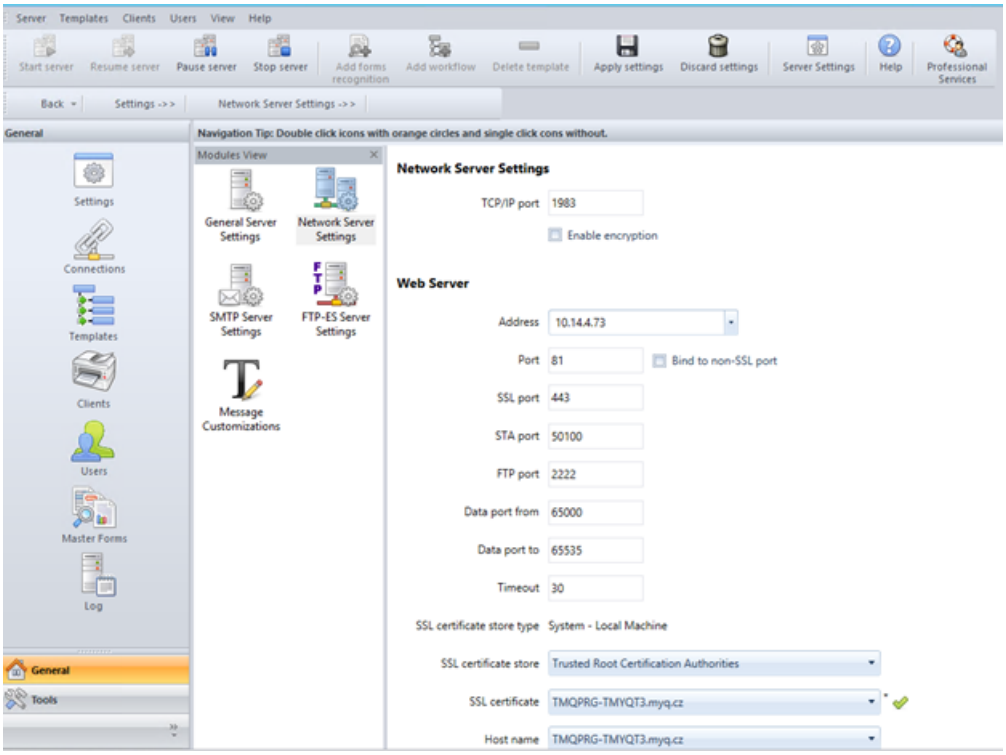
4. Check if the number corresponds to the MyQ device licenses number.

Configure ScannerVision

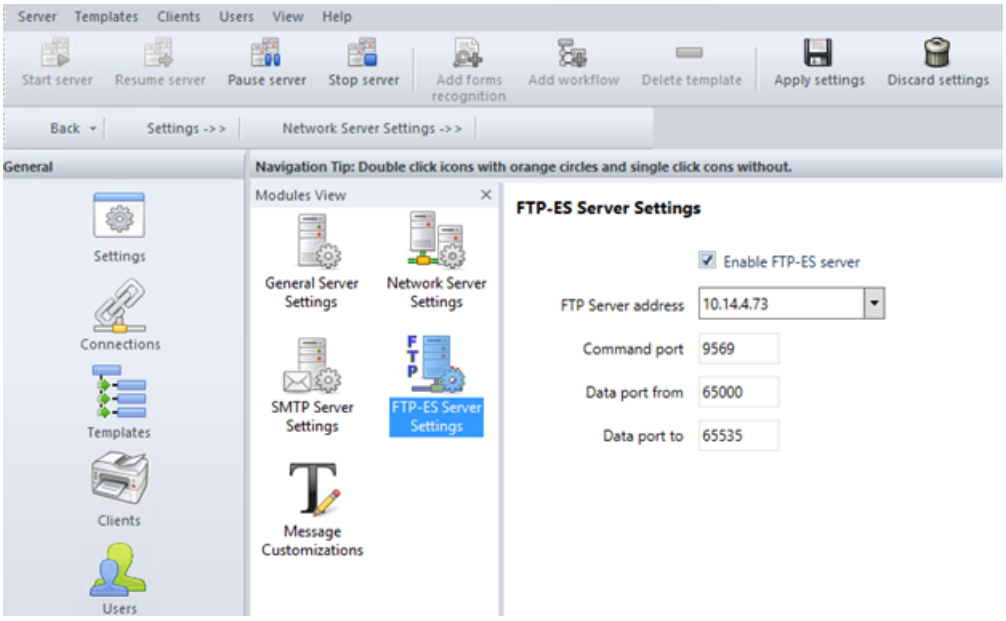
In order to set ScannerVision properly, you need to configure Network settings, Templates, Clients and Users.

Network Settings

1. Open ScannerVision. **Settings** is shown by default.
2. Click **Network Server Settings** in the **Module View**.



3. Add the IP address or hostname of the ScannerVision Web Server in the **Address** field.
4. Change the preset ports if necessary.
5. Enable/disable non SSL.
6. Configure the **FTP-ES server settings**:



7. **Save** your settings.

See also:

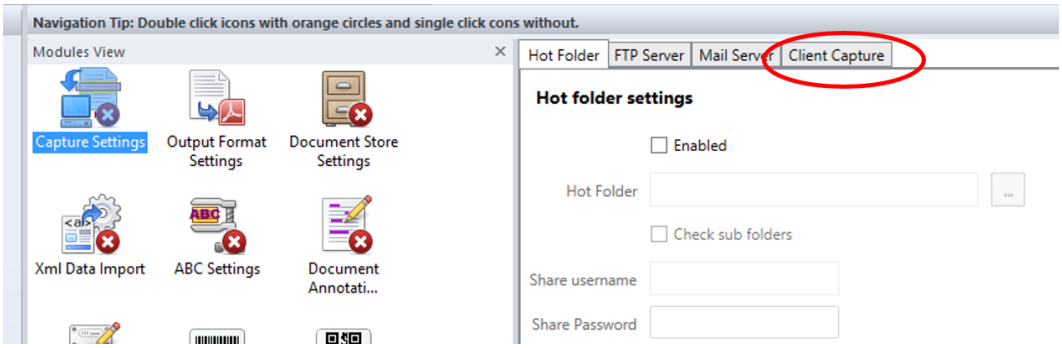
- Templates (see page 226)
- Clients (see page 228)
- Configuring Users (see page 229)

Templates

Templates control what actions ScannerVision performs. They determine where documents come from, what processing is done on them and where they ultimately end up. Multiple templates can be defined and assigned to users and groups.

To add a new template:

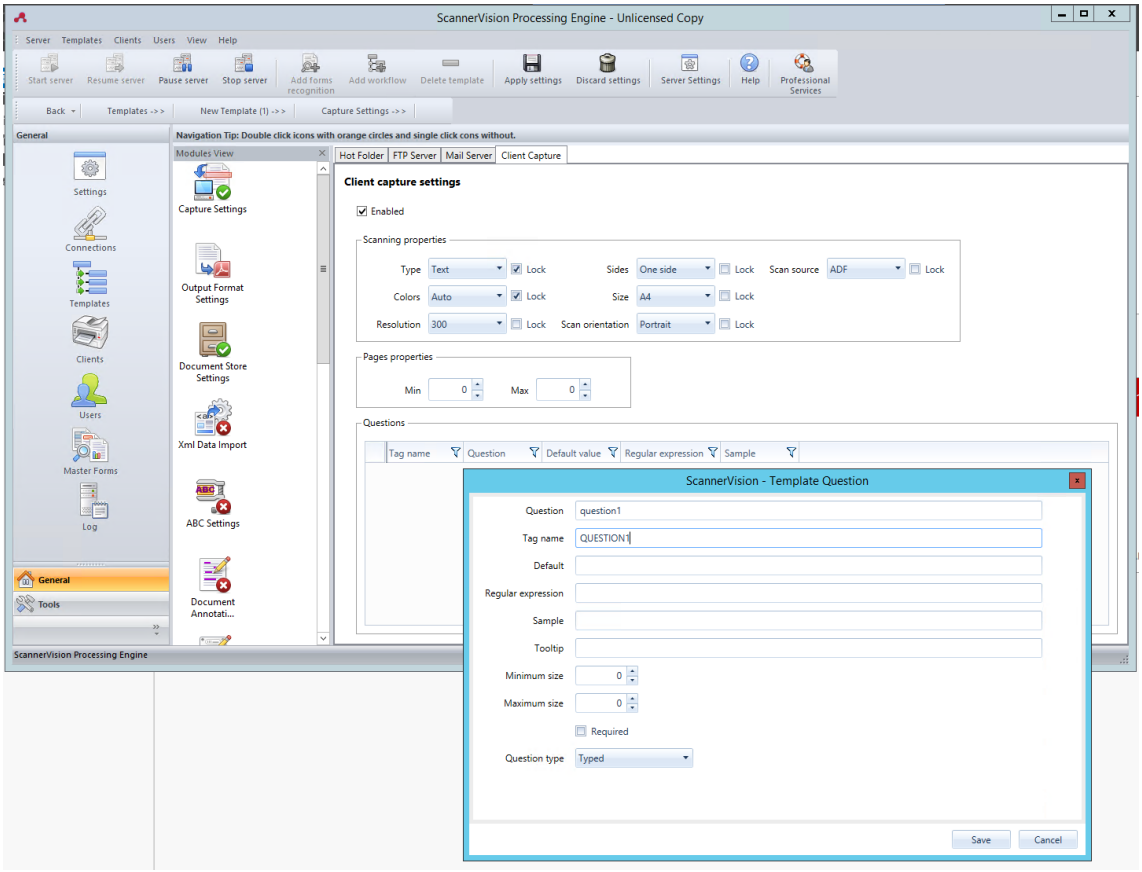
1. Open ScannerVision Processing Engine and click **Templates** in the **Navigation Panel**.
2. Click **Add Workflow** in the top menu.
3. **Name** the new template and mark it as **Enabled**.
4. Click **Apply Settings** in the top menu.
5. Once saved, double-click on the new template. In the right tab of the window, select **Client Capture**.
6. In the Client Capture tab, mark the **Enabled** checkbox. Now the template's settings are editable.



Adding Questions on a Template

Questions are used to capture necessary document information. To add a new **Question** to a template, in the Client Capture tab:

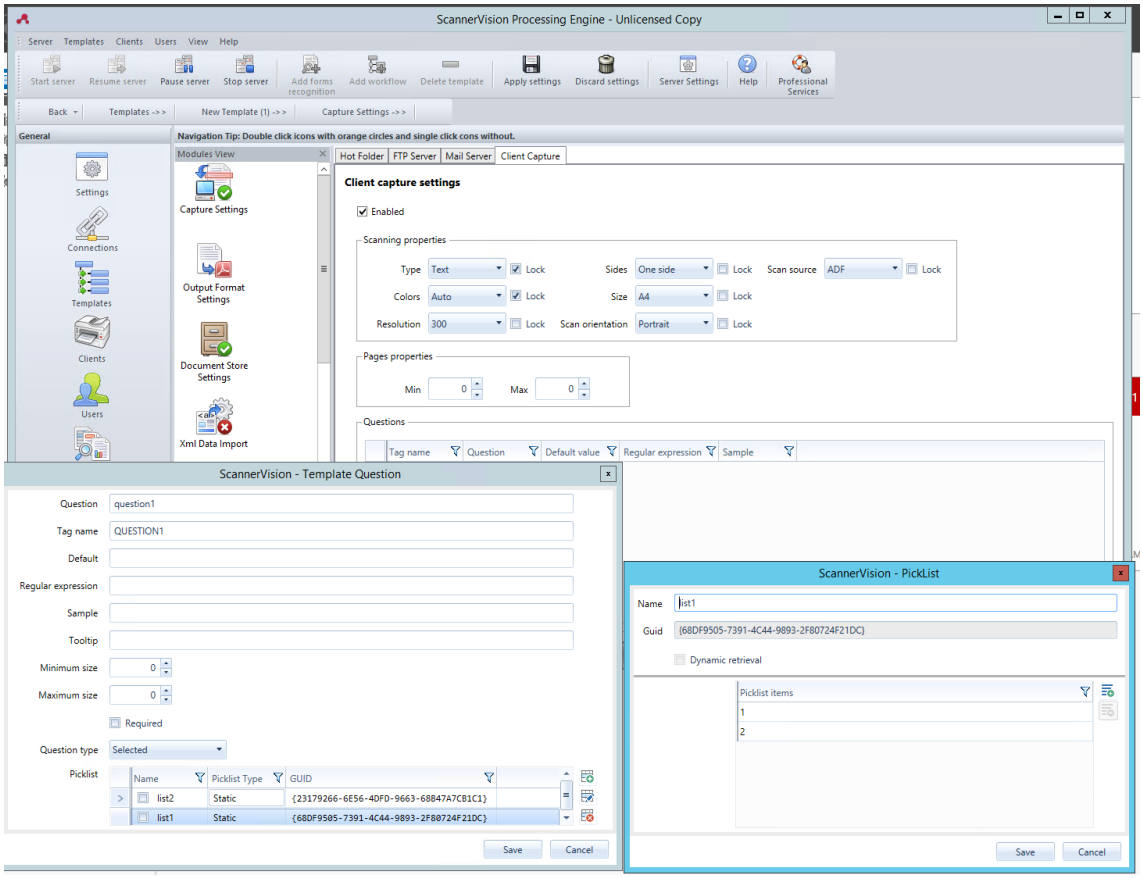
1. Right click on the **Questions** area.
2. Select **Add question**.
3. In the new Template Question window, fill in the **Question**, **Tag name**, and **Default** text fields, and any other of the optional fields.
4. In **Question Type** select *Typed*.
5. Click **Save**.



Adding a PickList to a Question

A **PickList** can be added to a **Question** within a template, if the **Question Type** selected is *Typed*. To add a **PickList**:

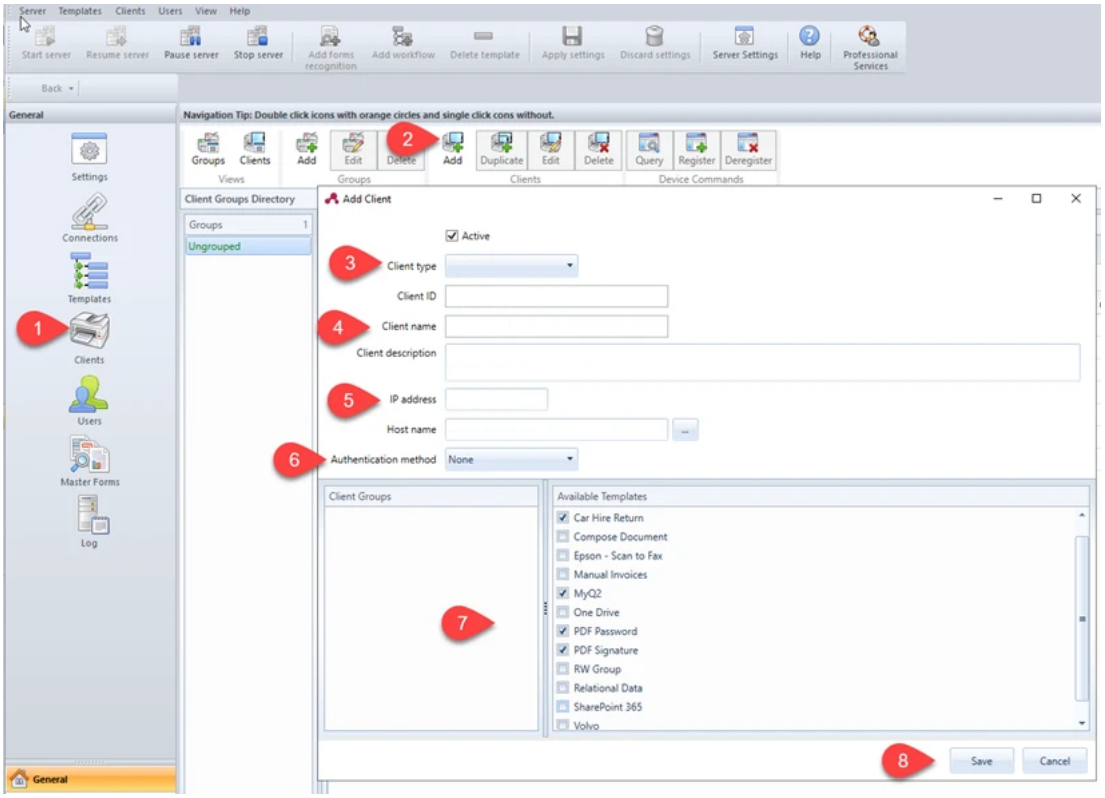
1. Click on the **Add PickList** button on the right.
2. Once there, select *Static* as the **PickList Type**.
3. In the Picklist window, enter a **Name** for the picklist.
4. Add picklist items by pressing the plus (**+**) button on the right.
5. Click **Save**.
6. Once saved, select the picklist(s) to be displayed for this question and click **Save**.



Clients

The clients you configure here represent the MyQ terminals connected to ScannerVision. To add a client, go to the ScannerVision Processing Engine and:

1. Click **Client** on the **Navigation Pane**.
2. Click **Add** under the **Clients** view.
3. Choose *MyQ* as the **Client type**.
4. Optionally add a **Client name** and **Client description**.
5. Add the printing device's **IP address** (make sure to use the device's IP address and not the MyQ server one).
6. Choose an **Authentication method** from:
    a. *None* - everyone can access the same templates
    b. *ScannerVision* - Used for Single Sign On; Users have customized template lists.
7. Choose the templates to be accessed by everyone, in case *None* was the authentication method of choice.
8. Click **Save**.

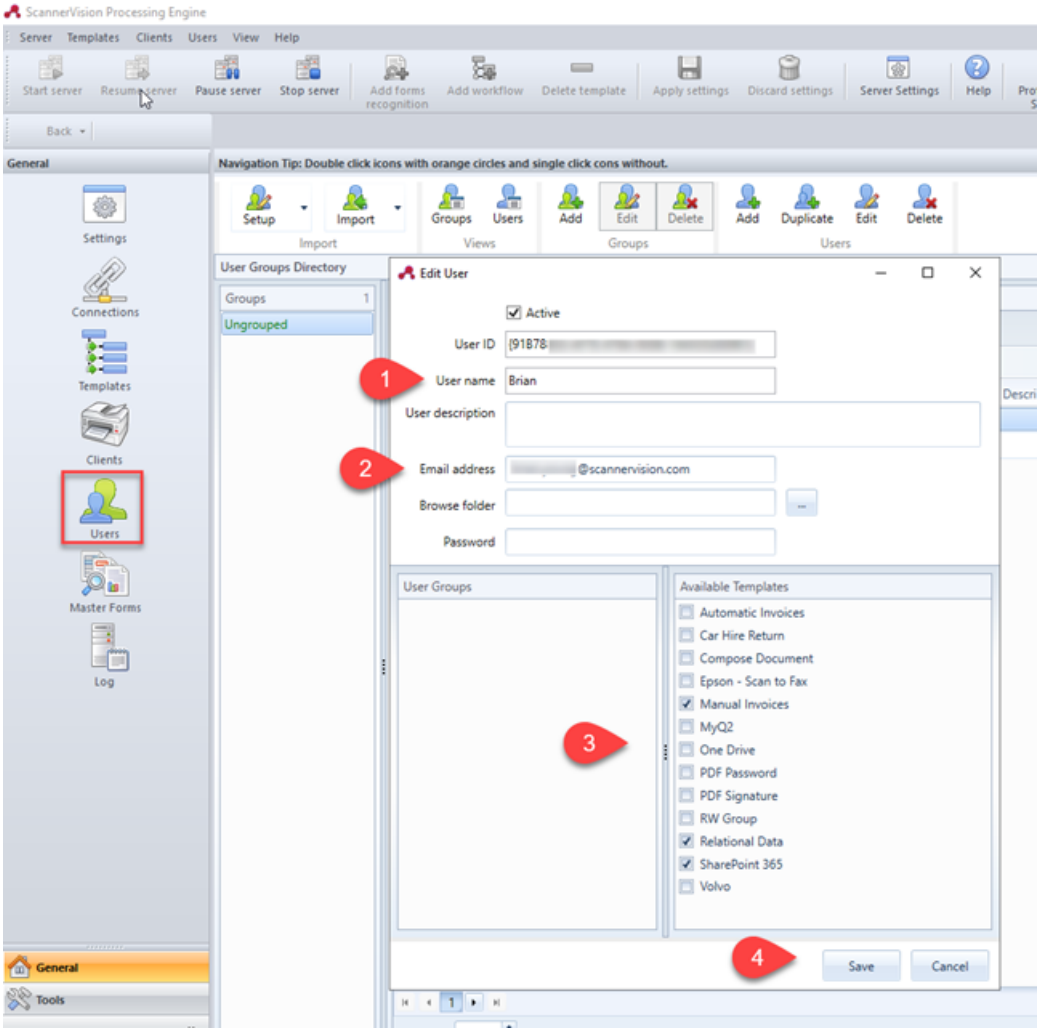


Configuring Users

Users can be imported from a Windows Server, LDAP, AD or they can be manually added. For further instructions, please check the *ScannerVision User Manual*. Users also need to have templates assigned to them.

Whichever method is chosen, the users in ScannerVision have to match MyQ Users. If users are imported, their properties such as names and email addresses will match, however **Templates** will still need to be assigned to them. To check and make necessary modifications, go to ScannerVision Processing Engine, click **Users** on the **Navigation Panel** and:

1. Make sure that the **User name** matches the MyQ user name (if users were manually added).
2. Make sure that the **Email address** matches the MyQ user's email address (if users were manually added).
3. Select templates for the user from the **Available Templates**.
4. Click **Save**.



Adding ScannerVision as a Terminal Action in MyQ

After configuring ScannerVision (network settings, templates, clients, users), you should create a MyQ Smart Workflow in **Terminal Actions**.

1. Go to **MyQ > Settings > Terminal Actions**.
2. Right-click on **Home screen**, select **Add action into this folder**, and then click on **External workflow** on the list of actions. The action is added to the list and the terminal preview. Double-click on it to modify its settings. The node's properties panel opens on the right side.
3. Fill out the **External workflow** as follows
    - Enter a **Title**: the name of the **External workflow** action in the **Home** screen pane and on the terminal preview.

- Change the **Printers** and/or **Rights** if you want to create a specific MyQ Smart Workflow.
  d. Click **Save**.
- Enter the **URL** of the ScannerVision server <hostname>:<port>. The port number is not required if the default settings (*80* for non SSL and *443* for SSL) are used on the ScannerVision server. If the port was changed, the port number is required.

Connect to 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.

Prerequisites

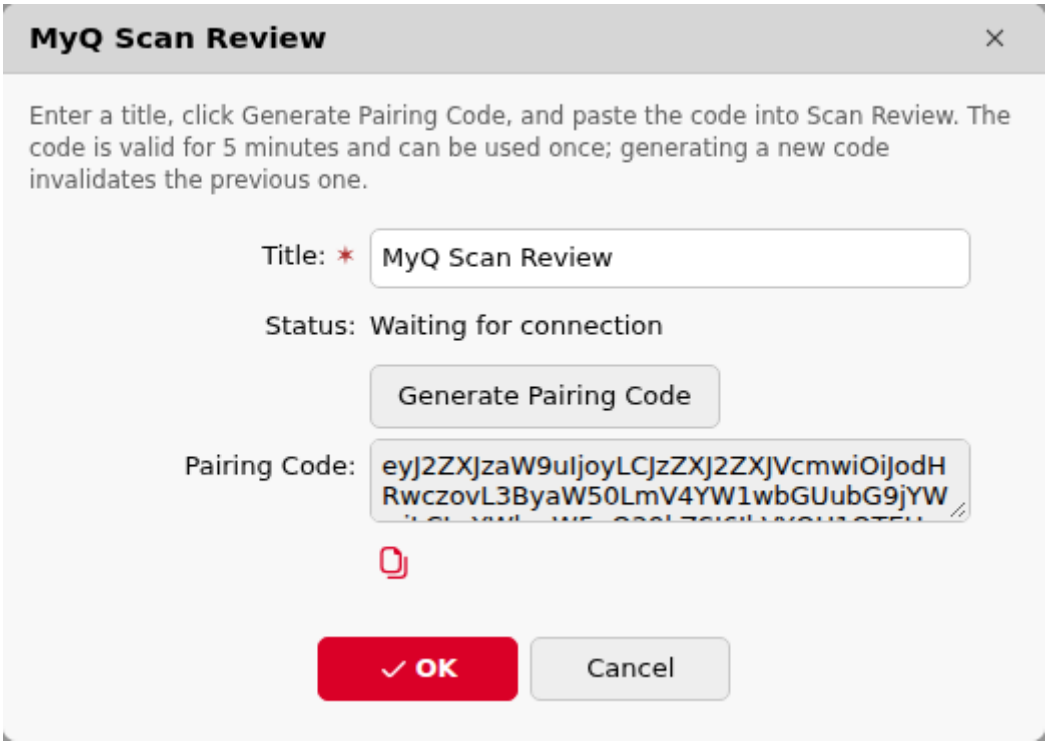
- Scan Review is installed and trusts your MyQ Server. See (10.3) MyQ Scan Review, (10.3) Pairing with Print Server
- You can access the Scan Review web interface on the Scan Review machine.
- You have a MyQ user account, other than ***admin**, that can sign in to Scan Review.

Add a MyQ Scan Review Connection

You pair the connection in two places: generate a pairing code in MyQ, then enter the code in Scan Review.

1. Sign in to the MyQ web administrator interface with the **Administrator** or **Manage settings** rights.
2. Go to **MyQ > Settings > Connections**, click **Add**, and select **MyQ Scan Review**.
3. In **Title**, enter a name for the Scan Review connection.
4. Click **Generate Pairing Code** and copy the code. The pairing code is valid for 5 minutes.

   If it expires, close the connection dialog, open it again, and generate a new code.



5. On the Scan Review machine, open the Scan Review web interface: use the Scan Review system tray menu, or go to `http://localhost:7184` in a browser.
6. Enter the pairing code and click **Save and continue**.
7. In Scan Review, configure the Scan Review hostname and HTTPS certificate. See (10.3) Configure Scan Review.
8. When Scan Review prompts you, sign in with a MyQ user account other than ***admin**.

After pairing, Scan Review registers its own REST API application in MyQ and sets up the connection. The **Scan Review** destination is now available in the Easy Scan terminal action.

Delete a MyQ Scan Review Connection

1. Go to **MyQ > Settings > Connections**.
2. Right-click the Scan Review connection and select **Delete**.
3. Click **Yes** to confirm.

> If MyQ shows the error **Connection "Scan Review" is in use and cannot be deleted**, remove the Scan Review destination from all terminal actions, and then delete the connection.

See also:

- (10.3) MyQ Scan Review
- (10.3) Configure Scan Review

8.26.10 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 User Authentication (see page 507).

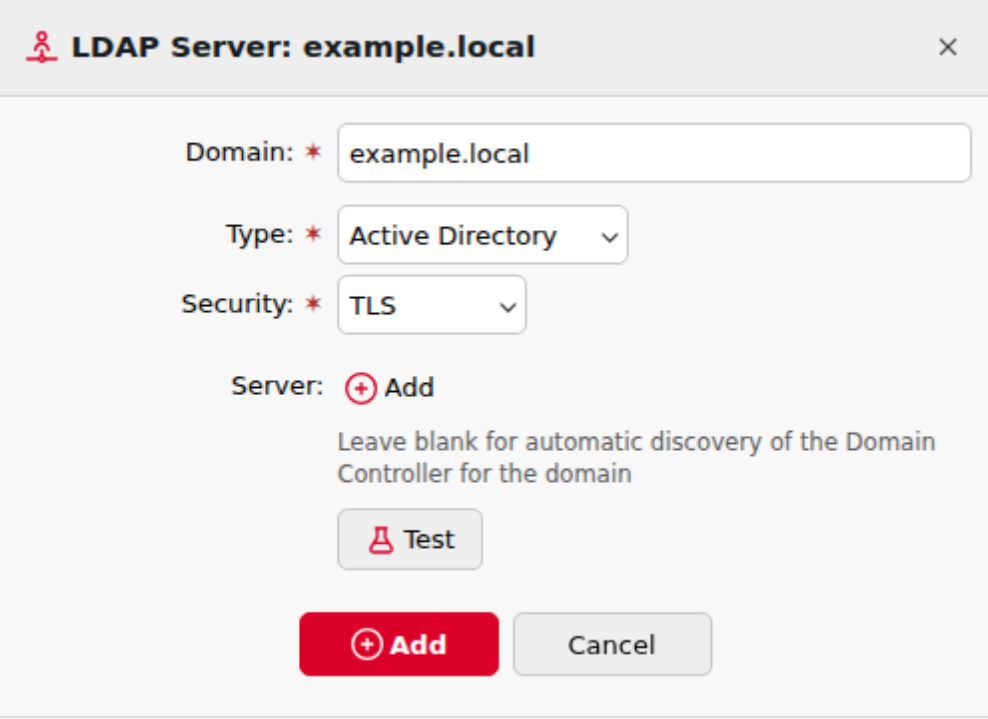
- On embedded terminals using the username + password login screen, and when printing via AirPrint, users linked to an external authentication server can authenticate with either their external account password or their MyQ PIN. MyQ checks the entered value locally first: if it matches the user's PIN, 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.



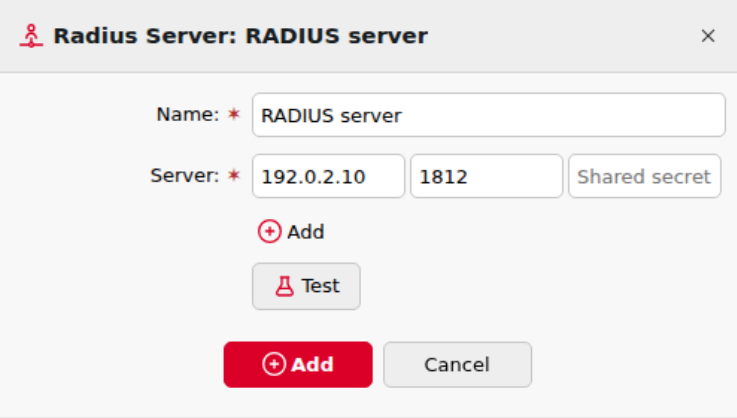
Add Microsoft Entra ID Server

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 (see page 202).
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:

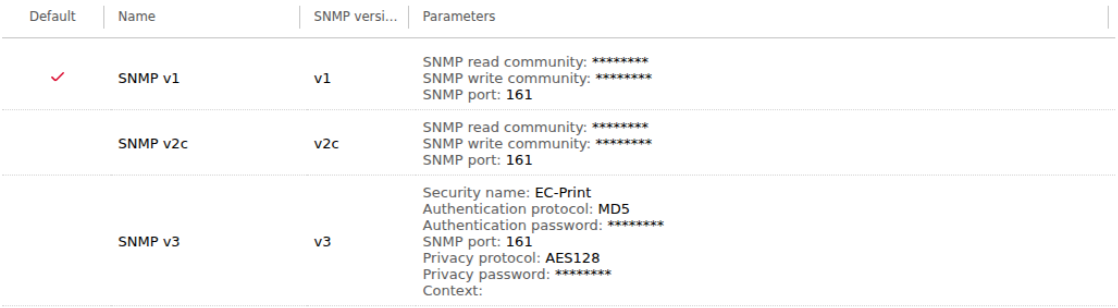
- Authenticate Users from LDAP or RADIUS (see page 500)
- Configure Microsoft Entra ID Authentication (see page 519)

8.26.11 SNMP Profiles

By default, the SNMP v1 protocol is used for communication with printing devices in the MyQ system. Instead of it, you can use the more recent SNMP v2c protocol or the SNMP v3 protocol, which significantly increases the communication security with a printing device.

Multiple SNMP profiles can be created in MyQ, and each printing device can be assigned one of the profiles. This way, you can have one profile for all printing devices with a particular SNMP configuration.

The default SNMP profile can be changed. To make any SNMP profile the default one, select it on the **SNMP** settings tab, and then click **Default** on the bar at the top of the tab (or right-click the profile, and then click **Default** on the shortcut menu).



Default	Name	SNMP versi...	Parameters
✓	SNMP v1	v1	SNMP read community: ******** SNMP write community: ******** SNMP port: 161
	SNMP v2c	v2c	SNMP read community: ******** SNMP write community: ******** SNMP port: 161
	SNMP v3	v3	Security name: EC-Print Authentication protocol: MD5 Authentication password: ******** SNMP port: 161 Privacy protocol: AES128 Privacy password: ******** Context:

Adding and Editing SNMP v1 and v2c Profiles

With the SNMP v1 and v2c protocols, a single string called "*SNMP Community string*" is used to allow access to the device. Only two parameters need to be set in MyQ: the **SNMP read community** parameter and the **SNMP write community** parameter. Their values have to match the values of their counterparts on the printer's Web User Interface (Read Community, Write Community).

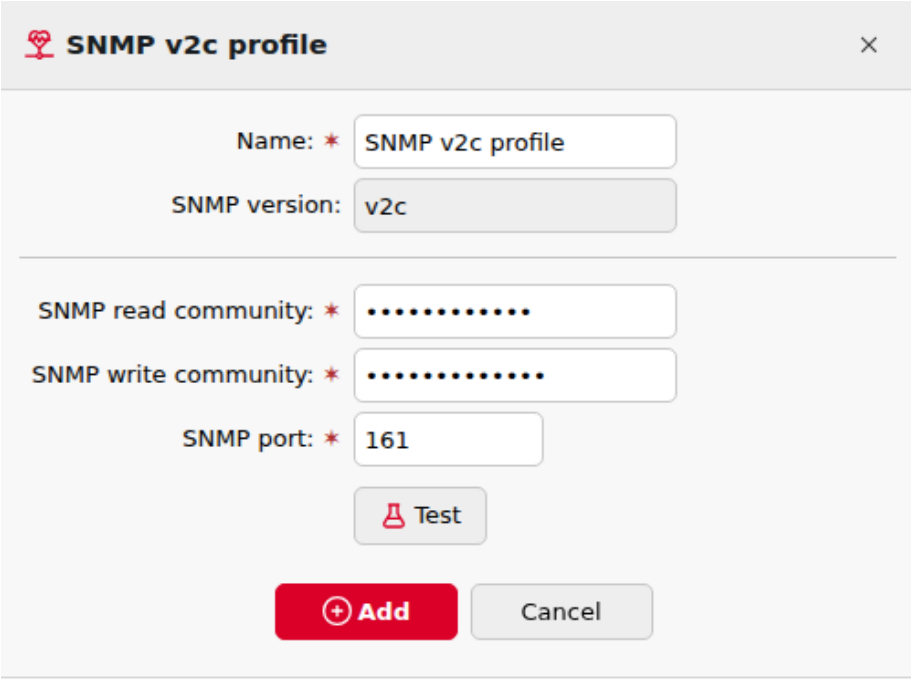
To add a new SNMP v1 or v2c profile:

1. On the MyQ Web Admin Interface, open the **SNMP** settings tab (**MyQ > Settings > SNMP**).
2. On the bar at the top of the **SNMP** tab, click **+Add SNMP profile**, and then click **+SNMP v1** or **+SNMP v2c** on the shortcut menu. The new SNMP profile properties panel opens on the right side of the screen.
3. On the panel, enter the name of the profile, set the parameters, and then click **Save**. The new profile is displayed on the list on the SNMP settings tab.

To open and edit a SNMP v1 or v2c profile:

1. To open the SNMP profile properties panel, select the profile on the **SNMP** settings tab, and then click **Edit** (or right-click the profile, and then click **Edit** on the shortcut menu, or double-click on the profile). The profile's properties panel opens on the right side of the screen.

2. On the SNMP profile properties panel, you can change the profile's name and enter the values of the **SNMP read community** parameter and the **SNMP write community** parameter, according to the values that are set on the printer's Web User Interface.
3. Click **Save** to submit and store the changes.



Adding and Editing SNMP v3 Profiles

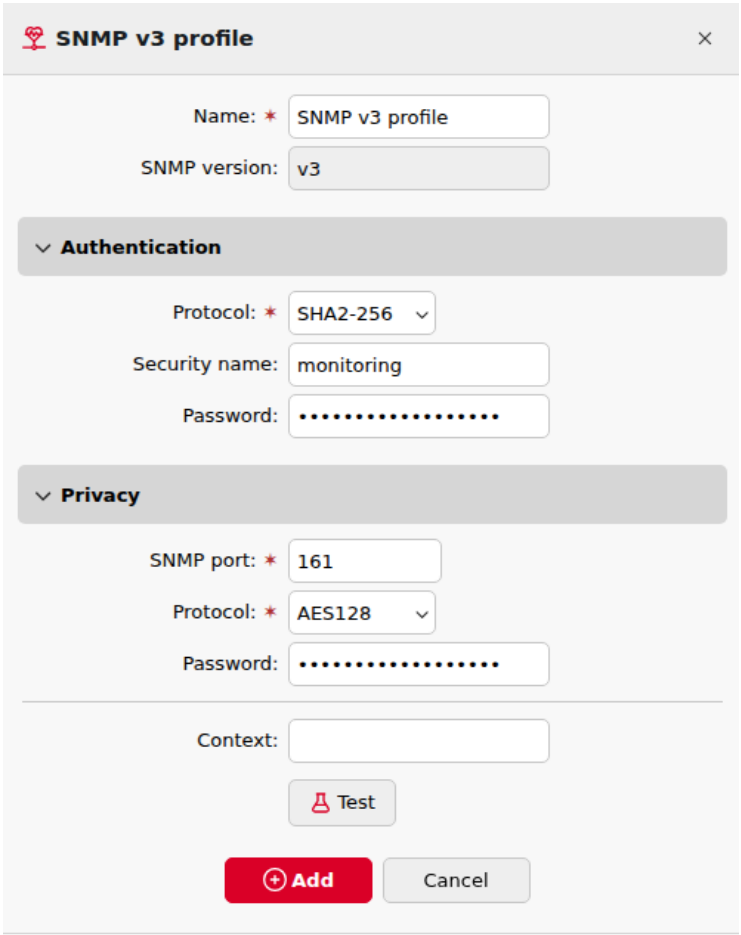
The SNMP v3 protocol contains additional elements of security, such as authentication and encryption. Each of these elements is set on the printing device and needs to be accordingly set in MyQ.

To add a new SNMP v3 profile:

1. On the MyQ Web Interface, open the **SNMP** settings tab. (**MyQ > Settings > SNMP**).
2. On the bar at the top of the **SNMP** tab, click **+Add SNMP profile**, and then click **+SNMP v3** on the shortcut menu. The new SNMP profile's properties panel opens on the right side of screen.
3. On the panel, enter the name of the profile, set the parameters, and then click **Save**. The new profile is displayed on the list on the **SNMP** tab.

To open and edit a SNMP v3 profile:

1. To open the SNMP profile properties panel, select the profile on the **SNMP** settings tab, and then click **Edit** (or right-click on the profile, and then click **Edit** on the shortcut menu). The properties panel opens on the right side of the screen.
2. On the SNMP profile properties panel, you can change the profile's name, set its authentication parameters, its privacy parameters and eventually enter a context name. The values of all of the parameters have to match the values that are set on the printer's Web User Interface.
3. Click **Save** to submit and store the changes.



Attaching SNMP Profiles to Printers

1. On the MyQ Web Administrator Interface, open the **Printers** main tab (**MyQ > Printers**).
2. On the tab, select the printing device, click **Actions**, and then click **Properties.** The printing device's properties panel opens on the right side of the screen.

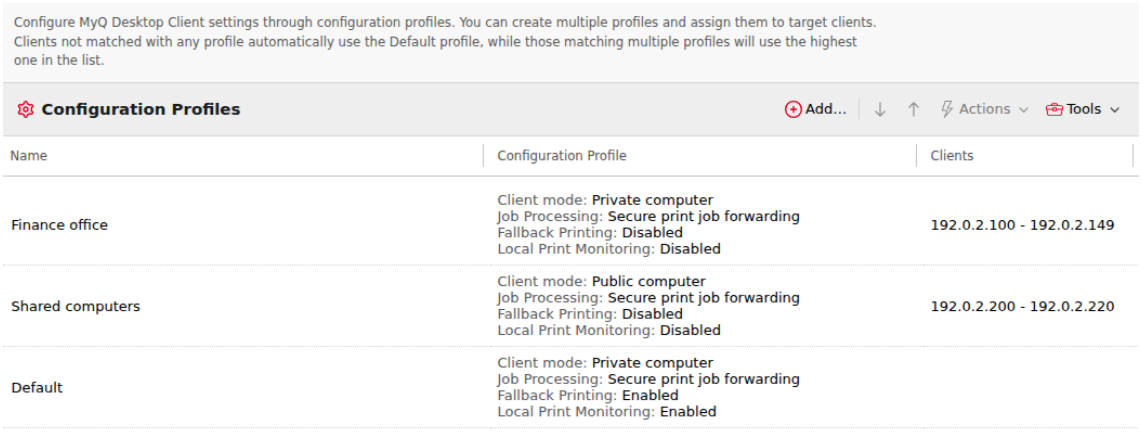
3. On the panel, go to the **Configuration** section.
4. Select a **Configuration Profile** that has the SNMP profile attached to it. In case of doubt, go to **MyQ > Settings > Configuration Profiles** and check the profiles.

8.27 MyQ Desktop Client Settings

MyQ administrators can save multiple different configurations for MyQ Desktop Client (MDC) and deploy different configurations based on location. For example, you can define different fallback printers in each office, or enable client spooling only for selected workstations only.

To manage MDC configuration profiles, go to **MyQ > Settings > MyQ Desktop Client**. Here you can create multiple configuration profiles, assign them to specific locations, and select print queues that will be installed on the computer.

Clients that are not matched in any of the profiles will use settings from the Default profile. If a client matches multiple profiles, the highest matched profile in this list will be used.

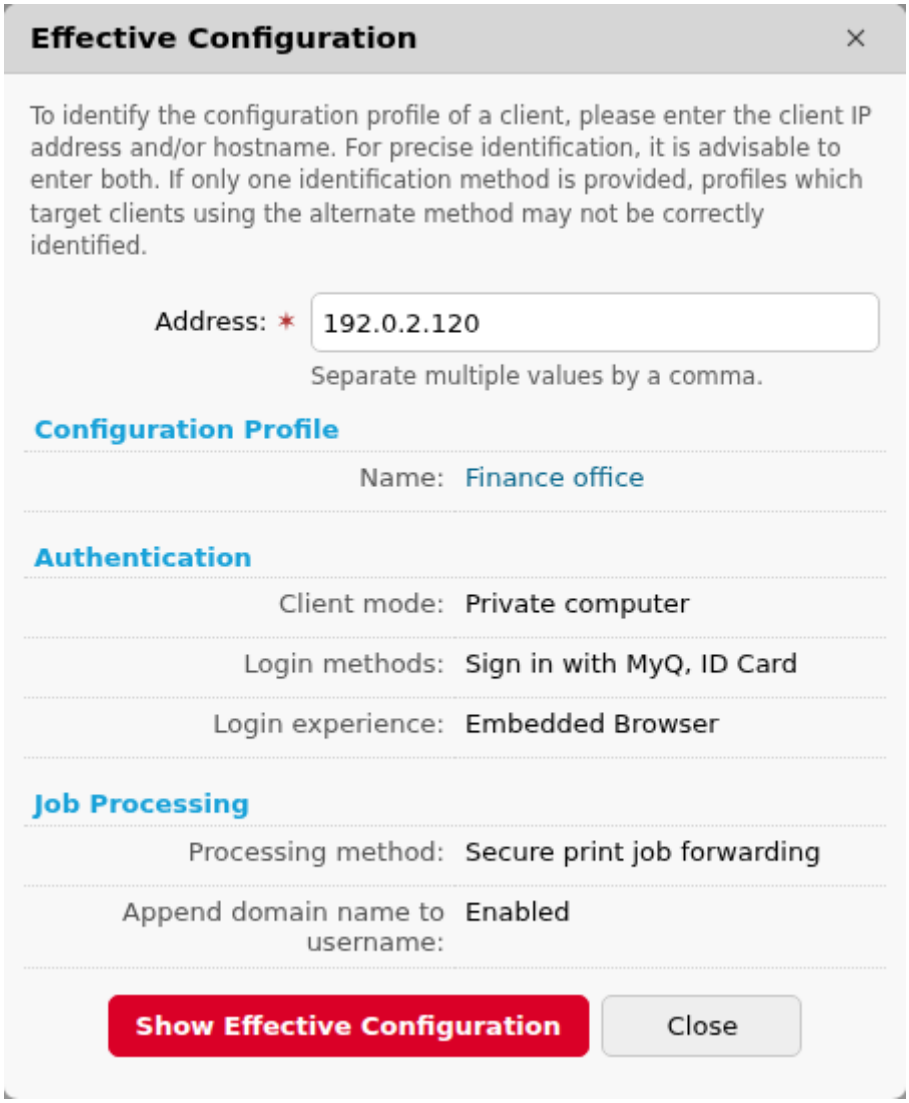


Settings available in the configuration profiles are similar to the settings described in the Desktop Client guide. See (10.2) MyQ Desktop Client.

8.27.1 Show Effective Configuration of a Client

The **Show effective configuration** tool is available in **MyQ > Settings > MyQ Desktop Client**, and allows you to see which configuration profile is being used by a particular client, based on its IP range or hostname.

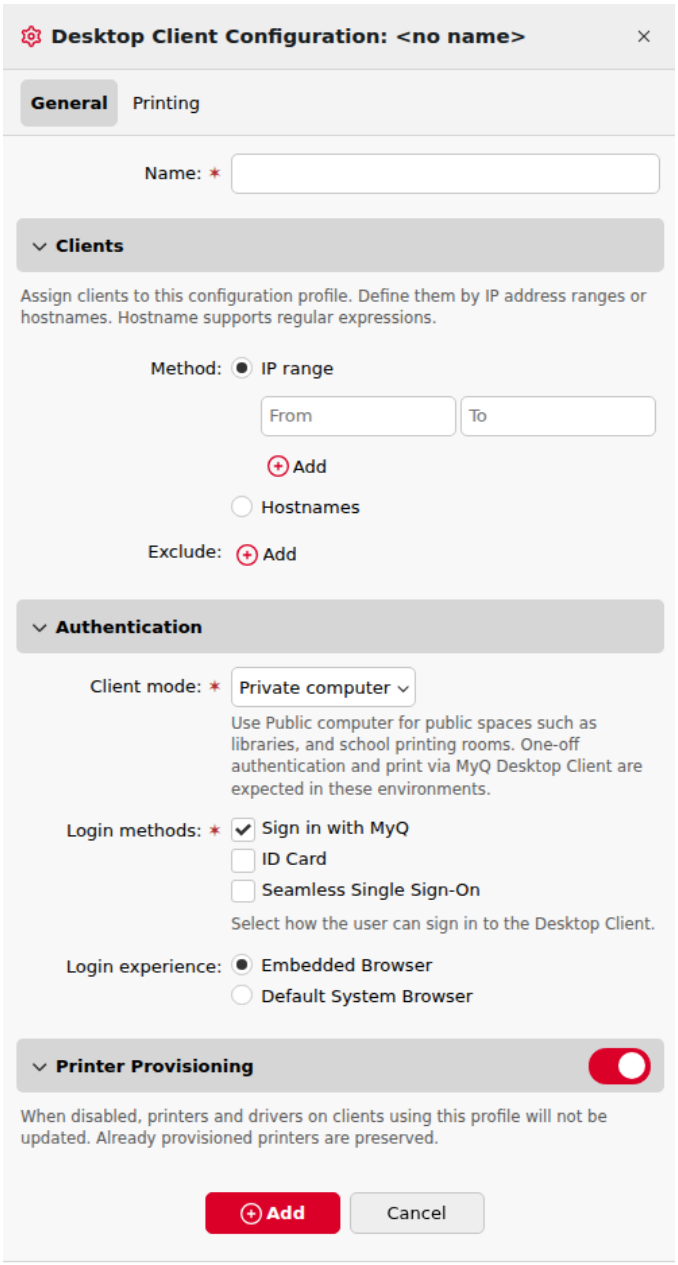
Select **Tools**, **Show effective configuration**, and specify the client IP or hostname of the client you would like to see the configuration profile of. The **Configuration profile**, **Authentication** settings, and **Job processing** settings of the relevant configuration profile are listed.



8.27.2 Desktop Client Configuration Profiles

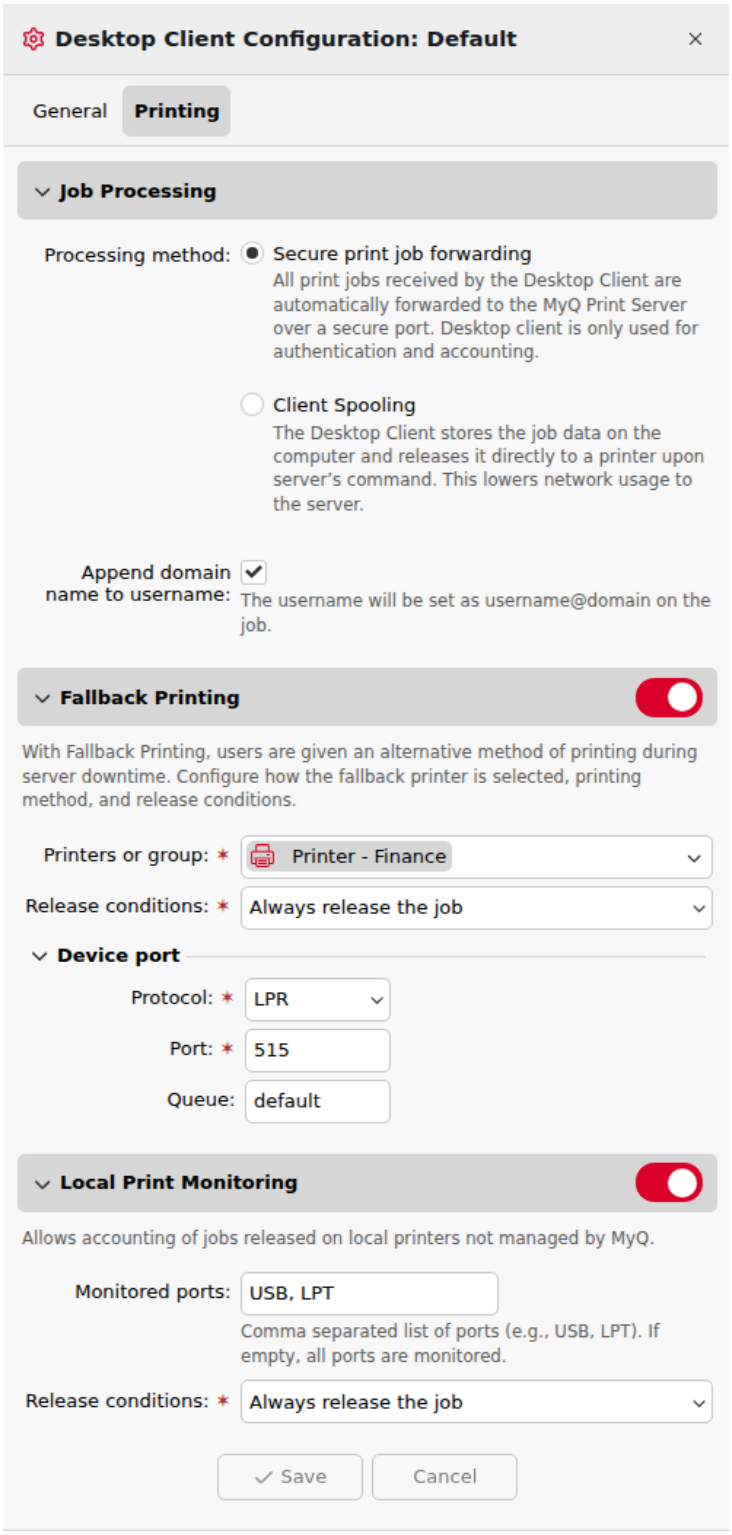
Create a Configuration Profile

1. Go to **MyQ > Settings > MyQ Desktop Client**, click **Add** in the Configuration Profiles section.
2. On the **General** tab enter a **Name** for your configuration profile.



3. In the **Clients** section specify which clients this configuration profile should apply to, either using an **IP range** or **Hostnames regex**. You can also add exclusions.
4. In the **Authentication** section select a **Client mode**.
    - **Private mode:** Desktop Client offers a more lenient authentication and session management approach, acknowledging the trust level of a personal or assigned device.
    - **Public mode:** designed with communal device security in mind, ensuring that print jobs and user sessions are managed to prevent unauthorized access.
      See (10.2) Public vs Private Mode.

5. In the **Authentication** section choose an appropriate **Login method:**
    - **Sign in with MyQ**
    - **ID Card** (requires a card reader on the user's device)
    - **Seamless Single Sign-On** (Seamless SSO uses Microsoft Entra ID Single Sign-on. This feature is supported on Windows only.)
6. In the **Authentication** section, chose which browser to use for client authentication:
    - **Embedded Browser**
      Use the built-in browser of the Desktop Client application.
    - **Default System Browser**
      Use the default browser of the client OS.
      Important: When using Default System Browser on clients in public mode, the administrator must ensure that browser data and cookies are cleared after each user session to prevent unauthorized access.
7. In **Printer Provisioning** choose to enable or disable Printer Provisioning. When disabled, printers and drivers on clients using this profile will not be updated, which can be helpful to prevent unwanted changes, while preserving past ones.



8. On the **Printing** tab in the **Job Processing** section select a **Processing method** from:

   a. **Secure print job forwarding**: All print jobs received by the Desktop Client are automatically forwarded to the MyQ Print Server over a secure port. Desktop client is only used for authentication and accounting.
   b. **Client spooling**: The Desktop Client stores the job data on the computer and releases it directly to a printer upon server's command. This lowers network usage to the server.
9. Choose if you want to **Append domain name to username**, if enabled the username will be set as username@domain on the job.
10. Enable or disable Fallback Printing, which allows users to be given an alternative method of printing during server downtime. Configure how the fallback printer is selected, the printing method, and release conditions. See (10.2) Fallback Printing.
11. Enable or disable **Local Print Monitoring**, which allows the accounting of jobs released on local printers not managed by MyQ.
    a. **Local Print Monitoring**: If enabled, jobs on printers not managed by MyQ server will be accounted.
    b. **Monitored ports**: Enter the names of the ports that you want to monitor, separated by comma (,). You can use '*****' to monitor all name-related ports (i.e.: USB* for ports USB1, USB2, etc.). Leave the field empty to monitor all ports.
    c. **Release conditions**: Select one of the available options - **Always release the job**, **Only if user has enough credit/quota**, **Only if print server is online**.
12. Click **Save**. Your configuration profile is created and automatically applied.

Connect to a Central Server

It is also possible to connect Desktop Client to a site via a Central Server.

1. Edit the installer name or config file as described above to correspond to the Server Address and Server Port of the Central Server.
2. Navigate to **Sites**, **Edit** the relevant site, and enter the **IP range** of the devices to be connected to this location with Desktop Client (it is also possible to create exclusions).
3. Desktop Client will now connect to the specified Site server.

8.28 Print Driver Settings

> ⚠ The information and instructions on this page relate to Legacy Printer Provisioning. If you have migrated to Printer Provisioning Profiles, or your account was created after the release of MyQ Print Server 10.2 patch 21. See (10.2) Printer Profile Provisioning.

Administrators can utilize the Printer provisioning capabilities of the MyQ Desktop Client 10.2 for automatic print driver deployment. This simplifies the process of creating printers on client computers as the Desktop Client can create printers on behalf of the administrator.

8.28.1 Printer Provisioning

Printer provisioning is a feature of the MyQ Desktop Client 10.2 that allows the administrator to deploy MyQ queues efficiently. The goal is to make it as automatic as possible, and with as little manual configuration on each client computer.

- Configure printers on a template computer by installing and configuring print drivers you want to use in your organization.
- As a signed-in administrator in the MyQ Desktop Client, capture these drivers on required operating systems, create as many print driver sets as you need, and upload them to the MyQ driver store on the Server.
- Enable Printer provisioning on the MyQ Web Interface by selecting the combination of the print driver set and queue.
- Desktop Clients connected to MyQ in your organization download its configuration, including the printers to be installed.
- MDC handles the printer deployment, and creates printers predefined by the administrator, pointing at queues the user has access to in MyQ.

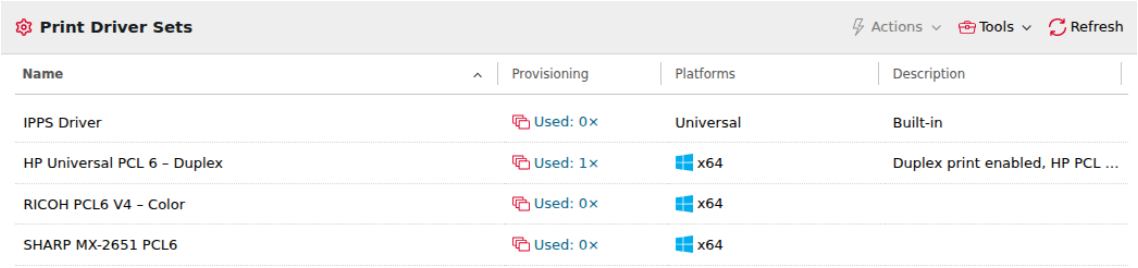
8.28.2 Capture and Upload Print Drivers

Learn how to capture and upload print drivers in the MyQ Desktop Client guide. See (10.2) Legacy Print Driver Capture.

> ℹ If you are using Print Server 10.2+ there is a built-in IPPS driver available. This driver can be chosen in on the Print Drivers page under Print Driver Sets, and in the Queue's MyQ Desktop Client tab. This enables provisioning of the queue by the Desktop Client as an IPPS printer.

8.28.3 Manage Print Drivers

In **Settings** – **Print Drivers**, you can manage print driver sets you captured with the Desktop Client.



After the first captured print driver is uploaded to the MyQ driver store, a new set is created. The profile's name can be adjusted in MDC during the process of driver capture (by default it is the name of the template printer from which the driver was captured).

A print driver set includes:

- the print driver itself
- printing defaults, such as paper format, color, and orientation
- capabilities and tray settings

In the print driver set detail, you can see:

General tab

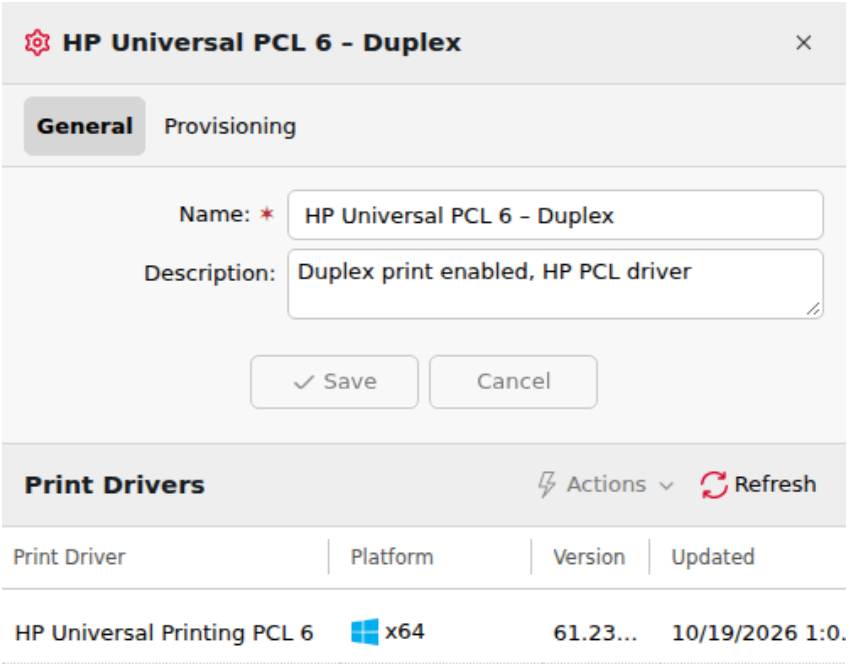
- Description: A note for administration purposes (provided when the driver is captured).
- Print Drivers: A list of print drivers that were captured in this set.

Queues tab

- The queues that have this print driver set in use.

8.28.4 Print Drivers

In the Print Drivers section, you will find the list of drivers in this set, the operating system that the driver was captured on, the version of the driver, and the date and time of the latest change (when the driver was either uploaded to the server by MDC or re-captured, and thus updated).



One print driver set can contain exactly one print driver for each supported OS/platform.

This can be achieved by capturing a driver on different operating systems and specifying the name of a print driver set that already exists in MyQ. These drivers are then bundled under this print driver set and will be deployed on the relevant platform automatically.

Example: **Kyocera driver with stapling enabled for Windows 64bit and macOS**

1. On Windows 64bit, the administrator installs a Kyocera driver, enables stapling in the driver printing defaults settings, and assigns this driver to the printer called **Kyocera Stapling Left**.
2. Using the Desktop Client, the driver is captured and uploaded to the MyQ driver store; the new print driver set **Kyocera Stapling Left** is created.
3. Now, on macOS, the administrator also installs the preferred Kyocera driver, enables stapling in the driver's settings, and during the driver capture, provides the same profile name to upload the driver under the same profile (**Kyocera Stapling Left**).
4. Administrator goes to the Print Drivers settings in MyQ, and this print driver set, select the queue **Staple_Left** and set that the final name of the installed printer to "Left Stapling" in MyQ.
5. Users running MDC with rights to print to queue **Staple_Left** will get the printer "Left Stapling" installed in the background; the correct driver for each platform will be installed for them.

8.28.5 Queues

Here you can adjust the queues that use a print driver set. All these queues are deployed to your users, and they use the print driver and configuration from this set.

8.28.6 Queue Settings for Printer Provisioning

> ⚠ Printer provisioning using queues is deprecated. Modern deployments must use Printer Provisioning Profiles.

In **Queues** – **queue detail** – **MyQ Desktop Client**, you can specify the print drivers to be installed on client computers with this queue as a destination. If you are deploying one queue multiple times, e.g. with different printing defaults, you will see all the print driver sets this queue is deployed with.

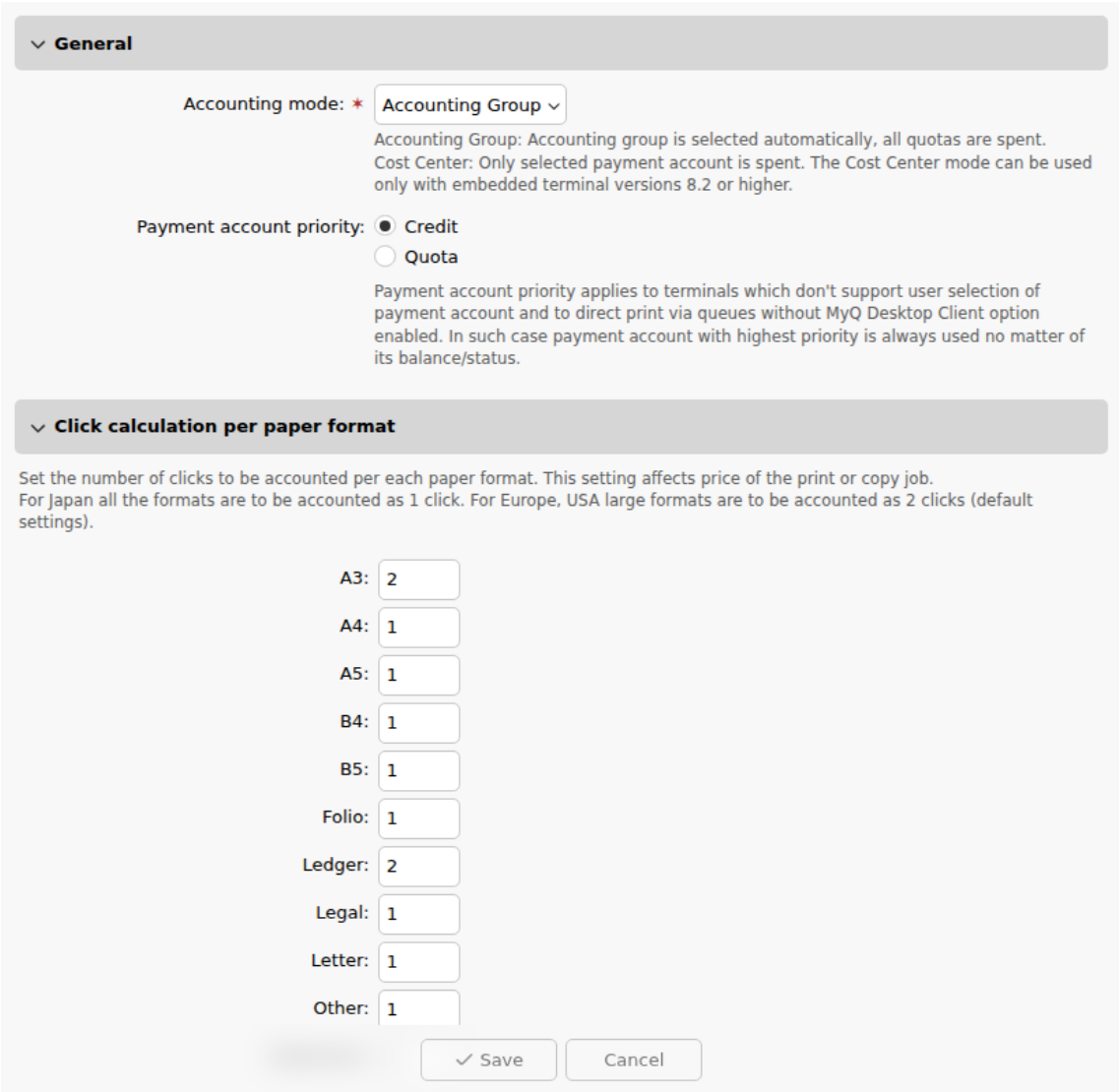
8.29 Accounting Settings

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.

You can also set the **Payment account priority**, which applies to terminals that don't support user selection of payment accounts, and to direct queues without the MyQ Desktop Client option. The payment account with the highest priority is always used in such cases:

- Credit
- Quota



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
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.

8.29.1 Click Calculation per Paper Format

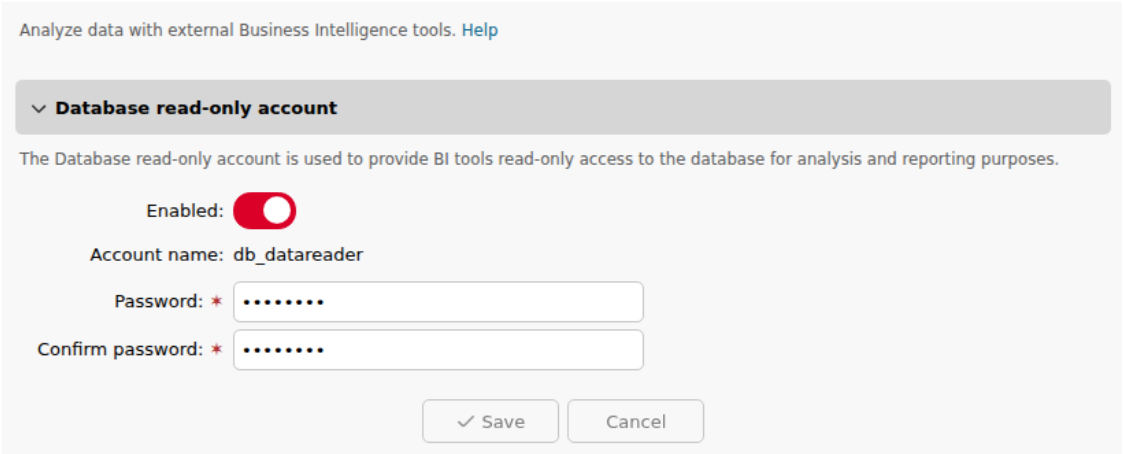
This setting affects print and copy click charges, and it may be used for accounting by embedded terminals when device settings are unknown.

- Ensure that it matches your fleet to avoid accounting errors.
- By default, large formats count as 2 clicks (common e.g., in Europe, USA). Adjust if 1-click counting is needed (e.g., Japan).
- Supported formats include A3, A4, A5, B4, B5, Folio, Ledger, Legal, Letter, Statement, and Other.

8.30 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:

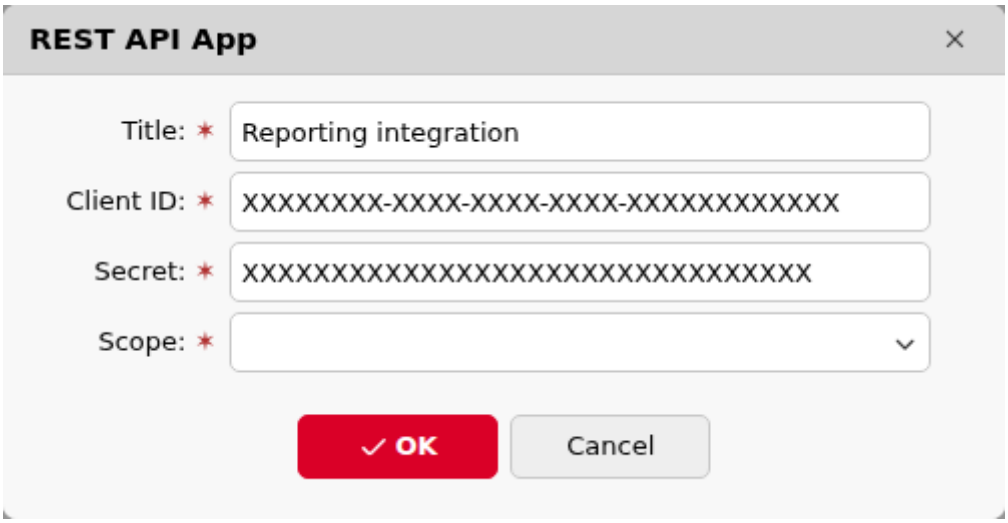
- **Account name**: *db_datareader*. This is the newly created read-only database user. The account name cannot be changed.
- **Password**: password for the *db_datareader* account, set by the administrator. A new password must be set every time when switching from the **Disabled** to **Enabled** state.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

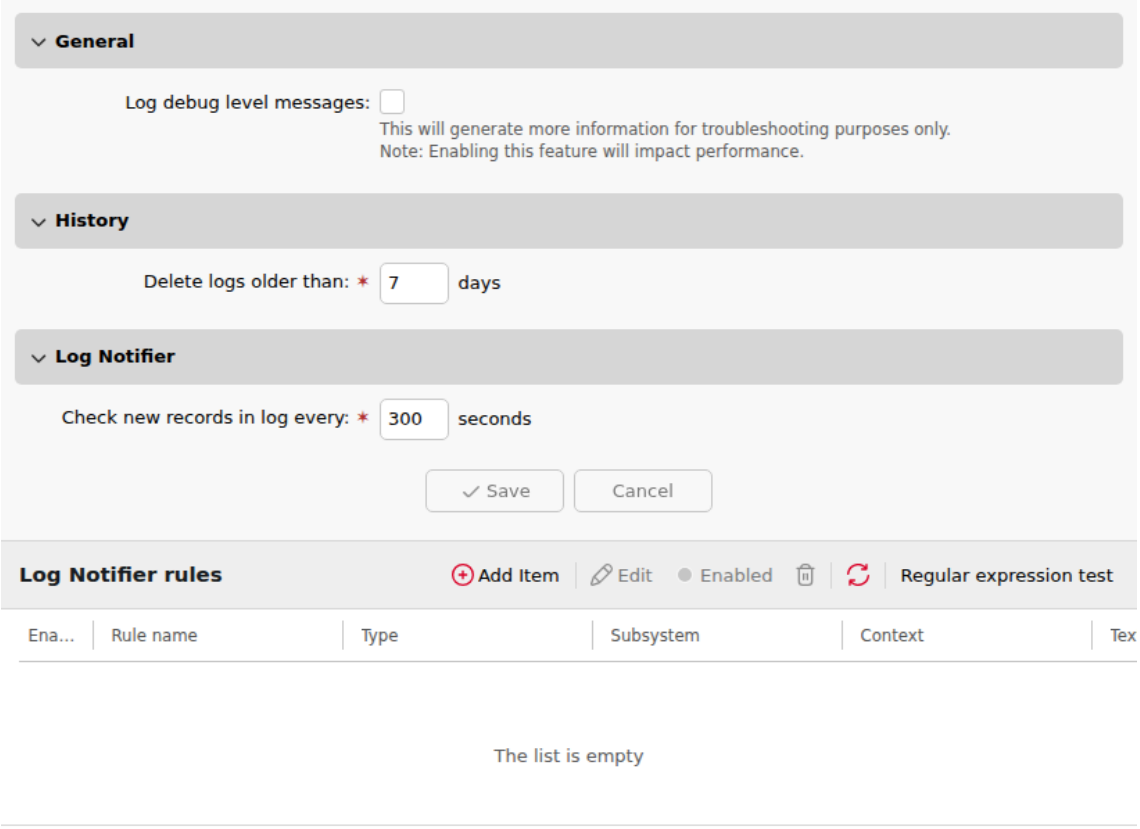
8.31 REST API Apps

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.



8.32 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.

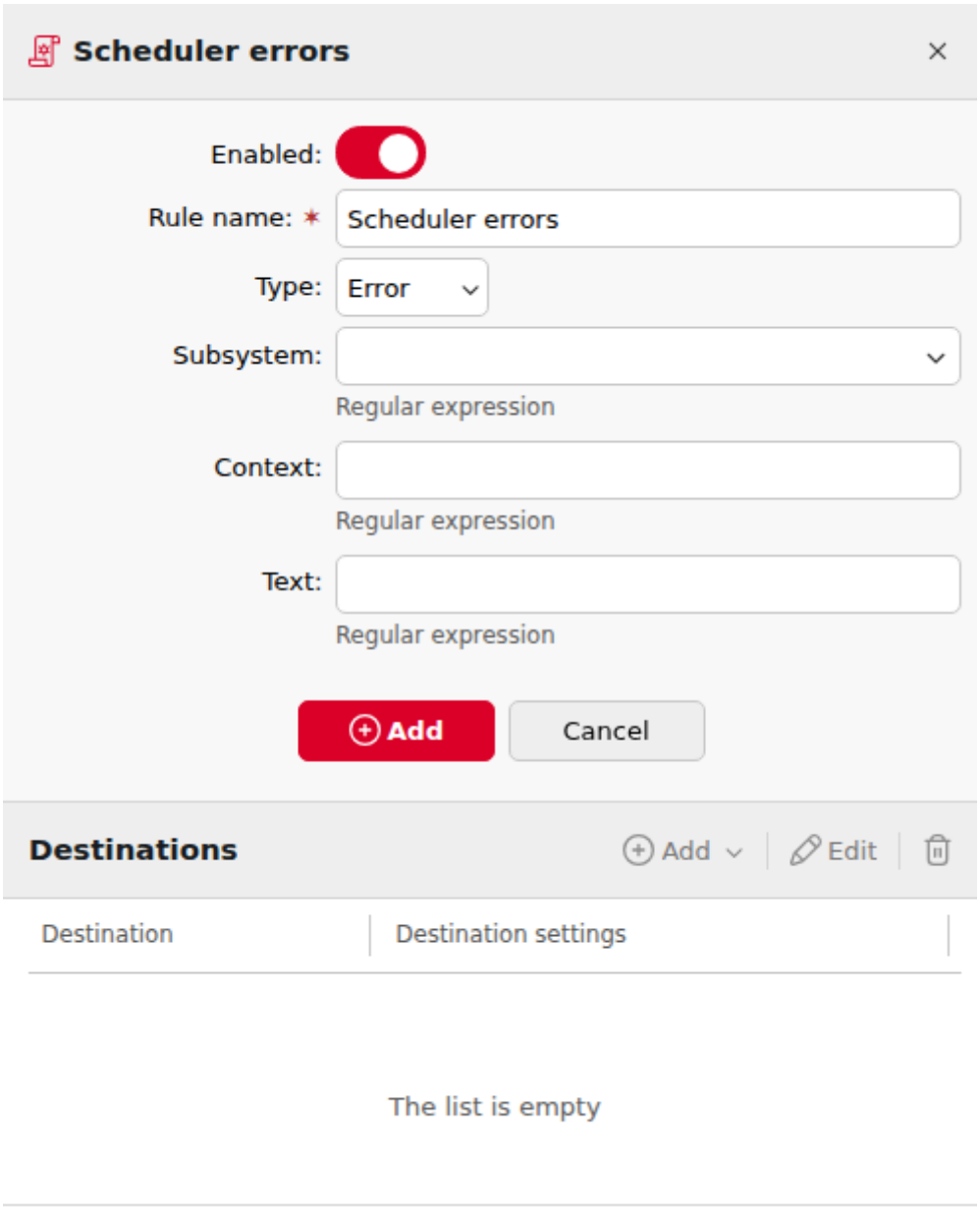
History – Here you can set when the logs should be deleted (in days).

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).

8.32.1 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.

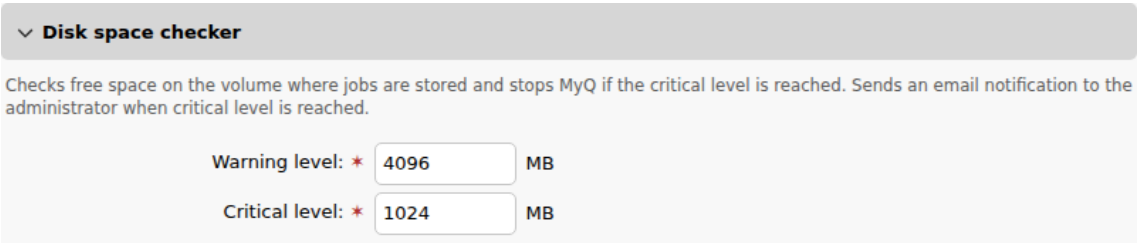
To enable/disable Log Notifier rules:

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

8.33 System Management Settings

On the **System Management** settings tab, you can change the settings of the MyQ history, reset MyQ components to apply settings previously made on other tabs, and also delete data from the MyQ database.

8.33.1 Disk Space Checker



The disk space checker protects the system against failure caused by insufficient disk space. You can set two levels of alert:

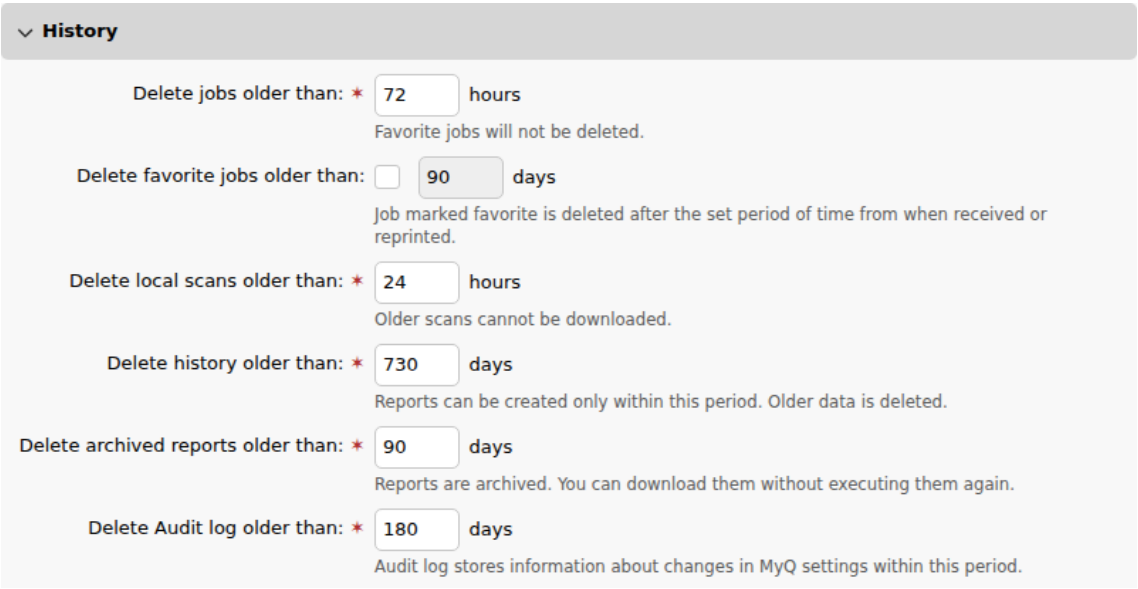
- **Warning level**: If the disk space reaches this level (4096MB by default), the administrator gets an email notification.
- **Critical level**: If the disk space reaches this level (1024MB by default), the administrator gets an email notification and MyQ services are automatically stopped to prevent corruption of the MyQ databases.

8.33.2 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 jobs older than**: Jobs remain on the MyQ server for the period set here. Older jobs (except for Favorite jobs) are deleted and cannot be printed. Favorite jobs stay on the server until they are manually deleted by the user or by the MyQ administrator. The default is 72 hours.
- **Delete favorite jobs older than**: If the checkbox is enabled, jobs marked as favorite are deleted after the set period of time from when received or reprinted. The default is 90 days.
- **Delete local scans older than**: Local scans (the scans stored on the MyQ server) remain on the MyQ server for the period set here. Older local scans are deleted and cannot be downloaded. The default is 24 hours.
- **Delete history older than**: This setting determines the time period for storing data of user sessions, alerts on printing devices, the device counter history, and closed alerts. Older data are deleted from the MyQ database and cannot be used in MyQ reports. The default is 730 days.
- **Delete archived reports older than**: Reports are archived for the period set here. Older reports are deleted. The default is 90 days.
- **Delete Audit log older than**: The audit log stores information about changes in MyQ settings for the period (in days) set here. Anything older is deleted. The default is 180 days.

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



8.33.3 Advanced

In the **Advanced** section, you can reset MyQ components to apply settings previously made on other tabs, delete all users without a session, and permanently remove inactive users, printers, groups and user data from the MyQ database.

Applying changes

Some changes of the MyQ server require a reset of some of the server's components. When you save these changes, the system proposes to automatically perform the reset. If you decide to skip this action, you need to reset the components later.

Use the **Apply settings** option to reset the components at any time. Click Apply Settings and then select the component that you want to reset:

- Restart HTTP Server (Apache)
- Reset all terminals
- Reconfigure MS Cluster monitoring script
- Reconfigure PM Server

The settings are applied immediately.

8.33.4 Data Deletion

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.

- **Delete users**: Deletes all users without user sessions. Users with sessions will not be deleted.
- **Delete projects**: Removes projects that were never used.
- **Deleted inactive users and groups**: Permanently removes all inactive users and all groups with no active users from the MyQ database.
- **Deleted printers**: Removes all printers which are deleted and have never been activated from the MyQ database.
- **User data**: **User Sessions, Jobs, Groups, Users, Vouchers**: Removes all user related data from the MyQ database.

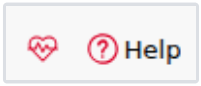
8.33.5 System Health Check

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.

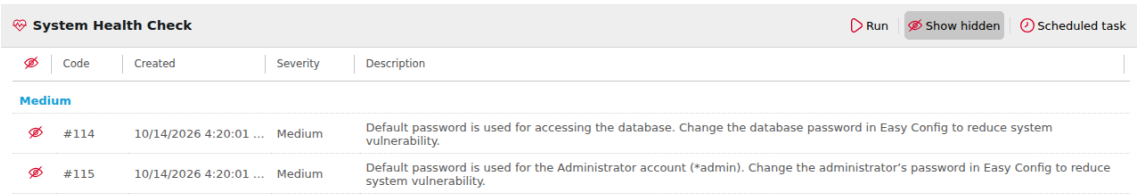
To access the system health check overview, log in as admin to MyQ and go to **MyQ > System Health Check** or click on the system health check button on the top-right side of the window.



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.

Error Code	Severity	Description	Troubleshooting Steps
101	High	Main database health issues	Run database consistency checks. Verify connectivity and restart services after ensuring sufficient disk space. Complete a database back-up and restore.
102	High	Log database health issues	Check log database and clear outdated logs using scheduled tasks. Complete a database back-up and restore.

Error Code	Severity	Description	Troubleshooting Steps
103	Medium	PIN length needs adjustment	Adjust PIN policies to enforce a higher minimum character count.
104	High	Disk space warning	Perform disk cleanup tasks and consider expanding storage or migrating data folders.
105	Critical	Disk space critical	Immediately free up disk space or expand storage. Verify shared drive accessibility in clustered environments.
106	High	Time zone misconfiguration	Synchronize time zones across servers and update configuration files to match the OS settings.
107	Medium	Queue errors	Review queue configurations and test printer connectivity using standard network diagnostic tools.
108	Medium	Obsolete terminal version	Deploy updated terminal packages and adjust device-specific settings to modern protocols.
109	High	HTTP server unresponsive	Restart HTTP services and verify firewall exceptions for critical ports. Confirm network settings, particularly IP/hostname. Check that system performance is higher than the minimum system requirements.
110	High	HTTP timeout	Inspect web server logs for conflicts and disable non-essential modules.

Error Code	Severity	Description	Troubleshooting Steps
111	High	Terminal package unresponsive	Restart terminal services or reinstall terminal software if issues persist. Check that system performance is higher than the minimum system requirements.
112	High	Services not running	Restart affected services and confirm service account permissions align with system requirements.
113	Medium	Service account mismatch	Reconfigure services to use appropriate system or domain accounts with necessary privileges.
114	Medium	Default database password	Change default database credentials and update configuration files accordingly.
115	Medium	Default admin password	Reset administrator passwords and enable multi-factor authentication for enhanced security.
116	High	Sites have not been replicated for more than 30 days	Verify replication settings in MyQ Web UI. Check network connectivity between Central and unreported Sites. Restart replication services.
117	Medium	Email duplicates found	Confirm `AllowEmailAddressDuplicity` in `config.ini`. Audit user email fields for duplicates.
118	High	Database page size 8 KB (may impact performance)	Create full database backup. Restore database with 16 KB page size. Monitor performance post-restore.

Error Code	Severity	Description	Troubleshooting Steps
119	Medium	Connection secret keys expired/near expiry	Identify expiring keys. Generate new keys and update API configurations. Restart affected services.
120	Medium/High	CA certificate expiring (Medium) or expired (High)	Check and replace expiring or expired certificates.
121	Medium/High	Server certificate expiring (Medium) or expired (High)	Check and replace expiring or expired certificates.

8.33.6 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	

8.33.7 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.

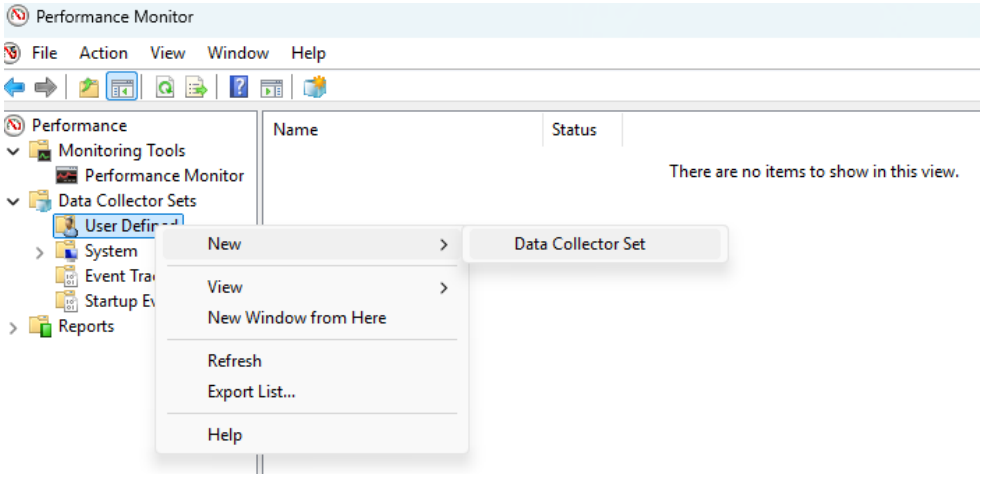
Performance Monitor is a Microsoft Management Console (MMC) snap-in that you can use to obtain system performance information. You can use this tool to:

- 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**.

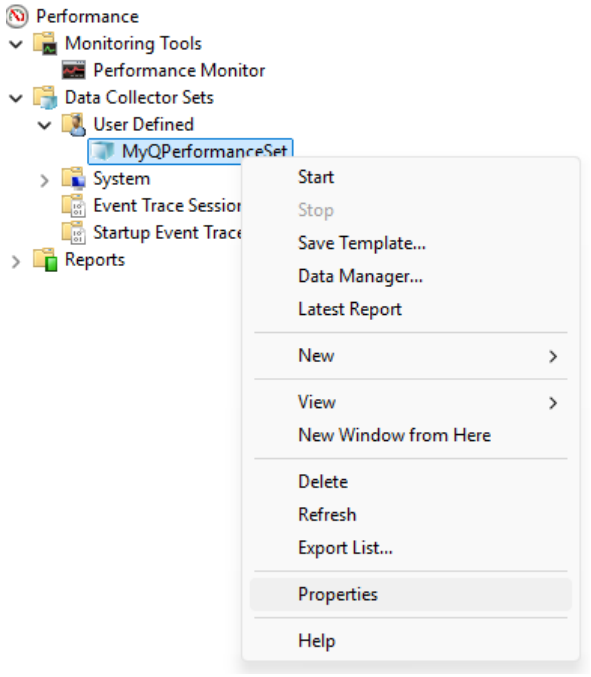


    c. In the first **Create new Data Collector Set** wizard dialog box:
        i. In the **Name** field type any descriptive name.
        ii. Select **Create from a template (Recommended)**.
        iii. Click **Next**.
    d. In the second **Create new Data Collector Set** wizard dialog box:

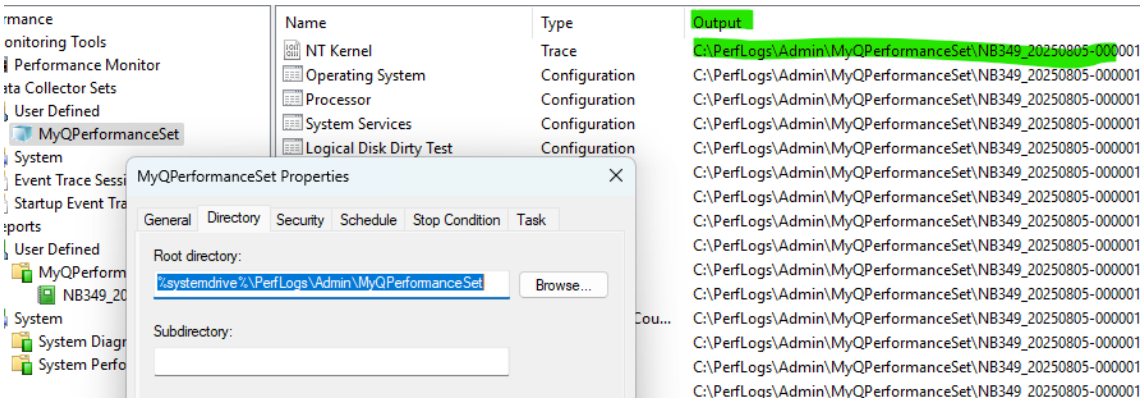
i. Select **System Diagnostics**.

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[24]
- Monitor Windows Server performance[25]

8.33.8 Advanced Security

MyQ security is structured in distinct layers, with enforcement handled by separate system components. This separation protects business-critical data and services, and administrators must understand it to configure advanced settings safely and responsibly.

This section covers the advanced security configuration options. For general advanced configuration options, see Advanced Configuration (see page 271).

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

⚠ Editing configuration files directly can affect system stability and security. These settings are intended for experienced administrators. Incorrect changes may result in service disruption or data loss. If you are unsure, contact MyQ Support before proceeding.

Path Conventions

- `{install}` – Application installation directory
  Defaults are `C:\Program Files\MyQ\` and `C:\Program Files\MyQ Central Server\`
- `{data}` – Application data directory.
  Defaults are `C:\ProgramData\MyQ\` and `C:\ProgramData\MyQ Central Server\`

Both locations may be customized during installation.

Security Architecture Overview

Security Layer	Print Server (& Central Server Patch 25+)	Central Server (before Patch 25)
Web TLS (HTTPS encryption)	**Component:** HTTP Router (Traefik) **Config:** `{data}\config.ini` `{data}\traefik.custom.rules.yaml`	**Component:** HTTP Server (Apache) **Config:** `{install}\Apache\conf\httpd.conf` (`SSLProtocol`, `SSLCipherSuite`)
HTTP Security Headers	**Component:** Apache (behind Traefik) **Config:** `{install}\Apache\conf\httpd.conf` (also edit `httpd.template.conf`)	**Component:** Apache **Config:** `{install}\Apache\conf\httpd.conf` (also edit `httpd.template.conf`)

Security Layer	Print Server (& Central Server Patch 25+)	Central Server (before Patch 25)
Non-Web Secure Communication (SMTP, IPP, LPR, WebSockets)	**Component:** MyQ internal components **Config:** `{data}\config.ini` (`[Security] sslProtocol=`)	**Component:** MyQ internal components **Config:** `{data}\config.ini` (`[Security] sslProtocol=`)

⚠ On both Print Server and Central Server (10.2 Patch 25 and later), TLS termination is handled by Traefik. Apache handles back-end requests only and is not exposed on public ports.
On Central Server versions **earlier than Patch 25**, TLS termination was handled by Apache directly.

Web TLS Configuration (HTTP Router – Traefik)

The HTTP Router (Traefik) is responsible for terminating HTTPS connections and managing TLS protocol versions and cipher suites.

Configure the Minimum TLS Version

To define the minimum allowed TLS version, set the SSL protocol in `config.ini`.

Open `config.ini` in a text editor and add or modify:

```
[Security]
sslProtocol=TLS1.3
```

Supported values:

- TLS1
- TLS1.1
- TLS1.2 (default from Print Server 10.2)
- TLS1.3

This setting applies to:

- HTTP Router (web HTTPS)
- SMTP

- IPP
- LPR
- Messages (WebSockets)

Restart all services after modification.

Configure Cipher Suites

Use Secure Presets (Recommended)

Open `config.ini` in a text editor and add or modify:

```
[Security]
sslCipherSuites=strict
```

Available modes:

- **compatible** (default)
  Allows selected weaker ciphers for legacy device compatibility.
- **strict**
  Disables weak ciphers.

The following ciphers allowed in *compatible* mode only:

- `TLS_RSA_WITH_AES_128_CBC_SHA`
- `TLS_RSA_WITH_AES_256_CBC_SHA`
- `TLS_RSA_WITH_AES_128_GCM_SHA256`
- `TLS_RSA_WITH_AES_256_GCM_SHA384`
- `TLS_RSA_WITH_3DES_EDE_CBC_SHA`
- `TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA`

Strict mode is recommended, but compatible mode remains the default due to legacy device requirements.

Allow Selected Cipher Suites

To to allow selected cipher suites, edit `traefik.custom.rules.yaml`. Then save the file and restart all services for the change to take effect.

Example:

```
tls:
  options:
    default:
      cipherSuites:
        - TLS_RSA_WITH_AES_256_GCM_SHA384
```

```
    - TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

Important!

Do NOT edit these files:

- `{install}\Server\traefik.rules.yaml`
- `{install}\Server\traefik.yaml`

These are default installation files and will be overwritten during upgrades.

If `sslProtocol=TLS1.3` is enforced, cipher selection is not configurable, and Traefik secure defaults are used.

Ensure connected devices support the selected cipher suites.

HTTP Security Headers (Apache)

Apache runs behind the HTTP Router and does not terminate TLS. Apache listens only on localhost and does not manage TLS protocol versions or cipher suites.

Apache is responsible for HTTP response security headers.

These include:

- Content-Security-Policy (CSP)
- Strict-Transport-Security (HSTS)
- X-Frame-Options
- X-Content-Type-Options
- Referrer-Policy
- Permissions-Policy
- Other header-level protections

Configuration Location

To modify the HTTP security header configuration, edit **both** of these files. Then restart MyQ services. If `httpd.template.conf` file is not modified, your changes will be overwritten during service updates.

- `{install}\Apache\conf\httpd.conf`
- `{install}\Apache\conf\httpd.template.conf`

Non-Web Secure Communication

Some MyQ components use secure communication independent of web HTTPS.

These include:

- SMTP
- IPP
- LPR
- Internal C++ components

TLS behavior for these components is controlled by the `sslProtocol` parameter in `config.ini`. This setting does not modify HTTP headers and does not directly modify Apache TLS behavior.

Force Kerberos-Only Authentication

For environments requiring strict authentication, add the following to `config.ini`:

```
[Security]
KerberosOnly=true
```

This disables NTLM fallback and enforces Kerberos-only authentication.

Ensure:

- Proper SPN registration.
- Correct Kerberos infrastructure configuration.

Misconfiguration may prevent authentication.

8.33.9 Advanced Configuration

Config.ini is a text file located by default in `C:\ProgramData\MyQ`. This file controls key aspects of Print Server behavior, including communication, job processing, logging, and user access.

You can edit `config.ini` using Notepad or any other text editor.

> ⚠ **Warning:** Incorrect values in this file may cause system outages or data loss.

Before You Edit

- Always back up the existing `config.ini` file.
- Only modify parameters supported in your installed version.
- Restart the Print Server after saving changes.
- Disable any temporary debugging parameters after use.

Only advanced users or system administrators should edit this file. When in doubt, contact support@myq-solution.com[26].

Example

```
;Print Server configuration
;You must restart the service for the changes to take effect

[General]
;Enabling duplicate email addresses
AllowEmailAddressDuplicity =true
;Configuring backups without data compression
backupCompressionLevel=0

[ExtraFeatures]
;Enabling user sync from multiple domains and Lotus Domino LDAP support
multipleDomains=1
lotusDomino=1

[UserSession]
;If the printer is unreachable longer than X seconds, interrupt the
session.
;Jobs that have not been sent to the printer yet, will not be printed.
;User can print them next time.
printerUnreachableTimeout=90
```

`[General]`

This section defines system-wide behaviors for email address duplicity, backup compression, domain mapping, printer conflict resolution, and user interface accessibility features, among others.

26. mailto:support@myq-solution.com

Parameter	Version	Default	Description
`AllowEmailAddressDuplicity`	10.2+	`false`	Enforcement of unique email addresses. When `true`, multiple users can share the same email address. **Values:** `true`, `false` **Note:** If a database with email duplicity is being upgraded, both email values persist and an alert is issued to the log.
`backupCompressionLevel`	8.2+	5	0 - 9 (0 = no compression , 9 = max compression)
`clientJobDataTimeout`	8.2+	90000	Timeout, in milliseconds, specifying the timeout period for the heartbeat from SPS to arrive during client spooling.
`cluster`	8.2+	1	Detects if PS is running in Cluster when starting services. This is used, e.g., for generating HW code in the License plugin. Works in installation key mode only
`dbMaxDeltaOAT`	8.2+	150000	DB health checker: maximum difference between next transaction ID and OAT. If it is bigger, a warning is logged, because it could signal the DB sweep is not being performed.

Parameter	Version	Default	Description
`dbMaxDeltaOIT`	8.2+	150000	DB health checker: maximum difference between next transaction ID and OIT. If it is bigger, a warning is logged, because it could signal the DB sweep is not being performed.
`dbMaxDeltaOldestSnapshot`	8.2+	100000	DB health checker: maximum difference between next transaction ID and oldest-snapshot. If it is bigger, a warning is logged, because it could signal the DB sweep is not being performed.
`ddiTimeout`	8.2+	360	DDI timeout, in seconds, when DDI is called from Web UI (Printers, Printer Discovery)
`debug`	8.2+	`false`	Enables debug mode. **Values:** `true`, `false`
`deletePrinterWithSameIP`	8.2+	0	Printer Discovery handling for printers with conflicting IP addresses. **Values:** • 0 (fail with error: "printer with IP address or hostname already exists") • 1 (replace current with new)

Parameter	Version	Default	Description
`domainsMapping`	10.2+	empty	Support for environments where the domain name and NETBIOS name are different. **Example value:** `domainsMapping="domain1=newdomain2.com, domain2a=newdomain2.cz, domain2b=newdomain2.cz"` …where `domain1` is the NETBIOS name, and `newdomain2.com` is the DNS name, with multiple domain mappings.
`enhancedAccessibility`	8.2+	`false`	Enables improves accessibility mode for Web UI. **Values:** `true`, `false` **Note:** For 10.1+, if `true` and no theme is selected, the high contrast theme is the default.

`[ExtraFeatures]`

This section enables optional and legacy-compatible features, including legacy LDAP and FTP compatibility, and granular debug logging for specific devices.

Parameter	Version	Default	Description
`DelegatesLimit`	8.2+	50	Sets the maximum number of returned user's delegates. **Values:** 50-100

Parameter	Version	Default	Description
`deleteCards`	8.2+	0	Enables the **Delete ID Cards** button on the dashboard and the rights to use it. **Values:** 0, 1
`domainLogin`	8.2+	0	Show domain on login page. **Values:** 0, 1
`eGoldFax`	10.2-10.2.26	0	Enables eGoldFax integration. **Values:** 0, 1
`enableReportSqlFilter`	8.2-10.1	0	Enables the SQL filter for reports. **Values:** 0, 1
`logDebugSpecificPrinter`	8.2.16+	0	Enables debug logging for individual printers. Use this option to minimize resource utilization when debugging. **Values:** 0, 1
`lotusDomino`	10.2+	0	Enables support for the legacy Lotus Domino LDAP server. **Values:** 0, 1
`multipleDomains`	8.2+	0	Enables synchronization of users from multiple domains. **Values:** 0, 1 **Note:** Requires user synchronization option **Append the domain name to the username**.

Parameter	Version	Default	Description
`registerUserName`	8.2-10.1	0	Enables web user registration based on username and PIN/password. **Values:** 0, 1
`scanFtpLegacyMode`	8.2+	0	Enables legacy FTP mode as a scan destination. This can be useful if issues arise when using native FTP mode. **Values:** 0, 1
`scheduleExternalCommand`	8.-10.1	0	Allows to add external command to scheduler. **Values:** 0, 1
`tonerSavePricelist`	10.3+	0	Allows assigning a second pricelist in a printer configuration profile, to be used if a job has TonerSaving enabled.

`[HttpChecker]`

These parameters configure internal health checks performed via HTTP, including timeouts and thresholds. They help identify slow or unresponsive components, and optionally restart the proxy when issues occur.

Parameter	Version	Default	Description
`connectTimeout`	8.2+	10	Timeout for the connect phase (in seconds).
`maxRequestTime`	8.2+	2	Minimal time for success query will be logged as slow (in seconds).

Parameter	Version	Default	Description
`restart`	10.1+	0	Restarts the HTTP proxy if the HTTP server responds but the HTTP proxy does not. **Values:** 0, 1
`timeout`	8.2+	20	Timeout for the entire request (in seconds).

`[JobAccounting]`

These parameters control how printed output is counted for accounting purposes. Define whether output should be measured in physical sheets or logical “clicks” (impressions), including special handling for duplex jobs.

Parameter	Version	Default	Description
`duplexInClicks`	8.2+	0	Accounting units for simplex and duplex counters: **Values:** 0 (sheets), 1 (clicks)
`papersInClicks`	8.2+	0	Accounting units for paper counters: **Values:** 0 (sheets), 1 (clicks)

`[JobDeleter]`

This section controls how often the system checks for and removes expired print jobs from the queue.

Parameter	Version	Default	Description
`period`	8.2+	3600	How often expired jobs are deleted/canceled (in seconds).

`[JobParser]`

This section controls how print jobs are analyzed before processing, including some diagnostic options.

Parameter	Version	Default	Description

aliases, e.g.,
`aliasA4`
`aliasB5`
`aliasLedger`
`aliasLegal`
	8.2+	empty	List of custom paper format aliases, as either string **names** or paper sizes in the form "**height** x **width**", where the width and height are integer numbers defining the paper size in tenths of millimeters.
			Example:
			`aliasA4= A4, 2970x2100`

`parameters`	8.2+	empty	MyQJobProcessor.exe supports following command line switches: • d (Write debug messages to standard output) • c (Check analysis result by rendering) • x (Log all exceptions (10.1+)) **Example:** `parameters=d,c,x`
`threadCount`	8.2+	2	Number of jobs that can be parsed in parallel.
`timeout`	8.2+	300000	Timeout (in milliseconds) for the external job parser to finish. If the time elapses, the external parser process terminates the job's metadata will be not set. The default 5min is enough to parse 4GB PCL6 file. Increase the timeout for larger jobs.

`[JobPreview]`

This section configures how print job previews are generated and displayed in the user interface, including timeouts, page limits, and custom preview tools for specific printer languages.

Parameter	Version	Default	Description
`jobPreviewPages`	8.2-10.1	5	Maximum number of pages to preview Set to zero (unlimited) to preview all pages. This value is used for the default preview generator only. For an external preview generator, use appropriate command line switches if your tool supports limiting pages.
`jobPreviewTimeout`	8.2-10.1	60	Defines timeout in seconds for the user defined external preview generator (implemented in PrintServerPlugin; C++). The timeout for the Default preview generator is set in [JobParser] `timeOut`.

Parameter	Version	Default	Description
`pcl5ToPdf_command`	10.1+	empty	Defines a custom tool for generating previews for jobs with PCL5 PDL. This tool is then used for all PDF previews. Custom PDF tools must support at least the %inFile% and %outFile% parameters. Optionally, they can support %pageCount%. **Example value:** `pcl5ToPdf_command="c:\folder name\pdfTool.bat" %inFile% %outFile% %pages%`
`pcl5ToPdf_removePrescribe`	10.1+	`true`	Controls whether to remove prescribe for preview files generated with a custom PCL5 PDF preview generator.
`pcl6ToPdf_command`	10.1+	empty	Defines a custom tool for generating previews for jobs with PCL6 PDL. This tool is then used for all PDF previews. Custom PDF tools must support at least the %inFile% and %outFile% parameters. Optionally, they can support %pageCount%. **Example value:** `pcl6ToPdf_command="c:\folder name\pdfTool.bat" %inFile% %outFile% %pages%`

Parameter	Version	Default	Description
`pcl6ToPdf_removePrescribe`	10.1+	`true`	Controls whether to remove prescribe for preview files generated with a custom PCL6 PDF preview generator.
`psToPdf_command`	10.1+	empty	Defines a custom tool for generating previews for jobs with PS PDL. This tool is then used for all PDF previews. Custom PDF tools must support at least the %inFile% and %outFile% parameters. Optionally, they can support %pageCount%. **Example value:** `psToPdf_command="c:\folder name\pdfTool.bat" %inFile% %outFile% %pages%`
`psToPdf_removePrescribe`	10.1+	`true`	Controls whether to remove prescribe for preview files generated with a custom PS PDF preview generator.
`uiWaitTimeout`	8.2+	5	Defines the timeout in seconds for which web UI waits for the job preview to be generated. When the timeout is reached, this message appears: *The preview is being generated. Try again later.* The maximum value is limited by the maximum execution time of a PHP script.

`[JobProcessor]`

This section configures how the print server prepares jobs for output, including font fallback logic for watermark rendering and compatibility options for controlling printer behavior.

Parameter	Version	Default	Description
`binaryFindReplaceEnabled`	10.2.22+	`false`	Enables the Binary Find & Replace engine. **Values:** `true`, `false` The server reads rules from `BinFindReplace\Config.json` and applies them to jobs in matching queues before parsing. Requires a service restart after changing.

Parameter	Version	Default	Description
`binaryFindReplaceEnabled`	10.2.22+	`false`	Enables the Binary Find & Replace engine. **Values:** `true`, `false` The server reads rules from `BinFindReplace\Config.json` and applies them to jobs in matching queues before parsing. Requires a service restart after changing.

Parameter	Version	Default	Description
`watermarkFontPath`	8.2+	`%WINDOWS_FONT_DIR%/times.ttf, %MYQ_APP_PATH%/Server/Fonts/AozoraMinchoRegular.ttf, %MYQ_APP_PATH%/Server/Fonts/android/DroidSansFallbackFull.ttf, %WINDOWS_FONT_DIR%/malgun.ttf`	Comma-separated list of TTF file paths, in descending priority. Reorder the list of paths to prioritize different scripts (useful for non-European customers). **Note:** The system falls back to the next file if a character is not available. If no font file contains the character, the first font is used and a warning is logged.

`[JobReleaser]`

This section enables job capture for debugging. When activated, the system saves the last job sent to each queue for troubleshooting purposes.

Parameter	Version	Default	Description
`captureJob`	8.2+	`false`	Captures job data being sent to a printer and writes it to a file in the Jobs folder. The last job for each queue is stored. Use only when debugging. **Values:** `true`, `false`

`[JobRoaming]`

This parameter should be used only during the upgrade from 10.2.23 or earlier, to 10.2.24 or later.

Parameter	Version	Default	Description
`legacySecuritySupport`	10.2.24+	`false`	Forces a receiving site server to accept roaming jobs without site-to-site authentication. **Values:** `true`, `false` **Note:** make sure to disable or remove this parameter after all sites have upgraded.

`[Mdc]`

This parameter controls the number of concurrent requests from MyQ Desktop Client.

Parameter	Version	Default	Description
`proxyWorkers`	10.2+	8	Maximum concurrent requests coming from MDC.

`[MicrosoftUniversalPrint]`

This section controls how often the system checks Microsoft Universal Print for new notifications, such as job status updates or errors.

Parameter	Version	Default	Description
`notificationPollingPeriod`	8.2+	30s	How often the server checks for printer notifications, in seconds.

The default notification polling is every 30 seconds, but polling at longer intervals (e.g., 60-120 seconds) can reduce server and network load in large deployments, at a cost of increased latency.

[NSP]

The Non-Session Page (NSP) is a process that periodically checks printers for any changes in the printer counters to detect any attempts to bypass MyQ.

Parameter	Version	Default value	Description
period	8.2+	600000	How often the NSP process runs, in milliseconds. The default value is equivalent to 10 minutes.

[OfflineLogin]

This section configures how many user are cached locally on devices for authentication when the main server is unavailable.

Parameter	Version	Default value	Description
maxUsers	8.2+	100	Maximum number of users sent to the device.

[PersonalQueues]

These parameters control which print queues are visible to users and how personal queue displays are filtered and organized. For more information, see Personal Queues (see page 540).

Parameter	Version	Default value	Description
`queues`	8.2+	empty	Comma separated list of allowed queues for the first queue. Supports the wildcard character %. **Examples:** • “Direct” - shows the Direct queue. • “Direct_%” - shows all queues that start with "Direct_"
`show`	8.2+	1	Set the types of queues that are visible. **Values:** • 1 (All) • 2 (Follow me and delegated) • 3 (Direct)
`showDirectQueueOnFirstRow`	8.2+	empty	Display personal queues with **direct type** first, with the queues filter is applied to it. From the second row on, only the "show" filter is applied. **Values:** 0, 1

`[PrinterEvents]`

This section defines parameters for monitoring printer supplies, such as toner levels.

Parameter	Version	Default	Description
`suppliesUpkeepPeriod`	8.2-10.0	1min	How often the supplies manager updates the state of toner level events.

`tonerLevelPredicateSustain`	8.2-10.0	5min	Configures the toner level event. This specifies for how long the toner level must be below a threshold for the event to occur. The reverse also applies - events are not triggered immediately because there can be brief spikes in toner level.

`[PrinterIO]`

This section defines how the system communicates with printers to retrieve device information, including SNMP object identifiers for reading printer models and specifications.

Parameter	Version	Default	Description
`macAddress`	8.2+	.1.3.6.1.2.1.2.2.1.6.1,.1.3.6.1.2.1.2.2.1.6.2	Specifies the list of OIDs for getting MAC addresses of the printers.

`model`	8.2+	.1.3.6.1.2.1.25.3.2.1.3.1, .1.3.6.1.4.1.11.2.4.3.1.12.1.2.78, .1.3.6.1.2.1.1.1.0	Comma-separated list of SNMP Object Identifiers (OIDs) where the model is read. To use a PJL query, include the special value “pjl”. **Example value:** `.1.3.6.1.2.1.25.3.2.1.3.1`, `.1.3.6.1.4.1.11.2.4.3.1.12.1.2.78`, `.1.3.6.1.2.1.1.1.0`
`oidDeviceType`	8.2-10.2.12	.1.3.6.1.2.1.25.3.2.1.2	One OID which is used for detecting the type of the device (in Printer Discovery)
`oidDeviceTypePrinter`	8.2-10.2.12	.1.3.6.1.2.1.25.3.1.5	The OID values (separated by comma) which describe printer device (in Printer Discovery)
`printerDiscoveryThreads`	8.2-10.2.12	128	Specifies the number of threads which are used for printer discovery

`[PrinterStatusChecker]`

This section configures how the print server monitors printer availability and status, including ping attempts, timeouts, and parallel thread limits for reachable and unreachable devices.

Parameter	Version	Default	Description
`errorMaxThreads`	8.2+	16	How many unreachable printers to check in parallel. If the printer is still unreachable, a check takes, in milliseconds: `pingTimeoutMS` * `pingAttempts`

`errorPeriodMS`	8.2+	30000	How often to check the unreachable printers using ping.
`icmpPing`	8.2+	1	By default MyQ uses the ICMP ping to check, if the printer is on-line. If this is set to 0, the driver specific ping is used instead. In case of the SNMP driver, it uses an SNMP GET request to the OID .1.3.6.1.2.1.1.1.0 (sysDescr).
`okMaxThreads`	8.2+	2	How many connected printers to check in parallel. First with a ping to check connectivity, and then it reads the status via SNMP, or other method depending on the printer driver.
`okPeriodMS`	8.2+	60000	How often to update status of connected printers.
`pingAttempts`	8.2+	3	Number of ping requests sent to the printer. If all fail, printer is unreachable.
`pingTimeoutMS`	8.2+	1000	Ping timeout in milliseconds
`totalCountersPeriod`	8.2+	10min	Period of reading of the total counters. Previously, the value was in milliseconds. From 8.1+ you can use the Duration syntax.

`[RateLimit]`

These parameters control security throttling with thresholds for failed authorization attempts.

Parameter	Version	Default value	Description
`thresholdCount`	10.2+	10	The number of failed API authorization requests from one IP address that can be made within the threshold, including login on Terminal (PIN, password, card).
`thresholdInterval`	10.2+	300	The interval during for which `thresholdCount` is applied, in seconds. The default is 5 minutes.

⚠ The rate limiter cannot be disabled. You can effectively disable by setting values that would be unlikely in practice. For example:

- `thresholdInterval=1`
- `thresholdCount=9999`

`[ResourceMonitoring]`

These parameters control how the system samples and logs resource usage data for performance monitoring and analysis.

Parameter	Version	Default value	Description
`sampleBatchPeriod`	10.2.13+	10	Period of batching the samples for logging, in minutes.
`sampleGatheringPeriod`	10.2.13+	5	Resource sampling period, in seconds.

`[Scan]`

This parameter controls the extension format of scanned document filenames.

Parameter	Version	Default value	Description
`threeCharExtensions`	8.2+	0	Enforce three-character file extensions (e.g. `.tif`, `.jpg`). **Values:** 0, 1

`[Security]`

This section defines system-wide security settings for communication protocols and authentication. Use these settings to align the system with your organization's security and compliance requirements.

For detailed guidance, see Advanced Security (see page 266).

Parameter	Version	Default value	Description
`caValidity`	8.2+	730	CA certificate validity in days.
`kerberosOnly`	10.2.13+	`false`	Forces Integrated Windows Authentication to allow Kerberos auth only. NTLM attempts are denied. **Values:** `true`, `false`
`sslCipherSuites`	10.2.7+	compatible	Possible values are: • compatible - deprecated weaker ciphers allowed • strict - no weak ciphers allowed

Parameter	Version	Default value	Description
`sslProtocol`	8.2+	TLS1.2 < 10.2: SSL2	Specifies the minimal security protocol which is used for communication. Possible values: SSL2, SSL3, TLS1, TLS1.1, TLS1.2, TLS1.3 **Note:** In MyQ 8.2.39+ / 10.1+ this setting also affects Traefik - If SSL2, SSL3, TLS1 -> TLS1 is used for Traefik This parameter affects the configuration of: • SMTP • IPP • LPR • Messages (WebSockets) • HTTP Router

`[SMTPClient]`

This section configures how the system connects to an external mail server when sending emails and notifications.

Parameter	Version	Default	Description
`domain`	8.2+	empty	Domain to be used in HELO command.
`timeout`	8.2+	30	PHP mailer SMTP timeout in seconds.

`[SMTPServer]`

This section controls how the system receives and handles email-related communication, including message size limits, encryption settings, and timeouts.

Parameter	Version	Default value	Description
`encryption`	8.2+	`true`	When set to `false`, the SMPT server does not announce its ability to use encryption. This forces clients to use an unencrypted connection or disconnect.
`maxMessageSize`	8.2+	47185920	Maximum message size in bytes that the SMTP server can receive. If exceeded, SMTP server returns a 552 error. Default value is equivalent to 45MB. 0 = unlimited message size (effectively up to the implemented limit, which is 2GB, or 2147483648)
`timeout`	8.2+	60000	Communication timeout, in milliseconds. Default is equivalent to 60 seconds.

`[Supplies]`

This section configures how the system monitors supply levels, which affects toner status monitor events, toner replacement prediction events, and detections of toner replacements.

Parameter	Version	Default	Description
`supplyLevelSustainPeriod`	10.1+	5min	Duration for which a supply level must be stable before it is marked as sustained.

[Terminal]

Parameter	Version	Default	Description
kyoceraLiteDummyJob	8.2+	1	If true, the Kyocera Embedded Lite terminal sends the "dummy job" to PM Server. If false, an empty filename is sent.
printedJobTimeOut	8.2+	1200	Timeout in seconds of locally spooled printed jobs.
sendCmdAttempts	8.2+	4	Number of packet retransmission attempts. A retransmission occurs when the terminal does not acknowledge the packet from the server. If all attempts fail, there will the "Terminal is not responding to the command" message in the log.
term5IdleTimeOutInMS	8.2+	35000	If the server does not receive any keep-alive packets from the terminal in this time period (in milliseconds), the terminal is considered abandoned and removed from the list of terminals. This value is used for terminals with firmware version equal or greater than 5.

[Testing]

This parameter provides a diagnostic option for UI debugging.

Parameter	Version	Default	Description
`disableTranslation`	10.1+	0	Rendering of language strings in the user interface. **Values:** 0 - Show translated strings 1 - Show translation IDs **Note:** Requires debug mode.

`[UserSession]`

This section defines how user sessions are managed on printing devices, including timeouts, job retry behavior, session recovery, and credit reservation settings.

Parameter	Version	Default	Description
`creditBlockingMaxPages`	8.2+	40	Used when automatic credit reservation is turn on on the account. The "Maximum reserved credit" value is calculated automatically as creditBlockingMaxPages * maxPagePrice. The maxPagePrice is calculated from the price list.

`creditBlockingMinPages`	8.2+	10	Used when the automatic credit reservation is turn on on the account. The "Minimal reserved credit" value is calculated automatically as creditBlockingMinPages * maxPagePrice. The maxPagePrice is calculated from the price list.
`jobSenderConnectTimeOutInMS`	8.2+	30000 ms	MyQ must connect with the printer within this timeout.
`jobSenderSendTimeOutInMS`	8.2+	3600000 ms	Jobs must be sent to the printer within this time limit. IPP only.
`jobSenderServerBusyRetryInMS`	8.2+	5000 ms	If the printer returns a server-busy error, MyQ waits for the specified retry interval before attempting to resend the job. For example, the IPP protocol may return the server-busy error if too many jobs are queued.
`jobSenderServerErrorMaxRetryInMS`	8.2+	30000 ms	Maximal retry interval after error when sending a job. See `jobSenderServerErrorMinRetryInMS` for more details.

`jobSenderServerErrorMinRetryInMS`	8.2+	5000 ms	If an error occurs when sending a job, MyQ waits for the specified retry interval before attempting to resend the job. For each subsequent attempt, the waiting time doubles, up to the value of `jobSenderServerErrorMaxRetryInMS`.
`jobSenderShutdownTimeOutInMS`	8.2+	600000	When MyQ finishes sending data, it closes the connection and waits for the close event from the printer. This parameter sets, in milliseconds, the timeout of waiting for the event (0 = infinite). The default is equivalent to 10 minutes. On some printers or in some networks the event does not come, so use a lower timeout to ensure that the user session finishes.
`nonSessionScanTimeOut`	8.2+	5	If a scan is received and there is no user session on the printer, MyQ searches for a recent user session to learn the user. This parameter specifies how far into the past (in seconds) MyQ looks.

`printerUnreachableTimeout`	8.2+	60	If the printer is unreachable for longer than this parameter, interrupt the session. Jobs that have not been sent to the printer yet, will not be printed. The user can print them in their next session.
`readyJobsSortAsc`	8.2+	`false`	How to sort ready jobs in the My Jobs screen

`[WebService]`

This parameter should be used only if your site needs legacy support for devices that use RPC.

Parameter	Version	Default	Description
`legacyTerminalUserRpcEnabled`	10.2.24+	not set	Enables support for legacy RPC access. Use this parameter only when you need to support older devices. **Values:** `true`, `false`

9 Printers

This section describes how to set up, manage, and monitor printing devices in MyQ. It covers printer and terminal settings, adding and discovering devices, activating and deactivating printers, editing device settings, organizing printers into groups, exporting printer information, monitoring offline and local printers, and configuring email notifications for device alerts.

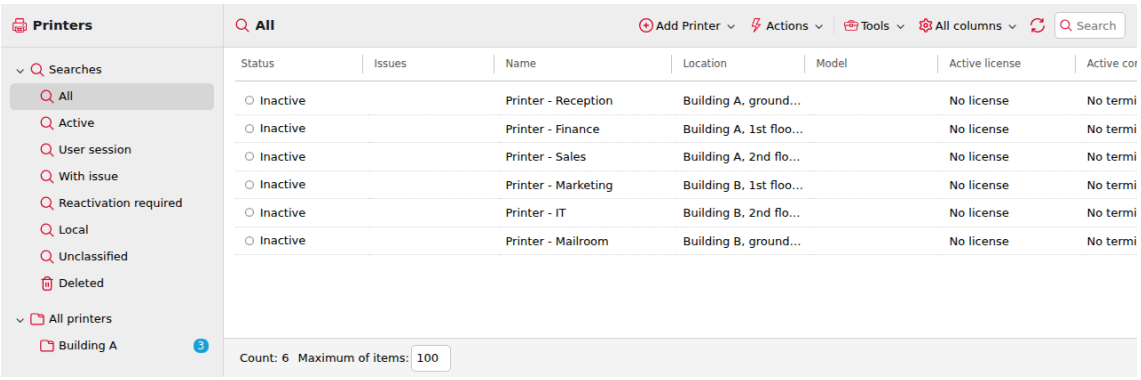
See also:

- Printers and Terminals Settings (see page 301)
- Manually Adding Printing Devices (see page 320)
- Printer Discovery (see page 314)
- Activating and Deactivating Printing Devices (see page 418)
- Managing Printers (see page 414)
- Monitoring Network Printers in Offline Mode (see page 421)
- Monitoring Local Printers (see page 422)
- Printer Events (see page 423)

9.1 Printers Tab

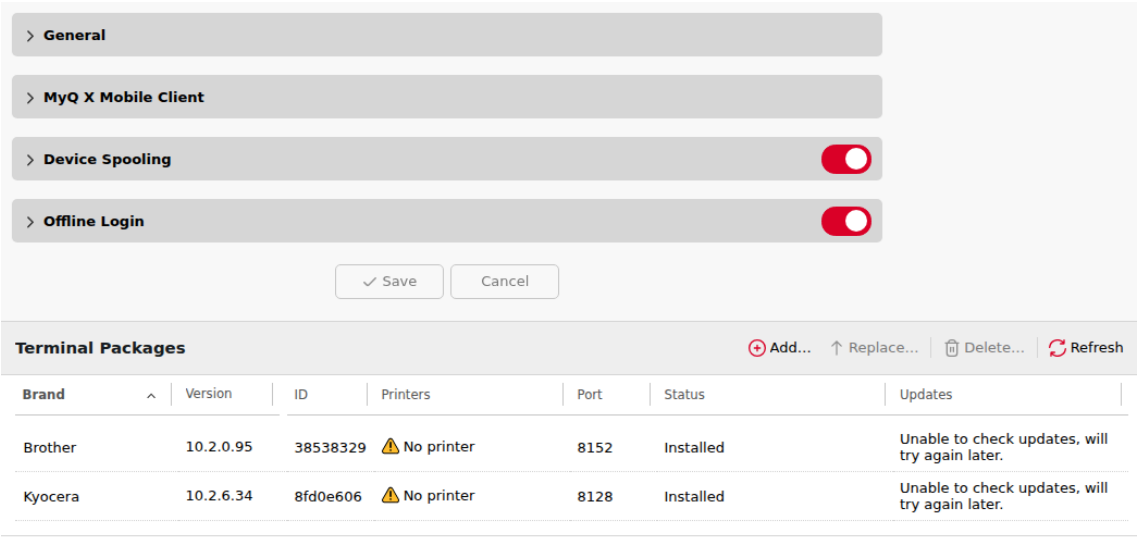
On the **Printers** main tab, you can see printing devices and information about them. With the **All** search option selected, you see all printing devices that are currently in the system. Apart from this option, you can select from the following:

- **Active** - select to display only active printing devices.
- **User session** - select to display only printing devices that are currently in use.
- **With issue** - select to display only printing devices with a reported issue (these printers are also listed on the **Home** page).
- **Re-activation required** - select to display the printing devices that must be activated again.
- **Local** - select to display only locally connected printing devices (USB, LPT).
- **Unclassified** - select to display only printing devices that do not belong to any group.
- **Deleted** - select to display only deleted printing devices.



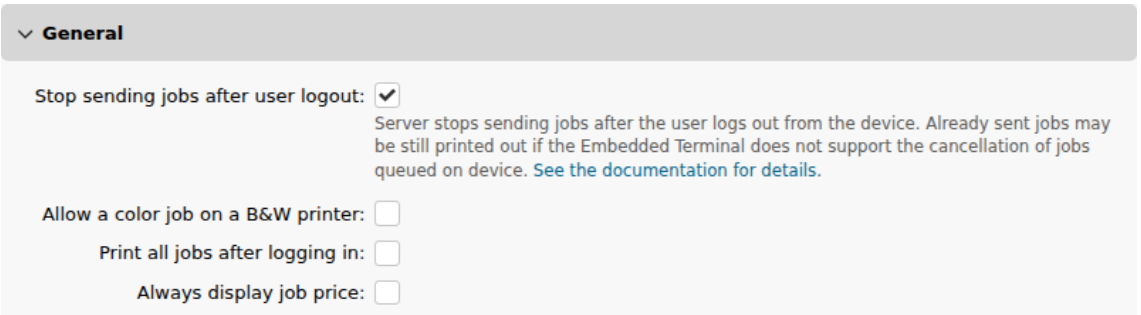
9.2 Printers and Terminals Settings

On the **Printers & Terminals** settings tab, you can manage your terminal packages, and configure multiple settings. The settings are divided in the **General, MyQ X Mobile Client, Device Spooling, Offline Login**, and **Terminal packages** sections.



9.2.1 General

In this section, the following settings are available:



- **Stop sending jobs after user logout**: If enabled, jobs requested for release by the user by clicking Print on the Embedded Terminal are stopped when the user logs out of the device. This effectively means that when a user starts printing a list of jobs and logs out, some pages/jobs already saved in the device's memory may be still printed. However, the print should eventually stop. Not yet released jobs will be returned to Ready status and available to the user again in My jobs.

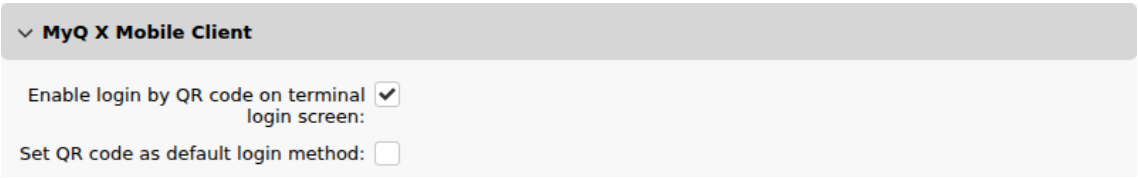
⚠ Kyocera terminal installations create an additional option to **Discard pending jobs on logout** which can be enabled in Settings – Configuration profiles – profile detail – Terminals tab, in the vendor-specific settings section (under the vendor's name available only when the terminal is installed on the Server).

- **Allow a color job on a B&W printer**: If enabled, color jobs can be printed on B&W printers.
- **Print all jobs after logging in**: If enabled, a **Print all jobs after logging in** checkbox is displayed on the terminal's Log in screen, and it is selected by default. If the user keeps it selected, all their jobs from the **Ready** tab are automatically printed as soon as they successfully log in. If the user disables the option, no jobs are printed automatically upon login.
- **Always display job price**: If enabled, a job's price on an Embedded terminal is displayed even when Credit or Quota are disabled. If disabled, a job's price on an Embedded terminal is not displayed unless Credit or Quota are enabled.

To enable any of the settings, select the checkbox next to them, and click **Save** at the bottom of the tab.

9.2.2 MyQ X Mobile Client

In this section, you have the following options:

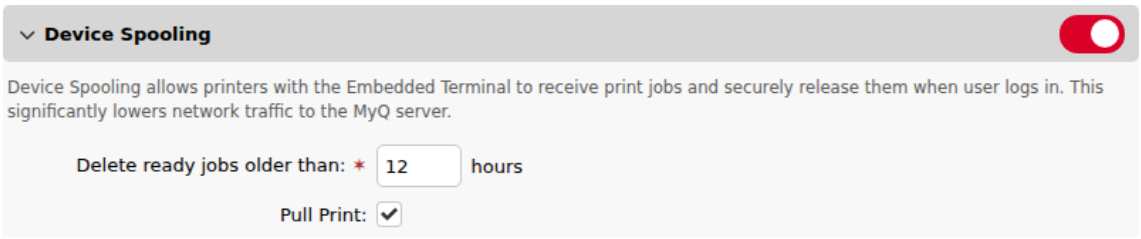


- **Enable login by QR code on terminal login screen**: If enabled, a QR code is displayed on the terminal login screen and can be used to log in (enabled by default).

- **Set QR code as default login method**: If enabled, a QR code is displayed on the terminal login screen and is the default method for logging in.

9.2.3 Device Spooling

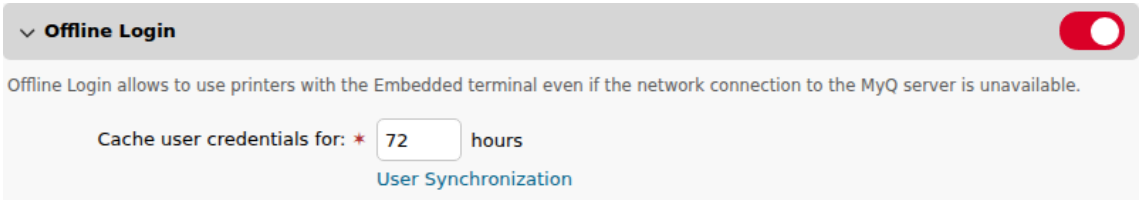
In this section, you can enable the Device Spooling feature for your embedded terminals and set it up.



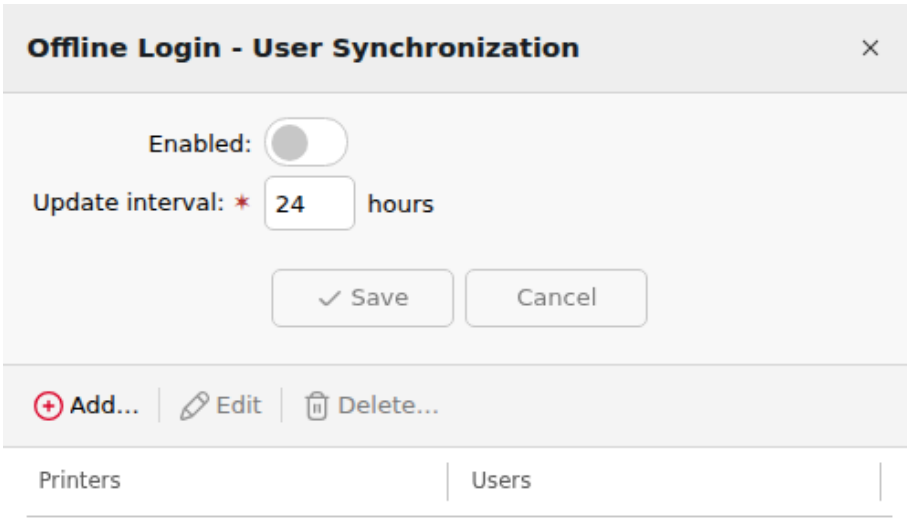
- **Enabled**: Enable/disable the **Device Spooling** feature (disabled by default).
- **Delete ready jobs older than __ hours**: Period of time after which the device spooled jobs are deleted. The default is *12* hours, and the allowed range is *1* to *72*.
- **Pull Print**: If enabled, you can use Pull-Print printing.

9.2.4 Offline Login

Offline Login allows to use printers with Embedded terminals even if the network connection to the MyQ server is unavailable. In this section, you have the following settings:



- **Enable/Disable**: Use the enable/disable switch in the section header to enable or disable the **Offline Login** feature (disabled by default).
- **Cache user credentials for __ hours**: The terminal caches user credentials for the given time, allowing them to log in while offline. The default is *72* hours, and the allowed range is *1* to *168*.
- **User Synchronization**: If enabled, the user's information can be synchronized to printers without the need for the user to log in to the printer first.



- **Enabled**: Enable/disable offline login user synchronization.
- **Update interval**: Set the interval of user synchronization between *1* and *168* hours.
- **Add, edit, delete** printers and users: Configure the printers and users for the offline login user synchronization.

9.2.5 Terminal Packages

In this section, you can manage your terminal packages.

- Click **Add...** to upload a terminal package to the server. In the pop-up window, browse and open the terminal package, and click **OK**. The terminal package is uploaded and installed. (Note that the terminal package service will automatically run under the Local System Windows account. To change it, go to MyQ Easy Config in the Easy Config Settings (see page 148) tab.)
  - If you are trying to update a terminal package by adding a later version of the same terminal package, a pop-up informs you that a previous version of the package is already installed, and to update it you must select that package and click **Replace...**
- Select an installed terminal package and click **Replace...** to upgrade it to the latest version. In the pop-up window, browse and open the terminal package, and click **OK**. The terminal package is uploaded and installed, and the device is automatically reactivated.
- Select an installed terminal package and click **Delete...** then click **Yes** to uninstall it from the server.

> ⚠ If you are upgrading terminal packages within a MS Cluster and are using patch 25+, you must first take the **TerminalsMonitor** script offline before the upgrade and bring it back online afterwards.

For specific terminal packages information and limitations, check the embedded terminal manuals:

- MyQ Brother Embedded
- MyQ Canon Embedded
- MyQ Epson Embedded
- MyQ Fujifilm Embedded
- MyQ HP Embedded
- MyQ KATUN Embedded
- MyQ Kyocera Embedded
- MyQ Kyocera Embedded Lite
- MyQ Lexmark Embedded
- MyQ Ricoh SmartSDK Embedded
- MyQ Sharp Embedded
- MyQ Sharp Luna Embedded
- MyQ Toshiba Embedded
- MyQ Xerox Embedded

In the Configuration profile options, these are represented as the type “Embedded”. On top of that, the Configuration profile also contains built-in types, such as network authentication. See Configuration Profiles (see page 310) .

9.2.6 Device Spooling

Device Spooling sends print jobs directly from a user workstation to a supported printing device, where they are stored locally until release. The print job does not pass through the MyQ Print Server.

Device Spooling can reduce network traffic between remote sites and the Print Server and can help maintain printing during server or network outages. For guidance on when to use Device Spooling and how it combines with Client Spooling, Offline Login, and Fallback Printing, see (v2) Spooling Strategy in the MyQ Deployment guide.

> ⚠ Device Spooling is supported on **Kyocera** and **Ricoh devices** with supported MyQ embedded terminals.

Device Spooling Ports and Modes

The port used to submit a job determines how it is processed and released.

Port	Mode	Behavior
10010	Direct print	The job prints immediately after it is received by the device.
10011	Secure hold print	The job is stored on the receiving device until the user authenticates and releases it. The job can only be released from that device.
10012	Pull print	The job is stored on the receiving device and can be released from another supported Device Spooling device on the same subnet.
10013	Delegated print	Similar to Device Spooling Pull Print, but the job can also be released by a delegate of the sending user.

Enable Device Spooling

1. In the MyQ Web Interface, go to **MyQ > Settings > Printers & Terminals**.
2. Expand **Device Spooling**.
3. Enable **Device Spooling**.
4. In **Delete ready jobs older than**, specify how long ready Device Spooling jobs remain stored on the device.
   The default is **12 hours**. The allowed range is **1–72 hours**.
5. To allow jobs spooled on one device to be released from other supported devices, enable **Pull Print**.
6. Click **Save**.
7. If the **Apply new settings** dialog appears, keep **Reset all terminals** selected and confirm the change.

The settings are distributed to the connected embedded terminals.

Configure Device Spooling Pull Print

When **Pull Print** is enabled, jobs submitted to port **10012** can be released from other supported Device Spooling devices on the same subnet.

The job stays on the device that received it. When a user signs in at another participating device, that device discovers the user's jobs on the subnet. When the user releases a job, the device that holds it sends the job to the user's device.

For Device Spooling Pull Print:

- All participating devices must be on the same subnet.
- The network must allow UDP broadcast between participating devices. Devices use it to discover jobs.
- Participating devices must be able to reach each other on the RAW printing port (TCP 9100). The device that holds a job uses this port to send the job to the release device.
- All participating devices must have synchronized system time. Configure the devices to use the same reliable time source.

Device Spooling Pull Print does not operate across subnets.

Configure IP Filters

For Device Spooling Pull Print to work correctly, participating devices must be able to communicate with each other.

On the printing devices, either:

- disable IP filtering; or
- configure the IP filter to include the IP addresses of all devices that can store or release Device Spooling Pull Print jobs.

Apply this configuration to every participating device.

Configure Client Printers for Device Spooling

To send jobs to Device Spooling, configure the client printer to send print data directly to the target device using the **RAW** protocol.

You don't need MyQ Desktop Client for Device Spooling. The workstation's print queue sends jobs directly to the Device Spooling port. Desktop Client is needed only if you use Device Spooling ports as Fallback Printing destinations.

See also: (10.2) Fallback Printing

Use:

- the hostname or IP address of the target printing device;
- the Device Spooling port for the required mode, as listed in **Device Spooling Ports and Modes**

The client printer must use a print driver and print language supported by the target device and Device Spooling.

Supported Print Languages

Device Spooling supports the following print languages:

- PCL XL
- PCL5c
- KPDL
- PDF

Confirm that the driver used by the client produces a supported print language.

Device Spooling Limitations

Consider the following limitations:

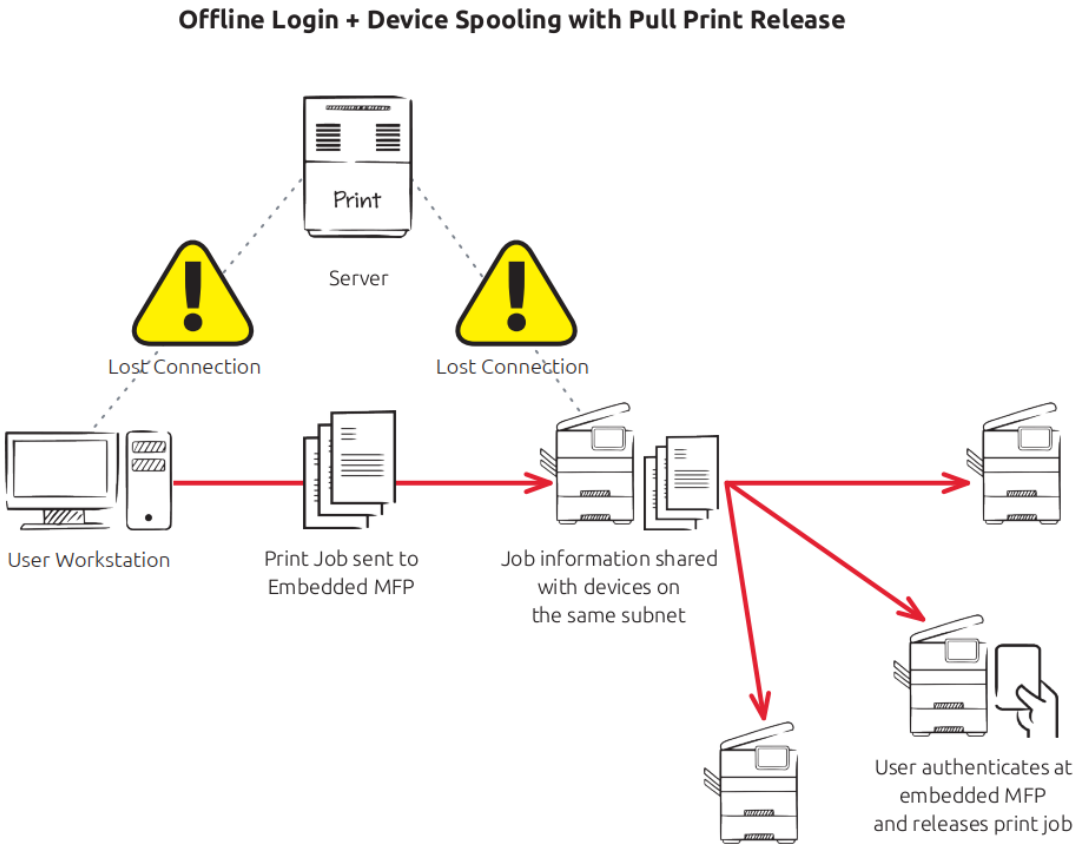
- Device Spooling Pull Print is limited to devices on the same subnet.
- Participating Pull Print devices must have synchronized time.
- Project Accounting is not supported. Device Spooling jobs are recorded without a project assignment.
- Favorite jobs are not supported.
- Job Roaming is not supported.
- Print Job Archiving is not supported.
- Job Preview is not supported.
- Device storage requirements are higher than with server-spooled printing because job files are stored on the printing device.

Use Device Spooling with Offline Login

Device Spooling can be combined with **Offline Login** to allow users to authenticate and release locally stored jobs when the Print Server is unavailable.

Offline Login caches user credentials on the embedded terminal. During an outage, users can authenticate using a cached PIN or ID card and access functions that do not require a live connection to the Print Server.

Offline Login provides authentication continuity; Device Spooling provides job storage and release. Offline Login does not spool print jobs by itself.



9 Offline Login with Device Spooling Pull Print

See also: Printers and Terminals Settings (see page 301)

Use Device Spooling with Fallback Printing

When MyQ Desktop Client is deployed, Device Spooling can also be used as a Fallback Printing destination.

Desktop Client can send fallback jobs directly to Device Spooling ports `10010–10013`, allowing the required direct, hold, pull, or delegated release behavior while the Print Server is unavailable.

See also: (10.2) Fallback Printing

Verify Device Spooling

Test the Device Spooling workflows you intend to use before production rollout.

1. Send a test job using each Device Spooling mode you intend to support.
2. Confirm that:
    - Direct print jobs print immediately.

- Secure hold jobs remain on the receiving device until the user authenticates.
- Pull print jobs can be released from another participating device on the same subnet.
- Delegated print jobs can be released by an authorized delegate.

3. If Offline Login is part of the deployment, make the Print Server temporarily unavailable.
4. Authenticate at the device using a cached PIN or ID card and confirm that the Device Spooling job can still be released.
5. Restore the Print Server connection.
6. Confirm that job accounting is reported correctly after connectivity is restored.

See also:

- Printers and Terminals Settings (see page 301)
- Main Communication Ports (see page 29)
- (v2) Spooling Strategy
- (v2) Resilience, Fallback & High Availability
- (10.2) Fallback Printing

9.3 Configuration Profiles

A configuration profile is used for multiple printers configuration. It is where you can add an installation package and attach it to printers to equip them with embedded terminals.

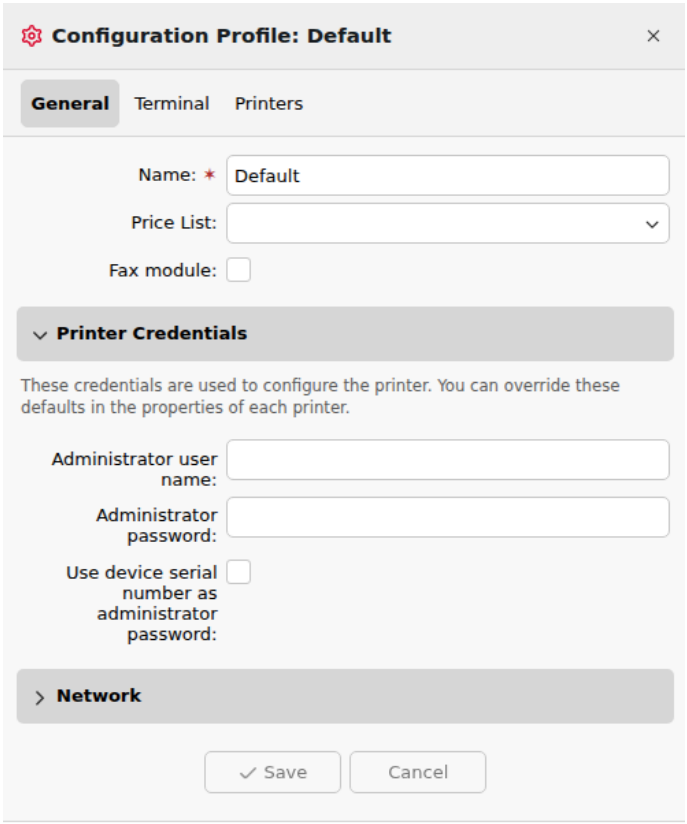
It is recommended to create a configuration profile per printer type if you have different printer types.

For a quicker setup you can clone your configuration profiles. With minimal editing you can then create a new profile. Printers will not be cloned to this new configuration profile. Go to **MyQ > Settings > Configuration Profiles**, select a configuration profile and click **Clone** on the menu bar (or right click and clone).

Configuration profiles are needed for printer discovery.

The following settings can be configured:

9.3.1 General Tab



- **Name:** It is mandatory to give the profile a name.
- **Price List**: Select a price list from the drop-down. For more information on price lists. See Price Lists (see page 674).
- **Fax module**: If selected, all printed faxes are charged on the FAX user account. It is available only for devices with the FAX option. Select only if the device has a fax module.
- **Printer Credentials**: The credentials are used to configure the printer(s) attached to the profile. You can override the defaults with the **Printer Credentials** in the properties of each printer.
- **Network:** Here you can add an SNMP profile and in **MyQ server address** select if the network should use the IP address or the Hostname (Hostname is used by default). See SNMP Profiles (see page 236).

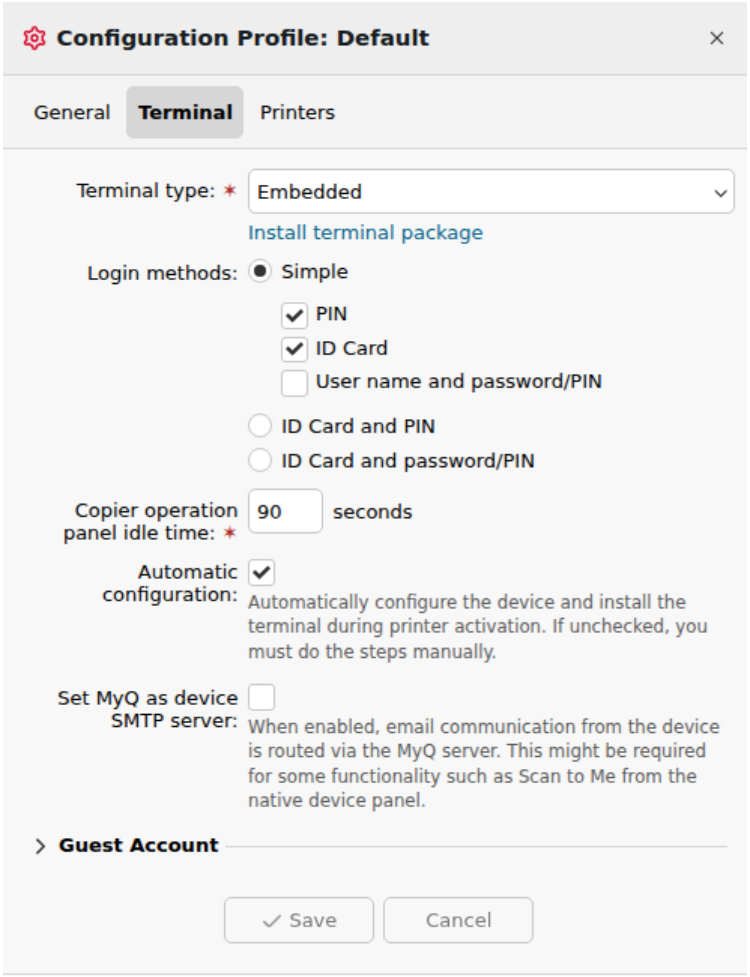
9.3.2 Terminal Tab

- **Terminal type**: Select a terminal type from the drop-down.

- Embedded
- Embedded Lite
- Kyocera Embedded Lite
- Felica Reader
- Kyocera Network authentication – this enables network authentication on the device and configures MyQ X Print Server as the authentication server. Users can authenticate with their MyQ X accounts on SFP devices and release jobs immediately. It may not be supported by all devices, ask your MyQ X provider.

If the type you want is missing, click **Install terminal package**. Once the package is installed, select it from the drop-down.

Based on the **Terminal type** selected, further configuration options will become available, these may vary based on the type selected.



- **Login methods**: select the login methods you want to be available on terminals with this configuration profile selected, the options are **PIN**, **ID Card**, and **User**

name and password/PIN, **ID Card** can also be combined with **PIN** or **Password** if double-authentication is required.
- **Copier operation panel idle time**: time (in seconds) for idle logout (mandatory field), the default is **90 seconds**.
- **Automatic configuration**: leave this option unchecked if you want to configure the device manually.
- **Set MyQ as device SMTP server**: When enabled, email communication from the device is routed via the MyQ server. This might be required for some functionality such as Scan to Me from the native device panel.
- **Guest Account**: click **Enable** if you wish to allow guest users to access terminals with this configuration profile enabled. Additional options allow you to select the user guests should be logged in as, and which screen to show immediately after a guest logs in.

Using Multiple Terminal Packages for the same Vendor

In certain situations, it may be necessary or helpful to utilize multiple terminal packages from the same vendor, for example when staggering updates to a large fleet, or because certain devices are not compatible with the latest terminal packages.

> ⚠ In order to run multiple terminal packages from the same vendor, one of those terminal packages must normally be a terminal version 10.2 or higher. Certain 10.1 terminal versions also support this feature.

To install multiple terminal packages, use the process described above under **Terminal tab**, but note that you may need to enable **Advanced settings** and specify a different **port** from that already used for packages from the same vendor.

In the main **Printers** tab, you can then right-click a printer and select **Choose terminal version**, select the desired terminal package for this printer from the drop-down list. If a printer is activated without specifying a terminal version, and more than one is available, the latest terminal package will be used by default.

For more information, see Using Multiple Terminal Packages for the same Vendor.

9.3.3 Vendor-Specific Options

Some options become available in the Terminal tab when a terminal package is installed. For information about vendor-specific options, see the following pages:

- (10.1) Vendor-Specific Options: Canon
- (10.2) Vendor-Specific Options: HP

- (10.2) Vendor-Specific Options: Kyocera
- (10.1) Vendor-Specific Options: Lexmark
- (10.1) Vendor-Specific Options: Sharp
- (10.1) Vendor-Specific Options: Sharp Luna
- (10.2) Vendor-Specific Options: Epson

9.3.4 Printers Tab

Click **Add** to add printers to the configuration profile from your printers list.

Select the added printers and click **Remove** to remove them from the configuration profile.

9.4 Adding Printing Devices

Printing devices must be connected to your MyQ account before they can be managed and used. You can add printing devices via:

- Printer Discovery (see page 314)
- Manually Adding Printing Devices (see page 320)
- Exporting and Importing Printers (see page 320)

9.4.1 Printer Discovery

On the **Printer Discovery** settings tab, you can create and run print discoveries to search for all network printing devices within a defined IP range of your company's network. You can create multiple discoveries for different subnets.

Automated Printer Discovery

It is possible to add an **Action** to your printer discovery. In that way you can add a **Configuration profile** to your printer discovery, or select to activate the discovered printers when you **Run** the printer discovery.

To add a print discovery, do the following:

1. On the **Home** tab, click **Discover printers** in the **Quick Setup Guide** section (or go to **MyQ > Settings > Printer Discovery**).
2. On this tab, click **Add Discovery**. The new printer discovery properties panel opens.
3. On the panel, you can change the **General** discovery configuration (described below).
4. You can also set special **Actions** to be performed during the discovery; see Printer Discovery Actions (see page 317).

5. Click **Save**. The new printer discovery appears on the list on the **Printer Discovery** settings tab.

To run a discovery and add printing devices:

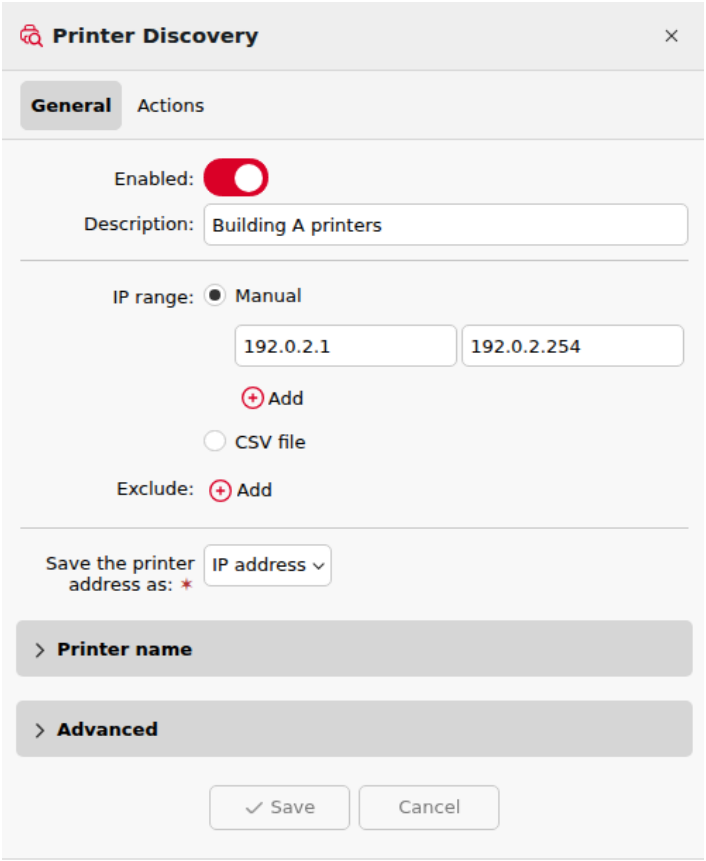
On the **Printer Discovery** settings tab, select the printer discovery that you want to use, and then click **Run**.

The Discovering tab with a list of discovered printing devices opens. You can choose to add either all of the discovered devices or just a selection of them:

- If you want to add all discovered devices, click **+Add to MyQ**, and then click **+Add all** in the drop-down. You can see the added printing devices on the **Printers** main tab.
- If you want to add selected devices, select the devices that you want to add, click **+Add to MyQ**, and then click **+Add selected**. You can see the added printing devices on the **Printers** main tab.

Printer Discovery General Configuration

The options on this page cover the most commonly used settings for printer discovery. For details about advanced options related to other MyQ features, see the MyQ Embedded Terminal guides.



- **Enabled** – Enables the discovery to be included in the scheduled run of print discoveries.
- **Description** – Specifies a custom description of the printer discovery.
- **IP range** – Defines the range of IP addresses used for discovery. Initially, the range is automatically detected from the server IP.
    - You can edit the ranges manually, or define ranges by importing a CSV file (one column, ascending order). You can also add and delete additional ranges.
    - To exclude an individual IP address, click **+Add** next to *Exclude*.
- **Save the printer address as** – Defines how the discovered device address is saved (IP address, Hostname, or FQDN).
- **Printer name** – Specifies the names of discovered printers when they are added to MyQ, either using a name template or a CSV file.
    - Name template – Defines a template for naming discovered devices using substitution variables:
        - `%model%` – Model of the printing device
        - `%ipByte4%` – Last byte of the device IP address
        - `%sn%` – Serial number

        - `%id%` – ID of the device in the MyQ database (if the printer name template contains this parameter, the name will not update if the devices is rediscovered)
        - `%hostname%` – Hostname resolved by DNS
        - `%snmpHostname%` – Hostname from the device MIB table via SNMP
        - `%FQDN%` – Fully Qualified Domain Name of the device
    - **CSV file** – Define printer names with a CSV file containing two columns, enter the file path, and select the value type under *First column in table*.
        - The first column identifies the device by IP address, hostname or serial number.
        - The second column contains the printer name that you want to assign.
          Example:

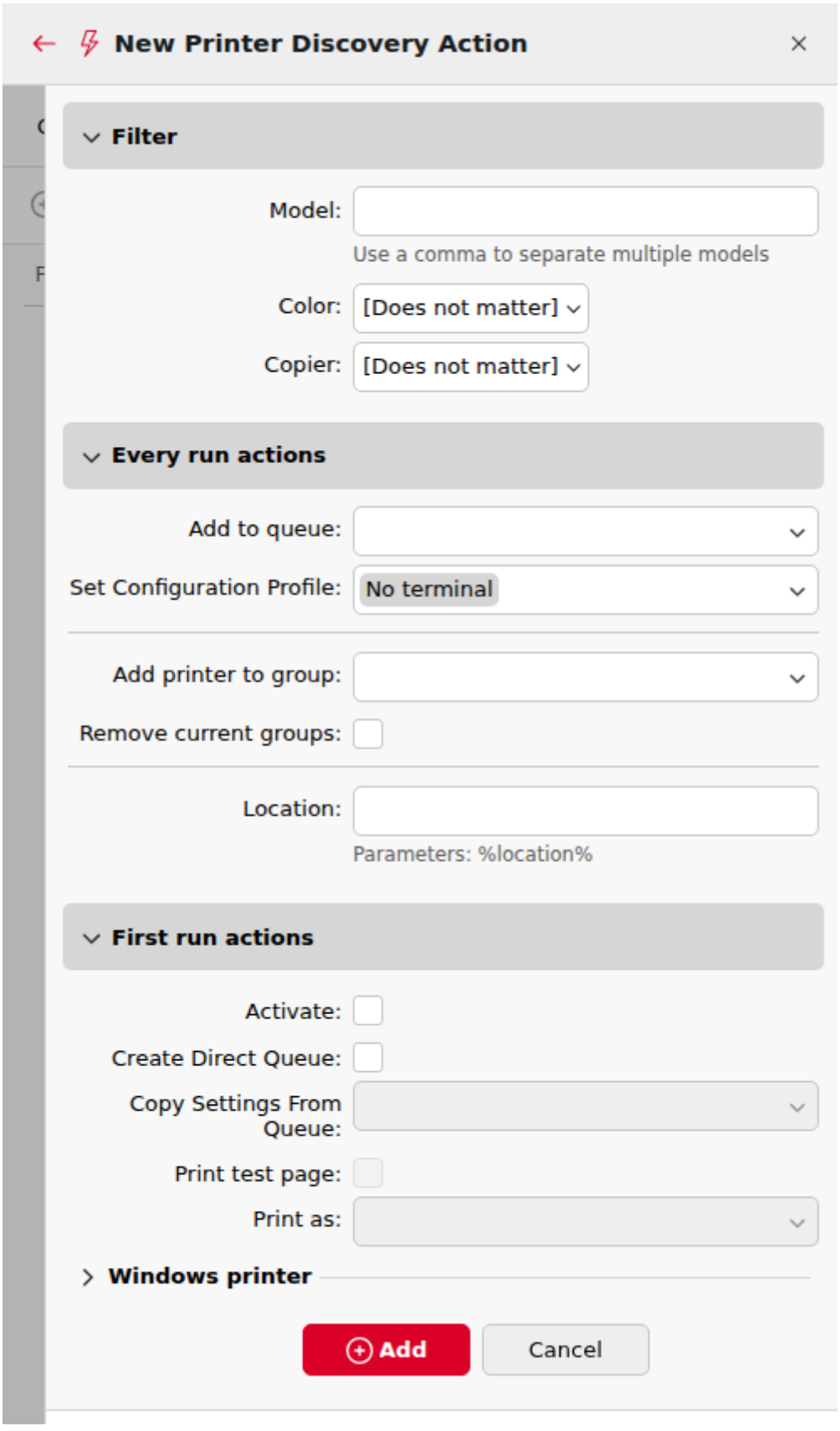
          ```
          list of IPs;Custom name
          10.0.0.11;Printer Name 1
          10.0.0.12;Printer Name 2
          ```

        - Only printers listed in the CSV file are added. Printers not listed are skipped.
- **SNMP** – Defines the SNMP profile and timeout (in milliseconds), controlling how long MyQ waits for device responses.
- **Initiated by terminal** – Enables discovery triggered by Java-based terminals that connect without a corresponding printer entry in MyQ.

Printer Discovery Actions

The actions mentioned below are basic actions that are commonly performed during printer discoveries.

Go to the **Actions** tab and click **+Add action**. The Actions properties panel opens.


New Printer Discovery Action
Filter
Model:
Use a comma to separate multiple models
Color:
[Does not matter]
Copier:
[Does not matter]
Every run actions
Add to queue:
Set Configuration Profile:
No terminal
Add printer to group:
Remove current groups:
Location:
Parameters: %location%
First run actions
Activate:
Create Direct Queue:
Copy Settings From Queue:
Print test page:
Print as:
Windows printer
Add
Cancel

Filter

Here you can specify the printing device models or the types of devices on which this action is performed during the discovery.

- Enter the model on which you want to perform the action. If you want to add more models, you have to separate them by commas (,).
- You can also select types of devices: color or B&W devices, and distinguish between copiers.

Every run actions

- **Add to queue**: Here you can select one or more queues where the device will be automatically added to.
- **Set configuration profile**: Here you can select a configuration profile from the dropdown or create a new one by selecting **+Add new**. It gives you the option to install a terminal package and set the login method for the printers in the discovery.
- **Add printer to group**: Here you can select a group where the device will be automatically added.
- **Remove current groups**: If you select this option, the device is removed from all of its current groups.
- **Location**: Here you can set the location of the printing device. There are three options:
    - You can manually define the location by entering any text. Each printing device discovered or updated within this printer discovery will contain this location.
    - You can automatically obtain the location via SNMP protocol by entering the **%location%** parameter. In such cases, the location is taken from the location parameter defined on the Web User Interface of each particular device discovered or updated within this printer discovery.
    - You can leave this setting empty. In this case, the location of the printing device is not set/updated
      during the discovery. Updated printers maintain their current location and new printing devices have the location parameter undefined.

The location of a printing device is displayed and can be changed on its properties panel.

You can add multiple filters for performing discovery actions: every filter specifies the type of printers the actions will be performed on and which actions will be included.

First run actions

- **Activate**: Automatically activates the device if the current license allows it.
- **Create direct queue**: If you select this option, MyQ will automatically create a direct queue for the device. The name of the queue is the same as the system name of the device. For more information about print queues, see Queues (see page 532).
- **Copy settings from the queue**: Here you can enter or select a direct queue from which the settings of the newly created queue are copied.
- **Print test page**: The MyQ server will automatically send a test page to the newly created direct queue.
- **Print as**: If you select the **Print test page** option, you have to select a user account under which the test page will be printed.
- **Windows printer**: In this section you can automatically install a print port and printer driver on the MyQ server.

9.4.2 Manually Adding Printing Devices

To manually add a device:

1. On the **Printers** main tab, click **+Add printer**. A drop-down box appears.
2. In this drop-down box, click **+Add printer**. The new printing device properties panel opens on the right side of the screen.
3. On the panel, enter the device name and IP address, and then click **Save**.

9.4.3 Exporting and Importing Printers

On the **Printers** main tab, you can export and import lists of printing devices and related metadata.

Export Printers to CSV

To export a list of printing devices:

1. On the **Printers** main tab, click **Tools**.
2. On the drop-down box, click **Export**.

> The printer admin password column is always empty. You cannot **Export** plain text passwords due to security reasons. However, you can **Import** passwords in plain text in the same column.

Import Printers from CSV

You can import a list of printers from a CSV file. The first row of the file must contain the column names, as in the following example:

```
PRINTER;LOCATION;IPADDRESS;SCANNERIP;ASSETNUMBER;CONTACT
```

To import a list of printing devices:

1. At the top of the **Printers** main tab, click **Tools**.
2. In the drop-down box, click **Import**.
3. Browse for your CSV file and click **OK**.

Your printers are now imported and visible in the **Printers** tab.

> A sample file called `Printers_example.csv` is included in `ProgramData\MyQ\Data\Import`. Customize this file for your own use.

Supported Columns

Export

- PRINTER
- LOCATION
- IPADDRESS
- SCANNERIP
- ENFORCEDMODEL
- ASSETNUMBER
- CONTACT
- PURCHASEDATE
- MODEL
- SERIAL NUMBER
- MAC
- B&W PRINT
- COLOR PRINT
- B&W COPIES
- COLOR COPIES
- SCANS
- FAX
- C
- M
- Y
- K
- A4 PAPER

Import

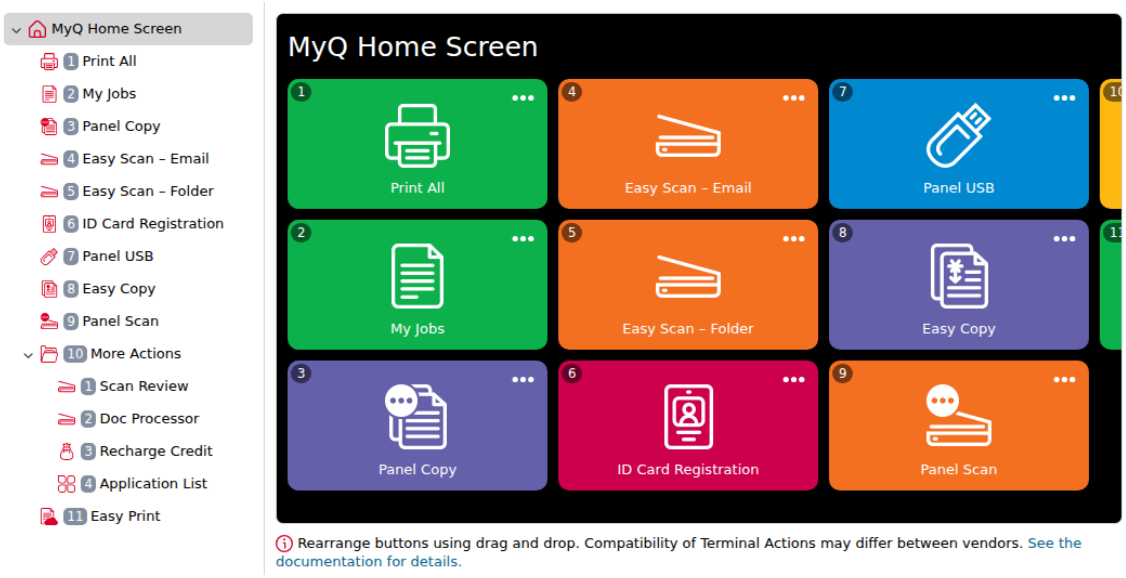
- PRINTER (required)
- IPADDRESS (required)
- LOCATION
- SCANNERIP
- ENFORCEDMODEL
- SERIAL NUMBER
- MAC
- ASSETNUMBER
- CONTACT
- PRINTER ADMIN
- PRINTER ADMIN PASSWORD

- A3 PAPER
- A5 PAPER
- B4 PAPER
- B5 PAPER
- OTHER PAPER
- FOLIO PAPER
- LEDGER PAPER
- LEGAL PAPER
- LETTER PAPER
- STATEMENT PAPER
- REST OF PAPER
- PRINT COLOR PAGES (L1)
- PRINT COLOR PAGES (L2)
- PRINT COLOR PAGES (L3)
- COPY COLOR PAGES (L1)
- COPY COLOR PAGES (L2)
- COPY COLOR PAGES (L3)
- PRINTER ADMIN
- PRINTER ADMIN PASSWORD

9.5 Terminal Actions

In the **Terminal Actions** settings tab on the MyQ Web administrator interface, you can view and manage embedded terminals features. The features are called actions and can be accessed from action nodes on the terminal. The action nodes correspond to buttons on the printing device display.

You can configure the layout of the display screen, as well as the behavior of each button. This means you are free to choose any combination of available actions and their positions on the screen. The layout is displayed on a WYSIWYG (*what-you-see-is-what-you-get*) terminal preview and can be configured there.



Terminal actions are arranged vertically in blocks of three. A maximum of eighteen terminal actions per level is allowed. If the number of terminal actions is greater than nine, the buttons are stretched to show arrows that allow switching between pages. This, however, depends on the terminal display and smaller screens have fewer top menu actions per page, as well as either pagination on the left or dotted pagination at the bottom.

Additional layout options are provided by the possibility to create folders and put action nodes inside. Folders can be used to group actions of the same type, such as scanning to different destinations, or to enable users to access a higher number of actions.

Users and groups can be given rights to different actions. This way, you can configure individual home screens for each user or group of users.

The terminal action nodes can be managed directly on the terminal screen preview where you can:

- Drag and drop actions to change their order.
- Drag and drop to place certain actions inside folders.
- Use the context menu of an action to **Edit** or **Delete** it.

9.5.1 Adding New Terminal Action Nodes

To add a new terminal action node:

1. Click on **Add Action** from the header options and select from **Folder**, **Print**, **Copy**, **Scan**, **Fax**, and **Others**.

2. Your new terminal action is created, you can now use the content menu on that action's icon to **Edit** the action or drag and drop it to change its position or place it into a folder.

Duplicating a terminal action

To create a new terminal action with the same general settings and parameters as an existing action, duplicate the action.

1. Click the three-dot-menu for the action that you want to duplicate.
2. Click Duplicate.

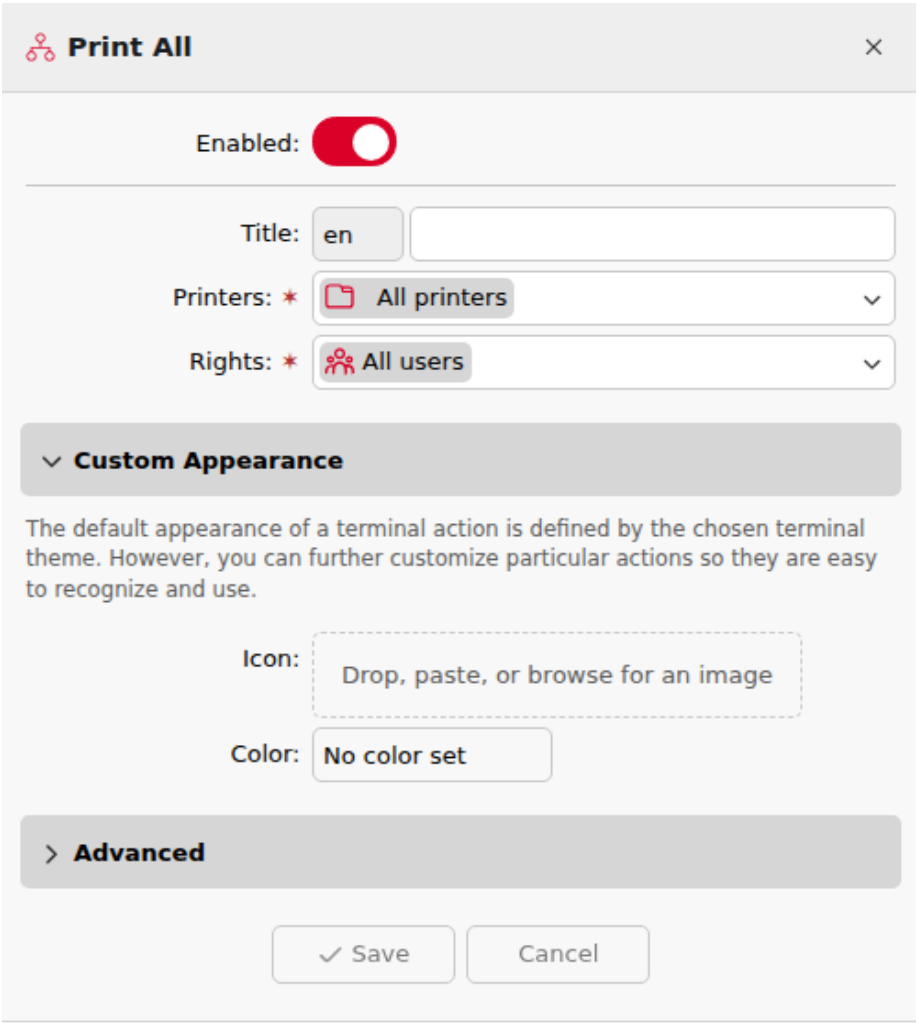
   A new terminal action appears with the name of the source action, followed by a number in parentheses.

> You cannot duplicate native panel actions or special purpose actions such as **Print All** or **My Jobs**.

9.5.2 Editing Terminal Action Nodes

Each action can be edited from its properties panel. To access the panel, double-click the terminal action node on the list of nodes or on the terminal screen preview. On the properties panel, you can see up to three settings tabs (depending on the particular action): **General**, **Destinations**, and **Parameters**. The Destinations and the Parameters tabs are mostly used in Easy Scan action nodes and are described there. See Easy Scan Settings (see page 328).

General Tab



- **Enabled**: If you disable the node, it is not displayed on the terminal and cannot be used there.
- **Title**: Allows you to change the action node's name. If you do not change it, the default name is used. Depending on the number of additional languages set on the MyQ Web administrator interface, you can use different names in different languages (additional languages can be set on the MyQ **General** settings tab.)
- **Printers**: Allows you to select the printers the action node will be available on. All printers are assigned by default. To add more printers, select them from the **Printers** drop-down.
- **Rights**: Allows you to select the users or the groups of users that will be able to see and use the action node. According to this setting, the layout and available features of the embedded terminal can vary depending on user's rights to particular nodes. By default, the right to see the node is given to all

users. To provide an additional user or a group of users with rights to the action node, select the user or group from the **Rights** drop-down.

- **Custom Appearance**: This option allows you to change the icon displayed for this terminal action. You can either Browse for a file on your device, drag and drop an image file onto the selector, or Paste a file from your clipboard. File types .jpg, .png, .gif, and .bmp can be used. The selected image will be re-sized automatically, and if it contains transparent space, the selected icon Color will be visible in the transparent parts of the image. In addition, you can select the custom color that will be displayed behind the icon.
- **Advanced/Reference**: This option allows admins to force extra features on the terminal, providing enhanced functionality and customization for various terminal actions. The value stored in the `Advanced/Reference` field is accessible through the MyQ X API, allowing for seamless integration and retrieval of terminal action data.

> ⚠ **Titles**, **Custom Icons**, and **Custom Colors** set here will override those set in the Terminal Theme Editor. See Terminal Theme Editor (see page 185).

9.5.3 Changing the Terminal Action Nodes Layout

To change the action nodes layout, simply drag and drop the action nodes on the terminal preview, their new order will be reflected in the left-hand panel.

Actions can be placed in a folder by drag and drop on the terminal action preview or using the same method in the left-hand panel.

If there are more than ten action nodes defined on the home screen or in any folder, move the scroll bar at the bottom of the preview screen to view the additional action nodes.

9.5.4 Deleting Terminal Action Nodes

You can delete terminal action nodes either from the action nodes list or from the terminal screen preview. Both actions have the same result: when you delete the node, it is removed from both locations.

Deleting Action Nodes from the Home Screen List

On the list of actions on the **Terminal Actions** settings tab, right-click the action node that you want to delete, and then click **Delete** on the shortcut menu. The action node disappears both from the list, and the terminal screen preview.

9.5.5 Restoring the Original Layout

On the bar at the top of the **Terminal Actions** settings tab, click **Tools**, and then click **Restore defaults…**. All your layout changes are reverted to the default settings.

9.5.6 Vendor Compatibility Specifics

Terminal actions compatibility may be different between brands. Check the respective Embedded Terminal guides for details:

- MyQ Brother Embedded
- MyQ Canon Embedded
- MyQ Epson Embedded
- MyQ Fujifilm Embedded
- MyQ HP Embedded
- MyQ KATUN Embedded
- MyQ Kyocera Embedded
- MyQ Kyocera Embedded Lite
- MyQ Lexmark Embedded
- MyQ Ricoh SmartSDK Embedded
- MyQ Sharp Embedded
- MyQ Sharp Luna Embedded
- MyQ Toshiba Embedded
- MyQ Xerox Embedded

9.5.7 User Connection to Cloud Storages

In order to use many cloud storage locations as a destination for Easy Scan, or source for Easy Print, individual users must connect their MyQ account to their personal cloud storage. The methods described below allow users to connect to:

- OneDrive
- OneDrive for Business (if connection was created manually and the option **Application has access to OneDrive for Business of all users** was not checked)
- Google Drive
- Box
- Dropbox
- SharePoint Online

If certain conditions are met, users will be able to connect their MyQ account to any cloud storage listed above. The conditions are:

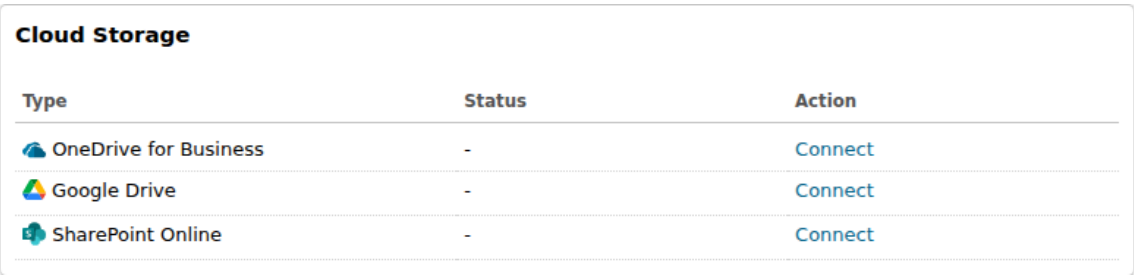
- There is at least one Easy Scan or Easy Print terminal action with this destination.

- The user has rights to see the Easy Scan or Easy Print button or is connected to cloud drive.

Users can then connect their cloud storage in one of two ways:

Via Home Screen Widget

After logging into their MyQ account, users with unconnected cloud storages will see a **Cloud Storage Widget** on their **Home** screen.



They simply need to click connect in this widget and follow the on-screen prompts to connect.

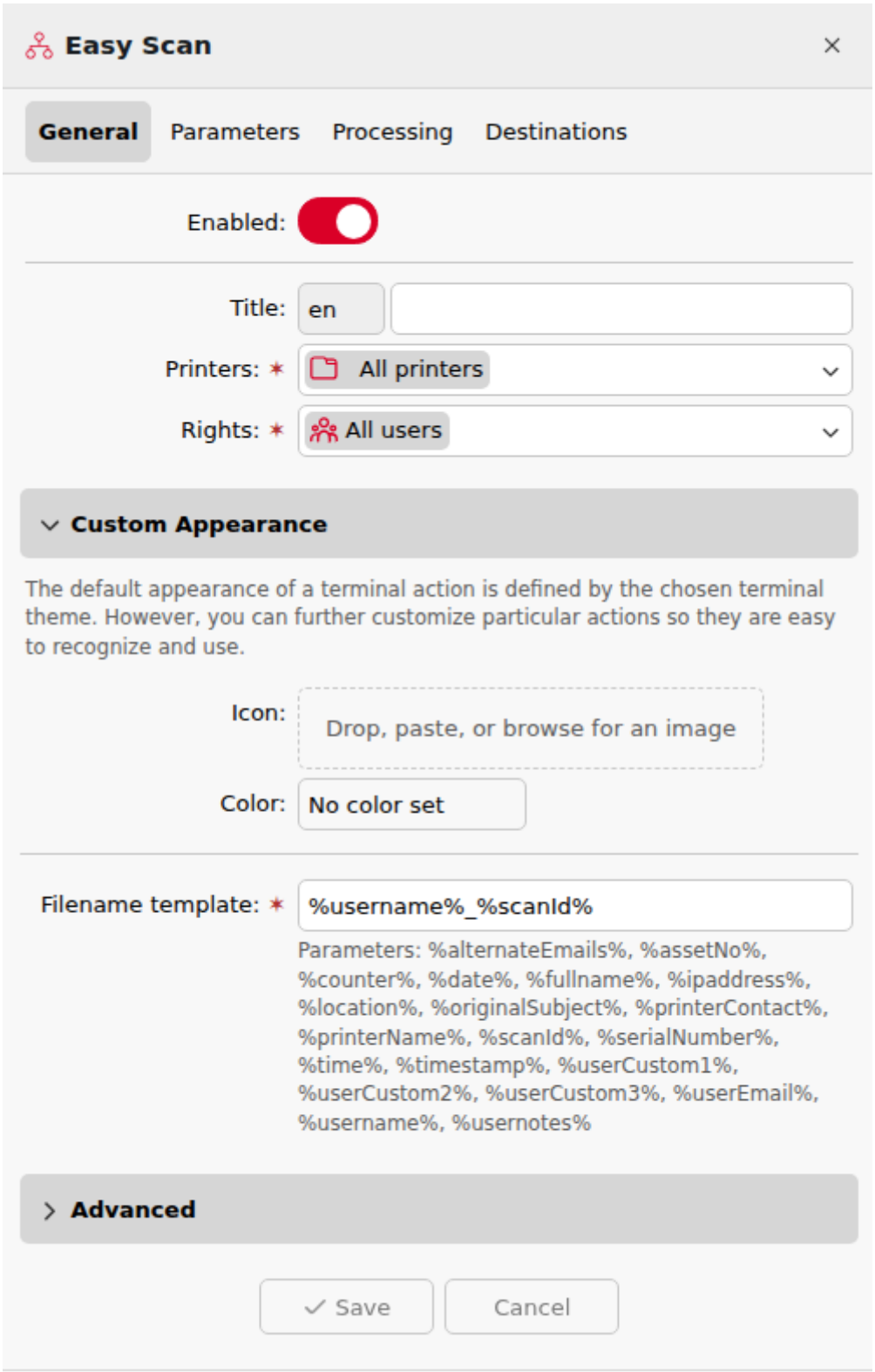
Via Email

If a user attempts to Easy Scan to or Easy Print from a cloud storage which is not connected, they will receive an automated email prompting them to connect.

They simply need to select **Connect [cloud storage]** in this email and follow the on-screen prompts to connect.

9.5.8 Easy Scan Settings

This section describes the settings needed to enable the **Easy Scan** action and define its
destinations and parameters. They can be changed on three tabs on the **Easy Scan** properties panel: **General**, **Destinations**, and **Parameters**.


Easy Scan
General
Parameters
Processing
Destinations
Enabled:
Title:
en
Printers: *
All printers
Rights: *
All users
Custom Appearance
The default appearance of a terminal action is defined by the chosen terminal theme. However, you can further customize particular actions so they are easy to recognize and use.
Icon:
Drop, paste, or browse for an image
Color:
No color set
Filename template: *
%username%_%scanId%
Parameters: %alternateEmails%, %assetNo%, %counter%, %date%, %fullname%, %ipaddress%, %location%, %originalSubject%, %printerContact%, %printerName%, %scanId%, %serialNumber%, %time%, %timestamp%, %userCustom1%, %userCustom2%, %userCustom3%, %userEmail%, %username%, %usernotes%
Advanced
Save
Cancel

The properties panel is automatically opened after the **Easy Scan** action node is created. You can also access it by double-clicking the terminal action node on the list of nodes or on the terminal screen preview.

See also:

- Terminal Actions (see page 322)
- Easy Scan Parameters (see page 330)
- Easy Scan Destinations (see page 342)
- Easy Scan Processing (see page 340)

General Limitations

- Not all Easy Scan parameters are supported by all vendors/machines.
- The "Allow custom values", "Allow multiple values" server scan settings are not supported automatically, they need to be enabled by the server administrator.
- Easy Scan supports only one folder-browsable destination, all the rest of the connected destinations on the server are supposed to work as they worked before.

Vendor Compatibility Specifics

Easy Scan compatibility may differ between brands. Please check the relevant terminal documentation for more details.

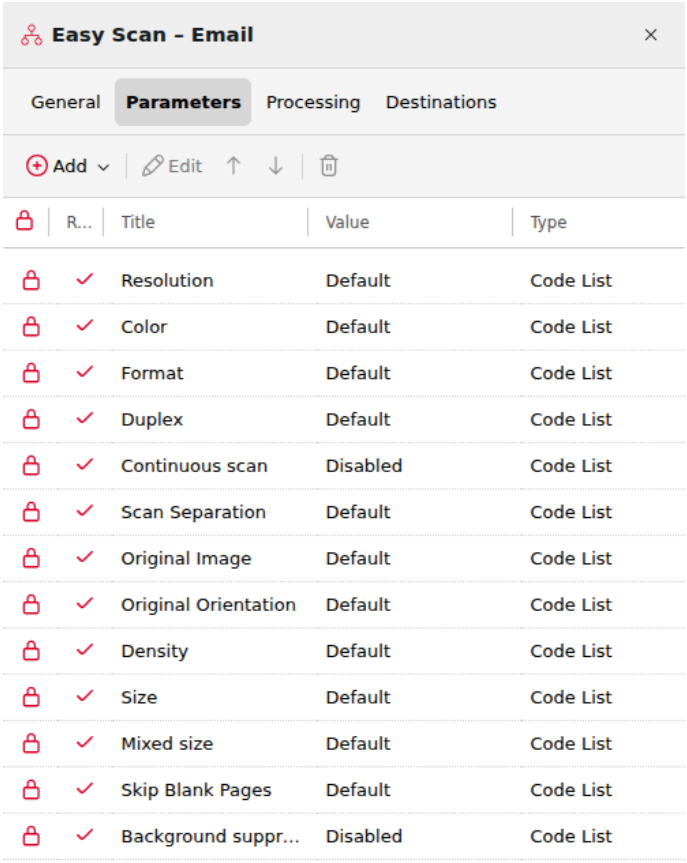
- MyQ Brother Embedded
- MyQ Canon Embedded
- MyQ Epson Embedded
- MyQ Fujifilm Embedded
- MyQ HP Embedded
- MyQ KATUN Embedded
- MyQ Kyocera Embedded
- MyQ Kyocera Embedded Lite
- MyQ Lexmark Embedded
- MyQ Ricoh SmartSDK Embedded
- MyQ Sharp Embedded
- MyQ Sharp Luna Embedded
- MyQ Toshiba Embedded
- MyQ Xerox Embedded

Easy Scan Parameters

On the **Parameters** tab, you can set the scanned file's parameters, such as resolution and format. You can select from a number of options for each parameter.

There are predefined parameters, but you can also create your own parameters.

> ⚠ All parameters are dependent on the particular printing device type. Therefore, some parameters and/or values might not be available.



Some parameters (e.g. resolution, color) significantly influence the scanned file's size. For example, a combination of higher resolution and full color will dramatically increase the file size.

You can allow users to change their scan settings from the terminal screen.

To do this, you have to modify the settings of the particular parameter on the **Parameters** tab on the **Easy Scan** action node properties panel. Open the parameter properties panel, uncheck the **Read Only** option (checked by default) and **Save**.

Predefined Parameters

Each parameter has a *Default* option. If selected, the actual values are taken from the default scan settings of the printing device.

- **Resolution** - The outgoing file's resolution. You can select from the following options:
  - 100 dpi
  - 200 dpi
  - 300 dpi
  - 400 dpi
  - 600 dpi
  - 1200 dpi
  - Default
- **Color** - The outgoing file's color scale. You can select from the following options:
  - Color
  - Grayscale
  - B&W (two tones)
  - Automatic
  - Default
- **Format** - The outgoing file's format. You can select from the following options:
  - PDF
  - JPEG
  - TIFF
  - XPS
  - HCPDF
  - Default
- **Duplex** - Simplex and Duplex scanning options. You can select from the following:
  - Single Sided
  - Duplex - binding on top
  - Duplex - binding on side
  - Booklet - binding on left
  - Booklet - binding on right
  - Default
- **Continuous scan** - With the continuous scan option *Enabled*, scan jobs are not sent until **Done** is tapped. After clicking **Scan**, the printing device scans another page.
  You can select from the following:
  - Disabled
  - Enabled
  - Default

- **Scan Separation** - If a document with multiple pages is scanned, scanned pages can be stored either separately (each page in a separate file) or all together in one file. You can select from the following options:
    - All pages together
    - Separate each page
    - Default
- **Original Image** - Determines the way in which the printing device is going to process the scanned page. You can select from the following options:
    - Text + Photo
    - Photo
    - Text
    - Default
- **Original Orientation** - Determines the scanned page's orientation in the outgoing file. The paper's position is relative to the person standing at the printing device. You can select from the following options:
    - Top Edge on Top: The page is displayed in a horizontal position (top edge of the page opposite to the person)
    - Top Edge on Left: The page is displayed in a vertical position (top edge of the page on the left hand side of the person)
    - Default
- **Density** - The picture's density in the outgoing file. The higher it is, the darker the resulting picture is. You can select from the following options:
    - Automatic
    - Lowest
    - Lower
    - Low
    - Normal
    - High
    - Higher
    - Highest
    - Default
- **Size** - The scanned output's size. This determines the size of the scanning area, therefore it should correspond to the actual size of the scanned paper. You can select from the following options:
    - Automatic
    - A3
    - A4
    - A5
    - A6
    - B4
    - B5
    - B6

    - Folio
    - Ledger
    - Letter
    - Legal
    - Oficio II
    - Statement
    - Default
- **Mixed Size** - This parameter enables automatic paper size recognition when different sizes of paper are used during scanning. To be able to use the **Mixed size** setting, the *A4*, *A3*, *Ledger* or *Letter* option must be selected in the **Size** setting. You can select from the following options:
    - On: The **Size** parameter is ignored and the size of each scanned image is recognized by the printing device.
    - Off: The **Size** parameter is used to decide the size of the scanned image.
    - Default
- **Skip blank pages** - With this parameter, you can select to skip blank pages in the scanned document. You can select from the following options:
    - Default
    - Yes
    - No

The additional parameter **Background Suppression** is available on Xerox terminals only.

- **Background Suppression** - Enabling this parameter will help to clear a scan or copy background when the original paper is tinted (this is common in eco friendly paper). You can select from the following options:
    - Default
    - Enabled
    - Disabled

Create Custom Parameters

You can create new parameters to be used in the scan metadata, or as parts of file names, addresses, subjects and email bodies, and as paths to folders, passwords to folders etc.

The following parameter types can be created: *Text, Password, Yes/No, MyQ Users, Code Book, User Properties, Device Properties, Address Book*.

To create a custom parameter:

1. On the action node properties panel, go to the **Parameters** tab.

2. On the tab, click **+Add**. The new Parameter properties panel opens on the right side of the screen.
3. Set the parameter, and then click **Save**. The new parameter is now displayed on the list on the **Parameters** tab.

Parameter Settings:

- **Title** - The parameter's name.
- **Type** - Select the parameter's type from the drop-down:
  - *Text* - Text (string) typed by the user on the embedded terminal. You can use these parameters in a variety of strings in MyQ: names of files, addresses, subjects or email bodies, paths to folders and many other. In the **Validator** field, regular expressions can be used to define or limit the user's input.
  - *Yes/No* - Boolean parameter with the options: *Yes, No.* You can use these parameters in the scan metadata file to provide answers on Yes-No questions concerning the scan, such as if the scan is private or if it should be archived.
  - *MyQ Users* - This parameter enables selecting scan recipients from the list of all MyQ users. The scan is sent to the recipient primary email set in the Email text box on their properties panel on the Users main tab of the MyQ Web Interface, or to the folder set in the Folder or email for storing scanned documents text box in the same location.
  - *Code Book* - The parameter uses a list of values from internal code lists. Users can select options from lists of values used in metadata and destinations.
    - **Internal code list**: You can predefine code lists with values and use the values as options available for users.
    - **LDAP sourced list**: This parameter enables selecting scan recipients directly from an LDAP server by importing the codes from the server.
    - **MS Exchange Address Book**: You can use this code book to get personal contacts from an MS Exchange server. The contacts are retrieved using an account defined by the administrator in the MyQ Web UI. This account requires special rights on the MS Exchange server that allow it to access other users' mailboxes. The user sees the first 50 contacts on the terminal. To look for more contacts they would have to use the search function.
  - *User Properties* - The parameter can represent MyQ user properties within the metadata file of the scanned document. You can select one of the following values to be represented by the parameter:
    - User name

        - Full name
        - Email
        - User's storage
        - Personal number
        - Phone
        - Notes
        - Accounting Group
    - *Device Properties* - The parameter can represent MyQ printing device's properties within the metadata file of the scanned document. You can select one of the following values to be represented by the parameter:
        - Name
        - Location
        - IP address
        - Brand
        - Model
        - Serial number
        - Asset number
        - Notes
    - *Address Book* - The parameter enables users to manage scan and fax recipients seamlessly via their personal address book.
        - Allow multiple values
        - Allow custom values
- **Default value** - A predefined value/option that will be used if nothing else is selected.
- **Required** - The parameter value has to be defined. If the parameter does not have a default value, users are not allowed to print before this value is entered in the particular text box on the terminal screen.
- **Read Only** - If this option is selected, the parameter cannot be changed by the users on the terminal screen.
- **Reference** - String that is used as a reference to the parameter. A parameter with the *parameterX* reference is referred to as *%parameterX%* in MyQ. For example, the reference of the often used user name parameter is *username*; the parameter is referred to as *%username%*.

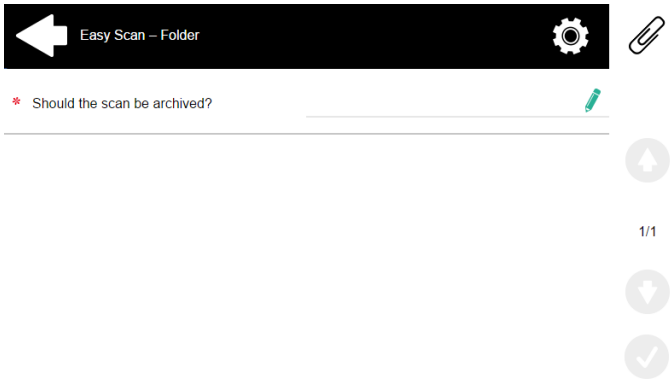
Custom Parameters Examples

These are some examples of using custom parameters.

Providing Additional Information in a Metadata File

In this example, you can see how to use parameters for obtaining additional information about the scan file or any other data provided by users. The parameter's **Type** can be *Text* or *Yes/No*.

As an example, we will create a *Yes/No* **Type** parameter, called **Should the scan be archived?**.



1. The **Title** will be shown on the screen, therefore we name it **Should the scan be archived?**.
2. The **Type** is *Yes/No*.
3. **Default value** is left unchecked.
4. **Read Only** is left unchecked.
5. We do not have to use the reference, as the parameter is not going to be used in any string in MyQ. Therefore, we can **Save** the parameter settings.

The following examples show possible values of the **Should the scan be archived?** parameter. A DMS software can automatically archive the scans with value *1* into a predefined folder.

```
<field>
  <name>Should the scan be archived?</name>
  <reference/>
  <value/>
</field>
```

```
<field>
  <name>Should the scan be archived?</name>
  <reference/>
  <value/>1</value>
</field>
```

Enabling Users to Scan to Their Home Folder Protected by Password

If you do not want to give to the MyQ server universal access to users' shared folders, but instead want to provide each user with separate rights to access their shared folder from MyQ, you can enable the scanning users to enter the password to their LDAP domain account to access the shared folder there.

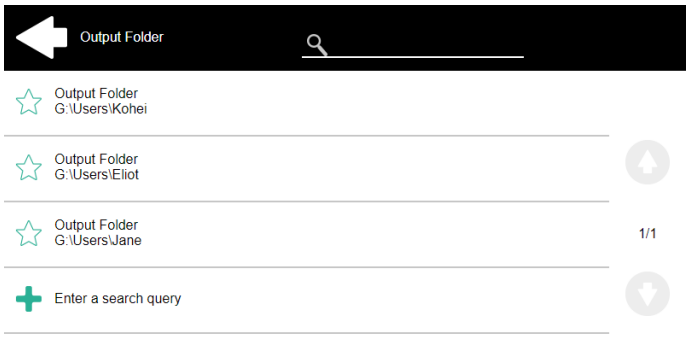
To be able to access their shared folders, users should have the LDAP domain defined in MyQ. The information about the domain is taken either from the **Authentication server** setting on the user's properties panel in MyQ, or from the user's MyQ user name (if the name is in the form *LDAPusername@domain.local*).

Users can **Connect** to their folder by entering the password in their MyQ Web Interface, or by email after completing a scan to this destination. then MyQ takes the name of the user's domain (either from the **Authentication server** setting, or from the back part of the user name) and attempts to log on the user's account on this domain (either the whole user name, or its front part). If the password is correct, MyQ saves the scan in the shared folder; otherwise it displays the error message "*Error while delivering a scan X/Y. Unable to write to the folder.*".

On the **Destinations** tab, set the **User's storage** destination type. In the **Parameters** section, select **Connect as: MyQ Print Server service** option and **Make the user doing the scan the owner of the file**.

Enabling Users to Select the Output Folder from a Code Book

In this example, you can see how to enable users to select the scan destination folder from a predefined code book. For this example, we have already created and saved the Easy Scan action node, and we have created a code book named *Folders*, which has names of folders as its values. The next step is to add and set up a new **Code Book** type parameter and a new **Folder** destination type for the Easy Scan action. The parameter is then used as a part of the path to the folder.



On the **Parameters** tab create a parameter with the following settings: **Title**: Output folder, **Type**: Code Book, **Code Book**: Folders, **Default value** (optional), **Read Only**: deselect, **Reference**: folder. If you want to allow users to select multiple recipients, select **Allow multiple values**.
If you want to allow users to enter their own value, select **Allow custom values**. If you don't want to allow empty values, select the **Required** option so that users have to enter its value before sending the file. Optionally, you can select a default value to define the folder where the output files will be saved, if users don't change it.

On the **Destinations** tab, create and set up a new destination. For this destination, you can use the parameter as any part of the destination path set in the **Destination folder** text box. To use the parameter, enter its reference name bounded in percentage signs as part of the path. In our example, we used a parameter with the reference name *folder* as the folder where the files are stored (*Users%folder%*).

Enabling Users to Search Recipients via LDAP Source Code Books

In this example, you see how to enable users to search for recipients on LDAP servers via LDAP Source code books. LDAP Source code books contain two parameters: **Title** and **Value**. The value of the **Title** parameter is used as an input for searching in the LDAP database and the **Value** parameter defines the value returned by the database. We use an LDAP Source code book with the **cn** attribute assigned to the **Title** parameter and the **mail** attribute assigned to the **Value** parameter. We also create a new parameter and a new folder destination for the feature. The scanning user types a string to be used in a search query. MyQ sends the query to the LDAP database to search for user accounts, whose **cn** begins with the entered string. The scanning user can select from the returned accounts. After they select the account, the value of the **mail** attribute of the account is used as the scan destination.

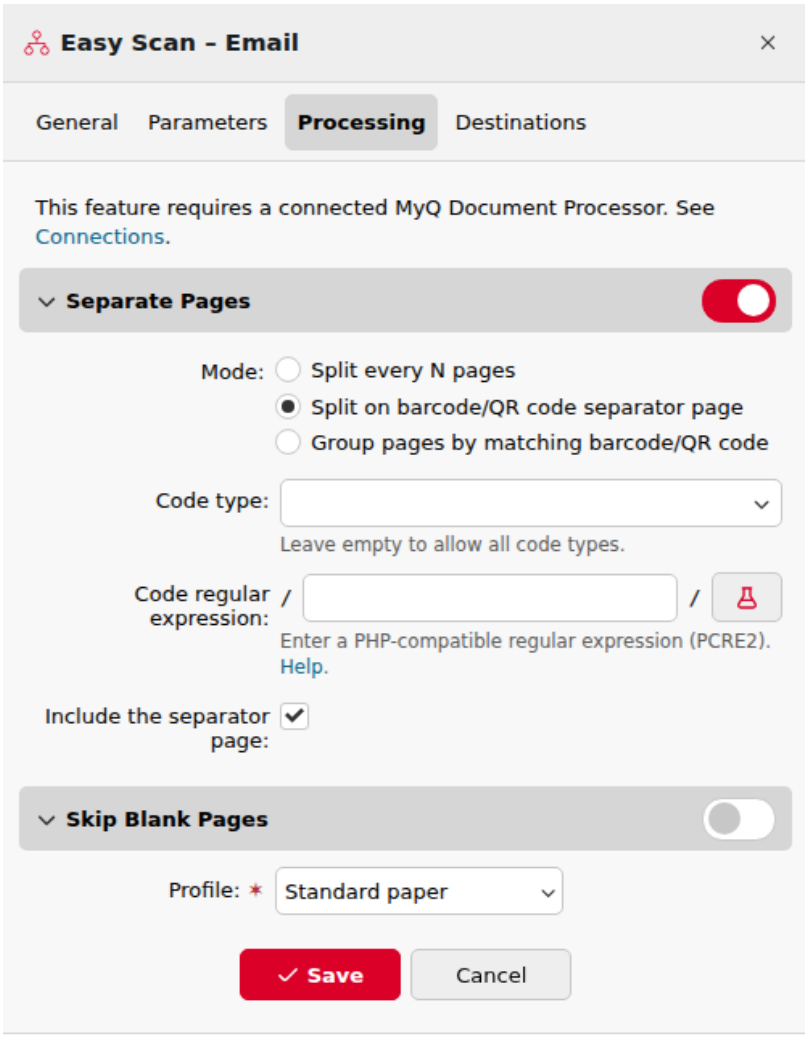
On the **Parameters** tab, create a parameter with the following settings: **Title**: Recipients, **Type**: Code Book, **Code Book**: Addresses (or the LDAP source code book that you want to use), **Read Only**: deselect, **Reference**: recipients. If you want to allow users to select multiple recipients, select **Allow multiple values**. If you want to allow users to enter their own value, select **Allow custom values**. If you don't want to allow empty values, select the **Required** option so that users have to enter its value before sending the file.

On the **Destinations** tab, create an **Email** destination type and enter the parameter in the **Recipient** text box, enclosed in percent signs (*%recipients%*).

Easy Scan Processing

The **Processing** tab configures document processing options for the Easy Scan action. These options are handled by the MyQ Document Processor service. To use any processing option, you must have at least one MyQ Document Processor connection configured in **MyQ > Settings > Connections**.

⚠ If any processing option is enabled, the Format parameter on the Parameters tab must be set to an OCR profile of type MyQ Document Processor.



Separate Pages

Use these options to automatically split a scanned multi-page document into separate
output files.

Split Every N Pages

Splits the scanned document into separate files after every N pages. Set the value of N to define the page interval.

Split on Barcode/QR Code Separator Page

Splits the scanned document when a page containing a recognized barcode or QR code
is detected. The barcode or QR code on that page acts as a separator between documents.

- **Code types:** Select which barcode or QR code types to recognize. The following
  types are supported:
  - AZTEC
  - CODABAR
  - CODE_39
  - CODE_93
  - CODE_128
  - DATA_MATRIX
  - EAN_8
  - EAN_13
  - ITF
  - MAXICODE
  - PDF_417
  - QR_CODE
  - RSS_14
  - RSS_EXPANDED
  - UPCA
  - UPCE
- **Code value (regex):** Optionally, enter a regular expression to filter which barcode values trigger a split. Only barcodes whose decoded text matches the expression will be used as separators.
- **Include separator page in split document:** If enabled, the page containing the separator barcode is included as the first page of the new output document. If disabled, the separator page is excluded from all output documents.

Group Pages by Matching Barcode/QR Code

Splits the scanned document so that pages containing the same barcode or QR code value are grouped into the same output file. A page with no recognized code is treated as having the same code as the previous page.

- **Code types:** Select which barcode or QR code types to recognize. See the list of supported types above.
- **Code value (regex):** Optionally, enter a regular expression to filter which barcode values are used for grouping.

Skip Blank Pages

When enabled, blank pages are automatically detected and removed from the scanned
output before processing. This prevents blank pages with punch holes or staple marks from being included unnecessarily. Select a paper profile that best matches the type of paper you need to scan.

The available profiles are:

- Standard paper
- Standard paper - staple
- Standard paper - punch
- Eco paper
- Eco paper - staple
- Eco paper - punch

See also:

- Connect to MyQ Document Processor (see page 201)
- (10.3) MyQ Document Processor
- OCR Profiles (see page 620)

Easy Scan Destinations

On the **Destinations** tab of the Easy Scan action node properties, you can define where the scanned file is sent.

To add a new destination, click **+Add**, multiple destinations can be added to one Easy Scan action. The Destination panel opens where you can set a target destination. Some destinations are available by default, others become available after certain

connections are established in **Network > Connections**. The available destinations are:

- Cloud storage
- eGoldFax
- Email
- Fax Server
- Folder
- FTP
- RightFax
- Secured link
- User’s email
- User’s storage
- Scan Review

Depending on the selected destination type, the panel contains the **General**, **Parameters** and **Advanced** sections.

General Section

- **Title**: Enter a title for the destination which will help distinguish it from other options.
- **Attach metadata file**: When selected, MyQ sends the scanned file with an XML file attachment, containing the scanned file's metadata.
- **Filename template**: Choose how the scanned file is named from the options:
  - **Default**: A combination of parameters set on the Actions **General** tab, when **Default** is selected, you can also enable **Allow to edit the filename**, which means users can edit filenames on the terminal.
  - **Custom**: Choose a new combination of parameters specific for files scanned to this destination.

Parameters Section

This section depends on the selected destination type. The available fields differ for each type. Some types share parameters, and some use unique parameters. Custom parameters can also be created, in the **Parameters** tab.

When setting up a cloud storage destination there is an additional option to allow users to **Browse folders**. If the type of cloud storage selected is External storage API, you can also enable or disable the option to **Delete files**.

Shared Parameters

Parameter	Description
%alternateEmails%	The value is taken from the **Alternate Emails** field of the user's properties panel.
%username%	The value is taken from the **User name** field of the user's properties panel.
%fullname%	The value is taken from the **Full name** field of the user's properties panel.
%userCustom1%	The value is taken from the **Custom 1** field of the user's properties panel.
%userCustom2%	The value is taken from the **Custom 2** field of the user's properties panel.
%userCustom3%	The value is taken from the **Custom 3** field of the user's properties panel.
%userEmail%	The value is taken from the **User Email** field of the user's properties panel.
%usernotes%	The value is taken from the **User Notes** field of the user's properties panel.
%timestamp%	Date and time of the scan.
%date%	Date of the scan.
%time%	Time of the scan.

Parameter	Description
%originalSubject%	This value is taken from the subject set on the printing device.
%ipaddress%	This value is taken from the **IP address/Hostname** field of the printing device's properties panel.
%scanId%	This value is an unique scan identification number generated on the MyQ server.
%printerName%	This value is taken from the **Name** field of the printing device's properties panel.
%location%	This value is taken from the **Location** field of the printing device's properties panel.
%serialNumber%	This value is taken from the **Serial number** field of the printing device's properties panel.
%assetNo%	This value is taken from the **Asset number** field of the printing device's properties panel.
%printerContact%	This value is taken from the **Contact** field of the printing device's properties panel.

Unique Parameters

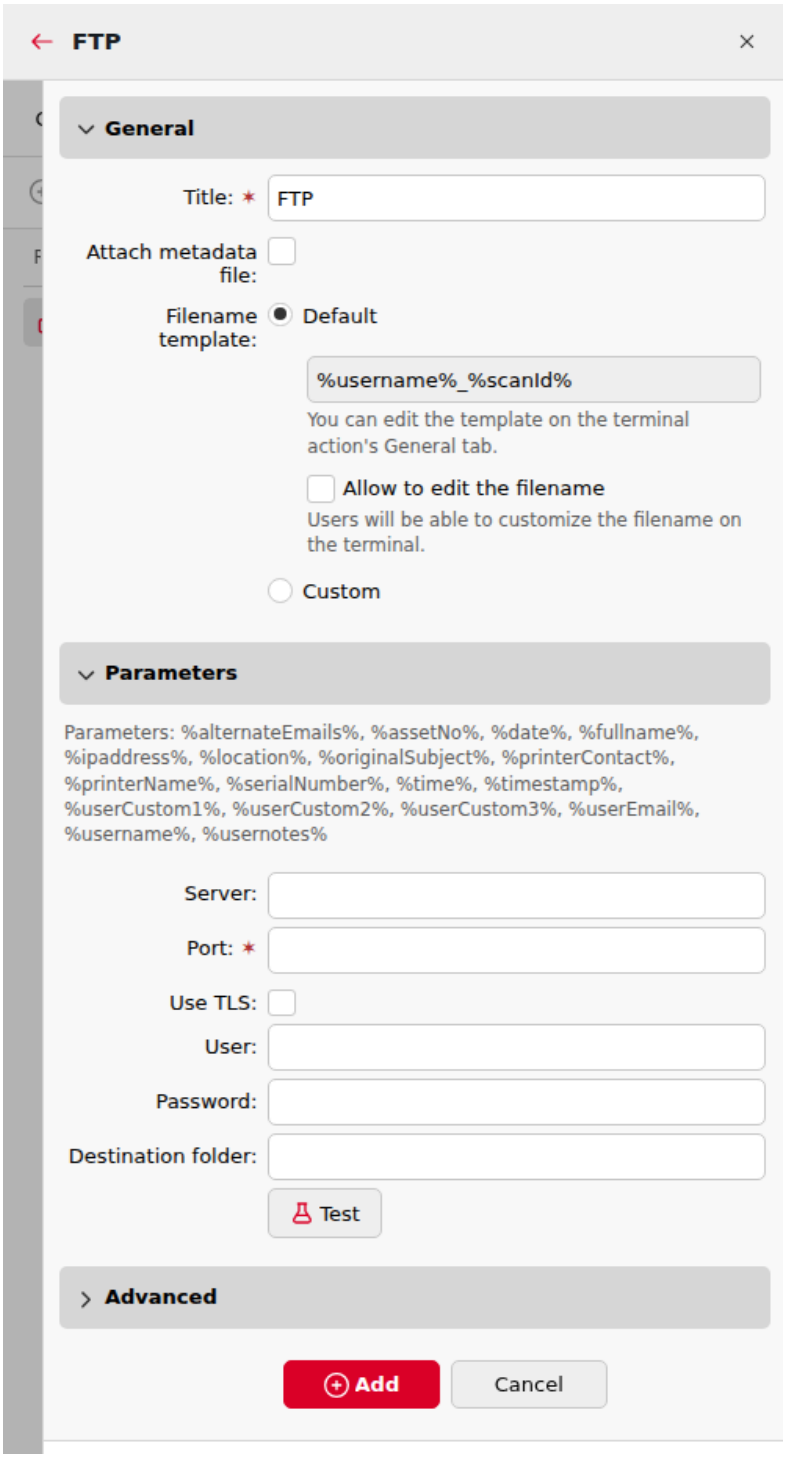
Parameter	Description
%counter%	If the **Scan Separation** parameter is set to **Separate each page**, this value shows the number of scanned pages. This parameter can be used only to create the filename template.
%originalBody%	This value is taken from the signature set on the printing device. It is used in the **User's email** destination type only.
%recipient%	The fax recipient. It is used in the **Fax Server** destination type only.
%number%	Fax number. It is used in the **Fax Server** destination type only.
%empty%	This parameter is used in the **Fax Server** destination type only. It ensures that the subject/message is empty; it is used in very specific cases.
%faxNumber%	RightFax fax number. This parameter has type Text and it is used in the **RightFax** destination type only.
%phonebook%	RightFax phonebook. This parameter has type Code Book and it is used in the **RightFax** destination type only.
%phonebookGroups%	RightFax phonebook groups. This parameter has type Code Book and it is used in the **RightFax** destination type only.

Advanced Section

This section contains the field **Metadata generator**, where a PHP class for custom data processing can be added.

Scan to FTP

Scanned documents can be sent to a folder defined on an FTP server.



Setting the connection in the **Parameters** section:

- **Server**: Enter the IP address or hostname of the FTP server
- **Port**: Enter the port used for the FTP protocol, the default port is *21*
- **Use SSL**: Select if you want to use secure communication
- **User**: Name of the user with an account on the server

- **Password**: The user's password
- **Destination folder**: You can specify the subfolder where the outgoing scan files will be stored (optional).

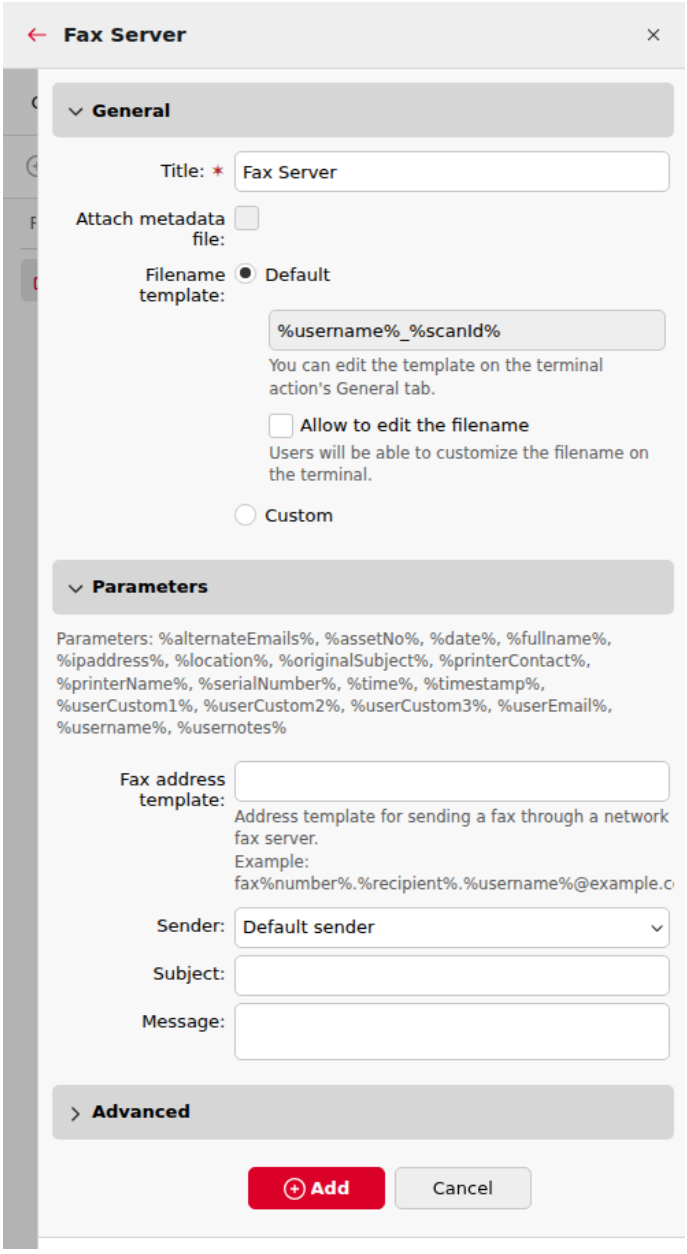
You can use the following parameters when defining the destination folder:

- *%username%*: User name of the user session owner
- *%fullname%*: Full name of the user session owner
- *%date%*: Date and time when the scan was taken
- *%originalSubject%*: The default subject set on the printing device
- *%ipaddress%*: IP address of the printing device
- *%scanId%*: Unique scan identification number generated on the MyQ server

After you fill the required parameters, you can click **Test** to test the FTP connection. MyQ tries to upload a dummy file named *rightsCheck.dat* to the defined destination folder under the defined user name and password, and informs you about the result.

Scan to a Fax Server

Scanned documents can be sent as emails to a fax server, which processes them and sends faxes to appropriate Fax numbers.



To send the document to a fax server, enter the appropriate email address template in the **Fax address template** field. You can use the following parameters:

- *%username%*: Name of the user session owner
- *%recipient%*: Fax recipient
- *%number%*: Fax number
- *%empty%*: This parameter ensures that the subject/message is empty; it is used in very specific cases
- *%ipaddress%*: IP address of the printing device
- *%scanId%*: Unique scan identification number generated on the MyQ server

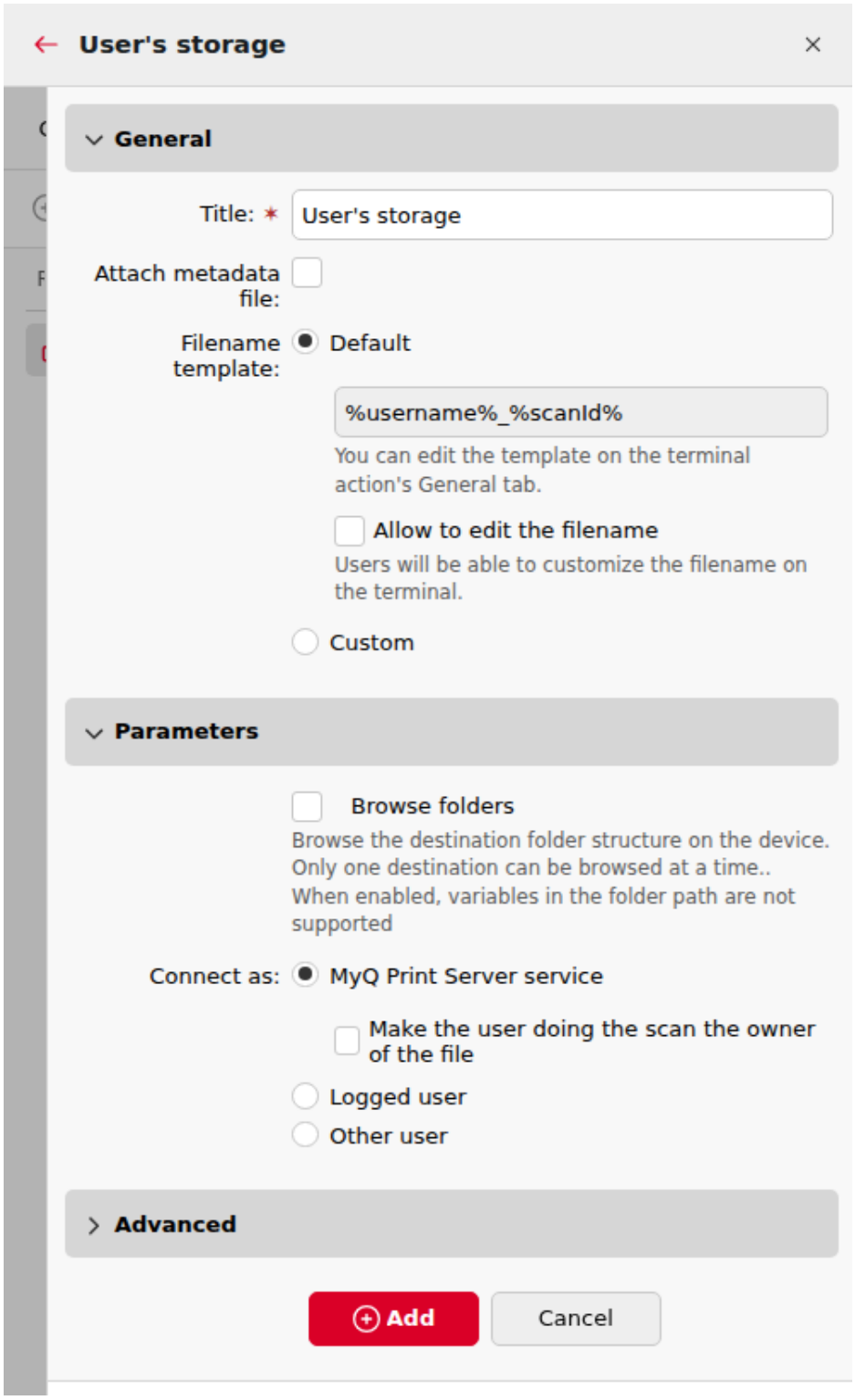
In the **Sender** drop-down, you can select one of the following addresses to be used as the fax sender:

- *Default sender*: The email set on the Network settings tab, under Outgoing SMTP server
- *MyQ@MyQ.local*: The sender is defined as *MyQ@MyQ.local*
- *Logged user*: Name of the user session owner
- *Printer contact*: The printing device contact email address set on its Web User Interface

You can also define the email's subject in the **Subject** text box, and the email's body in the **Message** text box.

Scan to User's Storage

Outgoing scan files are stored in the folder set in the **User’s storage** field on the **General** tab of a user’s properties.



Select the **Browse folders** option so users can browse one of their cloud destinations folder on the device.

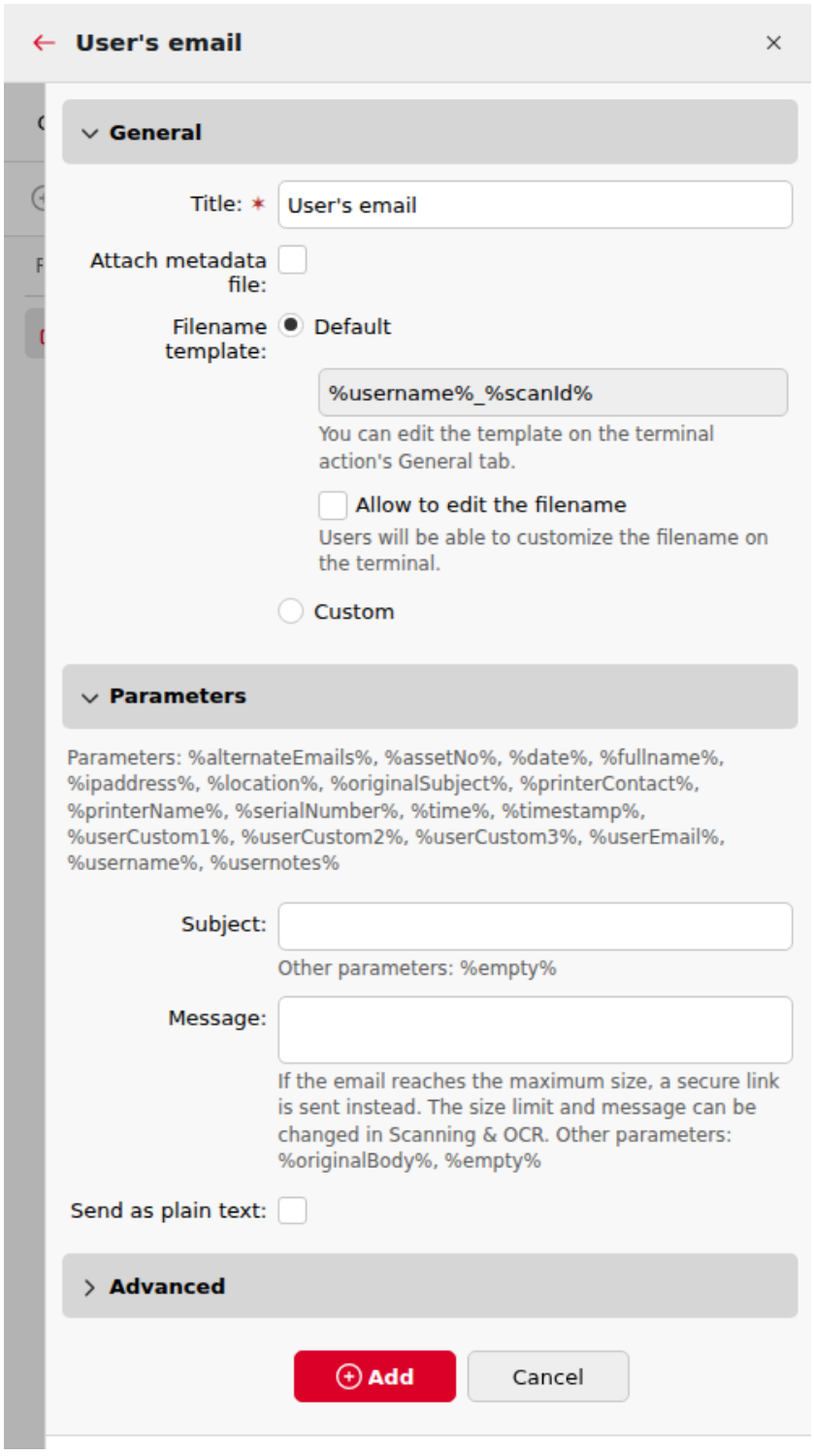
The **Connect as** parameter determines which account is used to access the destination folder and which account is recorded as the owner of the scanned file.

Option	Access	File owner	Description	When to use
MyQ Print Server service	MyQ service account	MyQ service account	MyQ accesses the destination folder using the account running the MyQ service.	Central or shared scan folders
Make the user doing the scan the owner of the file	Destination configuration	Scanning user	Changes only the owner of the scanned file. Folder access remains unchanged.	When the scanning user should be recorded as the file owner
Logged user	Scanning user account	Scanning user	MyQ accesses a shared folder using the domain account of the scanning user.	Personal user scan folders
Other user	Specified user account	Specified user	MyQ accesses a shared folder using the configured username and password.	Shared service or department accounts

- MyQ cannot change the owner of scanned files that are stored under the **Users** folder or any of its subfolders. If you want to use the **Make the user doing the scan the owner of the file** option, use a different folder than **Users** (or its subfolders) as the scan destination.
- When the scan is done by a hybrid Entra ID user (that is, the user has **On-premises username** and **On-premises domain** populated), MyQ uses `NETBIOS\username` for filesystem authentication instead of the Entra ID UPN.

Scan to User's Email

Scans are sent to the user's primary email address set in the **Email** field on the **General** tab of a user's properties.



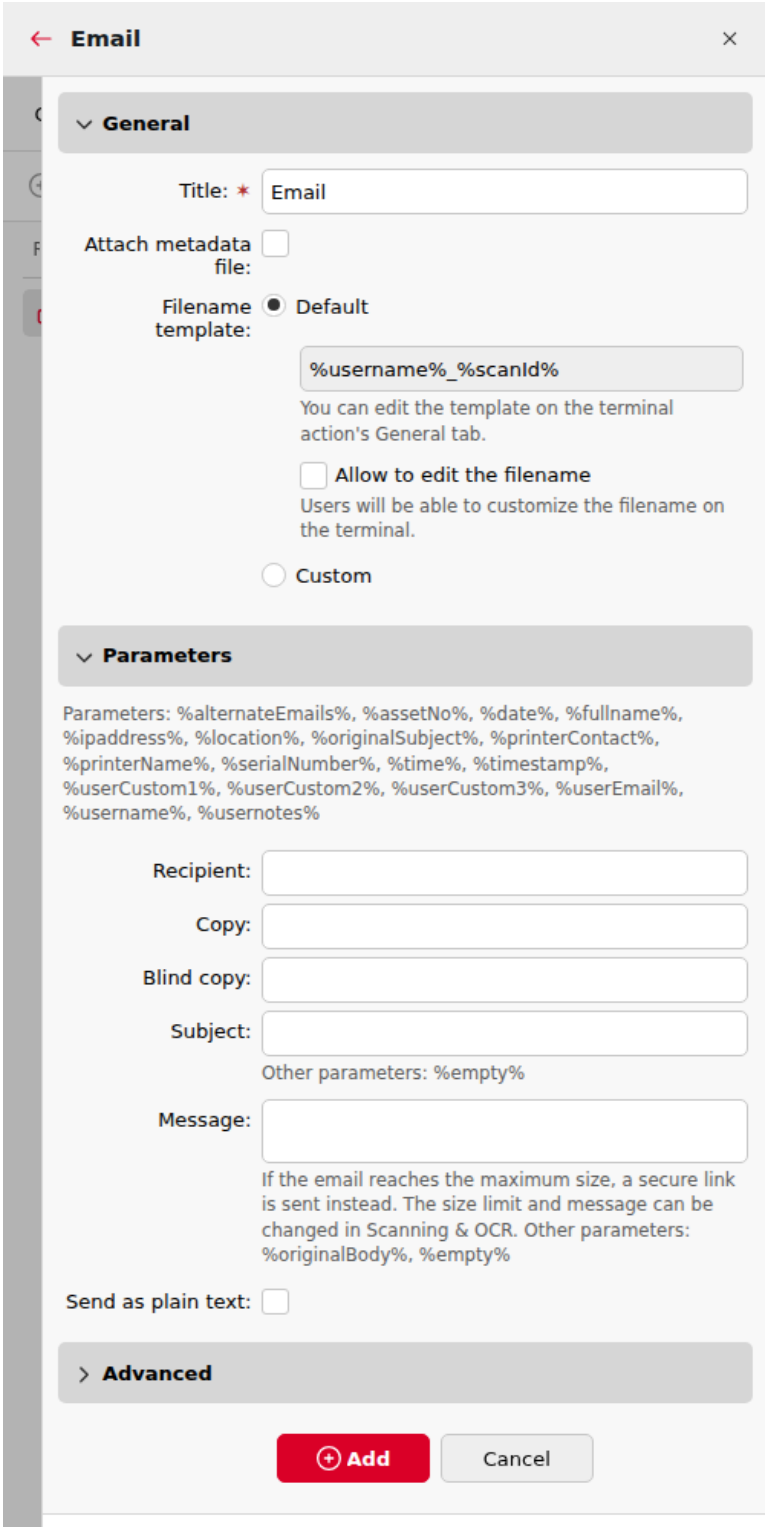
In the **Parameters** section, you can define the subject of the emails sent to this destination in the **Subject** text box, and the body of these emails in the **Message** text box. The subject or body can contain the following parameters: %alternateEmails%, %assetNo%, %date%, %fullname%, %ipaddress%, %location%,

%originalSubject%, %printerContact%, %printerName%, %serialNumber%, %time%, %timestamp%, %userCustom1%, %userCustom2%, %userCustom3%, %userEmail%, %username%, %usernotes%.

Emails with scans sent from MyQ contain graphics by default, enable the **Send as plain text** option to send these emails as plain text, which might be necessary, for example, if the email will be further processed by an automation service or fax servers.

Scan to Email

Scans are sent to the email address specified here.



In **Parameters** > **Recipient** field, you need to define the email recipient (or recipients).

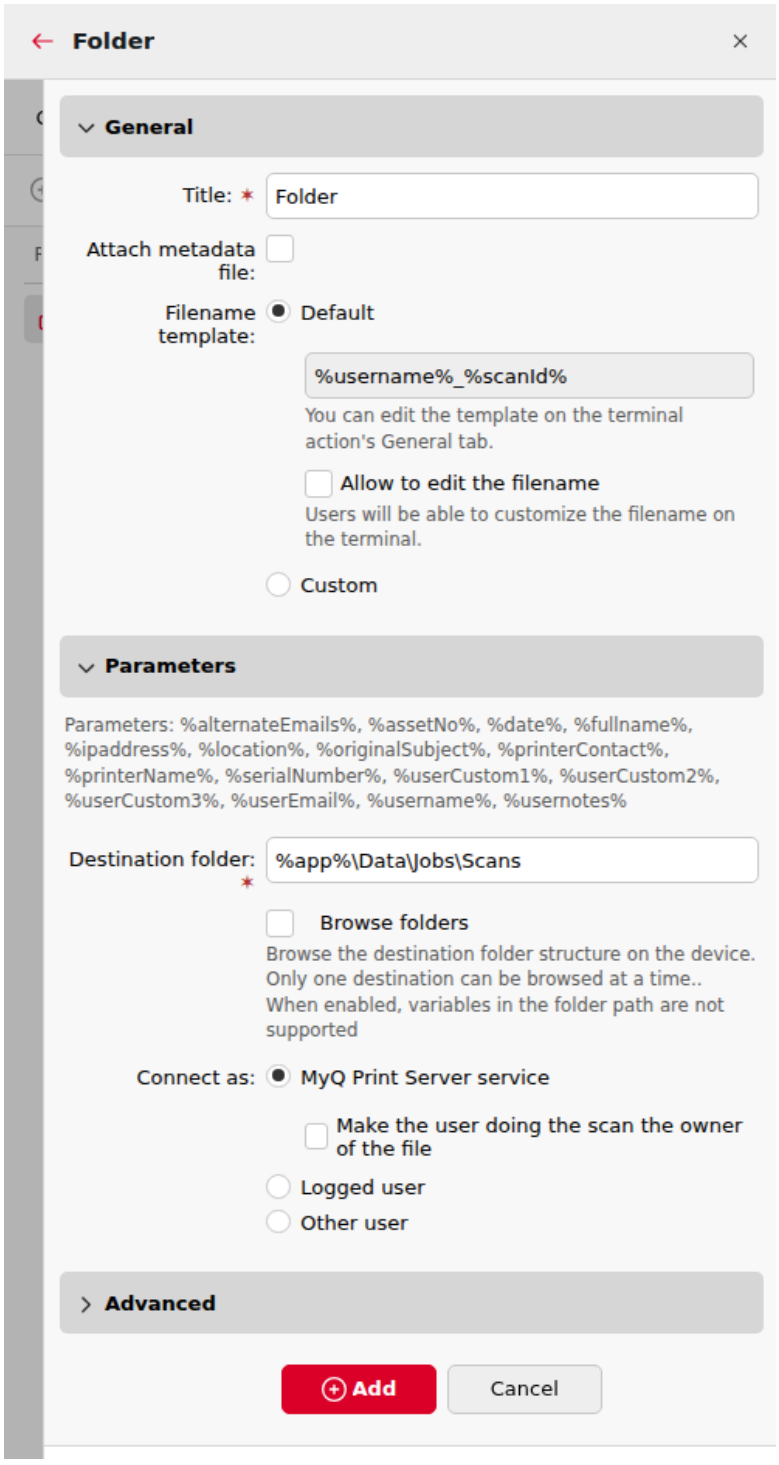
In addition, you can add recipients of a copy in the **Copy** text box, recipients of a blind copy in the **Blind copy** text box, the subject of the email in the **Subject** text box, and the body of the email in the **Message** text box.

Emails with scans sent from MyQ contain graphics by default, enable the **Send as plain text** option to send these emails as plain text, which might be necessary, for example, if the email will be further processed by an automation service or fax servers.

The text boxes under can contain the following parameters: %alternateEmails%, %assetNo%, %date%, %fullname%, %ipaddress%, %location%, %originalSubject%, %printerContact%, %printerName%, %serialNumber%, %time%, %timestamp%, %userCustom1%, %userCustom2%, %userCustom3%, %userEmail%, %username%, %usernotes%, %empty%

Scan to Folder

Scans are sent to the specified destination folder. If that folder does not exist, it is created automatically.



In the **Destination folder** field, type or browse and select the destination folder.

You can use the following parameters: %alternateEmails%, %assetNo%, %date%, %fullname%, %ipaddress%, %location%, %originalSubject%, %printerContact%, %printerName%, %serialNumber%, %userCustom1%, %userCustom2%, %userCustom3%, %userEmail%, %username%, %usernotes%.

Select the **Browse folders** option to allow users to browse one of their cloud destinations folder on the device.

The **Connect as** parameter determines which account is used to access the destination folder and which account is recorded as the owner of the scanned file.

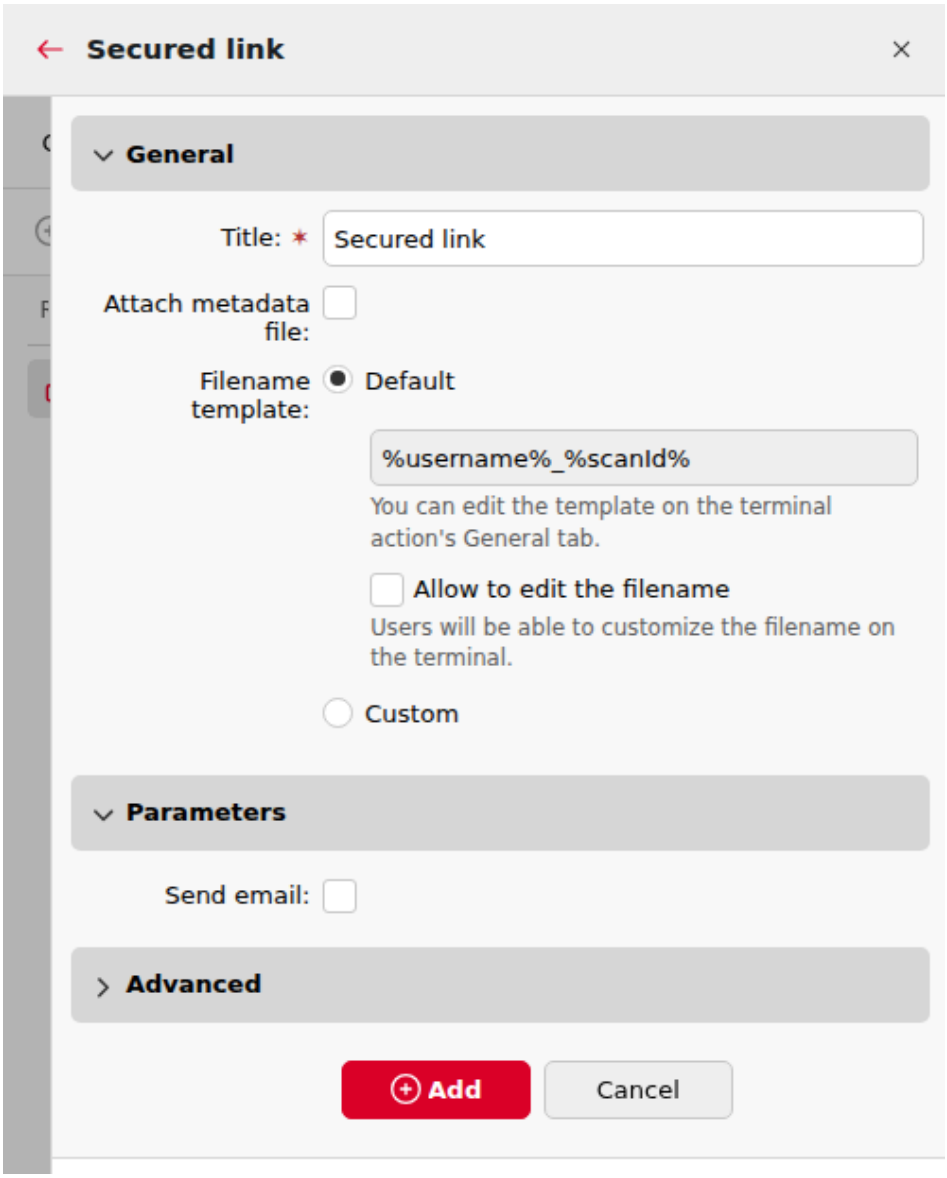
Option	Access	File owner	Description	When to use
MyQ Print Server service	MyQ service account	MyQ service account	MyQ accesses the destination folder using the account running the MyQ service.	Central or shared scan folders
Make the user doing the scan the owner of the file	Destination configuration	Scanning user	Changes only the owner of the scanned file. Folder access remains unchanged.	When the scanning user should be recorded as the file owner
Logged user	Scanning user account	Scanning user	MyQ accesses a shared folder using the domain account of the scanning user.	Personal user scan folders
Other user	Specified user account	Specified user	MyQ accesses a shared folder using the configured username and password.	Shared service or department accounts

- MyQ cannot change the owner of scanned files that are stored under the **Users** folder or any of its subfolders. If you want to use the **Make the user doing the scan the owner of the file** option, use a different folder than **Users** (or its subfolders) as the scan destination.
- When the scan is done by a hybrid Entra ID user (that is, the user has **On-premises username** and **On-premises domain** populated), MyQ uses `NETBIOS\username` for filesystem authentication instead of the Entra ID UPN.

Scan to Secured Link

Using this destination creates a secure link, stored on the MyQ Server, the scanned file can be downloaded via this link.

If in **Parameters** the **Send email** option is enabled, an email with the link is sent to the user's primary email address set in the **Email** field on the **General** tab of a user's properties.



Scan to OneDrive

To enable scanning to OneDrive:

1. Open an **Easy Scan** terminal action and on the **Destinations** tab select **Cloud storage** in the **+Add** dropdown.
2. Select the **OneDrive** option in the **Type** drop-down under **Parameters**. Select the **Browse folders** option if you want users to be able to browse one of their cloud destinations folder on the device.
3. Click **Save**.

Scan to OneDrive for Business

This article explains how to configure the Easy Scan terminal action to scan to OneDrive for Business.

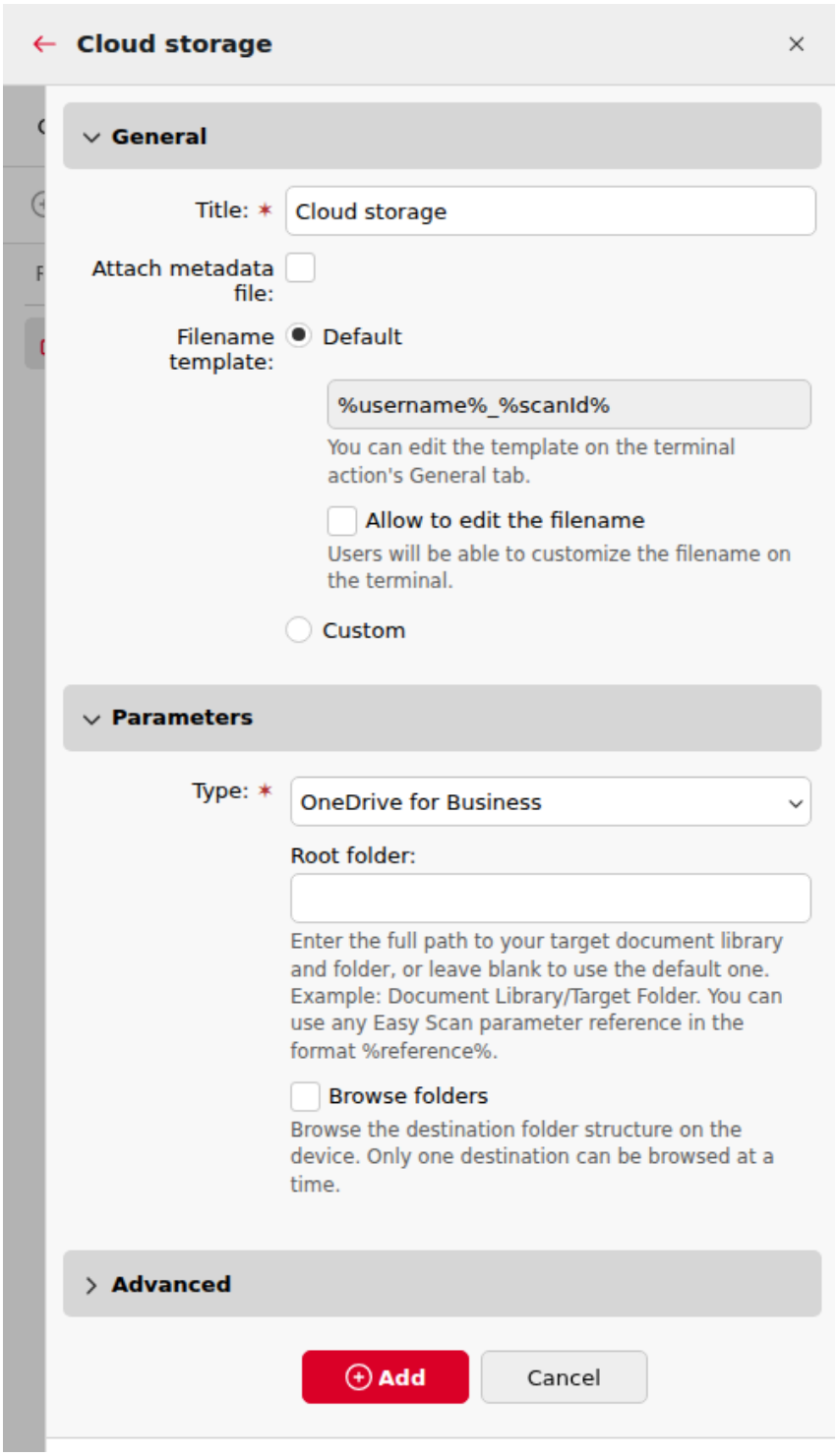
Prerequisites

- A OneDrive for Business connection is configured. For more information, see Connect to OneDrive for Business (see page 207).

Configure Easy Scan with the Destination OneDrive for Business

1. Open an **Easy Scan** terminal action and on the **Destinations** tab select **Cloud storage** in the **+Add** dropdown.
2. Under **Parameters,** select **OneDrive for Business** as the **Type**.
3. (Optional) Specify the **Root folder**. The root folder is the highest level directory into which a user can scan documents. If the root folder is not found, it is created automatically.

   Examples:
   - `finance/expense reports`
     Delivers scans to the “expense reports” folder in the user’s OneDrive.
   - `archive`
     Delivers scans to the “archive” folder.
4. (Optional) Enable **Browse folders** to let users browse the directories of the cloud destination folder on the device.
5. Click **Save**.



Pairing Users with Their OneDrive

When the Automatic mode was used or "*Application has access to OneDrive Business of all users*" was checked in the manual setup, there is no user interaction needed for

the users to use their OneDrive in MyQ. Users are paired with their OneDrive storage via User's Active Directory Object ID (UUID). These are automatically imported only with the Azure AD user's synchronization into MyQ. The UUID is synchronized from Central to Sites during user sync when Central users are synchronized with Azure AD. This process enables users at a Site to be automatically connected to their storage.

⚠ Users created manually or synchronized from sources other than Azure AD will see this OneDrive Business as "Connected" on their MyQ Web User Interface, but they are not paired with any OneDrive account.
If they opt to scan to their OneDrive account, they will receive an email prompting them to connect (if a user does this before OneDrive Business has been connected by an admin, no email prompt will be sent).

Re-authorizing the OneDrive Business Connection

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

The user will be shown the same dialogue as when the connection was created. The user can repeat all the steps to create a new secret for the existing OneDrive Business connection. Or they can perform step 3 - Administrator's consent, if it was not completed when the connection was created for any reason, for example, due to insufficient rights of the Azure administrator.

Also, the **Re-authorize** option allows you to change the type of connection created from automatic to manual, and vice versa.

Scan to Google Drive

MyQ supports both personal Google Drive and Google Drive for Workspace as scan destinations. If you want to use both, we recommend that you create a separate terminal action for each. If both destinations are used in the same action, folder browsing can be enabled for only one destination.

Set Google Drive as a Scan Destination

1. Open an **Easy Scan** terminal action and on the **Destinations** tab select **Cloud storage** in the **+Add** dropdown.

2. In the **Parameters** section under Type, select one of these options.
    - **Google Drive**
    - **Google Drive for Workspace**
3. Select **Browse folders** if you want users to be able to browse their My Drive and Shared Drives locations before scanning. If folder browsing is disabled, the scan is delivered to the root of the user's My Drive.
4. (Optional) With **Google Drive for Workspace** you can restrict browsing to a specific Shared Drive or folder:
    - **Drive name**
      Enter the display name (case-insensitive) of the Shared Drive as it appears in Google Drive for Workspace. When empty, the location defined by **Root folder** is resolved within My Drive instead.
      When **Browse folders** is enabled, terminal browsing is restricted to the specified Shared Drive. My Drive and other Shared Drives are hidden.
      When both **Drive name** and **Root folder** are empty, users can browse all accessible Shared Drives, or My Drive if none are available.
      When **Browse folders** is disabled, the **Drive name** field specifies the drive where scans are delivered.
    - **Root folder**
      Enter the path to a subfolder within the drive specified by **Drive name**, or within My Drive if **Drive name** is empty.
      When **Browse folders** is enabled, browsing starts from this folder. When **Browse folders** is disabled, **Root folder** specifies the exact delivery folder. When empty, the root of the target drive is used.
5. Click **Save**.

Scan to Box

To enable scanning to your Box cloud storage account:

1. Open an **Easy Scan** terminal action and on the **Destinations** tab select **Cloud storage** in the **+Add** dropdown.
2. Select the *Cloud Storage* option in the **Type** drop-down.
3. Select the `Box.com` option in the **Type** drop-down in the **Parameters** section. Select the **Browse folders** option if you want users to be able to browse one of their cloud destinations folder on the device.
4. Click **Save**.

Scan to Dropbox

To enable scanning to Dropbox:

1. Open an **Easy Scan** terminal action and on the **Destinations** tab select **Cloud storage** in the **+Add** dropdown.
2. Select the *Cloud Storage* option in the **Type** drop-down.
3. Select the *Dropbox* option in the **Type** drop-down in the **Parameters** section. Select the **Browse folders** option if you want users to be able to browse one of their cloud destinations folder on the device.
4. Click **Save**.

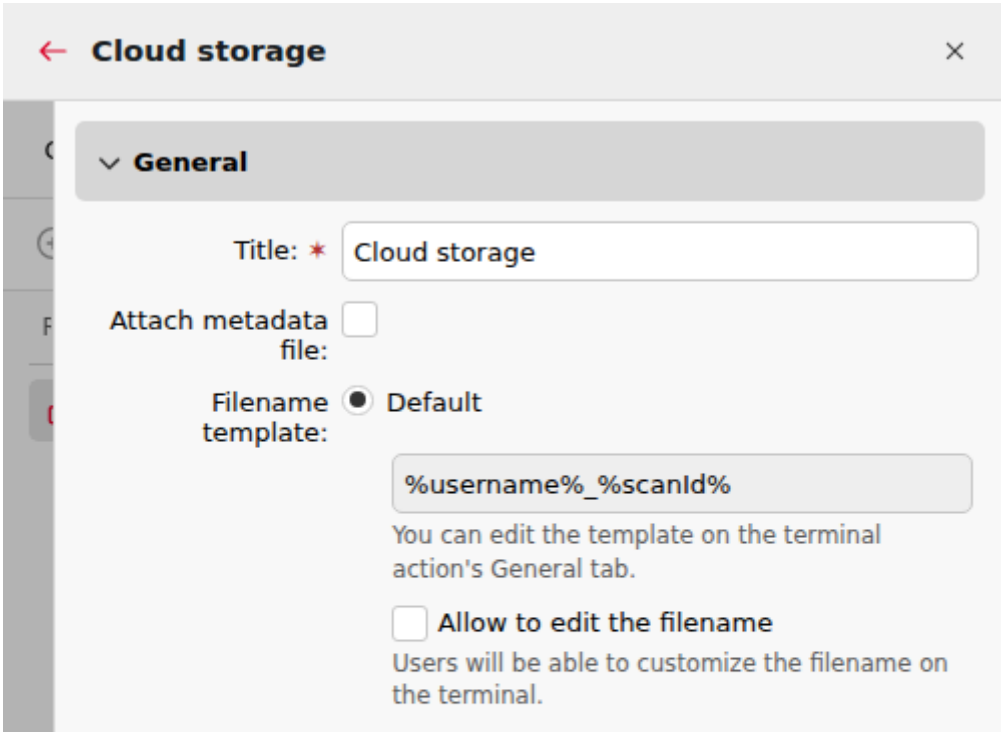
Scan to SharePoint Online

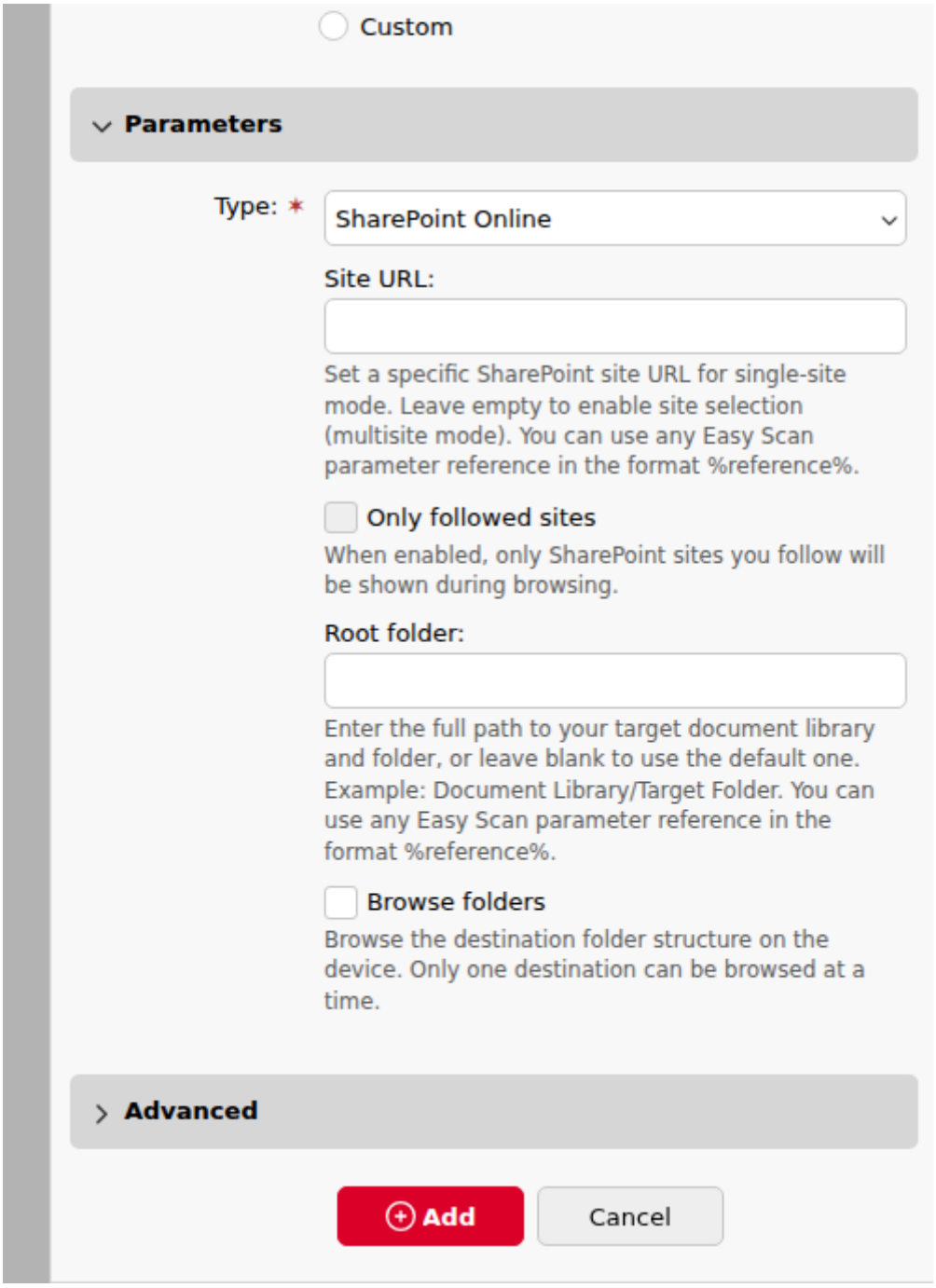
Prerequisites

- A SharePoint Online connection is configured. For more information, see Connect to SharePoint Online (see page 212).

Create and Set the SharePoint Online Destination

1. Open an **Easy Scan** terminal action and on the **Destinations** tab select **Cloud storage** in the **+Add** dropdown.
2. In the **Parameters** section, select *SharePoint Online*.





3. (Optional) Specify a Site URL and root folder for the scan destination to narrow the destination to one SharePoint site. The terminal does not show a site list. When folder browsing is enabled users can browse only within that site. When empty, the terminal shows a list of all sites or followed sites only; users select a site at the terminal. When folder browsing is enabled, users can browse document libraries and folders across SharePoint Online sites.

4. (Optional) Select **Only followed sites** to display only sites that the user follows. This option is unavailable in multi-site mode, and when application-wide access is enabled in the SharePoint Online connection settings.
5. (Optional) Select **Browse folders** to enable users to navigate within the SharePoint directory hierarchy.

Scan to Amazon S3

In order to scan to Amazon S3, you need to:

- Set up a bucket on the Amazon console. Your scans will be stored in this bucket.
- Create a user who will be used in the MyQ Web UI.
- Give the created user rights to the bucket.
- Fill in the **Client ID** and **Security Key** in the MyQ web administrator interface.
- Set up an Easy Scan terminal action to scan to Amazon S3.

Setting Up a Bucket on the Amazon S3 Console

You need an Amazon account to create a bucket to store the scans in. MyQ does not require any specific settings for scanning to an S3 bucket.

1. Login to Amazon Web Services with your Amazon account or create a new account. You need a credit card as proof of name. The credit card will also be used to charge the use of Amazon S3.
2. To create an S3 bucket, see Amazon Simple Storage Service[27].

> It is recommended to use a bucket lifecycle configuration. See Configuring a bucket lifecycle configuration[28].

Create a User in Amazon S3

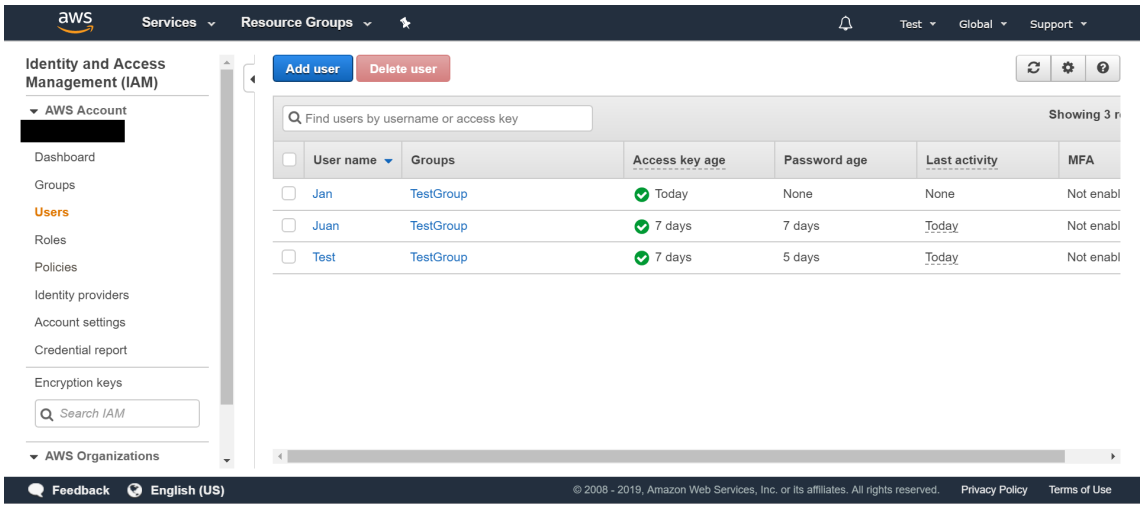
You need to create a user to make a connection between Amazon S3 and the MyQ Web UI.

1. Log in to the Amazon console.
2. Click the arrow next to your login name and select **My Security Credentials** from the drop-down menu.

---

27. https://docs.aws.amazon.com/AmazonS3/latest/gsg/s3-gsg.pdf
28. https://docs.aws.amazon.com/AmazonS3/latest/userguide/mpu-abort-incomplete-mpu-lifecycle-config.html

3. Click **Users** in the **Identity and Access Management (IAM)** panel and click **Add user**.



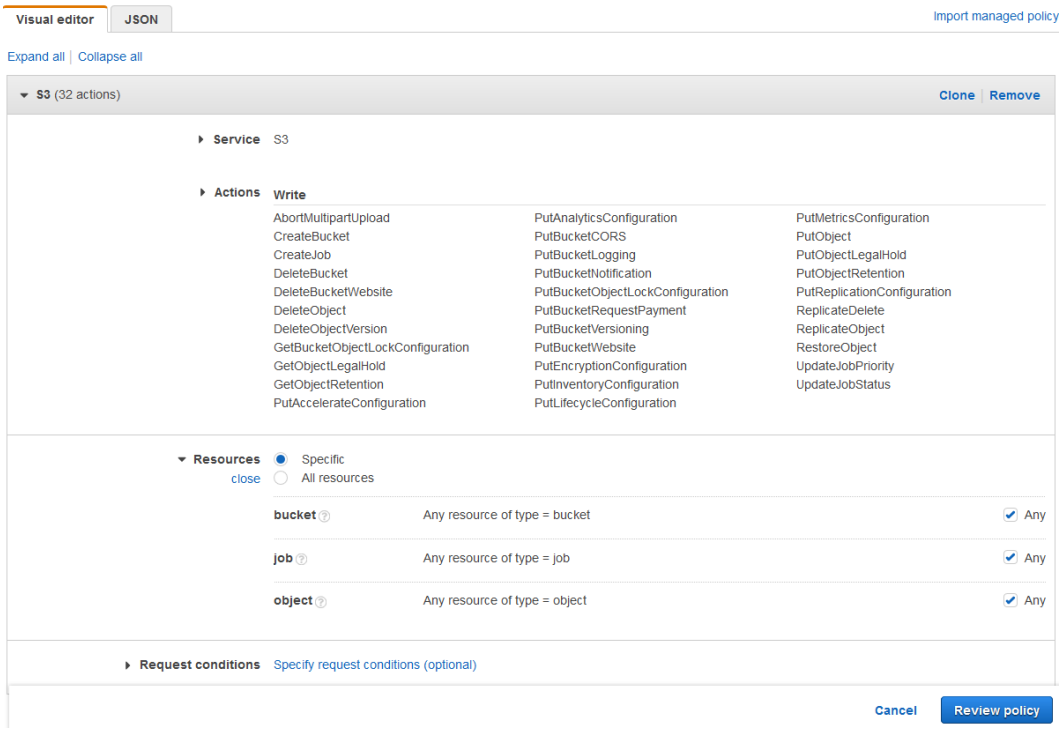
4. Follow the instructions to create the user.
5. Copy and save the **Client ID** and the **Access Key ID** of the created user, as you need them in the following steps.

Give User Access Rights to the Bucket

To give bucket permission to the user follow the short procedure below or see Change permissions for an IAM user[29]:

1. Click **Policies** in the **Identity and Access Management (IAM)** pane. Click **Create a new Policy**. The policy settings should be set as in the image below. If you do not want to provide the user with access to all buckets: deselect **Any** and click **Add ARN** to enter a specific bucket.

29. https://docs.aws.amazon.com/AmazonS3/latest/gsg/s3-gsg.pdf



2. Alternatively, use a JSON. This example would provide the same permissions as detailed in the screenshot above.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "MyQScan2S31",
            "Effect": "Allow",
            "Action": [
                "s3:ReplicateObject",
                "s3:PutObject",
                "s3:GetObjectRetention",
                "s3:AbortMultipartUpload",
                "s3:PutObjectRetention",
                "s3:DeleteObjectVersion",
                "s3:RestoreObject",
                "s3:PutObjectLegalHold",
                "s3:GetObjectLegalHold",
                "s3:DeleteObject",
                "s3:ReplicateDelete"
            ],
            "Resource": "arn:aws:s3:::*/*"
        },
        {
            "Sid": "MyQScan2S32",
            "Effect": "Allow",
            "Action": [
                "s3:PutAnalyticsConfiguration",
```

```
                "s3:PutAccelerateConfiguration",
                "s3:PutMetricsConfiguration",
                "s3:PutReplicationConfiguration",
                "s3:CreateBucket",
                "s3:UpdateJobStatus",
                "s3:PutBucketCORS",
                "s3:PutInventoryConfiguration",
                "s3:PutEncryptionConfiguration",
                "s3:GetBucketObjectLockConfiguration",
                "s3:PutBucketNotification",
                "s3:DeleteBucketWebsite",
                "s3:PutBucketWebsite",
                "s3:PutBucketRequestPayment",
                "s3:PutBucketLogging",
                "s3:PutLifecycleConfiguration",
                "s3:UpdateJobPriority",
                "s3:PutBucketObjectLockConfiguration",
                "s3:DeleteBucket",
                "s3:PutBucketVersioning"
            ],
            "Resource": [
                "arn:aws:s3:::*",
                "arn:aws:s3:*:130665556230:job/*"
            ]
        },
        {
            "Sid": "MyQScan2S33",
            "Effect": "Allow",
            "Action": "s3:CreateJob",
            "Resource": "*"
        }
    ]
}
```

3. Click **Groups** in the **Identity and Access Management (IAM)** pane. Click **Create New Group**. Give the group a name and **Save** it.
4. Click **Add Users to Group** and add the created user to the group.
5. Click the **Permissions** tab and click **Attach Policy**. Select the policy you just created and **Save** it all. The user now has ***Write*** access to the created bucket.

Set Up a Connection between MyQ and Amazon S3

1. Open the **Connections** settings tab of the MyQ Web Interface (**MyQ > Settings > Connections**).
2. Click **+Add** and select **Amazon S3** from the menu.
3. Add a **Title**. This will be used to identify the Cloud Storage Destination.

4. Add the **Access Key ID**, the **Security key** that you previously copied and saved, the **Region**, and **Bucket** and click **OK**.

Create and Set the Amazon S3 Destination

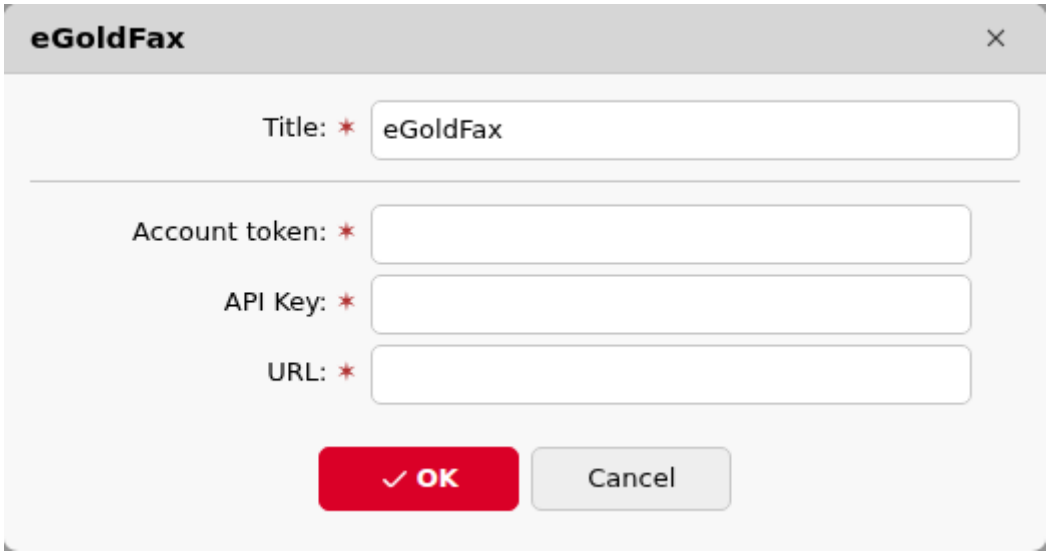
1. Open an **Easy Scan** terminal action and on the **Destinations** tab select **Cloud storage** in the **+Add** dropdown.
2. In the **Parameters** section, in the **Type** drop-down, select *Amazon S3* or any other **Title** you defined in the **Connections** settings in the previous steps and click **Save**.
3. Fill in the fields:
   - **Bucket**: the name of the Amazon S3 bucket to store the scans in.
   - **Region**: the region you have set when creating the bucket.
   - **Folder path**: enter the path of a subfolder.

Scan to eGoldFax

To scan to eGoldFax you need to first set up a connection to your eGoldFax service.

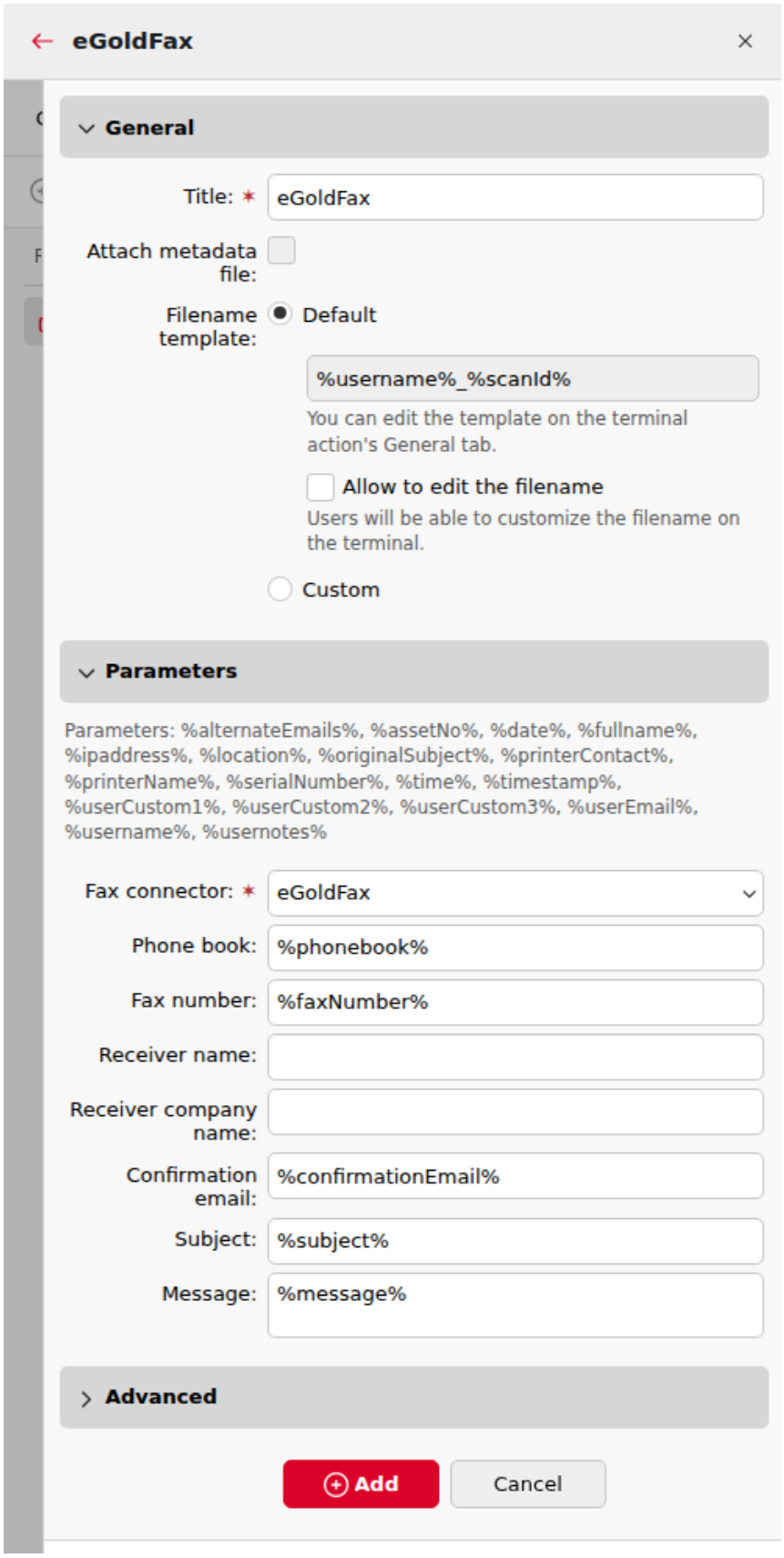
Set Up a Connection between MyQ and eGoldFax

1. Open the **Connections** settings tab of the MyQ Web Interface (**MyQ > Settings > Connections**).
2. Click **+Add** and select **eGoldFax** from the menu.
3. Add a title identifying the connection, and your **Account token**, **API key,** and **URL** from eGoldFax.



Create and Set the eGoldFax Destination

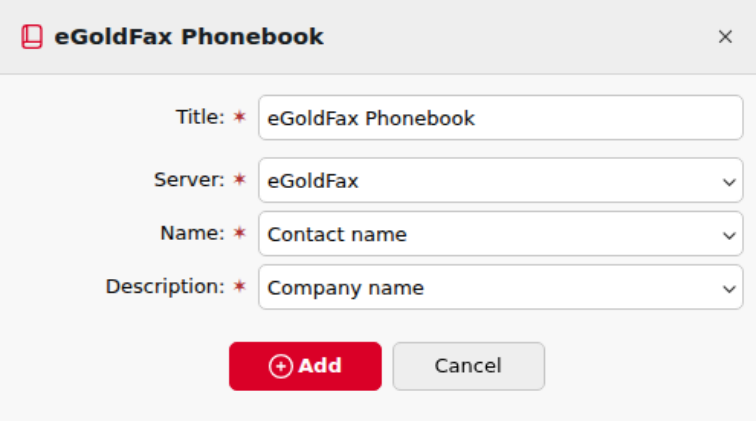
- Create a new destination (edit or create an Easy Scan terminal action; on its properties panel, in the **Destinations** tab, click **+Add**, select **eGoldFax**).


eGoldFax
General
Title: *
eGoldFax
Attach metadata file:
Filename template:
Default
%username%_%scanId%
You can edit the template on the terminal action's General tab.
Allow to edit the filename
Users will be able to customize the filename on the terminal.
Custom
Parameters
Parameters: %alternateEmails%, %assetNo%, %date%, %fullname%, %ipaddress%, %location%, %originalSubject%, %printerContact%, %printerName%, %serialNumber%, %time%, %timestamp%, %userCustom1%, %userCustom2%, %userCustom3%, %userEmail%, %username%, %usernotes%
Fax connector: *
eGoldFax
Phone book:
%phonebook%
Fax number:
%faxNumber%
Receiver name:
Receiver company name:
Confirmation email:
%confirmationEmail%
Subject:
%subject%
Message:
%message%
Advanced
Add
Cancel

eGoldFax Code Book

When eGoldFax is connected to MyQ, a Code Book is automatically created called **eGoldFax Phonebook**. In **MyQ > Settings > Code Books** you can edit the Code Book **Title**, and **Server** (if multiple instances of eGoldFax are connected).

You can set the **Name** display to **Contact name** or **Contact name (Company name)** and the **Description** to **Company name** or **Fax number**, this will be visible on the Embedded Terminal when scanning to a contact from the Code Book.



This Code Book can be added as a Parameter to the eGoldFax Easy Scan destination, allowing users to select contacts from the eGoldFax phonebook at an Embedded Terminal.

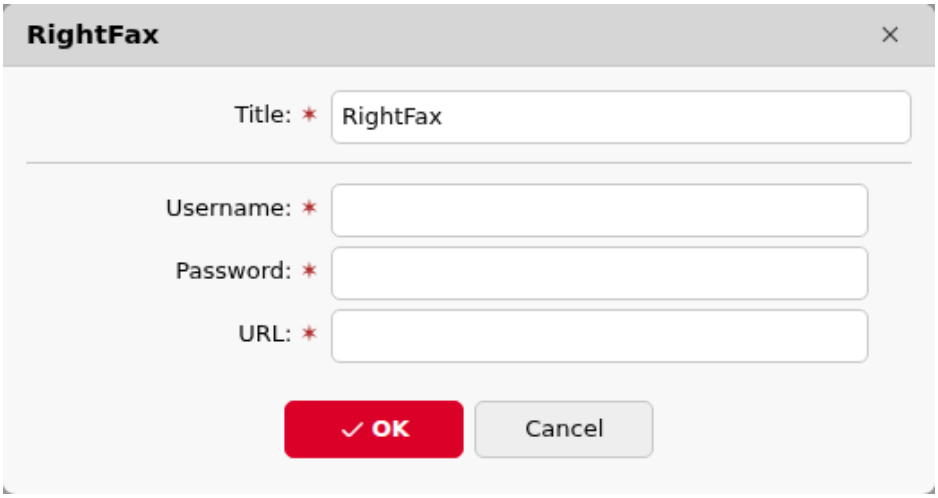
Additionally, **Confirmation email** is available as a parameter for eGoldFax Easy scan destinations. By default, it is set to %userEmail%, but it can be changed to another user attribute or set as a single constant email destination.

Scan to RightFax

Learn how to integrate RightFax with MyQ, configure code books for contact lookup, and enable users to send a fax to RightFax contacts and contact groups with Easy Scan.

Define a Connection to RightFax

1. Go to **MyQ > Settings > Connections** in the MyQ Web Interface.
2. Click **+Add** and select **RightFax** from the menu.
3. Enter a **Title** that identifies the connection, and provide your RightFax administrator **Username, Password,** and **URL** in the form `<protocol>://<hostname>/rightfax/api`.



In most cases, a single RightFax connection is enough. However, you can define more than one, for example for testing purposes.

Customize the RightFax Code Books

For each registered connection to RightFax, two code books are automatically generated:

- RightFax Phonebook
- RightFax Phonebook Groups

You can create multiple RightFax code books and use them in different terminal actions.

Code Book Parameters

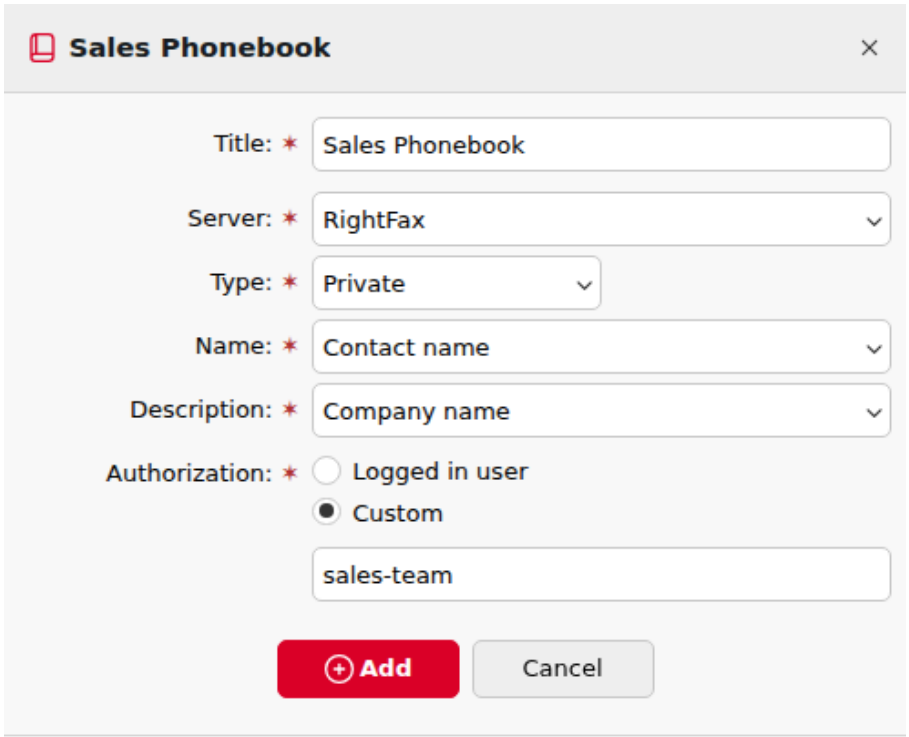
Only Title, Server, and Authorization are used for phonebook groups.

- **Title**
  Enter a name to identify the code book.
- **Server**
  Select the RightFax connection to use.
- **Type**
  Select whether to include **Private** or **Shared** contacts in the phonebook.
- **Name**
  Control what appears under the Name field on the terminal. Select from:
  - **Contact Name** (default)
  - **Contact Name (Company)**

- **Description**
  Control what appears under the Description field on the terminal. Select from:
  - **Company Name** (default)
  - **Fax Number**
- **Authorization**
  Specify the user whose contacts you want to provide in the code book.
  - **Logged in user** (default)
    This loads the contacts of the RightFax user who is logged in to the terminal.
  - **Custom**
    Specify a custom user whose phonebook will be used.

    Note: If Type is set to Shared, all shared contacts are available, regardless of which authorization method is used.

In the example below, *sales-team* is an account in the connected RightFax instance. When this code book is used as an Easy Scan destination, terminal users can send a fax to contacts of the sales-team only. Also, when selecting contacts, users will see the contact name and company, but not the contact fax number.

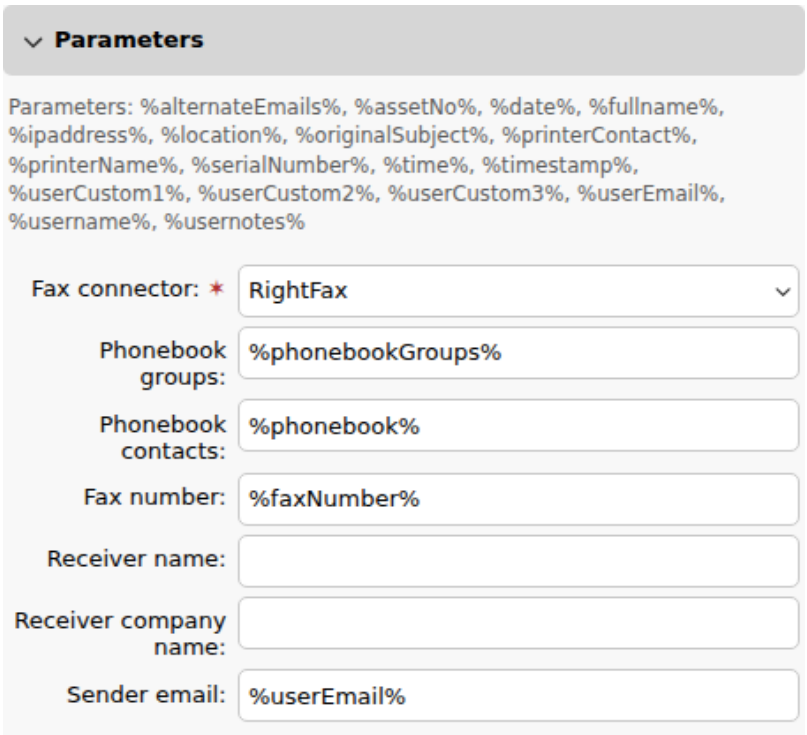


Set RightFax as an Easy Scan Destination

After you have created the RightFax connection and customized the code books, you are ready to add RightFax as an Easy Scan destination.

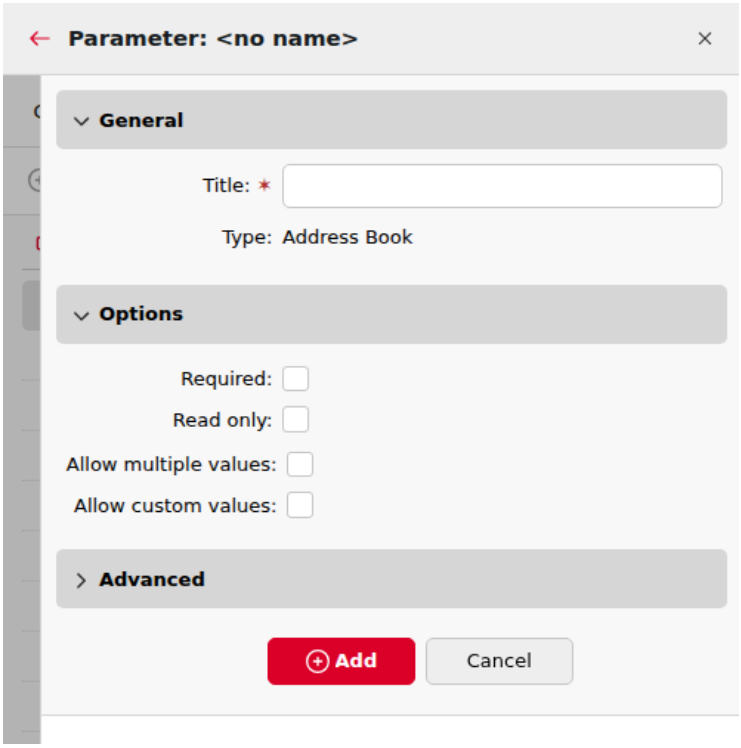
1. Open the properties panel of an Easy Scan terminal action.
2. In the **Destinations** tab, click **+Add**, and select **RightFax**.

   This step automatically adds **Fax number**, **Phone book** and **Phonebook groups** to the terminal action **Parameters**.
3. Configure the RightFax parameters. You can assign each parameter to a global variable, or define a new parameter and assign it in the **Parameters** of the terminal action.
   - **Fax number**
     The receiver fax number. This appears on the fax under **To:/Fax:**
   - **Sender email**
     The RightFax user email, which appears on fax under **From:**
   - **Receiver name** and **Receiver company name** are not assigned by default. If you map values to these parameters, they appear on the fax under **To:** and **Company:**.
4. Click **+Add** to save.



Scan to Contact from Address Book

To enable the Address Book parameter, the administrator has to set it up as a custom parameter for the Easy Scan action. See Custom Parameters Examples (see page 336).



If the Address Book is the only destination for the Easy Scan action, it is recommended to enable **Required**. Otherwise, the field would not be marked as mandatory with * (asterisk) on the Embedded Terminal.

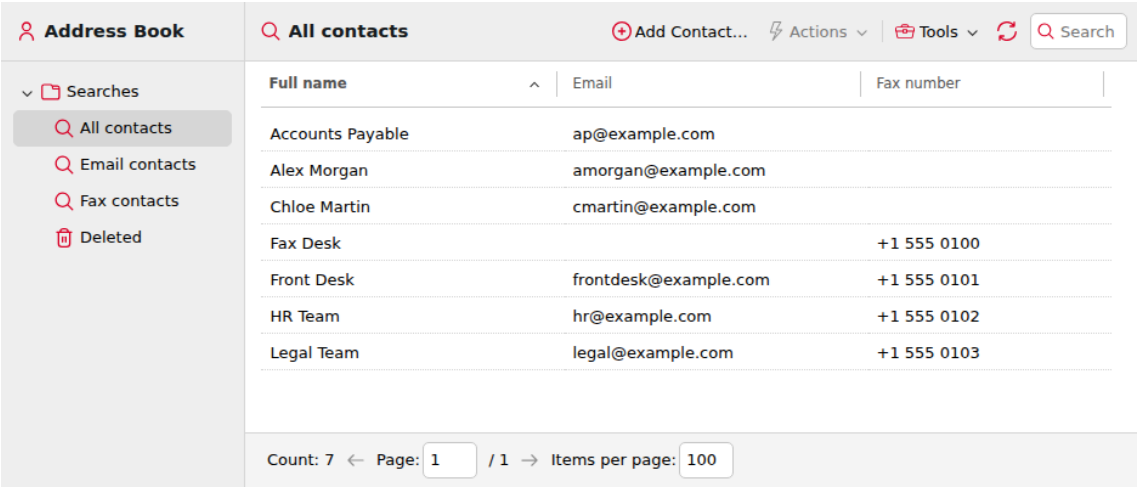
Once done, users can manage their Address Book on the MyQ Web UI and scans are sent to the contact from the users Address Book.

Accessing and Using Address Book

1. Log in to MyQ.
2. In the main menu, select **Address Book**.

Address Book is not available to built-in accounts such as *admin.

3. Here, you'll see your contact list with available columns: **Full name**, **Email**, and **Fax number**.



Managing Contacts

1. To add a contact, click on **Add contact**. A pop-up appears where you can enter the contact's **Full Name**, **Email**, and **Fax Number**.
2. To edit or remove a contact, locate the contact from the list and choose the respective option.
3. For searches, use the left pane. Options available: **All Contacts**, **Email Contacts**, **Fax Contacts**, and **Deleted**.
4. In the **Deleted** section, you can either **Restore** or **Permanently Remove** a contact.

> ⚠ All email inputs undergo validation checks to ensure they are of a valid email format.
> Fax numbers are saved without validation. Make sure your users understand what number formats are supported by Fax devices.

Using Address Book in Easy Scan

1. Log in to the terminal.
2. Choose **Easy Scan**.

3. In the parameters, select the **Address Book** option.
4. Browse and select a contact from your list as the destination.

> A user can only access contacts from their own Address Book. Accessing the contacts of another user, even by administrators, is prohibited.

Scan to Scan Review

The **Scan Review** destination sends scanned documents to a MyQ Scan Review document queue, where reviewers check them before they are approved. For an overview of Scan Review, see (10.3) MyQ Scan Review.

Prerequisites

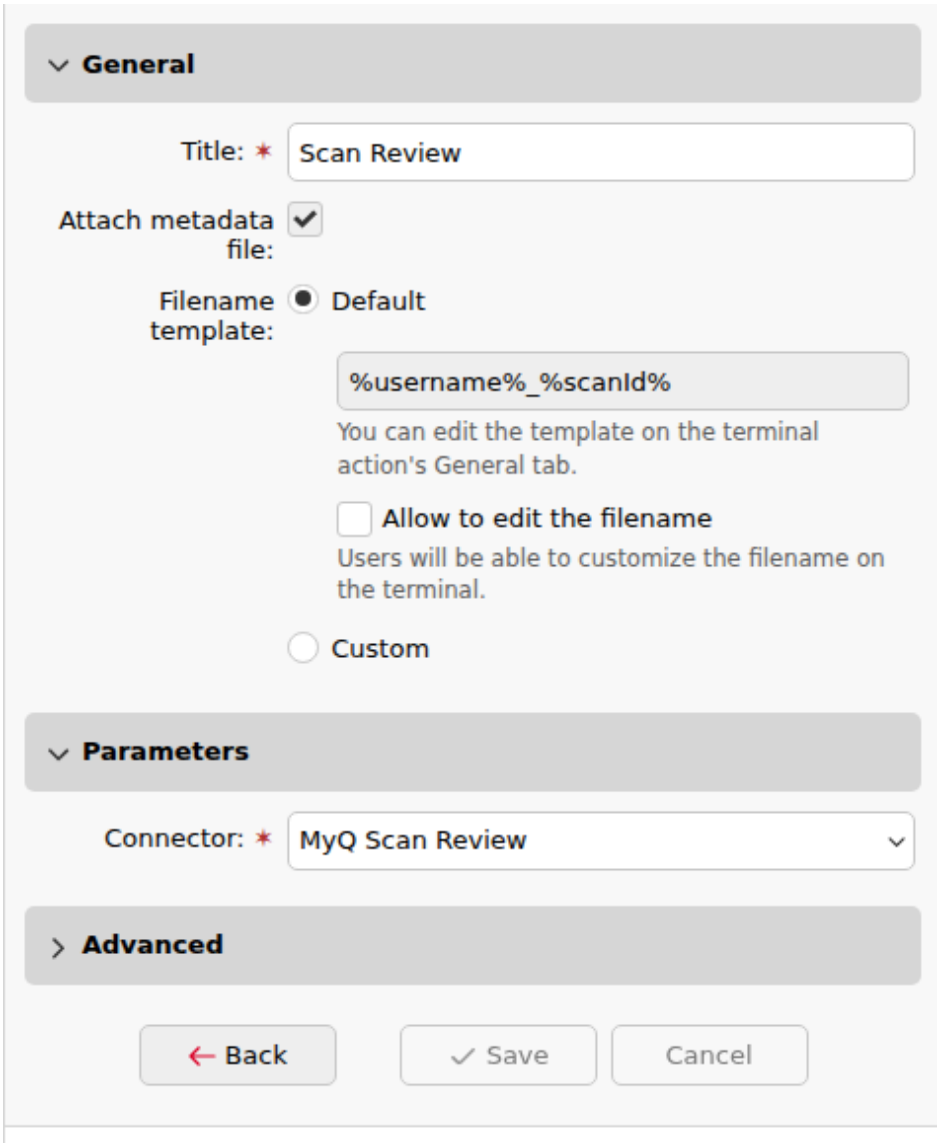
- A MyQ Scan Review connection is configured. For more information, see Connect to MyQ Scan Review (see page 231).
- An **Embedded Ultimate** license is assigned to each participating device.

Terminals with a lower license tier (Embedded, Embedded Lite) do not show an Easy Scan action with the Scan Review destination. If a terminal's license is downgraded from Ultimate, the action is hidden after the next user login. The terminal may need to be reactivated.

Create and Set the Scan Review Destination

1. Open an **Easy Scan** terminal action, or create one in **MyQ > Settings > Terminal Actions** (**Add Action > Scan > Easy Scan**).

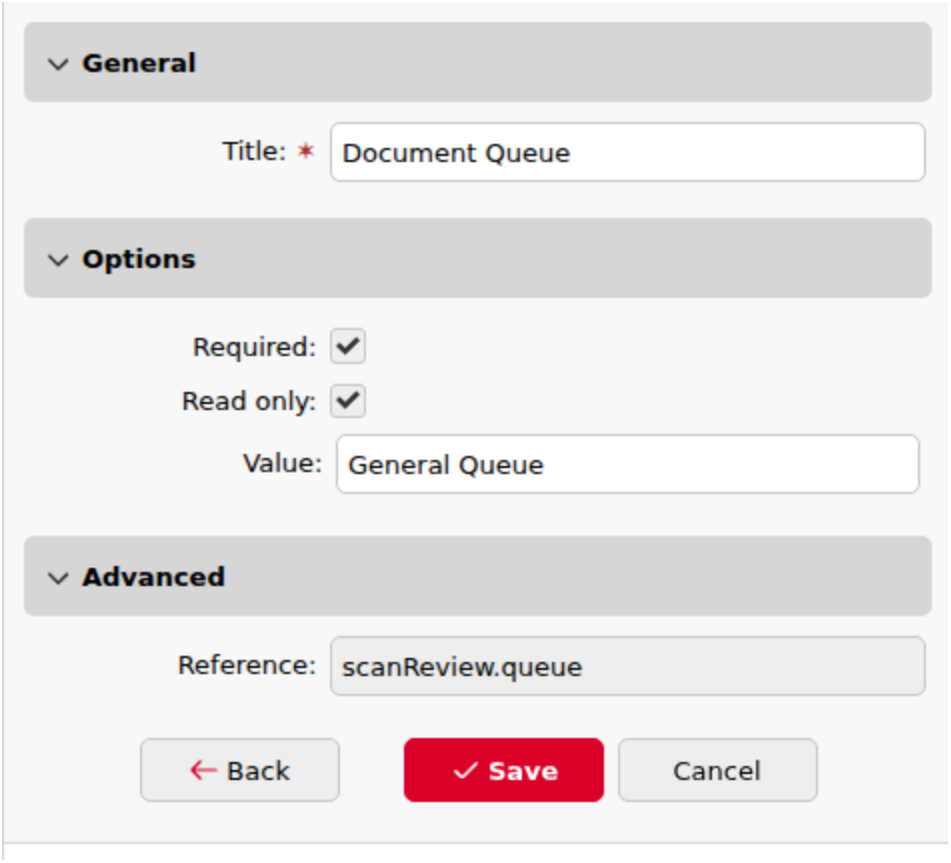
   On the **General** tab, use a **Title** that tells users where their documents go, for example, the review queue or the target location.
2. On the **Destinations** tab, select **Scan Review** in the **+Add** dropdown.
3. In the **General** section:
   - (Optional) Change the **Title**, for example, to tell several Scan Review destinations apart.
   - **Attach metadata file** is always selected for this destination.
   - **Filename template**: keep **Default** to use the template from the **General** tab of the terminal action, or select **Custom** to build one from the action's parameters, including custom parameters. See Easy Scan Destinations (see page 342).
4. In the **Parameters** section, in **Connector**, select the Scan Review connection.



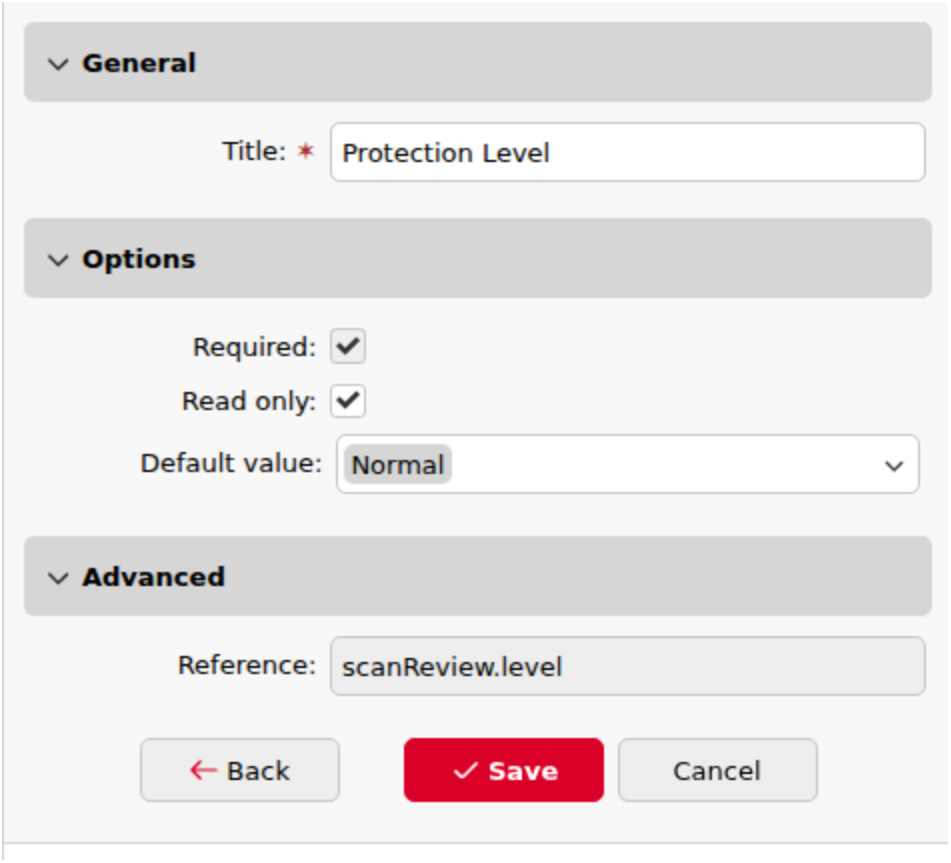
Set the Scan Review Parameters

On the **Parameters** tab of the terminal action, open each parameter's settings:

- **Document Queue**: in **Value**, enter the exact name of the Scan Review document queue that receives the documents. **Required** and **Read only** cannot be cleared.



- **Protection Level**: the protection level of the submitted documents.
  - To use a fixed level, select **Read only** and set a **Default Value**.
  - To let users choose the level at the terminal, clear **Read only** and leave **Default Value** empty.



- **Brand**, **Model**, and **Serial Number**: filled in automatically.
- (Optional) **Resolution**: we recommend at least **300 dpi** for Scan Review.

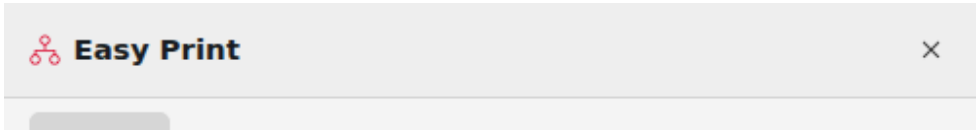
Additional Parameters

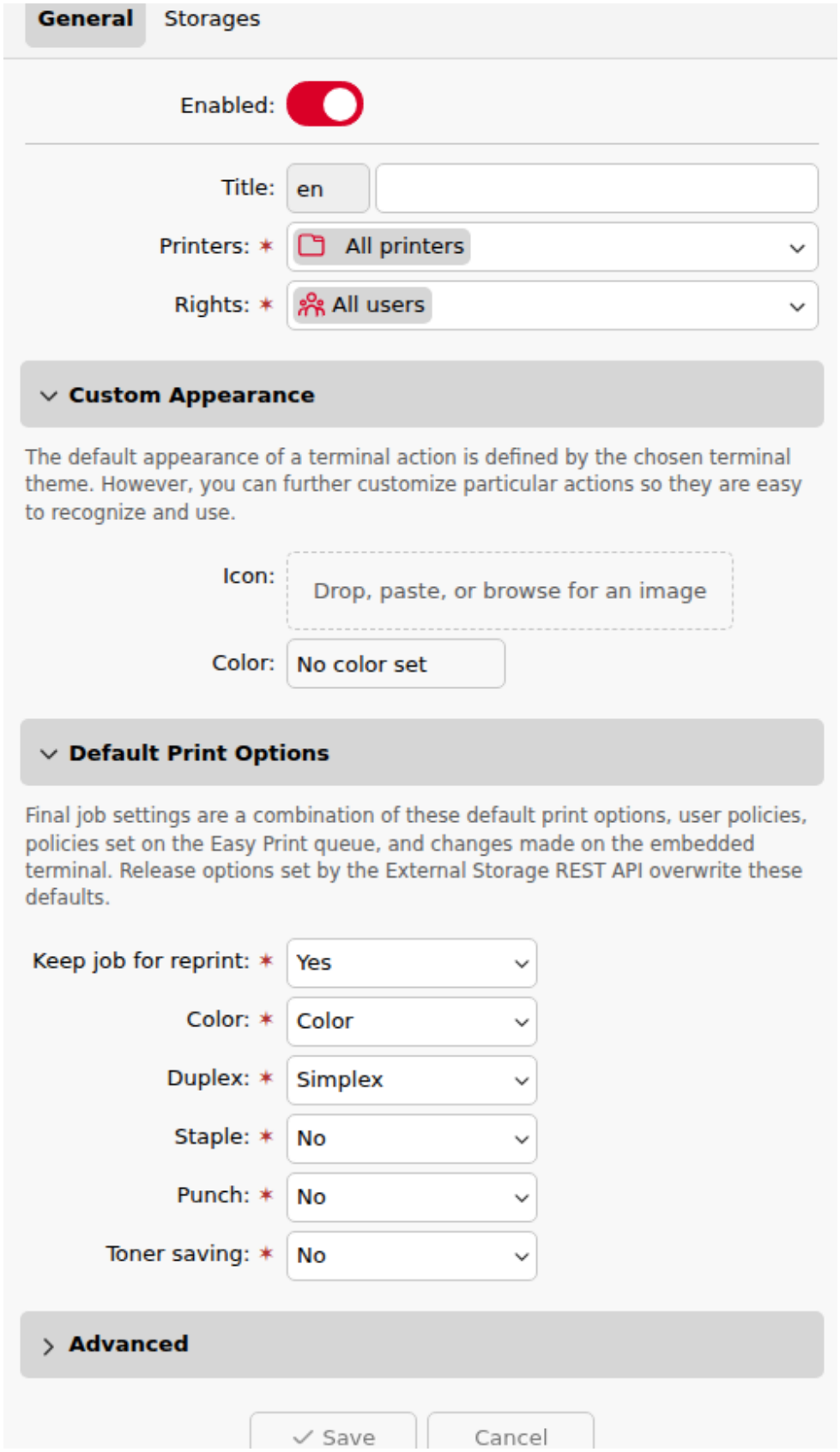
You can add custom parameters, such as a document ID, to help reviewers match paper originals with the scanned documents in the document queue. See (10.3) Archiving Process.

9.5.9 Easy Print Settings

The Easy Print terminal action allows users to print files without sending them first to MyQ. These files can be printed from multiple sources, like several cloud storages, network drives or local drives, and the user's default storage.

The properties panel is automatically opened after the **Easy Print** terminal action is created. You can also access it by double-clicking the terminal action node on the list of nodes or on the terminal screen preview.




General
Storages
Enabled:
Title:
en
Printers: *
All printers
Rights: *
All users
Custom Appearance
The default appearance of a terminal action is defined by the chosen terminal theme. However, you can further customize particular actions so they are easy to recognize and use.
Icon:
Drop, paste, or browse for an image
Color:
No color set
Default Print Options
Final job settings are a combination of these default print options, user policies, policies set on the Easy Print queue, and changes made on the embedded terminal. Release options set by the External Storage REST API overwrite these defaults.
Keep job for reprint: *
Yes
Color: *
Color
Duplex: *
Simplex
Staple: *
No
Punch: *
No
Toner saving: *
No
Advanced
Save
Cancel

General Tab

- **Enable/Disable** the action.
- **Printers**: Specify the printers where the action is available.
- **Rights**: Specify the users and/or user groups who can use the action.

You can set a **Custom Appearance** for the action.

- **Icon**: add an image for the terminal action.
- **Color**: select a color for the terminal action

You can specify the **Default Print Options** for the action.

> The final job settings are a combination of these default print options, policies set on the Easy Print queue, user policies, and changes made on the embedded terminal.

- Keep jobs for reprint
- Color
- Duplex
- Staple
- Punch
- Toner saving

Storages Tab

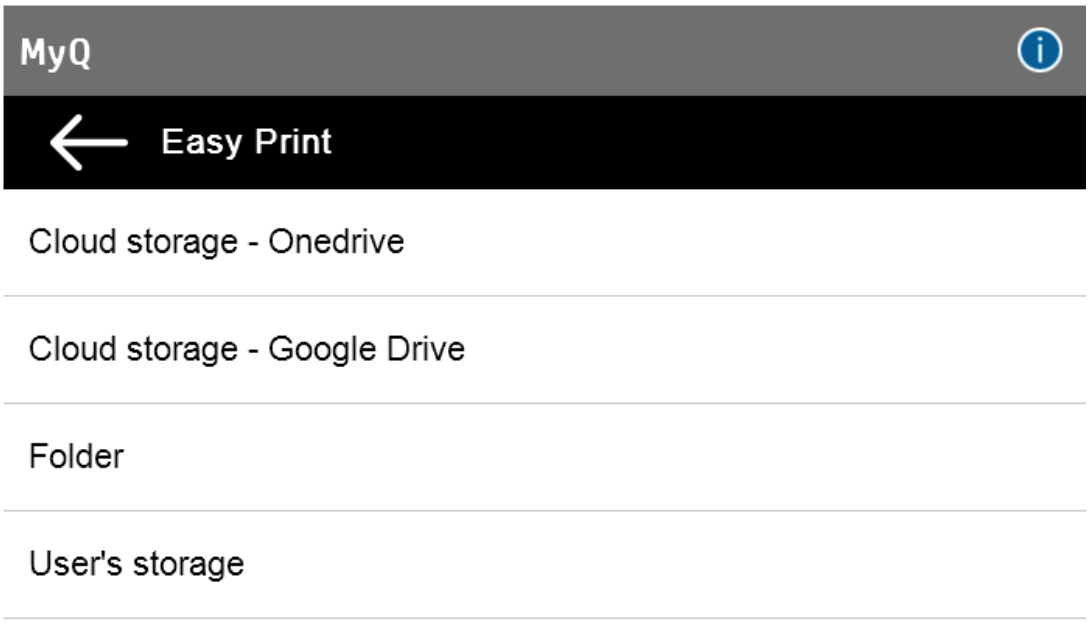
You can add one or more storage sources from the following:

- Cloud storage
- Folder
- User's storage

When Easy Print is used on the terminal, the user is presented with a list of possible sources associated with this action (this is skipped in case of a single source). After the source is selected, the user can browse it and select files for printing.

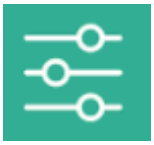
See also:

- Easy Print Sources (see page 386)



Once a file or files have been selected for printing, you can use the modify button to modify the print options (*Color, Duplex, Staple, Punch, Toner saving*, and *Copies*).

> These options are listed on all terminals, regardless of whether or not the specific terminal can complete a particular action, so it's possible that a selection made may be ignored.



10 Job Release Options

After pressing the print button, the files are downloaded from the source to the server, processed through the default Easy Print queue, and released immediately to the printer. It is also possible to cancel the whole downloading and printing process. In this case, files that have already been downloaded, but not printed are deleted from the server.

File Formats

The supported formats for Easy Print are: *bmp, jfif, jpe, jpeg, jpg, mime, png, tif, tiff, txt, urf,* and *pdf*.

If Microsoft Office suite or Libre Office are installed on the server, the **Microsoft formats** *doc, docx, xls, xlsx, ppt, pptx* and **Libre Office formats** are also supported. These are converted into PDF based on the settings in **Jobs** > **General** > **Office file formats**.

Vendor Compatibility Specifics

Easy Print compatibility may differ between brands. Please check the relevant terminal documentation for more details.

- MyQ Brother Embedded
- MyQ Canon Embedded
- MyQ Epson Embedded
- MyQ Fujifilm Embedded
- MyQ HP Embedded
- MyQ KATUN Embedded
- MyQ Kyocera Embedded
- MyQ Kyocera Embedded Lite
- MyQ Lexmark Embedded
- MyQ Ricoh SmartSDK Embedded
- MyQ Sharp Embedded
- MyQ Sharp Luna Embedded
- MyQ Toshiba Embedded
- MyQ Xerox Embedded

Easy Print Sources

The Easy Print terminal action allows users to print files without sending them first to MyQ. These files can be printed from multiple sources, like several cloud storages, network drives, or local drives, and the user's default storage.

To use Easy Print, a new terminal action has to be created in **Settings > Printers and Terminals > Terminal actions**. This action requires some additional configuration - which sources should be available for the user, and the default release options. It is possible to create multiple instances of the Easy Print action, each with different settings.

When this action is used on the terminal, the user is presented with a list of possible sources associated with this action (this is skipped in cases of a single source). After the source is selected, the user can browse it and select files for printing.

After pressing the print button, files are downloaded from the source to the server, processed through the default Easy Print queue, and released immediately to the

printer without any further interaction. It is also possible to cancel the whole downloading and printing process. In this case, files that have already been downloaded, but not printed, are deleted from the server. Files that have already been printed remain on the server and it is possible to reprint them.

Print from Box

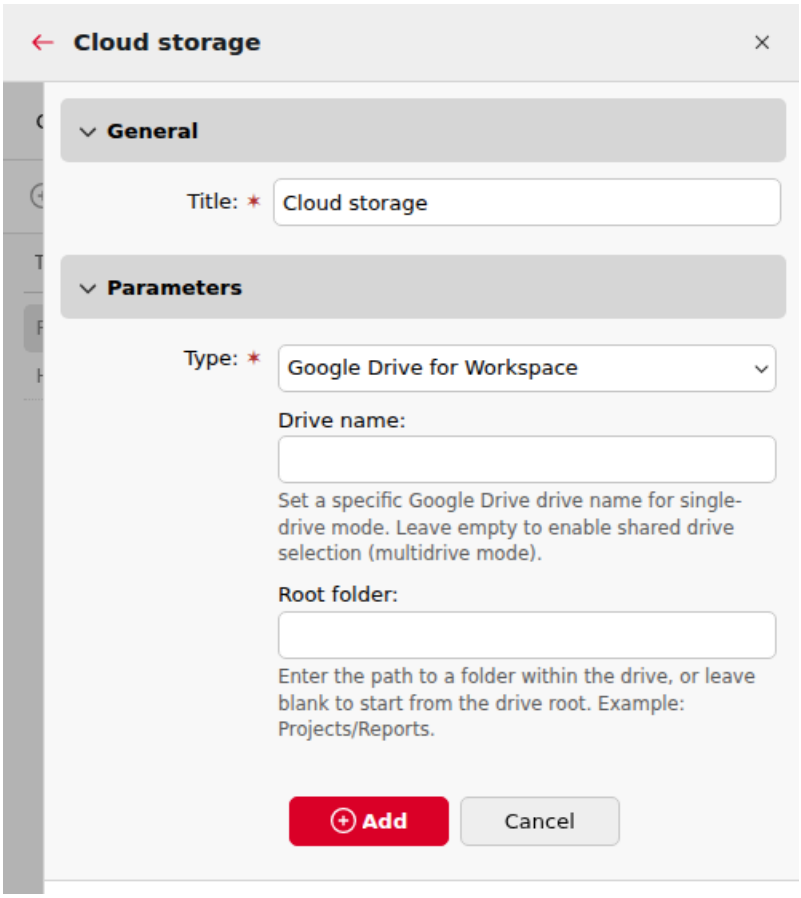
To connect Box as a cloud storage to the **Easy Print** terminal action:

1. Go to **MyQ > Settings > Terminal Actions**.
2. If there is an Easy Print action already added, you can configure it by double-clicking it or create a new one by clicking on the actions menu then **Add action into this folder** and selecting **Easy Print** from the list.
3. In the options menu, go to **Storages > Add > Cloud Storage.**
4. Under **General**, you can rename your cloud storage, and under **Parameters**, select the **Type** (`Box.com`) from the dropdown. Then click **Add**.

Print from Google Drive

To connect Google Drive or Google Drive for Workspace as a cloud storage for use with the **Easy Print** terminal action, follow these steps.

1. Go to **MyQ > Settings > Terminal Actions**.
2. If there is an Easy Print action already added, you can configure it by double-clicking it or create a new one by clicking on the actions menu then **Add action into this folder** and selecting **Easy Print** from the list.
3. In the options menu, go to **Storages > Add > Cloud Storage.**
4. Under **General**, you can rename your cloud storage, and under **Parameters**, set **Type** to *Google Drive* or *Google Drive for Workspace*. For **Google Drive for Workspace**, you can optionally set:
    - **Drive name**
      Enter the display name (case-insensitive) of the Shared Drive as it appears in Google Drive for Workspace. When empty, the location defined by **Root folder** is resolved within My Drive instead.
    - **Root folder**
      Enter the path to a subfolder within the drive specified by **Drive name**, or within My Drive if **Drive name** is empty.
5. Click **Add**.



Print from Dropbox

To connect Dropbox as a cloud storage to the **Easy Print** terminal action:

1. Go to **MyQ > Settings > Terminal Actions**.
2. If there is an Easy Print action already added, you can configure it by double-clicking it or create a new one by clicking on the actions menu then **Add action into this folder** and selecting **Easy Print** from the list.
3. In the options menu, go to **Storages > Add > Cloud Storage.**
4. Under **General**, you can rename your cloud storage, and under **Parameters**, select the **Type** (Dropbox) from the dropdown. Then click **Add**.

Print from OneDrive

To connect OneDrive as a cloud storage to the **Easy Print** terminal action:

1. Go to **MyQ > Settings > Terminal Actions**.

2. If there is an Easy Print action already added, you can configure it by double-clicking it or create a new one by clicking on the actions menu then **Add action into this folder** and selecting **Easy Print** from the list.
3. In the options menu, go to **Storages > Add > Cloud Storage.**
4. Under **General**, you can rename your cloud storage, and under **Parameters**, select the **Type** (OneDrive) from the dropdown. Then click **Add**.

Print from OneDrive for Business

This article describes how to configure the Easy Print terminal action to print from OneDrive for Business.

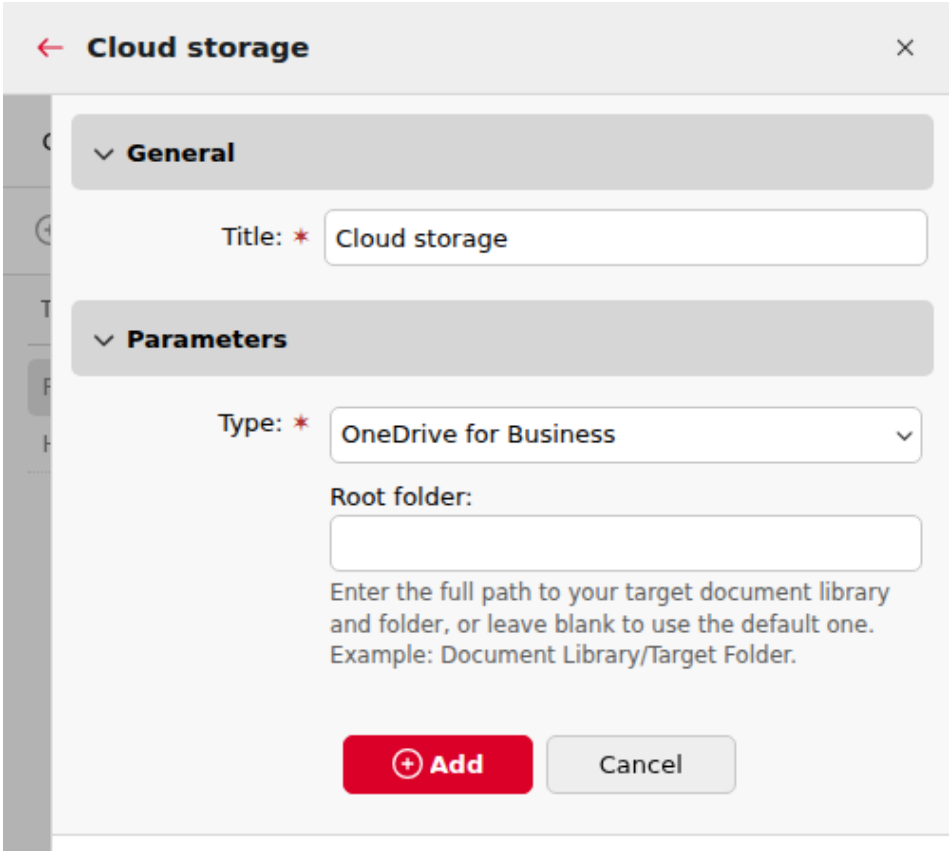
Prerequisites

- A OneDrive for Business connection is configured. For more information, see Connect to OneDrive for Business (see page 207).

Configure Easy Print with the Source OneDrive for Business

1. Go to **MyQ > Settings > Terminal Actions**.
2. Select **Easy Print** and click **Edit**.

   If the action is not visible, to add it go to **Add Action > Print > Easy Print**.
3. On the **Storages** tab, click **Add** and select **Cloud Storage.**
4. Under **General**, enter a title for the storage location.
5. Under **Parameters**, select OneDrive for Business as the **Type**.
6. (Optional) Specify the **Root folder**. The root folder is the highest level directory from which a user can print documents.
7. Click **Add**.



Print from SharePoint Online

This article describes how to configure the Easy Print terminal action to print from SharePoint Online.

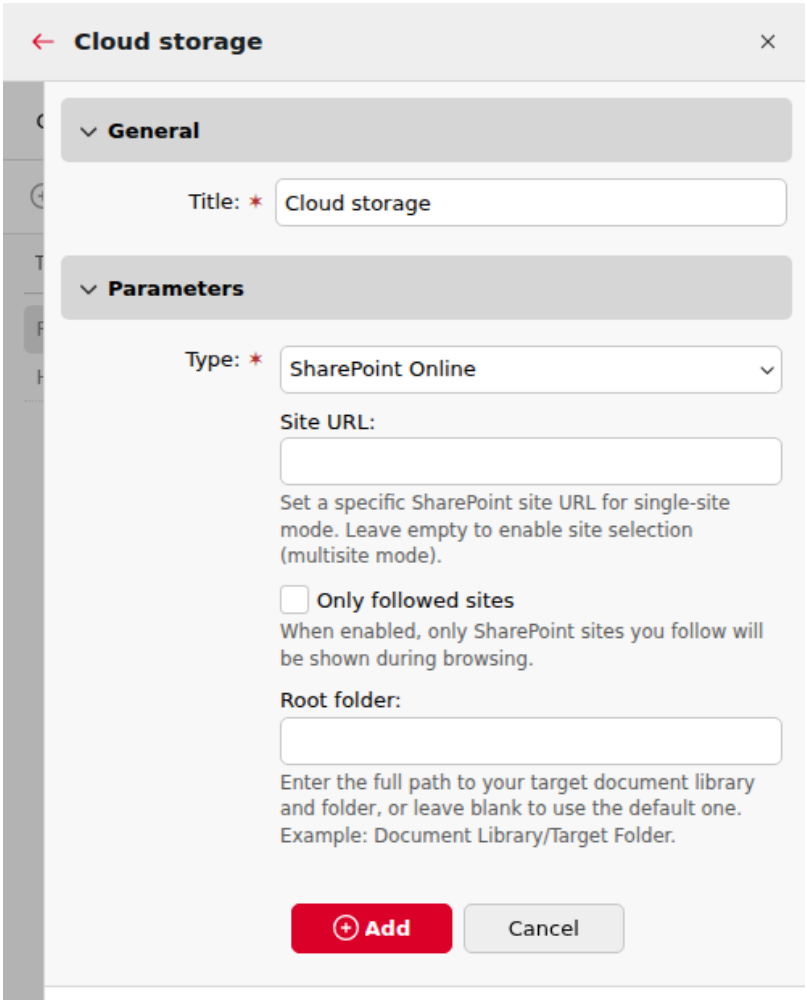
Prerequisites

- A SharePoint Online connection is configured. For more information, see Connect to SharePoint Online (see page 212).

To connect SharePoint Online as a cloud storage to the **Easy Print** terminal action:

1. Go to **MyQ > Settings > Terminal Actions**.
2. If there is an Easy Print action already added, you can configure it by double-clicking it or create a new one by clicking on the actions menu then **Add action into this folder** and selecting **Easy Print** from the list.
3. In the options menu, go to **Storages > Add > Cloud Storage.**
4. Under **General**, enter a name for the cloud storage location
5. Under **Parameters**, select the **Type** (SharePoint Online) from the dropdown

6. (Optional) Specify a **Site URL** and a **Root folder** to specify the location users can print from, optionally with folder browsing. When empty, users select a site at the terminal. When folder browsing is enabled, users can browse locations across SharePoint Online sites.
7. (Optional) Select **Only followed sites** to display only sites that the user follows. This option is unavailable when a Site URL or root folder is specified, and when application-wide access is enabled in the SharePoint Online connection settings.
8. Click **Add** to save the cloud storage location.

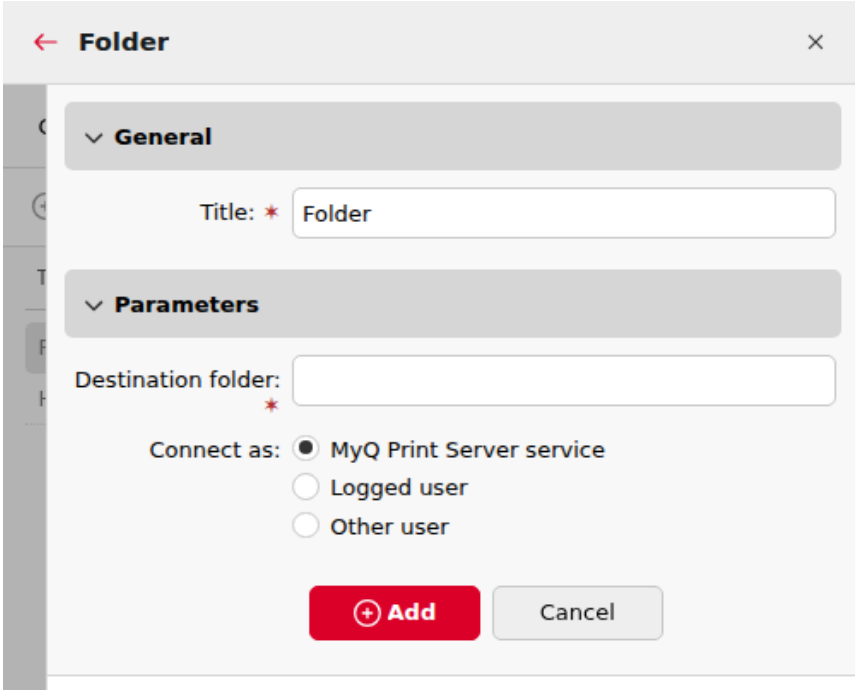


Print from Local Storage

To connect a local storage to the **Easy Print** terminal action:

1. Go to **MyQ > Settings > Terminal Actions**.

2. If there is an Easy Print action already added, you can configure that one by double-clicking it or create a new one by clicking on the actions menu then **Add action into this folder** and selecting **Easy Print** from the list.
3. In the options menu, go to **Storages > Add > Folder.**
4. Under **General**, give your folder a name, and under **Parameters** set up the destination folder. Then click **Add**.



Once this is set up, the user will see the option to browse this folder when using Easy Print.

Note

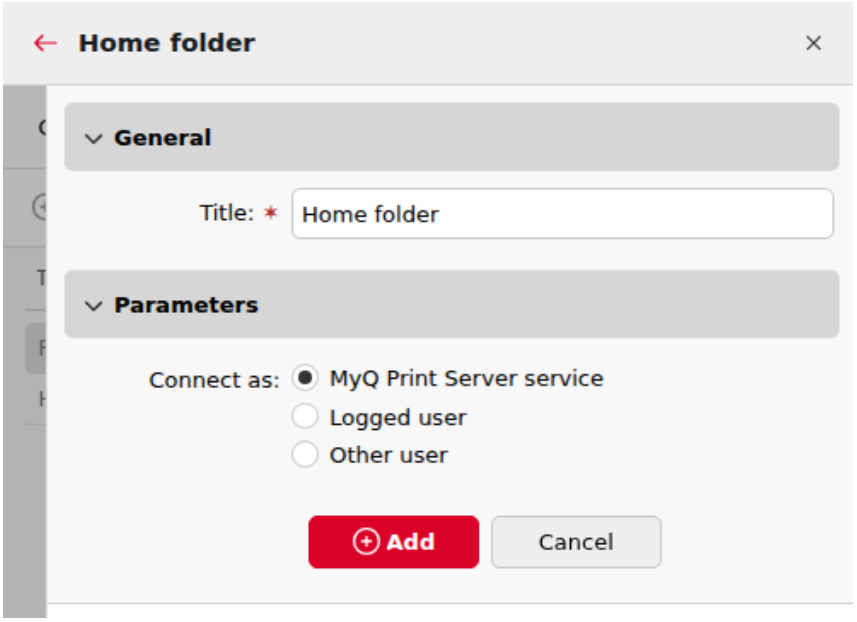
- For hybrid Entra ID users, MyQ uses `NETBIOS\username` for filesystem authentication under **As Logged-in user** or **MyQ service + Make user owner** modes.

Print from User Storage

To connect a user's storage to the **Easy Print** terminal action:

1. Go to **MyQ > Settings > Terminal Actions**.

2. If there is an Easy Print action already added, you can configure that one by double-clicking it or create a new one by clicking on the actions menu then **Add action into this folder** and selecting **Easy Print** from the list.
3. In the options menu, go to **Storages > Add > User's storage.**
4. Under **General**, give your folder a name, then click **Add**.



Once this is set up, the user will see the option to browse this folder when using Easy Print.

Note

- For hybrid Entra ID users, MyQ uses `NETBIOS\username` for filesystem authentication under **As Logged-in user** or **MyQ service + Make user owner** modes.

9.5.10 Easy Copy Settings

With the **Easy Copy** feature, users do not have to go to the often complicated and confusing copy screen of the printing device — they can copy directly from the MyQ terminal home screen with a single touch. Upon tapping the button, MyQ can simply proceed copying using the default settings of the printing device, or it can use different values of the Easy Copy action parameters.

By adding multiple Easy Copy action nodes and giving rights to different users or groups, you can create a variety of copying options for the selected users and groups.

On the **Parameters** tab, you can select from a number of options for each parameter.

> ⚠ All parameters are dependent on the particular printing device type. Therefore, some parameters and/or values might not be available.

Easy Copy Parameters

- **Copies** - Predefine the number of copies to be available *1-99*.
- **Color** - Color scale of the outgoing file. You can select from the following options:
  - Color
  - Monochrome
  - Automatic
  - Default
- **Duplex** - Simplex and Duplex scanning options. You can select from the following options:
  - Single Sided
  - Duplex
  - 1-sided to 2-sided
  - 2-sided to 1-sided
  - Default
- **Original Orientation** - Determines the page's orientation in the outgoing file. The paper's position is relative to the person standing at the printing device. You can select from the following options:
  - Top Edge on Top: The page is displayed in a horizontal position (top edge of the page opposite to the person)
  - Top Edge on Left: The page is displayed in a vertical position (top edge of the page on the left hand side of the person)
  - Default
- **Density** - Density of the picture in the outgoing file. The higher it is, the darker the resulting picture is. You can select from the following options:
  - Automatic
  - Lowest
  - Lower
  - Low
  - Normal
  - High
  - Higher
  - Highest

    - Default
- **Size** - Size of the scanned input. It determines the size of the scanning area; therefore, it should correspond to the actual size of the scanned paper. You can select from the following options:
    - Automatic
    - A3
    - A4
    - A5
    - A6
    - B4
    - B5
    - B6
    - Folio
    - Ledger
    - Letter
    - Legal
    - Statement
    - Default
- **Magnification** - With this parameter, you can determine the size of the copy. This way, you can make it smaller or larger than the original file. You can select from the following options:
    - Default
    - Same as original
    - A3
    - A4
    - A5
    - A6
    - B4
    - B5
    - B6
    - Folio
    - Ledger
    - Letter
    - Legal
    - Statement
- **Skip blank pages** - With this parameter, you can select to skip blank pages in the copied document. You can select from the following options:
    - Default
    - Yes
    - No
- **Mixed size** - This parameter enables automatic paper size recognition when different sizes of paper are used during copying.

- Yes: The output paper size parameter will be ignored and be decided by the device itself depending on the scanned image size.
- No: The output paper size must be set (everything but Auto) and the image will be zoomed and scanned to the same size.
- Default

General Limitations

- The exact list of supported parameters for Easy Copy depends on each vendor/machine.
- Continuous Scan is not supported by all machines even within the same brand.
- Continuous Scan jobs consisting of different formats may account the whole job as one format or different formats depending on SDK abilities. The final format (in case of single format accounting) also depends on SDK abilities.

Vendor Compatibility Specifics

Easy Copy compatibility may differ between brands. Please check the relevant terminal documentation for more details.

- MyQ Brother Embedded
- MyQ Canon Embedded
- MyQ Epson Embedded
- MyQ Fujifilm Embedded
- MyQ HP Embedded
- MyQ KATUN Embedded
- MyQ Kyocera Embedded
- MyQ Kyocera Embedded Lite
- MyQ Lexmark Embedded
- MyQ Ricoh SmartSDK Embedded
- MyQ Sharp Embedded
- MyQ Sharp Luna Embedded
- MyQ Toshiba Embedded
- MyQ Xerox Embedded

9.5.11 Easy Fax Settings

With the Easy Fax feature, users can fax their scanned documents in just two steps; all they need to do is tap the Easy Fax button on the home screen of the embedded terminal, and then type the fax number.

By adding multiple Easy Fax action nodes and giving rights to different users or groups, you can create a variety of faxing options for the selected users and groups

To enable the feature on a printing device, you need to enable the **Fax module** option on its properties panel in MyQ, deactivate and reactivate the device. Go to **MyQ > Settings > Configuration Profiles**. Select the configuration profile and click **Edit** (or double-click, or right-click and **Edit**). The properties panel opens on the right side. In the **General** tab, mark the **Fax module** checkbox. Click **Save**.

On the **Parameters** tab, you can select from a number of options for each parameter.

⚠ All parameters are dependent on the particular printing device type. Therefore, some parameters and/or values might not be available.

Easy Fax Parameters

- **Fax resolution** - Resolution of the outgoing fax file. You can select from the following options:
  - Normal
  - Fine
  - Super Fine
  - Ultra Fine
  - Default
- **Duplex** - Simplex and Duplex scanning options. You can select from the following options:
  - Single Sided
  - Duplex - binding on top
  - Duplex - binding on side
  - Booklet - binding on left
  - Booklet - binding on right
  - Default
- **Original Image** - Determines the way in which the printing device is going to process the scanned page. You can select from the following options:
  - Text + Photo
  - Photo
  - Text
  - Default
- **Size** - Size of the scanned input. It determines the size of the scanning area; therefore, it should correspond to the actual size of the scanned paper. You can select from the following options:
  - A3
  - A4
  - A5
  - A6

    - B4
    - B5
    - B6
    - Folio
    - Ledger
    - Letter
    - Legal
    - Statement
    - Oficio II
    - Default
- **Original Orientation** - Determines the page's orientation in the outgoing file. The paper's position is relative to the person standing at the printing device. You can select from the following options:
    - Top Edge on Top
    - Top Edge on Left
    - Default
- **Density** - Density of the picture in the outgoing file. The higher it is, the darker the resulting picture is. You can select from the following options:
    - Automatic
    - Lowest
    - Lower
    - Low
    - Normal
    - High
    - Higher
    - Highest
    - Default
- **Continuous scan** - With the continuous scan option *Enabled*, scan jobs are not sent until **Done** is tapped. After clicking **Scan**, the printing device scans another page. You can select from the following:
    - Disabled
    - Enabled
    - Default

Vendor Compatibility Specifics

Easy Fax compatibility may differ between brands. See the relevant terminal documentation for more details.

- MyQ Brother Embedded
- MyQ Canon Embedded
- MyQ Epson Embedded
- MyQ Fujifilm Embedded

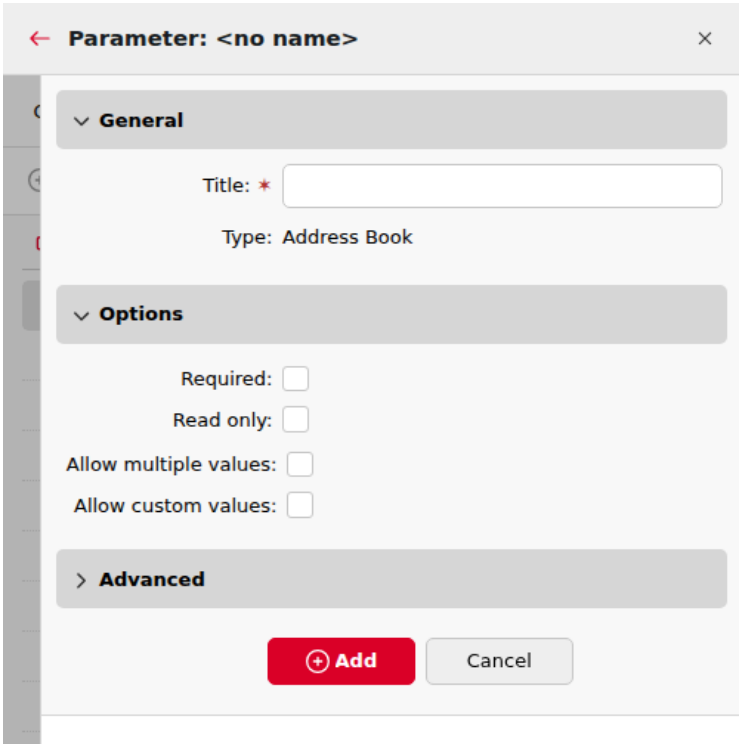
- MyQ HP Embedded
- MyQ KATUN Embedded
- MyQ Kyocera Embedded
- MyQ Kyocera Embedded Lite
- MyQ Lexmark Embedded
- MyQ Ricoh SmartSDK Embedded
- MyQ Sharp Embedded
- MyQ Sharp Luna Embedded
- MyQ Toshiba Embedded
- MyQ Xerox Embedded

Fax to a Contact from Address Book

To enable the Address Book parameter, the administrator has to set it up as a custom parameter for the Easy Fax action.

See also:

- Create Custom Parameters (see page 334)



It is not necessary to enable the Required field, as the Fax destination field is already mandatory in the Easy Fax's Phone Book where the user will be selecting contacts from their Address Book.

Once done, users can manage their Address Book on the MyQ Web UI and faxes are sent to the contact from the users Address Book.

Accessing and Using Address Book

1. Log in to MyQ.
2. In the main menu, select **Address Book**.

Address Book is not available to built-in accounts such as *admin.

3. The Address Book shows the contact list with available columns:
    - **Full name**
    - **Email**
    - **Fax number**

Managing Contacts

1. To add a contact, click on **Add contact**. A pop-up appears where you can enter the contact's **Full Name**, **Email**, and **Fax Number**.
2. To edit or remove a contact, locate the contact from the list and choose the respective option.
3. For searches, use the left pane. Options available: **All Contacts**, **Email Contacts**, **Fax Contacts**, and **Deleted**.
4. In the **Deleted** section, you can either **Restore** or **Permanently Remove** a contact.

All email inputs undergo validation checks to ensure they are of a valid email format.
Fax numbers are saved without validation. Make sure your users understand what number formats are supported by Fax devices.

Using Address Book in Easy Fax

1. Log in to the terminal.
2. Choose **Easy Fax**.
3. In the parameters, select the **Address Book** option.
4. Browse and select a contact from your list as the destination.

> A user can only access contacts from their own Address Book. Accessing the contacts of another user, even by administrators, is prohibited.

9.6 Release Stations

A Release Station is a browser-based kiosk application for secure job release on printers without embedded terminals. It provides a simplified My Jobs experience: users authenticate, view their queued jobs, and release them to a printer.

Release Station supports **Pull Print** and **Delegated Print** queues.

Typical deployments range from shared printing rooms to single-device kiosks:

- **Release Station** - A printing room with a pool of managed printers where users can select a printer and release their job.
- **Release Kiosk** - A single-printer enclosed in a self-service unit with a built-in touchscreen. Users authenticate, release their jobs, and collect the printed documents from the unit's output tray.

A Release Station is accessed via a dedicated URL in the format `https://<hostname>:<port>/release-station/<URL name>`. Users access the Release Station on a touchscreen device in kiosk mode, running a web application or kiosk Android app. After authenticating with a PIN, ID card, or their MyQ account credentials, users select a printer (if applicable), select their jobs, and release them for printing.

9.6.1 Licensing

Each printer in a Release Station consumes one Embedded Lite license, which is equivalent to half of one Embedded Terminal license. Only printers with a valid Embedded Lite license assigned are available in the **Select Printer** dialog in the Release Station app.

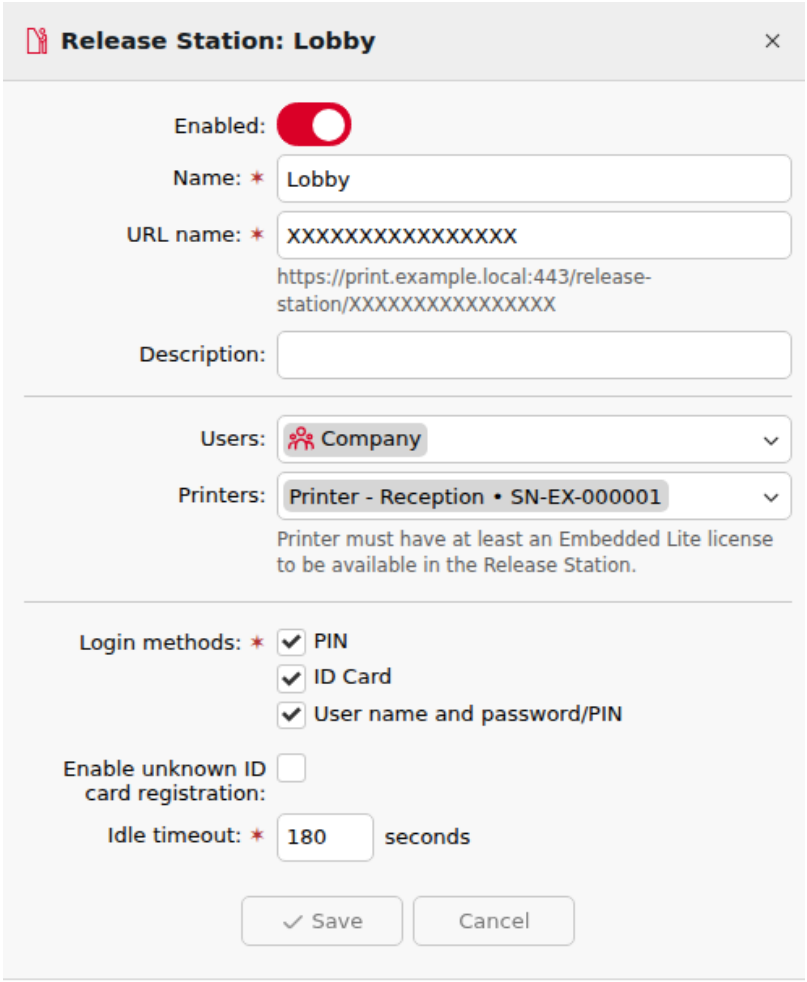
9.6.2 Release Stations Settings

To manage Release Stations, make sure that you have **Administrator** or **Manage Settings** permissions. Then go to **MyQ > Settings > Printers & Terminals > Release Stations**.

Administration actions on Release Stations are recorded in the Audit Log.

To create a release station:

1. Click **+Add**.
2. Fill in the Release Station properties. See below for field descriptions and allowed values.
3. Assign one or more printers.
4. Assign user groups or individual users.
5. Click **Save**.



9.6.3 Release Station Properties

- **Enabled**: Switches the Release Stations on and off. When disabled, users cannot log in to the Release Station.
- **Name**: The name of the Release Station, displayed in the Release Station app.
- **URL name:** The name used in the Release Station URL. Defaults to a random string to keep the URL difficult to guess. This can be changed to a human-readable value if required.
- **Description**: (Optional) An description displayed only in the Release Stations list in the administrator interface.
- **Users**: The users or groups permitted to log in to this Release Station.
- **Printers:** The printers controlled by this Release Station. Assign a single printer for release kiosk mode.
- **Login methods:** The login methods available to users on this Release Station. Select one or more of the following:
  - **PIN:** User logs in by entering their PIN only.
  - **ID Card:** User logs in by swiping their ID card.
  - **User name and password/PIN:** User logs in by entering their MyQ user name, followed by their password or PIN.

  All three methods are enabled by default. At least one method must remain selected. The Release Station login screen adapts its layout to match the enabled methods.
- **Enable unknown ID card registration:** (Optional) When enabled, users can swipe an unregistered ID card. This prompts the user to log in using their user name with their password or PIN.
- **Idle timeout:** The period of inactivity (in seconds) after which the Release Station automatically logs out the current user (default: 180 seconds). A timer appears in the header of the user interface.

9.6.4 Running a Release Station in Kiosk Mode

Release Stations are designed to run in a browser's kiosk mode on a dedicated touchscreen device, in landscape or portrait orientation. Kiosk mode prevents users from navigating away from the application.

Using Microsoft Edge (Recommended on Windows)

1. Install Microsoft Edge on the kiosk device.
2. Launch Edge in kiosk mode using the following command, replacing the URL with your Release Station URL:

```
msedge.exe --kiosk "https://<server-address>:<port>/release-station/
<url-name>" --edge-kiosk-type=fullscreen
```

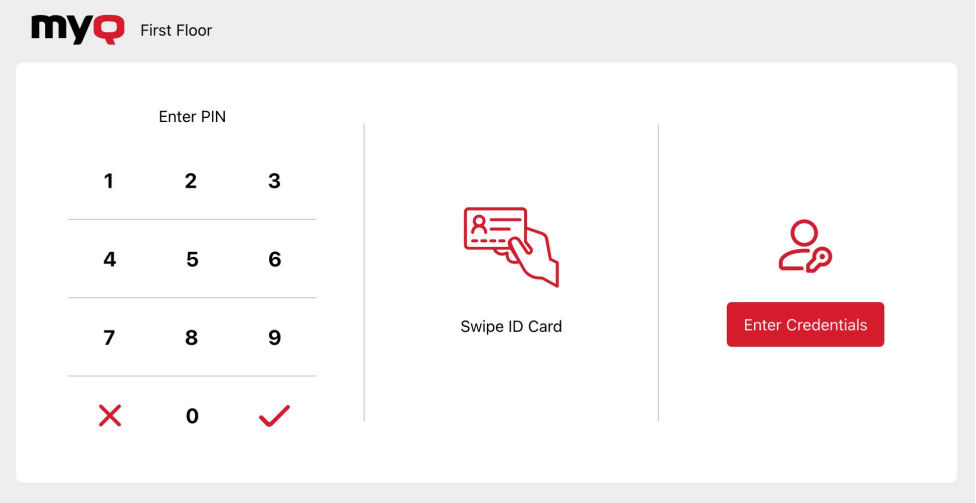
In full-screen kiosk mode, Edge hides the address bar and browser controls, and the browser automatically restarts if it crashes. For details on configuring Microsoft Edge kiosk mode, see the Microsoft Edge kiosk mode documentation[30].

9.6.5 Releasing Jobs

To send print jobs to a Release Station, print to any Pull Print or Delegated Print queue whose printers are assigned to the Release Station.

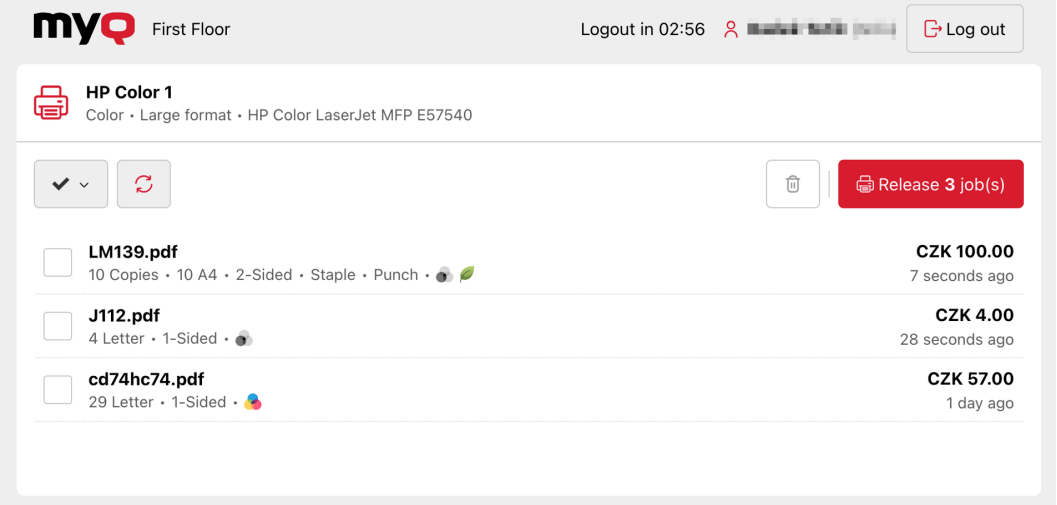
To release print jobs at a Release Station, follow these steps:

1. Log in using one of the available methods:
   - **PIN**: Enter your PIN on the keypad.
   - **ID Card:** Swipe your ID card.
   - **Enter Credentials:** Tap and log in with your MyQ username and password.



2. **Select a printer** from the list. If the Release Station has only one printer assigned, this step is skipped automatically.
3. **Select jobs** from your job list.

30. https://learn.microsoft.com/en-us/deployedge/microsoft-edge-configure-kiosk-mode



4. Select the **Release** button to print the selected jobs. The job list displays available jobs, and shows the following information for each job, where available:
    - Job name
    - Copy count
    - Page count and paper size
    - 1-sided or 2-sided
    - Staple flag
    - Punch flag
    - Color or monochrome
    - Eco print
    - Spooling time/date (relative)
    - Price (displayed if a pricelist is assigned to the **No Terminal** configuration)
5. Select **Log out** to end your session, or wait for the logout timer to expire.

Toolbar Actions

The job list toolbar provides the following actions:

- **Selection drop-down**: Commands to select or deselect jobs.
- **Refresh**: Reloads the job list.
- **Delete**: Deletes the selected jobs.
- **Release**: Releases the selected jobs to the chosen printer. Displays the count of jobs and total price if the user has a credit account.

9.6.6 Unknown ID Card Registration

If **Enable unknown ID card registration** is turned on for a Release Station and a user swipes an ID card that is not registered to any account, a prompt appears offering to add the ID card to their account.

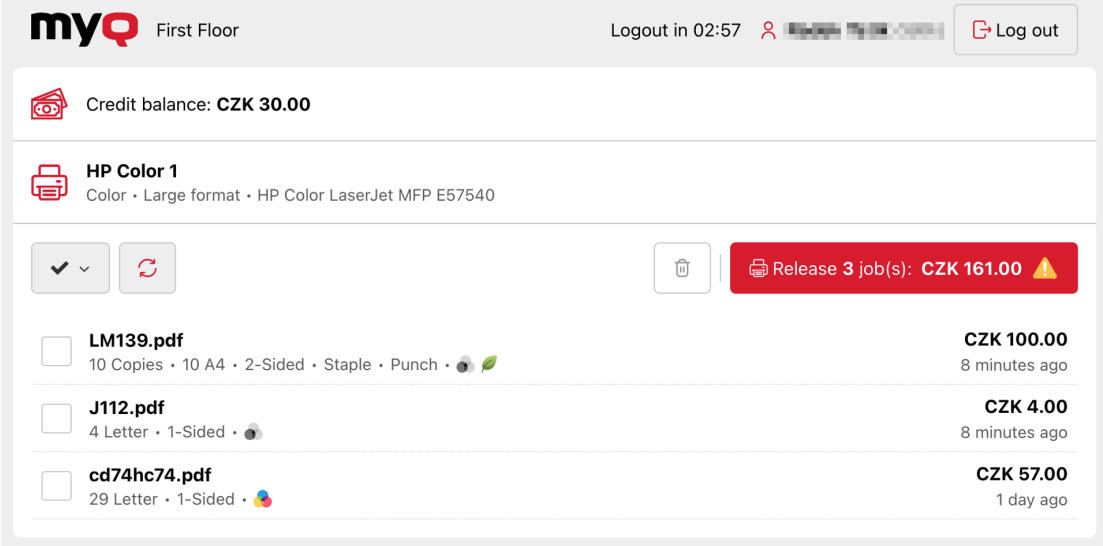
If the user taps **Yes** to register the card, they are prompted to enter their username, followed by their password or PIN. After a successful login, the card is added to the user's account. If the ID Card login method is enabled, the user can now log in by swiping their ID card.

9.6.7 Credit and Quotas

If the user account has credit or quota enabled, the current balance or quota status is displayed on the Jobs page after login.

With Credit Enabled

If credit is enabled, the current credit balance is displayed on the Jobs page. The Release button displays the total price of all selected jobs. If the total price exceeds the current balance, a warning icon is displayed. If the user taps **Release** anyway, an "Insufficient credit balance" error message is displayed.



With Quotas Enabled

If quota is enabled, the current quota status is displayed on the Jobs page. Each quota is displayed as a progress bar showing the quota type (total, color, mono, or

cost) and the remaining count. The progress bar shows what percentage of the quota remains. When the remaining count reaches the warning threshold, the bar turns red.

If the user has multiple quotas, the quota with the smallest remaining count is displayed for each quota type.

With Both Credit and Quota Enabled

If the user account has both credit and quota enabled, the Release Station displays credit or quota information based on the **Payment account priority** setting configured in **MyQ > Settings > Accounting**.

9.6.8 Limitations

- **Cost Centers:** Release Stations do not support Cost Centers accounting mode.
- **Quotas**: If the user's quota sufficient to start a job, the job is released. Release Station cannot interrupt a job if it exhausts the user quota mid-way through the job.
- **Projects:** When enabled, only jobs with a preassigned project can be released. Jobs without an assigned project are displayed but cannot be selected for release.
- **ID card readers** must be in keyboard emulation mode.
- **Personalization features,** such a custom logo, are not currently supported by Release Station.

See also:

- Microsoft Edge kiosk mode documentation[31]
- (v2) Printing with MyQ
- Queue Types (see page 533)
- Credit (see page 638)
- Quotas (see page 654)
- Accounting Settings (see page 249)
- ID Card Management (see page 508)

9.6.9 Set Up an Android Tablet with the MyQ Kiosk App

The MyQ Kiosk App runs as a device-locked interface enabling users to log in and release their print jobs at a Release Station. This procedure describes how to set up

31. https://learn.microsoft.com/en-us/deployedge/microsoft-edge-configure-kiosk-mode

an Android tablet as a dedicated kiosk device running the MyQ Kiosk App, and connect it to your Release Station.

Prerequisites

- A factory-resettable Android tablet
- Network credentials
- MyQ Release Station connection details

During set up scan the QR code to install the MyQ Kiosk App:

For manual installation, download the installer here:

- MyQ Kiosk App .apk[32]

Part 1: Set Up the Android Tablet

1. Factory reset the device.
2. On the Welcome screen, **do not tap Start**.

   Tap a blank part of the screen seven times in rapid succession.

32. https://docs.myq-solution.com/__attachments/a_30493ebfee7f9f6f260e9ec80a462525f50373a52eb75f2edd69b2bba4f5c9bd/kiosk-release.apk

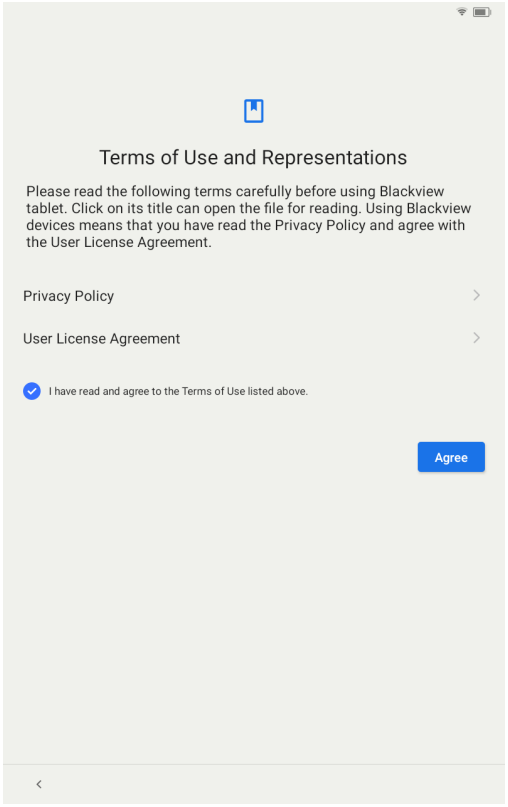


The QR scanner opens.

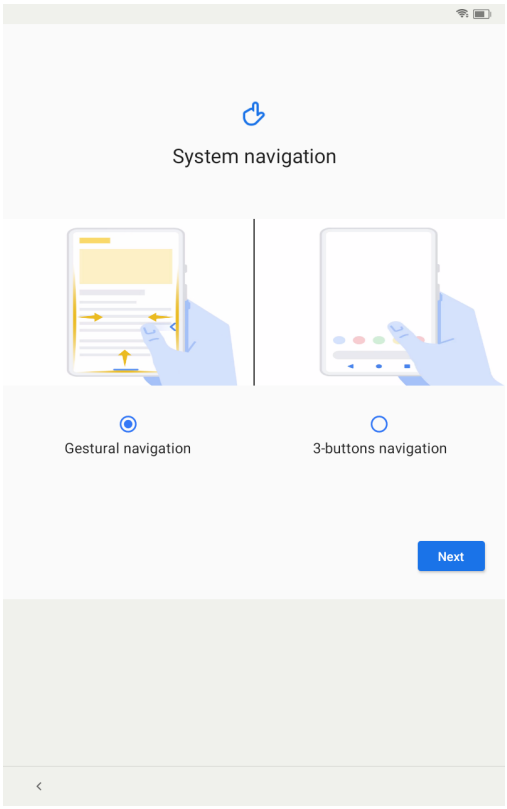
3. Scan the QR code to download the MyQ Kiosk App installer.
4. Connect the tablet to your network, and select that network.

   The *Getting Your Tablet Ready* screen appears.
5. Continue through the steps, and restart the device if prompted. When you see *This Device Belongs to Your Organization*, tap **Next**.
6. When the screen shows *Let's set up your work device,* tap **Accept & continue**.
7. When the message *This device isn't private* appears, review the privacy information and tap **Next**.

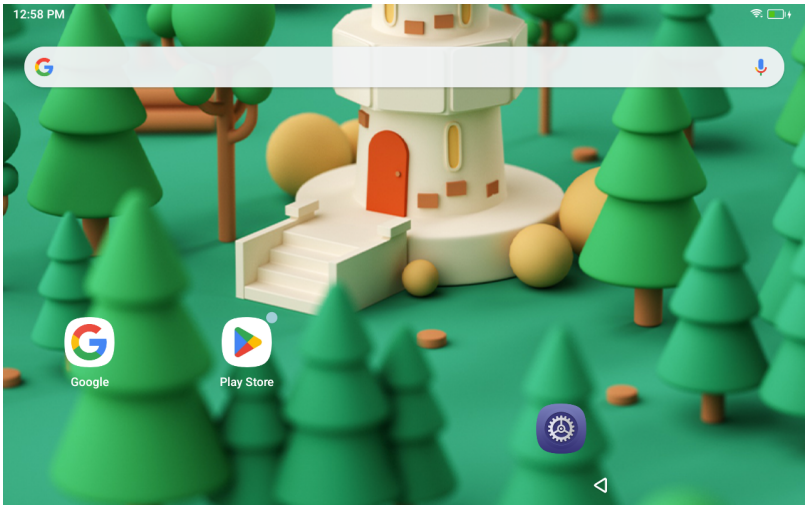
8. On the **Google Services** screen, choose your preferred options and tap **Accept**.
9. On the **Terms of Use and Representations** screen, agree to the Privacy Policy and User License Agreement.



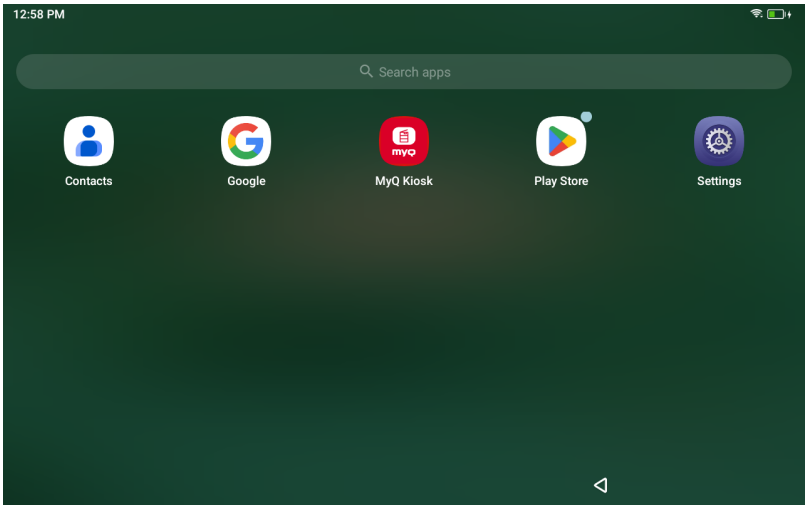
10. Under **System Navigation**, select a navigation mode and tap **Next**.



Setup is complete. The device returns to the home screen.



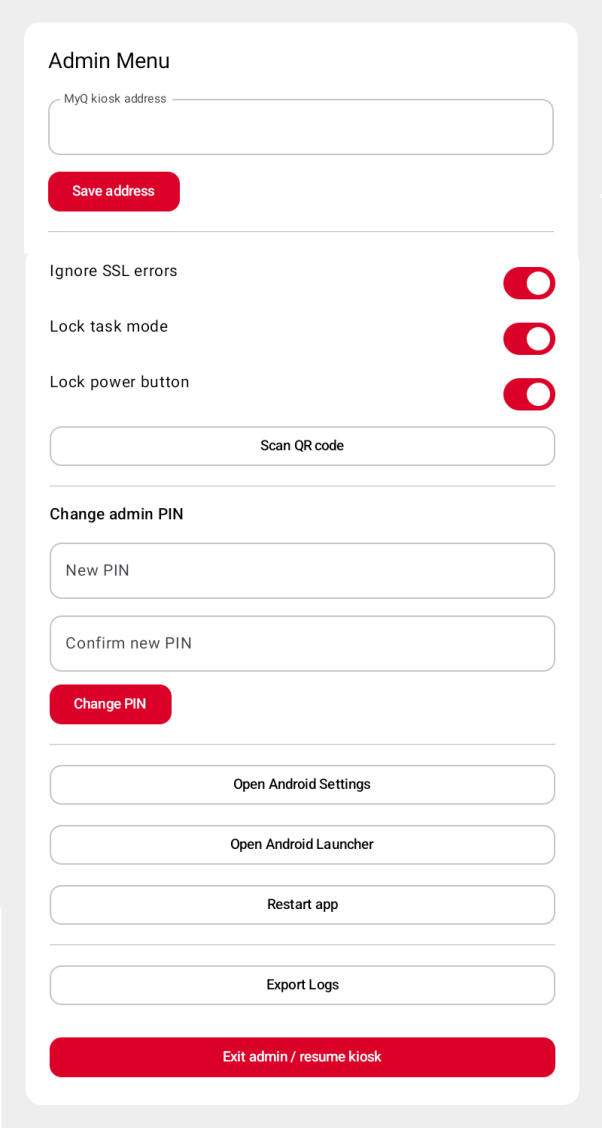
11. To verify your setup, swipe up on the home screen and verify that MyQ Kiosk appears among your apps.



Next, configure the MyQ Kiosk app.

Part 2: Configure the MyQ Kiosk App

1. From the home screen, swipe up to open the app list and tap **MyQ Kiosk**. The app opens with the message *MyQ Kiosk is not configured yet. Ask an administrator to set the kiosk address.*
2. To enter admin mode, tap the bottom-left corner of the screen seven times in rapid succession, then enter the admin PIN (default: `1234`).



3. Configure the following admin settings as needed:
    - **MyQ kiosk address**: the URL of your release station.
    - **Ignore SSL errors**: (recommended) prevent SSL errors from blocking communications. Use this, for example, in environments where self-signed certificates are used.
    - **Do not cache login credentials**: (recommended) prevent the app from storing user credentials.
    - **Lock Task Mode**: (recommended) restrict the device to the MyQ Kiosk App only, other apps cannot be used.
    - **Lock Power Button**: disable users from restarting the device by pressing the power button.
    - **Scan QR Code** *(coming soon)*: scan a QR code generated by the MyQ Server to automatically populate the Admin Menu settings.

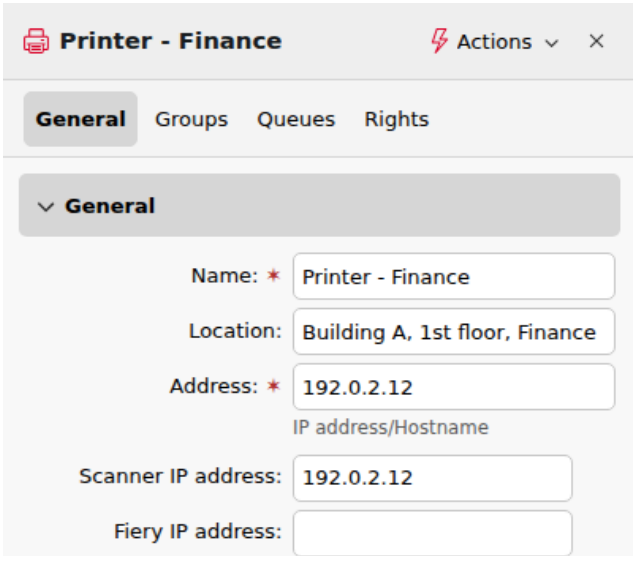
- **Change admin PIN**: (recommended) change the default `1234` to a unique value, then tap **Change PIN**.
- **Open Android Settings:** open the Android system settings. Because the MyQ Kiosk App is set as device administrator, this is the *only* way to reach system settings (for example, to change the time zone or keyboard).
- **Open Android Launcher**: access the Android home screen. Because the MyQ Kiosk App is the device administrator, this is the *only* way to reach the home screen.
- **Restart app:** close and restart the Kiosk App, returning to the home screen.
- **Export Logs:** export logs as a plain-text archive to `Downloads/MyQKioskLogs` on the device. Retrieve the file via USB or any other file-sharing method available on the device.

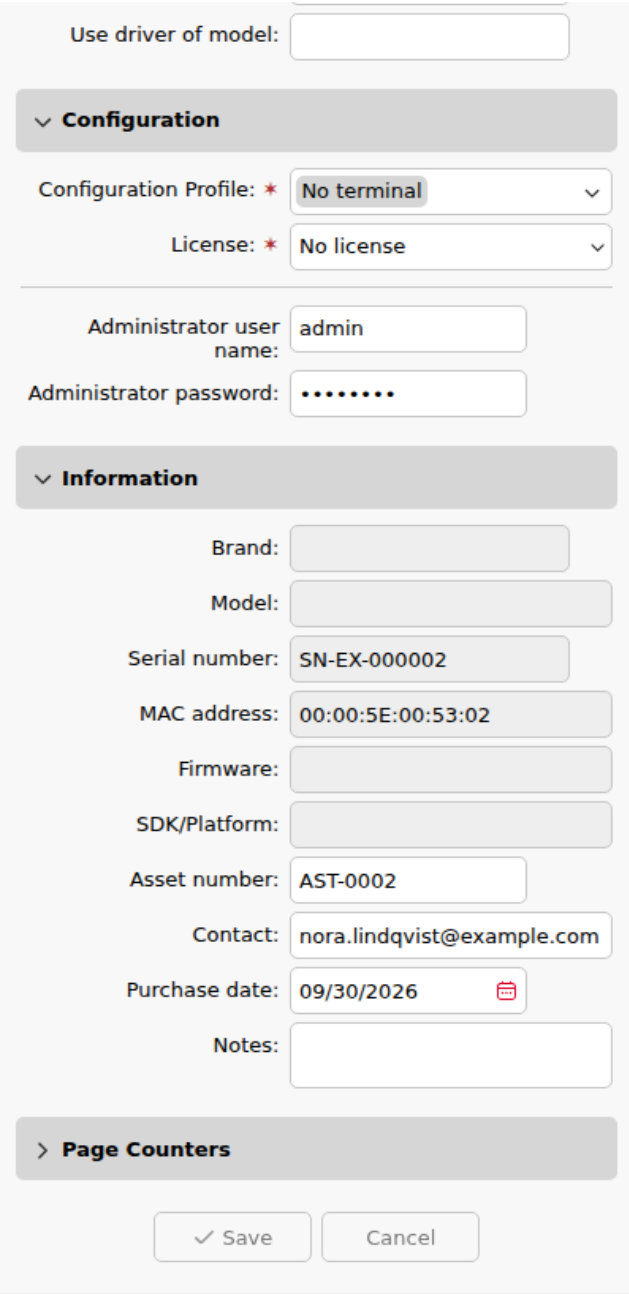
4. Tap **Exit admin / resume kiosk** to return to kiosk mode. If you have configured the Release Station URL correctly, the login screen appears and the device is ready for use.

9.7 Managing Printers

Each individual printing device has its own properties panel. To open the panel, double-click the printing device on the list of printing devices on the **Printers** main tab. The properties panel opens on the right side of screen. There you can **Deactivate** it or perform some specific **Actions** on this printer.

The panel is divided into four tabs: **General, Groups, Queues** and **Rights**. On the **General** tab, you can change the printing device settings, on the **Groups** tab, you can add the device to groups, on the **Queues** tab, you can add the printing device to queues and on the **Rights** tab you can give user rights to the device.





9.7.1 Printer Information and Settings

The settings mentioned below are basic printer settings displayed on each printer's properties panel. Required fields are marked with an asterisk (*).

General

- **Name***: Name of the printing device, any string can be used.
- **Location**: If it is required, you can specify the location of the printing device here.
- **IP address/Hostname***: The IP address or hostname of the printing device.

- **Scanner IP address**: The IP address of the scanner (if the device scanner has a different IP than the printing device).
- **Fiery IP address**: The IP address of the Fiery module (if the device is equipped with it).
- **Use driver of model**: Alternative model name. If your printing device is not listed in the current database of supported models, you can enter the type of supported printing device which stands close to your model. For more information, contact MyQ Support.

Configuration

- **Configuration Profile**: Select a profile from the drop-down or create a new one to embed the printer by clicking **+Add new**. Then add a **Name**, install the **terminal package**, set the **Login methods** and the **Printer credentials,** as applicable to the printer.
- **License:** Assign a license to the printer. After modifying this field, you must reactivate the printer.
- **Administrator user name**: Enter the admin user name. If you embed the printer separately this user name should match the one in the configuration profile.
- **Administrator password**: Enter the admin password. If you embed the printer separately this password should match the one in the configuration profile.

For Xerox devices, the administrator user name and password are a **mandatory requirement** for the device's remote setup and activation (both for devices with embedded terminals and without).

Information

- **Brand:** Information about the printing device manufacturer. It is automatically detected from the device.
- **Model:** Information about the printing device model name. It is automatically detected from the device.
- **Serial number**: The printing device serial number. It is automatically detected from the device.
- **MAC address**: The printing device MAC address. It is automatically detected from the device and it is used as a unique identification of the device in the MyQ system. Therefore, only one device with a particular MAC address can be activated.
- **Firmware**: The current firmware the device is running, this may not be visible depending on the device.

- **SDK/Platform:** The current platform the device is running, this may not be visible depending on the device.
- **Asset number**: Additional option for identification of the printing device.
- **Contact:** Contact info of the person responsible for the printing device maintenance.
- **Purchase date**: Purchase date of the printing device.
- **Notes:** Additional information about the printing device.

Page Counters

- **Black & White Print**: Total amount of B&W pages printed on the device.
- **Color Print**: Total amount of color pages printed on the device.
- **Black & White Copy**: Total amount of B&W pages copied on the device.
- **Color Copy**: Total amount of color pages copied on the device.
- **Single color copy**: Total amount of single color pages copied on the device.
- **Scanner:** Total amount of pages scanned on the device.
- **Fax:** Total amount of incoming faxes printed on the device
- **Print total counter adjust for load balancing**: The entered value is added to the printed pages counter to evenly spread print load between devices in tandem queues.

9.7.2 Deleting and Restoring Printers

If you delete a printing device, you will not be able to use it, but its data will be permanently stored in the MyQ database.

It is not possible to add the same device twice as its MAC address is unique and there cannot be two devices with an identical MAC address in the system. If you want to use the deleted device again, you have to restore and reactivate it.

Deleting Printers

To delete selected printing devices:

1. Select the printing devices you want to delete from the list on the **Printers** main tab.
2. Right click the device or click **Actions**. The Actions drop-down appears.
3. Click **Delete**. You can find the deleted printing devices under the **Deleted** search option.

Restoring Printers

To restore selected printing devices:

1. On the group tab on the left side of the **Printers** main tab, under **Searches**, select the **Deleted** search option. The list of deleted printing devices appears.
2. On the list, select the printing devices that you want to restore, right click the device or click **Actions**. The Actions drop-down appears.
3. In the drop-down, click **Restore**. The restored printing devices are not active; you have to activate them again.

9.7.3 Activating and Deactivating Printing Devices

Unless it was automatically activated during printer discovery, a newly added device is not active in MyQ and some of its data is not displayed (its serial number, type, counters, etc.). The next step is to activate the device. Although there is no limit to the number of printing devices you can add to the MyQ system, you cannot activate more printing devices than your license allows.

To activate selected printers:

1. After selecting the printers, right-click and click **Set configuration profile**. A pop-up window with a dropdown list of options opens.
2. Select a profile from the drop-down and click **OK**.
3. With your selection still intact, right-click once more and select **Activate**.

To activate all printers:

1. On the bar at the top of the **Printers** main tab, click **Actions**. The Actions drop-down appears.
2. Click **Activate all**.

To deactivate printing devices

1. On the list of printers on the **Printers** main tab, select the devices that you want to deactivate, and then click **Actions**. The Actions drop-down appears.
2. In the drop-down, click **Deactivate**.

9.7.4 Printer Groups

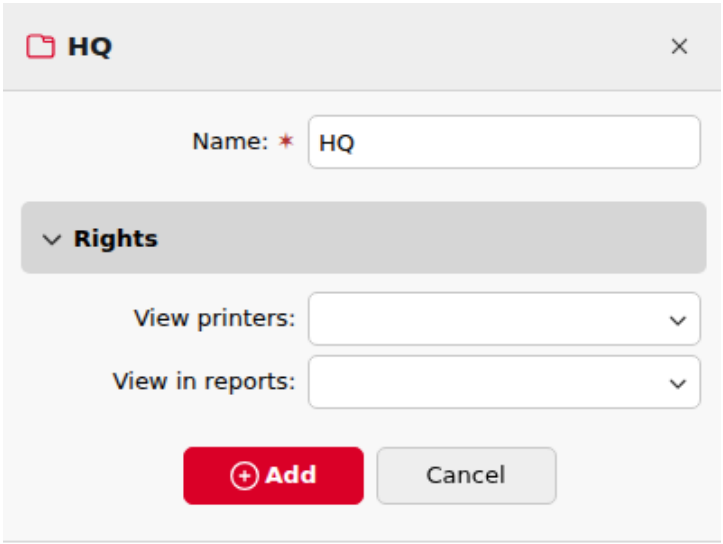
All printing devices in MyQ can be divided into groups based on their location, model, vendor, category, etc.

On the **Printers** main tab, you can create new groups of printing devices. There are a number of MyQ functions where groups are used, for example, they can be assigned

to particular print queues , users can be given rights and restrictions concerning particular groups, and reports can be set about particular groups only.

Creating Printer Groups

1. On the left side of the **Printers** main tab, right-click **All printers**, and then click **+Add group** on the shortcut menu. The new group properties panel opens on the right side of the screen.
2. On the panel, enter the name of the new group, give rights to users or groups of users, and then click **Save**.



Printer group rights:

- **View printers**: The right to see and manage printers from this group on the web user interface.
- **View in reports**: The right to see this group of printers in reports.

If you want the new group to be placed under an already existing group, select the parent group, and then click **+Add Group** (or right-click the parent group, and then click **+Add Group** on the shortcut menu).

Deleting Printer Groups

To delete a group of printing devices:
On the group tab on the left side of the **Printers** main tab, right-click the group you want to delete, and then click **Delete** on the shortcut menu.

Add a Printer to a Group

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, and then click **OK**.

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

Remove a Printer from a Group

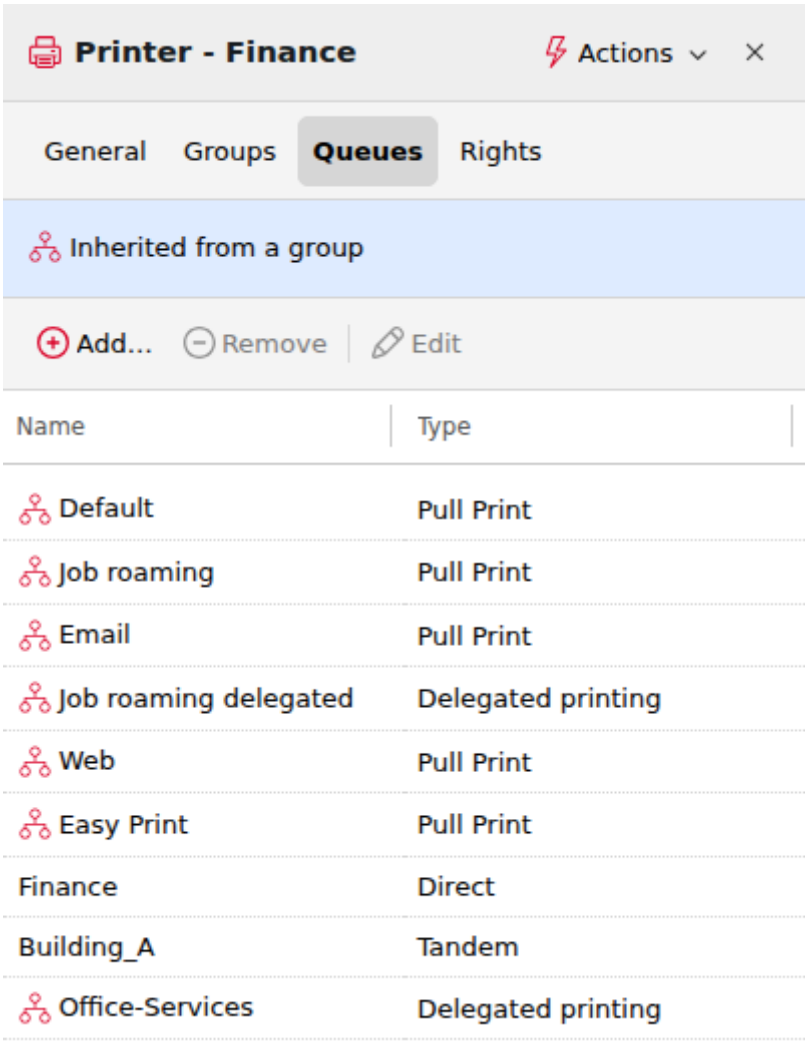
On the bar at the top of the **Groups** tab, click **–Remove**. The group disappears from the **Groups** tab.

To remove selected printing devices from a group on the **Printers** main tab, select the group there, select the printing devices that you want to remove, click **Actions**, and then click **Remove from group** in the **Actions** drop-down (or right-click the printer and click **Remove from group**).

9.7.5 Editing Printer Queues

To add a printer to a queue:

1. On the bar at the top of the **Queues** tab, click **+Add**. A search box appears to the left.
2. In the search box, find the queue where you want to add the device to, and then click **OK**.



To remove a printer from a queue:

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

9.8 Monitoring Network Printers in Offline Mode

The usual way of communication between the MyQ system and a printing device is via SNMP protocol. In case this method cannot be used, for example if the printing device does not support the SNMP protocol, you can use the MyQ parser to monitor the number of pages and other basic properties of jobs sent to be printed on a printing device. This accounting method is referred to as **Offline accounting**.

A disadvantage of the offline accounting feature is its inaccuracy. Due to the fact that the communication of MyQ and the printing device is one-sided and restricted to sending print data to the device, it is not possible to check if the data is actually printed. Therefore, MyQ charges the print job based on the information from the job parser received after the job is sent to the printing device. Even if the print job is canceled halfway through the print, it is charged as a whole.

To enable the offline accounting mode of a printing device:

1. On the **Printers** main tab, double-click the printing device to open its properties panel.
2. On the panel, in the **Use driver of model:** text box, enter the value *offline*, and then click **Save**.

Before enabling the offline accounting mode, deactivate the printing device. The **Use driver of model:** setting cannot be changed on activated printing devices. Once you enable the offline accounting mode, reactivate the printing device.

9.9 Monitoring Local Printers

Besides monitoring network printers, MyQ is able to monitor the number of printed pages on devices connected locally, via a parallel port or a USB port. In such cases, the number of printed pages is extracted from the print spooler as it is being processed by the print driver.

To extract the data provided by the spooler, you need to install the MyQ Desktop Client application to all the computers that you print from to MyQ, and set up **Local Print Monitoring** there. All jobs sent to selected types of ports will be detected from the print spooler.



Local Print Monitoring is available in MyQ Desktop Client.

See: (10.2) Local Print Monitoring

A disadvantage of the local print monitoring feature is its inaccuracy. As the communication of MyQ and the local printing device is one-sided and restricted to sending print data to the device, it is not possible to check if the data is actually printed. Therefore, MyQ charges the number of pages extracted from the spooler when they are sent to the printing device. Even if the print job is canceled halfway through the print, it is charged as a whole.

9.9.1 Accounting on Local Printers

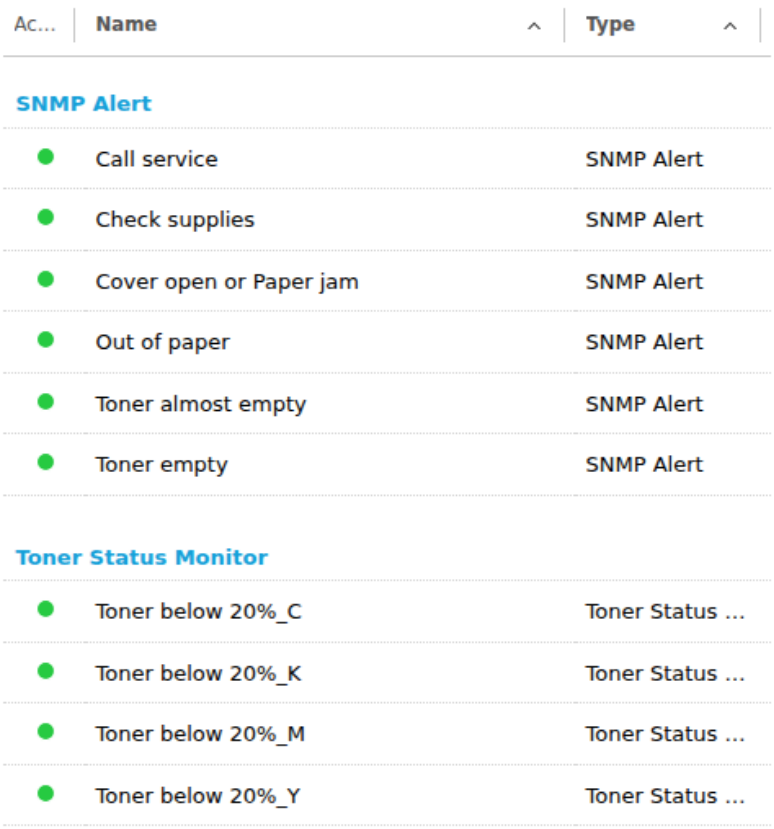
After a print job is sent to one of the local printing devices, the number of pages and other information about the print job are saved to the MyQ Desktop Client folder of the particular registry file. Once the connection with the MyQ server is established, all the information is automatically transferred to the MyQ server and deleted from the registry. Therefore, it is not necessary to be permanently connected to the MyQ Server online.

Once the server is connected and data is sent to the server, information about the job appear in an **Info** entry in the MyQ log. Each entry contains information about the user who printed, the printing device that the user printed on and the number of printed pages. The MyQ server automatically creates a new local type printing device. Its name has the following form: *printer@computer*.

An appropriate price list can be set for local printing devices. Therefore, they can be included in the monetary reports. If the user that prints on the local printing device already exists, their prints are simply assigned to them. Otherwise, the job is accounted to the ***unauthenticated user**.

9.10 Printer Events

Printer Events are customizable actions initiated by specific events, which are based on printing devices alerts. The alerts are set up by first defining the events, and then selecting and setting the actions triggered by these events. The actions are of two kinds: as a response to an event on a printing device, MyQ can send an email notification to one or more persons, or it can terminate the user session on the embedded terminal of the device.



Ac...	Name	Type
SNMP Alert		
●	Call service	SNMP Alert
●	Check supplies	SNMP Alert
●	Cover open or Paper jam	SNMP Alert
●	Out of paper	SNMP Alert
●	Toner almost empty	SNMP Alert
●	Toner empty	SNMP Alert
Toner Status Monitor		
●	Toner below 20%_C	Toner Status ...
●	Toner below 20%_K	Toner Status ...
●	Toner below 20%_M	Toner Status ...
●	Toner below 20%_Y	Toner Status ...

The events can be set on the Printer **Events** settings tab and the event actions on the **Event Actions** settings tab.

A report with the Event History type can be created, which informs about all events on selected printers or groups of printers during a certain period of time.

9.10.1 Events

There are ten predefined alerts on the **Events** settings tab. These correspond to common situations, such as empty toner or a printer out of paper, or to states of printing devices that require particular actions, such as technical support or supply check. They are triggered by the following states of a printing device:

- **Call service** — The printing device requires authorized technical service.
- **Check supplies** — Consumables of the printing device need to be checked.
- **Cover open or Paper jam** — Either a device cover is open or a paper is jammed.
- **Out of paper** — The printing device is out of paper.
- **Toner almost empty** — One or more toners on the device are almost empty.

- **Toner empty** — One or more toners on the device are empty.
- **Toner below 20%_C** — The Cyan toner on the device is below 20%.
- **Toner below 20%_K** — The Black toner on the device is below 20%.
- **Toner below 20%_M** — The Magenta toner on the device is below 20%.
- **Toner below 20%_Y** — The Yellow toner on the device is below 20%.

Changing the Monitored Toner Level

The toner level to be monitored is set to *20%* by default but can be easily changed following the instructions below:

1. On the alerts list on the **Events** tab, double-click the alert. The properties panel opens on the right side of the screen.
2. Change the value in the **Level below** field (in *%*).
3. Change the name of the alert according to the new monitored level.

Creating New Events

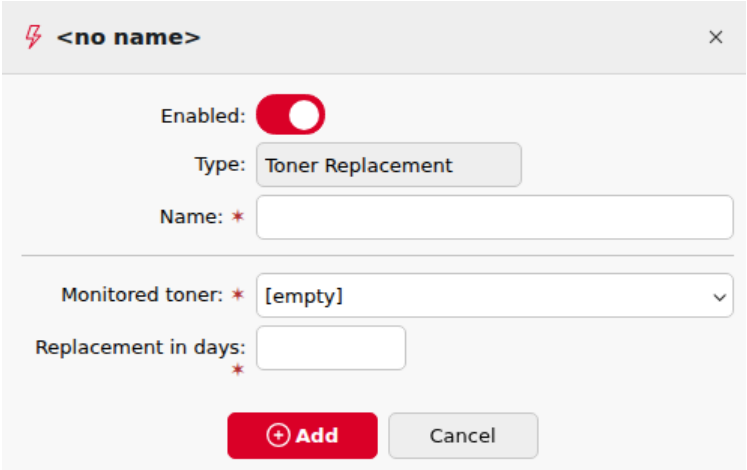
To create a new event, click **+Add** and a select the type of event to be created.

Available event types:

- **SNMP alert** - The SNMP alert event occurs when at least one of the predefined filter passes. If the event has no filters defined, it's never open. You can define the following filters: *Code from, Code to, Severity, Training, Group, Group Index, Brand, Model*.
- **Toner Status Monitor** - The event occurs when the toner level decreases below a predefined threshold. When the toner level rises again to or above the threshold, the event is closed. The monitored toner (*Black toner, Color toner, Any toner*) can be configured.
- **Total Counter Increase** - The event monitors when the print and copy counters on a device repeatedly reach a certain value. For each such event, two values need to be specified:
    - which type of counters should be monitored by this event; possible values are *Print & Copy total, Print & Copy mono, Print & Copy color*.
    - which repeatedly reached values should be monitored - this means that a value X needs to be specified and whenever the counters on a device reach a value that is evenly divisible by X, the actions are triggered
- **Toner Replacement** - The event is used to predict toner depletion. For each such event, two values need to be specified:
    - Monitored toner (*Cyan toner, Magenta toner, Yellow toner, Black toner*)
    - Replacement in days: number of days that serve as threshold for triggering actions - this means that user specifies value X and whenever

the predicted number of days left is less than or equal to this value, the associated actions get triggered

A properties panel opens to the right side of the screen. Fill in the mandatory information and click **Save**.



9.10.2 Event Actions

The two available actions are sending an email and logging the user out of an embedded terminal. Each action can be either applied to all printers, or it can be restricted to specific groups of printers.

There are four predefined event actions: **Toner below 20%_C**, **Toner below 20%_M**, **Toner below 20%_Y**, **Toner below 20%_K**. These actions apply to all printers and respond to the **Toner below 20%_C, Toner below 20%_M, Toner below 20%_Y, Toner below 20%_K** events.

Ac...	Name	Type	Event	Printer group	D...
Toner below 20%_C					
○	Toner below 20%_C	Send email	Toner below 20%_C	All printers	0 min
Toner below 20%_M					
○	Toner below 20%_M	Send email	Toner below 20%_M	All printers	0 min
Toner below 20%_Y					
○	Toner below 20%_Y	Send email	Toner below 20%_Y	All printers	0 min
Toner below 20%_K					
○	Toner below 20%_K	Send email	Toner below 20%_K	All printers	0 min

Create a New Event Action

1. Go to **MyQ > Settings > Event Actions** and click on **+Add action**. Select the type of action from the drop-down: **+Send email** or **Log out user**.
2. On the panel, set all the options of the action and click **Save**.

Setting Event Actions

The parameters described below belong to the **Send email** and **Log out user** event actions.

- **Enabled:** Enable or disable the event action.
- **Name:** Add a name for the action
- **Event:** Select the event that will initiate this action.
- **Printer Group**: Select the printer group(s) that the action applies to from the list.
- **Delay:** Set a time period after which the email is sent (in minutes).
- **Recipient:** Enter the email recipient(s). You can use the *%PRN.CONTACT%* parameter to send the email to the device's contacts.
- **Subject + Message**: Enter the email's subject and message. You can use the following parameters
    - %PRN.NAME%: name of the printer
    - %PRN.IP_ADDRESS%: IP address of the printer
    - %PRN.SERIAL_NUMBER%: serial number of the printer
    - %PRN.MODEL%: model name of the printer
    - %PRN.PRINTER_MONO%: counter of B&W pages printed on the device
    - %PRN.PRINTER_COLOR%: counter of color pages printed on the device
    - %PRN.COPIER_MONO%: counter of B&W pages copied on the device
    - %PRN.COPIER_ COLOR%: counter of color pages copied on the device
    - %PRN.SCANNER%: counter of scanned pages sent to email or folder
    - %SUPPLY.INFO%: all of the toner supply identifiers separated by semicolon
    - %TONER_C.LEVEL%: C toner level in percentage
    - %TONER_M.LEVEL%: M toner level in percentage
    - %TONER_Y.LEVEL%: Y toner level in percentage
    - %TONER_K.LEVEL%: K toner level in percentage
    - %PRN.ASSET_NO%: the asset number of the printer
    - %EVENT.TONER.LEVEL%: toner level information
    - %EVENT.TONER.INFO%: toner information

Event History

The MyQ administrator can view the **Event History** on the MyQ Web Administrator interface, in **MyQ > Event History**.

On the left side, there are the *Event, Created, Resolved*, and *Printer* search parameters that can be set to view specific events.

In **Tools: Save as CSV**, the Event History can be exported.

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.

See also:

- Users Settings (see page 442)
- User Synchronization (see page 453)
- Automatic User Registration (see page 440)
- User Authentication (see page 507)
- Data Privacy and Anonymization (see page 530)

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.

System users are are hidden from the list of users in the MyQ web UI.

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 431)

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

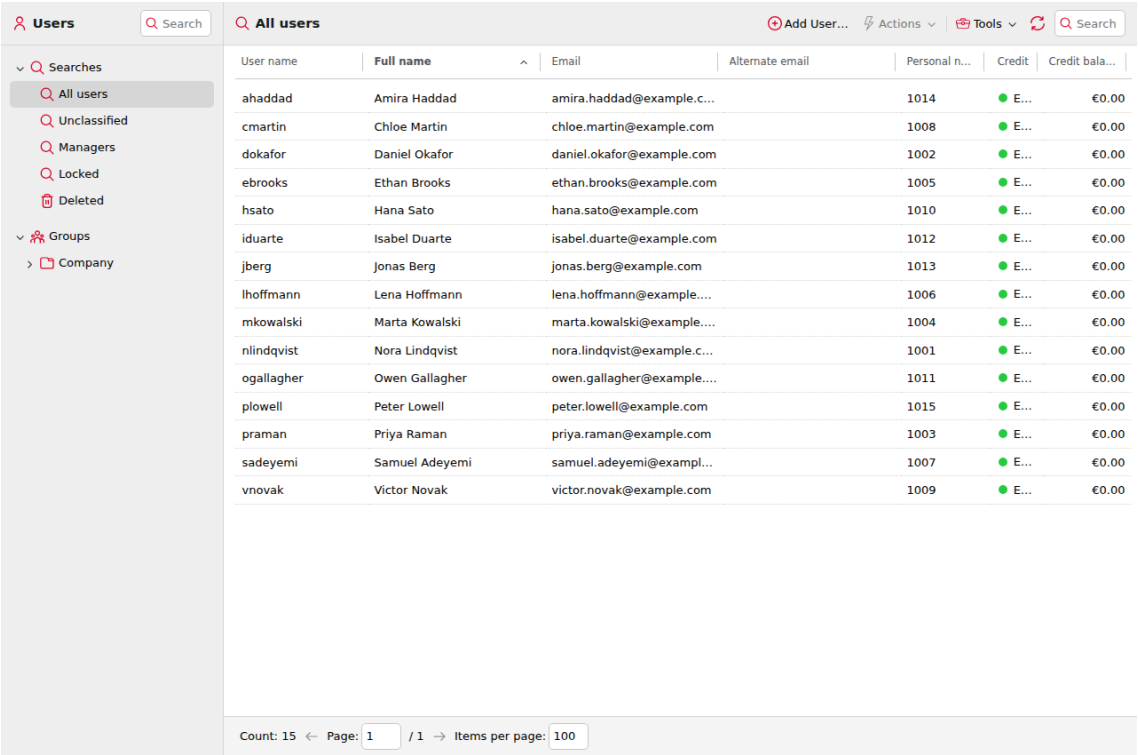
To delete a user:

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:

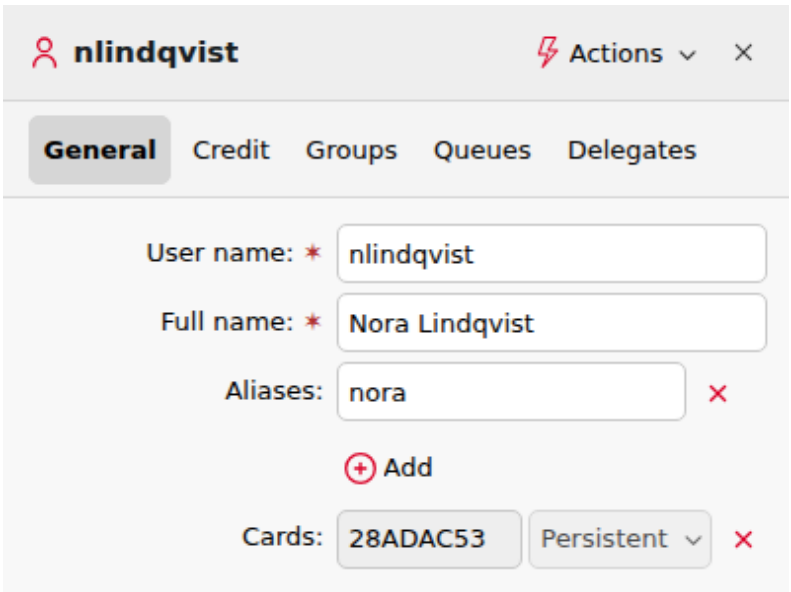
1. On the **Users** main tab, under searches, select the **Deleted** search option. The list of deleted users appears.
2. On the list, select the users that you want to restore, and then click **Actions**. The **Actions** drop-down box appears.
3. Click **Restore**.

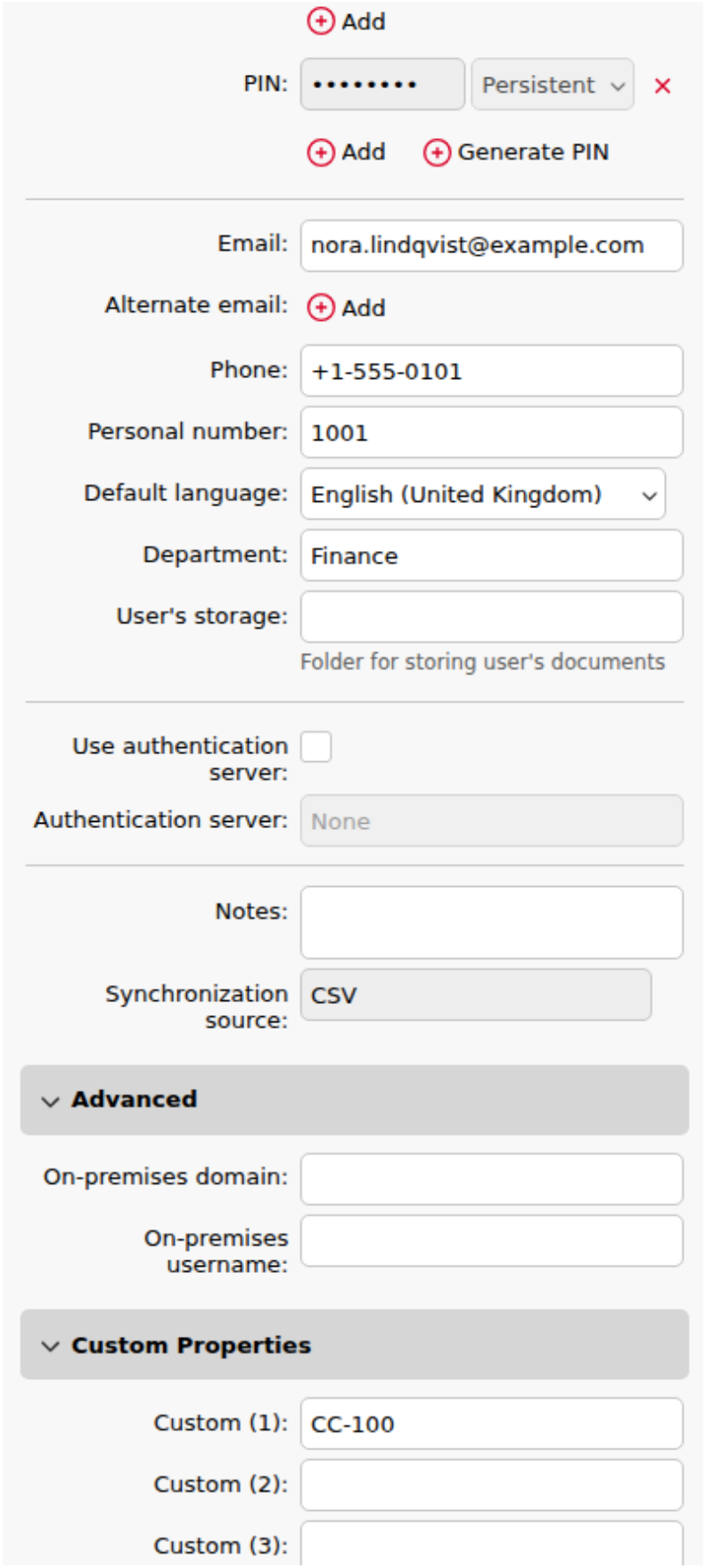


10.3 Editing User Accounts

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 **General**, **Groups**, **Queues**, and **Delegates** tabs. If Credit accounting is enabled for the user, the **Credit** tab is also available.




Add
PIN:
••••••••
Persistent
Add
Generate PIN
Email:
nora.lindqvist@example.com
Alternate email:
Add
Phone:
+1-555-0101
Personal number:
1001
Default language:
English (United Kingdom)
Department:
Finance
User's storage:
Folder for storing user's documents
Use authentication server:
Authentication server:
None
Notes:
Synchronization source:
CSV
Advanced
On-premises domain:
On-premises username:
Custom Properties
Custom (1):
CC-100
Custom (2):
Custom (3):



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.

Property	Description
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.
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.

Property	Description
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**.

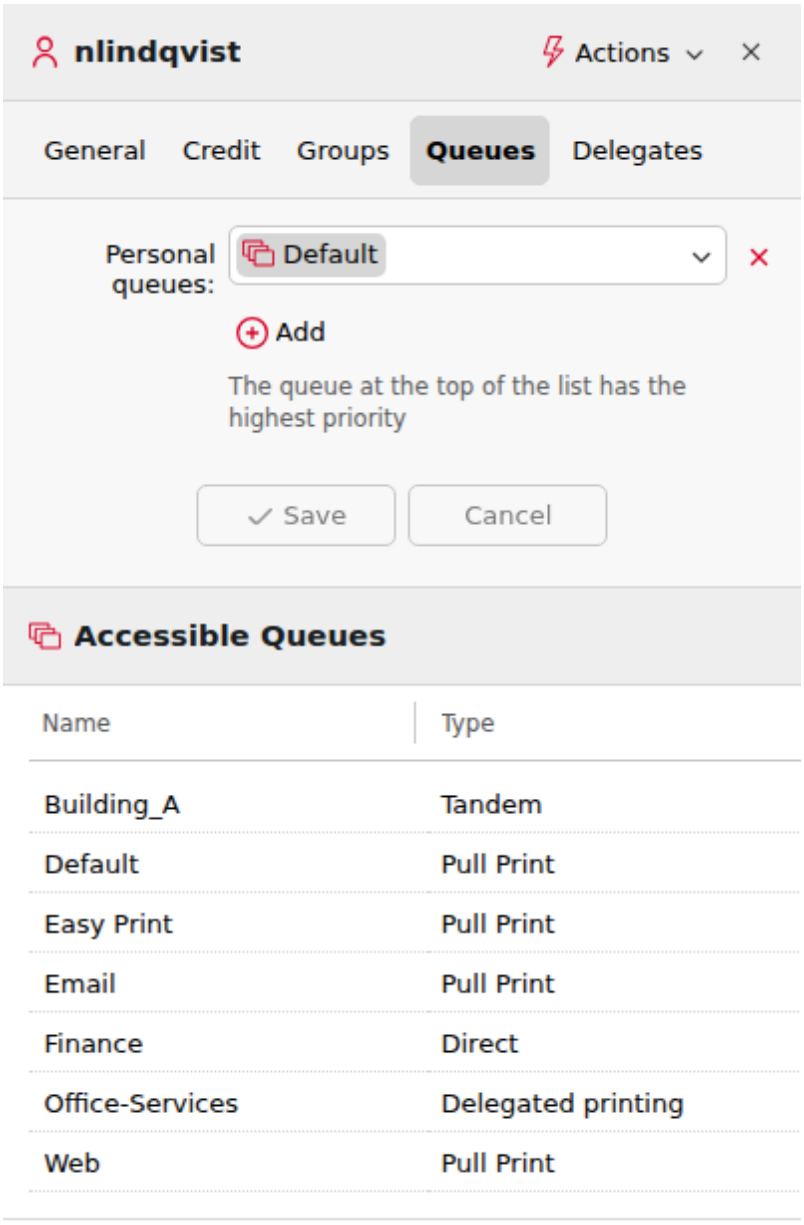
To remove a user from a group:

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 Queues Tab Overview

On the **Queues** tab, you can add Personal queues for a specific user, and see all the queues that the user can send jobs to.



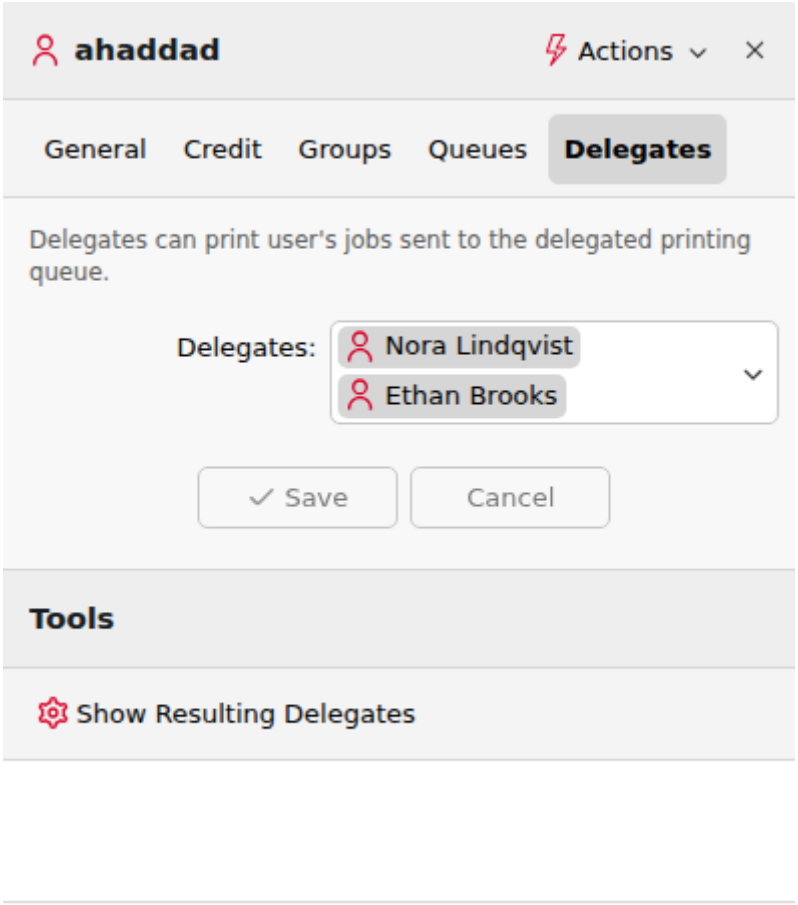
10.3.4 Selecting User Delegates

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).

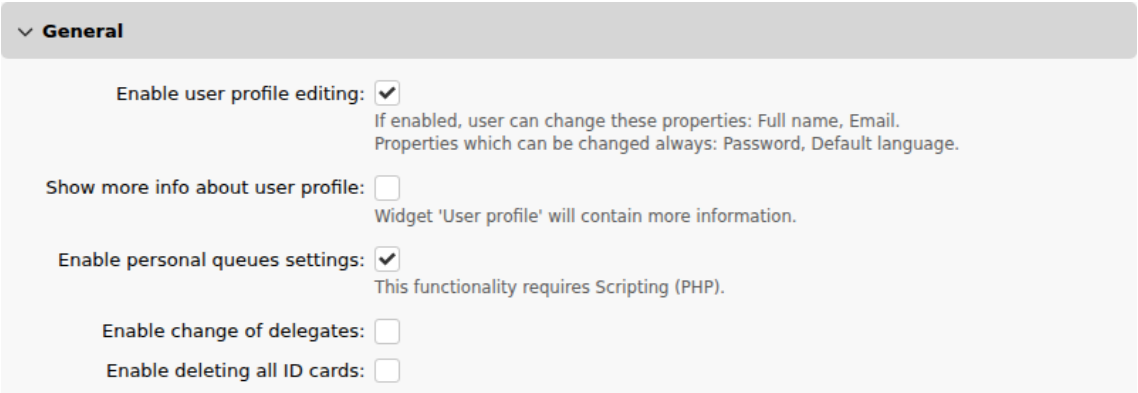
Show Resulting Delegates

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.

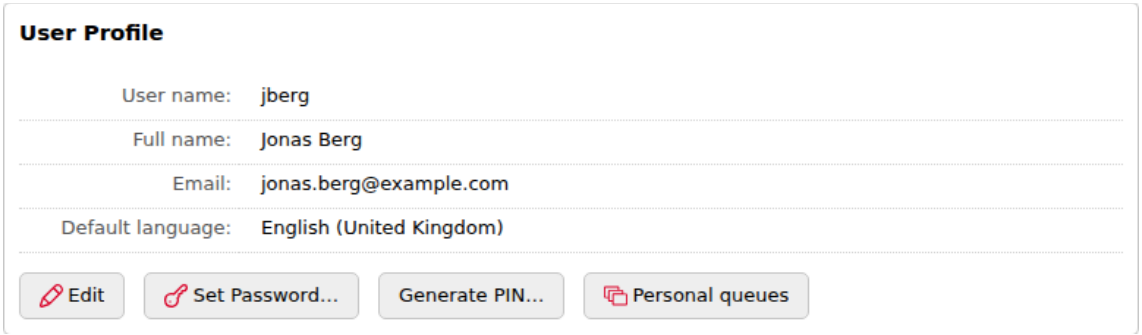
10.3.5 Enable User Profile Editing

By default, all users can change 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. On the **Users** settings tab, you can provide users with additional editing options: change their full name and email.

To enable users to change their full name and email, select the **Enable user profile editing** option.



Once user profile editing is enabled, users can open their profile management options by clicking **Edit** at the bottom-left corner of the **User profile** widget on their MyQ Web accounts.



10.4 User Groups

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

User groups enable to you efficiently manage access to print queues, print functions such as color printing or scanning, and reports.

See also:

- Queues (see page 532)
- Policies (see page 444)
- Reports (see page 680)

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**.

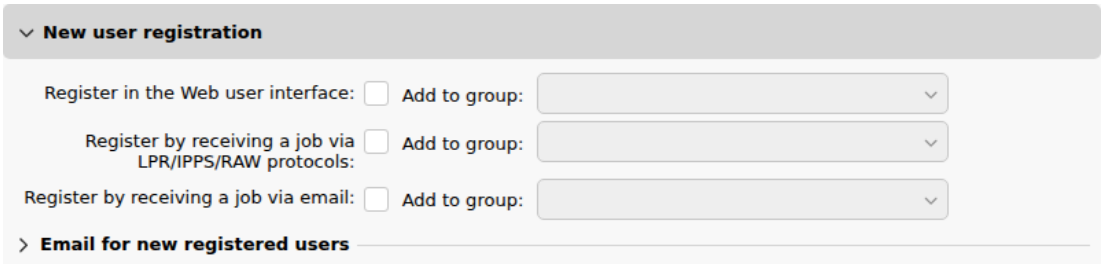
10.6 Automatic User Registration

Usually, only registered users can access the MyQ system and use the services there.

However, in some exceptional cases, it might be useful to enable automatic registration and thus provide all users with access to MyQ. Users can be automatically registered to the MyQ system in two ways:

- either they can register themselves on the MyQ Web User Interface or on an embedded terminal,
- or they can be automatically registered after sending a job to MyQ from their computer or via email as an attachment.

On the **Users** settings tab, under **New user registration**, you can enable and disable these options, and for each option, you can select one or more groups where the registered users will be added to.



10.6.1 Register on the Web User Interface

With this option selected, users can create accounts on the Web User Interface.

1. Click **New Account** at the bottom-left corner of the MyQ login window. The New Account registration widget opens.
2. Enter a name and email address.

3. Click **Register**.

   The newly created account is given the same name as the email address entered.

After creating the account, the **New account created** message box appears. After clicking **Show PIN** there, the user can see their username and password.

The user receives an email with information about the new account. The default message contains their user name and PIN. You can change the message in the **Email for new registered users** section.

10.6.2 Register by Receiving a Job via LPR/IPPS/RAW Protocol

With this option selected, users can register themselves by sending a print job from their computer via the LPR, IPPS or RAW protocol.

After a user sends the job, MyQ detects their name according to the currently set method of user detection, checks whether the user is already registered, and in case of an unknown sender user name, it creates a new account. The newly created account is given the same name as the job sender name detected this way.

10.6.3 Register by Receiving a Job via Email

With this option selected, users can register themselves by sending an email with an attached printable document.

The name of the newly created account is the email address that the email was sent from.

The user receives an email reply with information about the new account. The default message contains the user name and PIN. You can change the message in the **Email for new registered users** section.

Email for New Registered Users

Here you can change the email body that informs the new users about their account.

The values of the **%pin%**, **%username%** and the **%realname%** parameters are the user's PIN, user name and real name.
By clicking **Revert values**, you can reset the email body to the default.

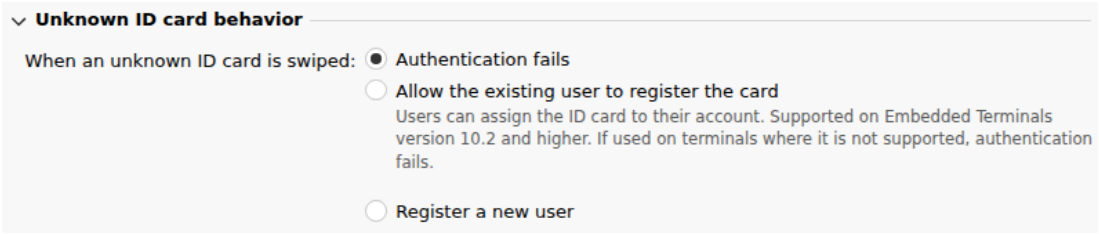
10.6.4 Self-Registration with an Unknown ID Card

You can allow users to self-register at a printing device with an embedded terminal by swiping an unknown ID card at the card reader. After swiping the card, a new

account called **anonymX** (anonym1, anonym2, etc.) is created and the user is automatically logged in to the terminal. There, the user can edit the account using the **Edit Account** action. If the **Enable user profile editing** option is enabled on the **Users** settings tab, they can change their full name, email and language; otherwise they can change the language only.

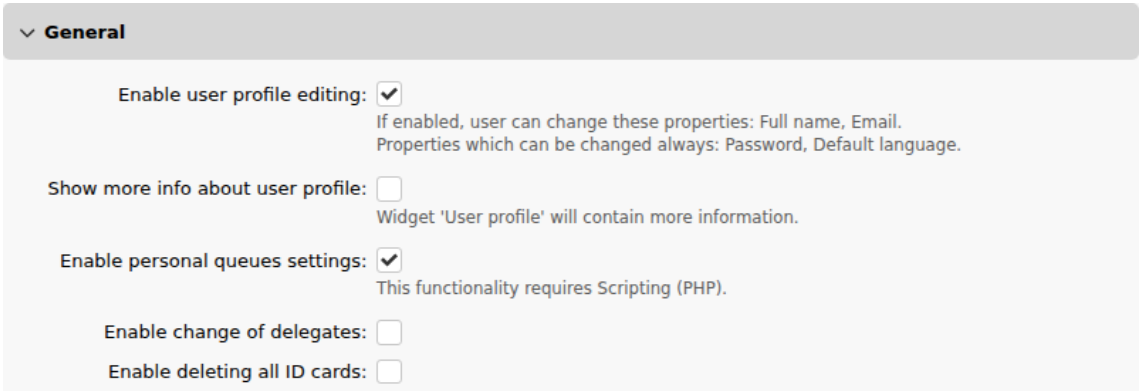
To control the settings for **Unknown ID card behavior**, go to **Settings > Users > User Authentication > Cards**. These options are available:

- **Authentication fails**
  This option disables log in with unknown ID cards.
- **Allow the existing user to register the card**
  After swiping, the user can register this card to their existing account. The user logs in with their account credentials and the card is registered to their account on the server.
- **Register a new user**
  This option creates a new user that is registered to that card. You can pre-select a group to add the user to, or leave this field blank and the new user will not be registered to any group.



10.7 Users Settings

In the **Users** settings tab (**MyQ > Settings > Users**), you manage MyQ users' **General** settings, **New user registration settings**, **Web Interface Session Timeout**, and MyQ **Account lockout** options.



10.7.1 General Settings

- **Enable user profile editing** - If enabled, users will be able to change their full name and email.
- **Show more info about user profile** - If enabled, the User profile widget will contain more user-related information (Personal number, Phone, PIN, Card, Aliases, Notes).
- **Enable personal queues settings** - If enabled, users can use personal queues.
- **Enable delegate changes** - If enabled, users will be able to change their delegates.
- **Enable deleting all ID cards** - If enabled, users will be able to delete all their ID cards.

See also:

- Enable User Profile Editing (see page 438)
- Personal Queues (see page 540)

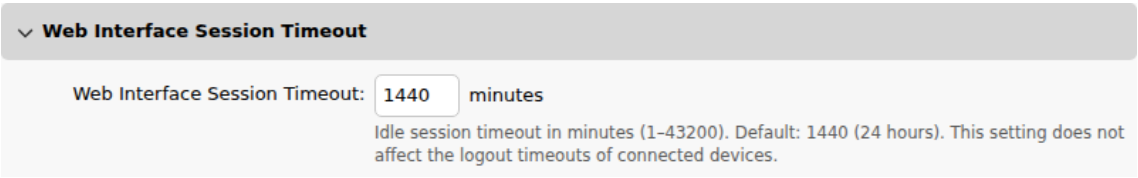
If all of the above are enabled, the users can view additional user information, **Edit** their account, **Delete all ID cards**, and use **Personal Queues** in their User profile widget:

10.7.2 New User Registration

Enable and configure automatic user registration to MyQ in a variety of ways.

See also: Automatic User Registration (see page 440)

10.7.3 Web Interface Session Timeout

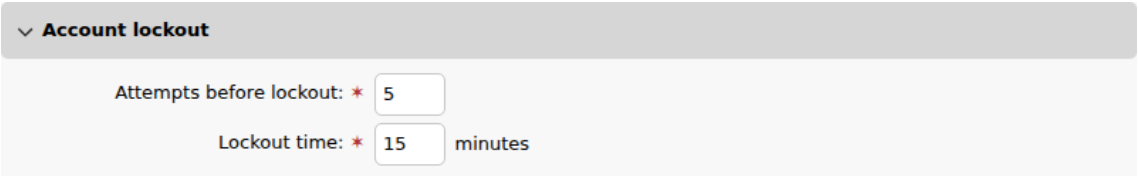


Set the idle timeout duration for web sessions, in minutes. If a user session is inactive for longer than the configured period, the session expires and the user must log in again. Changes take effect immediately for new requests without requiring a server restart.

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

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

10.7.4 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

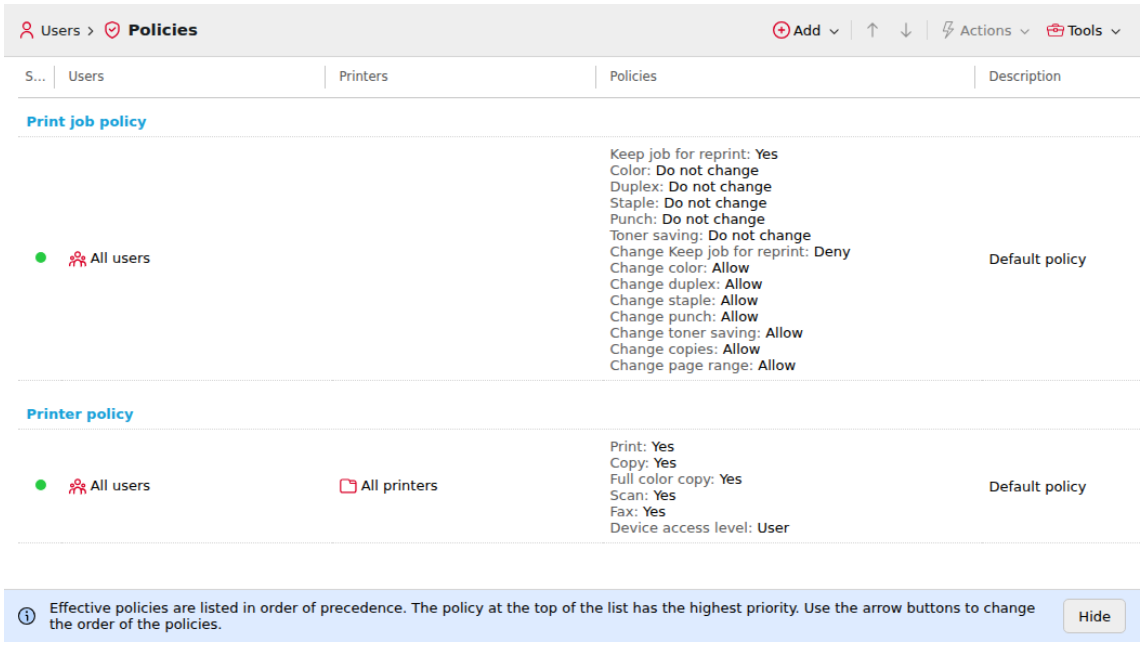
10.7.5 Policies

The **Policies** settings tab is divided into two sections. The **Print job policy** section contains settings that apply to all print jobs, all printers and selected users or groups.

The **Printer policy** section contains settings that apply to all queues, all print jobs, selected users (or groups) and selected printers.

Print job policies have the highest priority. Settings in the **Printer policy** section apply to all queues and all of the selected users, regardless of the settings of queues and print job policies.

Policies in both sections are listed in order of precedence: every policy has a higher priority than all the policies below it. If two policies are in conflict, the policy that is higher on the list applies. The default policy has the lowest priority and is always at the bottom of the list, other policies can be moved up and down the list by clicking the left or right arrow buttons on the **Policies** settings tab toolbar.



Print Job Policies

To open a print job policy properties panel, double-click the print job policy on the **Policies** settings tab list, under **Print job policy**.

The print job policy panel has the following sections and options:

- **Enabled** - Enable/disable the policy
- **Users and Groups** - Select users and groups of users that the policy will apply to
- **Description** - (Optional) Add a description for the policy.

Job Settings Defaults

These options control the default settings for print jobs. To modify an option, first select the checkbox.

- **Keep jobs for reprint:** *Do not change*, Yes, No
- **Color**: *Do not change, Force mono, Revert force mono*
- **Duplex**: *Do not change, Simplex, Duplex long edge, Duplex short edge*
- **Staple**: *Do not change, Yes, No*
- **Punch**: *Do not change, Yes, No*
- **Toner saving**: *Do not change, Yes, No*

Permissions

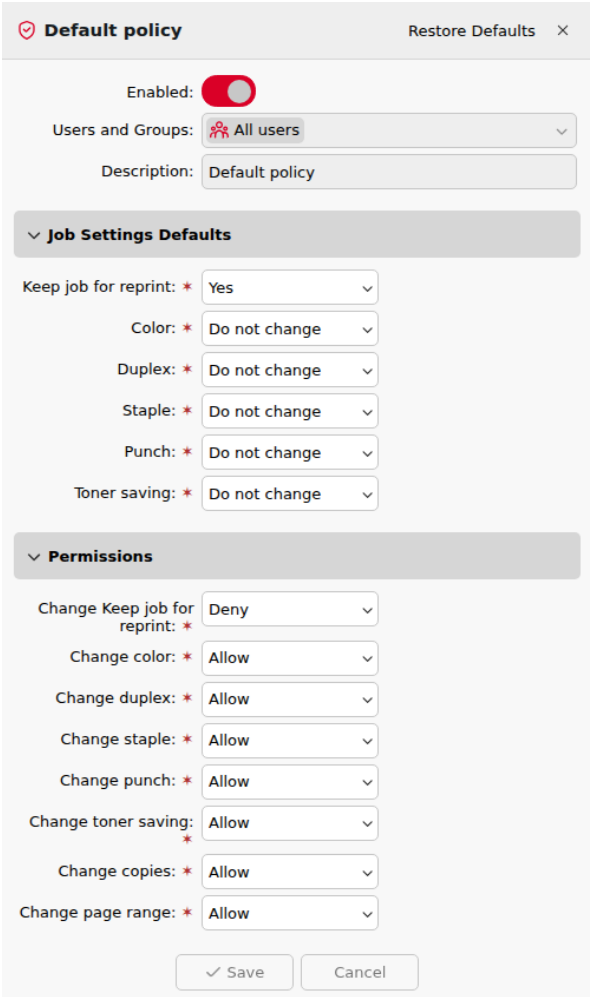
These options control if users are able to modify the job settings. Select a checkbox to modify a setting. For each one, you can choose *Allow* or *Deny*:

- **Change Keep jobs for reprint**
- **Change color**
- **Change duplex**
- **Change staple**
- **Change punch**
- **Change toner saving**
- **Change copies**
- **Change page range**

Default Print Job Policy

The **Default policy** applies to all users and has no restrictions. Except for its name and scope, all the settings of this policy can be changed.

To restore the default settings, click **Restore defaults** on the top-right corner of its panel.



Adding New Print Job Policies

1. On the bar at the top of the **Policies** settings tab, click **+Add**, and then click **+Add print job policy**. The new print job policy properties panel opens on the right side of the screen.
2. On the panel, select the users or group of users that the policy will apply to, optionally write a description of the policy, change its settings, and then click **Save**.

The new policy appears on the **Policies** setting tab, under **Print job policies**.

With all the **Permissions** set to *Deny*, users are not able modify their jobs on the MyQ Embedded terminals.

With the **Keep jobs for reprint** setting set to *No*, users are not able to add their jobs to **Favorites** on their account on the MyQ Web Interface or on MyQ Embedded terminals and they cannot reprint old jobs on the embedded terminals either.

The **Keep jobs for reprint** setting is also available when configuring a queue. The following combinations between the Keeps jobs for reprint Policy and Queue setting are available:

- Policy *ON* + Queue *ON* - The print job file is saved and can be reprinted even when not marked as favorite.
- Policy *ON* + Queue *OFF* - The print job file is saved only when marked as a favorite before printing. Favorite jobs can be reprinted.
- Policy *OFF* + Queue *ON* - The print job files are always saved, but because of the policy they cannot be reprinted or marked as favorite by the users. If the Policy is changed to *ON*, then the jobs can be reprinted later.
- Policy *OFF* + Queue *OFF* - The print job files are always deleted right after printing, cannot be reprinted or marked as favorite. If the Queue or Policy is changed to *ON*, jobs cannot be reprinted anyway.

With the **Change Keep jobs for reprint** permission set to *Allow*, the user can decide which jobs to keep and which to delete on release.

> **Limitation**
> When the permission for **Change Keep job for reprint** is set to *Allow* in an Easy Print action, the option is not displayed to the user.

Printer Policies

To open a printer policy properties panel, double-click the printer policy on the **Policies** settings tab, under **Printer policies**.

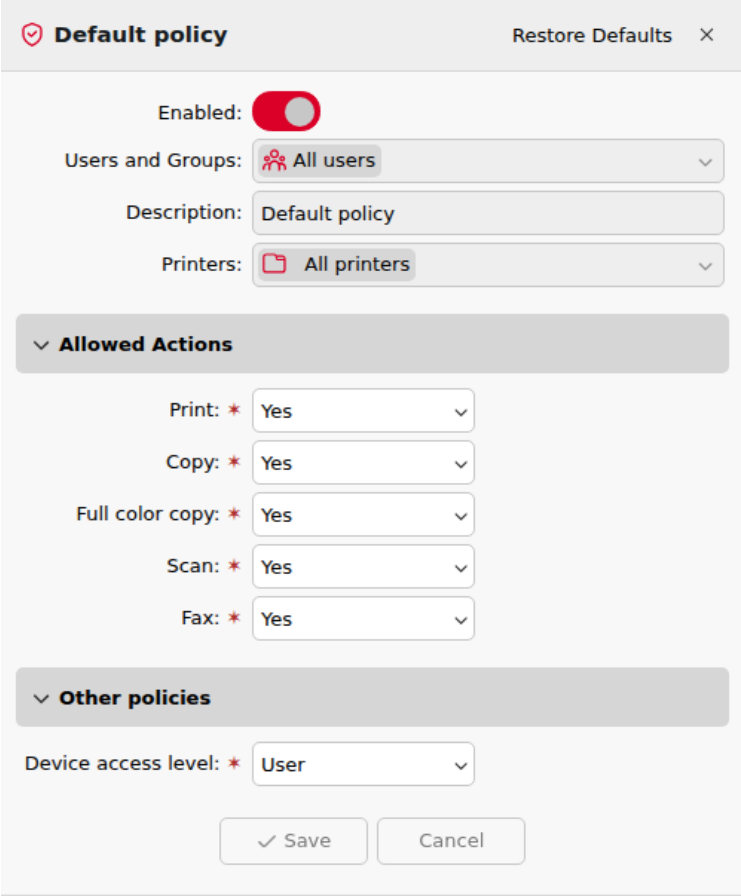
Each printer policy panel is divided into three sections:

- In the uppermost section, you can enable or disable the policy, select the **Users and Groups** of users that it will apply to, select the **Printers** that it will apply to, and write the policy's **Description**.
- In the **Allowed Actions** section, you can restrict access to particular operations on the selected printing devices. The available operations are:
  - **Print**
  - **Copy**
  - **Full color copy**
  - **Scan**
  - **Fax**
- In the **Other policies** section, you can provide users with administrator access to printing devices via the embedded terminal menu. For some devices, this option is not supported.

Default Printer Policy

The **Default policy** applies to all users, all printers, has no restrictions and gives users **User access** to embedded terminals. Except for its name and scope (It applies to all users and all printers), all settings of this policy can be changed.

You can restore the **Default policy** default settings by clicking **Restore defaults** on the top-right corner of its panel.



Adding New Printer Policies

1. On the bar at the top of the **Policies** setting tab, click **+Add**, and then click **+Add printer policy**. The new policy properties panel opens on the right side of screen.
2. On the panel, select the users or group of users that the policy will apply to, optionally write a description of the policy, change its settings, and then click **Save**. The new policy appears on the **Policies** settings tab, under **Printer policy**.

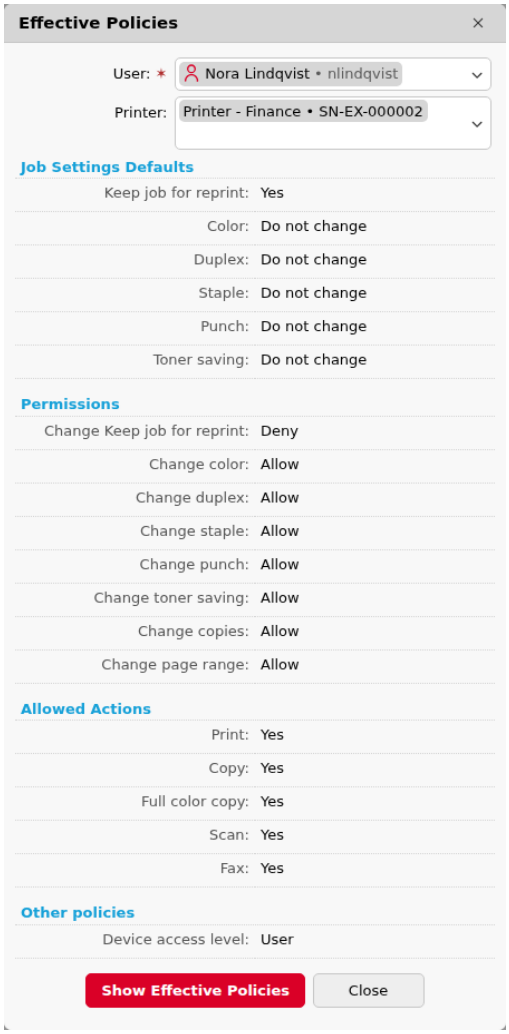
Checking Policies Applied to Individual Users

The levels of policy applied to individual users at specific printers can easily become complex, however, you can use the **Show Effective Policies** action to get a quick overview of policies on a user level.

1. From the **Users** tab, select **Actions** from the top-right of the navigation bar, and click **Show Effective Policies**.

2. Select the user for whom you want to view effective policies, and optionally, a specific printer, and click **Show Effective Policies.**

The policies currently applied to this user (on the relevant printer if selected) are listed in the categories **General**, **Allowed Actions**, **Other policies**, **Job Settings Defaults**, and **Permissions**.



10.7.6 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:

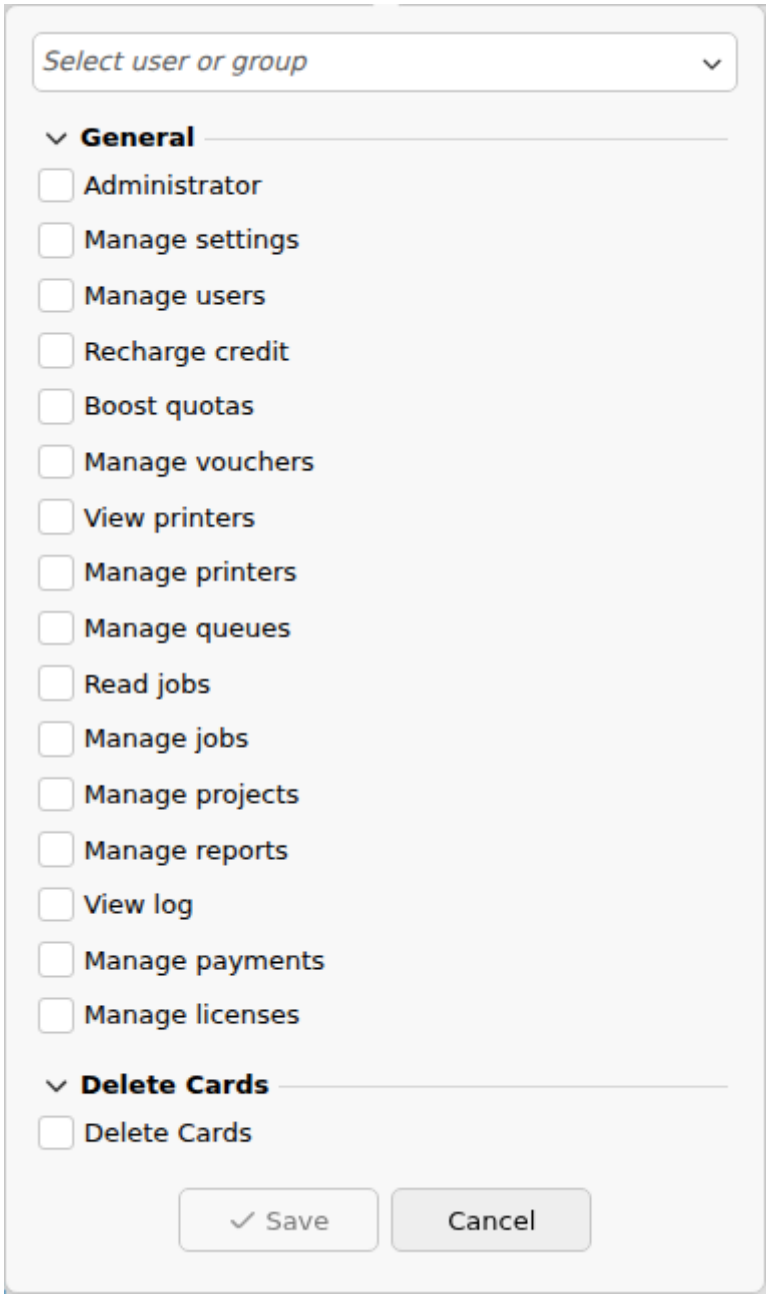
- **Add user** - add a new user or group with assigned rights.
- **Edit** - edit an existing user or group with assigned rights.
- **Delete** - delete a user or group with assigned rights.
- **Refresh** - refresh the list of users and groups.
- **Search** - search for a user or group with assigned rights.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

If the server is used as a Site server, user rights are managed by the Central server. The rights are visible in the Site server's Rights settings, but are non-editable.

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.
- **Boost quotas** - The user gets access to the **Quota Boosts** main tab.

- **Manage jobs** - The user can edit other users' jobs.
- **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 printers** - The user gets access to the **Printers** main tab, to monitor printers and change their settings, as well as the **Printers & Terminals** settings tab and all its subsections, where they can modify settings.
- **Manage projects** - The user gets access to the **Projects** main tab, can add projects and change their settings.
- **Manage queues** - The user gets access to the **Queues** main tab and can change the settings there.
- **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. Access to the **Quota** settings tab is granted, but the user is only allowed to change Quota definitions, not Quota global settings.
- **Manage vouchers** - The user gets 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 can delete other users' ID cards.

10.8 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.

10.8.1 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.

MyQ Property	Syncable	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.
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.

10.8.2 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.
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`	

MyQ Property	Default Attribute	Notes
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`	
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).

10.8.3 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.
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 431)
- Available Languages (see page 718)
- Transform User Data with RegEx (see page 503)
- Run and Schedule User Synchronization (see page 505)

10.8.4 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 475)

- Synchronize Users from Google Workspace (see page 478)
- Synchronize Users from Entra Domain Services (see page 483)

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 485).

Prerequisites

- 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

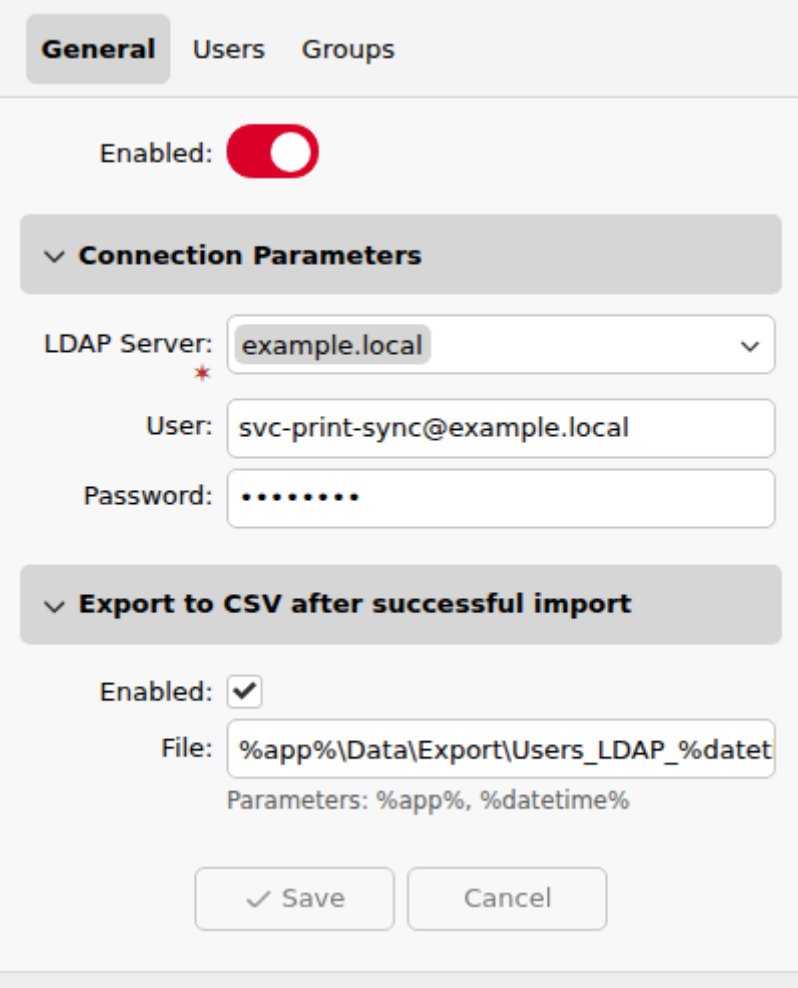
1. Go to **MyQ > Settings > User Synchronization**.
2. Click **+Add**.
3. Select **Add LDAP source**.

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.
Export to CSV after successful import	When enabled, MyQ writes a CSV file of imported users after each sync run.

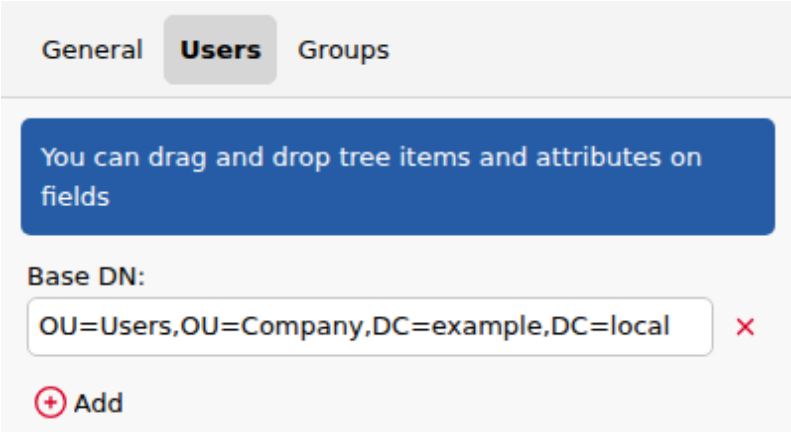
Setting	Description
File	File path using `%app%` and `%datetime%` parameters, for example `%app%\Data\Export\Users_LDAP_%datetime%.csv`.

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:

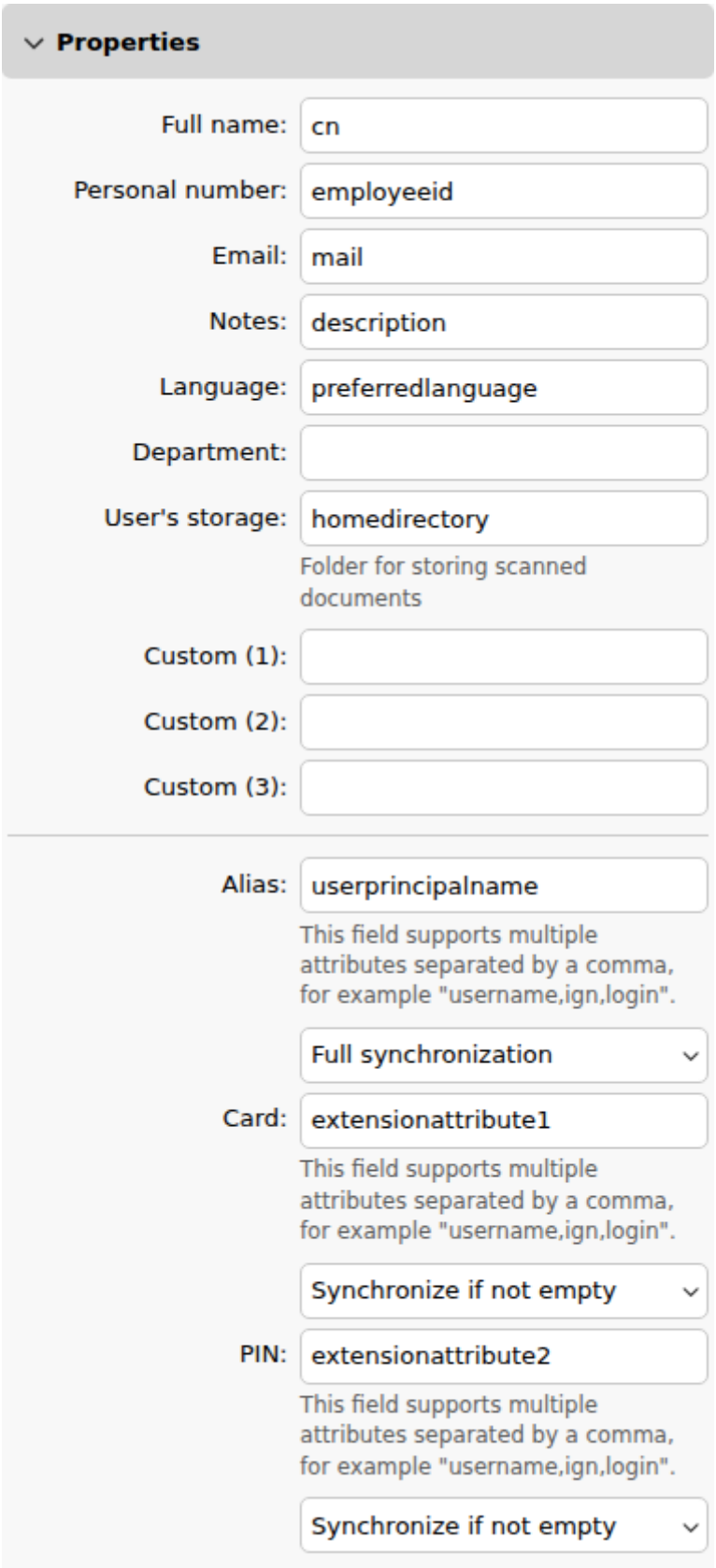
```
OU=Prague,DC=example,DC=com
```

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.


Properties
Full name:
cn
Personal number:
employeeid
Email:
mail
Notes:
description
Language:
preferredlanguage
Department:
User's storage:
homedirectory
Folder for storing scanned documents
Custom (1):
Custom (2):
Custom (3):
Alias:
userprincipalname
This field supports multiple attributes separated by a comma, for example "username,ign,login".
Full synchronization
Card:
extensionattribute1
This field supports multiple attributes separated by a comma, for example "username,ign,login".
Synchronize if not empty
PIN:
extensionattribute2
This field supports multiple attributes separated by a comma, for example "username,ign,login".
Synchronize if not empty

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.
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.

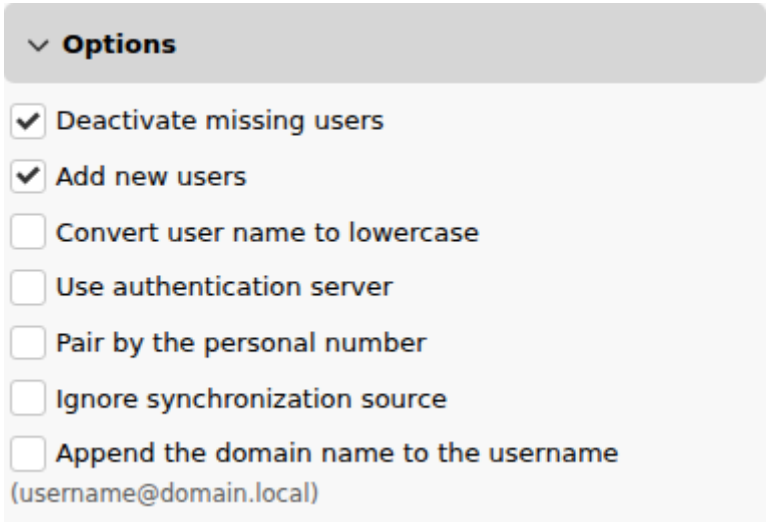
Card and PIN Synchronization

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.

Option	Description
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`.
`(&(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`

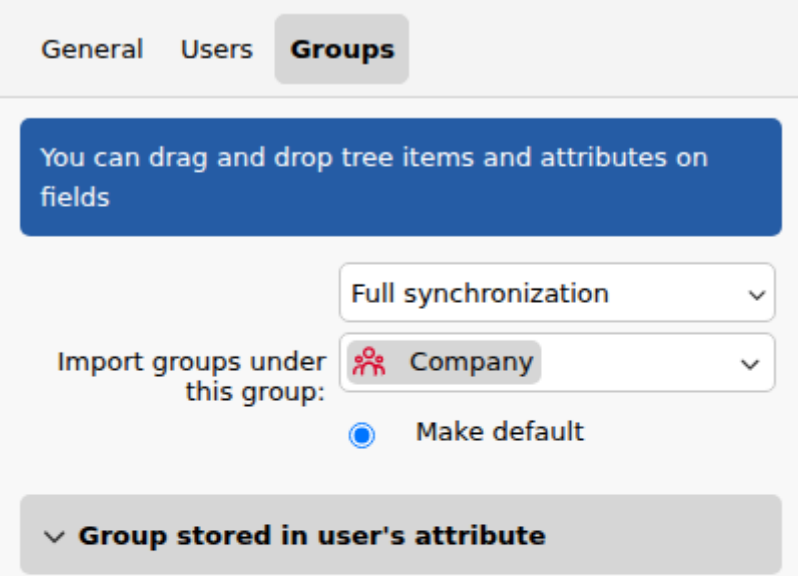
Transformation

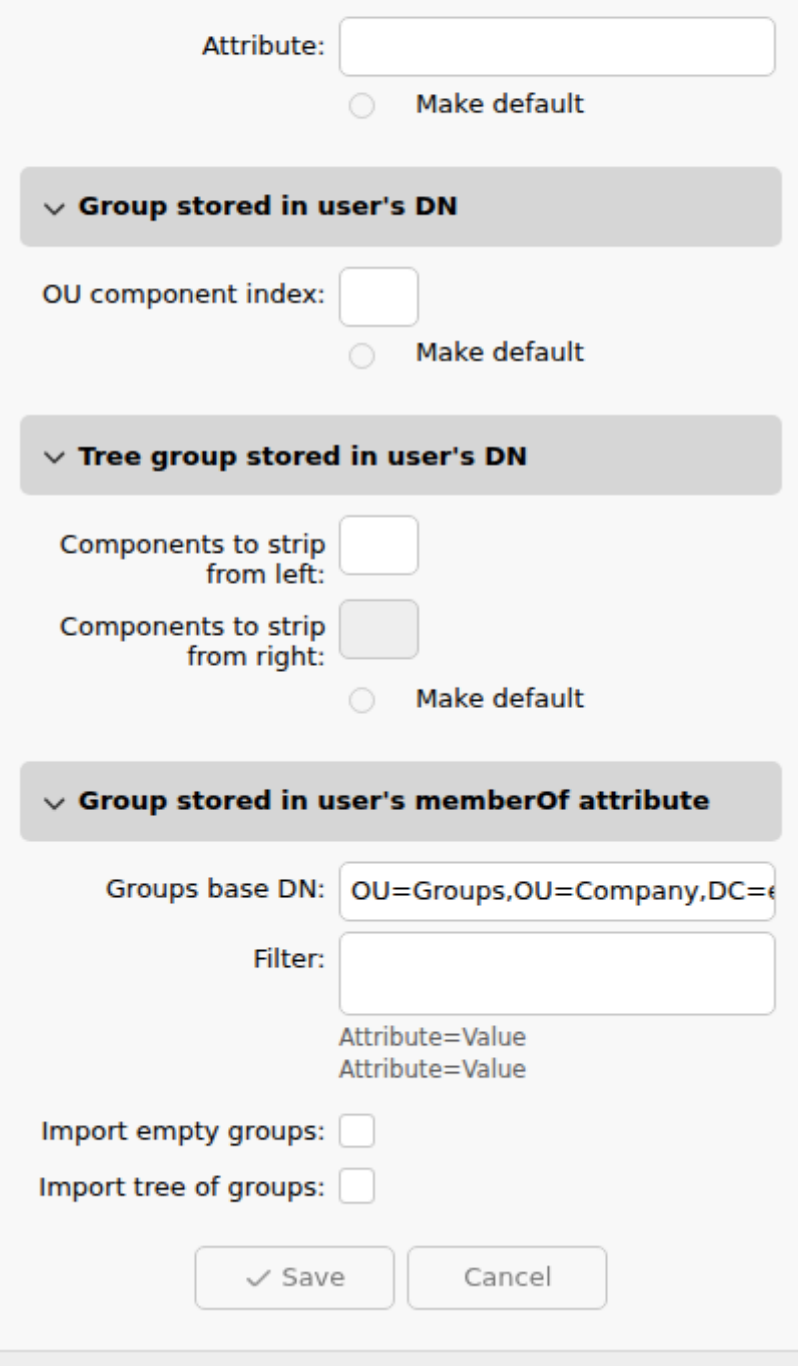
A regular expression transformation can parse or reformat directory values before MyQ stores them.

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`

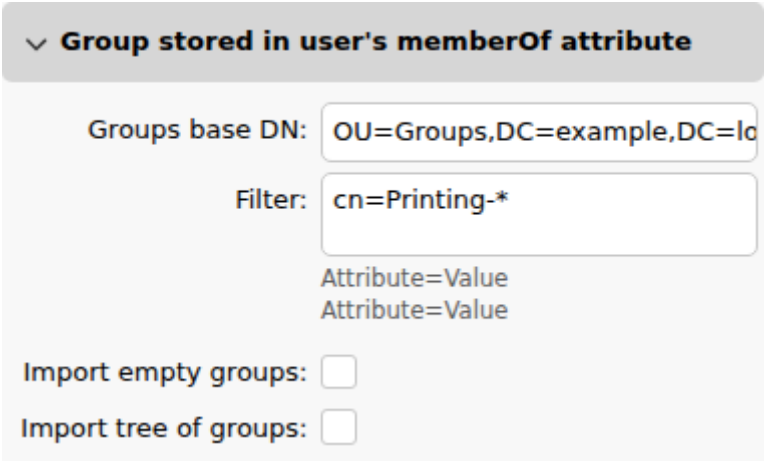
Configure **Strip from left** and **Strip from right** according to the number of components that must be excluded.

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 233)
- Available Languages (see page 718)

- Editing User Accounts (see page 431)
- Run and Schedule User Synchronization (see page 505)
- Transform User Data with RegEx (see page 503)

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 458)

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 503) .

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 233)

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 458). 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`.
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 458)
- Authentication Servers Settings (see page 233)
- Run and Schedule User Synchronization (see page 505)
- (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.

See also:

- (v2) User Synchronization
- Synchronize Users from LDAP (see page 458)

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)
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 458)
- Authentication Servers Settings (see page 233)
- Run and Schedule User Synchronization (see page 505)
- Manage LDAP Clients – Google Workspace Admin Help[33]
- Secure LDAP Schema – Google Workspace[34]

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 458).

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.

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.

33. https://support.google.com/a/answer/9048516
34. https://support.google.com/a/answer/9188164

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[35]
2. Configure Entra ID Domain Services to use Secure LDAP[36]

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

---

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

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

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 233)
- Run and Schedule User Synchronization (see page 505)
- Enable and configure Azure Active Directory Domain Services – Microsoft Learn[37]
- Configure Secure LDAP for Entra ID Domain Services – Microsoft Learn[38]

10.8.5 Synchronize Users from Microsoft Entra ID

Synchronize users from Microsoft Entra ID to create and maintain MyQ users and groups.

To synchronize users with Microsoft Entra ID, first plan your synchronization source, user identities, authoritative-source behavior, and multi-tenant environments. Then register a Microsoft Entra ID application. Finally, create a Microsoft Entra ID connection in MyQ that you can use in your synchronization.

See also:

37. https://docs.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-create-instance
38. https://docs.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-configure-ldaps

- (v2) Microsoft Entra Apps and MyQ
- Connect to Microsoft Entra ID (see page 202)
- (v2) User Synchronization
- (v2) Multi-domain and Multi-tenant Environments

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.

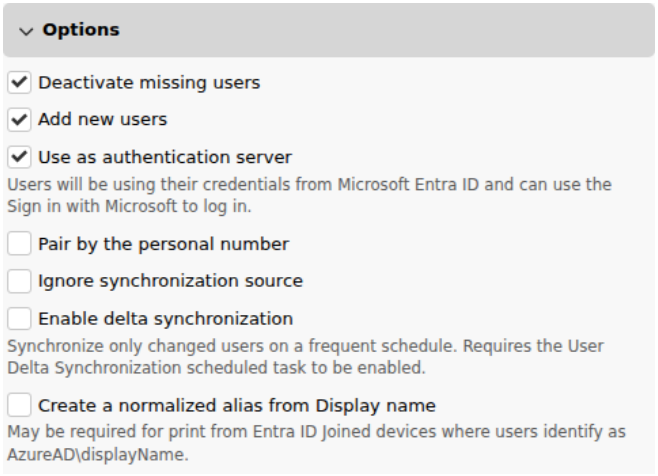
MyQ property	Available Entra attributes
Full name	`displayName`
Personal number	`employeeId`, `extensionAttribute1` – `extensionAttribute15`
Email	`mail`
Notes	`extensionAttribute1` – `extensionAttribute15`
Language	`preferredLanguage`
Department	`department`
Alias	`displayName`, `userPrincipalName`, `upnPrefix`, `mailNickname`, `onPremisesSamAccountName`, `onPremisesDomainName`, `extensionAttribute1` – `extensionAttribute15`
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:** Allows this synchronization source to match and update existing MyQ users even if they are associated with a different synchronization source. Enable this option when migrating users to Entra ID or consolidating multiple user sources without creating duplicate accounts.
- **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.

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.

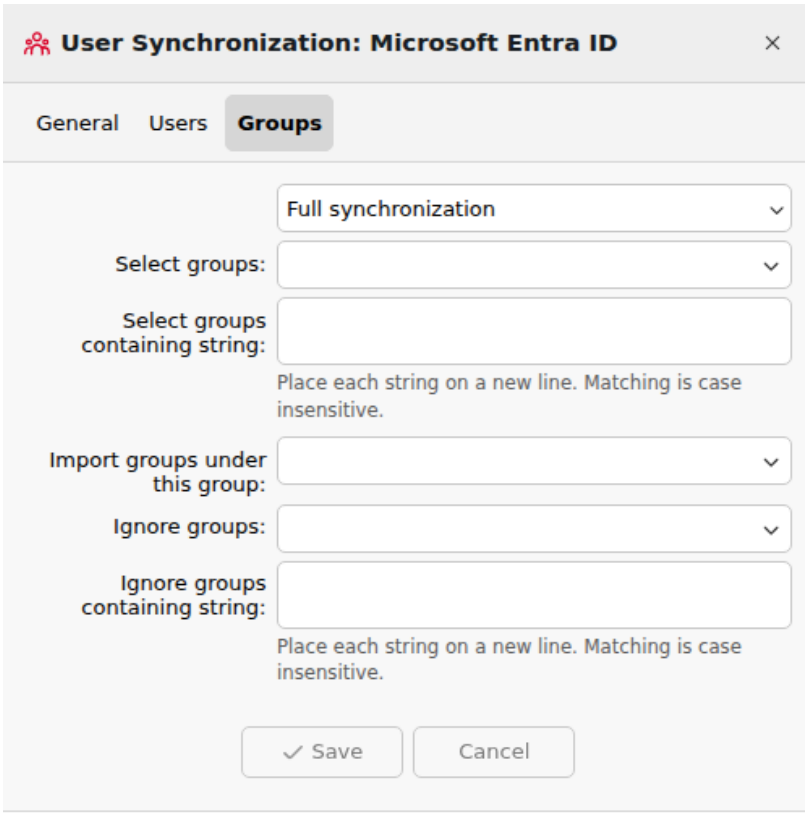
> **Limitation**
> If multiple synchronized users have the same display name, the normalized alias can be assigned only to the first matching user. In this case, MyQ cannot reliably distinguish the users from the concatenated name supplied with the print job.

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. To use this feature, enable the **User Delta Synchronization** scheduled task, and run synchronization at least once.

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 Microsoft Entra App Registration
- Connect to Microsoft Entra ID (see page 202)
- Run and Schedule User Synchronization (see page 505)
- Transform User Data with RegEx (see page 503)

10.8.6 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**.

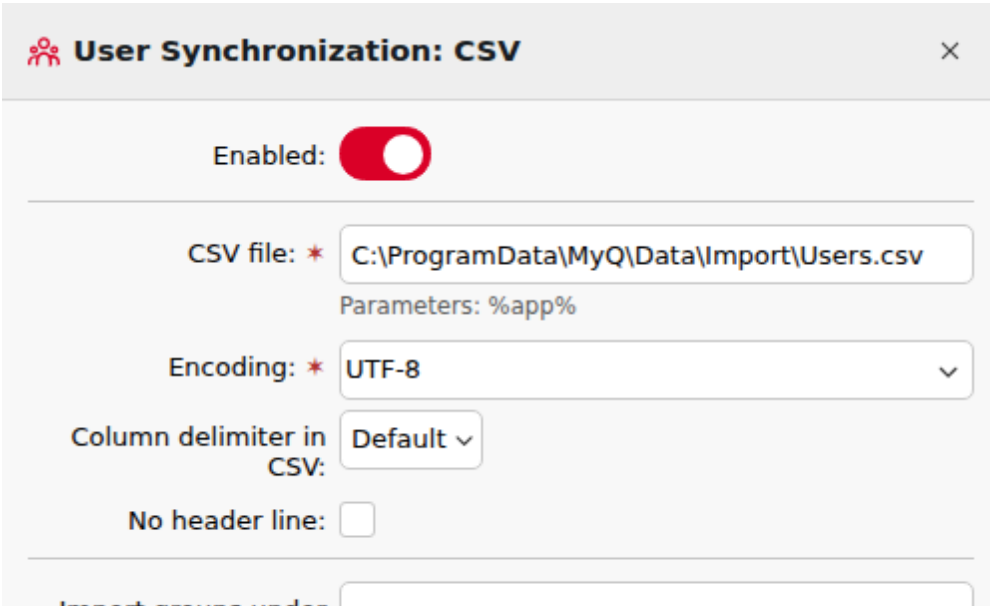
Key Considerations

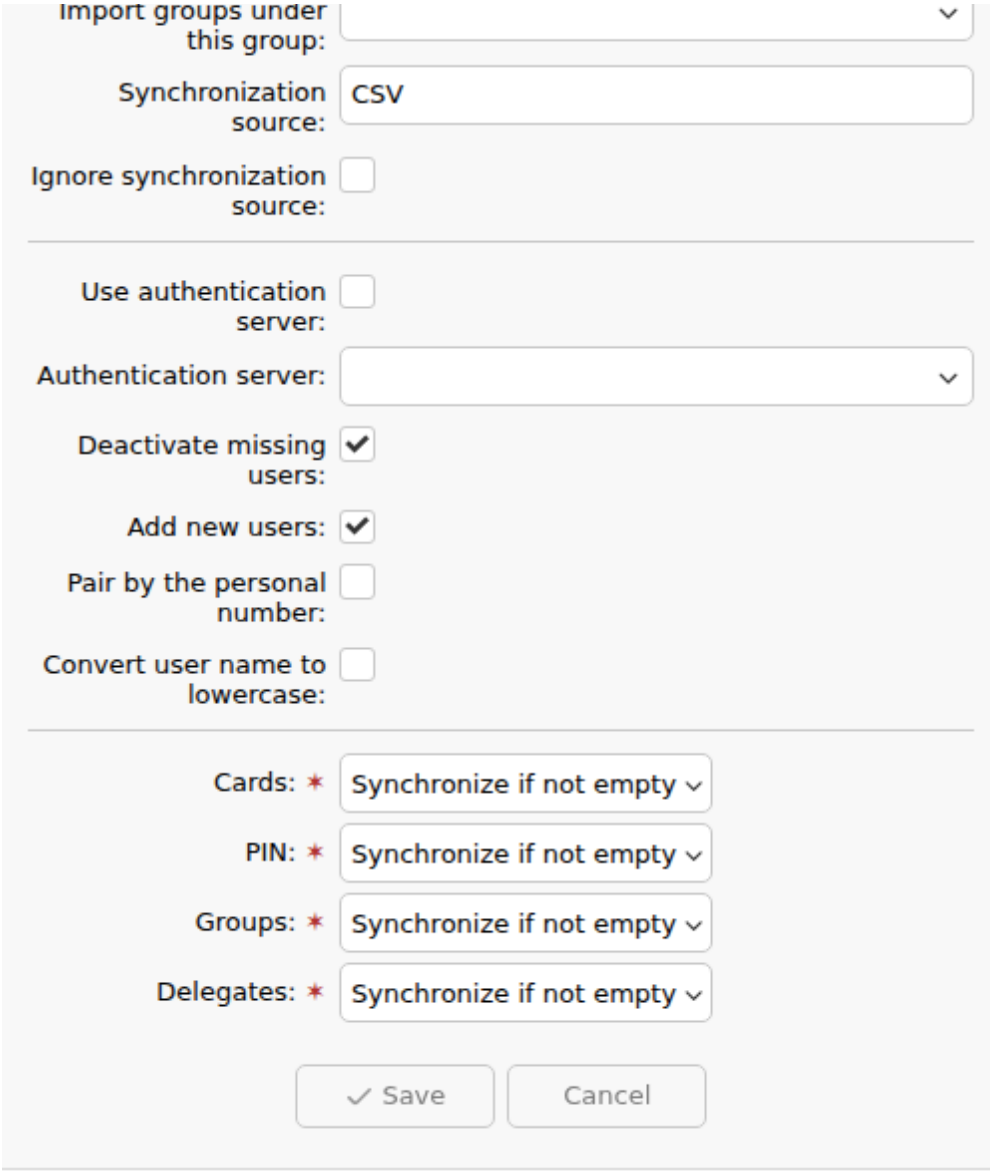
CSV is not a live directory. Unlike LDAP or Entra ID synchronization, CSV sync reflects only the contents of the file at the time the sync runs. If users are added or removed from the organization, the CSV file must be updated manually before the next sync.

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 453)
- Authentication Servers Settings (see page 233)
- Run and Schedule User Synchronization (see page 505)

10.8.7 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 External Authentication via API Connector (see page 515).

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 233)
- Synchronize Users from CSV (see page 493)
- Synchronize Users from LDAP (see page 458)
- External Authentication via API Connector (see page 515)

10.8.8 Using External Authentication Servers

In addition to the internal MyQ authentication methods (password, PIN or ID card), you can use two types of external authentication servers: LDAP and Radius.

With the two external methods, MyQ does not use the internal MyQ PIN or password for user authentication, but instead authenticates users against an LDAP or Radius server. After the user enters their credentials during the authentication, the credentials are sent to be verified directly by the external server. If there is no online connection with the LDAP or Radius server, users cannot log in.

To enable this method of authentication, perform these steps:

1. register the external authentication servers in MyQ

2. select to use them for user authentication

Selecting to use the registered external authentication servers for user authentication, can be done either automatically during the user import from an LDAP server or a CSV file, or manually on the properties panels of individual users.

Automatically Selecting the External Authentication Option

Importing Users from a CSV File

When you import users from a CSV file, you have two options of selecting the authentication server for the users:

1. You can select the **Use authentication server** option and select the server during the synchronization setup on the synchronization properties panel.
2. You can specify the **Authentication server** for a particular user in the **AUTHSERVER** field of the CSV file. If the field is not empty, its value has priority over the value selected on the properties panel.

Importing Users from an LDAP Server

During the users import from an LDAP server, you can select the **Use authentication server option**, to use the current synchronization source server for users authentication.

Unlike the **Use authentication server** setting for the import from a CSV file, which allows you to select the authentication server, the **Use authentication server** setting here gives you a single option – users will be
authenticated against the LDAP server where they are imported from.

Manually Selecting the External Authentication Option

To manually select the external authentication option

1. Open the **Users** main tab and double-click the user. The user's properties panel opens on the right side of screen.
2. On the panel, select the **Use authentication server** option. The Authentication server setting becomes available.
3. On the Authentication server drop-down box, select the server you want to use, and then click **Save** at the bottom of the panel.

See also:

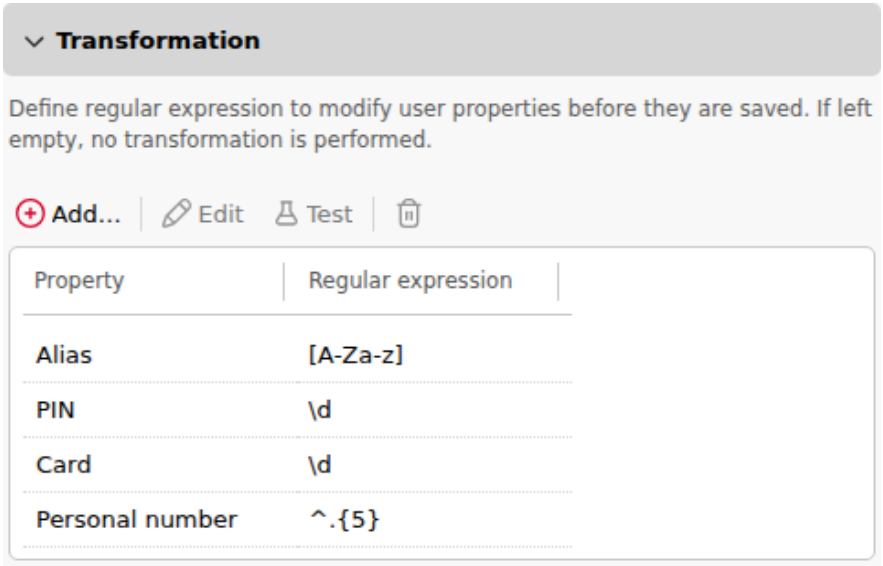
- Authentication Servers Settings (see page 233)
- Synchronize Users from CSV (see page 493)
- Synchronize Users from LDAP (see page 458)

10.8.9 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.

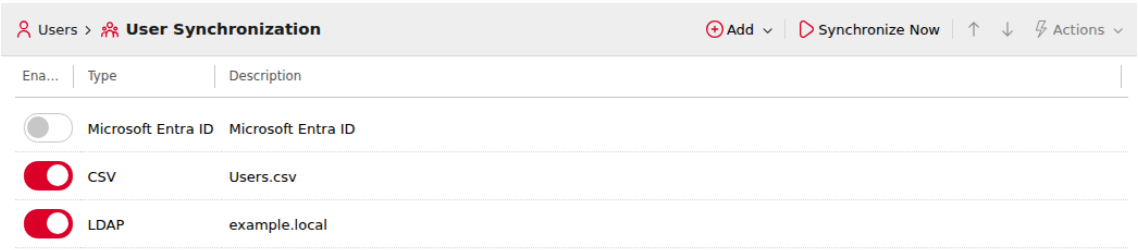
- **RegEx**: `.{3}$`

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.

10.8.10 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).

Entry	Meaning
`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 191)

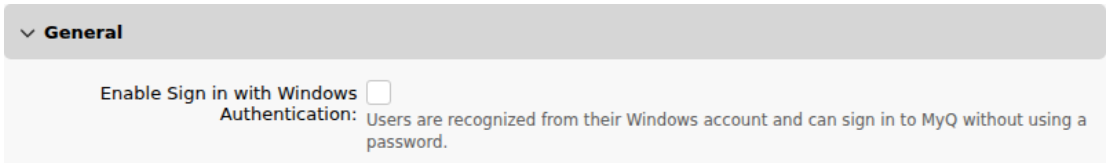
10.9 User Authentication

This section explains login methods that authenticate the user towards MyQ.

Users in MyQ can be assigned Authentication Servers which allow them to authenticate against LDAP servers, Microsoft Entra ID (including Microsoft Sign-in), and Radius.

In the **User Authentication** settings tab, the administrator can manage everything related to how users authenticate themselves in MyQ:

- ID Card Management (see page 508)
- PIN management (see page 513)
- Password Complexity (see page 515)
- External Authentication (see page 515)



10.9.1 Enable Sign-In with Windows

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.

See also:

- Authentication Servers Settings (see page 233)
- (v2) Integrated Windows Authentication
- Configure Integrated Windows Authentication (see page 523)
- Microsoft Learn - Integrated Windows Authentication[39]

10.9.2 ID Card Management

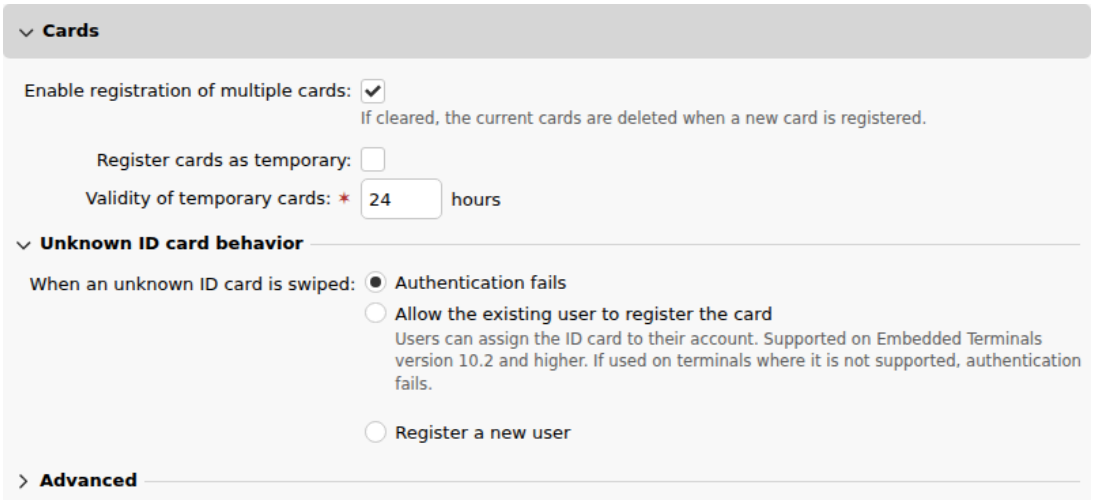
To manage ID card settings, go to **MyQ > Settings > User Authentication > Cards**.

The following options are available:

- **Enable registration of multiple cards** - This is enabled by default. If disabled, when a new card is registered, the current cards are deleted.
- **Register cards as temporary** - If this is enabled, ID cards can be registered as temporary.
  - **Validity of temporary cards** - Set the duration of the temporary cards validity in hours.
- **When an unknown ID card is swiped** - These options dictate what should happen when an unknown ID card is swiped. The options are:
  - Authentication fails.
  - Allow the existing user to register the card - an existing user can enter their login details after swiping the card and the card is registered to that user on the server.
  - Register a new user - registers the card as a new user on the server, you can choose if you would like users registered this way to be automatically assigned to a particular user group.
- **Card code transformation** - This transformation is used by Embedded terminals (with USB readers connected directly to the device) and by the reader for a HW terminal that is connected, usually, as a primary reader.
- **USB reader transformation** - Check the box to apply the transformation to card readers connected to a PC USB slot. These card readers are usually used to recharge credit or to associate cards with user accounts.

---

39. https://learn.microsoft.com/en-us/aspnet/web-api/overview/security/integrated-windows-authentication



Adding cards manually is not possible when cards are synchronized from an LDAP source. The manually added cards will be deleted during the next LDAP synchronization, and overwritten by the cards from the LDAP source.
Adding multiple cards via LDAP synchronization is supported.

ID Card Transformation

Transformation might be necessary if the customer needs to import card numbers from a third-party SW database and the card number format in this database doesn't match the format read by the MyQ card reader.

The third-party system card readers can give output in a different format than the card readers used in MyQ. In consequence, users card numbers imported from the third-party system can differ from the card numbers read by the MyQ card readers. To unify the format of the two outputs, you can define a specific sequence of commands that transforms the output of the MyQ card readers to the format used in the database of the third-party system.

With most of the MyQ card readers, you can use the card reader configuration software to set the format directly on the reader. However, it is simpler and faster to set one or two universal MyQ transformations than to separately change settings of each card reader.

How to set up the card transformation:

On the **User Authentication** settings tab, in the **Cards** section and under **Advanced**, you can define and use a transformation for card readers and select to use it on a USB reader connected to the administrator PC. The USB reader can be used to recharge credit or associate cards.

⚠ Please note that Transformation Commands are not displayed in the log. Only the full, extracted card number from the reader is shown. Once the registration process is complete, the transformed card number is stored in the user's profile.

Defining the Transformation

You can define the transformation by adding commands that can be found on the list below. The commands have to be separated by a semicolon (;) and are read and executed from left to right. For example in the transformation *CommandX;CommandY*, *Command X* is executed first and *Command Y,* second.

All the commands, except for the **+** command, are applied in the following way:

The first command of the transformation and each command immediately behind the **+** command are applied to the initial card number. All other commands are applied to the result of their predecessors.

ID Card Transformation Commands

- **ltrim(number of characters)** – Remove the first X characters from the left.
  ltrim(2): 123456 —> 3456
- **rtrim(number of characters)** – Remove the first X characters from the right (the last X characters).
  rtrim(2): 123456 —> 1234
- **prepend(character string)** – Add the string in front of the card number.
  prepend(AB): 123456 —> AB123456
- **append(character string)** – Add the string behind the card number.
  append(AB): 123456 —> 123456AB
- **left(number of characters)** – Select the first X characters from the left (and remove the rest).
  left(2): 123456 —>12
- **right(number of characters)** – Select the first X characters from the right.
  right(2):123456 —> 56
- **mid(number of characters, number of characters)** – Count X characters from the left and then remove Y number of characters.
  mid(2,2): 123456 —> 1256

- **lpad(number of positions, symbol)** – Complete the string to the length specified by the **number of positions** parameter by adding the value of the **symbol** parameter to the left (in front of the card number).
  lpad(12,0): 123456 —> 000000123456
- **hex2dec()** – Transform the card number from hexadecimal mode to decimal mode.
  hex2dec(): 1000AB —> 1048747
- **dec2hex()** – Transform the card number from decimal mode to hexadecimal mode.
  dec2hex(): 1048747 —>1000AB
- **hex2bin** – Transform the card number from hexadecimal mode to binary mode.
  hex2bin(): 1000AB —> 10000000000010101011
- **bin2hex** – Transform the card number from binary mode to hexadecimal mode.
  bin2hex(): 10000000000010101011 —> 1000AB
- **dec2bin** – Transform the card number from decimal mode to binary mode.
  dec2bin(): 100023 —> 11000011010110111
- **bin2dec** – Transform the card number from binary mode to decimal mode.
  bin2dec(): 11000011010110111 —> 100023
- **reverse()** – Reverse the byte sequence, i.e. take all the characters by two and reverse the order of the pairs. (The last pair goes first, the second last goes second, etc.)
  reverse(): 1234AB —> AB3412
- **reverseString()** – Reverse the character sequence. (The last character goes first, the second last goes second, etc.)
  reverseString(): 1234AB —> BA4321
- **reverseNibbleBits()** – Convert each character from hexadecimal mode to binary mode, reverse the character sequence of each quadruple and convert the result back to hexadecimal mode.
  reverseNibbleBits(): 10AB —> 0001 0000 1010 1011 —> 1000 0000 0101 1101 —> 805D
- **upper()** – Converts the string to upper case.
  upper(): Abcd —> ABCD
- **plugin(reference)** – Calls a card transformation plugin with the given reference. This option enables using custom PHP scripts for the transformation. For more information about this option, contact MyQ support.
- **asciiCode2ascii** – Converts ASCII characters encoded as hex-digits to ASCII characters.
  asciiCode2ascii(): 414F —> AO
- **"string 1" + "string 2"** – Merges the strings in front of and behind the **+** command.
  "string 1":

- Either the initial card number (if there are no commands preceding the **+** symbol),
- or the result of the last command before the **+** symbol (if there are no **+** commands preceding the **+** symbol),
- or the result of the previous **+** command.

"string 2":

- Either the initial card number (if there are no commands behind the **+** symbol or if the next command is another **+** command),
- or the result of the last command of the transformation (if there are no **+** commands behind the **+** symbol),
- or the result of the last command before another **+** command.

ID card transformation example:

Card number: 10AB

Card code transformation: hex2bin();lpad(16,0);reverseString();ltrim(8);reverseString();bin2hex() + ltrim(4);lpad(4,10AB)

Result: *1010AB*

Transformation process:
("10AB" —>"1 0000 1010 1011" —> "0001 0000 1010 1011" —> "1101 0101 0000 1000" —> "0000 1000" —> "0001 0000" —> "10") + ("10AB"" —> "" —> "10AB") ==> "1010AB"

Delete Cards

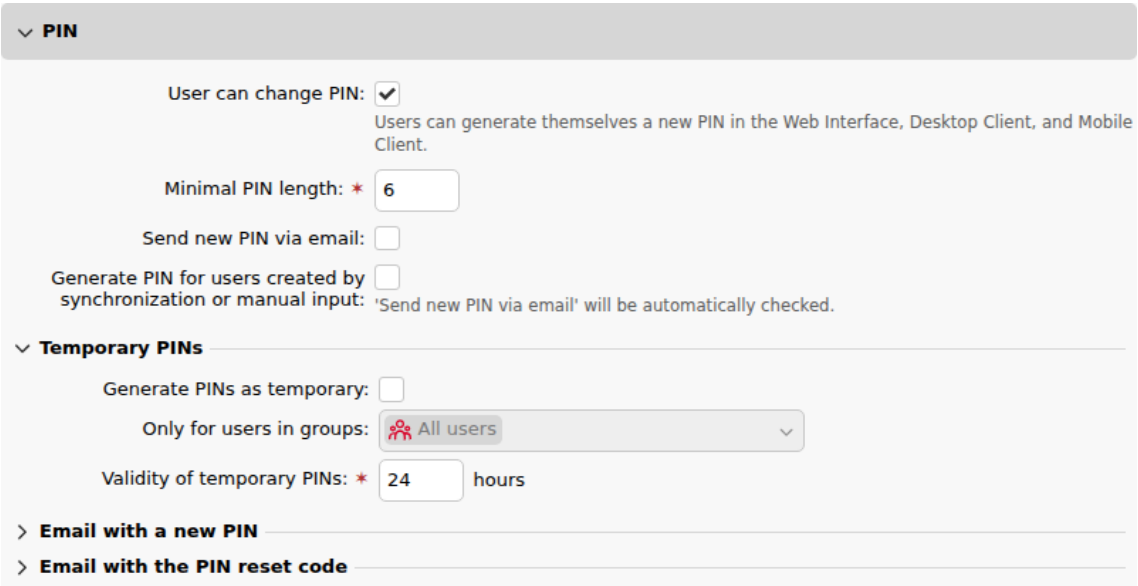
If you have the **Delete Cards** permission assigned to you, you can delete other user's cards. This is intended, for example, for situations where an organization has a Front Desk where you return your card and it should be removed from the system.

To do so:

1. Log in and open the MyQ Dashboard.
2. Click the **Delete cards…** option.
3. Fill in the ID card number (manually or by swiping the card at a reader connected to your computer).
4. Click **Enter** to search for the card.
5. When the user is found, click **X** to delete the card, and then **Save** the changes.

10.9.3 Generating PIN

On the **User Authentication** settings tab, under **PIN**, you can select multiple options concerning PIN generation.



Users Can Change Their PIN

With this 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.

Minimal PIN Length

This option determines the mandatory minimum PIN length. The number can be set between *4* and *16* - the default is *6*.
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 only for users with PINs, or all the active users. If the administrator chooses to generate new PINs for all users, the old PINs will be deleted and new PINs will be automatically sent via email to all the active users.

Generate PIN for Users Created in Synchronization or Manual Input

With this 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.

Send New PIN via Email

With this 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 templates are editable and the values can be reset to their defaults if needed, by clicking **Revert values**.

Temporary PINs

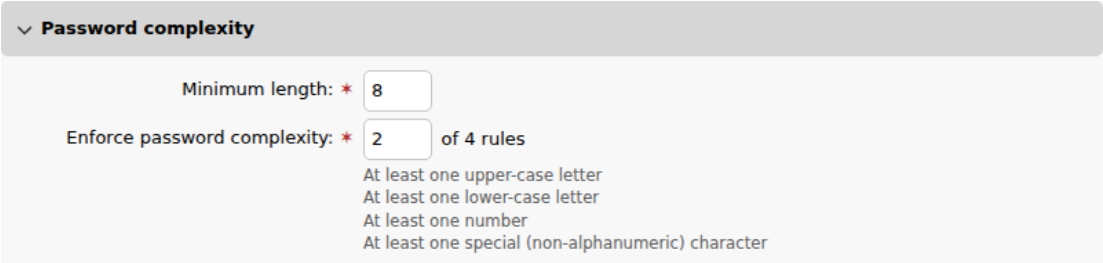
Generate PINs as temporary - With this option selected, for the selected user groups in the **Only for users in groups** field, the automatically generated PINs are always temporary. You can set the **Validity of temporary PINs** in hours (24 hours by default).

Limitations

- Users using an LDAP, Microsoft Entra ID, or Radius authentication server cannot sign in on the MyQ Web User Interface with a PIN.

10.9.4 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

10.9.5 External Authentication via API Connector

This page covers authenticating ID cards or PINs through a custom service via API. This is useful when your authentication service is not natively supported by MyQ. To authenticate user credentials against LDAP or Radius servers, see Authenticate Users from LDAP or RADIUS (see page 500).

External Authentication is used for login on the MyQ Embedded Terminal and MyQ Desktop Client. The MyQ Web User Interface and MyQ X Mobile Client require credentials set in MyQ.

How It Works

An API connector between MyQ and the authentication service is set up. MyQ requests authentication through this connector, and on the other side is the authentication service itself where users and their credentials are stored.

1. User attempts to sign in on the MyQ Embedded Terminal with one of these methods:
    - Swiping their ID card
    - Entering their PIN
2. The request is sent to the API connector, containing the login method type and the value.
3. The connector handles communication with the authentication service and returns the user who matches back to MyQ.

There are two modes of operation for External Authentication. Either it **can be the primary way of authenticating** users, or it can be configured **as a backup authentication** in case the authentication towards MyQ fails. For this, the option "Use only if authentication against MyQ DB fails" can be selected.

Authentication Request

Supported Login Methods

This setting **defines the login method** for which External Authentication is used. The other, unselected, login method authenticates the user against the credentials in MyQ.

- ID Card
- PIN

MyQ sends the type of login method together with the actual PIN/ID card value so that the API connector can recognize which user property should be used to find the correct user.

For example, if an ID Card is selected, and the user authenticates on the Embedded Terminal with an ID card, MyQ sends out `loginType=1&loginValue=1234`. This can be interpreted as the ID card number `1234`.

⚠ If a card reader that emulates keystrokes is connected to the device and a user swipes their card, MyQ cannot recognize if the value received is a PIN or ID card number. MyQ indicates this to the API connector (`loginType=7`). The connector should be configured to handle these requests, e.g. by attempting to authenticate towards both user properties.

Authentication Response

Supported User Identifiers

The API connector has to respond in a JSON format with one of the values back to MyQ to pair the correct user and log them into the client.

- Personal number of an existing user in MyQ
- Username of an existing user in MyQ

Example responses:

- `{"result":0,"personalNumber":"123456"}` means that the user was successfully identified by the authentication service and its personal number is `123456`. The user with this personal number in MyQ is authenticated.
- `{"result":0,"username":"JohnDoe"}` means that the user was identified and its username is `JohnDoe`. The user with this username in MyQ is authenticated.

Error States

- Invalid user (`{"result":1}`) – the user was found, but their account is invalid (e.g. deactivated)
- No user found (`{"result":2}`) – there is no user associated with the credentials

Common Use Cases

The External API connector can be used in its most simple way to “translate” requests. But it also allows more advanced authentication workflows as the connector itself can perform a set of operations before it returns the matching user back to MyQ.

Example 1: Authentication service not supported by MyQ is required

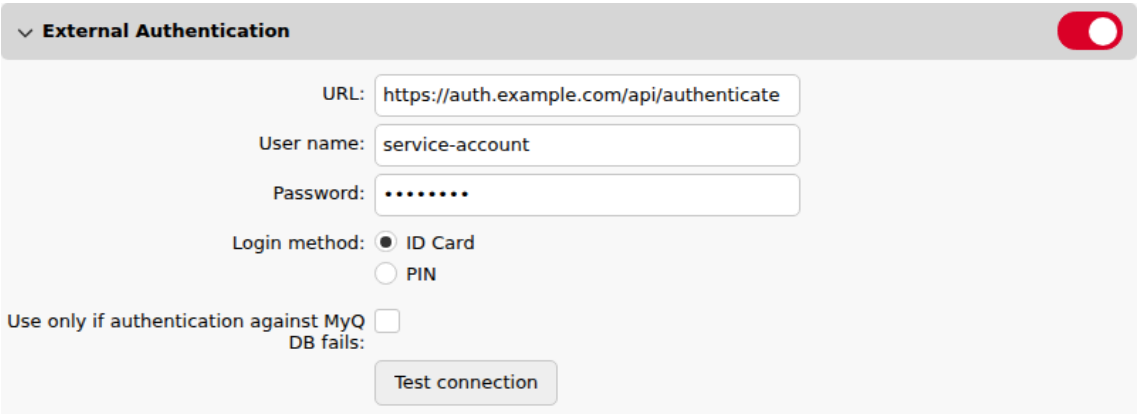
A connector that translates the API calls between MyQ and the remote authentication service.

Example 2: Advanced authentication workflow – multiple identities

External Authentication can be used in cases where some operation is required to happen between MyQ and the authentication server. This can be transformation, advanced user recognition in multi-domain environments, and more.

Setup External Authentication

External Authentication destination can be enabled and configured in **MyQ > Settings > User Authentication**.



- **URL**: type the URL where the API connector is running
- **User name**: type the user name required for the connection to the external server via API
- **Password**: type the password required for the connection to the external server via API
- **Login method**: choose the users login method - *ID Card* or *PIN*
- **Use only if authentication against MyQ DB fails**: this option defines whether the External Authentication will be the primary or secondary method for authentication
  - If enabled, the user is first authenticated towards the MyQ Print Server, and only after it fails, the next attempt goes through the remote authentication service
  - If disabled, no authentication towards the MyQ Print Server is performed, External Authentication service is always used

---

See also:

- Authentication Servers Settings (see page 233)

- (v5) External Authentication API
- Authenticate Users from LDAP or RADIUS (see page 500)

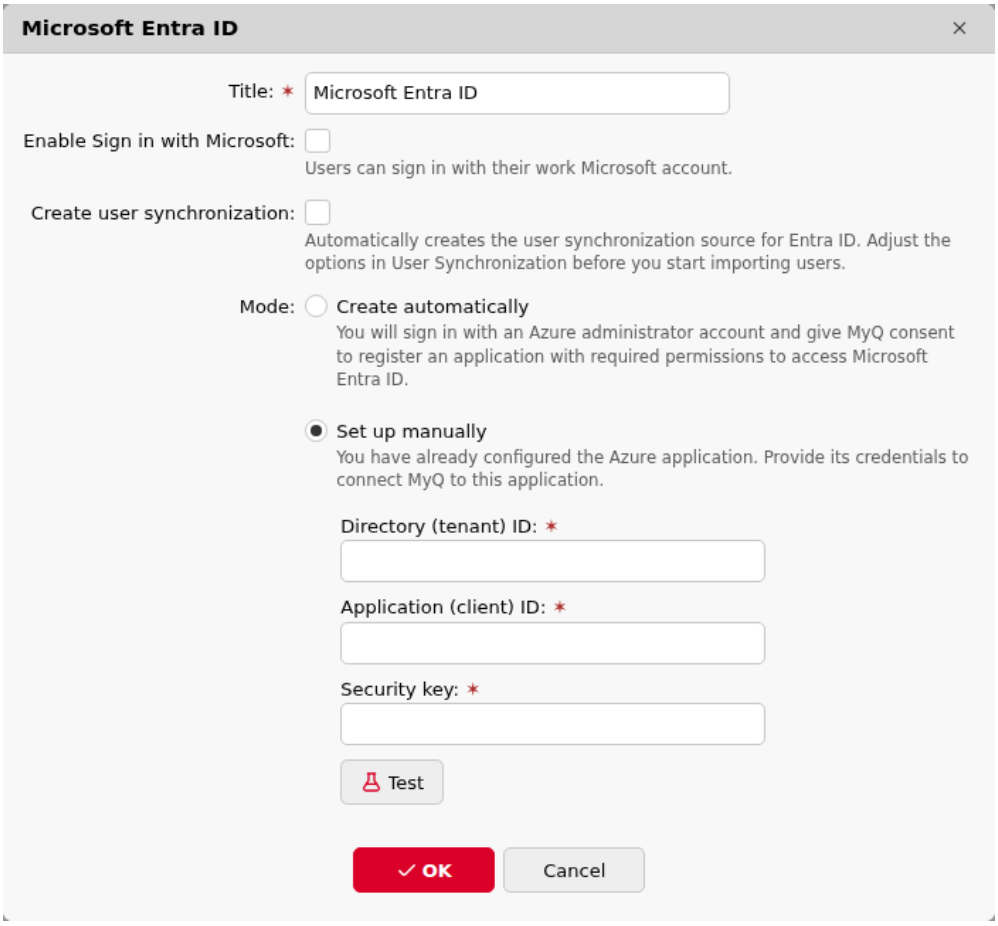
10.9.6 Configure Microsoft Entra ID Authentication

Configure Microsoft Entra ID as an authentication server to let MyQ users authenticate using their Microsoft identities. Entra authentication can be used with users synchronized from Microsoft Entra ID or assigned to individual MyQ users.

User authentication with Entra ID requires an existing Microsoft Entra ID connection in MyQ.

Add a Microsoft Entra ID Authentication Server

1. Go to **MyQ > Settings > Authentication Servers**.
2. Click **Add** and select **Microsoft Entra ID Server**.
3. Select the Microsoft Entra ID connection that should authenticate the users. If the required connection does not yet exist, select **Add New** and create it.
4. Enable **Sign in with Microsoft** if users should be able to authenticate through the Microsoft sign-in flow.
5. (Optional) Click **Test** to check that the connection to the server works.
6. Click **Save**.



Assign the Authentication Server to Users

Creating an authentication server does not automatically assign it to MyQ users. The Entra authentication server must also be assigned to the users who should authenticate against it.

You can assign it:

- automatically during Microsoft Entra ID user synchronization, or
- individually in a user's MyQ profile.

Assign during User Synchronization

When synchronizing users from Microsoft Entra ID, enable **Use as authentication server** in the synchronization source. MyQ assigns the associated Entra authentication server to the synchronized users. This determines that their external authentication is performed against Microsoft Entra ID.

This setting is independent of **Sign in with Microsoft**, which controls whether the Microsoft interactive sign-in method is available.

Use this approach when Entra ID is both the synchronization and authentication source for the same users.

Assign to an Individual User

To configure authentication for an individual user, open the user's properties and enable **Use authentication server**. Select the required Microsoft Entra ID authentication server.

Use individual assignment when only selected users should authenticate against Entra ID or when the users were created or imported from another source.

Choose How Users Authenticate

Users assigned to a Microsoft Entra ID authentication server can authenticate either by entering their Microsoft credentials or, on supported MyQ interfaces, through **Sign in with Microsoft**.

Microsoft Username and Password

When a user enters a username and password, MyQ authenticates the credentials against the assigned Microsoft Entra ID authentication server.

On Embedded Terminals using username and password authentication, MyQ first checks whether the entered value matches the user's MyQ PIN. If it does, the user is authenticated locally. Otherwise, the value is passed to the external authentication server as the user's password.

On the MyQ Web Interface, users assigned to an external authentication server cannot authenticate using their MyQ PIN.

Sign In with Microsoft

Sign in with Microsoft uses Microsoft's interactive authentication flow rather than requiring the user to enter Microsoft credentials directly into MyQ. It is available on:

- MyQ Web Interface
- MyQ Desktop Client
- MyQ X Mobile Client

It is not available as an Embedded Terminal authentication method.

Because authentication takes place through Microsoft, authentication requirements configured for the user's account, such as multi-factor authentication, can be applied during sign-in.

Signing out of MyQ does not necessarily end the user's Microsoft session. If the user remains signed in to Microsoft, Microsoft may reuse that session the next time authentication is requested.

Multiple Microsoft Entra Tenants

MyQ can authenticate users against multiple Microsoft Entra tenants.

Create a separate Entra connection and authentication server for each tenant. Give each one a clear and unique name so that users can identify the appropriate Microsoft organization when signing in.

When **Sign in with Microsoft** is enabled for multiple authentication servers, the available tenant sign-in options are presented to users during login.

In Central Server and Site Server environments, Entra authentication servers configured on the Central Server are automatically distributed to connected Site Servers.

All configured Entra authentication servers are available on every Site Server. They cannot be restricted to selected Sites.

Single Sign-On with MyQ Desktop Client

MyQ Desktop Client can use Microsoft Entra ID to authenticate supported Windows users automatically without requiring them to interact with the Microsoft sign-in page.

Desktop Client attempts Entra authentication silently using the identity of the signed-in Windows user. If Entra authentication fails, MyQ Desktop Client can fall back to Integrated Windows Authentication, if configured, and then to manual sign-in.

See also:

- Connect to Microsoft Entra ID (see page 202)
- Authentication Servers Settings (see page 233)
- (v2) Single Sign-On with Entra ID

- (v2) Multiple Microsoft Entra ID Tenants

10.9.7 Configure Integrated Windows Authentication

Integrated Windows Authentication (IWA) lets users authenticate to MyQ using their signed-in Windows identity. MyQ uses Kerberos where available and can fall back to NTLM unless Kerberos-only authentication is enforced.

Use IWA for users and workstations that are part of the same Active Directory domain as the MyQ server, or of a trusted domain. Users outside the domain environment need another authentication method.

Prerequisites

- Active Directory Domain Services (AD DS) is available.
- The MyQ server and client computers are joined to the same domain or trusted domains.
- DNS resolves the FQDN used to access the MyQ server.
- Time is synchronized between domain controllers, the MyQ server, and client computers.
- Users are synchronized to MyQ.
- Active Directory is configured as the authentication server for the affected users.
- You have the permissions required to register a Service Principal Name (SPN) in Active Directory.

Enable Windows Authentication in MyQ

1. Go to **MyQ > Settings > Users > User Authentication**.
2. Enable **Sign in with Windows Authentication**.
3. Save the settings.

Windows Authentication becomes available as an additional authentication method in the MyQ Web Interface.

Users who are not covered by IWA can continue to use other configured authentication methods.

Configure Kerberos

Kerberos is the preferred protocol for IWA.

MyQ uses the Windows HTTP Server API (`http.sys`) for Windows authentication. The HTTP Service Principal Name (SPN) must therefore be registered on the **computer account of the MyQ server**, not on a separate MyQ service account.

The SPN must correspond to the FQDN that users use to access MyQ.

Register the SPN

Open Command Prompt as a user with the required Active Directory permissions, on a domain controller or another computer with the appropriate Active Directory management tools.

Register the HTTP SPN:

```
setspn -S HTTP/myqserver.domain.com MYQSERVER
```

Replace:

- `myqserver.domain.com` with the FQDN used to access MyQ.
- `MYQSERVER` with the computer account name of the MyQ server.

Verify the registered SPNs:

```
setspn -L MYQSERVER
```

Confirm that the required `HTTP/<FQDN>` entry is present.

If users access MyQ through a different hostname, alias, or FQDN, ensure that the corresponding SPN configuration matches the address actually used by clients.

Configure Browser Authentication

For IWA to work in the MyQ Web Interface, the browser must recognize the MyQ server as an integrated-authentication destination and be permitted to send the signed-in user's Windows credentials automatically.

In managed environments, distribute the required browser settings centrally using Group Policy, MDM, or the browser's enterprise policy mechanism.

Microsoft Edge Example

On a client computer:

1. Open **Internet Options > Advanced > Security** and enable **Integrated Windows Authentication**.
2. Go to **Internet Options > Security > Local intranet > Sites > Advanced**.

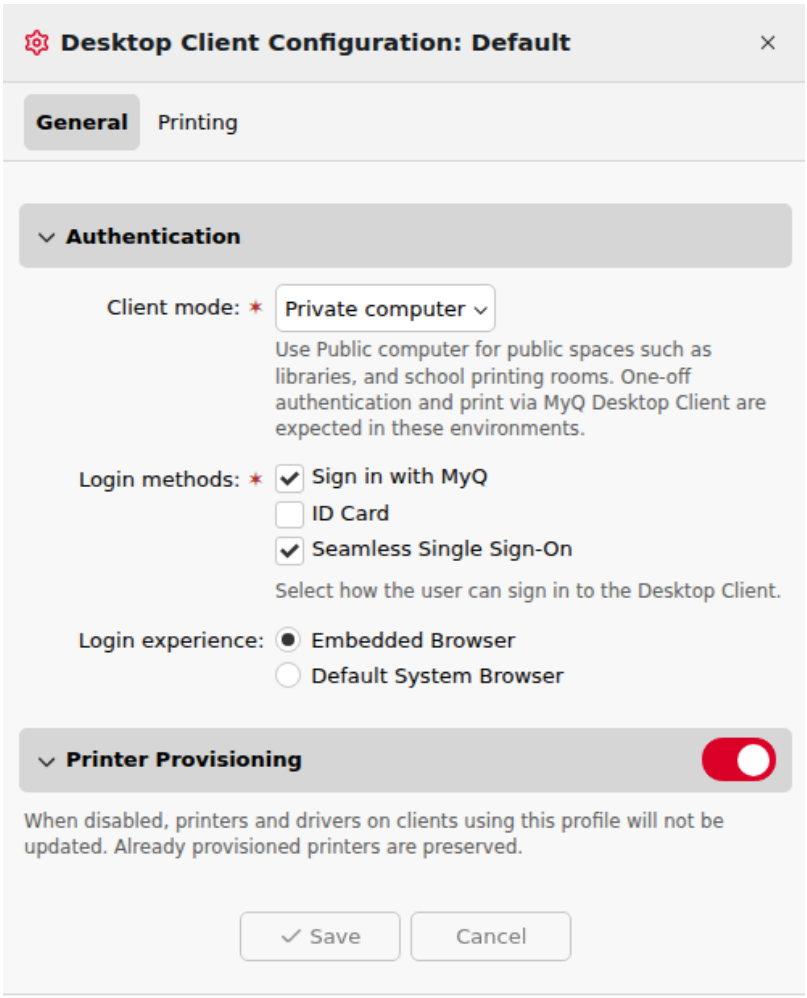
3. Add the FQDN of the MyQ server.
4. Go to **Local intranet > Custom level > User Authentication > Logon**.
5. Select **Automatic logon only in Intranet zone**.

Other supported browsers can require their own integrated-authentication policies. Use the browser vendor's enterprise documentation when deploying these settings centrally.

Enable Seamless Single Sign-On for MyQ Desktop Client

MyQ Desktop Client enables automatic user authentication through its configuration profile.

1. Go to **MyQ > Settings > MyQ Desktop Client**.
2. Open the required configuration profile.
3. On the **General** tab, under **Authentication**, enable **Seamless Single Sign-On**.
4. Save the profile.



When Seamless Single Sign-On is enabled, Desktop Client attempts to authenticate the signed-in Windows user automatically. Depending on the authentication methods configured for the user and environment, MyQ can use Microsoft Entra ID SSO or Integrated Windows Authentication before falling back to manual sign-in.

Kerberos and NTLM

MyQ attempts Kerberos when the required conditions are available. NTLM can be used as a fallback when Kerberos cannot be applied. Kerberos is recommended for normal IWA deployments.

If NTLM is required for compatibility, use NTLMv2. If your organization restricts or disables NTLM through domain policy, verify that Kerberos is working correctly for MyQ before applying the restriction to affected clients.

Enforce Kerberos for MyQ

MyQ provides a server-level configuration option to prevent NTLM fallback. Add the following to `config.ini` on the MyQ server:

```
[Security]
KerberosOnly=true
```

This setting affects Windows authentication in MyQ. It does not disable NTLM for other applications or services in the Windows domain.

Restart the relevant MyQ services after changing advanced configuration settings where required.

Domain-Wide Policies

Windows Group Policy can also control Kerberos and NTLM behavior across domain-joined systems.

Common policy areas include:

Purpose	Group Policy location
Kerberos ticket settings	**Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Kerberos Policy**
NTLM restrictions	**Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options**

Changes to domain-wide Kerberos or NTLM policies can affect services other than MyQ. Coordinate them with your Active Directory or security administrators.

Domain Mapping

Windows domain names can be presented in different formats during authentication.

For example:

- NetBIOS name: `ACME`
- DNS domain name: `acme.example.com`

The domain received during authentication must correspond to the domain configured for the user's authentication server in MyQ.

If the client presents a NetBIOS domain name while MyQ is configured with the DNS domain name, authentication can fail. This is particularly relevant when NTLM is used.

MyQ provides the `domainsMapping` advanced configuration parameter for mapping domain-name variants.

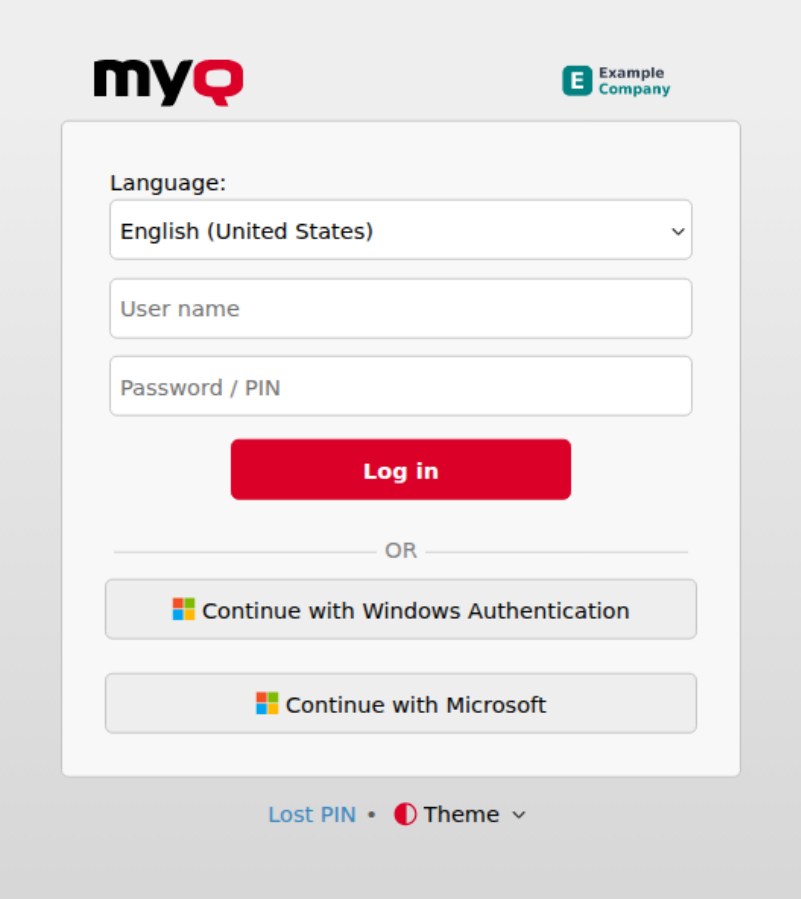
For the parameter syntax and advanced configuration procedure, see **Advanced Configuration**.

Verify Integrated Windows Authentication

After configuration, test IWA from a representative domain-joined workstation.

For the Web Interface:

1. Sign in to Windows as a MyQ user configured to authenticate against Active Directory.
2. Open the MyQ Web Interface using the FQDN configured for Kerberos.
3. Select the Windows Authentication sign-in option.
4. Confirm that the user is authenticated without entering additional credentials.



Also test MyQ Desktop Client if IWA is part of the Desktop Client configuration.

Verify Kerberos or NTLM Usage

Windows authentication is handled by Windows and Active Directory. MyQ logs therefore do not necessarily identify whether an individual IWA authentication used Kerberos or NTLM.

Use Windows and Active Directory security logs to verify the authentication protocol.

Relevant Kerberos events on domain controllers include:

- 4768: Ticket Granting Ticket request
- 4769: Kerberos service ticket request
- 4771: Kerberos pre-authentication failure
- 4775: Authentication failure
- 4624: Successful Windows logon

NTLM authentication attempts are also recorded in Windows security events.

These events can identify the authenticating user and originating computer, but they do not necessarily identify MyQ as the application that initiated the authentication.

Troubleshooting

If IWA does not work as expected, check the following.

Kerberos Falls Back to NTLM

Verify that:

- the client accesses MyQ using the expected FQDN,
- DNS resolves that FQDN correctly,
- the corresponding HTTP SPN exists,
- the SPN is registered on the MyQ server computer account,
- there are no duplicate SPNs in Active Directory,
- the client, server, and domain controllers have synchronized time.

Windows Authentication Does Not Start in the Browser

Verify that:

- Integrated Windows Authentication is enabled in the browser,
- the MyQ server is recognized as an intranet or integrated-authentication destination,
- browser enterprise policies allow automatic Windows authentication for the MyQ FQDN.

Test the configuration on a domain-joined workstation before applying it to the wider environment.

Authentication Works for Some Domains but Not Others

Verify:

- the trust relationship between the domains,
- the authentication server assigned to the affected users,
- the domain name presented by Windows during authentication,
- whether NetBIOS and DNS domain names need to be mapped using `domainsMapping`.

Authentication Fails After NTLM Is Disabled

Confirm that Kerberos authentication succeeds before enforcing Kerberos-only behavior or disabling NTLM through domain policy.

In particular, verify DNS, SPN registration, browser policy, and domain connectivity.

See also:

- (v2) Integrated Windows Authentication
- Configure Microsoft Entra ID Authentication (see page 519)
- Authentication Servers Settings (see page 233)
- Advanced Configuration (see page 271)

10.10 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.

10.10.1 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.

10.10.2 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:

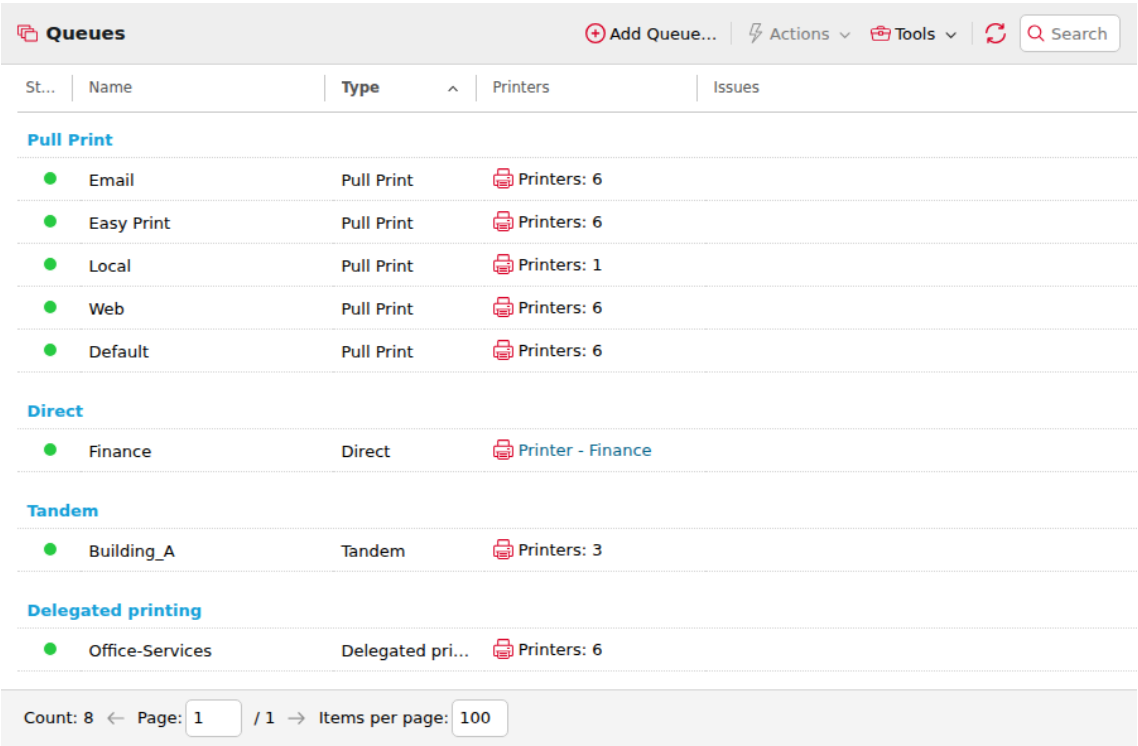
On the **Users** main tab of the MyQ Web Interface, select the users that you want to anonymize, then click **Actions** (or select the users, and then right-click any of them), and finally click **Anonymize**.

See also:

- Reports (see page 680)

11 Queues

On the **Queues** main tab, you can see queues and information about them. The queues are divided into groups according to their type: **Pull Print**, **Direct**, **Tandem**, and **Delegated printing**.



11.1 Default Queues

After installing MyQ, there are five default **Pull Print** queues on the **Queues** main tab: **Default**, **Easy Print**, **Email**, **Local**, and **Web**.

- **Default**: Pull Print queue where all users have access and all printers are assigned.
- **Easy Print**: Pull Print queue using the Easy Print feature.
- **Email**: All jobs sent from email are assigned to this queue.
- **Local**: Used with locally connected printing devices (USB, LPT).
- **Web**: All jobs sent directly from the web user interface are assigned to this queue.

If you are using a Central-Site environment, the following queues are also available by default:

- **Job Roaming**: Job Roaming enables users to transfer their jobs from one location to another. Jobs sent to one branch are automatically assigned to this

system queue and can be printed on printing devices at any other branch. This queue can be used in a Central-Site environment only.
- **Job roaming delegated**: Delegated printing jobs used with job roaming are automatically assigned to this system queue. This queue can be used in a Central-Site environment only.

See also:
- Queue Types (see page 533)
- Adding, Copying, and Deleting Queues (see page 535)
- Editing Queues (see page 536)
- Online/Offline Queues (see page 539)
- Personal Queues (see page 540)
- Advanced Queue Options (see page 542)
- User Detection Methods (see page 576)
- Binary Find & Replace (see page 580)

11.2 Queue Types

For each queue, except for the default queues, you can select from four options as to what happens with the jobs that are sent there. This section describes these four queue types.

See also:
- (v2) Queue Types in the Deployment guide

11.2.1 Direct

A direct queue can have only one printing device assigned to it. Print jobs in this queue are sent directly to the printing device and are immediately printed.

When you add printers using printer discovery, you can automatically create a direct queue for every newly discovered device.

11.2.2 Tandem

A tandem queue can be used on places with multiple printers and a higher printing volume. Jobs sent to this queue are evenly distributed among the devices and do not have to wait for one particular printer. This way, a large volume of print jobs can be spread between printers and printed in a significantly shorter time.

The queue can have multiple printing devices assigned to it. Print jobs from the queue are distributed among the printing devices that are not busy at the moment and they are immediately printed. If there are multiple idle printing devices, the print job is sent to the printer with the lowest printed pages counter.

To maintain a balanced printing device load, make sure that the printed page counters on all of the used printing devices are similar. Otherwise the printing devices with the lower printed page counter might be overused.

You can manually change the page counter on the **Printer total counter adjust for load balancing:** setting on the printing device properties panel on the **Printers** main tab. The number that you enter is added to the counter.

11.2.3 Pull Print

With this queue, users can send multiple jobs and print them when they want on any of the printers assigned to the queue.

The queue can have multiple printing devices assigned to it. All of the assigned printers have to be equipped with MyQ terminals. Jobs sent to a pull print queue are processed by the system and saved on the server.

Once the user logs in on any printer assigned to this queue, the print job is sent to this device and the user can print it.

To use a pull print queue, an embedded terminal or a Release Station is required.

For more information on embedded terminals, see:

- MyQ Brother Embedded
- MyQ Canon Embedded
- MyQ Epson Embedded
- MyQ Fujifilm Embedded
- MyQ HP Embedded
- MyQ KATUN Embedded
- MyQ Kyocera Embedded
- MyQ Kyocera Embedded Lite
- MyQ Lexmark Embedded
- MyQ Ricoh SmartSDK Embedded
- MyQ Sharp Embedded
- MyQ Sharp Luna Embedded
- MyQ Toshiba Embedded
- MyQ Xerox Embedded

11.2.4 Delegated

The delegated printing feature enables users and groups of users to choose delegates who can print their print jobs. After the delegating user (or group of users) sends a job to the **Delegated printing** queue, all delegates can see the jobs and print them.

The **Delegated printing** queue type works in the same way as the **Pull Print** queue type, except that it supports the delegate printing feature.

The delegates do not need to have rights to the delegated printing queue where the job was sent.

11.3 Adding, Copying, and Deleting Queues

11.3.1 Adding a Queue

1. On the **Queues** main tab, click **+Add queue**. The new queue properties panel opens on the right side of the screen.
2. On the panel, add a **Name** for the queue, select a **Type**, further modify the queue's settings (Queues general settings), and click **Save**.

11.3.2 Deleting a Queue

1. On the list of queues on the **Queues** main tab, select the queues that you want to delete, and then click **Actions** (or right-click the queue). The Actions drop-down box appears.
2. In the **Actions** drop-down box, click **Delete**. The queues disappear from the list.

11.3.3 Copying a Queue’s Settings

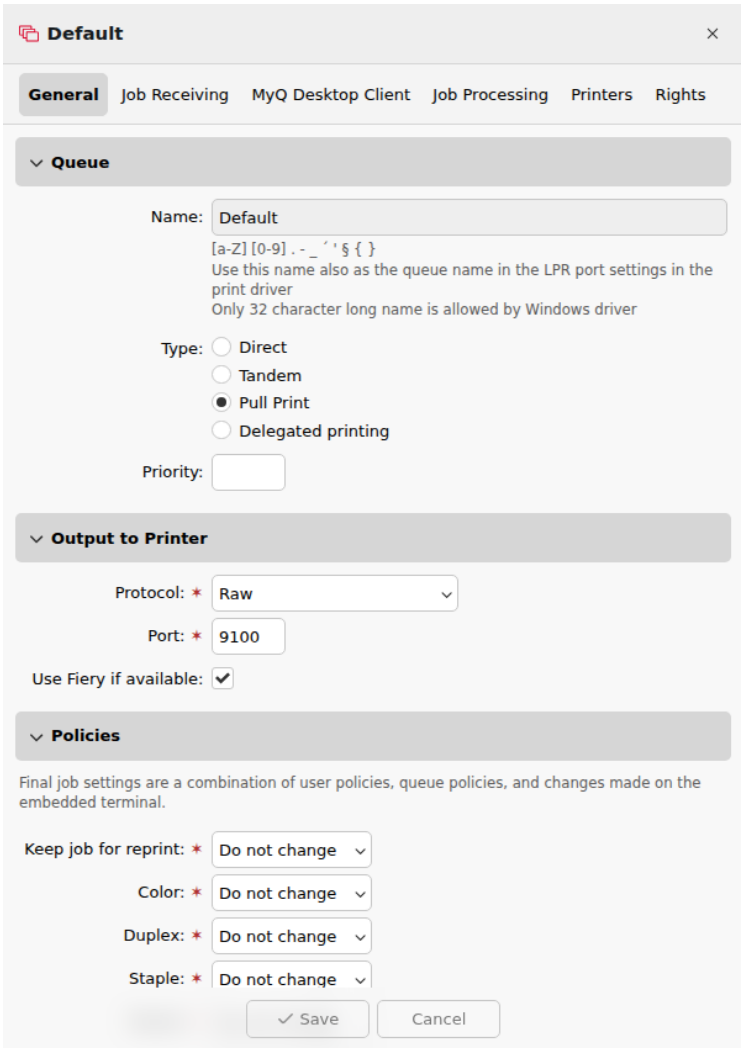
To speed things up when you are creating new queues, or editing your existing ones, you can copy the settings from a **Source Queue** to a **Target Queue**.

1. On the **Queues** main tab right-click the queue you want to copy the settings of, or copy settings to and select **Copy settings from Queue**.
2. A dialog box opens where you can: select the **Target Queue** (the queue to which the settings will be copied) and select the **Source Queue** (the queue settings will be copied from).

3. In addition, you can select which settings to copy from **Job Parsing**, **PJL Detection**, **and Print Drivers**. Click save to copy the settings to the **Target Queue**.

11.4 Editing Queues

Each individual queue has its own properties panel. To open the panel, double-click the queue on the list of queues on the **Queues** main tab (or right-click the queue, and then click **Edit**). The properties panel opens on the right side of the screen.



The basic setup of a queue can be done in four tabs: the **General** tab, the **Job receiving** tab, the **Printers** tab, and the **Rights** tab.

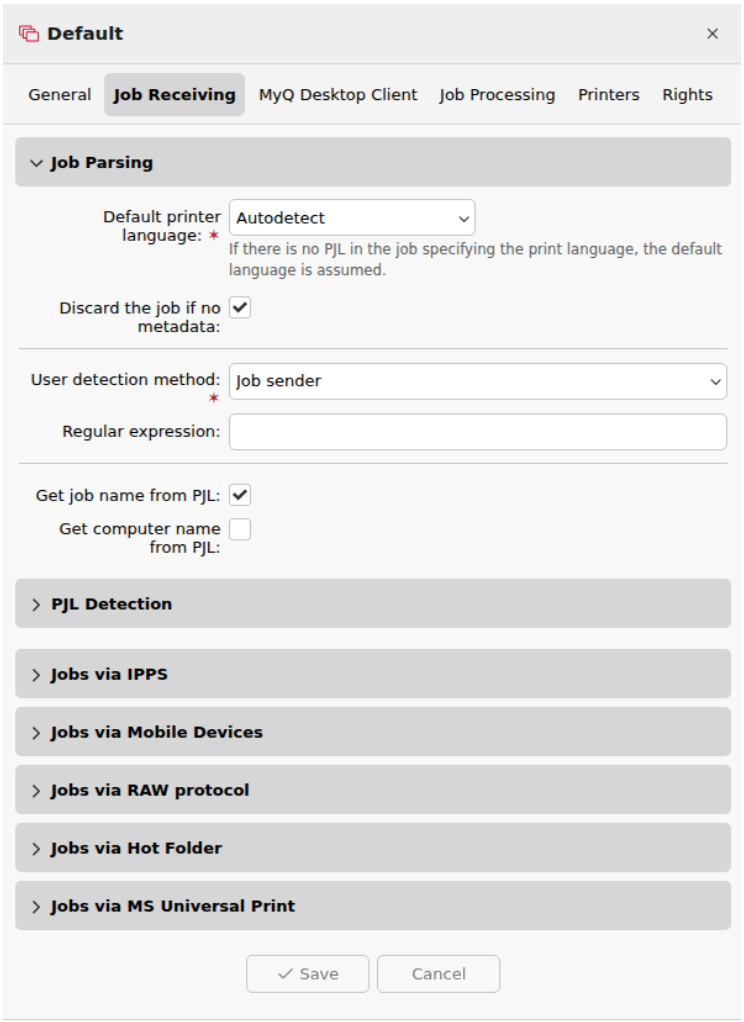
11.4.1 General Tab

- **Name:** Enter a name for the queue. This is an essential parameter for directing print jobs to MyQ and it is part of the print port setting. It is unique, case-sensitive, and cannot contain diacritics and spaces. This entry is mandatory.
- **Type:** Select a type for the queue. The available queue types are: *Direct*, *Tandem*, *Pull Print*, and *Delegated Printing*.

See also:
- (v2) Queue Types

11.4.2 Job Receiving Tab

- **Discard the job if no metadata**: Set the queue to discard a job if it was not parsed correctly.
- **User detection method**: Set the user detection method.
- **Get job name from PJL**: Set the queue to receive the job name from PJL.



See also:

- User Detection Methods (see page 576)

11.4.3 Printers Tab

By default, the **All printers** group is automatically assigned to every queue. You can delete this group to restrict the number of assigned printers.

To add a printing device or a group of printing devices to the queue:

1. On the bar at the top of the **Printers** tab, click **+Add**. A search dialog box appears.
2. In the dialog box, find the printing device (or group of printing devices) that you want to add to the queue, and then click **OK**.

To remove a printing device or a group of printing devices from the queue:

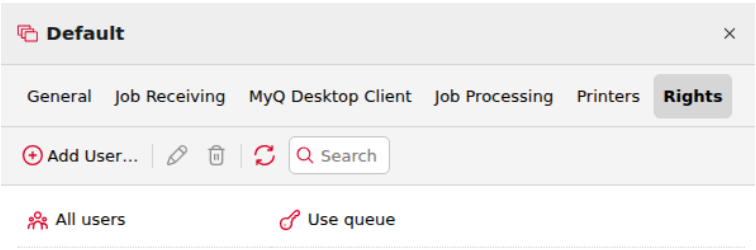
1. On the bar at the top of the **Printers** tab, select the printing device (or group of printing devices), and then click **–Remove**. The printing device (or group of printing devices) disappears from the **Printers** tab.

11.4.4 Rights Tab

By default, the **All users** group is automatically assigned to every queue. You can delete this group to restrict the number of users with the right to use the queue.

To provide a user or a group of users with rights to the queue:

1. On the bar at the top of the **Rights** tab, click **+Add User**. The Select user or group dialog box appears.
2. In the Select user or group dialog box, select the user (or group of users) that you want to provide with rights to the queue, and then click **OK**.



To remove the rights to the queue from a user or a group of users, on the **Rights** tab, select the user (or group of users), and then click the remove button (**X**). The user (or group of users) disappears from the **Rights** tab.

See also:

- Rights (see page 450)

11.5 Online/Offline Queues

While default queues are always online, each of the manually added queues can be switched to offline mode. Queues switched to offline mode do not receive any print jobs. However, users can still print jobs that are already waiting in these queues.

Jobs sent to an offline queue are rejected with the log message: *"Unknown or inactive queue '...'. The job was discarded."* displayed in the log, on the **Log** main tab of the MyQ Web Interface.

To switch between the online and offline mode of a queue:

1. Select the queue from the list on the **Queues** main tab, and then click **Actions** (or right-click the queue). The Actions menu appears.
2. In the Actions menu, click **Offline** (or **Online**). The queue switches to the selected mode.

11.6 Personal Queues

Personal queues in MyQ enable users to select the queues where their print jobs are sent to. The users can create multiple queues to ascertain that at least one of them has available printing devices where the job can be released.

If a user is not allowed to send the job to the currently checked personal queue, MyQ skips it and moves to the next one. If all personal queues are skipped, the job is sent to the queue set on the print port.

11.6.1 Activating Personal Queues

To activate personal queues:

1. On the **Users** settings tab, select the **Enable personal queues settings** option.
2. On the properties panel of the queue where the user's jobs are sent to by the print driver, add the PHP script shown below. The script moves the jobs to the first available personal queue of the user.

```
// get all user's queues sorted by priority
$personalQueues = $this->owner->personalQueues;
// loop them
foreach ($personalQueues as $q) {
// skip queue if no printer is available
if ($q->isAnyPrinterAvailable() === false) {continue;}
// queue printer is available, move job to queue
$this->moveToQueue($q->name);
// job is moved, stop the loop
break;}
```

After the feature is set up, each user can see a button for setup of their personal queues on their account on the MyQ Web Interface.

11.6.2 Setting Personal Queues

Once the feature is activated, both the MyQ users and the MyQ administrator can add and delete personal queues.

MyQ Users

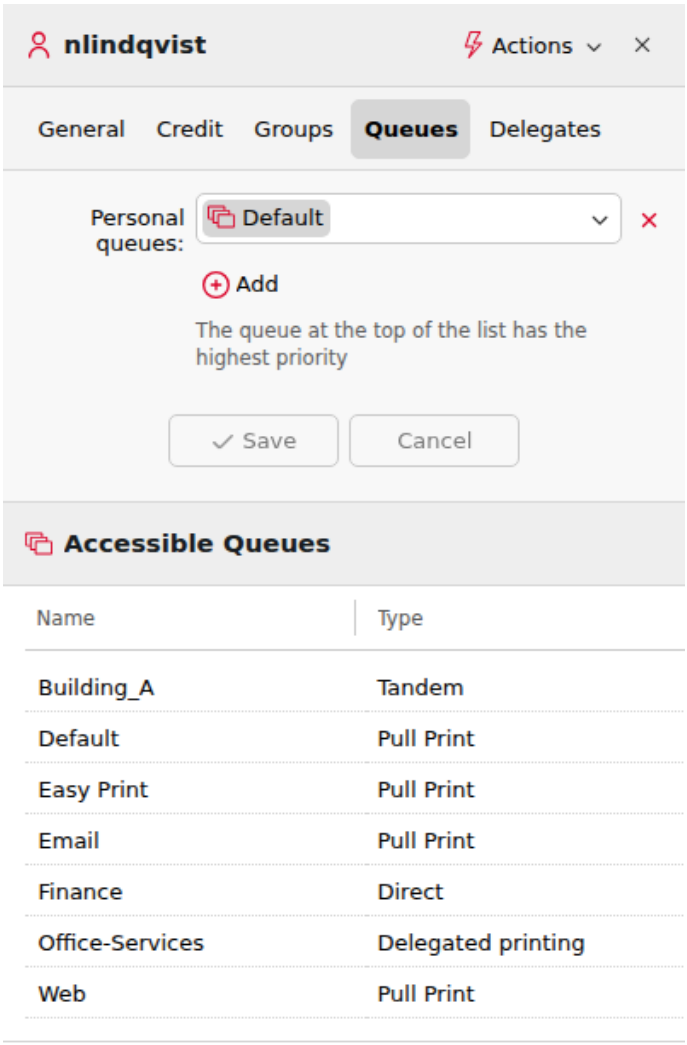
Users add and delete the personal queues on their user account on the MyQ Web Interface. To do this, they need to log in to the interface, then click **Personal queues** there, and lastly set the queues in the Personal queues dialog box.

After the user sends the job, MyQ checks the personal queues and sends the job to the first queue with available printing devices.

MyQ Administrator

The MyQ administrator adds and deletes the user's personal queues on the **Queues** tab of the user's properties panel on the **Users** main tab in the MyQ Web Administrator Interface. To access the tab, open the **Users** main tab (**MyQ > Users**), then double-click the user (or right- click the user, and then click **Edit** on the shortcut menu) to open the properties panel, and lastly click **Queues** on the panel.

On the **Personal queues** section, add and/or delete personal queues for the user.



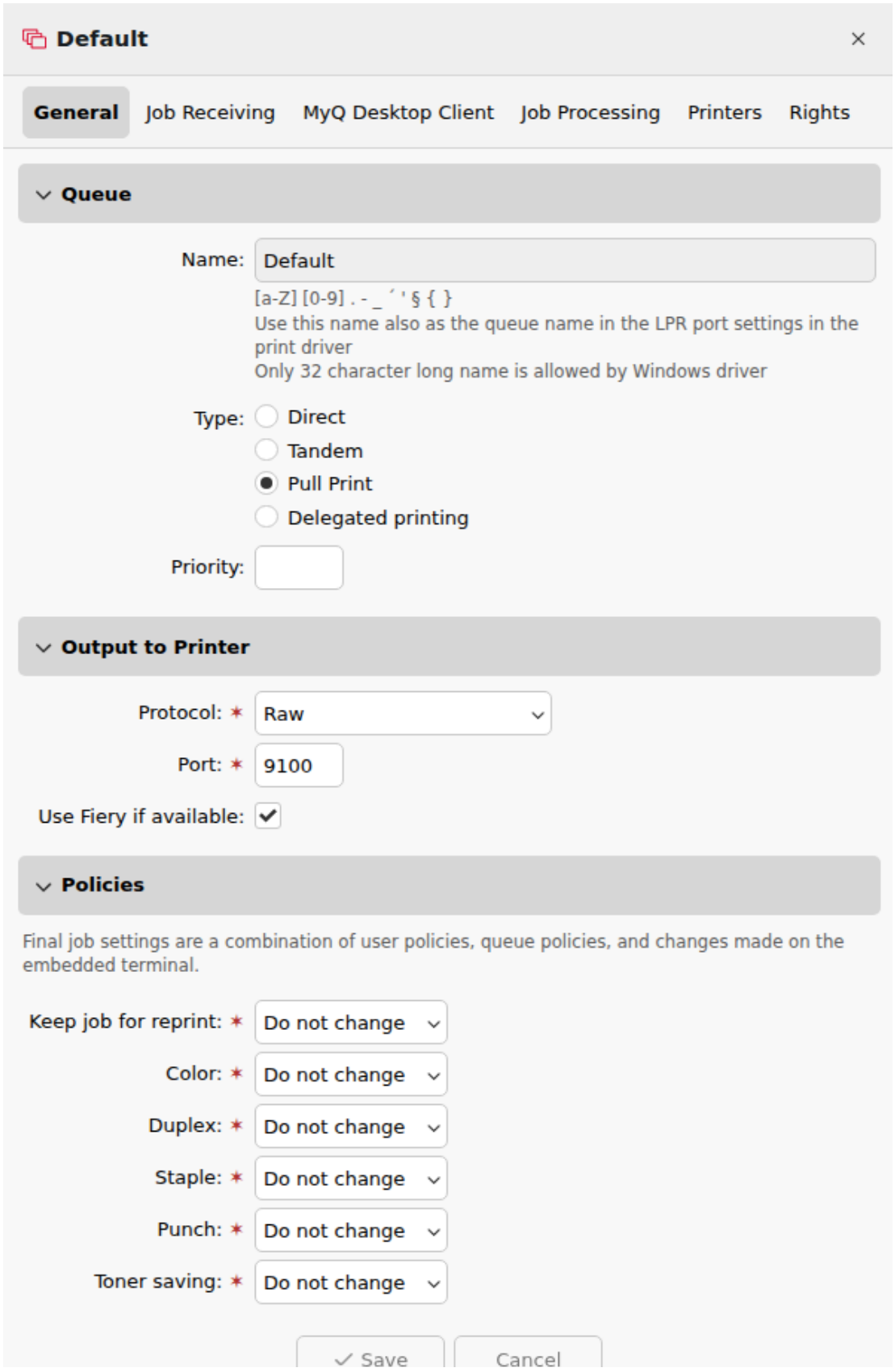
11.7 Advanced Queue Options

Once you have created a queue and set the basic options, like the name, type, printers and rights assignments, you can select some of the more advanced queue and job management features:

- General (see page 542)
- Job receiving (see page 545)
- Job processing (see page 552)
- MyQ Desktop Client (see page 550)
- Job Scripting (see page 556)

11.7.1 General Tab

Available advanced settings on a queue's general tab:


Default
General
Job Receiving
MyQ Desktop Client
Job Processing
Printers
Rights
Queue
Name:
Default
[a-Z] [0-9] . - _ ´ ' § { }
Use this name also as the queue name in the LPR port settings in the print driver
Only 32 character long name is allowed by Windows driver
Type:
Direct
Tandem
Pull Print
Delegated printing
Priority:
Output to Printer
Protocol:
Raw
Port:
9100
Use Fiery if available:
Policies
Final job settings are a combination of user policies, queue policies, and changes made on the embedded terminal.
Keep job for reprint:
Color:
Duplex:
Staple:
Punch:
Toner saving:
Do not change
Save
Cancel

Queue section

- **Priority**: When multiple jobs from pull print queues are to be released at the same time, the jobs
  that are sent to the queues with a higher priority are released before the jobs with lower priority. For example, if there are three jobs waiting to be released on a printing device, one with a priority number *0*, one with a priority number *-1* and one with a priority number *2*, the job with the priority number *2* is printed first, the job with the priority number *0* is printed second and the job with the priority number *-1* is printed third.
- **Keep jobs for reprint**: *Yes, No.* The **Keep jobs for reprint** setting is also available when configuring a Print Job Policy.

See also:

- Policies (see page 444)

Output to printer section

- **Protocol**: By default, print jobs are sent from MyQ to printing devices via the Raw protocol. Instead of it, you can use one of the alternative standard protocol options (*IPP, IPPS* or *LPR*) or the MyQ printing protocol, which can be used in two versions:
  - MPP: jobs sent via this protocol are compressed
  - MPPS: jobs sent via this protocol are compressed and encrypted via SSL
- **Port:** Here you can change the port of the selected protocol.
- **Use Fiery if available**: If you use a Fiery module for processing Postscript jobs, make sure that this option is selected and set the IP address of the module on the properties panel of the printing device to which the module is connected. Otherwise, you can deselect the option.

Policies section

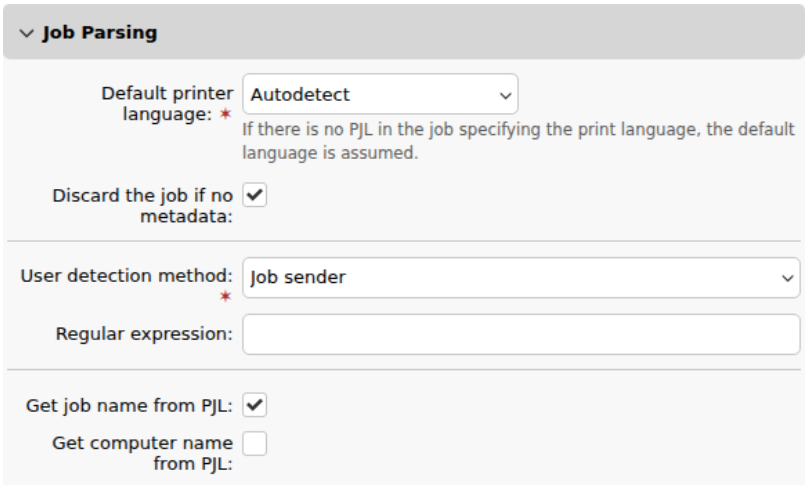
The final job settings are a combination of these queue settings, user policies and user changes made on the embedded terminal. All settings are set to *Do not change* by default.

- **Color:** *Do not change, Color, B&W*
- **Duplex:** *Do not change, Simplex, Duplex long edge, Duplex short edge*
- **Staple:** *Do not change, No, Yes*
- **Punch:** *Do not change, No, Yes*
- **Toner saving:** *Do not change, No, Yes*

11.7.2 Job Receiving Tab

On the **Job Receiving** tab of each queue, you can set how a job is parsed and other job receiving options.

Job Parsing



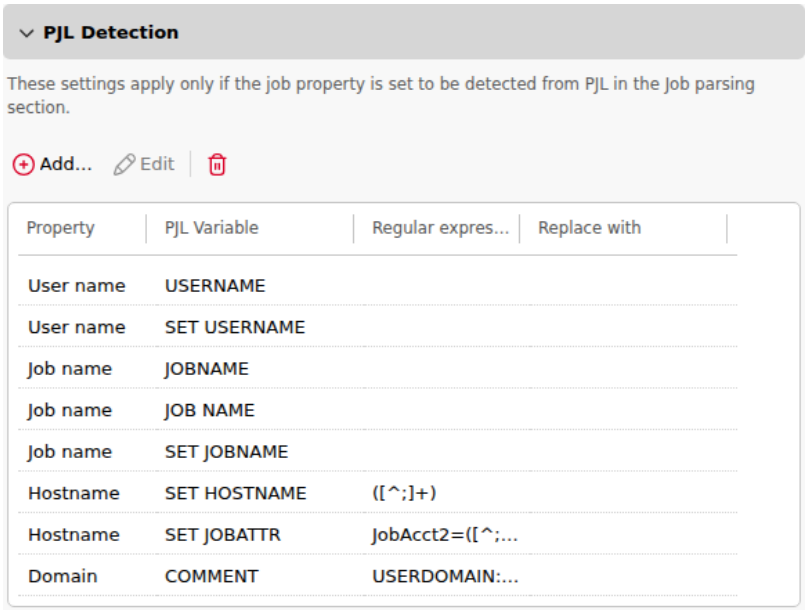
- **Default printer language**: Choose the default printer language from the drop-down menu. The available options are:
  - **Unknown**
  - **Autodetect** (default setting)
  - **PCL 5**
  - **PostScript**
  - **ESC/P**
  - **Prescribe**
  - **PCL 6**
  - **PDF**
  - **JPEG**
  - **XPS**

  If there is no PJL in the job specifying the print language, the default language is assumed.
- **Discard the job if no metadata**: If this option is selected, MyQ discards all jobs that do not contain metadata from the Job Parser. It can be used together with the **Credit** or **Quota** features to prevent printing jobs without necessary information (number of pages, color etc.). When a job is discarded due to this setting, the following message appears in the MyQ Log: "*Job metadata is required for the queue but the job parser is turned off. Job is canceled. | queue=QueueX*".
  This option requires Job Parser to be enabled.

- **User detection method**: Select how the job owner is identified.
  - Job Sender (default)
  - Sender's computer name
  - Print Server's DNS name
  - Sender's computer DNS name
  - Detect user from the job name
  - User detection from PJL
- **Regular expression**: You can use regular expressions to capture a part of the string that MyQ detects within any of the user detection methods. MyQ uses regular expressions with the ECMAScript engine, meaning that the first captured group is used: first, MyQ finds the first match for the regular expression, and then it identifies the job owner with the first group captured in the match. This way you can search for a string and define which part of it will be identified as the job owner. For example, you can use the regular expression to find an email address in the detected name string and use the group capturing to save just the part preceding the @ symbol.
- **Get job name from PJL**: With this option enabled, MyQ takes the job name from the *JOB NAME* parameter in the PJL header instead of detecting it from the LPR protocol.
- **Get computer name from PJL**: With this option enabled, MyQ takes the computer name from the PJL header instead of detecting it from the LPR protocol.

PJL Detection

These settings apply only if the job property is set to be detected from PJL in the Job parsing section. Click **+Add** to select a PJL property (from Job name, User name, Hostname and Domain) and set variables and regular expressions, **Edit** to modify any existing variables.



The job name in the PJL header may differ from the printed document's name.

See also: User Detection Methods (see page 576)

Jobs via IPPS

This section appears only when **Jobs via IPPS** is enabled in **MyQ > Settings > Jobs**.

Address

View the address that you must use to direct jobs to this queue for IPPS printing, in the format:

`https://{hostname}:{port}/queue/{queue-name}`

Release Options

You can select from the following release options for IPPS printing:

- **MyQ default release options**
- **Pass-through options of a selected printer** (pass-through mode): select which printer is used as the source of IPP attributes. This controls which printer capability profile is presented by the queue. If the printer is not found, the default release options are applied.

Only the *Job sender* user detection method can be used with IPPS printing.

See also: Jobs via IPPS (see page 595)

Jobs via Mobile Devices

When enabled, the queue is available to the **MyQ X Mobile Client** and can be published as a discoverable printer for **AirPrint** on iOS, iPadOS, and macOS, and **Mopria Print Service** on Android.

To enable mobile printing for the queue, set **Jobs via Mobile Devices** to **Enabled** and click **Save**.

AirPrint and Mopria clients must be able to discover the queue on the network. You can provide discovery in either of the following ways:

- **MyQ Mobile Print Agent:** use the agent to publish enabled MyQ queues for discovery on the client network.
- **DNS-SD:** manually publish MyQ queues using DNS Service Discovery. Use this option when you need DNS-based discovery instead of Mobile Print Agent.

Pull Print and Delegated queues can be made available to mobile devices.

When enabled, the queue is accessible from the MyQ X Mobile Client (iOS and Android) and is broadcast as a discoverable printer for AirPrint (iOS and macOS) and Mopria Print Service (Android).

Only the *Job sender* user detection method can be used with this queue.

To enable, set **Jobs via Mobile Devices** to **Enabled** and click **Save**.

Both the Mobile Client and AirPrint/Mopria use this setting, but have different infrastructure requirements:

- **MyQ X Mobile Client**: requires the Mobile Client app to be installed on the user's device. No additional server-side components are needed beyond this queue setting.
- **AirPrint and Mopria:** requires MyQ Mobile Print Agent to be installed, running, and connected to the MyQ server. The agent broadcasts enabled queues for discovery on the local network.

Pull Print and Delegated queues are displayed as available printers on the user's device.

See also:

- (10.2) MyQ X Mobile Client
- (1.3) Mobile Print Agent
- Jobs via IPPS (see page 595)
- Configure DNS-SD for AirPrint and Mopria Discovery (see page 572)

Jobs via RAW Protocol

The RAW protocol is the default protocol for systems that do not use Windows OS and for standard TCP/IP. The advantage of this protocol is that it sends data without further processing and has smaller packet headers.

As RAW comes without any job metadata, you must use a different port for each queue (starting from port *9100*). The used ports are added to Windows Firewall.

Click **+Add** next to **Port** and select a port.

Make sure that the queue has the following settings:

- **User detection method**: Select *User detection from PJL*, *MyQ Desktop Client* or *Detect user from the job name*
- If *User detection from PJL* is selected, **+Add** the desired PJL variable(s) and regular expression(s)

Because there are no metadata, the queue is determined by the TCP port, the user always from the PJL and the sending computer is the client's IP address.

Jobs via Hot Folder

In this section, you can associate the queue with one or multiple network folders where print jobs are stored.

If the folder is password protected, MyQ will use the credentials of the account MyQ service is running under.

The MyQ server will regularly monitor the network folder for new files. If there is new job in the folder, the MyQ server checks if it is supported for printing. Supported files will be downloaded and deleted from the folder, unsupported files will be deleted. The operation is logged in the MyQ log, for example:

```
"job 123.prn was downloaded from \\serverXYZ\folder1"
```

`"job 123.cpr was deleted from \\serverXYZ\folder1, file type is not supported"`

- Directly supported files: **.prn, .pcl, .ps, .eps, .pdf, .jpg, .bmp, .tif, .png, .txt**
- MS Office files are supported, but they are converted to PDF: **.doc, .docx, .xls, .xlsx, .ppt, .pptx, .odt, .ods, .odp**
- Files must be copied to the hot folder using standard SMB protocol or MyQ will not detect them.

Only the following user detection methods can be used: *Job sender*, *Detect user from the job name*, *User detection from PJL*.

Click **+Add** next to **Hot folder** and type the folder path.

Jobs via MS Universal Print

In this section, you can associate the queue with MS Universal print.

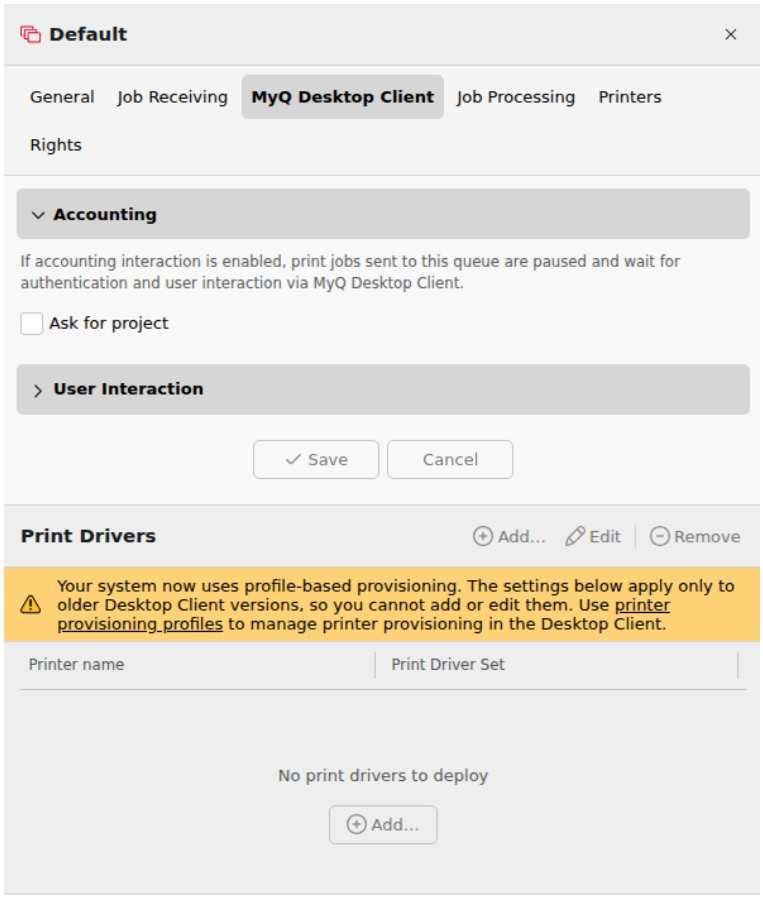
To do that, set the option to **Enabled**, and click **Save**. After a few minutes, your queue will be available as a virtual printer in MS Azure Universal Print.

See also:

- (v2) Set up Microsoft Universal Print
- Connect to Microsoft Universal Print (see page 220)

11.7.3 MyQ Desktop Client Tab

On the MyQ Desktop Client tab of each queue, you can set up accounting options and employ PHP scripts to set up interaction with MyQ users via dialog boxes displayed in MyQ Desktop Client on their computer.



If you have any form of accounting enabled (Credit, Quota, Projects), the **Accounting** section is visible and you can modify the settings for newly created queues. If accounting options are disabled, the section is not visible. If you disable any form of accounting and then re-enable it, the settings in the MDC tab are remembered.

- Mark the **Ask for project** checkbox if you want users to select projects before printing a job.
- Mark the **Ask for payment account (credit, quota, cost center)** checkbox if you want users to select a payment account before printing a job (enabled by default).

For more information, check the *MyQ Desktop Client* guides.

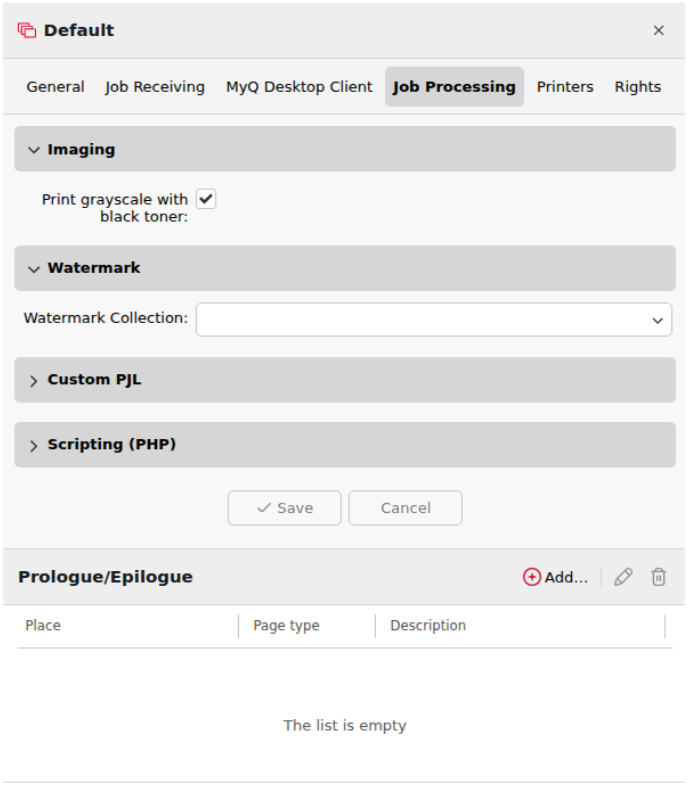
In the **User interaction** section, you can enable **User interaction**, add the script in the field, and click **Save**.

See also:

- User Interaction Scripting (see page 561)

11.7.4 Job Processing Tab

On the **Job processing** tab of each queue, you can enforce additional job processing actions by selecting one or more of the predefined job settings or by creating any number of custom PJL commands.



Imaging

Mark the checkbox if you want to **Print grayscale with black toner**.

Watermark

Choose your saved watermarks from the **Watermark** drop-down.

Custom PJL

You can set custom PJL commands to enforce other actions or provide additional information to the MyQ server. For example, you can use `@PJL SET PAPER=A4` to enforce the A4 paper format or `@PJL COMMENT="USERDOMAIN:somedomain.com;"` to provide the MyQ server with the information about the domain of the printing user.

You can also use the following MyQ variables: `%jobname%`, `%username%`, `%userID%`, `%fullname%`, `%personalnumber%`.

When you enter your own PJL sequence, it is necessary to enter the correct syntax. The command should always start with **@PJL**.

To be applied, a PJL command has to be supported by the printing device where the job is released. The information on what PJL commands are supported by a particular model of printing devices can be found in the documentation provided by the device manufacturer.

Staple and Punch PJL Values

When using custom PJL commands to control stapling or punching, MyQ recognizes the following values. These values are also used internally when release options are evaluated across print job policies, printer policies, and queue release policies.

Staple

Value	Description	PJL Command(s)
`0`	No stapling	—
`1`	Top left	`@PJL SET STAPLE=LEFTTOP`
`2`	Top right	`@PJL SET STAPLE=RIGHTTOP`
`3`	Two staples	`@PJL SET STAPLE=LEFT2PORT`
`100`	Unknown	`@PJL SET STAPLE=RIGHT2PORT` / `LEFTTOPSLANTPORT` / `RIGHTTOPSLANTPORT`

Punch

Value	Description	PJL Command(s)
`0`	No punching	—
`1`	Two holes (left)	`@PJL SET PUNCH=LEFTPORT` + `@PJL SET PUNCHHOLE=JP2`
`3`	Four holes (left)	`@PJL SET PUNCH=LEFTPORT` + `@PJL SET PUNCHHOLE=EU4`
`100`	Unknown	All other PUNCH/PUNCHHOLE combinations

PJL commands must be supported by the target printing device. Refer to your device manufacturer's documentation for a full list of supported PJL commands. Combinations that do not map to a named value are reported internally as 100 (unknown) and passed through to the device as-is.

Scripting (PHP)

You can use PHP scripts to further process the job after it is received by the MyQ server. Together with the PJL options and customizable queues, PHP scripting provides you with a large variety of job management options, such as the distribution of jobs between printing devices based on their size or color.

See also:

- Job Scripting (see page 556)
- Prologue, Epilogue (see page 554)

Prologue, Epilogue

Some printing devices brands support the Prescribe PDL (page description language), which can be used to set up special rules for additional modification of the printed output. For example, you can use Prescribe to add a custom header or footer to selected document pages or to the whole document.

In MyQ, these rules are part of the options available on the properties panels of print queues. For each queue, you can create custom rules by importing a text file with a set of Prescribe commands and selecting the part of the printed document the commands should be applied to.

Multiple rules can be defined for each queue.

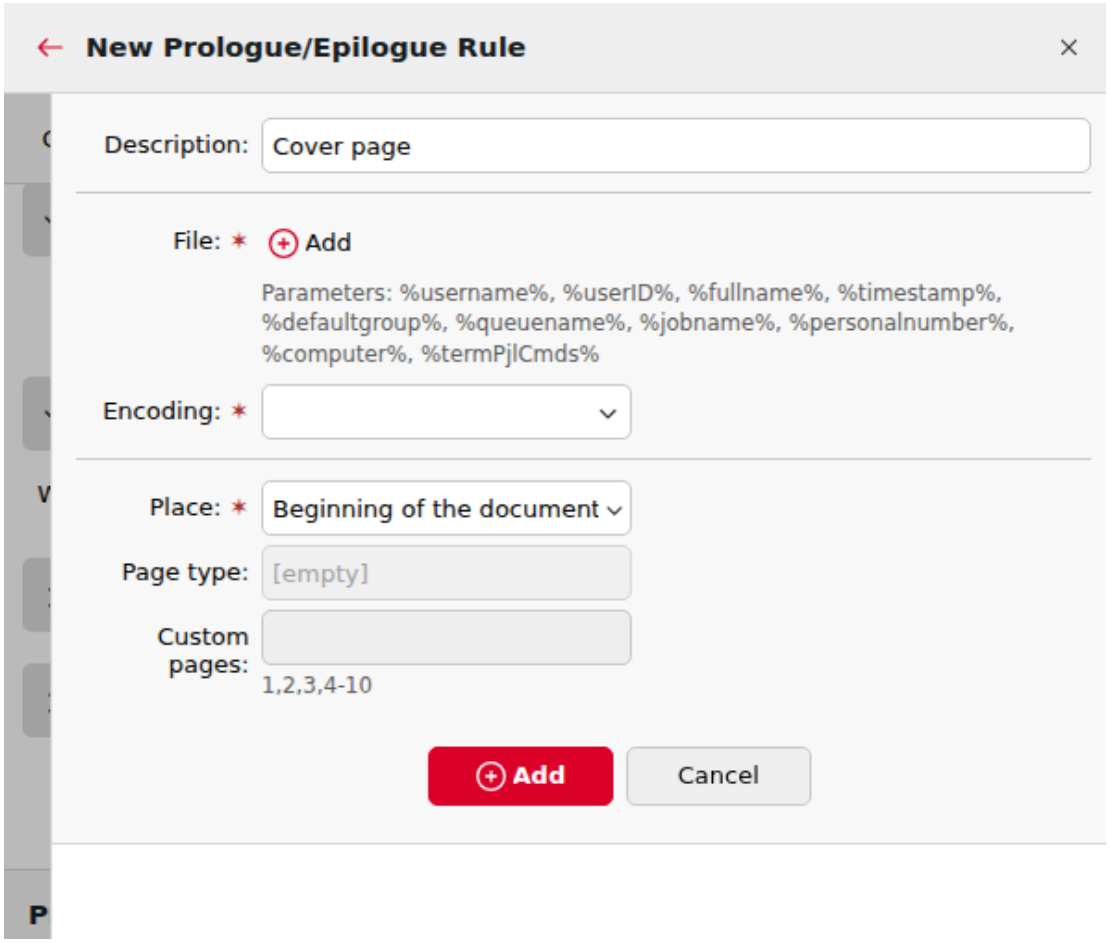
Prologue/epilogue functionality is only fully supported when using the PCL5 language. With other PDLs it is only possible to add a prologue placed at the beginning of the document.

Rules can be added and edited in the **Job processing** tab, on the **Prologue/Epilogue** section of a queue's properties panel.

Go to the **Queues** main tab (**MyQ > Queues**), right-click on the queue where you want to set up the rules, and click **Edit** (or select the queue, click **Actions** on the bar at the top of the tab, and then click **Edit**, or double-click on the queue).

Adding Rules to a Queue

1. Open the queue properties panel.
2. Click **Job Processing**. The Job Processing tab opens.
3. In the **Prologue/Epilogue** section, click **+Add**. A panel with the settings of the new rule opens.
4. Set up the rule, and then click **Add**. The new rule is added to the list of rules on the **Prologue/Epilogue** section.



Editing a Rule

To open the settings of a rule, double-click the rule on the **Prologue/Epilogue** section.
The available settings are:

- **Description:** Here you can type a description of the rule. You will see this description in the rules overview.
- **File:** Here you can upload the text file with the Prescribe code. The following substitution variables can be used: %username%, %userID%, %fullname%, %timestamp%, %defaultgroup%, %queuename%, %jobname%, %personalnumber%, %computer%, %termPjlCmds%.
- **Encoding:** Select the encoding that is used in the text file with the Prescribe code.
- **Place:** The object defined by the Prescribe code can be placed to the *beginning of the document*, *end of the document*, *beginning of selected pages, end of selected pages, beginning of the print file, end of the print file*.
- **Page type:** Select the pages the Prescribe code will apply to: *All pages, Odd pages, Even pages* or *Custom pages*.
- **Custom Pages**: Here you can further specify the pages the Prescribe code will apply to.

Deleting a Rule

1. Open the queue properties panel.
2. On the panel, click **Job processing**. The Job processing tab opens.
3. On the tab, in the **Prologue/epilogue** section, select the rule, click **Delete**, and then confirm the action in the confirmation dialog box. The rule is removed from the panel.

11.7.5 Job Scripting

PHP scripts can be used to further process a job after it is received by the MyQ server (job processor scripting) or to provide users with basic interaction options via MyQ Desktop Client (user interaction scripting). An overview of classes and functions used can be found in Job Scripting Reference.

See also:

- Job Scripting Reference (see page 567)
- User Interaction Scripting (see page 561)

- Job Processor Scripting (see page 557)

Job Processor Scripting

A Job Processor script is PHP code that runs in the context of a job being processed. The script runs after a job has been parsed and all user/queue policies have been applied. It runs before the job is made `ready` or `paused`.

⚠ To use job scripting, make sure that **Unlock Job Scripting** is enabled in your Easy Config Security settings.

The typical usage of the script is the modification of the job based on its properties. For example:

```
if ($this->pageCount > 10) {
  $this->duplex = "longEdge";
}
```

In this example, if the job has more than 10 pages then it is released as duplex. `$this` is the job being processed and is an instance of the `Job` class.

You can use basic PHP functions. For details about available classes and functions, see Job Scripting Reference.

Set up job processing with scripting

1. Open the queue where you want to use scripting and go to the **Job processing** tab.
2. Expand the **Scripting (PHP)** section.
3. Type your PHP script into the field **Actions after processing**.
4. Click **Save**.

ℹ **See also:**

- Easy Config Security (see page 150)
- Job Scripting Reference (see page 567)

PHP Scripts Actions Examples

In this section you can find examples covering a variety of job management options. These examples should give you an idea about how to use the PHP scripting in MyQ. You can also substitute the properties and methods in the examples to use them as building blocks of more complex scripts.

Actions based on the number of pages

Move jobs with a higher number of color pages to a monochrome queue.

```
if ($this->colorCount>20) {
 $this->moveToQueue("ForceMonochrome");
 }
```

Delete jobs with a large number of pages.

```
if ($this->pageCount>500) {
 $this->delete();
 }
```

Actions based on the size of the job

Move large jobs to a dedicated queue.

```
if ($this->dataSize>1000000) {
 $this->moveToQueue("LargeJobs");
 }
```

Delete oversized jobs.

```
if ($this->dataSize>5000000) {
 $this->delete();
 }
```

Actions based on paper format

Move jobs with the A3 paper format to a dedicated queue.

```
if ($this->paper==="a3") {
 $this->moveToQueue("LargePaperFormat");
 }
```

Actions based on the job owner

Move jobs of a certain owner to a dedicated queue.

```
if ($this->owner->name==="eliot.kate") {
 $this->moveToQueue("EliotKate");
 }
```

Change the owner of the job.

```
if ($this->owner->name==="eliot.kate") {
 $this->owner=MyQ()->getUserByUserName("simon.kate");
 }
```

Actions based on the duplex property

Move duplex jobs to a duplex queue.

```
if ($this->duplex) {
 $this->moveToQueue("Duplex");
 }
```

Move simplex jobs to a simplex queue.

```
if ($this->duplex===false) {
 $this->moveToQueue("Simplex");
 }
```

Actions based on the color property

Move color jobs to a color queue.

```
if ($this->color) {
 $this->moveToQueue("Color");
 }
```

Actions based on the job name or the source application

Move jobs printed in MS Word to a dedicated queue.

```
if (strpos($this->name,"Microsoft Word")!==false) {
 $this->moveToQueue("MSWord");
 }
```

Delete jobs sent from Facebook.

```
if (strpos($this->name,'Facebook')!==false) {
 $this->delete();
 }
```

Actions based on the rights to a queue

Move jobs of users who are not allowed to print to one queue to a different queue

```
if ($this->owner->canPrintToQueue("Color")===false) {
 $this->moveToQueue("Monochrome");
 }
```

Actions based on group membership

Move jobs sent by members of a group to a dedicated queue

```
if ($this->owner->hasGroup("Clerks")) {
 $this->moveToQueue("Clerks");
 }
```

Actions based on the PDL of the job

Move all jobs sent in a certain PDL to a dedicated queue

```
if ($this->lang===0) {
 $this->moveToQueue("UnknownPDL");
 }
```

Sending custom log messages to MyQ

Send a log info message to MyQ Log

```
MyQ()->logInfo("This message appears in the MyQ log.");
```

Complex actions

If the number of pages multiplied by the number of copies exceeds a certain number, delete the job and inform the user

```
// get the number of pages and the number of copies
$pages_number = $this->pageCount; $copies_number = $this->copies;
// if total (pagescopies) exceeds 500, delete the job and notify its owner
if ( $pages_number * $copies_number>500) {
 $this->delete(); $this->owner->sendNotification("error","Job refused",
"Cannot
 print jobs exceeding 500 pages.");
```

```
}
```

Move the job to a queue, if allowed

```
if ($this->color) {
  if ($this->owner->canPrintToQueue("JPS2")) {
     $this->moveToQueue("JPS2");
  } else {
     $this->owner->sendEmail("Job error", "Color printing denied");
     $this->delete();
  }
}
```

Move the job to the first available personal queue

```
// get all user's queues sorted by priority
$personalQueues = $this->owner->personalQueues;

// loop them
foreach ($personalQueues as $q) {
    // skip queue if no printer is available
    if ($q->isAnyPrinterAvailable() === false) {
        continue;
    }

    // queue printer is available, move job to queue
    $this->moveToQueue($q->name);
    // job is moved, stop the loop
    break;
}
```

User Interaction Scripting

A User Interaction Script allows to program an interaction with the job owner and modify the job based on the user's response. Specifically, it allows to display a series of UI dialogs with questions and action buttons (*YES/NO, PRINT/NO, YES/NO/CANCEL*). Depending on the user selection, further dialogs can be displayed and actions can be taken. Finally when the last dialog is processed, the script is finished and the job is set as `ready` and can be released.

If a User Interaction Script is present, it must be first successfully executed before the job can be released. The job is forced in the `pause` state until then.

Basic PHP functions can be used, and almost all of those described in Job Scripting Reference. The only two methods not supported by the feature are `$this->job->setPrinted()` and `$this->job->pause()`. Apart from the common classes, methods, and properties, you can use several additional functions to communicate with the MyQ Desktop Client application.

How to Write a User Interaction Script

On the MyQ Desktop Client tab of a queue, in the **User Interaction** section, add the script in the field, and click **Save**.

First, you need to define the `main()`. function. This function decides if the dialog box should be opened (under which conditions) and which dialog box should be shown.

Then you can define on-click functions with reactions to the selected option: `onYes(), onNo(), onPrint(), onCancel()`.

Public properties are kept between calls. In fact, they are sent to the client and back.

Script Structure

See the following script:

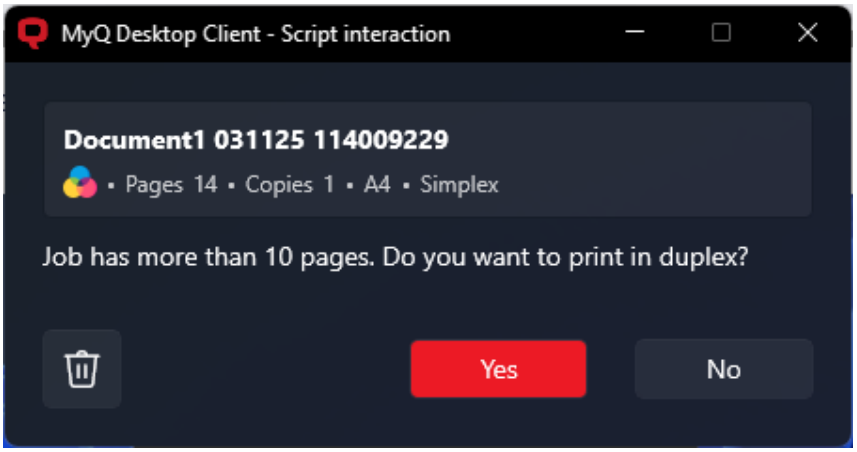
```
public $hasMoreThan10pages;

// script entry point
function main() {
    /** Job object */
    $job = $this->job;
    $this->hasMoreThan10pages = $job->pageCount > 10;
    // Show dialog if the job has more than 10 pages
    if ($this->hasMoreThan10pages === true) {
        $this->dialogYesNo("Job has more than 10 pages. Do you want to
print in duplex?");
    }
}

// If yes clicked
function onYes() {
    // $this->hasMoreThan10pages is available also here
    $this->job->duplex = 'longEdge';
}

// If no clicked
function onNo() {
    // nothing. Job will be released.
}
```

Using the above script, this dialog is displayed in MDC:



If you are familiar with the PHP language, the script is actually a body of the `class UserScript {...}` statement.

You can define properties like `$hasMoreThan10pages`. Properties are persistent among multiple script invocations for the same job. Use them to store a state between multiple dialogs.

There is the `main` function. It's called once when the script starts. Use it to display the first dialog.

Then there are the `onXXX` functions. They are the action handler called when an `XXX` button is pressed. For example, the `Yes` button is handled via the `onYes` function.

If you display no dialog, the script is finished.

API Reference

See Job Scripting Reference on how to modify the job and also for many other operations you can perform.

The User interaction script runs in the context of the User class. The sent job can be accessed as `$this->job`.

Objects from all classes, except for the Session class, can be accessed via the job object, for example the `owner $this->job->owner`. Objects from the Session class can be accessed via the `MyQ()` global feature; for example: `MyQ()->logInfo("This message appears in the MyQ log.");`.

UserScript Class

User Interaction Script is the body of the `UserScript` class as described above. MyQ also provides several built-in methods of the User class in addition to your own methods.

Dialog Creation Methods

Function	Description
void **dialogYesNo**(string $text)	Creates a dialog with the `$text` as the content and Yes, No buttons.
void **dialogPrintNo**(string $text)	Creates a dialog with the `$text` as the content and Print, No buttons.
void **dialogYesNoCancel**(string $text)	Creates a dialog with the `$text` as the content and Yes, No, and Cancel buttons.
void **dialog**(string $text, Field[] $fields)	Creates a dialog with the `$text` as the content and an array of custom fields. A field can be a button or any other field type, like a list, for example. Buttons are always displayed below other fields.
FieldButton **button**(string $title, string $id)	Creates a custom button which can be used in the `dialog()` function. `$title` is a text displayed on the button. The button `$id` is used when executing the button handler. MyQ searches for an `onXXX` handler where `XXX` is the `$id`.
FieldList **singleSelectList**(string $name, array $items)	Creates a list of options from which the user can choose only one (radio group). It can be used in the `dialog()` function. The `$items` is an associative array where the key is an item's reference and the value is an item's display name visible in the UI.

Function	Description
FieldMultiSelectList **multiSelectList**(string $name, array $items)	Creates a list of options from which the user can choose multiple ones (check boxes). It can be used in the `dialog()` function. The `$items` is an associative array where the key is an item's reference and the value is an item's display name visible in the UI.

onCancel Method

`onCancel` handles the Cancel button and is provided by default. It calls `terminate()`. You can provide your own implementation to change the behavior.

Other Methods

Function	Description
void **terminate**()	Terminates the script processing. The script has not been executed successfully and the job stays in the `pause` state. The user must execute the script again.
mixed **getField**(string $name)	Gets the value of the field with the `$name` after the user has interacted with the dialog. The field must have been created by the methods `singleSelectList` (the result is a scalar value) or `multiSelectList` (the result is an array of values, which can be an empty array).

See also:

- Job Scripting Reference (see page 567)
- User Class (see page 570)
- Session Class (see page 572)

User Interaction Script Examples

Print a Color Job in B&W

```
// script entry point
```

```
function main(){
// If the job is color, show a Yes/No dialog to ask if they want to print
the job in B&W.
 if ($this->job->color){
  $this->dialogYesNo("Jobs sent to this queue are printed in B&W,
  do you still want to send the job here?"); }
}

// If Yes clicked, the user is informed that the job was sent to the B&W
queue via a MDC
notification.
function onYes(){
 $this->job->owner->sendNotification("info","Job successfully sent","Your
job was sent
 to the B&W queue.");
}

// If No clicked, the job is deleted and the user is informed about it via
a MDC
notification.
function onNo(){
 $this->job->delete(); $this->job->owner->sendNotification("info","Job
deleted","Your
 job was deleted.");
}
```

Move a Job to a Personal Queue

```
// script entry point
function main() {
    /** Job object */
    $job = $this->job;

    // Get the personal queues and create a list
    $queues = $job->owner->getPersonalQueues();
    $queueList = [];
    foreach ($queues as $queue) {
        $queueList[$queue->name] = $queue->name;
    }

    $list = $this->singleSelectList('Personal queues', $queueList);

    $this->dialog('Select a queue', [
        $list,
        $this->buttonPrint(),
        $this->buttonCancel()
    ]);
}

// If print clicked
function onPrint($inputs) {
    $queue = $this->getField('Personal queues');
    $this->job->moveToQueue($queue);
```

```
}

// If cancel clicked
function onCancel() {
    // nothing. Job will be released.
}
```

Job Scripting Reference

This is a reference of classes and functions you can use in job processor scripting and user interaction scripting. Scripts can use the following classes:

- `Job`
- `User`
- `Queue`
- `QuotaInfo`
- `Session`

The object of the `Job` class represents the job sent to MyQ, the object of the `User` class represents the job's owner, and the object of the `QuotaInfo` class represents quotas of the job's owner. The `Queue` class can be used to move the job to one of the personal queues of the job's owner and methods of the `Session` class may be used for additional specific tasks, such as sending a log message to MyQ.

See also:

- Job Processor Scripting (see page 557)
- User Interaction Scripting (see page 561)
- Job Class (see page 567)
- User Class (see page 570)
- Queue Class (see page 571)
- Session Class (see page 572)
- QuotaInfo Class (see page 572)

Job Class

The **Job** class has the following methods and properties:

Methods

- `pause()` : Pause the job.
- `copyToQueue(string $queueName)` : Copy the job to queue `$queueName` . The new job is processed normally according to the rules in the target queue.

- `moveToQueue(string $queueName)` : Move the job to queue `$queueName` . The new job is processed normally according to the rules in the target queue.
- `setReleased()` : Set the job as released (printed) without actually releasing it. (`setPrinted` is still supported for BC).
- `delete()` : Delete the job.
- `setProject(string $projectCode)` : Assign the job to the given project by project code.
- `setAccount(string $accountReference)` : Assign payment account to the job.

Properties

Job Properties show how the job looks after applying user/quota policies. This is how the job will be released. The `null` value means that the job parser was not able to get the property from the job file.

By setting a property, you can modify how the job will be released. This overrides any user/quota policy. If you set a property to `null`, the job will be released as originally received.

Setting `monoCount` , `colorCount` or `paper` doesn't actually modify the job. The new values are used only for credit/quota calculations.

Name	Type	Writable	Description
`name`	string	yes	Name of the job
`dataSize`	int	yes	Data size of the job in bytes
`queue`	Queue	-	Job's queue
`monoCount`	int	yes	Count of the monochrome pages of the job
`colorCount`	int	yes	Count of the color pages of the job
`pageCount`	int	-	Total sum of the pages of the job

Name	Type	Writable	Description

`paper`	string	yes	Format of the paper with the following strings as its values:
			`a4`
			`a3`
			`other`
			`a5`
			`b4`
			`b5`
			`folio`
			`ledger`
			`legal`
			`letter`
			`statement`
			This variable is employed by the 'set' method in MyQ. Use it in commands of the PHP script.

`duplex`	string	yes	Job is in duplex. Possible values:
			`simplex`
			`longEdge`
			`shortEdge`
			Note: Changing this property only updates the metadata of the job. The job is not converted to simplex/duplex.

`color`	Boolean	-	Job is in color. Note: Changing this property only updates the metadata of the job. The job is not converted to B&W/color.
`owner`	User[ ]	yes	Owner of the job Note: The user policies are not updated; Projects are not updated.

Name	Type	Writable	Description
`copies`	int	yes	Number of copies of the job Note: Changing this property only updates the metadata of the job. The number of copies to be released is not changed.
`tonerSaving`	Boolean	yes	Toner Saving mode enabled
`filename`	string	yes	A path including the filename of the job. The path is relative to the job folder. Note: The path must exist, otherwise the job is not parsed and is declared as "deleted".
`lang`	int	-	The PDL of the job with the following integers as its values: UNKNOWN = 0, PDL_PCL = 1, PDL_PS = 2, PDL_ESCP = 3, PDL_PRESCRIBE = 4, PDL_PCLXL = 5, PDL_PDF = 6, PDL_JPEG = 7
`stapling`	string	yes	Staples the document. The following values are available: `no`, `topLeft`, `topRight`, `twoStaples`, `unknown`. The legacy value `yes` is still accepted for backward compatibility.
`punching`	string	yes	Punches the document. The following values are available: `no`, `twoHoles`, `fourHoles`, `unknown`. The legacy value `yes` is still accepted for backward compatibility.

User Class

The **User** class has the following methods and properties:

Methods

- `sendEmail(string $subject, string $body)` : Send an email to the user.
- `bool canPrintToQueue(string $queueName)` : The user has the rights to send jobs to the queue.
- `bool hasGroup(string $name)` : The user is a member of the group.
- `sendNotification(string $type, string $title, string $body)` : Send a notification to the user via MyQ Desktop Client:
  - type: info, warning, error
  - title: notification title
  - body: notification text (plain text format)
- `QuotaInfo getQuotaInfo()` : Get information about user's quotas.

Properties

Name	Type	Writable	Description
`name`	string	-	Login name of the user
`email`	string	-	Email of the user
`fullname`	string	-	Name and surname of the user
`delegates`	User[ ]	-	Array of the user's delegates
`notes`	string	-	Notes
`personalQueues`	Queue[ ]	-	Array of personal queues ordered by priority

Queue Class

The **Queue** class has the following methods and properties:

Methods

- `bool isAnyPrinterAvailable()` : There is at least one printing device available to the queue.

Properties

Name	Type	Writable	Description
`name`	string	-	Name of the queue

Session Class

The session object is accessible via the MyQ() global function. The **Session** class has the following methods:

Methods

- `User getUserByUserName(string $userName)` : Find a MyQ user by their user name. If no user is found, `null` is returned.
- `logError(string $message)` : Create an error message in the MyQ log.
- `logWarning(string $message)` : Create a warning message in the MyQ log.
- `logInfo(string $message)` : Create an info message in the MyQ log.
- `logNotice(string $message)` : Create a notice message in the MyQ log.
- `logDebug(string $message)` : Create a debug message in the MyQ log.
- `string getJobsPath()` : Get the path to the folder on the MyQ server where the print job is stored. Ends with a backslash.

QuotaInfo Class

The **QuotaInfo** class contains information about the user's current state of quotas. It has the following methods:

- `bool canColor()` : Check if the user can print or copy in color.
- `bool canPrint()` : Check if the user can print.
- `bool canCopy()` : Check if the user can copy.
- `bool canScan()` : Check if the user can scan.

11.7.6 Configure DNS-SD for AirPrint and Mopria Discovery

DNS Service Discovery (DNS-SD) allows users to discover MyQ queues as network printers without manually configuring a queue URL. You can use DNS-SD to publish queues to **AirPrint** clients on iOS, iPadOS, and macOS and to Android devices using **Mopria Print Service**.

For most environments, **MyQ Mobile Print Agent** provides the simpler method for publishing MyQ queues. Use manual DNS-SD when you want to provide printer discovery through your DNS infrastructure instead.

This procedure uses **Windows Server DNS Manager**. DNS-SD uses standard PTR, SRV, and TXT records, so you can create equivalent records using another DNS platform.

Prerequisites

- You have permission to create records in the DNS zone used by your client devices.
- **Jobs via IPPS** is enabled in **MyQ > Settings > Jobs**.
- You know the IPPS port used by the Print Server.
- **Jobs via Mobile Devices** is enabled for every queue that you want to publish.
- The queue names that you publish do not contain spaces.

You can view the IPPS address and port on the queue's **Job Receiving** tab.

Prepare the DNS Search Domain

1. On the Windows server, open **Server Manager > Tools > DNS**.
2. In **DNS Manager**, expand the domain where you want to advertise the MyQ queues, for example `acmedom.org`.
3. Under the domain, right-click **_udp** and select **New Domain**.
4. Enter `_dns-sd` as the domain name.
5. Right-click **_dns-sd** and select **Other New Records > Pointer (PTR)**.
6. Create the following PTR records, replacing `acmedom.org` with your domain:

Record	Host name
`b`	`acmedom.org`
`lb`	`acmedom.org`

The `b` record provides standard browsing and the `lb` record provides legacy browsing.

Add Printer Service Records

Repeat this section for every MyQ queue that you want to publish.

Create the `_ipps` Domain

1. Under your DNS domain, right-click **_tcp** and select **New Domain**.
2. Enter `_ipps` as the domain name.

You only need to create the `_ipps` domain once.

Create the PTR Record

1. Right-click **_ipps** and select **Other New Records > Pointer (PTR)**.

2. Leave **Host IP Address** empty.
3. In **Host name**, enter:

   `DefaultPullPrint._ipps._tcp.acmedom.org`

   Replace `DefaultPullPrint` with the MyQ queue name and `acmedom.org` with your domain.
4. Click **OK**.

Create the SRV Record

1. Right-click **_ipps** and select **Other New Records > Service Location (SRV)**.
2. Configure the record:

Field	Value
Service	MyQ queue name, for example `DefaultPullPrint`
Protocol	`_ipps`
Port number	IPPS port used by the Print Server
Host offering this service	Print Server hostname, for example `print.acmedom.org`

3. Click **OK**.

Use the IPPS port shown in MyQ rather than assuming a particular port value.

Create the TXT Record

1. Right-click **_ipps** and select **Other New Records > Text (TXT)**.
2. Set **Record name** to the MyQ queue name, for example `DefaultPullPrint`.
3. Enter the DNS-SD attributes for the queue. For example:

```
txtvers=1
qtotal=1
rp=ipp-airPrint/DefaultPullPrint
ty=MyQ Default
adminurl=https://print.acmedom.org
note=Default Pull Print Queue
priority=0
product=(MyQ)
printer-state=3
printer-type=0xC0B0DE
Transparent=T
```

```
Binary=T
Fax=F
Color=T
Duplex=T
Copies=T
Collate=T
Punch=F
Staple=F
Bind=F
Sort=F
Scan=F
PaperMax=legal-A4
pdl=application/octet-stream,application/pdf,application/postscript,image/
jpeg,image/png,image/urf
air=username,password
TLS=1.2
kind=document,photo
URF=W8,SRGB24,CP255,RS600,DM1
```

Adjust the queue name, server address, description, and advertised capabilities for your environment.

4. Click **OK**.

Choose the Queue Endpoint

The `rp` value in the TXT record determines the queue endpoint and authentication behavior.

For authenticated AirPrint printing on iOS, iPadOS, and macOS, use:

`ipp-airPrint/{queue-name}`

For example:

`ipp-airPrint/DefaultPullPrint`

The user is prompted for MyQ credentials when connecting for the first time. **Jobs via Mobile Devices** must be enabled for the queue.

For macOS clients, you can alternatively publish the standard IPPS endpoint:

`queue/{queue-name}`

This uses the signed-in system user instead of IPP authentication and is supported for macOS clients.

Add Universal Discovery Records

1. Right-click **_ipps** and select **New Domain**.
2. Name the domain `_sub`.

3. Right-click **_sub** and select **New Domain**.
4. Name the domain `_universal`.
5. Right-click **_universal** and select **Other New Records > Pointer (PTR)**.
6. Leave **Host IP Address** empty.
7. Set **Host name** to the service record for the queue, for example:

   `DefaultPullPrint._ipps._tcp.acmedom.org`
8. Click **OK**.

Repeat the PTR record for each queue that you publish.

Verify DNS-SD Discovery

After configuration, your DNS hierarchy should contain:

- `_udp > _dns-sd` with the `b` and `lb` PTR records;
- `_tcp > _ipps` with PTR, SRV, and TXT records for each published queue;
- `_tcp > _ipps > _sub > _universal` with PTR records for the published queues.

On macOS:

1. Open **System Settings > Printers & Scanners**.
2. Click **Add Printer, Scanner or Fax**.
3. Confirm that the published MyQ queue appears as an available printer.

See also:

- Job Receiving Tab (see page 545)
- Jobs via IPPS (see page 595)
- Queues (see page 532)
- (1.3) Mobile Print Agent
- (v2) Selecting Printing Methods

11.8 User Detection Methods

One of the essential MyQ functions is to identify the owner of a sent print job. You can select from a number of identification options. The most common way is to identify the user as the OS account where the job was sent from (Job sender). If there are many users who send their jobs from one account, you can use one of the

three authentication options: *prompt for a PIN/card, prompt for a username and password or prompt the user to select from a list*.

Apart from the above-mentioned options, MyQ offers several advanced identification options that can be used in special cases, such as if you want to use a DNS server to identify the user's computer or detect the user from the job name.

The available user detection methods are described in the sections below.

11.8.1 Job Sender

The basic and most common user detection method option is to identify the owner as the OS user account where the job was sent from.

If the user logs on the account **Eliot.Kate** and sends the job from there, MyQ identifies them as **Eliot.Kate**.

11.8.2 Sender’s Computer Name

With the **Sender's computer name** option selected, the job owner is identified as the name of the computer where the job is sent from. This way, it does not matter on which OS account the sending user is logged in, and all jobs are accounted on the computer.

By default, the **Computer detection method** is set to *Default* mode. This is the standard setting that works in almost all cases. For information about alternative options, please contact your MyQ support.

A regular expression can be used to capture a part of the detected string.

11.8.3 Using a DNS Server to Resolve the Job Owner

With the two user detection method options: **Print server's DNS name** and **Sender's computer DNS name**, a DNS server is used to resolve the job owner as one of the two respective values:

1. **Print server's DNS name** : The computer or server where the print driver is installed. If the DNS server succeeds in resolving the server IP address, the job owner is identified with the server name; otherwise, the job owner is identified with the IP address.
2. **Sender's computer DNS name**: The computer where the job is sent from. If the DNS server succeeds in resolving the computer IP address, the job owner is identified with the computer name; otherwise, the job owner is identified with the IP address.

The actual value depends on the location where the print driver is installed.

For example: If the print driver is installed on the print server Server 1 and shared with the computer *laptop100* where the user prints from, the values are different:

- When you select the **Print server's DNS name** method, the job owner is identified with the server, e.g. Server1.domain.com,
- When you select the **Sender's computer DNS name** method, the job owner is identified with the computer, e.g. laptop100.domain.com.

If the computer does not use shared drivers but sends the jobs via its own drivers, both values are the same.

A regular expression can be used to capture a part of the detected string.

11.8.4 Detect User from the Job Name

With the **Detect user from the job name** option, the job owner is identified with the name of the print job. This method can be used in cases where jobs are automatically generated and sent to print by external systems, such as ERP systems. These jobs can have a specific form where the user name is part of the job name, for example *user16@documentxy.com*.

The **Only for LPR user** setting is displayed after you select the **Detect user from the job name** option. This setting allows you to combine the **Detect user from the job name** method with the **Jobs sender** identification method. The job owner is first detected as the job sender and only if the username matches the name entered in the **Only for LPR user** text box, the job owner is identified with the job name.

This advanced user identification method may be required, for example, for some prints from the SAP system. Prints from SAP are usually not sent directly to printing devices, but first to the Windows spooler (SAP LPD or SAP Print) which processes and forwards the prints to the device. This service usually runs under the system account (*SYSTEM*), and therefore the job sender detected from each such job is *SYSTEM*. In such cases, you can enter the user *SYSTEM* in the **Only for LPR user** text box. MyQ detects the sender and if it is *SYSTEM*, it identifies the job owner as the job name.

11.8.5 User Detection from PJL

With the **User detection from PJL** identification option, MyQ detects the job owner from one of the command lines of the print job's PJL header.

To select the line that is used for the definition of the job owner, click **+Add** and enter the variable (*SET USERNAME*) in the **PJL Variable** field. You can enter multiple

variable/regex sets by clicking **+Add** for each one in a new line. MyQ tries to find a PJL line containing the first defined variable, and then eventually repeats the search for the next variable, until it either finds a non-empty value with the definition of the job owner or there are no more variables to search for.

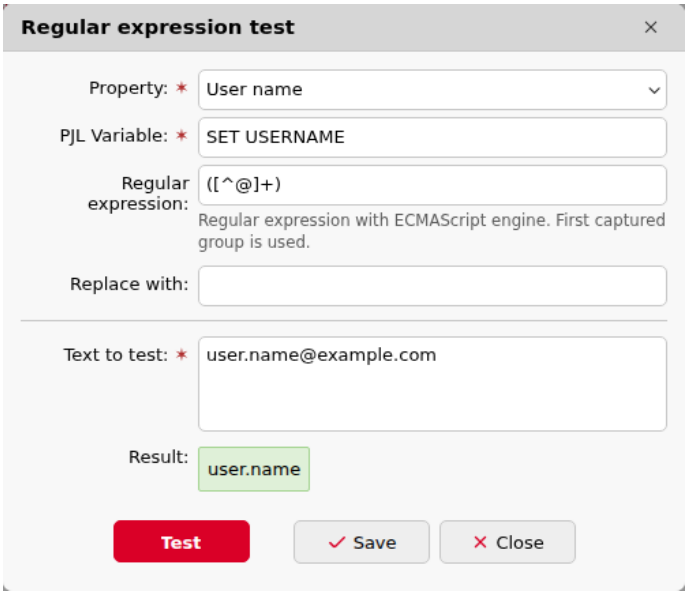
A regular expression can be used to capture a part of the detected string. If no regular expression is specified, the whole string of the PJL variable is used.

Click **Edit** to modify any existing variables, **Test** to actually test if your regular expressions work, and **X** to delete a variable/regex set.

In the below example, you can see how a variable/regex set works, and if it manages to find the user by searching for the username in the email address from the PJL header:

- In the **Text to test** field, there should be the text from the print job's PJL header:
  user.name@domain.tld
- In the **PJL Variable** field, there should be the *SET USERNAME* variable, or any other variable used to detect the job owner.
- In the **Regular expression** field, there should be the regular expression you want to use in order to detect the user name. In the example, the *([^@]+)* regex checks if a character is not "@" and uses it, and "*+*" means to proceed with the next character. The result is that it takes all characters before it reaches "@".

After clicking **Test**, the test result is displayed at the bottom. In this example, *user.name* was successfully detected.



11.9 Binary Find & Replace

Binary Find & Replace lets administrators fix or patch print job streams before they are parsed by MyQ. It works by applying a sequence of hexadecimal find-and-replace rules to each job at the byte level, targeting specific PDL commands (PCL, PJL, PostScript) as they enter a queue. Rules are defined per queue, run in a single streaming pass, and take effect immediately on save — no service restart required.

> **Warning!**
> This feature manipulates raw byte streams. A misconfigured rule can corrupt a print job or make it unprintable. Test in a non-production queue first. You should be comfortable working with hex data and the relevant PDL (PCL, PJL, PostScript).

11.9.1 Enabling Binary Find & Replace

The feature is disabled by default. To enable it, follow these steps.

1. Modify `config.ini` in the application data director (default: `C:\ProgramData\MyQ`) to include these lines:

```
[JobProcessor]
binaryFindReplaceEnabled=true
```

2. Restart all MyQ services with Easy Config.

This enables Binary Find & Replace and creates the directory `BinFindReplace` in the application data directory, if it does not exist.

To disable the feature, set `binaryFindReplaceEnabled=false` and restart all MyQ services.

11.9.2 Using the Replacement Rules File

Create `Config.json` in the `BinFindReplace` folder inside the data directory (e.g., `C:\ProgramData\MyQ\BinFindReplace\Config.json`). Changes to the file take effect immediately, and no service restart is required. If the file is invalid, an error is logged and the entire file is skipped.

Example:

```
{
  "queues": {
    "Default": ["FixTraySelection", "InjectWatermarkHeader"],
    "Web": ["GlobalBanner"]
  },
  "filters": {
    "FixTraySelection": {
      "find": "1B266C3148",
      "replace": "1B266C3248"
    },
    "InjectWatermarkHeader": {
      "find": "40504A4C20454E544552",
      "replace":
"40504A4C2053455420555345523D2241646D696E220D0A40504A4C20454E544552"
    },
    "GlobalBanner": {
      "find": "1B452A",
      "replace": ""
    }
  }
}
```

Filters are defined in the `Config.json` file, with a unique name and a pair of find–replace strings. To delete the matched bytes, use an empty string as the replace value (as for `GlobalBanner` in the example).

Filters in each queue array are applied in sequence, each operating on the output of the previous one, in a single pass over the print file. Additional filters can be added with no performance cost. The result is streamed directly to output without buffering the full job. A filter ID can appear multiple times in a queue array, in any combination with other filters.

Field Reference

Field	Type	Description
`queues`	Object	Maps queue names (case-sensitive) to an ordered array of filter IDs. Queues not listed are unaffected.
`filters`	Object	Named filter definitions; where each key is a filter ID and each value is a find/replace pair.
`find`	String	Hex bytes to find. Must be non-empty and even-length, and is case-insensitive.

Field	Type	Description
`replace`	String	Hex bytes to substitute. An empty string deletes the matched bytes. Must be even-length, and is case-insensitive.

Note the following requirements:

- Hex characters only: `0-9`, `a-f`, `A-F`, case-insensitive
- The strings `find` and `replace` must contain a whole number of bytes (2 hex characters per byte)
- The `find` string cannot be empty.
- The values for `find` and `replace` must be different.
- Every filter ID in `queues` must be defined in `filters`.
- Maximum size for each `find` and `replace` value is 256 KB.
- The output of any single filter cannot expand to more than 64× the size of its input.

11.9.3 Logging

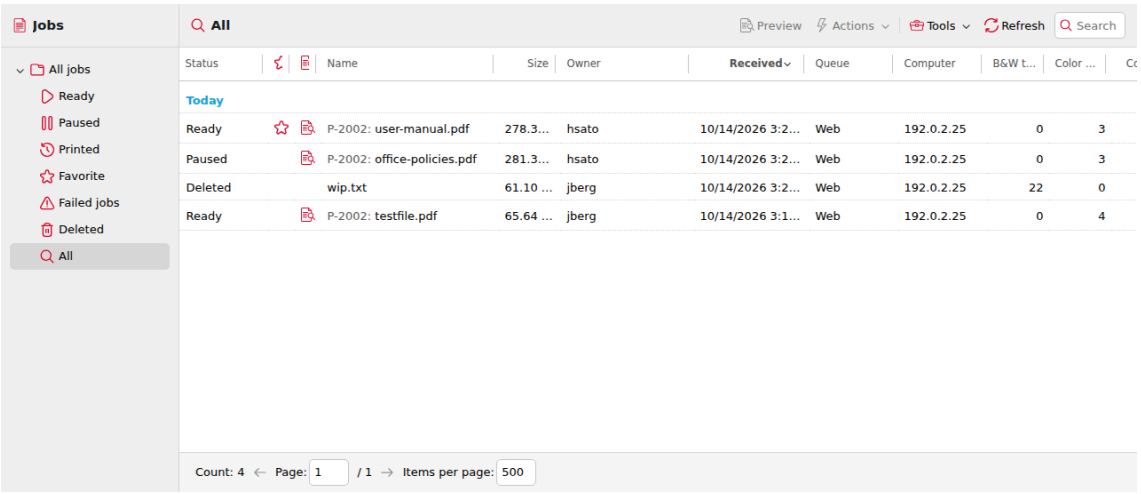
Events related to this feature appear in **MyQ > Log**, identified with the text *Binary Find & Replace*.

12 Jobs

MyQ receives, processes, stores, and tracks print jobs submitted by users. Use the job management features to:

- Configure global job-processing settings.
- Monitor jobs and their current status.
- Edit, pause, resume, delete, or mark jobs as favorites.
- Configure job parsing, preview, privacy, archiving, and retention.
- Process jobs using PJL commands or PHP scripts.
- Notify users and administrators when jobs are refused.

12.1 Working with the Jobs List



Open **Jobs** to view and manage print jobs submitted to the MyQ server.

Use the left menu to filter the displayed jobs by **Ready**, **Paused**, **Printed**, **Favorite**, **Failed**, or **Deleted.** Select **All** to remove the status filter.

Favorite is not a job status. It filters for jobs marked as favorites, regardless of their processing status.

Select a job to view its details or perform available actions.

12.2 Job Statuses

Jobs in the list may appear with the following statuses:

Status	Meaning
Processing	MyQ is examining the job and preparing it for printing.
Ready	The job is waiting to be printed.
Paused	The job was paused manually or automatically by MyQ.
Printing	The job is being sent to the printing device.
Printed	The job was sent to the printer. On supported printers with an Embedded Terminal 8.1 or later, MyQ can update the status according to the actual printing result.
Failed	The job could not be processed or printed.
Deleted	The job was deleted from the MyQ server.

12.2.1 Favorite Jobs

You can mark any job that has not been deleted as a **Favorite**. Favorite jobs are retained for reuse unless automatic deletion of favorite jobs is enabled in the system management settings.

Favorite jobs originating from an external code book may also be removed if they are no longer available from the code book's data source.

See also:

- Jobs Settings (see page 584)
- Editing & Deleting Jobs (see page 587)
- User Detection Methods (see page 576)
- Job Scripting (see page 556)
- Log Settings (see page 253)

12.3 Jobs Settings

On the **Jobs** settings tab, you can set the global properties of jobs in the MyQ print environment.

12.3.1 General

Here you can set the **Maximum job size** (default size is *600MB*).

In the **Office file formats** subsection, select the method MyQ uses to process and print MS Office and LibreOffice attachments.

See also: Set Up Office Document Processing (see page 588)

12.3.2 Notifications on Job Receiving Errors

Check the **Notify the administrator via email** and/or the **Notify the job sender via email** boxes, to send notification emails about refused jobs.

The job sender is always notified via MyQ Desktop Client, if installed.

12.3.3 Job Parser

Here you can set the **job parsing mode**, which dictates which level of job details will be reported. You need to activate the Job Parser if you want to know job details (page count, color, paper size, etc.) before the job is printed. It is necessary for features like credit, quota and PHP scripting. There are three levels of job parsing available:

- **Basic (lower CPU usage)** - This method doesn't estimate number of mono and color pages.
- **Standard (default option)** - This method will estimate the number of monochrome and color pages. This method is optimal for most office documents.
- **Enhanced (higher CPU usage)** - Every page of the document will be rendered and estimated as monochrome or color based on the rendered data. This method is recommended when printing complex PostScript or PDF documents and facing inaccuracy in Standard job parsing method.

See also: Job Parser (see page 590)

12.3.4 Jobs via LPR Protocol

Here you can enable the **Jobs via LPR protocol** feature (*enabled* by default). If it is deactivated, MyQ cannot receive print jobs via LPR.

The server knows the job sender (to be able to notify MyQ Desktop Client about job processing) through the hostname sent by the LPR protocol. The maximum length of the hostname is 31 characters.

The maximum job size received over LPR is *100GB*. Jobs with a size of over *2GB* are described as: "*More than 2GB*"; for jobs below *2GB*, the real size is displayed.

It is recommended to keep the **Jobs via LPR protocol** option enabled. If it is disabled, jobs sent from print drivers cannot be received by MyQ.

You can also change the **port** here, although it is recommended to use the default setting (*515*).

See also: Jobs via LPR Protocol (see page 592)

12.3.5 Jobs via IPPS

Here you can enable printing jobs via the IPPS protocol. You can also change the **port** here (default is *443*), and enable the **Require authentication** option to enforce authenticated-only IPP printing.

See also: Jobs via IPPS (see page 595)

12.3.6 Jobs via Email

Here you can enable or disable the Jobs via Email feature and configure the mailbox MyQ polls for incoming print jobs. Supported attachment formats are PDF/A, TXT, and JPEG. For MS Office formats, MS Office or LibreOffice must be installed on the MyQ server. The maximum message size, including all attachments, is 500 MB.

See also: Jobs via Email (see page 601)

12.3.7 Jobs via Web

Here you can enable or disable the Jobs via Web feature, which allows users to upload and submit print jobs directly from the MyQ web interface. You can also configure the allowed users and set the maximum upload file size (20–120 MB; default 120 MB).

See also: Jobs via Web (see page 604)

12.3.8 Job Preview

Here you can enable/disable and set up **Job Preview** and set the **Number of pages** (to include all pages in the preview set the value to 0).

See also: Job Preview (see page 606)

12.3.9 Job Archiving

This feature is visible if your activated license includes Job Archiving.

You can automatically archive all print jobs that are sent to MyQ. On selected brands of printing devices, you can also archive all copy and scan jobs.

See also: Job Archiving (see page 606)

12.3.10 Job Privacy

Here you can enable the **Job Privacy** feature, which limits access to sensitive job metadata for everyone except the job owner and their delegates.

> ⚠ Once enabled, the **Job Privacy** feature cannot be disabled.

In addition, you can enable or disable the option to **Hide job names on the device**. Enabling this option means the names of jobs released to devices are redacted so that they are not visible in the device's job history.

See also: Job Privacy (see page 608)

12.3.11 Watermark Collections

Here you can set up watermark collections.

See also: Watermark Collections (see page 608)

12.4 Editing & Deleting Jobs

To open a print job properties panel, double-click the job on the list on the **Jobs** main tab (or select the job, then click **Actions** on the toolbar above, and then click **Edit** in the job action dialog box). The panel opens on the right side of screen.

On the panel, you can see general information about the print job, such as its name and ID, size, its author and the IP address of the author's computer. If you use the **Job Parser** tool, you can see additional data such as the B&W total, color copies, number of copies, paper format, duplex, toner saving, staple, punch, the printer language used, and the price of the job.

You can also change the print job's **Owner** and **Project** in their respective list boxes.

Only an administrator and user group leaders can change the owner of a print job. The administrator can move jobs between all users and the user group leader can move jobs between members of their subordinate group.

If you change the job owner, the new owner has to have rights to the current queue and project. If you change the project, the current job owner has to have rights to the new project.

12.4.1 Deleting Jobs

To delete selected jobs:

1. On the jobs list on the **Jobs** main tab, select the jobs that you want to delete, and then click **Actions**.
2. In the Actions drop-down box, click **Delete**. You can find the deleted jobs on the **Deleted** jobs list.

See also:
- Job Parser (see page 590)

12.5 Set Up Office Document Processing

MyQ can process and print MS Office and LibreOffice attachments received via Jobs via Email, Jobs via Web, and Easy Print. This page covers the prerequisites, processing method options, and the local admin account configuration required for the Convert to PDF method.

12.5.1 Prerequisites

- Microsoft Office (64-bit, minimum version 2016, with latest service pack) or LibreOffice (minimum version 6, 64-bit) is installed on the MyQ server. If both are installed, MS Office handles MS Office formats and LibreOffice handles LibreOffice formats.

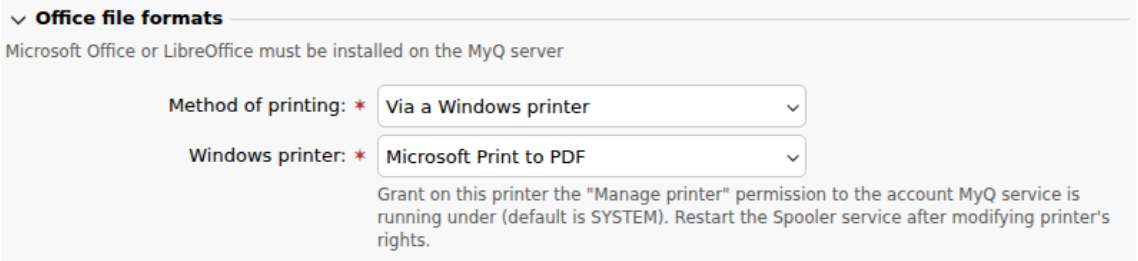
After installation, restart MyQ services for the server to begin recognizing these formats.

12.5.2 Select a Processing Method

Go to **MyQ > Settings > Jobs > General > Office file formats** and select one of the following:

- **Convert to PDF** (default): MyQ opens the document in the Office application, converts it to PDF, and sends it directly to the printing device. The device must support direct PDF printing.

- **Via a Windows printer:** MyQ opens the document in the Office application and prints it using a selected Windows print driver. Select the driver from the drop-down. You must also update the printer's security settings to allow the MyQ services account to print: in **Devices and Printers**, right-click the printer, open **Properties > Security**, and grant **Print** and **Manage printers** permissions to the account running MyQ services.



12.5.3 Enable Office Document Processing

1. Install the corresponding Office package or packages on the MyQ server.
2. Open each application that will be used for conversion (*Word, Excel, PowerPoint, LibreOffice, etc.*), and click through any welcome screens and dialog boxes that might appear during the initial application startup.
3. Enter any necessary license information and complete any activation steps, if required.
4. Open MyQ Easy Config and go to **Settings**. Under **Windows Services Account**, ensure that **Local System account** is selected, and click **Save**. MyQ services restart automatically.

See also:

- Jobs via Email (see page 601)
- Jobs via Web (see page 604)
- Easy Print Settings (see page 382)

12.6 Notifications on Job Receiving Errors

In case a print job is refused for some reason, for example if it was sent to a wrong queue, or if the user has been denied printing by a MyQ policy, the job owner and the MyQ administrator can both be informed about the event.

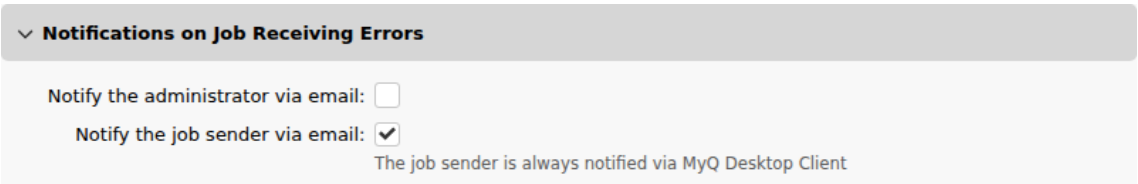
The administrator can be notified via email, and the user can be notified via email or via a small pop-up dialog box at the bottom-right corner of the screen. Users are just notified about the event, whereas the administrator is informed about the problem's details.

To be able to see the pop-up messages, users should have the MyQ Desktop Client application installed and running on their computers.

To activate the notifications via email

On the **Jobs** settings tab, under **Notifications on jobs receiving errors**, you can select two options:

- **Notify the administrator via email**: The email message is sent to the administrator's email address set on the **General** settings tab, under **General**.
- **Notify the job sender via email**: the email message is sent to the primary email address set as **Email** on the user's properties panel on the **Users** settings tab.



To activate the notifications via the MDC pop-up window

The only condition for activation of the pop-up notification for a user is for MyQ Desktop Client to be installed and running on their computer.

See also:

- (10.2) MyQ Desktop Client

12.7 Job Parser

An embedded print job parser is a part of the MyQ system. This tool provides you with additional information about individual print jobs.

Based on those, you can set additional print job rules, or control the job price before a job is printed. This is important, especially for credit accounting and quotas.

The page counts and price from the job parser are an estimate made before the job is printed. Final accounting is based on the output that the printing device reports after

the job is complete. If a job is interrupted, for example by a cancellation, paper jam, or device error, only the pages that were actually printed are accounted.

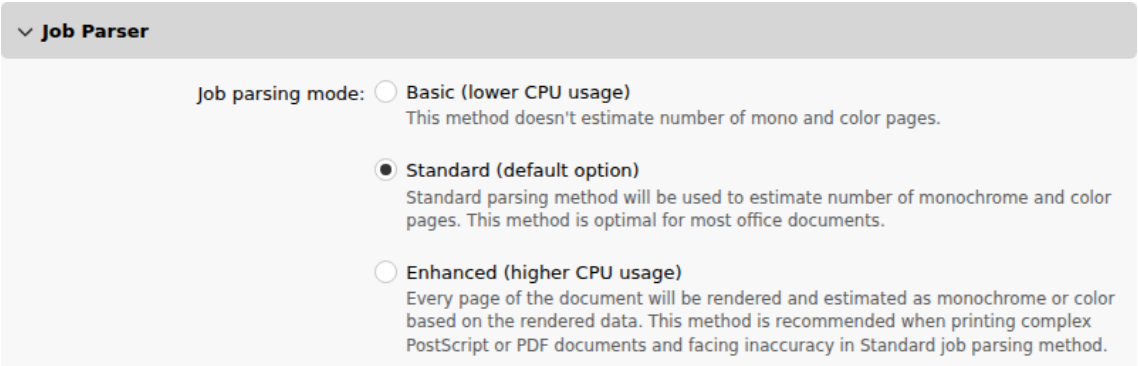
The job parser supports the majority of available printer drivers in PCL5, PCL6 and PostScript.

The job parser provides the following information:

- page description language (PDL): A page description language (PDL) is a language that describes the appearance of a printed page. It receives a code of a document sent to a printing device, interprets it and uses it to instruct the printing device where and how to place text and graphics onto the print page. The most common page description languages are **PCL5**, **PCL6** (XL) and **PostScript**.
- job name
- user name
- number of B&W pages
- number of color pages
- number of copies
- Simplex/Duplex option
- paper format
- staple
- punch
- toner saving

The job parser is activated by default on the **Jobs** settings tab during a new installation. An upgrade will keep the old setting.

There are three available **Job parsing modes**:



- **Basic (lower CPU usage)**: This method doesn't estimate the number of mono and color pages.
- **Standard (default option)**: The standard parsing method will be used to estimate the number of monochrome and color pages. This method is optimal for most office documents.

- **Enhanced (higher CPU usage)**: Every page of the document will be rendered and estimated as monochrome or color based on the rendered data. This method is recommended when printing complex PostScript or PDF documents and facing inaccuracy in the Standard job parsing method.

12.8 Jobs via LPR Protocol

MyQ Print Server can receive print jobs from client computers using the LPR protocol. The client printer sends the job to the Print Server and identifies the destination using the **MyQ queue name**.

Jobs via LPR are enabled by default. For new deployments, consider IPPS where appropriate; LPR remains useful for existing print-driver environments and manually configured printers.

MyQ Print Server receives LPR jobs with its own print spooler. You don't need to install the Windows LPD Print Service on the Print Server.

12.8.1 Enable Jobs via LPR

1. In the MyQ Web Interface, go to **MyQ > Settings > Jobs**.
2. In **Jobs via LPR protocol**, make sure the feature is enabled.
3. If required, change the LPR port. The default and recommended port is **515**.
4. Click **Save**.



If Jobs via LPR is disabled, MyQ cannot receive print jobs submitted using LPR.

The Print Server identifies the sending workstation from the hostname supplied through LPR. The maximum hostname length is **31 characters**.

The maximum job size received through LPR is **100 GB**. Jobs larger than 2 GB are displayed with the size **More than 2GB**.

12.8.2 Before You Configure Client Printers

For each client printer, you need:

- the hostname or IP address of the MyQ Print Server

- the **case-sensitive** name of the MyQ queue
- a suitable print driver

The client computer must be able to reach the LPR port configured on the Print Server.

12.8.3 Configure LPR Printing on Windows

To manually configure a Windows printer to send jobs to a MyQ queue:

1. Open **Control Panel > Devices and Printers**.
2. Select any printer and click **Print server properties**.
3. Open the **Ports** tab and click **Add Port**.
4. Select **Standard TCP/IP Port** and click **New Port**.
5. In the wizard, click **Next**.
6. In **Printer Name or IP Address**, enter the hostname or IP address of the MyQ Print Server.
7. Optionally change the port name, and click **Next**.
8. When prompted for additional port information, select **Custom** and click **Settings**.
9. Configure the port:
    - **Protocol:** LPR
    - **Queue Name:** the MyQ queue name
    - **LPR Byte Counting Enabled:** selected
    - **SNMP Status Enabled:** deselected
10. Click **OK**, then complete the wizard.

The queue name is case-sensitive.

Assign the Port to a Printer

1. In **Devices and Printers**, right-click the printer and select **Printer properties**.
2. Open the **Ports** tab.
3. Select the LPR port you created.
4. Click **Apply**, then **OK**.

If MyQ Desktop Client is installed and the port name matches an existing MyQ queue name, MDC can automatically associate the printer with that queue.

12.8.4 Configure LPR Printing on macOS

To manually configure a macOS printer to send jobs to a MyQ queue:

1. Open **System Settings > Printers & Scanners**.
2. Click **Add Printer, Scanner or Fax**.
3. Open the **IP** tab.
4. Configure the printer:
   - **Address:** hostname or IP address of the MyQ Print Server
   - **Protocol: Line Printer Daemon - LPD**
   - **Queue:** the MyQ queue name
   - **Name:** a display name for the printer
   - **Location:** optionally enter the printer location
   - **Use:** select the appropriate print driver, or **Generic PostScript Printer** if no suitable device-specific driver is available
5. Click **Add**.

The queue name is case-sensitive.

12.8.5 Verify LPR Printing

After configuring the client printer:

1. Send a test job to the printer.
2. In the MyQ Web Interface, open **MyQ > Jobs** and confirm that the job was received.
3. Verify that the job is assigned to the expected user and queue.
4. Release or print the job according to the queue type and confirm the expected output.

If the Print Server does not receive the job, verify that **Jobs via LPR protocol** is enabled, the client is using the configured LPR port, and the queue name matches the MyQ queue exactly.

See also:

- Queues (see page 532)
- Jobs via IPPS (see page 595)
- Main Communication Ports (see page 29)
- (v2) Selecting Printing Methods
- (10.2) Printer Profile Provisioning

12.9 Jobs via IPPS

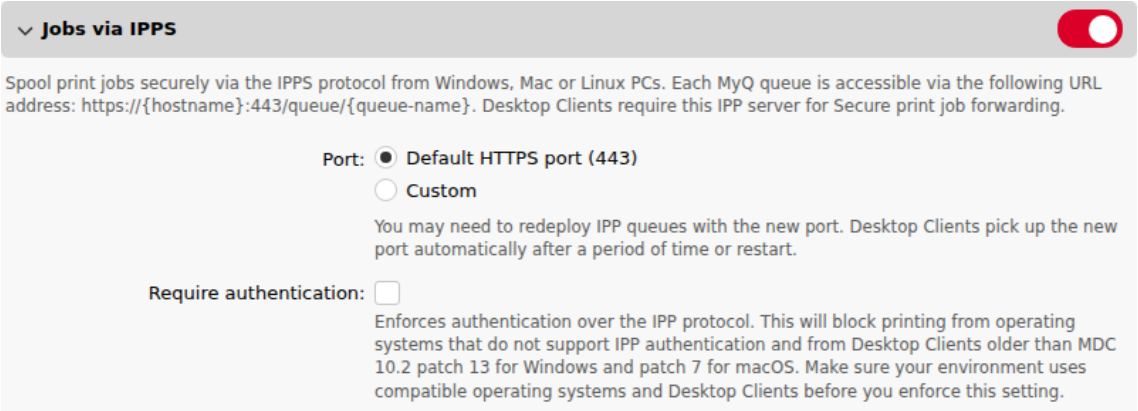
To use your Print Server as an IPP printer for Windows, macOS, Linux, and Chromebook clients, enable and configure print job submission using IPPS.

> The maximum job size received over IPPS is unlimited.

12.9.1 Prerequisites

- IPP client is enabled on both the server running Print Server and the client machines.
  On Windows 10/11, this should be enabled by default, but on Windows Servers, you need to enable it explicitly. Go to **Control Panel - Programs - Turn Windows features on or off.** On the Features tab install "Internet Printing Client", and restart the machine.
- The MyQ certificate is installed on all client machines that will be printing.

12.9.2 Enable Jobs via IPPS



1. Go to **MyQ > Settings > Jobs > Jobs via IPPS**.
2. Enable jobs via IPPS.
3. (Optional) Specify a custom port.

   By default, IPPS uses the same port as the Web Server.
4. (Optional) Enable **Require authentication**. When this option is enabled, IPP communication must include authentication headers to print to this endpoint.
5. Click **Save**.

6. Then, on each IPP client, set the following URL:

   `https://{hostname}:{port}/queue/{queue-name}`

Notes:

- PM Server reserves ports for IPP (631) and IPPS (717). Do not use them.
- IPPS configuration changes take effect when you click **Save**. At this point you will be prompted to confirm the restart of the HTTP Router. Then you should reconfigure all IPP clients to use the new settings.

12.9.3 View IPPS Hostname and Port

You can easily view the IPPS URL, with hostname and port, for your Print Server. Go to **MyQ > Queues > Add Queue**, and check the **Jobs via IPPS** section of the **Job Receiving** tab.

12.9.4 Configure IPPS on Client Systems

Configure IPPS on Windows

When adding a new network printer for IPPS, add the printer by searching for it using the queue URL in the format `https://{hostname}:{port}/queue/{queue-name}`.

Sharing a Windows IPPS printer is not supported.

For managed environments, use MyQ Desktop Client printer provisioning or GPO instead of manual configuration.

Configure IPPS on macOS

1. Go to **System Preferences > Printers & Scanners**.
2. Click **+** to add a new printer and go to the **IP** tab.
3. Fill in the following fields:
   - **Address**: enter the server hostname or IP address and port, for example `print.example.com:443`.
   - **Protocol**: select **Internet Printing Protocol - IPP**.
   - **Queue**: enter `/queue/` followed by the queue name, for example `/queue/marketing`.
4. Click **Add**.

Configure IPPS on Linux

1. Set up a CUPS service and open the **Add Printer** dialog.
2. Click **Enter URL** and enter the printer URL in the format `https://{hostname}:{port}/queue/{queue-name}`.
3. Click **Forward**.
4. In the **Choose Driver** pane, select **Select printer from database**, then select **Generic**.
5. Click **Forward**, then select **IPP Everywhere** as the driver.
6. Click **Forward**, enter a name for the printer, and click **Finish**.

Configure IPPS on Chromebook

You can use IPPS in both managed environments and with Bring Your Own Device (BYOD) devices. For workspace-managed environments, you can deploy IPPS queues via the Google Admin Console. For BYOD Chromebook devices**,** users can install the MyQ X Chromebook Client extension from the Chrome Web Store to provision IPPS queues automatically, or add a printer manually using the IPPS URL.

⚠ The Require Authentication option is not currently supported by the MyQ X Chromebook Client extension.

12.9.5 User Authentication

IPP supports user authentication out of the box. During printing, the IPP server can prompt the client to authenticate by entering credentials for an existing MyQ account.

You can enforce authentication for all IPP and IPPS print jobs by enabling the **Require authentication** option. When enabled, the IPP server rejects any print job that does not include a valid authentication header.

When **Require authentication** is enabled:

- IPP communication must include authentication headers to print to this endpoint.
- When printing from MyQ Desktop Client, authentication is performed silently using the bearer token.
- When printing without MyQ Desktop Client, the user is prompted for their MyQ credentials.

Enabling **Require authentication** blocks printing from:

- Operating systems that do not support IPP authentication.
- MyQ Desktop Client versions older than MDC 10.2 patch 13 for Windows and patch 7 for macOS.

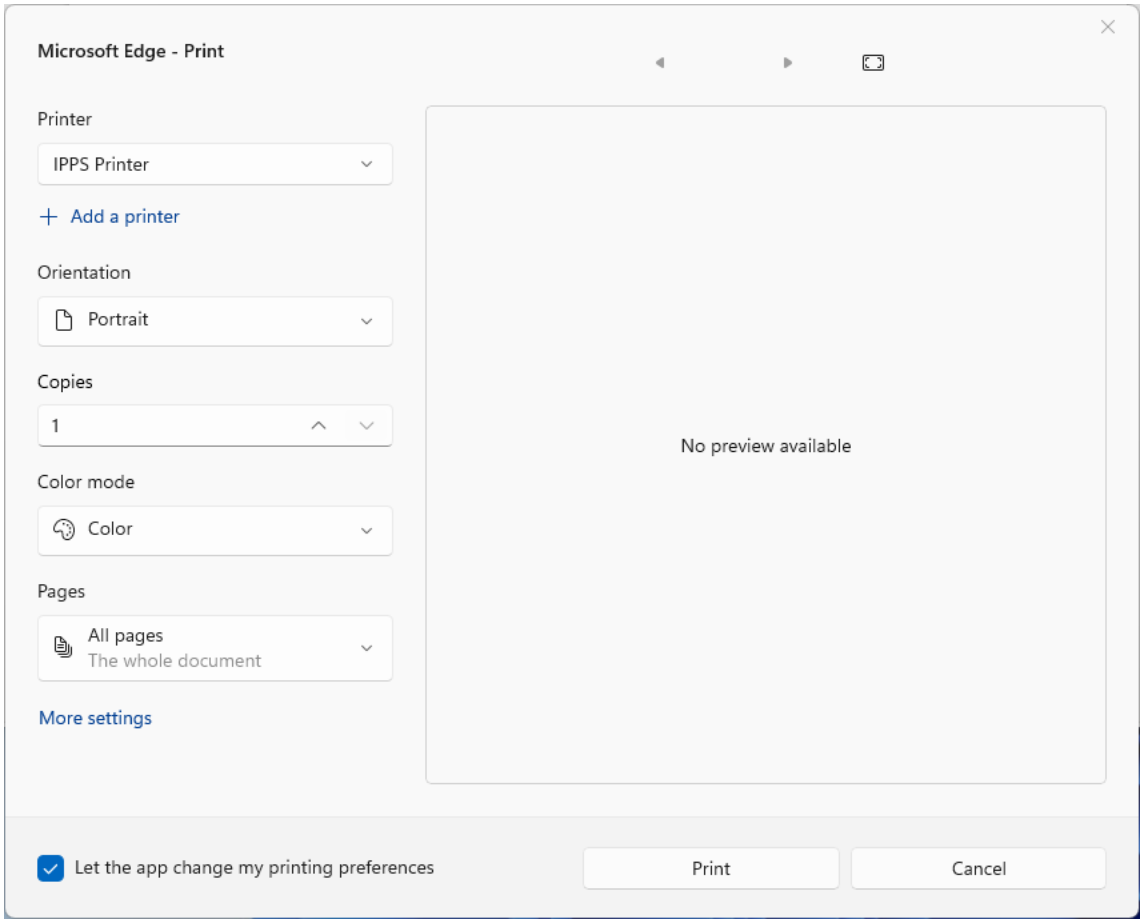
12.9.6 Standard Print Options

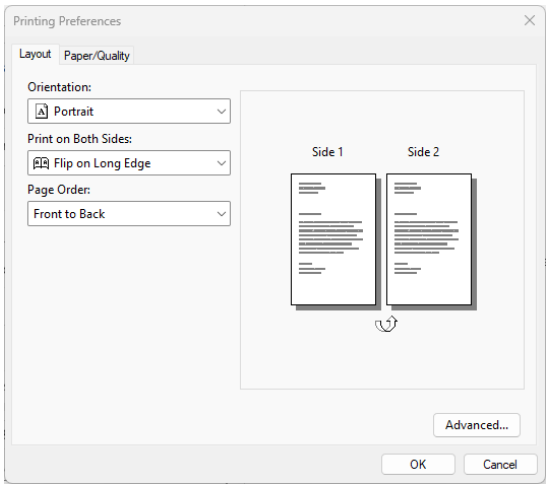
The IPPS server offers a set of standard print options that users can change when printing. By default, the available options are:

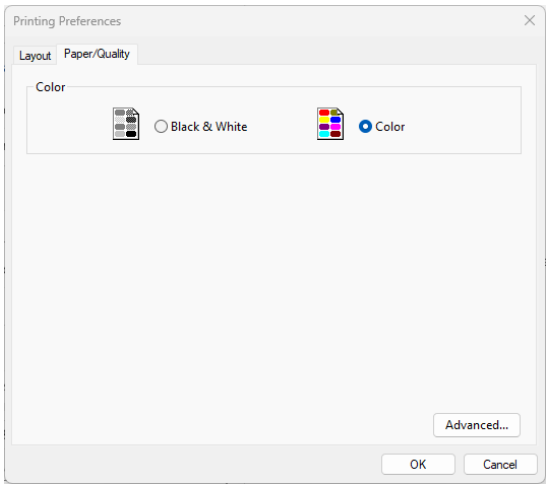
- Copies
- Color mode: Color, Monochrome, Grayscale
- Pages: All pages, Custom (page range selection)
- Duplex (Print on both sides): Flip on Long Edge, Flip on Short Edge, None (Simplex)
- Page order: Front to back, Back to front
- Paper sizes: A3, A4, A5, B4, B5, Folio, Ledger, Legal, Letter, Statement, Other (any other
  unrecognized format)

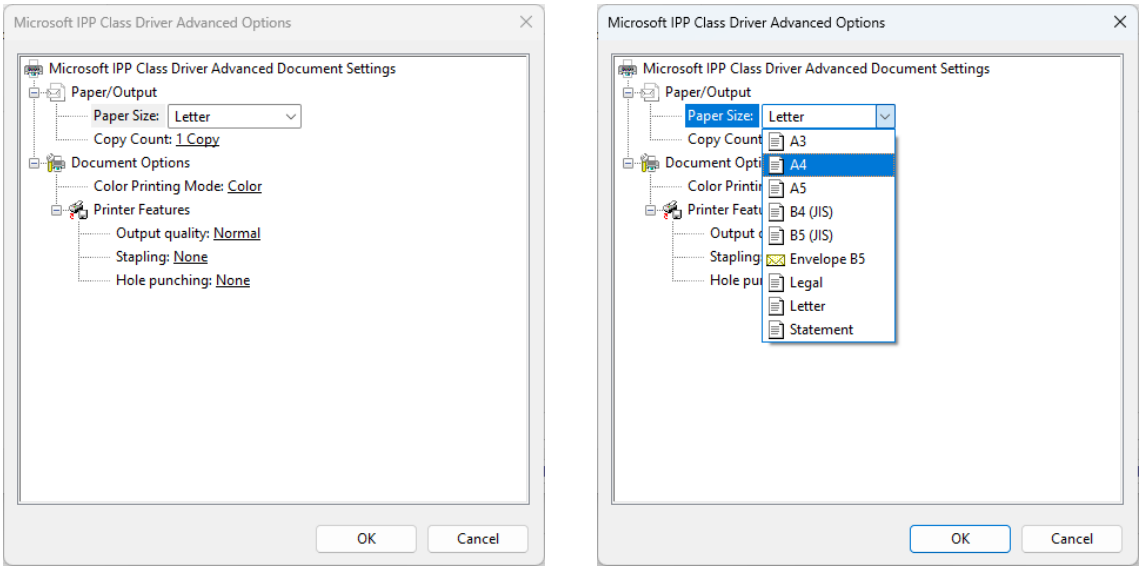


The available options and their names differ depending on the OS used and the application for printing. Some apps might display options that MyQ does not support; these are ignored during processing and release.


Microsoft Edge - Print
Printer
IPPS Printer
Add a printer
Orientation
Portrait
Copies
1
Color mode
Color
Pages
All pages
The whole document
More settings
No preview available
Let the app change my printing preferences
Print
Cancel


Printing Preferences
Layout
Paper/Quality
Orientation:
Portrait
Print on Both Sides:
Flip on Long Edge
Page Order:
Front to Back
Side 1
Side 2
Advanced...
OK
Cancel


Printing Preferences
Layout
Paper/Quality
Color
Black & White
Color
Advanced...
OK
Cancel



12.9.7 Extended Print Options with IPPS Pass-Through

When a queue is configured to use IPPS pass-through, MyQ propagates the full set of IPPS capabilities from the target printer to the queue. This allows client operating systems to display additional printer-specific options, such as:

- Advanced stapling and punching combinations
- Tray or media source selection
- Other printer-specific IPPS options supported by the device and the client OS

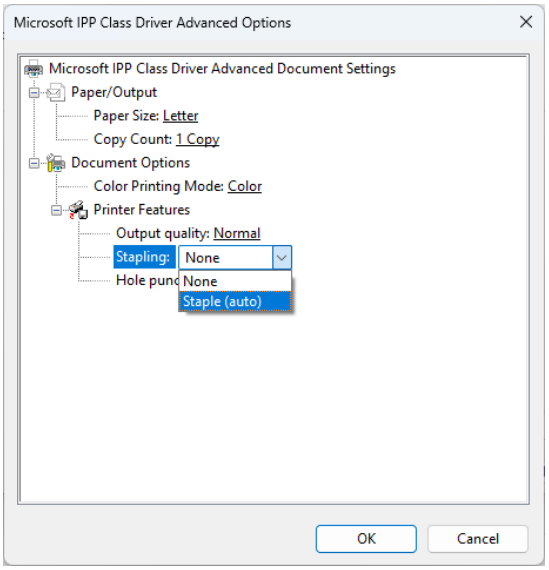
The available extended options depend on what the printer reports through IPPS and what the client OS renders in its print dialog. This is particularly relevant for environments using **Windows Protected Print (WPP)**, where printing is performed exclusively over IPPS.

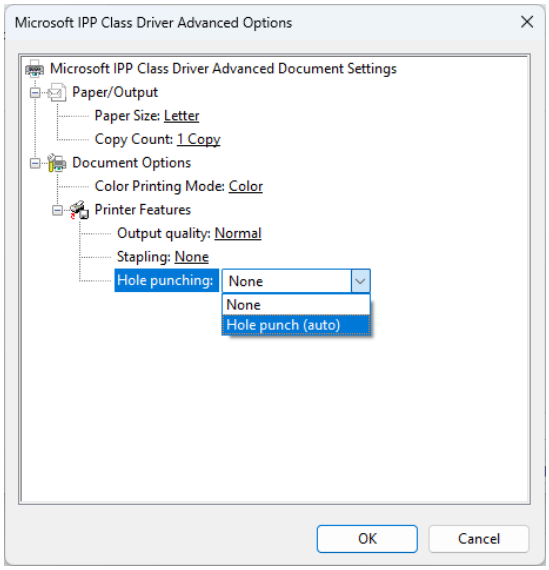
See also: Job Receiving Tab (see page 545)

12.9.8 Finishing Options

As mentioned previously, the support for advanced finishing parameters is limited. The IPPS currently supports Staple Yes (Auto) and No, and Hole punch Yes (Auto) and No.

When "Yes (Auto)" is selected, the final staple and punch positions will be determined by the device on which the job is eventually released. The default settings of the device will be used, based on the regional device settings and the installed finisher type.





12.10 Jobs via Email

Jobs via Email allows users to submit print jobs by sending email attachments to a designated mailbox. MyQ polls the mailbox at a configured interval, retrieves messages, and processes attachments as standard print jobs. The email body can optionally be printed as well.

All jobs submitted via email are assigned to the Email queue and can only be released on devices assigned to that queue.

This method is useful for guest and remote users, BYOD scenarios, and environments where users cannot reach the print server directly. It can also drive automated guest account creation when combined with user self-registration.

12.10.1 Prerequisites

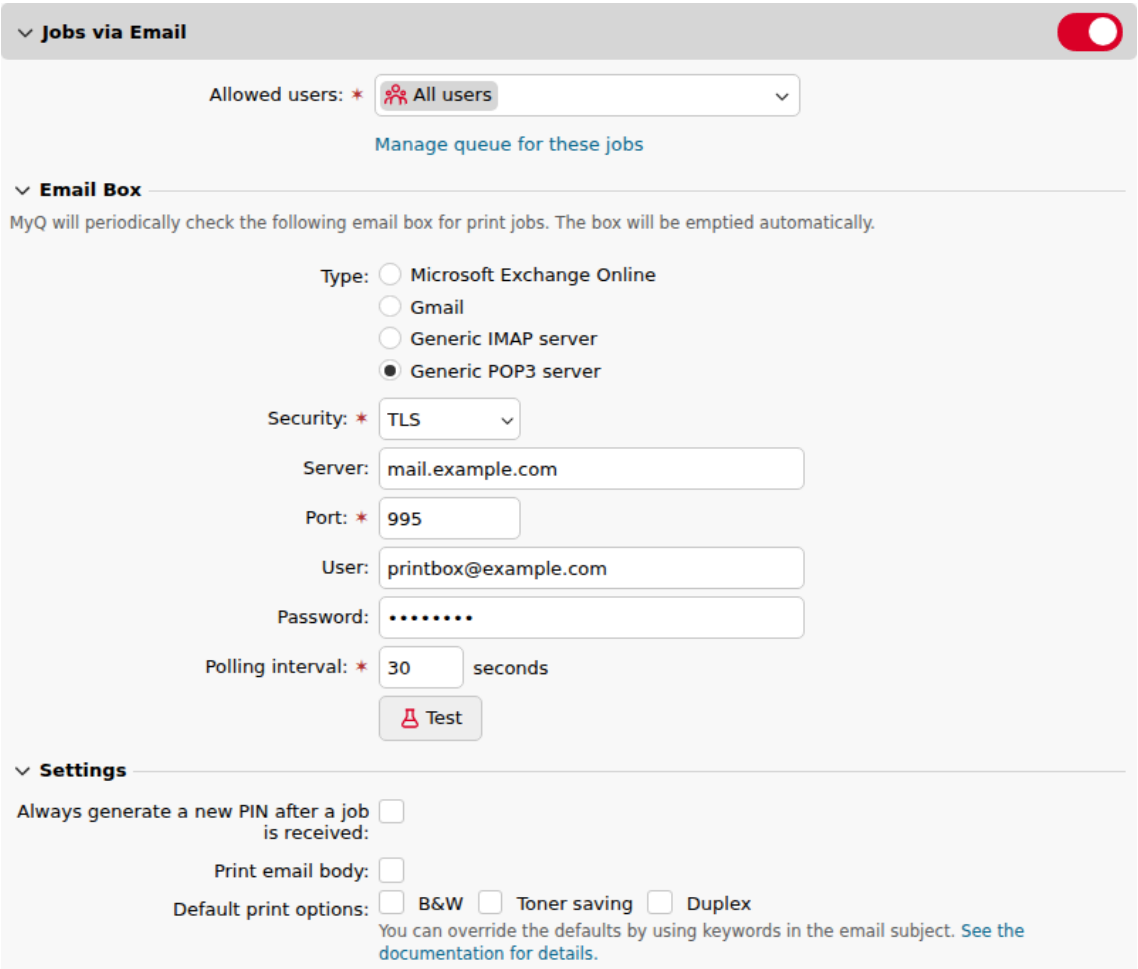
- A dedicated mailbox for receiving print jobs, accessible via POP3, IMAP, Microsoft Exchange Online, or Gmail.
- For Exchange Online: a registered Azure application with the required permissions.
- For Gmail: a Gmail with OAuth2 connection configured under **MyQ > Settings > Connections**.
- For MS Office format attachments: see Office Format Processing.

12.10.2 Supported Formats

PDF/A, TXT, and JPEG are supported natively. For MS Office formats (Word, Excel, PowerPoint), additional server-side configuration is required – see Office Format Processing.

The maximum message size, including all attachments, is 500 MB.

12.10.3 Enable Jobs via Email



1. Go to **MyQ > Settings > Jobs** and locate the **Jobs via Email** section.
2. Set the feature to **Enabled**.
3. In **Allowed users**, specify which users may send jobs via email, or leave set to all users.
4. Select the queue to which incoming email jobs will be assigned.

12.10.4 Configure the Email Box

Under **Email Box**, configure the mailbox MyQ will poll for incoming jobs. The box is emptied automatically.

Microsoft Exchange Online

Exchange Online uses IMAP to collect emails for printing.

If a Microsoft Exchange Online connection has already been configured under **MyQ > Settings > Connections**, it is available in the **Connection** field. If not, click the **Connection** field and then click **Add** to create one. Enter a **Title**, **Client ID**, and **Tenant ID**, then click **OK**.

- **User**: the email address of the mailbox that will receive print jobs.
- **Polling interval**: how often MyQ checks for new messages, in seconds.

Click **Test** to verify the connection, then click **Save**.

Gmail

Gmail uses IMAP to collect emails for printing.

If a Gmail with OAuth2 connection has already been configured under **MyQ > Settings > Connections**, it is available in the **Connection** field. If not, click the **Connection** field and then click **Add** to create one. Enter a **Title**, **Client ID**, and **Security key**, then click **OK**.

- **User**: the email address of the Gmail mailbox that will receive print jobs.
- **Polling interval:** how often MyQ checks for new messages, in seconds.

Click **Test** to verify the connection, then click **Save**.

Generic POP3 or IMAP Server

- **Type:** select **Generic POP3 server** or **Generic IMAP server**.
- **Security:** select **None**, **SSL**, or **STARTTLS**.
- **Server**: the IP address or hostname of the mail server.
- **Port:** confirm the correct protocol port for your selected type and security option.
- **User:** the email address of the mailbox.
- **Password**: the password for the mailbox account.
- **Polling interval**: how often MyQ checks for new messages, in seconds.

Click **Test** to verify the connection, then click **Save**.

12.10.5 Additional Settings

- **Always generate a new PIN after a job is received**: when enabled, a new PIN is generated each time a user sends a job via email, replacing any existing PIN. If this option is enabled, also enable **Send new PIN via email** under **MyQ > Settings > Users > PIN** – otherwise users will not receive their new PIN and will be unable to log in.
- **Print email body**: when enabled, the body of the email is printed in addition to any attachments. You can restrict the body print to **B&W**, **Toner saving**, and/or **Duplex** using the Default print options.
- **Subject keywords**: users can override the default print options by adding keywords to the email subject line. Keywords take priority over Default print options. Available keywords:

Keyword	Effect
`#color`	Color print
`#mono`	Monochrome print
`#duplex`	Print on both sides
`#simplex`	Print on one side
`#ecoon`	Toner saving on
`#ecooff`	Toner saving off

Keywords can appear anywhere in the subject and do not need to be separated. For example: `MyPrintJob #mono#duplex`.

See also:

- Connections Settings (see page 198)
- Jobs Settings (see page 584)
- Automatic User Registration (see page 440)
- Connect to Microsoft Exchange Online (see page 217)

12.11 Jobs via Web

Jobs via Web allows users to upload and submit print jobs directly from the MyQ web interface without installing a print driver. Once the feature is enabled, a **Print File**

button appears on each user's web interface account. Users click the button, select a file, and the job is queued for authenticated release at a printing device.

All jobs submitted via the web interface are assigned to the Web queue and can only be released on devices assigned to that queue.

This method is useful for guests, contractors, and users on platforms where driver installation is not practical.

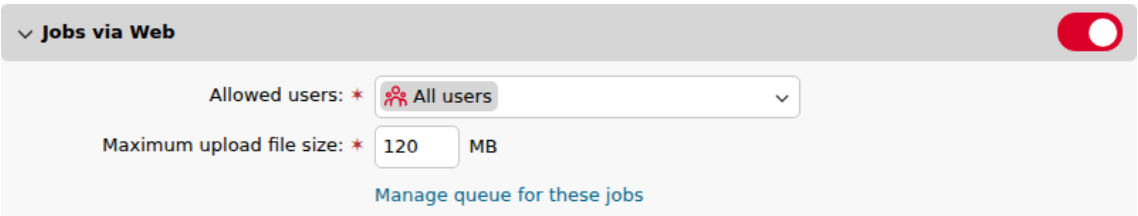
12.11.1 Prerequisites

- The Web queue must exist and have at least one printing device assigned to it.
- For MS Office format uploads: see Set Up Office Format Processing.

12.11.2 Supported Formats

PDF/A, JPEG, BMP, TIF, PNG, and TXT are supported natively. For MS Office formats (Word, Excel, PowerPoint) and LibreOffice formats, additional server-side configuration is required.

12.11.3 Enable Jobs via Web



1. Go to **MyQ > Settings > Jobs** and locate the **Jobs via Web** section.
2. Set the feature to **Enabled**.
3. In **Allowed users**, specify which users or groups may submit jobs via the web interface, or leave it set to All Users.
4. Set the **Maximum upload file size** as required. The allowed range is 20–120 MB; default is 120 MB.
5. Click **Save**.

See also:

- Set Up Office Document Processing (see page 588)

- Jobs Settings (see page 584)

12.12 Job Preview

The **Job Preview** feature is used to generate previews of jobs that are stored on the server. The most common use case is viewing a job before printing it, be it in either the MyQ Web UI, the MyQ mobile application, or on an embedded terminal. In addition, it is also internally used during Job Archiving, where the Job Preview engine is used to generate a PDFA preview of the given job.

To enable Job Preview, go to **MyQ > Settings > Jobs > Job Preview**.



It is possible to limit the **Number of pages** to be generated (*1* by default) in the preview. To include all the pages, set the value to *0*. When the number of pages is changed and there is an already existing generated preview for a job with the old number of pages, the next request to generate a preview will generate a new one with the currently selected number of pages.

Remotely stored jobs cannot be previewed. This applies to Job Roaming, Client Spooling, Device Spooling and Easy Print.

12.13 Job Archiving

With a dedicated **Job Archiving** license and the Jobs Preview feature set up on the MyQ server, you can automatically archive all print jobs that are sent to MyQ. On selected brands of printing devices, you can also archive all copy and scan jobs.

This way you can have full control over what has been printed, scanned and copied within your printing environment, which can be required for example in high security areas in order to be able to identify sources of data leaks.

For information on how to acquire the **Job Archiving** license, please contact the MyQ Sales department.

See also:

- Job Preview (see page 606)

12.13.1 Setting Up Job Archiving

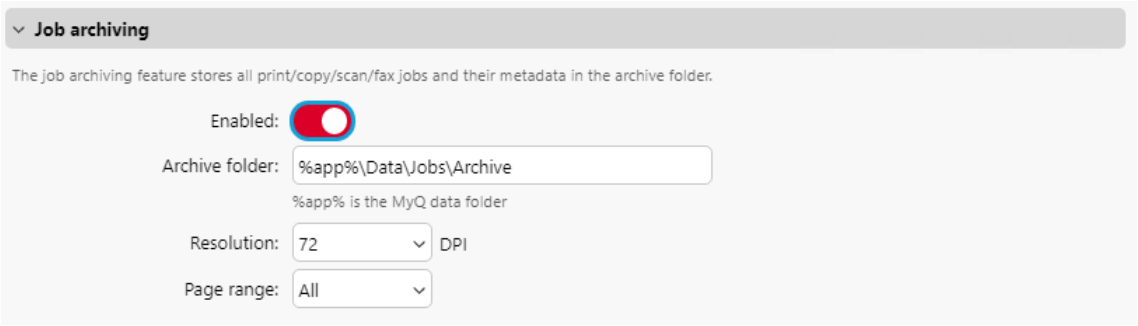
The feature is not part of the default setup of the MyQ server and before the **Job archiving** license is added to the server, the settings of the feature on the MyQ Web Interface are hidden from the administrator.

After you add the licenses, you can set up the feature on the **Jobs** settings tab, in the **Job archiving** section.

You can enable or disable the feature and change the **Archive folder**, where the jobs are archived (by default it is the *Archive* sub-folder of the MyQ data folder).

In the **Resolution** drop-down, you can choose *72 (default), 100, 200, 300,* or *200* DPI.

In the **Page range** drop-down, you can choose *All (default), 1, 2, 3, 4, 5*.



12.13.2 Viewing Archived Jobs

The jobs are stored in subfolders of the **Archive folder**, each of these sub-folders has the form:
YYYY-MM-DD-XXXX, where the front part informs about the date when the sub-folder was created, while the number at the last part serves to sort sub-folders created in the same day.

In the subfolders, you can find two files for each of the printed, copied or scanned jobs:

- a PDF file with the preview of the job
- an XML file with basic information about the job, such as the type of the job or the username of the printing user.

12.14 Job Privacy

The Job privacy feature limits access to sensitive job metadata for everyone, except for the job owner and their delegates.

To enable the feature in the **Jobs** settings tab, go to **MyQ > Settings > Jobs**.



If you have a MyQ Central server setup and Job Privacy is enabled at your Central server, it will be automatically enabled on all the connected Site servers.

> ⚠ Once the Job Privacy feature is enabled, it cannot be disabled again!

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

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

The Job Privacy feature is now enabled.

In addition, you can enable or disable the option to **Hide job names on the device**. Enabling this option means the names of jobs released to devices are redacted so that they are not visible in the device's job history.

12.15 Watermark Collections

On the MyQ Web Interface, you can create collections of watermarks and associate them with the queues where they will be used. Each collection can contain multiple watermarks and can be associated with any number of queues.

PostScript, PCL6 and PDF drivers are supported, but should be selected by the user when they want to see the watermarks printed in their document.

Jobs sent to a queue will have the watermarks of the associated collection printed on each page.

Individual watermarks can be positioned horizontally at the top of the page, horizontally at the bottom of the page, or diagonally. The text size of the watermark can be from *6* to *25*. You can also represent the text of the watermark as a QR code or a Bar code.

A watermarks collection cannot be deleted if there is at least one queue attached to it.

12.15.1 Creating, Editing, and Deleting Watermark Collections

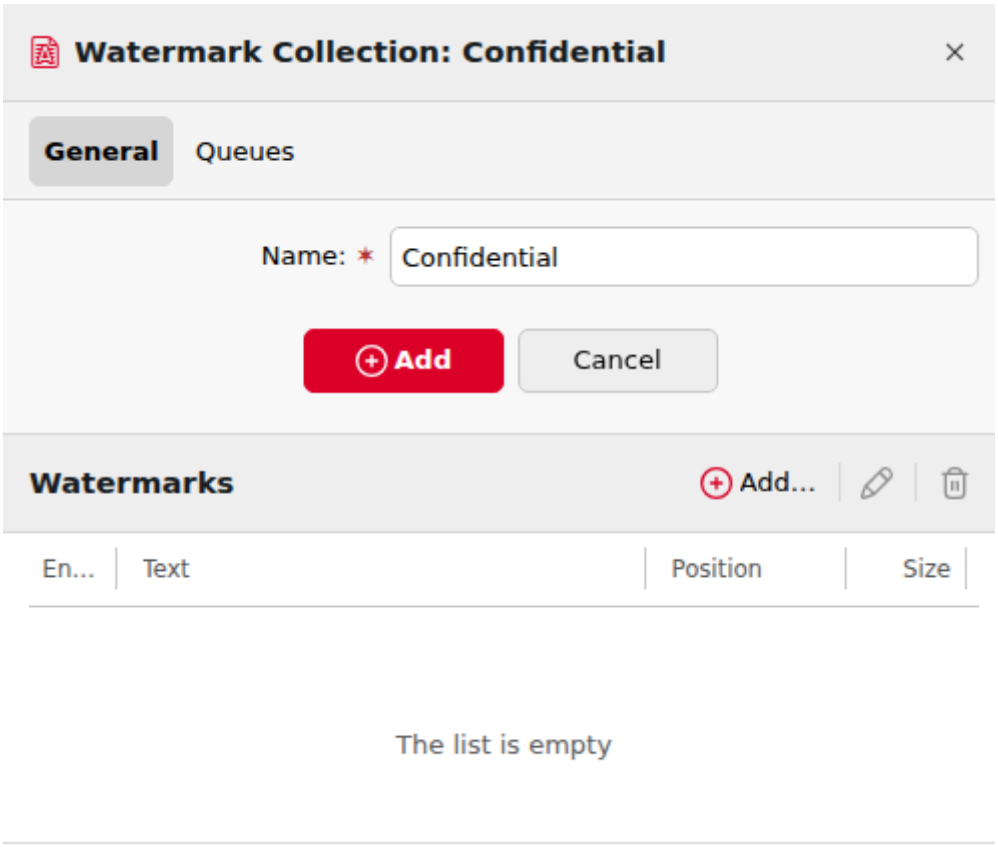
The watermarks collections can be created in the **Watermark collections** section at the bottom of the **Jobs** settings tab.

Creating a New Watermark Collection

To create a new watermark collection:

1. Go to **MyQ > Settings > Jobs** and in the **Watermark collections** section, click **+Add**.

   The properties panel of the new collection opens.
2. Enter the **Name** of the collection, then click **Add watermark**
3. Click **Save**.



Editing a Watermark Collection

The properties panel of the collection opens immediately after the collection is created. To open a properties panel of an already existing collection, select it on the list on the **Jobs** settings tab, under **Watermark collections**, and click **Edit**.

On the properties panel, you can rename the collection, create and remove watermarks, and assign or remove them from queues.

Deleting a Watermark Collection

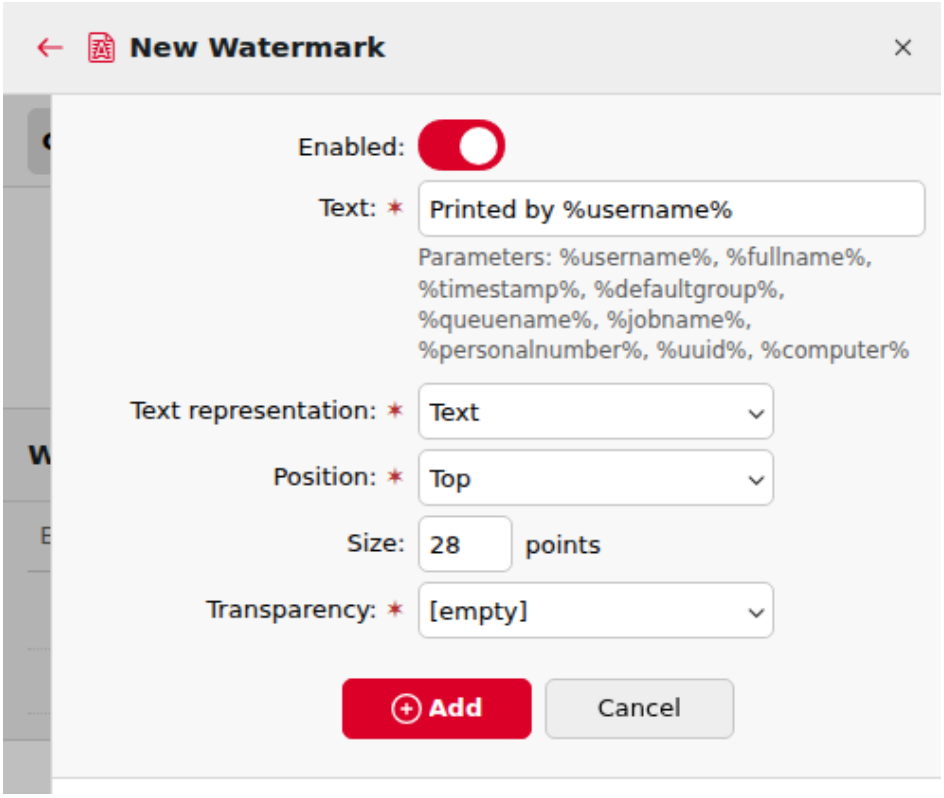
On the **Jobs** settings tab, under **Watermark collections**, select the collection that you want to delete, and then click **Delete**.

12.15.2 Adding, Editing, and Deleting Watermarks

Within each watermark collection, you can create an unlimited number of watermarks. Each of the watermarks in the collection can be activated or deactivated.

Creating a new watermark

On the properties panel of the watermark collection, on the **General** tab, click **+Add watermark**. The properties panel of the new watermark opens. On the panel, set up the watermark, and then click **Save**.



Editing a watermark

The properties panel of a watermark opens immediately after the watermark is created. To open the properties of an already existing watermark, double-click it on the list on the **Jobs** main tab, under **Watermark collections**.

Each watermark has the following properties:

- **Enabled**: Enable/disable the watermark
- **Text**: Text of the watermark; max. length: 512 characters.
- **Text representation**: National characters which are included in the font (standard New Times Roman) are included for Text. The QR/Bar Codes support generally any Unicode text. Restrictions can be found here: QR Code[40], Code 128[41], PDF417[42], and the most restrictive Code 39[43]. The text can be represented in the following forms:

40. https://en.wikipedia.org/wiki/QR_code
41. https://en.wikipedia.org/wiki/Code_128
42. https://en.wikipedia.org/wiki/PDF417
43. https://en.wikipedia.org/wiki/Code_39

    - Text
    - QR Code
    - BAR Code 128
    - BAR Code 39
    - BAR Code PDF417
- **Position**: The watermark's position on the page (the default is: *Bottom right*)
    - Top
    - Top Left
    - Top Right
    - Bottom
    - Bottom Left
    - Bottom Right
    - Diagonal: "Bottom to Top" (only available when *Text* is selected as **Text representation**; greyed out in *QR* and/or *BAR code*)
    - Diagonal: "Top to Bottom" (only available when Text is selected as **Text representation**; greyed out in *QR* and/or *BAR code*).
- **Size**: The watermark's text size (the default is: *28* and the **Font** is *Times New Roman*, which can be changed in the *config.ini*) should be a number from *6-85*
    - *28* is small,
    - *57* is medium,
    - *85* is large.
- **Transparency**: Only visible when *Text* is selected as **Text representation**. The available values are:
    - Dark
    - Medium
    - Light

A watermark in Postscript does not reflect paper orientation. It always prints as portrait.

Deleting a watermark

On the properties panel of the watermark collection, select the watermarks that you want to delete, and then click **Delete**.

12.15.3 Attaching Watermark Collections to Queues

You can attach a watermark collection to a queue either within the setup of the collection, or within the setup of the queue.

Each queue can have only one watermark collection attached to it.

Attaching watermark collections to queues within the setup of the queues

The collection can be selected on the **Job processing** tab of the properties panel of the queue. To open the properties panel, go to **MyQ > Queues**, and then double-click the queue on the list. On the **Job processing tab,** in the **Watermark** section, select the **Watermark** from the drop-down, and then click **Save**.

Attaching watermark collections to queues within the setup of the collections

To assign a new queue to a watermark collection, select it on the on the list on the **Jobs** settings tab, under **Watermark collections**, and click **Edit**.

1. On the properties panel of the watermark collection, click **Queues**. The **Queues** tab opens.
2. On the tab, click **+Add**. A dialog box with a selection of queues appears.
3. Select the queue from the drop-down, and then click **OK**.

13 Scanning & OCR

MyQ allows you to scan documents directly from printing devices and deliver them to a range of destinations, including user email, cloud storage, FTP servers, and more.

Easy Scan is the recommended way to scan in MyQ. Configured by an administrator as a terminal action, Easy Scan provides a one-tap scanning experience on the embedded terminal with flexible destinations and processing options, including OCR.

MyQ also supports Optical Character Recognition (OCR), either through the MyQ Document Processor or by integrating a third-party OCR application via hot folder.

For devices that do not have a MyQ embedded terminal installed, or in cases where a device's native scan panel options are not fully supported by MyQ, scanning to a user's email via the device's SMTP server is also supported.

See also:

- Easy Scan Settings (see page 328)
- Easy Scan Processing (see page 340)
- OCR Profiles (see page 620)
- Using Document Processor (see page 614)

13.1 Using Document Processor

MyQ Document Processor extends Easy Scan with advanced document processing capabilities. This page describes common scanning use cases and provides recommendations for configuring your scan profiles.

Administrators configure these options on individual scan profiles. Once configured, processing occurs automatically when users scan documents with the profile.

See also:

- (10.3) MyQ Document Processor
- Connect to MyQ Document Processor (see page 201)

13.1.1 Quick Reference

Feature	Use it for
Split by page count	Same-length documents scanned as one long stack
Split by barcode	Different-length documents scanned as one mixed stack
Group by barcode	Multi-page documents that shouldn't be just split apart
Skip blank pages	Removing accidental blank pages from the result

Desired result	Recommended format
Preserve the scanned appearance and make the document searchable	Searchable PDF (PDF/A)
Extract unformatted text	TXT
Edit document content	DOCX
Work with tabular data	XLSX
Continue editing content as slides	PPTX

Best practices

- Start from the Print Server language settings
- Use as few languages as possible
- Default to PDF/A and use editable formats only when needed

13.1.2 Scanning Use Cases

Splitting a Scan into Separate Documents

When users scan a stack of pages, Document Processor can automatically split the output into separate files. This produces one file per document instead of one long file that must be divided manually.

Split by Page Count

Best for: Batches in which every document has the same number of pages, such as a stack of four-page contracts.

How it works: Configure a page interval on the scan profile. For example, an interval of four pages creates a separate document from every four scanned pages.

> This option works reliably only when every document in the batch has the configured number of pages. Documents of a different length will be split incorrectly.

Split by Barcode or QR Code

Best for: Mixed batches containing documents of different lengths, such as invoices, HR forms, or incoming mail. A barcode identifies where a new document begins, so users do not need to count pages or scan each document separately.

You can use barcode splitting in two ways.

Option 1: Barcode on a separator page

1. Place a barcode separator sheet before each document in the stack.
2. Scan the complete stack.
3. Document Processor starts a new output file whenever it detects a barcode that meets the configured requirements.
4. Depending on the scan profile configuration, the separator page is either included in or excluded from the output.

Option 2: Barcode on the first page

1. Ensure that the first page of each document contains a barcode, or attach a barcode label to it.
2. Scan the complete stack.
3. Document Processor starts a new output file whenever it detects a barcode that meets the configured requirements.

Barcodes that are smudged, too small, damaged, or poorly printed might not be detected. If a barcode is not detected, the affected pages might be joined to the preceding document or otherwise grouped incorrectly.

Grouping Documents by Barcode

Best for: Related pages or document parts that carry the same barcode and must be delivered as one file. For example, several parts of an order might all contain the same order barcode.

How it works: Enable barcode splitting and the grouping (append) option on the scan profile. Document Processor combines pages with the same barcode value into one output file instead of delivering each barcode-separated part as a separate file.

Example: Three scanned document parts contain the barcode `ORDER-5521`. Without grouping, Document Processor creates three separate files. With grouping enabled, Document Processor combines them into one file. Pages without a barcode are grouped with the preceding page that contains one.

Skipping Blank Pages

Best for: Removing unwanted blank pages, such as the blank backs of single-sided documents scanned in duplex mode.

How it works: Enable blank-page removal and select a paper profile that matches the documents being scanned. Document Processor then detects and removes blank pages before delivering the output file.

The following paper profiles are available:

- Standard paper
- Standard paper – staple
- Standard paper – punch
- Eco paper
- Eco paper – staple
- Eco paper – punch

Select the profile that best matches the paper being scanned. An unsuitable profile can cause near-blank pages, such as pages containing a faint stamp or a single line, to be removed. It can also cause pages with background markings to be retained when they should be removed.

If blank pages are regularly detected incorrectly, review the selected paper profile.

13.1.3 OCR Output Formats

When Document Processor processes a scan with OCR, the selected output format determines how the recognized content is delivered. Each format serves a different purpose.

Searchable PDF (PDF/A)

Use it for: Retaining the scanned appearance while making the document searchable and suitable for long-term archiving.

How it works: The scanned page image is retained and an invisible text layer is added. Users can search, copy, and index recognized text without replacing the page image with reconstructed content.

Choose PDF/A when: Visual fidelity, searchability, or long-term storage is more important than editing. This is the recommended format for most scanning profiles.

Plain Text (TXT)

Use it for: Extracting text without formatting or layout.

How it works: Formatting, page layout, and images are discarded. The output contains only the recognized text.

Choose TXT when: Only the textual content is required, such as when passing recognized text to another system. TXT produces the simplest output file.

> **Editable output may require reformatting**
> When creating DOCX, XLSX, or PPTX files, the OCR engine interprets the scanned content and predicts its structure, formatting, and alignment. These predictions might not match the original document, particularly for complex layouts, tables, forms, and slides. Review the output and correct its formatting, alignment, or structure as necessary.

Word Document (DOCX)

Use it for: Turning a scanned document into editable content.

How it works: Document Processor reconstructs the recognized text, images, and layout in a Word document. Differences in spacing, line breaks, formatting, or positioning are normal.

Choose DOCX when: Users need to edit or reuse content from documents such as letters, reports, or contracts.

Excel Spreadsheet (XLSX)

Use it for: Scans containing tables, forms, or other content arranged in rows and columns.

How it works: Document Processor reconstructs the recognized content and tabular structure in a worksheet.

Choose XLSX when: Users need to work with scanned tabular content as data. For primarily narrative content, such as letters or contracts, use DOCX instead.

PowerPoint Presentation (PPTX)

Use it for: Scanned content that originated as presentation slides or must be edited as a presentation.

How it works: Document Processor reconstructs the recognized text, images, and layout on presentation slides.

Choose PPTX when: Users need to continue editing the scanned content as a slide deck.

13.1.4 Best Practices for OCR Profiles

Use the Print Server Languages as a Starting Point

When configuring a Document Processor OCR profile, use the General language and Additional languages configured on the MyQ Print Server as a reference. These indicate the languages commonly used by your organization.

Check the configured languages in **MyQ > Settings > General > Additional Languages**, and then select only those expected in documents processed by the profile.

Use as Few Languages as Possible

OCR accuracy is highest when the profile includes only the languages present in the scanned documents.

The OCR engine compares recognized characters and words against each selected language model. Selecting unnecessary languages can reduce recognition accuracy and increase processing time.

When configuring a profile:

- Select only one language when documents are consistently written in that language.
- Do not enable additional languages “just in case.”
- Enable multiple languages only when documents processed by the profile genuinely contain them.
- Consider creating separate profiles for documents in different languages.

Use PDF/A by Default

For most scanning needs, Searchable PDF (PDF/A) is the appropriate default format. It retains the scanned page image while adding a searchable text layer.

DOCX, XLSX, and PPTX reconstruct recognized content in an editable format. Their layout can differ from the scanned document and might require additional formatting. TXT retains only the recognized text.

Use an editable format only when users need to modify or reuse the recognized content.

13.2 OCR Profiles

MyQ uses OCR Profiles to define the OCR processing method and output format of scanned scanned documents. When an OCR profile is selected as the scan format in an Easy Scan action, MyQ then processes it according to the profile, before forwarding the output to the configured scan destination.

The following methods are available:

- **OCR via MyQ Document Processor:** use this option to process scans using the MyQ Document Processor.
- **OCR via Hot Folder**: use this option to integrate with a third-party OCR application.

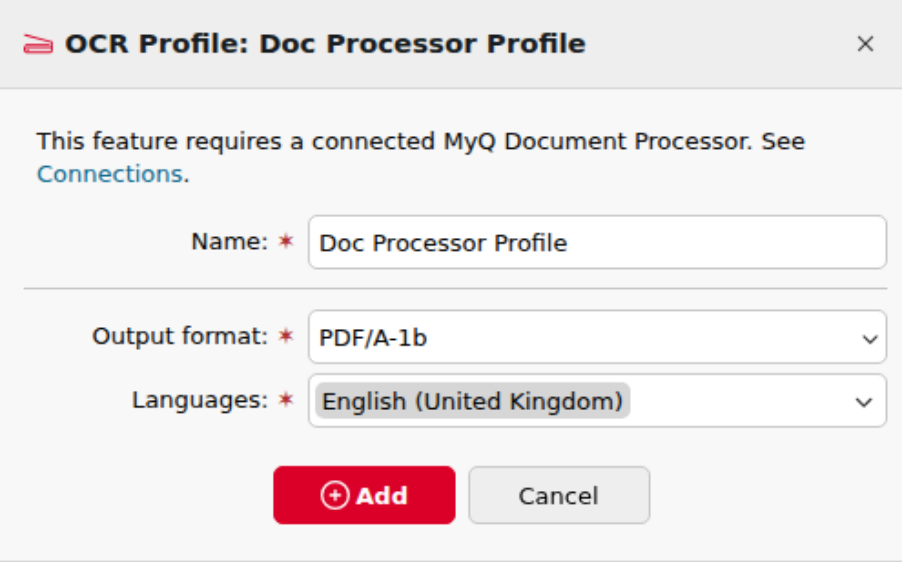
To create and manage OCR Profiles, go to **MyQ > Settings > Scanning & OCR > OCR Profiles**.

13.2.1 OCR via MyQ Document Processor

To use the MyQ Document Processor service for scan processing, define an OCR profile. Before you use this type of profile, first go to **MyQ > Settings > Connections** and create a connection to at least one MyQ Document Processor connection.

MyQ Document Processor Profile Settings

- **Name:** A unique name for the profile. The name appears in the Easy Scan action parameters in the Format option.
- **Output Format:** The format of the output document. The following output formats are supported:
  - pdf
  - PDF/A-1b
  - PDF/A-2b
  - PDF/A-3b
  - txt
  - docx
  - xlsx
  - pptx
- **Languages:** Select only the languages expected in the input documents. Selecting unnecessary languages can significantly reduce recognition accuracy.



Notes:

- If multiple MyQ Document Processor connections are configured, MyQ selects one at random for each job.

- OCR processing time varies depending on the processing mode, the size of the document, and the speed of the Document Processor service.

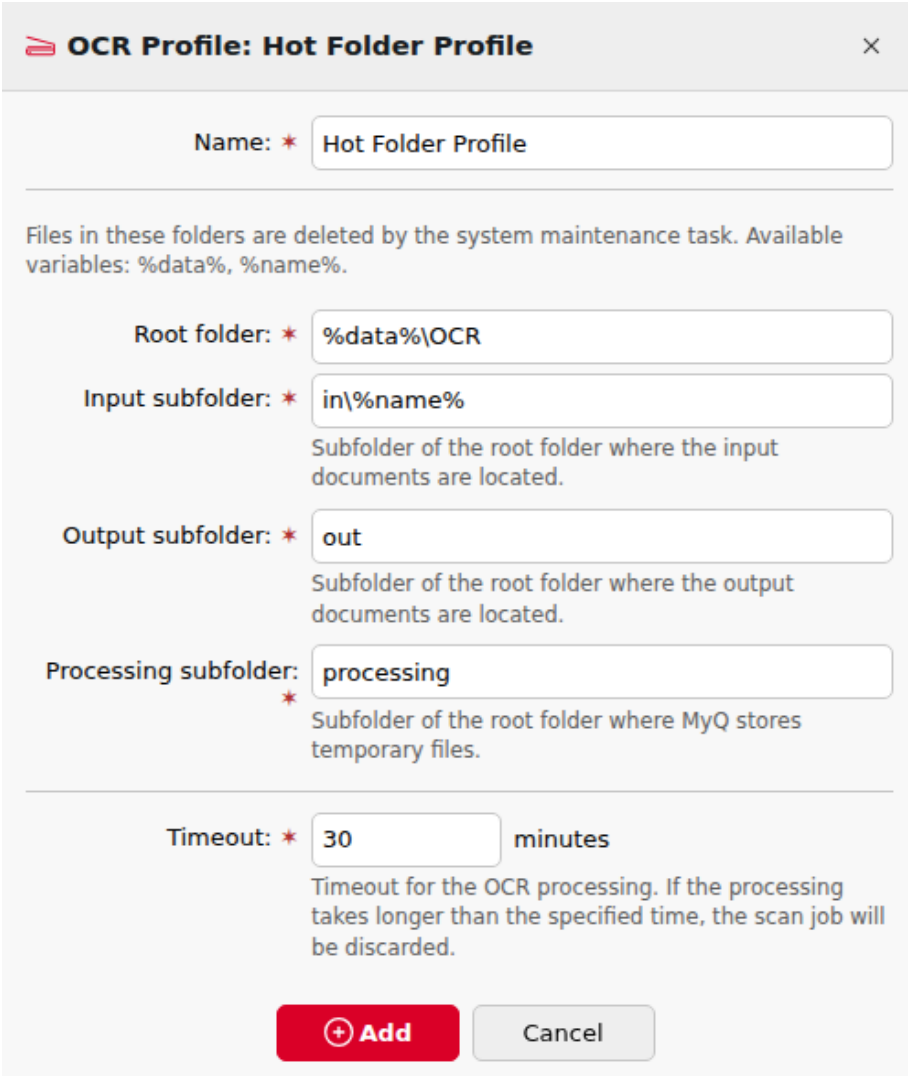
13.2.2 OCR via Hot Folder

The hot folder integrates MyQ with a third-party OCR application. The external application watches an input folder for documents to process, then writes the processed output to an output folder. MyQ monitors the output folder and delivers the processed document according to the configured Easy Scan destination.

The processed document must have the same filename as the input document. Only the file extension changes, based on the output format set by the external application.

Hot Folder Profile Settings

- **Name:** A unique name for the profile. The name appears in the Easy Scan action parameters in the Format option.
- **Root folder:** The root folder where the input, output, and processing subfolders are located.
- **Input subfolder**: The subfolder where the external OCR application watches for incoming documents.
- **Output subfolder:** The subfolder where the external OCR application writes the processed document.
- **Processing subfolder**: A helper subfolder where MyQ stores intermediate files.
- **Timeout**: The maximum time allowed for OCR processing. If processing exceeds this limit, the scan job is discarded.



Notes:

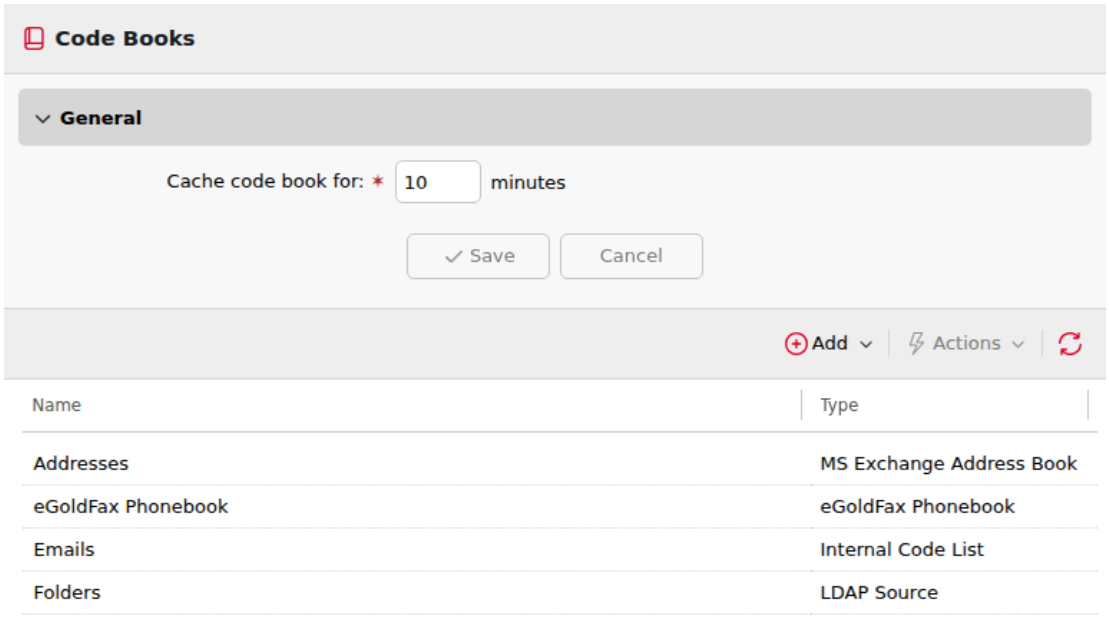
- Scan jobs processed with OCR may be large files. Ensure sufficient storage is available in the system temporary folder, which is used for intermediate results.
- If any processing error occurs, the scan job is discarded, an error is logged, the job owner is notified by email, and all associated job files are deleted.

See also:

- Connect to MyQ Document Processor (see page 201)
- Easy Scan Processing (see page 340)
- Using Document Processor (see page 614)

13.3 Code Books

On the **Code Books** settings tab (**MyQ > Settings > Code Books**), you can add code books and code lists with defined values for each of them. These code books and lists can be used with your scan profiles in multiple ways, such as allowing users to use scan recipients from an LDAP source, set up output folders from an internal code list, search users from an MS Exchange address book, etc.



In the **General** section you can find the **Cache code book for: __ minutes** setting. The value set here determines how long the code book will be cached in MyQ, to be available in case of a lost connection between the MyQ server and the LDAP server. The default value is *10* minutes.

Below that, you can add and modify your code books.

You can add the following code books:

- LDAP Source
- Internal code list
- MS Exchange Address Book
- RightFax Phonebook
- RightFax Phonebook Groups
- eGoldFax Phonebook

⚠ When you create a RightFax or eGoldFax connection, their corresponding code books are generated automatically**.**

To add a new code book, click **+Add** and select the type you want to add from the drop-down.

To delete a code book, select it, click **Actions**, and select **Delete**, or right-click on the code book and select **Delete**.

To edit a code book, select it, click **Actions**, and select **Edit**, or right-click on the code book and select **Edit**, or double-click on the code book.

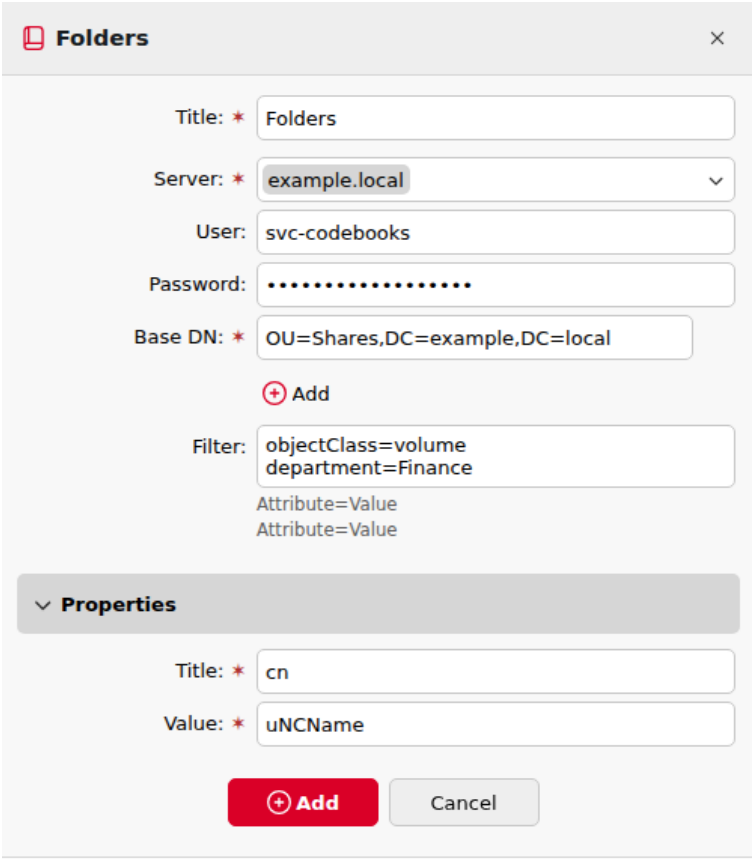
See also:

- Scan to eGoldFax (see page 370)
- Scan to RightFax (see page 373)
- LDAP Source Code Books (see page 625)
- Internal Code List (see page 627)
- MS Exchange Address Book (see page 629)

13.3.1 LDAP Source Code Books

On the **Code Books** settings tab (**MyQ > Settings > Code Books**), you can enable selecting scan recipients directly from an LDAP server by importing the codes from that server.

In the Code Books section, click **+Add** and select *LDAP Source* from the drop-down. The new code book's properties panel opens on the right side of the screen.



On the properties panel, fill in the required information, and click **Save**:

- **Title** - The code book's name.
- **Server** - The LDAP server that you want to import the attributes from.
- **User** - The user name for accessing the LDAP domain server.
- **Password** - The password for accessing the LDAP domain server.
- **Base DN** - The base domain(s) that you import the attributes from. Click **+Add** to add a text box for an additional base DN, and then enter the domain. You can add multiple domains this way.
- **Filter** - You can filter the users import by specifying the attributes' values. **Attribute=Value**. Users with different values in this attribute are not accepted and are filtered out of the import. You can use the ***** symbol to search for substrings. The symbol can be appended from both sides. For example, if you add a cn=*in* condition, only users whose common name attribute contains "in" are accepted. Add one condition per one raw. Users are accepted if they satisfy at least one condition.
- **Properties**: **Title**, **Value** - Define the titles and values of the code for each user by entering their attributes from the LDAP database. For example, you can enter the *cn* attribute as the **Title** and the *folder* attribute as the **Value**. This

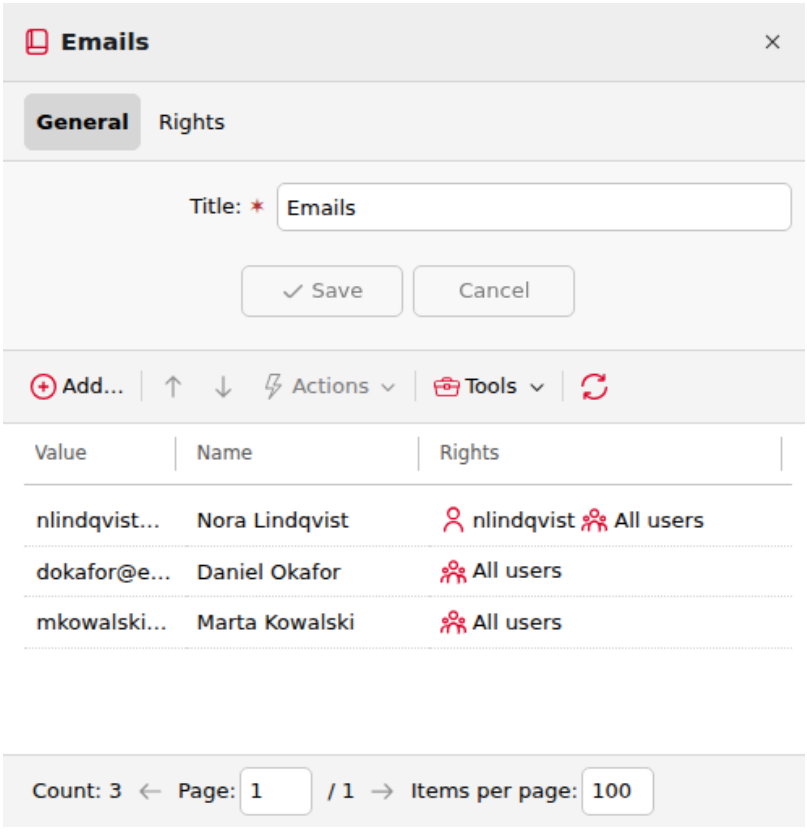
way, each code will contain the user's folder and its title will be the user's full name.

After opening the LDAP Source Code Books on a terminal, only the first 50 entries are shown. Users can search for any non-listed entries using the name of the un-listed contact. Email, Fax and Phone are shown separately.

13.3.2 Internal Code List

On the **Code Books** settings tab (**MyQ > Settings > Code Books**), you can predefine code lists with values and use the values as options available for users.

In the Code Books section, click **+Add** and select *Internal code list* from the drop-down. The new code book's properties panel opens on the right side of the screen.



On the properties panel, on the **General** tab, enter a **Name** for your new internal code list, and click **Save**. The new code list is added to the list on the **Code Books** settings tab.

On the **Rights** tab, you can provide users or groups of users with the right to use the code list. Click **Add User** and select the user or group from the drop-down. Check the boxes for the rights you want to assign to them.

Add new codes to an existing code list

1. Double-click on the code list (or right-click the code list and click **Edit**). The code list's properties panel opens on the right side of the screen.
2. On the panel, click **+Add**.
3. Enter the **Code** name and its **Description** (the description will be shown on the terminal). You can also assign access **Rights** to this code to users or groups. Finally, click **OK**.

Import codes from a CSV file

A sample CSV file called `CodeBook_example` is available in `ProgramData\MyQ\Data\Import`, this CSV can be populated with relevant information and imported.

1. Double-click on the code list (or right-click the code list and click **Edit**). The code list's properties panel opens on the right side of the screen.
2. On the panel, click **Tools**, and select **Import from CSV file**.
3. In the Import from CSV file panel, browse and select the CSV file that you want to import, select the **Column delimiter** used in the file, select the character set (**Charset**) used in the file, choose if you want to **Update existing values** and/or **Skip header line**, and click **OK**.

Each line of the CSV file has to consist of either one, two or three columns. The first column contains the code, while the optional second and third columns contain the code's description and the users or groups with access to this code. For example:

Code1,This is Code 1,All users
Code2,This is Code 2,"eliot.kate"
Code3, This is Code 3
Code4

13.3.3 MS Exchange Address Book

You can use an MS Exchange Address Book to retrieve personal contacts from the user's mailbox from the MS Exchange Server. You can set parameters for Email, Fax and Phone.

⚠ MS Exchange Server 2019 is supported; MS Exchange Server 2016 and MS Exchange Server 2013 SP1 (from build 15.0.847.32) may work but are not supported.

MS Exchange Server Configuration

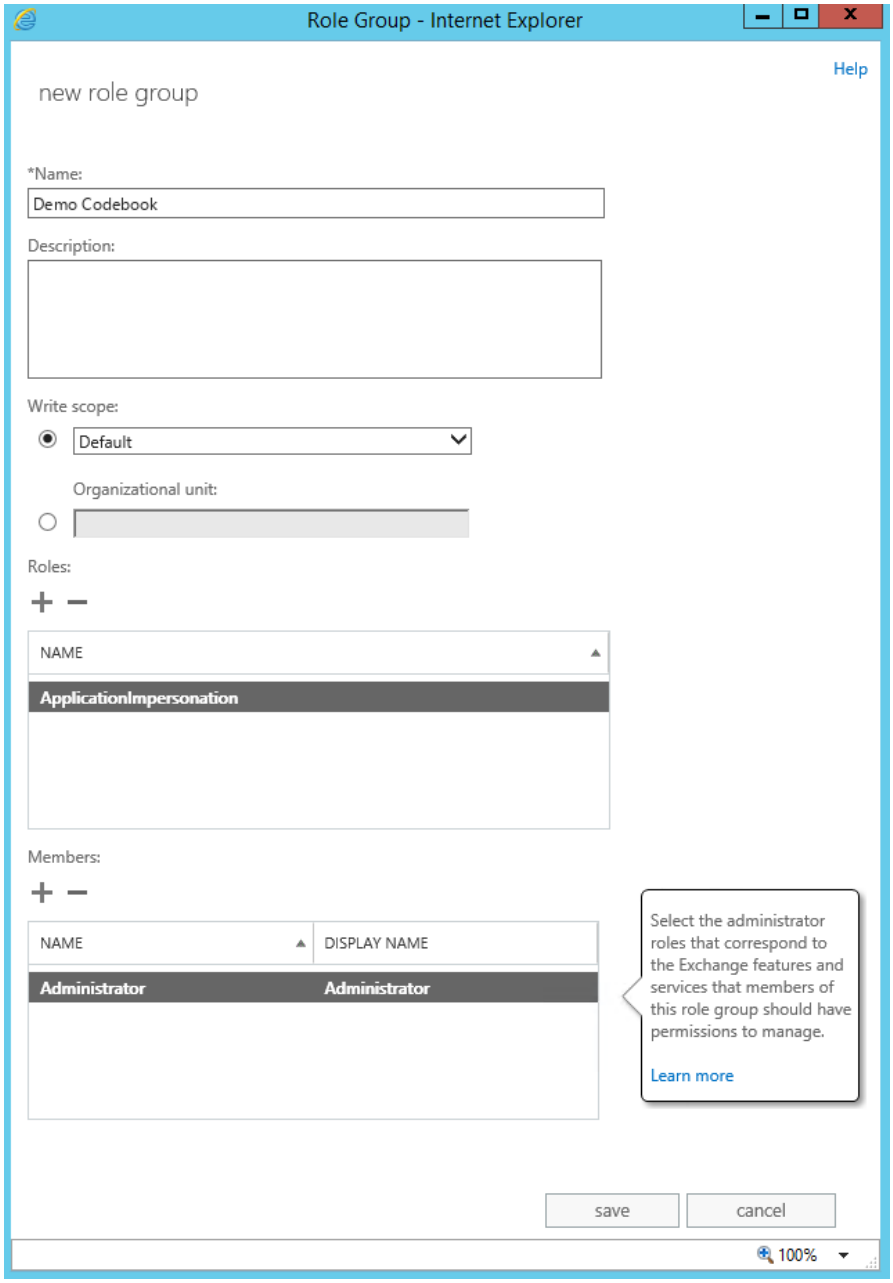
All settings on IIS[44] (Internet Information Services) have to be set up correctly to allow third-party applications (MyQ) to communicate with the EWS service.

On your MS Exchange Server, the only necessary setting is configuring an account with the '**ApplicationImpersonation'** right, in order to be able to access other users' mailboxes.

To do that:

- Log in to your Exchange Admin Center[45].
- Go to the **permissions** tab, and Create (+) a new **Admin Role**.
- In this new role, add the **ApplicationImpersonation** right.
- In this new role, add user/admin account that you want to use in MyQ for accessing personal contacts of other users' mailboxes.

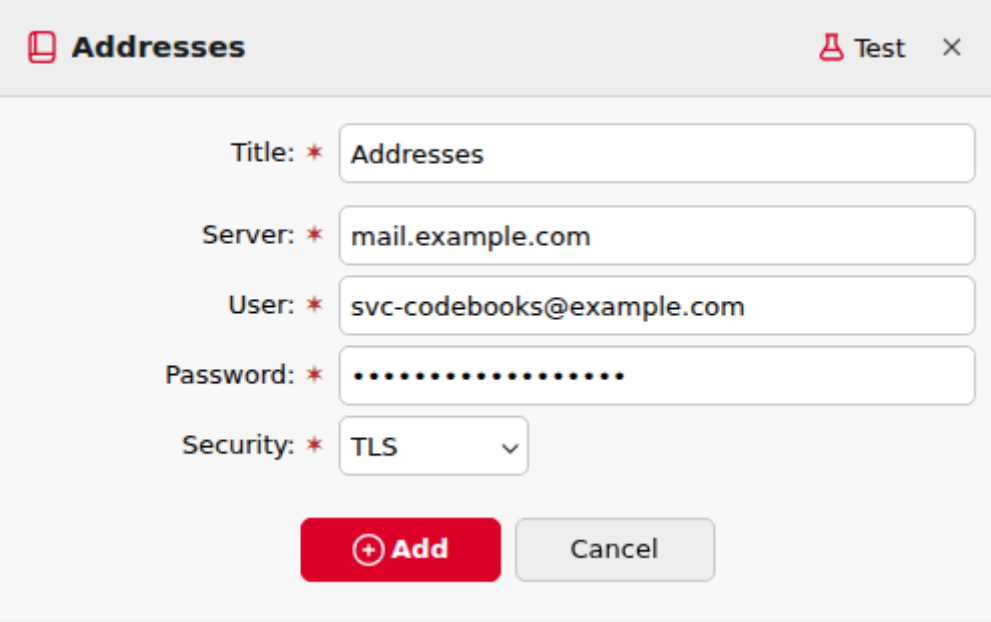
44. https://www.iis.net/
45. https://admin.exchange.microsoft.com/



Adding a New MS Exchange Code Book in MyQ

On the **Code Books** settings tab (**MyQ > Settings > Code Books**), in the Code Books section, click **+Add** and select *MS Exchange Address Book* from the drop-down. The new code book's properties panel opens on the right side of the screen.

On the properties panel, fill in the required information:

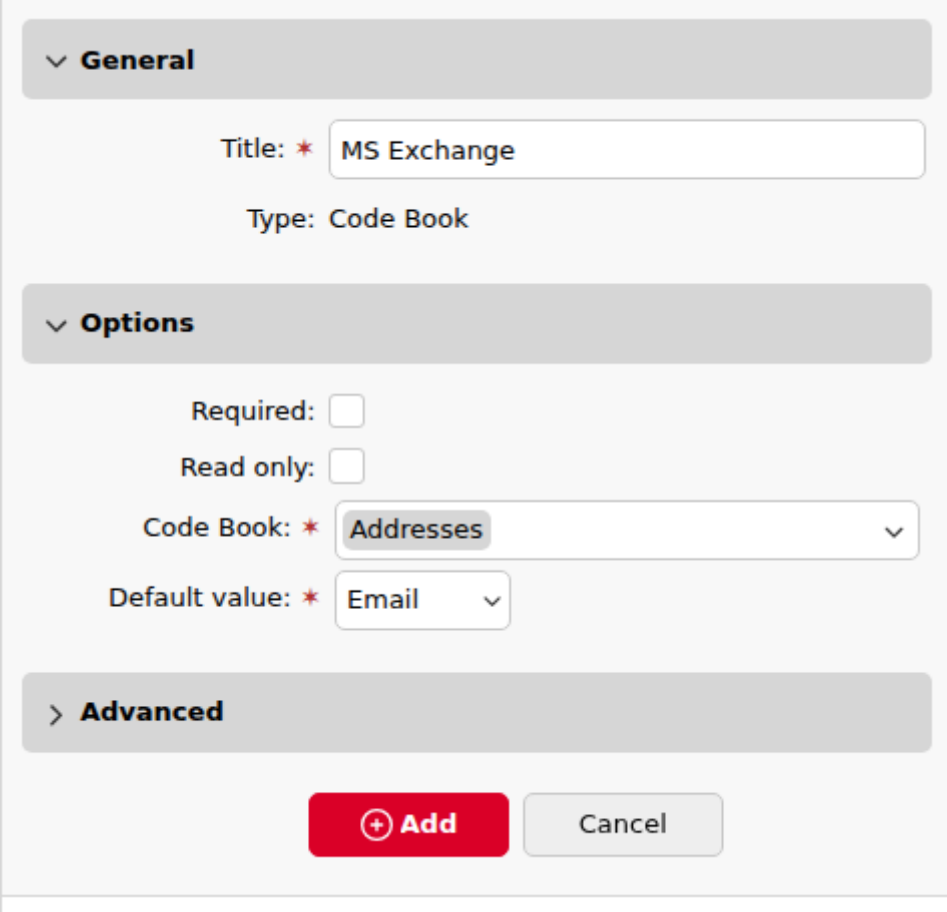


- **Name**: Add a name for the code book.
- **Server**: The host name or the IP address of the MS Exchange Server.
- **User**: The name of the user who has the required rights (*applicationImpersonation* to access other users' mailboxes) on the MS Exchange Server.
- **Password**: The above user's password.
- **Security**: Select *None* or *SSL*.

Click **Test** to check the connection to the MS Exchange Server, and click **Save** to make the new MS Exchange code book available.

Using MS Exchange Code Books on a MyQ Scan Profile

Go to **MyQ > Settings > Terminal Actions** and create a new parameter for a scan profile of your choice. To do that, double-click the scan profile. In the properties panel that opens on the right side of the screen, go to the **Parameters** tab. Click **+Add** and fill in the required information to setup the new parameter.



- **Title:** Add a title for this new parameter.
- **Type**: Select *Code Book* from the drop-down.
- **Code Book**: Select your MS Exchange Address Book from the drop-down.
- **Default value**: Select the type of contact to be displayed for the user:
  - *Email*: Will display emails from retrieved contacts.
  - *Phone*: Will display phone numbers from retrieved contacts.
  - *Fax*: Will display fax numbers from retrieved contacts.
- **Required**: Mark the checkbox if you want to make this parameter mandatory.

After opening the MS Exchange code book on a terminal, only the first 50 items are shown. Users can search for any non-listed items by using the name of the hidden contact. Email, Fax and Phone are separately shown.

In case you are using custom certificates and you are getting a connection error when trying to see the Exchange Address Book: It may be required to add the issuer's certificate manually into the *C:\Program Files\MyQ\PHP\cacert.pem* file for the connection to work.

13.4 Scan to Me

For most scanning workflows, **Easy Scan** is the recommended method. Easy Scan is configured as a terminal action and delivers scanned documents to user email, cloud storage, FTP servers, and more, with a single tap on the embedded terminal.

The workflow described on this page applies to those edge cases where Easy Scan is not available – for example, on devices whose native scan panel options are not fully supported by MyQ.

Scan to Me allows users to scan a document from the device's native panel and deliver it to their MyQ account using the device's built-in SMTP client. The device sends the scanned document as an email attachment to the MyQ SMTP server. MyQ receives the job, identifies the sending device, identifies the user currently logged on to that device, and routes the document to the configured destination, which could be the user's primary email address or their scan storage folder.

The destination is determined by the recipient email address used on the device.

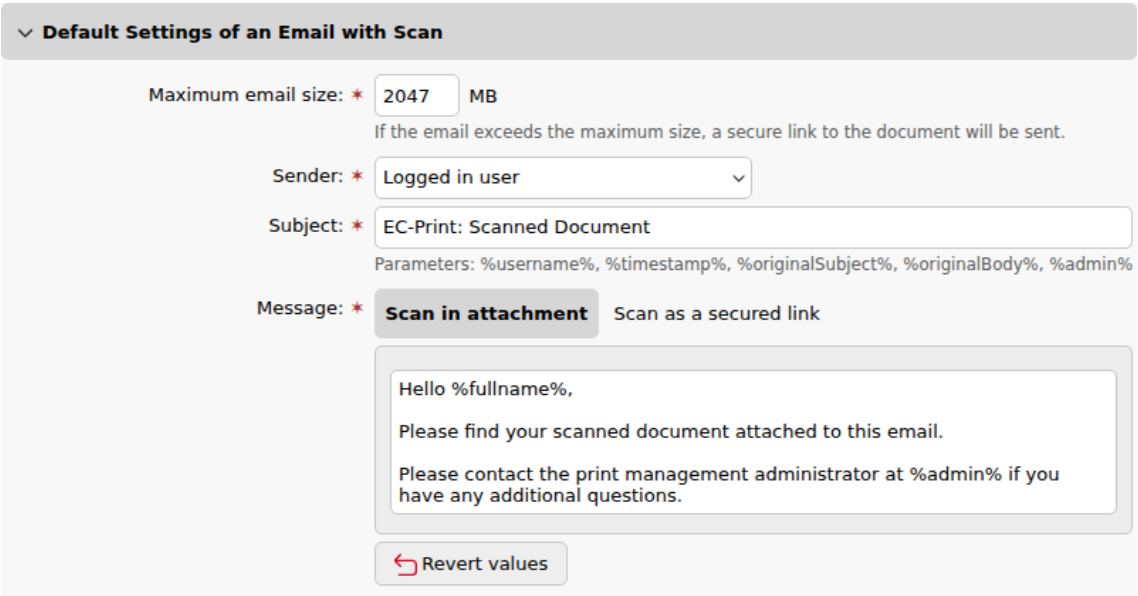
Make sure that the time and date are set correctly on the printing device.

13.4.1 Setting Up Scanning via Device SMTP

Setup consists of the following steps:

1. Set up scanning on the MyQ server.
2. Set SMTP on the printing device.
3. Set the destinations for MyQ users on the MyQ server.

Set Up Scanning on the MyQ Server



1. Go to **MyQ > Settings > Scanning & OCR** and configure the **Default Settings of an Email with Scan**. The following options are available:
   - **Maximum email size:** If the email exceeds the maximum size, a secure link to the document will be sent.
   - **Sender:** The sender of the scan. Available options are:
     - Logged in user
     - Default sender (`MyQ@MyQ.local`)
   - **Subject:** Defines the subject line of the email. You can insert valued dynamically using substitution variables: `%username%`, `%timestamp%`, `%originalSubject%`, `%originalBody%`, and `%admin%`
   - **Message type:** You can send the scanned document as an attachment or as a downloadable link. Select **Scan in attachment** or **Scan as a secured link**.
   - **Message body:** Customize the email body.
2. Go to **MyQ > Settings > Configuration Profiles**, open the corresponding profile for the device. On the Terminals tab, make sure that the **Set MyQ as device SMTP server** option is enabled.

Configure SMTP on the Printing Device

To activate Scan to Me on a device, first enable and configure SMTP in the device web interface. For information about how to access the device web interface and locate the relevant settings, see the printer manual.

Perform the following steps on the printing device's web interface:

- Enable the SMTP protocol.
- Enter the MyQ server IP address or hostname as the SMTP server address.
- Ensure that the SMTP port matches the SMTP port that is configured in **MyQ > Settings > Network > MyQ SMTP server**. The default port in MyQ is *25*.
- Enter a sender email address. This value is arbitrary.

Set the Destinations for MyQ Users on the MyQ Server

On each user's properties panel, set the appropriate fields according to the following table:

Option	Field	Value
Send scans to the user's primary email	**Email**	User's primary email address
Store scans in the user's scan folder	**User's storage**	Path to the folder where the document should be stored

---

13.4.2 Provide Users with Scan Destinations

To allow users to send scans to the correct MyQ destination from the native scan panel of the device, provide them with the appropriate recipient email addresses:

- `email@domain.local` - routes the scan to the user's primary email.
- `folder@domain.local` - routes the scan to the user's scan storage folder.

You can add these addresses to the device's address book as shortcuts so that users can select them quickly from the native **Scan and Send** action.

See also:

- Easy Scan Settings (see page 328)
- Configuration Profiles (see page 310)

- Editing User Accounts (see page 431)

14 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.

See Accounting Settings (see page 249).

14.1 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 **MyQ > Settings > Jobs**.
- **Currency**: Monetary accounting and all payment providers use the currency set on the General settings tab. Go to **MyQ > Settings > General** and 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.

14.2 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 638).

14.3 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 Quotas (see page 654).

14.4 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 Projects (see page 668).

14.5 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 Price Lists (see page 674).

14.6 Credit

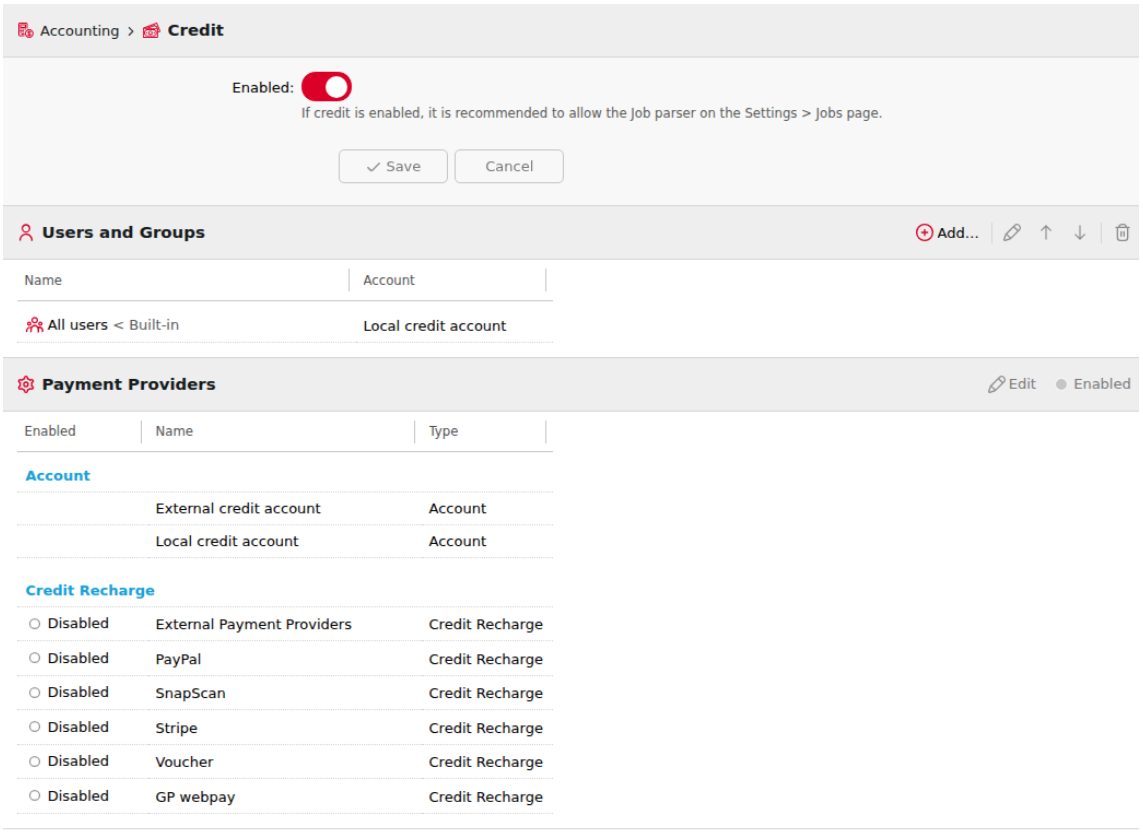
With the credit accounting feature activated, users can copy, print and scan only if they have enough credit on their account in MyQ. Printing is allowed only for print jobs that do not exceed the current credit, and copying is terminated after credit is exceeded, although there can be an overflow of 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.

To enable and configure credit, go to **MyQ > Settings > Credit**.



14.6.1 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.

14.6.2 Activating and Setting Up Credit

Enable Credit

To set up credit accounting, go to **MyQ > Settings > Credit** and **Enable** credit.

Enable Credit for Users and Groups

You can activate credit for a user or for a group of users.

1. Under **Users and Groups**, click **+Add item**. A new item appears on the list of users and groups on the **Credit** settings tab.
2. Select a **Name** from the drop-down list.
3. Select an **Account** from the drop-down list. The available options are:

    - Local credit account
    - External credit account
4. Click **OK** to save the settings.

Enable Payment Providers

You can enable and disable the available payment methods for credit recharge.

- 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).

14.6.3 Managing Credit Manually

Administrators can change users' credit in the MyQ Web Interface. An authorized user can also recharge or reset credit if they have the required rights.

Action	Effect
Recharge credit	Adds the entered amount to the current balance. Enter a negative amount to reduce it.
Reset credit	Replaces the current balance with the entered amount.
Bulk credit recharge	Imports recharge amounts for multiple users from a CSV file.
Release blocked credit	Releases credit blocked for a selected user.

Prerequisites

- You are an administrator, or you have the **Recharge credit** right (**Rights** settings tab).
- If you start the action from **Users**, you also have the **Manage Users** right.

Recharge or Reset Credit

You can start either action from **Credit Statement** or **Users**:

- **Credit Statement:** Go to **MyQ > Credit Statement**, then click **Recharge credit** or **Reset credit**. In the dialog, enter a card ID or select a user or group.
- **Users:** Go to **MyQ > Users** and select the users. Click **Actions > Credit > Recharge credit** or **Reset credit**. For a group, right-click the group in the left panel and select the action.

Enter the amount and confirm the action. **Recharge credit** adds that amount to each selected user's balance; for example, entering `-100` reduces each balance by 100. **Reset credit** sets each selected user's balance to the amount entered.

Recharge Credit from a CSV File

1. Go to **MyQ > Users** or **MyQ > Credit Statement**.
2. Click **Tools > Bulk credit recharge**.
3. Select the CSV file and click **OK**.

Each nonempty row must contain a user name and a recharge amount, separated by the delimiter configured under **MyQ > Settings > General > Column delimiter in CSV**. Check the result in the **Credit** column on **Users**.

Release Blocked Credit

To release blocked credit, go to **MyQ > Users**, select the user and click **Actions > Credit > Release blocked credit**.

14.6.4 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 450)

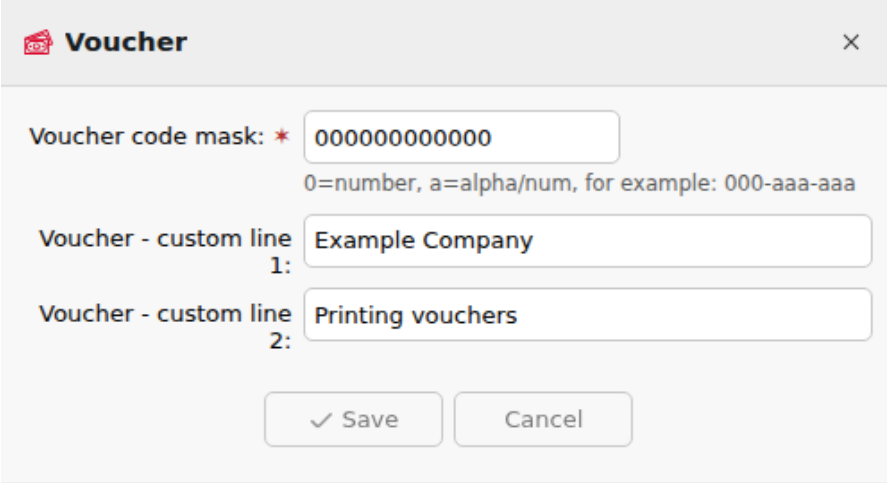
Setting the Voucher Format

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.



Remember 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. Go to **MyQ > Settings > Personalization**.
2. On the tab, under **Custom application logo**, click **+Add**, browse and upload the logo file.
3. Click **Save** .

   A preview of the new logo is displayed on the tab.

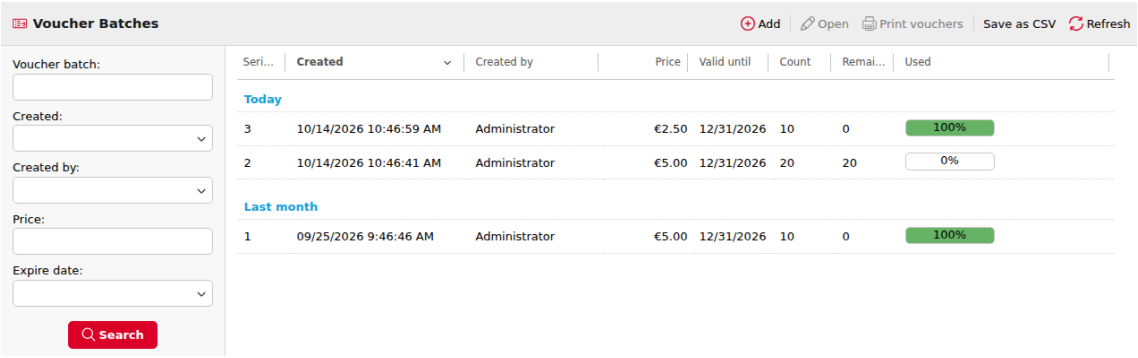
See also:

- Personalization Settings (see page 182)

Voucher Batches

Vouchers can be generated on the **Voucher Batches** tab of the MyQ Web Interface.

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.



Add a Voucher Batch

1. Go to **MyQ > Voucher Batches** and click **+Add**. The Add voucher batch dialog box appears.
2. 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. Double-click a voucher batch to view its usage.

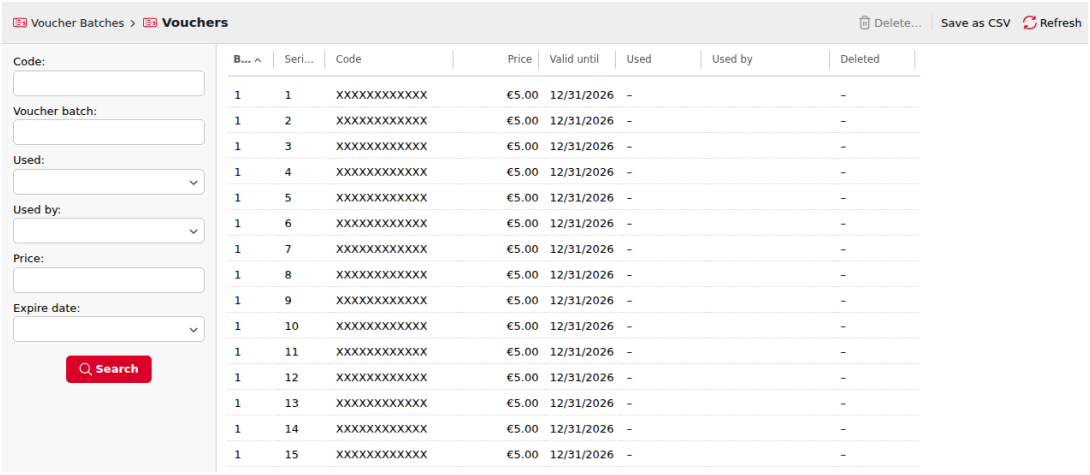
Vouchers Usage Overview

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.



14.6.5 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.

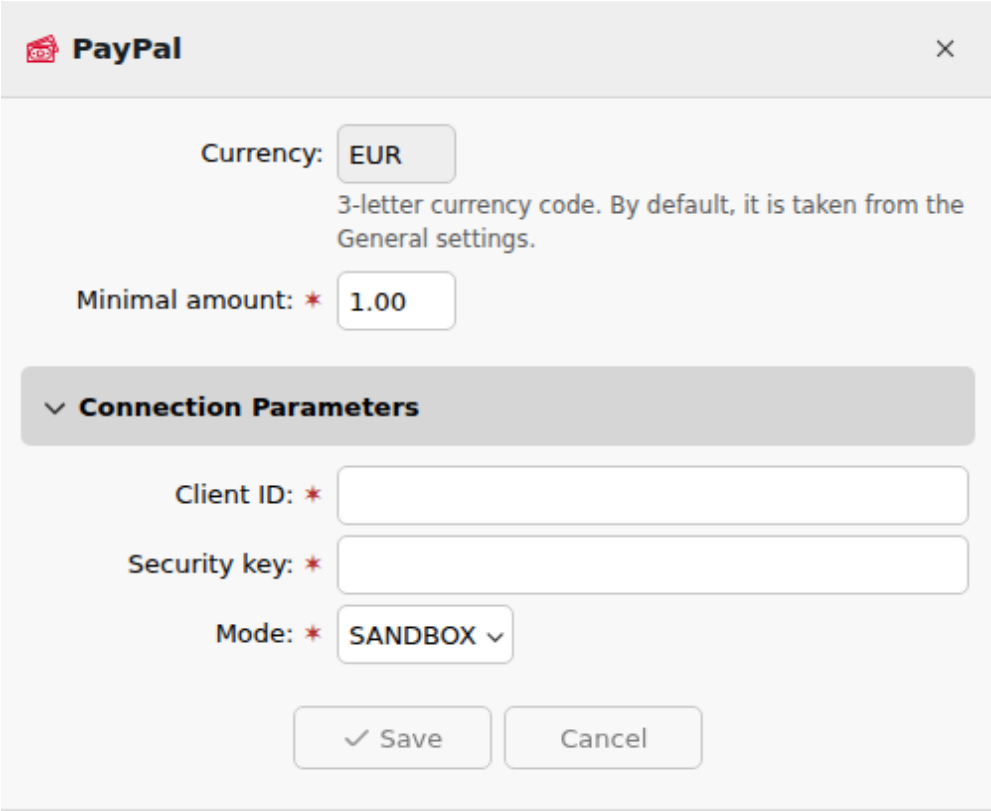
Setting Up PayPal Payments

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.

14.6.6 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.

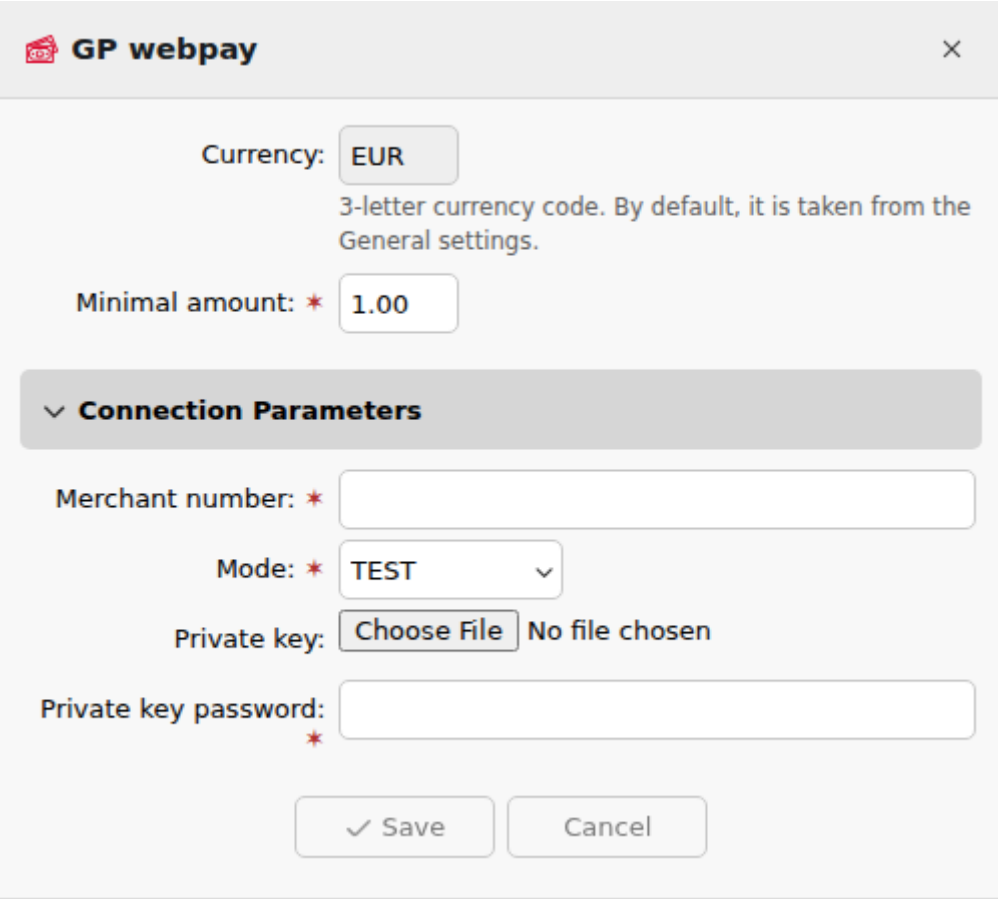
Setting Up GP webpay

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.

14.6.7 Recharging Credit via SnapScan

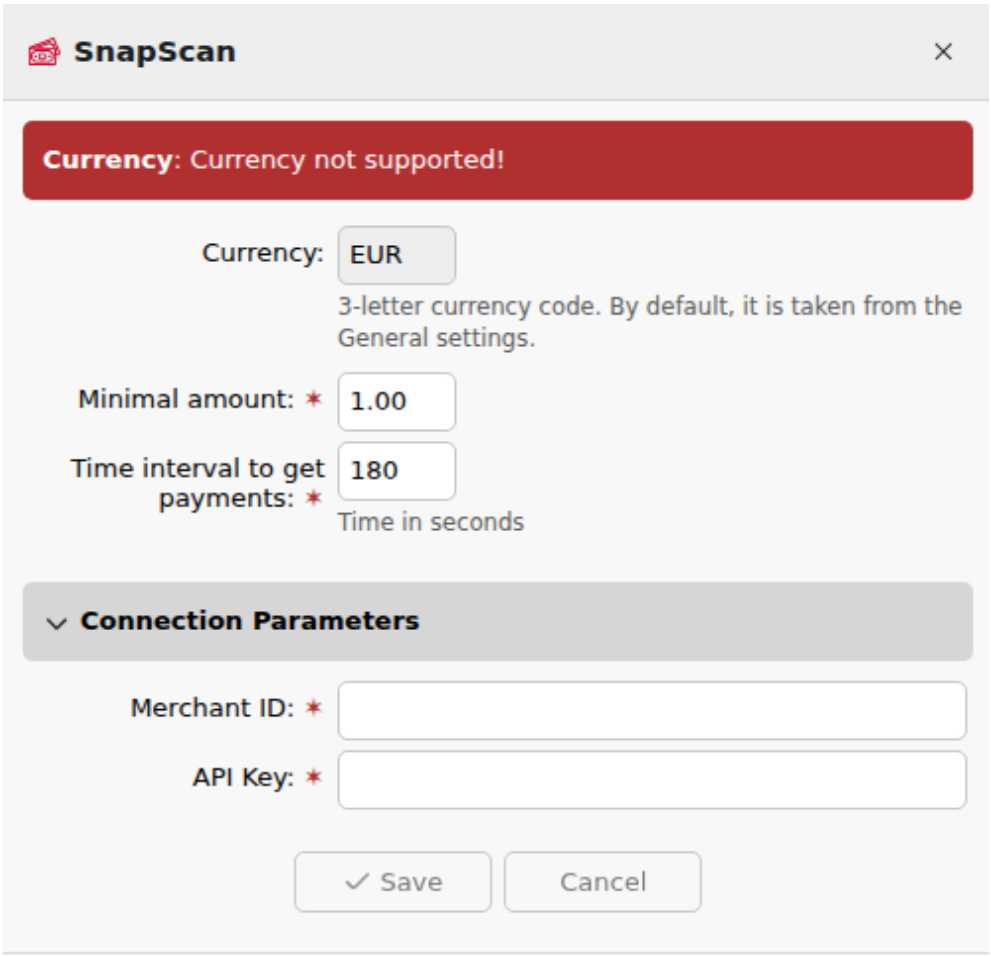
With the **SnapScan** app, users can pay for their MyQ credit via a QR code displayed in the app on their mobile phones.

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.

14.6.8 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.

See also:

- 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

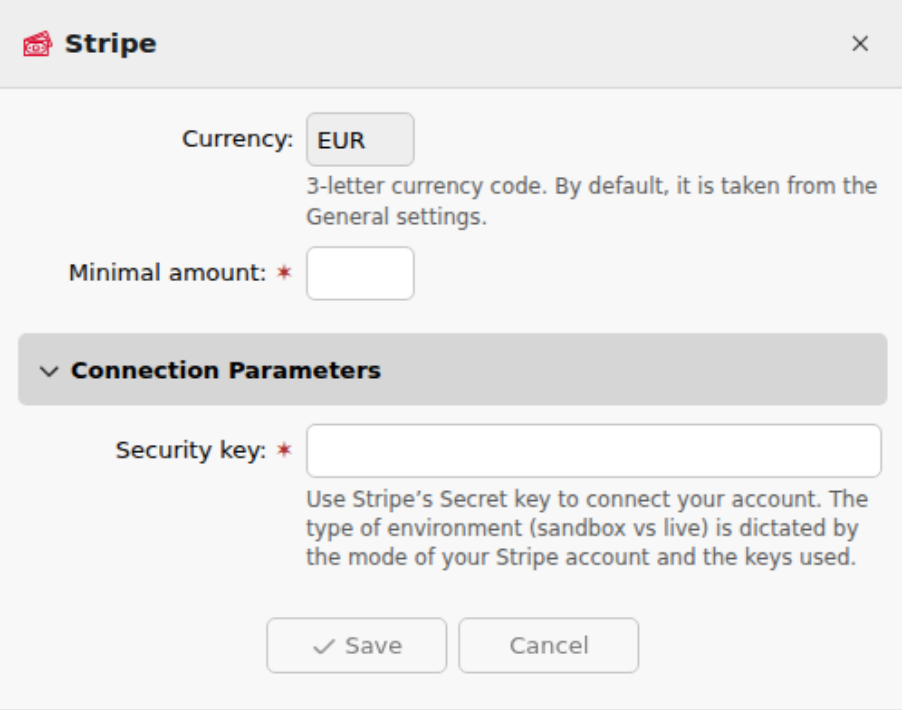
You generate a restricted key in your Stripe Dashboard.

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.

14.6.9 Credit Accounting Reports

On the **Reports** main tab, you can create, edit and generate two types of reports with information about credit:

- The **Credit balance** type of reports contains information about the actual state of the credit balances of the selected users (or members of the selected group). The data are ordered by user name.
- The **Credit operations** type of reports shows all changes of credit balance of the selected users (or members of the selected group) over a defined time period. It also contains information about the person who either spent or recharged the credit, the type of the recharge method and eventually about numbers of used credit vouchers. The data are ordered chronologically.

See also:

- Reports (see page 680)

14.7 Quotas

With the quota feature activated, you can set a limit to the usage of print related services. You can either limit the number of printed or scanned pages, or set an overall cost limit for all the services using prices from a price list. If the limit is close to be reached, the user or group receive an email with a warning and if the limit is reached or exceeded, they can be prevented from further printing and copying.

Each quota can monitor one of the following parameters:

- the total number of printed and copied pages
- the number of printed and copied color pages
- the total number of printed and copied monochrome pages
- the total number of scanned pages
- the overall cost of print services

Quotas are active permanently until disabled and they reset after the specified interval. Users can check their quota status on their web user interface and in the MyQ mobile application. If a printing device is equipped with an embedded terminal, users can see the current percentage of their quota status there.

The quota on overall cost of print services requires setting a price list with prices of particular functions (print/copy/scan – B&W/color) on each printer. Both types of quota (the quota on the number of pages and the quota on the overall cost) require using the Job parser to get the print job metadata (number of pages, color etc.).

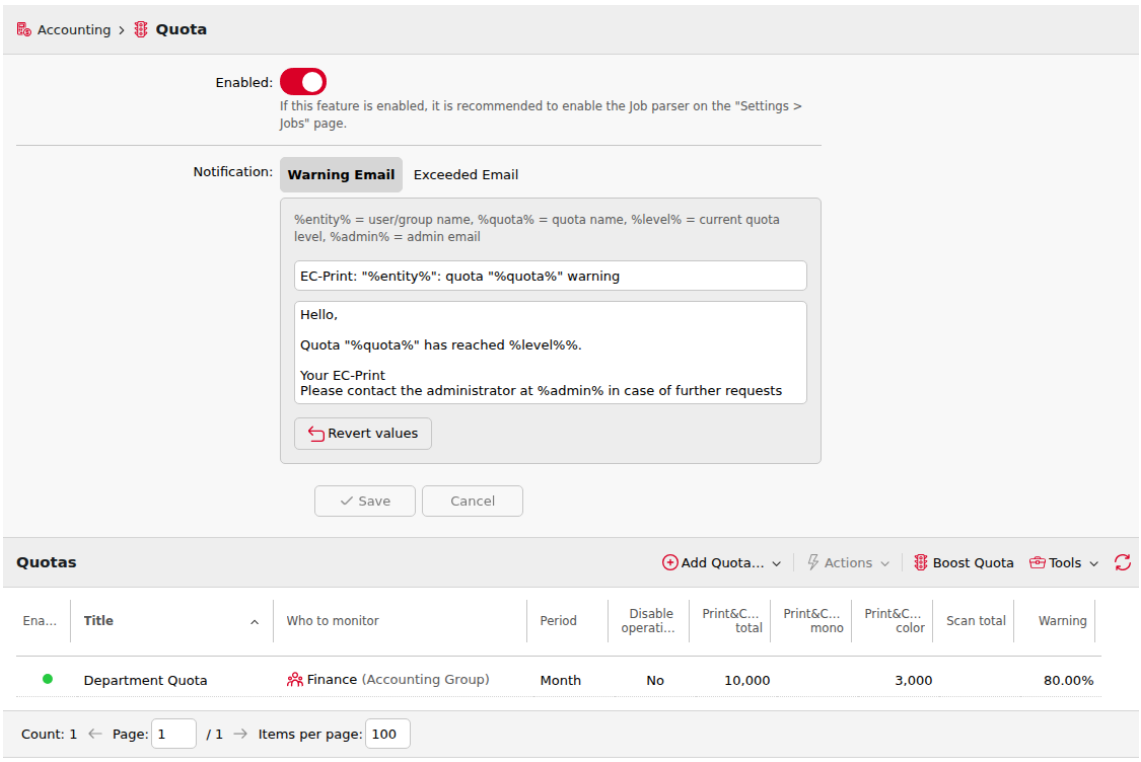
See also:

- Price Lists (see page 674)
- Job Parser (see page 590)

14.7.1 Activating and Setting Up Quotas

To enable the Quota feature, go to **MyQ > Settings > Quota** and select **Enabled** at the top of the **Quota** settings tab. Each quota can then be individually enabled or disabled on its properties panel.

In the **Warning Email** tab you can type the subject and the body of the email that is sent after reaching the preset warning (e.g. 80% of the quota) and, on the **Exceeded Email** tab, the subject and the body of the email that is sent when the limit of a user or group is reached or exceeded.



14.7.2 Creating Quotas

To add a new quota:

1. On the bar in the bottom section of the **Quota** settings tab, click **+Add Quota**.
2. Select if the quota should be applied to a **User**, **Members of a group**, or an **Accounting group**. The quota editing panel opens.
3. Enter the quota name, set its parameters, and click **Save**.

The new quota is enabled and appears on the **Quota** overview list.

A user can be assigned only one direct quota. This means you can create a quota specifically for an individual **User** and another for a broader category such as an **Accounting Group** or **Cost Center**. If the user belongs to an Accounting Group or Cost Center, they will inherit the shared quota assigned to that group. However, if a user already has an individual quota, it is not possible to assign them an additional quota through the **Members of Group** category if they are part of that group.
Example:
John is a member of the **Finance** group and has an individual printing quota (his **User** quota). In addition, they share a monthly printing limit assigned to their department through the **Accounting Group: Finance** quota. However, it is not possible to create a separate **Members of Group: Finance** quota, as this would result in John having two personal quota accounts, which is not allowed.

Bulk Quota Import Using CSV

A sample CSV file called `Quota_example` is available in `ProgramData\MyQ\Data\Import`, this CSV can be populated with relevant information and imported.

To create several quotas at once, import them using a CSV file. In Quota settings, go to **Tools** and select **Import**.

Set Counters and Limits with a Single Line

You can set a quota with multiple counters and limits for an entity using a single row. Separate them with the pipe character (|) and follow the same order in the counters and limits sections. For example:

```
NAME;MONITOR;ENTITY;COUNTER;PERIOD;LIMIT
QUOTA1;user;timcanterbury;mono|color|total|scan;day;20|30|50|10
```

This row creates four quotas for the user timcanterbury:

- Mono: 20 per day
- Color: 30 per day
- Total: 50 per day
- Scan: 10 per day

The information in the following table should be used to correctly format the CSV. Column order does not matter, and non-required columns can be omitted.

Column	Type	Required	Description
name	string	Yes	Name of quota
monitor	string • `user` • `group` • `members`	Yes	Who to monitor.
entity	string	Yes	User or Group When group used, full path must be specified. Example: `group level 1|target group`. Use same separator as for users import/export.

counter	Unique list of comma-separated values (at least one) from: • `cost` Costs • `mono` Print&Copy mono • `color` Print&Copy color • `total` Print&Copy total • `scan` Scan total	Yes	Monitored value. The number and order of values for `counter` must correspond to the values in `limit`. Examples: 1. Single value: `counter=cost` and `limit=50` 2. Multiple values: `counter=cost,color,scan` and `limit=50,20,200`
period	string • `week` • `month` • `quarter` • `half year` • `year` • `day` • `last x days`	Yes	Quota period.

period start	One number, two numbers with comma or time of day. Exact format depends on Quota period type.	No	Adjusting period start. Values and default values differs based on what Quota period is selected. **Day**: Time of the day, 00:00 - 23:59 or 00:00 - 11:59 am/pm. Examples: `00:00` (default), `09:08 AM`, `11:25`, `1:23pm`, `23:59`. **Week**: Day of the week 1 - 7. Examples: `1` = Monday (default), `7` = Sunday **Month**: Day of the month, 1 - 28, default is `1`. **Quarter**, **Half year** and **Year**: Two values divided by `,` (comma). • First number is day of the month, 1 - 28, default is `1`. • Second number is month, 1 - 12. Examples: `1` = January (default), `12` = December

			Last X days: How many days from “now” will be counted into quota, 1 - 365, default is 30.
limit	List of comma-separated positive numbers (at least one).	Yes	If `counter` is type `cost`, a decimal value can be used to represent a currency amount. In other cases, `limit` represents pages. The list of values in `limit` corresponds to the values in `counter`. Examples: 1. Single value: `counter=cost` and `limit=50` 2. Multiple values: `counter=cost,color,scan` and `limit=50,20,200`
enabled	`0` / `1`	No	Enable or disable quota Default: 1

warning	number (0 - 100)	No	Warning level. When quota reach this level, email is sent to the entity. Default: 80
disable operations	`0` / `1`	No	Enable or disable operations after quota is reached. Default: 0
valid from	date string	No	Determines from which day is the quota valid from in form of `YYYY-MM-DD`. Example: `2024-07-25`
terminate job	`0` / `1`	No	Terminate the current job when reached. Default: 0

warning recipients	List of recipients which can be username or email address, divided by comma `,`.	No	When warning level of quota is reached, these recipients will be notified by email. To send notification to current user who is triggering this notification, use `%MONITORED_USER%` placeholder. Available only if “who to monitor” type is “User” or “Members of a group”. Default: empty, not sending warning email to anyone.

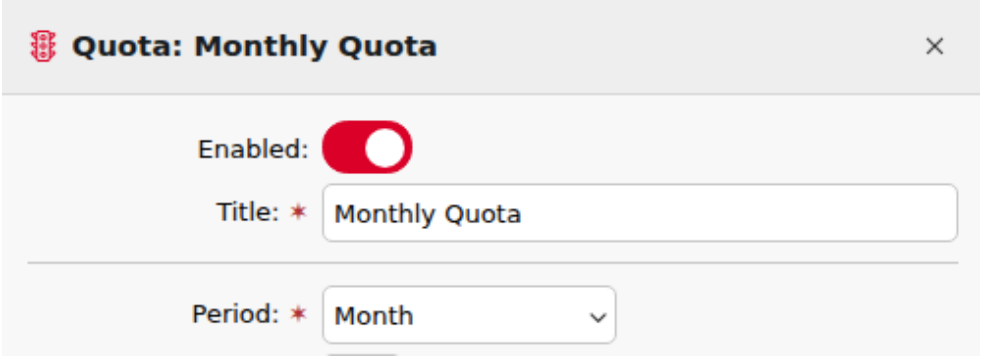
reached limit recipients	List of recipients which can be username or email address, divided by comma `,`.	No	When quota is reached, these recipients will be notified by email. To send notification to current user who is triggering this notification, use `%MONITORED_USER%` placeholder. Available only if "who to monitor" type is "User" or "Members of a group". Default: empty, not sending reached email to anyone.

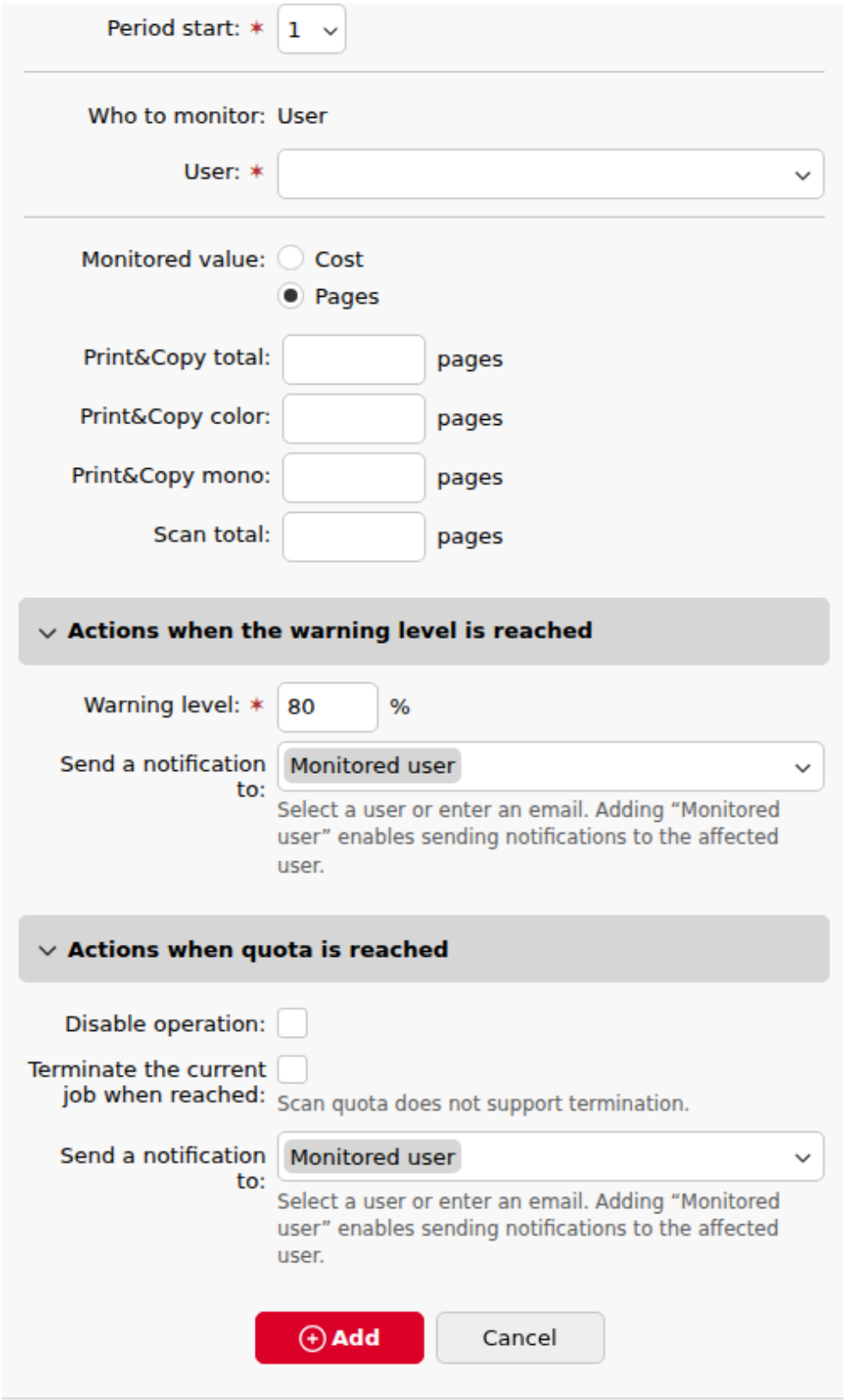
See also:

- Editing Quotas (see page 663)

14.7.3 Editing Quotas

The quota properties panel opens immediately after a new quota is created. To open an already existing quota, double-click on it on the list on the **Quota** main tab (**MyQ > Quota**). After you set the properties, click **Save** to submit the changes.





Each quota has the following set of properties:

Enable and Name the Quota

- Each quota is enabled by default. To disable or re-enable it, click the **Enabled** button.
- Enter the name in the **Title** text box.

Time Period

- In the **Period** list, select the reset period of the quota (*Day, Week, Month, Quarter, Half year, Year, Last X days*). The default period is *Month*. The *Last X days* period counts the number of pages or the overall cost over the last X days. For example, if the quota is 10 pages over three days and the user printed 5 pages the day before yesterday and two pages yesterday, they can print up to three pages today.
- In the **Period start** list, select the date when the period starts for the *Month, Quarter, Half year* and *Year* **Period**, day of the week for the *Week* **Period** or the number of days for the *Last X days* **Period**.
    - If you choose the *Day* **Period**, you must also set a time at the **Reset quota at** field.

Monitored Users or Groups

In this section you can specify the monitored **User**, **User Group**, or **Accounting Group**, based on the selection you made when creating the quota.

Monitored Value

- If you select *Cost* as the **Monitored value**, the quota is counted in amount of money spent.
    - Set the quota cost **Limit**
- If you select *Pages* as the **Monitored value**, the quota is counted in the amount of printed, copied and/or scanned pages.
    - Set the **Print&Copy total, Print&Copy color, Print&Copy mono** (supported by terminals 8.1 or newer) and **Scan total** in pages.



If the monitored value is set to 0, this operation is effectively disabled for this quota. For example, if the **Print&Copy color pages** value is set to **0**, no color pages can be printed or copied within this quota. Correspondingly, no email notifications will be sent stating that this quota limit is reached.

Actions Taken When the Warning Level Is Reached

- Enter the warning level (in %) in the **Warning level** text box.

- Select the user/s, user group/s, or accounting group/s you want to be notified when the **Warning level** is reached in the **Send a notification to** combo box. You can also type an email address to notify into this box. By default, this is the **Monitored User**.

Actions Taken When the Quota Is Reached

- You can disable one or more operations after the quota is reached or exceeded.
    - If the **Monitored value** is *Cost*, select them under **Disable operations**. The options are **Print, Copy, Color print** (on terminals 8.1 or newer), **Color copy** (on terminals 8.1 or newer), and **Scan**.
    - If the **Monitored value** is *Pages*, mark the **Disable operation** checkbox and the operation that has reached the limit will be disabled.
- Mark the **Terminate the current job when reached** checkbox if you want to interrupt the current job when the quota is reached. If both **Disable operation** and **Terminate the current job when reached** are checked, the job will be interrupted when the quota is reached, and the user will be redirected to the MyQ home screen. If **Disable operation** is checked and **Terminate the current job when reached** is not, the current job will be finished, and the user will be redirected to the MyQ home screen.
    - The action is not supported in scan quotas.
- If you want to notify someone after the quota is reached, select the user/s, user group/s, or accounting group/s in the **Send a notification to** combo box. You can also type an email address to notify into this box. By default, this is the **Monitored User**.

14.7.4 Boosting Quotas

In situations when a user or an accounting group have reached their quota and urgently need to print, you can boost the quota by a specific number of pages or by a specific amount. Quotas can be boosted on two tabs of the MyQ Web Interface: the **Quota Boosts** main tab and the **Users** main tab. Records of the boosted quotas appear on the boost quota records list on the **Quota Boosts** main tab.

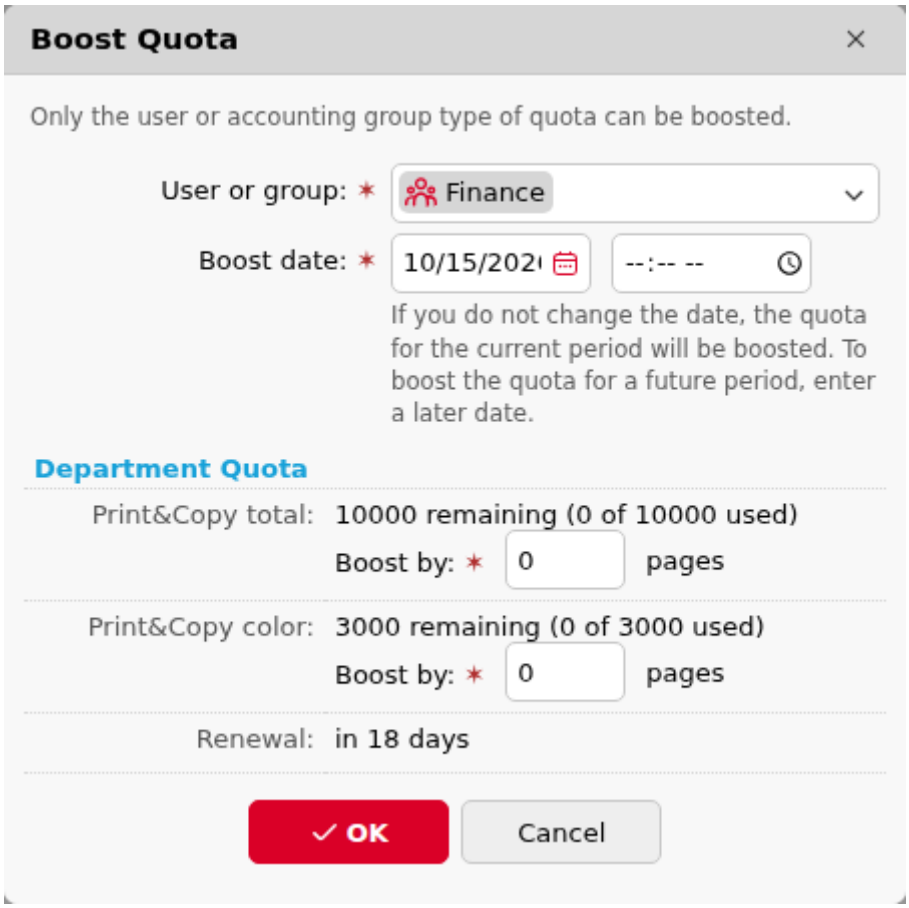
You can create Quota Boosts for the following quota types:

- User
- Accounting Group

Boosting Quotas on the Quota Boosts Main Tab

On the MyQ Web Interface, go to **MyQ > Quota Boosts**. To boost a quota here:

1. On the bar at the top of the tab, click **+Add**. The Boost quota dialog box appears.
2. Select the **User or group** and the **Boost date**, and then click **OK**. The Boost quota dialog box extends – more sections are displayed. The first of the new sections shows the current availability of operations and the rest show the quotas applied to the user (or groups of users).
3. Enter the number of pages or the amount of money to the **Boost By** text box in the particular quotas sections (each quota has to be boosted separately), and then click **OK**.



Boosting Quota of a Particular User on the Users Main Tab

On the MyQ Web Interface, go to **MyQ > Users**. To boost a quota here:

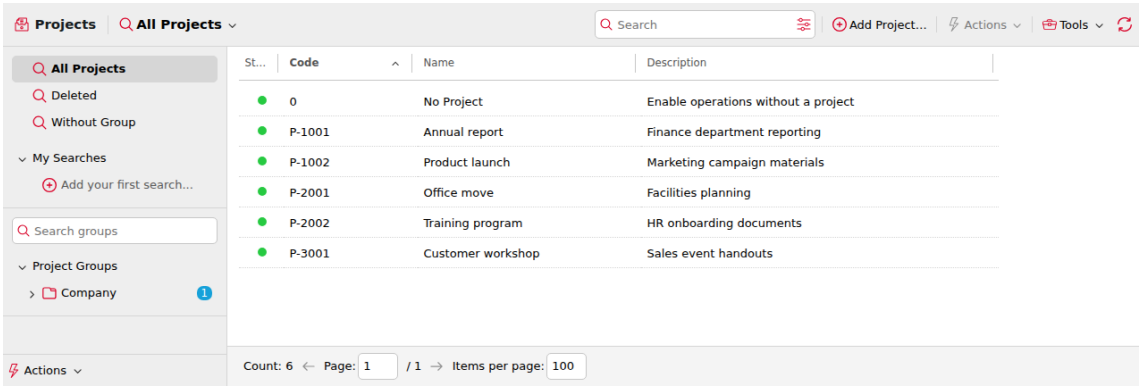
1. On the tab, select the user, click **Actions**, and then click **Boost quota** in the drop-down (or right-click the user, and then click **Boost quota** on the shortcut menu). The Boost quota dialog box appears with the user selected in the **User or group** drop-down.

2. Enter the number of pages or the amount of money to the **Boost By** text box in the particular quota sections (each quota has to be boosted separately), and then click **OK**.

The administrator can also release blocked quota for a user by clicking **Actions** and then clicking **Release blocked quota** (or by right-clicking the user and selecting **Release blocked quota**).

14.8 Projects

With the project accounting feature activated, users can assign print, copy, and scan jobs to particular projects and consequently distribute the print cost among the projects and charge it appropriately. Project accounting can also be used as another independent level of internal accounting in addition to devices, users, and groups. Projects can be manually created on the MyQ web interface or imported from a CSV file. They can be assigned to print jobs in the MyQ Desktop Client pop-up window, on the MyQ web interface, on an embedded terminal, on a touch panel of a HW terminal, or in the MyQ X Mobile Client app.



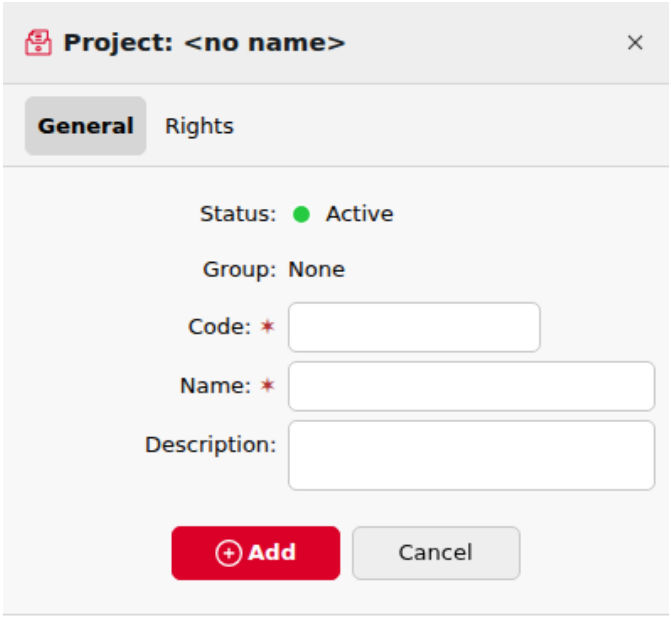
14.8.1 Enable Projects

Go to **MyQ > Settings > Projects** to enable or disable projects, and change the global settings of the projects feature.

- Select **Enabled** to globally activate project accounting
- **Scan without project**: Select this option to let users scan directly. To require users to select a project, leave this option unselected.

14.8.2 Creating Projects

You add new projects in the **Projects** tab.



1. Go to **MyQ > Projects** and click **+Add project**. The new project properties panel opens.
2. On the **General** tab, enter the following:
   - **Code**: a unique code for the project
   - **Name:** a name to identify the project
   - **Description**: add an optional description.
3. Click **Add** or **Save**.
4. Click on the **Rights** tab, to manage user rights to the project (all users have rights to a project by default). On the bar at the top of the **Rights** tab, click **+Add User**. The Select user or group dialog box appears, where you can select the user (or group of users) that you want to provide with rights to the project, and then click **OK**. To remove the rights from a user, select the user and click the trash can button.

14.8.3 Managing Projects

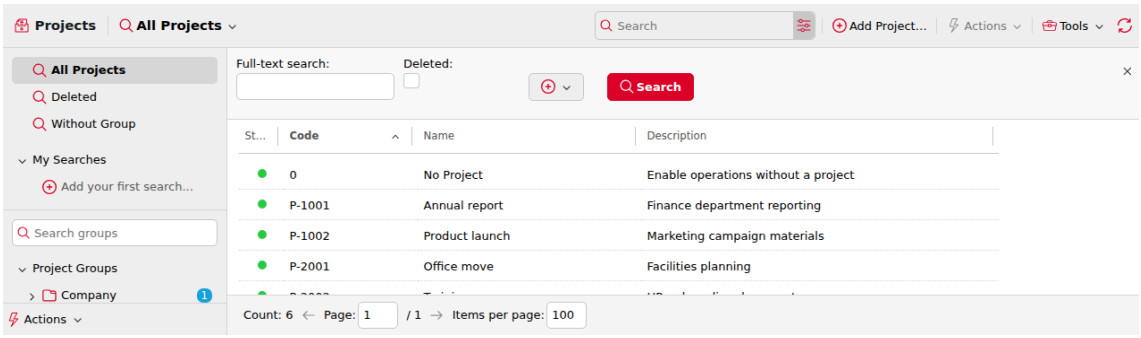
After the projects are created, you can see them listed on the **Projects** main tab. Using the buttons on the bar at the top of the tab, you can add new projects, edit current projects, import projects from CSV files and display/hide deleted projects.

Searching Projects

You can use the search function to easily find particular projects:

- **Full-text search** allows you to search a project's name or description.
- **Deleted** specifies whether or not deleted projects will be included.

- **Group** allows you to limit the search to projects in a particular group.
- **Has group** restricts the search to projects that have been added to any group.



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.
3. 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.

Restoring Deleted Projects

1. Click **Deleted** projects in the left-hand panel.
2. Right-click the project and select **Restore**.

Managing Project Groups

For convenience, you can manage projects in groups, for example on a functional or geographical level. The maximum is five levels deep. Rights set on the group level will automatically be inherited by sub-groups and/or the projects inside these groups.

It is then possible to set specific rights to sub-groups or specific projects. After saving these rights they will not be overwritten by the default group rights.

Creating Groups

1. Right-click **Project groups** and select **Add Project Group**.
2. Set the **Name** of the group and click **Add**.

Adding a Project to a Group

1. Select the group that you want to add a project to.
2. Click **Add Project** on the menu bar.
3. Enter the project details and click **Add**.

14.8.4 Importing Projects

To add multiple projects to MyQ at once, import a CSV file. You can import projects manually and as a scheduled task.

> See the sample `Projects_example` in `ProgramData\MyQ\Data\Import`. Use this file as a template to prepare data for import.

You can import projects with a hierarchy.

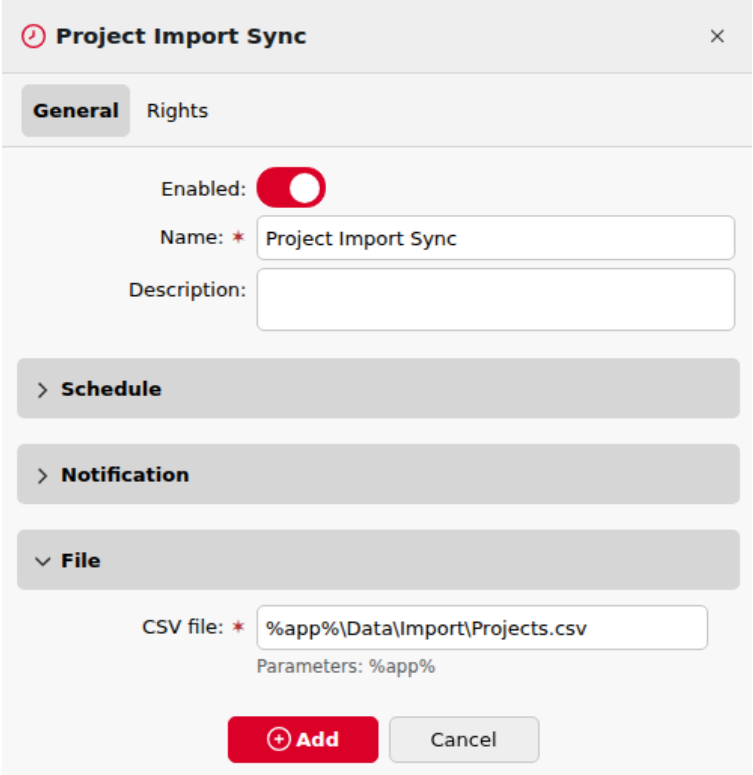
Within the CSV import, new projects are added and existing projects are updated. Projects already present in MyQ that are not listed in the CSV file are left untouched. Each project is recognized by the value of its code and updated only if the CSV file contains a row with the same code.

Import Projects Manually

On the **Projects** main tab, click **Tools**, and select **Import**. The Import dialog box appears. Click **Choose File** and select the CSV file, and then click **OK**. After the import is done, imported projects are listed on the **Projects** main tab. An information message appears at the top of the tab. By clicking log for details, you can display the import log.

Any errors occurring during the import can be related to incorrect syntax or non-existing users or group of users listed in the CSV file.

Import Projects with a Scheduled Task



1. Go to **MyQ > Settings > Task Scheduler**, click **+Add**, and then **Import projects from CSV**. The properties panel of the new schedule opens on the right side of the screen.
2. On the panel, set up the schedule.
3. In the **File** section, add the path to the **CSV file** (the file should be stored on the MyQ server).
4. Click **Save**.

See also: Task Scheduler Settings (see page 191)

CSV File Syntax

Each row must consist of six columns, separated by the delimiter set on the **General** settings tab, under **Column delimiter in CSV**. The file must contain a header row, otherwise an error occurs and the projects will not be imported. The order of the columns is irrelevant; each column is identified by its name in the header, which must always be in English, regardless of the language setting in MyQ.

Values:

- **active:**

    - 1=project is added to MyQ
    - 0 =project is added to MyQ as deleted.
- **code:** unique code of the project
- **name:** name of the project
- **groups:** the path of the project in the hierarchy. Levels must be separated by the pipe character (|). If the column is empty, the project is created in or moved to the root of the hierarchy.
- **description:** internal description of the project
- **users** the users or groups of users allowed to use the project. Multiple entries should be separated by commas (,).

14.8.5 Assigning Projects to Print Jobs

If project accounting is enabled, unassigned print jobs are paused and have to be assigned to a project before they can be printed. They are displayed on the **Jobs** main tab, under **Paused**. You can assign them on the **Jobs** main tab, in the MyQ Desktop Client pop-up window, or on an embedded terminal.

Users who want to print an unassigned job on an embedded terminal have to select one of their projects (projects they have rights to) or eventually select the **Without project** option there (if they are allowed to print without projects). The same applies to scanning and copying – users have to select one of the projects or the **Without project** option before opening the particular panel or performing a quick action. The exact behavior of project accounting on embedded terminals can vary depending on vendor and device model. See the particular embedded terminal manual for further information.

Assigning Projects to Print Jobs

This option is available on computers with either Windows or macOS. It requires the MyQ Desktop Client application running on the computer where the print job is sent from.

MyQ Desktop Client is running in the background and, unless Project accounting or any other features of the application are active for the logged user, all print jobs are sent to MyQ without any intervention. Once the user has rights to more than one projects, all the jobs that they send are paused and the MyQ Desktop Client pop-up window opens to offer the available projects to the user. If only one project is available to the user, it is automatically assigned, and the job is sent to the server.

The user can assign the job to an available project and print within that project. If printing without a project is allowed in MyQ, the user can select the **No project** option; otherwise they have to select one of the available projects. If there are more jobs waiting in the queue, the user can check the ones to be printed to a particular project and jobs for another project can be printed in the next step.

See also: (10.2) MyQ Desktop Client

Assigning Projects on the Jobs Main Tab

To assign a project to a print job:

1. On the **Paused** list on the **Jobs** main tab, double-click the print job that you want to assign the project to. The print properties panel opens on the right side of the screen.
2. On the panel, select the **Project** that you want to assign to the job, and then click **Save**.

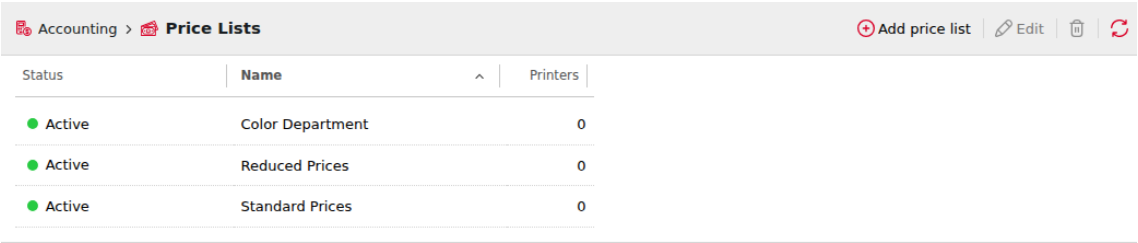
14.9 Price Lists

On the **Price Lists** settings tab, you can create price lists and attach them to configuration profiles. Price lists are used to assess the price of each printing device operation. That is necessary for monetary accounting and MyQ advanced features such as credit accounting and monetary quotas.

> ⚠ MyQ uses price lists to estimate the cost of each job and, depending on the user's credit balance or quota, the job is released or denied.
> When a user prints a page range, MyQ cannot precisely calculate the number of color and B&W pages because it parses the entire job rather than the selected page range. Therefore, MyQ assumes that **all pages in the selected range are color**, and the remainder are B&W.

You can also set discounts or increase the price of print, copy, scan and fax services for particular users and groups.

To open the **Price Lists** settings tab, go to **MyQ > Settings > Price Lists**.

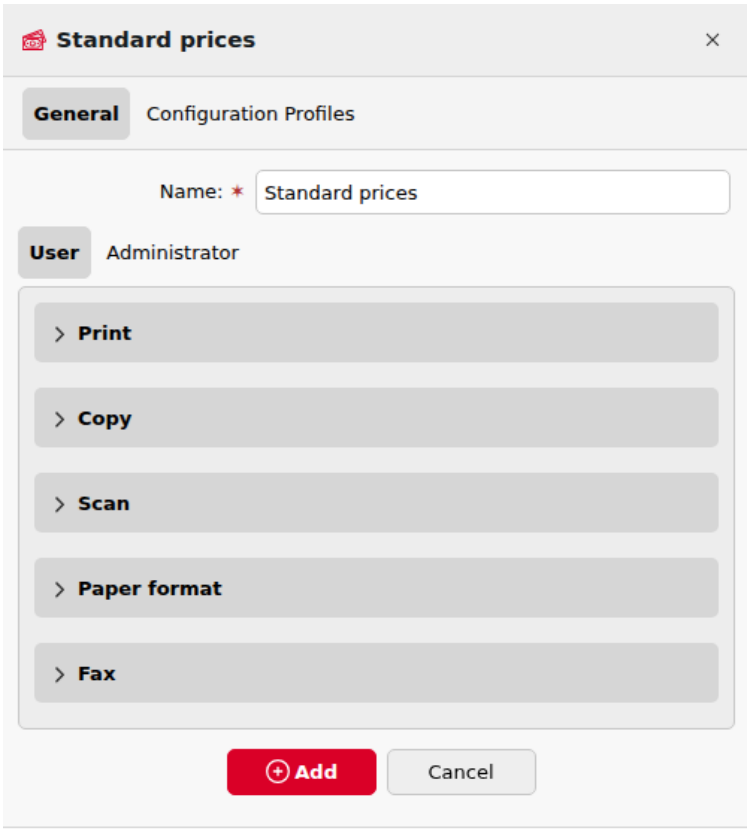


14.9.1 Adding Price Lists

1. On the bar at the top of the **Price Lists** settings tab, click **+Add price list**. The new price list properties panel opens on the right side of the screen.
2. On the panel, enter the price list name.
3. Set up the price list.
4. Click **Save**.

14.9.2 Editing Price Lists

On the properties panel of the price list, you can rename the price list, define prices of print, copy, scan and fax services and attach the price list to printing devices. To open the panel, double-click the price list on the list of price lists on the **Price Lists** settings tab.



Setting Prices of Print, Copy, Scan and Fax Services

On the **General** tab of the price list's properties panel, you can set prices of print, copy, scan, paper format, and fax services. There are two sub-tabs: the **User** sub-tab, where you set prices for MyQ users, and the **Administrator** sub-tab, where you set prices for the MyQ administrator.

- **Print:** In this section, you can set the price per printed page for monochrome and full-color print. Some printing devices allow pricing according to coverage of paper. You can set prices for three states of coverage: **Low**, **Medium** and **High**.
- **Copy:** In this section, you can set the price per copied page for monochrome, full color and single color copying. Some printing devices allow pricing by coverage of paper. You can set prices for three states of coverage: **Low**, **Medium** and **High**.
- **Scan:** In this section, you can set the price per scanned page.
- **Paper format**: In this section, you can set the price per sheet for different paper formats.
- **Fax:** In this section, you can set the price per printed faxed page.

Some printing devices lack the counters necessary for obtaining information about some parameters, for example information about paper size. Those parameters are not counted in the final price of jobs that are carried out on these machines.

Whenever the price list is updated (its parameters values are changed and the price list is saved), a new price list is created. Pages printed with the previous version of the price list are counted according to the old settings.

Coverage Accounting

The coverage of a print job cannot be calculated by the job parser in advance; therefore, all print job pages are regarded as having **High** coverage before the release of the print job.

After the job is printed, the actual toner coverage is calculated by the machine and correctly accounted. Credit is deducted based on the real coverage accounting provided by the printer after the job is printed.

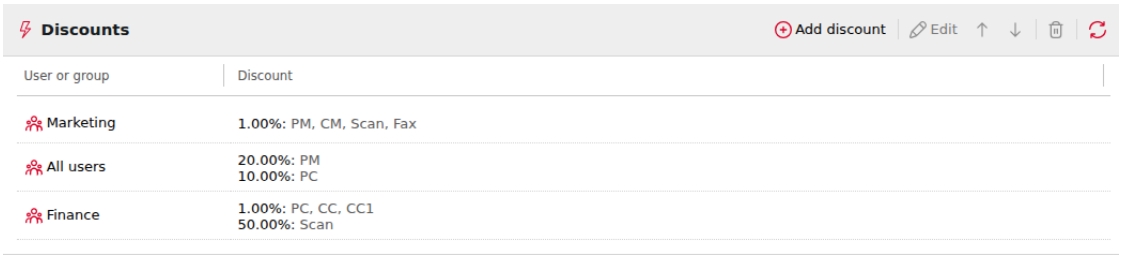
This may cause situations where a user has enough credit to print a job (for example, that has **Low** coverage on all pages) but won't be allowed because the system calculated the price before job release as **High** coverage.

14.9.3 Using Discounts

The prices set in price lists are applied to all users and groups without any distinction. To distinguish between particular users and groups, you can provide the users and groups with discounts, or increase the prices in the list for them.

The discounts are set in percent and are applied to all price lists. Within the discount, you can set a particular value for each print, copy, scan or fax price lists' item. The price of an action is increased by setting a negative discount for the item, for example a *-15%* discount.

The **Discounts** section, where the discounts are set, is also part of the **Price Lists** settings tab.



Creating a New Discount

1. Click **+Add discount** at the upper-left corner of the **Discounts** section. The new discount properties panel appears on the right side of the screen.
2. Set the discount.
3. Click **OK** to save it.

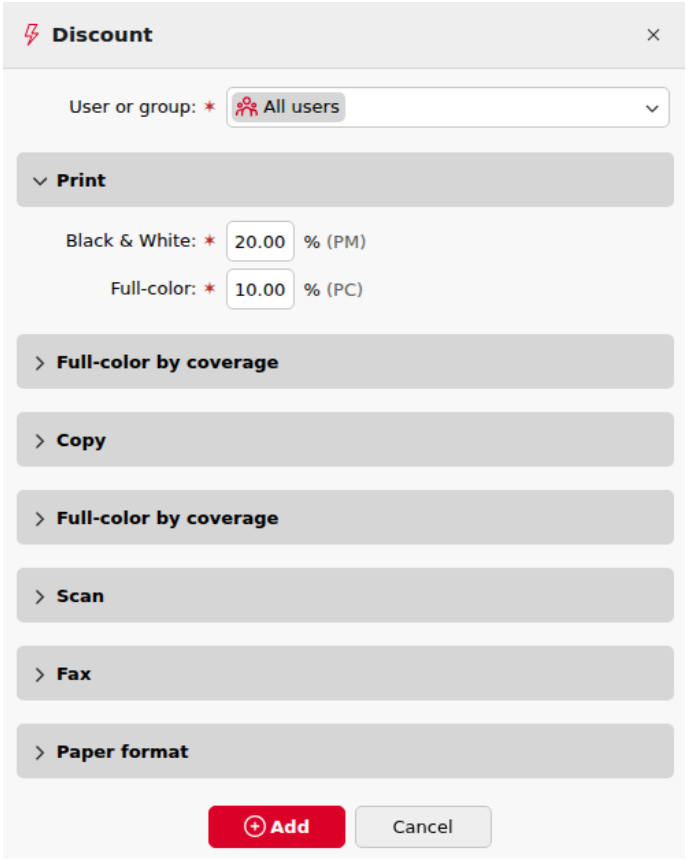
Editing a Discount

To open the editing options of a discount, double-click the discount (or right-click the discount, and then click **Edit** on the shortcut menu, or select the discount and click **Edit**). The discount's properties panel appears on the right side of the screen.

For each discount, you need to set the user or group that it will be applied to, and the values of each item (such as B&W print or Full-color copy) of the discount in percent.

To increase the price of an item, set the discount to a negative number (such as *-15%*).

After the discount is set, click **OK** to save it.



Deleting a Discount

1. Select the discount.
2. Click the the trash can, or right-click and select **Delete**.

14.9.4 Assigning Price Lists to Devices

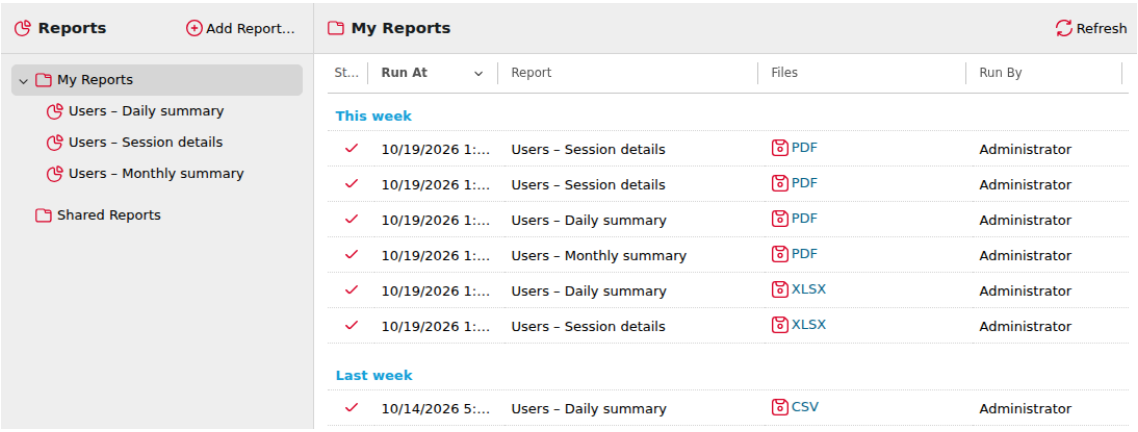
1. On the list of price lists on the **Price Lists** settings tab, double-click the price list. The new price list properties panel opens on the right side of the window.
2. Go to the **Configuration Profiles** tab.
3. Click **+Add**. The Select Configuration Profile window opens.
4. In the dialog box, select the configuration profile that you want to attach the price list to.
5. Click **OK**. The configuration profile appears on the printing devices list on the **Printers** tab.

You can also attach a price list to a configuration profile when you go to **Settings, Configuration Profiles**. In the overview, double-click a profile and change the **Price List** in the right pane on the window.

You cannot attach more than one price lists to a single configuration profile. If you add a price list to a configuration profile that already has a different price list attached to it, the old price list is replaced by the new one.

15 Reports

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*).

15.1 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.

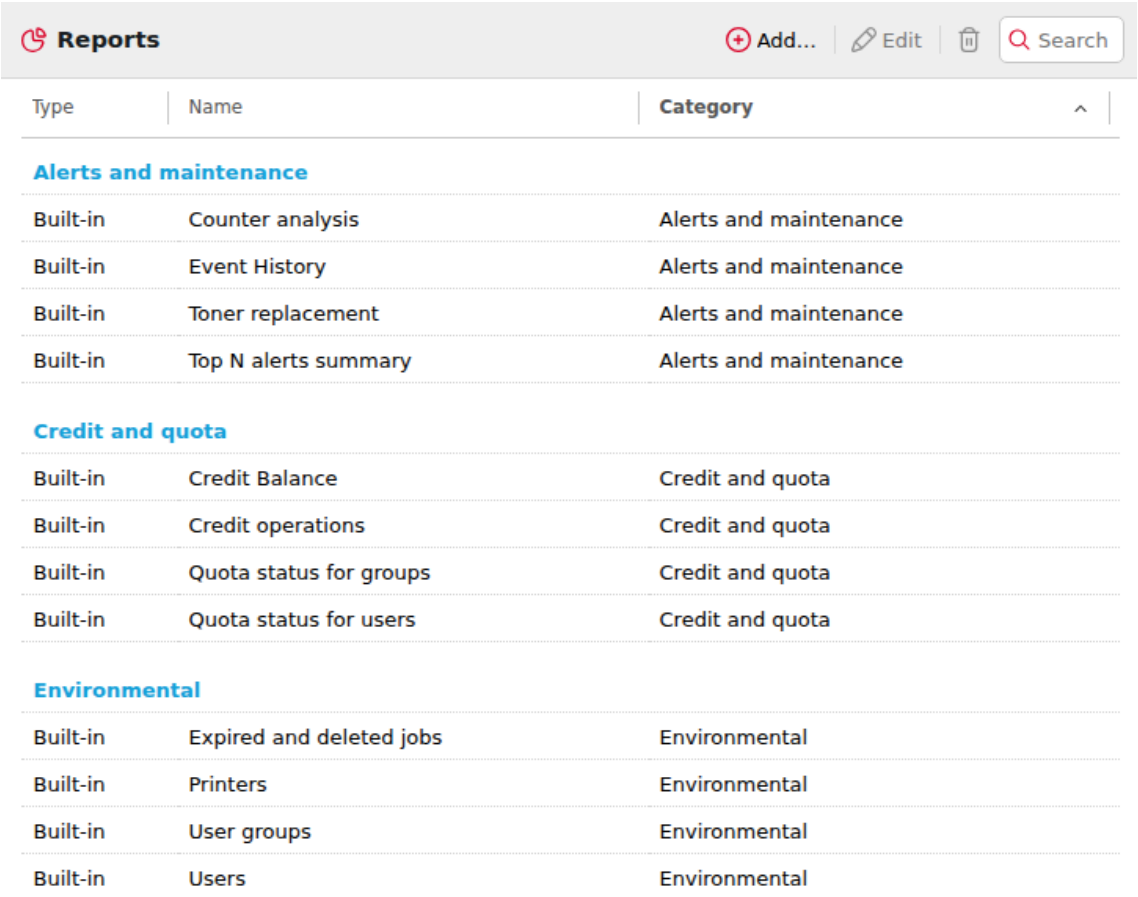
See also:

- Personalization Settings (see page 182)

15.2 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 of all 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

15.2.1 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.

15.2.2 Report Categories

Each category below lists its reports in a table. In the tables:

- **Charts**: *Yes* means that charts are available for the report.

- **Aggregated Columns**: *Yes* means that the report supports aggregated columns.
- **Job Privacy**: *Not available* means that the report is not available when Job Privacy is enabled. *Excludes user data* means that the report can be used when Job Privacy is enabled, but it excludes user-specific information.
- In the *Counters by Function* reports, 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.

Alerts and Maintenance Reports

Alerts and Maintenance reports provide information about device alerts and unusual changes on device counters.

Report	Description	Charts	Aggregated Columns	Job Privacy
Counter Analysis	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.			Not available
Event History	Occurrence of predefined device errors and alerts. It only shows alerts that are turned on in **Settings** > **Events** in the MyQ Web UI.			

Report	Description	Charts	Aggregated Columns	Job Privacy
Toner Replacement	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	Most common errors and alerts. The number of alerts shown can be customized.	Yes		

Credit and Quota Reports

Credit and Quota reports contain information about credit and quota usage, for example the remaining credit balances or the state of quota of selected users.

Report	Description	Charts	Aggregated Columns	Job Privacy
Credit Balance	Current Credit balance.			
Credit Operations	List of credit transactions (top-up and spent).			

Report	Description	Charts	Aggregated Columns	Job Privacy
Quota Status for Groups	All of the accounting/cost center group quotas.			
Quota Status for Users	User-based quotas usage and settings.			

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.

Report	Description	Charts	Aggregated Columns	Job Privacy
Expired and Deleted Jobs	List of expired/deleted jobs and the environmental impact of not printing them. They are sorted by print queue.			Excludes user data
Printers	Environmental impact of each printer.			
User Groups	Environmental impact of each User Group.			
Users	Environmental impact of each User.			Not available

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.

Report	Description	Charts	Aggregated Columns	Job Privacy
Day of the Week	Output volume by day of the week.	Yes		
Hourly Activity	Output volume by time of day.	Yes		
Monthly Statistics	Output volume by month.	Yes		
Price List Comparison	Price lists applied to various printer groups.			
Weekly Statistics	Output volume by week.	Yes		

Groups Reports

Groups reports contain information about group membership, printed pages, weekly stats etc.

Report	Description	Charts	Aggregated Columns	Job Privacy
Counters by Function and Duplex (BETA)	Counters per group by print/copy, color, and duplex.			Not available
Counters by Function and Paper Format (BETA)	Counters per group by print/copy, color, and paper format.			Not available
Counters by Function Paper Format and Duplex (BETA)	Counters per group by color, duplex, and paper format.			Not available

Report	Description	Charts	Aggregated Columns	Job Privacy
Daily Summary	Summary of the daily output by group.			
Day of the Week	Summary of the daily output based on the day of the week by group.			
Monthly Summary	Summary of the monthly output by group.		Yes	
Top N	Groups sorted by largest output volume. 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**.	Yes		
Total Summary	Total output volume per group for a predefined period.		Yes	Not available
User Group Membership	List of members of the group and their membership options.			Not available

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.

Report	Description	Charts	Aggregated Columns	Job Privacy
Daily Summary	List of print jobs printed by user on a daily basis.			Not available
Expired and Deleted Jobs	List of expired and deleted jobs.		Yes	Not available
Favorite Jobs	List of user's favorite jobs.			Not available
Printed Jobs Summary	List of all the print jobs printed by the user for a predefined period.			Not available

Printers Reports

The following reports are included in the **Printers** category:

Report	Description	Charts	Aggregated Columns	Job Privacy
Counters by Function and Duplex (BETA)	Counters per device by print/copy, color, and duplex.			Not available
Counters by Function and Paper Format (BETA)	Counters per device by print/copy, color, and paper format.			Not available
Counters by Function Paper Format and Duplex (BETA)	Counters per device by color, duplex, and paper format.			Not available

Report	Description	Charts	Aggregated Columns	Job Privacy
Daily Summary	List of print jobs printed by device on a daily basis.		Yes	
Day of the Week	Summary of the daily output based on the day of the week by device.		Yes	
Meter Reading via SNMP	Device's total output volume. This report (unlike the rest of MyQ reports) includes accounting data of the jobs bypassing MyQ server.			
Monthly Summary	Summary of the monthly output by device.			
Top N	Printers sorted by largest output volume.	Yes		
Total Summary	Total output volume per printer for a predefined period.		Yes	Not available

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.

Report	Description	Charts	Aggregated Columns	Job Privacy
Counters by Function and Duplex (BETA)	Counters per project by print/copy, color, and duplex.			Not available

Report	Description	Charts	Aggregated Columns	Job Privacy
Counters by Function and Paper Format (BETA)	Counters per project by print/copy, color, and paper format.			Not available
Counters by Function Paper Format and Duplex (BETA)	Counters per project by color, duplex, and paper format.			Not available
Daily Summary	List of print jobs printed by project on a daily basis.		Yes	
Day of the Week	Summary of the daily output based on the day of the week by project.		Yes	
Monthly Summary	Summary of the monthly output by project.		Yes	
Print Jobs per Project	List of print jobs assigned to each project.			Not available
Project Groups Total Summary	Total output volume per project for a predefined period.			
Projects per User	Output volume per user and project. The data is grouped by user.		Yes	Not available
Top N	Projects sorted by largest output volume.	Yes		
User Project Assignment	List of projects assigned to each user.			Not available

Report	Description	Charts	Aggregated Columns	Job Privacy
Users per Project	Members of each project.		Yes	
User Session Details	List of all the user's interactions on the device sorted by project.		Yes	Not available

Users Reports

Users reports can contain various information about users, print jobs, credit statements, printed pages, and more.

Report	Description	Charts	Aggregated Columns	Job Privacy
Counters by Function and Duplex (BETA)	Counters per user by print/copy, color, and duplex.			Not available
Counters by Function and Paper Format (BETA)	Counters per user by print/copy, color, and paper format.			Not available
Counters by Function Paper Format and Duplex (BETA)	Counters per user by color, duplex, and paper format.			Not available
Daily Summary	List of print jobs printed by user on a daily basis.			Not available
Day of the Week	Summary of the daily output based on the day of the week by user.			Not available

Report	Description	Charts	Aggregated Columns	Job Privacy
Monthly Summary	Summary of the monthly output by user.			Not available
Session Details	List of all user's interactions on the device.			Not available
Top N	Users, sorted by largest output volume.	Yes		Not available
Total Summary	Total output volume per user for a predefined period.			Not available
User Rights	List of users with enhanced access rights.			Not available

15.3 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, the MyQ Print Server does accounting via SNMP, based on the data the device provides.

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.

15.4 Creating Reports

15.4.1 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.

15.4.2 Editing a Report

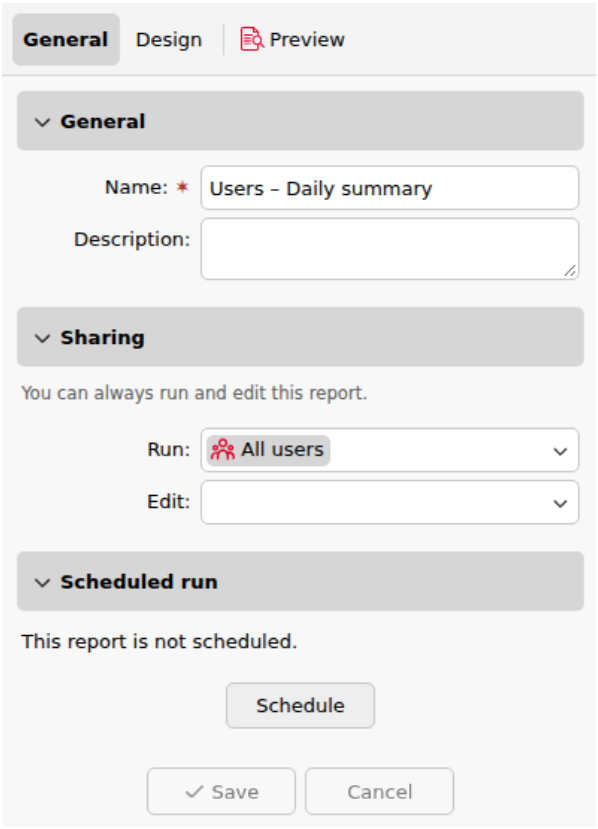
To edit a report, go to **MyQ > Reports**, click the three-dot menu for the report you want to schedule, and select **Edit**. The report opens in edit mode.

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.

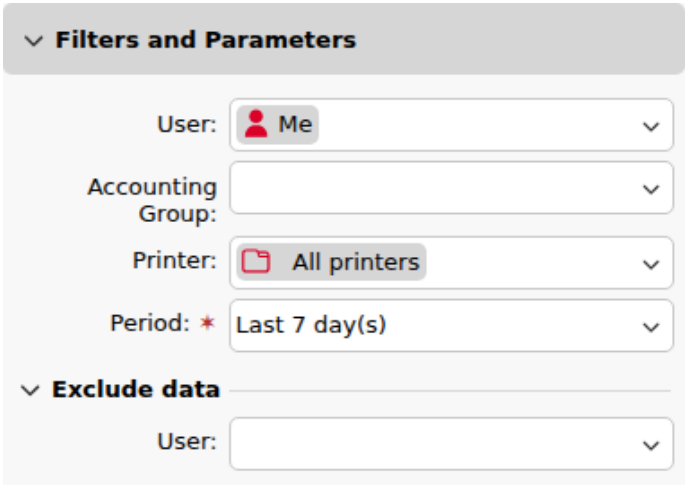
- **Schedule run**: Define a scheduled task to run the report at regular intervals.



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:



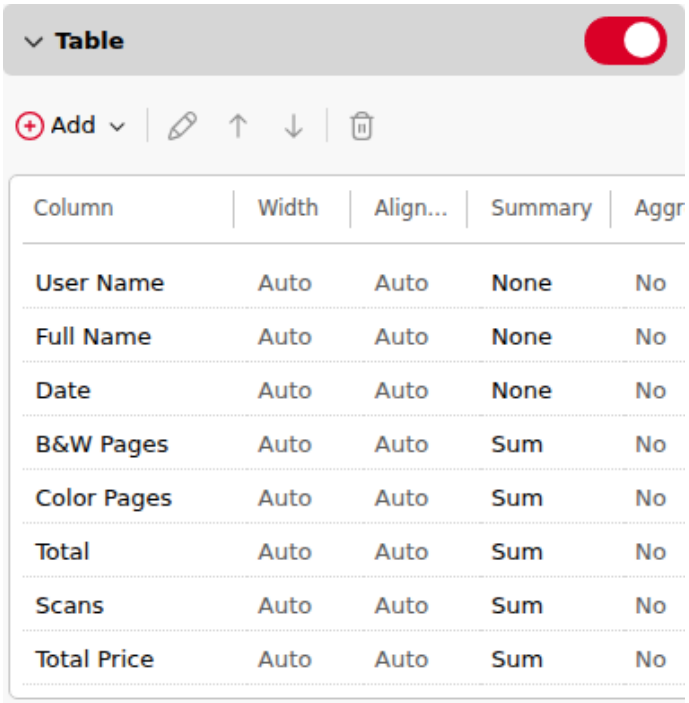
- **User**: Select the users to be included in the report. If you select the **Me** option and share this report with all users, each user can only see just the data that concern themselves; this way you can make personalized reports for each user.
- **Accounting Group**: Select the accounting groups 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.



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.

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.

15.4.3 Cloning Reports

Any user can clone an existing report that they have access to. Cloning 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.

15.5 Running Reports

Reports can be run on-demand or scheduled to run automatically at specified intervals. This section describes both approaches.

15.5.1 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.

15.5.2 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 191)

15.6 Aggregated Columns in Reports

For some types of reports, you can create your own 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. The following reports support aggregated columns:

Category	Report types
Groups	Monthly summary; Total summary
Print jobs	Expired and deleted jobs
Printers	Daily summary; Day of the week; Meter reading via SNMP; Total summary
Projects	Daily summary; Day of the week; Monthly summary; Project groups total summary; Projects per user; Users per project

15.6.1 Create an Aggregated Column

1. Go to **MyQ > Reports** and open a report for editing.
2. Select the **Design** tab.

3. In the **Table** section, click **Add**, and select **Add aggregated column.**

   The properties for your new aggregated column opens.

4. Set the properties:
   - **Column**: enter a name for the new column.
   - **Width**: specify the width. Leave empty for automatic width.
   - **Alignment**: select from *Auto* (default), *Left*, *Right* and *Center*.
   - **Summary**: select *None* or *Sum*.
   - **Columns**: select the columns used to calculate the aggregated operation.
   - **Aggregate operation**: select *Sum* or *Average*.
5. Click **Save**.

   The new column is listed with the other table columns, and you can double-click on it to edit it.

15.7 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

15.8 Connect to Power BI Tools

MyQ exposes data for analysis with external BI (Business Intelligence) tools. The information in this section refers to the setup and use of Microsoft Power BI with MyQ.

First configure the Power BI embedded database, and then start creating reports.

You can create reports according to your specific requirements. It is possible to create reports manually, or use the Power BI template created by MyQ in order to generate reports quickly.

See also:

- https://docs.microsoft.com/en-us/power-bi/fundamentals/desktop-getting-started

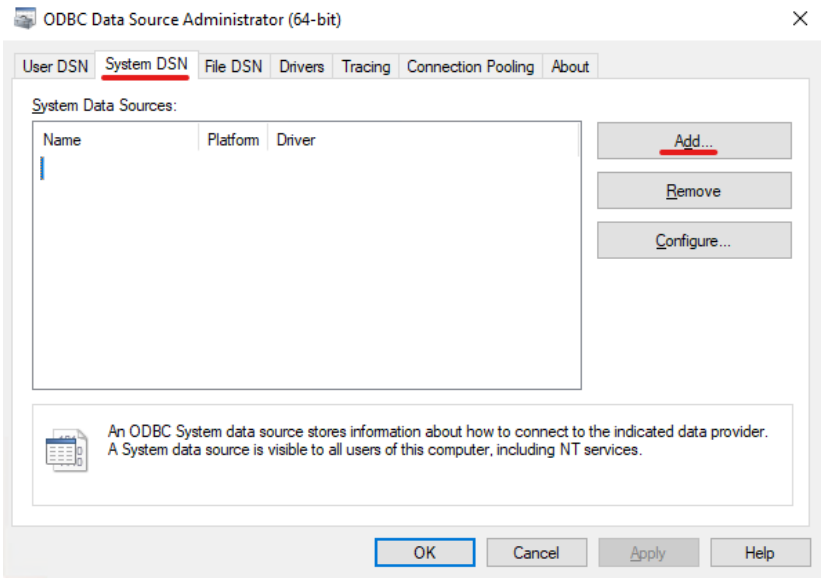
15.8.1 Configure Power BI Embedded DB

Power BI can access the MyQ Embedded Database via ODBC. In order to create an ODBC data source:

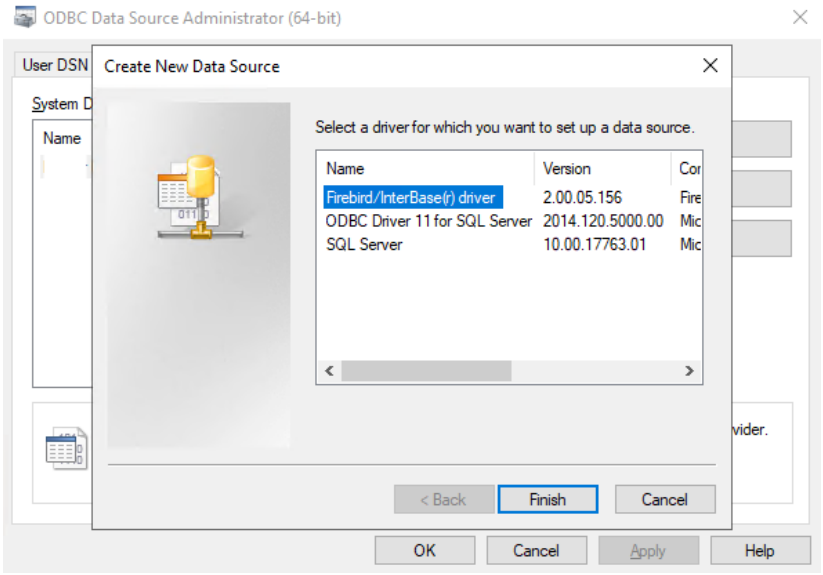
Power BI will only let you connect to a ODBC data source that is available on the local PC it is running within. Your data source should be created on the same PC that Power BI desktop run.

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.

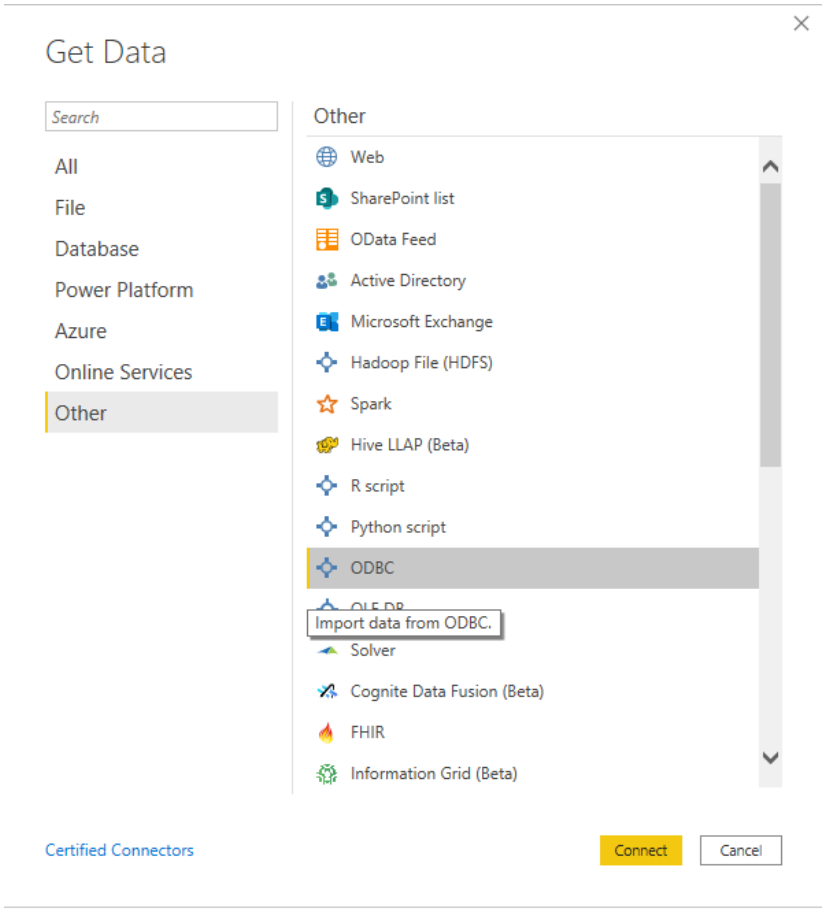
- **Data Source Name (DSN)**: Add a name as an identifier for the connection
- **Database**: Add the path to your database file (*C:\ProgramData\MyQ\MYQ.FDB* by default)
- **Client**: Add the path to the Firebird library client used for the connection. It is recommenced to use the MyQ Print Server client, found in *C:\Program Files\MyQ\Firebird\fbclient.dll* by default

- **Database Account**: Add the Database Account user name. 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 Easy Config, the default one is *masterkey*.

15.8.2 Create Power BI Reports Manually

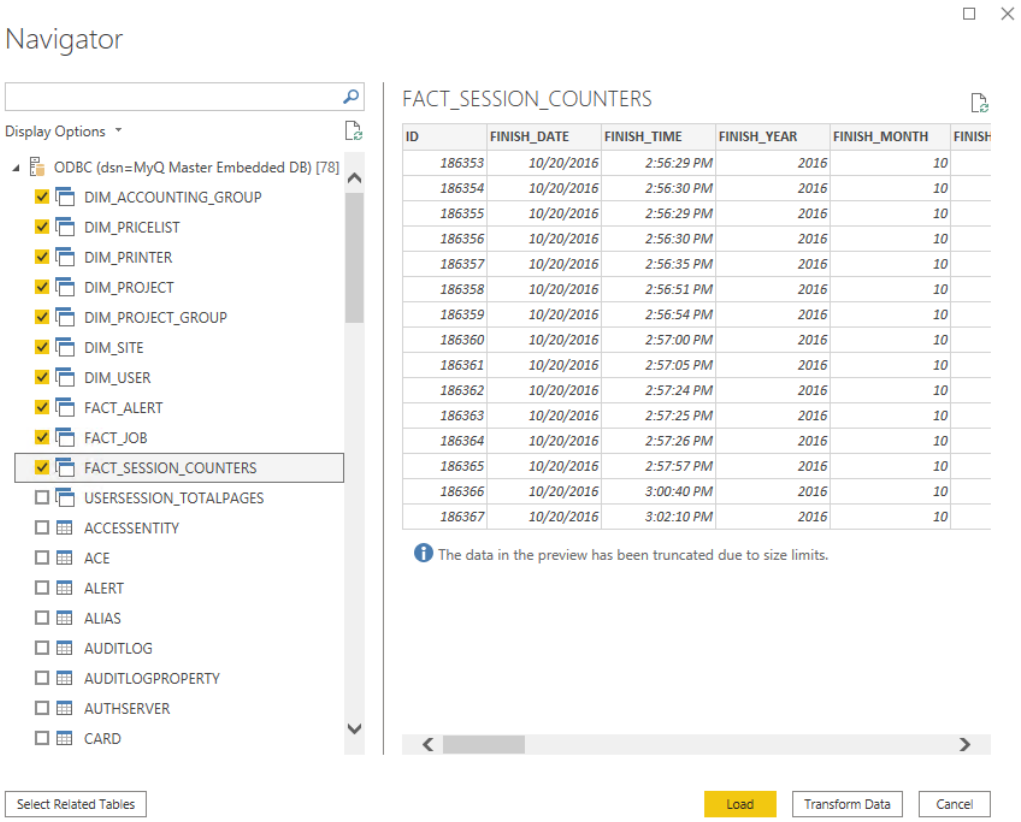
To manually create the reports, open Power BI and:

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**.

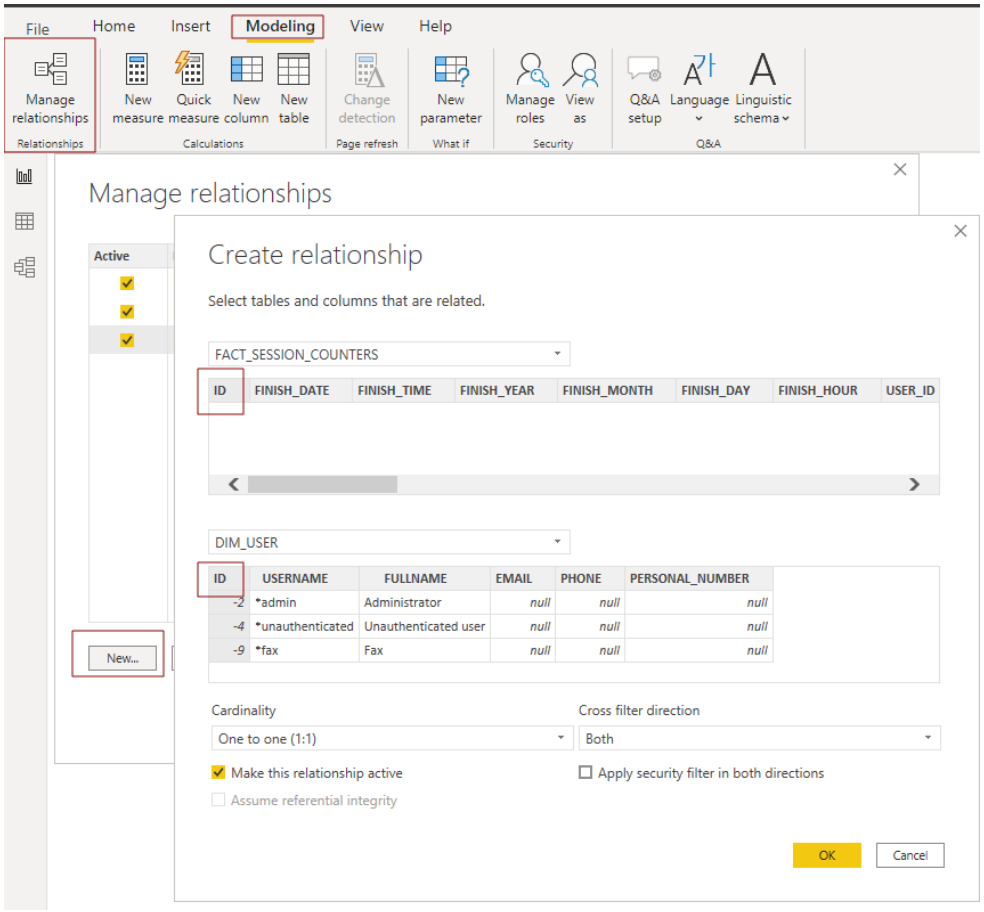




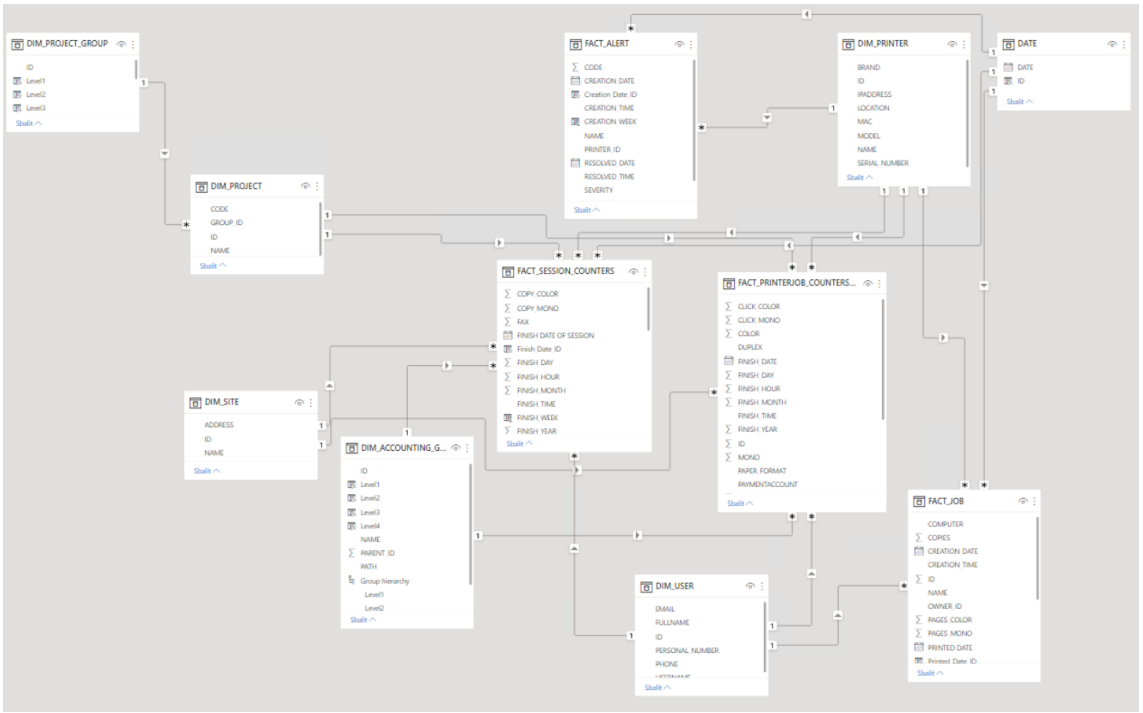
2. In the Navigator window, select all the options with the **DIM_** and **FACT_** prefixes and click **Load** (see Database Views and Dimensions (see page 708)).



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.



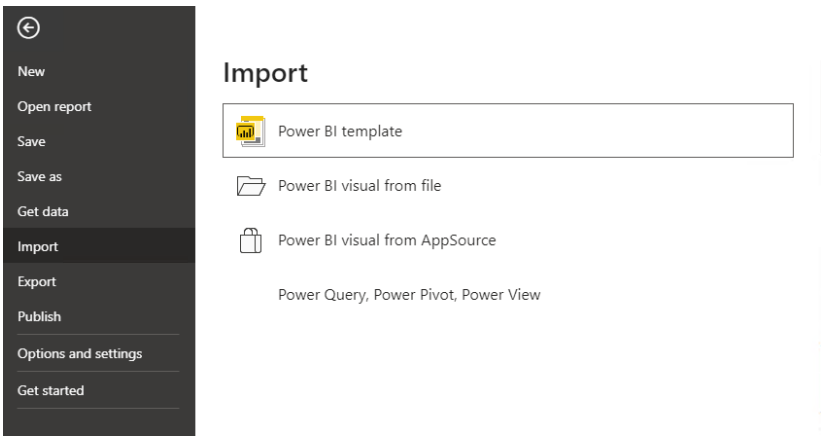
15.8.3 Create Power BI Reports via Template Import

An ODBC DSN must be configured before using the template.

ODBC 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.



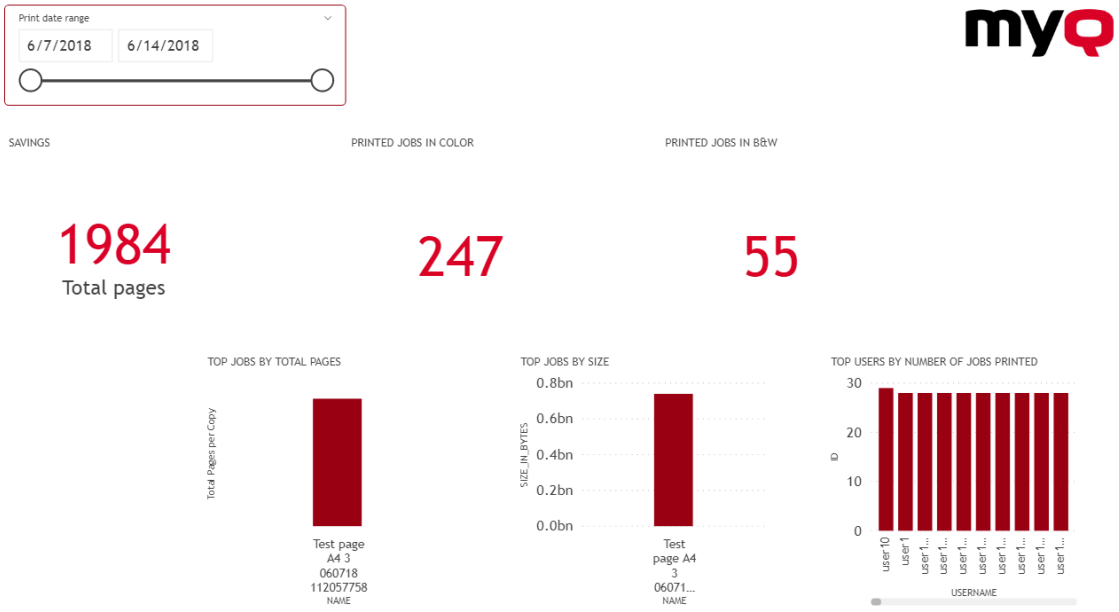
2. Establish the connection to your database:
    a. Add the **Data source name (DSN)** you created in the ODBC Data Sources app and click **Load**.

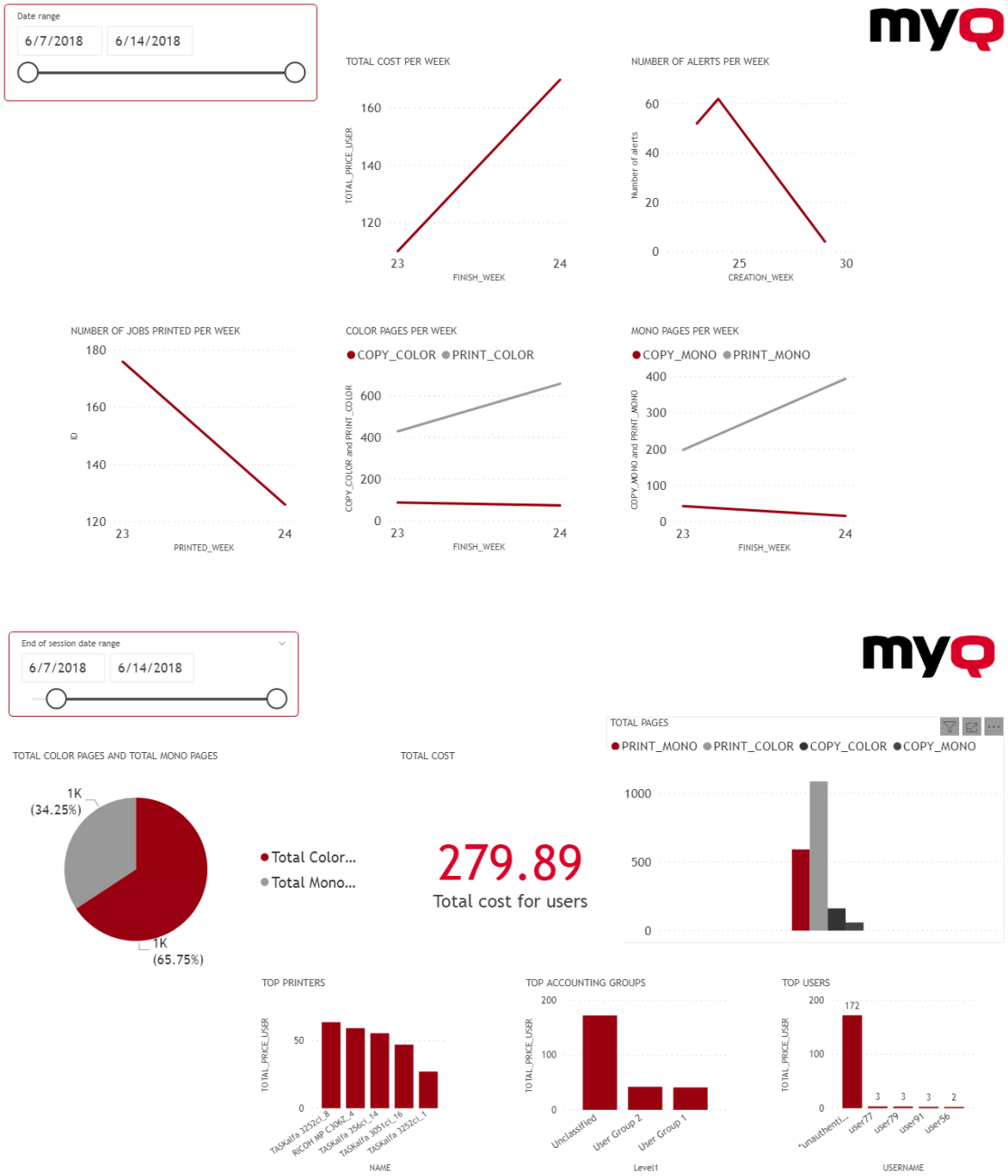


3. Power BI imports the data. The reports can be edited; the changes are saved in a different file so the template can be reused.

15.8.4 Sample Power BI Reports

The examples below were generated using the MyQ template.





15.8.5 Database 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
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

Field Name	Description
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

Field name	Description
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
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

Field name	Description
Period	Number of days from the toner installation to the toner replacement
Pages	Number of pages printed by the toner
Printer_Id	ID of the printer where the toner was installed

V_TONERS_INSTALLED

Field name	Description
Name	Name of the toner
Type	Type of the toner (`cyan` or `magenta` or `yellow` or `black`)
Installed	Date and time in which the toner was installed
Replaced	NULL
Counters	Total number of pages printed with the toner type since the toner type installation
Period	Number of days since the toner installation
Pages	Number of pages printed by the toner
Printer_Id	ID of the printer where the toner was installed

Printer jobs counter fact (fact_PRINTERJOB_COUNTERS_V3) - Information about printer jobs counters

Field name	Description
PRINTERJOB_ID	Printer job Id
USER_ID	User Id
USER_GROUP_ID	Group of users
PRINTER_ID	Printer Id

Field name	Description
PROJECT_ID	Project Id (-56 for jobs without project)
SITE_ID	Site id
TYPE	Job type. Values: `print`, `copy`, `scan`, `faxRx` (Incoming fax -print), `faxTx` (Outgoing fax - scan)
PAYMENTACCOUNT	Payment Account. Values `Credit`, `Quota`, `Cost Center`
FINISH_DATE	Date when job was finished
FINISH_TIME	Time when job was finished
FINISH_YEAR	Year when job was finished
FINISH_MONTH	Month when job was finished
FINISH_DAY	Day of a month when job was finished
FINISH_HOUR	Hour when job was finished
PAPER_FORMAT	Paper format
DUPLEX	Duplex print. Values: `Yes`, `No`
SHEETS	Used sheets of paper
MONO	Monochrome print job
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

Field name	Description
JOB_ID	Job id (Reference to user's job)

Job Fact (fact_job) - Information about print jobs

Field Name	Description
ID	Job ID
SESSION_ID	Session ID
NAME	Job name
OWNER_ID	Job owner ID
PRINTER_ID	Printer ID where the job was printed. Null if not printed
COMPUTER	Computer name or address where the job was sent from
SIZE_IN_BYTES	Job size in bytes
PAGES_MONO	Number of pages in black and white
PAGES_COLOR	Number of pages in color
DUPLEX	Duplex print. Values: `1 = Duplex`, `0 = Simplex`
COPIES	Number of copies
STATE	Job state. Values: `Ready`, `Printed`, `Expired or deleted`
PRINTED_DATE	Date when the job was printed
PRINTED_TIME	Time when the job was printed
CREATION_DATE	Date when the job was created
CREATION_TIME	Time when the job was created

Session Fact (**FACT_SESSION_COUNTERS**) - Information about sessions

Field Name	Description
ID	User session ID
FINISH_DATE	Date when session was finished
FINISH_TIME	Time when session was finished
FINISH_YEAR	Year when session was finished
FINISH_MONTH	Month when session was finished
FINISH_DAY	Day when session was finished
FINISH_HOUR	Hour when session was finished
USER_ID	User ID
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

Field Name	Description
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
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)

Field Name	Description
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.

16 Available Languages

Language	Abbreviation
Arabic (Saudi Arabia)	`ar`
Bosnian (Bosnia & Herzegovina)	`bs`
Bulgarian (Bulgaria)	`bg`
Chinese (China)	`zh-CN`
Chinese (Taiwan)	`zh-TW`
Croatian (Croatia)	`hr`
Czech (Czech Republic)	`cs`
Danish (Denmark)	`da`
Dutch (Belgium)	`nl-BE`
Dutch (The Netherlands)	`nl`
English (United Kingdom)	`en`
English (United States)	`en-US`
Estonian (Estonia)	`et`
Finnish (Finland)	`fi`
French (France)	`fr`
German (Germany)	`de`
Greek (Greece)	`el`
Hungarian (Hungary)	`hu`
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`

17 Release History

- MyQ X 10.3 RC (see page 722)
- MyQ X 10.3 RTM (see page 721)

17.1 MyQ X 10.3 RTM

17.1.1 MyQ Print Server 10.3 RTM

26 October, 2026

Changes

- Increased the minimum required Software Assurance date to 1 March, 2026. To upgrade to 10.3, your Software Assurance must be valid until at least that date.
- Updated OpenSSL to 3.5.8
- Updated PHP to 8.5.12
- Updated Traefik to 3.7.13

Bug Fixes

- Jobs printed with the HP Universal PCL driver with multiple copies and stapling are stapled together instead of each copy stapled separately.
- Jobs printed with the Ricoh PS driver are always printed in duplex, even when 2-sided printing is turned off in the driver.
- Booklet and stapling options are lost from jobs printed with the Fiery driver.
- Gmail connection used as an outgoing SMTP server fails with an authentication error.
- Enabling **Jobs via MS Universal Print** on a queue fails with the error "Duplicate attribute name in IPP message", and the printer is not available in Windows.
- Scan functions, such as Scan to Me, fail on devices with an Embedded Lite license with the error "Printer has no license for scanning".

Device Certifications

- Added support for Canon imageFORCE C3026.
- Added support for Epson AM-C10000.
- Added support for Epson DS-71000.
- Added support for HP LaserJet MFP X53052.
- Added support for HP Color LaserJet MFP X77823 and X77830, HP LaserJet MFP X72826 and X72831, HP Color LaserJet Enterprise MFP 4801 and X47635, with embedded terminal.

- Added support for HP LaserJet Enterprise 5501 and 6500, HP Color LaserJet Enterprise 4701 and X45135.
- Added support for Ricoh P C300W.

17.2 MyQ X 10.3 RC

17.2.1 MyQ Print Server 10.3 RC

14 September, 2026

Security

- Improved security for CSV exports.
- PM Server now uses the server certificate instead of a self-signed certificate.
- A new helper is used for cloud connections.

Improvements

- NEW FEATURE Improved WPP support in MyQ queues. IPP attributes can be passed from the printer to the Windows workstation.
- NEW FEATURE Use MyQ Document Processor as an OCR and scan processing service, configured in Easy Scan Processing via OCR Profiles. See (10.3) MyQ Document Processor.
- NEW FEATURE Use MyQ Scan Review as an Easy Scan destination, for digitization of documents with preserved authenticity and integrity. See (10.3) MyQ Scan Review.
- NEW FEATURE Provide your own common-area printing solutions with kiosk-based job release to one or more devices. Each device must have at least Embedded Lite license assigned. See Release Stations (see page 401).
- Added the **Delta Synchronization for Entra ID** feature, and a new scheduled task for lightweight, frequent synchronization.
- **Embedded Lite** was added to the **Terminal type** in terminal configuration profiles. This new type will support future Embedded Lite terminals.
- **Require authentication** for IPPS jobs, in **MyQ > Settings > Jobs**.
- Include **device logs from up to 5 printers** when generating support data.
- Added **eGoldFax as a standard connection** type. Previously, this feature was enabled using a config.ini parameter.
- MS Cluster deployments: terminal packages cannot be changed while terminal monitor scripts are running. Take the scripts offline before upgrading terminals, then bring them back online.
- Optimized the speed of long running database queries under certain condition.

Changes

- .NET 4.8 or later is a system requirement for Print Server. Ensure this requirement is met before you upgrade Print Server. An unsupported .NET Framework version prevents services from starting.
- Added "Rate Us" option to the dashboard (appears 30 days after installation).
- By default, MyQ X now uses the cloud helper application `helper2.myq-solution.com`.
- Easy Scan properties has new "Job Processing" tab for MyQ Document Processor settings.
- MyQ uses a new cloud application for OneDrive Personal. Users will need to reconnect their OneDrive cloud storages.
- New license type - Embedded Ultimate. Enables activated devices to use MyQ Scan Review.
- OCR profiles can now have two types: Hot Folder and Document Processor.
- Removed Firebird Client ADO.NET.msi file.
- Removed option to disable scanning in **MyQ > Settings > Scanning & OCR**.
- Removed support for MyQ OCR Server. Replaced by MyQ Document Processor (MDP) and option to use "hot folder".
- Removed support for versions older than MyQ Desktop Client 10.2.
- Removed support for HW-11-T, TerminalPro, Recharge Terminal, and Android Terminal.
- Removed unsecure port option for Site connections.
- SharePoint Online, OneDrive for Business and Entra ID setup now use the new pass-through redirect.
- Terminal licenses can now be assigned manually to printers.
- The EULA has been updated. You can view it during installation or upgrade.
- The list of available languages in the terminal action **Edit account** is now limited to languages from **MyQ > Settings > General** (default + additional languages).
- Updated Apache to 2.4.68
- Updated Firebird to 4.0.7
- Updated MAKO to 8.4
- Updated Microsoft Playwright to 1.62.0
- Updated OpenSSL to 3.5.7
- Updated PHP to 8.5.9
- Updated Traefik to 3.7.11
- Updated libcurl to 8.21.0

Device Certifications

- Added Embedded terminal support for Lexmark CX950.
- Added embedded terminal support for multiple Brother devices.

- Added paper counters to Kyocera TASKalfa Pro 15000c, Konica Minolta AccurioPress 6136P and 14010.
- Added support for Brother DCP-L5512DW.
- Added support for Brother HL-EX470.
- Added support for Brother HL-L8230CDW and HL-L8240CDW.
- Added support for Brother MFC-EX670.
- Added support for Brother MFC-EX915DW.
- Added support for Brother MFC-J5955DW.
- Added support for Brother MFC-L6912DW.
- Added support for Brother MFC-T910DW.
- Added support for Canon imageFORCE 1440P, 1643 and C1333P.
- Added support for Canon imageFORCE 520.
- Added support for Canon imageFORCE C5170.
- Added support for Canon MF660C Series.
- Added support for HP DesignJet T250, T520 and T630.
- Added support for HP LaserJet M203dw.
- Added support for Lexmark MX532.
- Added support for Ricoh IM 25/35/45/6010.
- Added support for Ricoh Pro C5400S and C5410S.
- Added support for RISO SF 5x50EII.
- Added support for Toshiba e-STUDIO6526AC and 6527AC.
- Corrected counters reading of Epson AM-C4/5/6000.
- Corrected toner reading of Lexmark MX722.

18 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[46]
Technical support	support@myq-solution.com[47]
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.

46. mailto:info@myq-solution.com
47. 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

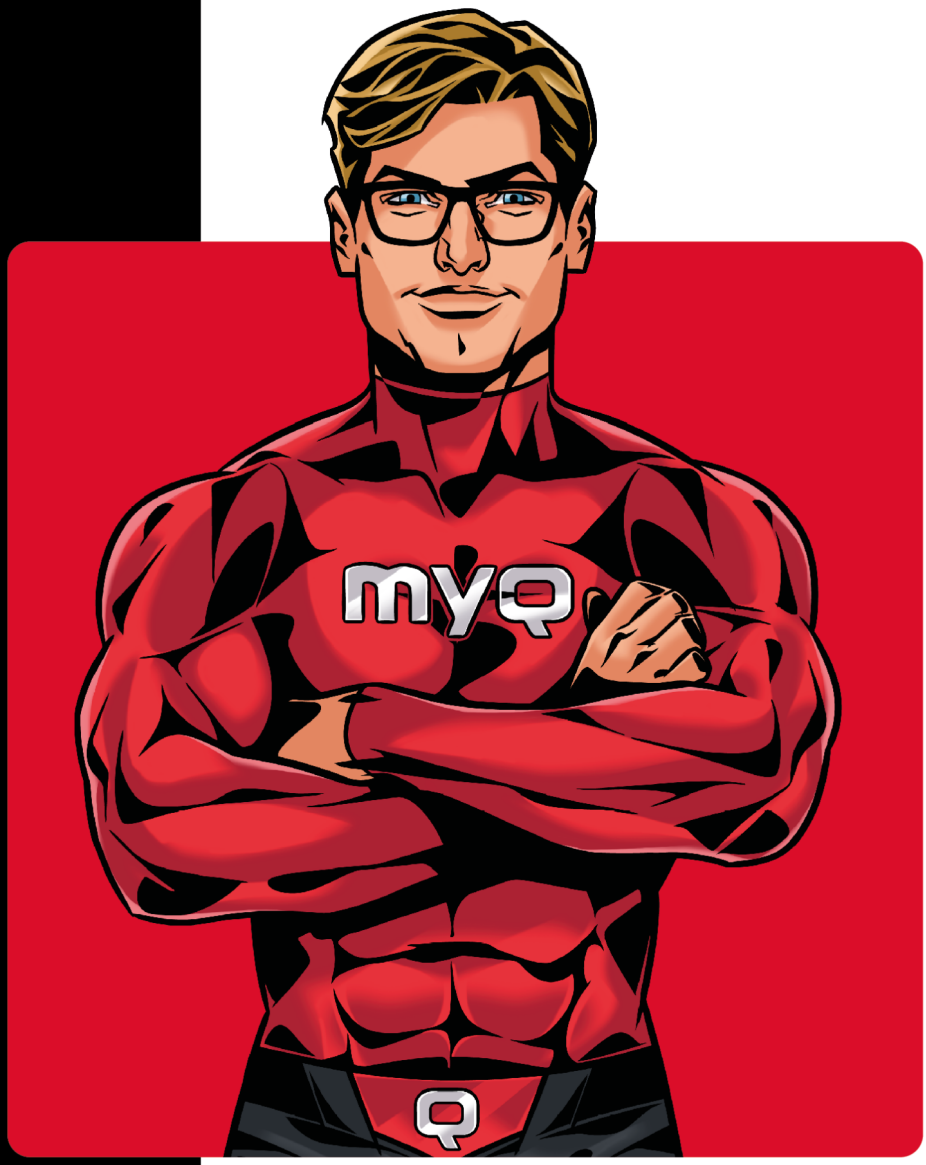
50+ million
Trusted users

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

ISO 9001 TÜV SÜD ISO 14001 ISO/IEC 27001