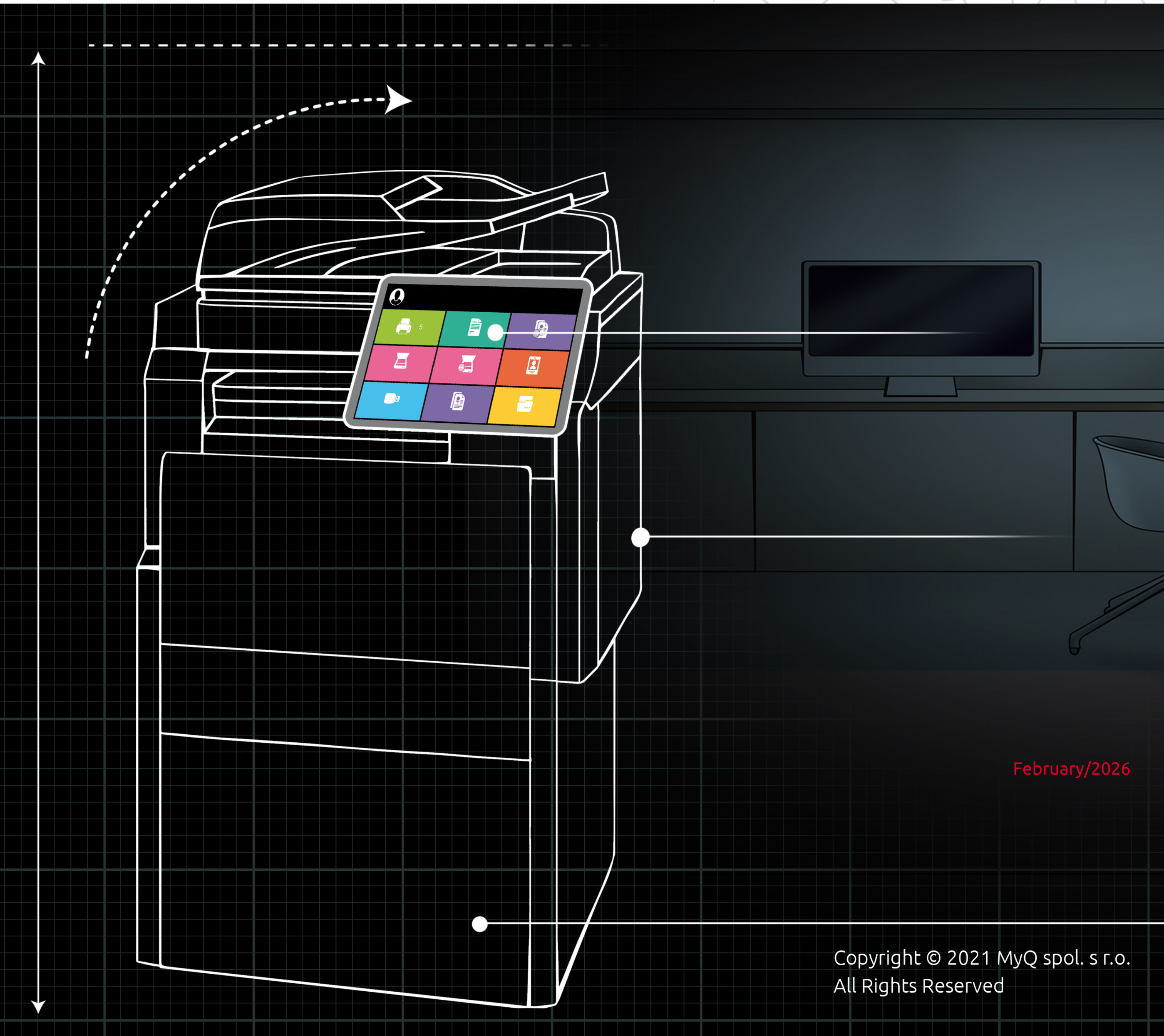
Print Server 10.2



February/2026

Table of Contents

MyQ Print Server 10.2

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

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

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

All changes compared to the previous version are listed in the release notes, available online and in PDF.

1 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.

1.1 MyQ Print Server - Standalone mode

1.1.1 MyQ Print Server Hardware requirements up to 600 devices

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

*It is recommended to use +1 physical core if Credit/Quota is used.
(calculated with AMD Ryzen Threadripper 1920X 3,5GHz)

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

1.1.2 Recommendations

- Install Windows updates outside of working hours.
- Always monitor the server performance during peak usage hours and adjust the settings accordingly.

- Changing the power plan of Windows Server in *Control Panel – Hardware – Power Options* from Balanced (the default setting) to **High performance** is recommended to utilize the maximum performance. This may help speed up database operations.

1.2 MyQ Print Server - Site mode (Central Server & Site Servers architecture)

1.2.1 Site servers Hardware requirements up to 30 000 devices

	1-10 devices	**11-100 devices**	**101-300 devices**	**301-600 devices**	**601 - 30 000 devices**
Physical Core	5	6	8	10	10
RAM	6GB	8GB	12GB	14GB	14GB
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	30GB	33GB - 350GB	380GB - 1TB	1,4T - 2TB	2TB per 600 devices

(calculated with AMD Ryzen Threadripper 1920X 3,5GHz)

For the **MyQ Central Server** Hardware specification, see (10.2) System Requirements in the MyQ Central Server guide.

1.2.2 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

1.2.3 Recommendations

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

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

1.2.4 Storage

The MyQ Print Server installation files are approximately 700MB.

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.

MyQ data folder (jobs, main database, and log database increasing):		
10k jobs	**100k jobs**	**1M jobs**
35GB	300GB	3,5TB

Counted for jobs with 2,9MB size.

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.).

1.2.5 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.

1.2.6 MyQ Desktop Client

If there are 100 - 1000 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.

1.2.7 Recommended no. 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.

1.2.8 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.

1.3 Additional software required

- .NET Runtime 8
- ASP .NET Core 8
- Windows Desktop Runtime 8

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

1.3.1 Windows Server 2022 Core

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

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

Restart the server after installation is finished.

1.3.2 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.

1.3.3 Security

DigiCert Global Root CA certificate (required for Installation Key license activation) → https://www.digicert.com/kb/digicert-root-certificates.htm#roots.
It should be included by default in the latest updated Windows versions.
Supported Public Key Infrastructure for asymmetric cryptography.

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

1.4 MyQ installation in Private Cloud

MyQ can also be installed in Private Cloud. For requirements and further details, see Installation in Private Cloud.

1.5 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.

1.5.1 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 printers' status.

1.5.2 Incoming Ports

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

Protocol	Port	Configurable	Description
TCP	**21**	Yes (WebUI)	FTP protocol for receiving scans(1). The server runs only in passive mode and each data connection runs over a dynamic port in the 49152 - 65535 range.
TCP	**25**	Yes (WebUI)	SMTP over StartTLS(2) for Scan Management function, receiving email notifications from printers, and for receiving emails with jobs.

Protocol	Port	Configurable	Description
TCP	**443**	Yes (Easy Config)	HTTPS protocol for: • Accessing MyQ web interface. • Mobile printing (AirPrint/Mopria; printing URL **/ipp-airPrint/<queue name>**). • Communication with Embedded terminals. • Job roaming among MyQ servers. Previously, this port was 8090 and it is preserved as such for upgraded installations.
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.
UDP	**11112**	No	Communication with MyQ Desktop Client (MDC) 10.0 and lower. The answer is returned on a dynamic port in the 49152 - 65535 range. Not required with MDC 10.2+.

- (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 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

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.

1.5.3 Outgoing Ports

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

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:

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.

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:

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

1.5.4 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)**	• HTTP or HTTPS: 443 (default) - it depends on the configuration in MyQ Easy Config. • SMTP: 25 (default) - it depends on the port configured 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 (Pull Print). **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.

<table>
<tr><th colspan="2">HP</th></tr>
<tr><td>If SSL is on, it's used for the following events:</td><td>All types of events go through SSL.</td></tr>
<tr><td>MyQ Server
(Protocol: Port - Description)</td><td>HTTP or HTTPS: 8090 (default) - it depends on the configuration in MyQ Easy Config.
SMTP: 25 (default) - it depends on the port configured in MyQ, Settings, Network, SMTP. Used for Panel Scan to email.</td></tr>
<tr><td>Package
(Protocol: Port - Description)</td><td>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).</td></tr>
<tr><td>Printer
(Protocol: Port - Description)</td><td>(OUT) 57627 - non SSL.
(OUT) 7627 - SSL.</td></tr>
<tr><th colspan="2">Toshiba</th></tr>
<tr><td>If SSL is on, it's used for the following events:</td><td>All types of events go through SSL.</td></tr>
<tr><td>MyQ Server
(Protocol: Port - Description)</td><td>HTTP or HTTPS: 8090 (default) - it depends on the configuration in MyQ Easy Config.
SMTP: 25 (default) - it depends on the port configured in MyQ, Settings, Network, SMTP. Used for Panel Scan to email.</td></tr>
<tr><td>Package
(Protocol: Port - Description)</td><td>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).</td></tr>
</table>

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)**	• HTTP or HTTPS: 8090 (default) - it depends on the configuration in MyQ Easy Config. • SMTP: 25 (default) - it depends on the port configured 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)**	• HTTP: (OUT) 80 - Used to access to Xerox EIP • 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)**	• HTTP or HTTPS: 8090 (default) - it depends on the configuration in MyQ Easy Config. • SMTP: 25 (default) - it depends on the port configured 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 (Pull Print). **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)**	• HTTP or HTTPS: 8090 (default) - it depends on the configuration in MyQ Easy Config. • SMTP: 25 (default) - it depends on the port configured 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)**	• HTTP or HTTPS: 8090 (default) - it depends on the configuration in MyQ Easy Config. • SMTP: 25 (default) - it depends on the port configured 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)**	• HTTP or HTTPS: 8090 or 443(default) - it depends on the configuration in MyQ Easy Config. • SMTP: 25 (default) - it depends on the port configured in MyQ, Settings, Network, SMTP Used for Email 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. Eg 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)**	• HTTP or HTTPS: 8090 or 443 (default) - it depends on the configuration in MyQ X Easy Config. • SMTP: 25 (default) - it depends on the port configured 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)**	• HTTP or HTTPS: 8090 or 443 (default) - it depends on the configuration in MyQ X Easy Config. • SMTP: 25 (default) - it depends on the port configured 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**.

2 Installation

A comprehensive guide to installing and upgrading all MyQ components is available here.

This chapter 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.

1. Download the latest available version of MyQ 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.

2.1 Installation 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.

For an overview of MQ in the cloud, see MyQ in Cloud.
For more information about the cloud deployment, see Deployment in the Cloud.

2.1.1 Private Cloud Using 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 and can be found in system requirements.
- 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. See main communication ports for a full list.

- The geolocation of the cloud server should be as physically close as possible.
- The Ping answer from printers to the cloud server should be within 750 ms (max 1 second, can be adjusted in config.ini)

For more information about *Azure - Extend an on-premises network using VPN*, see: https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/vpn#architecture

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.

2.1.2 Private Cloud Using Amazon

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. Refer to the MyQ X Documentation for detailed system requirements.
- **AWS VPC Setup:** Create an AWS Virtual Private Cloud (VPC) with necessary resources like subnets, route tables, and gateways. Follow the procedure outlined in the AWS VPC guide.
- **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. Detailed steps can be found in the AWS Site-to-Site VPN documentation.

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

For details, refer to the AWS guide.

- **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. Follow the steps in the AWS Customer Gateway guide.

- **Create a Virtual Private Gateway:** This is the VPN gateway on the AWS side. After creation, attach it to your VPC. Instructions are detailed in the AWS Virtual Private Gateway guide.
- **Configure Routing:** Update your VPC's route table to direct traffic through the VPN connection to your on-premises network. Refer to the AWS Route Table Configuration.
- **Update Security Groups:** Modify the security group associated with your EC2 instance to allow necessary inbound and outbound traffic. See the AWS Security Group guide for details.
- **Create the VPN Connection:** Establish the VPN connection between your AWS VPC and your on-premises network by configuring the necessary tunnels. Detailed instructions can be found here.
- **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.

2.1.3 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. For detailed information, refer to the Compute Engine Overview.
- **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. For more details, see the Cloud VPN Overview.
- **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. Learn more in the VPC Networks Documentation.
- **Latency Considerations**: Select a region close to the on-premises network to minimize latency. All resources should ideally be in the same region.

Setup Steps

1. **Create a Project**:
   - Organize resources by creating a new project or using an existing one in Google Cloud. For instructions, visit the Google Cloud Console.
2. **Set Up a VPC Network**:
   - Create a custom VPC with subnets and appropriate IP ranges not overlapping with the on-premises network. For guidance, see the Quickstart: Create and Manage VPC Networks.

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 Classic VPN Topologies or HA VPN Topologies 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. Learn more from the Compute Engine Documentation.
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.

2.2 OEM Migration

Since **10.1 Patch 3**, it is possible to 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.

The same feature is implemented in (10.2) Central Server.

2.2.1 Prerequisites

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

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

2.2.2 Recommended steps

Before you begin, we recommend you read our Upgrading MyQ Guide.

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

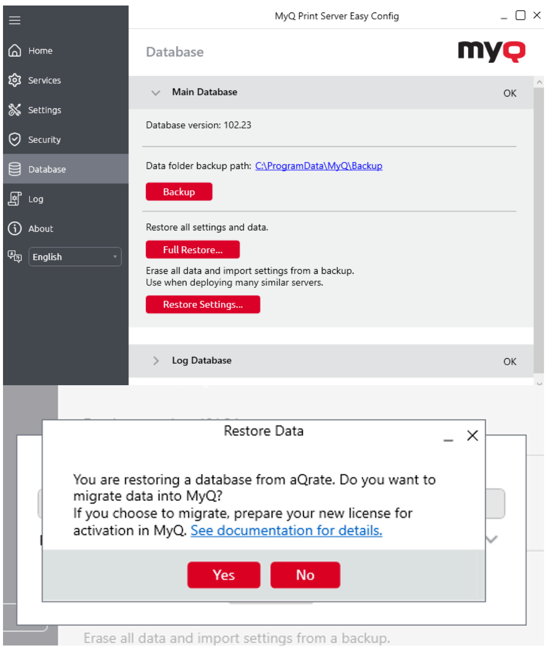
Licenses

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.

2.2.3 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 (`10.1 Patch 3` 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

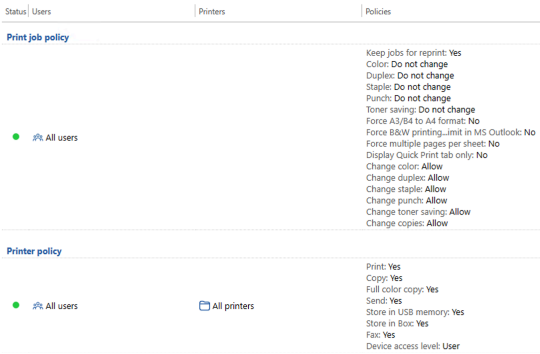
All data except some settings are migrated without any changes. Database restore runs as usual, after the restore is finished and all following database upgrades are completed, the corresponding settings are updated.

Settings Migration

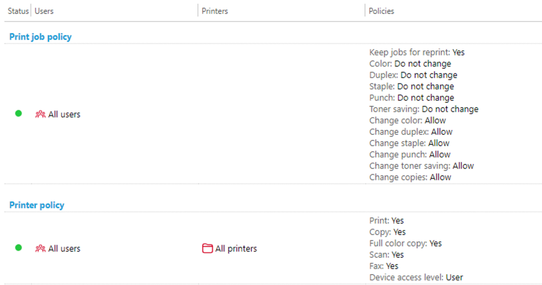
Settings are migrated with some transformation due to differences in OEM brands.

User policies

Currently, KNM and aQrate have an extended list of default user policies compared to MyQ - one policy is replaced with several other extra policies, see screenshots. So 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.



1 KYOCERA Net Manager – default policies

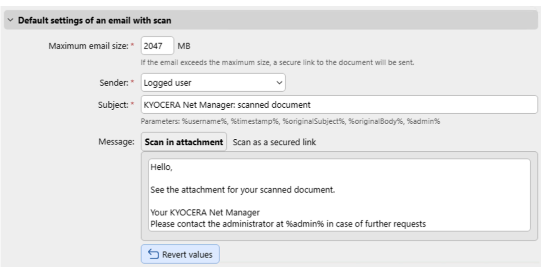


2 MyQ – default policies

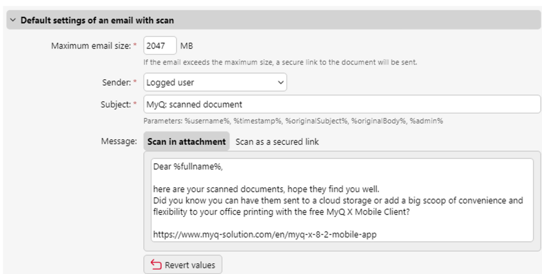
Email templates

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.



3 KYOCERA Net Manager – emails with scan



4 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.

Site name (Central-Site environments)

Settings → Server Type → Site server → Site name - since **10.1 Patch 3** 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.

2.3 Updating MyQ

A comprehensive guide to updating all MyQ components is available here.

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

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

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

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

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

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

A direct upgrade to version 8.0 and higher versions from versions lower than 6.0 is no longer supported. These versions have to be upgraded via an intermediary version, for example via 6.2.

- For version 4.2 or lower, the intermediary versions are: 4.3 -> 5.2 -> 7.1.
- For version 5.2 to 5.10 the intermediary version is 7.1.

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, except that you are asked to choose upgrade options.

You can find an upgrade manual with more details on the MyQ Community portal.

3 MyQ and MS Cluster

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

A complete list of MyQ Print Server system requirements can be found here.

3.1 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 Print 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 to have 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).

3.2 Licenses

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

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

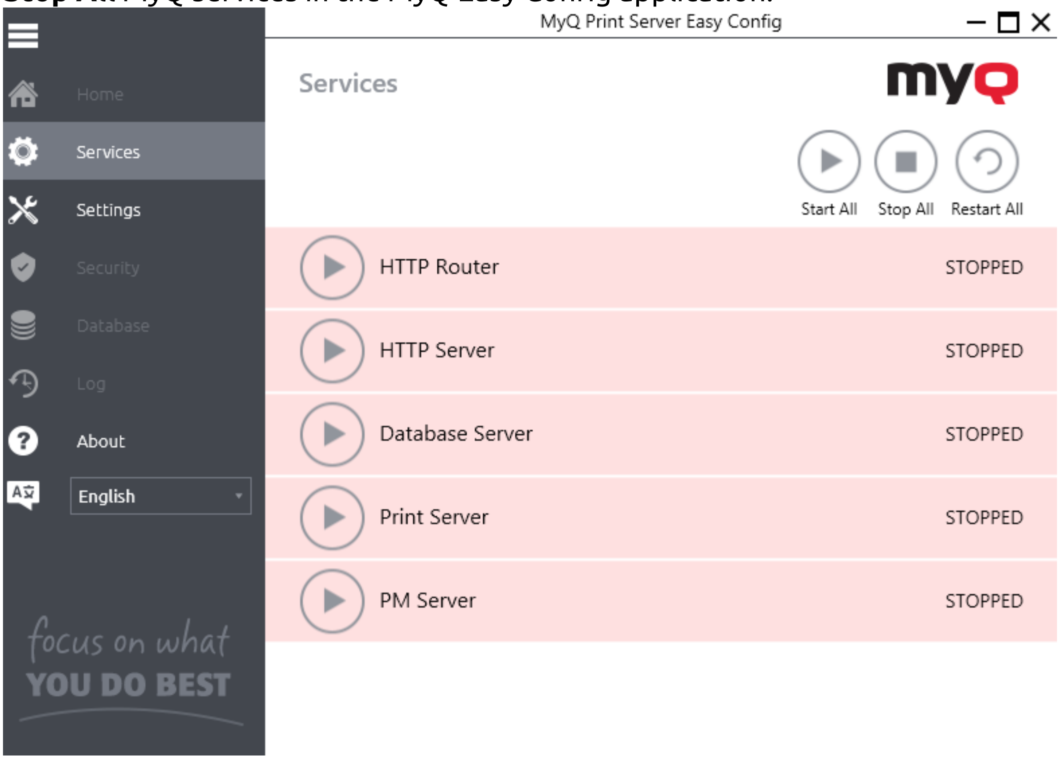
- MyQ server in Site mode - licenses are received from the Central server automatically every day or during MyQ service or Cluster Node restart.
- MyQ server in Standalone mode - needs an extra licenses set for each node; each licenses set must be activated only on one node.

3.3 Setup

3.3.1 Installing MyQ Print Server in the cluster (all nodes)

On each cluster node, do the following:

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

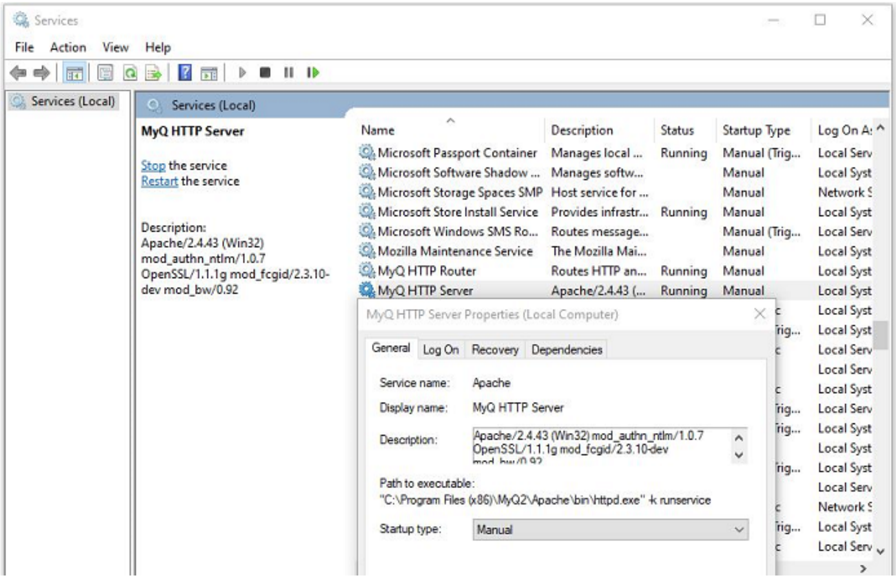


3.3.2 Setting services to manual startup (all nodes)

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

The following services need to be changed this way:

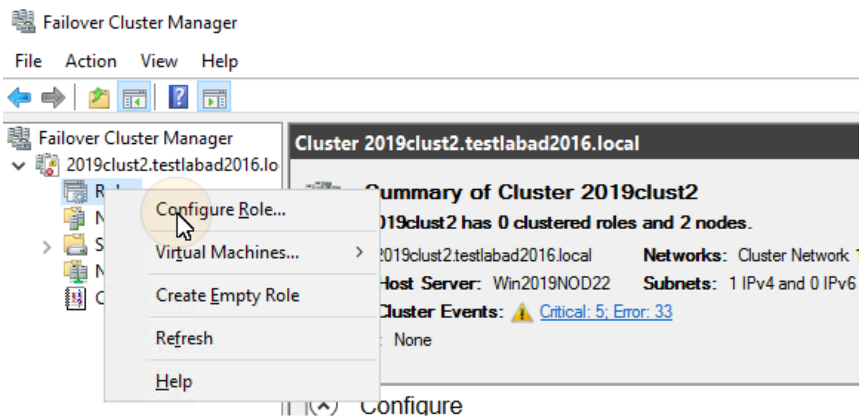
- MyQ HTTP Server
- MyQ HTTP Router
- Firebird Server - DefaultInstance
- MyQ Print Server
- MyQ Svc (not available in version 8.1+)
- PM Server
- Brand Terminals (only if embedded terminals are used)



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

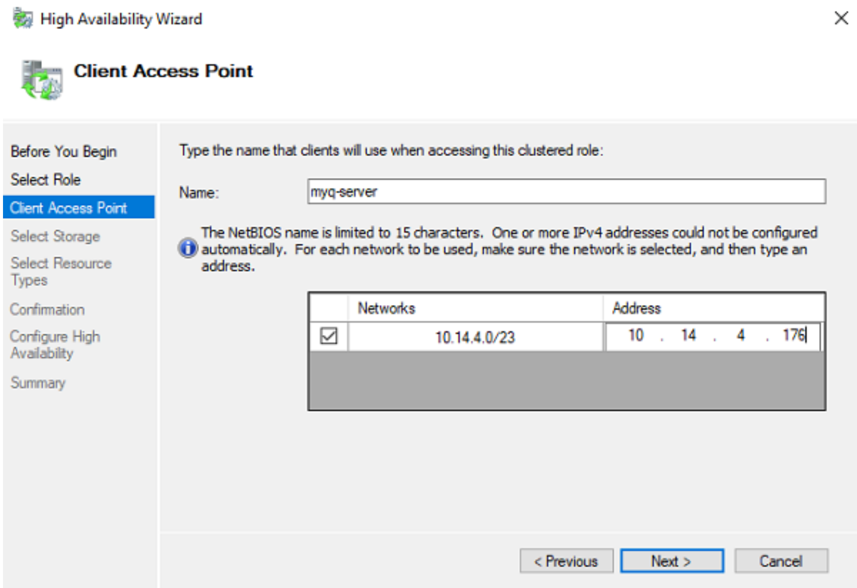
Open Failover Cluster Manager and do the following:

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

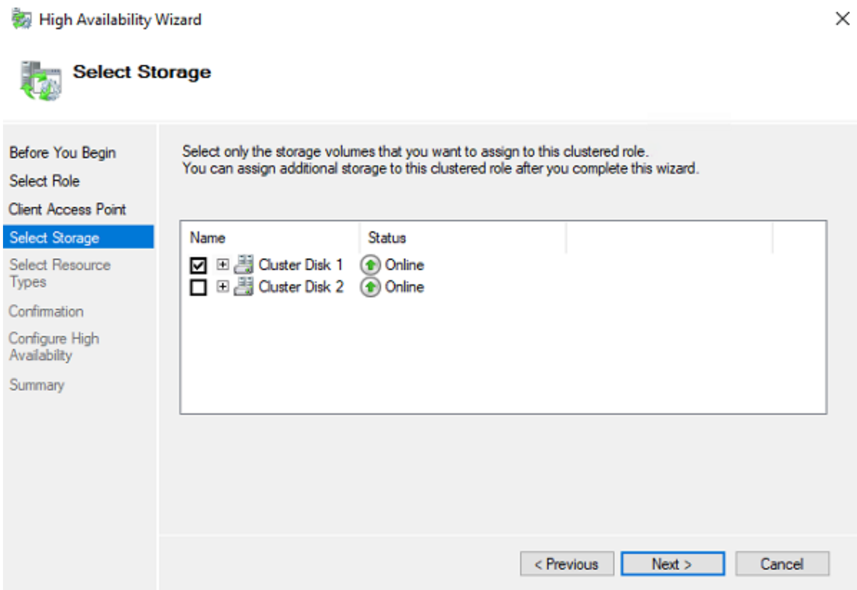


2. Click **Next**. The Select role tab opens.
3. On the tab, select **Other Server**, and click **Next**. The Client Access Point tab opens.

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



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



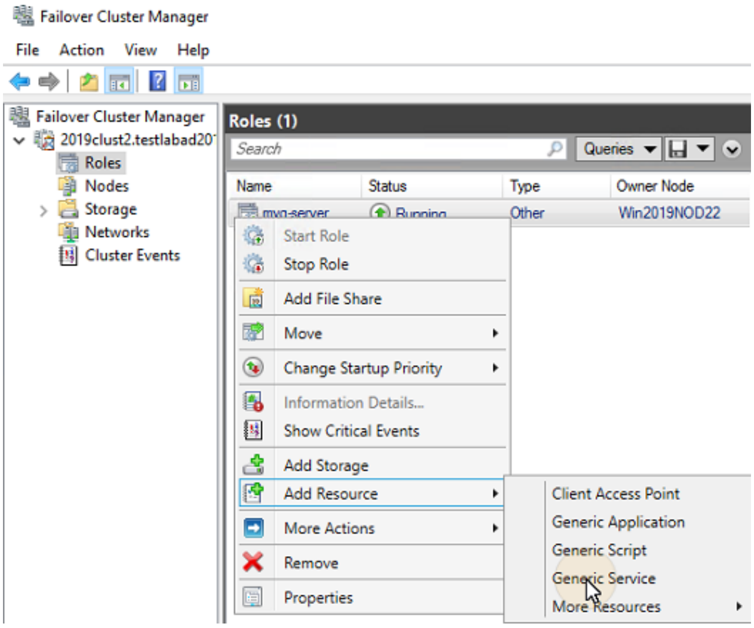
6. Click **Next** to finish the installation process.

3.3.4 Adding MyQ Resources (Failover Cluster Manager)

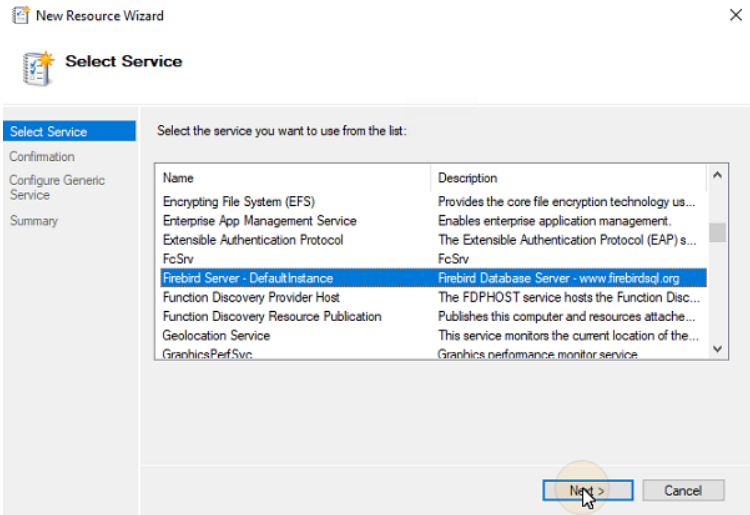
Once the MyQ server role is created and configured, MyQ resources need to be configured as well, in the **Roles** tab in Failover Cluster Manager.

Add the Firebird server - 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:

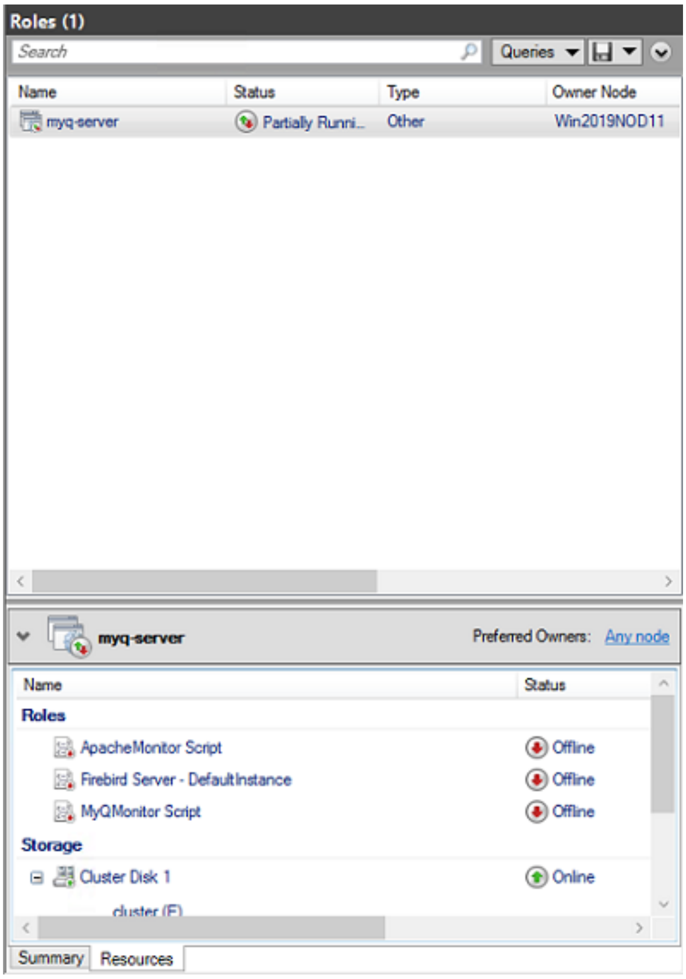
1. Right-click the MyQ server role, click **Add resource** on the shortcut menu, and click **Generic Script**. The New Resource Wizard opens.
2. Enter the path to the **MyQMonitor.jse** script, located in the MyQ installation folder, and click **Next**. The Confirmation tab opens. The default path to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

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.

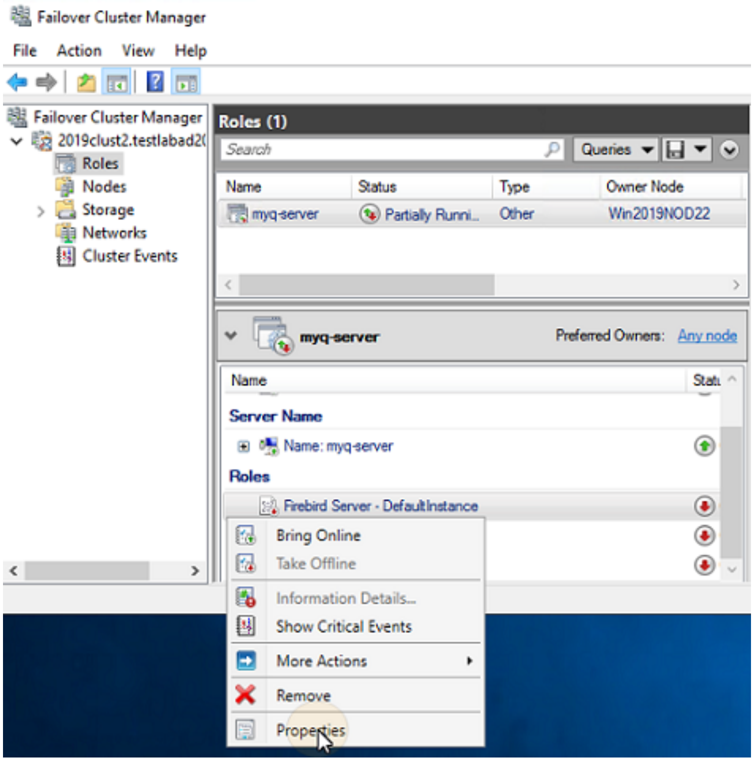
3.3.5 Setting Resources Dependencies (Failover Cluster Manager)

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

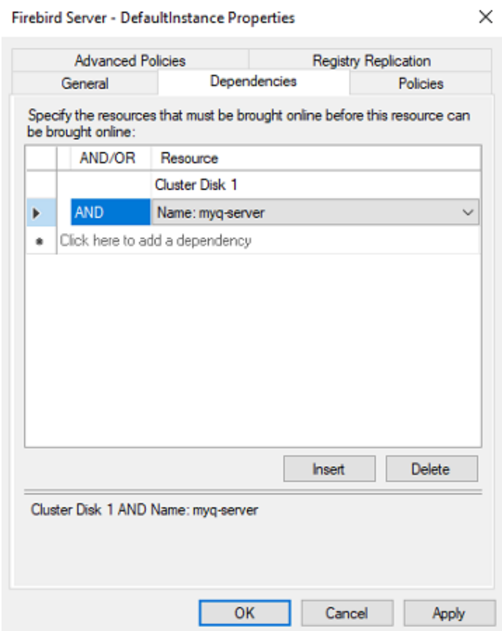


Set the Firebird Server - DefaultInstance service dependency

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.



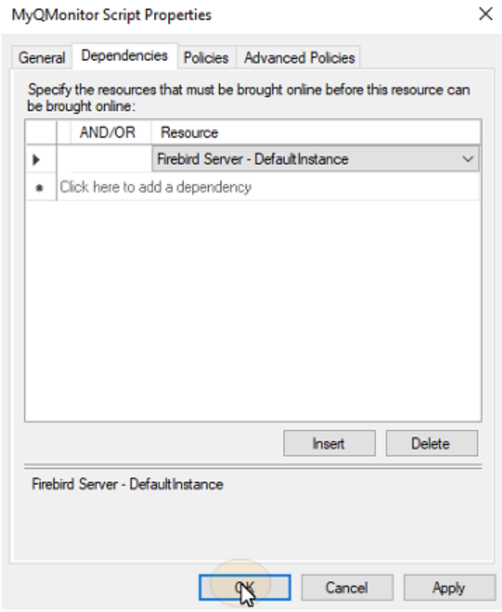
2. In the dialog box, open the **Dependencies** tab, add the shared disk drive (or NAS) where the system is supposed to work on, add the name of the MyQ server role, and click **OK**. The dependency is set.



Set the MyQMonitor script dependency

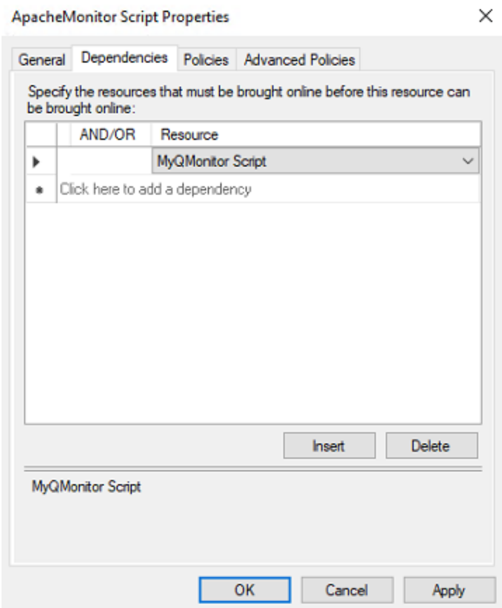
1. In the list at the bottom of the tab, right-click **MyQMonitor Script**, and click **Properties**. The MyQMonitor Script Properties dialog box opens.

2. In the dialog box, open the **Dependencies** tab, add the **Firebird Server - DefaultInstance**, and click **OK**. The dependency is set.



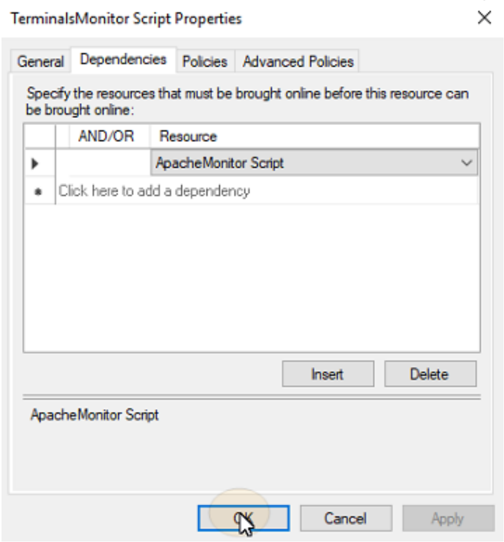
Set the ApacheMonitor script dependency

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 (only if embedded terminals are used)

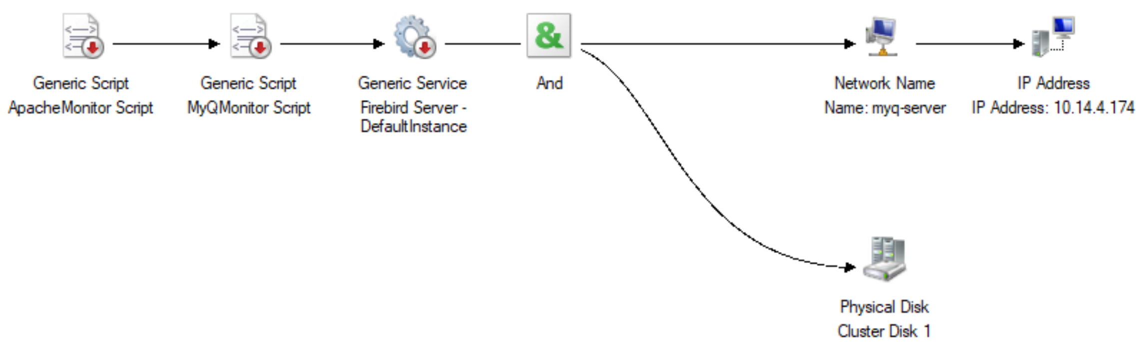
1. In the list at the bottom of the tab, right-click **TerminalsMonitor Script**, and click **Properties**. The TerminalsMonitor Script Properties dialog box opens.
2. In the dialog box, open the **Dependencies** tab, then add the **ApacheMonitor Script**, and click **OK**. The dependency is set.



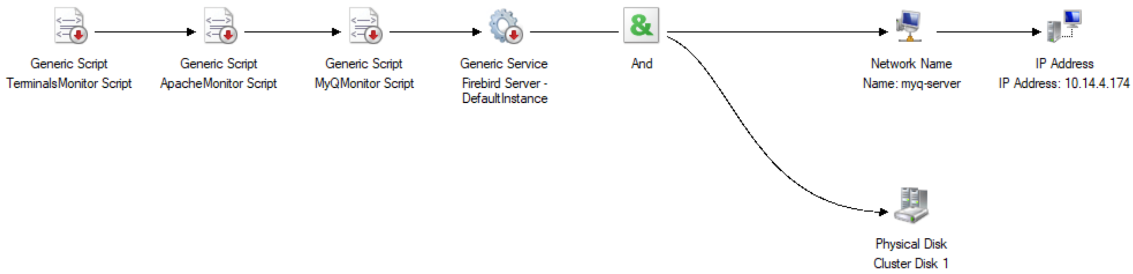
Once you upload an Embedded terminal installation package on the MyQ web administrator interface of the MyQ cluster server, the cluster uses the script to distribute the package among all the other nodes.

3.3.6 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:



5 Dependency graph of the cluster on the MyQ server



6 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**.

3.4 Additional Setup

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

3.4.1 Setting up the 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.

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

On each node of the cluster, you need to set the location of the **Data** folder and 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. (For more information about how to do this, check here).
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.

3.4.3 Running MyQ in the MS Cluster environment

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

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

3.4.4 Starting the system (Failover Cluster Manager)

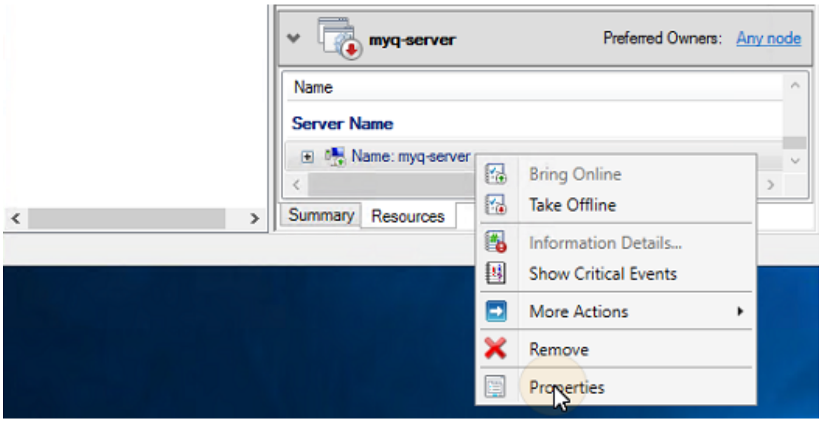
To start the system, you have to bring the resources of the MS Cluster online. For information on how to do this, check here.

3.4.5 Setting hostname of the MyQ server role

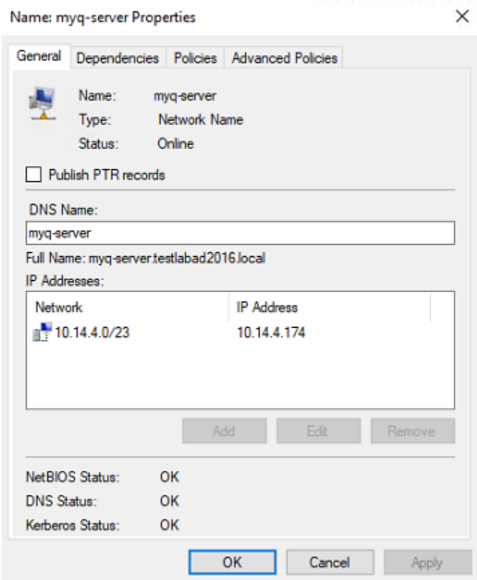
On the **Resources** tab of the MyQ server role in Failover Cluster Manager, you can see (and change) the DNS Name of the MyQ server role. The **Full name** of the role (DNS + domain) needs to be used as the server hostname and as the MyQ X Mobile Client server in MyQ.

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

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



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



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

1. On the **Network** settings tab of the MyQ web administrator interface of the MyQ cluster server, use the **Full name** (DNS + domain) of the MyQ server in 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.

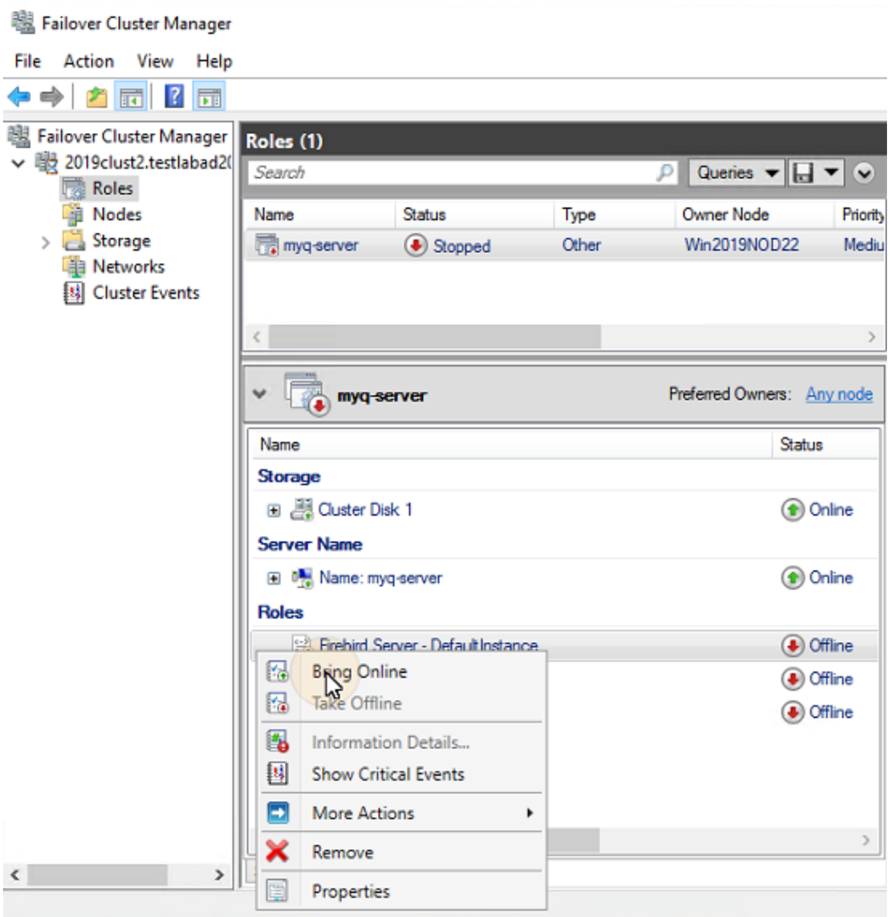
3.5 Configuration and Maintenance

The below chapters show additional configuration and maintenance steps.

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

To start the system, you need to bring all the MS Cluster resources online - the **Firebird Server - 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.

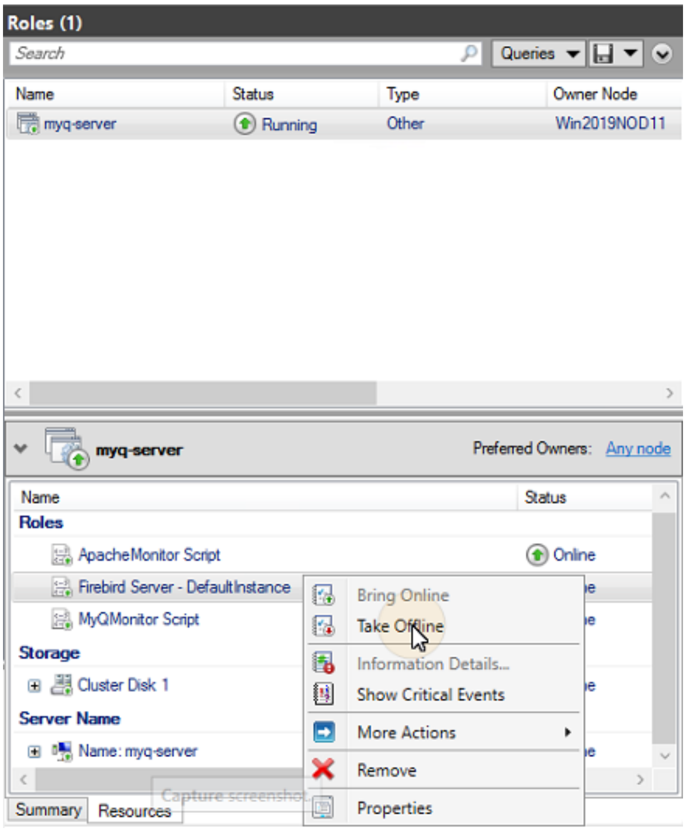


3.5.2 Taking the MS Cluster resources offline (Failover Cluster Manager)

To make sure that all the MS Cluster resources -except for **Storage** and **Server Name**- are offline, it is sufficient to take the **Firebird Server - 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.



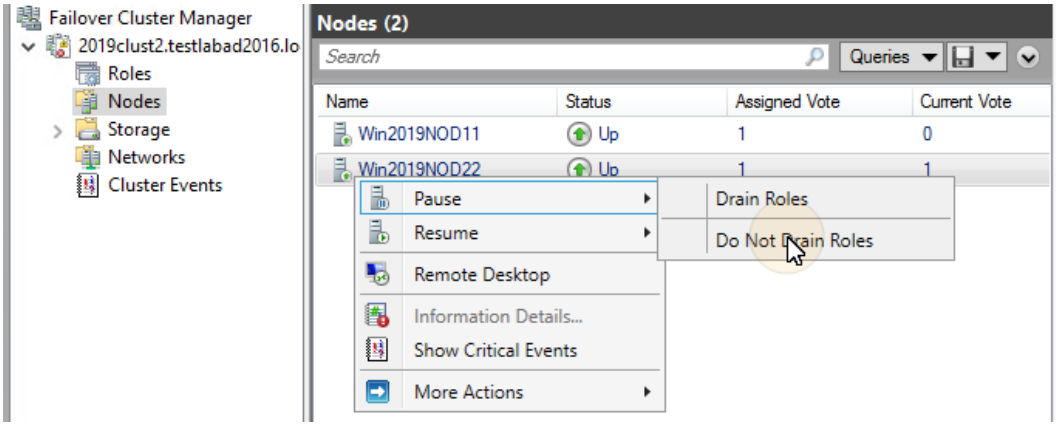
3.5.3 Restarting MyQ services via the MS Cluster (Failover Cluster Manager)

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

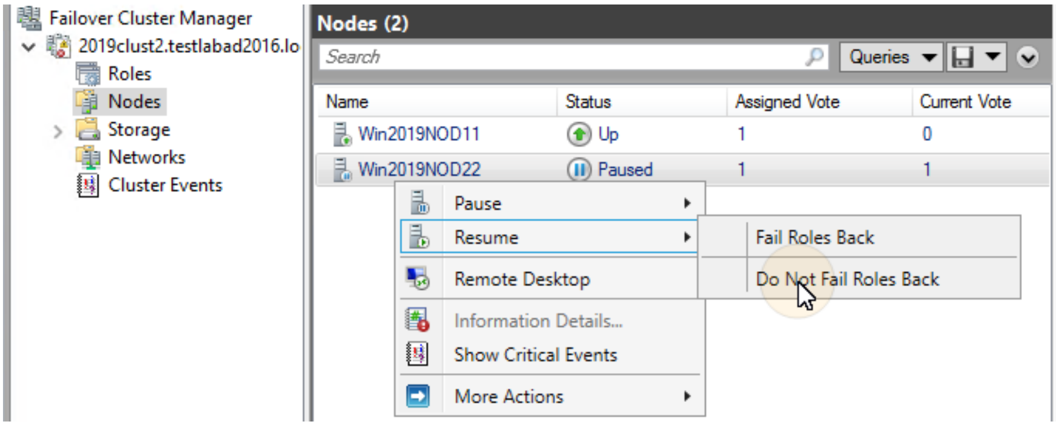
3.5.4 Changing the MyQ admin credentials (active node)

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**.



3.6 Backup and Restore

3.6.1 Backing up the MyQ database on the MS Cluster

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

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

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

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

1. **Start All** services via MyQ 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.

3.6.3 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.

3.7 Upgrading MyQ in a Cluster

3.7.1 Necessary steps before the upgrade

Before starting the upgrade, make sure that you have an up-to-date and properly finished backup of the MyQ database. The database can be backed up either manually in MyQ 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.

3.7.2 Upgrading MyQ (all nodes)

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

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

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

1. **Start All** services via MyQ 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.

3.8 Recommended Troubleshooting

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

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

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

4 MyQ Easy Config

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

It automatically opens if you keep the **Finish installation in MyQ® Easy Config** option selected during the installation of the server. Otherwise, you can find it on the Apps screen in Windows 8.1+, Windows Server 2016 and newer. After you open the application, you see its menu on the left side. From this menu, you can access the following settings:

- On the **Home** tab, you can quickly change the default passwords for the Server and Database Administrator accounts and generate data for support. You can also be redirected to the MyQ Web Administrator Interface to finish the server setup.
- On the **Services** tab, you can view and control MyQ services.
- On the **Settings** tab, you can modify the Windows Services, Server administrator, and Database Administrator accounts, change file paths of the MyQ system data and jobs files, change the port configuration of the MyQ server, and clean up your Cache and Temp folders.
- On the **Security** tab, you can enable/disable unsecure communication, and manage the MyQ DB, the Log Database, and print jobs encryption.
- On the **Database** tab, you can view information about the Main and Log Databases, as well as backup, and restore your database.
- On the **Log** tab, you can view all the operations executed by the MyQ system.
- On the **About** tab, you can view information regarding the current version of MyQ.
- In addition, you can select the MyQ Easy Config display language from the drop-down list.

If there are no issues, the "*It looks good here!*" message is displayed on the Home tab.

4.1 Home

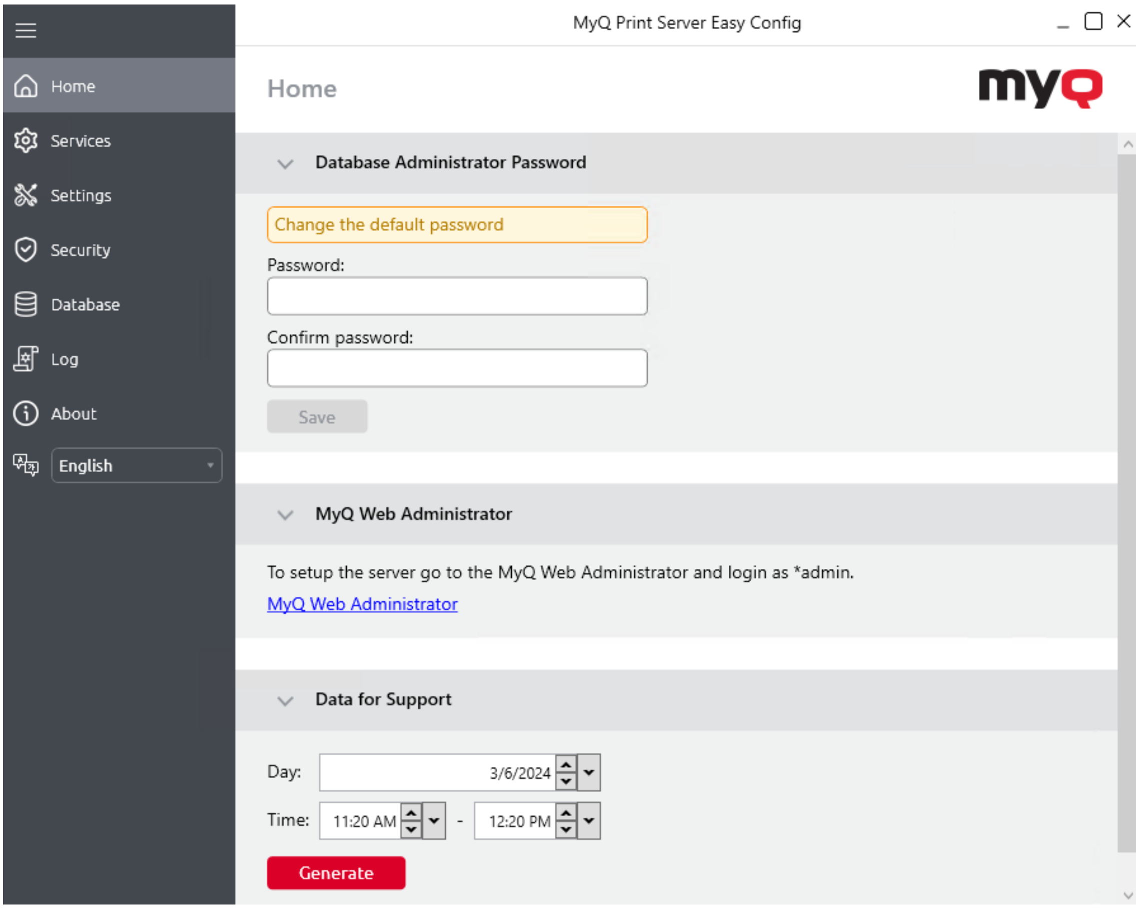
Once you open the MyQ Easy Config application on the Home tab for the first time, you will be prompted to create passwords for the Server Administrator Account and Database Administrator. These accounts will be important for server management and database security.

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.

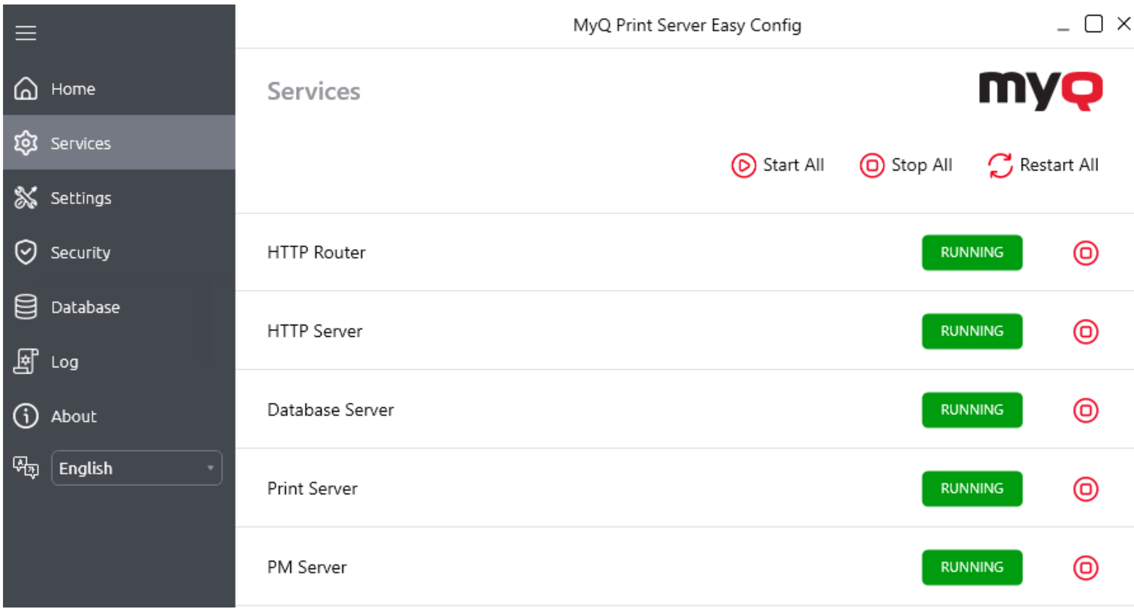


After you change the Server Administrator Account and Database Administrator passwords for the first time, its initial setup section disappears from the **Home** tab. These passwords can be later changed from the **Security** tab.

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

4.2 Services

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

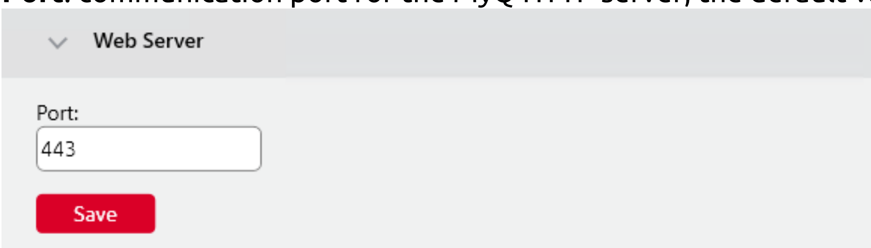


4.3 Settings

4.3.1 Web Server Ports

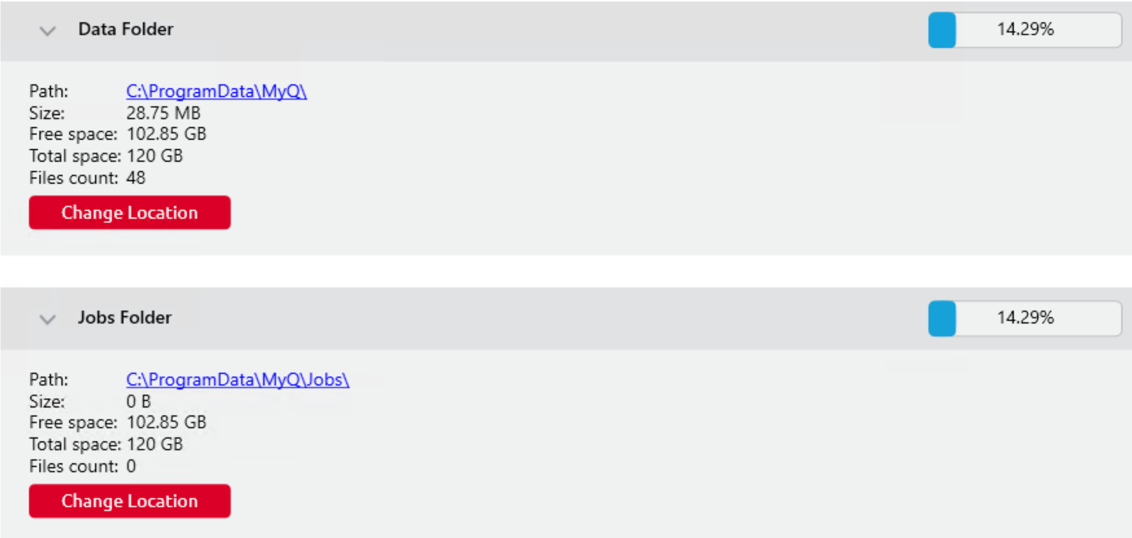
On the **Settings** tab, under **Web Server**, you can change the port for the connection to the MyQ Web server:

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



4.3.2 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 for the database, and *C:\ProgramData\MyQ\Jobs* for the 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:

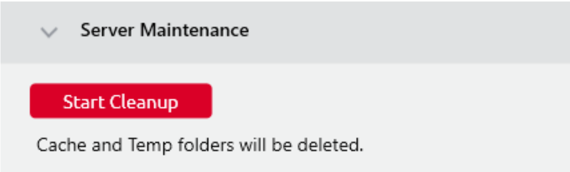
1. On the **Settings** tab, in the respective section, click **Change Location**. The **Change folder location** dialog box appears.
2. In the dialog box, under **New folder**, enter the path to the new folder or click the browser icon and find the folder location.
3. Under **Change Operation**, select 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. You can do this using this guide: https://stackoverflow.com/questions/182750/map-a-network-drive-to-be-used-by-a-service/4763324#4763324 or it should work when you mount the drive on Windows startup.

4.3.3 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.

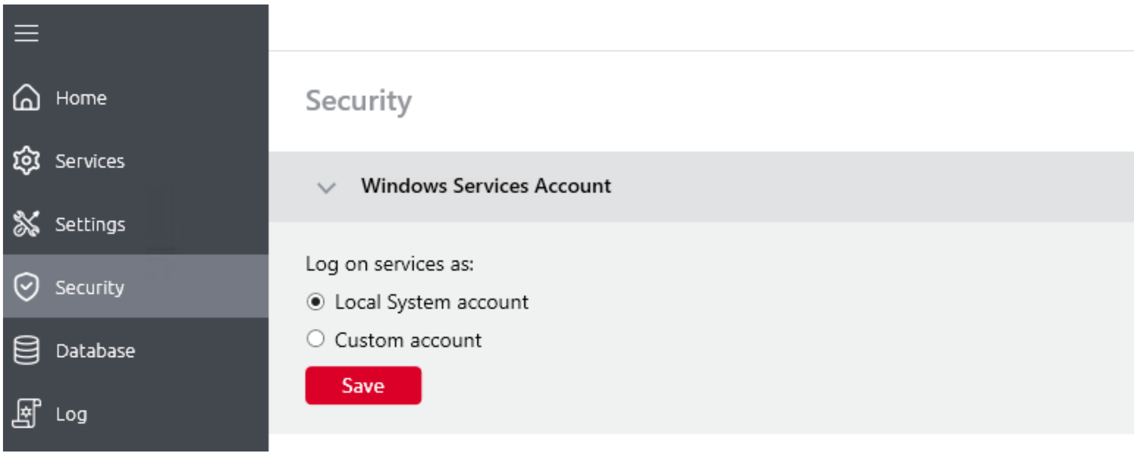
To delete the two folders, click **Start Cleanup**.



4.4 Security

4.4.1 Windows Services Account

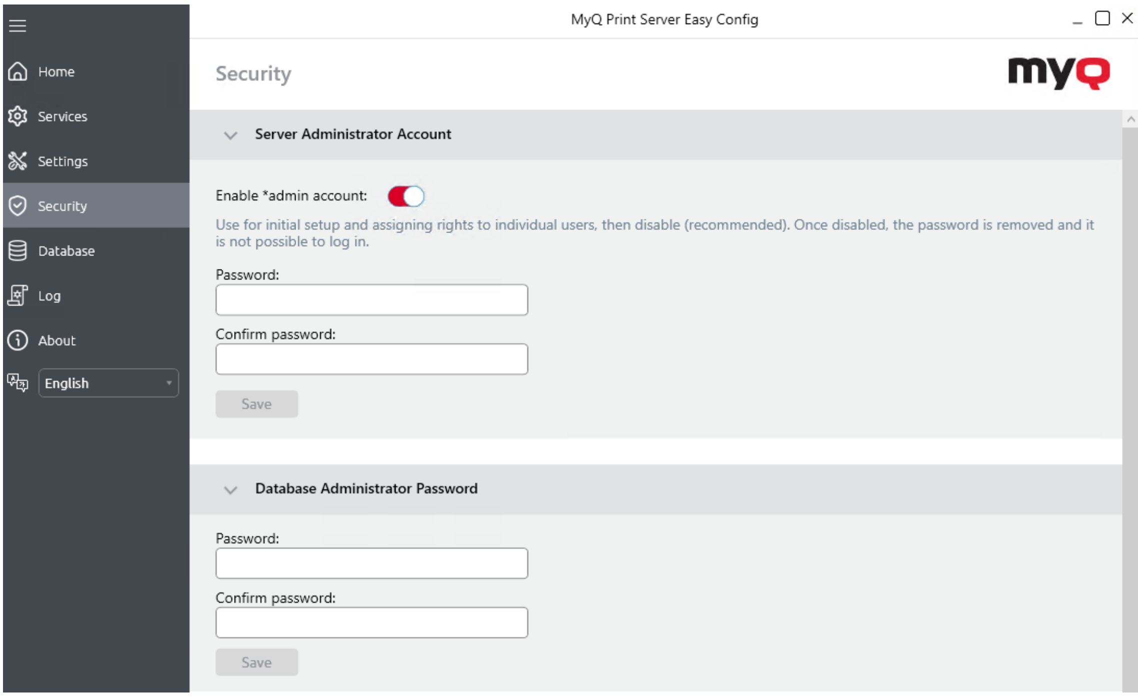
MyQ Windows Services run, by default, under the *Local System* account, meaning the account that was used during the installation.



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

- Under *Log on services as*, select **Custom account**.
- Click on **Browse,** select the user account to be used for 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.

4.4.2 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 user name is *SYSDBA* and its default password is *masterkey*.

4.4.3 Unlocking the MyQ Administrator account

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

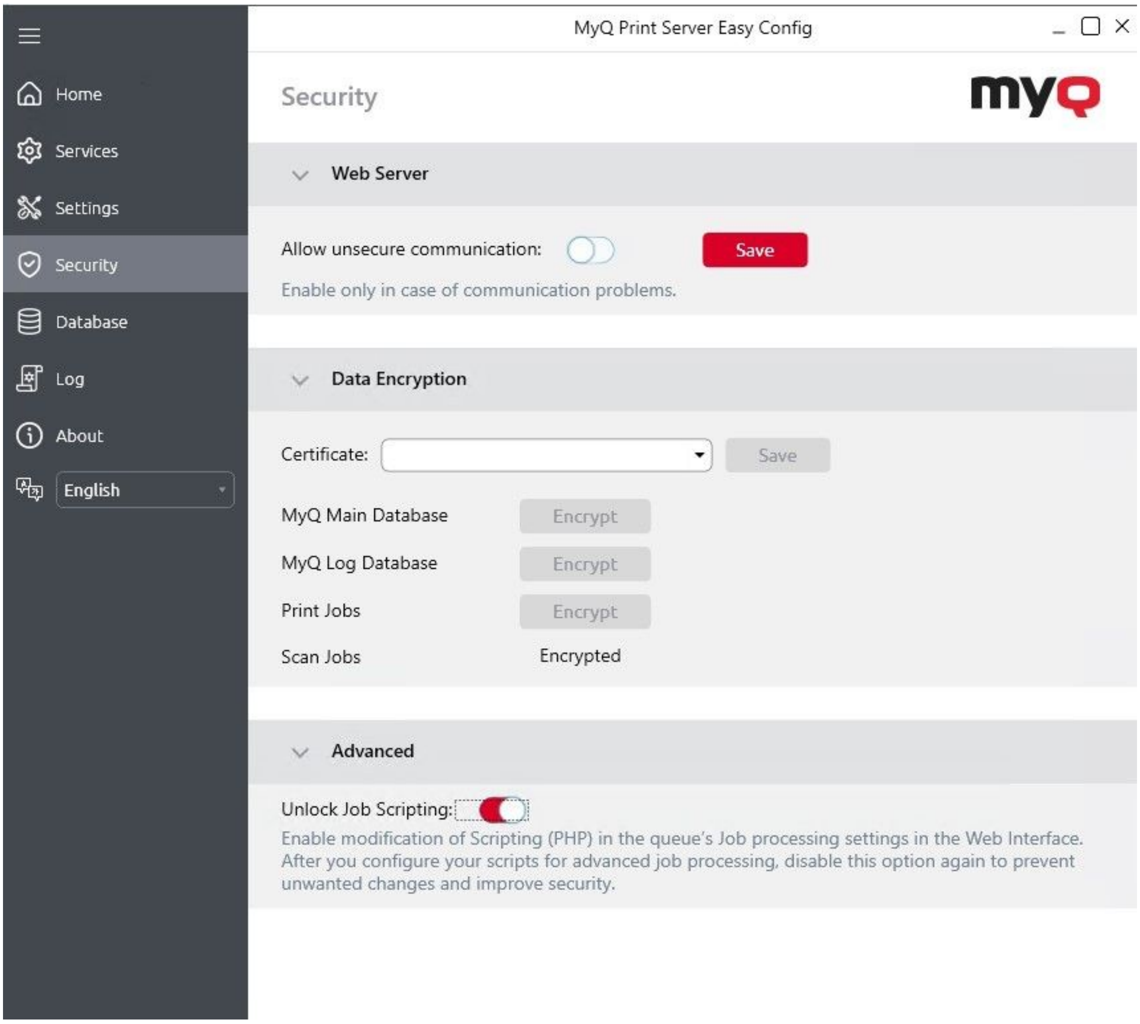
The admin can see a warning that the *admin account is locked, and unlock it, in the **Server Administrator Account** section on the **Security** tab. Once they click **Unlock**, the account is unlocked.

4.4.4 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.

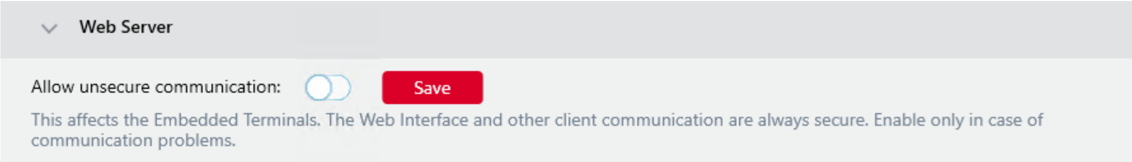


Click **Encrypt** next to **MyQ Main Database**, **MyQ Log Database**, or **Print jobs**. **Scan Jobs** are encrypted by default.

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

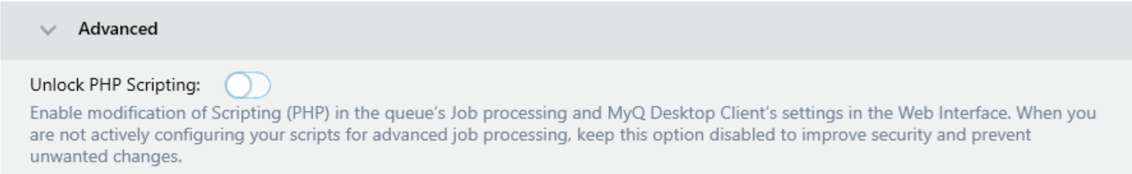
After the encryption, the **Encrypt** button will change to **Decrypt** so you can reverse the action.

4.4.5 Web Server



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

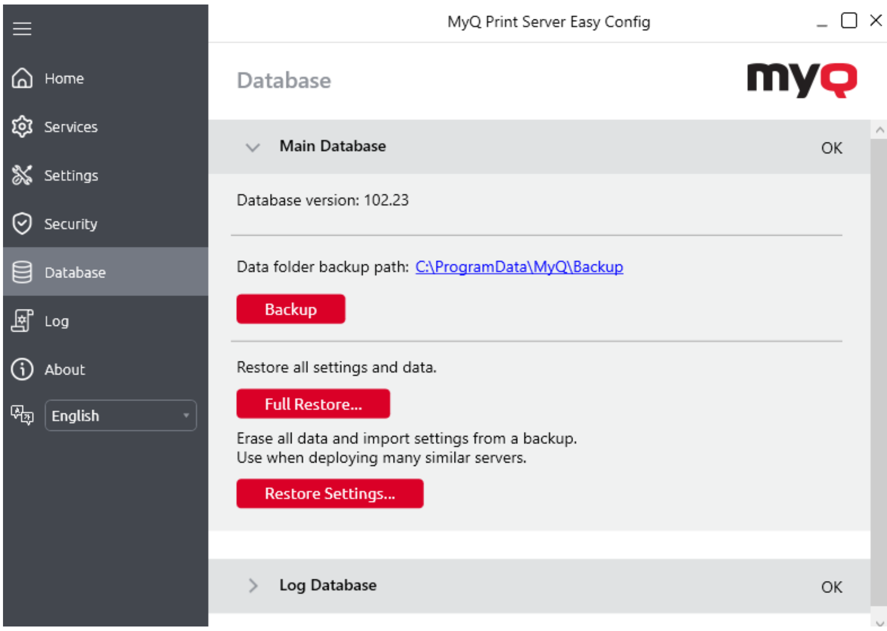
4.4.6 Unlocking PHP Scripting



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.

4.5 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.



4.5.1 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.

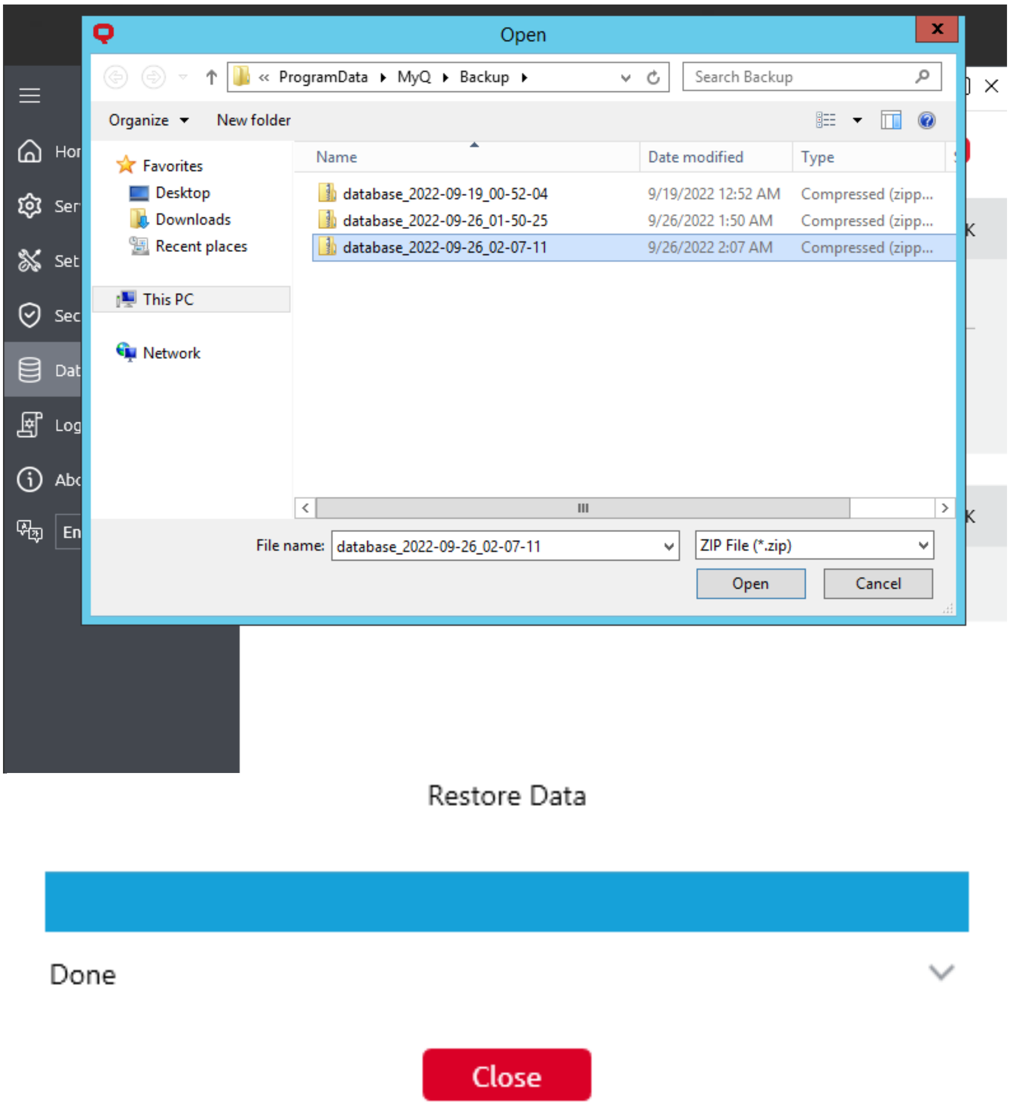
> Print jobs (by default in C:\ProgramData\MyQ\Jobs) are not part of the backup, due to their size.
>
> If required (especially favorite jobs could be required by users after restoring MyQ on the new server), they must be copied and backed up manually or using 3rd-party software.

4.5.2 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.



4.5.3 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.

4.5.4 Embedded Terminals

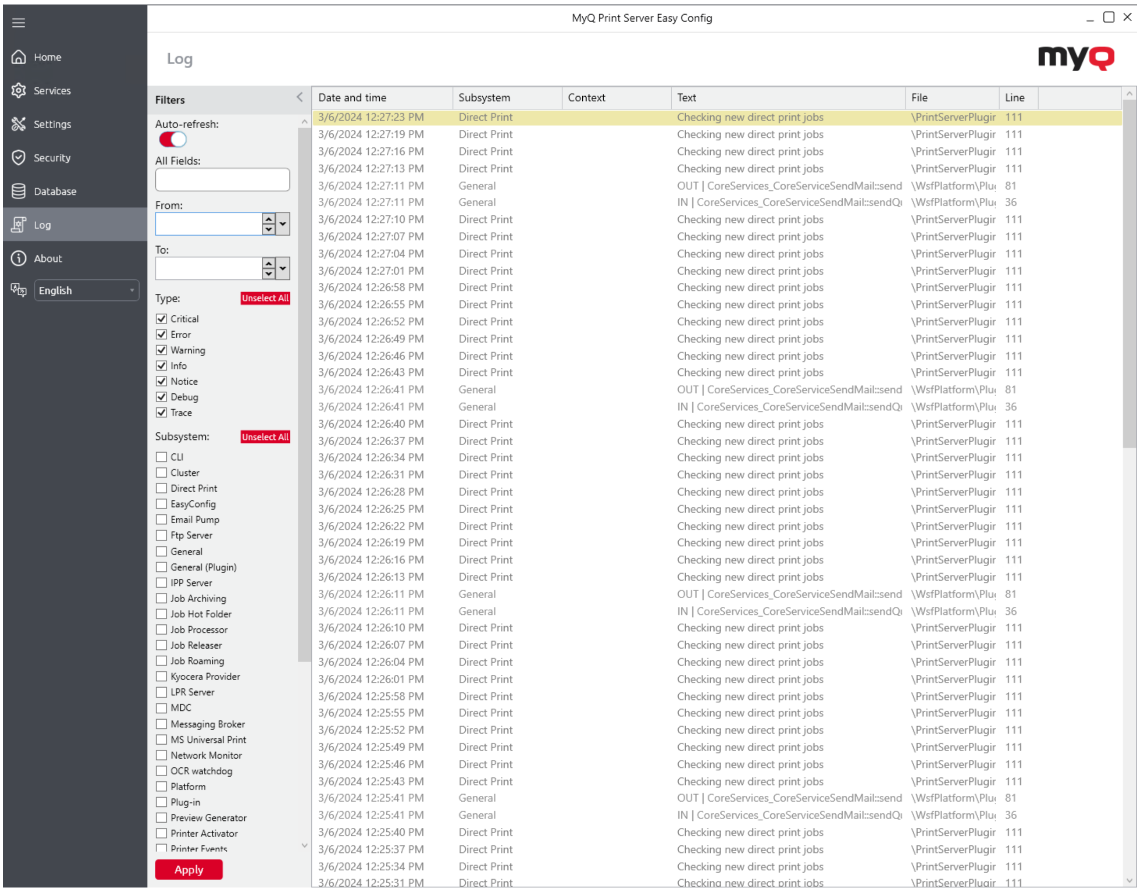
While restoring the database, MyQ checks terminal packages in the database and file system and synchronizes their state:

- 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.

4.6 Log

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


MyQ Print Server Easy Config
Home
Services
Settings
Security
Database
Log
About
English
Log
myQ
Filters
Auto-refresh:
All Fields:
From:
To:
Type:
Unselect All
Critical
Error
Warning
Info
Notice
Debug
Trace
Subsystem:
Unselect All
CLI
Cluster
Direct Print
EasyConfig
Email Pump
Ftp Server
General
General (Plugin)
IPP Server
Job Archiving
Job Hot Folder
Job Processor
Job Releaser
Job Roaming
Kyocera Provider
LPR Server
MDC
Messaging Broker
MS Universal Print
Network Monitor
OCR watchdog
Platform
Plug-in
Preview Generator
Printer Activator
Apply
Date and time
Subsystem
Context
Text
File
Line

5 MyQ Web Interface

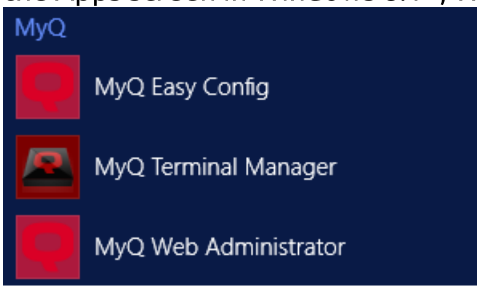
This topic describes the MyQ Web Interface where you manage most of MyQ functions. It shows you how to access the web interface and the two menus where you can access all settings and functions on the web interface: the Main menu, and the Settings menu. Furthermore, it describes the web interface's Home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

5.1 Accessing the MyQ Web Interface

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

There are three ways to open the MyQ Web Interface:

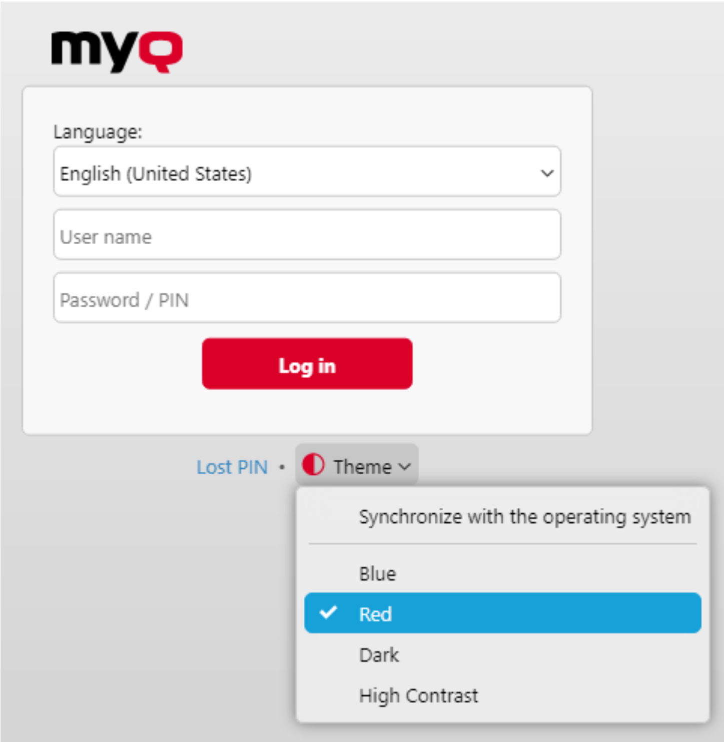
1. Open your web browser, and then enter the web address in the form: *https://*MyQserver*:8090*, where *MyQserver* represents the IP address or the host name of your MyQ server and *8090* is the default port for access to the server.
2. Log on to the interface from the MyQ Easy Config **Home** tab, by clicking on the **MyQ Web Administrator** link in the **MyQ Web Administrator** section.
3. Open the MyQ Web Administrator application. You can find this application on the Apps screen in Windows 8.1+, Windows Server 2016 and newer.



5.2 Logging in as an administrator

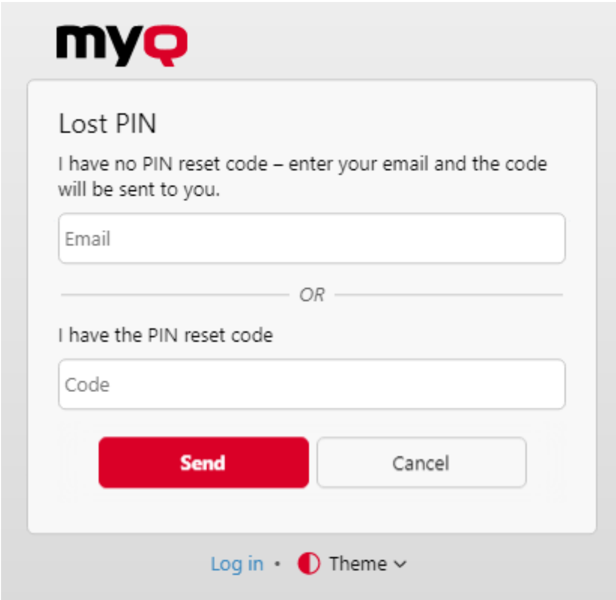
Enter the Server administrator name (**admin*) and the password that you have set in the MyQ Easy Config application, and then click **Log In**. If you have not changed the default password yet (not recommended), enter the default one: *1234*.

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



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

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.



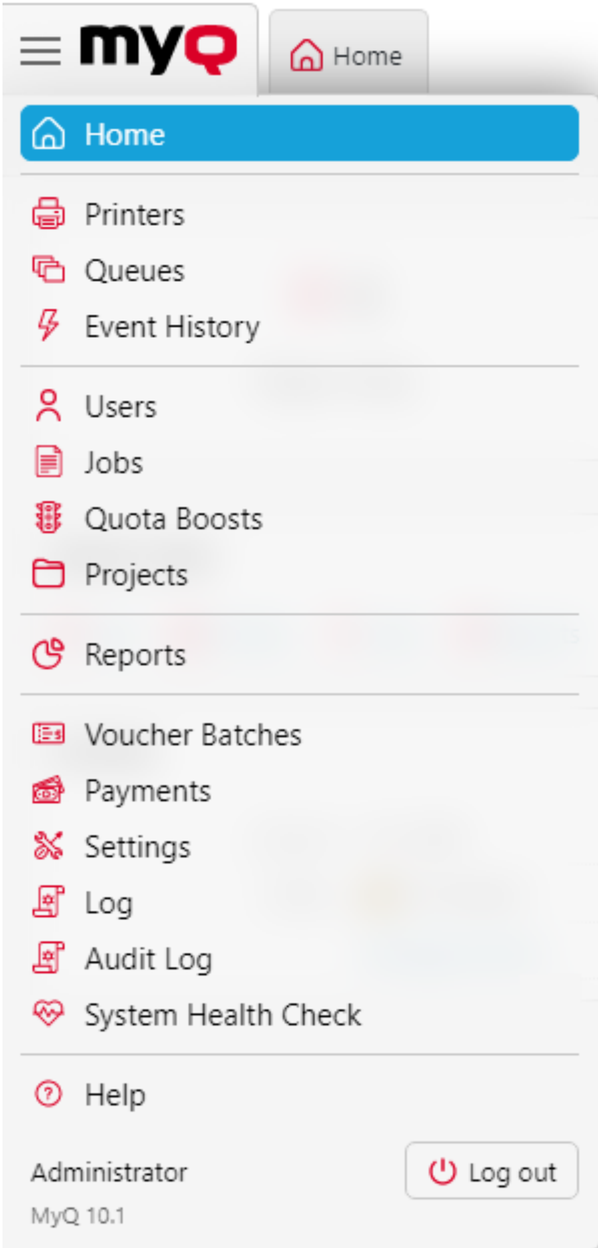
5.3 Main Menu and Settings Menu

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.



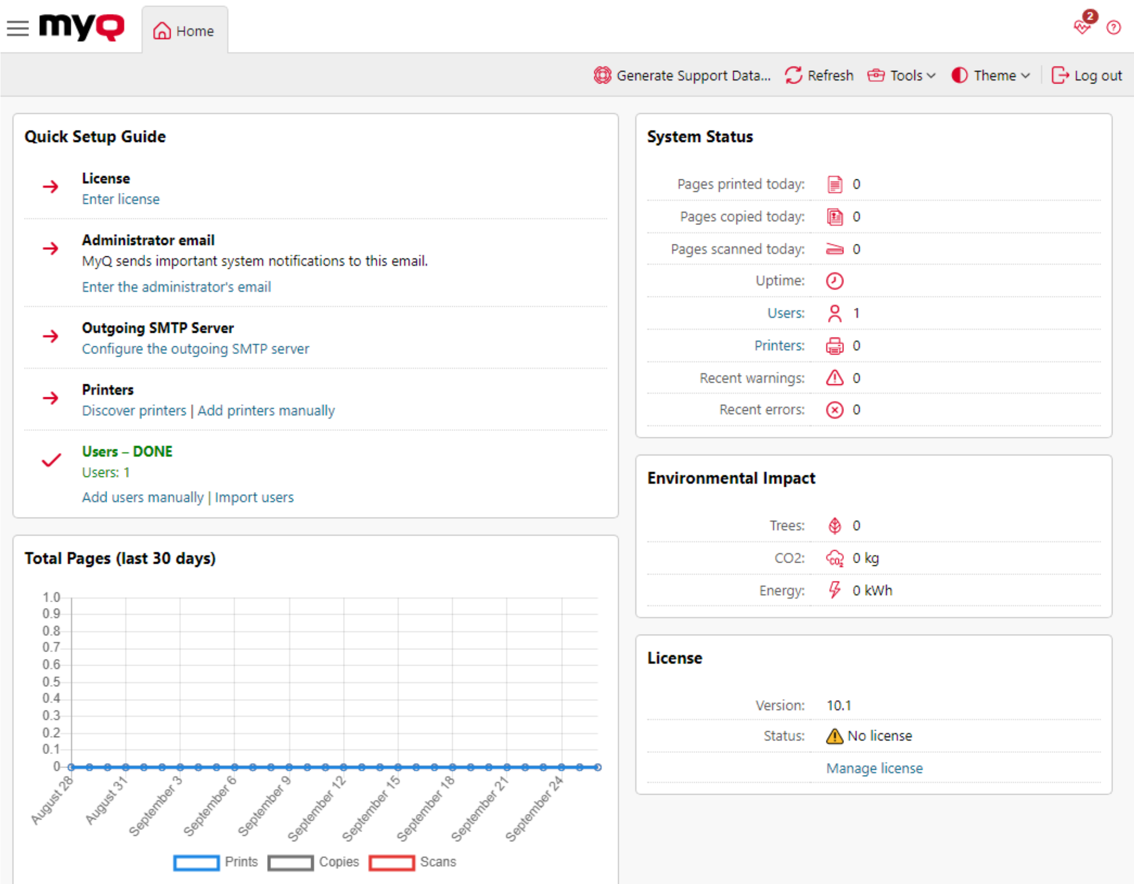
Settings menu

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.

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

By default, there are seven widgets on the dashboard: **Quick Setup Guide**, **System Status**, **Total Pages (last 30 days)**, **Environmental Impact**, **Updates**, **License**, and **Printers with Issue**. Apart from these, you can also add the following widgets:

- **Quick Links**: From the **Quick Links** widget, you can directly access the most important tabs of the MyQ Web Interface: Jobs, Printers, Users, Reports, Settings, and Log.
- **Top Active: Printers**: Shows the most active printing devices.
- **Top Active: Groups**: Shows the most active printing groups.
- **Top Active: Users**: Shows the most active users.

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

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.

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

The **Environmental Impact** widget shows your environmental impact in Trees, CO_2, and Energy.

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

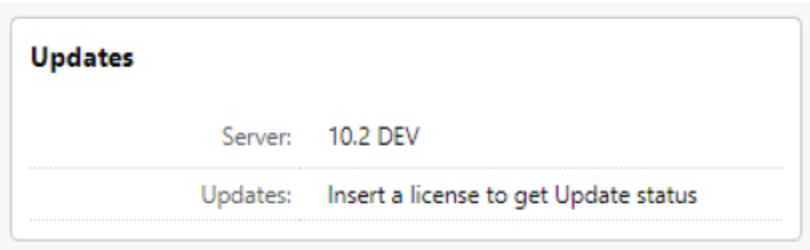
The **Updates** widget shows available updates for the MyQ installation and its components (terminal packages). To get the updates status, a valid license needs to be added to MyQ. Once a license is added, the MyQ administrator (or a user with the Manage settings rights) may see the following:

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

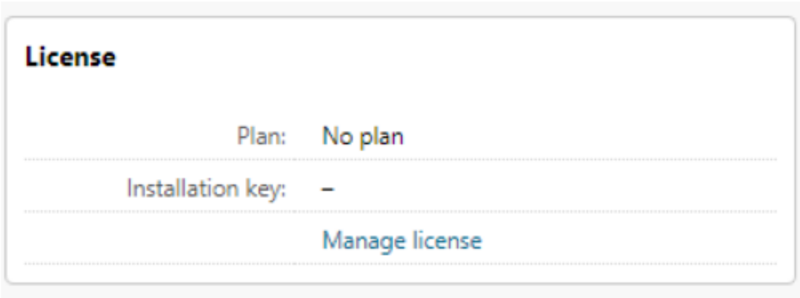
In the event that a license has been installed, the update information may not be immediately downloaded and displayed in the widget. If there is no information about updates, the "**Check now**" button is displayed in the widget. The administrator can manually initiate the retrieval of update information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

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

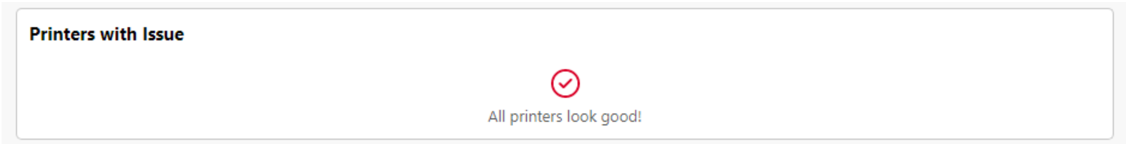
If the server is offline or there are any errors, a warning is displayed on the widget.



The **License** widget shows license information and can redirect you to the **License** settings tab.



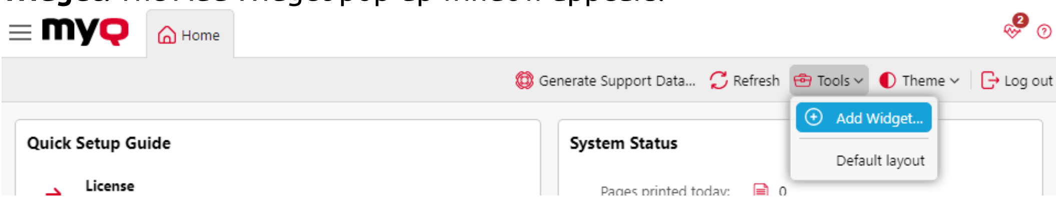
Printers with Issue shows unreachable active printers and active printers with unresolved alerts. You can also see these issues in the **Issues** column, in the **Printers** overview (**MyQ, Printers**).



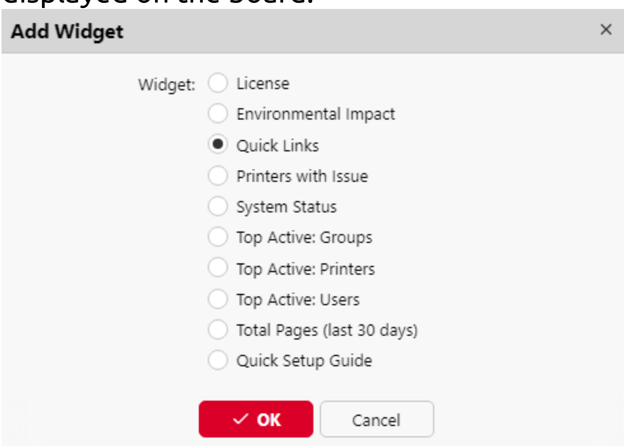
Adding new widgets and moving widgets on the dashboard

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.

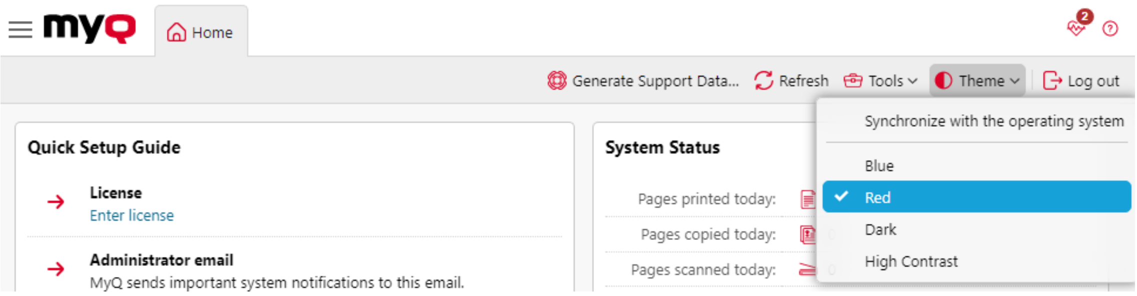
To delete widgets, click on the three dots at the top-right corner of the widget, and click **Remove**.

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

Changing 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



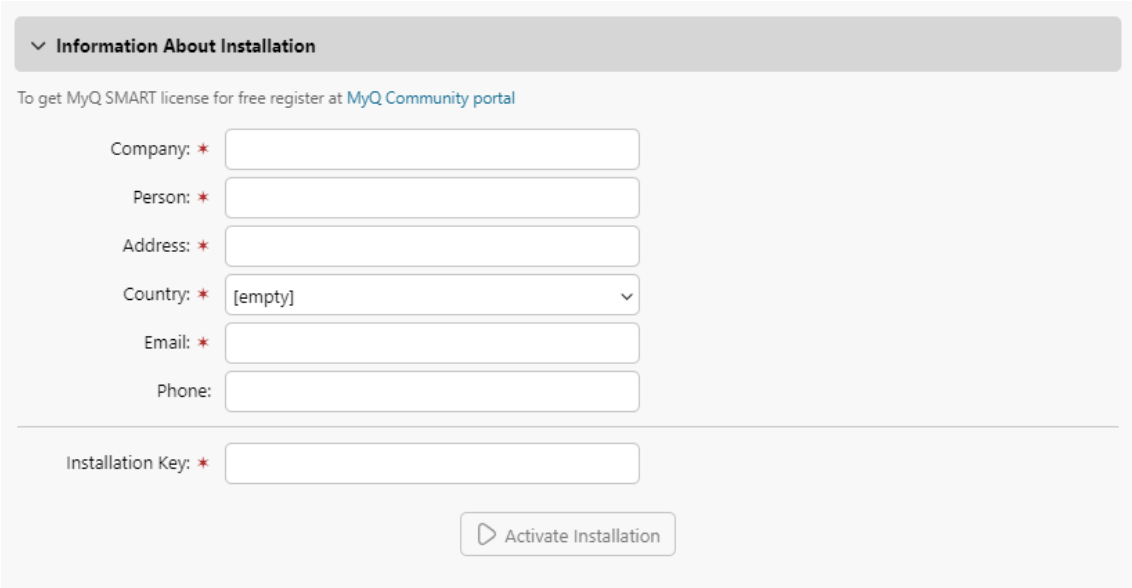
5.4.1 Quick Setup Guide

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

License

Adding and activating licenses

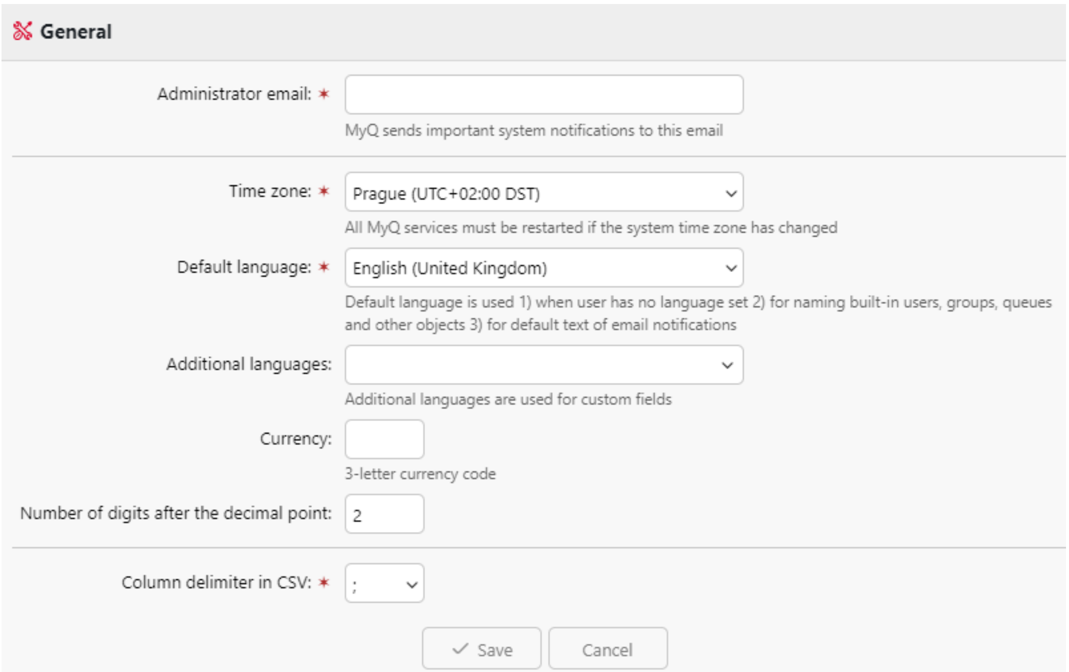
Click **Enter License**. The **License** settings tab opens. You are asked to enter the following information about your installation:



Then, **Enter the installation key** in the field and activate your licenses.

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.

5.4.2 Generate Support Data

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

The *.zip* file includes the **Logs** folder which contains:

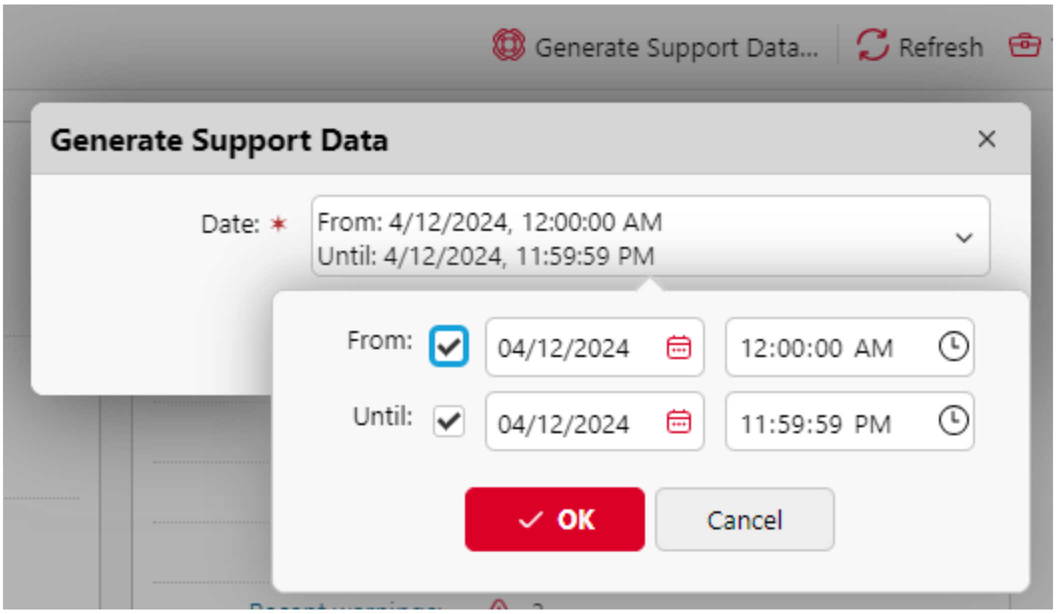
1. MyQ log as XLSX
2. MyQ-helpdesk.xml - XML file with all the necessary information about the MyQ configuration
3. myq.exe dump files
4. Logs, PM Server directories from MyQ's data folder.
5. Logs with Windows events. Currently, there are two logs - one for the Application channel and one for the System channel. The included events are of Critical, Error, and Warning severity.
6. Config.ini, traefic.custom.rules.yaml

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, but they differ from each other.

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

1. Click **Generate Support Data** on the bar at the top-right of the **Home** dashboard. The Generate Support Data dialog box appears.

2. In the dialog box, specify the **Date** range of the MyQ events to include in the *MyQ-helpdesk* file, and then click **Export**. The file is generated and saved to your *Downloads* folder.

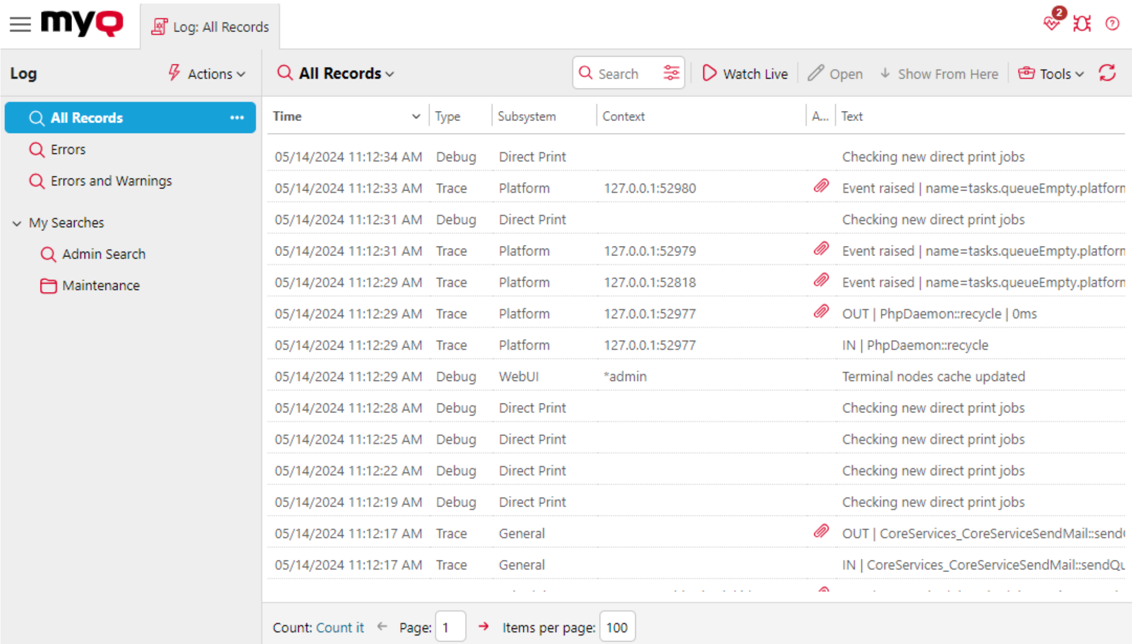


5.5 MyQ Log

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.



5.5.1 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.

5.5.2 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.

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

You can filter the log on the panel:

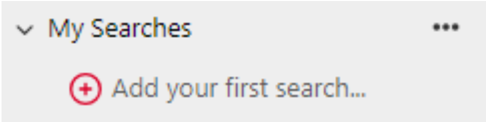
- After you pause the log, you can select the period in the **Date** combo box.
- In the **Verbosity** field you can select the type of log entries you want to view (*Critical, Info, Error*, etc.).
- In the **Subsystem** combo box, you can select/type one or more subsystems to be displayed in the log.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

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

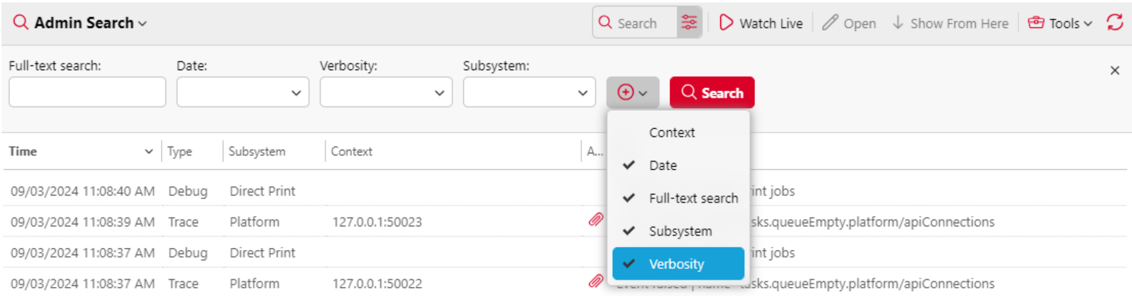
5.5.4 My Searches

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:

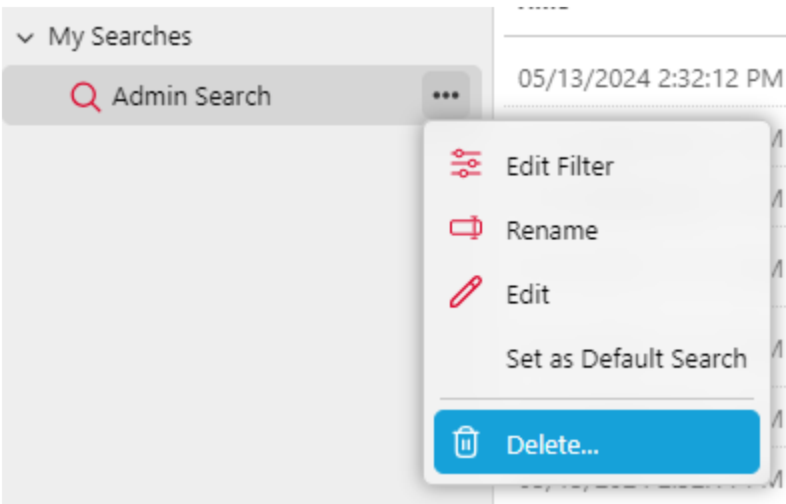
1. Click **Add your first search** or use the context menu and select **Add search** (if saved searches have already been created.



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:

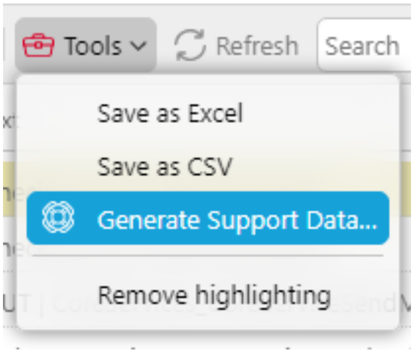


- **Edit Filter:** displays the filter editor for the search.
- **Rename:** allows the user to rename the search.
- **Edit:** opens advanced properties in the right panel including sharing options.
- **Set as Default Search:** sets the search as the default one.
- **Delete:** deletes the search.

5.5.5 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.

5.5.6 Highlighting log messages

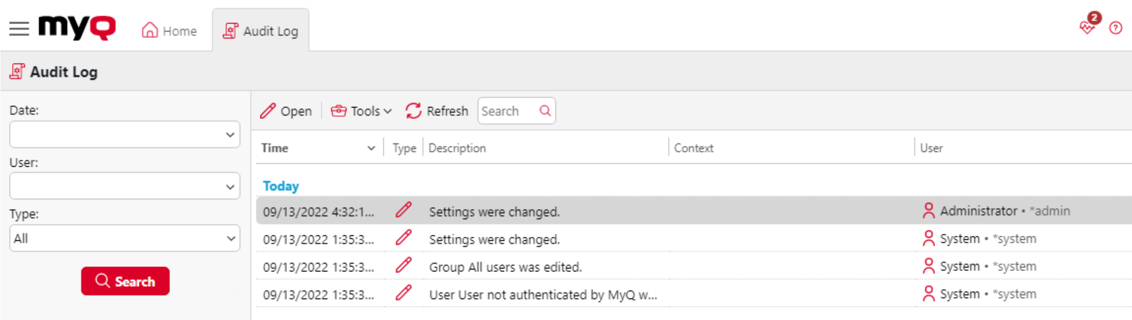
You can highlight particular log messages. To do so, select the message that you want to highlight and then press the **SHIFT + SPACE** keyboard shortcut.

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

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

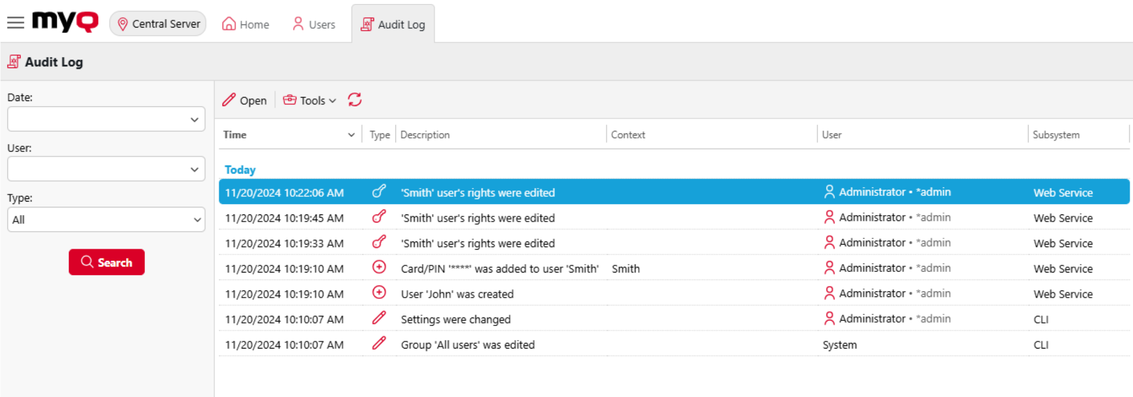
5.6 MyQ Audit Log

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.

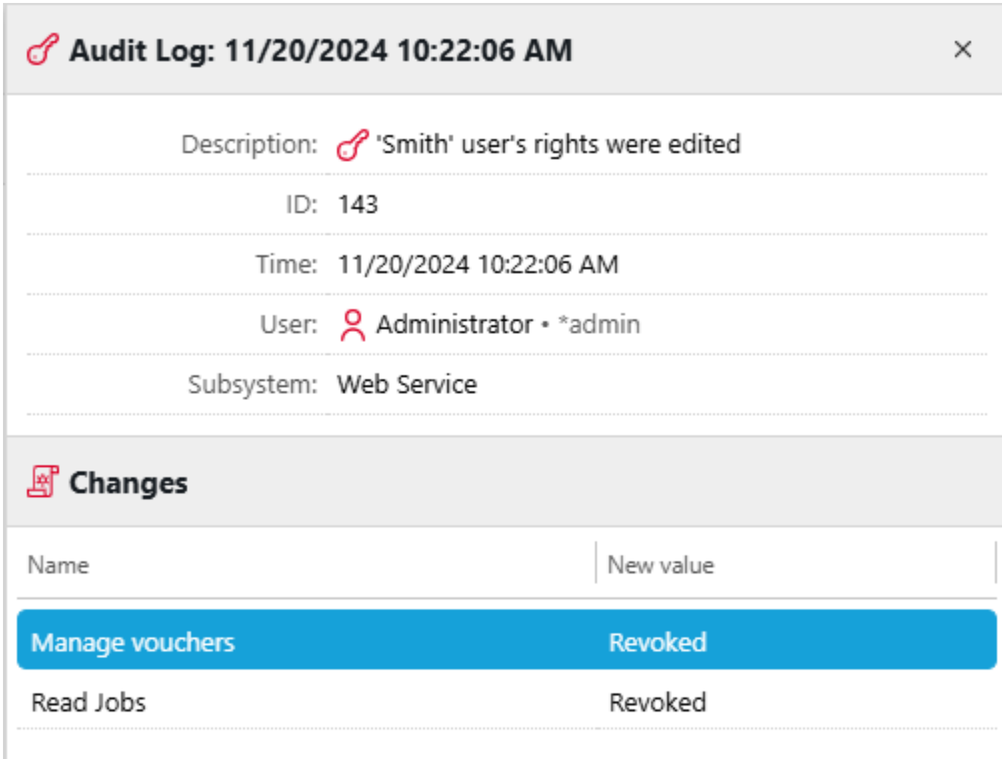


5.6.1 Opening the MyQ Audit Log

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



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



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

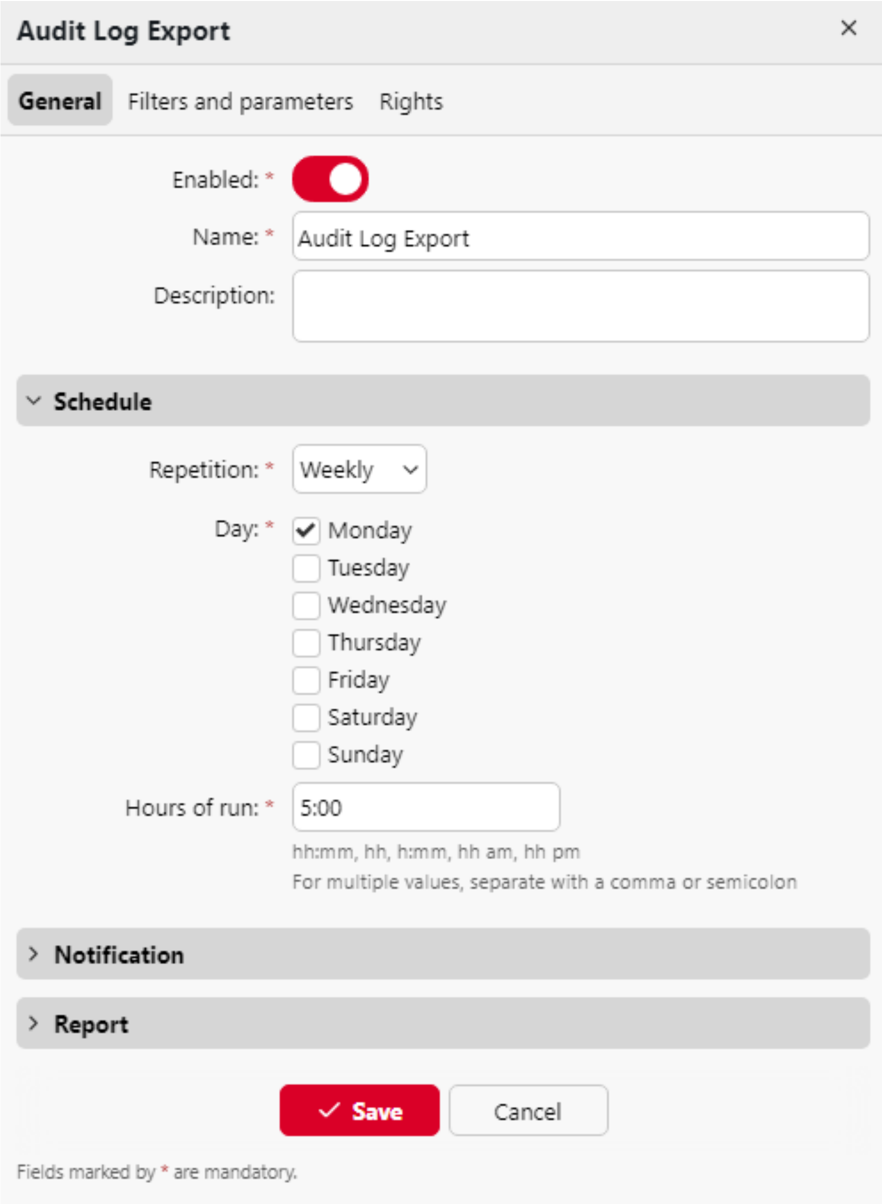
The displayed data can be filtered by a time period, the user who made the changes and the type of the event.

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.

5.6.3 Exporting the Audit Log

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

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



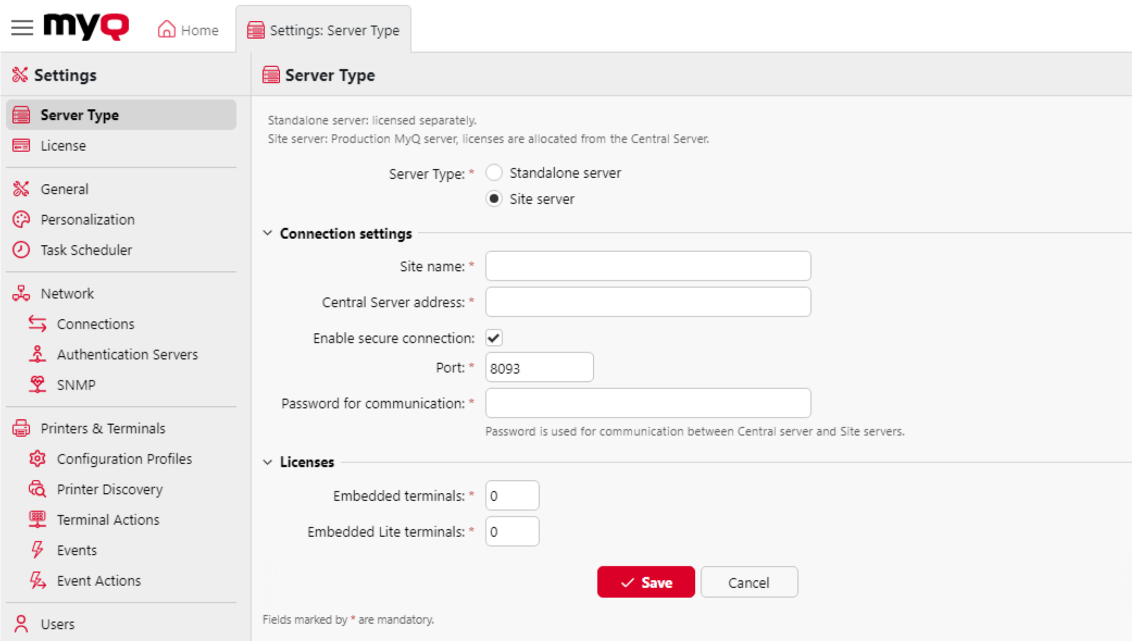
6 MyQ System Settings

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

- In the General settings tab, you can set the administrator email, change regional settings, and other general settings.
- In the Personalization settings tab, you can add custom help links and custom logos to be used in various parts of the MyQ system.
- In the Network settings tab, you can modify network settings such as certificates, server ports, etc.
- In the Authentication servers settings tab, you can add LDAP and Radius servers for user authentication.
- In the Task scheduler settings tab, you can add new task schedules, change their settings and run scheduled tasks.
- In the Log & Audit settings tab, you can set the Log notifier feature, which enables sending notifications about selected log events to the administrator and/or any number of MyQ users.
- In 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.

6.1 Server Type Settings

In the **Server Type** settings tab, the MyQ administrator can set the type of server to use:

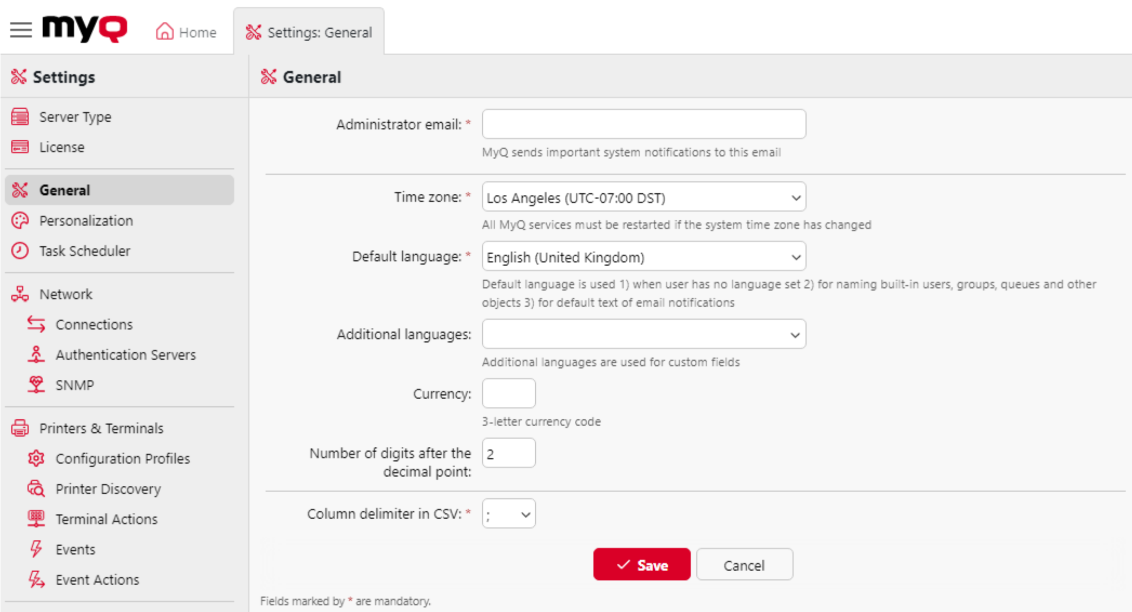


- **Standalone server** - this is enabled by default. It corresponds to the MyQ Print server.
- **Site server** - this option can only be used within a MyQ Central server installation.
  - **Site name** - add a name for your site server.
  - **Central Server address** - add the Central server's host name or IP address.
  - **Enable secure connection** - enabled by default. The connection between the Central server and the Site servers is secure.
  - **Port** - *8093* by default.
  - **Password for communication** - password used for the communication between the MyQ Central server and Site servers.
  - **Embedded terminals** - add the number of embedded terminal licenses to be used on this Site server (distributed by the Central server).
  - **Embedded Lite terminals** - add the number of embedded lite terminal licenses to be used on this Site server (distributed by the Central server).

> ⚠ In older versions, in the **Server type** settings tab, it was possible to switch between the Standalone server, a Site server, or a Central server. This is no longer available, as the MyQ Print server and MyQ Central server are different products and use separate installers. If you have such a setup and plan to upgrade to MyQ Central server 8.2+, be advised that the upgrade will not be successful. It is required to upgrade your system to version 8.1, download the latest MyQ Central server installer, and **migrate** your setup. For more information, see (10.2) Updating MyQ.

6.2 General Settings

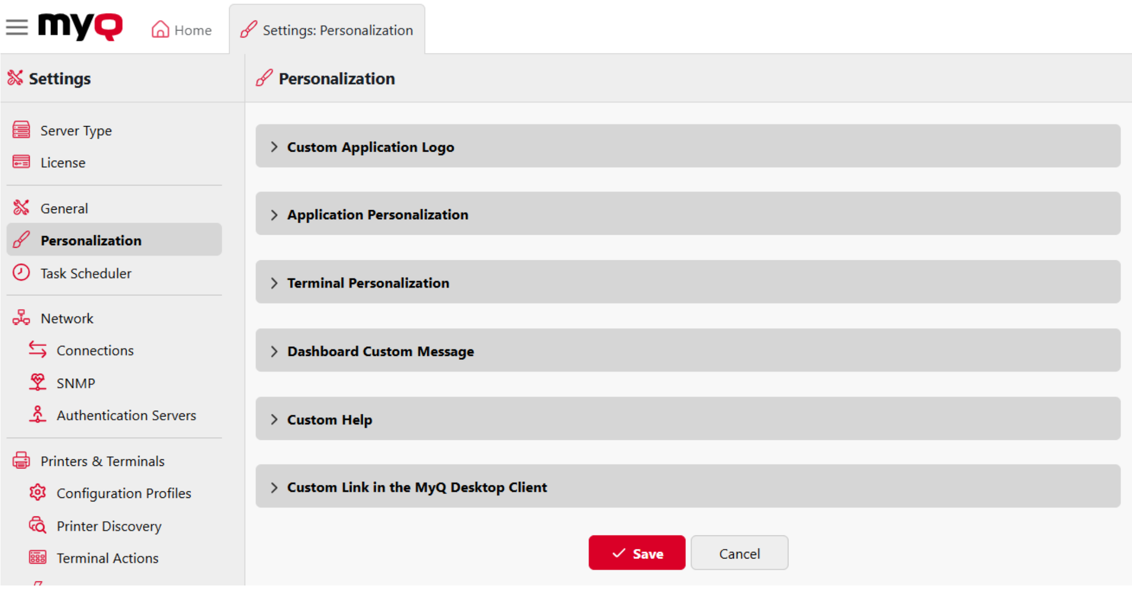
In the **General** settings tab. you can set the administrator email, time zone, default and additional languages, currency, and the column delimiter in CSV files.



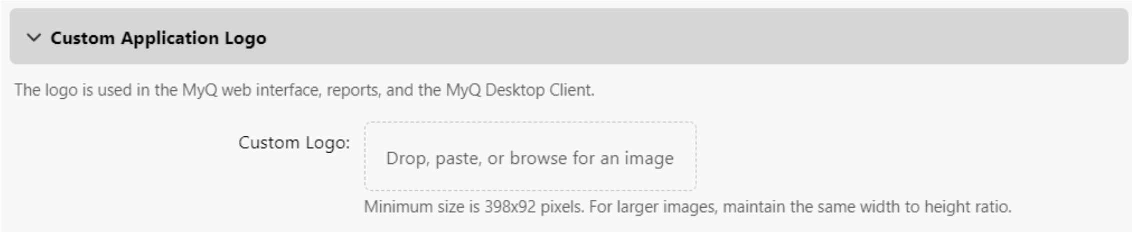
- **Administrator email**: The administrator email receives important system messages (disk space checker warnings, license expiration, etc.) automatically sent from MyQ.
- **Time zone**: For the proper functioning of the MyQ system, make sure that the time zone set here is the same as the time zone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

6.3 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.



6.3.1 Custom Application Logo



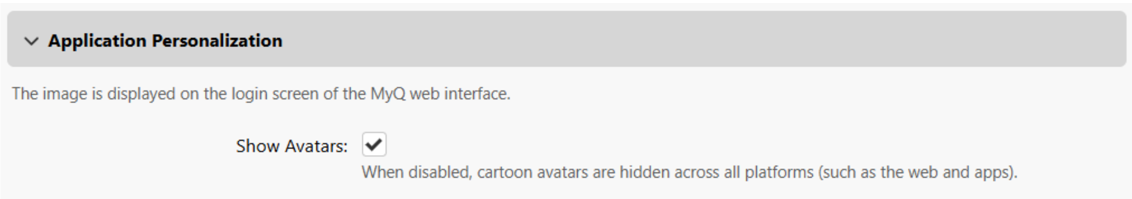
Here you can add your company's logo to be used in the MyQ system. The logo will appear on the upper right corner of the MyQ Web Interface, on MyQ credit vouchers, and on reports.

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.

6.3.2 Application Personalization

Here you can enable or disable the MyQ branding avatars that are generally shown on login screens, currently on the Web Interface. In the future, it will disable these avatars across all platforms (Desktop Clients, Mobile Client, etc.).

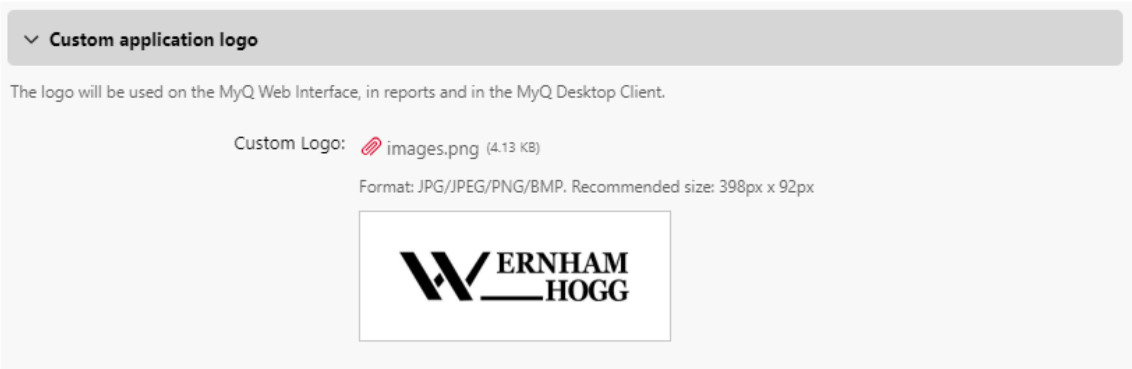


6.3.3 Terminal Personalization

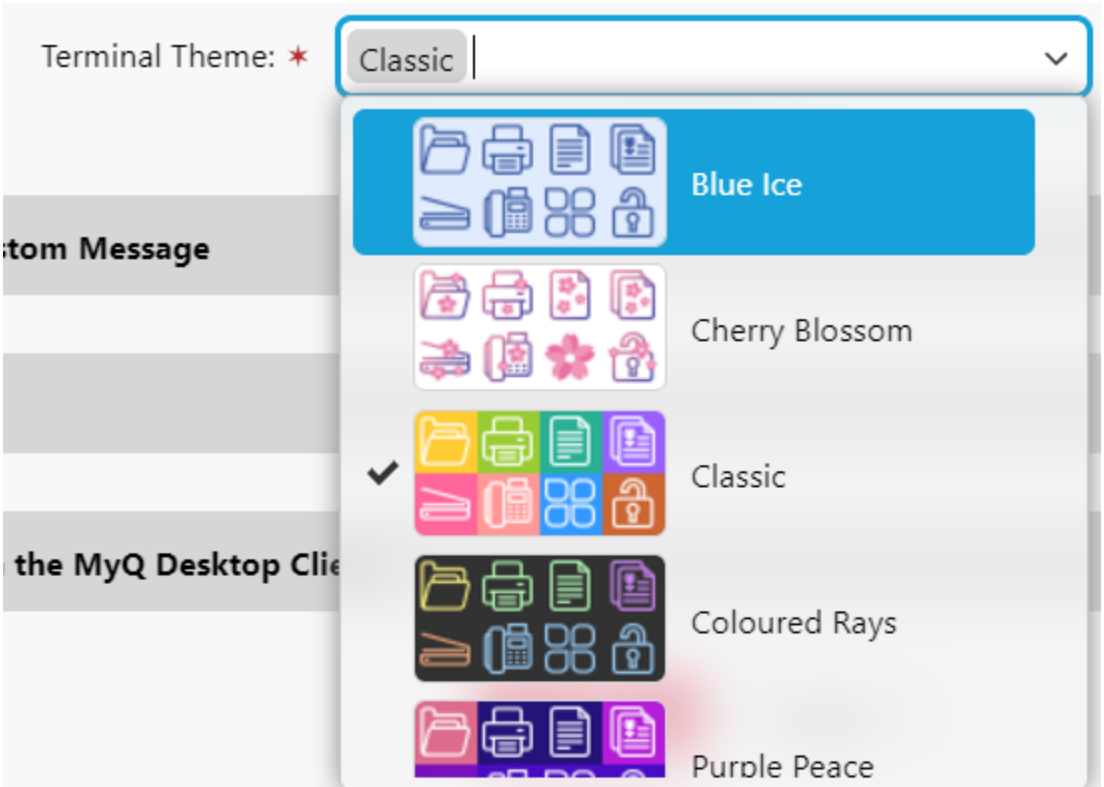
Here you can add your company's logo to be used on all your MyQ embedded terminals.

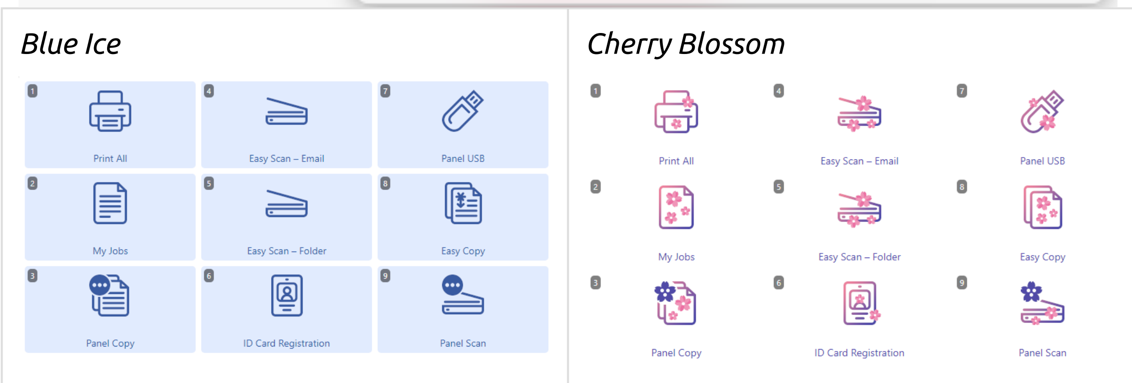
Supported formats are *JPG/JPEG/PNG/BMP* and the recommended size is *340px* x *92px*.

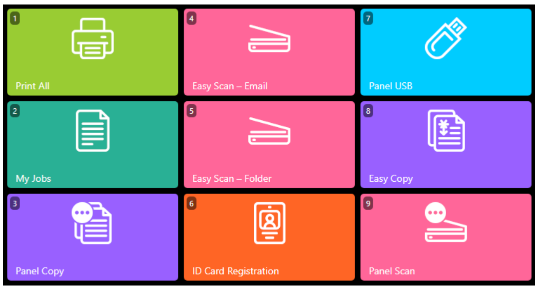
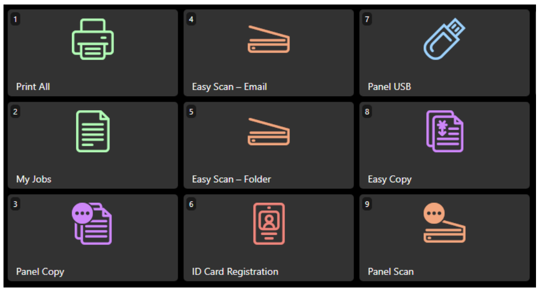
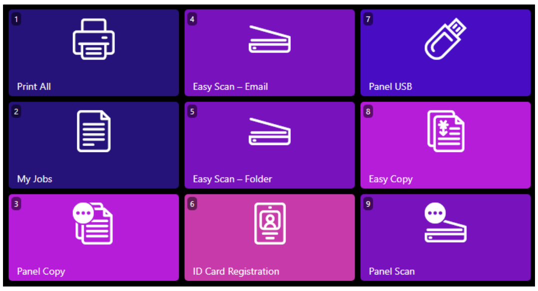
To import the custom logo, click **+Add**, **Browse** for the file and **Open** it, and then click **Save** at the bottom of the tab. A preview of the new logo is displayed on the tab.



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





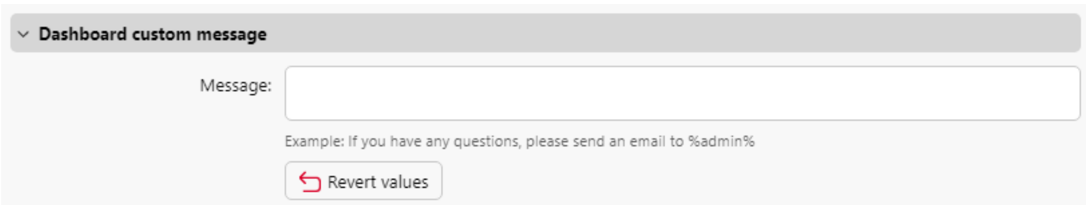
Classic 	*Colored Rays* 
Purple Peace 	*Spring Touch (Default)* 

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.

6.3.4 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.

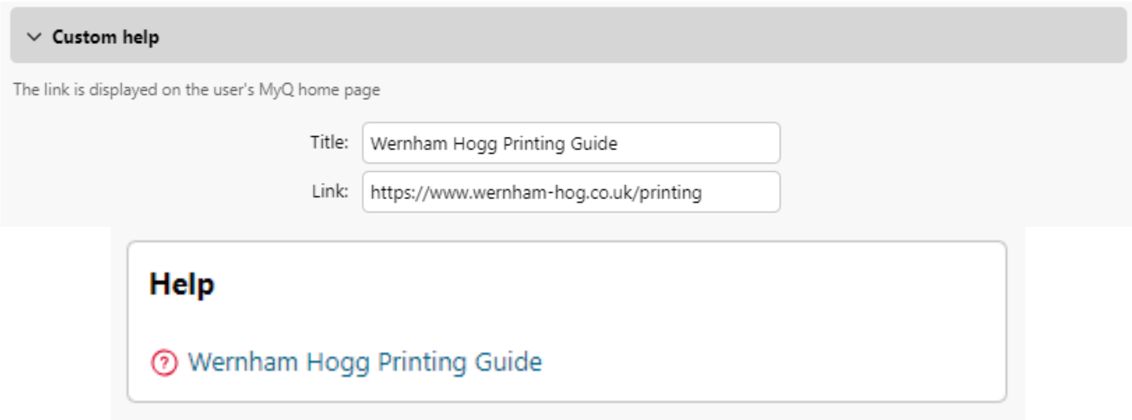
The *%admin%* parameter can be used to display the email address of the MyQ administrator within the message (the Administrator email set on the General settings tab).



6.3.5 Custom Help

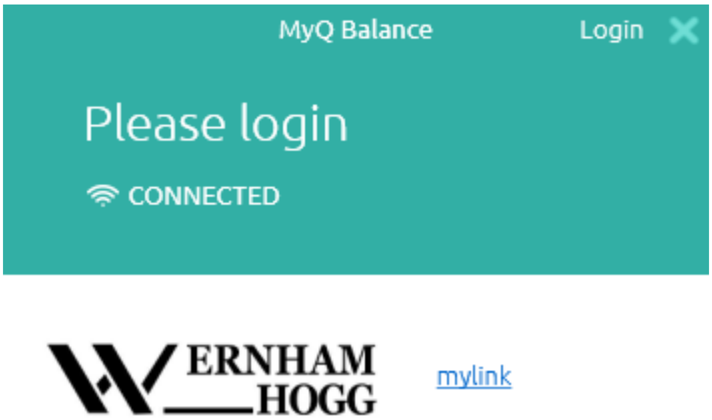
Here you can add a link to your own web-based help that will be displayed as a widget on the user's MyQ home page.

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.



6.3.6 Custom Link in the MyQ Desktop Client

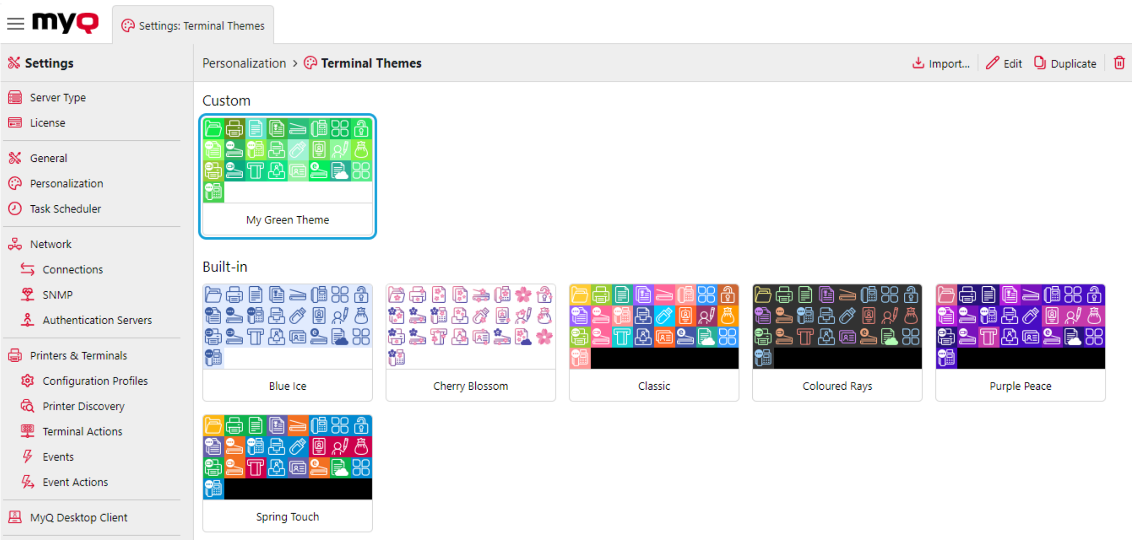
Here you can add a link to your own web-based help (weblink, network path or local path) that will be displayed in the MyQ Desktop Client.



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.

6.3.7 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 the MyQ Theme Editor App.
- **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.

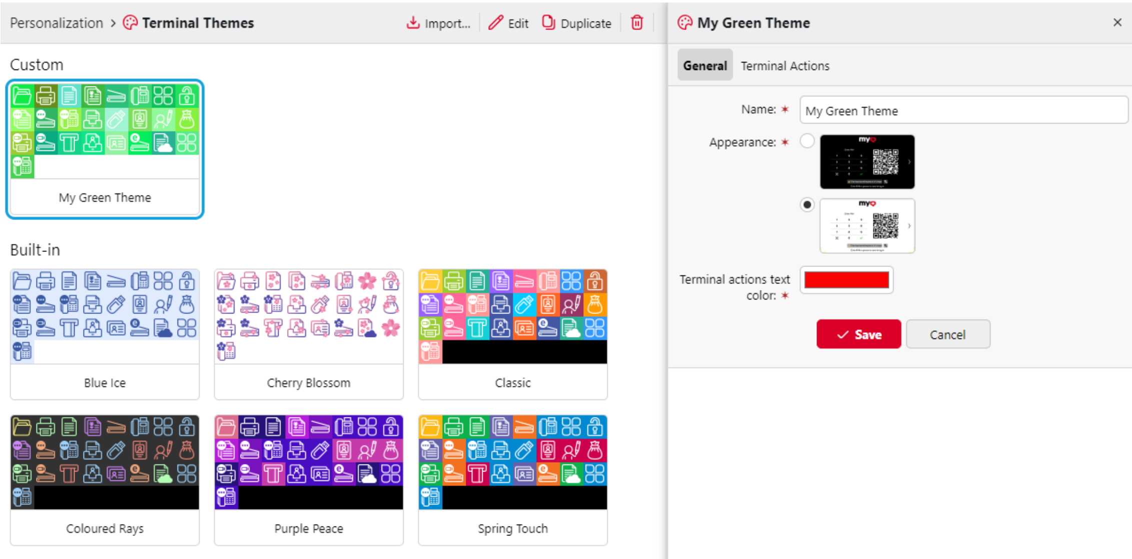
Select a built-in theme and click **Duplicate** to create an identical custom theme. This custom theme can then be edited.

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 further edited in Terminal Actions Settings.

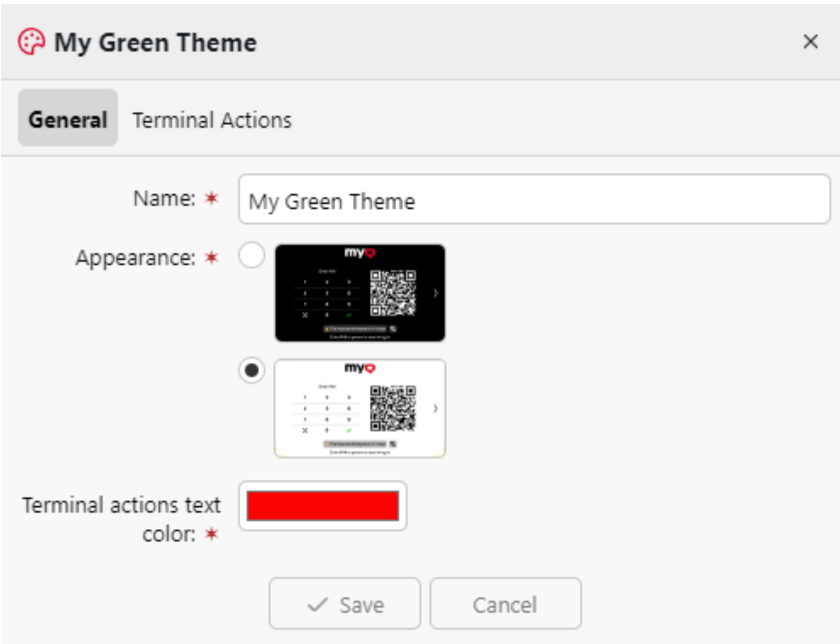
For example, in the terminal theme editor you can create a theme where, by default, **Easy Scan** actions are green and have a scanner icon. However, after creating an **Easy Scan** action to **Scan to Dropbox**, that action node can be edited in Terminal Actions Settings to display a Dropbox logo and 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:



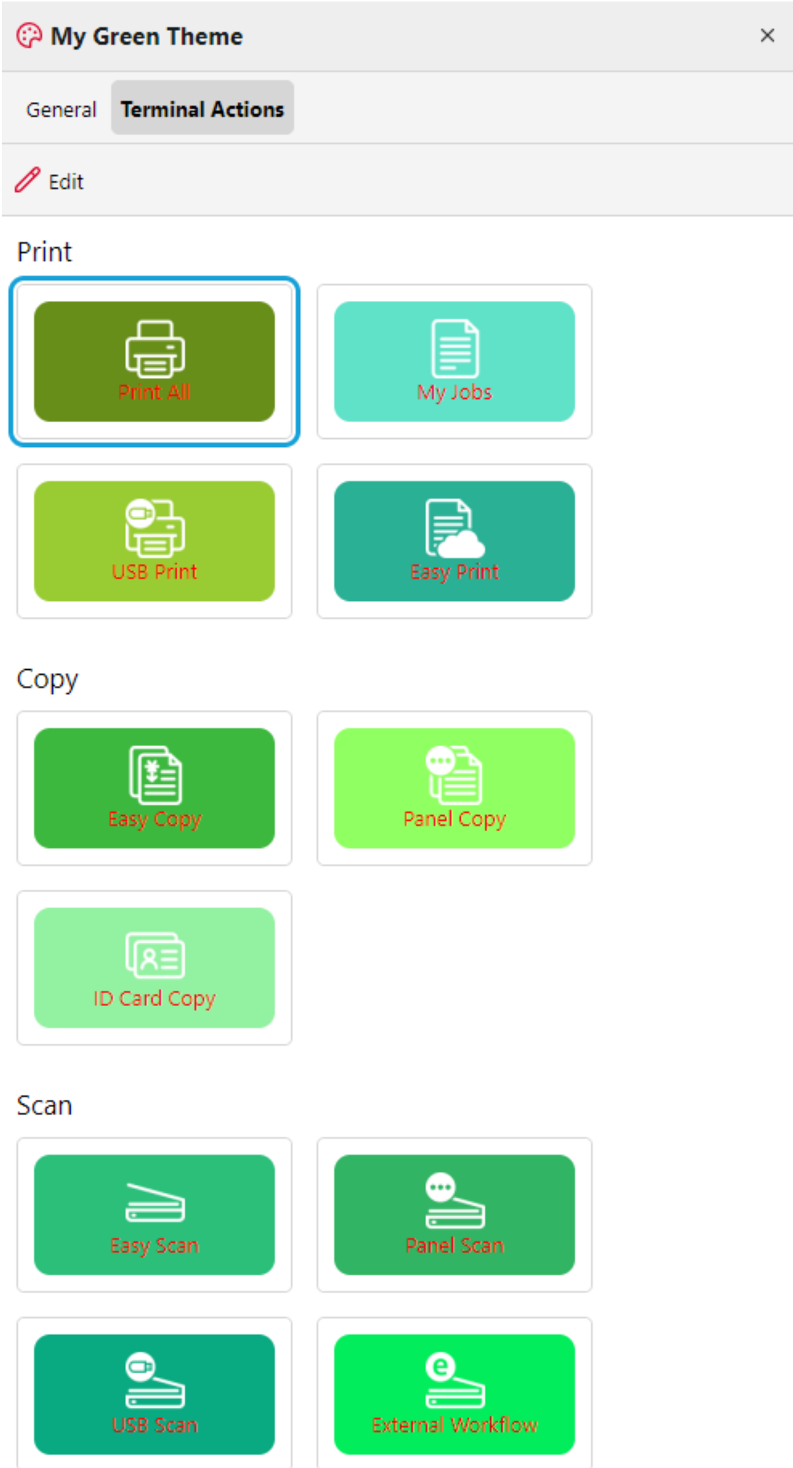
- **Name**: the name of your custom theme.
- **Appearance**: choose black or white as the background color of your theme.

- **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.

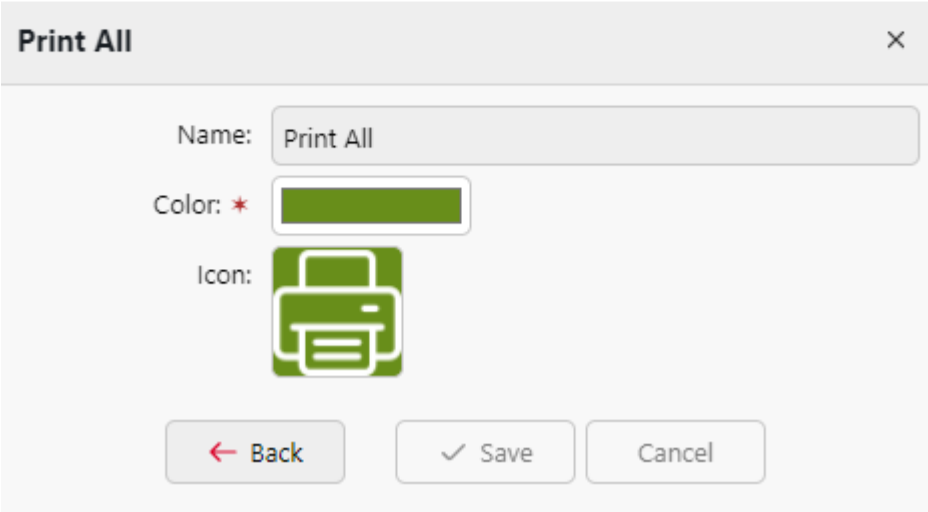
Terminal Actions Tab

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.

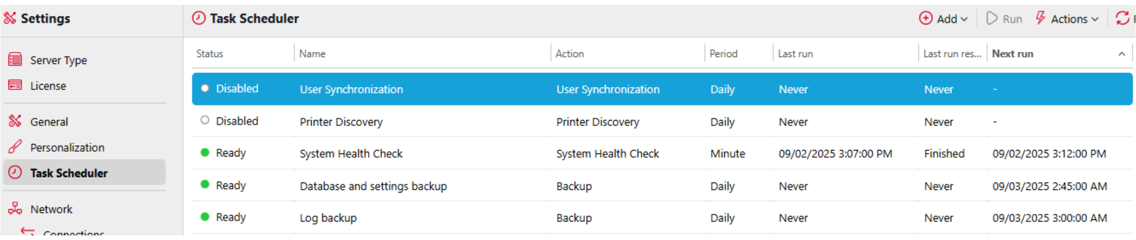
Click **Save** to save your changes and **Back** to return to the previous menu and select another terminal action to edit.

6.4 Task Scheduler Settings

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

Database and settings backup, Log backup, System Health Check, History deletion, Printer Discovery, System maintenance, and **User Synchronization**.

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



6.4.1 Running and setting task schedules

To manually run a task schedule:

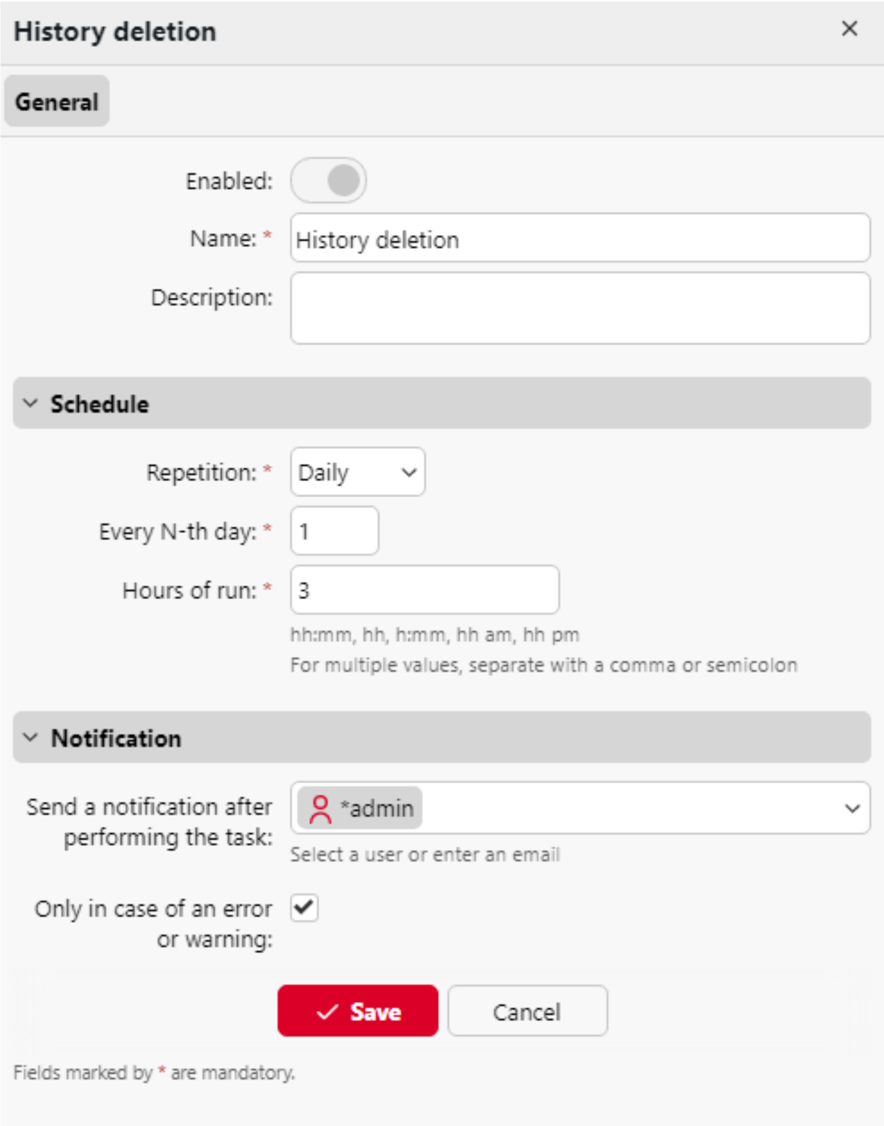
- Select the task schedule that you want to run.
- Click **Run** on the **Task Scheduler** toolbar.

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, is particular to the type of task. It contains options such as the format of an export, the settings of a synchronization/discovery, or a destination folder.

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

6.4.2 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.
- **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.

6.4.3 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:

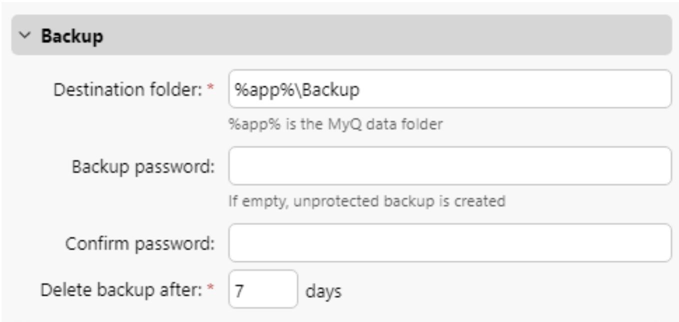
1. Double-click the schedule that you want to set. The respective schedule properties panel opens on the right side of the screen.
2. On the bar on the upper-left corner of the panel, click **Rights**. The **Rights** tab opens.
3. Click **+Add user**. The Select user or group dialog box appears.
4. Select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

6.4.4 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.

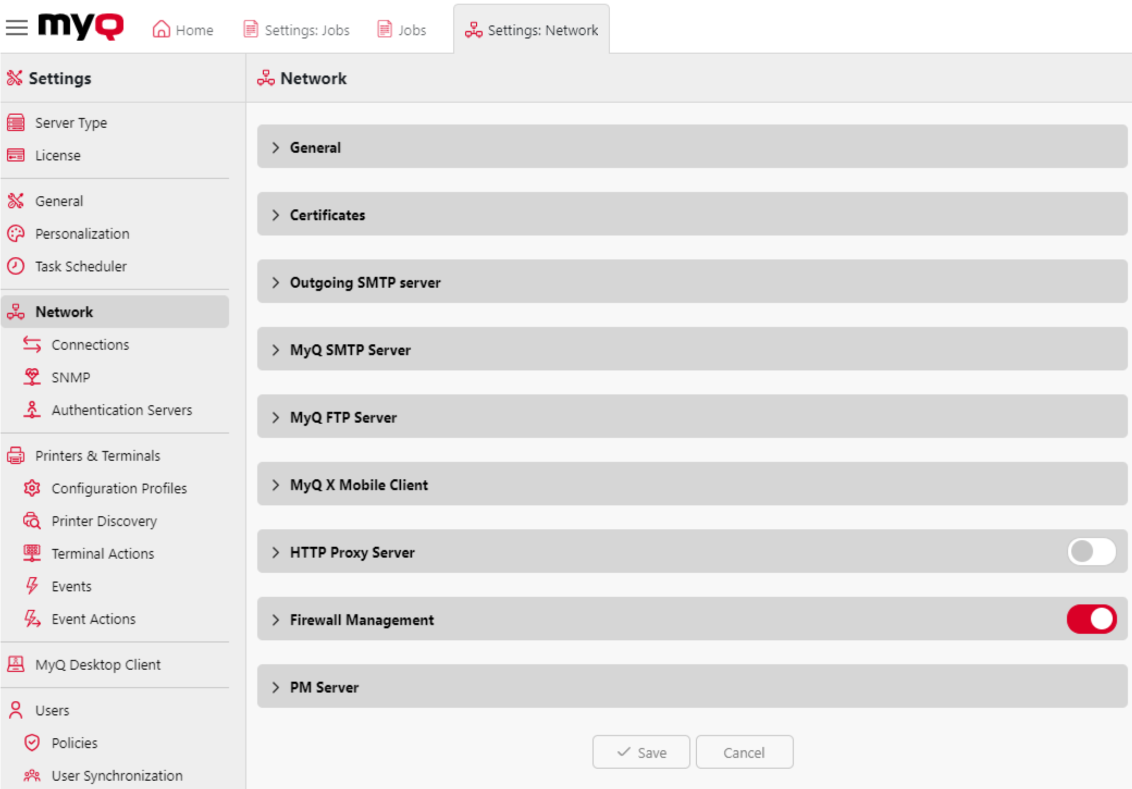
Backup settings

- **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.



6.5 Network Settings

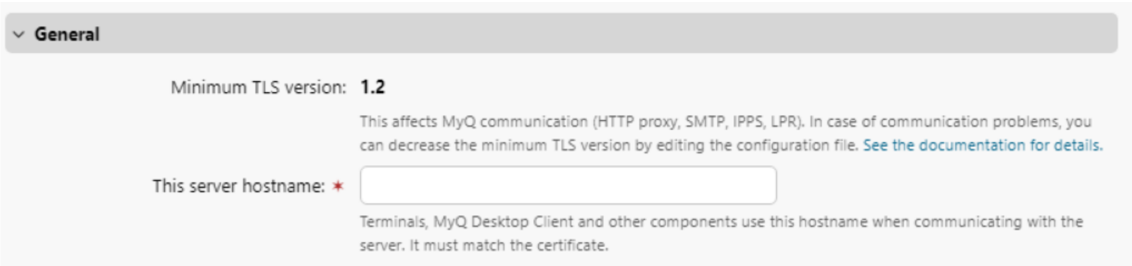
On the **Network** settings tab, you can manage the network communication between the MyQ server and other parts of the MyQ solution. It is divided into the following sections: **General, Communication Security, Outgoing SMTP Server, MyQ SMTP Server, FTP Server, MyQ X Mobile Client, HTTP Proxy Server,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



6.5.1 General

In this section, you can view the current **Minimum TLS version (1.2)** that affects MyQ communications (HTTP proxy, SMTP, IPPS, LPR). See how 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.

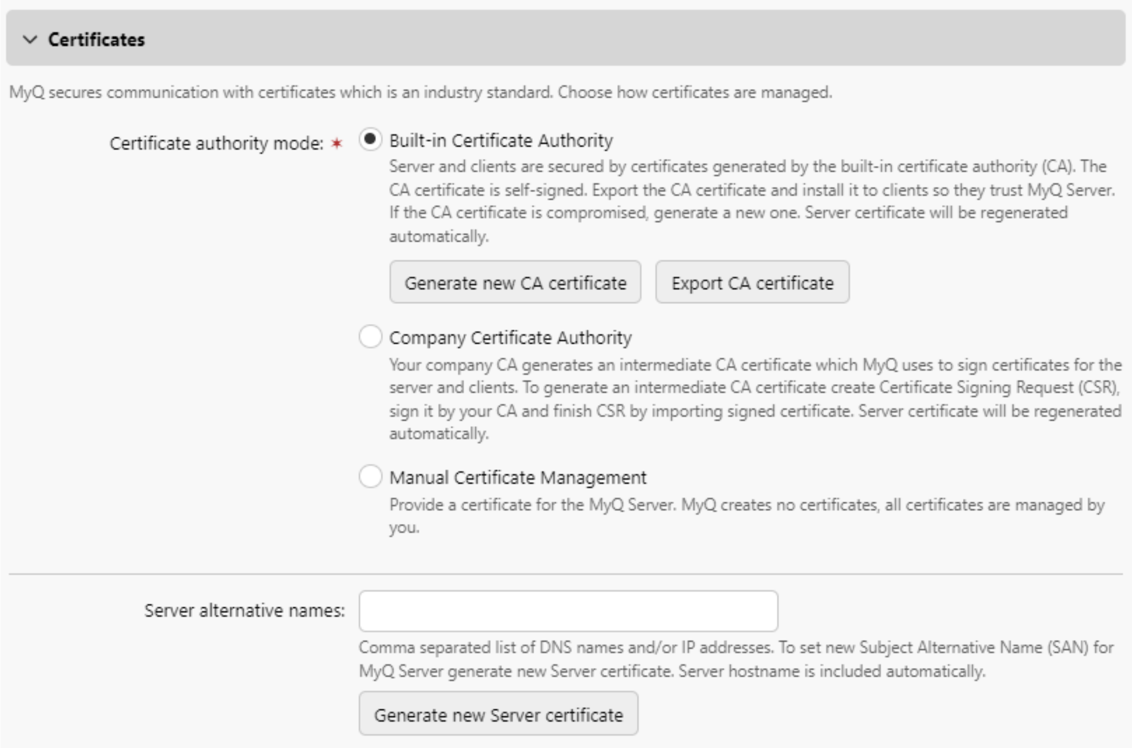
6.5.2 Certificates

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

+ private key separately) or in *PFX* format. The *PFX* format may be password encrypted. This mode is recommended only for expert users.



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**.

6.5.3 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*.

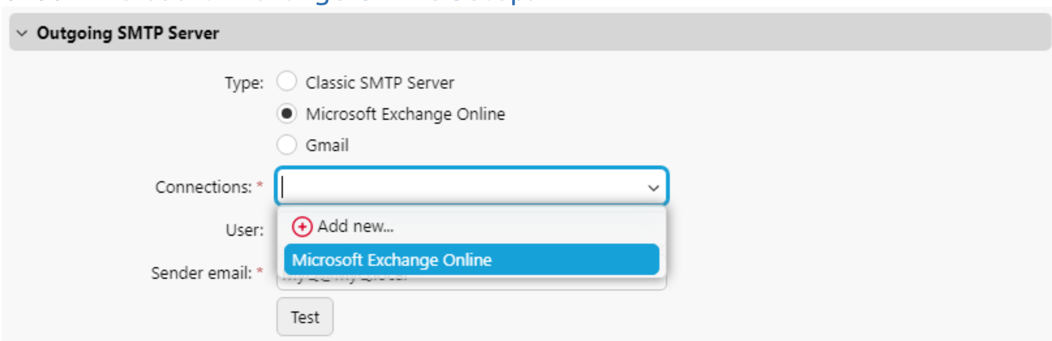
For *Classic SMTP Server*:

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.

For *Microsoft Exchange Online*:

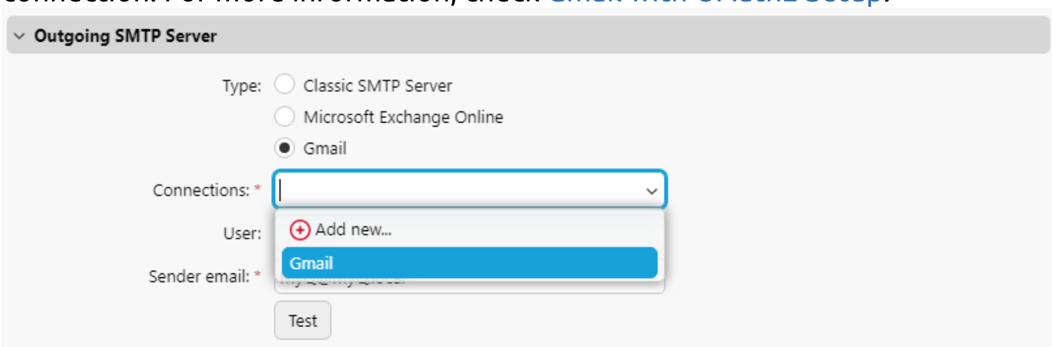
1. If you have already set up a Microsoft Exchange Online server in the **Connections** settings, the server is available in the **Connections** field drop-down. If not, you can click on the **Connections** field and then click **Add new** to add your Microsoft Exchange Online server connection. For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



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.

For *Gmail*:

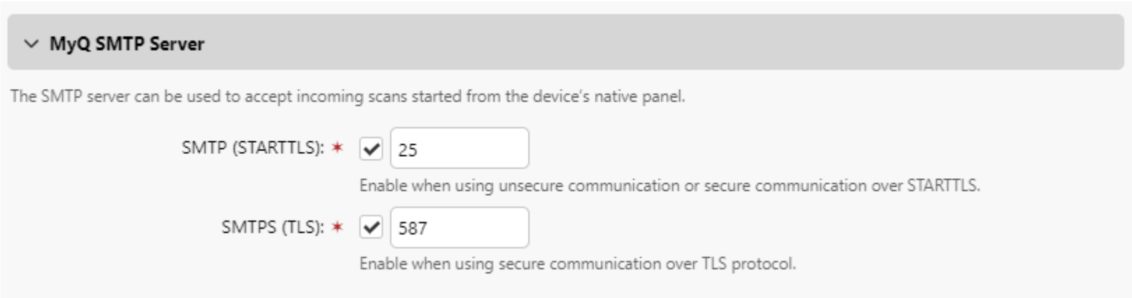
1. If you have already set up a Gmail server in the **Connections** settings, the server is available in the **Connections** field drop-down. If not, you can click on the **Connections** field and then click **Add new** to add your Gmail server connection. For more information, check Gmail with OAuth2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



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.

6.5.4 MyQ SMTP Server

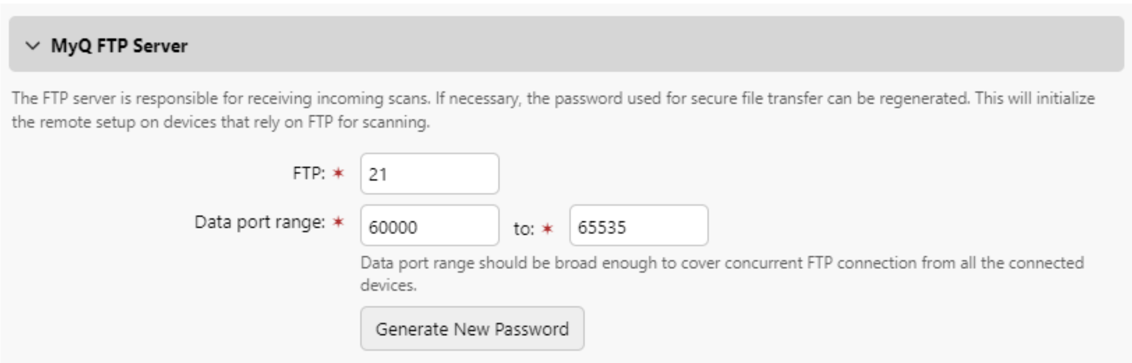


In this section you can view and modify the SMTP server settings.

- **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.

6.5.5 MyQ FTP Server

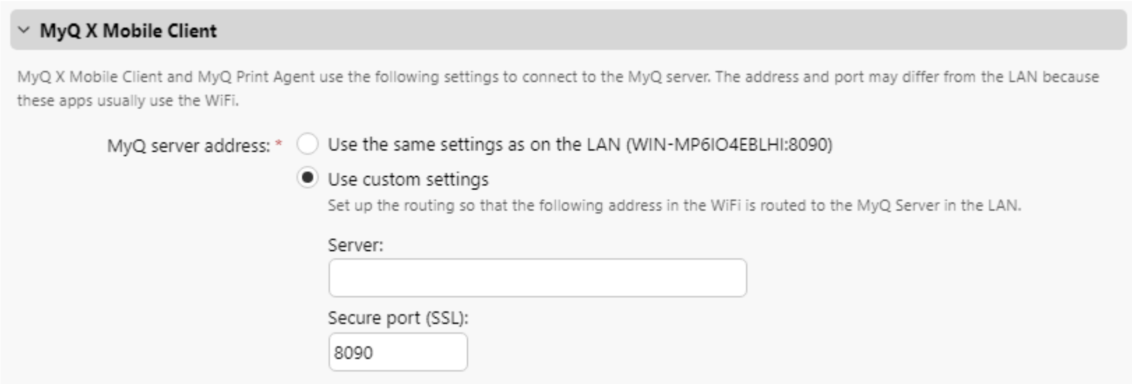


In this section, you can set the **FTP server port** that terminals use when sending scan jobs to MyQ over the FTP protocol. The FTP port is *21* by default, and the range is *0 to 65535.* If you click the **Generate new password** button, there is a confirmation pop-up informing that if a new password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

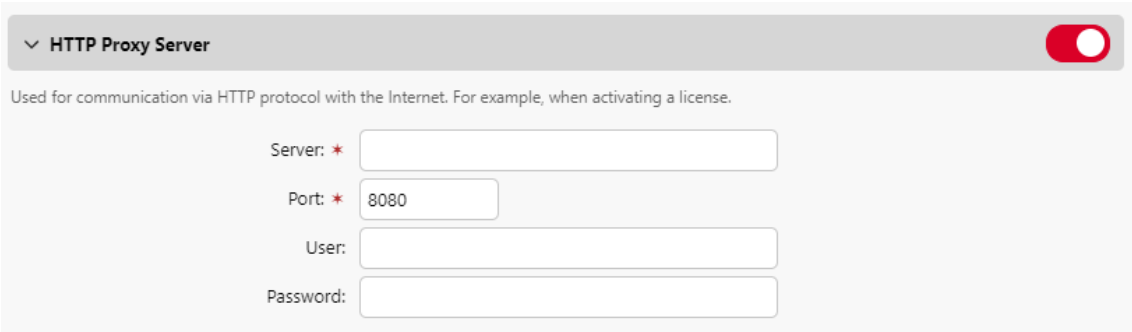
6.5.6 MyQ X Mobile Client

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.



6.5.7 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.

6.5.8 Firewall Management

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

6.6 Connections Settings

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

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

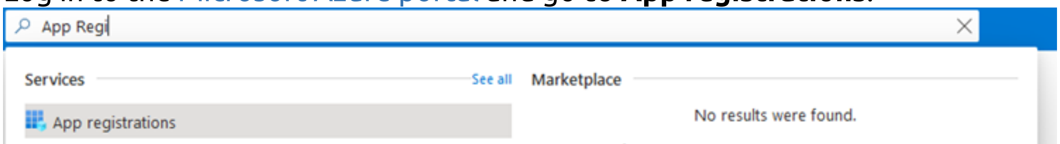
- Amazon S3
- External Storage API
- Gmail
- Microsoft Entra ID
- Microsoft Exchange Online
- Microsoft Universal Print

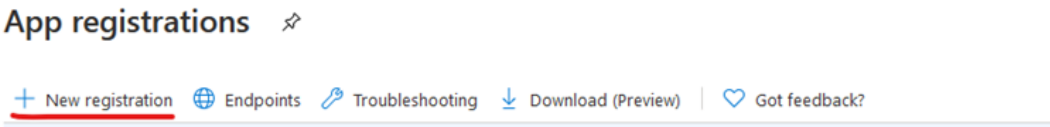
- OneDrive for Business
- RightFax
- SharePoint Online
- the MyQ and ScannerVision integration (embedded terminals and a **MyQ Ultimate license** are required)

6.6.1 Microsoft Exchange Online Setup

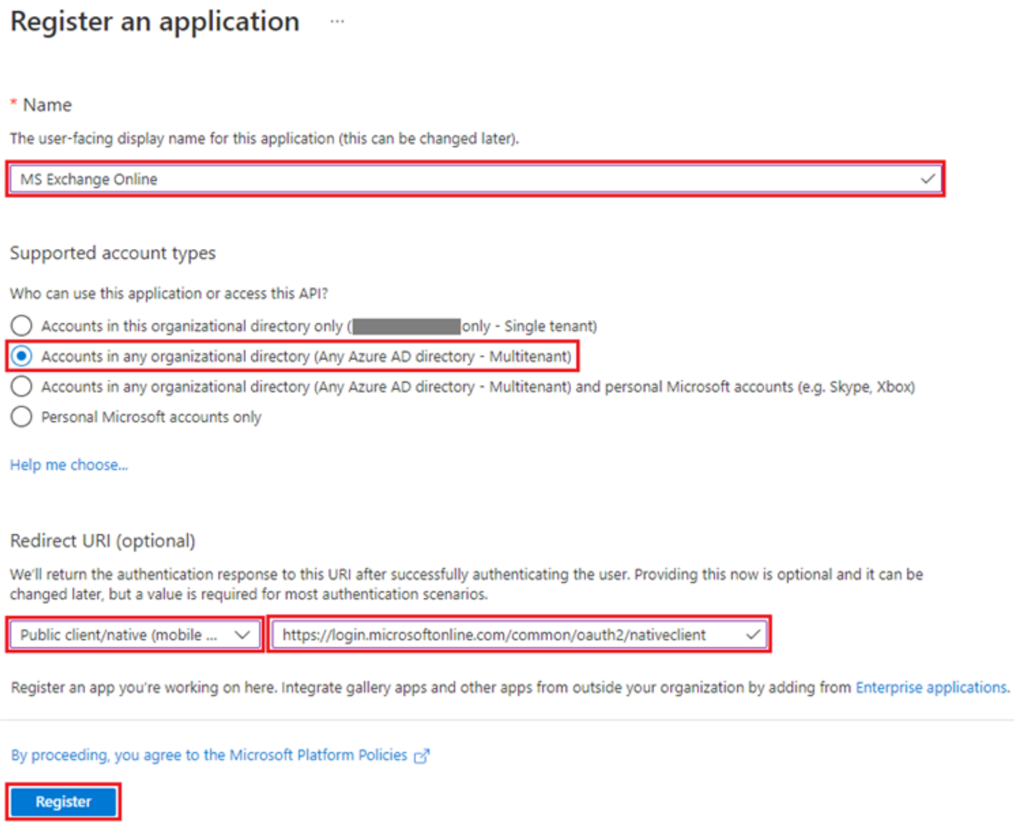
It is necessary to set up Microsoft Exchange Online in Microsoft Azure first, and then configure it in MyQ.

Microsoft Exchange Online setup in Microsoft Azure

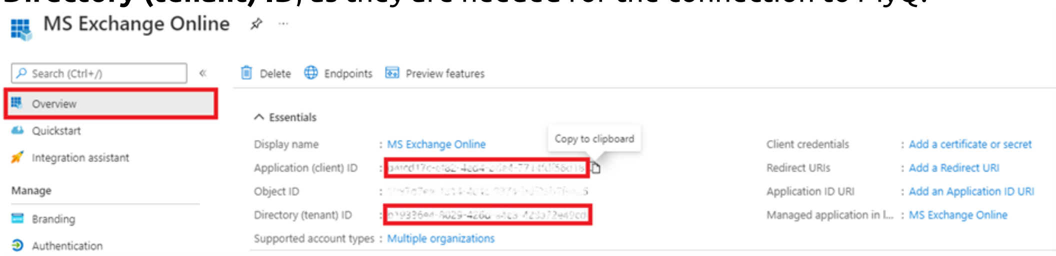
1. Log in to the Microsoft Azure portal and go **to App registrations**.


2. Create a **New registration**:


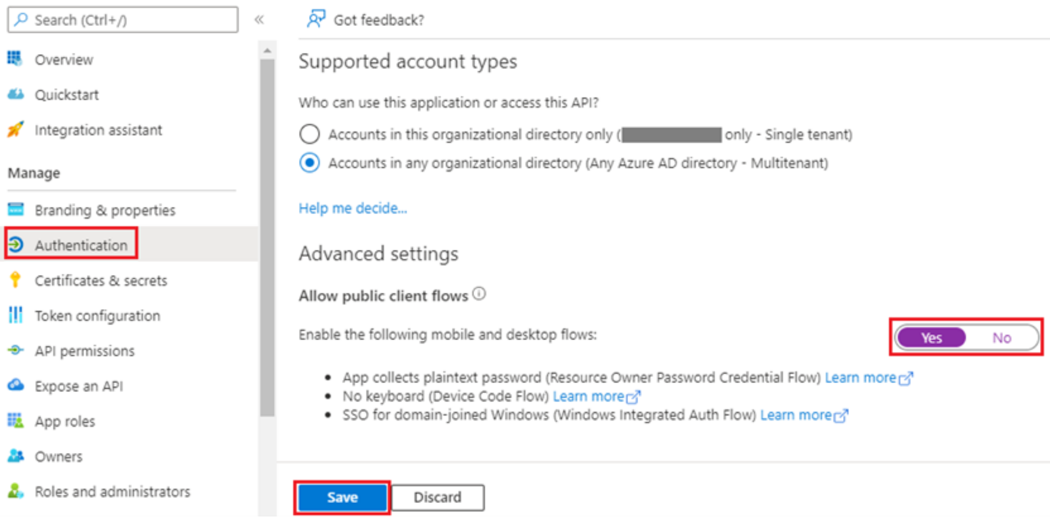
3. Create an Azure application:
   a. **Name** - The name for this application (this can be changed later). For example, *MS Exchange Online*. It is important to use the same name as the one used in MyQ under Connections.
   b. **Supported account types** - Who can use this application or access this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



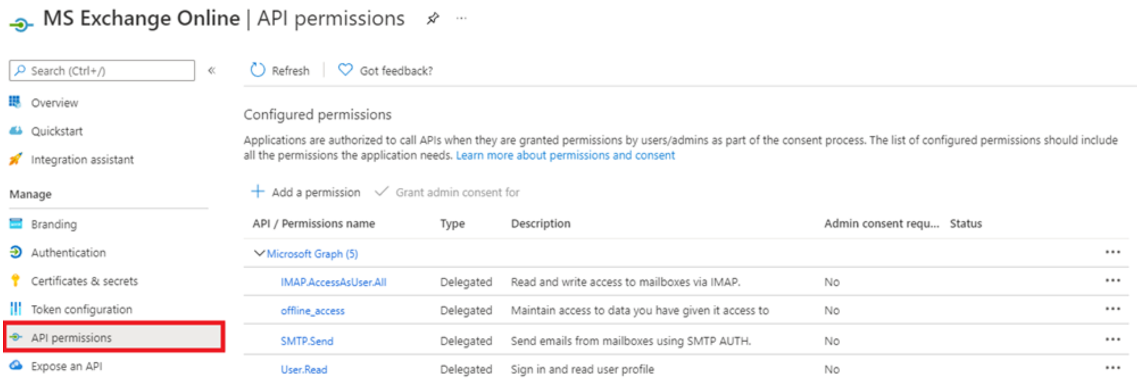
4. The new app overview page opens. Copy the **Application (client) ID** and the **Directory (tenant) ID**, as they are needed for the connection to MyQ.



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

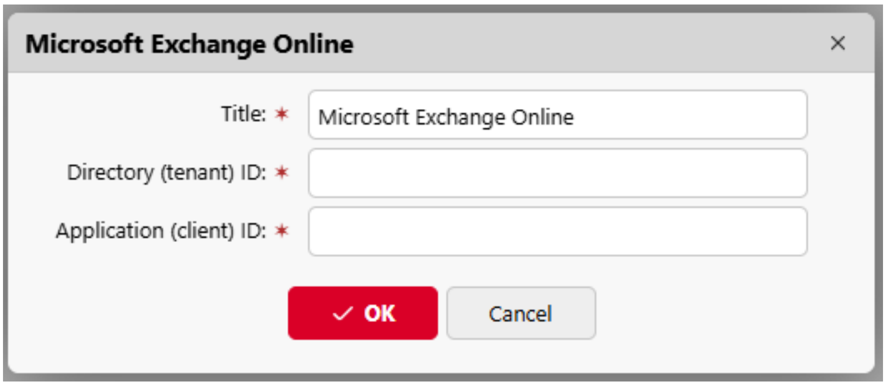


6. On the left-hand menu, click **API permissions** and add the additional permissions required for the correct functionality:
    a. Microsoft Graph: **offline_access** - Allows the app to see and update the data you gave it access to, even when you are not currently using the app. This does not give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



Microsoft Exchange Online setup in MyQ

1. Log in to the MyQ web administrator interface, and go to **MyQ, Settings, Connections**.
2. Click **+Add** and select *Microsoft Exchange Online* from the list.
3. In the pop-up window, fill in the required fields:



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

The email functionality will not work until the confirmation is successfully completed.
***This confirmation must be done with the Microsoft account that owns the email box (email address), which is used to connect to the exchange (Sender email** in the **MyQ, Settings, Network** tab).*
For example, if you use the sender email "print@somedomain.com", then you need to authenticate on the Microsoft website as this user during this step.

Microsoft Exchange Online is now connected to MyQ and is ready to be used in the **Network** settings tab, as an Outgoing SMTP server, and in the **Jobs** settings tab, in Jobs via Email as a POP3 or IMAP server.

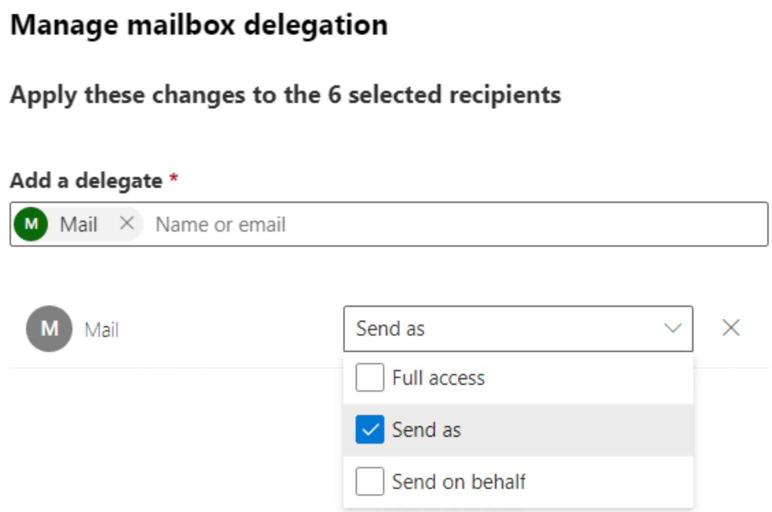
Additional Settings

Send scan as the logged-in user

If MyQ is set to send scans as the logged-in user in 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.

1. Log in to Exchange admin center.

2. Go to Mailboxes, select all users.
3. Click on “**Mailbox delegation**”.
4. Select the mailbox that has been authenticated in MyQ when the MS Exchange Online connector was created (you can find it in MyQ, Settings, Connections).
5. Choose "**Send as**" permission.



6. Click Save.

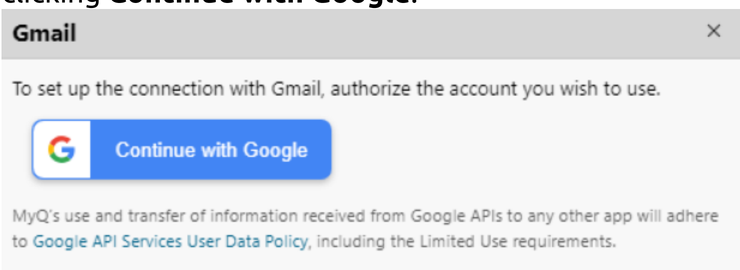
Your selected mailbox for outgoing emails has now been assigned the rights to send scanned documents on behalf of the user who scanned them.

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

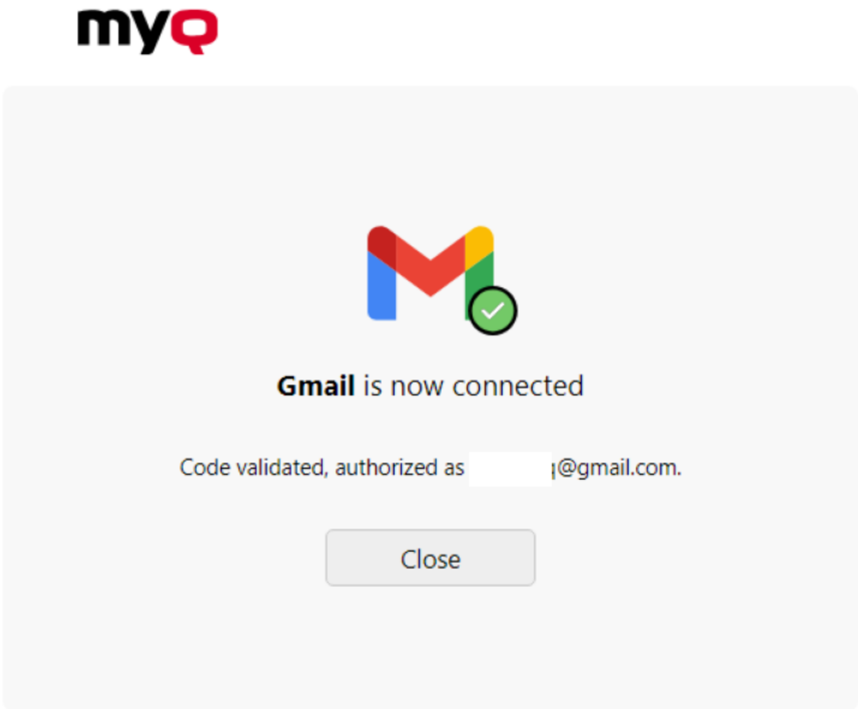
6.6.2 Gmail with OAuth2 Setup

To configure Gmail with OAuth2 in MyQ:

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



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



Gmail is now connected to MyQ and is ready to be used in the **Network** settings tab as an Outgoing SMTP server, and in the **Jobs** settings tab, in Jobs via Email as a POP3 or IMAP server.

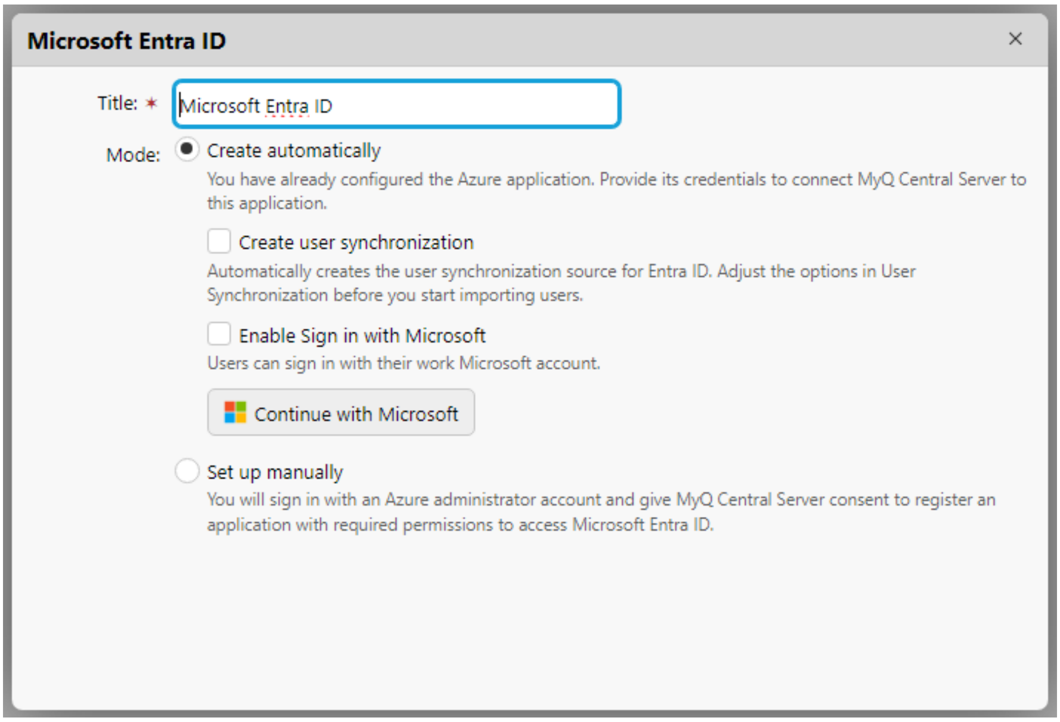
> MyQ's use and transfer of information received from Google APIs to any other app will adhere to Google API Services User Data Policy, including the Limited Use requirements.

6.6.3 Set Up Entra ID with Microsoft Graph API

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

Create a Microsoft Entra ID Connection

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



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

Create Automatically

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

Considerations

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

Prerequisites

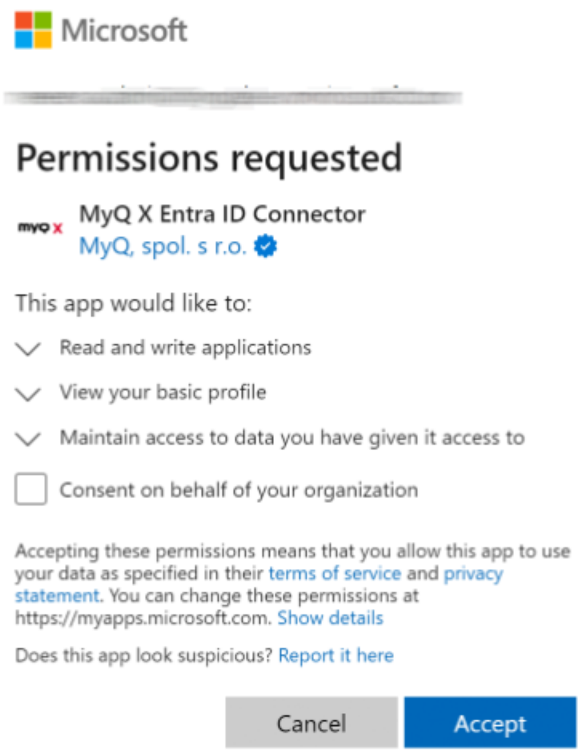
- For creating the service principal on the customer's tenant, **Application Administrator** or **Cloud Application Administrator** roles are required.
- For granting admin consent to the service principal, the **Global Administrator** role is required.
- To finish all steps in the automatic setup, the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

Steps to automatically set up the Microsoft Entra ID application

1. The administrator signs in with their Azure Administrator account. **MyQ X Entra ID Connector** service principal is created on the tenant.
2. The administrator grants the **delegated** permission to manage Azure applications.
   a. Permissions requested in this step:

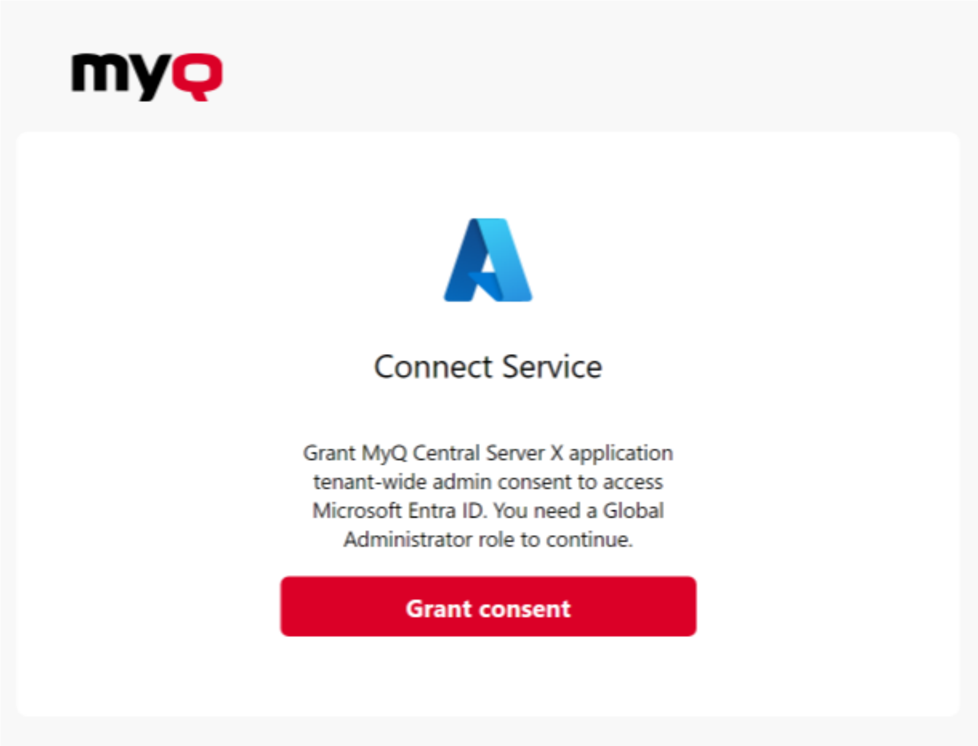
      `Application.ReadWrite.All` (to retrieve a Security key)

      `Directory.Read.All` (to read the default domain name in the connected tenant so that it can be displayed in MyQ).



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

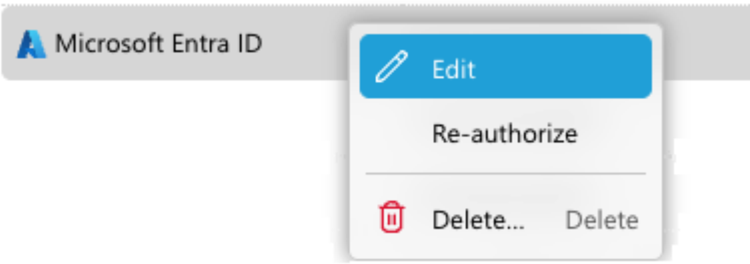
- Permissions requested in this step:
  `Group.Read.All`
  `User.Read.All`



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

Re-authorizing the Entra ID Connection

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



Application Management

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

Additional information

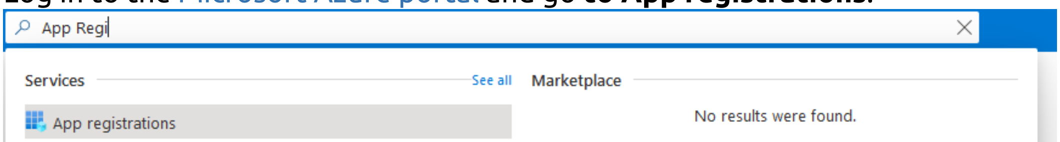
- If the automatic setup is completed again, it does not create a new instance of the application on the tenant, but the current application is updated (e.g. new secret on the service principal on the tenant created). If the *MyQ X Entra ID Connector* application has been removed from Azure, it is created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

Manual Setup

If you are manually creating an Azure application to link more than one of these services, you can either create one with all required permissions, or create a separate app for each of Entra ID, OneDrive for Business, and SharePoint Online. Read more here.

Microsoft Entra ID Application Configuration

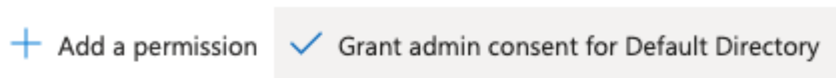
1. Log in to the Microsoft Azure portal and go **to App registrations**.



2. Click **New registration** to create a new application or select an existing application.
3. If you are creating a new application, set the **Name** and in **Supported account types** select *Accounts in this organizational directory only ({Tenant name} only - Single tenant)* option if all your users are members of your tenant. Multitenant application can also be used if required, depending on the target audience of the application.
4. You can skip the **Redirect URI** settings for now (described in step 7). Click **Register** to create the application.
5. From the application's Overview screen, go to **API Permissions** and select **Microsoft Graph API** and the required type of permission (**Delegated** or **Application**) as illustrated below.
   - The following permissions are required:
     - `Microsoft Graph \ Group.Read.All`
     - `Microsoft Graph \ User.Read`
     - `Microsoft Graph \ User.Read.All`

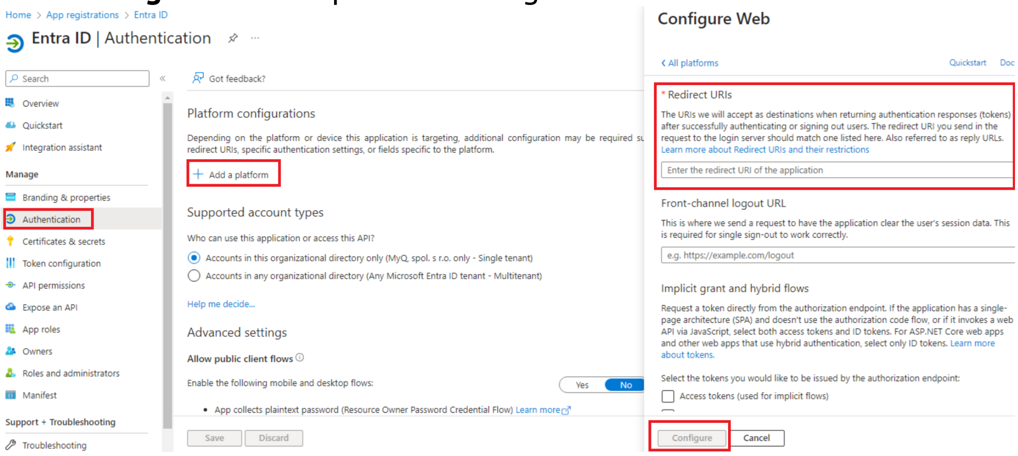
API / Permissions n...	Type	Description	Admin consent req...	Status
Microsoft Graph (3)				
Group.Read.All	Application	Read all groups	Yes	Granted for Default Directory
User.Read	Delegated	Sign in and read user profile	No	Granted for Default Directory
User.Read.All	Application	Read all users' full profiles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

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

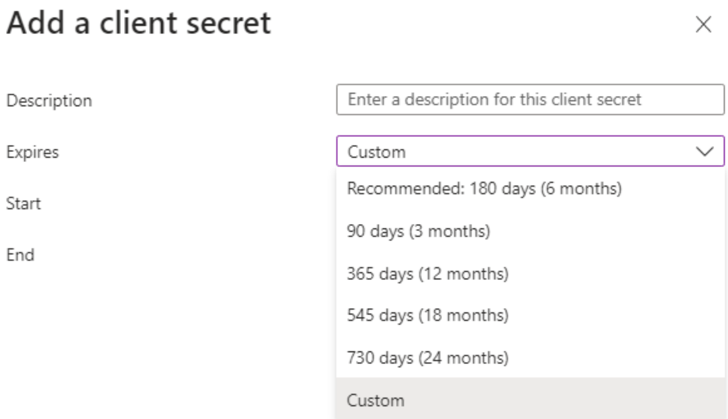


   Use "**Add a permission**" to add new permission.
   Use "**Grant admin consent for Default Directory**" to set the status of the permission as "Granted for Default Directory".
7. Go to **Authentication**, and under Platform configurations click **Add a platform**.
   - Select **Web**, and list all redirect URLs for your MS Entra ID application. For the actual URLs, use the hostname (and port) of your server in the following format:
     `https://{hostname:port}/auth`

- Additionally, click **Add a platform** and select **Single-page application.** Add the following redirect URL, ensuring that the trailing slash is included:
  `https://helper.myq.cz/openid/`
  All servers that use Entra ID sign-on must have a redirect defined in the Azure application. Make sure to perform this step for every print server and central server in your deployment.
- Click **Configure** for each platform configuration.



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

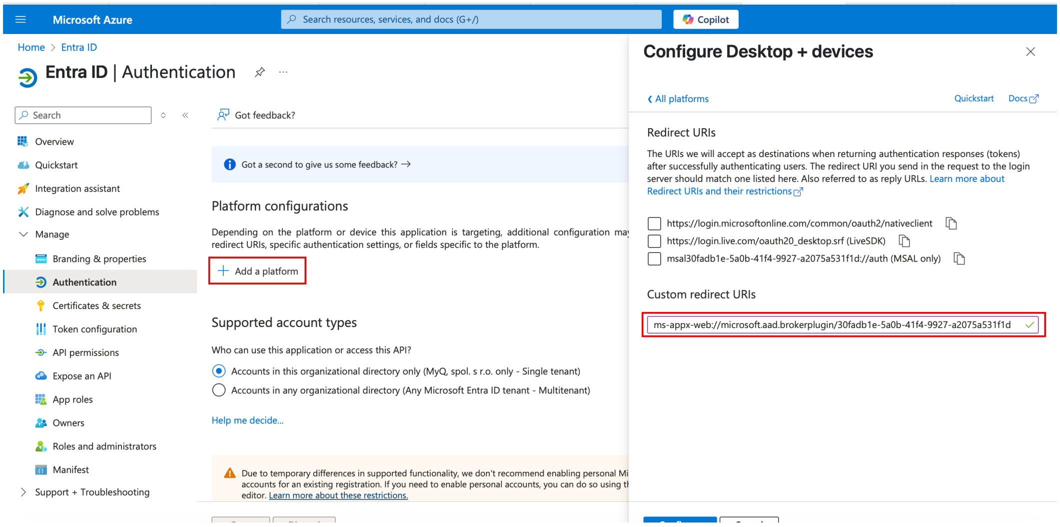


   a. Click **New client secret**.
   b. Add a **Description**.
   c. Set the expiration for the key.
   d. Click **Add**.
   e. Save the **client secret key Value**, because you need it for the configuration in MyQ and you cannot retrieve it later.

Using MyQ Desktop Client with Seamless Single Sign-on

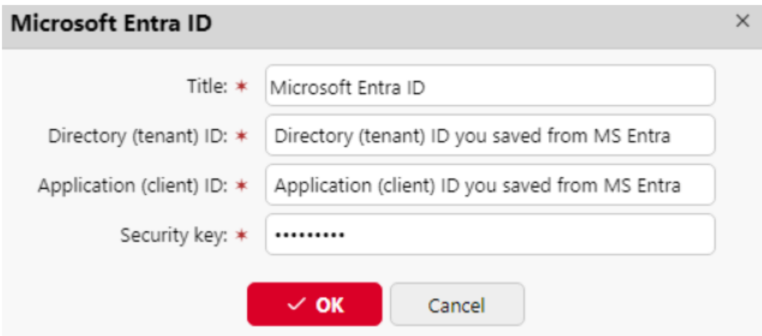
In order to utilize Seamless Single Sign-on in MyQ Desktop Client you must create a correctly configured application. Use the instructions above and from Step 7:

1. Select **Add a Platform** and select **Mobile and desktop applications**.
2. Add Custom redirect URIs `ms-appx-web://microsoft.aad.brokerplugin/30fadb1e-5a0b-41f4-9927-a2075a531f1d` where `30fadb1e-5a0b-41f4-9927-a2075a531f1d` is the **Application (client) ID**.



Configuration in MyQ

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



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

Click **Save**. Your Microsoft Entra ID connection is now complete.

Microsoft single sign-on

To use Microsoft single sign-on:

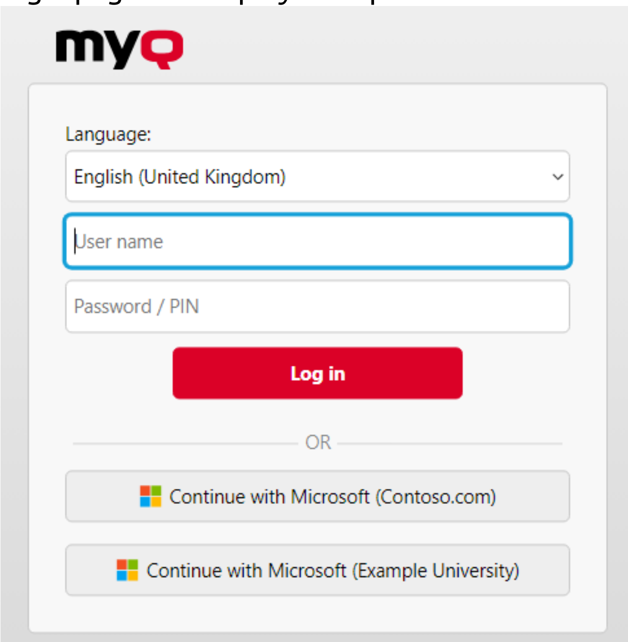
1. Enable "**Use as an authentication server**" in **Microsoft Entra ID synchronization source - Users tab** prior to synchronizing users or enable

Microsoft Entra ID as an authentication server manually for selected users in their details on the **Users** main page.
2. In the Microsoft Entra ID authentication server settings, enable displaying the '**Sign in with Microsoft**' login method.

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

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

- The user clicks the single sign-on button.
  - If the user is not signed in to Microsoft in the browser, they are forwarded to the Microsoft login page to sign in, and then logged into MyQ with the provided account.
  - If the user is signed into two Microsoft accounts, they are forwarded to the Microsoft login page and are given a choice to select the account to continue with.
- Logout in MyQ Web UI signs out the user only locally, not from Microsoft.
- In cases where multiple Entra ID authentication servers are configured, the login page will display multiple "Continue with Microsoft" buttons.



Limitations

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

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

1. Adding a Microsoft Entra ID authentication server in **MyQ > Settings > Authentication Servers**.
2. Adding a Microsoft Entra ID synchronization source in **MyQ > Settings > User Synchronization**.

Entra ID (Azure) Multi-Tenant Synchronization and Authentication

You can now use multiple Entra ID tenants in MyQ environments to synchronize and authenticate users. This is particularly useful in shared print infrastructure settings, such as those found in the public sector, where multiple organizations manage printers from a single location, while each uses its own Entra ID.
Follow one of the processes as described above but repeat it to set up multiple instances. Ensure that clear and unique naming is given to each tenant, which will allow users to identify which is relevant for their use.

6.6.4 OneDrive for Business Setup

The connection between MyQ X and OneDrive for Business is configured in **MyQ > Settings > Connections**.

Click **Add** and select **OneDrive for Business**.

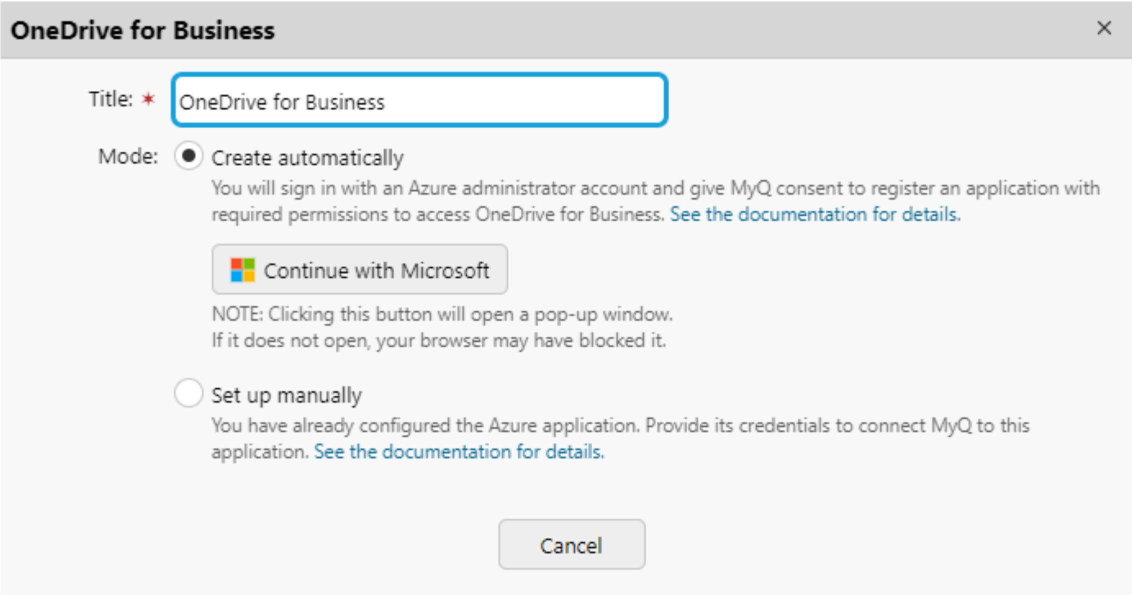
In the pop-up window, add a **Title** for your connection, and then you can select the preferred **Mode**:

- *Create automatically*: MyQ X will facilitate the Azure application required for accessing OneDrive for Business content.
- *Set up manually:* You want to manage all aspects of the application, and thus create it manually in your Azure tenant.

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

Create Automatically

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



Considerations

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

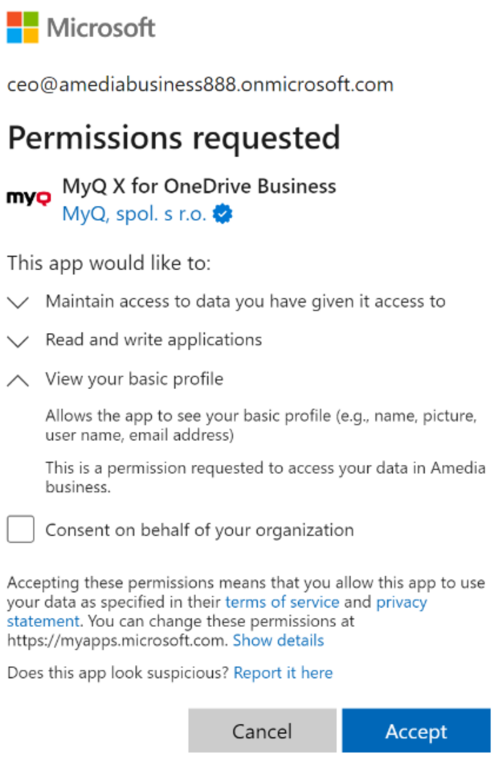
Prerequisites

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

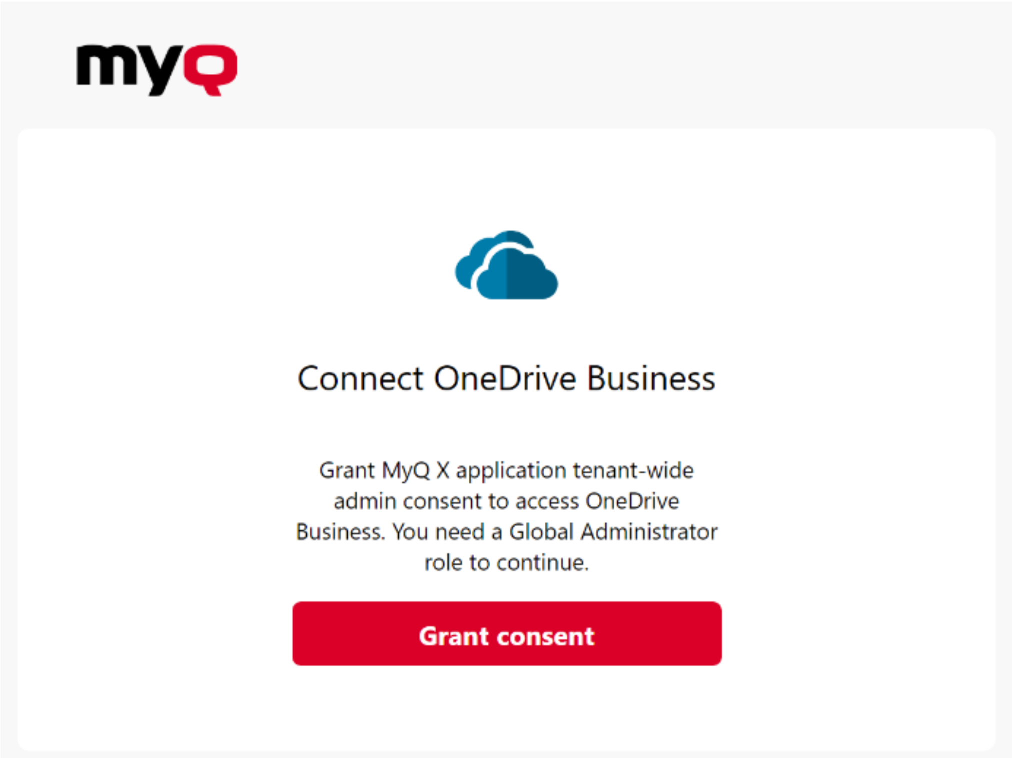
Steps to automatically set up the OneDrive for Business application

1. The administrator signs in with their Azure Administrator account. MyQ X for OneDrive for Business service principal is created on the tenant.
2. The administrator grants the **delegated** permission to manage Azure applications.
    a. Permissions requested in this step:
       `Application.ReadWrite.All` (to create a Security key)

`Directory.Read.All` (to read the default domain name in the connected tenant so that it can be displayed in MyQ).



3. The administrator grants the MyQ X for OneDrive for Business enterprise application **permissions to read/write to OneDrive** and **grants admin consent** (individual users do not have to consent subsequently)
   - Permissions requested in this step: `Files.ReadWrite.All`.



4. Once the process is completed, the OneDrive for Business connector is saved, and the connection details are securely saved in MyQ.

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.

Application management

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

Additional information

- If the automatic setup is completed again, it does not create a new instance of the application on the tenant, but the current application is updated (e.g. new secret on the service principal on the tenant created). If the *MyQ X for OneDrive Business* application has been removed from Azure, it is created again.
- Service principal (enterprise application) is created on the tenant after Step 1 (without necessary permissions which are granted in Step 3). If the authorization code is provided in Step 2, **the connector can be saved**. Step 3 can be finished later (by right-clicking the OneDrive Business connector and selecting *Re-authorize*).
- To better understand what MyQ is doing in this mode, Microsoft explains this method in their Developer documentation – Understand user and admin consent from the perspective of the application developer

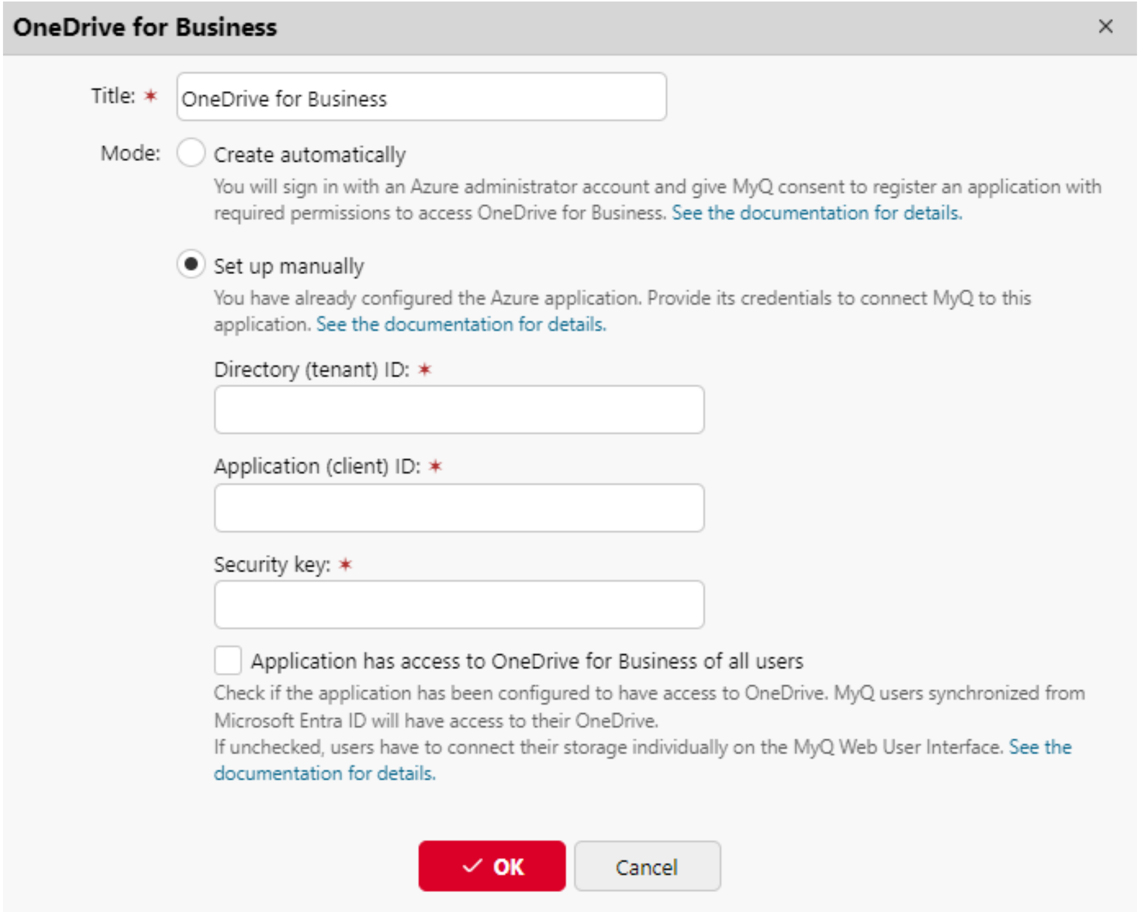
Set Up Manually

If you are manually creating an Azure Application to link more than one of these services: Entra ID, OneDrive for Business, SharePoint Online, we recommend you create one single application to link them all to, rather than one for each. Read more here.

It is expected that the administrator has configured the Azure application manually. They can directly provide credentials to their application - Tenant ID (*directory ID*), Application ID (*client ID*), Security key (*secret key*), and have set up the Redirect URI as `https://helper.myq.cz/` - without which OneDrive Business will not function.

Follow the steps to manually create an Entra ID connection here.
During this process, you will obtain the **Tenant ID**, **Client ID**, and **Security key** of the application that you will provide to MyQ X in the next steps.

In the pop-up window, fill in the required information:



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

Click **Save** and your OneDrive for Business connection is now complete.

Option “Application has access to OneDrive Business of all users”

The **Application has access to OneDrive Business of all users** checkbox lets the administrator set whether the application has already been given access to the OneDrive storage of users or not.

- If **unchecked**, it is expected the application has been given only *Delegated* permissions, which means each user has to manually log in to the MyQ Web User Interface and click the “Connect” link to give the application permissions to access their data.

API / Permissions name	Type	Description	Admin Consent Re...	Status	
Microsoft Graph (2)					...
Files.ReadWrite	Delegated	Have full access to user files	-		...
User.Read	Delegated	Sign in and read user profile	-		...

- If **checked**, it is expected the application has been assigned *Application* permissions to access OneDrive data and the administrator has granted admin consent to the application, all manually in Azure Portal. The users do not have to manually connect their storage, OneDrive Business storage appears to be connected in the widget on their MyQ Web User Interface.
  Conditions when this option is **enabled**:
  - Manually created Azure application must have `Files.ReadWrite.All` permission of the ***Application*** **type** (not *Delegated*).
  - **Admin consent granted** ("Granted" displayed in the Status column), can be granted with the "Grant admin consent" option.

+ Add a permission ✓ Grant admin consent for Amedia business

API / Permissions name	Type	Description	Admin consent requir...	Status	
Microsoft Graph (2)					...
Files.ReadWrite.All	Application	Read and write files in all site collections	Yes	Granted for ...	...
User.Read	Delegated	Sign in and read user profile	No	Granted for ...	...

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.

Learn how to use your OneDrive as a destination for Easy Scans here.

6.6.5 SharePoint Online Setup

The connection between MyQ X and SharePoint Online is configured in **MyQ> Settings > Connections**.

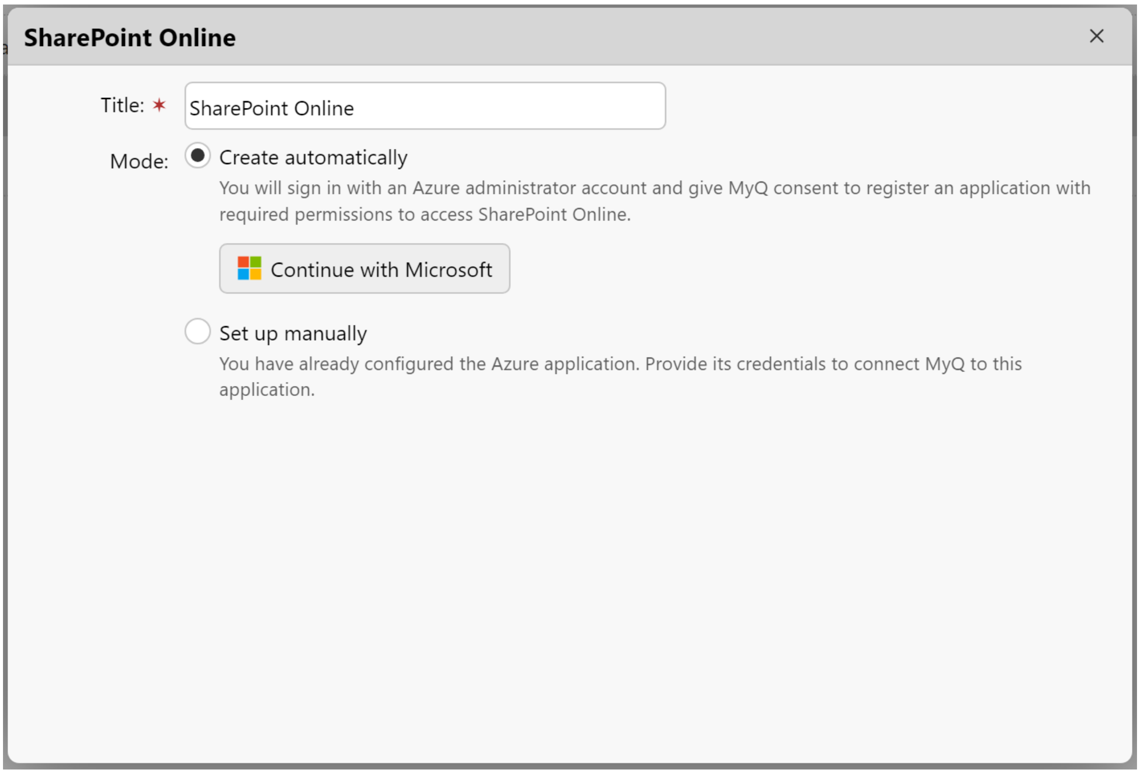
Click **Add** and select **SharePoint Online**.

In the pop-up window, add a Title for your connection, and then you can either select:

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

Create Automatically

This mode allows the administrator to have MyQ create the **Enterprise Application (Service Principal)** on their tenant and grant this application permissions to access SharePoint Online folders and files.



Considerations

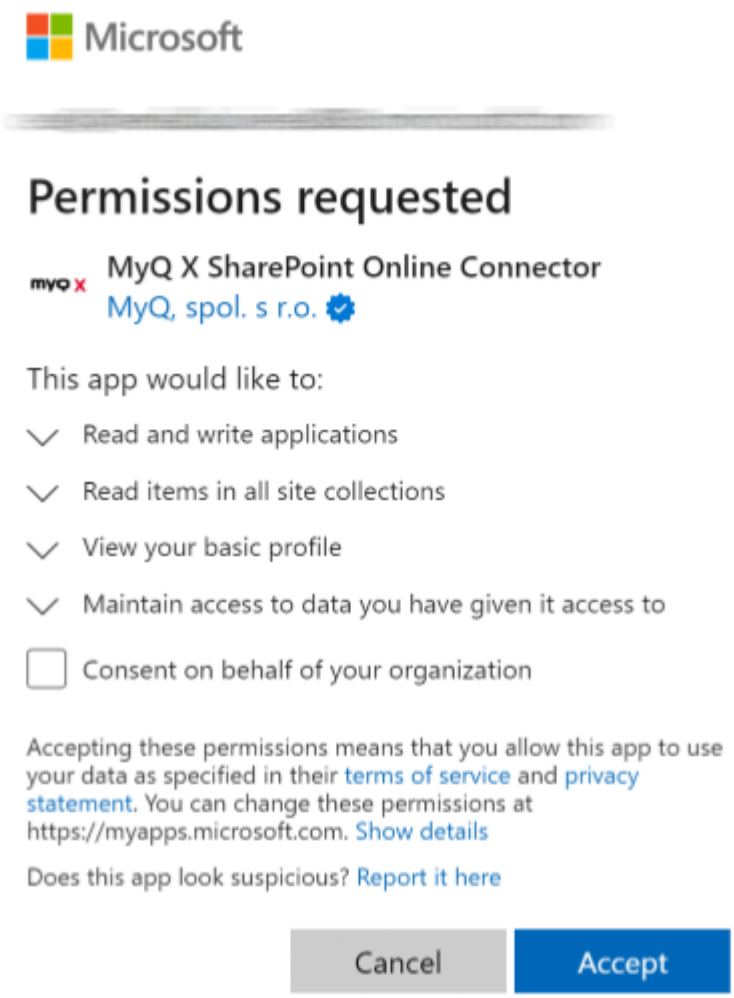
If you are hesitant to grant even temporary administrative access for the creation of a client secret, the automatic connection procedure to *SharePoint Online* will not be available for use. In such cases, it's advisable to manually create an application within your organization's Azure environment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

Prerequisites

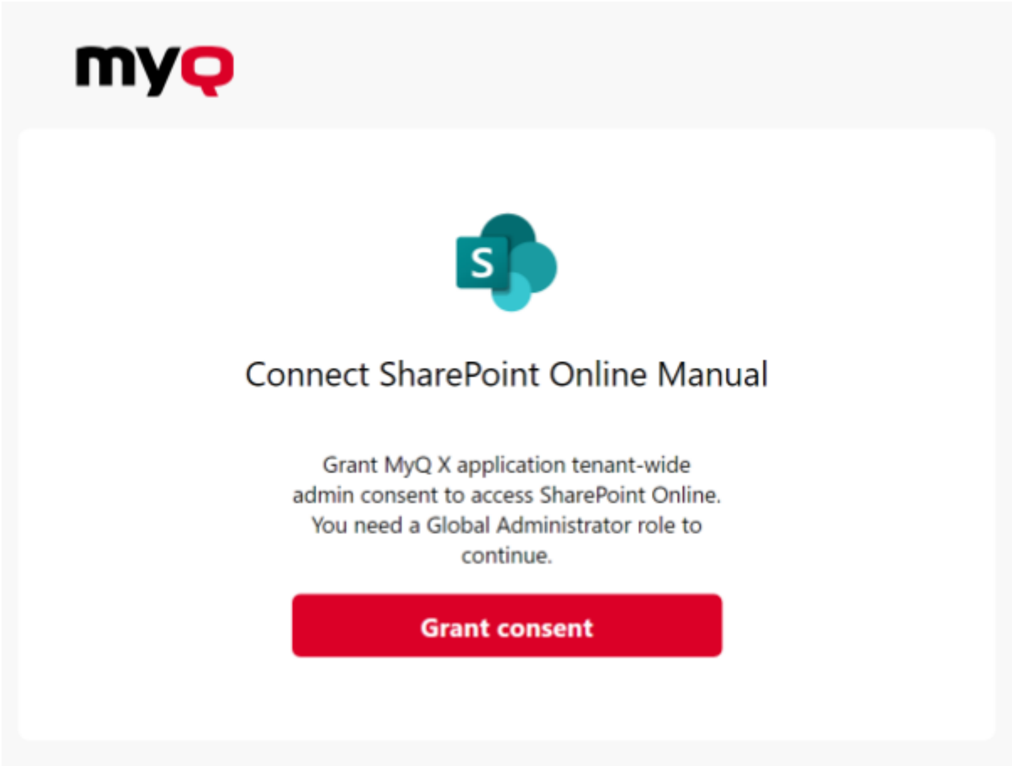
- For creating the service principal on the customer's tenant, **Application Administrator** or **Cloud Application Administrator** roles are required.
- For granting admin consent to the service principal, the **Global Administrator** role is required.
- To finish all steps in the automatic setup, the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

Steps to automatically set up the SharePoint Online Application

1. The administrator signs in with their Azure Administrator account. **MyQ X SharePoint Online Connector** service principal is created on the tenant.
2. The administrator grants the **delegated** permission to manage Azure applications.
    a. Permissions requested in this step: `Application.ReadWrite.All` (to create client secret) `Directory.Read.All` (to read default domain name in connected tenant)



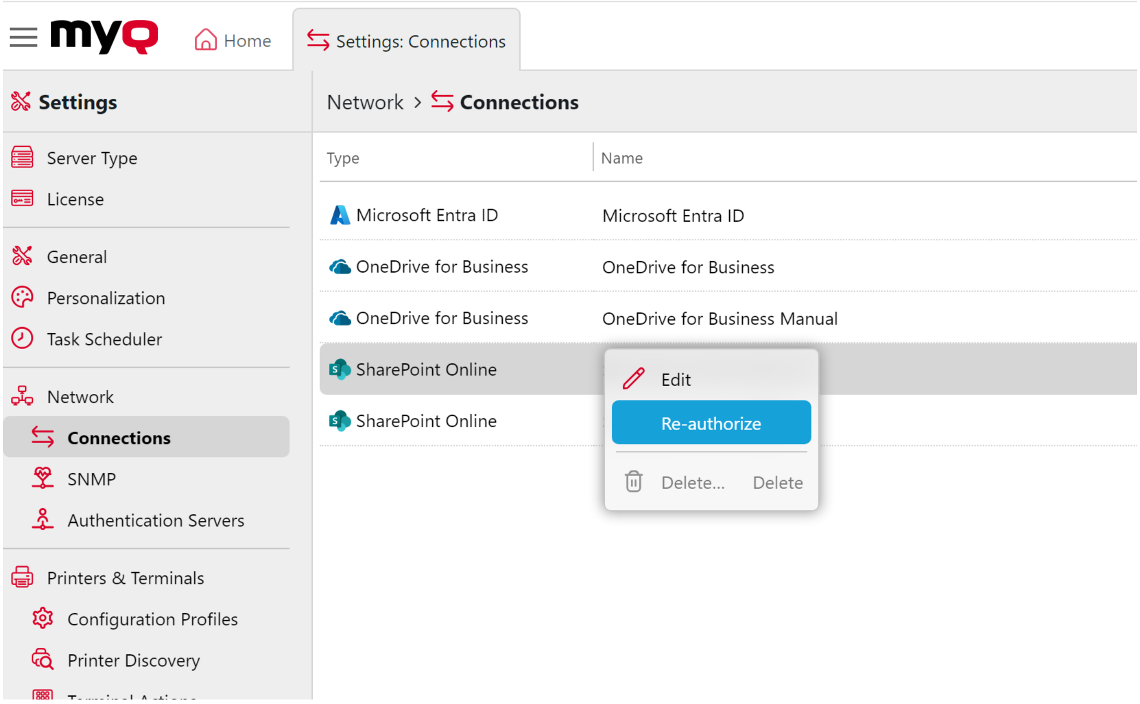
3. The administrator grants the **application** permissions **to read and write files** and **grants admin consent** (individual users do not have to consent subsequently)
    - Permissions requested in this step: `Sites.ReadWrite.All`



4. Once the process is completed, the **SharePoint Online** connector is saved, and the connection details are securely saved in MyQ.

Re-authorizing the SharePoint Online Connection

The automatic connection to *SharePoint Online* can be changed after it has been created. The Re-authorize option will be available in the context menu by right-clicking on the connection.



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 *SharePoint Online* 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.

Application management

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

Additional information

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

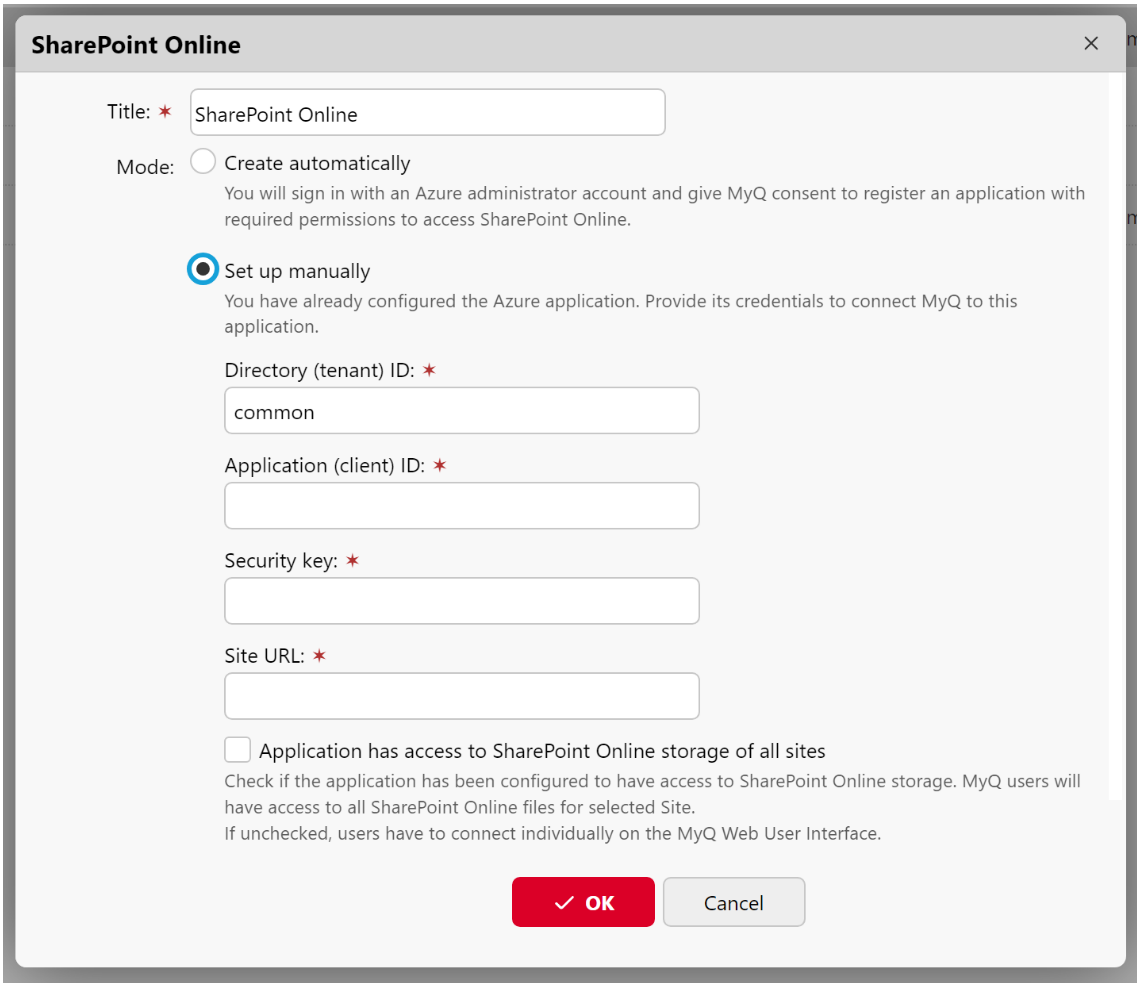
MyQ X users can interact with SharePoint Online files without having individual Microsoft accounts or being synchronized with users from Microsoft Azure AD. The application acts on behalf of the users, based on the permissions assigned to it by the organization's administrator in Azure.
All MyQ X users gain uniform full rights to access files on the SharePoint Online site, regardless of whether they have a Microsoft account within the organization or any individual permissions.

Set Up Manually

If you are manually creating an Azure Application to link more than one of these services: Entra ID, OneDrive for Business, SharePoint Online, we recommend you create one single application to link them all to, rather than one for each. Read more here.

It is expected that the administrator has configured the Azure application manually. They can directly provide credentials to their application - Application ID (*client ID*), Security key (*secret key*) and Site URL.

In most cases, it's enough to leave a prefilled Directory (tenant) ID as `common`. It should contain a specific tenant ID in case of using the '*Application has access to SharePoint Online storage of all sites*' option.



Enabling Application-Wide Access

This feature is designed to simplify access to SharePoint Online files, enabling MyQ X users to read and write files hosted on a selected SharePoint Online site without the need for individual Microsoft account logins.

When the option "*Application has access to SharePoint Online storage of all sites*" is enabled in the connection settings, it grants MyQ X users application-wide access to read and write files on any selected SharePoint Online site. This is achieved by configuring the application in Azure to have the necessary permissions to access SharePoint Online storage across all sites.

To implement this functionality, the application must be registered in Azure Entra ID with the appropriate permissions to access SharePoint Online. The required permission is `Sites.ReadWrite.All`, which allows the application to read and write files in all site collections without requiring individual user logins. This permission is granted via consent from an administrator in the Azure portal.

Configuration Steps

1. Register MyQ X as an application in Microsoft Entra ID (Azure).

2. Assign the `Sites.ReadWrite.All` permission to the application in Azure AD.
3. Admin consent is required to enable these permissions for the application.
4. In MyQ X connection settings, specify the SharePoint Online site by its URL.
5. Enable the "Application has access to SharePoint Online storage of all sites" option.

> With this option enabled, MyQ X users can interact with SharePoint Online files without having individual Microsoft accounts or being synchronized with users from Microsoft Azure AD. The application acts on behalf of the users, based on the permissions assigned to it by the organization's administrator in Azure.
> **All MyQ X users gain uniform full rights to access files on the SharePoint Online site, regardless of whether they have a Microsoft account within the organization or any individual permissions.**

Disabling Application-Wide Access

If the option is disabled, users must individually connect to the SharePoint Online storage through the MyQ X Web UI. They are required to login using a `connect` link, which necessitates having a Microsoft account within their organization. Upon connecting, an access token for SharePoint Online is stored in MyQ X.

User Token Authentication

When application-wide access is disabled, any action performed on files within the SharePoint Online site is executed under the individual user's account. The user's access token is unique and subject to the specific permissions of that user's Microsoft account. This ensures that file interactions are securely managed and adhere to the organization's access control policies.

Security Considerations

- When enabling application-wide access, it is crucial to understand the security implications of granting the application extensive permissions to SharePoint Online. Administrators should carefully consider the necessity of these permissions relative to their organizational security policies.
- Individual user token authentication offers a more granular level of access control, applying the specific permissions of each user's Microsoft account to their interactions with SharePoint Online files.

> Learn how to use your SharePoint Online as a destination for Easy Scans here.

6.6.6 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.

Requirements

Minimum requirements prior to the installation:

- MyQ Ultimate license (license for the MyQ server + license for ScannerVision)
- 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)

Additional Information

Additional information about MyQ products can be found in the MyQ Docs portal:

- *MyQ Embedded Terminal Manuals* for branded embedded terminals information
- *ScannerVision User Manual* for advanced ScannerVision user information

ScannerVision Server Installation

.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.

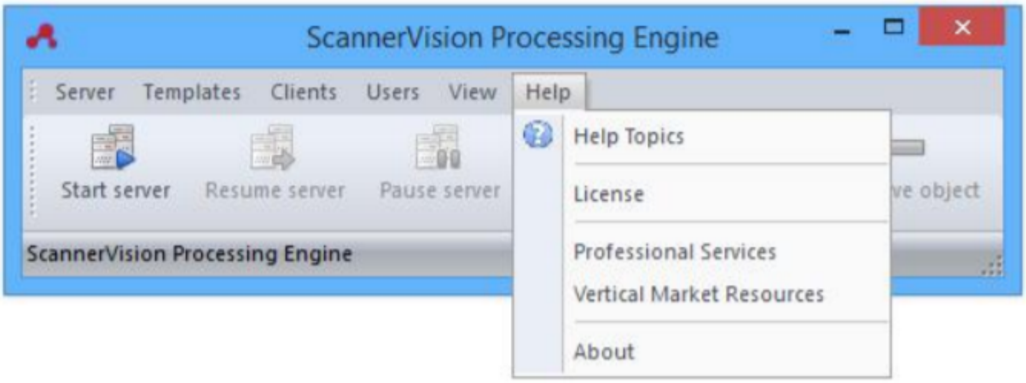
To install the ScannerVision server:

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

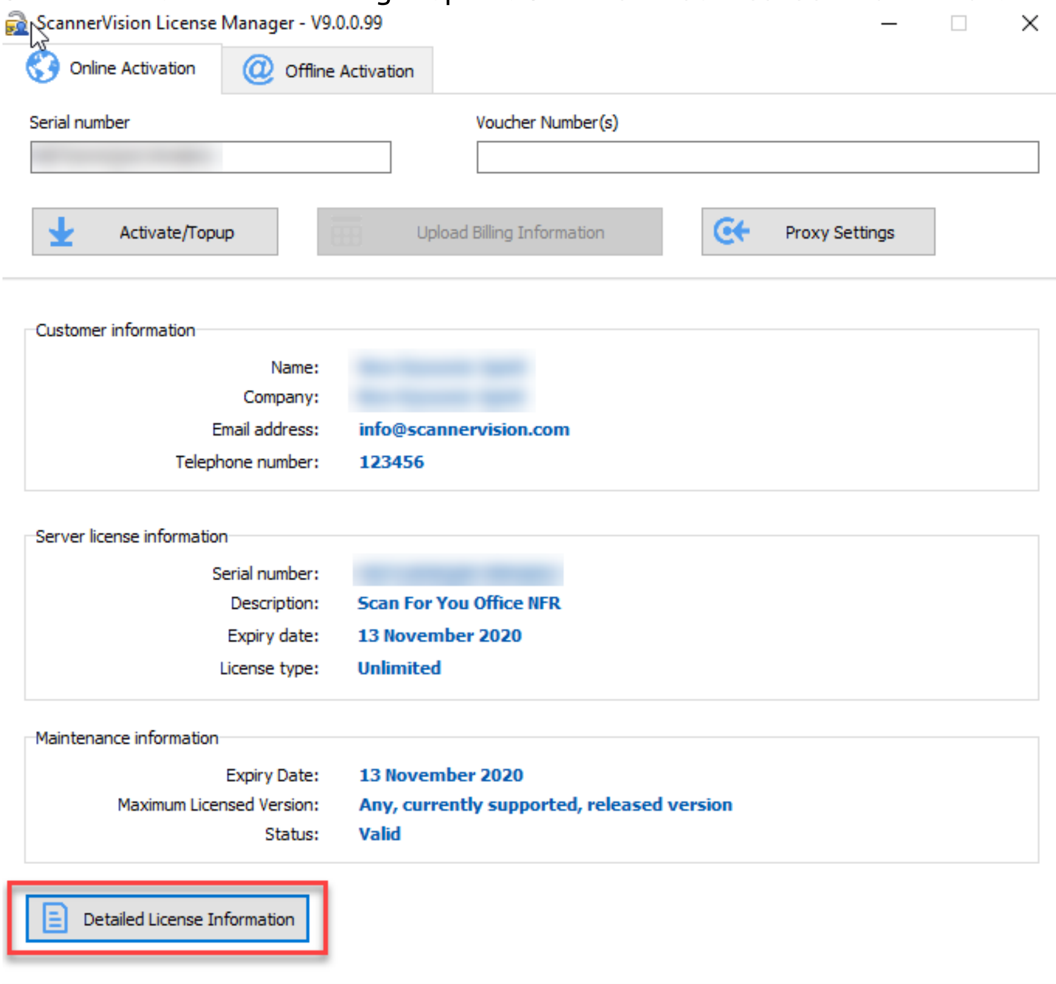
License check

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

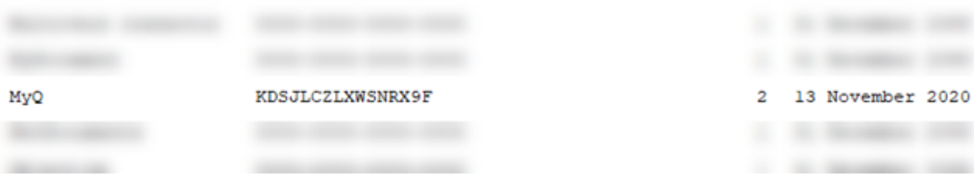
- Open the ScannerVision Processing Engine user interface application.
- On the top menu, click **Help, License**.



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



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



Configuration

Once the ScannerVision server is installed, there are configuration steps to be done, both in MyQ and in ScannerVision:

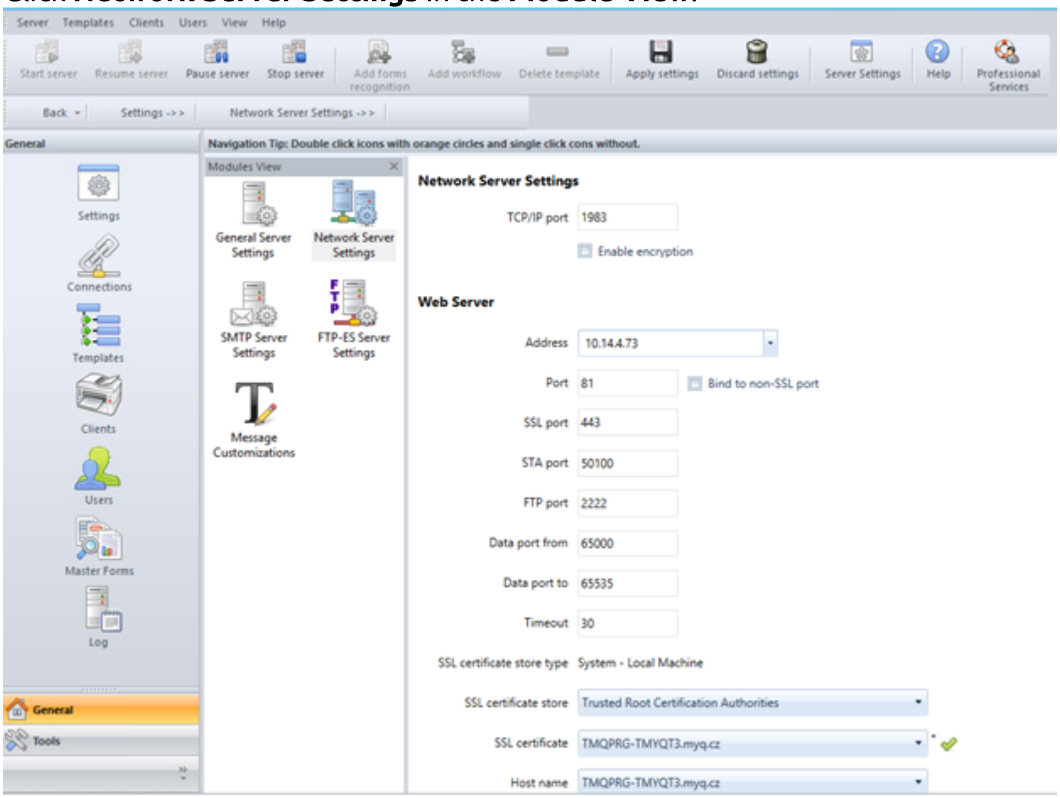
- Configuring ScannerVision
  - Templates
  - Clients
  - Users
- Adding ScannerVision as a terminal action in MyQ

Configuring ScannerVision

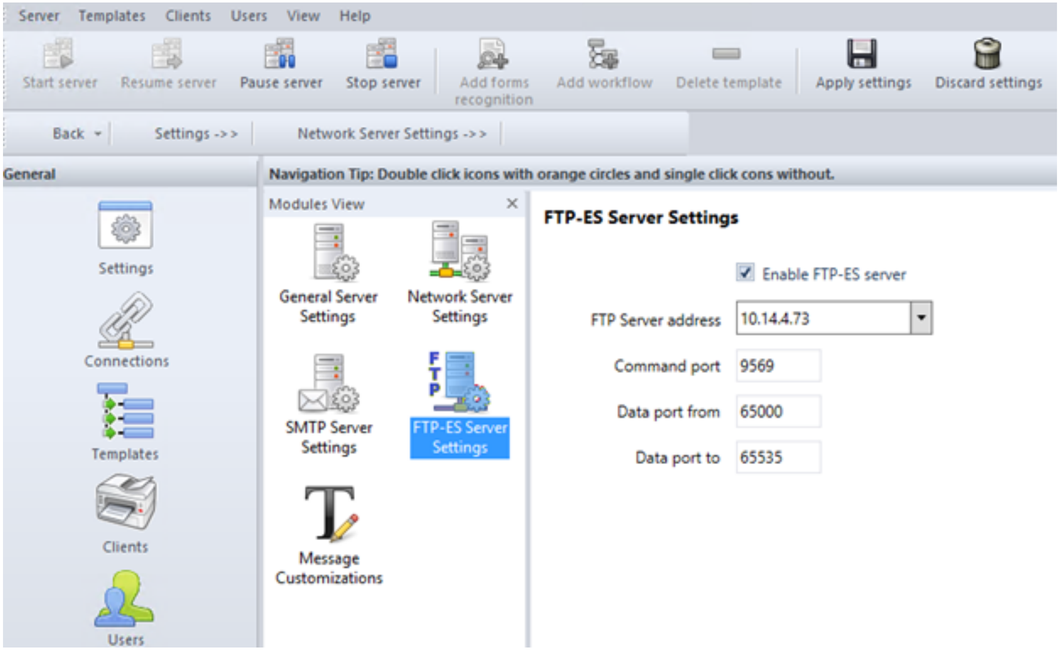
In order to set ScannerVision properly, you need to configure Network settings, Templates, Clients and Users.

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**:



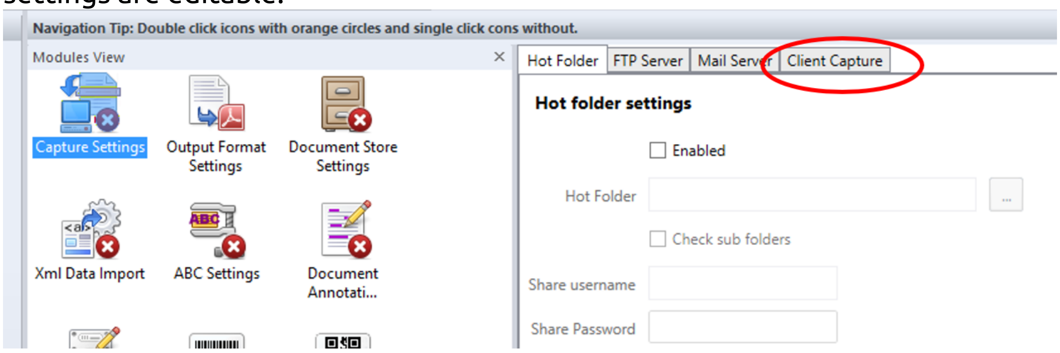
7. **Save** your settings.

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:

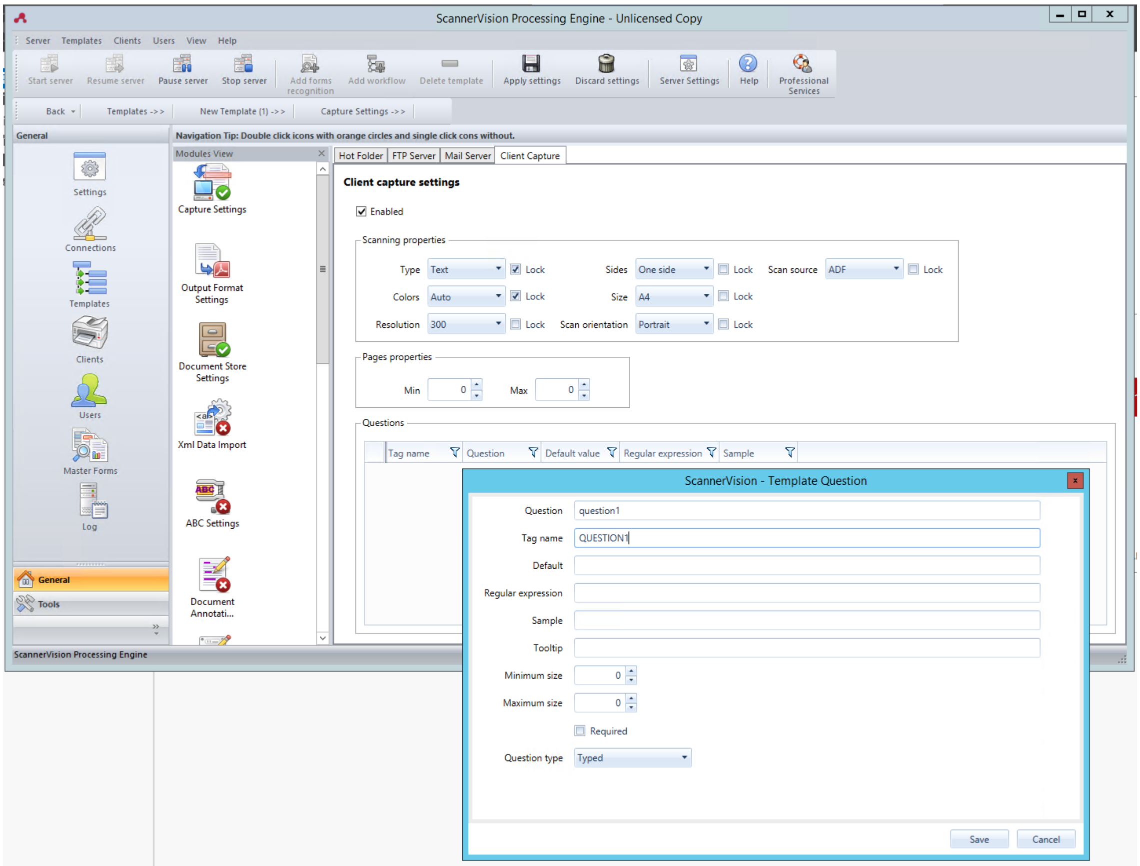
1. Open ScannerVision Processing Engine and click **Templates** in the **Navigation Panel**.
2. Click **Add Workflow** in the top menu.
3. **Name** the new template and mark it as **Enabled**.
4. Click **Apply Settings** in the top menu.
5. Once saved, double-click on the new template. In the right tab 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:

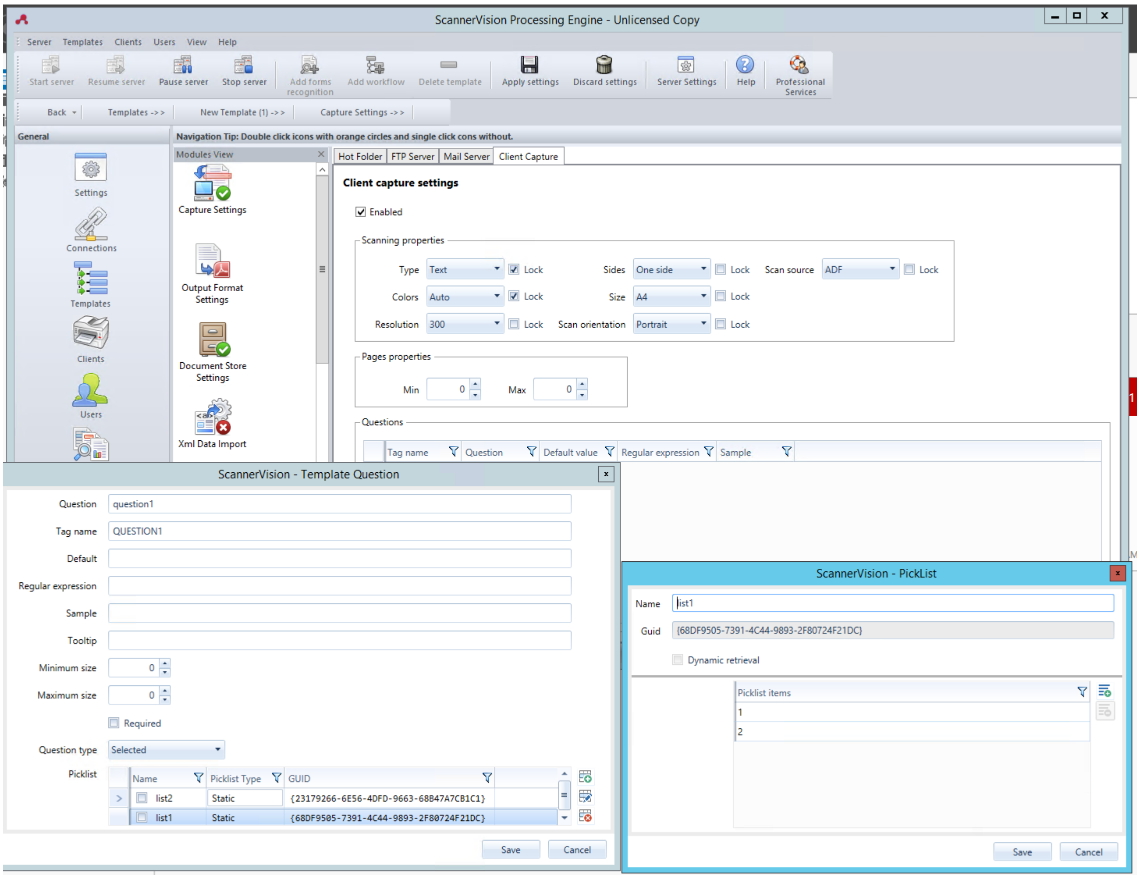
1. Right click on the **Questions** area.
2. Select **Add question**.
3. In the new Template Question window, fill in the **Question**, **Tag name**, and **Default** text fields, and any other of the optional fields.
4. In **Question Type** select *Typed*.
5. Click **Save**.



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**:

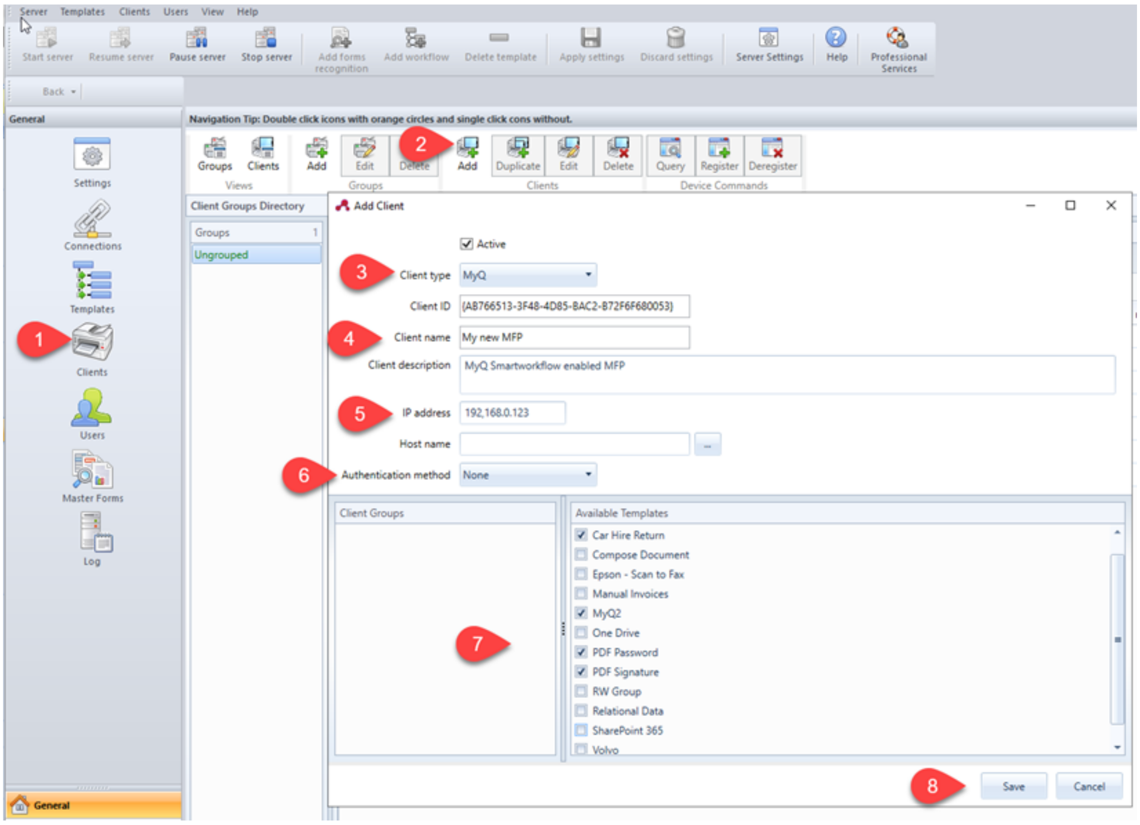
1. Click on the **Add PickList** button on the right.
2. Once there, select *Static* as the **PickList Type**.
3. In the Picklist window, enter a **Name** for the picklist.
4. Add picklist items by pressing the plus (**+**) button on the right.
5. Click **Save**.
6. Once saved, select the picklist(s)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

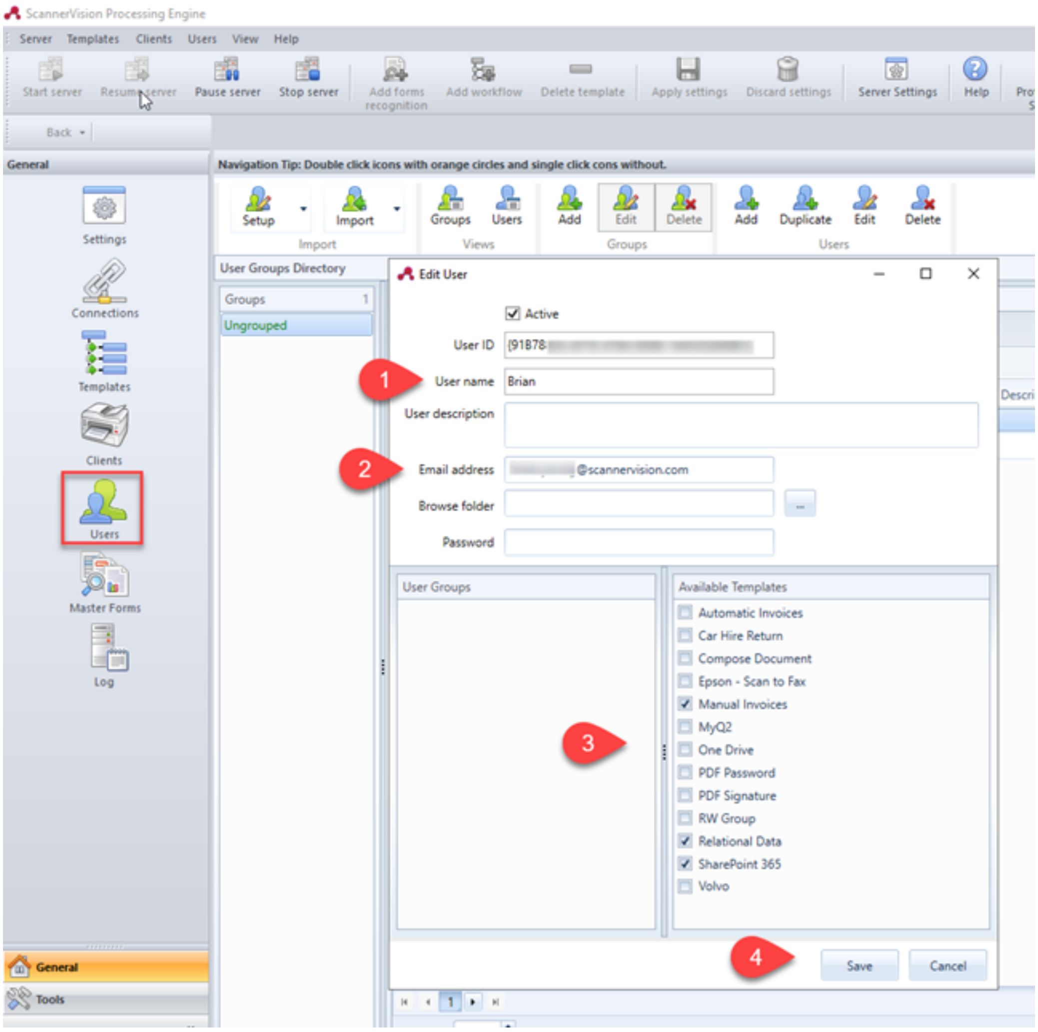


Configuring Users

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:

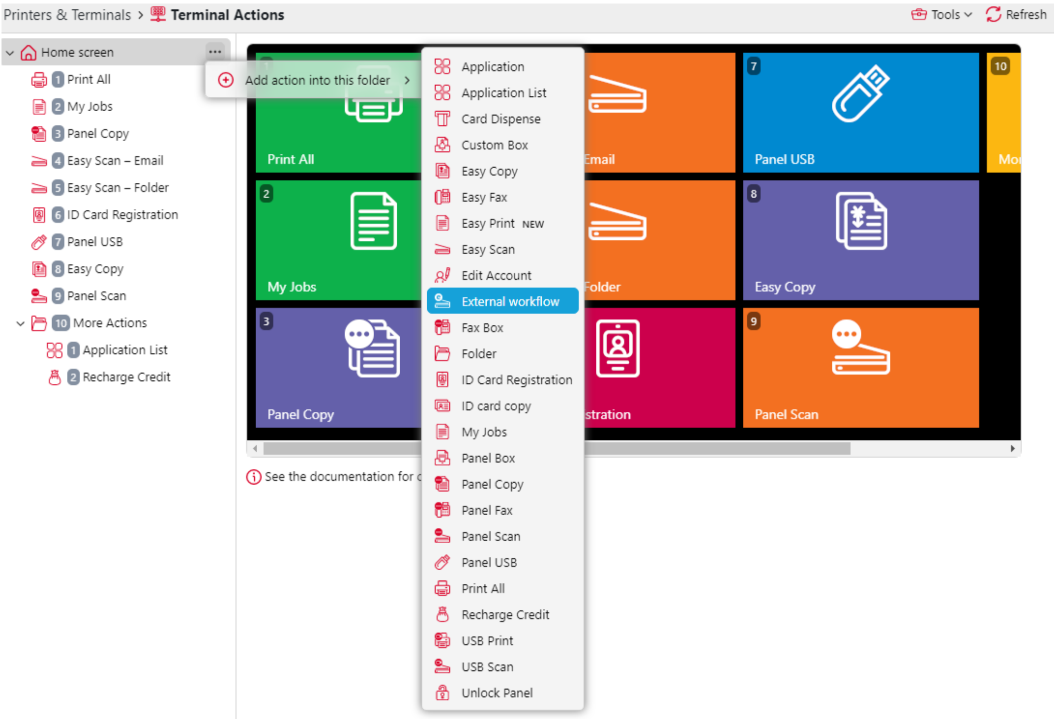
1. Make sure that the **User name** matches the MyQ user name (if users were manually added).
2. Make sure that the **Email address** matches the MyQ user's email address (if users were manually added).
3. Select templates for the user from the **Available Templates**.
4. Click **Save**.



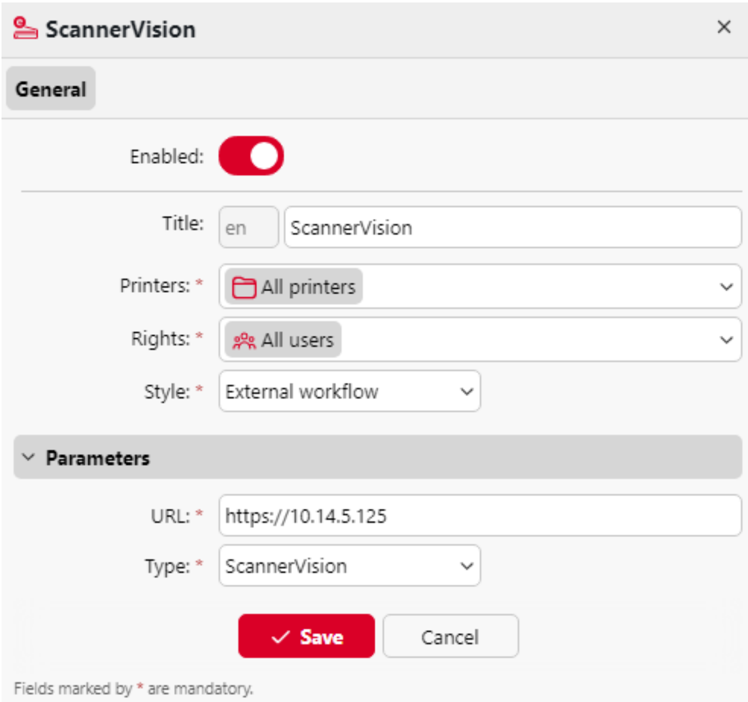
Adding ScannerVision as a Terminal Action in MyQ

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:



a. Enter a **Title**. After saving, this will be shown as the name of the **External workflow** action in the **Home** screen pane and on the terminal preview.
b. Enter the **URL** of the ScannerVision server; *ScannerVisionServer:port*. *http* or *https* depends on the ScannerVision server settings.
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.
For example: *https://10.14.5.125* for SSL only with the default port used and *http://10.14.5.125:81* for non SSL and the port was changed from *80* to *81*.
c. Change the **Printers** and/or **Rights** if you want to create a specific MyQ Smart Workflow.
d. Click **Save**.

6.6.7 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.

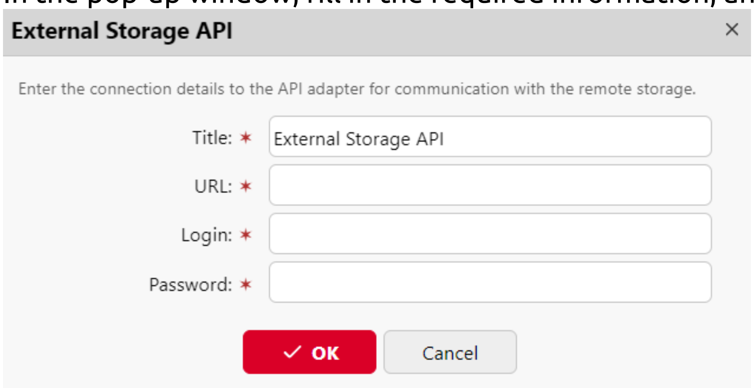
Example usage

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.

6.7 Authentication Servers Settings

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

The following authentication methods are supported:

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

In **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.

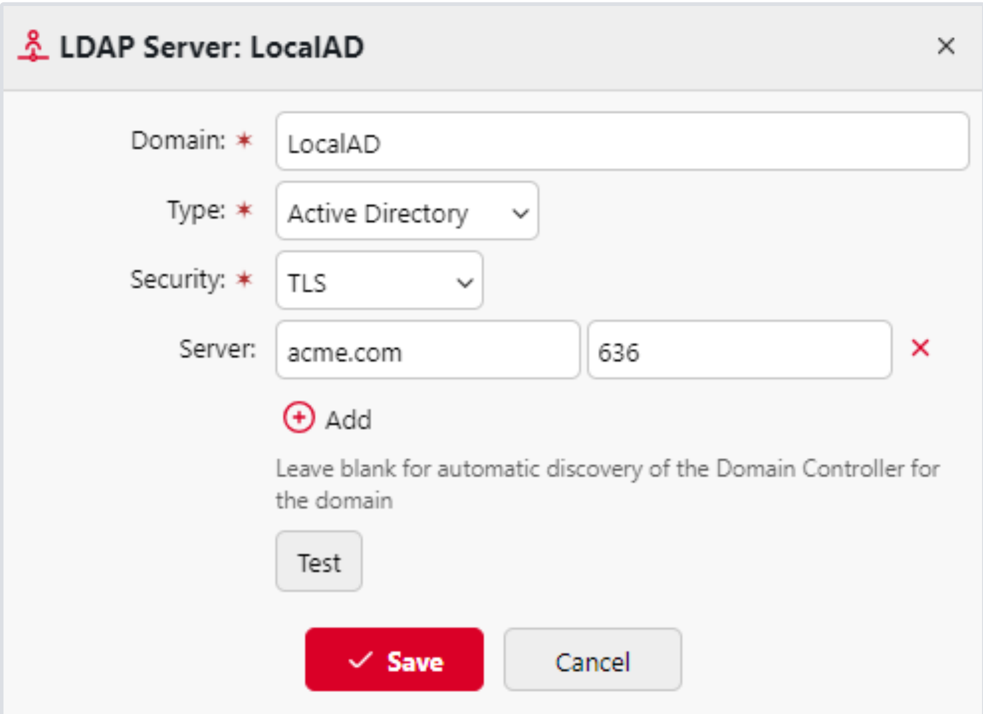
> If you only authenticate users against MyQ (ID cards, PINs, and passwords), and thus do not use any remote authentication servers, or need to integrate with another external authentication provider, see User Authentication for details.

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

6.7.1 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

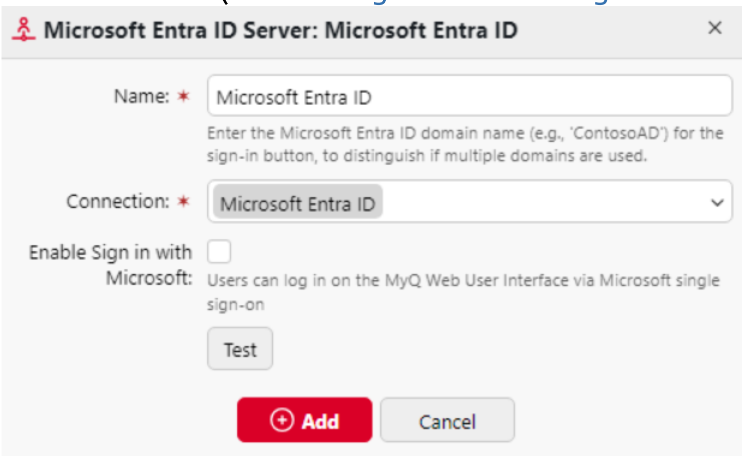
    - another supported option such as **Novell**, **OpenLDAP**, or **Google Workspace**.
4. Configure the **security settings**:
    - Select the security protocol for the LDAP connection.
    - For **Active Directory**, you must select **TLS**.
5. Configure the **server connection**:
    - Enter the **server 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.

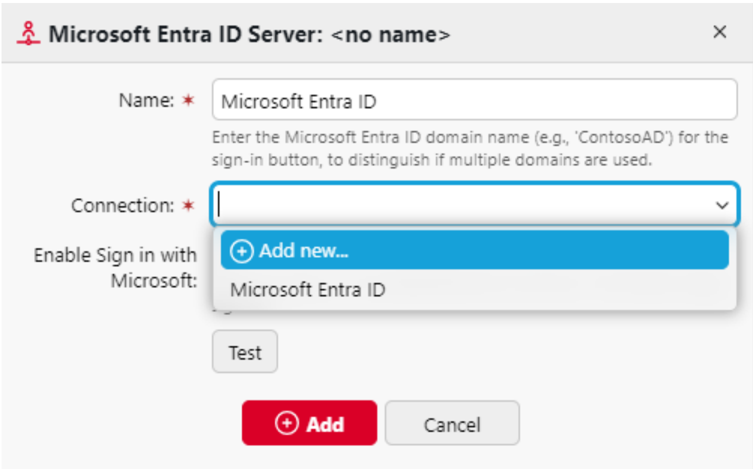


6.7.2 Add Microsoft Entra ID Server

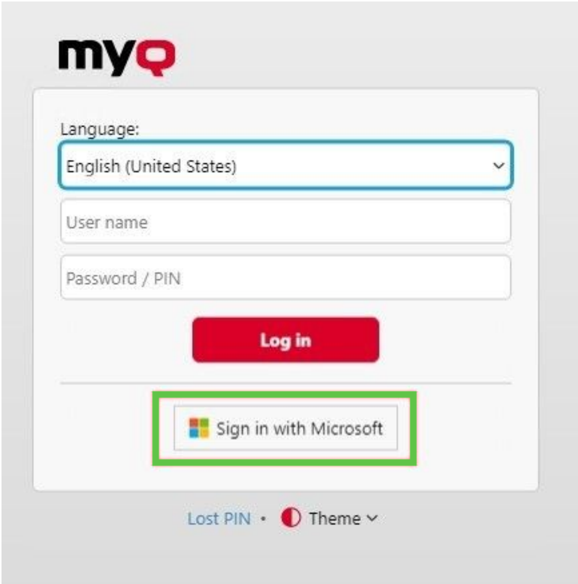
1. Click **+Add** and select **Microsoft Entra ID Server**. The new Microsoft Entra ID server properties panel opens on the right side of the screen.

2. If you have already added Microsoft Entra ID in the **Connections** settings, the server appears on the list. If not, click **Add new**, add the Microsoft Entra ID connection first (follow the guide for creating a new Entra ID connector).



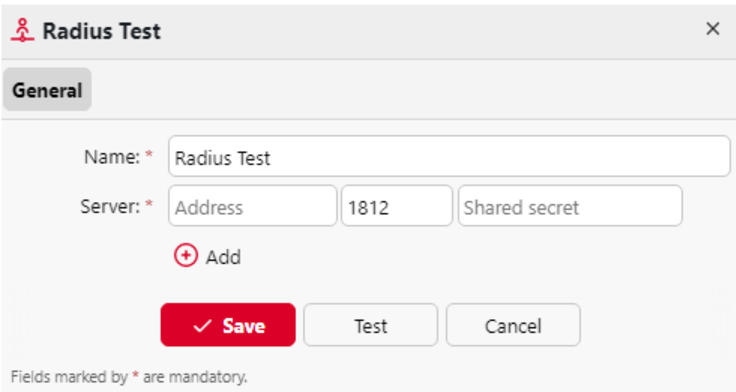


3. Check the **Enable Sign in with Microsoft** checkbox if you want to allow users the login method Sign in with Microsoft.
4. Click **Save**. The Microsoft Entra ID Server now appears on the list of servers.



6.7.3 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.

6.8 MyQ Desktop Client Settings

This feature requires MyQ Desktop Client 10.2+. Older versions are configured during installation or in the application's settings.

Administrators now have the option to save multiple different configurations for MyQ Desktop Client (MDC) in MyQ, so that they can deploy different configurations based on locations; for example, define different fallback printers in each of their offices or enable client spooling only for selected workstations.

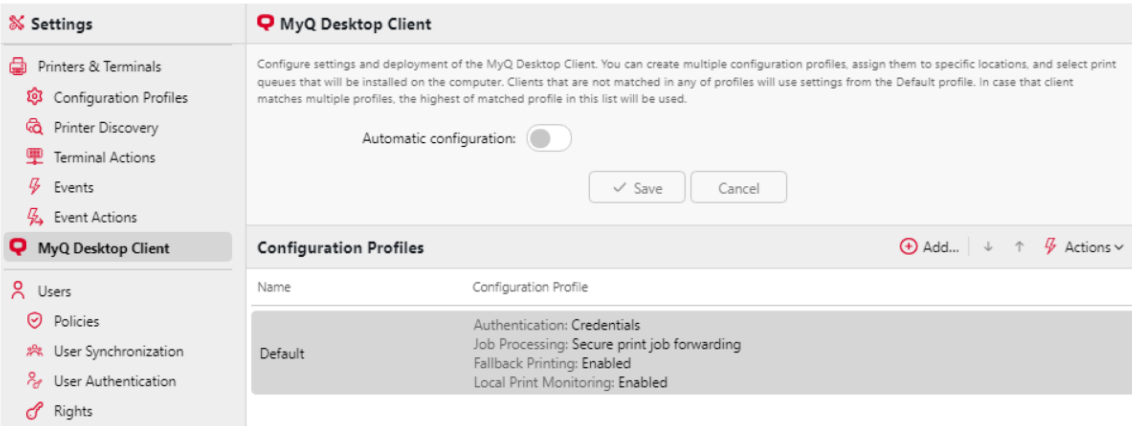
It is possible to configure profiles prior to deploying MyQ Desktop Client 10.2+. Once MyQ Desktop Client connects to the server, it starts automatically using settings from applicable profiles if this feature is enabled.

On the MyQ Desktop Client Settings tab (**MyQ > Settings > MyQ Desktop Client**), you can configure the MDC settings and deployment.

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. In case that the client matches multiple profiles, the highest matched profile in this list will be used.

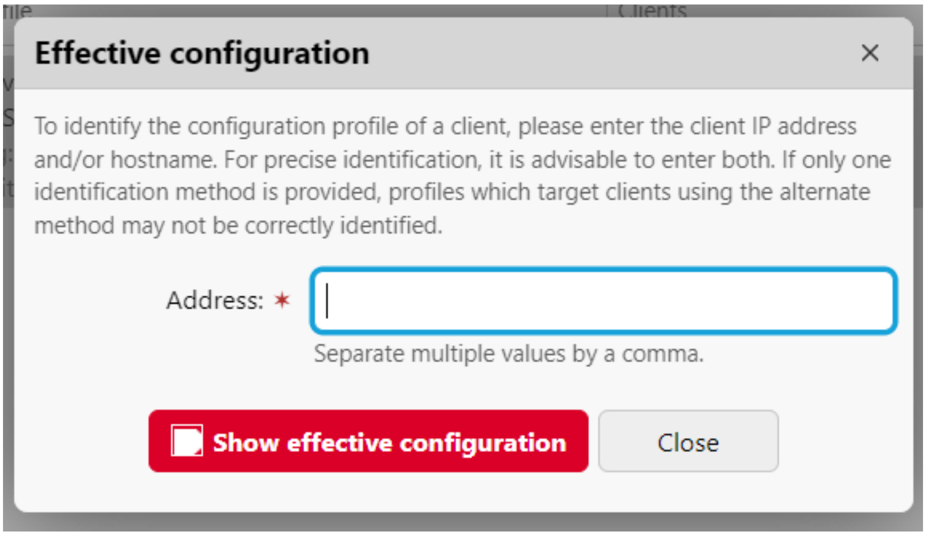
Switch **Automatic configuration** on and click **Save** to use the feature.



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

6.8.1 Show Effective Configuration of a Client

The **Show effective configuration** tool is available in **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.

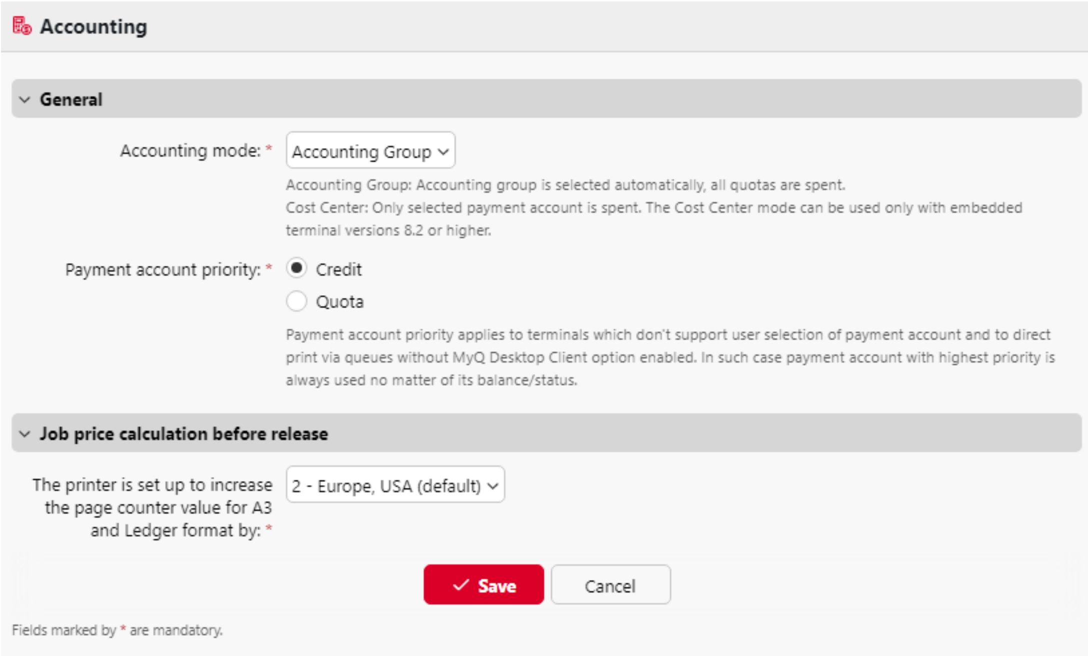


Select **Tools**, **Show effective configuration**, and specify the client IP or hostname of the client you would like to see the configuration profile of. The **Configuration profile**, **Authentication** settings, and **Job processing** settings of the relevant configuration profile are listed.

6.9 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.
- 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:

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

If you use the **Cost Center** mode on embedded terminals with a version older than 8.2, the terminals activation fails. The following error message can be found in the log: "*Terminal is incompatible | reason=Terminal version must be at least 8.2 in cost center mode*".
If you switch to the **Cost Center** mode on embedded terminals with a version older than 8.2, the following warning can be found in the log: "*This terminal is not supported in cost center accounting mode. Upgrade terminal at least to version 8.2*".
Switch to the **Accounting Group** mode or upgrade your embedded terminals to version 8.2 for the terminals to be successfully activated and work properly. If you choose to switch, your terminals need to be re-activated. This can be done automatically by clicking **OK** in the Apply Settings pop-up, or manually on each device.

Comparison between Accounting Group and Cost Center

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

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

6.9.1 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.

6.10 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 Printer Provisioning Profiles for more information.

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.

Printer provisioning is supported for MyQ 10.2 and MyQ Desktop Client 10.2.

6.10.1 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.

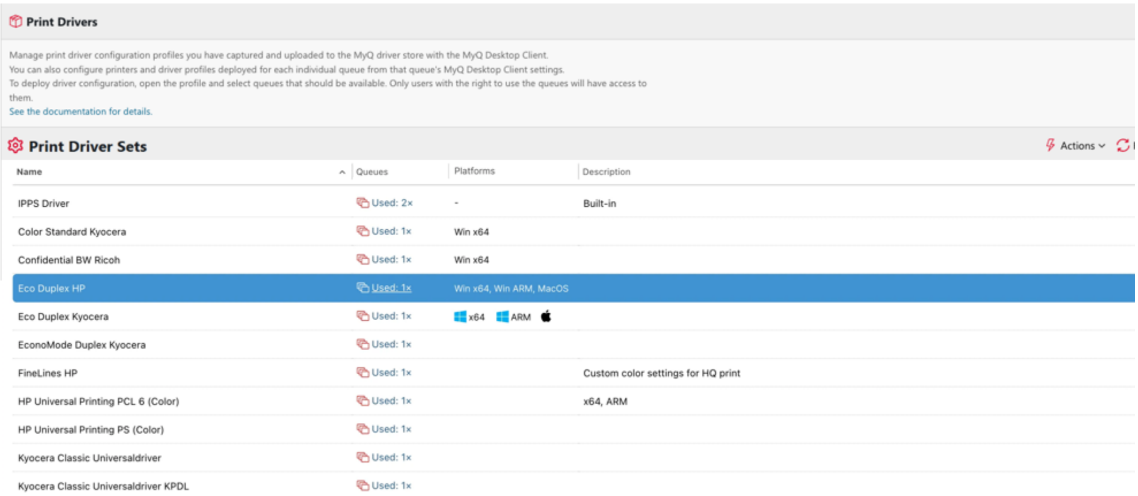
6.10.2 Capture and Upload Print Drivers

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

> 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.

6.10.3 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

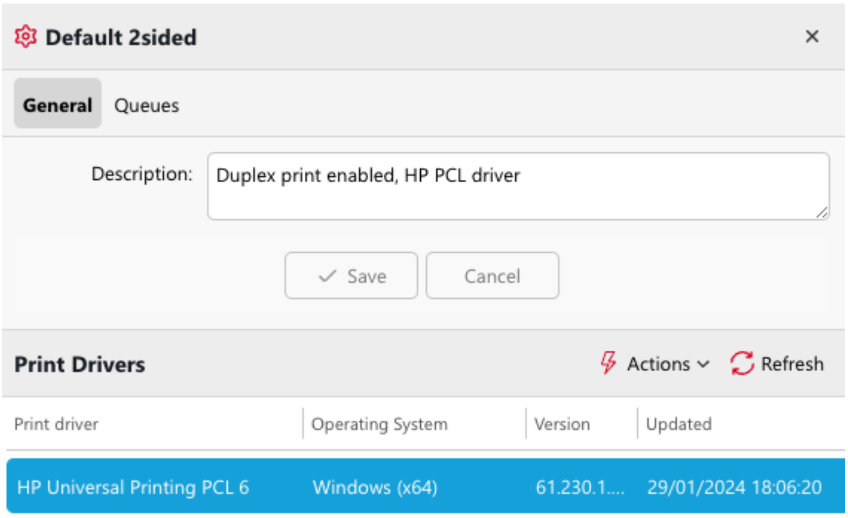
- Description: A note for administration purposes (provided when the driver is captured).
- Print Drivers: A list of print drivers that were captured in this set.

Queues tab

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

6.10.4 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.

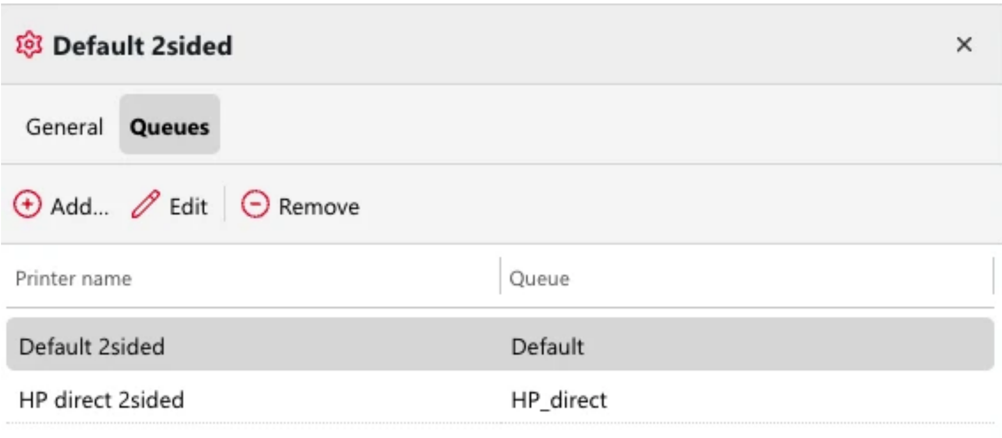
Example: **Kyocera driver with stapling enabled for Windows 64bit and macOS**

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.

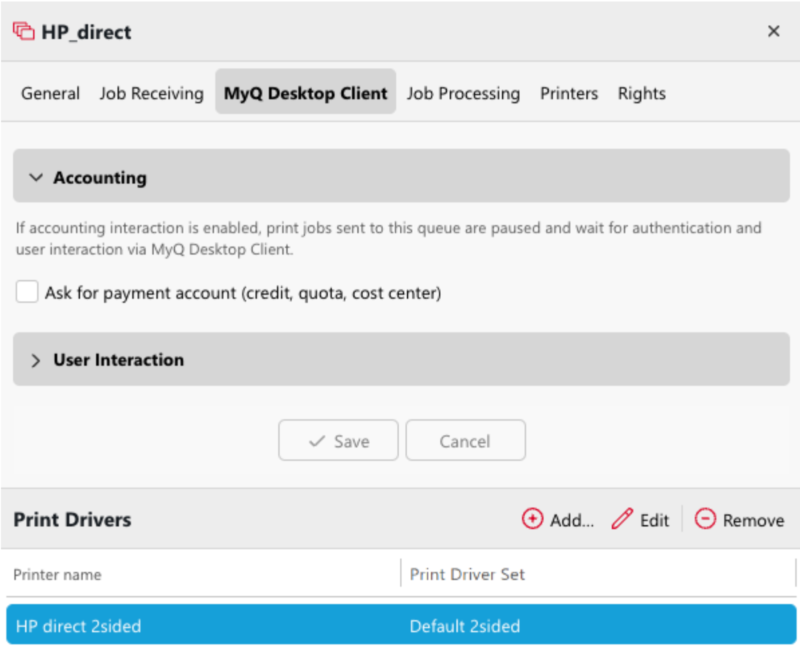
6.10.5 Queues

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.



6.10.6 Queue settings for Printer Provisioning

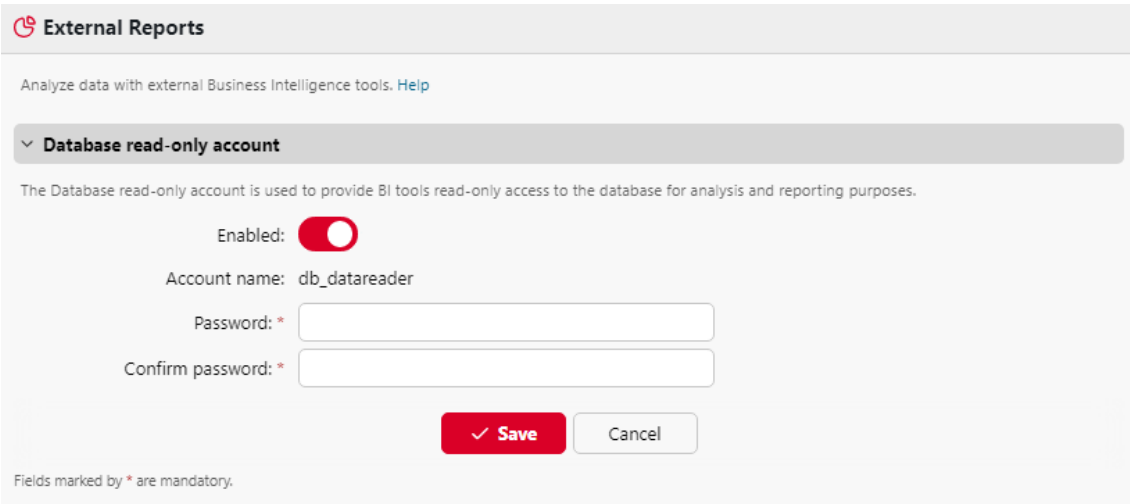
In **Queues** – **queue detail** – **MyQ Desktop Client**, you can specify the print drivers to be installed on client computers with this queue as a destination. If you are deploying one queue multiple times, e.g. with different printing defaults, you will see all the print driver sets this queue is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



6.11 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:

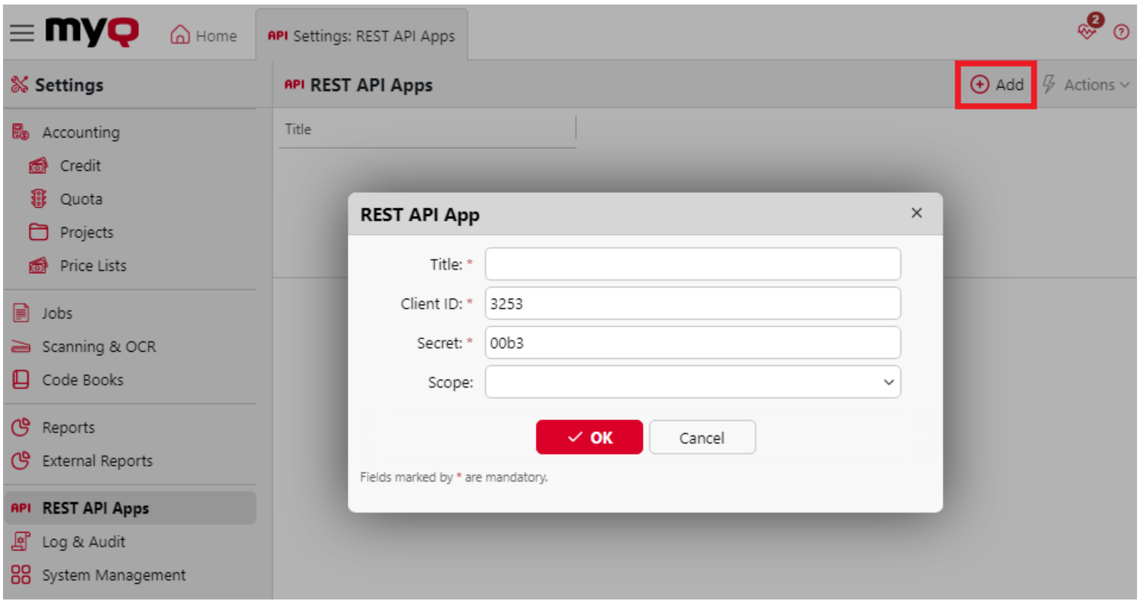
- **Account name**: *db_datareader*. This is the newly created read-only database user. The account name cannot be changed.
- **Password**: password for the *db_datareader* account, set by the administrator. A new password must be set every time when switching from the **Disabled** to **Enabled** state.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

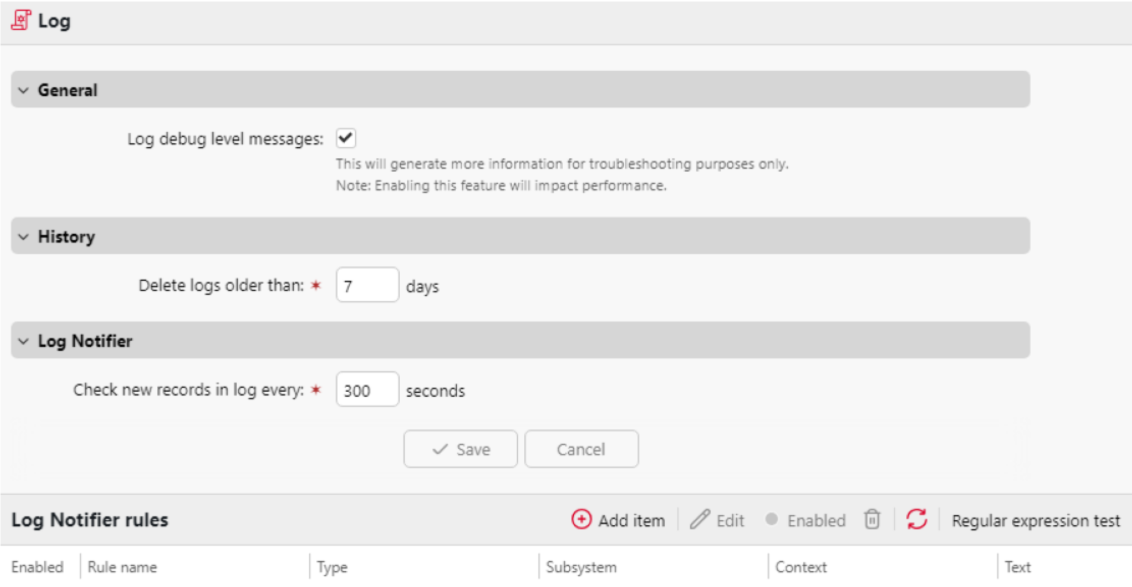
6.12 REST API Apps

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.



6.13 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.

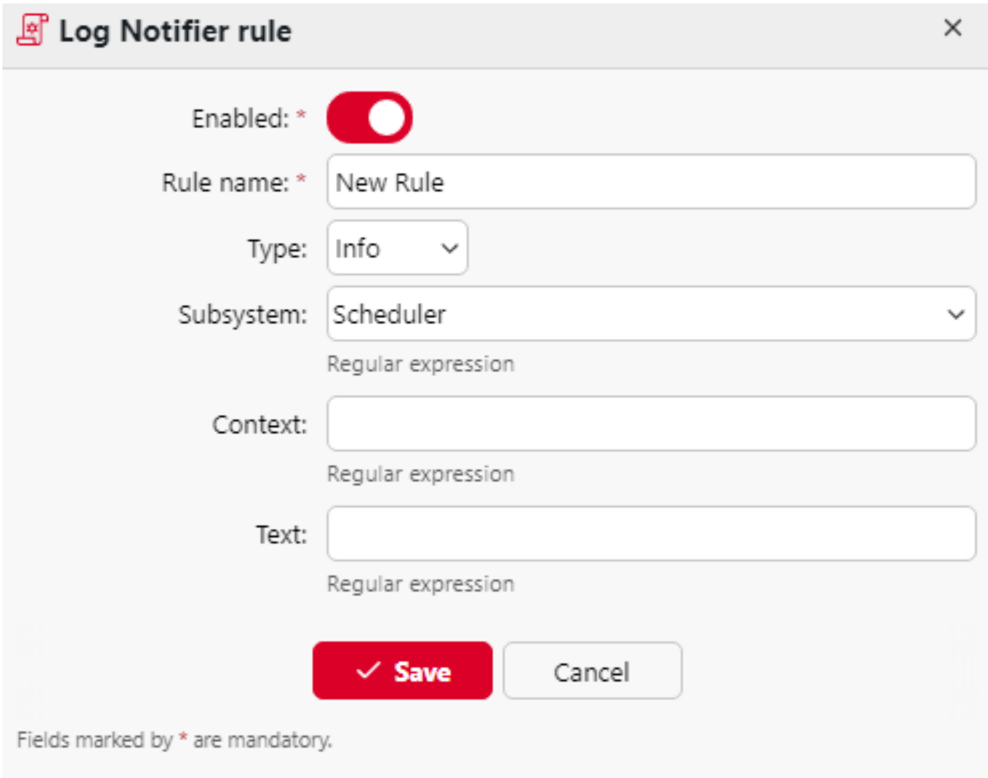
History – Here you can set when the logs should be deleted (in days).

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).

6.13.1 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.

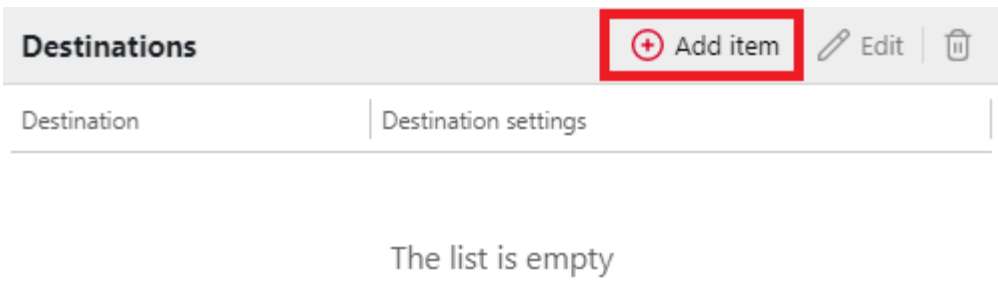


To open the editing options of a rule, double-click the rule (or right-click the rule, and then click **Edit** on the shortcut menu). The following settings can be changed:

- **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**.

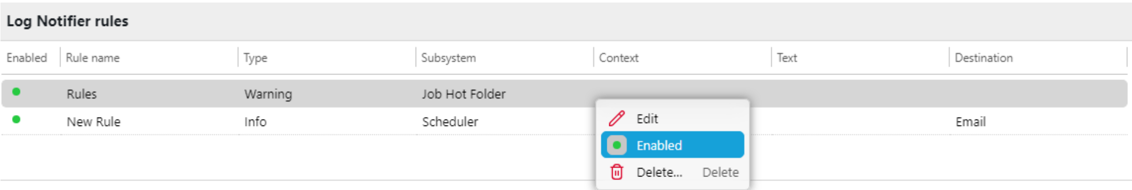


You can select between two destination options: **E-mail** and **Windows Event Log**. If you select the **E-mail** destination, you need to add one or more recipients; you can either select them from the list of MyQ users in the **Recipients** drop-down or directly

type the addresses there. After you set the destination, click **Save**.
The new rule is displayed on the tab.

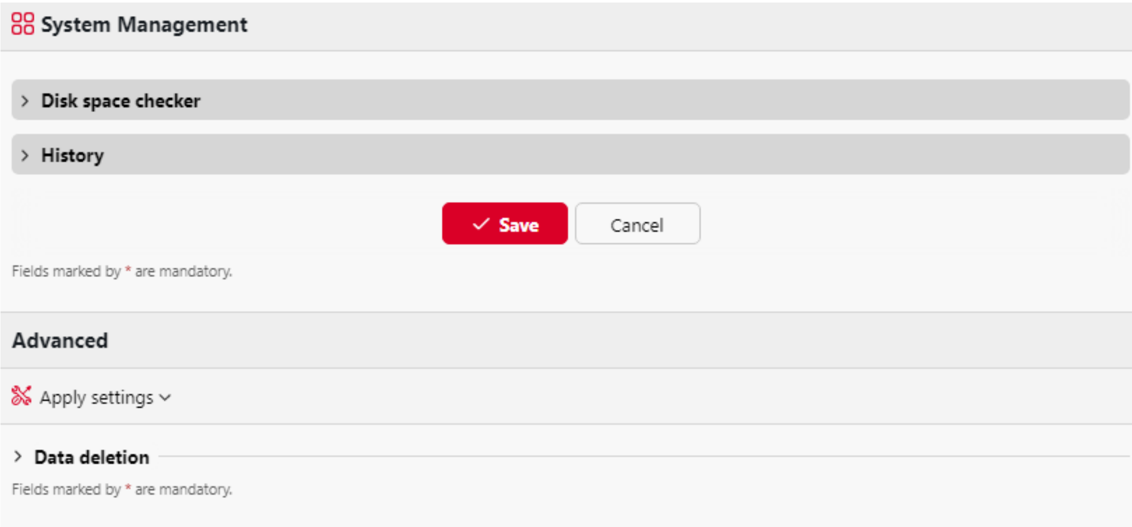
To enable/disable Log Notifier rules:

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

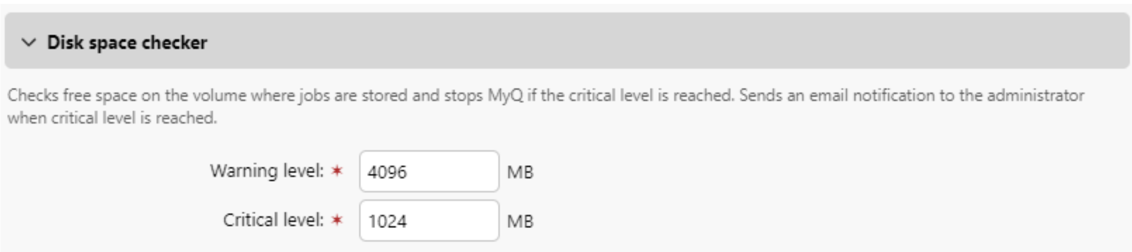


6.14 System Management Settings

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.



6.14.1 Disk Space Checker



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

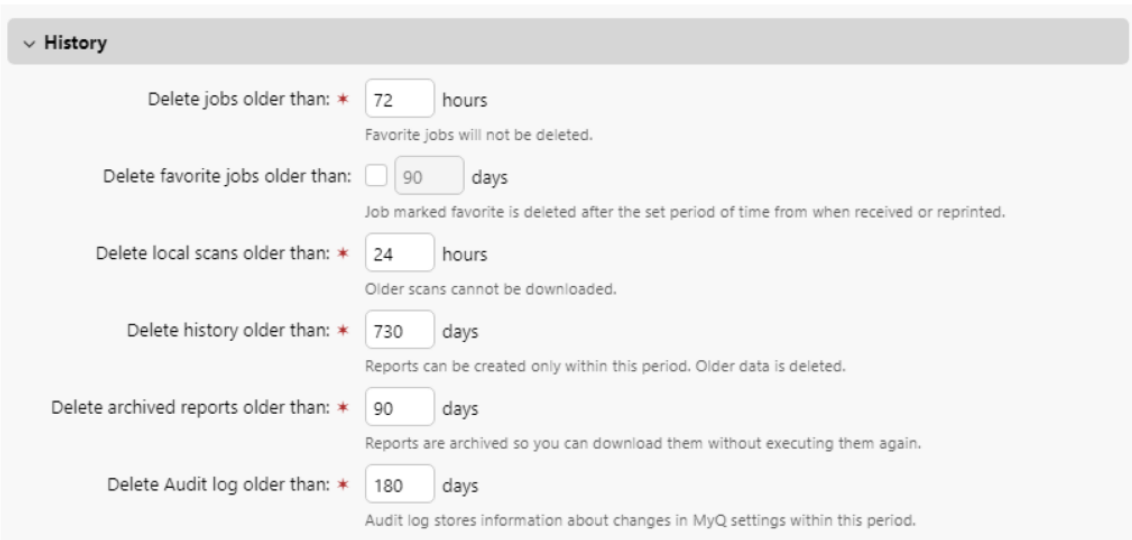
- **Warning level**: If the disk space reaches this level (4096MB by default), the administrator gets an email notification.
- **Critical level**: If the disk space reaches this level (1024MB by default), the administrator gets an email notification and MyQ services are automatically stopped to prevent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

6.14.2 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**.



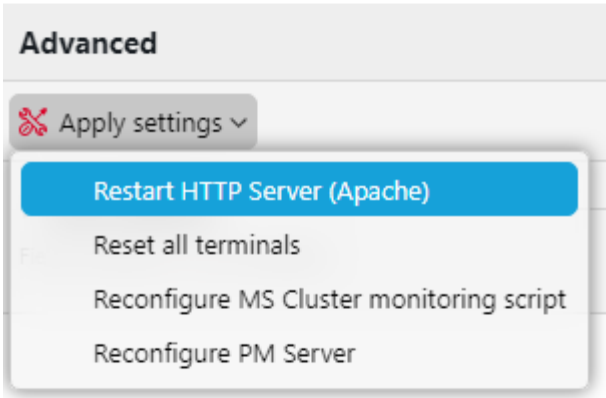
6.14.3 Advanced

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.

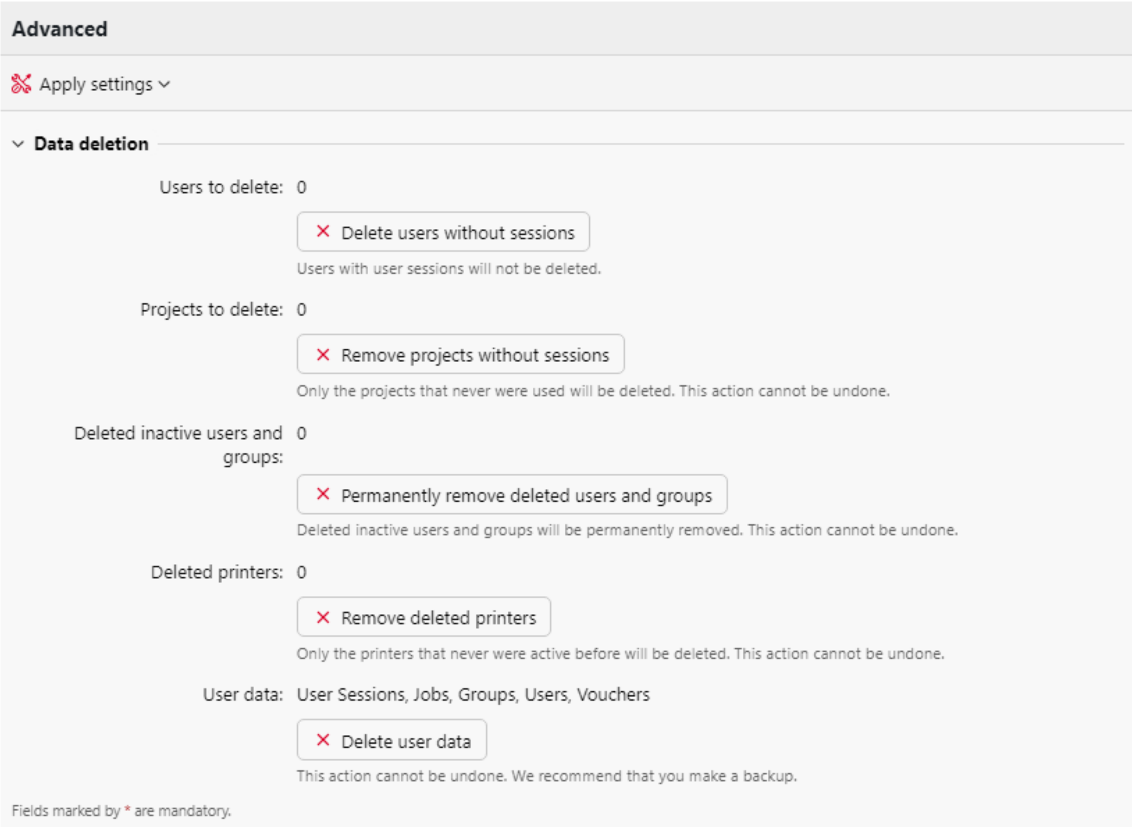
Via the **Apply settings** button, you can reset the components at any time. After you click the button, click a component that you want to reset, and the settings will be applied without further notice.



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.



6.15 Advanced Security

Security in print management is crucial as it involves managing sensitive documents and networked devices. Proper security measures help prevent unauthorized access to print jobs, ensuring confidentiality and compliance with privacy regulations.

Implementing secure print solutions, such as user authentication and encrypted communication channels, mitigates risks of data breaches through intercepted print jobs.

6.15.1 Advanced Security Configuration

The config.ini file can be used for further configuration of the MyQ Print Server. It contains sections with parameters and values for multiple settings, including security. For details, see Advanced Configuration Reference.

> We recommend that you consult with MyQ Support before editing the file.

Security Section

In MyQ X, communication security can be adjusted in various ways, providing maximum flexibility to suit any environment.

Security settings of the majority of components can be set with the **config.ini** file. Those components are HTTP Router, HTTP Server, SMTP, IPP, LPR, and Messages (WebSockets).

HTTP Components

For secure network communication, the **HTTP Router** is a key component.

While, e.g., the minimum SSL/TLS version configured in **config.ini** (see below) also applies to HTTP Router, it can be additionally configured with a file called **traefik.custom.rules.yaml** in more detail. The options set in the **traefik.custom.rules.yaml** file take precedence over the **config.ini** settings.

Secondly, the HTTP Server uses settings from the **httpd.conf** file.

> When editing the HTTP Router settings, make sure you work with the file **traefik.custom.rules.yaml** in *C:\ProgramData\MyQ*, and **not** with the files **traefik.rules.yaml** and **traefik.yaml** in *C:\Program Files\MyQ\Server* that contain the installation defaults, and are reverted after every MyQ X upgrade.

6.15.2 Common Security Settings

Minimum TLS version

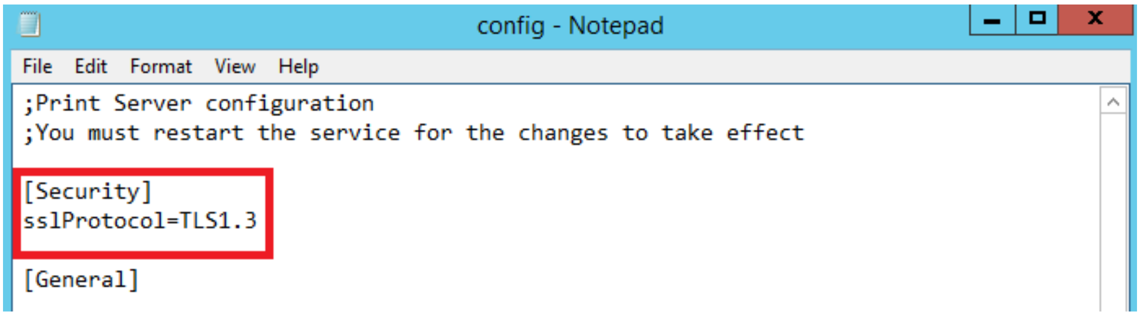
To specify the minimum security protocol used for communication, go to **C:\ProgramData\MyQ** and open the **config.ini** file in a text editor.

Add a section called **[Security]** and in a new line under that, add the parameter **sslProtocol** with the value you want. The possible values are *TLS1, TLS1.1, TLS1.2,* and *TLS1.3.*

> From MyQ Print Server 10.2, the default value is *TLS1.2.*

For example, you can add:

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



This applies to all components mentioned above, including the HTTP Router, and thus improves the overall communication security of the entire system.

Save the file and restart all services for the change to take effect.

Supported Cipher Suite

A full list of supported ciphers is available here.

You can also modify the set of supported ciphers alongside the TLS version.

You can do so with the following options:

Use strict secure defaults

You can use the `config.ini` flag `sslCipherSuites` to enable the strict secure mode. It uses the defaults of the HTTP Router component (and compared to the standard behavior, it deprecates ciphers considered weak).

This flag supports these options:

- `compatible`
  Enforces support of selected weak ciphers; might be needed for communication with older devices.
- `strict`
  No weak ciphers allowed.

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

Ciphers allowed in the compatible mode and not in the strict mode are:

`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`

While it is **recommended to always prefer the strict mode** that disables weak ciphers, it is not currently MyQ X's default mode.
By default, MyQ X operates in the compatible mode due to the nature of printing systems, device support, and general update availability. Many still supported printing devices do not have (and might never have) available updates compatible with the strict mode.

Allow only selected ciphers

By editing `traefik.custom.rules.yaml`, you can specify what ciphers will be allowed by the HTTP Router during communication.

Example use:

```
tls:
  options: { default: { cipherSuites: [ TLS_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_3DES_EDE_CBC_SHA ] } }
```

When `sslProtocol` is set to allow only TLS 1.3, no ciphers can be disabled or specifically enabled. Secure defaults given by the HTTP Router defaults are used.

Make sure that the connected devices support the required ciphers, and if not, look up available firmware upgrades that may bring security improvements.

Force Kerberos-Only Authentication

For environments that require the strictest security, you can configure MyQ to **use Kerberos** only. This disables NTLM fallback for MyQ applications and enforces Kerberos-only authentication.

To configure this, in the `[Security]` section of the server `config.ini` file, add the following parameter:

`KerberosOnly=true`

Important! Ensure that your environment is correctly configured for Kerberos, including proper SPN registration.

6.16 Advanced Configuration Reference

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.

6.16.1 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.

6.16.2 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 support for eGoldFax and Lotus Domino
eGoldFax=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
```

6.16.3 `[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.

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.
`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.

Parameter	Version	Default	Description
`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.

6.16.4 `[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. Once documenting, mention the maximum recommended delegates. **Values:** 0, 1

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+	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**.
`registerUserName`	8.2-10.1	0	Enables web user registration based on username and PIN/password. **Values:** 0, 1

Parameter	Version	Default	Description
`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

6.16.5 `[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).
`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).

6.16.6 [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)

6.16.7 [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).

6.16.8 [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.

6.16.9 `[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`.
`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.

Parameter	Version	Default	Description
`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%`
`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.

Parameter	Version	Default	Description
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.

6.16.10 [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
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.

6.16.11 [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

6.16.12 [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.

6.16.13 [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.

6.16.14 [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.

6.16.15 [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.

6.16.16 [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.

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

6.16.17 [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.

6.16.18 [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

6.16.19 [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.

6.16.20 `[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`

6.16.21 `[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.

6.16.22 `[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

6.16.23 `[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.

Parameter	Version	Default value	Description
`caValidity`	8.2+	730	CA certificate validity in days.

Parameter	Version	Default value	Description
`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
`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

6.16.24 `[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.

6.16.25 [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.

6.16.26 [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.

6.16.27 [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.

Parameter	Version	Default	Description
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.

6.16.28 [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.

6.16.29 [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

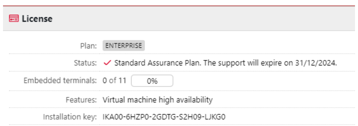
7 Licenses

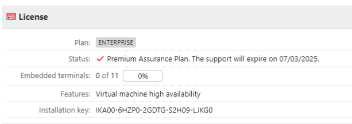
The MyQ X licensing model uses an Installation Key per MyQ setup. A single installation key can contain license information for several products (for example, a perpetual license with a number of Embedded Terminal licenses).

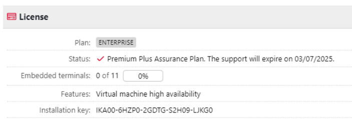
Your license will impact:

- The number of Embedded Terminals you can use.
- The number of Printer Provisioning Profiles you can create.
- If your purchase is subscription based (requires renewal) or perpetual (no renewal required, although to access support you may need to extend an assurance plan).
- Whether or not you can use ScannerVision.
- Whether or not you have Virtual Machine High Availability (VMHA).

You can view your current license in the License Settings of you MyQ User Interface, or in the **Licences** widget shown on your dashboard. Three types of assurance plan are available, Standard, Premium, and Premium Plus. For more information on assurance plans, see https://www.myq-solution.com/en/software-assurance.







This topic discusses the following subjects:

- how to add and activate licenses
- how to delete licenses
- how to extend software assurance licenses
- how to migrate old licenses to MyQ X
- VMHA License

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

7.1 Adding Licenses

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

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

A license is required to activate devices for monitoring only, however, the total number of such devices allowed is not limited by the license. This means that in order to activate Single-Function-Printers (SFPs) you need at least one Embedded Lite or full Embedded license assigned to that server. This applies to both standalone Print Servers and sites with licenses allocated from a Central Server.

The number of devices that can be activated with embedded terminals is limited by your purchased licenses (the number of desired embedded terminals is specified when the license is purchased).

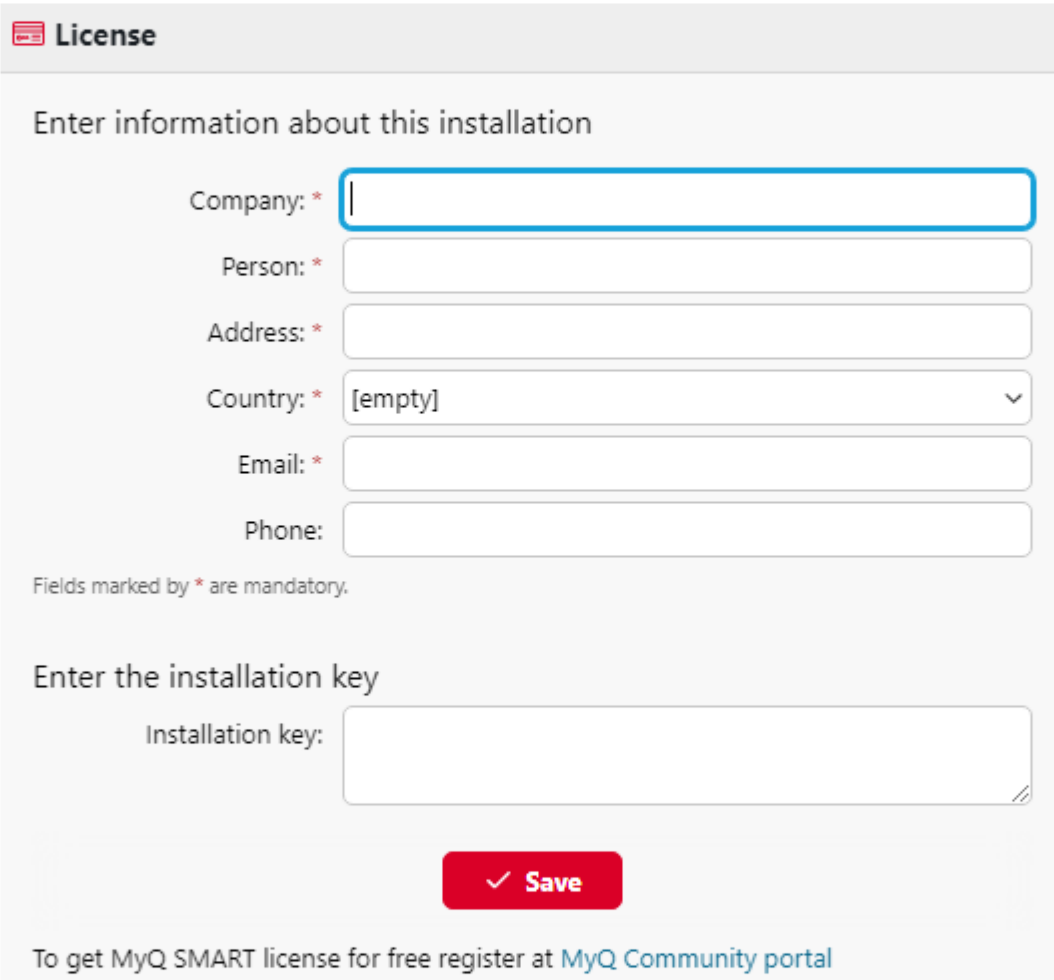
Non-MFPs printers are automatically assigned with an Embedded lite license (2x non-MFPs printers = 0,5 EMB lite + 0,5 EMB lite = 1xEMB license).

7.1.1 Adding Licenses on the Home Screen

The first time you set up the MyQ system, you can add new licenses on the **Home** screen, in the **Enter license** section, under the Quick Setup Guide.

7.1.2 Adding Licenses on the License Settings Tab

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



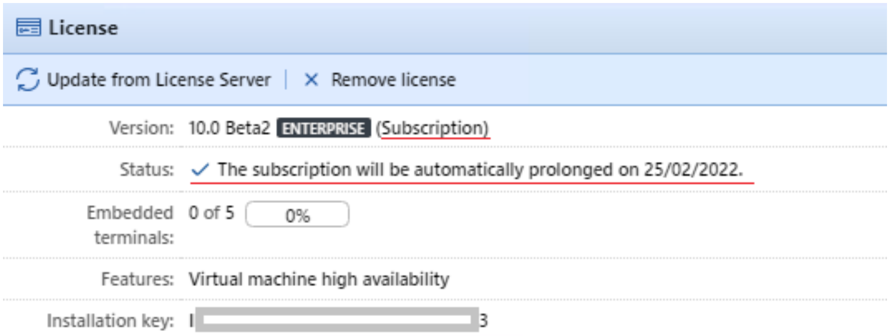
- **Company** - Your company's name
- **Person** - Your full name (e.g. the MyQ administrator's name)
- **Address** - The company's address
- **Country** - Select the country from the drop-down
- **Email** - Your email address
- **Phone** - Your phone number (optional)

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

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

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

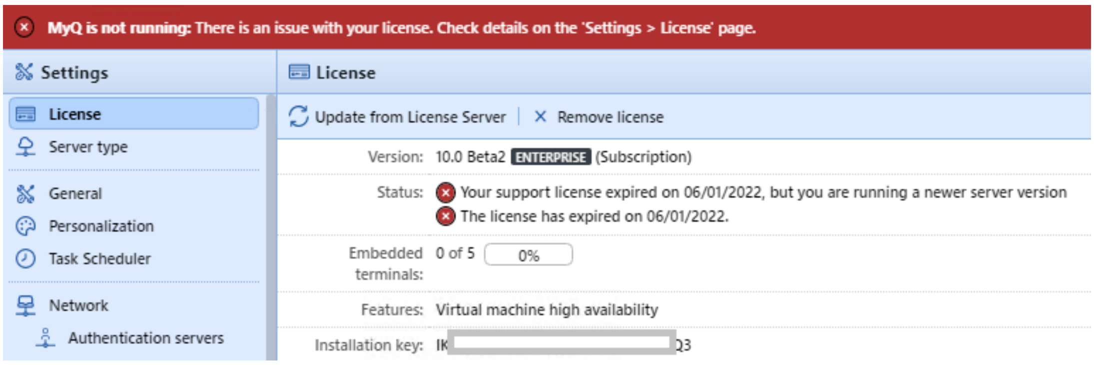
If you are using a subscription license, you can see when the subscription is expiring or when it is going to be automatically prolonged:



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

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

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



If the MyQ server cannot connect to the License server:

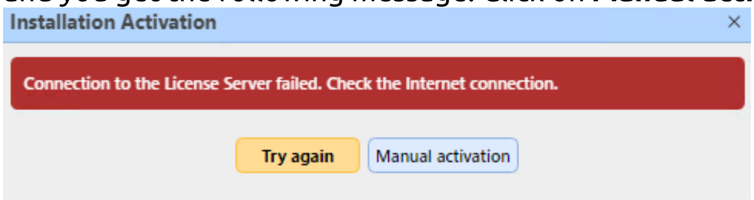
- After the first unsuccessful connection, the MyQ server starts displaying the alert banner "*MyQ server cannot connect to License server, subscription cannot be prolonged and all services will stop in X days. Check internet connection and try to connect manually*". X = number of days until the expiration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

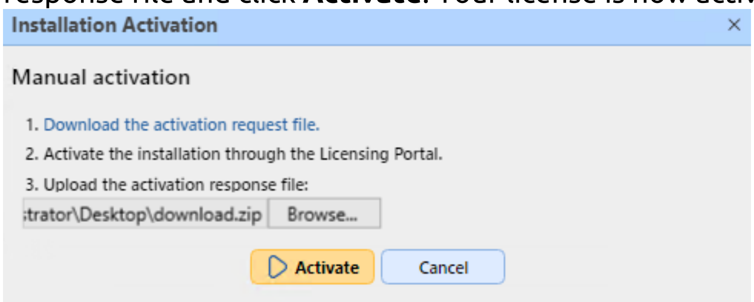
> If you have more than one Embedded licenses and you are using them, for example, as 3 Embedded lite licenses, the status bar in your Licenses overview will show that you are using one Embedded license, since the number is rounded down.

7.2 Activating Licenses

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

7.2.1 To manually activate a license:

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


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


7.2.2 Reactivating Licenses in Case of Hardware Change

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

Steps:

1. Prepare the **new server** with a clean MyQ installation.
2. Create a backup of MyQ (MyQ Easy Config\Database\Backup) on the **old MyQ server**.
   a. Print jobs (by default in C:\ProgramData\MyQ\Jobs) are not part of the backup, because of size.
   b. If required (especially favorite jobs could be required by users after restore MyQ on the new server), they must be copied and backed up manually or by a 3rd-party software.
   c. 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.
3. Restore the backup file from step 2 on the **new MyQ server** (MyQ Easy Config\Database\Restore).
4. With the Installation key now in MyQ Web UI\Settings\License on the **new MyQ server**, you should request for license installation keys activation in 10 days.
5. Generate the Helpdesk support file from the new MyQ server installation (MyQ Web UI\Log\Tools\Generate data for support).
6. Create a Support request (type License issue) for reactivating the installation key with attached Helpdesk support file on the **MyQ Helpdesk partner portal**.
7. When reactivation is confirmed in the task, activate the installation key in MyQ Web UI\Settings\License on the **new MyQ server**.

Notes:

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

> ⚠ Before switching to the new server, disable all MyQ-related services on the old server (via **Services.msc**) and set their startup type to **Disabled**. This prevents the old server from reactivating automatically if it reboots.

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

Steps:

1. Check MyQ Web UI\Settings\License in case any HW changes are done on MyQ server.
2. If the installation key in MyQ Web UI\Settings\License requires activation in 10 days or less, continue with the next steps.
3. Generate the Helpdesk support file (MyQ Web UI\Log\Tools\Generate data for support).
4. Create a Support request (type License issue) for reactivating the installation key with the Helpdesk support file attached on the **MyQ Helpdesk partner portal**.
5. When reactivation is confirmed in the task, activate the installation key in MyQ Web UI\Settings\License.

Notes:

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

7.3 Deleting Licenses

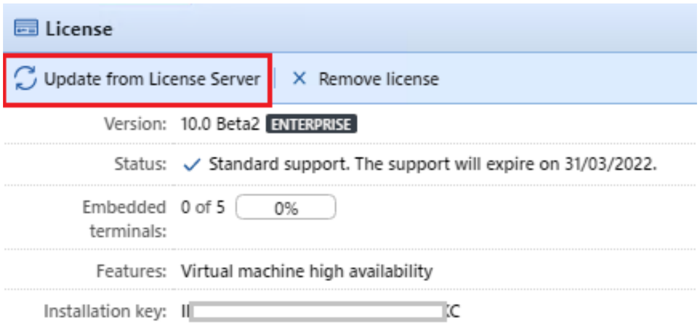
To delete a license:

In **Settings** > **Licenses** click **Remove license**. A prompt will ask you to confirm the action.

7.4 Extending Software Assurance Licenses

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

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



7.4.1 Manual activation

1. Once your additional licenses order is approved, go to the MyQ Web Administrator interface, in **MyQ, Settings, License**, and click the **Update from License Server** button. Since there is no network, you will be prompted to **Download** the activation request file.
2. After you download the file, go to the MyQ X Partner portal, under your Project, in the Installations tab. Click **Offline activation**.
3. In the pop-up window, upload the *offlineActivation.zip* file you downloaded from the MyQ Web Administrator interface, and click **OK**. The activation response file is then automatically downloaded.
4. Go back to the MyQ Web Administrator interface, upload the activation response file and click **Activate**. Your additional licenses are added and activated.

7.5 Migrating Old Licenses to MyQ X

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

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

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

The software assurance expiration date is recalculated during the migration:

1. Expiration dates are converted to a real number and the average is computed. *(for example, you have 100 x Embedded (E) and 200 x Embedded Lite (EL) | so 100 x 'expiration date' of (E) + 200/2 x 'expiration date' of (EL)) / count of ((E) + (EL/ 2))*
2. The computed average is a real number and, converted back to the date format may produce, for example, *23h:56min* - for this reason 1 day is added.

3. From the average corrected date, only the month + year are used, without day + time, and one month is added to the final date.

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

The prerequisites for license migration are:

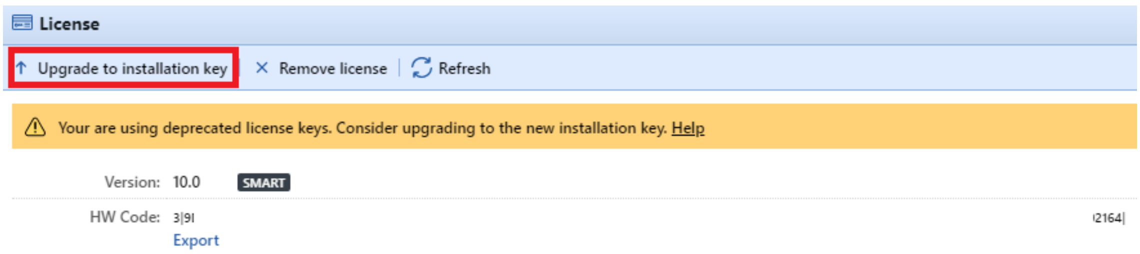
- MyQ Print Server or MyQ Central Server 8.2 or higher installed (valid support required).
- Valid support required; support date for version 8.2 is 15 January 2021, but it is recommended having valid support all the time, especially when there are planned system changes and MyQ Helpdesk would be contacted.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

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

7.5.1 Migration Process

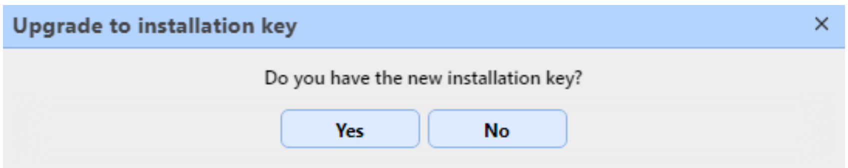
You can start the license migration process in the MyQ web administrator interface.

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

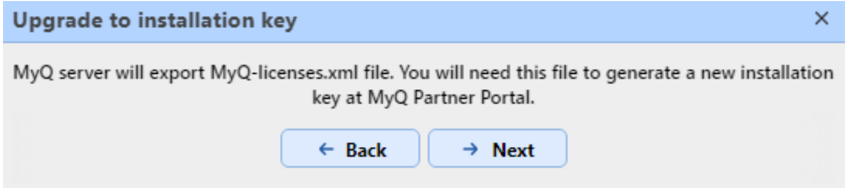


The Upgrade to installation key wizard starts, guiding you through the upgrade:

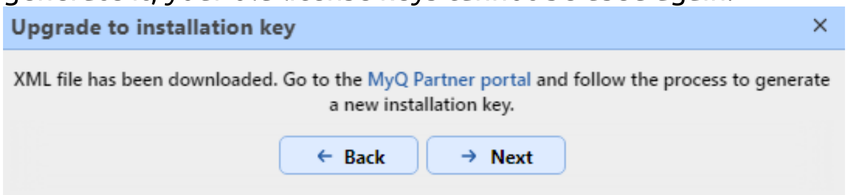
1. If you already have an Installation Key, click **Yes** and continue to step 4. If not, click **No**.



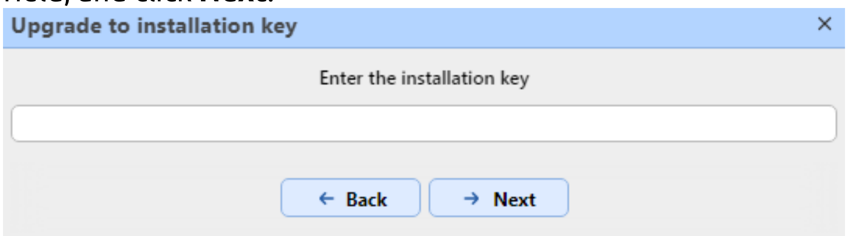
2. The MyQ server will now export the *MyQ-licenses.xml* file. You need this file to generate the new installation key at the MyQ X Partner Portal. Click **Next**.



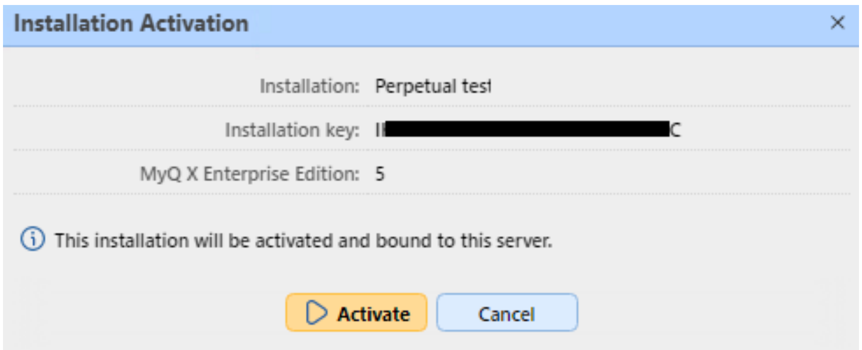
3. The *MyQ-licenses.xml* file has been downloaded. Go to the MyQ X Partner portal and follow the process to generate a new installation key. Once you generate it, your old license keys cannot be used again.



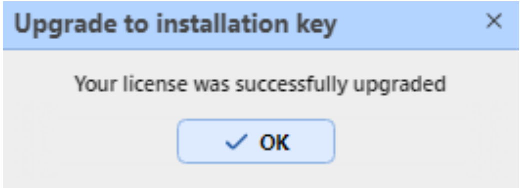
4. Back in the MyQ web administrator interface, insert the installation key in the field, and click **Next**.



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



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



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

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

7.6 VMHA License

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

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

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

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

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

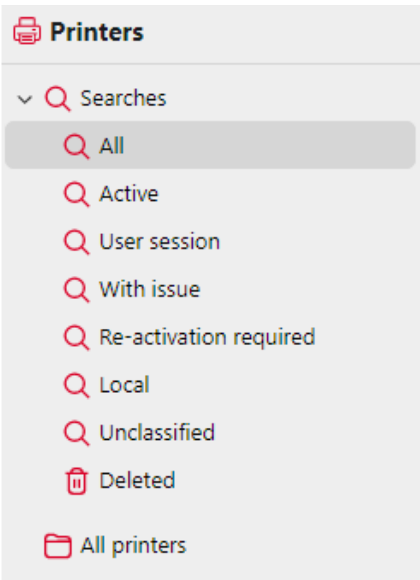
8 Printers

This topic discusses one of the key functions of MyQ — setup and management of printing devices. It covers the following subjects:

- Printers and Terminals settings.
- Overview, adding, activating and deleting printing devices: Manually adding printing devices, Discovering printing devices, Activating and deactivating printing devices, Deleting and undeleting printers.
- Individual device settings, creating groups of printing devices and exporting the list of printing devices: Editing printers, Printer Groups, Exporting printers.
- Monitoring of offline and local printing devices: Monitoring network printers in offline mode, Monitoring local printers.
- Sending email notifications of printing device alerts: Printer Events.
- Creating and assigning SNMP profiles: SNMP profiles.

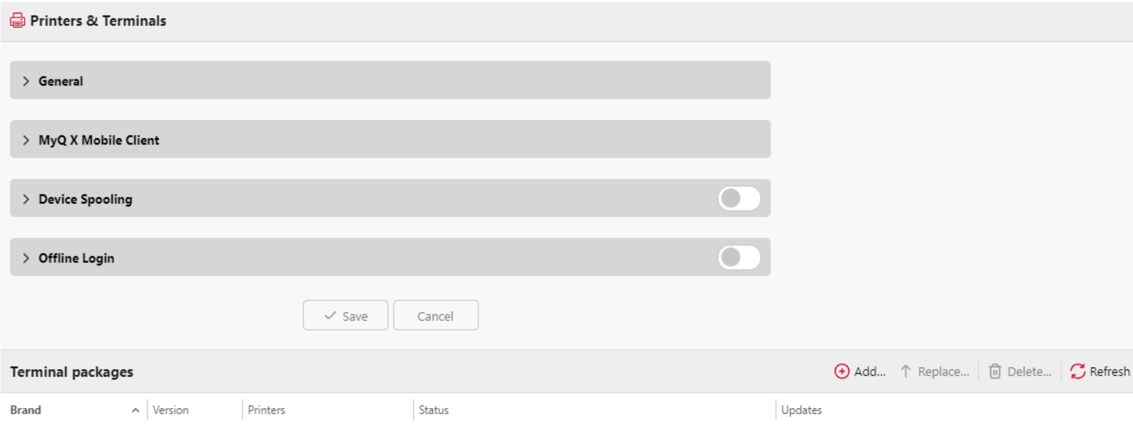
On the **Printers** main tab, you can see printing devices and information about them. With the **All** search option selected, you see all printing devices that are currently in the system. Apart from this option, you can select from the following:

- **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.



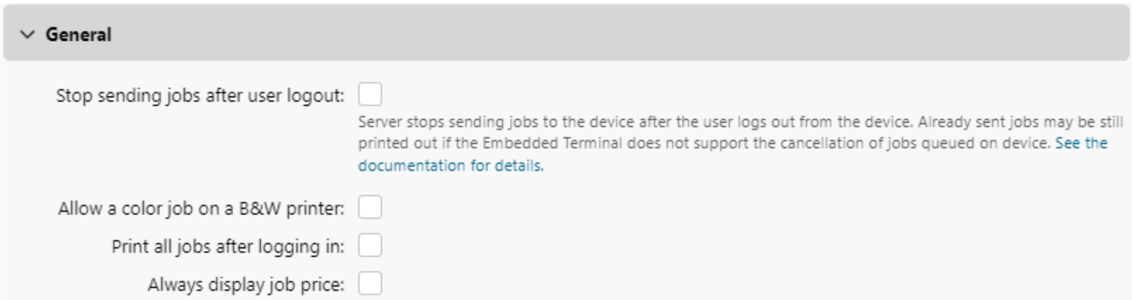
8.1 Printers and Terminals Settings

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.



8.1.1 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.

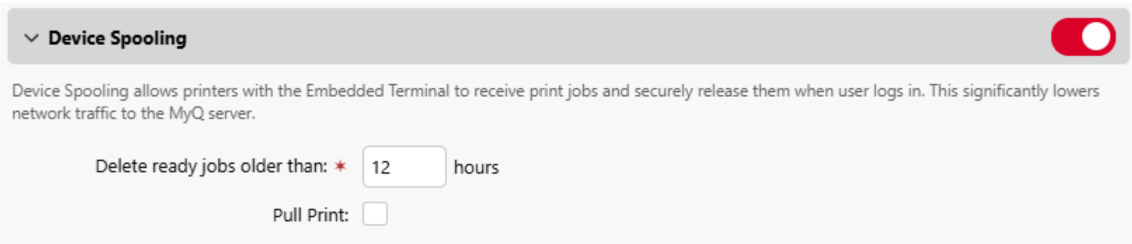
8.1.2 MyQ X Mobile Client

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.

8.1.3 Device Spooling

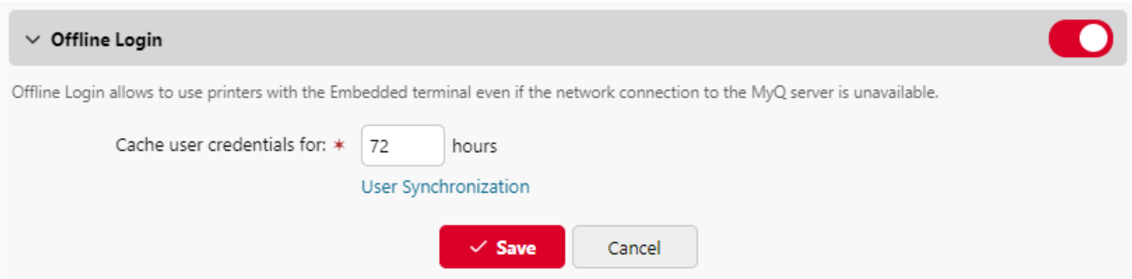
In this section, you can enable the Device Spooling feature for your embedded terminals and set it up.



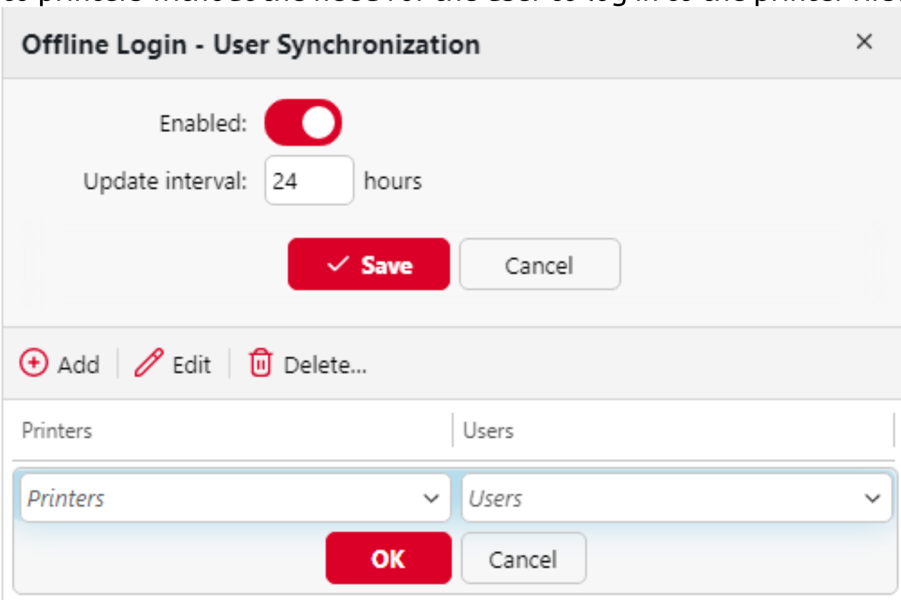
- **Enabled**: Enable/disable the **Device Spooling** feature (disabled by default).
- **Delete ready jobs older than __ hours**: Period of time after which the device spooled jobs are deleted. The default is *12* hours, and the allowed range is *1* to *72*.
- **Pull Print**: If enabled, you can use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

8.1.4 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.

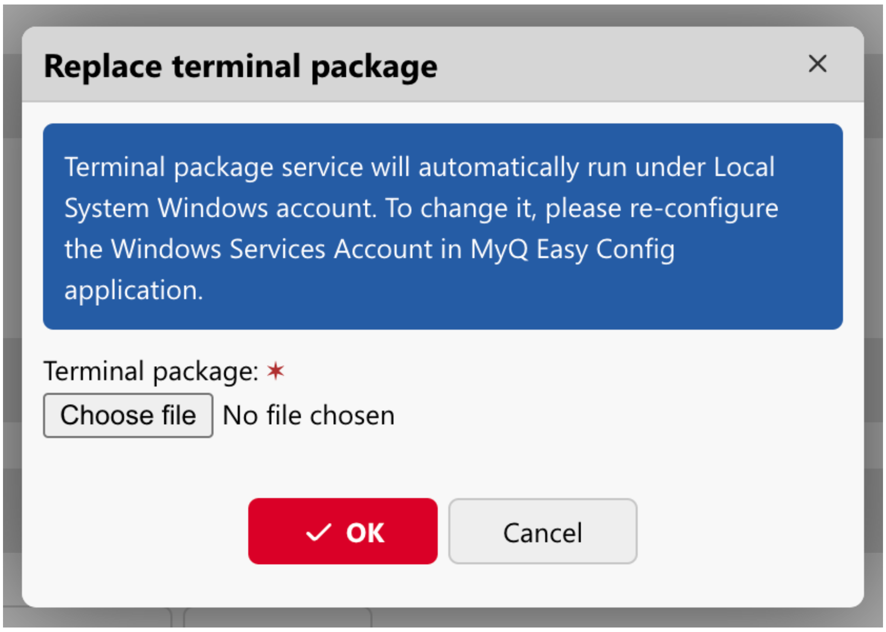
  

  - **Enabled**: Enable/disable offline login user synchronization.
  - **Update interval**: Set the interval of user synchronization between *1* and *168* hours.
  - **Add, edit, delete** printers and users: Configure the printers and users for the offline login user synchronization.

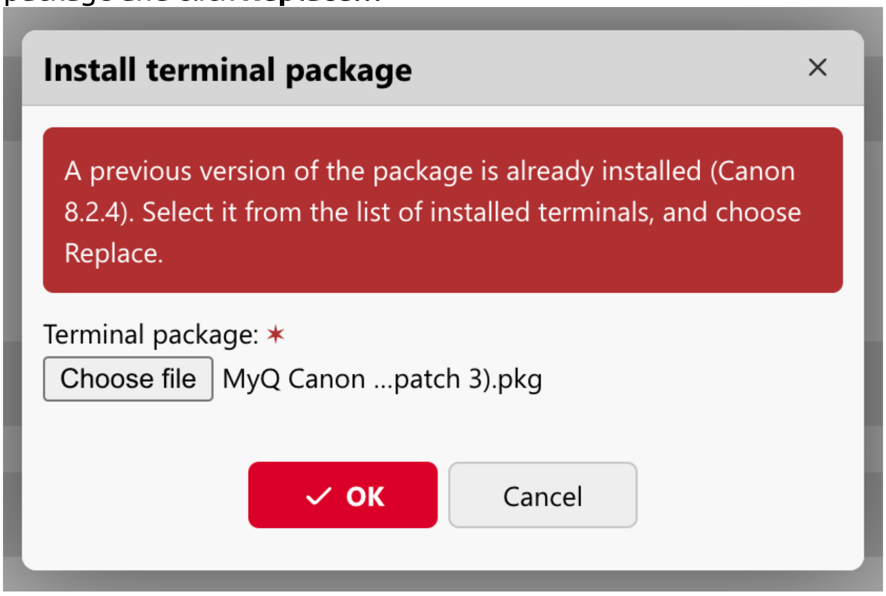
8.1.5 Terminal packages

In this section, you can manage your terminal packages.

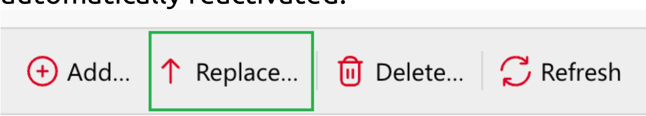
- Click **Add...** to upload a terminal package to the server. In the pop-up window, browse and open the terminal package, and click **OK**. The terminal package is uploaded and installed. (Note that the terminal package service will automatically run under the Local System Windows account. To change it, go to MyQ Easy Config in the Settings tab.)



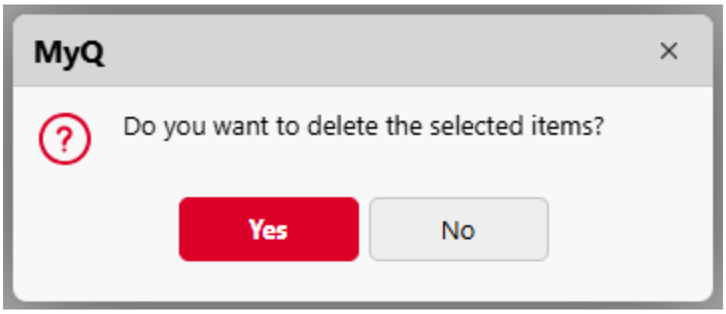
- ◦ If you are trying to update a terminal package by adding a later version of the same terminal package, a pop-up informs you that a previous version of the package is already installed, and to update it you must select that package and click **Replace...**



- 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.



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

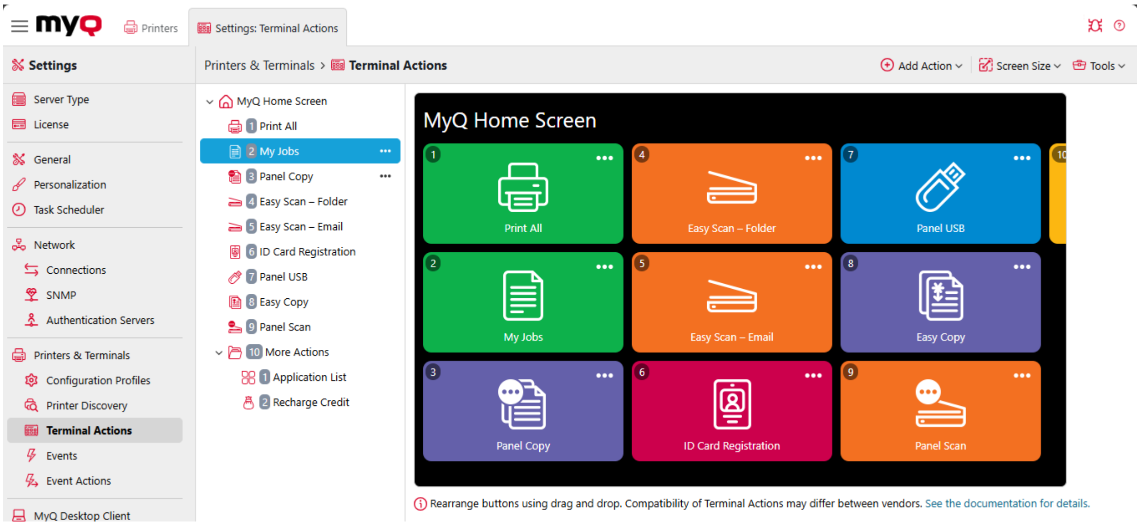
- MyQ Canon Embedded (10.1)
- MyQ Epson Embedded
- MyQ Fujifilm Embedded
- MyQ HP Embedded
- MyQ KATUN Embedded
- MyQ Kyocera Embedded
- MyQ Kyocera Embedded Lite (8.1)
- MyQ Lexmark Embedded (10.1)
- MyQ Ricoh SmartSDK Embedded (10.1)
- MyQ Sharp Embedded
- MyQ Sharp Luna Embedded (10.1)
- MyQ Toshiba Embedded (8.2)
- 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 (for hardware terminals, network authentication, and more). See details in Configuration Profiles.

8.1.6 Terminal Actions Settings

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.

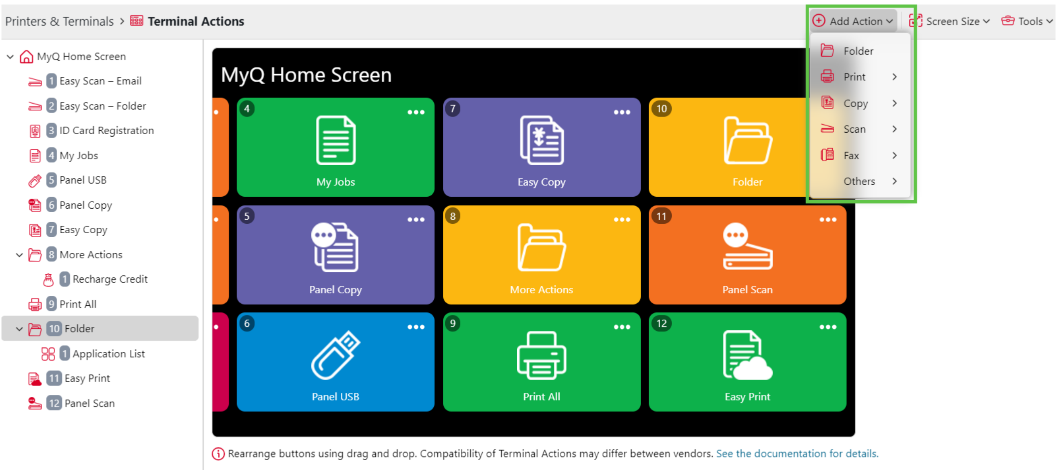
The terminal action nodes can be managed directly on the terminal screen preview where you can:

- 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.

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**.

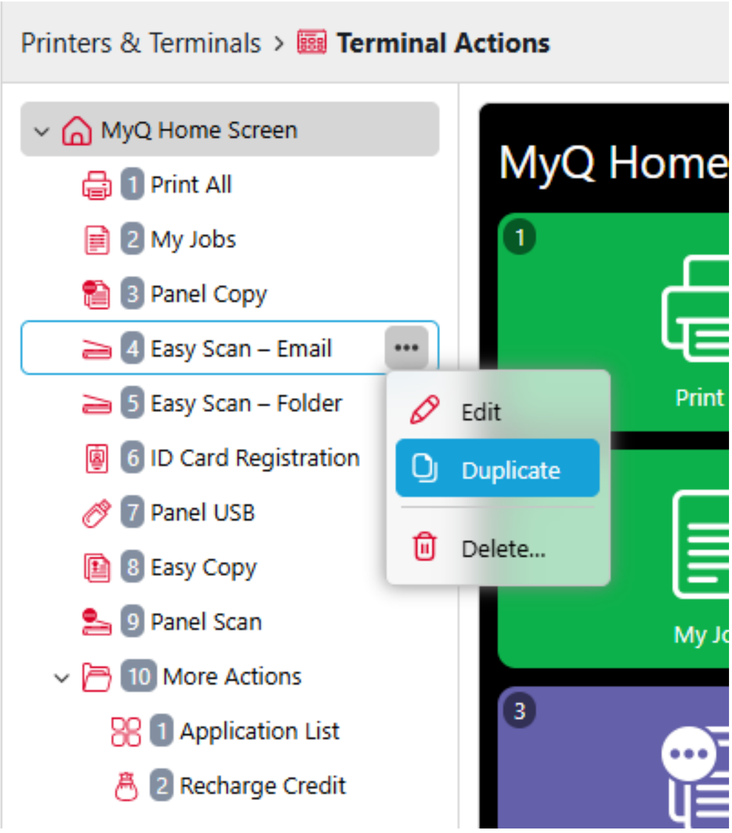


2. Your new terminal action is created, you can now use the content menu on that action's icon to **Edit** the action or drag and drop it to change its position or place it into a folder.

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.

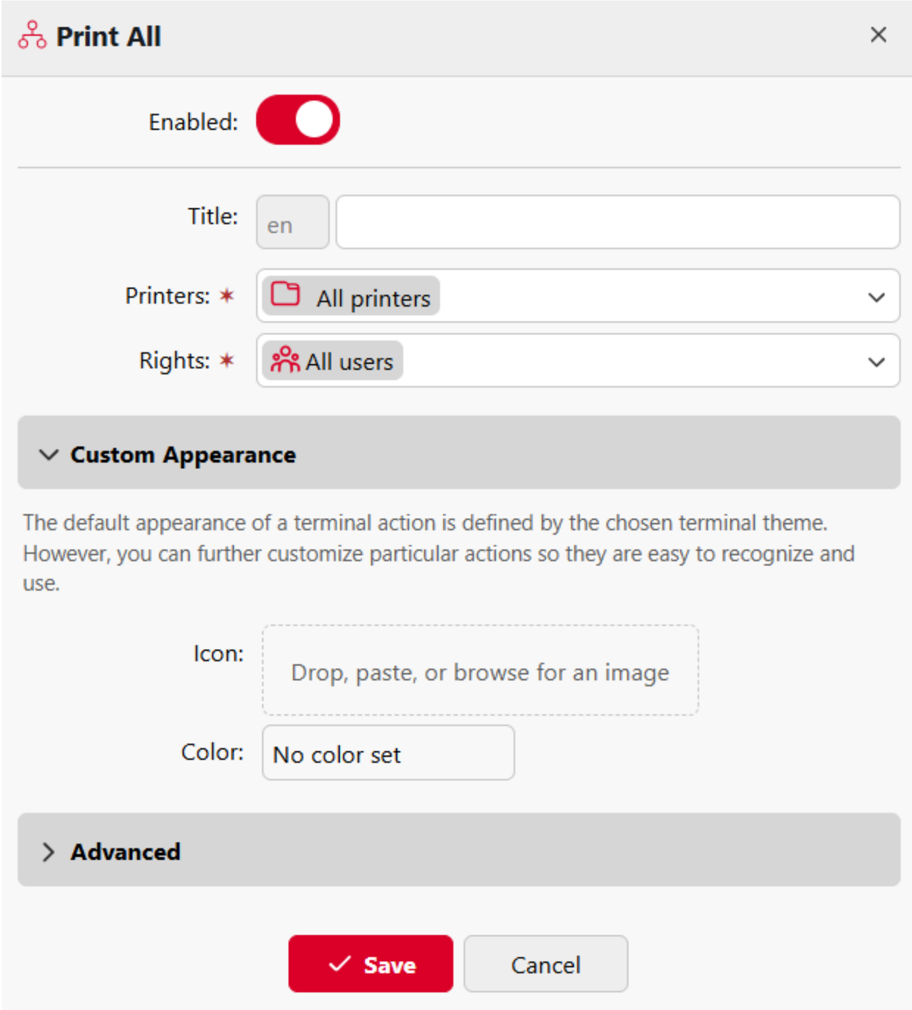


You cannot duplicate native panel actions or special purpose actions such as **Print All** or **My Jobs**.

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.

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.

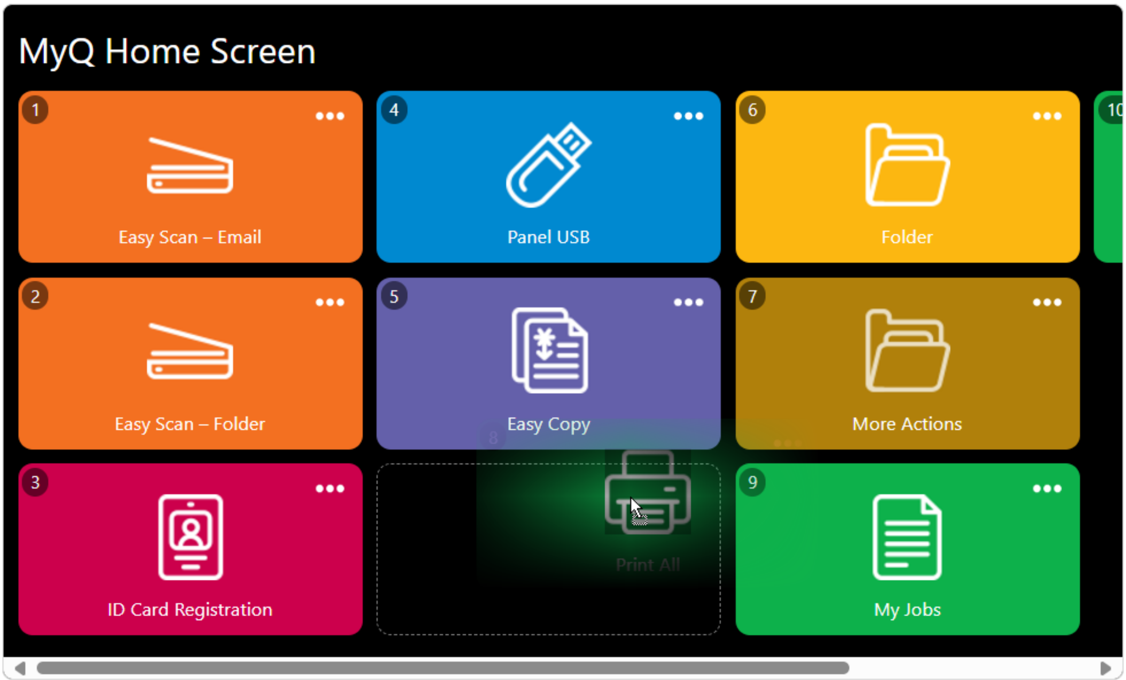
- **Advanced/Reference**: This option allows admins to force extra features on the terminal, providing enhanced functionality and customization for various terminal actions. The value stored in the `Advanced/Reference` field is accessible through the MyQ X API, allowing for seamless integration and retrieval of terminal action data.

> **Titles**, **Custom Icons**, and **Custom Colors** set here will override those set in the Terminal Theme Editor.

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.

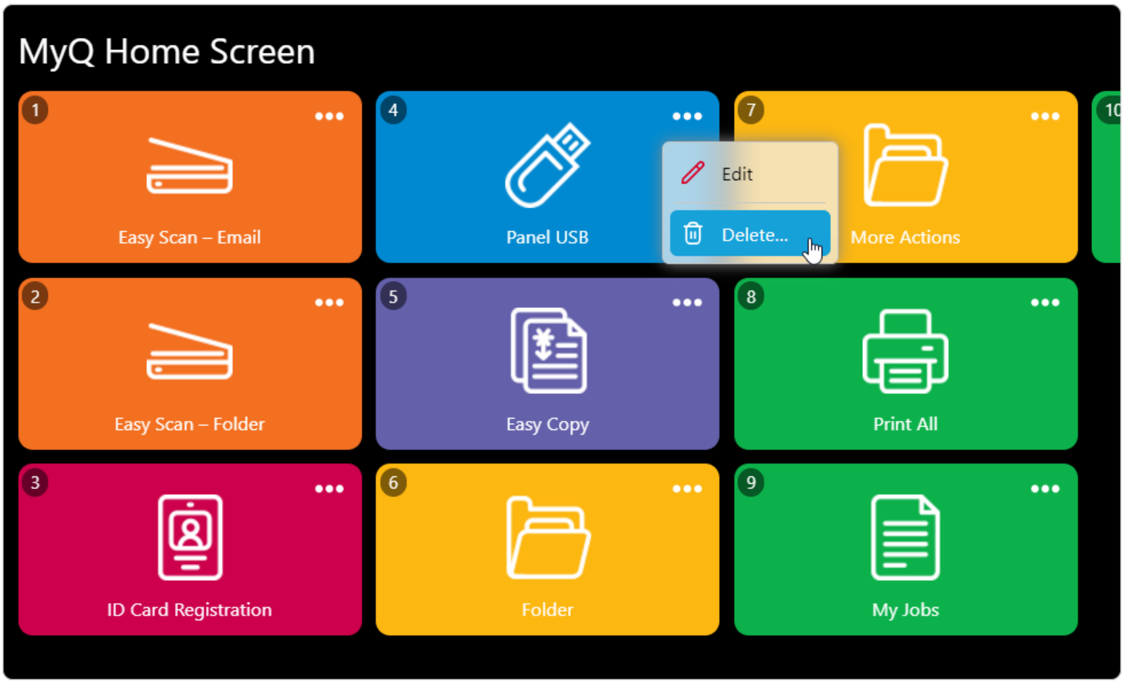


7 Drag and Drop to Change Action Order

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.

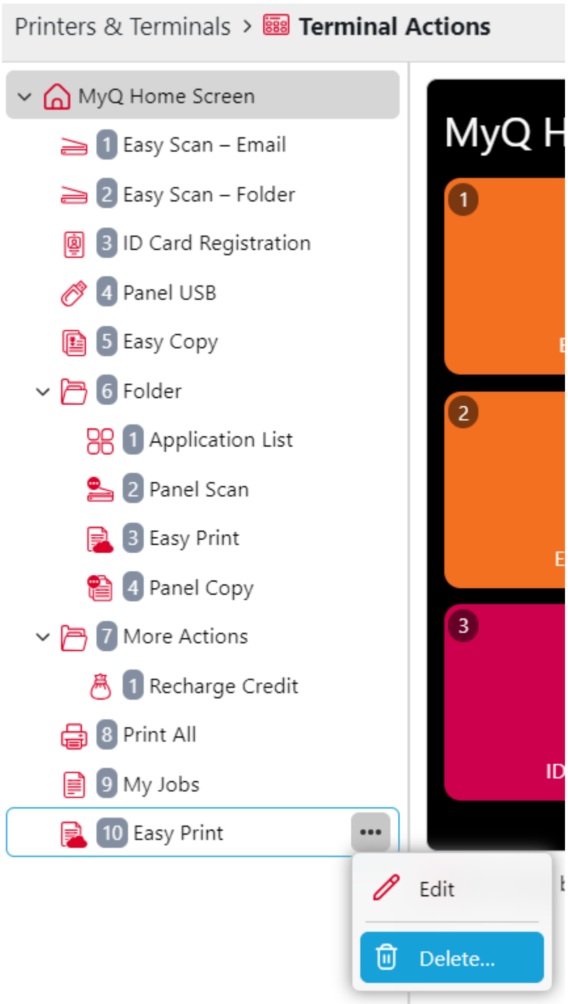
Deleting terminal action nodes

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.



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.

Vendor Compatibility Specifics

Terminal actions compatibility may be different between brands. Check the respective Embedded Terminal guides for details:

- MyQ Canon Embedded (10.1)
- MyQ Epson Embedded
- MyQ Fujifilm Embedded
- MyQ HP Embedded
- MyQ KATUN Embedded
- MyQ Kyocera Embedded
- MyQ Kyocera Embedded Lite (8.1)
- MyQ Lexmark Embedded (10.1)
- MyQ Ricoh SmartSDK Embedded (10.1)
- MyQ Sharp Embedded

- MyQ Sharp Luna Embedded (10.1)
- MyQ Toshiba Embedded (8.2)
- MyQ Xerox Embedded

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**.

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.

- The **General** tab settings are described in Editing terminal action nodes.
- The **Destinations** tab settings are described in Easy Scan destinations.
- The **Parameters** tab settings are described in Easy Scan parameters.

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.

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**. The Destination panel opens where you can set the target destination.

Depending on the selected destination type, the panel contains the **General**, **Parameters** and **Advanced** sections.

> Information for end users on completing connections to their personalized Easy Scan destinations is available here.

General section

- **Type** - Select the destination type from the drop-down. Available options: *Cloud storage, Custom destination, Email, FTP, Fax Server, Folder, Secured link, User's email, User's storage.*
- **Filename Template** - Here you can create the template of the scanned file name. The text of the template can be combined with MyQ parameters to provide additional information about the scanned file. The following parameters are available: %alternateEmails%, %assetNo%, %counter%,

%date%, %fullname%, %ipaddress%, %location%, %originalSubject%, %printerContact%, %printerName%, %scanId%, %serialNumber%, %time%, %timestamp%, %userCustom1%, %userCustom2%, %userCustom3%, %userEmail%, %username%, %usernotes%

- **Title** - Add a title for the destination.
- **Attach metadata file** - If this option is selected, MyQ sends the scanned file with an XML file attachment, containing the scanned file's metadata.

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.

Parameter	Description
%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.
%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.

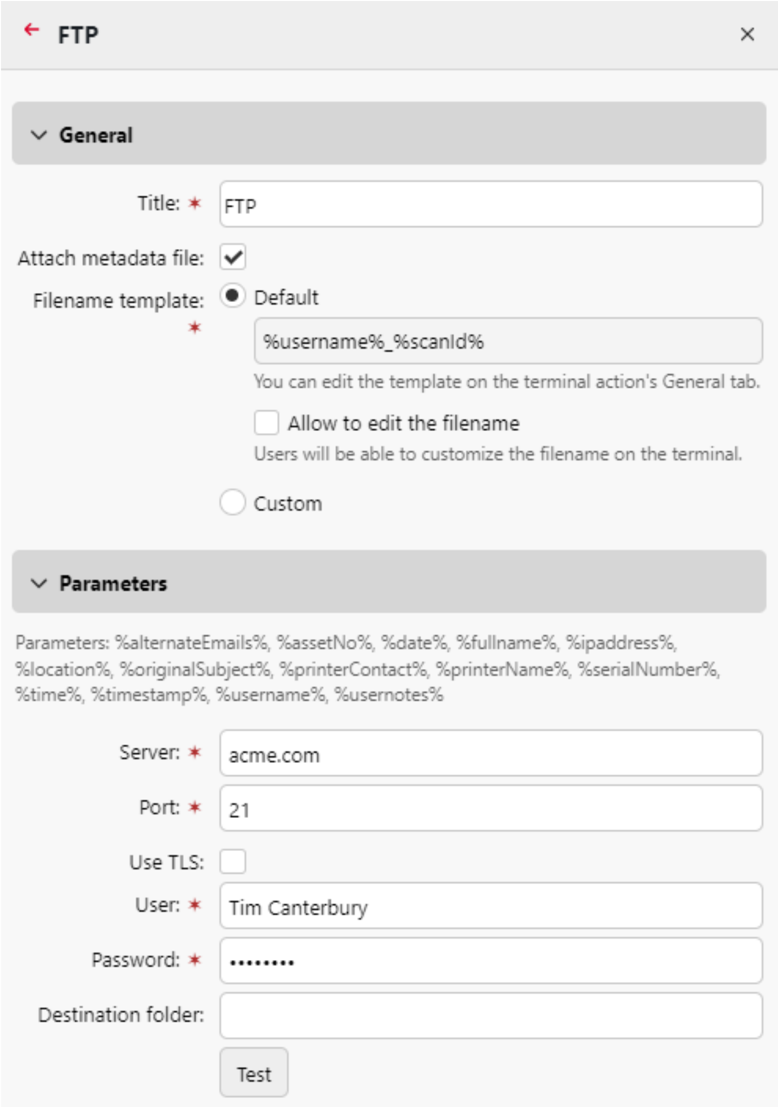
Parameter	Description
%printerContact%	This value is taken from the **Contact** field of the printing device's properties panel.

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.

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:

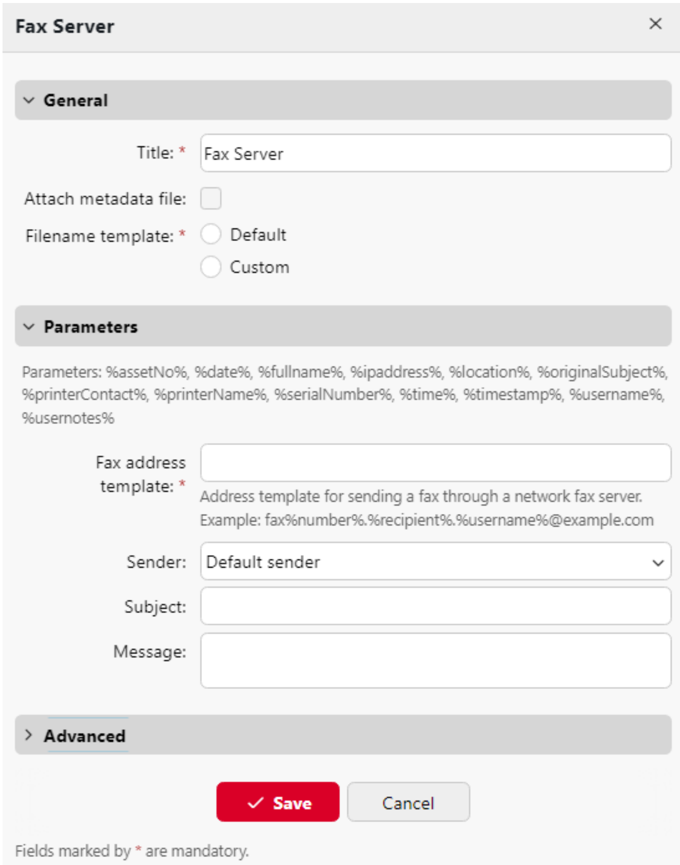
- *%username%*: User name of the user session owner
- *%fullname%*: Full name of the user session owner
- *%date%*: Date and time when the scan was taken
- *%originalSubject%*: The default subject set on the printing device

- *%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

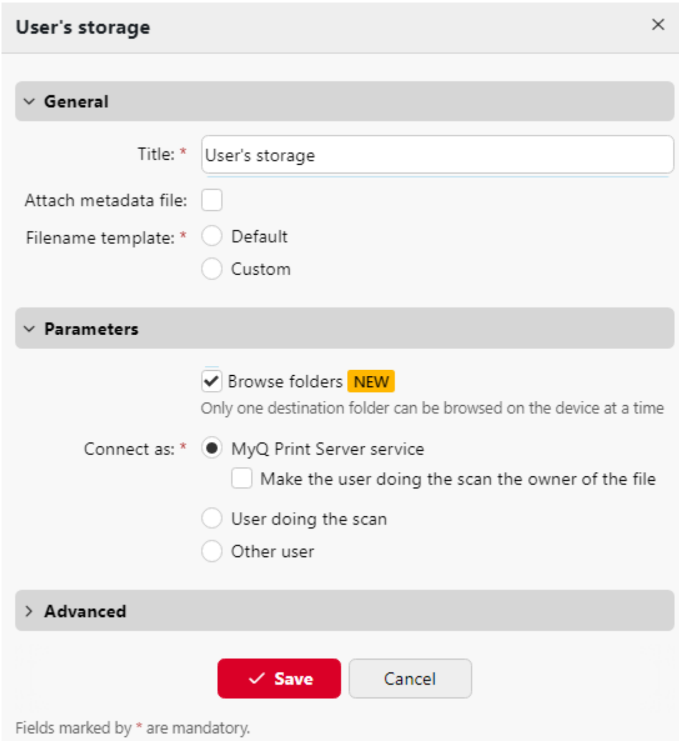
In the **Sender** drop-down, you can select one of the following addresses to be used as the fax sender:

- *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 **Folder for storing scanned documents** text box on the user properties panel.



Select the **Browse folders** option so users can browse one of their cloud destinations folder on the device.

The **Connect as** parameter determines in which way the scan will be stored in the folder:

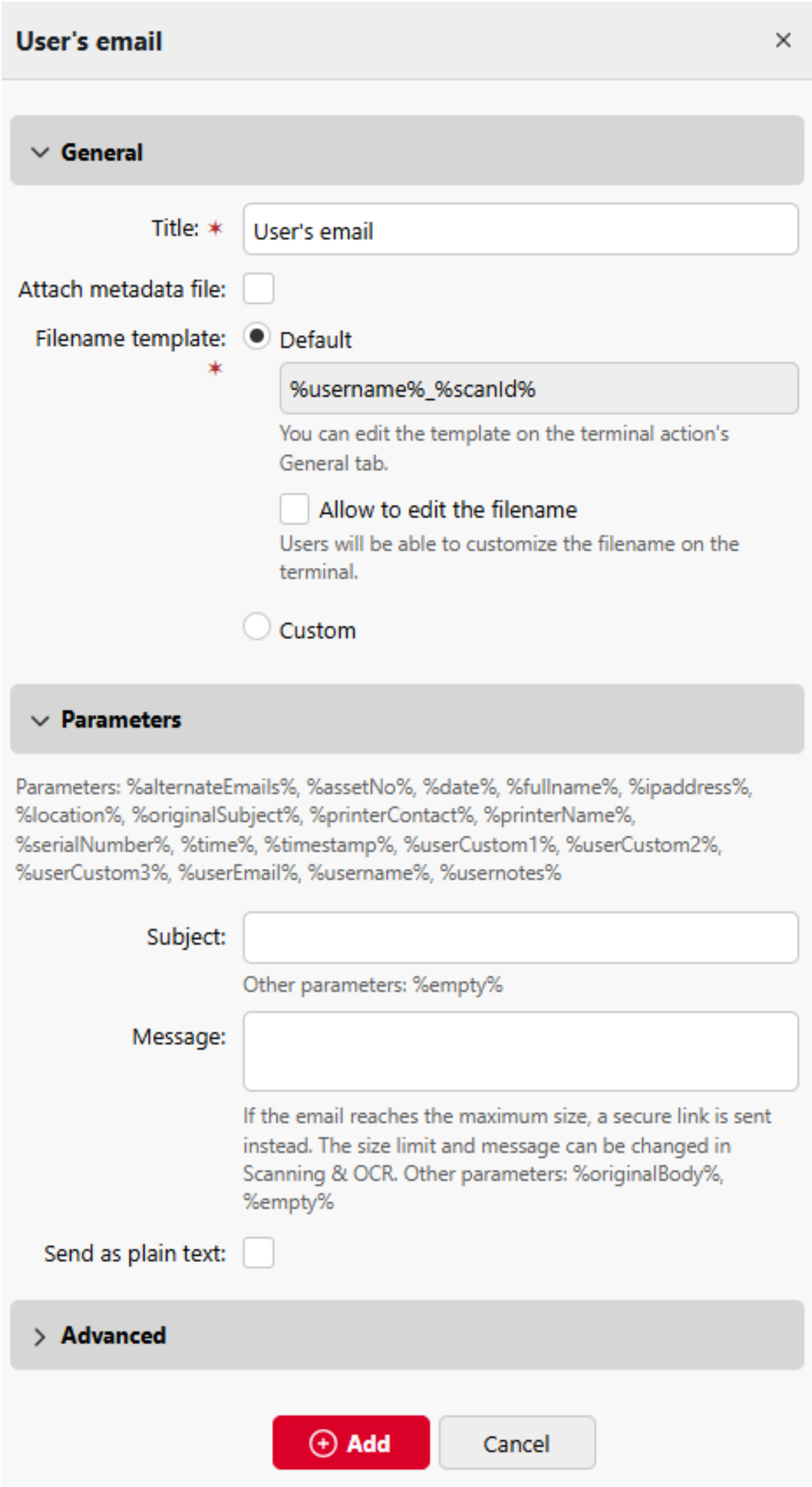
- If you select the **MyQ Print Server service** option, the rights for access to the destination folder have to be provided to the account under which the MyQ service runs. This account will also be set as the owner of the scanned file.
  - If you select the **Make the user doing the scan the owner of the file** option, the user doing the scan will be set as the owner of the scanned file.
- If you select the **User doing the scan** option, MyQ will expect the folder to be a shared folder on the domain account of the user doing the scan, and will use the entered password to access this folder. The user doing the scan will also be set as the owner of the scanned file. Users can then save passwords in the MyQ

Web User Interface used to access secured shared folders they have available, instead of providing them manually on the Embedded Terminal during each scan. When no password is saved at the time of scan, the user receives an email to connect the folder to have the scan delivered.
- If you select the **Other user** option, MyQ will expect the folder to be a shared folder on the domain account of the specified user and will use the entered username and password to access the folder. The user specified here will also be set as the owner of the scanned file.
    - If you select the **Make the user doing the scan the owner of the file** option, the user doing the scan will be set as the owner of the scanned file.

> 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.

Scan to User's Email

Scans are sent to the user's primary email address set in the **Email** text box on the user's properties panel (on the **Users** main tab of the MyQ Web Interface).



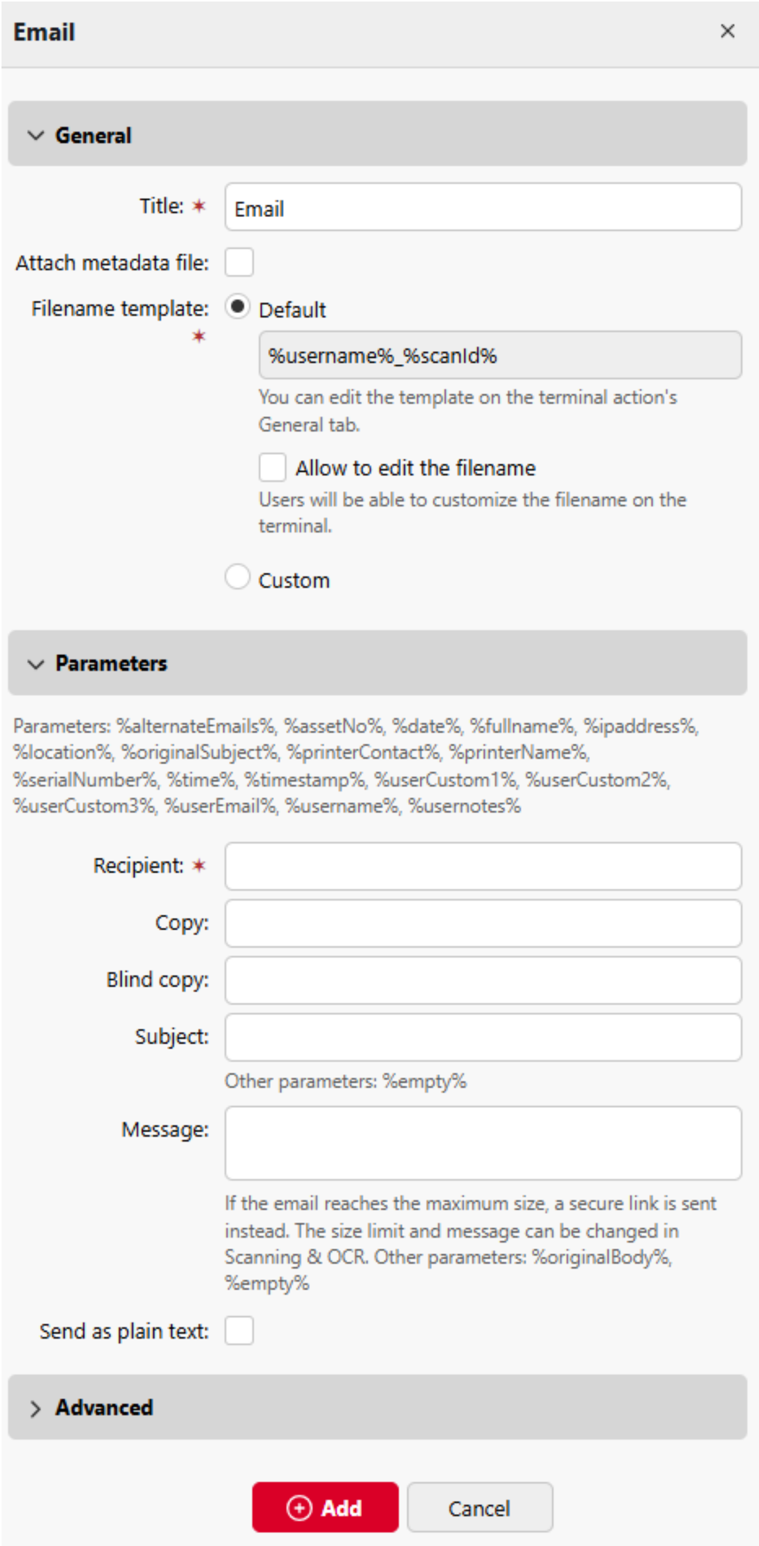
In the **Parameters** section, you can define the subject of the emails sent to this destination in the **Subject** text box, and the body of these emails in the **Message** text box. The subject or body can contain the following parameters: %alternateEmails%, %assetNo%, %date%, %fullname%, %ipaddress%, %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 the **Parameters** section, in the **Recipient** text box, 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.

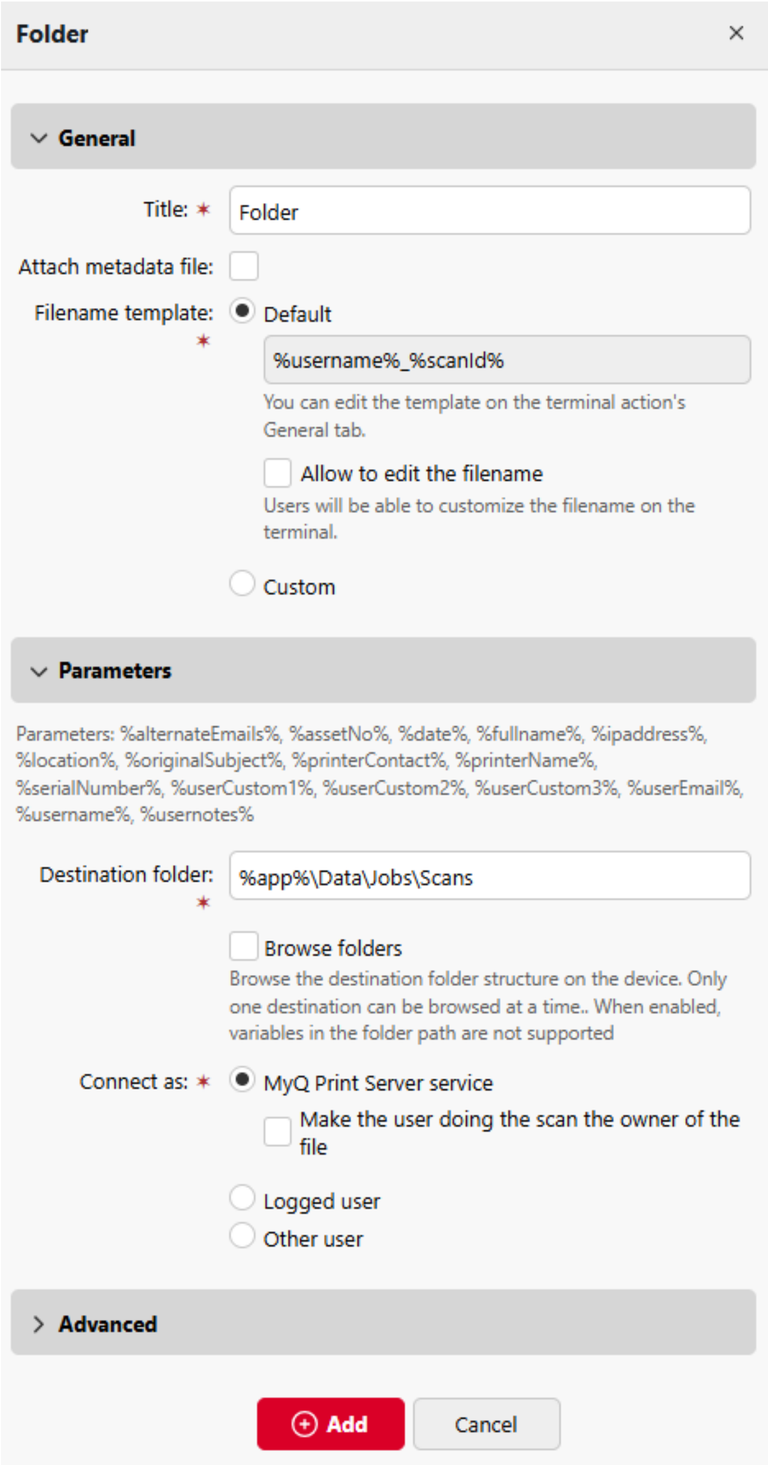
Emails with scans sent from MyQ contain graphics by default, enable the **Send as plain text** option to send these emails as plain text, which might be necessary, for example, if the email will be further processed by an automation service or fax servers.

> From MyQ server 10.0+ the *%empty%* parameter can be used in the **Subject** and **Message** text boxes. If used, the subject and/or the body of the email are left empty.

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%

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.

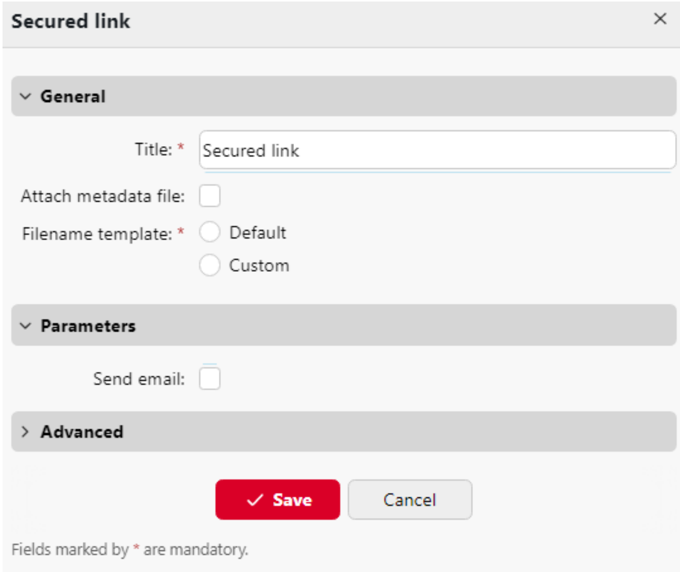
The **Connect as** parameter determines how the scan will be stored in the folder:

- **MyQ Print Server service**
  Access to the destination folder must be provided to the account under which the MyQ service runs. This account will also be set as the owner of the scanned file.
  - **Make the user doing the scan the owner of the file**
    When enabled, the user performing the scan is set as the owner of the scanned file.
- **Logged user**
  The shared folder is under the domain account of the user performing the scan. This user is also set as the owner of the scanned file. If the user has not paired their destination folder, or if their password has changed, the user receives an email with a link where they can enter their credentials to connect to the destination folder.
- **Other user**
  The shared folder is under the domain account of the another user than the logged in user. This other user is identified by entering their username and password. The other user is also set as the owner of the scanned file.
  - **Make the user doing the scan the owner of the file**
    When enabled, the user performing the scan is set as the owner of the scanned file.

MyQ cannot change the owner of scanned files that are stored under the **Users** folder or any of its 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.

Scan to Secured Link

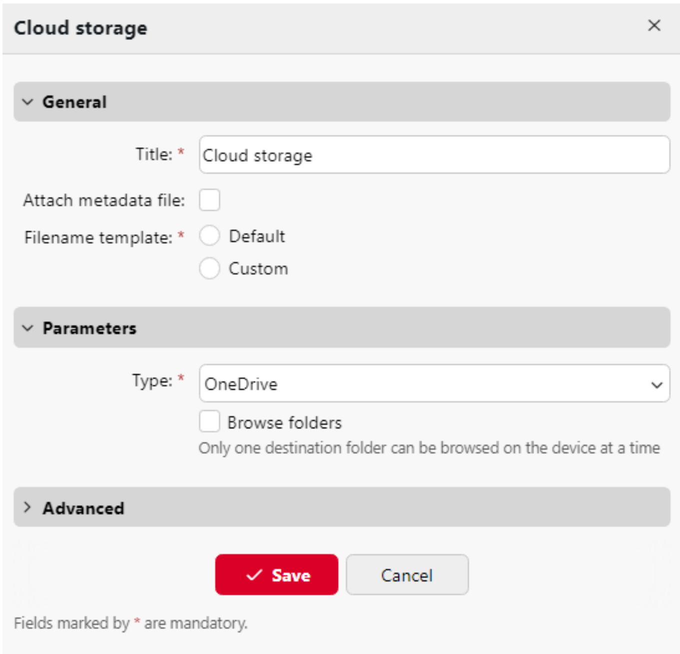
An email with a link to the scanned file is sent to the user's primary email address set in the **Email** text box on the user's properties panel (on the **Users** main tab of the MyQ Web Interface). Sending scans to this destination works in a similar way as sending them to the **User's Email** destination, with one important exception: instead of the scanned file, the email contains a secure link to the file, which is stored on the MyQ server, and can be downloaded via this link.



Scan to OneDrive

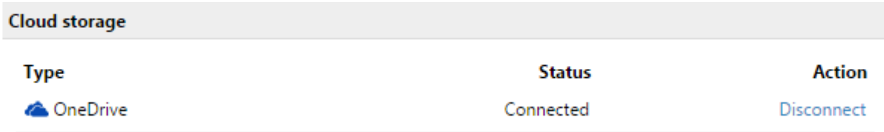
To enable scanning to OneDrive:

1. Select the **Cloud storage** option in the **Type** drop-down.
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**.



If the following two conditions are met, the cloud storage widget is displayed on the **Home** screen of the user logged on the MyQ Web Interface:

- There is at least one **Easy Scan** terminal action with this destination.
- The user has rights to see the **Easy Scan** button or is connected to cloud drive.



Cloud storage

Type	Status	Action
OneDrive	Connected	Disconnect

To be able to store the outgoing scan file on OneDrive, the user has to be connected.

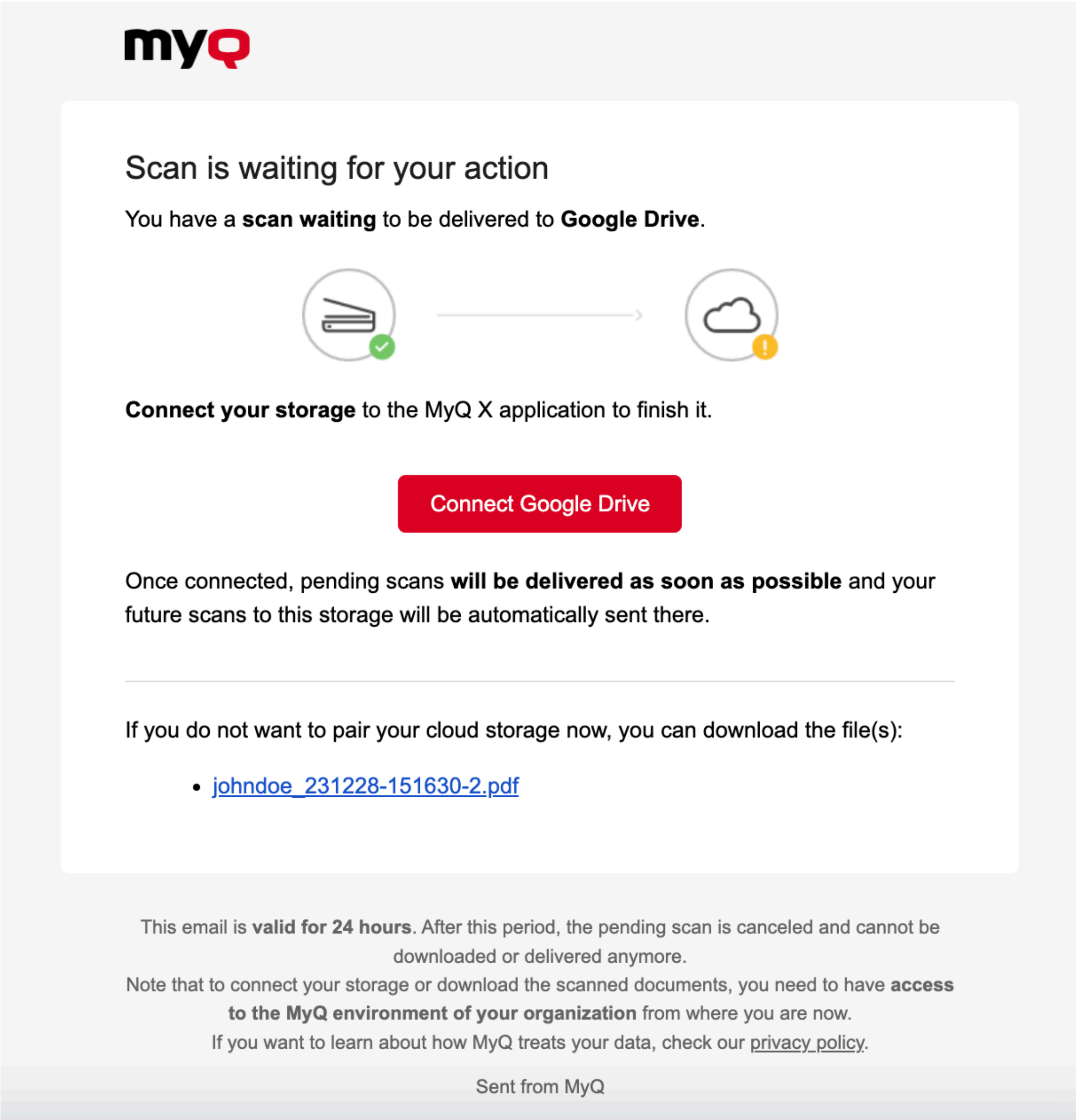
To connect to OneDrive, the user has to perform the following actions:

1. Log in to the MyQ Web User Interface with your user account.
2. On the **Cloud storage** widget, click **Connect**. The Cloud storage dialog box appears.
3. Sign-in to OneDrive and confirm permissions (when asked about the permissions, click **Allow**).
4. The OneDrive connection status changes to **Connected**.

Alternatively:

If an admin has connected OneDrive to **Easy Scan**, but an individual user has not yet connected their personal account, they can still use **Easy Scan** with OneDrive set as the destination.

An email will be sent to the users email address allowing them to connect to OneDrive, after which their scanned document/s will be delivered there. This email is valid for 24 hours after the scan has taken place. This email also contains a secure link to directly download the scanned document/s.



In a case where a user attempts to use **Easy Scan** to send a file to Onedrive, but they are not connected, **and** there is no email address associated with that user, the user will receive an on-screen prompt to connect their cloud storage via the web interface and try again.

Scan to OneDrive for Business

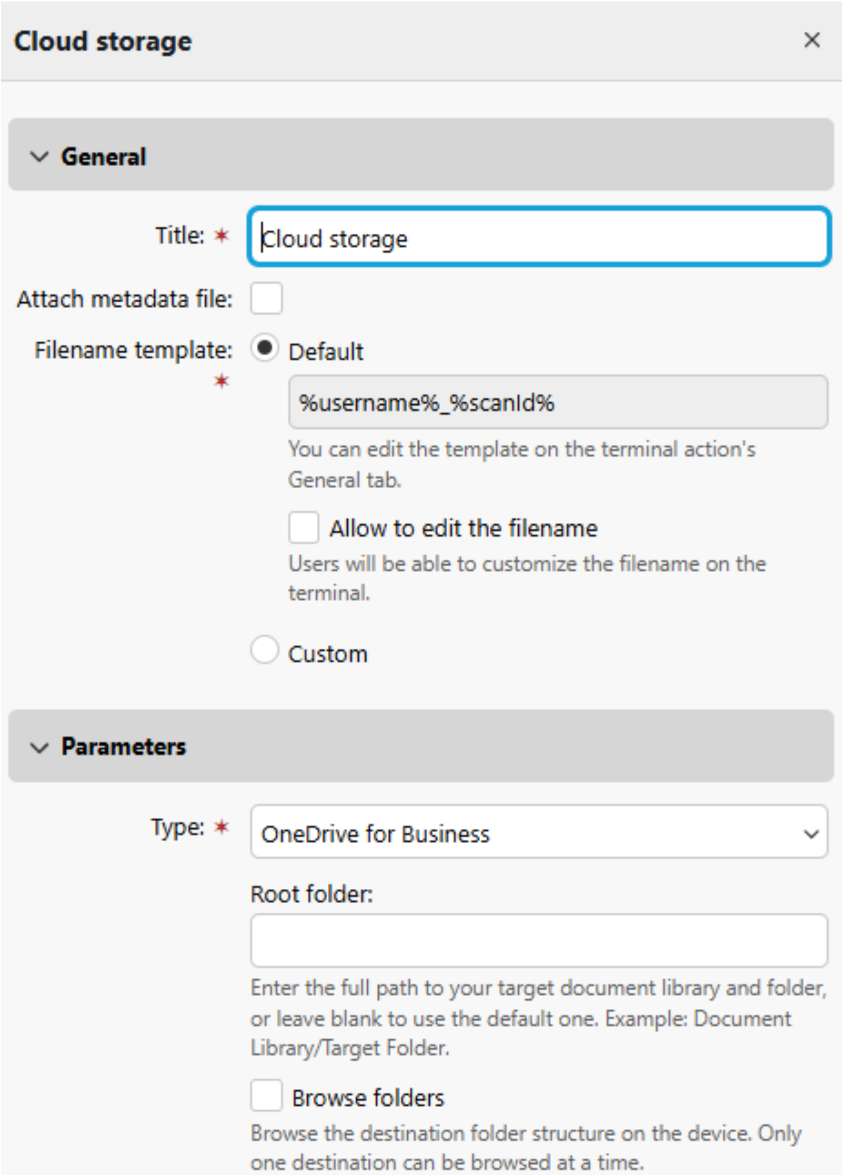
This article explains how to configure the Easy Scan terminal action to scan to OneDrive for Business.

Prerequisite

- A OneDrive for Business connection is configured. For more information, see OneDrive for Business Setup.

Configure Easy Scan with the destination OneDrive for Business

1. Go to **MyQ > Settings > Terminal Actions**.
2. Select **Easy Scan** and click **Edit**.
   If the action is not visible, to add it go to **Add Action > Scan > Easy Scan**.
3. On the **Destinations** tab, click **+Add** and select **Cloud Storage**.
4. Under **Parameters,** select **OneDrive for Business** as the **Type**.
5. (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.
6. (Optional) Enable **Browse folders** to let users browse the directories of the cloud destination folder on the device.
7. 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.

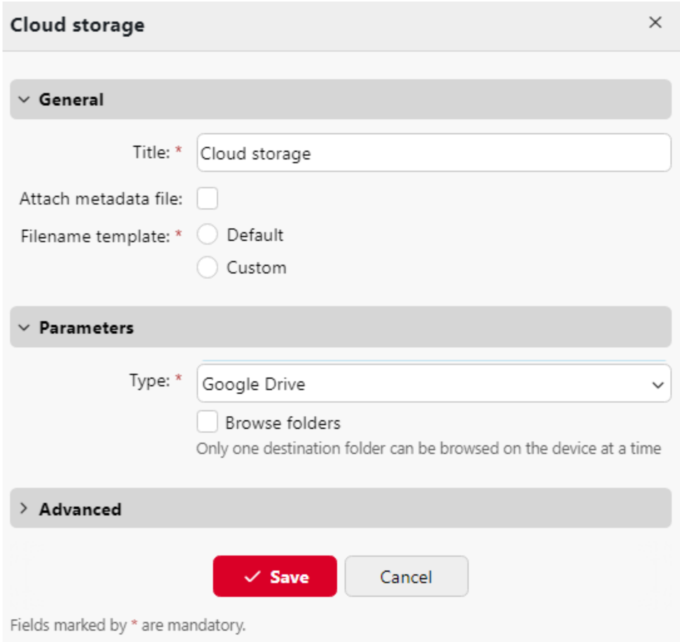
The user will be shown the same dialogue as when the connection was created. The user can repeat all the steps to create a new secret for the existing OneDrive Business connection. Or they can perform step 3 - Administrator's consent, if it was not completed when the connection was created for any reason, 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

To enable scanning to Google Drive:

1. Select the *Cloud Storage* option in the **Type** drop-down.
2. Select the *Google Drive* 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.
3. Click **Save**.



If the following two conditions are met, the cloud storage widget is displayed on the **Home** screen of the user logged on the MyQ web interface:

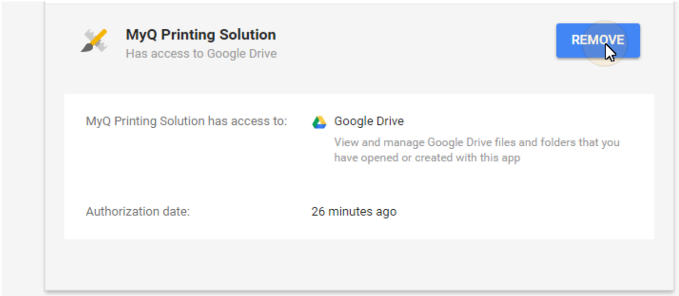
1. There is at least one **Easy Scan** terminal action with this destination.
2. The user has rights to see the **Easy Scan** button or is connected to Google drive.

To be able to store the outgoing scan file on Google Drive, the user has to be connected.

To connect to Google Drive, the user has to perform the following actions:

1. Log in to the MyQ Web user interface with your user account.
2. On the Cloud storage widget, click **Connect**. The Cloud storage dialog box appears.
3. Click **Continue with Google**.
4. Sign-in to Google Drive and confirm permissions. (When asked about the permissions, click **Allow**).
5. The Google Drive connection status changes to **Connected**.

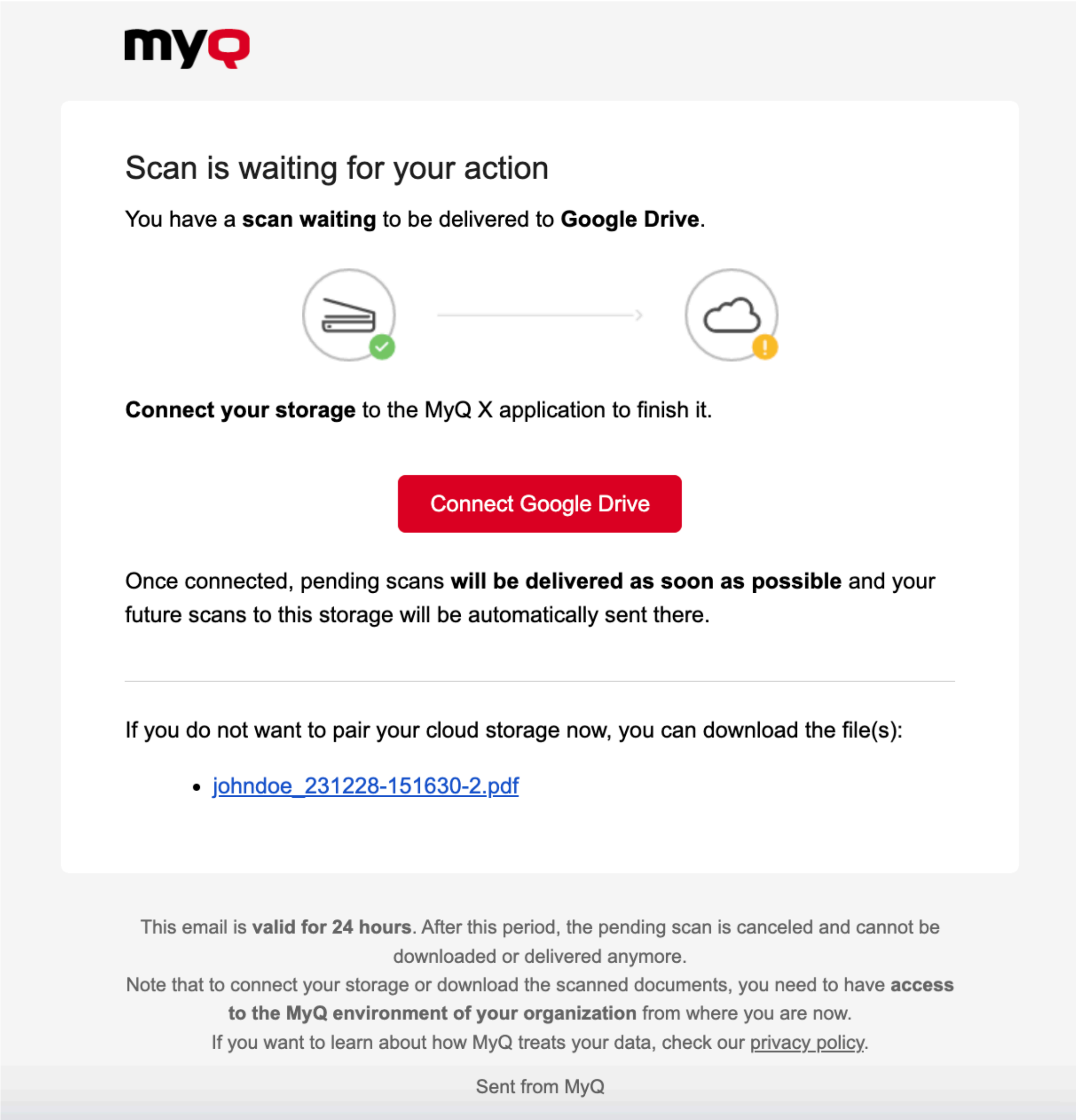
A single Google user account can be connected to only one server at a time. If the user wants to connect the account to another server, they need to remove **MyQ Printing Solution** from the connected applications. This can be done on the **Apps with access to your account tab** under **My Account/Sign in & security/Apps with account access/MANAGE APPS**.



Alternatively:

If an admin has connected Google Drive to **Easy Scan**, but an individual user has not yet connected their personal account, they can still use **Easy Scan** with Google Drive set as the destination.

An email will be sent to the users email address allowing them to connect to Google Drive, after which their scanned document/s will be delivered there. This email is valid for 24 hours after the scan has taken place. This email also contains a secure link to directly download the scanned document/s.

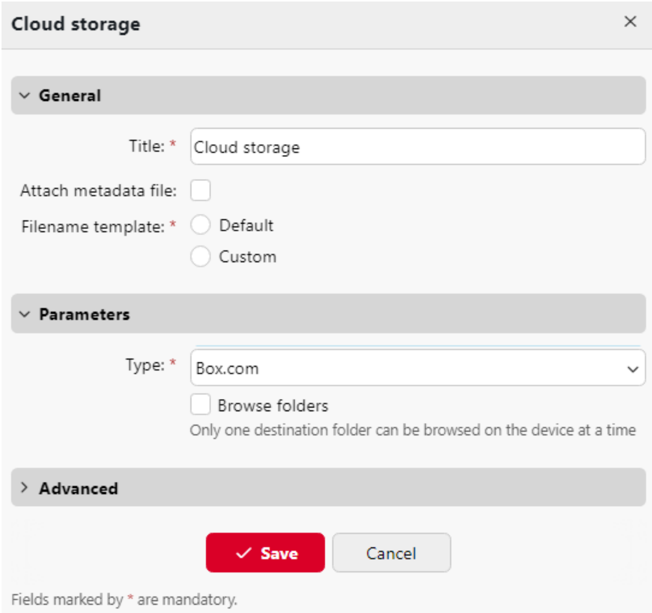


In a case where a user attempts to use **Easy Scan** to send a file to Google Drive, but they are not connected, **and** there is no email address associated with that user, the user will receive an on-screen prompt to connect their cloud storage via the web interface and try again.

Scan to Box

To enable scanning to your Box cloud storage account:

1. Select the *Cloud Storage* option in the **Type** drop-down.
2. 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.
3. Click **Save**.



If the following two conditions are met, the cloud storage widget is displayed on the **Home** screen of the user logged on the MyQ Web Interface:

1. There is at least one **Easy Scan** terminal action with this destination.
2. The user has rights to see the **Easy Scan** button or is connected to cloud drive.

To be able to store the outgoing scan file on Box, the user has to be connected.

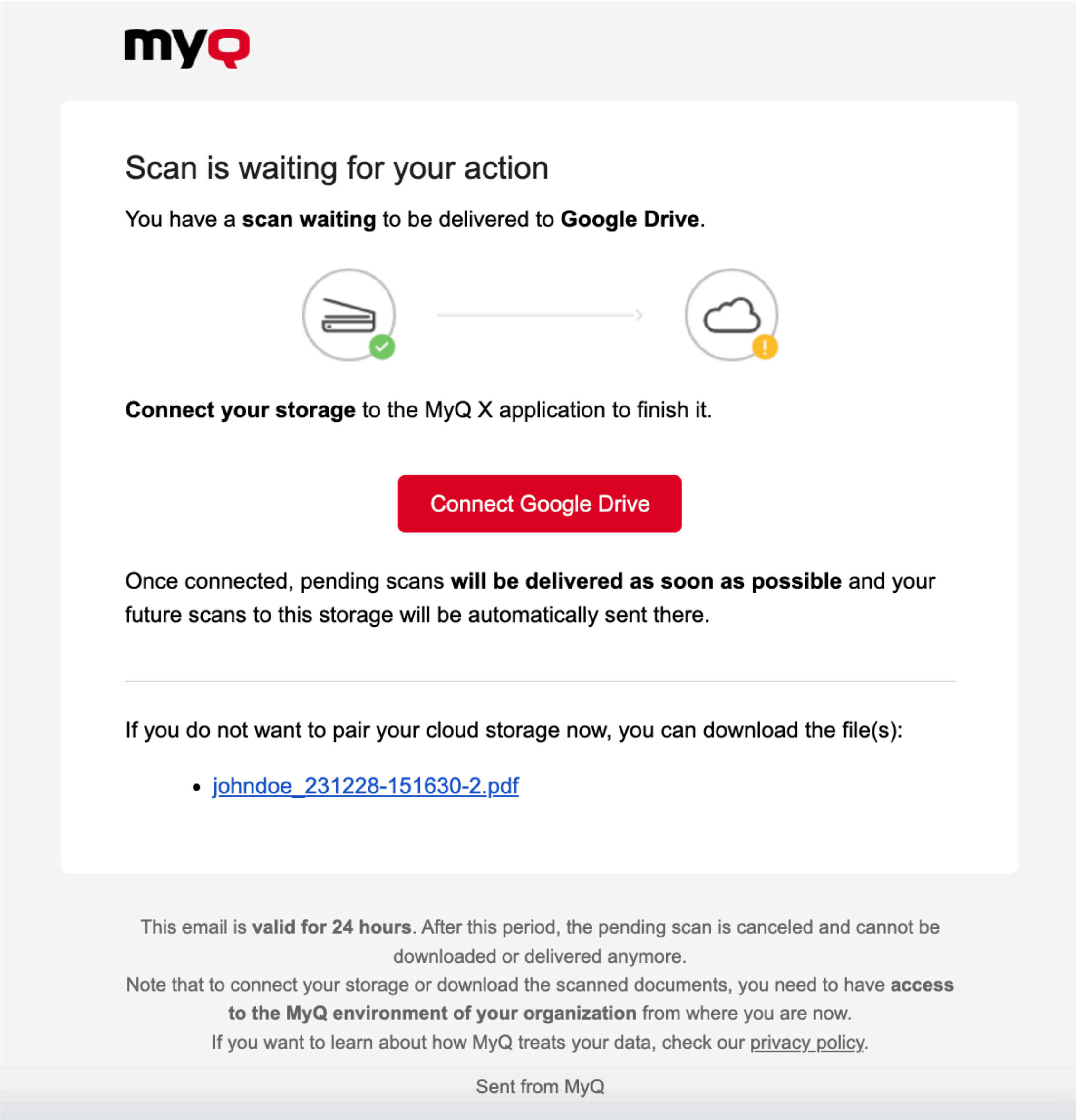
To connect to Box, the user has to perform the following actions:

1. Log in to the MyQ Web user interface with your user account.
2. On the Cloud storage widget, click **Connect**. The Cloud storage dialog box appears.
3. Sign-in to Box and confirm permissions (when asked about the permissions, click **Allow**).
4. The Box connection status changes to **Connected**.

Alternatively:

If an admin has connected Box to **Easy Scan**, but an individual user has not yet connected their personal account, they can still use **Easy Scan** with Box set as the destination.

An email will be sent to the users email address allowing them to connect to Box, after which their scanned document/s will be delivered there. This email is valid for 24 hours after the scan has taken place. This email also contains a secure link to directly download the scanned document/s.

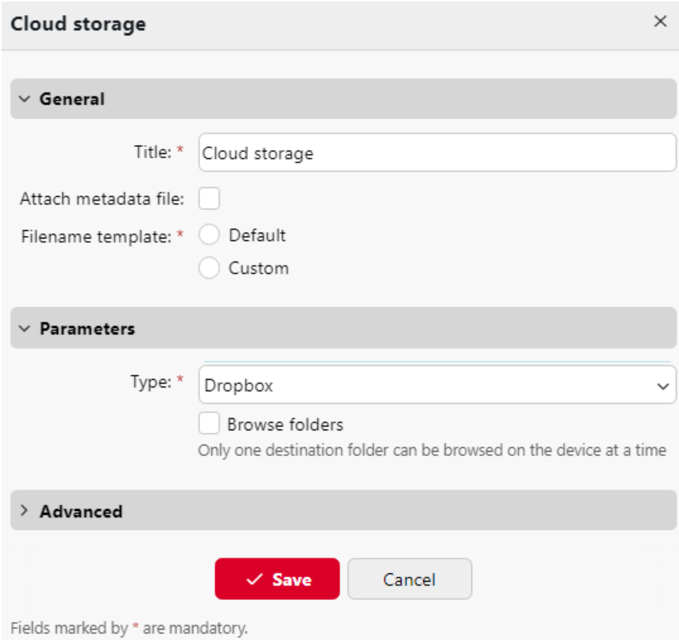


In a case where a user attempts to use **Easy Scan** to send a file to Box, but they are not connected, **and** there is no email address associated with that user, the user will receive an on-screen prompt to connect their cloud storage via the web interface and try again.

Scan to Dropbox

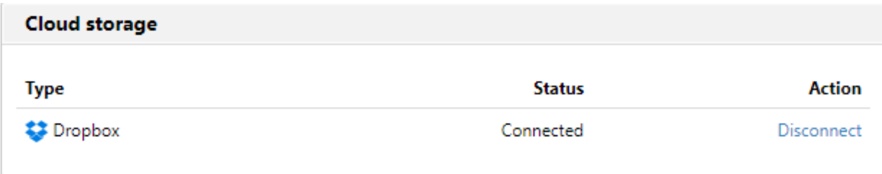
To enable scanning to Dropbox:

1. Select the *Cloud Storage* option in the **Type** drop-down.
2. 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.
3. Click **Save**.



If the following two conditions are met, the cloud storage widget is displayed on the **Home** screen of the user logged on the MyQ web interface:

1. There is at least one **Easy Scan** terminal action with this destination.
2. The user has rights to see the **Easy Scan** button or is connected to cloud drive.



To be able to store the outgoing scan file on Dropbox, the user has to be connected.

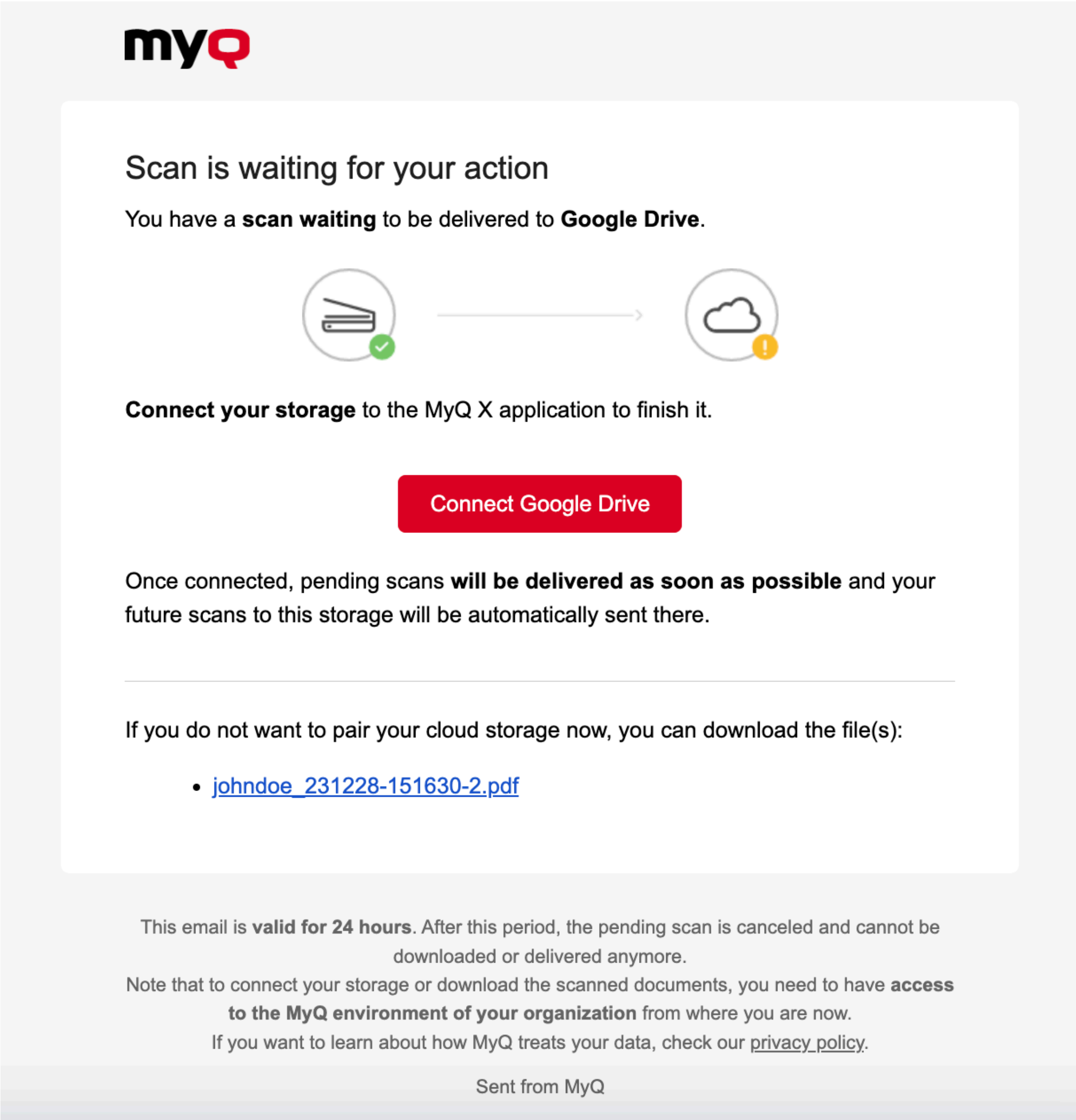
To connect to Dropbox, the user has to perform the following actions:

1. Log in to the MyQ Web User Interface with your user account.
2. On the **Cloud storage** widget, click **Connect**. The Cloud storage dialog box appears.
3. Sign-in to Dropbox and confirm permissions (when asked about the permissions, click **Allow**).
4. The Dropbox connection status changes to **Connected**.

Alternatively:

If an admin has connected Dropbox to **Easy Scan**, but an individual user has not yet connected their personal account, they can still use **Easy Scan** with Dropbox set as the destination.

An email will be sent to the users email address allowing them to connect to Dropbox, after which their scanned document/s will be delivered there. This email is valid for 24 hours after the scan has taken place. This email also contains a secure link to directly download the scanned document/s.



In a case where a user attempts to use **Easy Scan** to send a file to Dropbox, but they are not connected, **and** there is no email address associated with that user, the user will receive an on-screen prompt to connect their cloud storage via the web interface and try again.

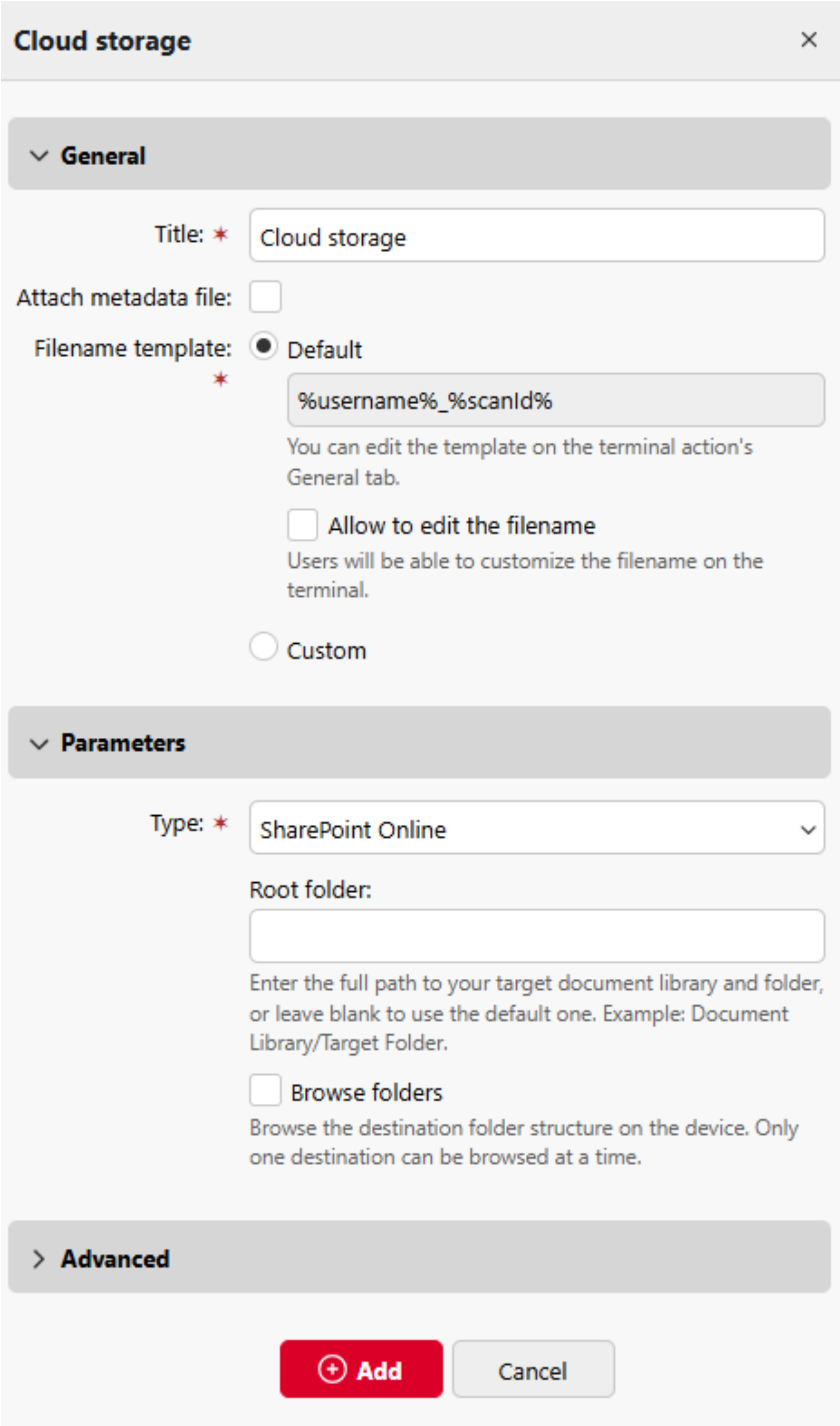
Scan to SharePoint Online

> The process for creating a connection to SharePoint Online is described here.

Create and set the SharePoint Online destination

- Create a new destination (edit or create an Easy Scan terminal action; on its properties panel, in the **Destinations** tab, click **+Add**).

- On the new destination's properties panel, under **General**, select the *Cloud Storage* option in the **Type** drop-down.
- In the **Parameters** section, in the **Type** drop-down, select *SharePoint Online*.
- Optionally, you can specify a **Root folder** to scan to and enable or disable folder browsing.



Connect a user's MyQ account to SharePoint Online

If the following two conditions are met, the cloud storage widget is displayed on the **Home** screen of the user logged on the MyQ Web Interface:

- There is at least one **Easy Scan** terminal action with this destination.
- The user has rights to see the **Easy Scan** button or is connected to cloud drive.

To be able to store the outgoing scan file on SharePoint Online, the user has to be connected.

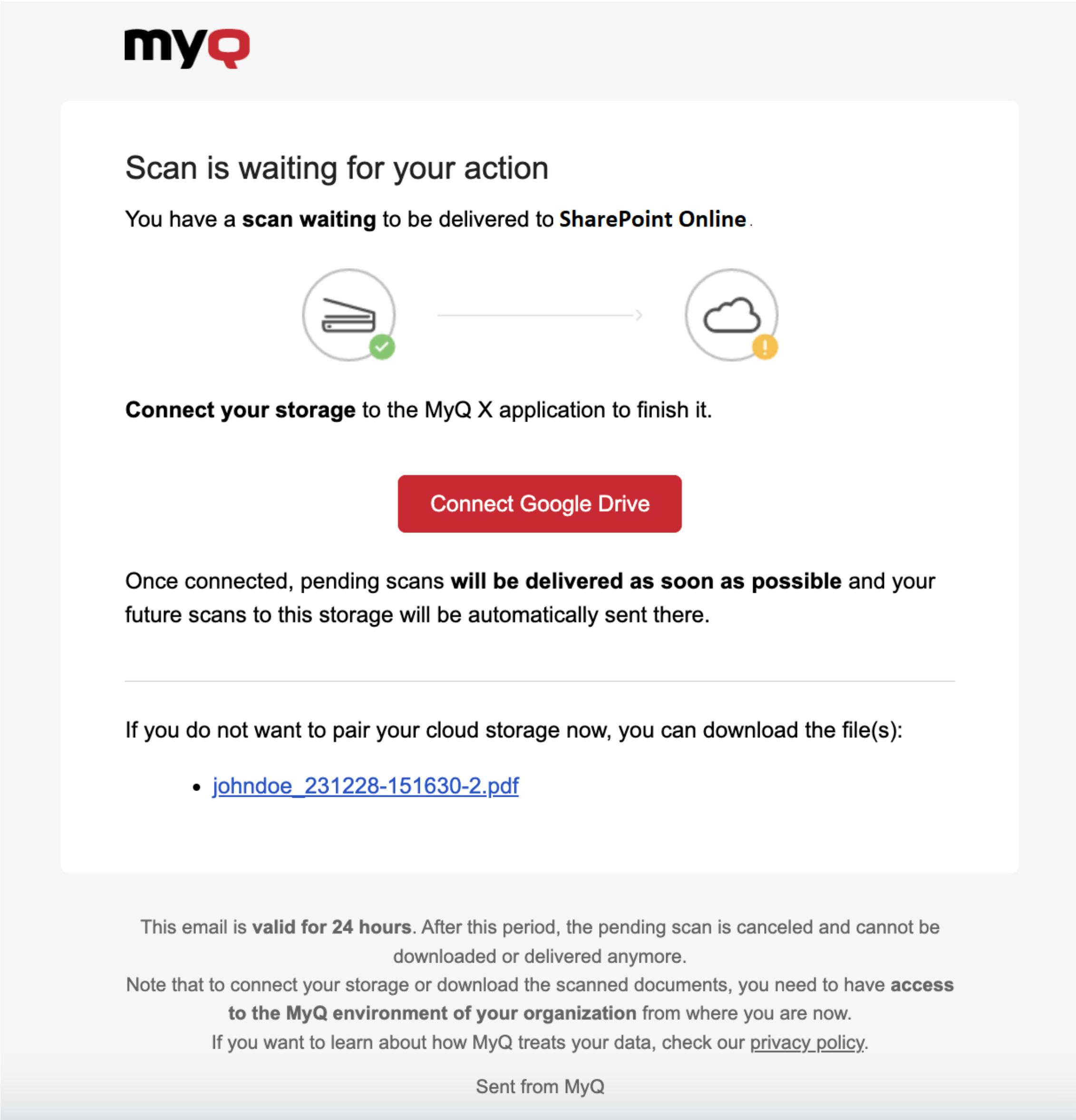
To connect to SharePoint Online, the user has to perform the following actions:

1. Log in to the MyQ Web User Interface with your user account.
2. On the **Cloud storage** widget, click **Connect**. The Cloud storage dialog box appears.
3. Sign-in to SharePoint Online and confirm permissions (when asked about the permissions, click **Allow**).
4. The SharePoint Online connection status changes to **Connected**.

Alternatively:

If an admin has connected SharePoint Online to **Easy Scan**, but an individual user has not yet connected their personal account, they can still use **Easy Scan** with SharePoint Online set as the destination.

An email will be sent to the users email address allowing them to connect to SharePoint Online, after which their scanned document/s will be delivered there. This email is valid for 24 hours after the scan has taken place. This email also contains a secure link to directly download the scanned document/s.



In a case where a user attempts to use **Easy Scan** to send a file to SharePoint Online, but they are not connected, **and** there is no email address associated with that user, the user will receive an on-screen prompt to connect their cloud storage via the web interface and try again.

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.

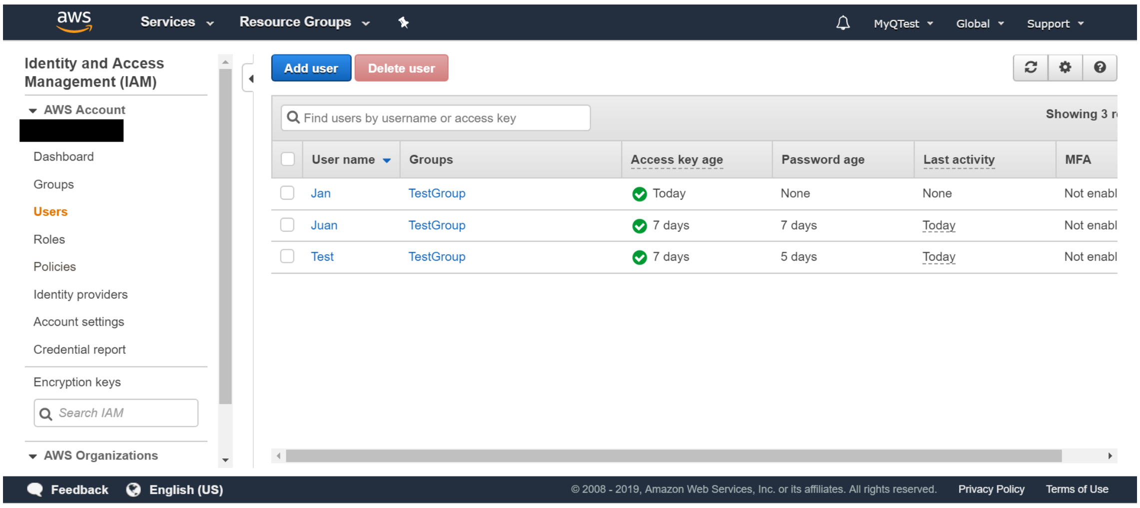
1. Login to https://console.aws.amazon.com/s3 and sign in with your Amazon account or create a new account. You need a credit card as proof of name. The credit card will also be used to charge the use of Amazon S3.
2. Use the https://docs.aws.amazon.com/AmazonS3/latest/gsg/s3-gsg.pdf to guide you through creating a S3 bucket.

> It is recommended to use a bucket lifecycle configuration, details of how to do so can be found here.

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.
3. Click **Users** in the **Identity and Access Management (IAM)** panel and click **Add user**.

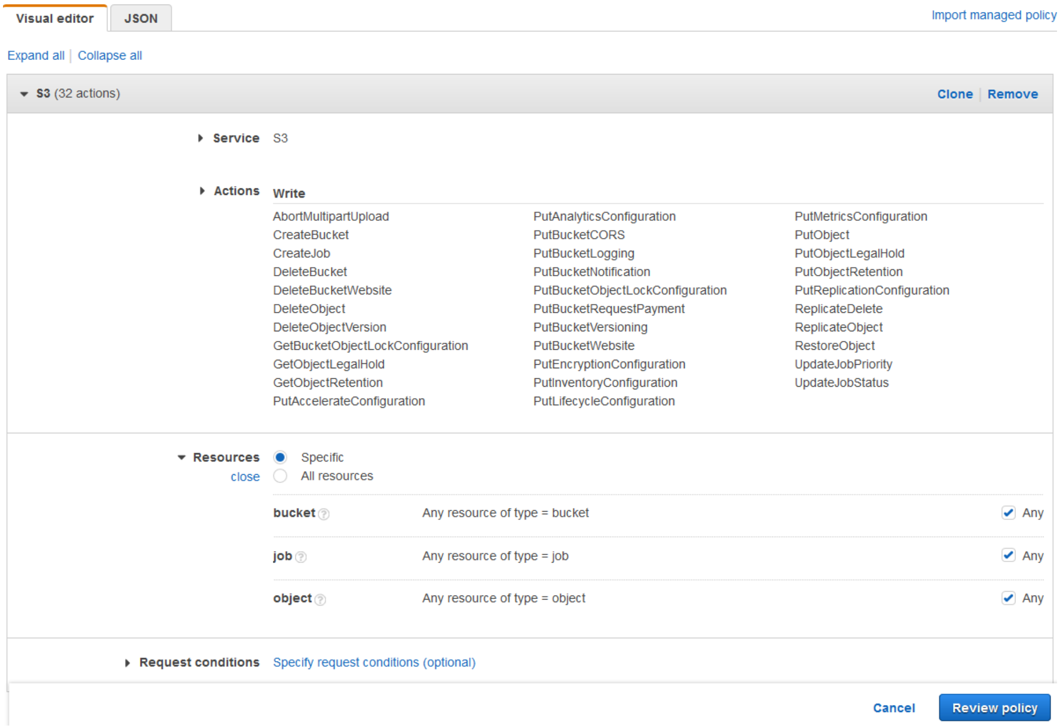


4. Follow the instructions to create the user.
5. Copy and save the **Client ID** and the **Access Key ID** of the created user, as you need them in the following steps.

Give user access rights to the bucket

To give bucket permission to the user, you can follow the official instructions, or follow the short procedure below:

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.



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.

Setup 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

- Create a new destination (edit or create an Easy Scan terminal action; on its properties panel, in the **Destinations** tab, click **+Add**).

- On the new destination's properties panel, under **General**, select the *Cloud Storage* option in the **Type** drop-down.
- 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**.
- 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.

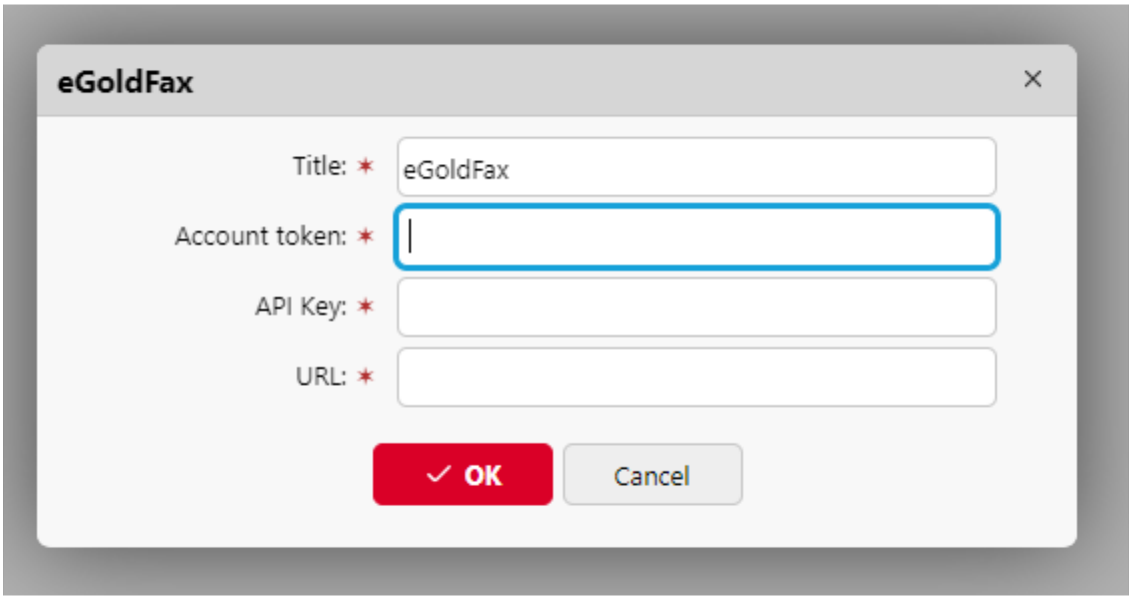
Scan to eGoldFax

To scan to eGoldFax you need to first set up a connection to your eGoldFax service.

> ⚠ Connecting to eGoldFax must be enabled as an extra feature in config.ini. The parameter is `eGoldFax`. We recommend consulting with MyQ support before editing the config.ini file.

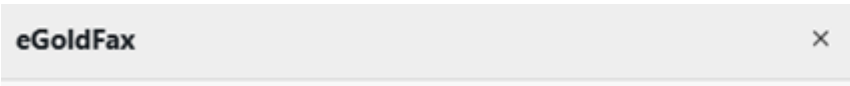
Setup a Connection Between MyQ and eGoldFax

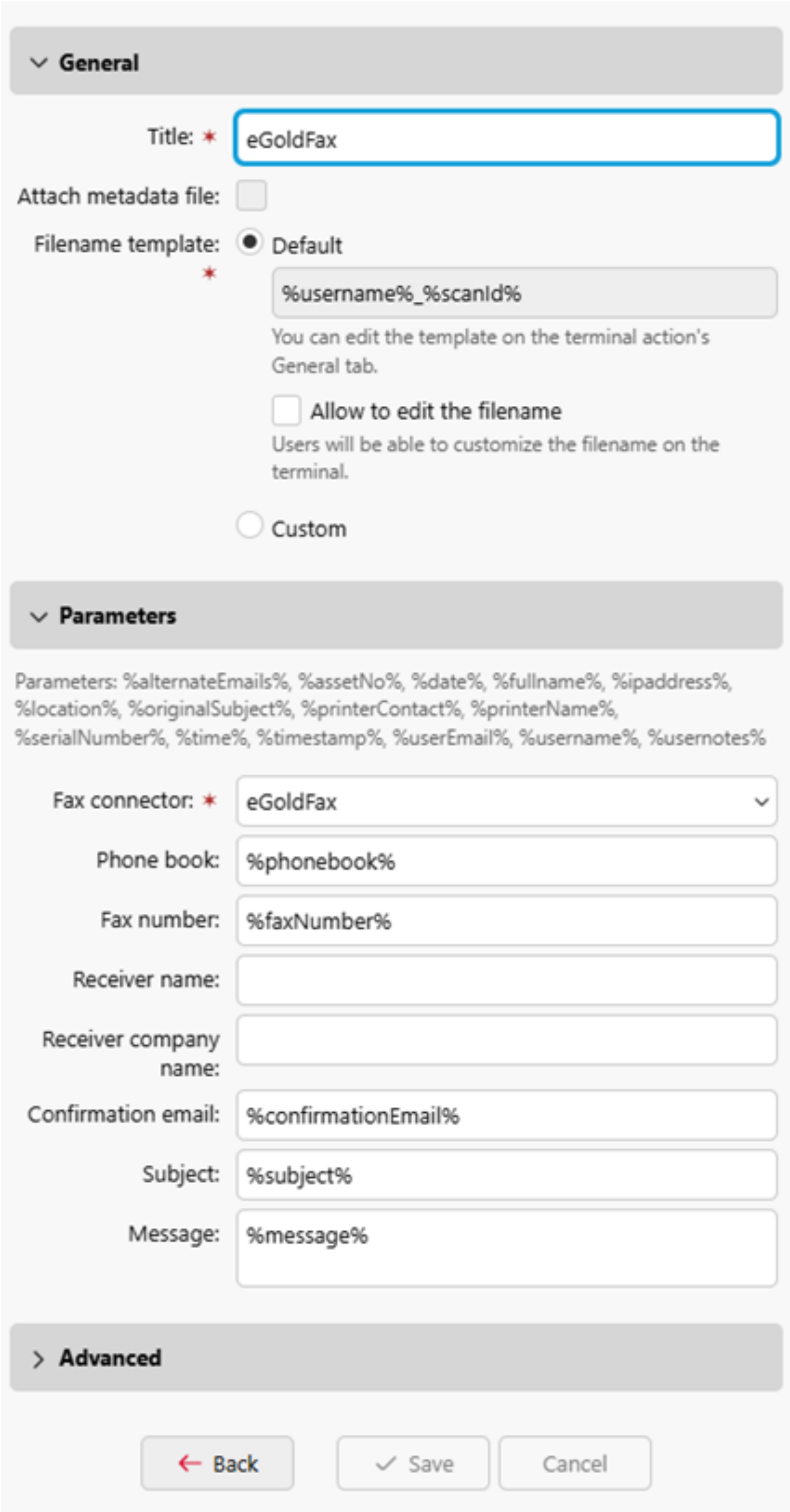
1. Open the **Connections** settings tab of the MyQ Web Interface (**MyQ, Settings, Connections**).
2. Click **+Add** and select **eGoldFax** from the menu.
3. Add a title identifying the connection, and your **Account token**, **API key,** and **URL** from eGoldFax.



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**).

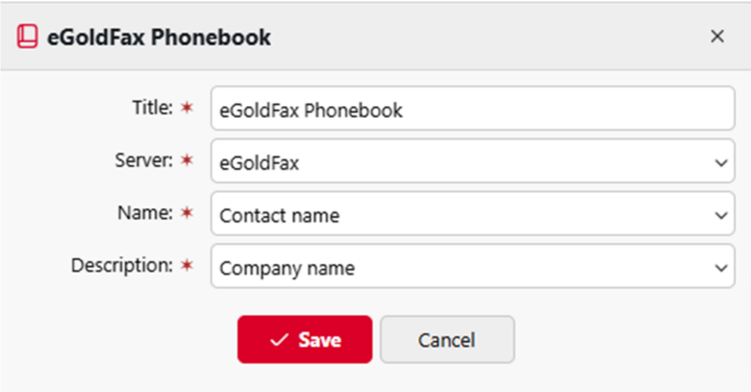




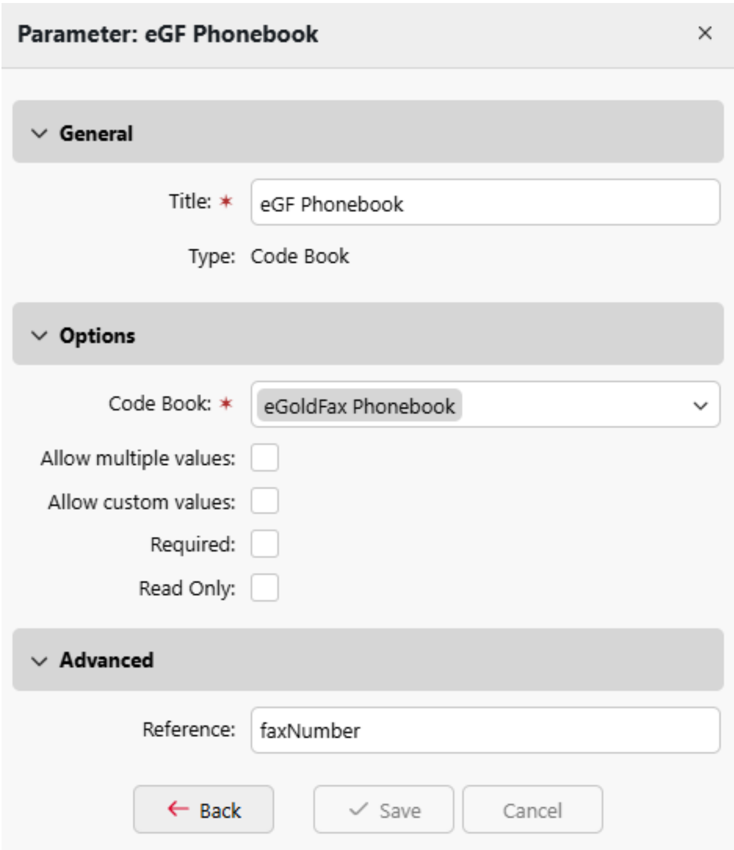
eGoldFax Code Book

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).

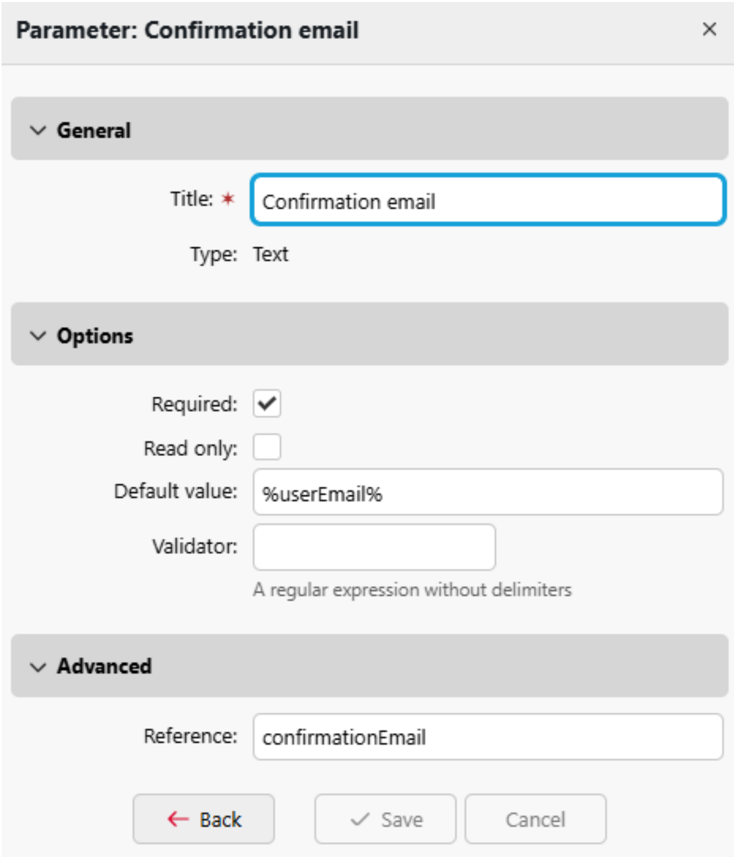
You can set the **Name** display to **Contact name** or **Contact name (Company name)** and the **Description** to **Company name** or **Fax number**, this will be visible on the Embedded Terminal when scanning to a contact from the Code Book.



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.

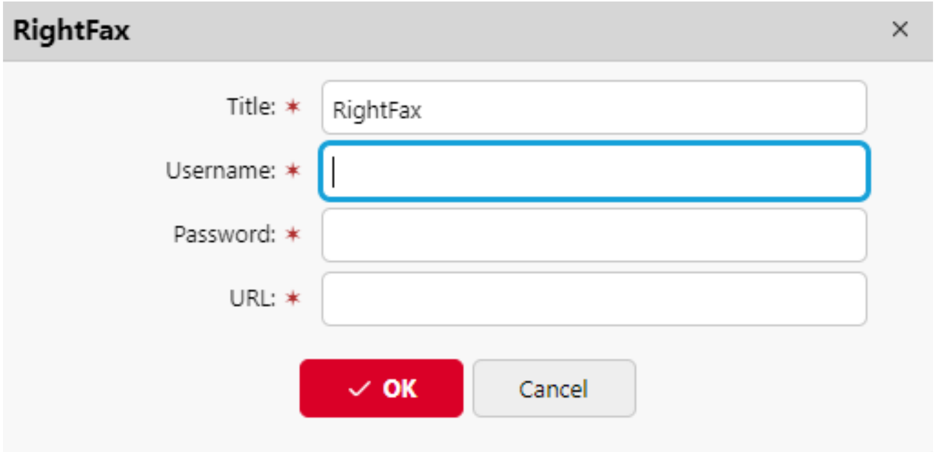


Scan to RightFax

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

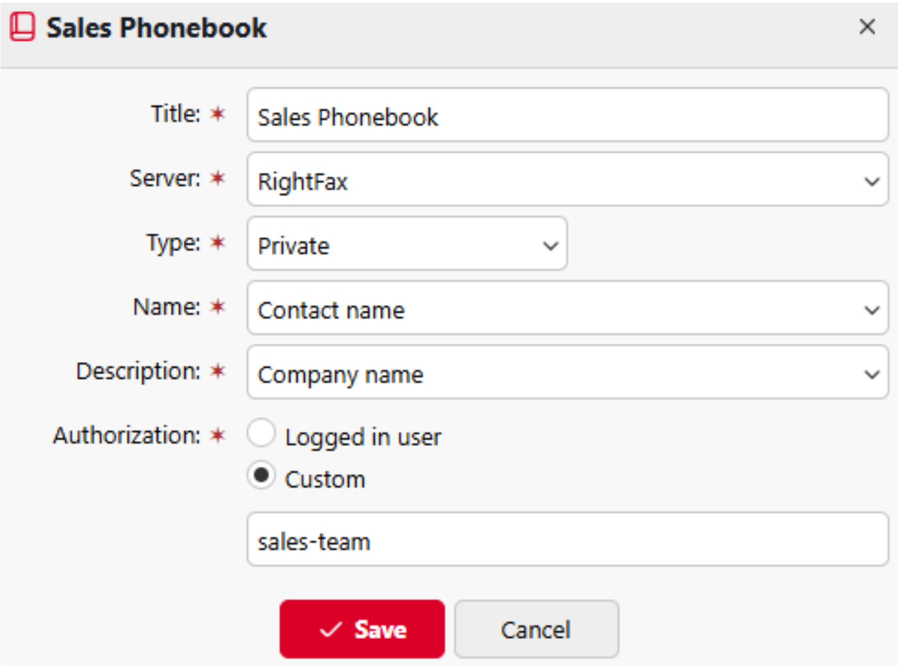
Only Title, Server, and Authorization are used for phonebook groups.

- **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.



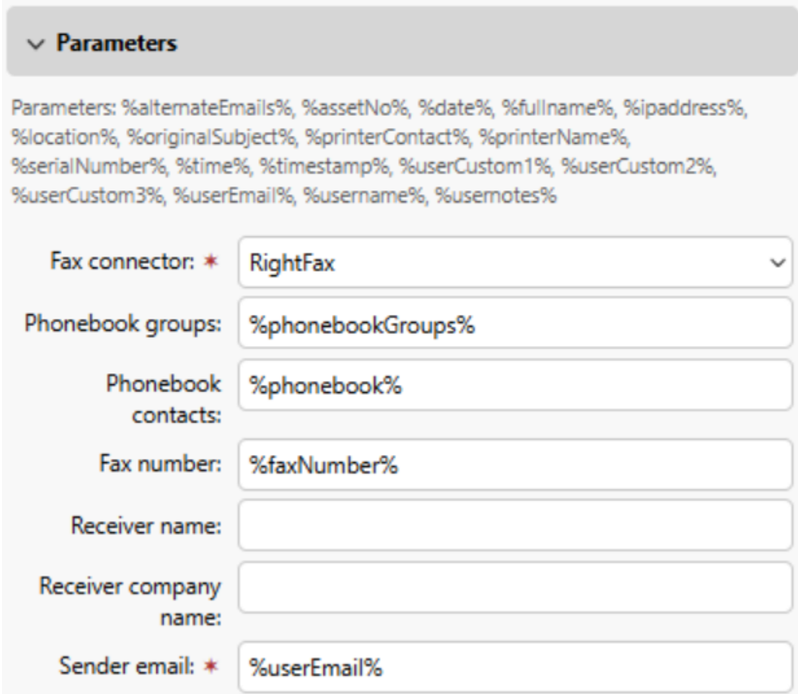
Set RightFax as an Easy Scan Destination

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:**

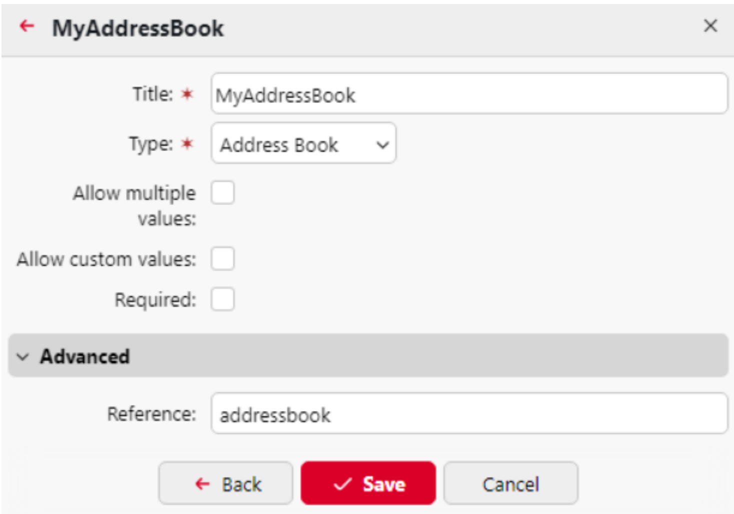
  - **Receiver name** and **Receiver company name** are not assigned by default. If you map values to these parameters, they appear on the fax under **To:** and **Company:**.

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.

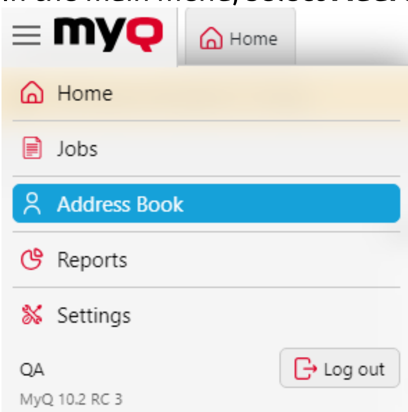


If the Address Book is the only destination for the Easy Scan action, it is recommended to enable **Required**. Otherwise, the field would not be marked as mandatory with * (asterisk) on the Embedded Terminal.

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.

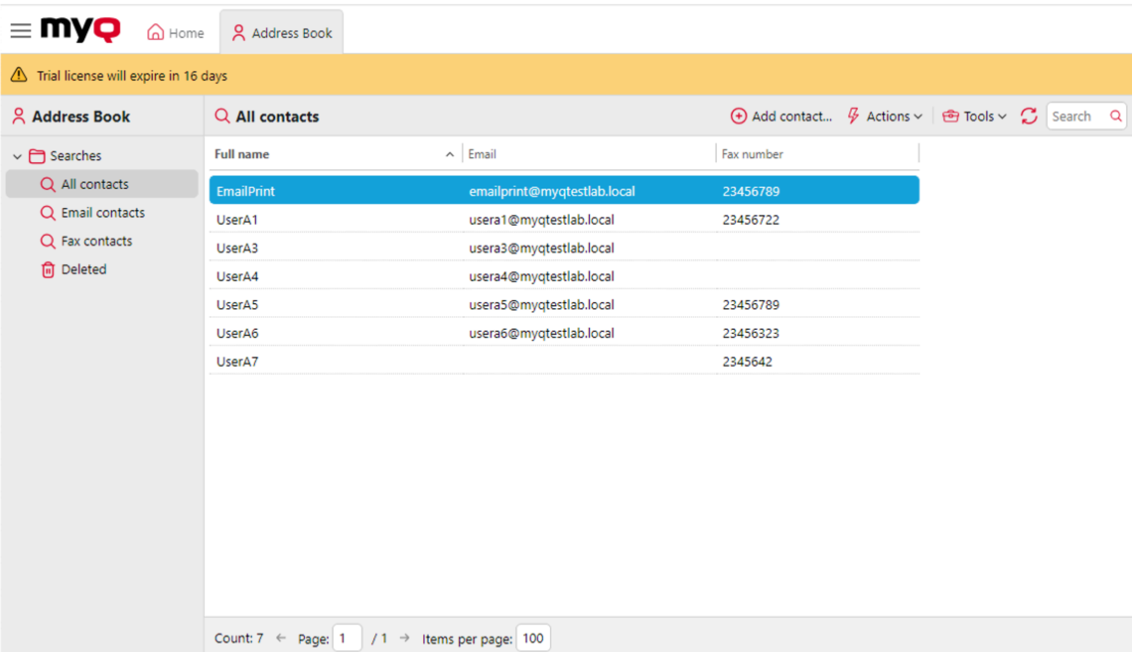
Accessing and Using Address Book

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.

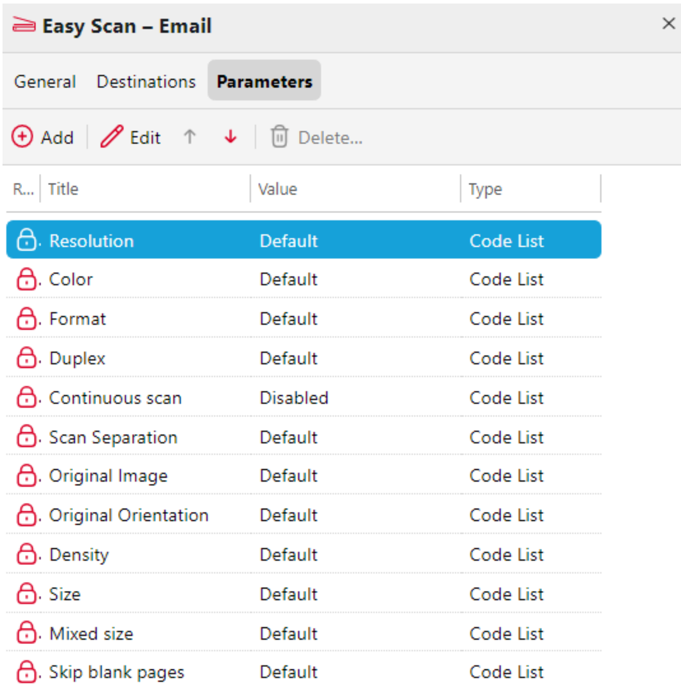
> A user can only access contacts from their own Address Book. Accessing the contacts of another user, even by administrators, is prohibited.

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.

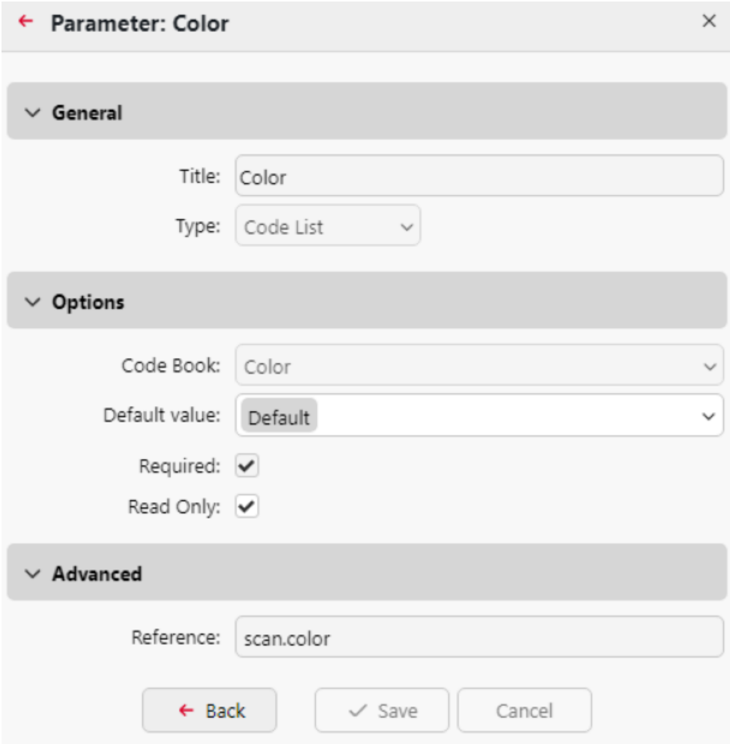
> All parameters are dependent on the particular printing device type. Therefore, some parameters and/or values might not be available.



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
- **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

Background Suppression is currently only supported on Xerox terminals.

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%*.

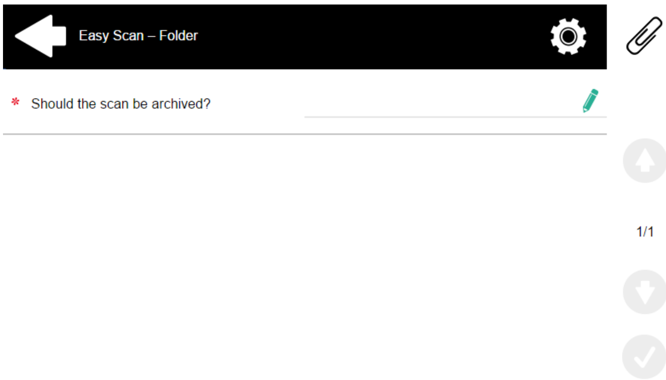
Custom Parameters Examples

These are some examples of using custom parameters.

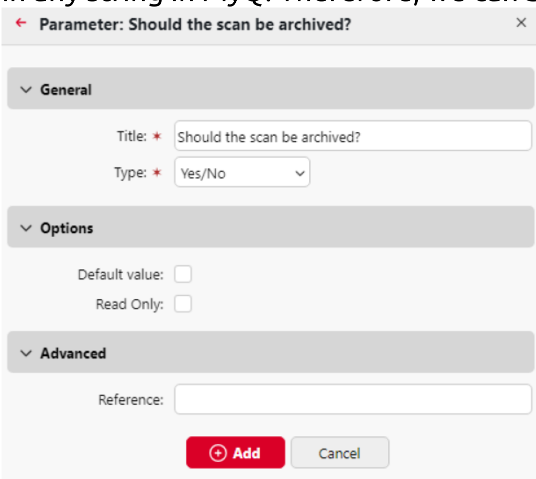
Providing additional information in a metadata file

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.

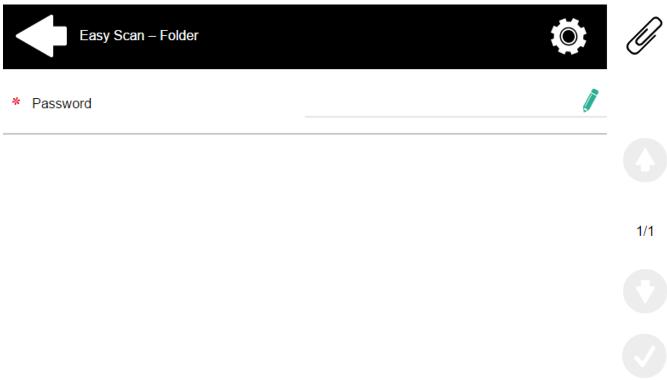


The following two figures show two possible values of the **Should the scan be archived?** parameter. A DMS software can automatically archive the scans with value *1* into a predefined folder.


```
- <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

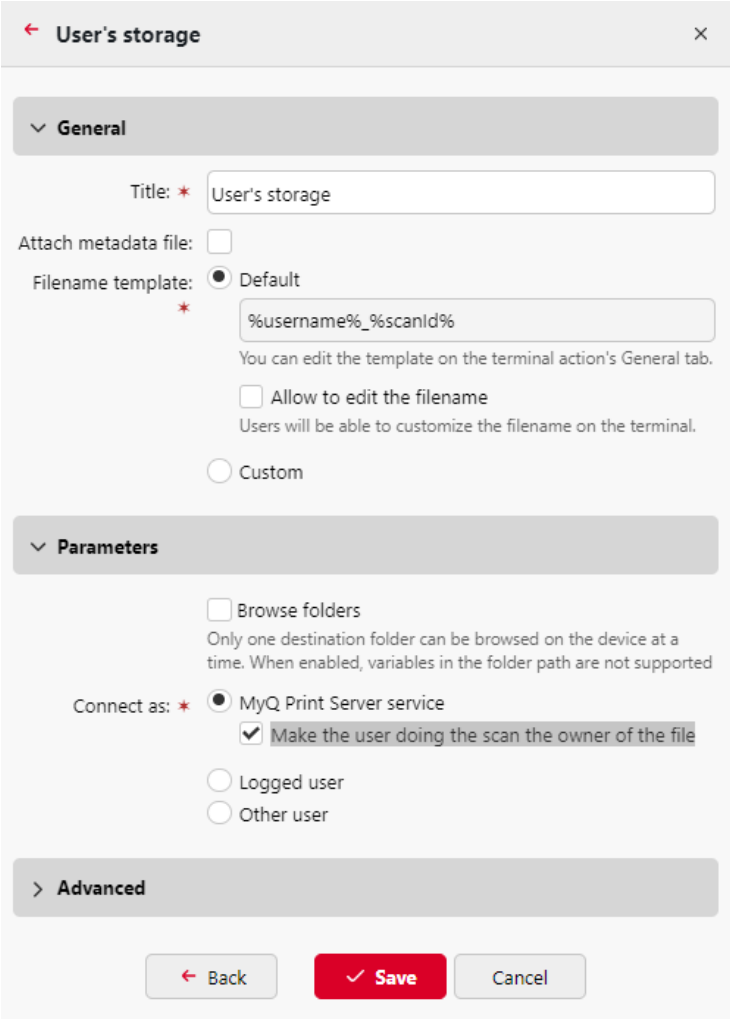
If you do not want to give to the MyQ server universal access to users' shared folders, but instead want to provide each user with separate rights to access their shared folder from MyQ, you can enable the scanning users to enter the password to their LDAP domain account to access the shared folder there.



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.*".

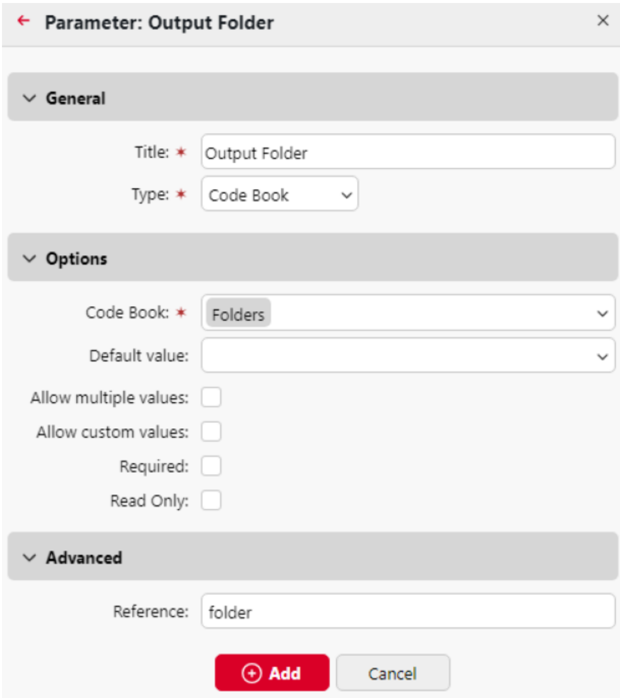
On the **Destinations** tab, set the **User's storage** destination type. In the **Parameters** section, select **Connect as: MyQ Print Server service** option and **Make the user doing the scan the owner of the file**.



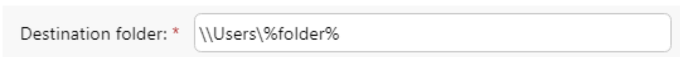
Enabling users to select the output folder from a code book

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.



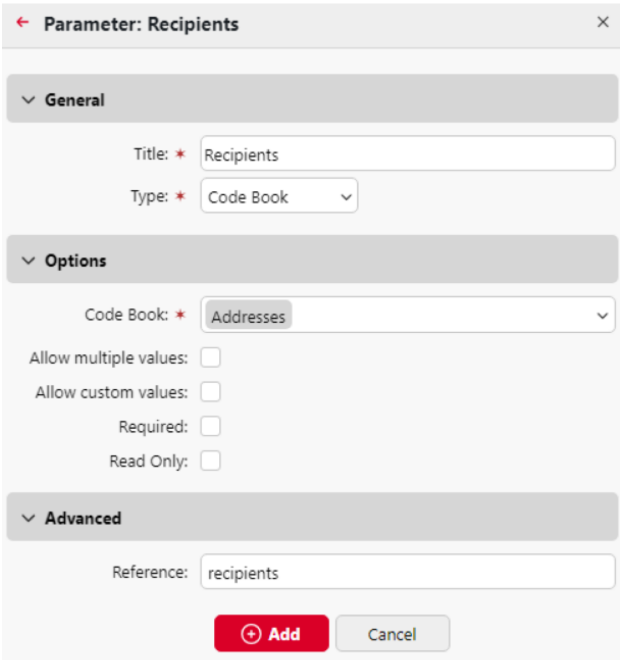
On the **Destinations** tab, create and set up a new destination. For this destination, you can use the parameter as any part of the destination path set in the **Destination folder** text box. To use the parameter, enter its reference name bounded in percentage signs as part of the path. In our example, we used a parameter with the reference name *folder* as the folder where the files are stored (*Users%folder%*).



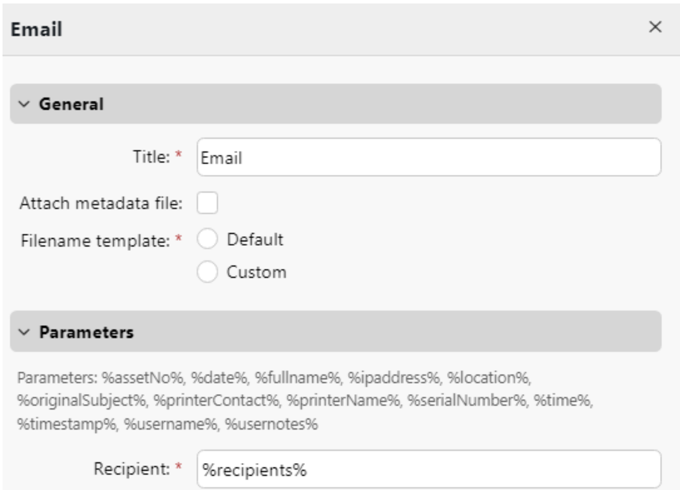
Enabling users to search recipients via LDAP Source code books

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 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.

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.

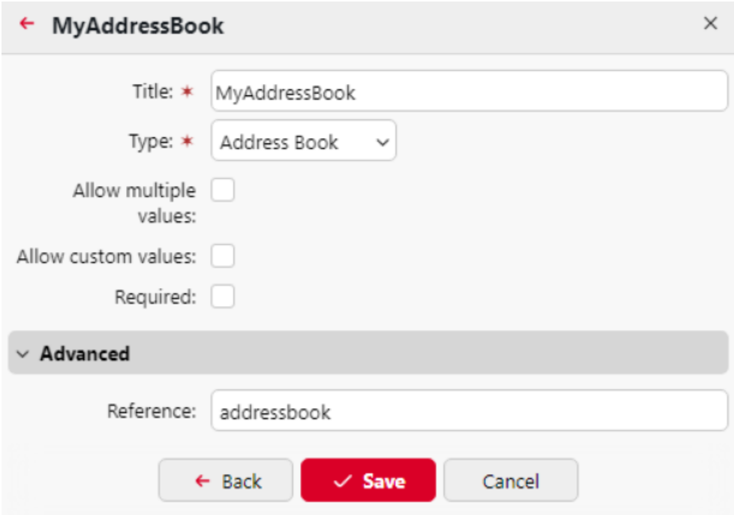
Easy Fax Parameters

- **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

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.

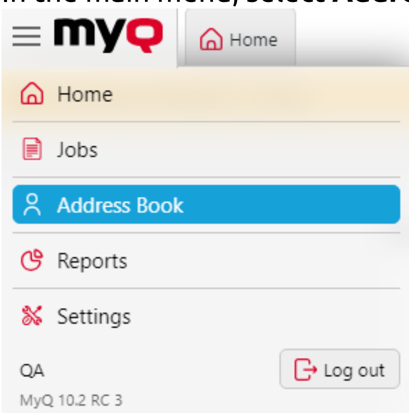


It is not necessary to enable the Required field, as the Fax destination field is already mandatory in the Easy Fax's Phone Book where the user will be selecting contacts from their Address Book.

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.

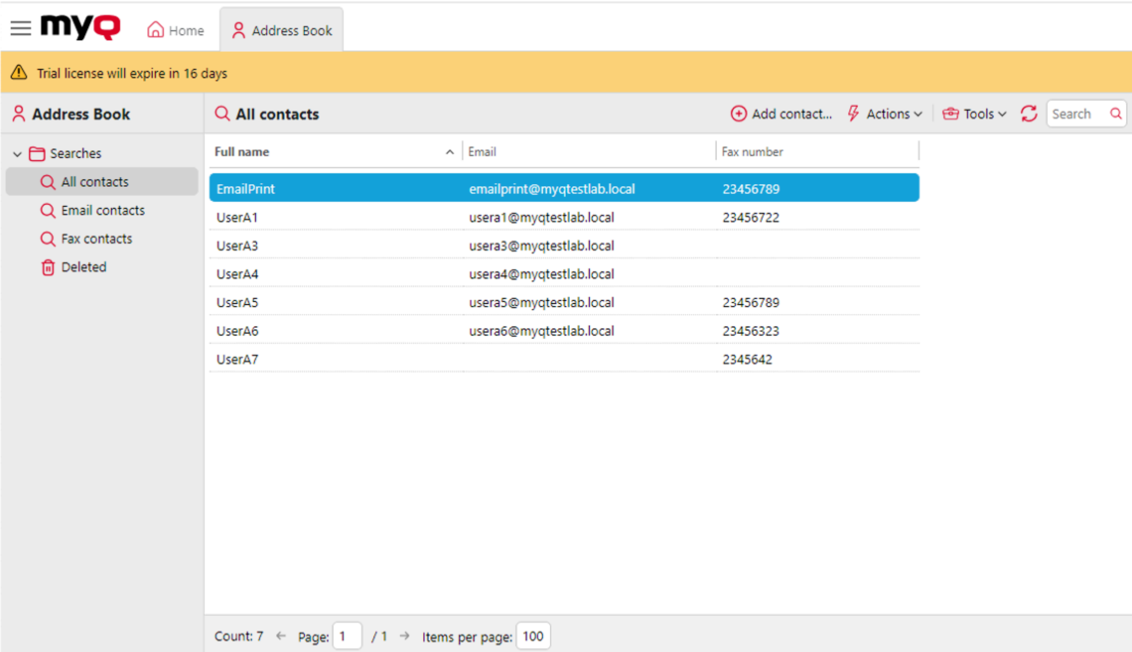
Accessing and Using Address Book

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. 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 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.

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 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*.

Add the Easy Print terminal action

1. Go to **MyQ > Settings > Terminal Actions.**
2. Select the Home Screen or any folder in the Terminal Actions tree.
3. Click **Add Action.** A list of available actions opens.

> You can create multiple instances of the Easy Print action, and configure each one with different settings.

4. Select **Easy Print**. The action is added.
5. Click **Edit** on the action menu to configure the settings for your action, including which storage sources are available to the user and the default release options.

Easy Print Settings

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.

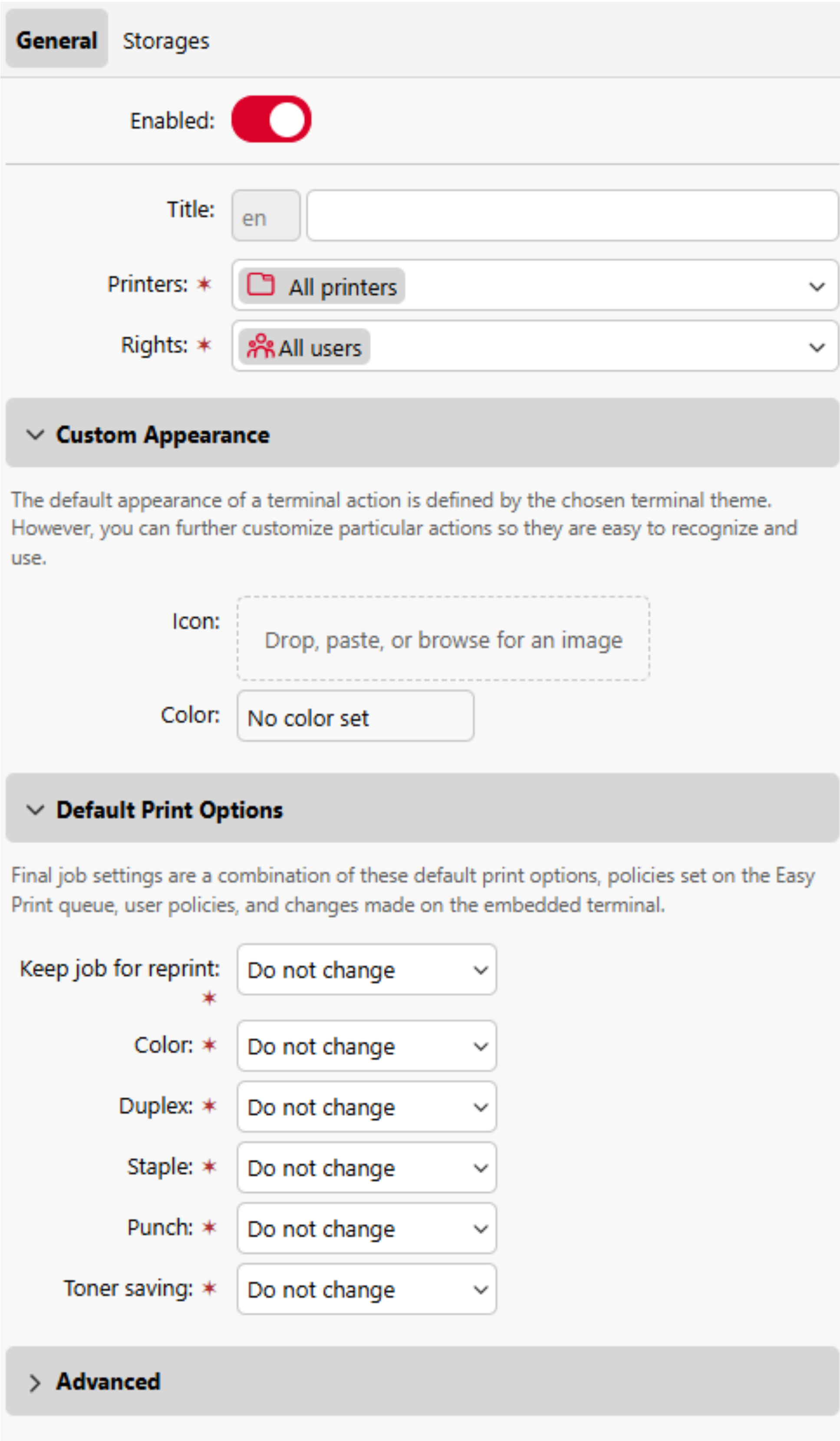
- **Icon** - add an image for the terminal action.
- **Color** - select a color for the terminal action

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**

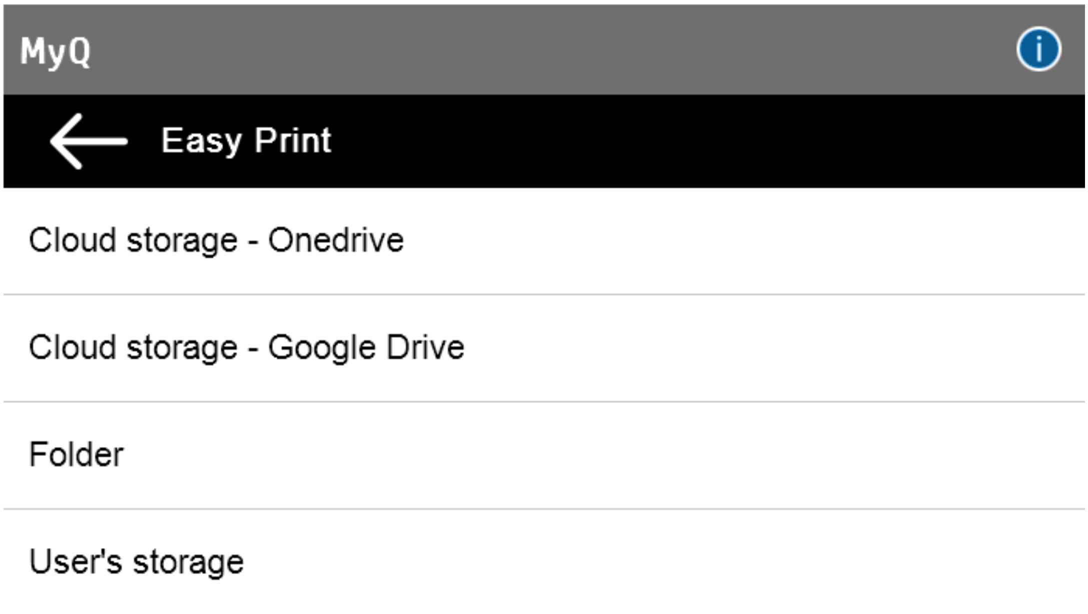


Storages tab

You can add one or more storage locations. These types are supported:

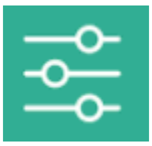
- **Cloud storage**
- **Folder**
- **User’s storage**

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. For more information about how to connect these sources, see Easy Print Sources.



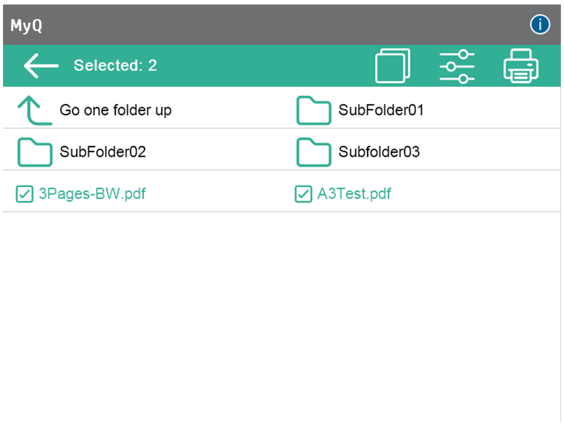
Once a file or files have been selected for printing, you can use the modify button to modify the print options (*Color, Duplex, Staple, Punch, Toner saving*, and *Copies*).

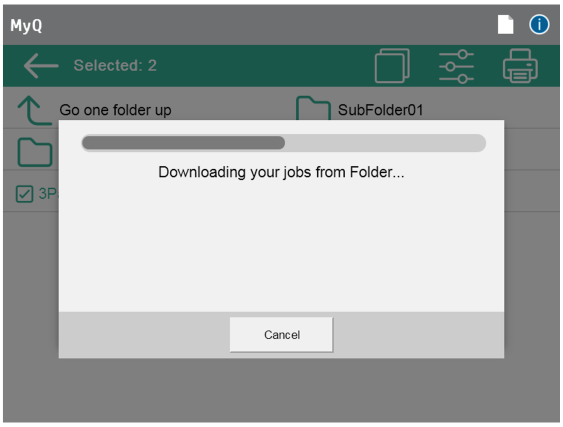
> These options are listed on all terminals, regardless of whether or not the specific terminal can complete a particular action, so it’s possible that a selection made may be ignored.



8 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.





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.

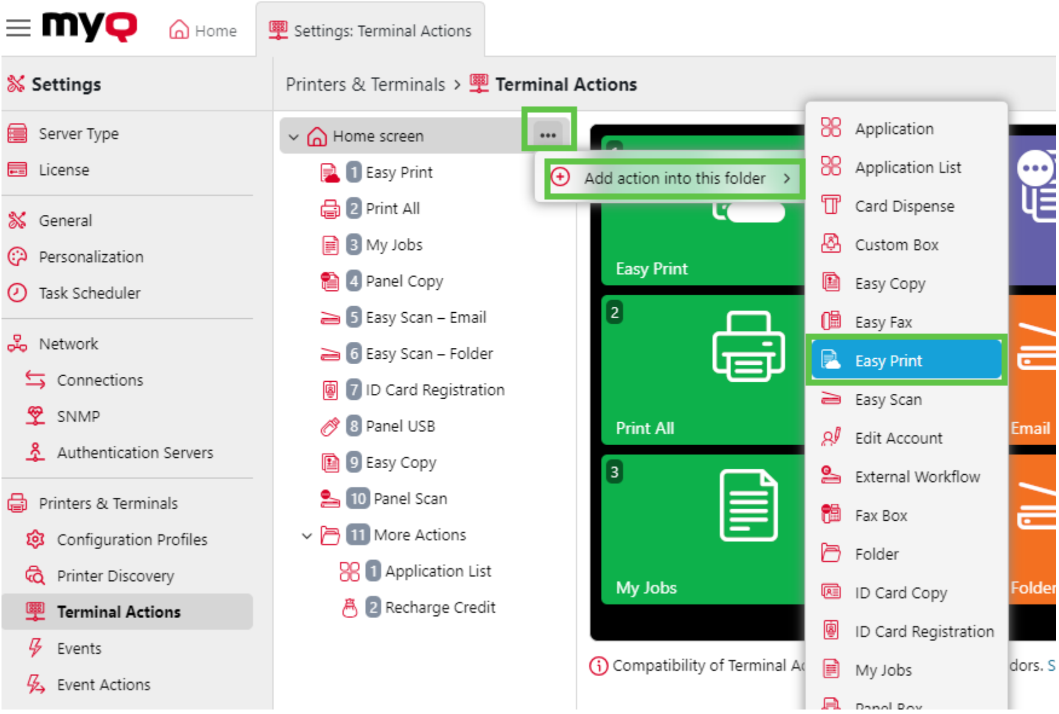
When this action is used on the terminal, the user is presented with a list of possible sources associated with this action (this is skipped in cases of a single source). After the source is selected, the user can browse it and select files for printing.

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.

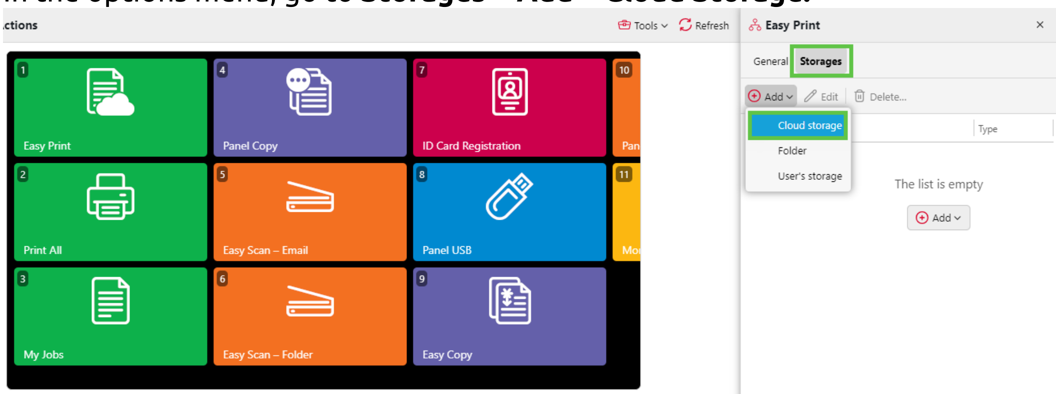
Easy Print from Box

To connect Box as a cloud storage to the **Easy Print** terminal action:

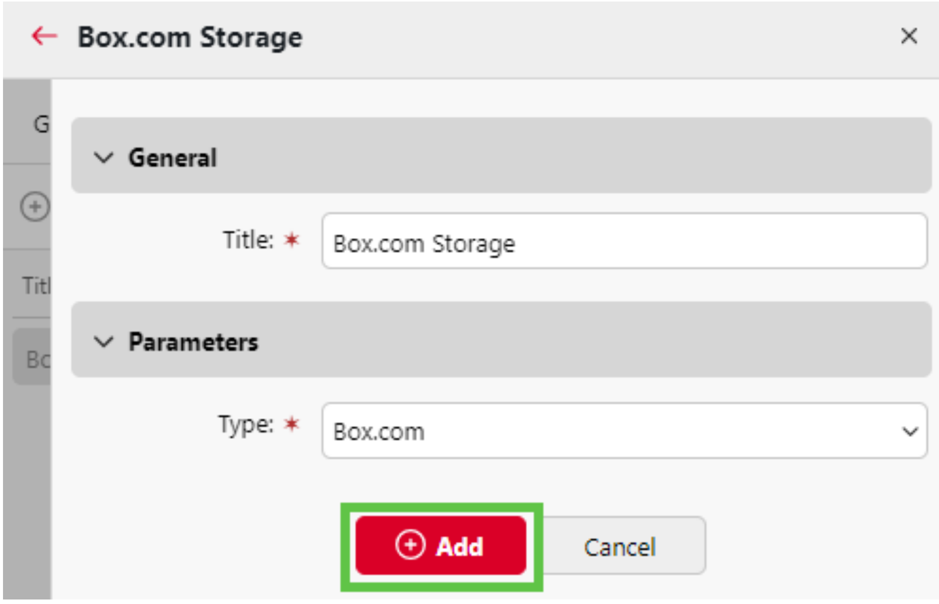
1. Go to **MyQ > Settings > Terminal Actions**.
2. If there is an Easy Print action already added, you can configure it by double-clicking it or create a new one by clicking on the actions menu then **Add action into this folder** and selecting **Easy Print** from the list.



3. In the options menu, go to **Storages > Add > Cloud Storage.**

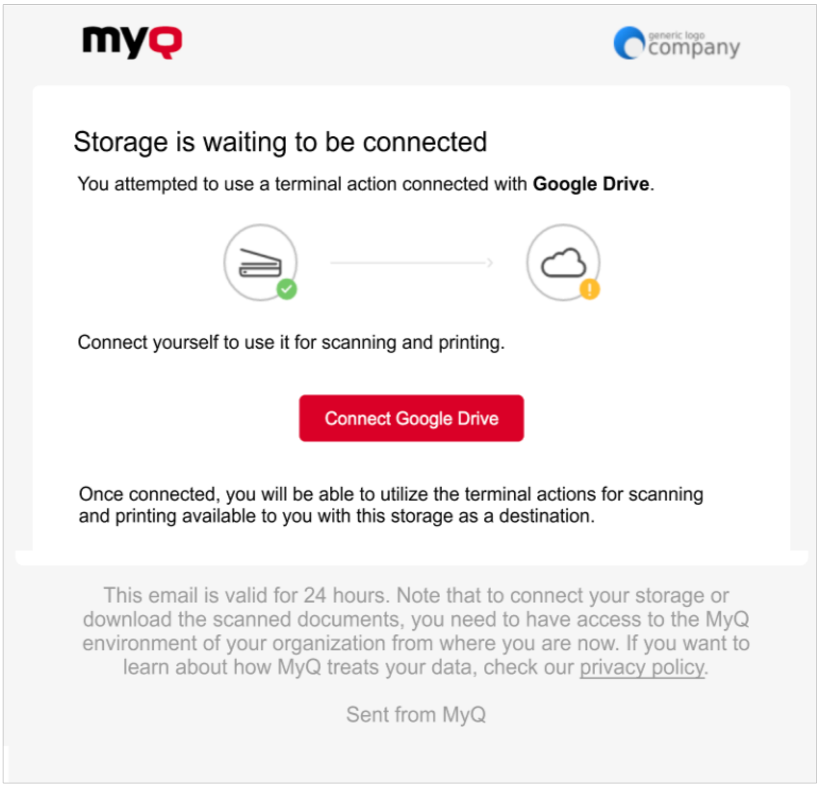


4. Under **General**, you can rename your cloud storage, and under **Parameters**, select the **Type** (`Box.com`) from the dropdown. Then click **Add**.



If an admin has connected a Cloud Storage (for example, Box) to **Easy Print**, but an individual user has not yet connected their personal account, they can still use **Easy Print** with Box set as the source.

An email will be sent to the user's email address allowing them to connect to the cloud storage.



9 Connection email example

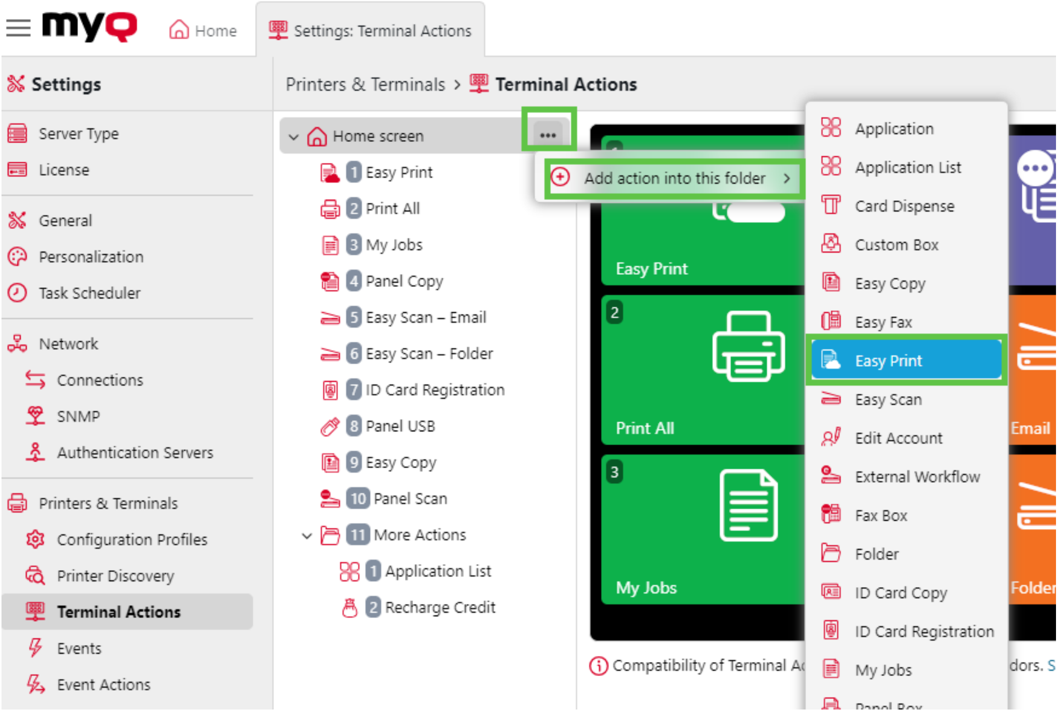
In a case where a user attempts to use **Easy Print** to print a file from Box, but they are not connected, **and** there is no email address associated with that user, the user will receive an on-screen prompt to connect their cloud storage via the web interface and try again.

> ⚠ This does not work with local/network directories, only with Cloud storages.

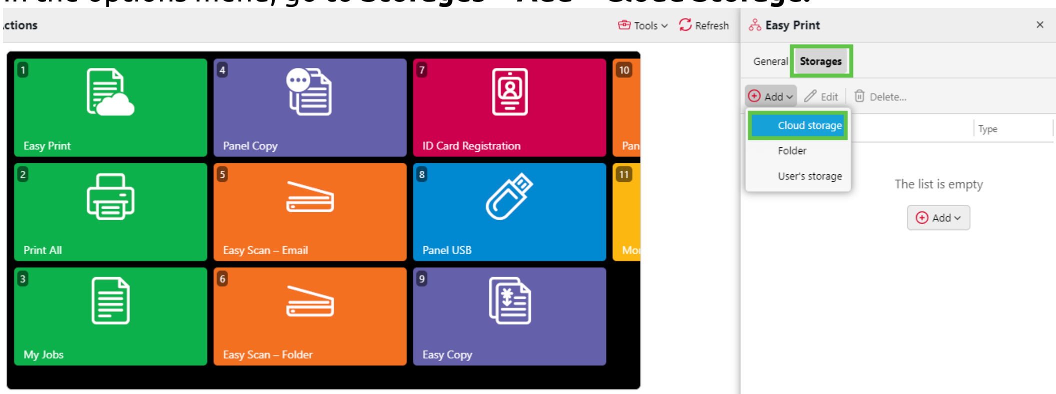
Easy Print from Google Drive

To connect Google Drive as a cloud storage to the **Easy Print** terminal action:

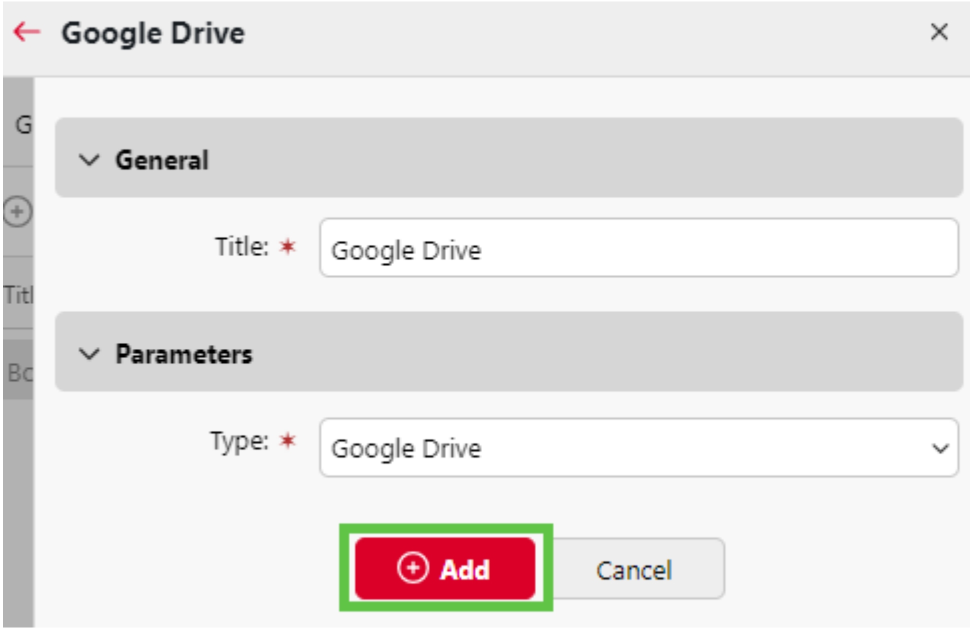
1. Go to **MyQ > Settings > Terminal Actions**.
2. If there is an Easy Print action already added, you can configure it by double-clicking it or create a new one by clicking on the actions menu then **Add action into this folder** and selecting **Easy Print** from the list.



3. In the options menu, go to **Storages > Add > Cloud Storage.**

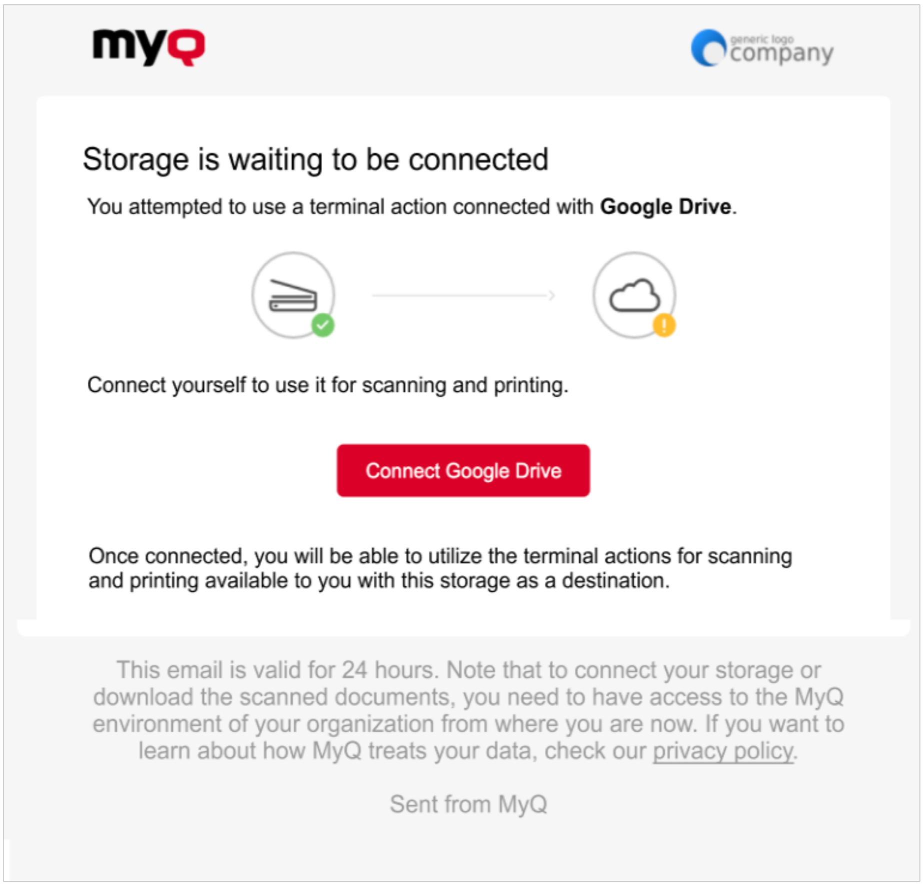


4. Under **General**, you can rename your cloud storage, and under **Parameters**, select the **Type** (Google Drive) from the dropdown. Then click **Add**.



If an admin has connected a Cloud Storage (for example, Google Drive) to **Easy Print**, but an individual user has not yet connected their personal account, they can still use **Easy Print** with Google Drive set as the destination.

An email will be sent to the user's email address allowing them to connect to Google Drive.



10 Connection email example

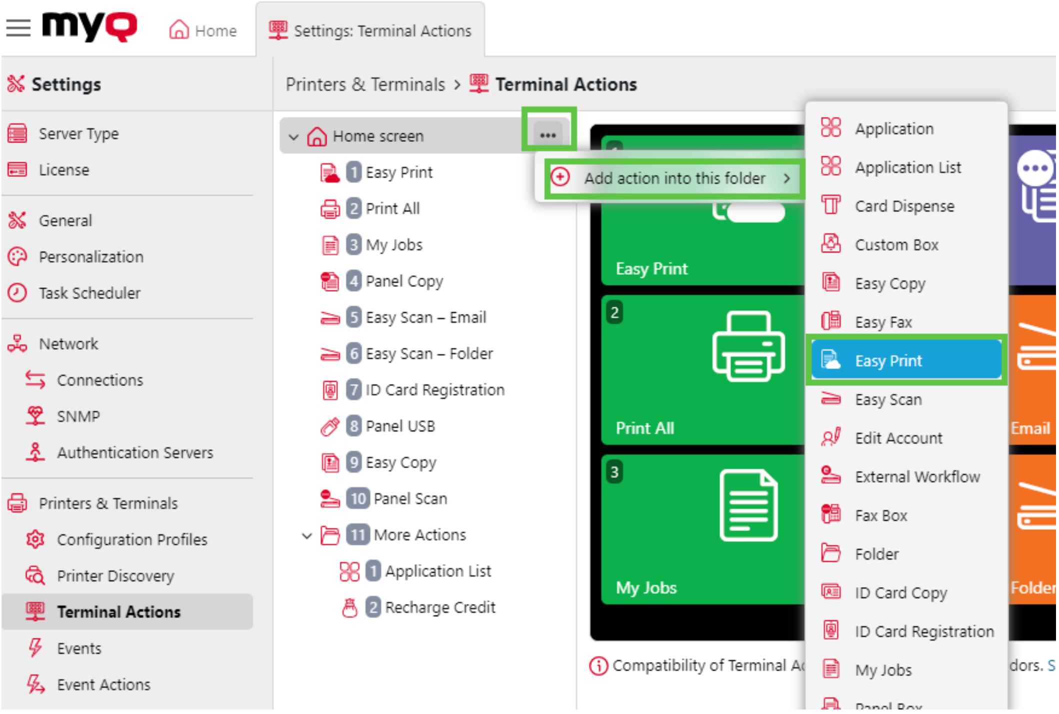
In a case where a user attempts to use **Easy Print** to print a file from Google Drive, but they are not connected, **and** there is no email address associated with that user, the user will receive an on-screen prompt to connect their cloud storage via the web interface and try again.

> ⚠ This does not work with local/network directories, only with Cloud storages.

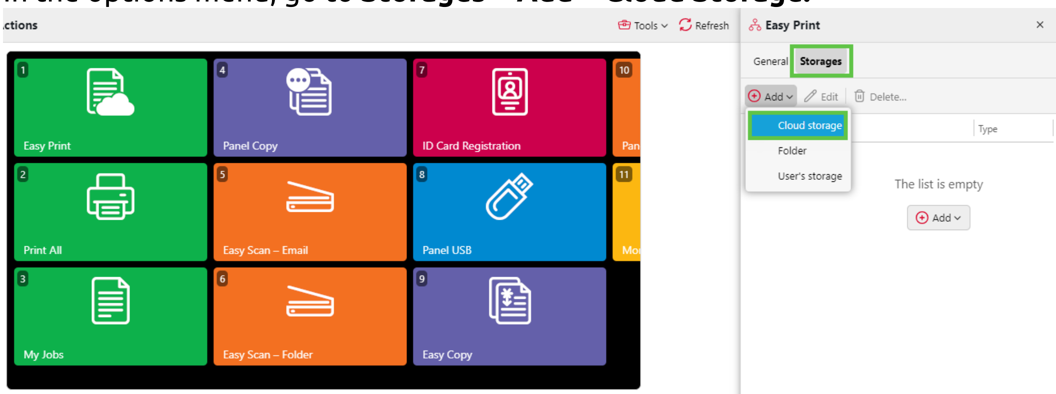
Easy Print from Dropbox

To connect Dropbox as a cloud storage to the **Easy Print** terminal action:

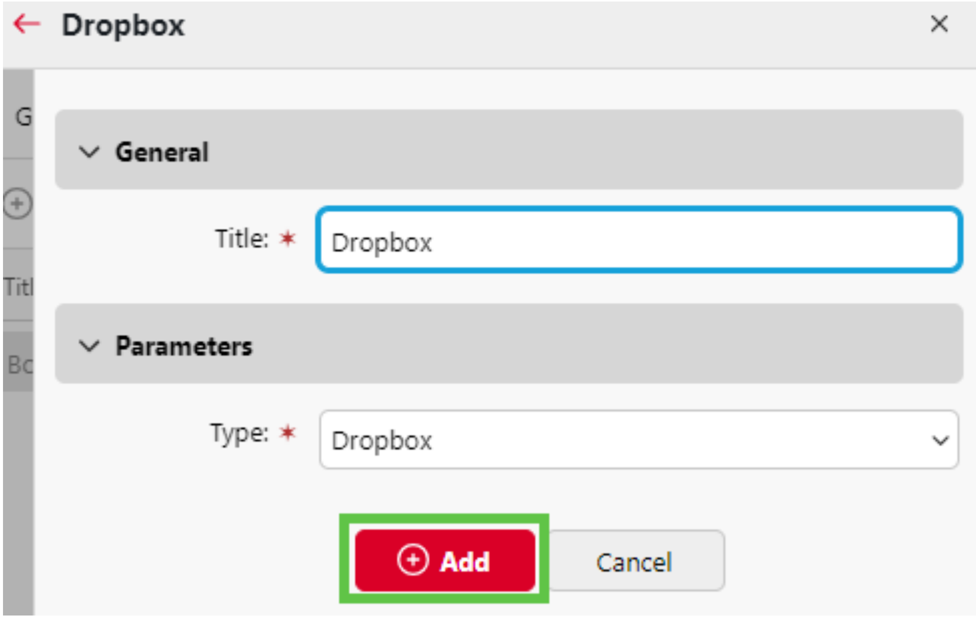
1. Go to **MyQ > Settings > Terminal Actions**.
2. If there is an Easy Print action already added, you can configure it by double-clicking it or create a new one by clicking on the actions menu then **Add action into this folder** and selecting **Easy Print** from the list.



3. In the options menu, go to **Storages > Add > Cloud Storage.**

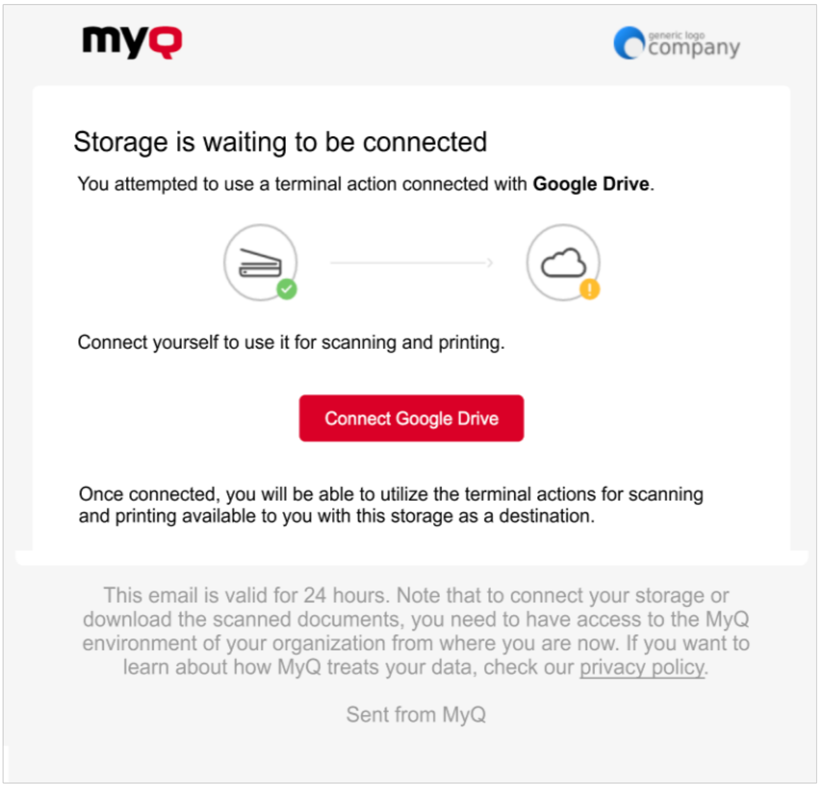


4. Under **General**, you can rename your cloud storage, and under **Parameters**, select the **Type** (Dropbox) from the dropdown. Then click **Add**.



If an admin has connected a Cloud Storage (for example, Dropbox) to **Easy Print**, but an individual user has not yet connected their personal account, they can still use **Easy Print** with Dropbox set as the destination.

An email will be sent to the user's email address allowing them to connect to Dropbox.



11 Connection email example

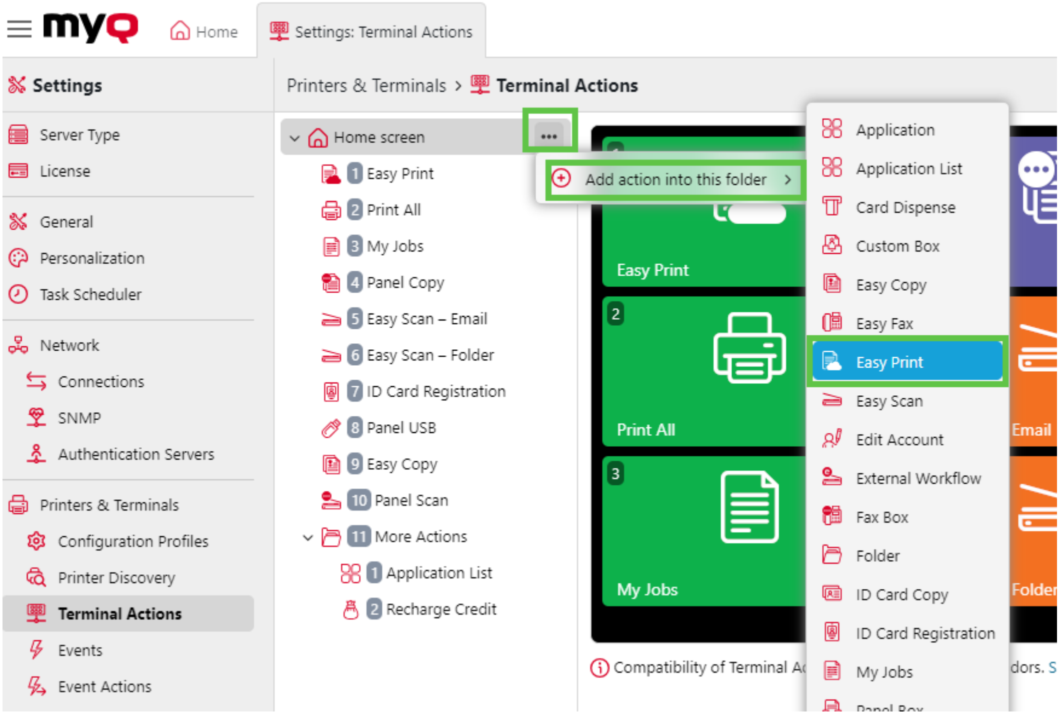
In a case where a user attempts to use **Easy Print** to print a file from Dropbox, but they are not connected, **and** there is no email address associated with that user, the user will receive an on-screen prompt to connect their cloud storage via the web interface and try again.

> ⚠ This does not work with local/network directories, only with Cloud storages.

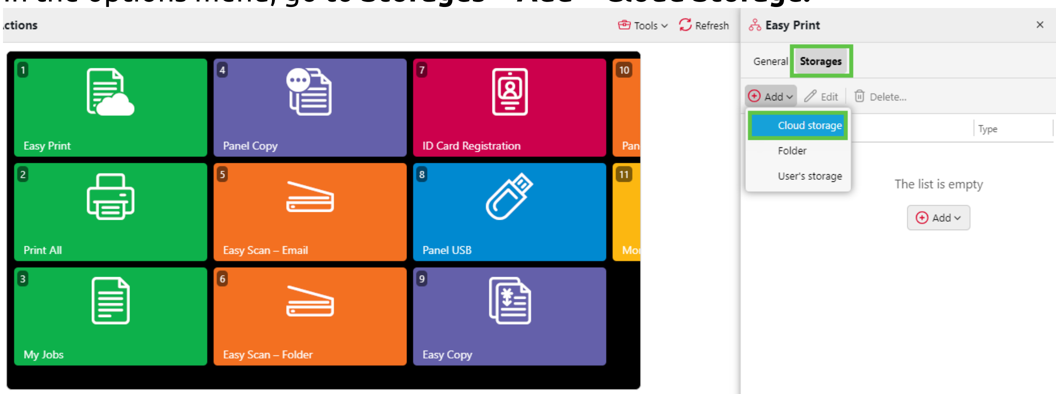
Easy Print from OneDrive

To connect OneDrive as a cloud storage to the **Easy Print** terminal action:

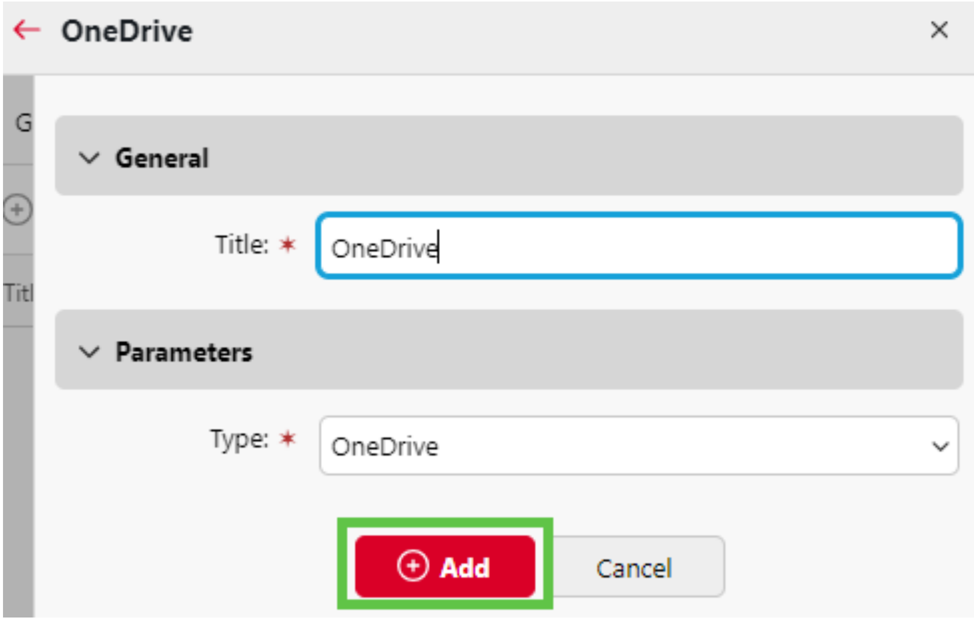
1. Go to **MyQ > Settings > Terminal Actions**.
2. If there is an Easy Print action already added, you can configure it by double-clicking it or create a new one by clicking on the actions menu then **Add action into this folder** and selecting **Easy Print** from the list.



3. In the options menu, go to **Storages > Add > Cloud Storage.**

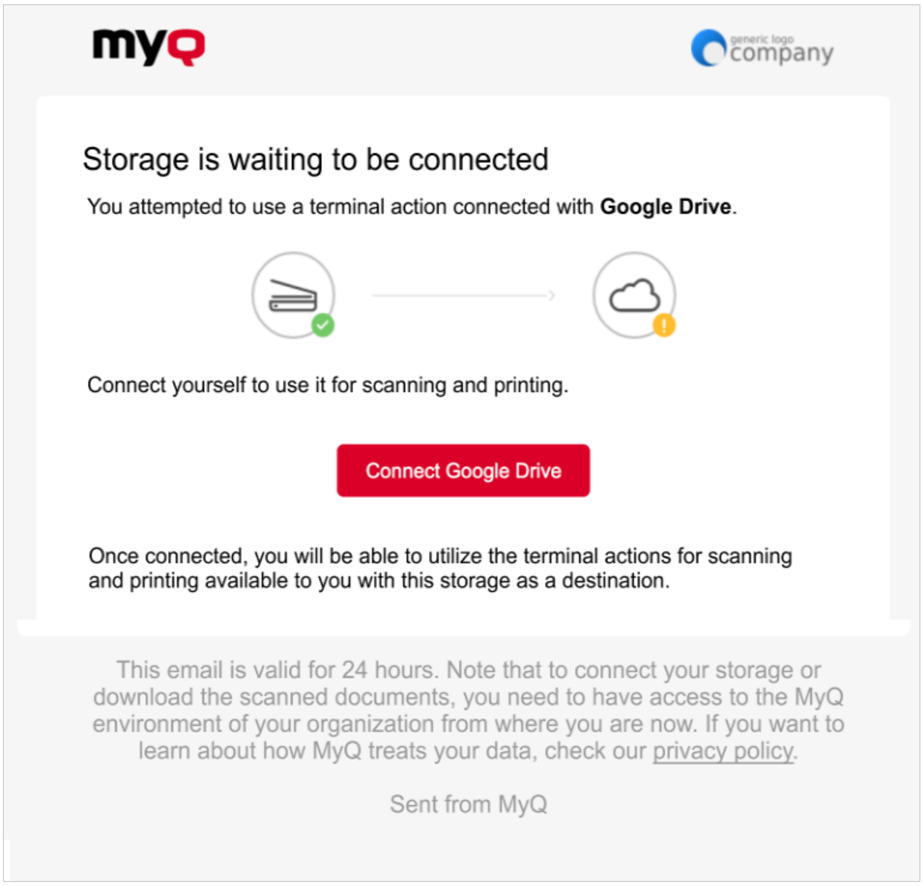


4. Under **General**, you can rename your cloud storage, and under **Parameters**, select the **Type** (OneDrive) from the dropdown. Then click **Add**.



If an admin has connected a Cloud Storage (for example, OneDrive) to **Easy Print**, but an individual user has not yet connected their personal account, they can still use **Easy Print** with OneDrive set as the destination.

An email will be sent to the user's email address allowing them to connect to OneDrive.



12 Connection email example

In a case where a user attempts to use **Easy Print** to print a file from OneDrive, but they are not connected, **and** there is no email address associated with that user, the user will receive an on-screen prompt to connect their cloud storage via the web interface and try again.

> ⚠ This does not work with local/network directories, only with Cloud storages.

Easy Print from OneDrive for Business

This article describes how to configure the Easy Print terminal action to print from OneDrive for Business.

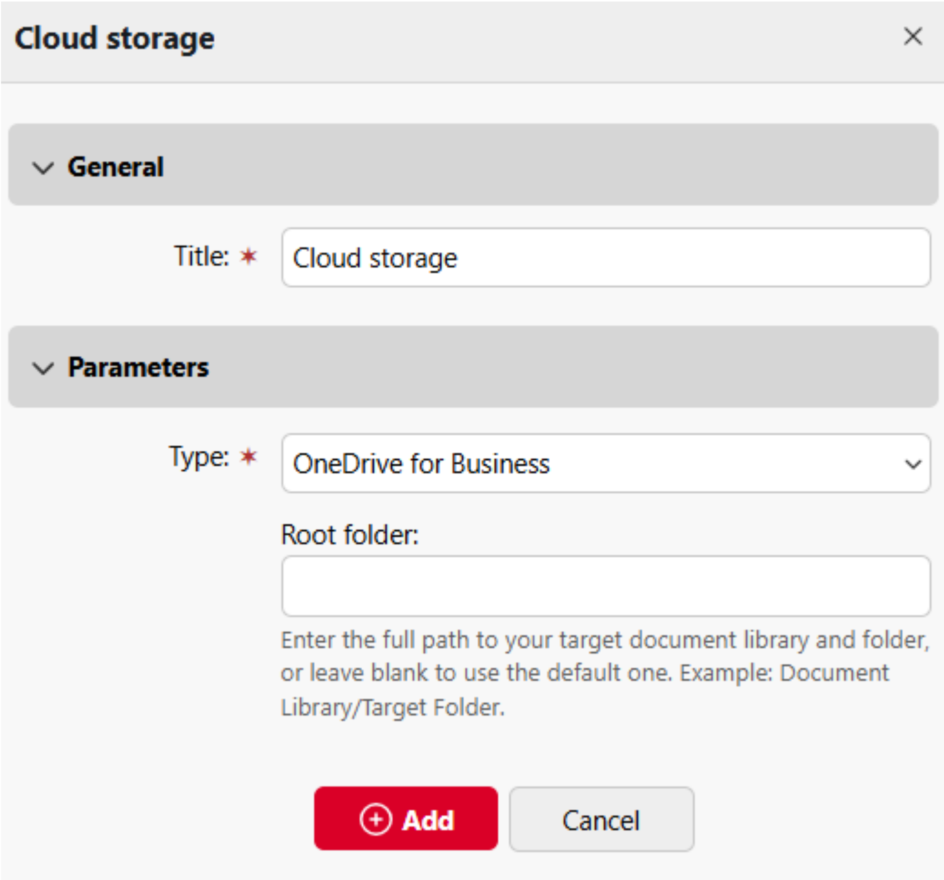
Prerequisite

- A OneDrive for Business connection is configured. For more information, see OneDrive for Business Setup.

Configure Easy Print with the source OneDrive for Business

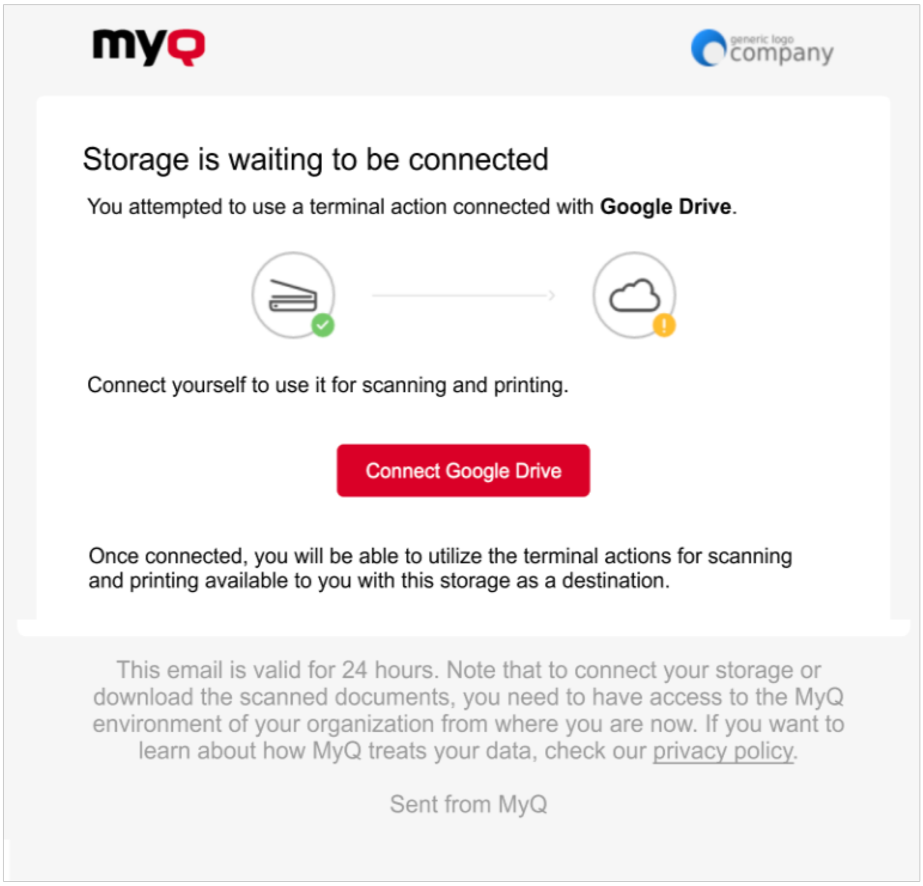
1. Go to **MyQ > Settings > Terminal Actions**.

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**.



If an admin has connected a Cloud Storage (for example, OneDrive for Business) to **Easy Print**, but an individual user has not yet connected their personal account, they can still use **Easy Print** with OneDrive for Business set as the destination.

An email will be sent to the user's email address allowing them to connect to OneDrive for Business.



13 Connection email example

In a case where a user attempts to use **Easy Print** to print a file from OneDrive for Business, but they are not connected, **and** there is no email address associated with that user, the user will receive an on-screen prompt to connect their cloud storage via the web interface and try again.

> ⚠ This does not work with local/network directories, only with cloud storage.

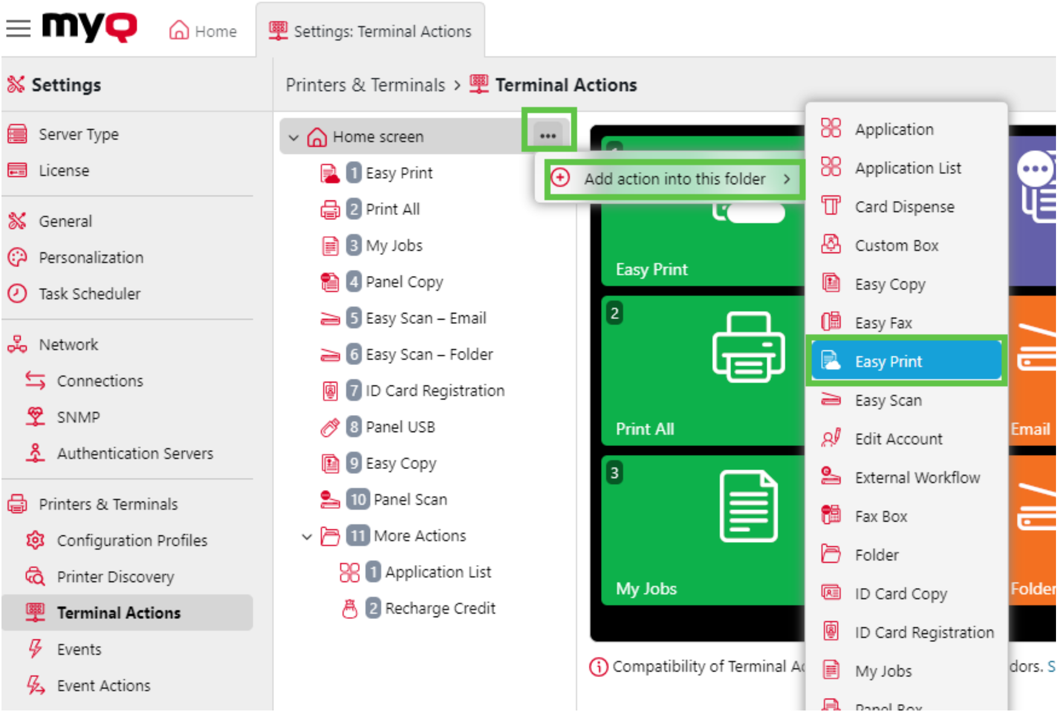
Easy Print from SharePoint Online

> ℹ This option is not available by default. To make it available, you need to set up a connection to it first. For more information on how to do that, see the SharePoint Online Setup.

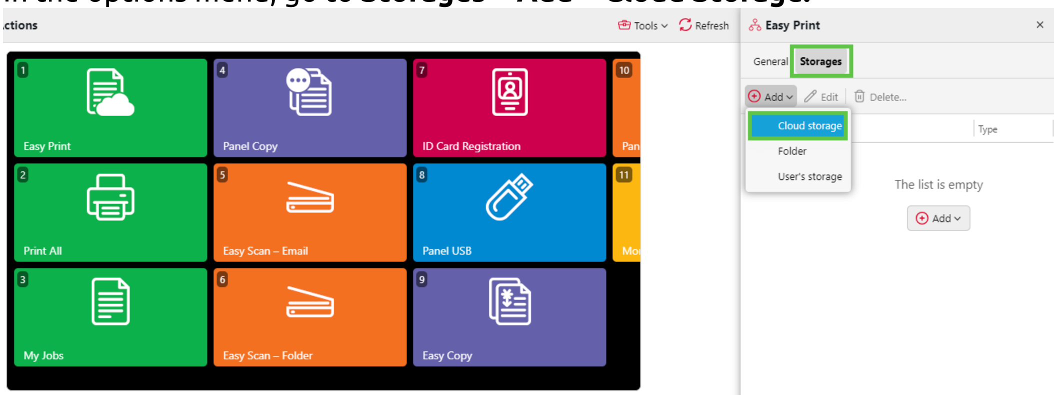
To connect SharePoint Online as a cloud storage to the **Easy Print** terminal action:

1. Go to **MyQ > Settings > Terminal Actions**.

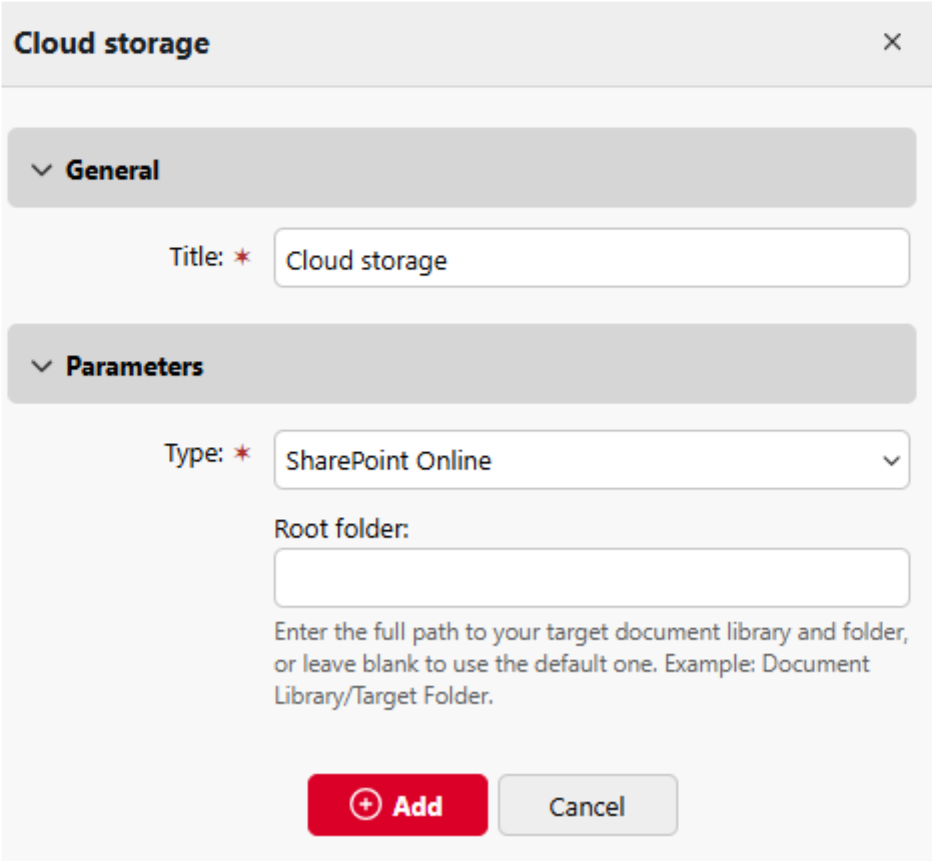
2. If there is an Easy Print action already added, you can configure it by double-clicking it or create a new one by clicking on the actions menu then **Add action into this folder** and selecting **Easy Print** from the list.



3. In the options menu, go to **Storages > Add > Cloud Storage.**

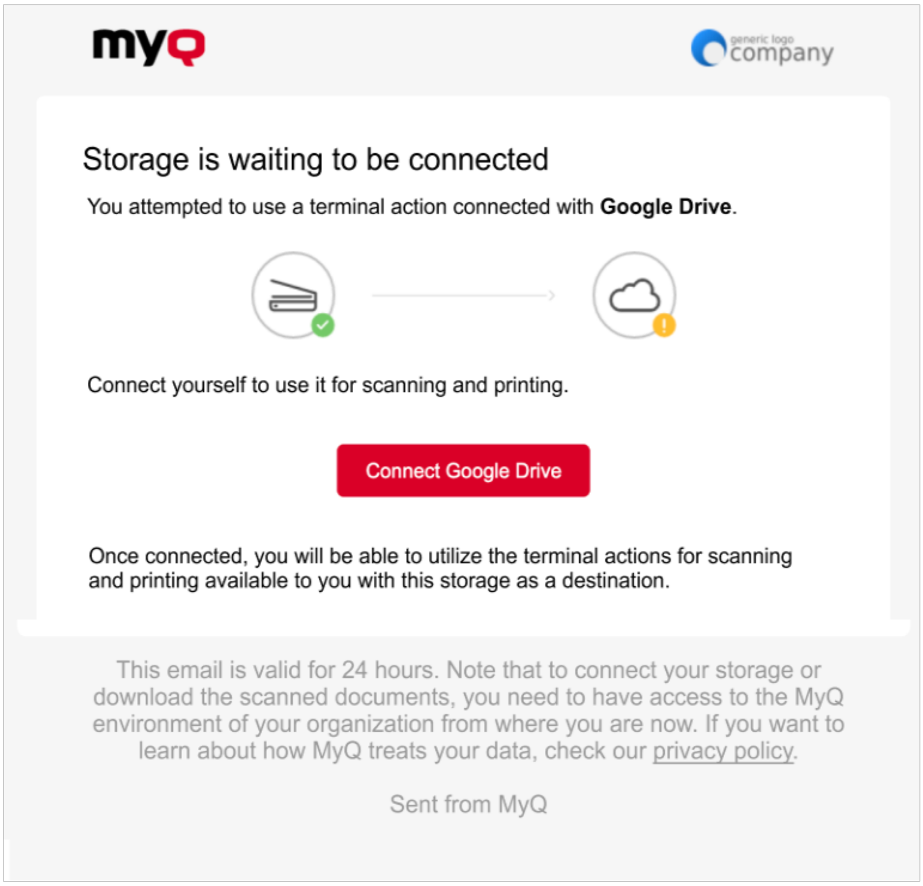


4. Under **General**, you can rename your cloud storage, and under **Parameters**, select the **Type** (SharePoint Online) from the dropdown, optionally you can specify a **Root folder** to print from. Then click **Add**.



If an admin has connected a Cloud Storage (for example, SharePoint Online) to **Easy Print**, but an individual user has not yet connected their personal account, they can still use **Easy Print** with SharePoint Online set as the destination.

An email will be sent to the user's email address allowing them to connect to SharePoint Online.



14 Connection email example

In a case where a user attempts to use **Easy Print** to print a file from SharePoint Online, but they are not connected, **and** there is no email address associated with that user, the user will receive an on-screen prompt to connect their cloud storage via the web interface and try again.

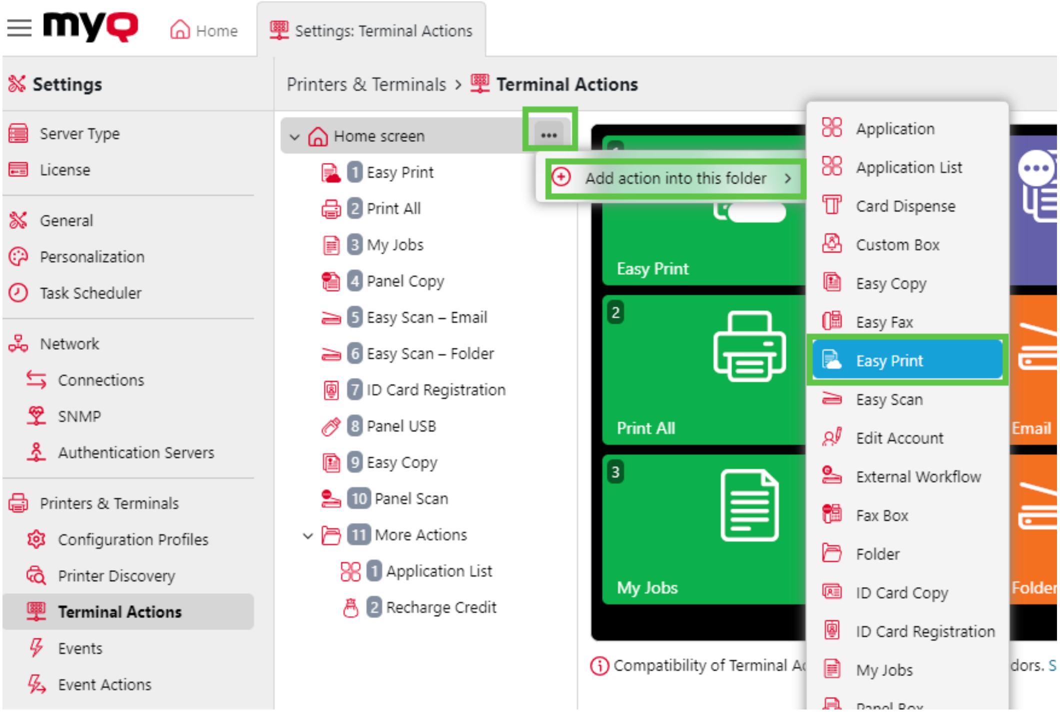
> ⚠ This does not work with local/network directories, only with Cloud storages.

Print from Local Storage

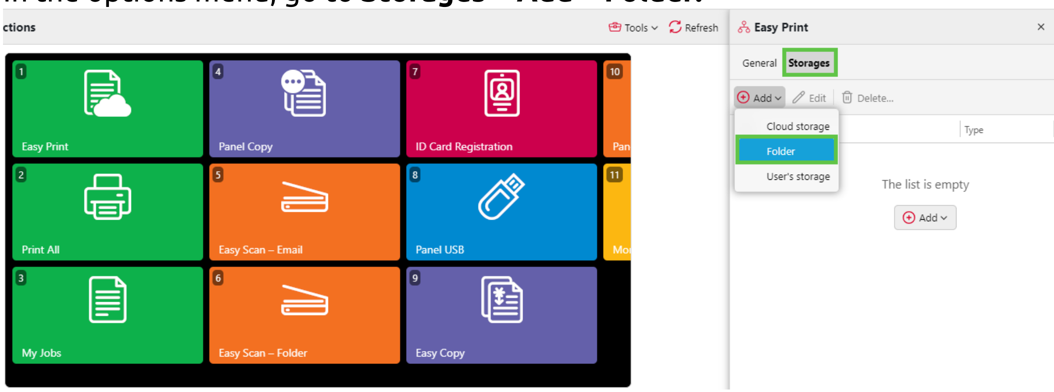
Connect a Local Storage

To connect a local storage to the **Easy Print** terminal action:

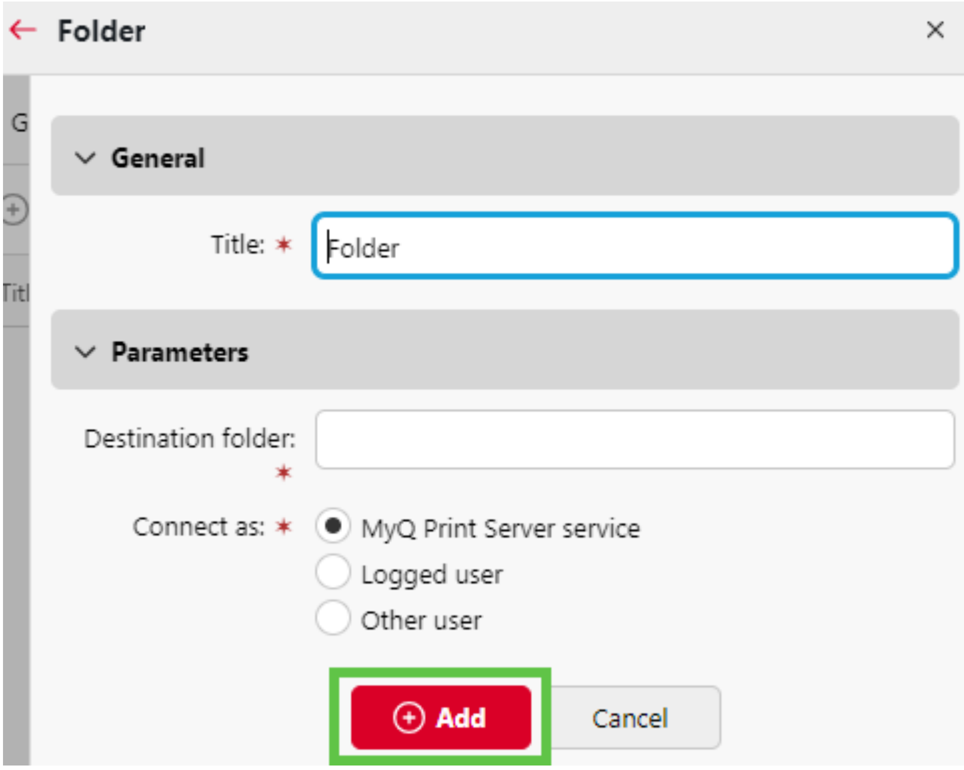
1. Go to **MyQ > Settings > Terminal Actions**.
2. If there is an Easy Print action already added, you can configure that one by double-clicking it or create a new one by clicking on the actions menu then **Add action into this folder** and selecting **Easy Print** from the list.



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**.



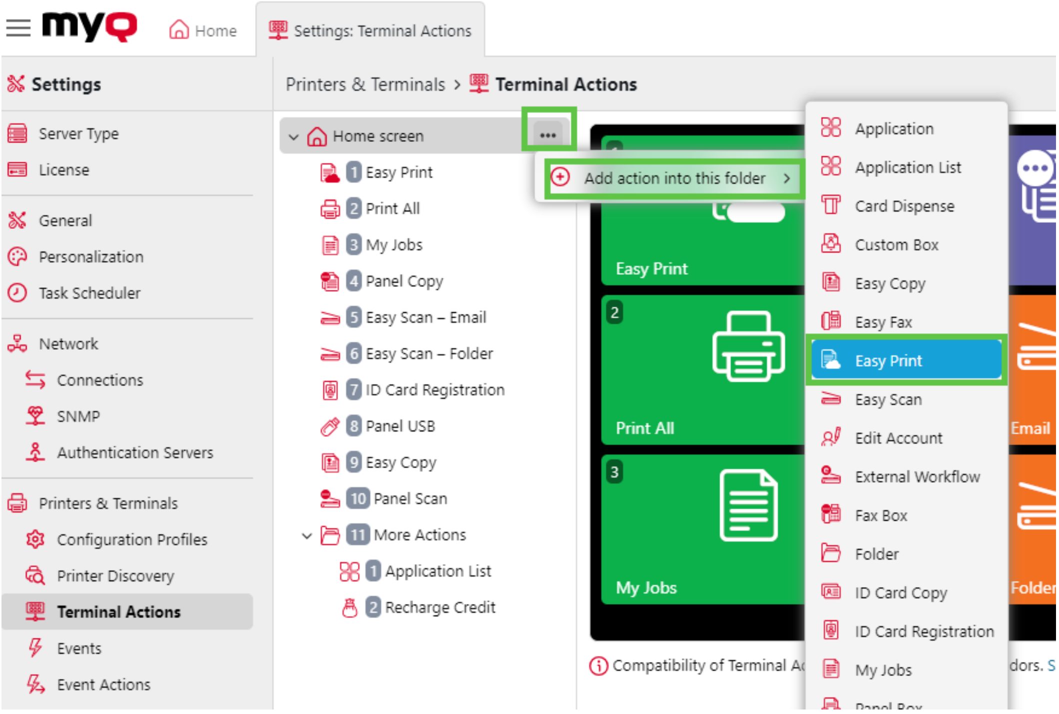
Once this is set up, the user will see the option to browse this folder when using Easy Print.

Print from User Storage

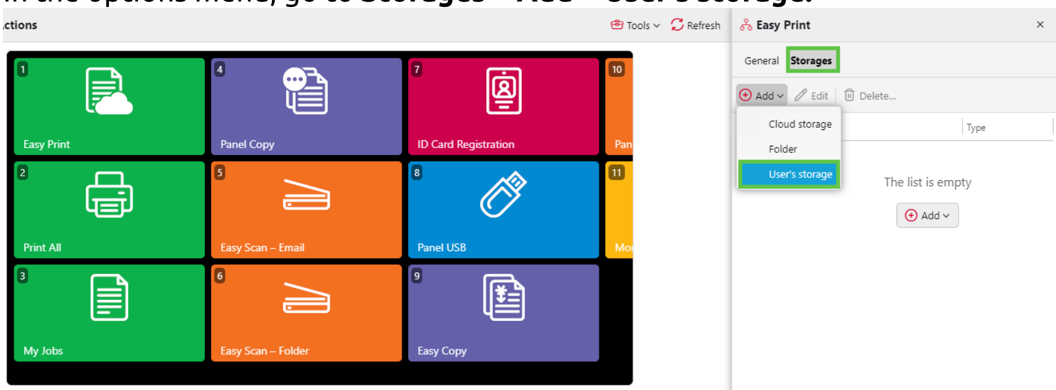
Connect a User's Storage

To connect a user's storage to the **Easy Print** terminal action:

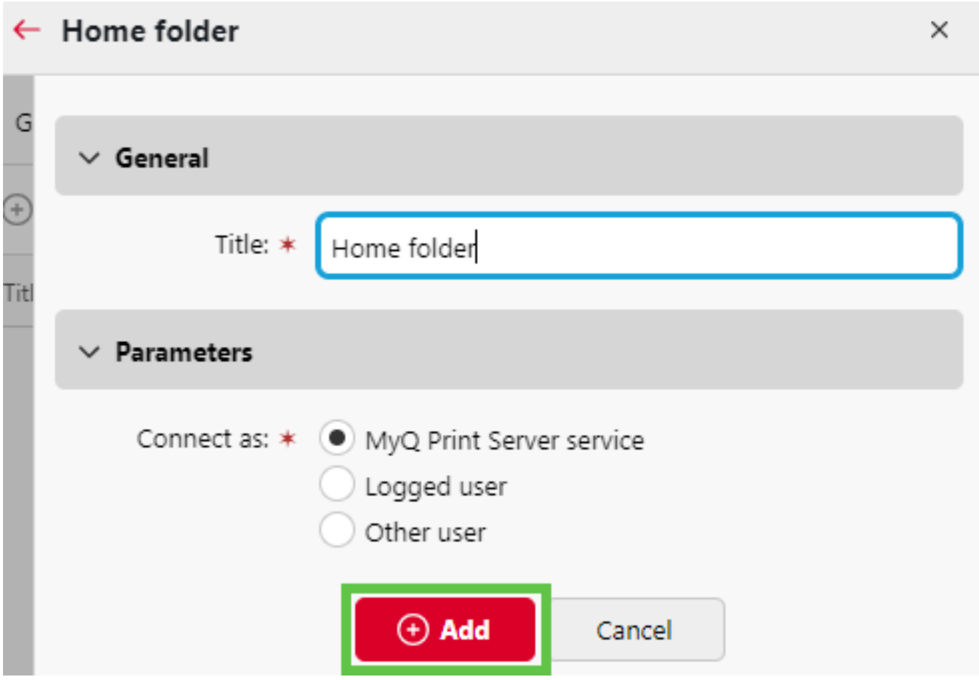
1. Go to **MyQ > Settings > Terminal Actions**.
2. If there is an Easy Print action already added, you can configure that one by double-clicking it or create a new one by clicking on the actions menu then **Add action into this folder** and selecting **Easy Print** from the list.



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.

8.2 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**.

8.3 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.

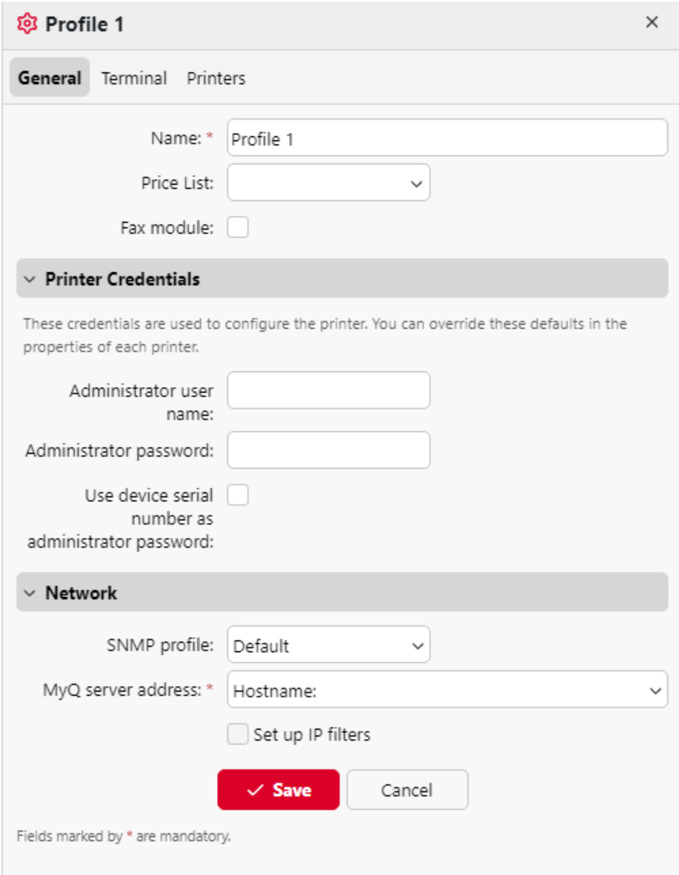
It is recommended to create a configuration profile per printer type if you have different printer types.

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.

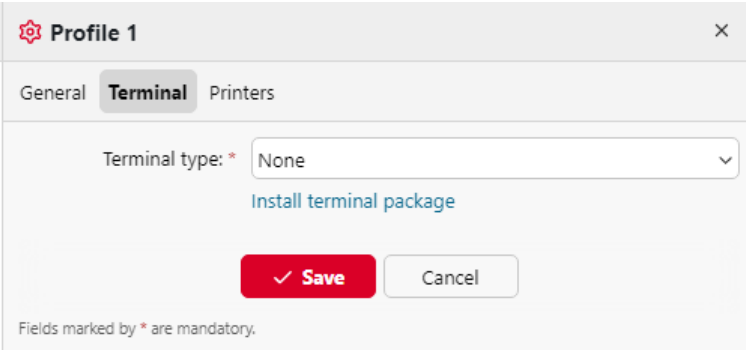
The following settings can be configured:

8.3.1 General tab



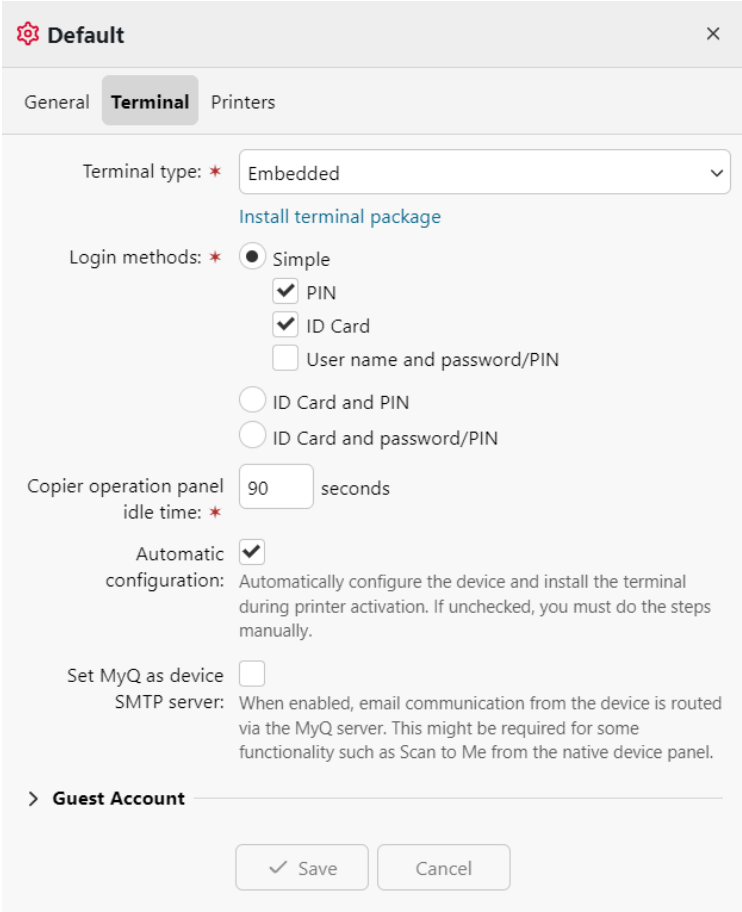
- **Name -** It is mandatory to give the profile a name.
- **Price List** - Select a price list from the drop-down. For more information on price lists, see Price Lists.
- **Fax module** - If selected, all printed faxes are charged on the FAX user account. It is available only for devices with the FAX 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: see SNMP profiles, and in **MyQ server address** select if the network should use the IP address or the Hostname (Hostname is used by default).

8.3.2 Terminal tab



- **Terminal type** - Select a terminal type from the drop-down.
  - Embedded
  - Kyocera Embedded Lite
  - HW-11-T
  - Felica Reader
  - Android Terminal
  - MyQ TerminalPro / TCPCONV2 / NET2USB Converter V2
  - MyQ TerminalPro / TCPCONV2 / NET2USB Converter V2 + Touch Panel
  - 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.



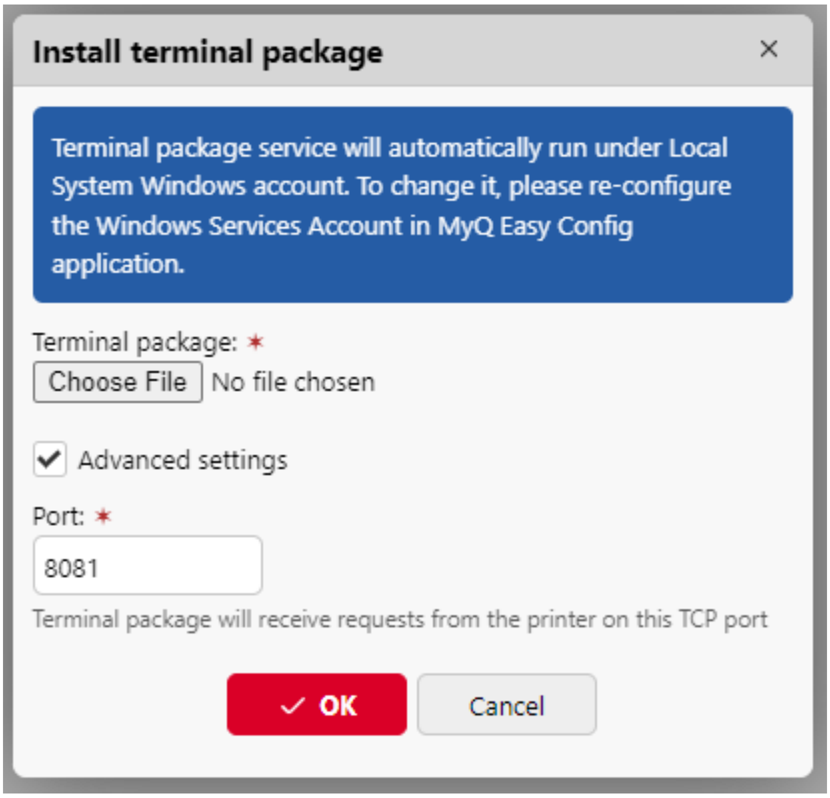
- **Login methods**: select the login methods you want to be available on terminals with this configuration profile selected, the options are **PIN**, **ID Card**, and **User name and password/PIN**, **ID Card** can also be combined with **PIN** or **Password** if double-authentication is required.
- **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

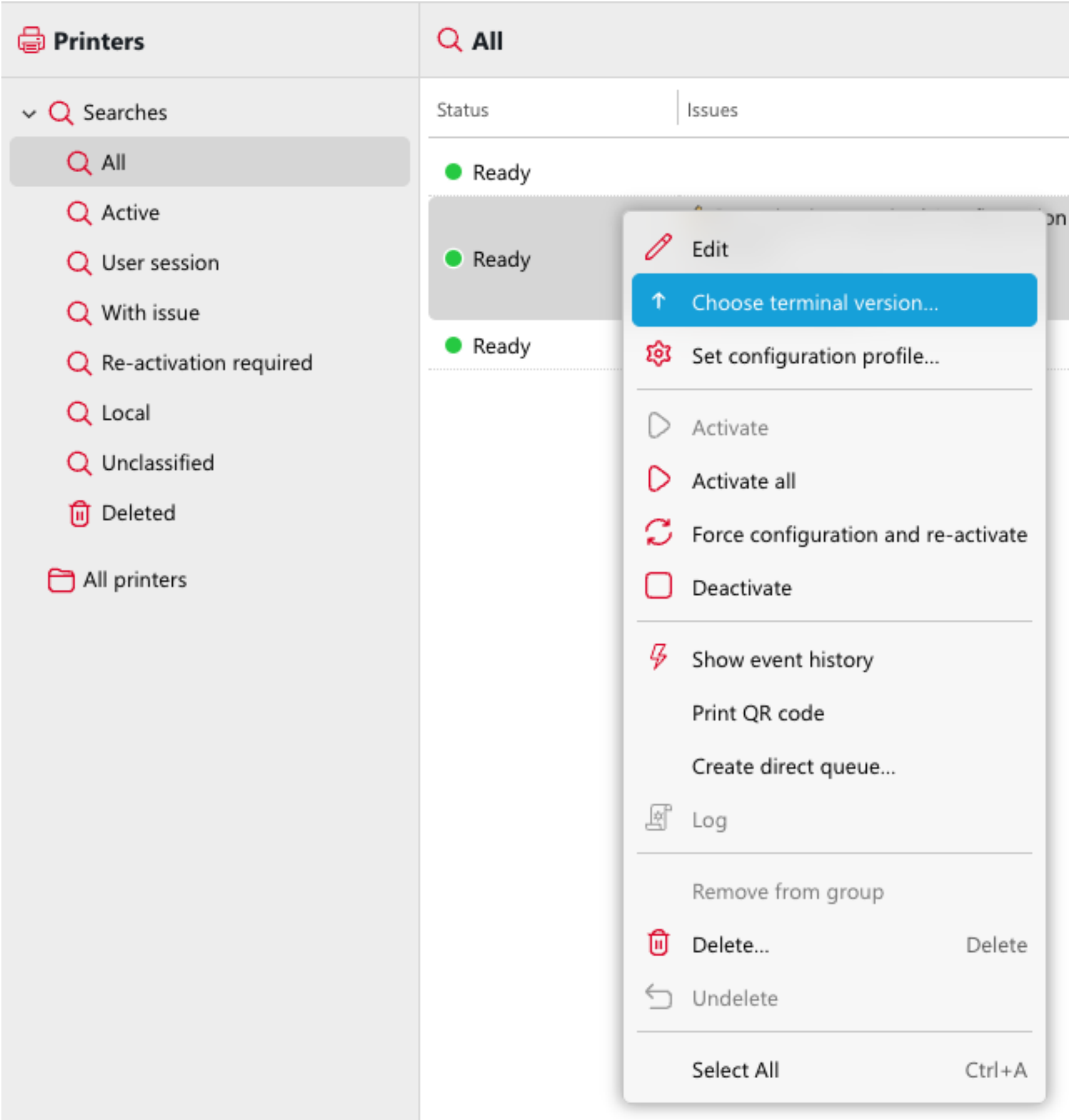
In certain situations, it may be necessary or helpful to utilize multiple terminal packages from the same vendor, for example when staggering updates to a large fleet, or because certain devices are not compatible with the latest terminal packages.

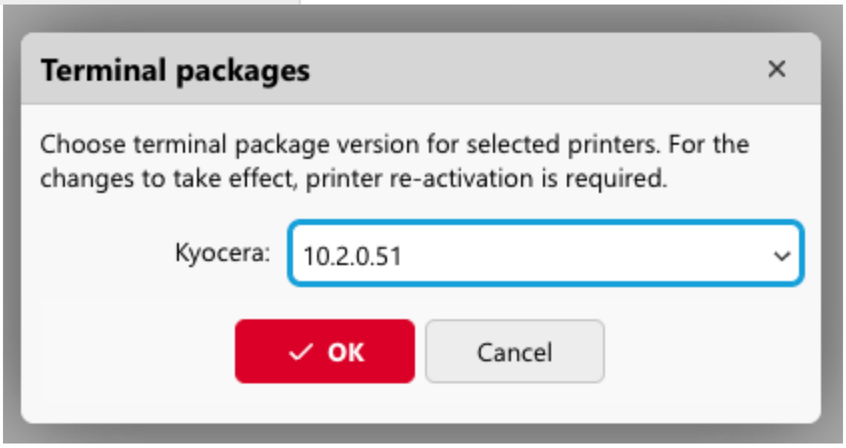
> ⚠ In order to run multiple terminal packages from the same vendor, one of those terminal packages must normally be a terminal version 10.2 or higher. Certain 10.1 terminal versions also support this feature.

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.





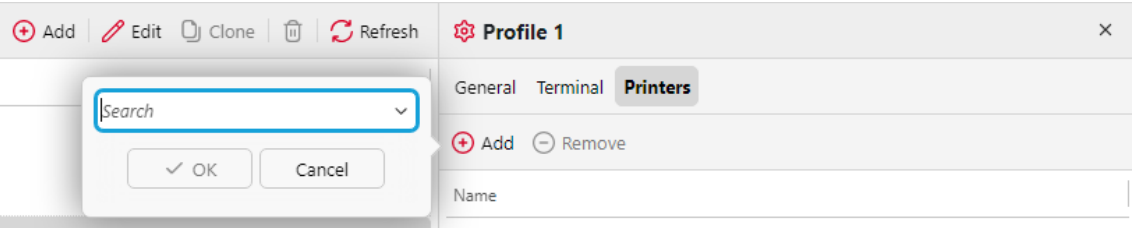
For more information, see Using Multiple Terminal Packages for the same Vendor.

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

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.

8.3.3 Additional options

The following options may become available according to the installed terminal package. It depends on brand and model if they will function on your printer:

- Login methods
- Guest Account
- Guest screen
- Local administration PIN
- Language selection
- Display numeric keypad
- ID Card reader type
- Validate security certificates
- Scan delivery method
- Skip Blank Pages Level

8.4 Discovering Printing Devices

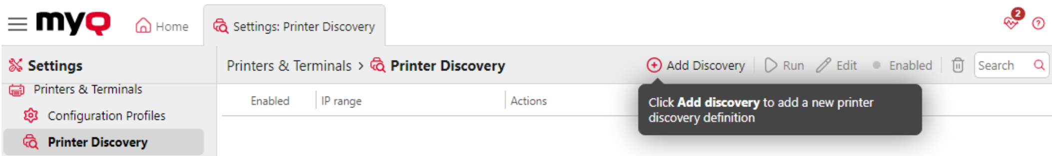
On the **Printer Discovery** settings tab, you can create and run print discoveries to search for all network printing devices within a defined IP range of your company's network. You can create multiple discoveries for different subnets.

8.4.1 Automated printer discovery

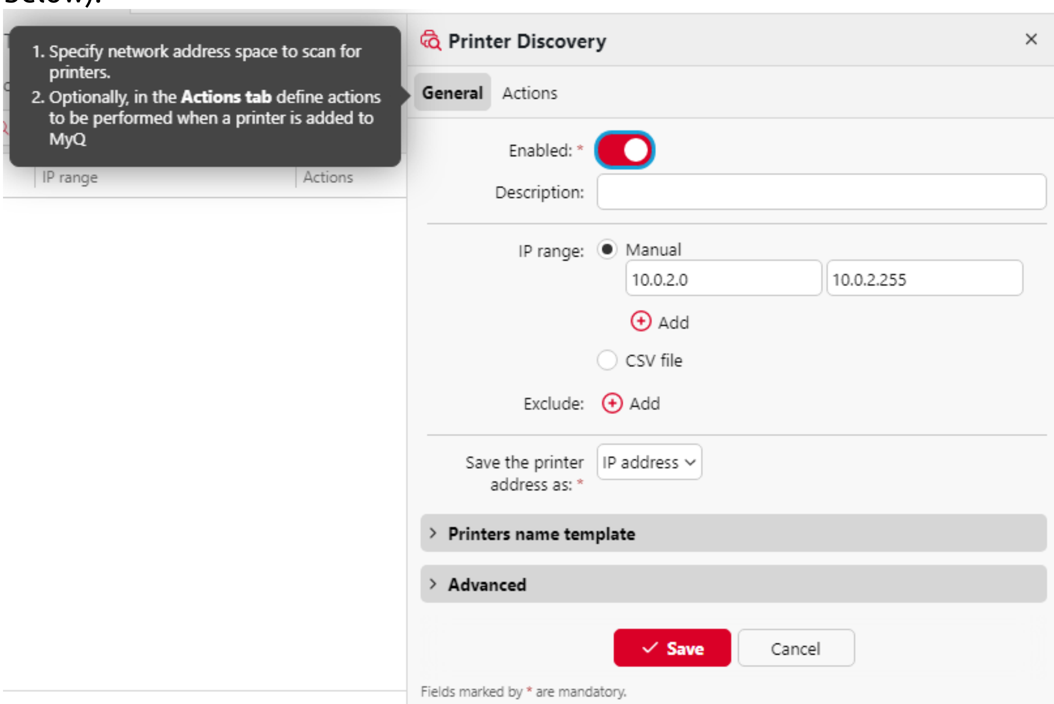
It is possible to add an **Action** to your printer discovery. In that way you can add a **Configuration profile** to your printer discovery, or select to activate the discovered printers when you **Run** the printer discovery.

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.



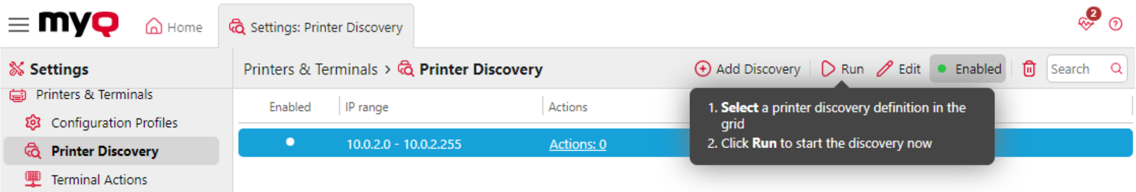
3. On the panel, you can change the **General** discovery configuration (described below).



4. You can also set special **Actions** to be performed during the discovery; see Printer discovery actions.
5. Click **Save**. The new printer discovery appears on the list on the **Printer Discovery** settings tab.

8.4.2 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**.

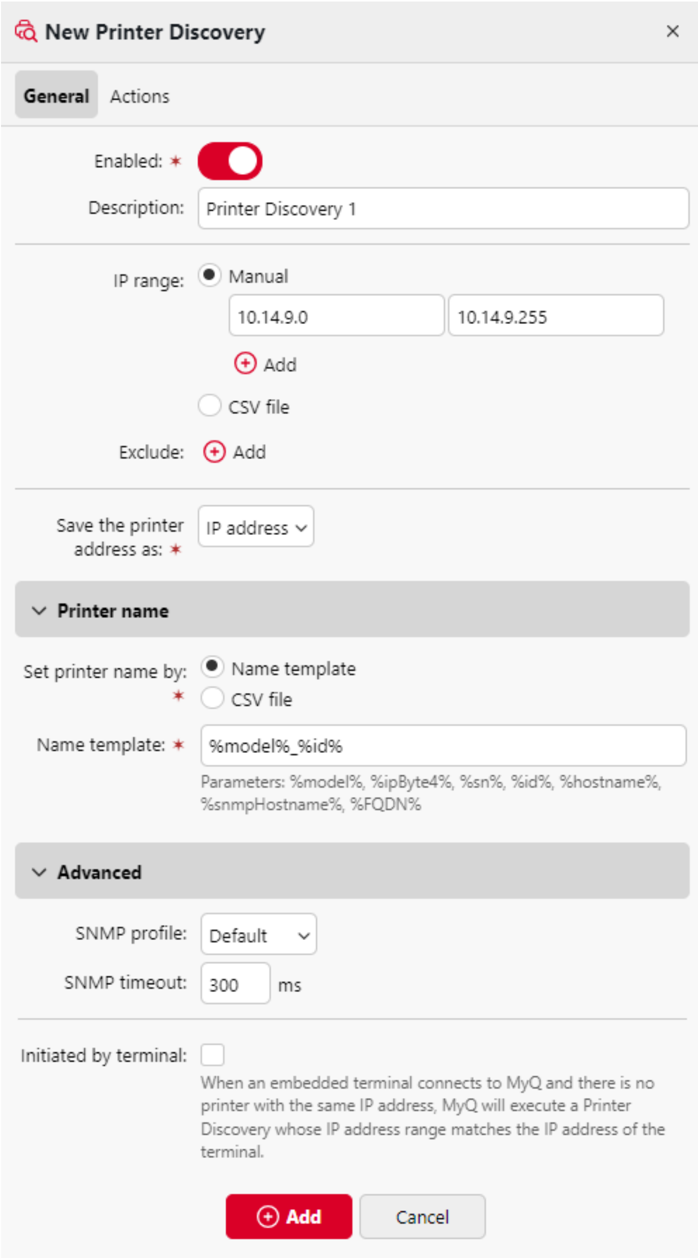


The Discovering tab with a list of discovered printing devices opens. You can choose to add either all of the discovered devices or just a selection of them:

- 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.

8.4.3 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:

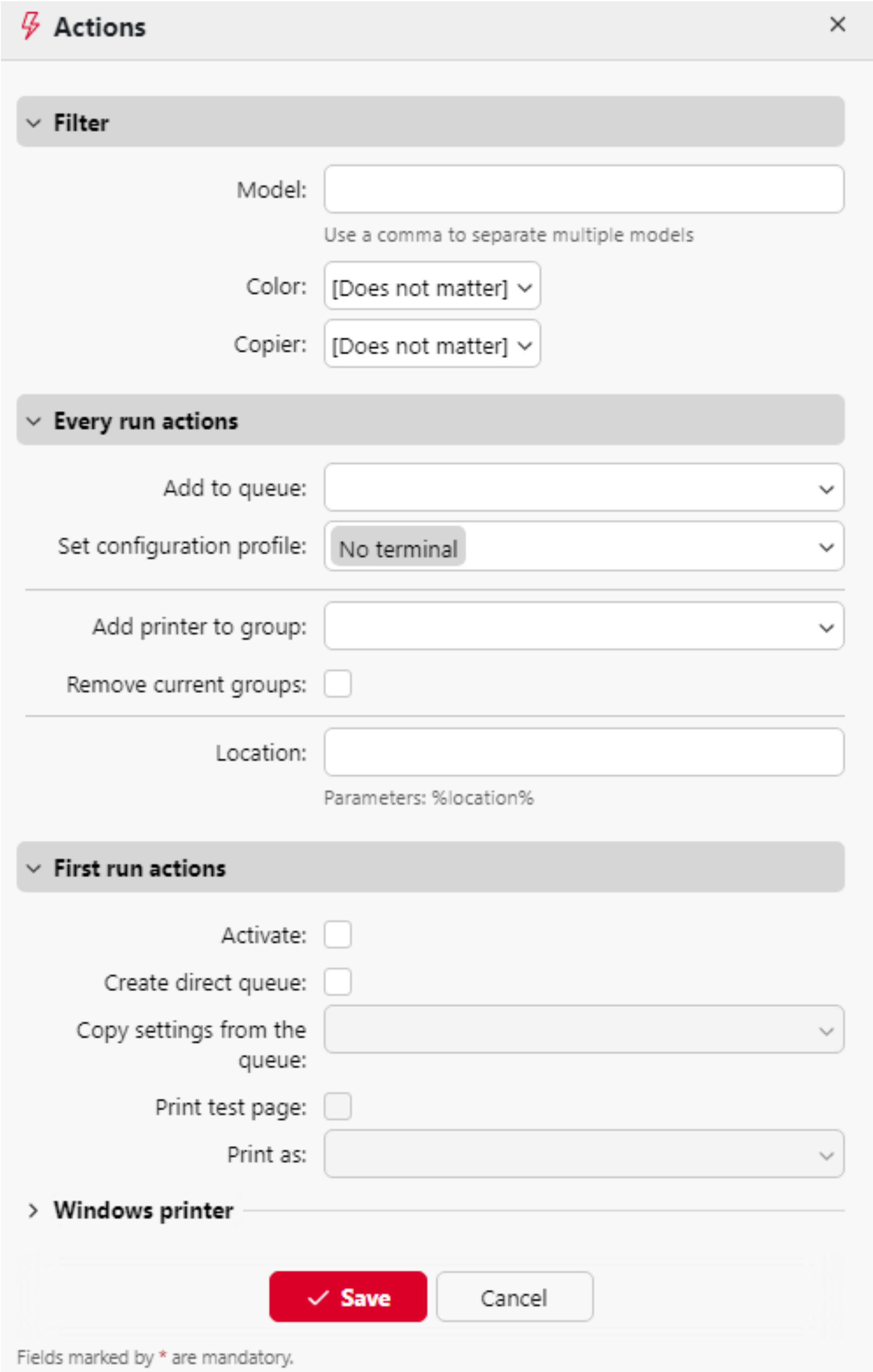
      ```
      list of IPs;Custom name
      10.0.0.11;Printer Name 1
      10.0.0.12;Printer Name 2
      ```

    - 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.

8.4.4 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.


Actions
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 the queue:
Print test page:
Print as:
Windows printer
Save
Cancel
Fields marked by * are mandatory.

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

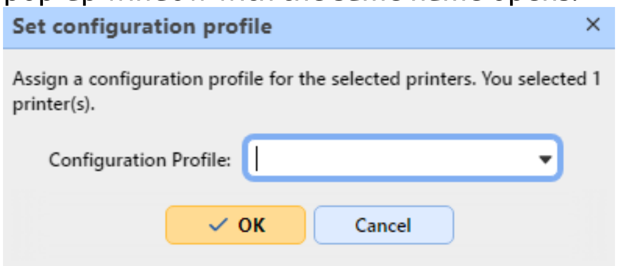
- **Activate**: Automatically activates the device if the current license allows it.
- **Create direct queue**: If you select this option, MyQ will automatically create a direct queue for the device. The name of the queue is the same as the system name of the device. For more information about print queues, see Queues.
- **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.

8.5 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 the same name 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**.

8.6 Deleting and Restoring Printers

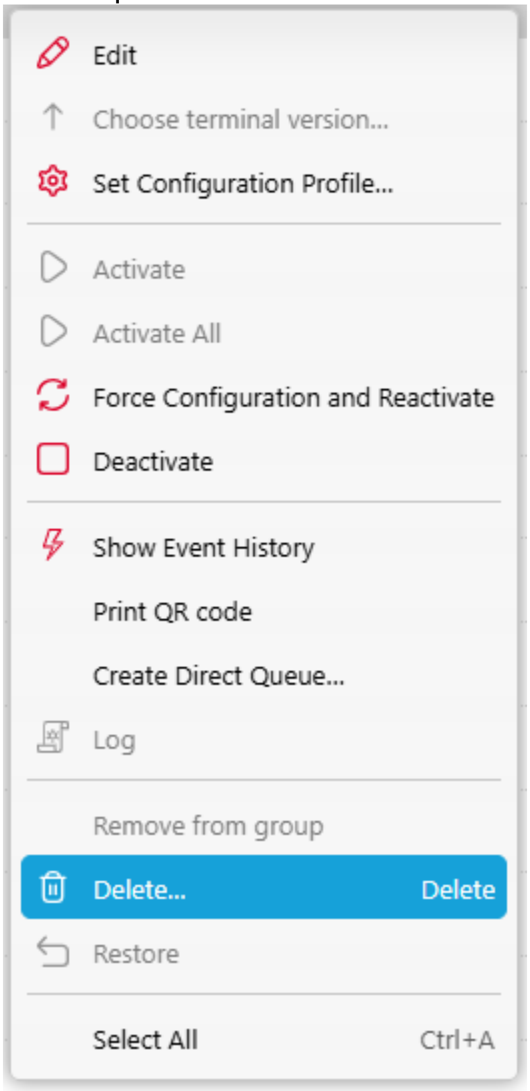
If you delete a printing device, you will not be able to use it, but its data will be permanently stored in the MyQ database.

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.

8.6.1 Deleting printers

To delete selected printing devices:

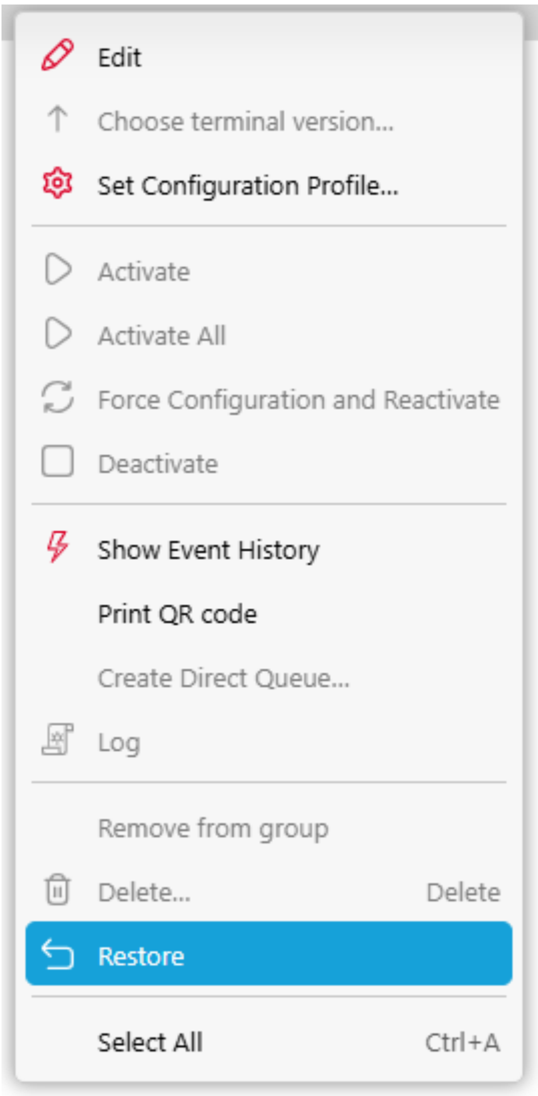
1. Select the printing devices you want to delete from the list on the **Printers** main tab.
2. Right click the device or click **Actions**. The Actions drop-down appears.
3. Click **Delete**. You can find the deleted printing devices under the **Deleted** search option.



8.6.2 Restoring printers

To restore selected printing devices:

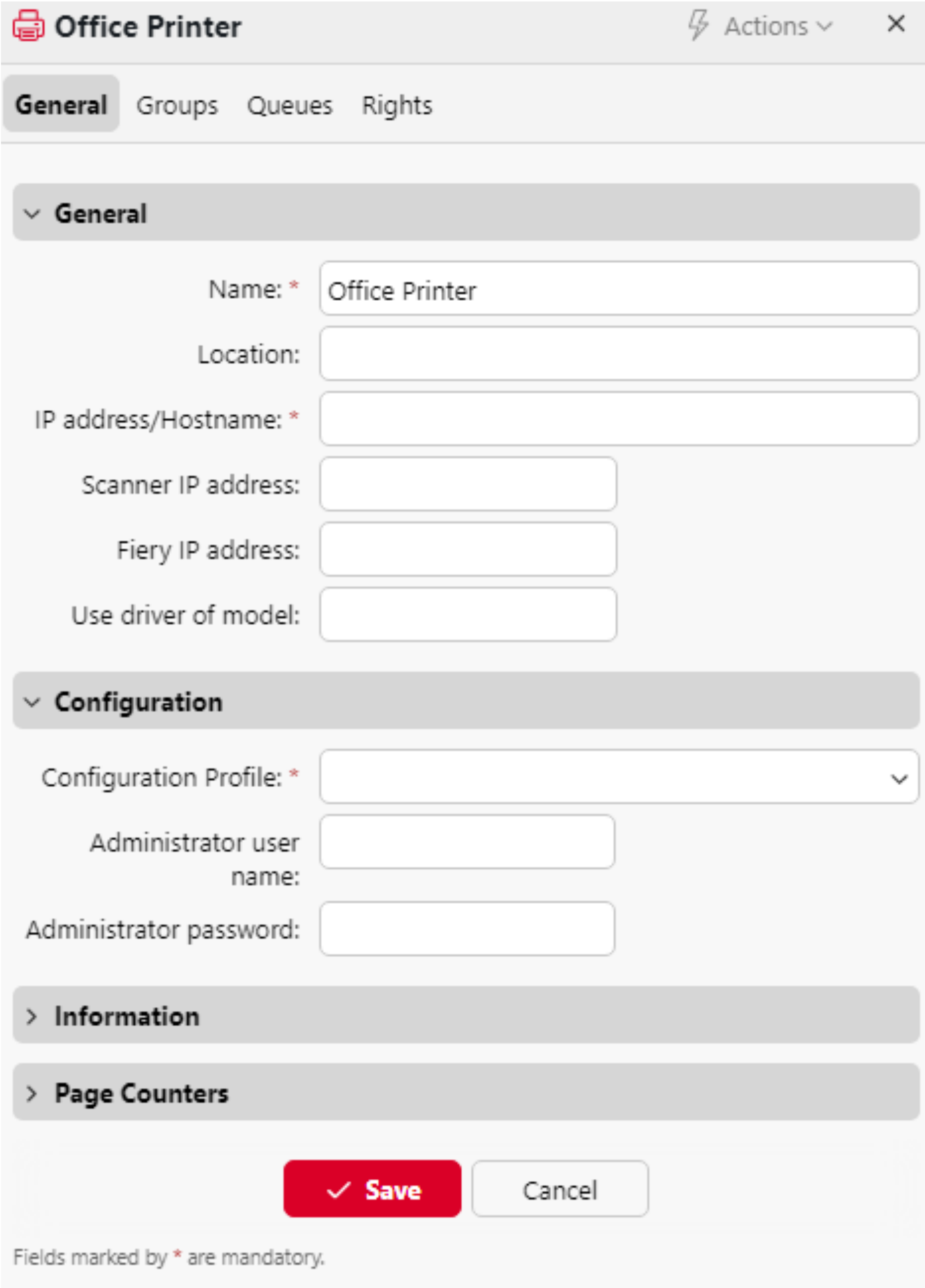
1. On the group tab on the left side of the **Printers** main tab, under **Searches**, select the **Deleted** search option. The list of deleted printing devices appears.
2. On the list, select the printing devices that you want to restore, right click the device or click **Actions**. The Actions drop-down appears.
3. In the drop-down, click **Restore**. The restored printing devices are not active; you have to activate them again.



8.7 Editing 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.



8.7.1 Printer Information and Settings

The settings mentioned below are basic printer settings displayed on each printer's properties panel.

General section

- **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, please contact support@myq-solution.com.

Configuration section

- **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.
- **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 section

- **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 section

- **Black & White Print** - Total amount of B&W pages printed on the device.
- **Color Print** - Total amount of color pages printed on the device.

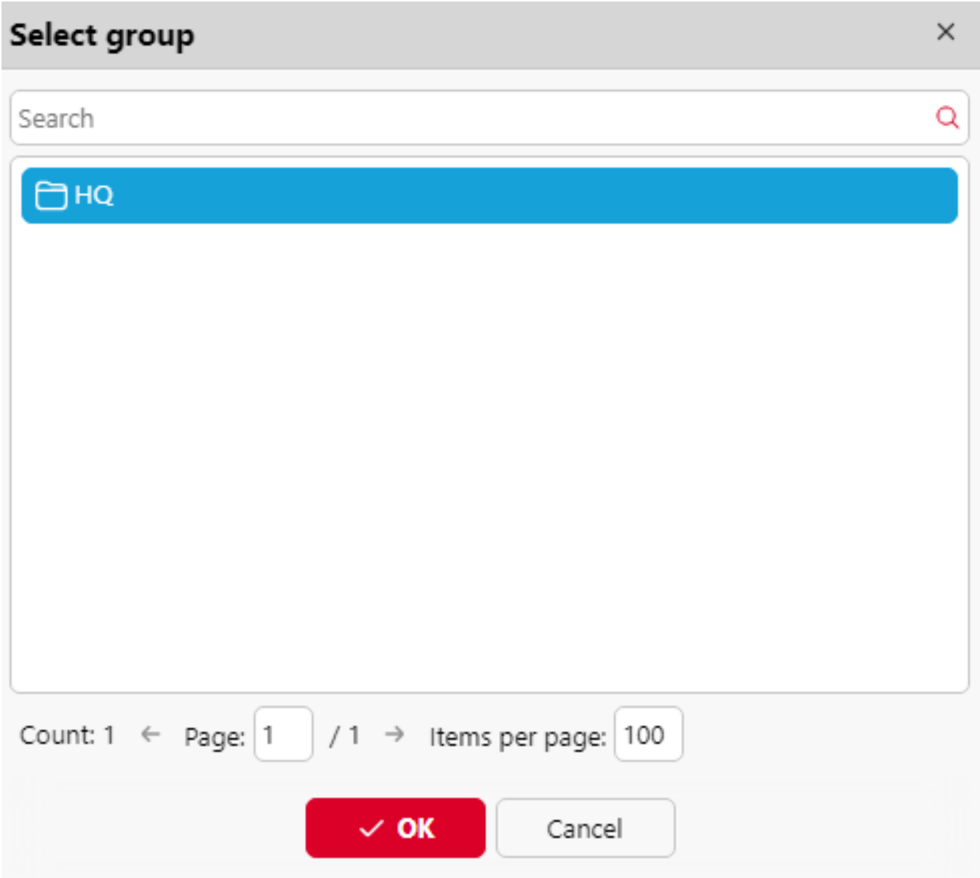
- **Black & White Copy** - Total amount of B&W pages copied on the device.
- **Color Copy** - Total amount of color pages copied on the device.
- **Single color copy** - Total amount of single color pages copied on the device.
- **Scanner** - Total amount of pages scanned on the device.
- **Fax** - Total 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.

8.7.2 Adding/Removing Printers to Groups

To 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.

To remove a printer from a group:

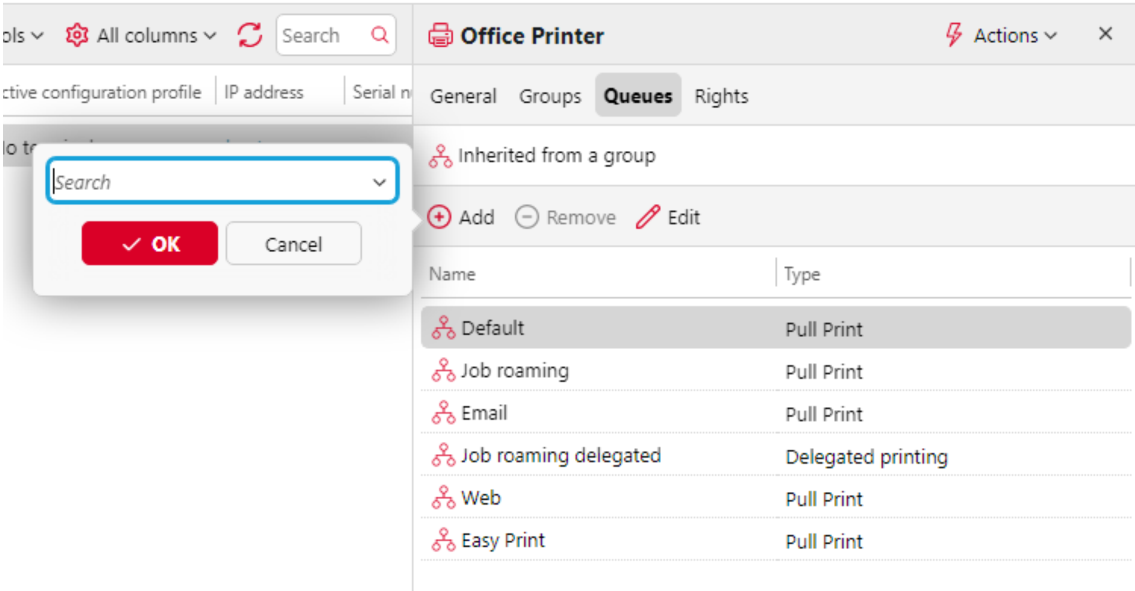
On the bar at the top of the **Groups** tab, click **–Remove**. The group disappears from the **Groups** tab.

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**).

8.7.3 Adding/Removing Printers to 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.

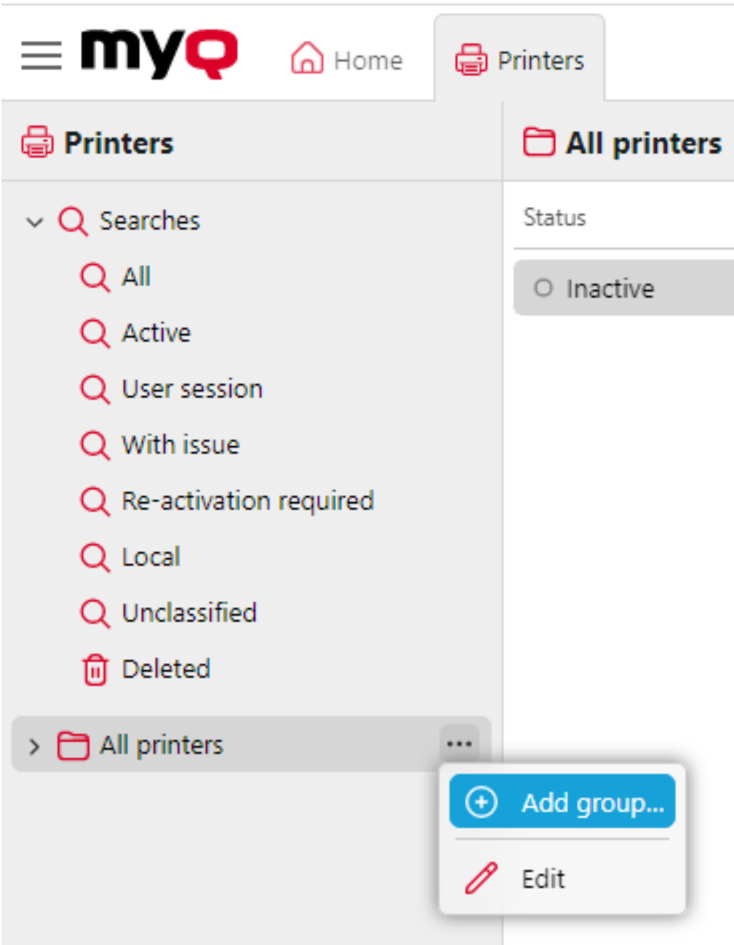
8.8 Printer Groups

All printing devices in MyQ can be divided into groups based on their location, model, vendor, category, etc.

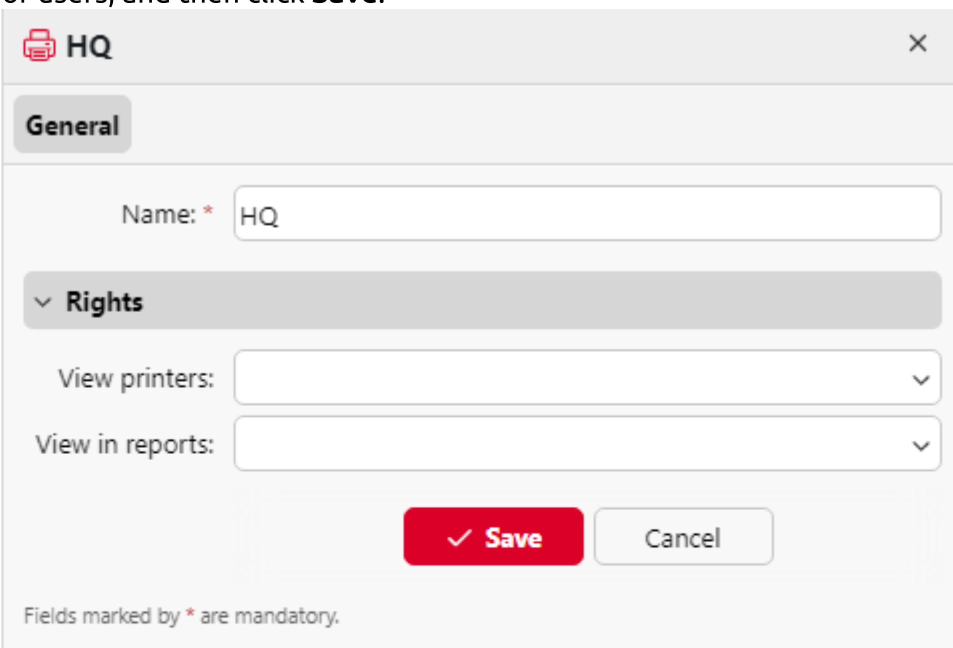
On the **Printers** main tab, you can create new groups of printing devices. There are a number of MyQ functions where groups are used, for example, they can be assigned to particular print queues (see Queues), users can be given rights and restrictions concerning particular groups (see Rights) and reports can be set about particular groups only (see Reports).

8.8.1 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).

8.8.2 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.

8.9 Exporting and Importing Printers

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

8.9.1 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.

8.9.2 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.

8.9.3 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
- 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)

Import

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

- PRINTER ADMIN
- PRINTER ADMIN PASSWORD

8.10 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. See Activating and deactivating printing devices for more information.

8.11 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 (10.2) MyQ Desktop Client .

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.

8.11.1 Accounting on local printers

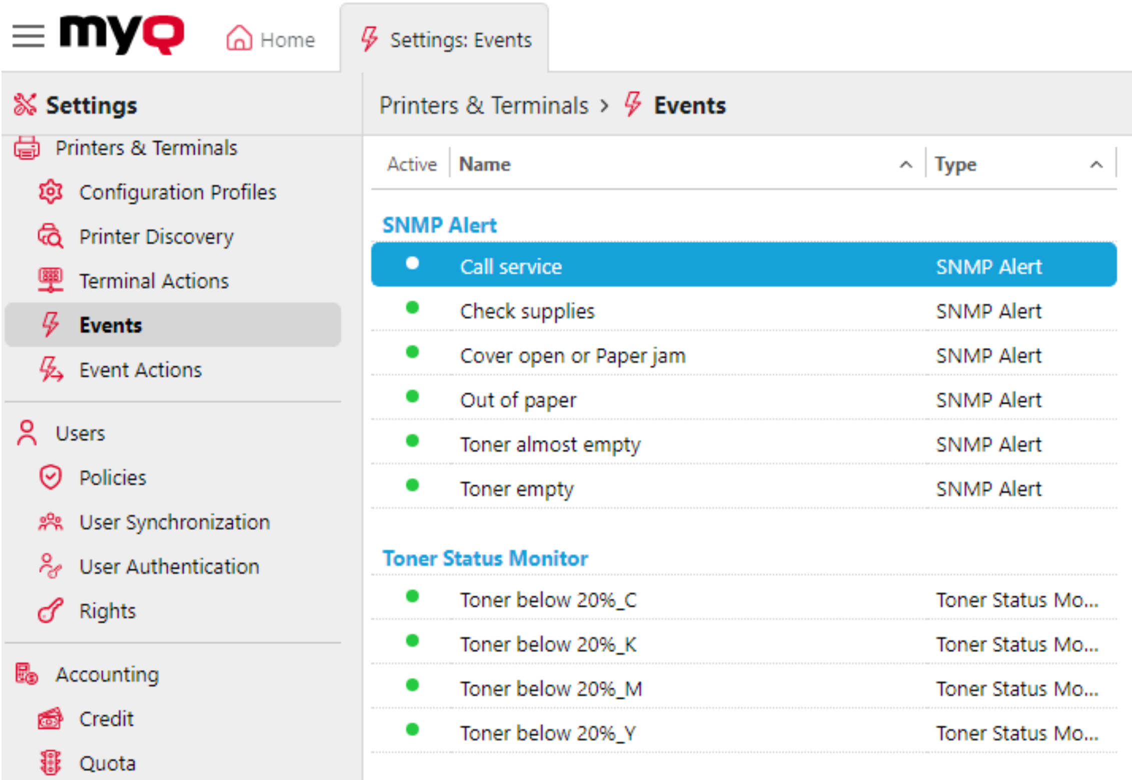
After a print job is sent to one of the local printing devices, the number of pages and other information about the print job are saved to the MyQ Desktop Client folder of the particular registry file. Once the connection with the MyQ server is established, all the information is automatically transferred 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**.

8.12 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.



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.

8.12.1 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 toner level to be monitored

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.

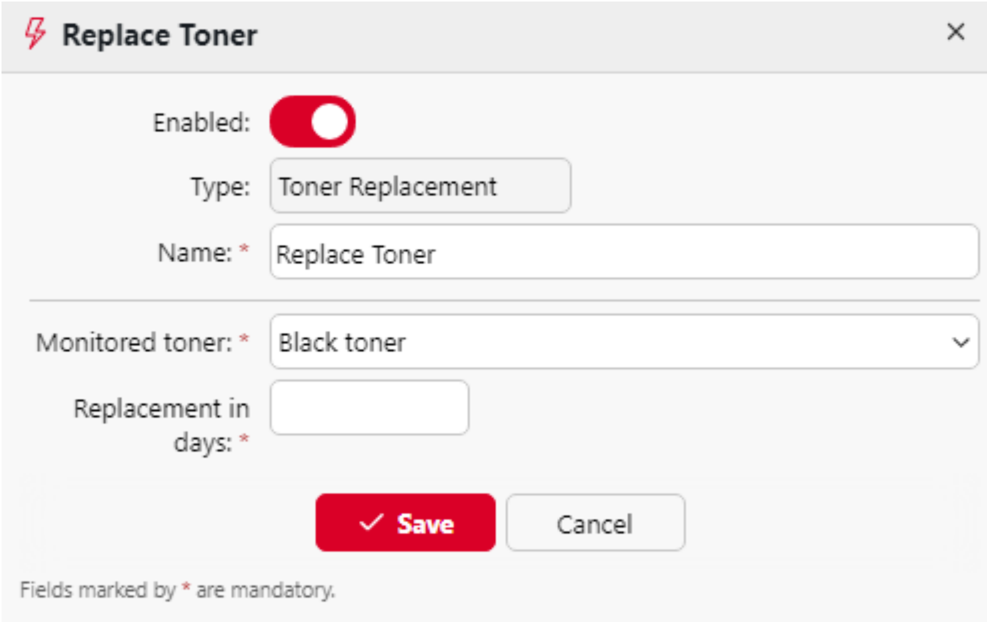
Creating new events

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

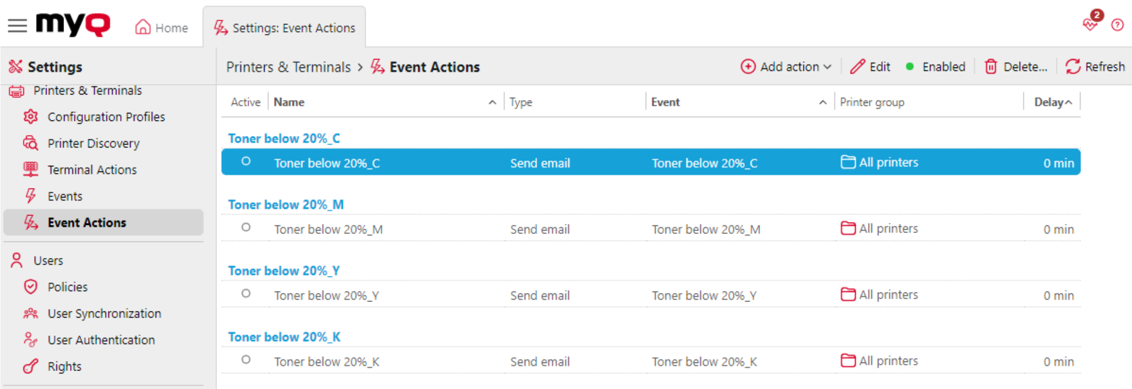
A properties panel opens to the right side of the screen. Fill in the mandatory information and click **Save**.



8.12.2 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.



To 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**.

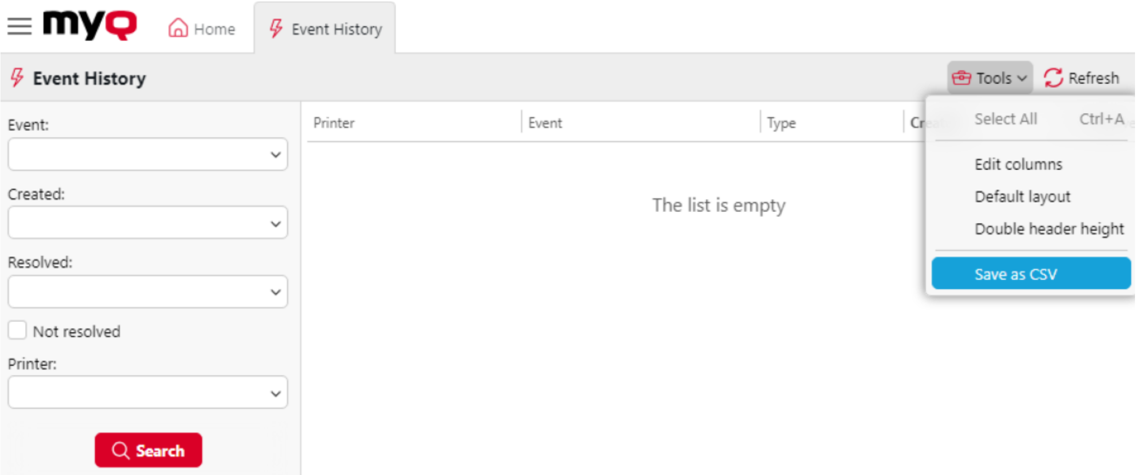
Setting event actions

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.

8.13 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).

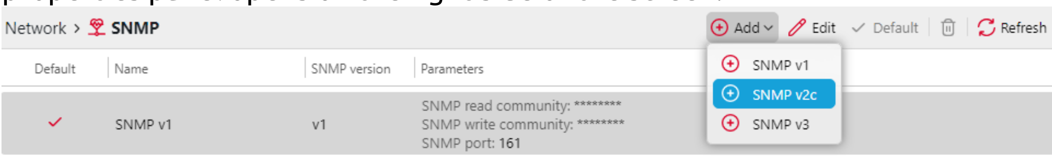
8.13.1 Adding and editing SNMP v1 and v2c profiles

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:

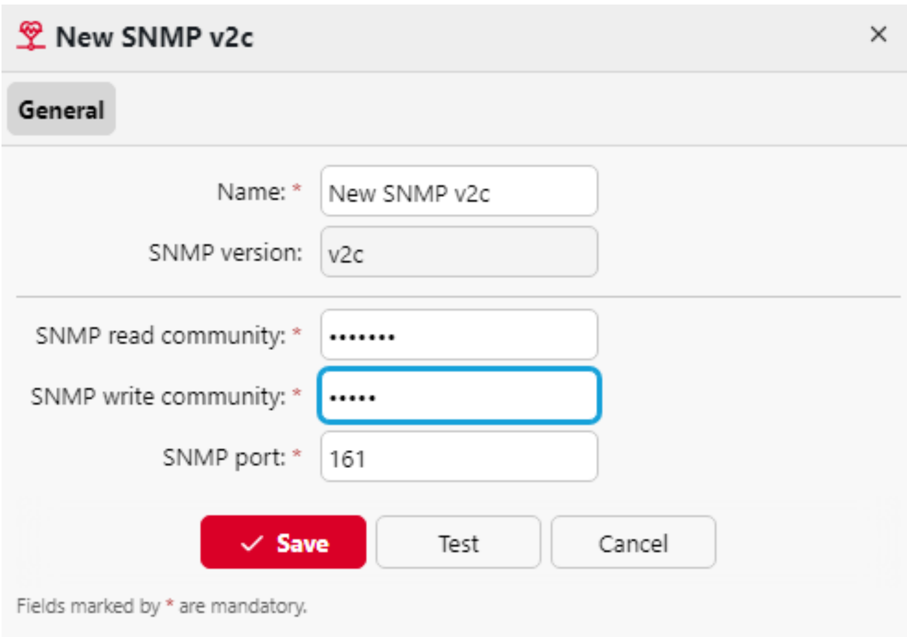
1. On the MyQ Web Admin Interface, open the **SNMP** settings tab (**MyQ, Settings, SNMP**).
2. On the bar at the top of the **SNMP** tab, click **+Add SNMP profile**, and then click **+SNMP v1** or **+SNMP v2c** on the shortcut menu. The new SNMP profile properties panel opens on the right side of the 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.



8.13.2 Adding and editing SNMP v3 profiles

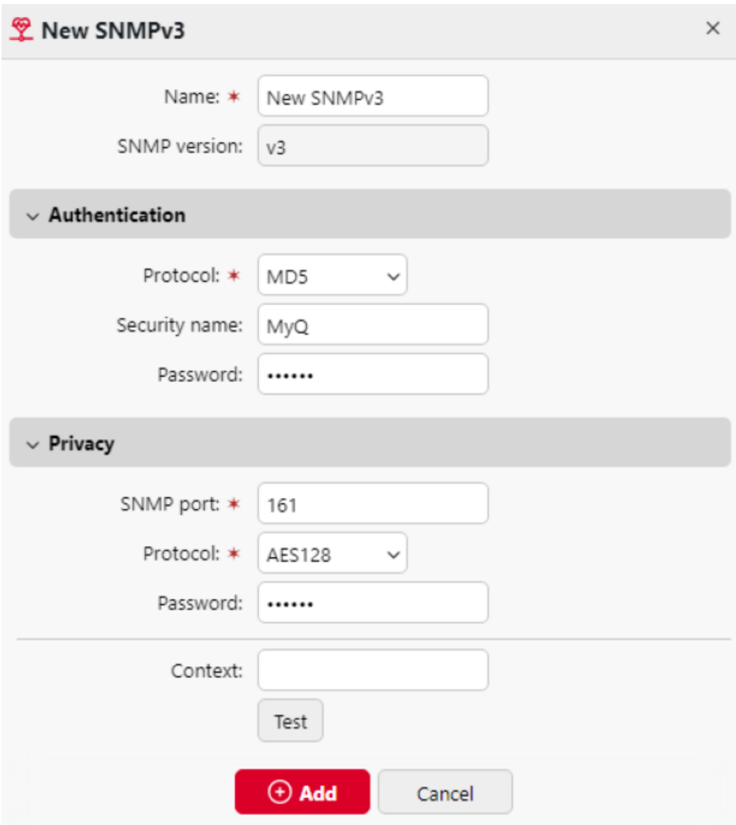
The SNMP v3 protocol contains additional elements of security, such as authentication and encryption. Each of these elements is set on the printing device and needs to be accordingly set in MyQ.

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.

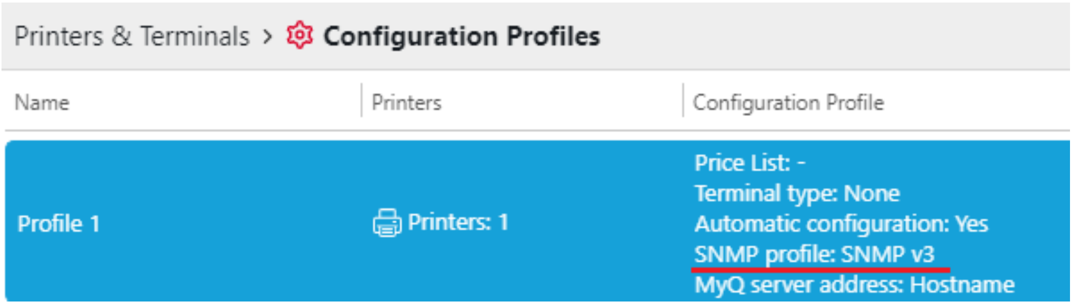
To open and edit a SNMP v3 profile:

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.



8.13.3 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.



9 Users

This topic discusses one of the key MyQ functions: setting and management of users (user accounts). It covers the following subjects:

- Overview, registration, adding, importing, synchronizing and deleting users: List of users, Automatic user registration, Adding and deleting users manually.
- PIN generation: Generating PIN.
- Individual user settings: Editing user accounts, Enable user profile editing, User Groups, Exporting users.
- Job policies concerning users and printers: Policies and Effective Policies for specific users.
- Special administrative rights: Rights.
- Securing the personal data of MyQ users, anonymization: Securing MyQ users personal data.
- User synchronization from LDAP, CSV files, or Microsoft Entra ID, together with manual and scheduled runs of synchronizations: User import and synchronization.
- User authentication using an LDAP or Radius server: Using External Authentication Servers.
- Identifying the owner of a sent job: Detecting job owners.

9.1 List of Users

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

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.

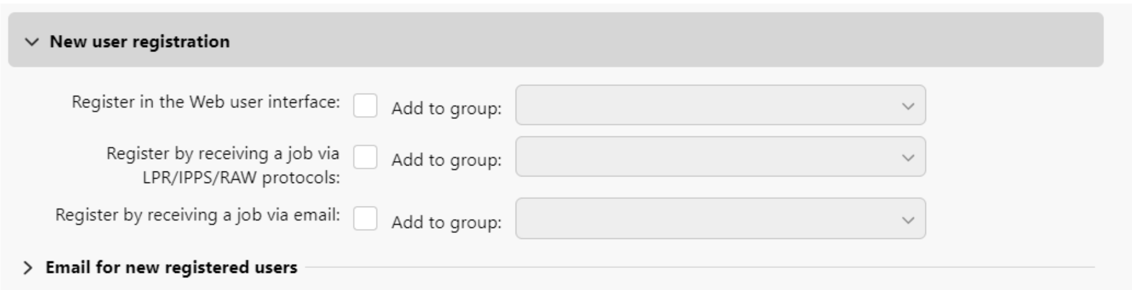
9.2 Automatic User Registration

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.

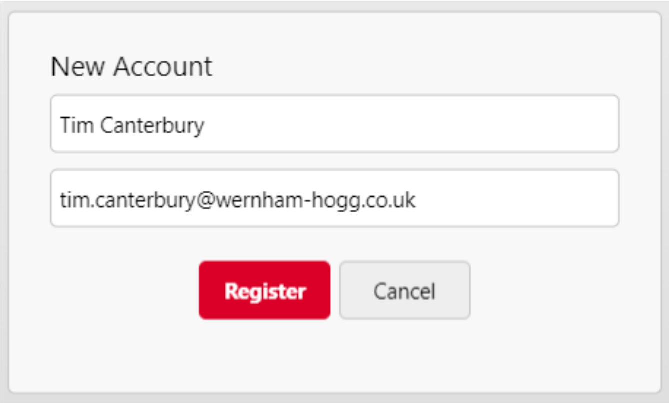
On the **Users** settings tab, under **New user registration**, you can enable and disable these options, and for each option, you can select one or more groups where the registered users will be added to.



9.2.1 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.

9.2.2 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.

9.2.3 Register by receiving a job via email

With this option selected, users can register themselves by sending an email with an attached printable document. For more information about sending print jobs via email, see Printing from email and from the MyQ Web UI.

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.

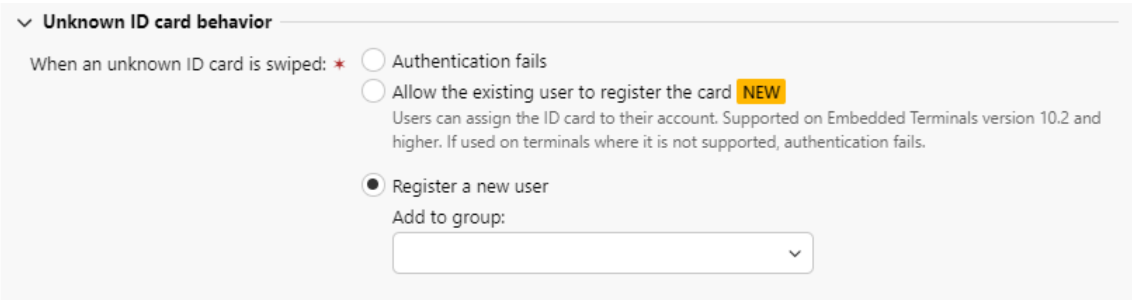
The values of the **%pin%**, **%username%** and the **%realname%** parameters are the user's PIN, user name and real name.
By clicking **Revert values**, you can reset the email body to the default.

9.2.4 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.

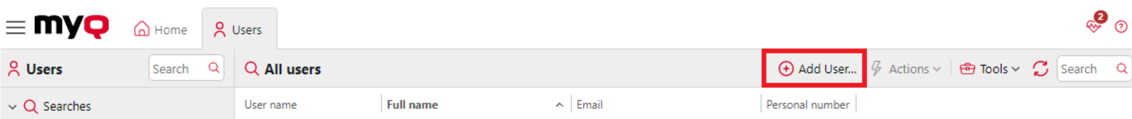


9.3 Adding and Deleting Users Manually

9.3.1 Adding Users

To manually add a new user, follow these steps:

1. On the **Users** main tab, click **+Add User**. The properties panel of the new user opens on the right side of the screen.
2. On the panel, enter the username and full name of the user, and eventually set other data of the user account (see User information and settings), and then click **Save**.



9.3.2 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.

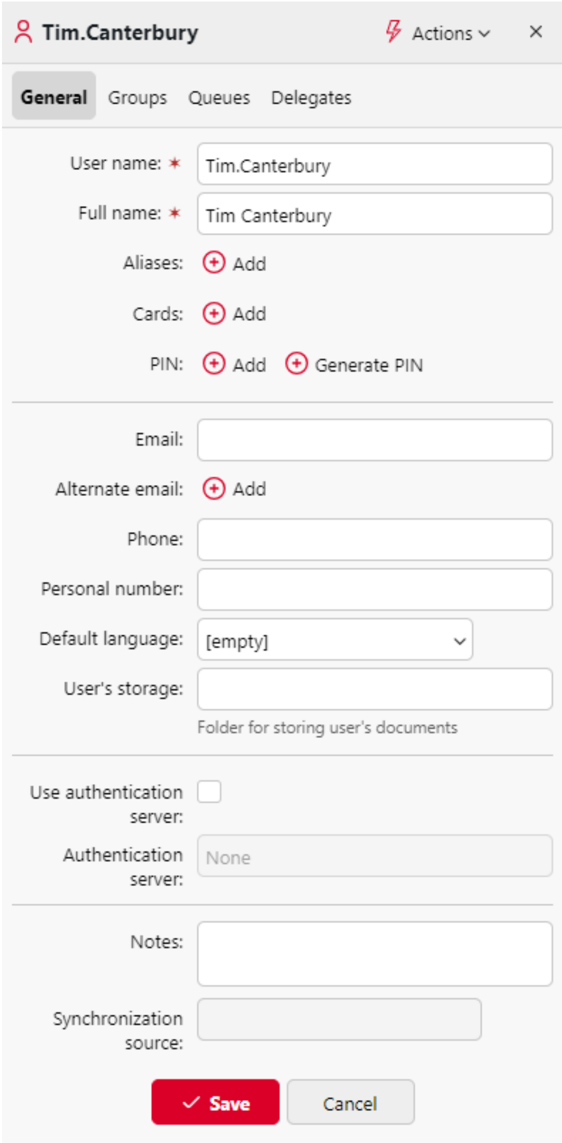
Restoring users

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**.

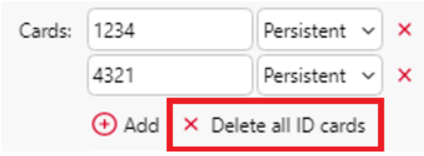
9.4 Editing User Accounts

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 four tabs: **General**, **Groups**, **Queues**, and **Delegates**. If Credit accounting is enabled for the user, the **Credit** tab is also available.

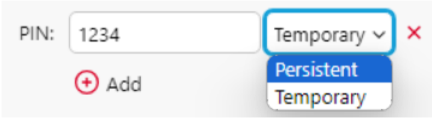


9.4.1 User Information and Settings

- **User name -** Here you can enter or change the user name. This entry is mandatory. It is unique and is used to identify the user. It is compared to the parameter obtained from the **User detection method**. For more information, see User detection methods.
- **Full name -** Here you can enter or change the user's full name. This entry is mandatory.
- **Alias -** In addition to their user name, each user can have a number of aliases. MyQ treats the aliases as alternative user names.
- **Card -** Here you can set the number of the user's identification card. If the **Enable deleting all ID cards** option is enabled in **MyQ**, **Settings**, **Users**, the **Delete all ID cards** button is available here.



- **PIN** - Here you can manually create or automatically generate new PIN codes for the user and remove existing ones. An unlimited number of PINs can be added. The PINs can be either *Persistent* or *Temporary*. For security reasons we recommend automatically generating PINs.

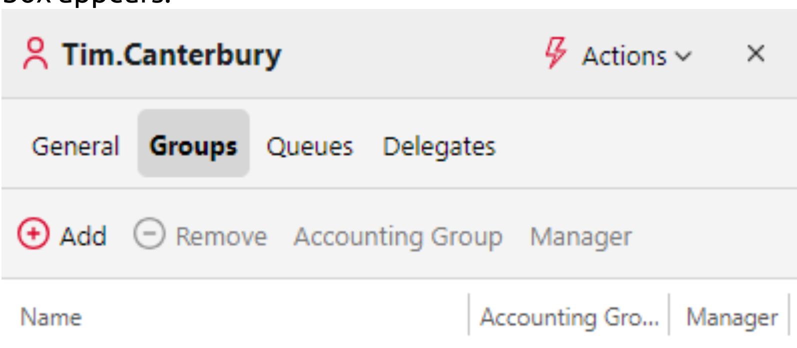


- **Email** - Here you can enter or change the user's email.
- **Alternate email** - Here you can add alternate email addresses for the user to be used as a scan destination.
- **Phone** - Here you can set the user’s phone number
- **Personal number** - The personal number can be used as the user ID in MyQ. The primary ID is the **user name** property.
- **Default language** - Here you can select the language of the user's sessions on MyQ embedded terminals.
- **User's storage** - Here you can set the folder, where scanned documents are saved. For more information, see Scan to Me.
- **Use authentication server** - If you select this option, an LDAP server is used for the user authentication. The user uses their LDAP credentials to authenticate to MyQ instead of having a password set in MyQ. Select the domain for the authentication on the setting below.
- **Authentication server** - Here you can select the server for user authentication.

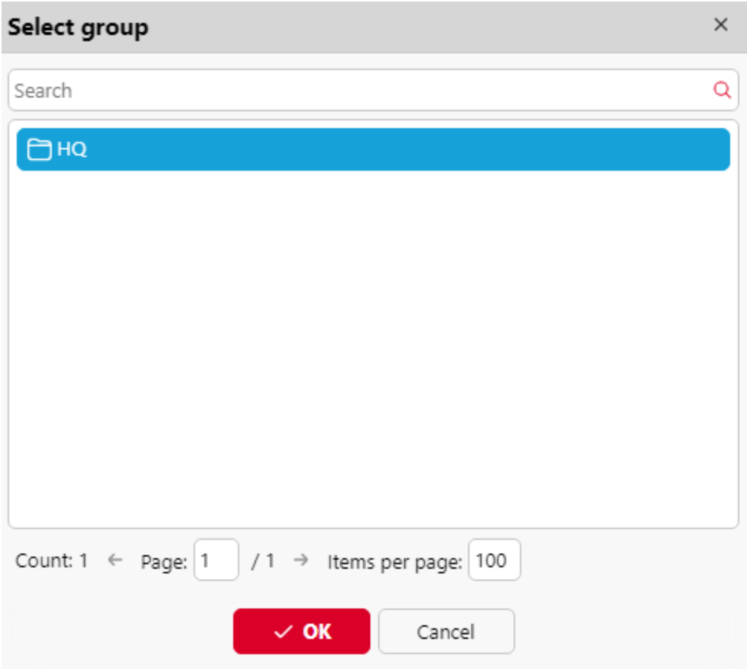
9.4.2 Adding Users to and Deleting Users from Groups

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 (see 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**.

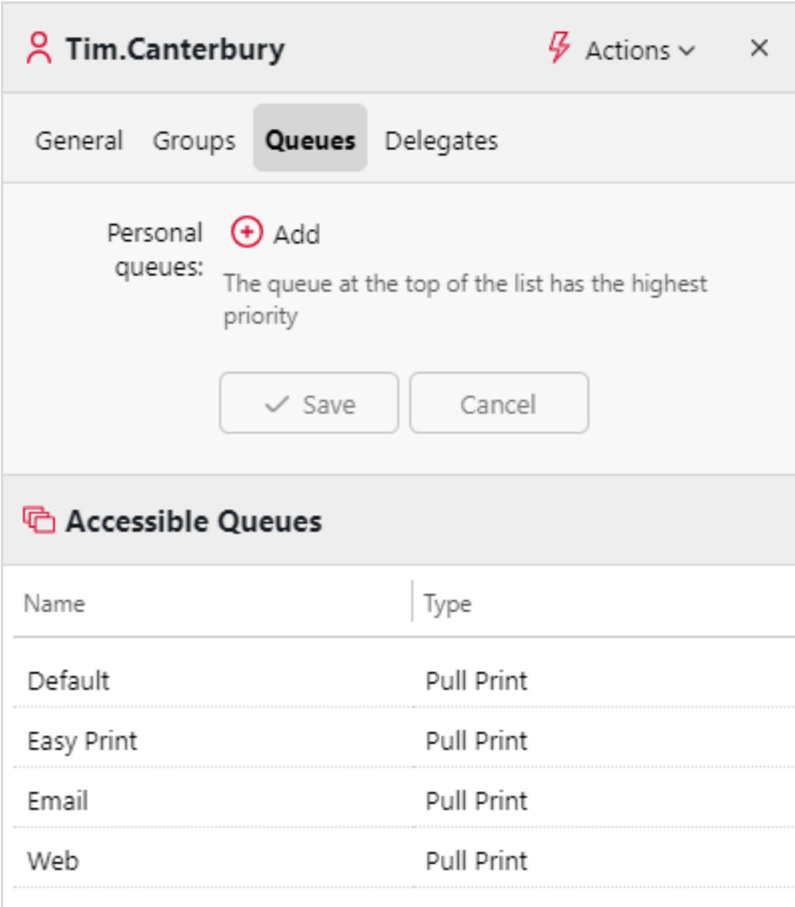
To remove a user from a group:

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.

9.4.3 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.



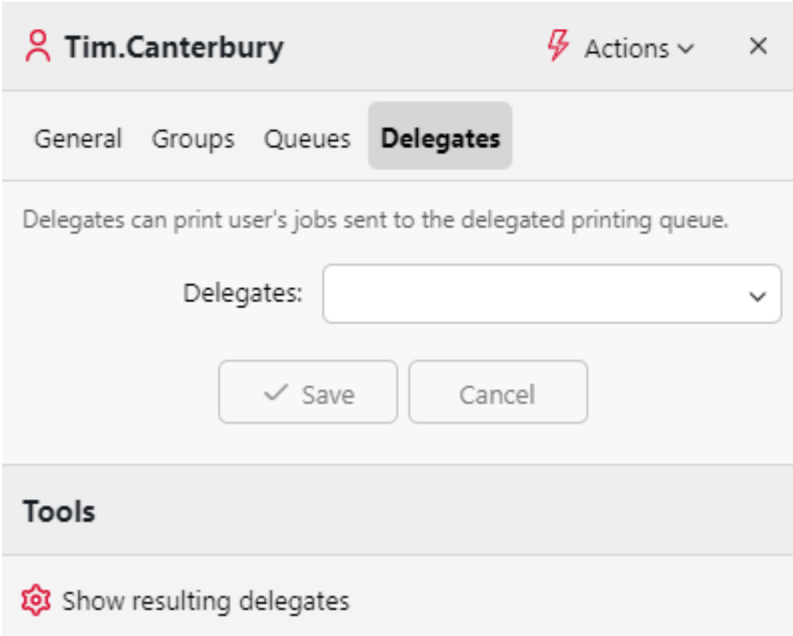
9.4.4 Selecting User Delegates

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*). For more information about the delegate printing feature, see Delegated printing.

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

To select delegates:

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

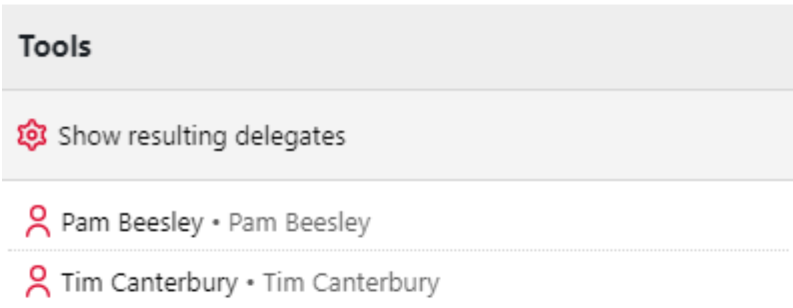


To deselect delegates:

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

Show resulting delegates

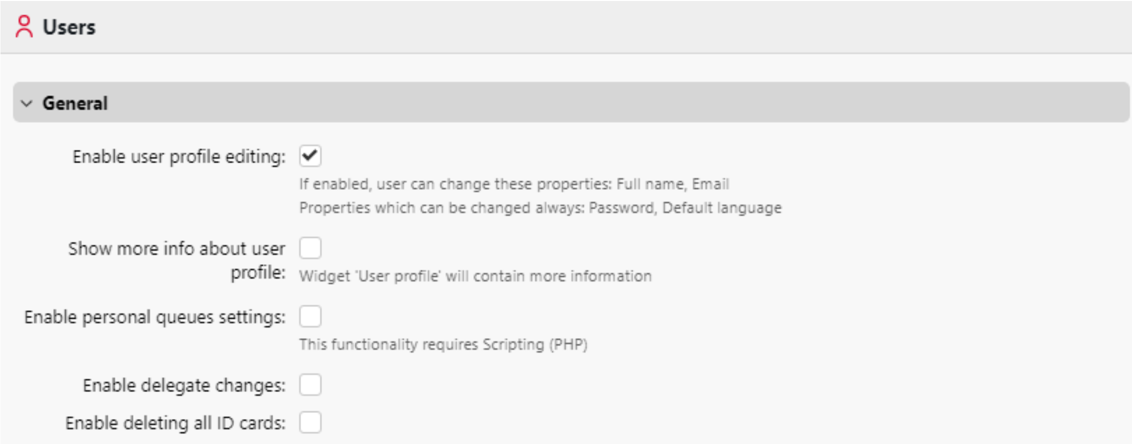
You can use the **Show resulting delegates** tool to show you each delegate for a specified user. This is helpful if you have added one or more user groups as delegates for a user, and will show each user who is now a delegate as a result of adding their user group.



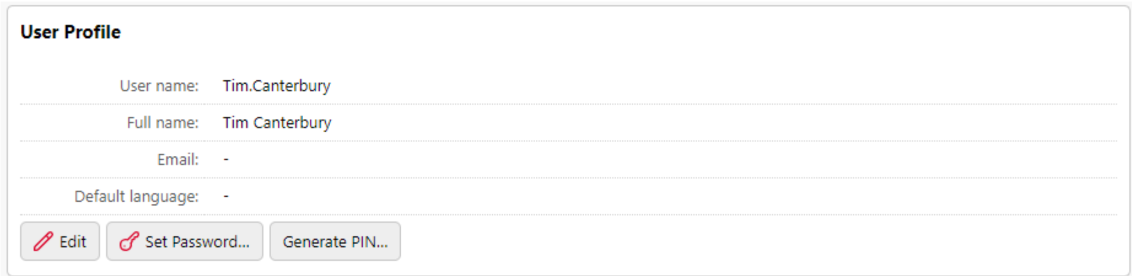
9.5 Enable User Profile Editing

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.



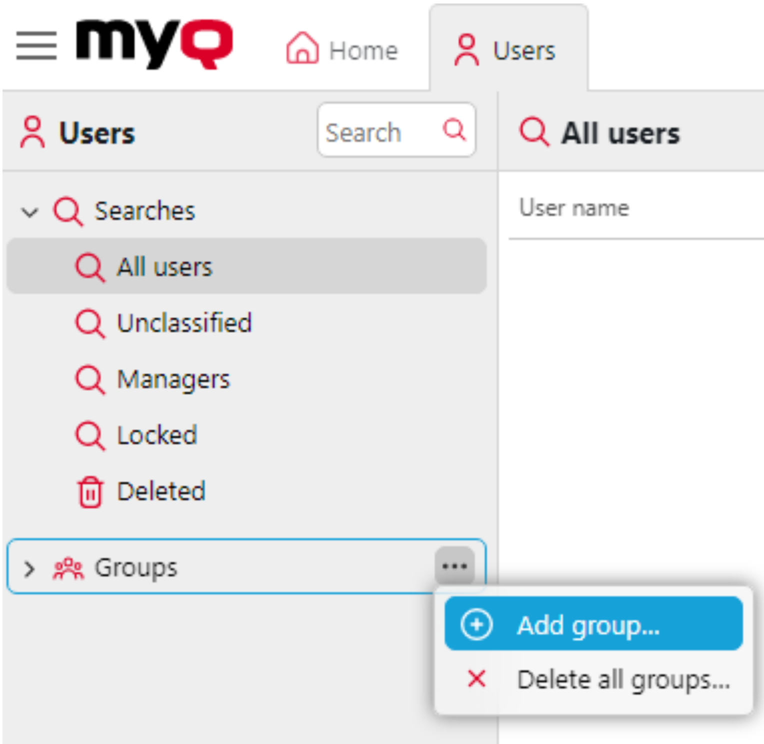
9.6 User Groups

On the **Users** main tab, you can create new user groups. In MyQ, different groups of users can be given different access rights to print queues (see Queues), print functions, such as color printing or scanning (see Policies), and reports (see Reports).

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).

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**.

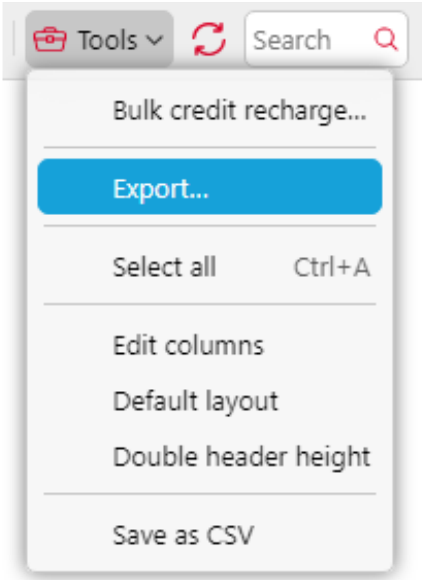
9.7 Exporting Users

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**.

9.8 Security 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.

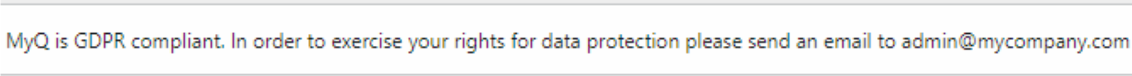
9.8.1 Providing users with their personal data

On their MyQ Web accounts, MyQ users can see the **User profile** widget with the personal information stored in MyQ.

On their Web account, MyQ users can generate reports related to their activity within MyQ, such as printing, copying and scanning to see what information is available in these reports (see 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 (see Personalization).



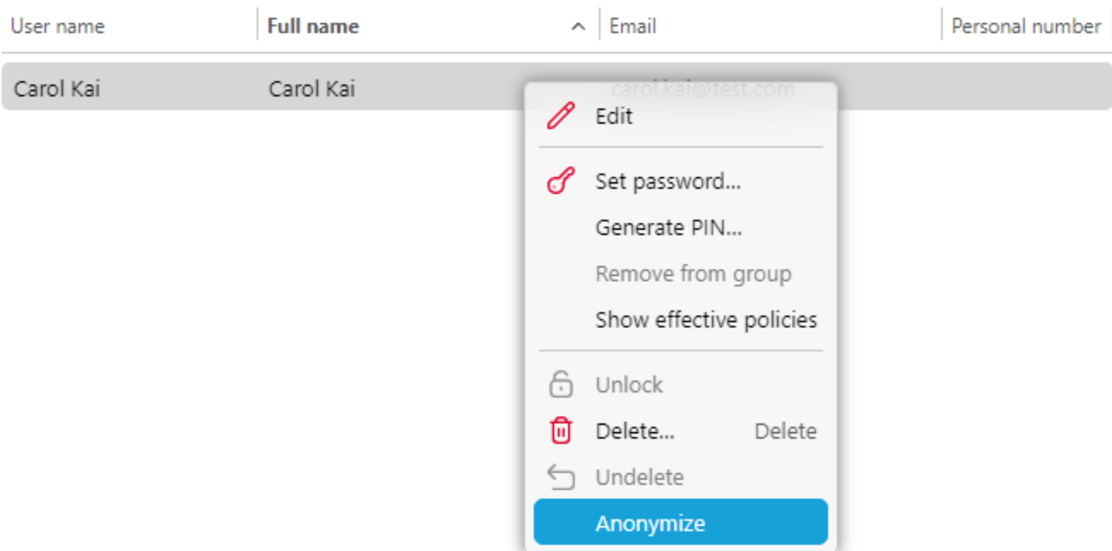
9.8.2 Anonymizing users

After the anonymization, the user is completely removed from the system and replaced by a randomly generated name in all of the relevant MyQ reports.

After a user is anonymized, all of their personal data (including username and email) are permanently erased from the system and cannot be retrieved.

To anonymize a user:

On the **Users** main tab of the MyQ Web Interface, select the users that you want to anonymize, then click **Actions** (or select the users, and then right-click any of them), and finally click **Anonymize**.



9.9 User Import and Synchronization

User synchronization is a method of synchronizing user related data in the MyQ database with data in external sources, such as LDAP servers or CSV files. Importing new users is an optional part of the synchronization process. Within the synchronization setup, you can activate or deactivate the new users import; if you deactivate it, MyQ only updates accounts of users that already are in its database.

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

- User synchronization from LDAP servers
- User synchronization from Microsoft Entra ID with Microsoft Graph
- User synchronization from CSV files
- User synchronization from Azure AD with SLDAP
- User synchronization from Google Workspace
- Using external authentication servers
- Manual and scheduled synchronization run

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

9.9.1 User Properties in MyQ

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

- **Custom Properties**: attributes can be used to map any other relevant attributes that exist in your synchronization source.

> The properties listed above can be used in certain reports.

9.9.2 User Synchronization from LDAP Servers

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

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

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

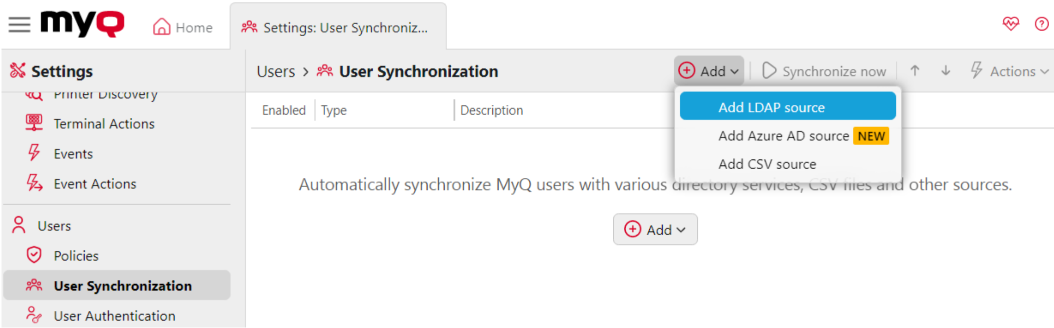
> OpenLDAP, with its default settings, limits the number of returned entries and the maximum total time for a query. The default size limit is 500 entries and the default time limit is one hour. In case of a larger customer installation with OpenLDAP, you must adjust these limits appropriately in the OpenLDAP settings, otherwise the user sync will give incomplete results.
> For more details see: https://www.openldap.org/doc/admin24/limits.html

Creating an LDAP Synchronization

Before creating the synchronization, you have to add the LDAP server to MyQ. You do this on the Authentication Servers settings tab. Set **Security** to *SSL* and the server port to *636*.

To create a new LDAP synchronization:

1. Add the new synchronization:
   On the **User Synchronization** settings tab, click **+Add**. A drop-down box appears.

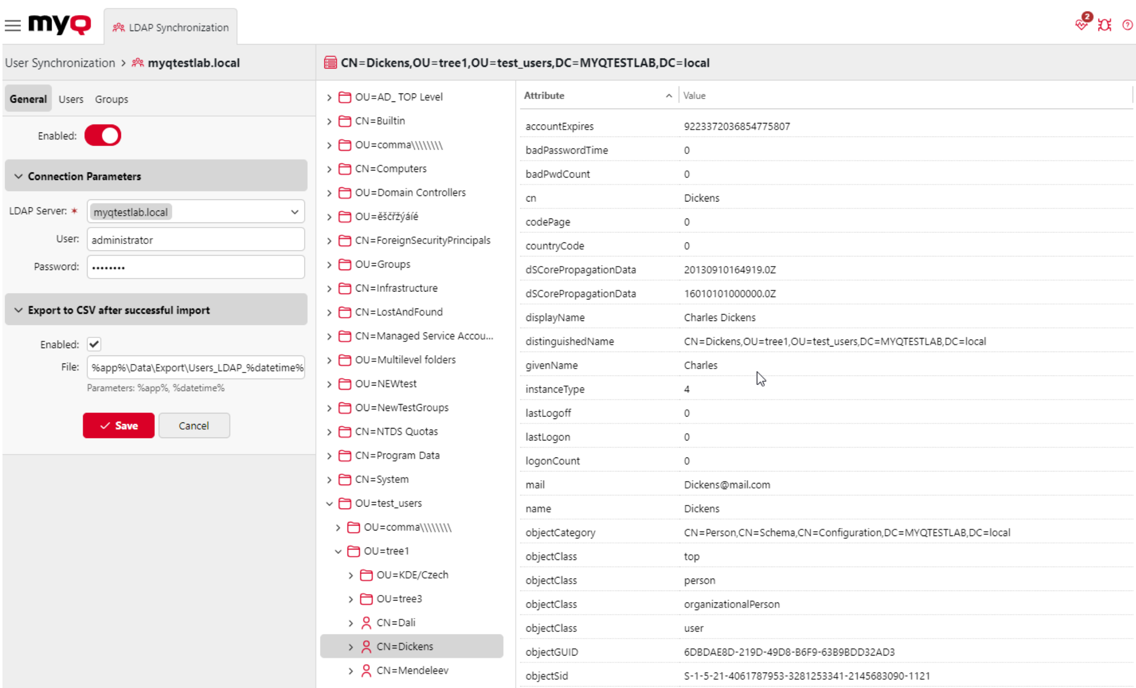


In the drop-down, click **Add LDAP source**. The LDAP synchronization properties panel opens. On the panel, you can set up the synchronization.

2. Set up the synchronization on the LDAP synchronization properties panel: Set up the synchronization on all three tabs on the LDAP synchronization properties panel. On each of the tabs, click **Save** after changing the settings. For more information, see Setting up the LDAP synchronization.
3. Return to the **User Synchronization** settings tab: The new LDAP synchronization is displayed on the list of synchronizations on the **User Synchronization** settings tab.

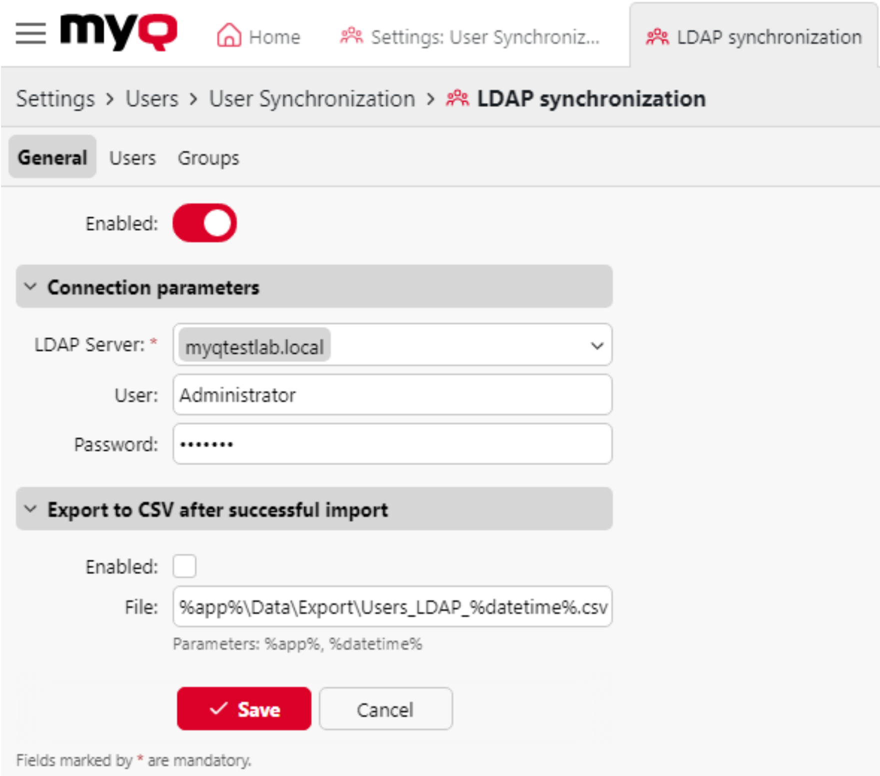
Setting up an LDAP Synchronization

The setup consists of three parts: creating the synchronization on the **General** tab, setting import of users on the **Users** tab and setting import of groups on the **Groups** tab. You can swap between these tabs on the bar at the upper-left corner of the LDAP synchronization properties panel.



General Tab

On the **General** tab, set the general properties of the synchronization: enable or disable the synchronization, select the LDAP server domain, enter user name and password for access to the server, eventually select to export the imported users to a CSV file. See the list below for a description of individual settings.



- **Enabled**: Here you can enable or disable the synchronization.
- **LDAP Server**: Here you can select the domain that you want to synchronize from.
- **User**: Enter the username for access to the LDAP domain server.
- **Password**: Enter the password for access to the LDAP domain server.
- **Enabled**: If you enable the **Export to CSV after successful import** option, MyQ creates a CSV file with the imported users after the synchronization.
- **File**: Select the folder where you want to save the created file.

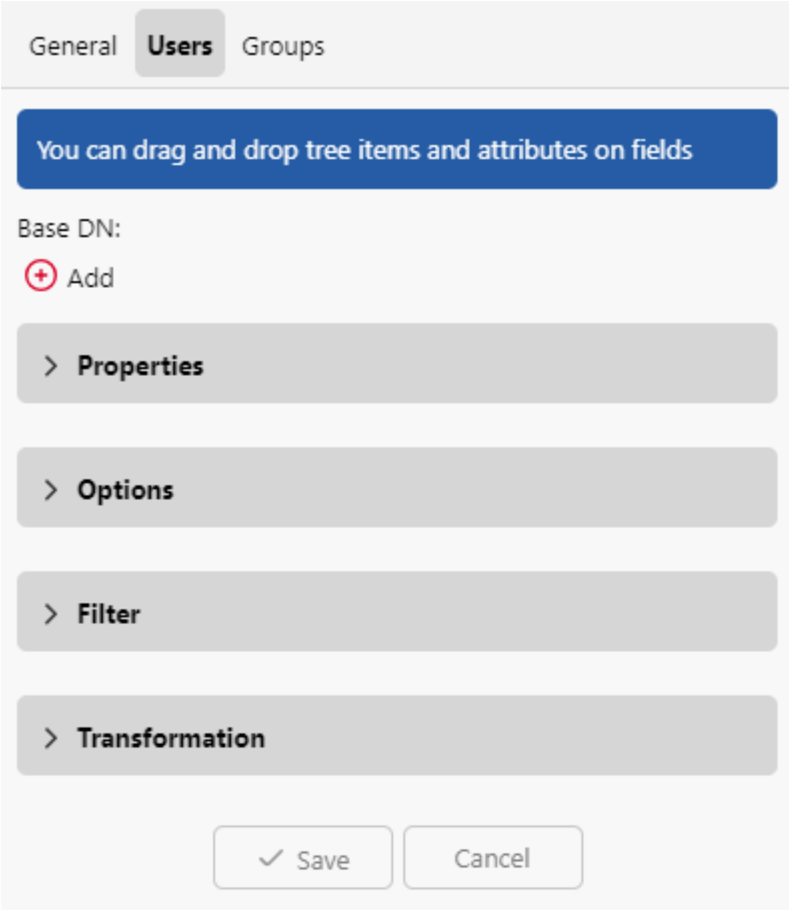
After you correctly set the connection parameters (LDAP server, user and password) and save the settings, the LDAP browser opens on the right side of the screen.

> In the **User** setting, a sub-domain user account with enough rights can also be used for authentication, but the sub-domain has to be specified in the username.

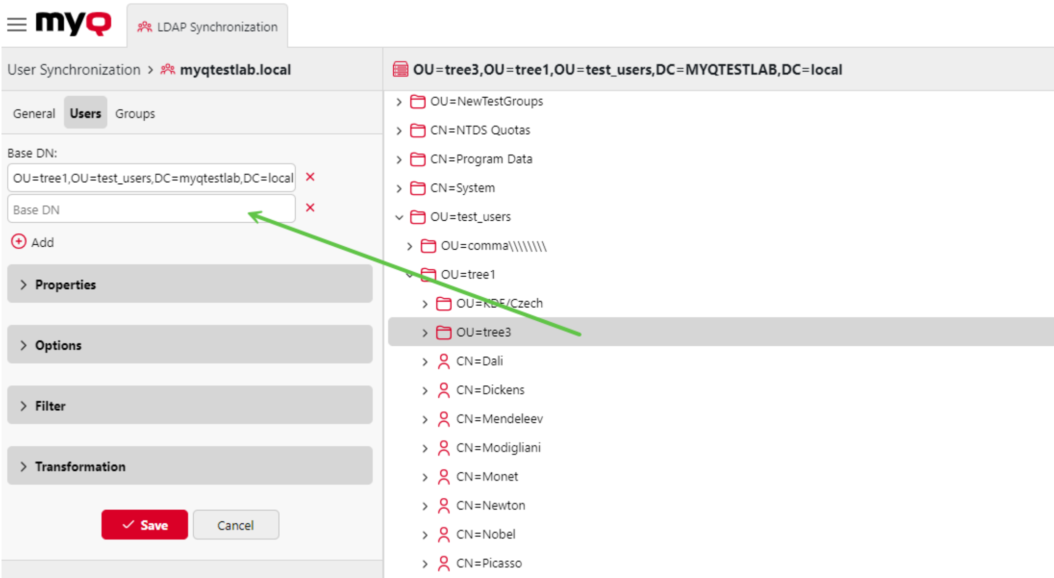
For example, the user *Administrator* connects to the *testAD.local* LDAP server, but their account is in the *cz.testAD.local* sub-domain. For successful authentication, the filled in username should be: *Administrator@cz.testAD.local*

Users Tab

On the **Users** tab, pick one or more base DNs (distinguished names) from which you import the users. In addition, you can assign user attributes from the LDAP server to user properties in MyQ and select additional options concerning the synchronization.



- **Base DN**: Here you can pick the base domain or domains from which you import users. Click **+Add** to add a text box for the new base DN, and then drag a group from the database browser and drop it in the text box. You can add multiple domains this way.



- **Properties**: These are the properties of every individual user. MyQ will automatically find and assign the user's **SAM account name** to **user name**, **cn** to **full name** and **mail** to **Email** (this applies to Active directory and OpenLDAP only). The user name property is the only one that cannot be changed. To assign an attribute to a property, write the name of the attribute in the property text box or drag it from the attributes of any individual user and drop it in the text box. The following properties support adding multiple values to them, separated by a semicolon (;):
  - **Alias**
  - **PIN**
  - **Card**

For example, in the **Alias** property, you could add *alias1;alias2;alias3*.

The AD attribute name should not contain the semicolon (;) character. If a semicolon is part of the attribute's name, that attribute will not be synchronized in MyQ.

For the **Card** and **PIN** properties, the administrator can choose one of the following options:

1. **Do not synchronize:** This option will skip the synchronization of these values.
2. **Full synchronization:** This option will replace the existing values with the new values from LDAP, irrespective of whether the new value is empty or not.
3. **Synchronize if not empty:** This option will replace the existing values only if the new values from LDAP are not empty. It won't remove the existing values if the corresponding value in LDAP is empty.
4. **Add new:** This option will update the existing values by adding new values from LDAP, without replacing the existing ones.

For assigning default languages to users, you have to use an attribute from the LDAP server that has the language abbreviations as its values. For example, you can create and use an attribute called **lang** with the values *en* for English, *hr* for Croatian, etc. The list of the abbreviations used in MyQ can be found here.

- **Options**: For a description of the common synchronization options, see User information and settings. The basic options that are common for both the synchronization from LDAP servers and for synchronization from CSV files are:
    - **Deactivate missing users**: If you select this option, MyQ deletes users that are imported from the current synchronization source and that are not in the source anymore. To delete users that were added from different sources, select the **Ignore synchronization source** option together with this option.
    - **Add new users**: If you select this option, MyQ adds new users from the current synchronization source. If you do not select it, MyQ updates the user accounts of the users who are already in MyQ, but does not add any new users.
    - **Convert user name to lowercase**: Unlike some other systems that do not differ between two words with the same letters but different cases (such as "Pear", "pear"), MyQ is case sensitive. You can use the **Convert user name to lowercase** option to prevent creating multiple accounts for one user.
    - **Use authentication server**: If you select this option and a user logs in by entering their username and password, the credentials are not authenticated against the MyQ database, but instead against an LDAP or Radius server. If you synchronize users via LDAP, the source LDAP server is automatically assigned as
      the authentication server. If you synchronize users via CSV, you can select the authentication server from the list of predefined authentication servers.
    - **Pair by the personal number**: If you select this option, MyQ identifies users by their personal number instead of their user names. This way you can keep track of a single user with different names in different sources or a user whose name has changed for some reason. For example, if this option is activated and a username in LDAP changes from *cat.stevens* to *yusuf.islam*, MyQ does not create a new user account, but recognizes the old user by their personal number.
    - **Ignore synchronization source**: If this option is not selected, MyQ recognizes two users from different synchronization sources as two different entities. This can cause conflicts during synchronizations from multiple sources. If it is selected, MyQ ignores the synchronization sources and treats all users the same, regardless of their synchronization source. For example, if you run a synchronization and MyQ would import/update a user that has been already added from a different synchronization source, it does not update the user. Instead, it shows the message *The name/alias "X" is already used by the user "X"* among the synchronization results. After you select the **Ignore synchronization source** option, the user is updated by the latest synchronization.
      If you select this option together with the **Deactivate missing users** option, all users that were added from different sources and are not in the current synchronization source are deleted during the synchronization.
    - **Append the domain name to the username** (*username@domain.local*): With this option selected, the name of the domain can be retrieved from the MyQ username. The information about the domain may be needed for example, when scanning to users' home folders is used on an embedded terminal.

- **Filter**: You can filter the users import by specifying the values of attributes. Add the conditions in the form of LDAP filter syntax. Users with a different value on this attribute are not accepted and are filtered out of the import. For example:

Search filter	Description
(objectClass=*)	All objects.
(&(objectCategory=person)(objectClass=user)(!(cn=andy)))	All user objects but "andy".
(sn=sm*)	All objects with a surname that starts with "sm".
(&(objectCategory=person)(objectClass=contact)(|(sn=Smith)(sn=Johnson)))	All contacts with a surname equal to "Smith" or "Johnson".

For attributes where the values are strings, such as the cn attribute, you can use the wildcard * symbol to search for substrings.

DN attributes (like memberOf) do not accept wildcard * search and must be searched by the whole string.

If the filter field is left empty, the current default filter for the respective LDAP source type is applied automatically.

Handling Special Characters in Raw LDAP Queries
When constructing raw LDAP queries, it is crucial to properly escape special characters within attribute values to ensure accurate query processing by the LDAP server. Special characters such as backslashes (\), semicolons (;), asterisks (*), parentheses ((and)), and null characters (\0) must be escaped only when they appear in attribute values (e.g. user’s attribute - **email**, **department**, **memberOf**, etc), not when they are part of the LDAP query syntax.
Escaping Rules:

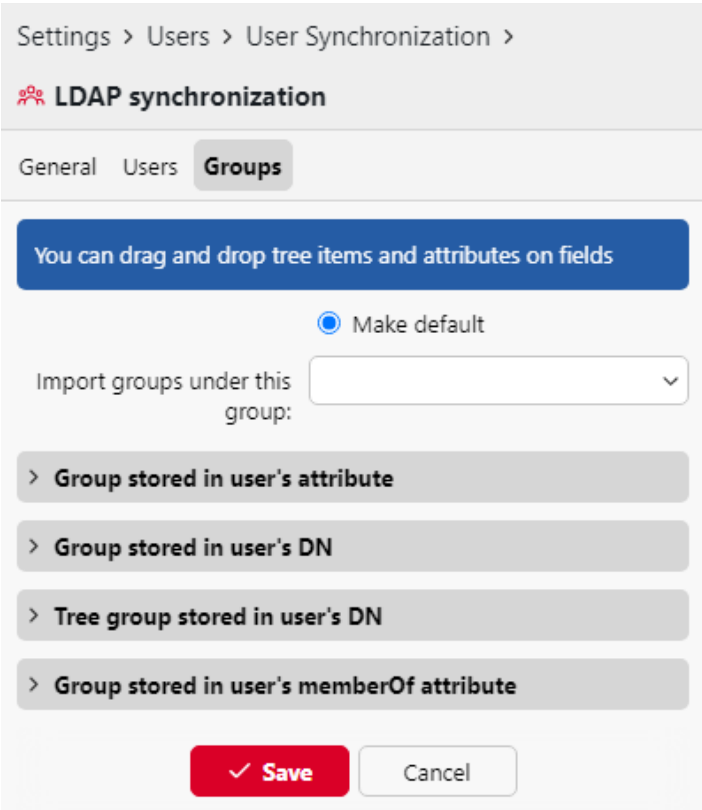
- `\` (backslash) escapes to `\5c`
- `;` (semicolon) escapes to `\3b`

- `*` (asterisk) escapes to `\2a`
- `(` (left parenthesis) escapes to `\28`
- `)` (right parenthesis) escapes to `\29`
- `\0` (null character) escapes to `\00`

- **Transformation**: this feature enables administrators to define regular expressions (RegEx) to transform user data during the synchronization process, details are available here.

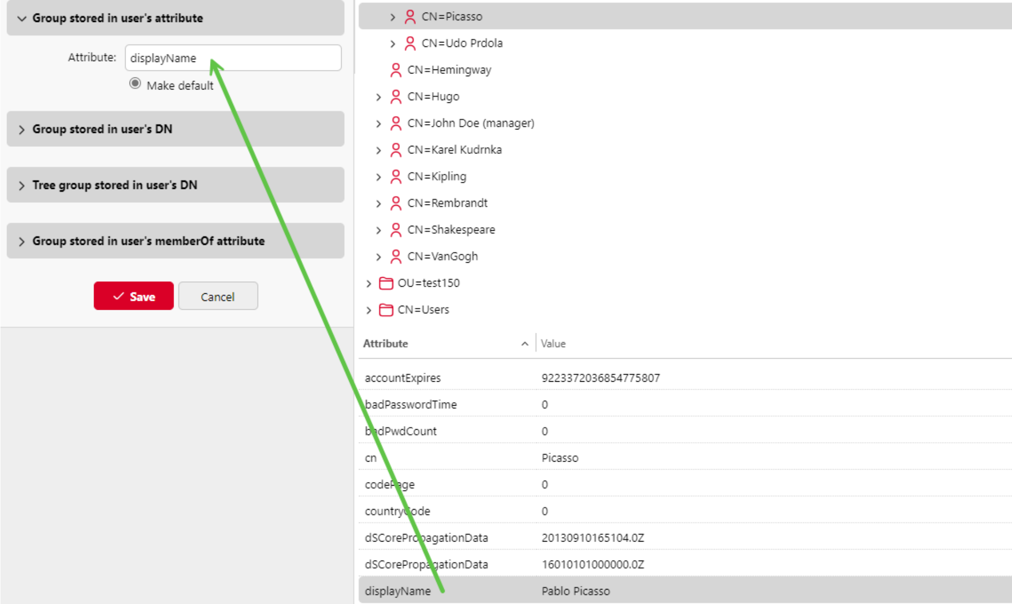
Groups Tab

On this tab, you can import groups and the group structure from the LDAP source. There are four different ways of specifying which groups are imported. You can use multiple different methods together and by each method, you can create different groups of users. You can also select to import the groups under an existing group in MyQ.

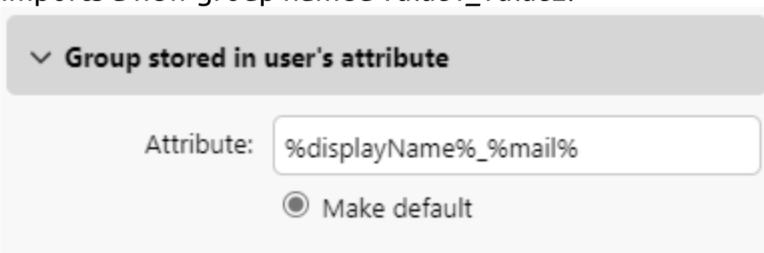


- **Do not change default group**: A user can be a member of multiple groups but all their prints, copies and scans are accounted to only one group: the default (accounting) group of the user. If you select this option, the default group of the selected user does not change during the synchronization.
- **Import groups under this group**: You can select an existing group in MyQ under which you import the groups from the LDAP database.

- **Groups stored in user's attribute**:
    - **Attribute**: You can select this option if you want to use an attribute that defines groups in the LDAP database. To add it, type the name of the attribute in the property text box or drag the attribute from any individual user and drop it in the **Attribute** text box.

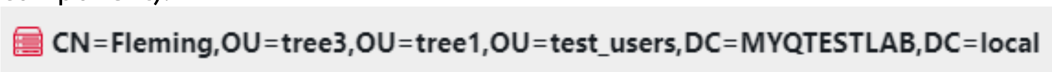
      You can also create groups by combining multiple attributes. To create such groups, put each of the attributes between two percentage signs (%). For example, the combination of attributes *%attribute1%_%attribute 2%* , imports a new group named *value1_value2*.

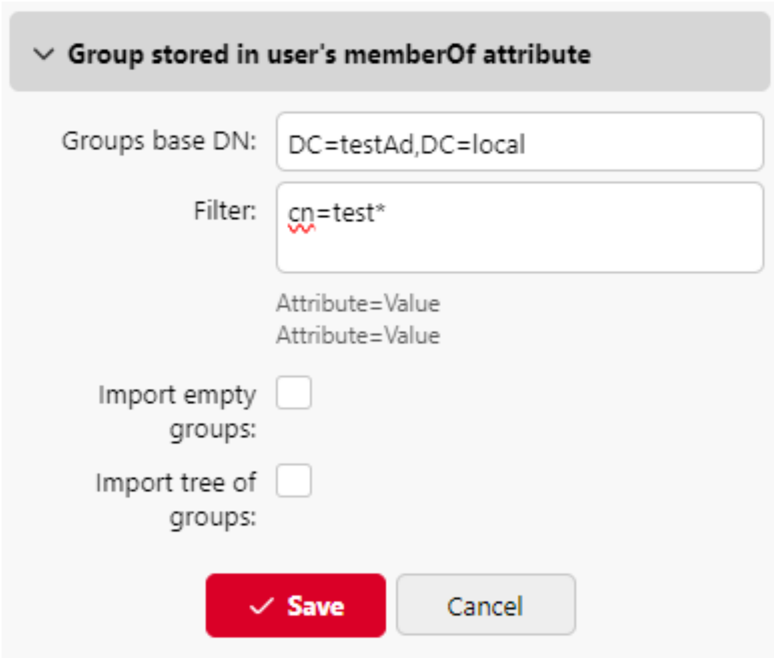
      Furthermore, you can create tree structures of groups by separating the attributes with vertical bars. For example, the combination of attributes *%attribute1%|%attribute2%*, imports a group *value1*, and its sub-group *value 2*.
    - **Make default**: If you select this option, the group becomes the default group of the imported user.
- **Group stored in user's DN**:
    - **OU component index**: Here you can select a group by its OU (organizational unit) index among the DN components. The index is counted from right to left: the first OU group from the right has index *1*, the second from the right has index *2* and so on.

    On the image above, there are two OU groups: *test_users* has index *1* (as it is the first OU group from the right), *tree1* has index *2*. The other components are not OU and therefore have no index.
  - **Make default**: If you select this option, the group becomes the default group of the imported user.
- **Tree group stored in user's DN**: Here you can import the whole tree structure of groups. You can restrict the import to any part of the structure by striping the DN components from the left and from the right. In the respective text boxes, enter the amount of components to be striped from the left and from the right side. You have to strip at least one component from the left (the user CN component) and one component from the right (the right-most DC component).

  On the image above, there are six components. If you strip one component from the left and one from the right, you import the following structure of groups: *MYQTESTLAB > test_users > tree1 > tree3*. By stripping components from the left, you remove the groups from the bottom to the top of the structure. By stripping components from the right, you remove the groups from the top to the bottom of the structure.
  - **Make default**: If you select this option, the bottom group of the imported structure becomes the default group of the imported user.
- **Group stored in user's memberOf attribute**:
  - **Group base DN**: MyQ can import security and distribution groups stored in the user's **memberOf** attribute. The security groups are used to define access permissions granted to their members. Distribution groups can be used for sending emails to a group of users. To specify which groups should be taken into consideration during the import, you have to insert the groups base DN. MyQ imports only groups that are included in the base DN; other groups stored in the **memberOf** attribute are ignored. The group base DN does not have to be in the same organizational unit as the users base domain. If a user is member of more than one group on the LDAP server, all the groups are stored in the **memberOf** attribute. Therefore, the **Make default** option, which requires a single value, is not available for this method of import.
    To add the groups base DN, drag it from the database browser and drop it in the **Group base DN** text box.
  - **Filter**: You can filter this import by specifying the values of attributes. Add the conditions in the form: *Attribute=Value*. Groups with a different value on this attribute are not accepted and are filtered out of the import. You can use the ***** symbol to search for substrings. The symbol can be appended from both sides. For example, if you add a *cn=*in** condition, only users whose common name attribute contains "*in*" are accepted. You can add one condition per row. Groups are accepted if they satisfy at least one condition.



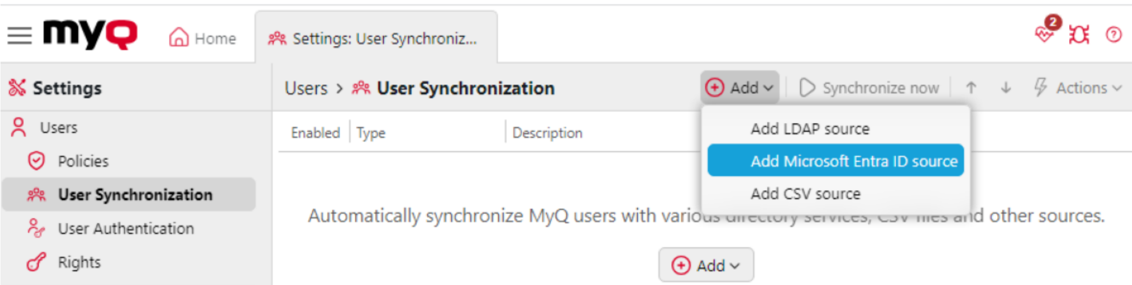
- **Import empty groups**: If you select this option, groups from the **Group base DN** are imported even if there is no user having them in their **memberOf** attribute.
- **Import tree of groups**: If you select this option, the whole tree structure is imported. Otherwise all groups are added separately; not as a part of a tree structure.

9.9.3 User Synchronization from Microsoft Entra ID with Microsoft Graph

Microsoft Entra ID (formerly Azure AD) with Microsoft Graph is a service accessed from the Microsoft Azure Portal, it must be enabled and configured before it can be used to synchronize users to MyQ.

Add Microsoft Entra ID as a Source

Once the Microsoft Entra ID connection is established, go to **MyQ > Settings > User Synchronization**. Click **Add**, and then click **Add Microsoft Entra ID source**.



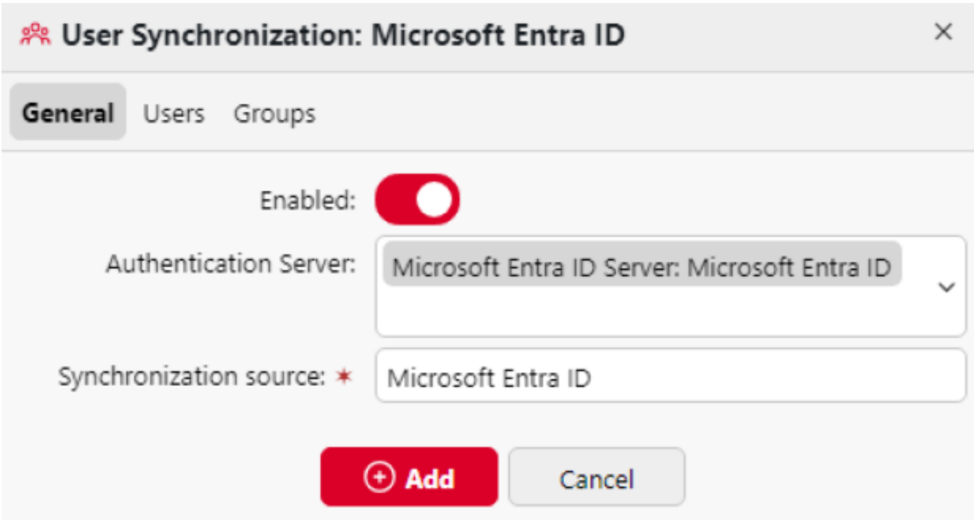
Once the source is established, configuration options allow you to edit how users are imported.

- In the **General** tab the **Authentication Server** and **Synchronization Source** can be set, and the synchronization can be enabled or disabled.
- In the **Users** tab, the users that should be imported can be selected, their properties can be set, and various other options can be enabled or disabled.
- In the **Groups** tab you can set rules not for which users to import (this is set in the **Users** tab), but how to group users that are imported, based on their grouping in your Entra ID source.

General Tab

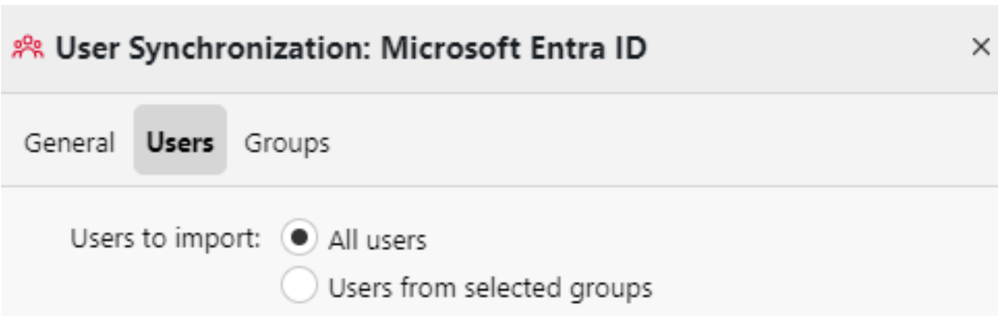
This tab opens by default when you select **Add Microsoft Entra ID source**. The following options are available:

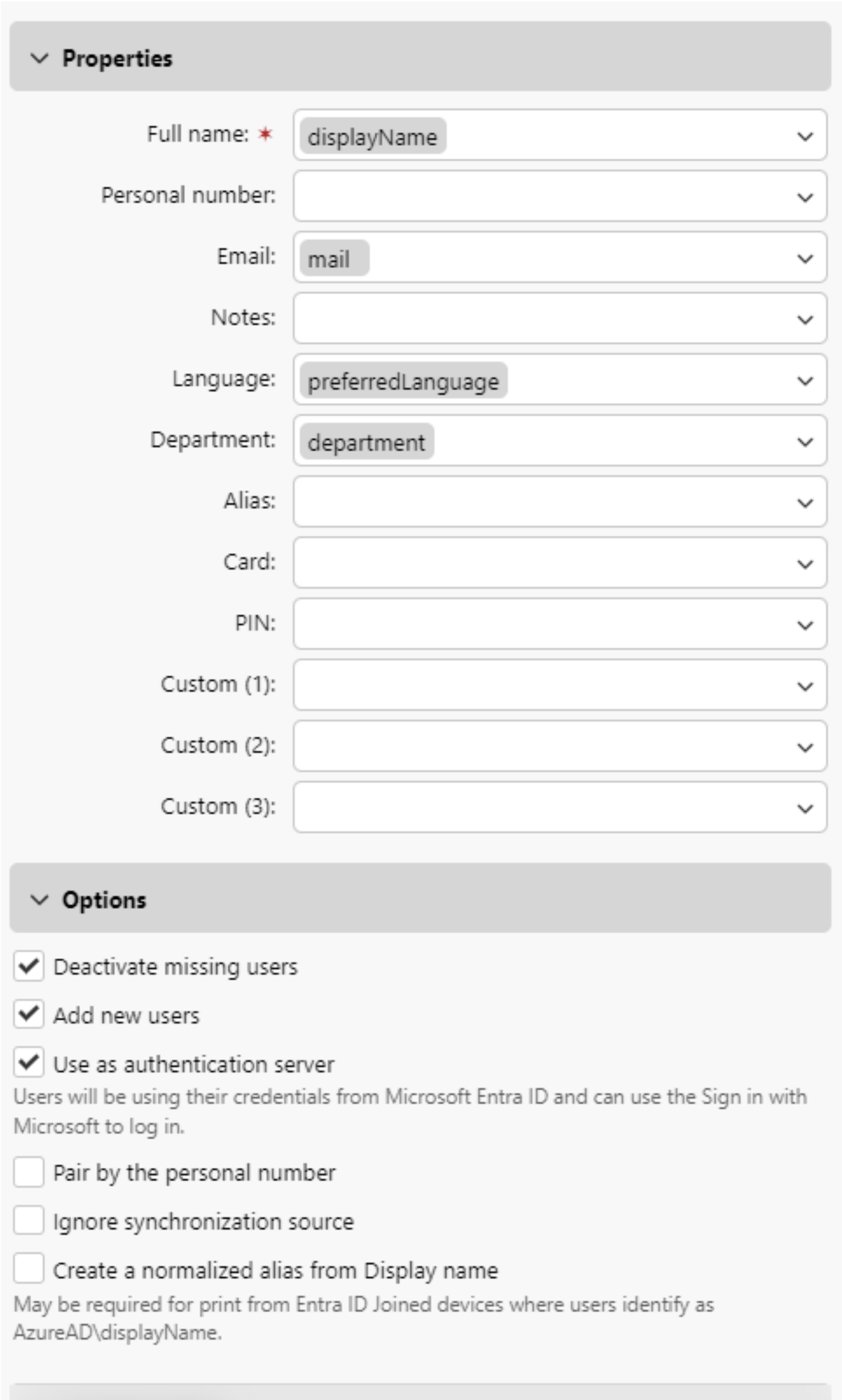
- **Enable**: use this toggle to enable or disable the user synchronization.
- **Authentication Server**: select the authentication server you wish to use. This server should already be connected and configured according to these instructions. If multiple connections are established, you can select which to use for this user synchronization.
- **Synchronization Source**: give this particular user synchronization a name which allows it to be easily identified. This is especially important if you are using multiple Entra ID tenants, to differentiate between them.



Users Tab

This tab allows you to select which **Users to import**, their **Properties**, and various **Options** for user synchronization.




Properties
Full name: *
displayName
Personal number:
Email:
mail
Notes:
Language:
preferredLanguage
Department:
department
Alias:
Card:
PIN:
Custom (1):
Custom (2):
Custom (3):
Options
Deactivate missing users
Add new users
Use as authentication server
Users will be using their credentials from Microsoft Entra ID and can use the Sign in with Microsoft to log in.
Pair by the personal number
Ignore synchronization source
Create a normalized alias from Display name
May be required for print from Entra ID Joined devices where users identify as AzureAD\displayName.

Users to Import

This is where you can select which users you want to import from your Entra ID Tenant into MyQ. You can select from **All users** or **Users from selected groups**. In the latter option, the groups refer to existing user groups in your Entra ID source, you can choose to use these groups, ignore them, or organize them further in MyQ in the **Groups** tab.

Properties

In the **Properties** section, you can map user information from Microsoft Entra ID to the credentials in MyQ. A predefined selection of recommended values is provided. If the predefined value is not used, a manually typed custom attribute can replace it and synchronize a different user attribute from Entra ID.

Property Name	Description	Predefined Attribute/s
Full name	Users' full name.	`displayName`
Personal number	User identification number.	`employeeId` or `extensionAttribute1` to `extensionAttribute15`
Email	Users' email.	`mail`
Notes	Relevant notes.	`extensionAttribute1` to `extensionAttribute15`
Language	Users preferred language.	`preferredLanguage`
Department	Users' department.	`department`

Property Name	Description	Predefined Attribute/s
Alias	An alternative name or username.	`displayName` , `userPrincipalName` , `upnPrefix` , `mailNickname` , `onPremisesSamAccountName` , `onPremisesSamAccountName@onPremisesDomainName` , and `extensionAttribute1` to `extensionAttribute15`
Card	The users' ID card number.	`employeeId` or `extensionAttribute1` to `extensionAttribute15`
PIN	The users' PIN.	`employeeId` or `extensionAttribute1` to `extensionAttribute15`
Custom (1)	Custom attribute to assign to other relevant information.	`extensionAttribute1` to `extensionAttribute15`
Custom (2)	Custom attribute to assign to other relevant information.	`extensionAttribute1` to `extensionAttribute15`
Custom (3)	Custom attribute to assign to other relevant information.	`extensionAttribute1` to `extensionAttribute15`

> For the **Alias** property, if the attribute `onPremisesSamAccountName@onPremisesDomainName` is used, the user's Alias after synchronization will be a combination of the user's Microsoft Entra ID attributes `onPremisesSamAccountName` and `onPremisesDomainName` in the format, for example, user@myq.cz.

Options

- **Deactivate Missing Users**: this option allows the system to automatically deactivate users in MyQ X who are no longer present in the Microsoft Entra ID source.
- **Add New Users**: when enabled, this feature automatically adds new users found in the Microsoft Entra ID source to MyQ X.
- **Use as authentication server**: if you plan to authenticate users towards Azure using Active Directory credentials and use the Microsoft single-sign-on option, select the **Use as authentication server** option and click **Save**.
- **Pair by the personal number**: check this box if you wish to update users based on their personal number. If the personal number option is checked, during re-synchronization, the system will look for the user by their personal number. If a match is found, the user details will be updated, otherwise, a new user will be created.

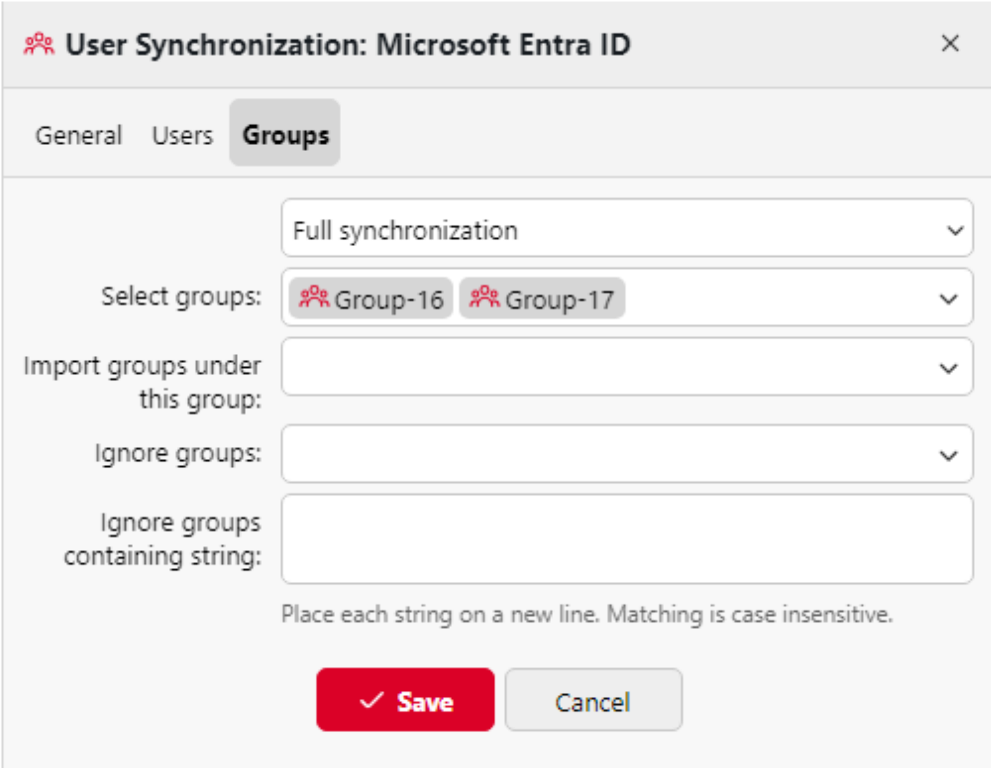
> Since MyQ Print Server 10.2 RC 4, the **Pair by the personal number** option is checked by default for all newly created synchronization sources and cannot be changed. Sources created in 10.1 after migration to 10.2 allow editing this option. Pairing Users by personal number is strongly recommended.

- **Ignore Synchronization Source**: this option provides the ability to selectively ignore certain aspects or data from the Microsoft Entra ID source during synchronization.
- **Create normalized alias from Display name**: this option means an additional alias is added to the user on top of those configured in the user attributes section, this alias takes the form of `AzureAD\concatedDisplayName`. It allows proper recognition of users who print from Entra ID Joined devices.

> If two or more users have the same Full Name synced from Entra ID, a normalized Alias will be created only for the first user. There is no way to distinguish Job owners for this case in the ADD environment since the printer’s driver provides only a concatenated user’s Name and Surname.

Groups Tab

The **Groups** tab does not specify which user groups to import, but how they should be organized within MyQ. Which user groups are imported is controlled in **Users > Users to import**.



The following options are available:

- Select type of synchronization: In a synchronization source, you can adjust the level of synchronization on the **Groups** tab. It is possible to select from the following levels:
    - **Full synchronization**: synchronize groups 1:1 as they are in the source, meaning users are both added to and removed from groups as in the source.
    - **Synchronize if not empty**: leave a user in at least one group even after they lose all memberships in the directory.
    - **Add new**: ensure that once a user is assigned to a group in MyQ, they do not lose this membership even after they are removed from a group in the source directory.
- **Select groups**: this allows you to select the groups that exist in your instance of Entra ID which you want to include as groups within MyQ.
- **Import groups under this group**: allows you to select an existing user group in MyQ to use as a parent group for any groups synchronized from this source.
- **Ignore groups**: select what Active Directory groups you do not want to use in this synchronization.
- **Ignore groups containing string**: fulfills the same function as **Ignore groups** allowing you to specify groups to be ignored according to a string they contain.

Group Synchronization - Example Scenario

Administrators have enhanced control over group memberships during Entra ID user synchronization. With the **Select groups** filter option in the Entra ID User Sync source settings, you can specify which group memberships are imported into MyQ without affecting the overall user synchronization process.

Example:

The Entra ID group structure is as follows:

- **All students**: 1,500 users
- **Class1A**: 1,000 users
- **Class1B**: 500 users

MyQ Settings:

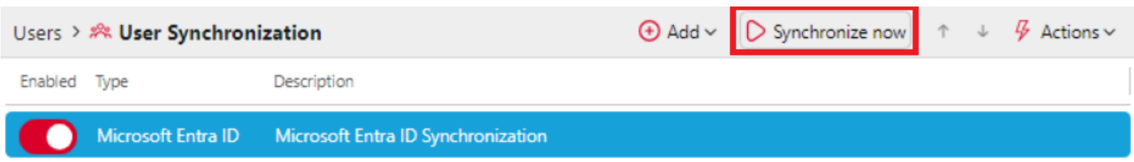
- In the **Users** tab under **Users to import** select **Users from selected groups** and specify the **All students** group to synchronize all 1,500 users.
- In the **Groups** tab under **Select groups**, select **Class1B** only.

Result:

- All 1,500 users are synchronized to MyQ.
- Only the 500 users in **Class1B** have their group membership applied in MyQ.
- The remaining 1,000 users are imported without any group membership.
- Users who are also members of **Class1A** do not have this membership applied in MyQ.

Synchronize Now

Users can be now synchronized by selecting your Microsoft Entra ID source from the list and clicking **Synchronize now**. It is also possible to schedule user synchronization using the task scheduler.



Multi-Tenant Synchronization and Authentication

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

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

9.9.4 User Synchronization from CSV Files

To synchronize users from a CSV file, you have to create a new CSV synchronization on the **User Synchronization** settings tab and on the synchronization properties panel, add the source file and set properties of the synchronization.

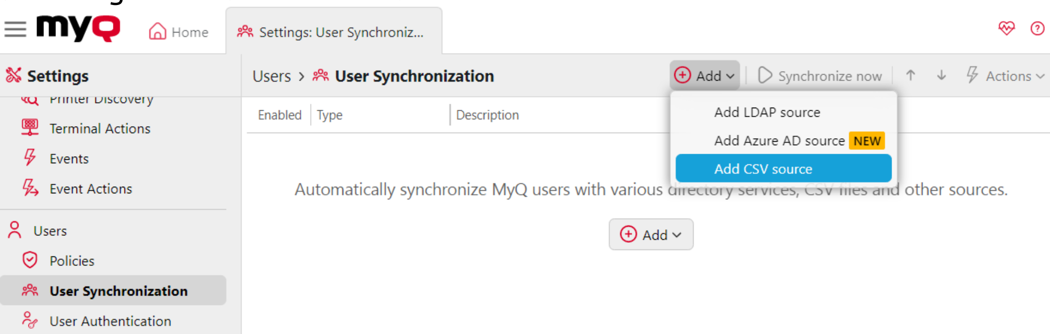
After the synchronization is set up, you can either manually run it on the **User Synchronization** settings tab or set it as a regular task on the **Task Scheduler** settings tab.

> A sample CSV file called `Users_example` is available in `ProgramData\MyQ\Data\Import`, this CSV can be populated with relevant information and imported.

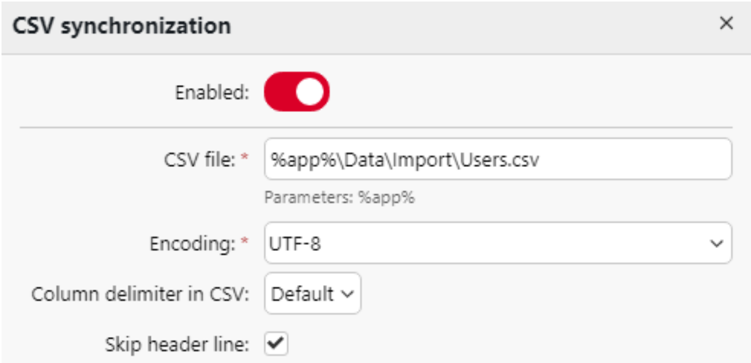
Creating a new CSV synchronization

To create a new synchronization:

1. On the bar at the top of the **User Synchronization** settings tab, click **+Add**, and then click **Add CSV source**. The CSV synchronization properties panel appears on the right side of the screen.



2. **Set up the synchronization**: On the CSV synchronization properties panel, set the path to the CSV file in the **CSV file** field, and configure the synchronization. For information about the synchronization options, see "CSV synchronization setup options" below.



3. **Save** the setup.

CSV synchronization setup options

These are the CSV synchronization setup options:

- **Enabled**: Here you can enable or disable the synchronization.
- **CSV file**: Here you can set the path to the CSV file on the MyQ server.
- **Encoding**: Select the encoding that is used in the CSV file. The default value depends on the OS settings of the computer where you access the MyQ Web Interface on.
- **Column delimiter in CSV**: Select the delimiter that is used in the CSV file. If you select the **Default** option, MyQ scans for the delimiter set on the **Column delimiter in CSV** drop-down list box on the **General** settings tab.
- **No header line**: This option is *disabled* by default, meaning that the first row of the CSV will be read as a header row and columns will be imported based on their header value. If this option is *enabled*, the CSV should contain no header row, and columns will be imported based on their order (in order of appearance in the CSV File Syntax table below).
- **Import groups under this group**: Here you can select an existing group in MyQ under which you import the groups from the CSV file.
- **Synchronization source**: Here you can specify a different source than the CSV to be marked as the synchronization source by the MyQ system. For example, you can insert an LDAP server domain.
- **Ignore synchronization source**: If you select this option together with the **Deactivate missing users option**, all users that are not in the current synchronization source are deleted.
- **Use authentication server**: If you select this option, an LDAP or Radius server is used for the authentication of the imported users.
- **Authentication server**: Here you can select the LDAP or Radius domain for the user authentication.
- **Deactivate missing users**: If you select this option, MyQ deletes users that are imported from the current synchronization source and that are not in the source anymore. To delete users that were added from different sources, select the **Ignore synchronization source** option together with this option.
- **Add new users**: If you select this option, MyQ adds new users from the current synchronization source.

- **Pair users by personal number**: If you select this option, multiple accounts with a single personal number are paired.
- **Convert user name to lowercase**: If you select this option, all letters in user names are converted to lowercase.
- **Cards/PIN/Groups/Delegates**: In each of the mandatory drop-down boxes, you can select from these synchronization options for the respective parameter (Cards, PIN, Groups):
  - **Do not synchronize**: The value of the respective parameter in MyQ is not changed.
  - **Full synchronization**: The value of the respective parameter in MyQ is always replaced by the value in the CSV file. If the value in the source file is empty, the value in MyQ is erased.
  - **Synchronize if not empty**: If the respective field in the CSV file is not empty, the parameter value in MyQ is replaced by the value in the CSV file. Otherwise, the parameter value remains unchanged. This is the default setting.
  - **Add new**: If the parameter is already set in MyQ, it is not replaced. Only new values are added.

CSV File Syntax

In the table below, you can find information about individual fields of the CSV file.

A single word or a plain number can be put in the CSV fields as they are, while more complex strings, such as full name or email address, have to be bounded by quotes.

Column name	Mandatory	Description
FULLNAME	Yes	Name of the user in double quotation marks, for example "*Thomas Pineapple*".
USERNAME_ALIASES	Yes	Login of the user and eventually their aliases. The login should be the same as the user's domain login name, for example *Tom*. When you import multiple aliases, separate them with commas, for example "*Tom,Tommy,Apple*".
EMAIL	No	Email of the user, for example "*t.pinapple@domain.com*".
CARDS	No	Number of the user's authentication card/chip. It has to be inserted in the form in which it is read by the card/chip reader, for example *7E9700C9*.

GROUPS	No	Here you can add user groups. You can import a whole branch of the groups tree structure. The groups on the imported branch have to be separated by vertical bars. If you want to import multiple groups (or groups tree branches), separate them by commas. For example, if you add two branches separated by a comma: "*Activities|Outdoor|Swimming,Activities|Outdoor|Birdwatching*", MyQ imports a single parent group *Activities* with a single child group *Outdoor*, with two child groups *Swimming* and *Birdwatching* (*Activities>Outdoor>Swimming,Birdwatching*). Commas and vertical bars cannot be used in group names as they are used as group delimiters.
CODE	No	The personal number of the user. The ID number must be unique for each user. This parameter is very useful when using multiple sync sources.
SCANSTORAGE	No	The folder or email where the user wants their scans to be sent to, for example "*\Users\Tommy*".
PIN	No	You can define one or more PINs to be assigned to users within the synchronization process. It is not absolutely necessary, as PINs may also be generated later within the setup of the user account. The PINs should be in the hashed MD5 format, for example *14BFA6BB14875E4*.
MANAGED_GROUPS	No	You can make the user the manager of a particular group by adding the group or path to the group here in the way in which you would import the group. If you want the user to be a manager of a child group, enter a whole branch ending with this group. For example, enter the branch "*Activities|Outdoor|Swimming*" to make the user a manager of the *Swimming* group. If there are no parents of the group in the group structure, enter just the group name, e.g. *Activities*. Commas and vertical bars cannot be used in group names as they are used as group delimiters.

AUTHSERVER	No	In this field you may define the domain for user authentication, for example "*testAD.local*".
PHONE	No	The user's phone number, for example *080008020*.
LANG	No	Default language of the user, for example *en*.
PWD	No	If you want to use the MyQ password, insert the password in the hashed MD5 format, for example *18BFA6BB14875E8*. If you are using a different authentication server (i.e. LDAP server), you can leave it empty.
EXTID	No	EXTID is an internal MyQ parameter. This field has to be left empty.
DELEGATES	No	For each user, you can import any number of delegates. If you import multiple delegates, separate them with commas, for example "*Carol,Kohei,Eliot*".
ALTERNATEEMAILS	No	Comma separated list of the user's alternate emails.
DEPARTMENT	No	User’s department, for example *Marketing*.
CUSTOM1	No	User’s “Custom 1” field from profile.
CUSTOM2	No	User’s “Custom 2” field from profile.
CUSTOM3	No	User’s “Custom 3” field from profile.

```
“FULLNAME”; ”USERNAME_ALIASES”; “EMAIL”; “CARDS”; “GROUPS”; “CODE”;
“SCANSTORAGE”; “PIN”; “MANAGED_GROUPS”; “AUTHSERVER”; “PHONE”;
“LANG”; “PWD”; “EXTID”; “DELEGATES”

“Thomas Pineapple”; “Tom, Tommy, Apple”; “t.pinapple@domain.com”;
7E9700C9;”Imported Users, Activities|Outdoor|Swimming,
Activities|Outdoor|Birdwatching”;22212;”\\Users\Tomy”;
14BFA6BB14875E4;Birdwatching;testAD.local;080008020;en; 18BFA6BB14875E8; ;“Carol,Kohei,Eliot”;
```

9.9.5 User Synchronization from Entra ID (Azure AD) with SLDAP

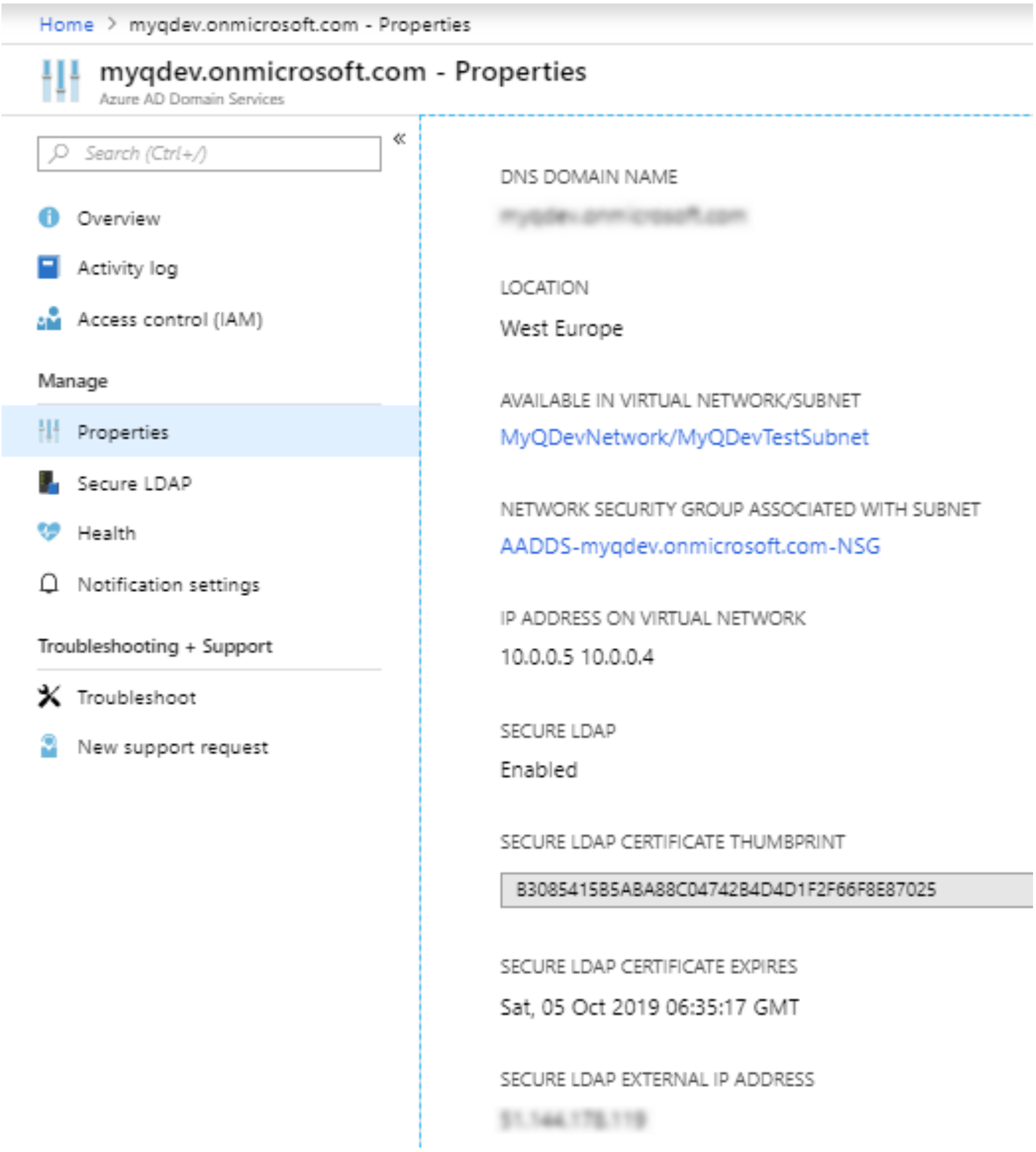
Entra ID (formerly Azure AD) with SLDAP is a service accessed from the Microsoft Azure Portal. It has to be enabled and configured in Azure Active Directory Domain Services.

The activation and setup of the service are described in the following Microsoft guides:

- To enable and configure Azure Active Directory Domain Services: https://docs.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-create-instance
- Configure Entra ID Domain Servers to use SLDAP: https://docs.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-configure-ldaps

After you activate the Entra ID, you need to add it to MyQ and set up the synchronization in the standard way (see User Import and synchronization). When setting up the **Authentication server** in MyQ, you need to make sure that the LDAP server parameters are set to the following values:

- **Domain** = *DNS DOMAIN NAME* of the Entra ID Domain
- **Security**: *SSL*
- **Server** = *SECURE LDAP EXTERNAL IP ADDRESS* of the Entra ID Domain



9.9.6 User Synchronization from Google Workspace

Use this procedure to synchronize users and groups from Google Workspace.

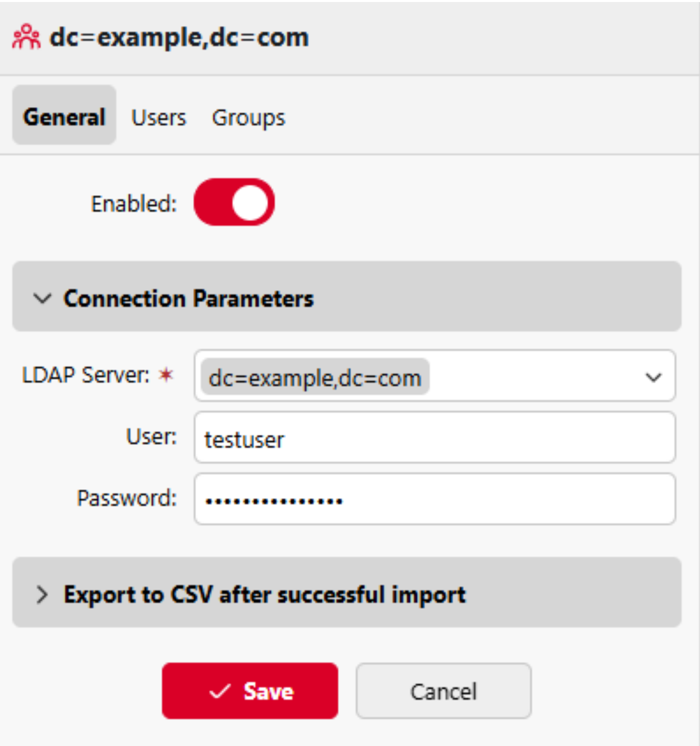
Prerequisites

- Google Workspace authentication server in MyQ.
- Certificates and credentials to an LDAP client, which you get from Google Admin console.

Synchronize Users from Google Workspace

1. Go to **MyQ > Settings > User Synchronization**.
2. Click **+Add** and select **Add LDAP Source**.

3. Under **Connection Parameters**, select the LDAP server, and enter the username and password.
4. Click **+Add** to save changes.
5. On the **Users** tab, add one or more **Base DNs** from which to synchronize users.
6. Configure the remaining options as required, and click **Save**.
7. To run the synchronization, go to **MyQ > Settings > User Synchronization,** and click **Synchronize Now**. If you have configured everything correctly, users and groups from your Google Workspace directory are now visible under **MyQ > Users**.
8. (Optional) To synchronize automatically on schedule, go to **MyQ > Settings > Task Scheduler**, and configure the **User Synchronization** task.



More Information

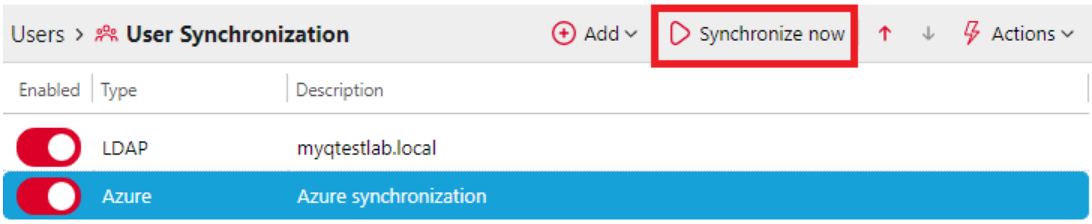
- (v1) Synchronize Users from Google Workspace
- Authentication Servers Settings
- Setting up an LDAP Synchronization
- Manual and Scheduled Synchronization Run

9.9.7 Manual and Scheduled Synchronization Run

The synchronization can be manually run on the **User Synchronization** tab of the MyQ Web Interface, or it can be set as a scheduled task on the **Task Scheduler** tab.

Manual synchronization run

On the **User Synchronization** settings tab, select the synchronizations that you want to run, and then click **Synchronize now** on the bar at the top of the tab.



The **Synchronize Now** button will start the synchronization, unless another one is already running. In this case, an error message will be displayed.

Upon start, the **Synchronization Results** panel opens and displays the operation log live. The log tail is automatically monitored when the panel is scrolled to the bottom. A spinning wheel at the bottom of the log indicates that synchronization is in progress.

The **Cancel** button cancels the process. It may take some time until the synchronization is actually canceled.

The **Save** button downloads the synchronization log.

Scheduled synchronization run

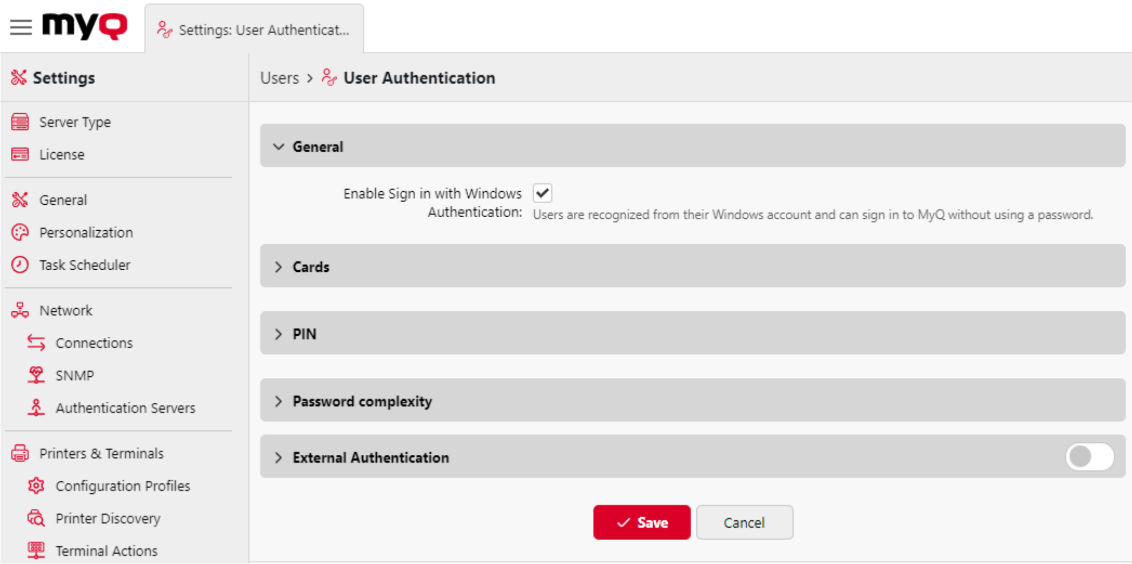
On the **Task scheduler** settings tab, you can setup a scheduled run of the synchronization. For more information about this option, see Task scheduler.

9.10 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.
See Authentication Servers Settings for details.

In the **User Authentication** settings tab, the administrator can manage everything related to how users authenticate themselves in MyQ:

- ID Card management
- PIN management
- Password Complexity
- External Authentication



9.10.1 Enable Sign-In with Windows

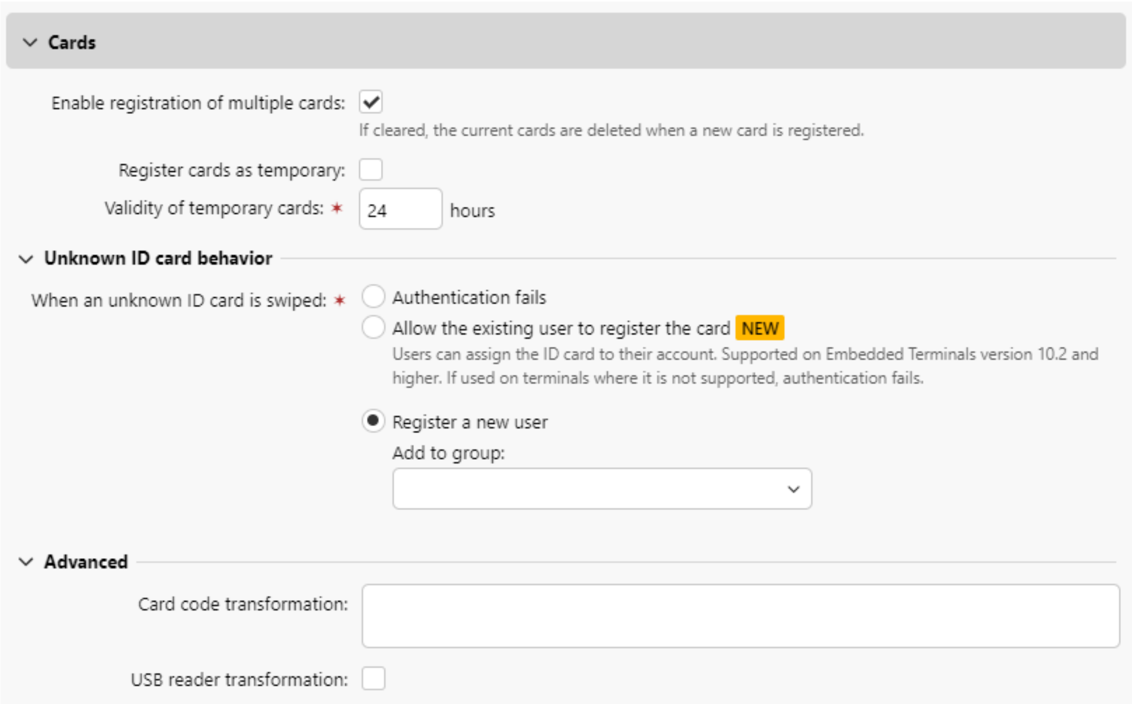
Enabling this option means those using a Windows account correctly synchronized with MyQ will not need to enter their MyQ login details to access the web interface. You can learn more about Integrated Windows Authentication here.

9.10.2 ID Card Management

In the **User Authentication** settings tab, in the **Cards** section, there are the following ID Card management options:

- **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.



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 the LDAP synchronization is supported.

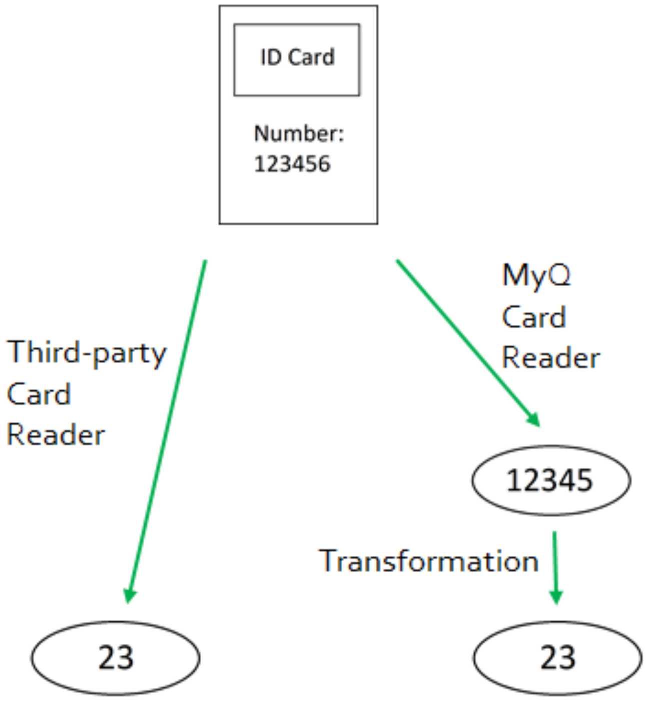
ID Card Transformation

This topic discusses the ID Card transformation feature in MyQ. The 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.

Available options:

- **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.

> ⚠ 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 —> 100000000000010101011

- **bin2hex** – Transform the card number from binary mode to hexadecimal mode.
  bin2hex(): 100000000000010101011 —> 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*

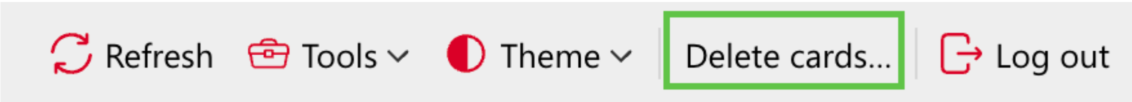
Transformation process:
("10AB" —>"1 0000 1010 1011" —> "0001 0000 1010 1011" —> "1101 0101 0000 1000" —> "0000 1000" —> "0001 0000" —> "10") + ("10AB"" —> "" —> "10AB") ==> "1010AB"

Delete Cards

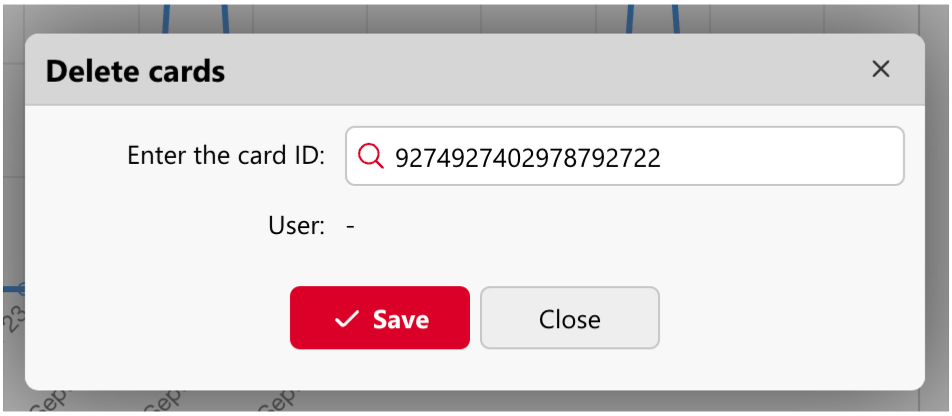
If you have the **Delete Cards** permission assigned to you, you can delete other user's cards. This is intended, for example, for situations where an organization has a Font Desk where you return your card and it should be removed from the system.

To do so:

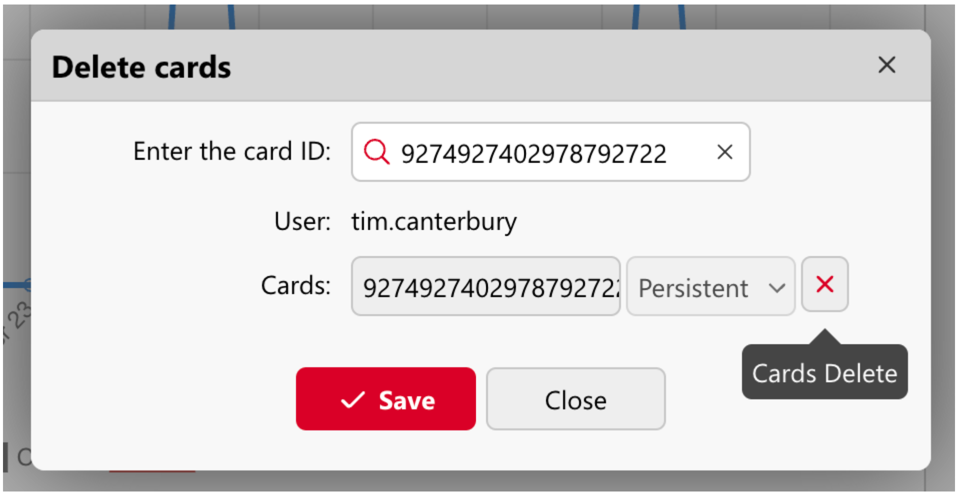
- Log in and open the MyQ Dashboard.
- Click the **Delete cards...** option.



- Fill in the ID card number (manually or by swiping the card at a reader connected to your computer):

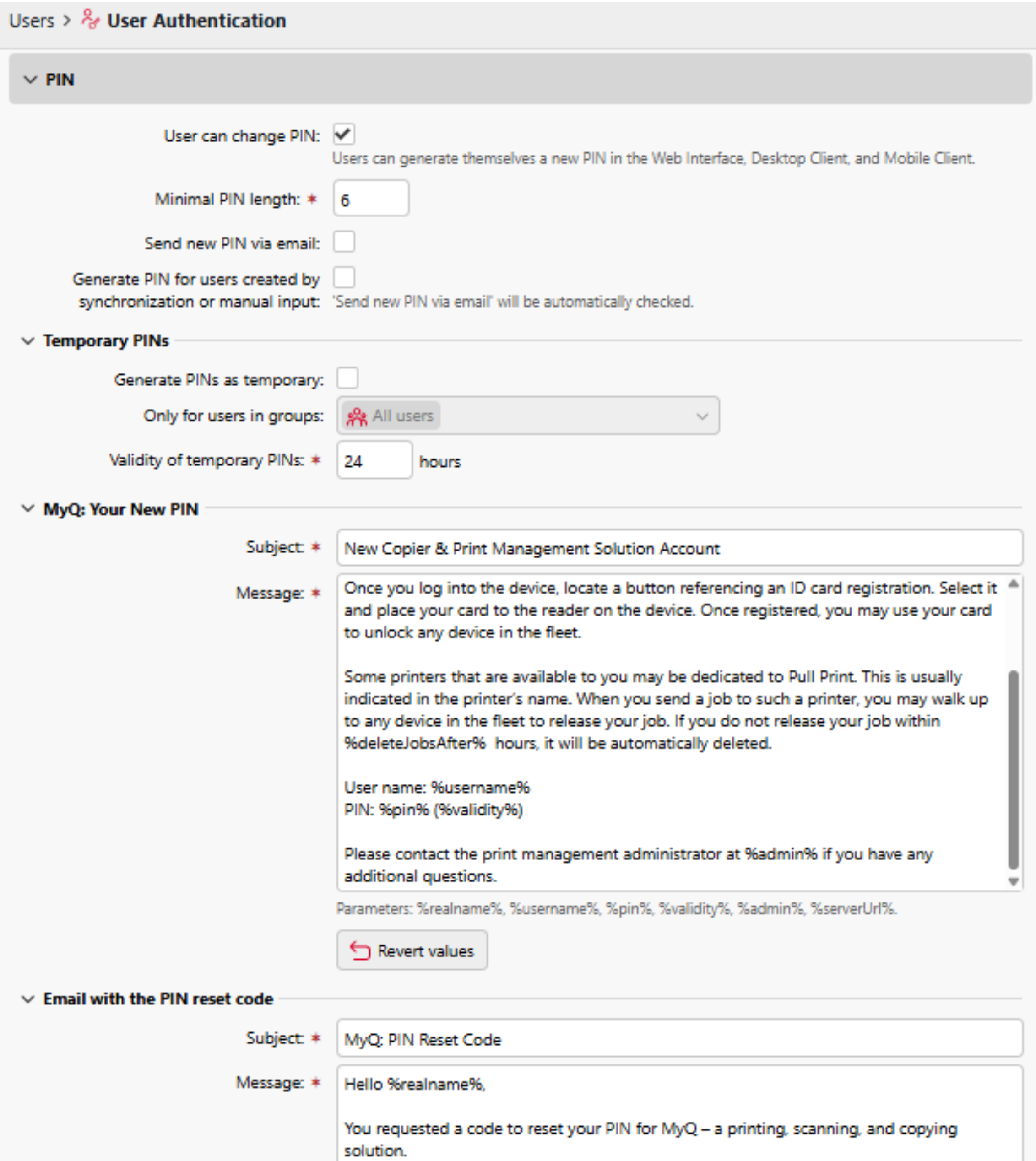


- Click **Enter** to search for the card.
- When the user is found, click **X** to delete the card, and then **Save** the changes.



9.10.3 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

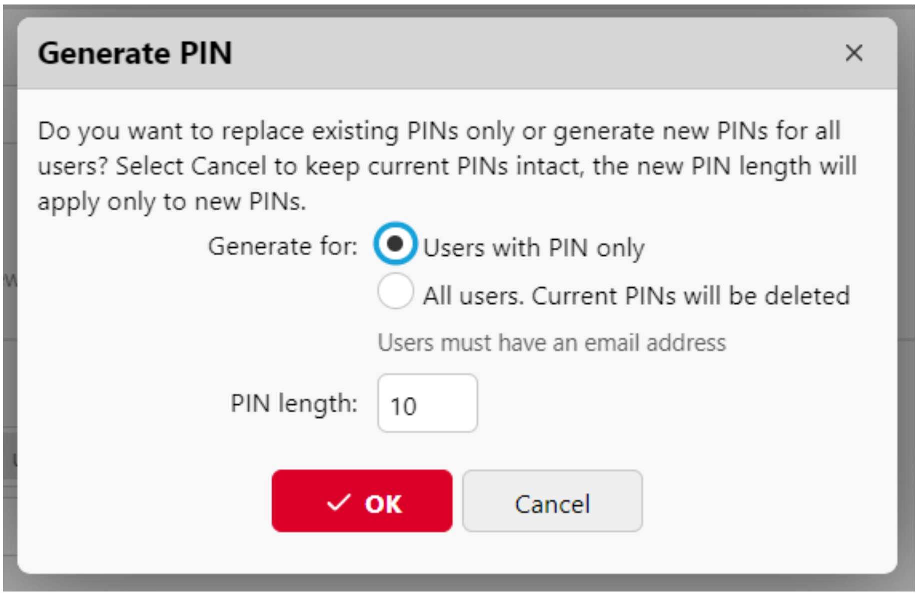
This option determines the mandatory minimum PIN length. The number can be set between *4* and *16* - the default is *6*.
If the administrator creates the PIN manually, it cannot be shorter than the value set in this field. If the PIN is generated by the system, it cannot be shorter than the value in 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).

Find out more about utilizing temporary PINs here.

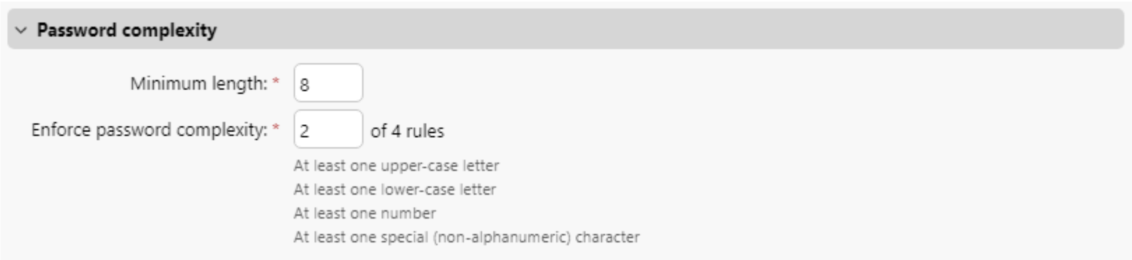
Limitations

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

9.10.4 Password Complexity

In this section, the administrator manages the password complexity of MyQ users accounts.

- **Minimum length** - set the minimum character length for the password, in range *1-100* (*8* by default).
- **Enforce password complexity** - set how many of the four password complexity rules are to be enforced (*2* by default):
  - At least one upper-case letter
  - At least one lower-case letter
  - At least one number
  - At least one special (non-alphanumeric) character



9.10.5 Using External Authentication Servers

In addition to the internal MyQ authentication methods (password, PIN or ID card), you can use two types of external authentication servers: LDAP and Radius.

With the two external methods, MyQ does not use the internal MyQ PIN or password for user authentication, but instead authenticates users against an LDAP or Radius server. After the user enters their credentials during the authentication, the credentials are sent to be verified directly by the external server. If there is no online connection with the LDAP or Radius server, users cannot log in.

To enable this method of authentication, you have to take two steps:

1. register the external authentication servers in MyQ
2. select to use them for user authentication

To register external authentication servers in MyQ, see Authentication Servers Settings.

Selecting to use the registered external authentication servers for user authentication, can be done either automatically during the user import from an LDAP server or a CSV file, or manually on the properties panels of individual users.

Automatically selecting the external authentication option

Importing users from a CSV file

When you import users from a CSV file, you have two options of selecting the authentication server for the users:

1. You can select the **Use authentication server** option and select the server during the synchronization setup on the synchronization properties panel.
2. You can specify the **Authentication server** for a particular user in the **AUTHSERVER** field of the CSV file. If the field is not empty, its value has priority over the value selected on the properties panel.

For more information about importing users from CSV files, see User synchronization from CSV files.

Importing users from an LDAP server

During the users import from an LDAP server, you can select the **Use authentication server option**, to use the current synchronization source server for users authentication. For information about importing users from LDAP servers, see User synchronization from LDAP servers.

Unlike the **Use authentication server** setting for the import from a CSV file, which allows you to select the authentication server, the **Use authentication server** setting here gives you a single option — users will be authenticated against the LDAP server where they are imported from.

Manually selecting the external authentication option

To manually select the external authentication option

1. Open the **Users** main tab and double-click the user. The user's properties panel opens on the right side of 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.

9.10.6 External Authentication

Administrators can benefit from **using external authentication servers** for authenticating users into MyQ. This is helpful mainly in environments where an authentication service not natively supported by MyQ is used.

> 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
   - By swiping an ID card
   - By entering a 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

API Documentation

For **implementation details**, containing information about the API endpoints and valid responses, see the MyQ API documentation:

- External Authentication API

Common use cases

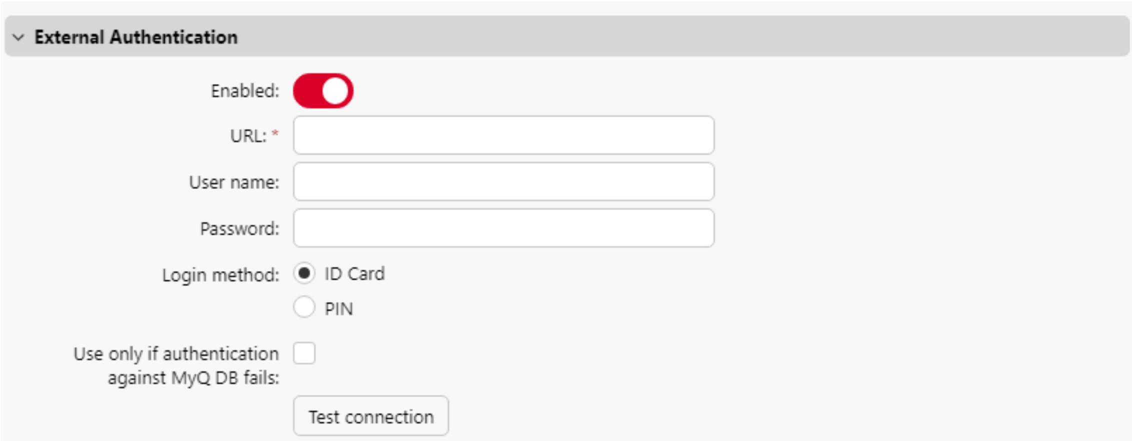
The External API connector can be used in its most simple way to “translate” requests. But it also allows more advanced authentication workflows as the connector itself can perform a set of operations before it returns the matching user back to MyQ.

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

9.11 Policies

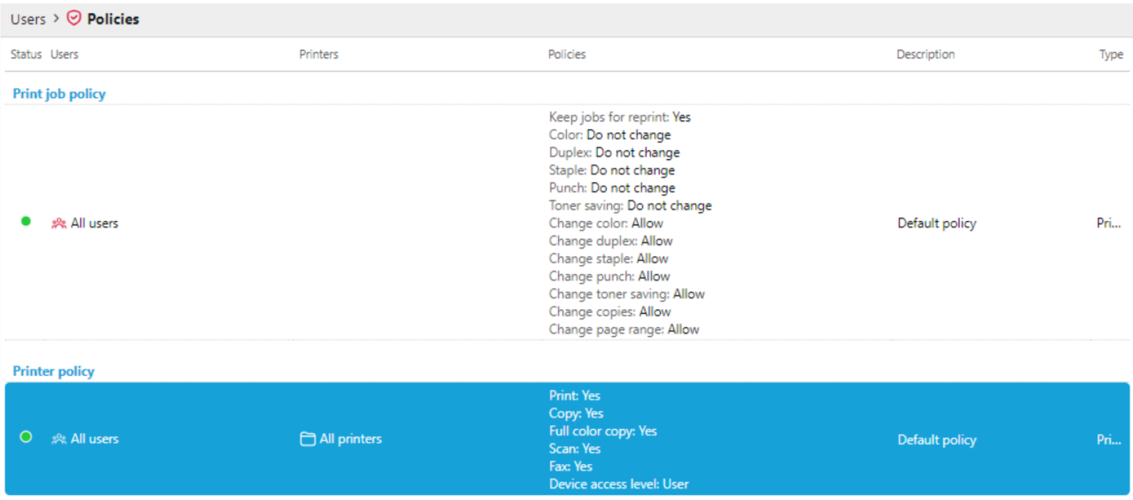
The **Policies** settings tab is divided into two sections. The **Print job policy** section contains settings that apply to all print jobs, all printers and selected users or groups.

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.

For more information about creating and applying user policies, see (v1) User 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.



9.11.1 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

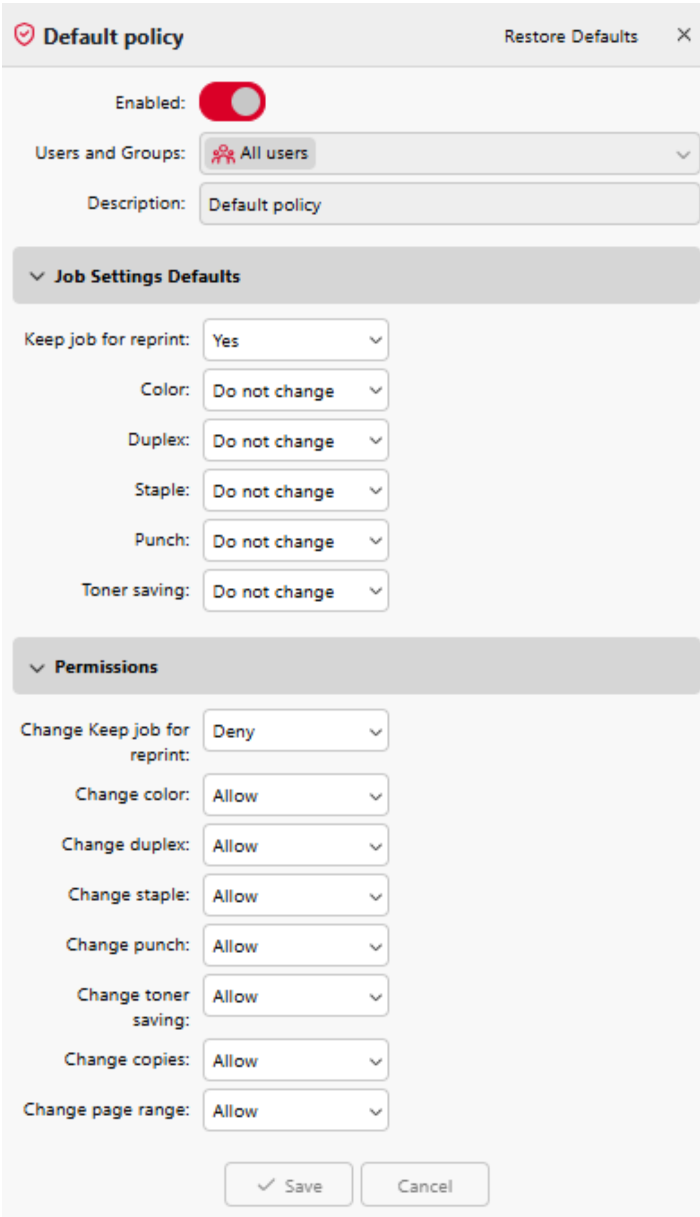
These options control if users are able to modify the job settings. Select a checkbox to modify a setting. For each one, you can choose *Allow* or *Deny*.

- **Change Keep jobs for reprint**
- **Change color**
- **Change duplex**
- **Change staple**
- **Change punch**
- **Change toner saving**
- **Change copies**
- **Change page range**

9.11.2 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.



9.11.3 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.

9.11.4 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:

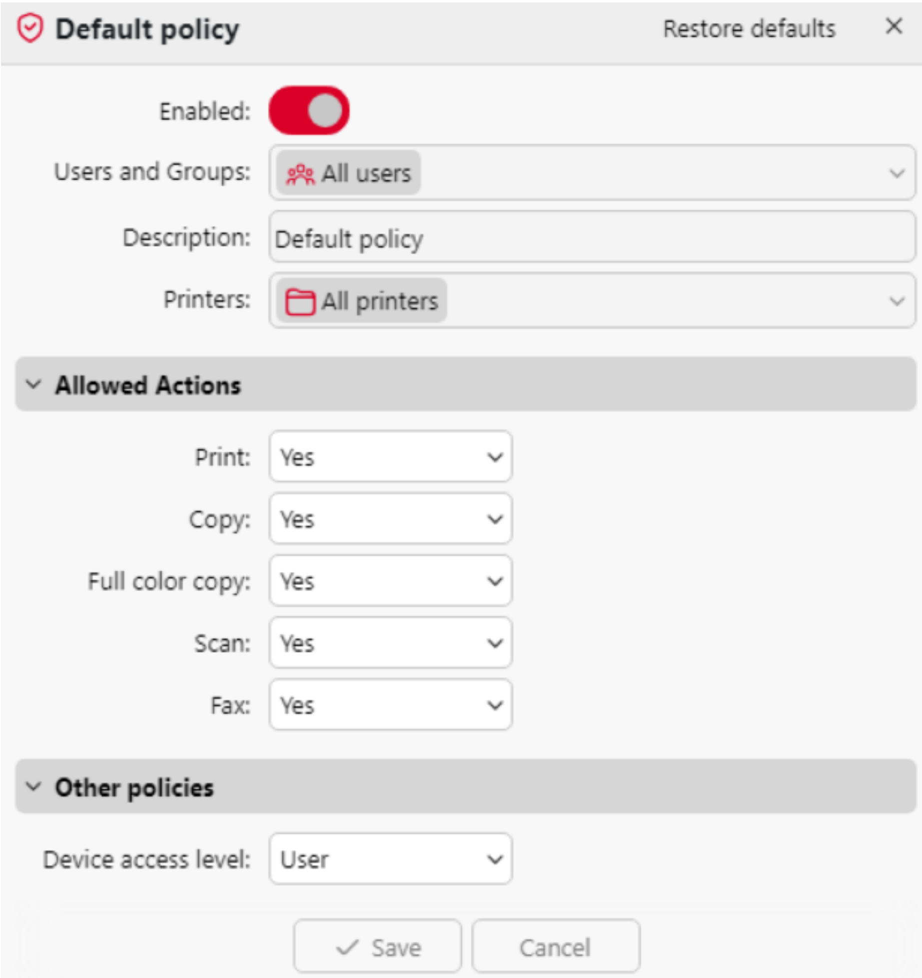
- In the uppermost section, you can enable or disable the policy, select the **Users and Groups** of users that it will apply to, select the **Printers** that it will apply to, and write the policy's **Description**.
- In the **Allowed Actions** section, you can restrict access to particular operations 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.



9.11.5 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

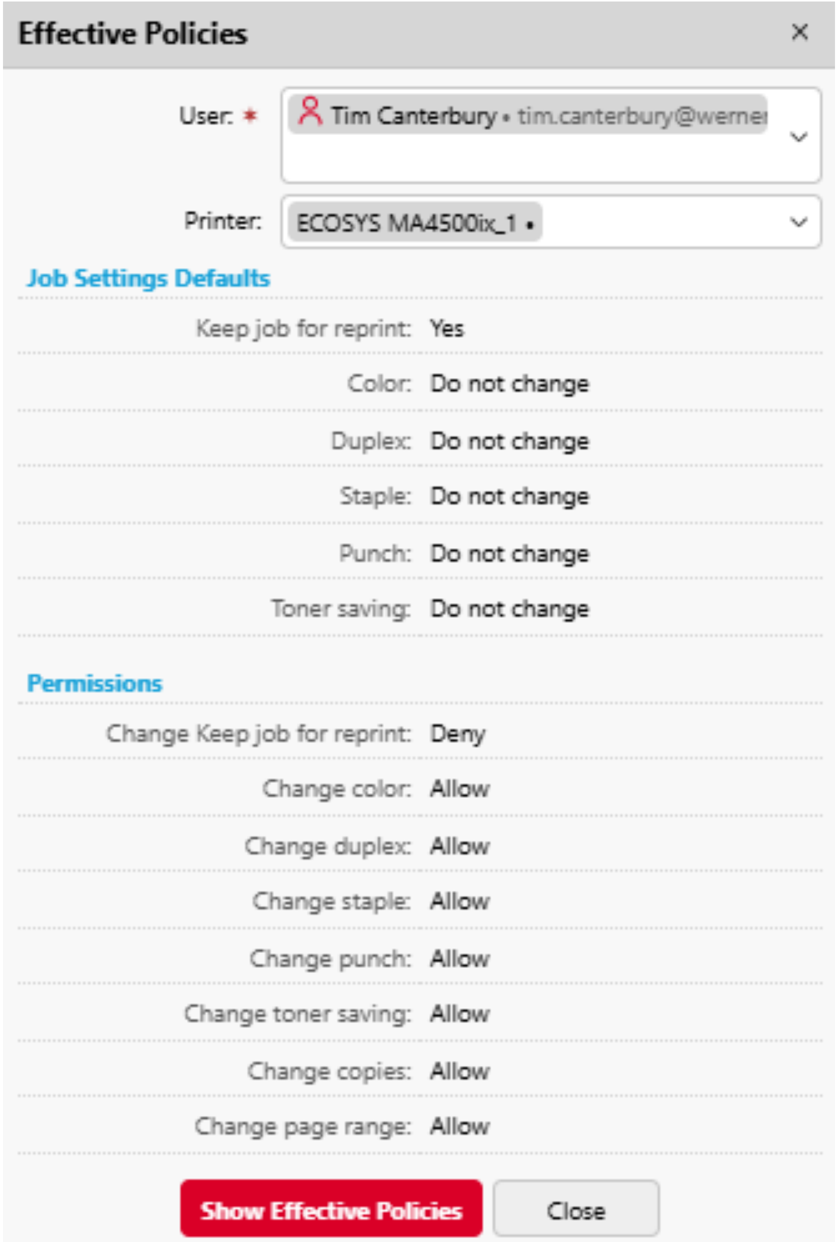
Save. The new policy appears on the **Policies** settings tab, under **Printer policy**.

9.11.6 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.

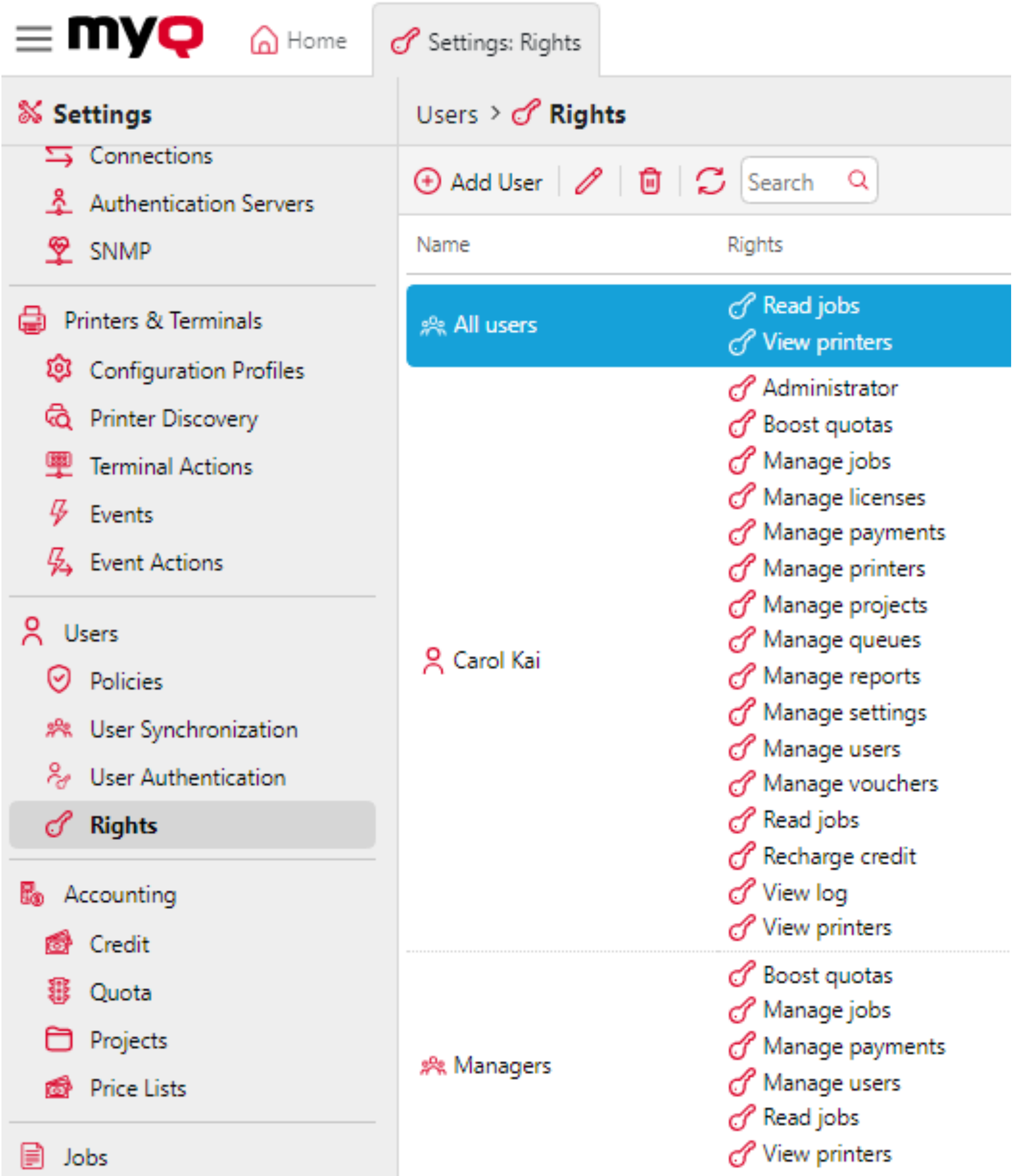
1. From the **Users** tab, select **Actions** from the top-right of the navigation bar, and click **Show Effective Policies**.
2. Select the user for whom you want to view effective policies, and optionally, a specific printer, and click **Show Effective Policies.**

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**.



9.12 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.



On the toolbar at the top, you can:

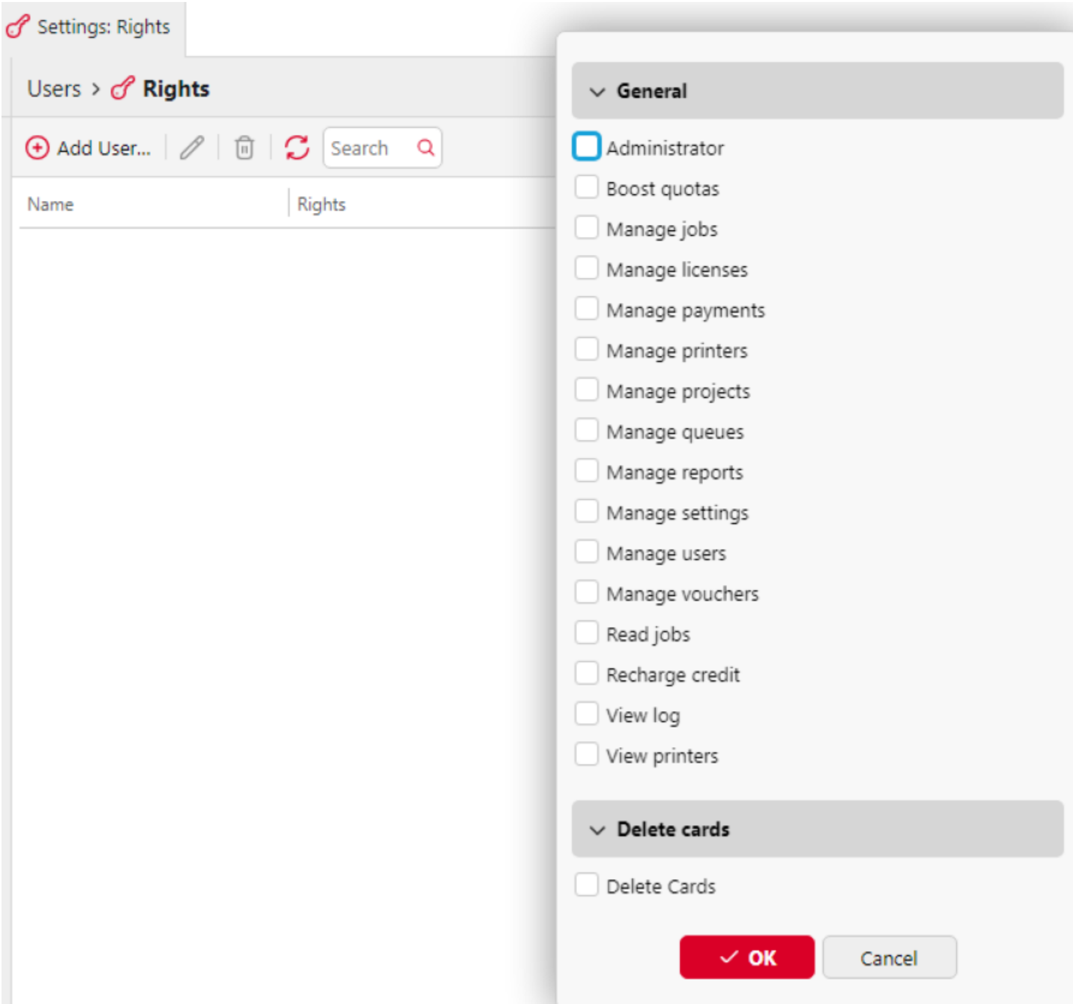
- **Add user** - add a new user or group with assigned rights.
- **Edit** - edit an existing user or group with assigned rights.
- **Delete** - delete a user or group with assigned rights.
- **Refresh** - refresh the list of users and groups.
- **Search** - search for a user or group with assigned rights. 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.

9.12.1 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.



9.12.2 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.

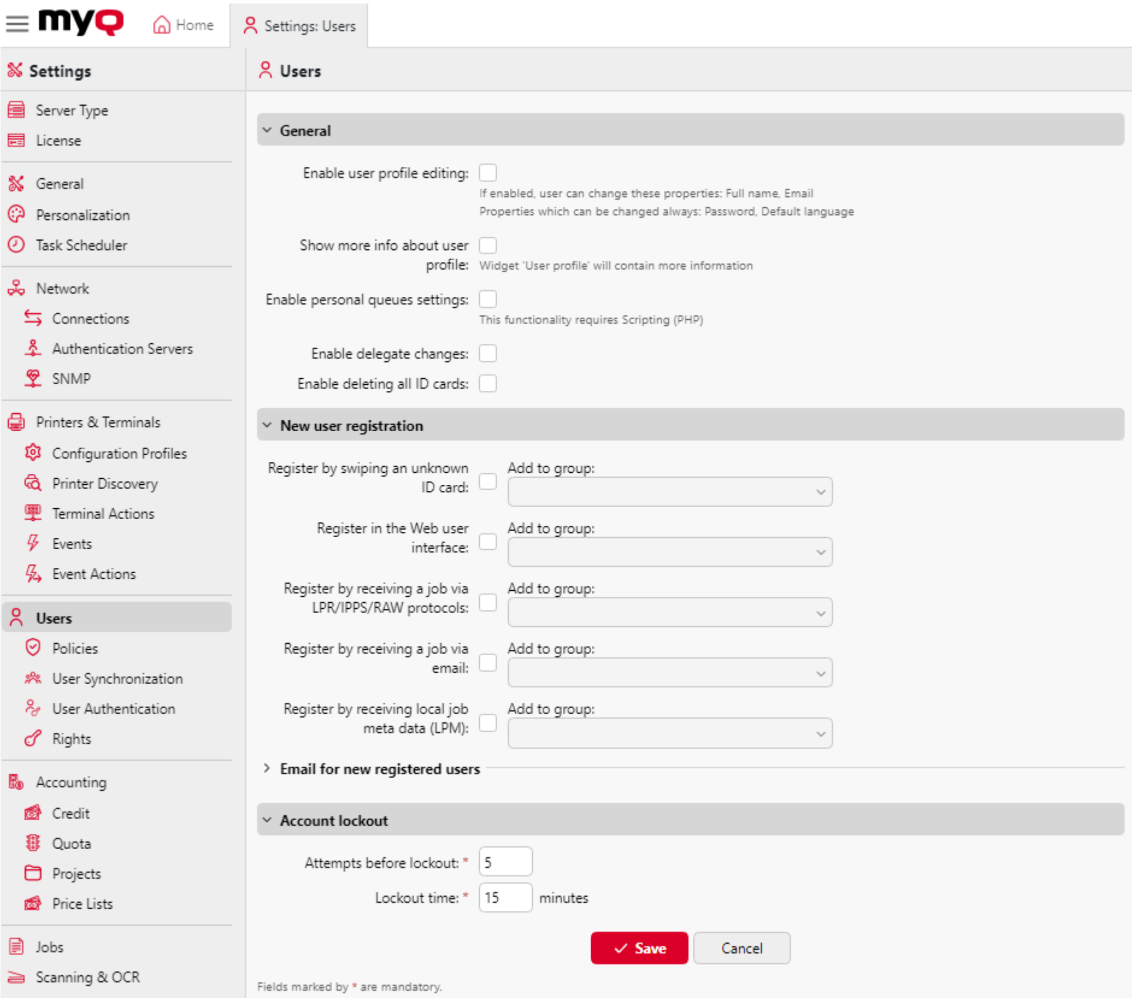
In the user rights panel, under the **General** section, you can assign rights concerning the general run of MyQ. These rights are described below:

- **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.

9.13 Users Settings

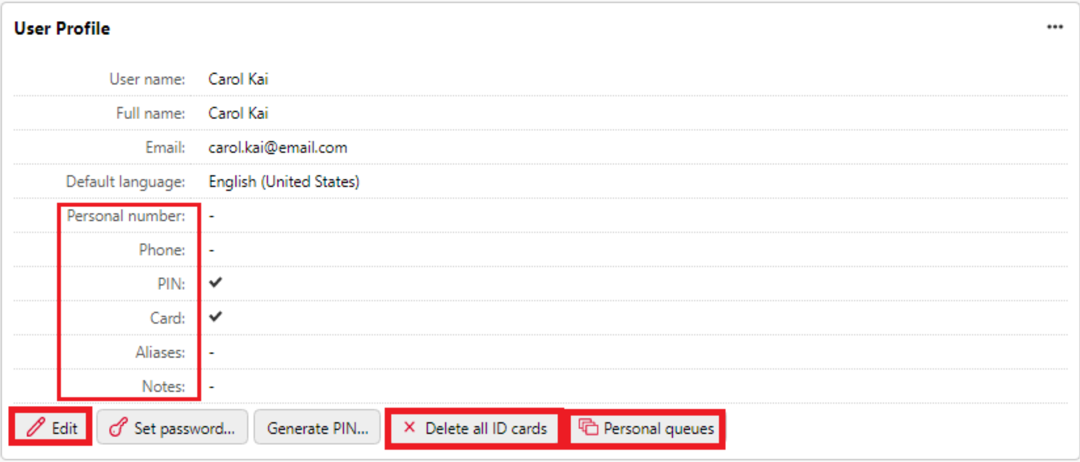
In the **Users** settings tab (**MyQ, Settings, Users**), the MyQ administrator can manage MyQ users’ **General** settings, **New user registration settings**, and MyQ **Account lockout** options.



General section

- **Enable user profile editing -** If enabled, users will be able to change their full name and email. For more information, check Enable user profile editing.
- **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. For more information, check Personal Queues.
- **Enable delegate changes -** If enabled, users will be able to change their delegates. For more information, check Delegated Printing.
- **Enable deleting all ID cards -** If enabled, users will be able to delete all their ID cards.

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:



New user registration section

In this section, the MyQ administrator can enable automatic user registration to MyQ in multiple ways, For more information, check Automatic user registration.

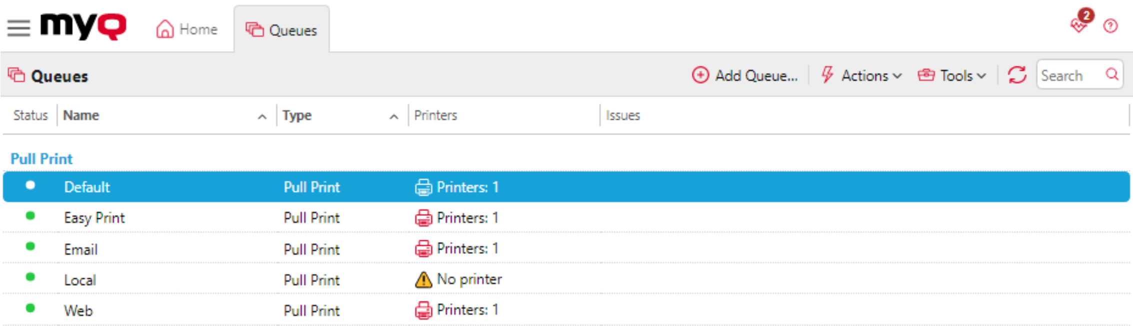
Account lockout section

In this section, the MyQ administrator can set the number of failed login **Attempts before lockout** (*5* by default), and the **Lockout time** in minutes (*15* minutes by default).

10 Queues

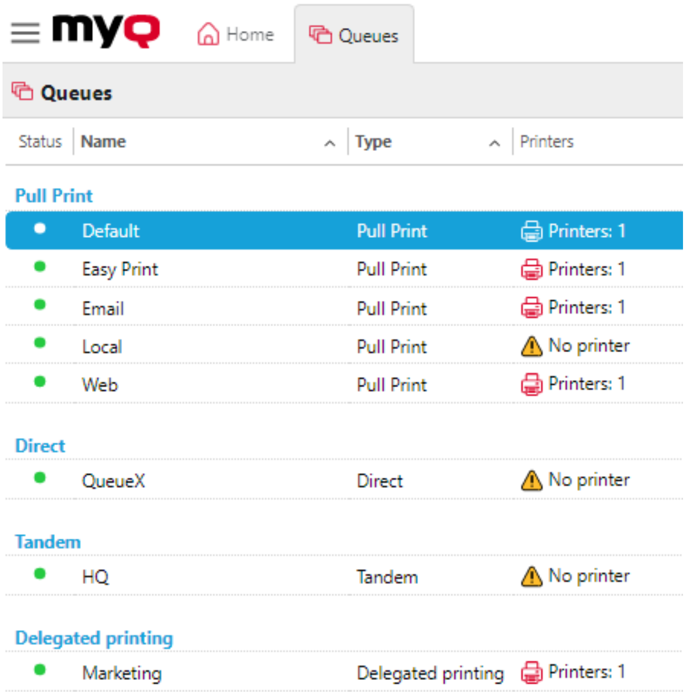
This topic discusses one of the key functions of MyQ: setup and management of print queues. It covers the following subjects:

- Overview, adding and deleting queues: List of queues, Adding, copying, and deleting queues.
- Individual queues settings: Editing queues.
- Direct, Tandem, Pull Print, and Delegated printing queue types: Queue types.
- Ways of detecting users: User detection methods.
- You can create collections of watermarks and associate them with queues: Watermarks.
- Some extra options for queues: Advanced queue options.



10.1 List of 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**.



10.1.1 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 MyQ Central and Site servers 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 only be used in a MyQ Central and Site servers environment; for more information, see the *MyQ Central Server Installation Guide*.
- **Job roaming delegated**: Delegated printing jobs used with job roaming are automatically assigned to this system queue. This queue can only be used in a MyQ Central and Site servers environment; for more information, see the *MyQ Central Server Installation Guide*.

10.2 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.

10.2.1 Direct queue type

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.

10.2.2 Tandem queue type

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.

10.2.3 Pull Print queue type

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 hardware terminal is required.

For more information on embedded terminals, see:

- MyQ Canon Embedded (10.1)
- MyQ Epson Embedded
- MyQ Fujifilm Embedded

- MyQ HP Embedded
- MyQ KATUN Embedded
- MyQ Kyocera Embedded
- MyQ Kyocera Embedded Lite (8.1)
- MyQ Lexmark Embedded (10.1)
- MyQ Ricoh SmartSDK Embedded (10.1)
- MyQ Sharp Embedded
- MyQ Sharp Luna Embedded (10.1)
- MyQ Toshiba Embedded (8.2)
- MyQ Xerox Embedded

10.2.4 Delegated printing queue type

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. For further information about the **Delegated printing** feature, see Delegated printing.

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.

10.3 Adding, Copying, and Deleting Queues

10.3.1 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**.

10.3.2 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.

10.3.3 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**.

10.4 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.

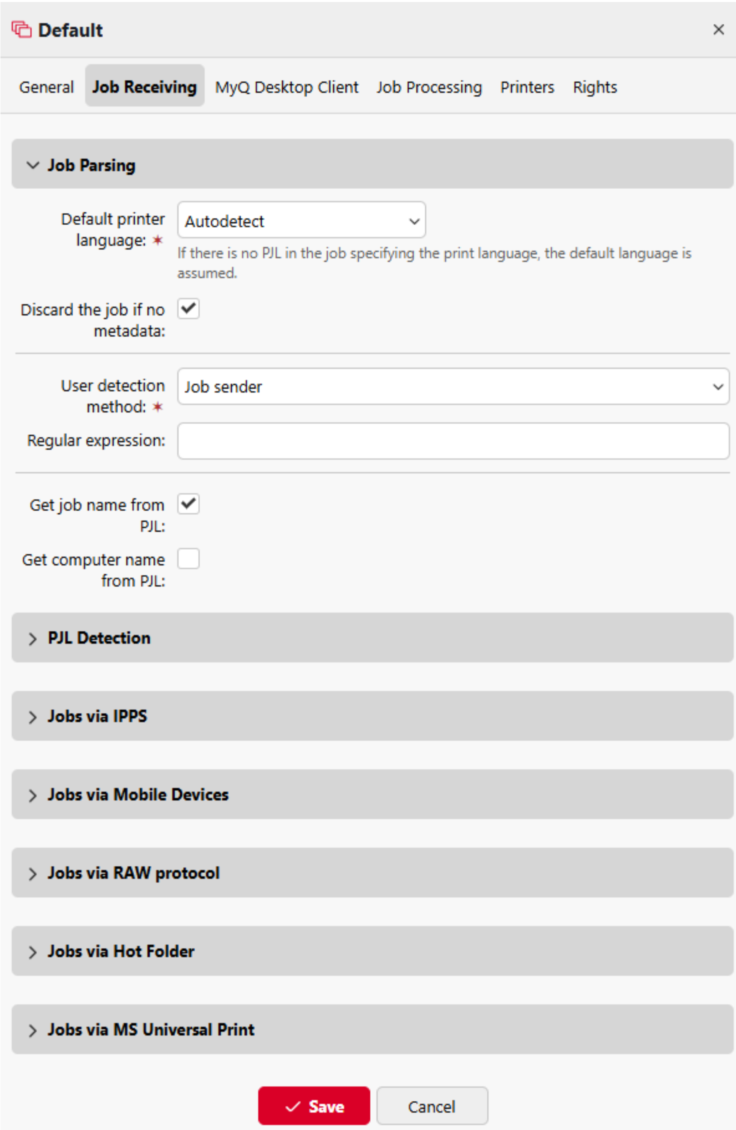
The basic setup of a queue can be done in four tabs: the **General** tab, the **Job receiving** tab, the **Printers** tab, and the **Rights** tab.

General tab settings

- **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*. For more information, see Queue types.

Job receiving tab settings

- **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. For more information, see User detection methods.
- **Get job name from PJL** - Set the queue to receive the job name from PJL.



Printers tab settings

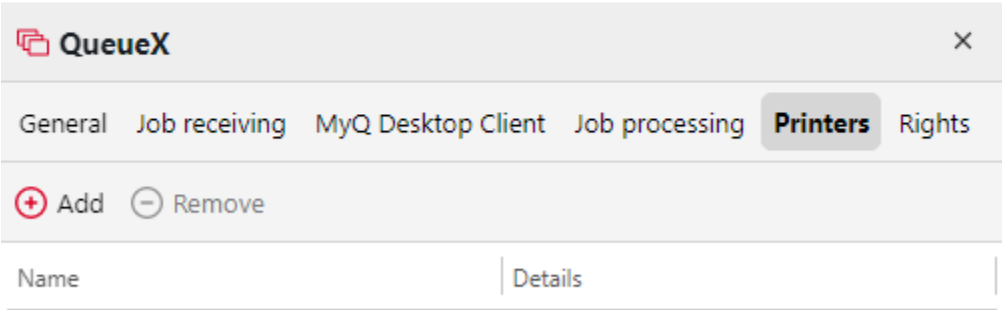
By default, the **All printers** group is automatically assigned to every queue. You can delete this group to restrict the number of assigned printers.

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.

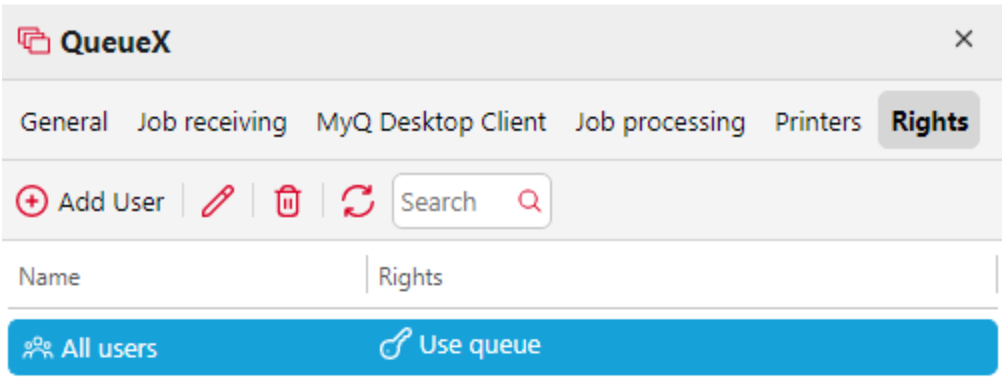


Rights tab settings

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:

1. 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.

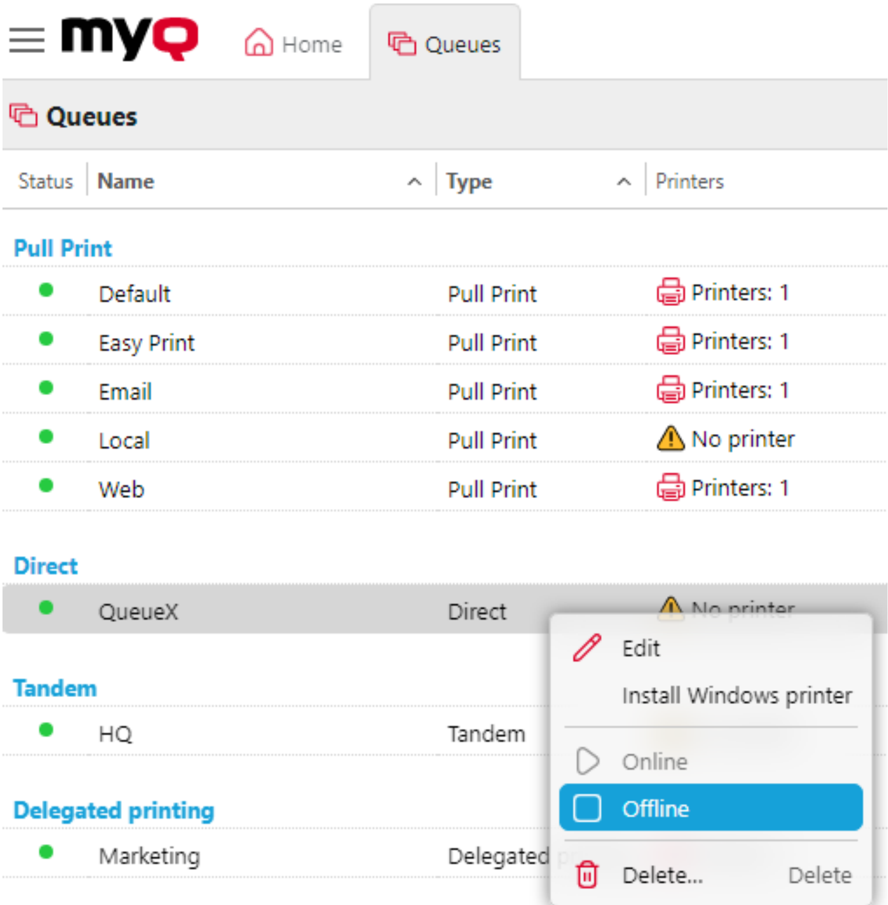
10.5 Online/Offline Queues

While the default queues are always online, each of the manually added queues can be switched to the offline mode. Queues switched to the 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 drop-down box appears.
2. In the Actions drop-down box, click **Offline** (or **Online**). The queue switches to the offline or (online mode).



10.6 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.

10.6.1 Activating the feature

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;}
```

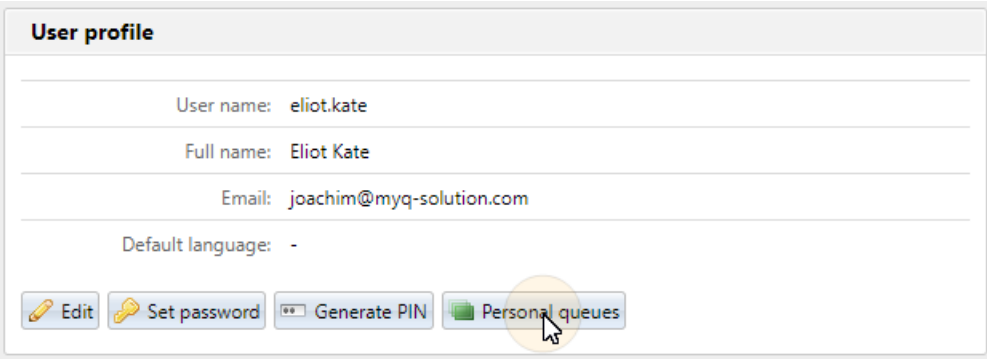
After the feature is set up, each user can see a button for setup of their personal queues on their account on the MyQ Web Interface.

10.6.2 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.

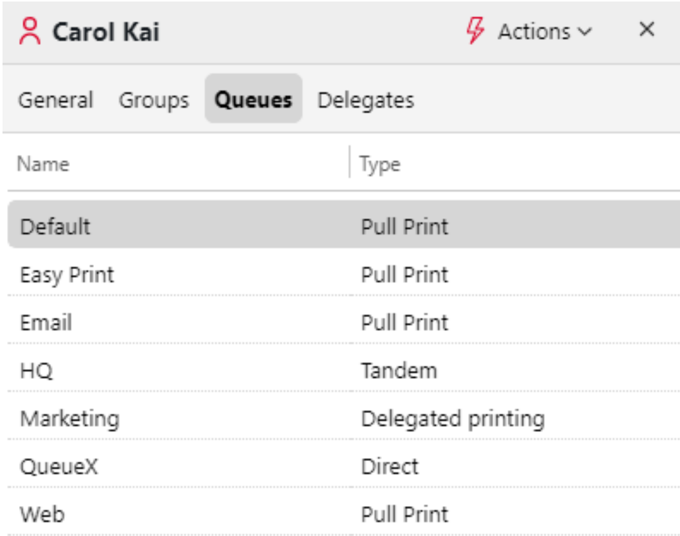


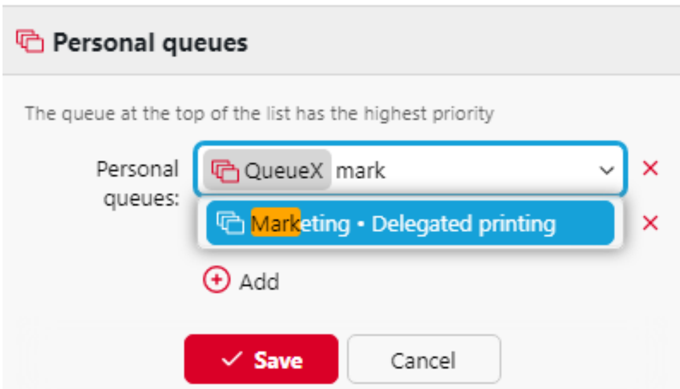
After the user sends the job, MyQ checks the personal queues and sends the job to the first queue with available printing devices.

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.





10.7 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
- Job receiving
- Job processing
- MyQ Desktop Client
- Job Scripting

10.7.1 General Tab

Available advanced settings on a queue's general tab:

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. You can find the available combinations in Print Job Policies.

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.

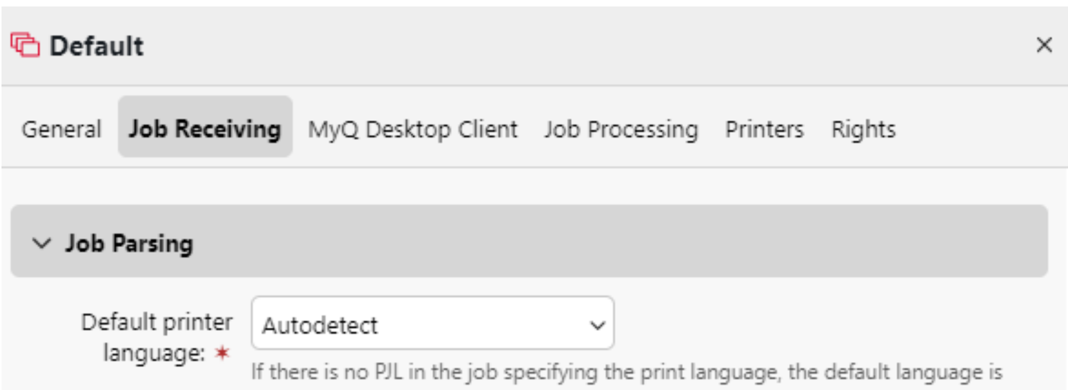
Policies section

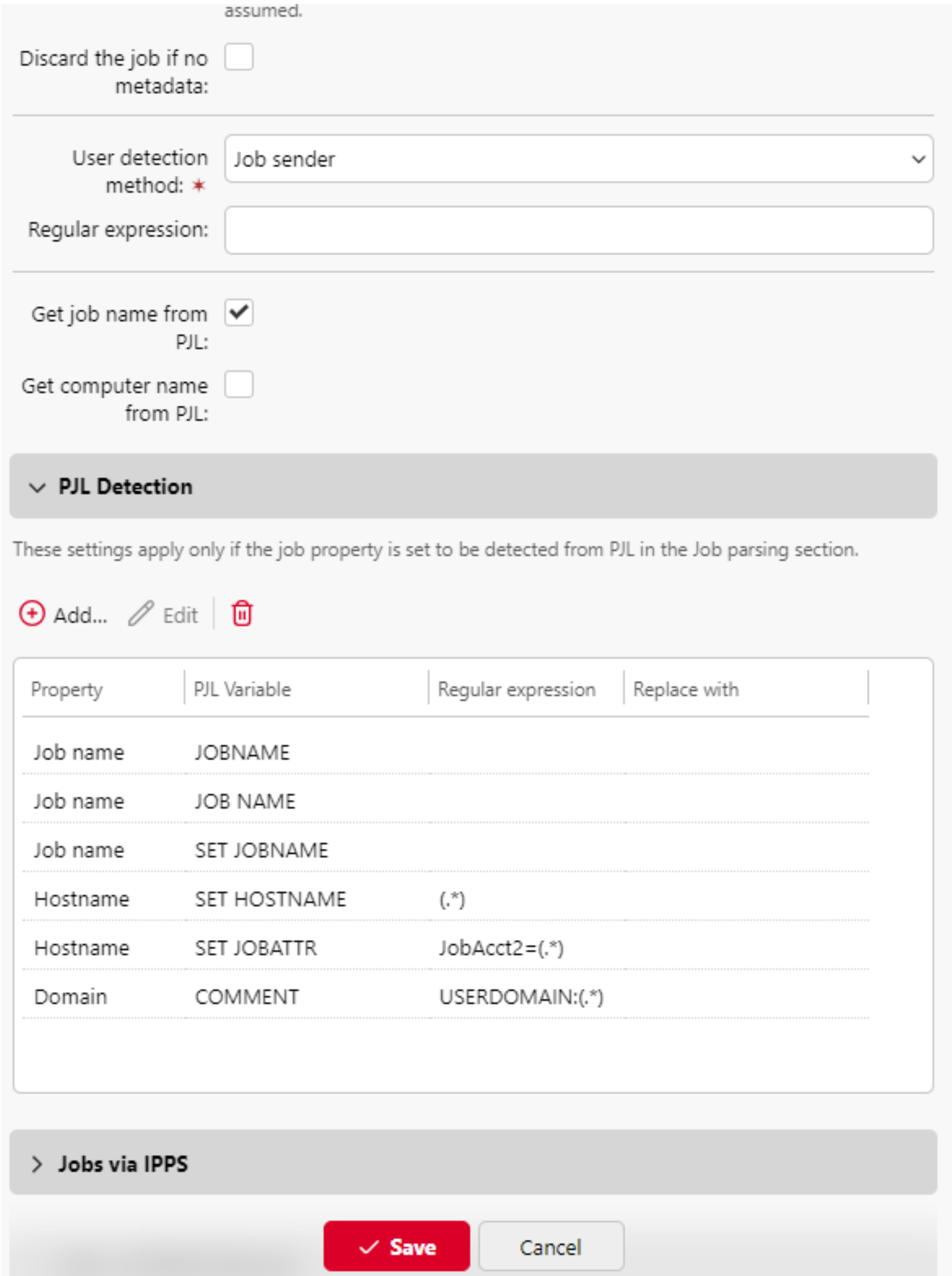
The final job settings are a combination of these queue settings, user policies and user changes made on the embedded terminal. All settings are set to *Do not change* by default.

- **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*

10.7.2 Job Receiving Tab

On the **Job receiving** tab of each queue, you can set how a job is parsed and other job receiving options.





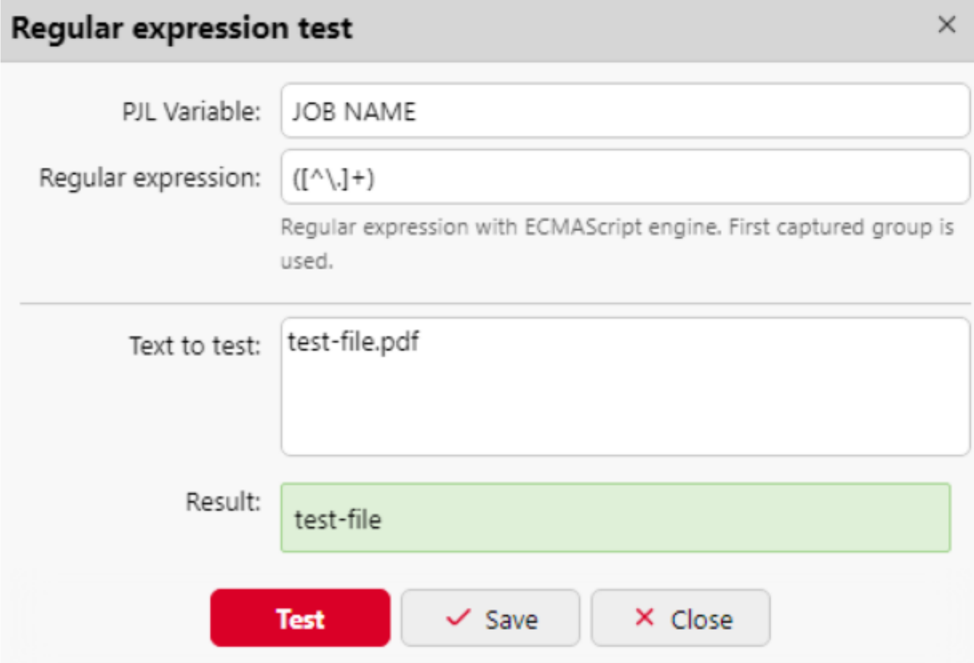
Job parsing section

- **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*".
  If you select this option, make sure that the Job Parser is enabled. In new installations the Job Parser is activated by default.
- **User detection method**: Select how the job owner is identified (*Job sender* by default). Described in detail in user detection methods.
- **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. Click **+Add** to enter PJL variables and regular expressions, **Edit** to modify any existing variables, **Test** to actually test if your regular expressions work, and **X** to delete a variable/regex set. The job name in the PJL header may differ from the printed document's name.
  In the below example, you can see how a variable/regex set works, and if it manages to find the job name from the PJL header:
    - In the **PJL Variable** field, there should be the *JOB NAME* variable, or any other variable used to detect the job name.
    - In the **Regular expression** field, there should be the regular expression you want to use in order to detect the job name. In the example, the *([^\.]+)* regex takes all characters before it reaches dot (which is specified as "\." – backslash is required in case of dot, because it is one of the special characters).
    - In the **Text to test** field, there should be the text from the print job's PJL header:
      test-file.pdf

After clicking **Test**, the test result is displayed at the bottom. In this example, *test-file* was successfully detected.



- **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. Click **+Add** to enter PJL variables and regular expressions, **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 **PJL Variable** field, there should be the *SET JOBATTR* variable, or any other variable used to detect the computer name.
  - In the **Regular expression** field, there should be the regular expression you want to use in order to detect the computer name.
  - In the **Text to test** field, there should be the text from the PJL header.

  After clicking **Test**, the test result is displayed at the bottom.

Jobs via Raw Protocol Section

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 Section

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 ("*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.

> To use this option, you first need to set up MS Universal print.

Jobs via Mobile Devices

In this section, you can make the queue available in the MyQ X Mobile Client, and in AirPrint and Mopria.

Mark the **Enabled** checkbox, and click **Save**.

> Only the *Job sender* user detection method can be used with this queue.

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:

- Job sender
- Sender's computer name
- Print server's DNS name
- Sender's computer DNS name
- Detect user from the job name
- MyQ Desktop Client
- User detection from PJL

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.

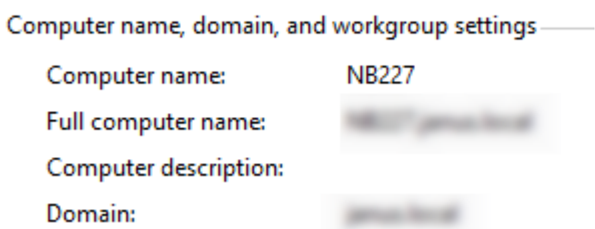
If the user logs on the account **Eliot.Kate** and sends the job from there, MyQ identifies them as **Eliot.Kate**.

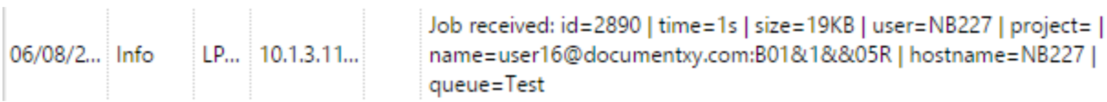
Sender's Computer Name

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.





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.

05/31/2...	Info	LPR ...	10.1.3....	Job received: id=2770 | time=1s | size=88KB | user=WIN-GOMOSMT0AO9.[illegible].local | project= | name=user16 | hostname=10.1.3.110 | queue=Test

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.

05/31/2...	Info	LPR ...	10.1.3....	Job received: id=2772 | time=1s | size=88KB | user=10.1.3.110 | project= | name=user16 | hostname=10.1.3.110 | queue=Test

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.

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.

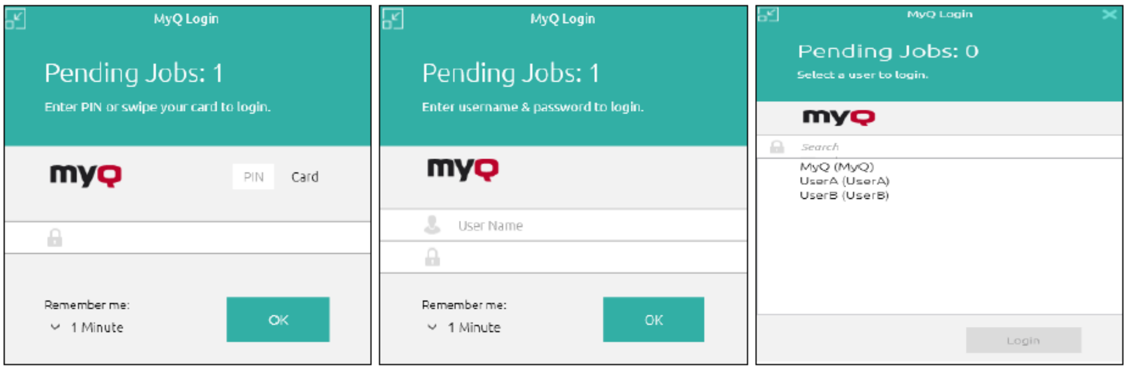
This advanced user identification method may be required, for example, for some prints from the SAP system. Prints from SAP are usually not sent directly to printing devices, but first to the Windows spooler (SAP LPD or SAP Print) which processes and forwards the prints to the device. This service usually 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.

MyQ Desktop Client

From Print Server Version 10.2 RC 8+ MyQ Desktop Client has been deprecated as a queue user detection method. You may still see this option listed in the web interface, but **Job Sender** or another detection method should be used.

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.

When a user sends a job to this queue, the job is automatically paused on the MyQ server and remains in the **Paused** status with the **unauthenticated* user as the job owner, until the user authenticates themselves via the MyQ Desktop Client application. Depending on the setting of the application's **Authentication method**, the user is prompted to either enter their PIN, swipe their card at a card reader, enter their user name and password, or select themselves on the list of all MyQ users. After the user is authenticated, the job's status on the MyQ server is changed to **Ready** and the job owner changes to the correct user name and it can be printed. If the user fails to authenticate themselves in MyQ Desktop Client, the job is rejected.



For information on how to install and set up MyQ Desktop Client, see the (10.2) MyQ Desktop Client documentation.

In cases where there is no card reader connected to the computer where the users identify themselves from, users can type the card number instead of swiping it.

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.

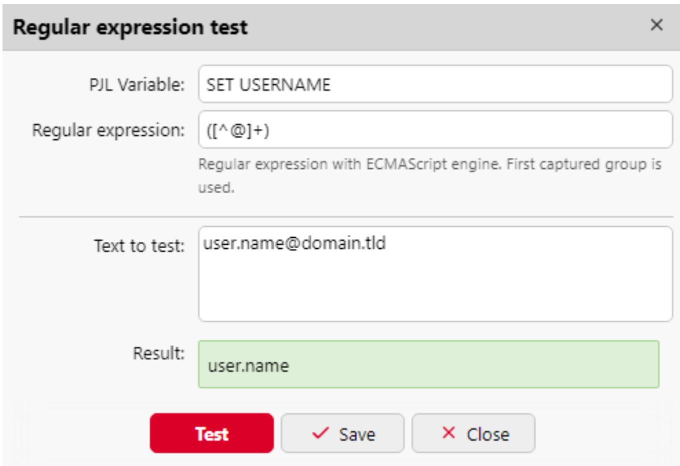
A regular expression can be used to capture a part of the detected string. If no regular expression is specified, the whole string of the PJL variable is used.

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:

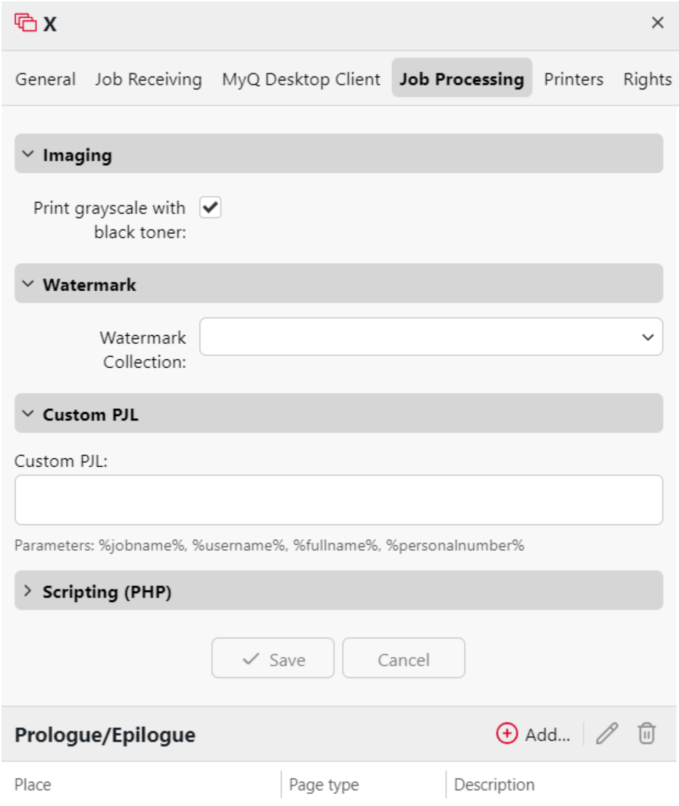
- In the **Text to test** field, there should be the text from the print job's PJL header:
  user.name@domain.tld
- In the **PJL Variable** field, there should be the *SET USERNAME* variable, or any other variable used to detect the job owner.
- In the **Regular expression** field, there should be the 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.



10.7.3 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 section

Mark the checkbox if you want to **Print grayscale with black toner**.

Watermark section

Choose your saved watermarks from the **Watermark** drop-down.

Custom PJL section

In the **Custom PJL** field, 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=A*4 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.

Scripting (PHP) section

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.

Scripting is detailed in Job Scripting.

Prologue/epilogue section

You can find further details in Prologue/epilogue.

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.

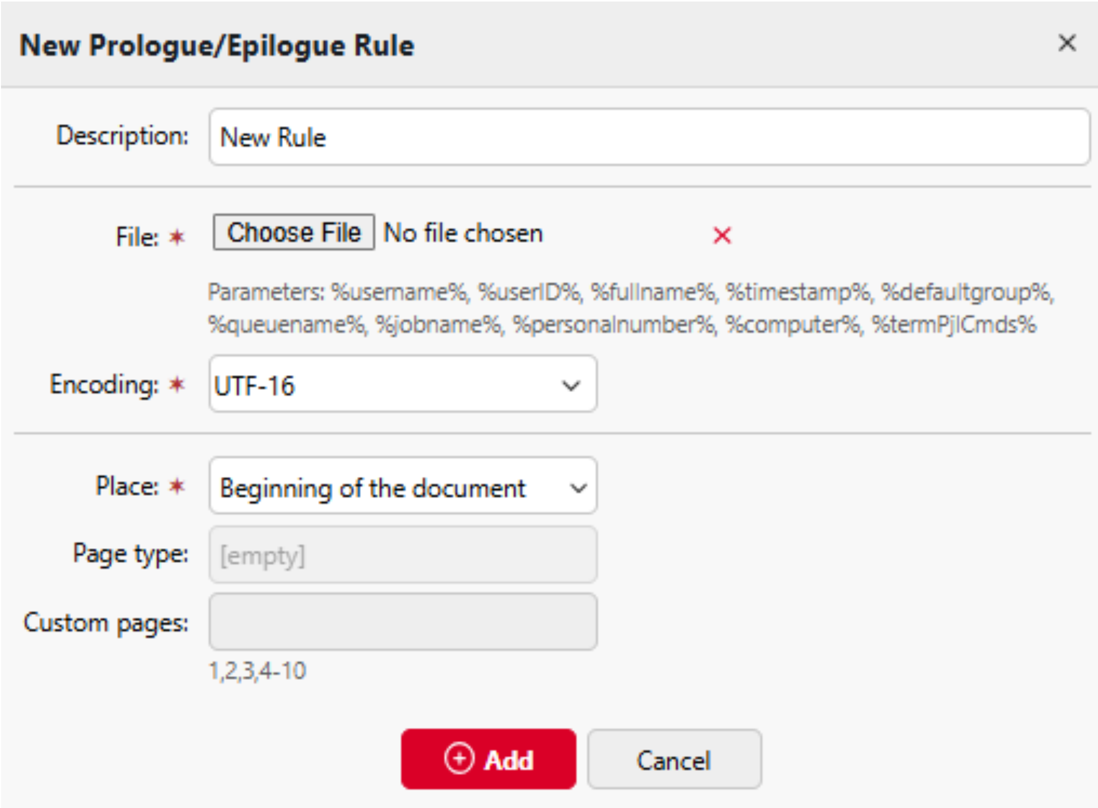
Adding, Editing, and Deleting Rules

The 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.

10.7.4 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.

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**.

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:

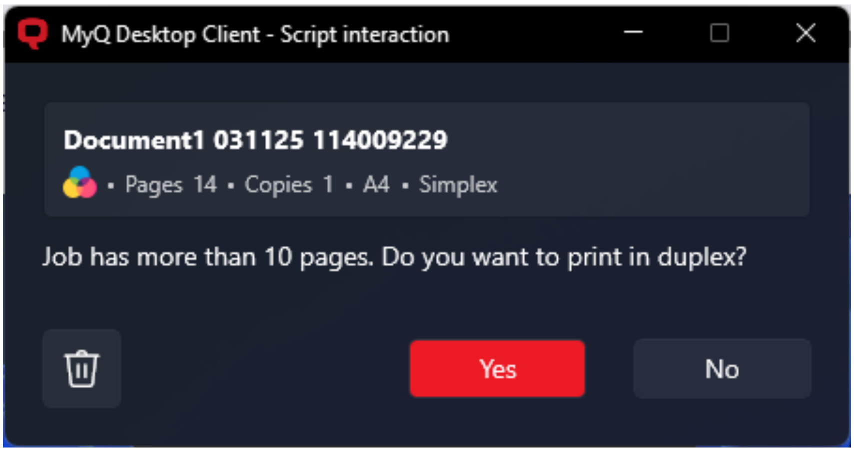
```
public $hasMoreThan10pages;

// 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).

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 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.

There are five classes that can be used within the scripts: Job, User, Queue, Session, and QuotaInfo. 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.

Job Class

The **Job** class has the following methods and properties:

Methods

- this **pause**() - Pause the job.
- this **copyToQueue**(string $queueName) - Copy the job to queue `$queueName`. The new job is processed normally according to the rules in the target queue.
- this **moveToQueue**(string $queueName) - Move the job to queue `$queueName`. The new job is processed normally according to the rules in the target queue.
- this **setReleased**() - Set the job as released (printed) without actually releasing it. (`setPrinted` is still supported for BC).
- this **delete**() - Delete the job.
- this **setProject**(string $projectCode) - Assign the job to the given project by project code.
- this **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

Name	Type	Writable	Description
colorCount	int	yes	Count of the color pages of the job
pageCount	int	-	Total sum of the pages of the job
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	Writabl e	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.
tonerSavi ng	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 options are available: no, yes, topRight, twoStaples.
punching	string	yes	Punches the document, the following options are available: no, yes, twoHoles, threeHoles, fourHoles.

User Class

The **User** class has the following methods and properties:

Methods

- this **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.
- this **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.
- this **logError(***string $message***) -** Create an error message in the MyQ log.
- this **logWarning(***string $message***) -** Create a warning message in the MyQ log.
- this **logInfo(***string $message***) -** Create an info message in the MyQ log.
- this **logNotice(***string $message***) -** Create a notice message in the MyQ log.
- this **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.

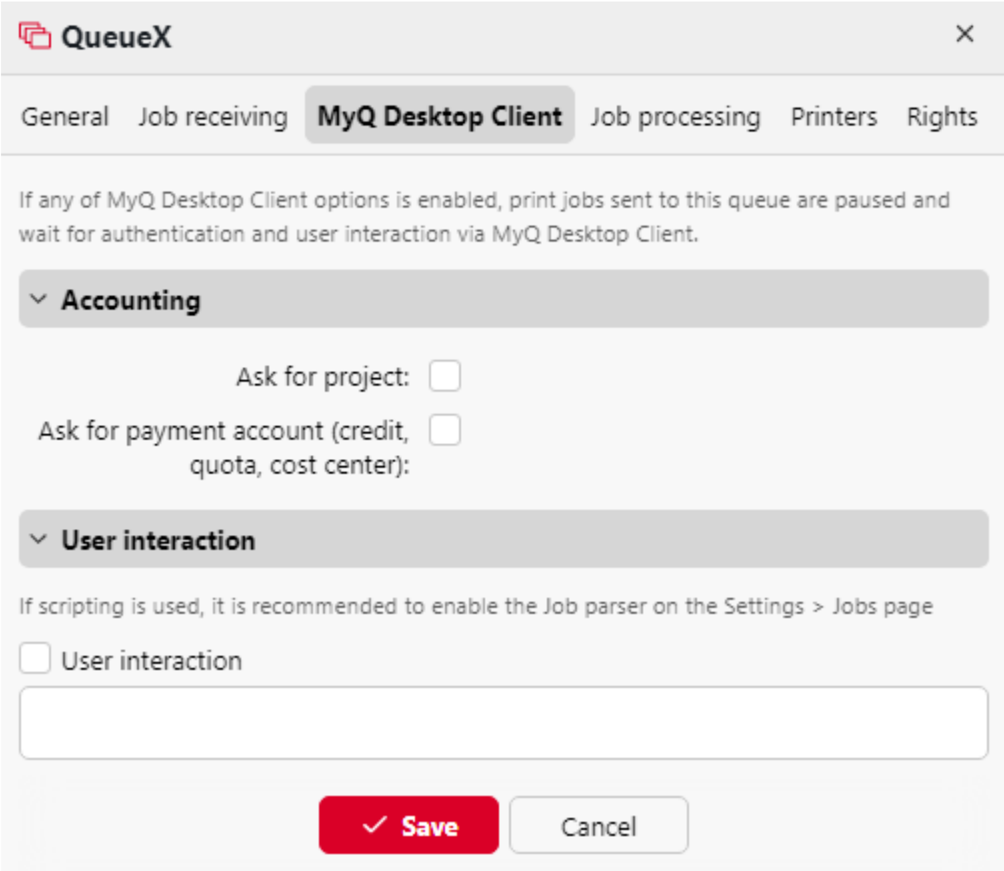
QuotaInfo Class

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.

10.7.5 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** (described in User Interaction Scripting), add the script in the field, and click **Save**.

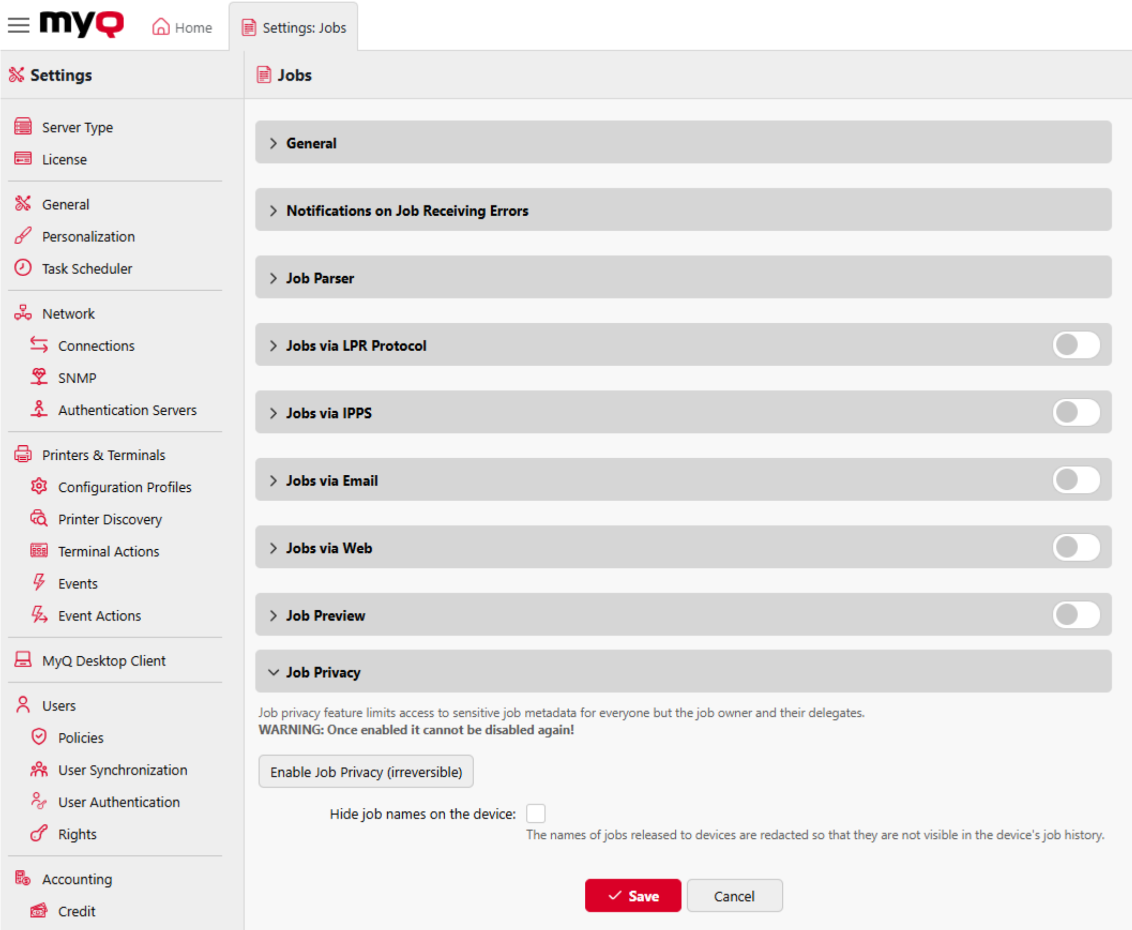
11 Jobs

This topic discusses one of the key functions of MyQ — setting and management of print jobs. It covers the following subjects:

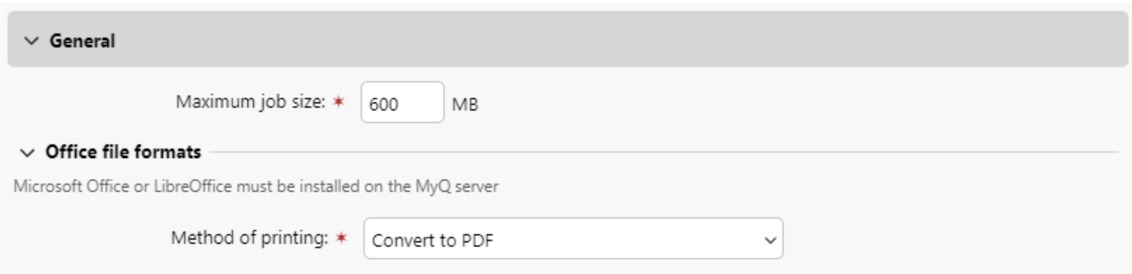
- Print jobs global settings: Jobs settings tab
- Print jobs list, individual jobs settings and deleting jobs: List of jobs, Editing & Deleting jobs.
- Print jobs parser: Jobs Parser
- Notifying users and the administrator about refused jobs: Notifying the admin and users about refused jobs
- Using PJL commands for additional job processing actions: Processing Jobs via PJL Commands
- You can use PHP scripts to further process the job after it is received by the MyQ server: Scripting (PHP)
- When your brand supports PDL (page description language) check out this chapter: Prologue, Epilogue
- Setting up and previewing jobs: Jobs Preview
- When you have a dedicated Job Archiving license and the Job Preview feature set up on the MyQ server, you can automatically archive all print jobs that are sent to MyQ: Job Archiving

11.1 Jobs Settings Tab

On the **Jobs** settings tab, you can set the global properties of jobs in the MyQ print environment.



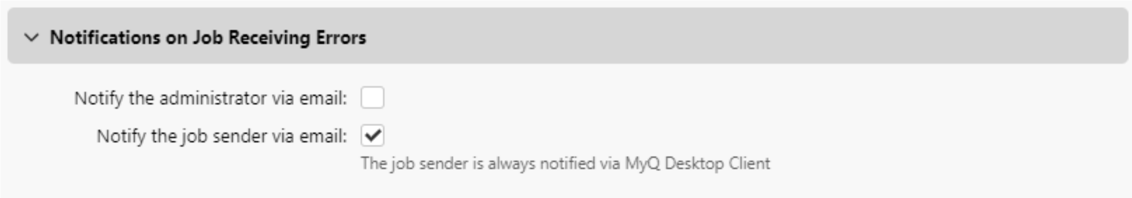
11.1.1 General



Here you can set the **Maximum job size** (default size is *600MB*).

In the **Office file formats** subsection, you can select the method of processing and printing the Office format files. You can select from *Convert to PDF* (default) and *Via a Windows printer*. For details check Processing documents in Office formats.

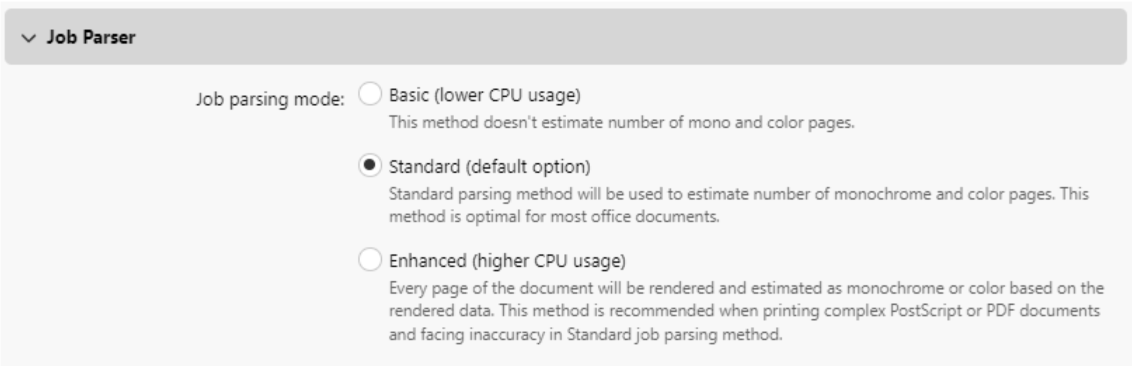
11.1.2 Notifications on Job Receiving Errors



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.

11.1.3 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.

11.1.4 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.

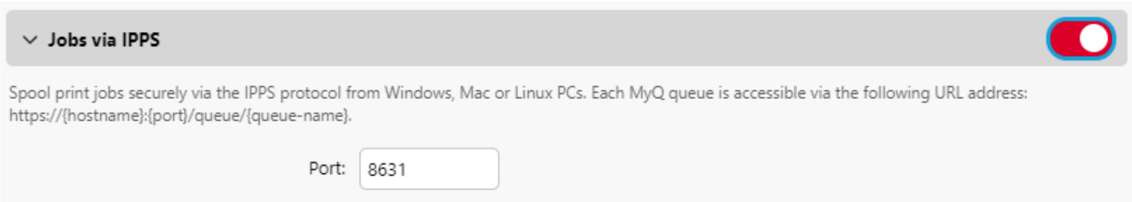
The server knows the job sender (to be able to notify MyQ Desktop Client about job processing) through the hostname sent by the LPR protocol. The maximum length of the hostname is 31 characters.

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*).

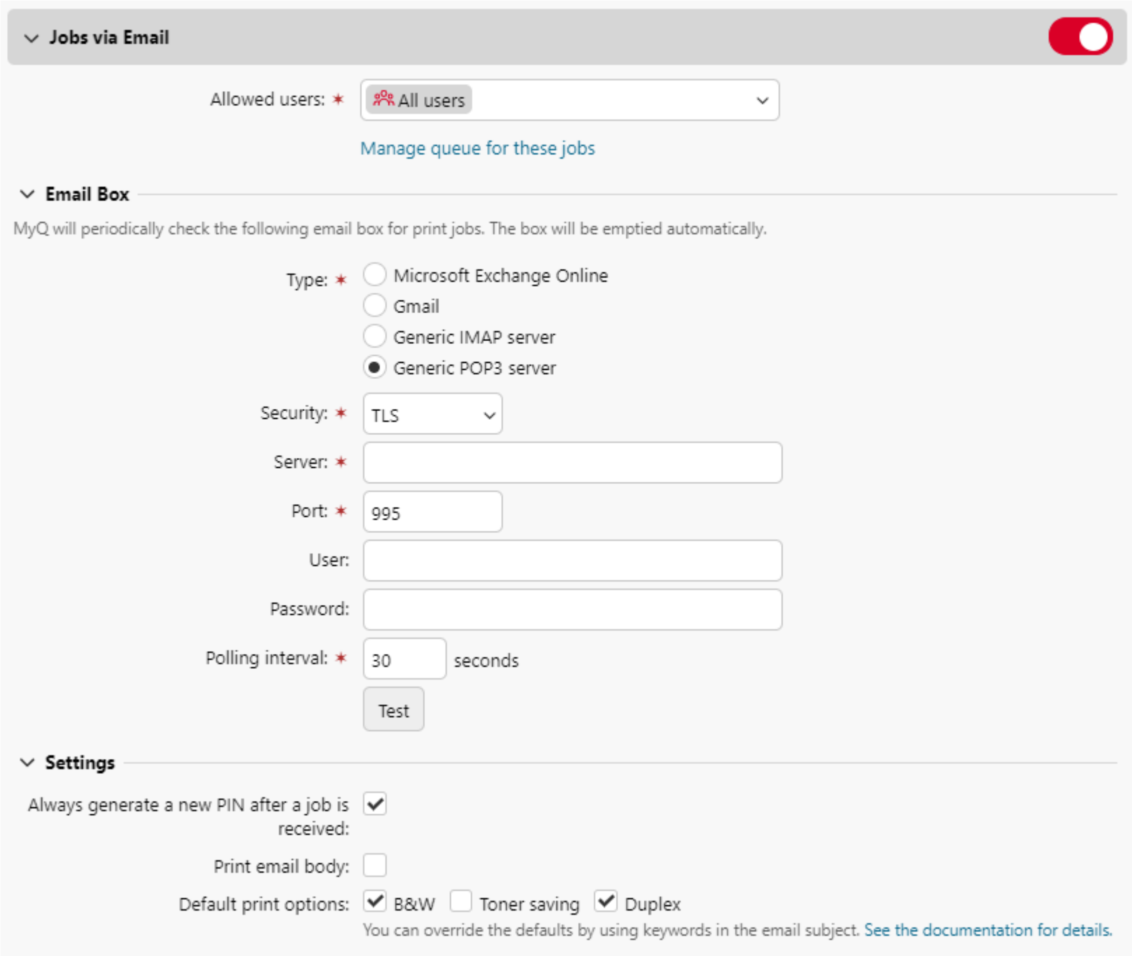
11.1.5 Jobs via IPPS



Here you can enable printing jobs via the IPPS protocol. You can also change the **port** here (default is *8631*).

For more information, see Jobs via IPPS.

11.1.6 Jobs via Email



Here you can enable or disable the **Jobs via Email** feature, which enables receiving print jobs sent via email. The email attachment is processed and sent as a print job (the email body can be processed as well). PDF/A, TXT and JPEG formats are supported. For MS Office formats, MS Office or LibreOffice must be installed on the MyQ server.

You can select the **Allowed users** who are able to send **Jobs via Email** and manage which queues will be used for these jobs.

You can set up an **Email Box**, a specified email which will be regularly checked for print jobs, the inbox will be emptied automatically. Enter the **Type** of box (Microsoft Exchange Online, Gmail, Generic IMAP server, or Generic POP3 server), the **Security** (none, TLS, or STARTTLS), the **Server**, **Port**, **User**, **Password**, and **Polling interval** in seconds.

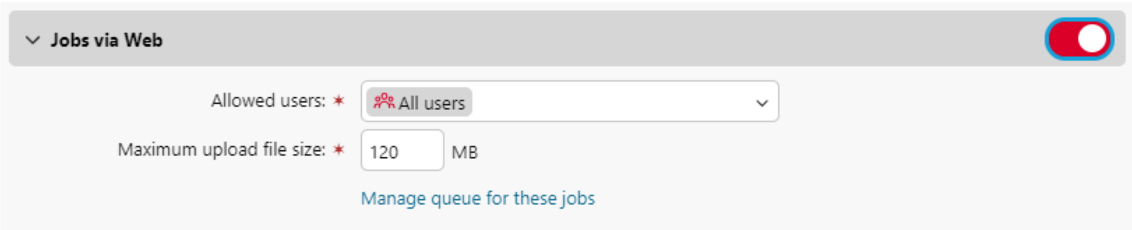
Additionally, in the **Settings** section you can:

- Enable the option to **Always generate a new PIN after a job is received**, this will generate a new PIN for a user each time they send a job via email.
- Enable **Print email body**, which will print the main text of an email in addition to any attachments.

- Dictate **Default print options** for jobs via email, choose from **B&W**, **Toner saving**, and **Duplex**.

For more information, see Printing from email and from the MyQ Web UI.

11.1.7 Jobs via Web

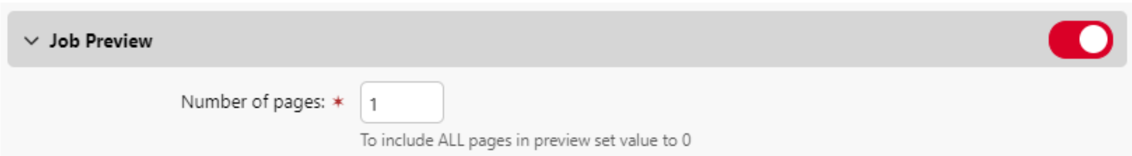


Here you can enable or disable the **Jobs via Web** feature, which enables users receiving print jobs via the MyQ web interface. You can also set the maximum job file size here between *20MB* to *120MB* (*120MB* by default).

Select the **Allowed users**, and the **Maximum upload file size**, the default is 120MB.

For more information, see Printing from email and from the MyQ Web UI.

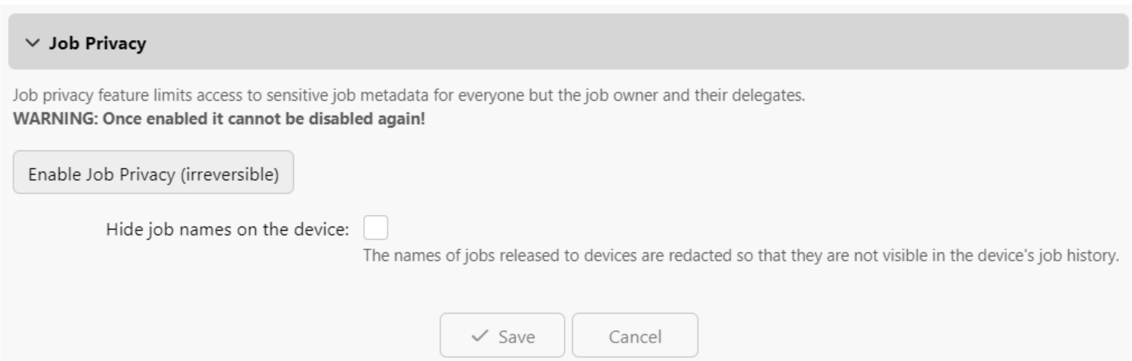
11.1.8 Job Preview



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).

For more information, see Jobs preview.

11.1.9 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.

For more information, see Job Privacy.

11.1.10 Watermark Collections

Here you can set up watermark collections.

For more information, see Watermarks.

11.2 List of Jobs

On the list of jobs on the **Jobs** main tab, you can see all print jobs and information about them.

11.2.1 Jobs display options

On the left side of the **Jobs** main tab, you can see the **All jobs** drop-down menu. On the menu you can select from the following options:

- **Ready** - Displays jobs ready to print.
- **Paused** - Displays paused jobs.
- **Printed** - Displays printed jobs.
- **Favorite** - Displays favorite jobs.
- **Failed jobs** - Displays failed jobs.
- **Deleted** - Displays deleted jobs.
- **All** - Displays all jobs.

11.2.2 Job status

There are seven print job status types:

- **Processing** - The job is being examined and prepared for printing.
- **Ready** - The job has been placed on a print queue and is waiting for users to authorize it or for preceding jobs to finish.
- **Paused** - The job has been manually paused by the user or automatically by the MyQ system.
- **Printing** - The job is being sent to the printing device.
- **Printed** - The job has been printed and is stored on the MyQ server. The print job is marked as Printed when it was completely sent to the printer. On a printer where MyQ can check actual printing results (printers with EMB terminal 8.1 and higher), this status is updated according to the printing results.
- **Failed** - The job was either not parsed correctly, failed to be processed or had no metadata (not allowed) and failed to be printed. Failed jobs will be automatically deleted after the number of days set in the **History** section of your Log settings.
- **Deleted** - The job has been deleted from the MyQ server.

11.2.3 Favorite jobs

All print jobs, except for the deleted ones, can be marked as **Favorite**. Favorite print jobs are only automatically deleted if this option is enabled in the System management settings, and remain permanently stored on the MyQ server, except for favorite jobs from external code books that are no longer available at the code book's data source.

11.3 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. For more information, see Job Parser.

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.

11.3.1 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.

11.4 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.

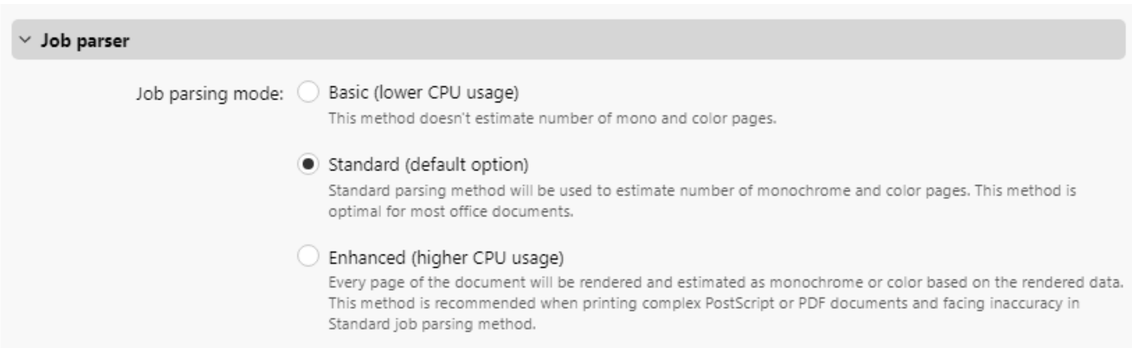
The job parser supports the majority of available printer drivers in PCL5, PCL6 and PostScript.

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**:



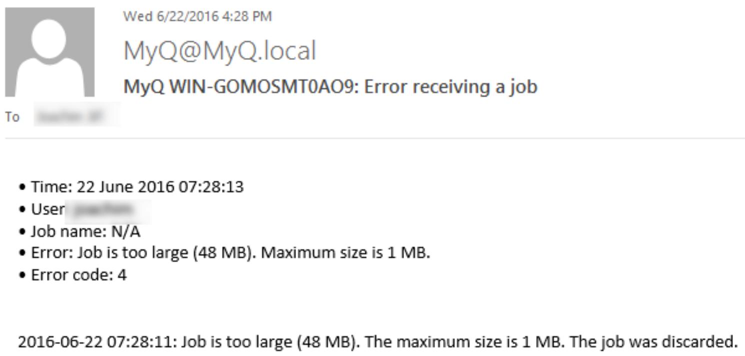
- **Basic (lower CPU usage)** - This method doesn't estimate the number of mono and color pages.
- **Standard (default option)** - The standard parsing method will be used to estimate the number of monochrome and color pages. This method is optimal for most office documents.
- **Enhanced (higher CPU 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.

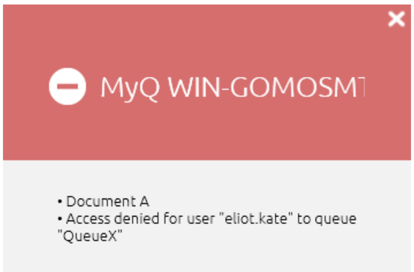
11.5 Notifying the Admin and Users about Refused Jobs

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.

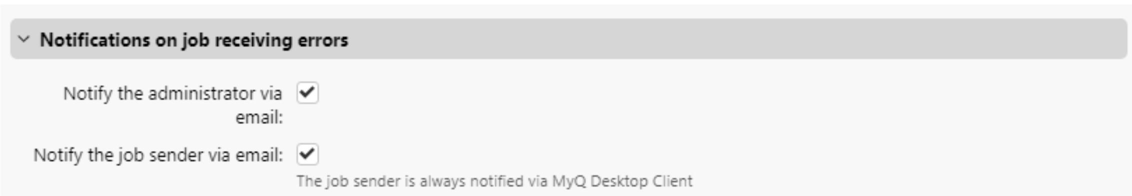




To activate the notifications via email

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

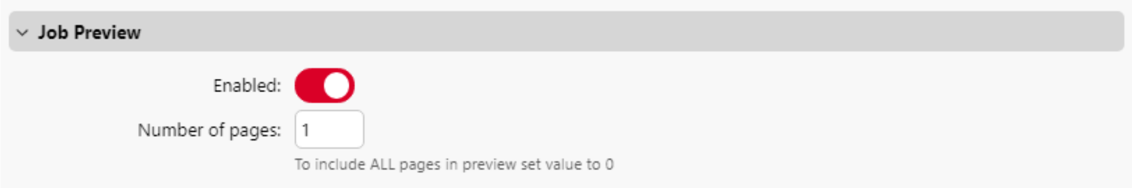
The only condition for activation of the pop-up notification for a user is for MyQ Desktop Client to be installed and running on their computer.

For information on how to install and set up MyQ Desktop Client, see the *MyQ Desktop Client for Windows or macOS* guide.

11.6 Job Preview

The **Job Preview** feature is used to generate previews of jobs. 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.

11.7 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.

11.7.1 Setting up job archiving

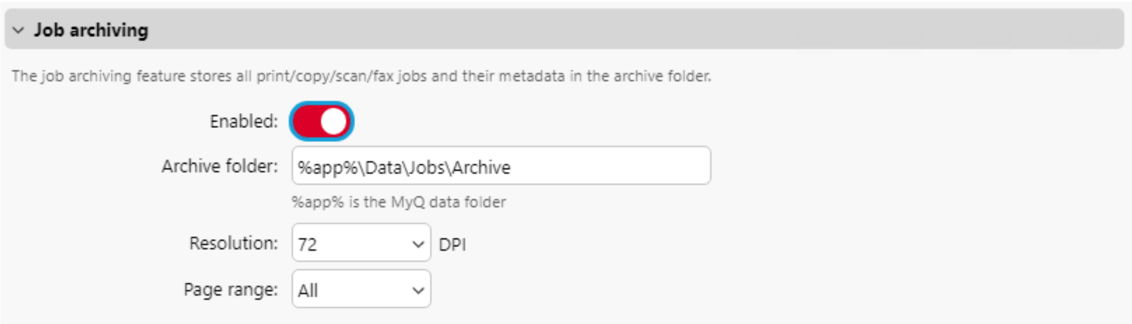
The feature is not part of the default setup of the MyQ server and before the **Job archiving** license is added to the server, the settings of the feature on the MyQ Web Interface are hidden from the administrator.

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.*

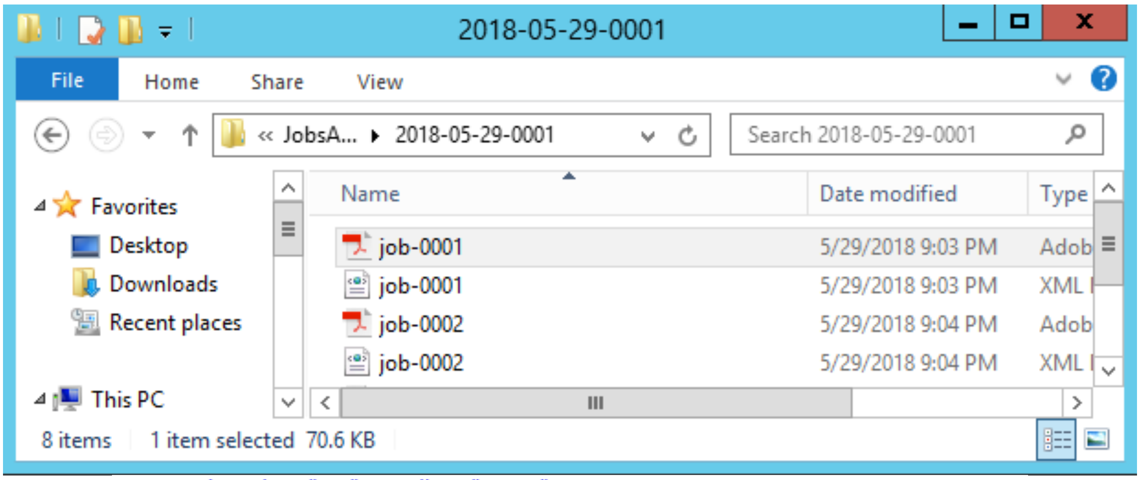


11.7.2 Viewing archived jobs

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.




```
<?xml version="1.0" encoding="UTF-8"?>
- <data>
    <timestamp>2018-05-29 21:03:39</timestamp>
    <username>eliot.kate</username>
    <jobType>copy</jobType>
    <serverName>10.14.5.96</serverName>
    <serverVersion>7.1.0.366</serverVersion>
    <printerAddr>10.14.4.12</printerAddr>
  - <files>
      <file>job-0001.pdf</file>
    </files>
</data>
```

11.8 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.

Prerequisites

- IPP client is enabled on both the server running Print Server and the client machines.
  On Windows 10, 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.
  For example, in MyQ Server 8.2+, you can create a self-signed certificate in the following way (see Network Settings for more information):
  a. Go to **MyQ > Settings > Communication Security**.
  b. Select *Built-in Certificate Authority*, add your hostname as a Subject Alternative Name (SAN), click **Generate new**, click **Save**, and then **Export**.
  c. Install the certificate and place it into Trusted Root Certification Authorities.
  d. Restart all MyQ services.

11.8.1 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. Click **Save**.
5. Configure each IPP client with the URL *https://{hostname}:{port}/queue/{queue-name}*

Notes:

- Do not use ports 631 and 717. These are reserved by the PM Server for IPP and IPPS, respectively.
- 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.

11.8.2 View IPPS Hostname and Port

You can easily view the IPPS URL, with hostname and port, for your Print Server. Go to **Queues>Add Queue**, and check the **Jobs via IPPS** section of the **Job Receiving** tab.

11.8.3 Configure IPPS on Clients

Now, you are ready to use IPPS for job submission. Continue to the Deployment guide on IPPS printing, where you find steps to configure an IPPS printer on Windows, macOS, Chromebook, and Linux clients.

11.8.4 Supported Features

User Authentication

IPP supports user authentication out of the box. During printing, the IPP server can return to the client that it requires authentication. The user might then be prompted to enter credentials for an existing MyQ X account to submit a document.

This feature is generally well-supported on macOS or mobile clients, but it is not supported well on Windows yet; instead, the job is identified from the username of the job submitter.

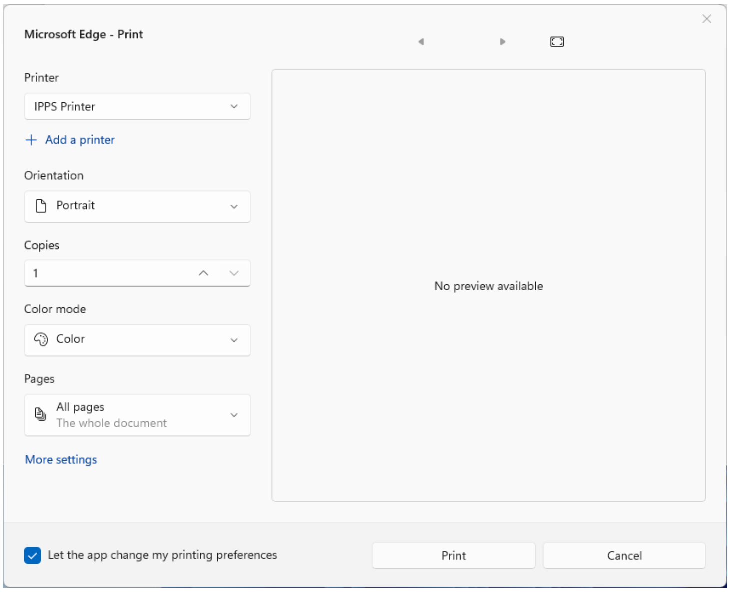
Standard Print Options

The IPPS Server offers a set of standard print options available to be changed by the printing user. Since the IPPS protocol is a driverless printing method designed primarily for compatibility, it offers commonly used printing preferences but does not support advanced finishing, tray selection, and various other preferences found in regular print drivers.

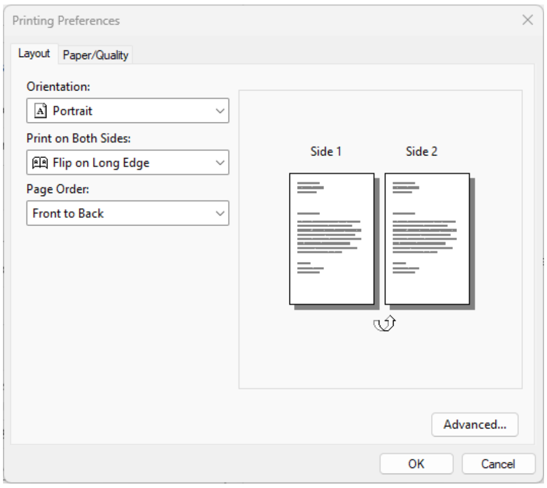
The supported print options are the following:

- Copies
- Color mode: Color, Monochrome, Grayscale
- Pages: All pages, Custom (page range selection)
- Duplex (Print on both sides): Flip on Long Edge, Flip on Shoer 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)

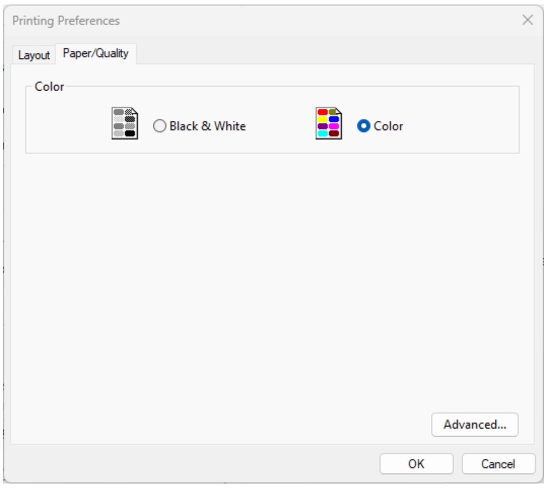
The available options and their names will also differ depending on the OS used and the application from which the user is printing. Some apps might always display some print options despite their lack of support in MyQ X, these will be ignored during processing and release.



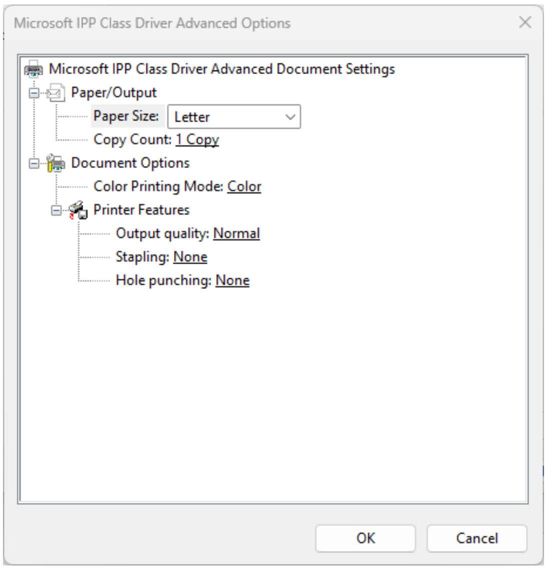
Microsoft Edge - Print
Printer
IPPS Printer
Add a printer
Orientation
Portrait
Copies
1
Color mode
Color
Pages
All pages
The whole document
More settings
No preview available
Let the app change my printing preferences
Print
Cancel

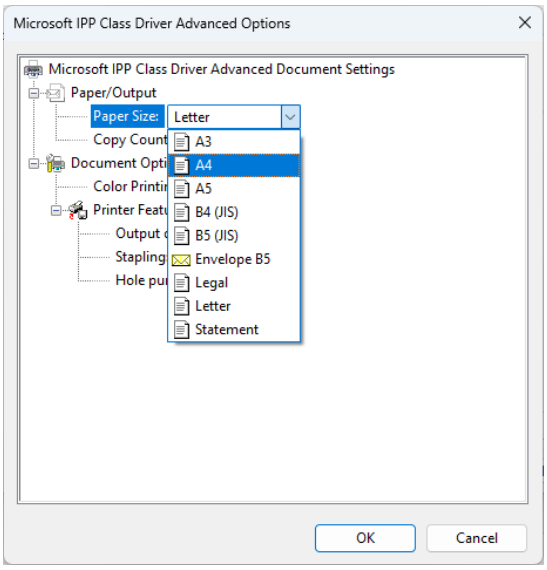


Printing Preferences
Layout
Paper/Quality
Orientation:
Portrait
Print on Both Sides:
Flip on Long Edge
Page Order:
Front to Back
Side 1
Side 2
Advanced...
OK
Cancel



Printing Preferences
Layout
Paper/Quality
Color
Black & White
Color
Advanced...
OK
Cancel

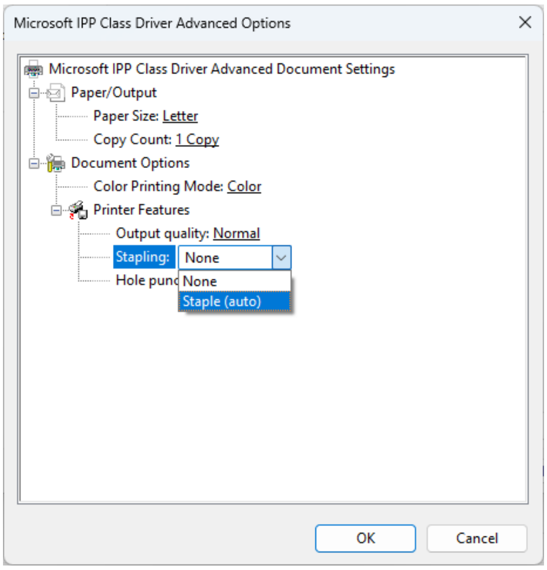


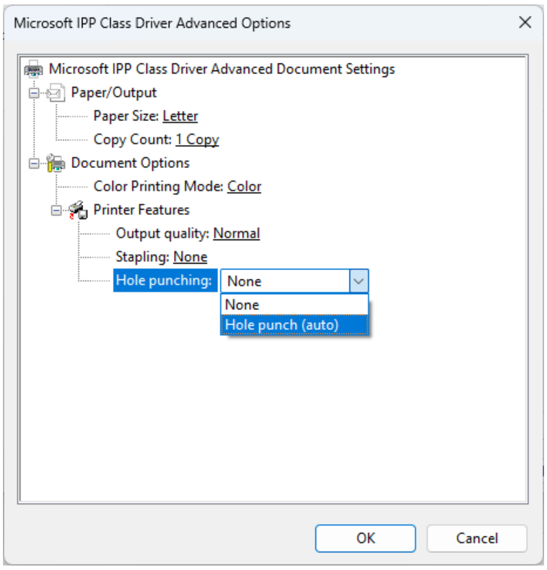


Finishing Options

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.





11.9 Job Privacy

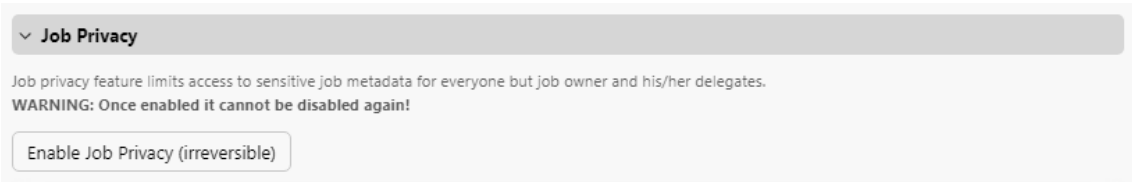
The Job privacy feature limits access to sensitive job metadata for everyone, except for the job owner and their delegates.

You can enable the feature in the **Jobs** settings tab (**MyQ, Settings, Jobs**).

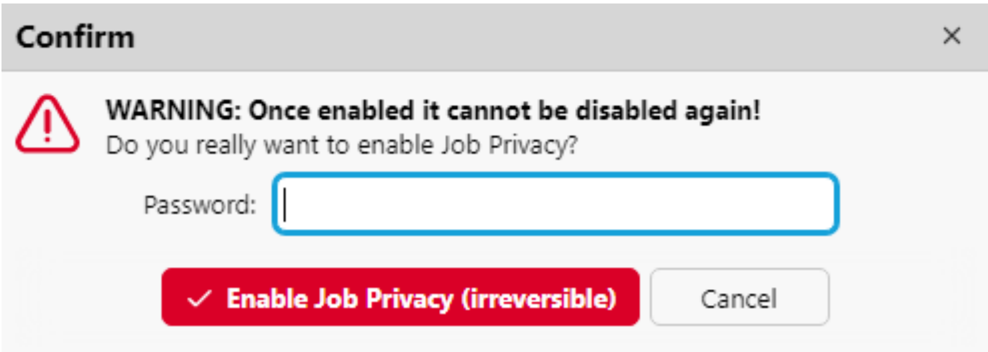
If you have a MyQ Central server setup and Job Privacy is enabled at your Central server, it will be automatically enabled on all the connected Site servers.

> ⚠ Once the Job Privacy feature is enabled, it cannot be disabled again!

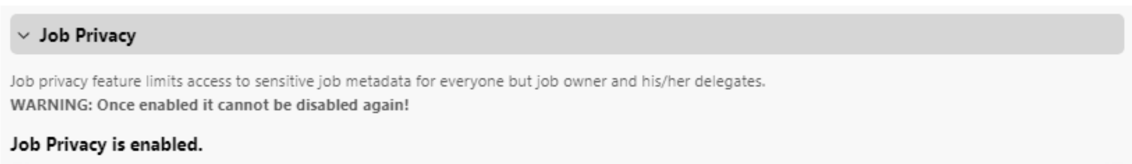
To use the feature, click on the **Enable Job Privacy (irreversible)** button.



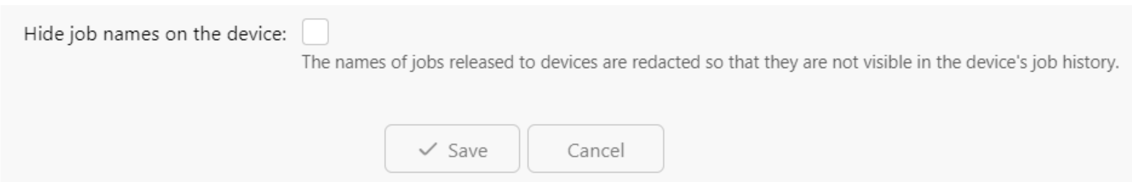
In the confirmation pop-up, type your MyQ administrator password in the **Password** field, and click **Enable Job Privacy (irreversible)**.



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.



11.10 Watermarks

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.

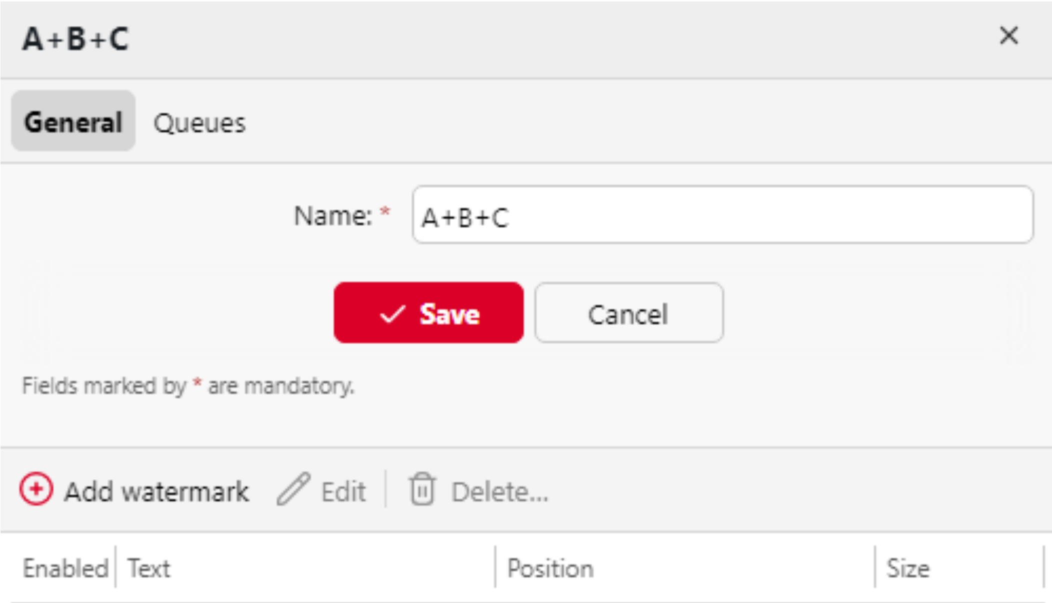
11.10.1 Creating, editing, and deleting watermark collections

The watermarks collections can be created in the **Watermark collections** section at the bottom of the **Jobs** settings tab (**MyQ, Settings, Jobs**).

Creating a new watermark collection

To create a new watermark collection:

1. On the **Jobs** settings tab, in the **Watermark collections** section, click **+Add**. The properties panel of the new collection opens on the right side of the screen.
2. On the panel, enter the **Name** of the collection, then **Add watermarks** to it, and lastly 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

To delete a collection:

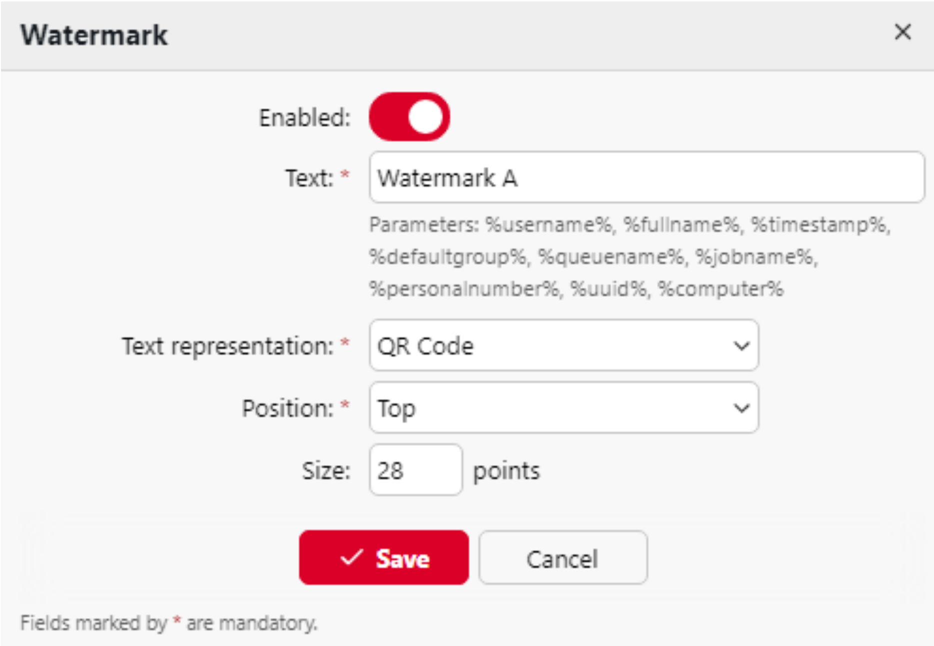
On the **Jobs** settings tab, under **Watermark collections**, select the collections that you want to delete, and then click **Delete**.

11.10.2 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, Code 128, PDF417, and the most restrictive Code 39. The text can be represented in the following forms:
  - 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**.

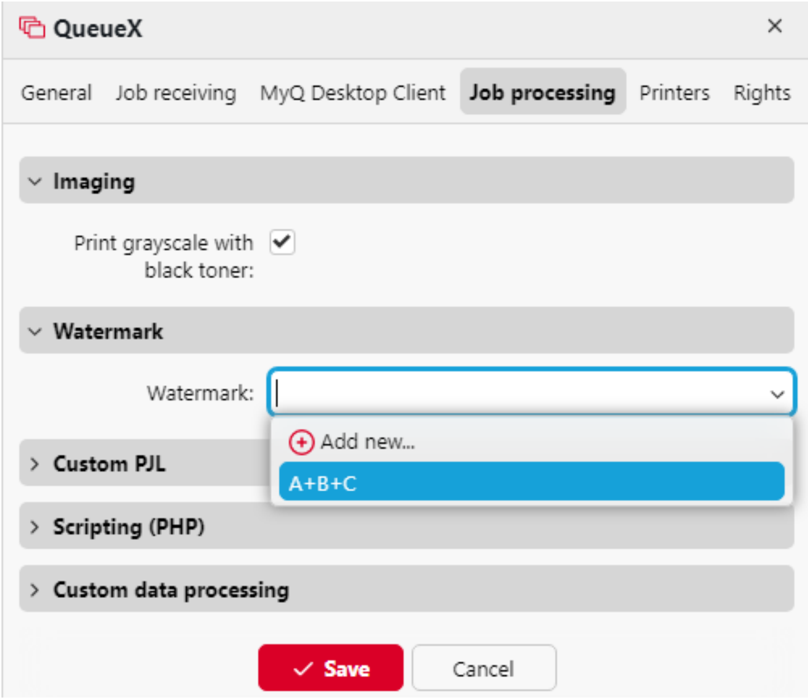
11.10.3 Attaching watermark collections to queues

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

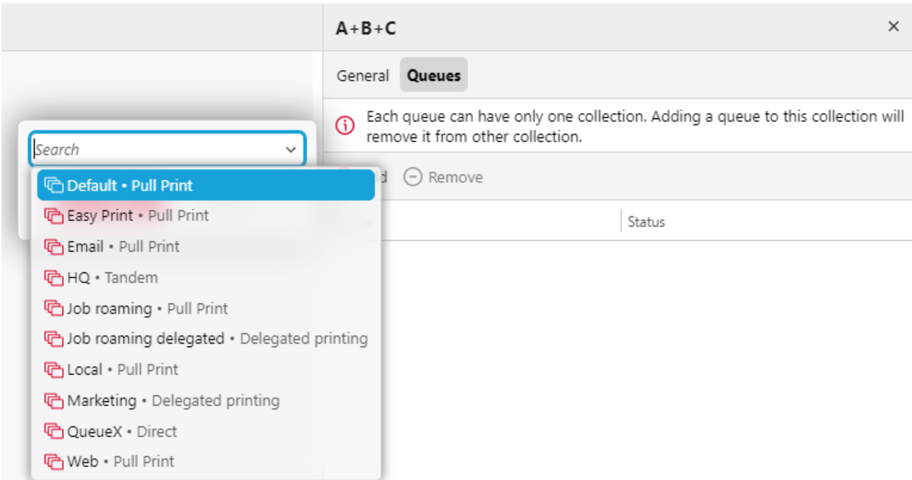
The collection can be selected on the **Job processing** tab of the properties panel of the queue. To open the properties panel, go to **MyQ, Queues**, and then double-click the queue on the list. On the **Job processing tab,** in the **Watermark** section, select the **Watermark** from the drop-down, and then click **Save**.



Attaching watermark collections to queues within the setup of the collections

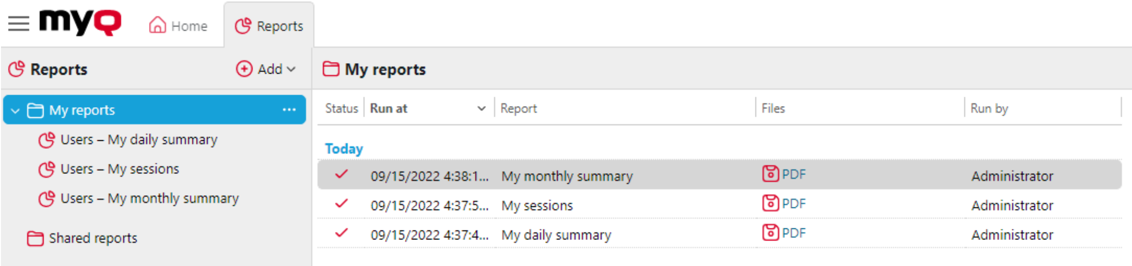
To assign a new queue to a watermark collection, select it on the on the list on the **Jobs** settings tab, under **Watermark collections**, and click **Edit**.

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**.



12 Reports

In the MyQ web interface, on the **Reports** main tab (**MyQ, Reports**), you can create and generate reports with a variety of data concerning your printing environment. The reports can be related to users, printing devices, print jobs, etc.



Reports in MyQ are divided into two main categories: **My reports** and **Shared reports**. **My reports** show
users reports created by themselves, while **Shared reports** show them reports created by the administrator or by other users.

There are three default reports: **My daily summary**, **My sessions** and **My monthly summary**. These are displayed in the **My reports** folder of the MyQ administrator, who can modify them, delete them or change their design. For all the other users, the default reports are displayed in the **Shared reports** folder and cannot be changed in any way.

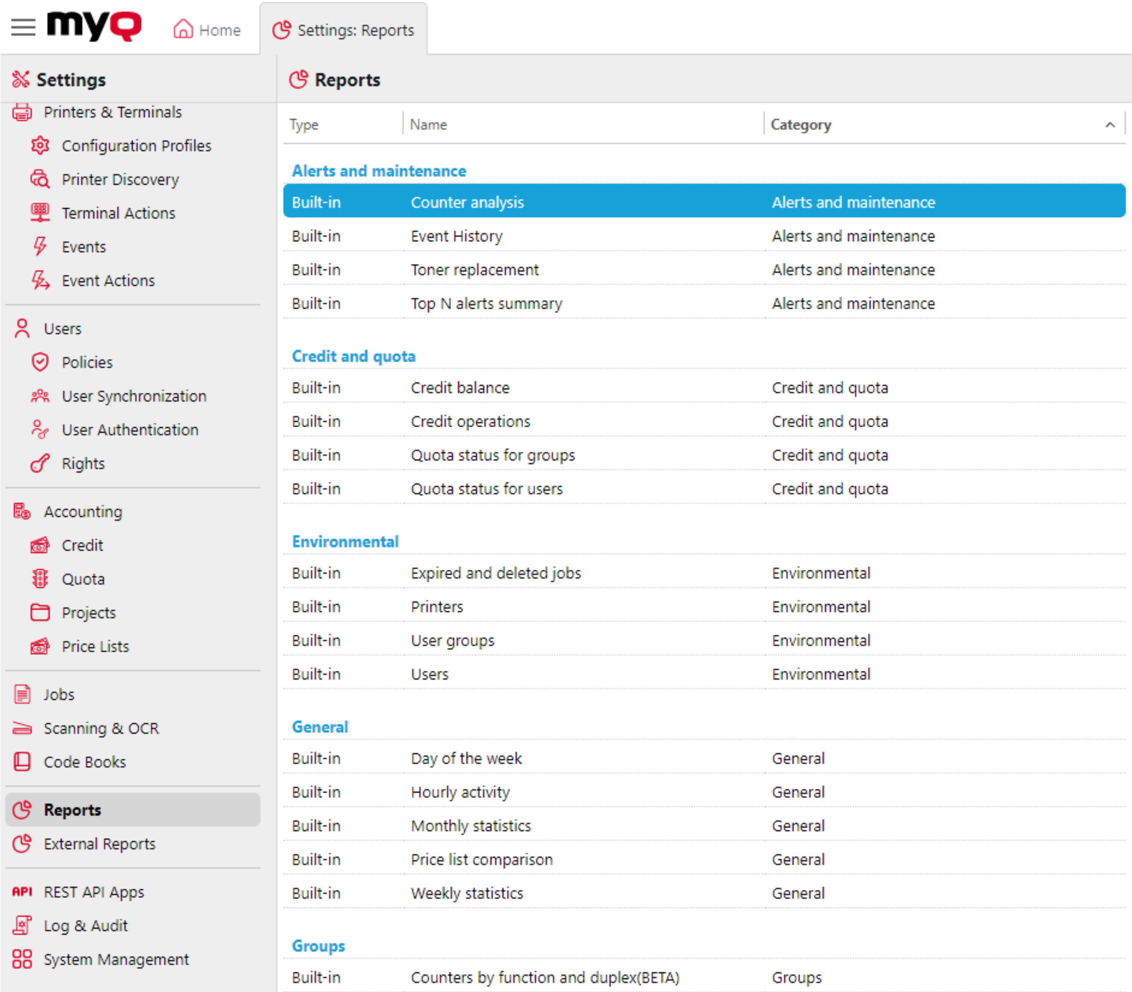
In addition to the three default reports, the administrator can create an unlimited number of reports and sort them into sub-folders of the **My reports** folder. Users can create their own reports but they are limited to use only certain report types depending on the rights granted by the administrator.

Each report can be directly displayed on the web interface and saved in any of the following formats: *PDF, CSV, XML, XLSX* and *ODS*. The reports can be automatically generated and stored in a predefined folder. There is no data limitation for the generated report, it includes all the data from the specified period.
All the reports have the MyQ logo displayed by default, but it can be replaced by your company's logo. To upload a custom logo go to **MyQ, Settings, Personalization**. In the **Custom application logo** section, click **+Add** next to **Custom logo** and upload your own file (supported formats - *JPG, JPEG, PNG, BMP* and recommended size - *398px* x *92px*).

12.1 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*).

You can overview all of the report types on the **Reports** settings tab, under **Report types** (in **MyQ, Settings, Reports**).



Providing users with rights to use a report

The administrator can run all the built-in reports and provide other users and groups with rights to run them as well. In **MyQ, Settings, Reports**, right-click on a report and click **Edit**. On the **General** tab, in the **Permission for running the report** field, choose users and groups from the list and click **Save**.

You can also add custom report types developed by the MyQ development team. To do so, just click **+Add**, upload the custom report definition file, select users or groups to access it, and click **OK.** For more information about custom report types, please contact MyQ support.

12.1.1 Report Categories

- Alerts and Maintenance - These reports provide information about device alerts and unusual changes on device counters.

- Credit and Quota - These reports contain information concerning credit and quota, for example the remaining credit or the state of quota of selected users.
- Environmental - These reports inform about the environmental impact of printing. They show how many trees needed to be harvested, how much energy was spent and how much carbon dioxide was emitted during the production of the paper used for printing and copying within your company's printing environment.
  Data sources vary in their estimations. MyQ calculations in the report are based on the following data estimates:
  - **Carbon dioxide for paper production**: 12,7 gram per paper sheet
  - **Energy used for production**: 48 Wh per paper sheet or 32Wh for a recycled paper sheet
  - **Trees**: 8333 paper sheets are counted as 1 tree.
- General - These reports provide general information about the MyQ system, such as total counters statistics and printing peaks or comparison of price lists used for printers.
- Groups - These reports inform about groups of users. They can contain information about membership, printed pages, weekly stats etc.
- Print Jobs - These reports contain information about jobs printed in MyQ, such as the list of all expired and deleted jobs over a certain period.
- Printers - These reports inform about all the printing devices in the MyQ system (both local and network). Generated reports can contain graphs of the device usage, daily, weekly and monthly counters, etc.
- Projects - These reports contain information regarding projects and project accounting in MyQ, such as daily summary of projects or projects assigned to selected users over a certain period.
- Users - These reports can contain various information about users. They can concern their print jobs, credit statements, printed pages etc.

Alerts and Maintenance Reports

The following reports are included in the **Alerts and Maintenance** category:

Counter Analysis

This report shows the page counts per session, covering B&W pages, color pages, total pages, and scans by the user. It shows sessions where the counters reached or exceeded the predefined value.

> The report is not available when Job Privacy is enabled.

Event History

This report shows the occurrence of predefined device errors and alerts. It only shows alerts that are turned on in **Settings** > **Events** in the MyQ Web UI.

Toner Replacement

This report shows the toner usage, the date the toner was installed or replaced, and the pages printed for each toner container.

The number displayed in the Toner replacement report in the Pages printed and Total counters columns depends on the toner it relates to:

- **Pages printed -** The number of pages printed with the replaced toner. Only color pages for color toners (CMY) and all pages for black toners (K) are considered.
- **Total counters -** Total counters of the printer related to the replaced toner. Color pages for color toners (CMY) and all pages for black toners (K) are considered.

Top N Alerts Summary

This report shows the most common errors and alerts. The number of alerts shown can be customized.

> Charts are available for this report.

Credit and Quota Reports

The following reports are included in the **Credit and Quota** category:

Credit Balance

This report shows the current Credit balance.

Credit Operations

This report shows a list of credit transactions (top-up and spent).

Quota Status for Groups

This report shows all of the accounting/cost center group quotas.

Quota Status for Users

This report shows the user-based quotas usage and settings.

Environmental Reports

> The information in these reports is based on the following data:
> *1 tree = 8333 pages / 1 page = 12.7g of CO2 / 1 page = 48Wh of energy / 1 recycled page = 32Wh of energy*

The following reports are included in the **Environmental** category:

Expired and Deleted Jobs

This report shows a list of expired/deleted jobs and the environmental impact of not printing them. They are sorted by print queue.

> When Job Privacy is enabled, this report can be used but will exclude user-specific information.

Printers

This report shows the environmental impact of each printer.

User Groups

This report shows the environmental impact of each User Group.

Users

This report shows the environmental impact of each User.

> The report is not available when Job Privacy is enabled.

General Reports

The following reports are included in the **General** category:

Day of the Week

This report shows the output volume by day of the week.

Charts are available for this report.

Hourly Activity

This report shows the output volume by time of day.

Charts are available for this report.

Monthly Statistics

This report shows the output volume by month.

Charts are available for this report.

Price List Comparison

This report shows the price lists applied to various printer groups.

Weekly Statistics

This report shows the output volume by week.

> Charts are available for this report.

Groups Reports

The following reports are included in the **Groups** category:

Counters by Function and Duplex(BETA)

This report shows counters per group by print/copy, color, and duplex.
The function field refers to whether a page was printed or copied.

Reports marked as BETA only contain data from Embedded Terminals running MyQ 8+. If some of your Embedded Terminals run earlier versions of MyQ, their data will not be included in the report.

The report is not available when Job Privacy is enabled.

Counters by Function and Paper Format(BETA)

This report shows counters per group by print/copy, color, and paper format.

The function field refers to whether a page was printed or copied.

Reports marked as BETA only contain data from Embedded Terminals running MyQ 8+. If some of your Embedded Terminals run earlier versions of MyQ, their data will not be included in the report.

The report is not available when Job Privacy is enabled.

Counters by Function Paper Format and Duplex(BETA)

This report shows counters per group by color, duplex, and paper format.

The function field refers to whether a page was printed or copied.

Reports marked as BETA only contain data from Embedded Terminals running MyQ 8+. If some of your Embedded Terminals run earlier versions of MyQ, their data will not be included in the report.

The report is not available when Job Privacy is enabled.

Daily Summary

This report shows a summary of the daily output by group.

Day of the Week

This report shows a summary of the daily output based on the day of the week by group.

Monthly Summary

This report shows a summary of the monthly output by group.

> This report supports aggregated columns.

Top N

This report shows the groups sorted by largest output volume.
Charts are available for this report.

> It will show the top 5 by default, but this can be changed in the **Design** section of the report, under **Filters and Parameters**, by changing the number for **N**.

Total Summary

This report shows the total output volume per group for a predefined period.

> This report supports aggregated columns.

> The report is not available when Job Privacy is enabled.

User group membership

This report shows the list of members of the group and their membership options.

> The report is not available when Job Privacy is enabled.

Printers Reports

The following reports are included in the **Printers** category:

Counters by Function and Duplex(BETA)

This report shows counters per device by print/copy, color, and duplex.
The function field refers to whether a page was printed or copied.

> Reports marked as BETA only contain data from Embedded Terminals running MyQ 8+. If some of your Embedded Terminals run earlier versions of MyQ, their data will not be included in the report.

> The report is not available when Job Privacy is enabled.

Counters by Function and Paper Format(BETA)

This report shows counters per device by print/copy, color, and paper format.

The function field refers to whether a page was printed or copied.

Reports marked as BETA only contain data from Embedded Terminals running MyQ 8+. If some of your Embedded Terminals run earlier versions of MyQ, their data will not be included in the report.

The report is not available when Job Privacy is enabled.

Counters by Function Paper Format and Duplex(BETA)

This report shows counters per device by color, duplex, and paper format.

The function field refers to whether a page was printed or copied.

Reports marked as BETA only contain data from Embedded Terminals running MyQ 8+. If some of your Embedded Terminals run earlier versions of MyQ, their data will not be included in the report.

The report is not available when Job Privacy is enabled.

Daily Summary

This report shows the list of print jobs printed by device on a daily basis.

This report supports aggregated columns.

Day of the Week

This report shows a summary of the daily output based on the day of the week by device.

This report supports aggregated columns.

Meter Reading via SNMP

This report shows the device's total output volume.

This report (unlike the rest of MyQ reports) includes accounting data of the jobs bypassing MyQ server.

Monthly Summary

This report shows a summary of the monthly output by device.

Top N

This report shows the printers sorted by largest output volume.

Charts are available for this report.

Total Summary

This report shows the total output volume per printer for a predefined period.

This report supports aggregated columns.

The report is not available when Job Privacy is enabled.

Print Jobs Reports

Reports in this category should not be used for accounting purposes. Print Job reports display print jobs either as received by MyQ (for devices without an embedded terminal) or they reflect the printing parameters selected on the embedded terminal, rather than the final printed outcome.

The following reports are included in the **Print Jobs** category:

Daily Summary

This report shows the list of print jobs printed by user on a daily basis.

The report is not available when Job Privacy is enabled.

Expired and Deleted Jobs

This report shows the list of expired and deleted jobs.

This report supports aggregated columns.

The report is not available when Job Privacy is enabled.

Favorite Jobs

This report shows the list of user's favorite jobs.

The report is not available when Job Privacy is enabled.

Printed Jobs Summary

This report shows the list of all the print jobs printed by the user for a predefined period.

The report is not available when Job Privacy is enabled.

Projects Reports

The following reports are included in the **Projects** category:

Counters by Function and Duplex(BETA)

This report shows counters per project by print/copy, color, and duplex.
The function field refers to whether a page was printed or copied.

Reports marked as BETA only contain data from Embedded Terminals running MyQ 8+. If some of your Embedded Terminals run earlier versions of MyQ, their data will not be included in the report.

The report is not available when Job Privacy is enabled.

Counters by Function and Paper Format(BETA)

This report shows counters per project by print/copy, color, and paper format.

The function field refers to whether a page was printed or copied.

Reports marked as BETA only contain data from Embedded Terminals running MyQ 8+. If some of your Embedded Terminals run earlier versions of MyQ, their data will not be included in the report.

The report is not available when Job Privacy is enabled.

Counters by Function Paper Format and Duplex(BETA)

This report shows counters per project by color, duplex, and paper format.

The function field refers to whether a page was printed or copied.

Reports marked as BETA only contain data from Embedded Terminals running MyQ 8+. If some of your Embedded Terminals run earlier versions of MyQ, their data will not be included in the report.

The report is not available when Job Privacy is enabled.

Daily Summary

This report shows the list of print jobs printed by project on a daily basis.

This report supports aggregated columns.

Day of the Week

This report shows a summary of the daily output based on the day of the week by project.

This report supports aggregated columns.

Monthly Summary

This report shows a summary of the monthly output by project.

This report supports aggregated columns.

Print Jobs per Project

This report shows the list of print jobs assigned to each project.

The report is not available when Job Privacy is enabled.

Project Groups Total Summary

This report shows the total output volume per project for a predefined period.

Projects per User

This report shows the output volume per user and project. The data is grouped by user.

This report supports aggregated columns.

The report is not available when Job Privacy is enabled.

Top N

This report shows the projects sorted by largest output volume.

Charts are available for this report.

User Project Assignment

This report shows the list of projects assigned to each user.

The report is not available when Job Privacy is enabled.

Users per Project

This report shows the members of each project.

This report supports aggregated columns.

User Session Details

This report shows the list of all the user's interactions on the device sorted by project.

This report supports aggregated columns.

The report is not available when Job Privacy is enabled.

Users Reports

The following reports are included in the **Users** category:

Counters by Function and Duplex(BETA)

This report shows counters per user by print/copy, color, and duplex.
The function field refers to whether a page was printed or copied.

Reports marked as BETA only contain data from Embedded Terminals running MyQ 8+. If some of your Embedded Terminals run earlier versions of MyQ, their data will not be included in the report.

The report is not available when Job Privacy is enabled.

Counters by Function and Paper Format(BETA)

This report shows counters per user by print/copy, color, and paper format.

The function field refers to whether a page was printed or copied.

Reports marked as BETA only contain data from Embedded Terminals running MyQ 8+. If some of your Embedded Terminals run earlier versions of MyQ, their data will not be included in the report.

The report is not available when Job Privacy is enabled.

Counters by function paper format and duplex(BETA)

This report shows counters per user by color, duplex, and paper format.

The function field refers to whether a page was printed or copied.

Reports marked as BETA only contain data from Embedded Terminals running MyQ 8+. If some of your Embedded Terminals run earlier versions of MyQ, their data will not be included in the report.

The report is not available when Job Privacy is enabled.

Daily Summary

This report shows the list of print jobs printed by user on a daily basis.

The report is not available when Job Privacy is enabled.

Day of the Week

This report shows a summary of the daily output based on the day of the week by user.

The report is not available when Job Privacy is enabled.

Monthly Summary

This report shows a summary of the monthly output by user.

The report is not available when Job Privacy is enabled.

Session Details

This report shows the list of all user's interactions on the device.

The report is not available when Job Privacy is enabled.

Top N

This report shows the users, sorted by largest output volume.

Charts are available for this report.

The report is not available when Job Privacy is enabled.

Total Summary

This report shows the total output volume per user for a predefined period.

The report is not available when Job Privacy is enabled.

User Rights

This report shows the list of users with enhanced access rights.

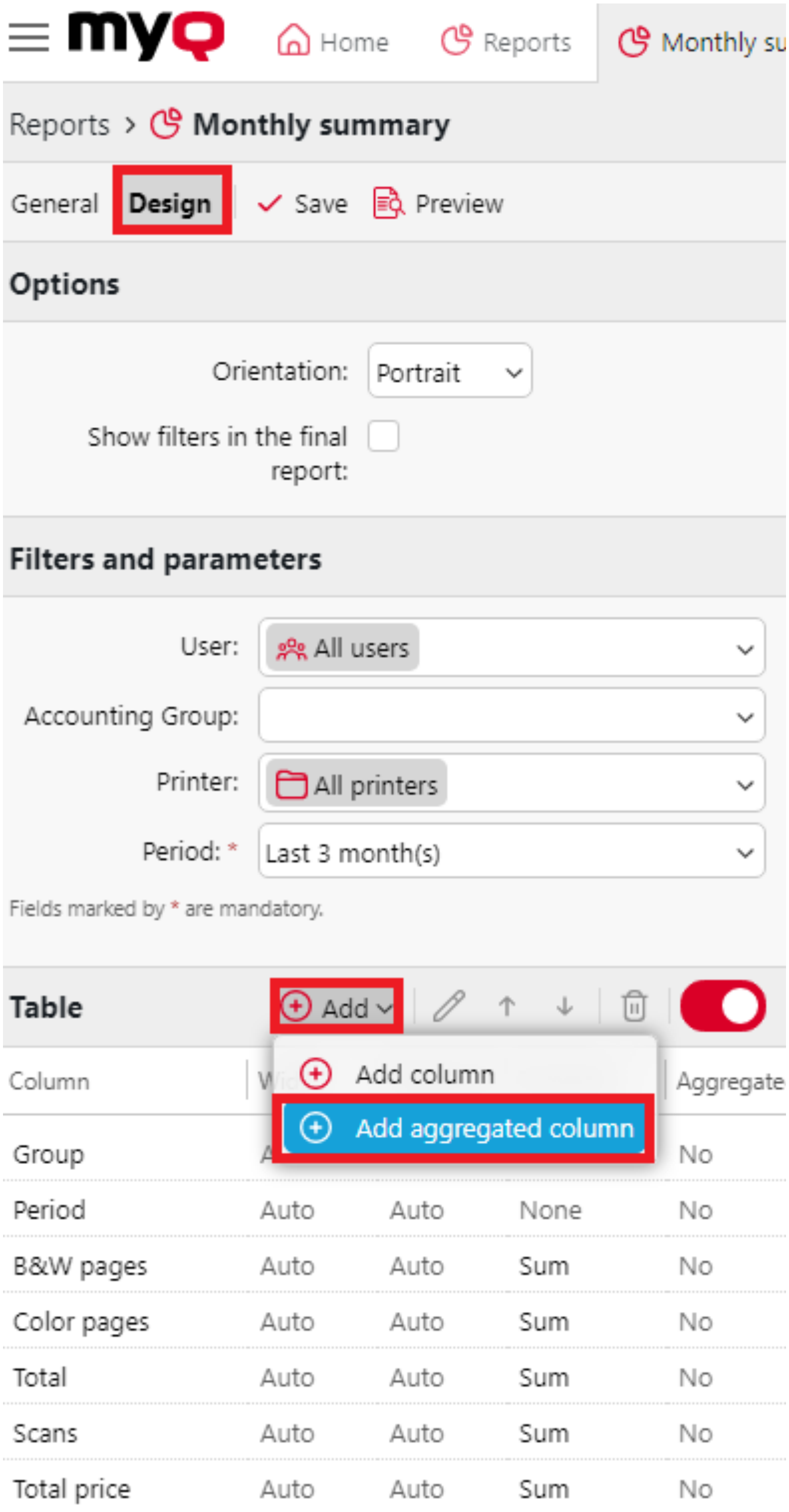
> The report is not available when Job Privacy is enabled.

12.1.2 Creating New Aggregated Columns

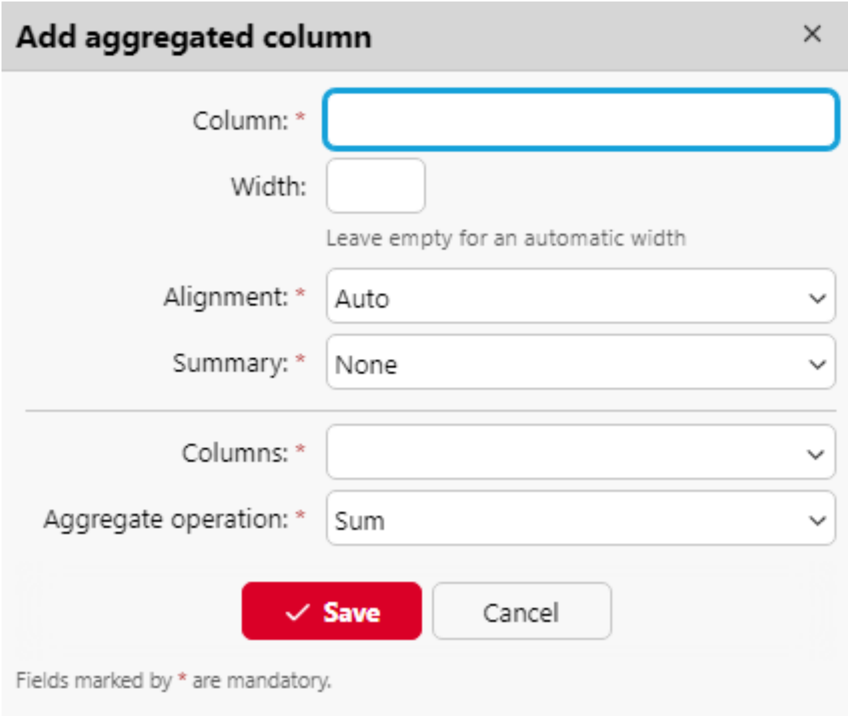
For some types of reports, you can create any number of custom aggregated (summary) columns. An aggregated column can display either the sum or the average of a selection of any number of other columns available for the type.

To create a new aggregated column for a report:

1. Go to **MyQ**, **Reports**. On the list of reports on the right side, select the report and click **Edit** on the ribbon (or right-click, edit). The report properties panel opens on a new window.
2. Go to the **Design** tab on the properties panel.
3. In the **Table** section, click **+Add**, and select **+Add aggregated column** from the list. The properties panel of the new column opens.



4. In the panel, set the properties, select the **Aggregate operation** you want to use (*Sum* or *Average*), and click **Save**. The new column is listed with the other table columns, and you can double-click on it to edit it.



Supported types of reports for aggregated columns

The aggregated (summary) columns can be created for the following types of reports:

- From the **Groups** category: Monthly summary, Total summary
- From the **Print jobs** category: Expired and deleted jobs
- From the **Printers** category: Daily summary, Day of the week, Meter reading via SNMP, Total summary
- From the **Projects** category: Daily summary, Day of the week, Monthly summary, Project groups total summary, Projects per user, Users per project.

12.2 Reporting Sources

Accounting in MyQ depends on the MyQ server version, the MyQ embedded terminal version and the printing device. MyQ 8.0+ currently uses the user-session architecture. The values in every report are based on user sessions (except for the **Meter reading via SNMP** printers report, described below).

- Counters are calculated in the following way:
  - B&W pages = B&W prints + B&W copies + Fax
  - Color pages = Color prints + Color copies + Single color copy
  - Total Pages = B&W pages + Color pages
  - Total prints = B&W prints + Color prints
  - Total copies = B&W copies + Color copies
- Price related columns include discounts.
- Any printers monitored via MyQ Desktop Client are included in the reports.

- Any non-MyQ users activity (*unauthenticated) is included in the reports.
- MyQ does not track deleted printers. If a deleted printer is later added and activated in MyQ, the reports will not include any activity during the time the device was deleted.
- If a printer is deactivated but not deleted, the reports include information about the period it was inactive only after it is reactivated. In that case, after the reactivation, all the activity is accounted to users not authenticated in a single session. The reports cannot include printers' data while they are deactivated.
- When an embedded terminal is installed on the printing device, accounting is also done for any direct/tandem print queues of the device.
- When an embedded terminal is not installed or a device is used with a MyQ Hardware terminal, accounting is done via SNMP by the MyQ Print Server (depends on provided data via SNMP from the device).

Values calculation in the Meter reading via SNMP printers report

The values in this report are based on counters read directly from the printers.

- Any printers monitored via MyQ Desktop Client are **not** included in the reports.
- The highest and lowest values are compared for a selected period and printer/ group of printers.
- The total value displayed in the report is the summary of all the subtotal values, without *Pages printed* while the device was deactivated.

12.3 Report Values Description

Description of values in the reports' default and additional columns and how they are accounted.

These values are accounted as page counts in the following way: 2 clicks for the A3/ Ledger page format and 1 click for the rest (A4 etc..); in case of Duplex, it is 4 clicks for the A3 / Ledger format and 2 clicks for the rest (A4 etc.). L formats are coverage counters.

- B&W prints
- B&W copies
- Color prints
- Color copies
- Single color copy
- Total prints
- Total copies
- Fax
- Color pages (L1)
- Color cost (L1)
- Color pages (L2)
- Color cost (L2)
- Color pages (L3)
- Color cost (L3)

- Print color pages (L1)
- Copy color pages (L1)

> If discounts are used, they are not applied to all “cost” values in reports, e.g. *Color cost (L1)", "Color cost (L2)" or "Color cost (L3)*. However, "Total cost", "Color cost" do reflect discounts.

These values are accounted as paper sheets in the following way : 1x A3 / 1x A4 etc.

- A4 paper
- A3 paper
- A5 paper
- B4 paper
- B5 paper
- Other paper
- Folio paper
- Ledger paper
- Legal paper
- Letter paper
- Statement paper
- Rest of the paper formats

These values are accounted as paper sheets as well, however, when a printing device is used without an installed Embedded terminal, this counter is specified via SNMP and depends on the counter used from the printing device.

- Simplex
- Duplex

> Terminals version 7 and lower might have reported Duplex values differently depending on the vendor – either as the number of images (e.g. 1 page printed duplex as Duplex=2) or the number of sheets (Duplex=1). Since Terminals 8.2, these values are unified as the number of sheets. The combination of data from older Terminals with Terminals 8.2 in Reports may cause an inconsistency in the Duplex values.

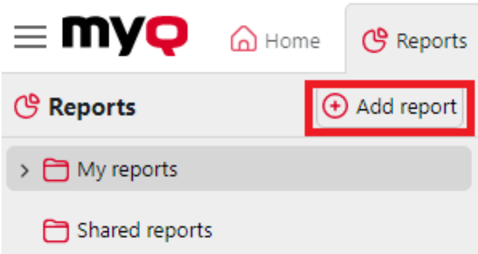
A job printed in 1x A3 monochrome sheet, on both sides in duplex mode, on a device where an Embedded terminal is installed, is accounted in MyQ as 1x A3 paper + 4x print monochrome and 1x duplex. In the MyQ log it will look like this:

PM=4, A3=1, Duplex=1

12.4 Creating, Editing and Cloning Reports

12.4.1 Creating Reports

1. In **MyQ > Reports**, click **+Add report**. The Add report dialog box appears.



2. Select the type of the new report and the folder to place it, and click **OK**. The report is saved, and opens in edit mode on the Design tab.

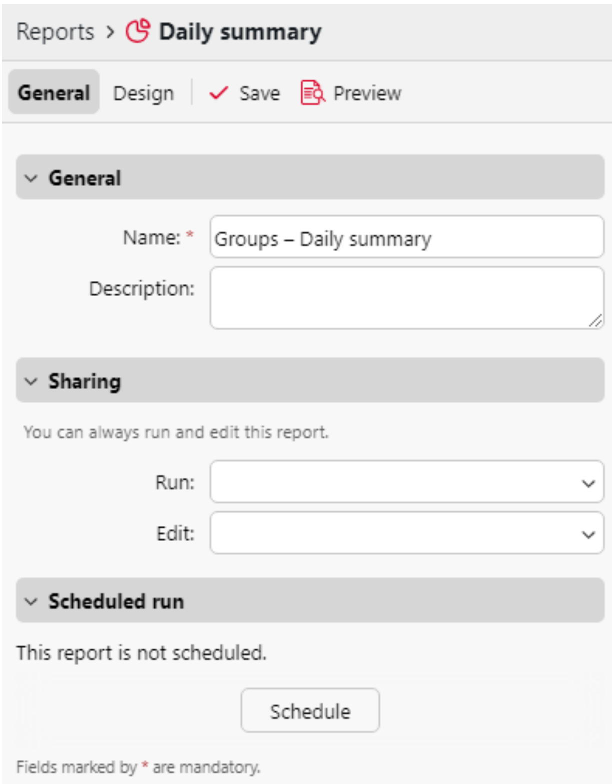
12.4.2 Editing a Report

To edit a report, go to **MyQ > Reports**, click the three-dot menu for the report you want to schedule, and select **Edit**. The report opens in edit mode.

General Tab

On the General tab of the report editor, you can configure these options:

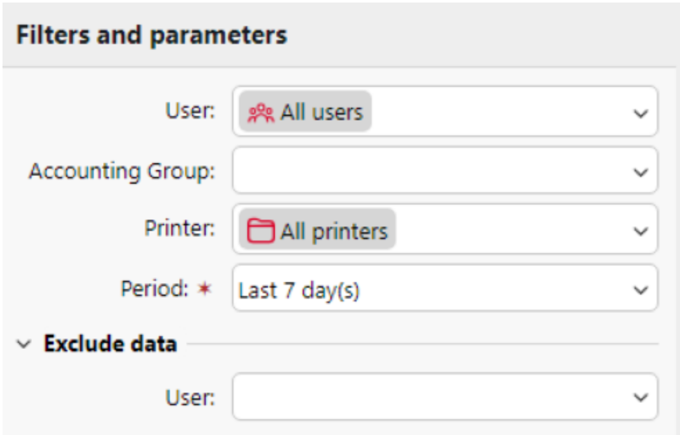
- **Name:** customize the report name.
- **Description**: add an optional description for the report.
- **Sharing**: specify what users or groups can **Run** and **Edit** the report.
- **Schedule run**: Define a scheduled task to run the report at regular intervals.



Design Tab

Filters and parameters

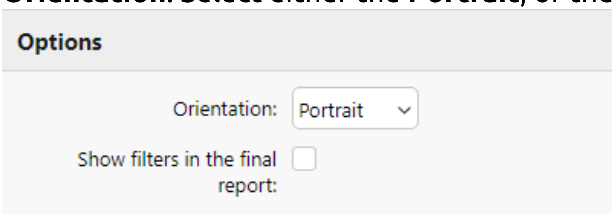
Available filters and parameters differ depending on the report type. These are the main parameters available for most of the standard reports types:



- **User**: Select the users to be included in the report. If you select the **Me** option and share this report with all users, each user can only see just the data that concern themselves; this way you can make personalized reports for each user.
- **Accounting Group**: Select the accounting groups of users to be included in the report.
- **Printer**: Select the printers to be included in the report.
- **Period**: Select the time period to be covered by the report.
- **Exclude data - User:** Select the users to be excluded from the report (only available in reports where *User* is one of the filters used).

Options

- **Orientation**: Select either the **Portrait**, or the **Landscape** orientation.



- **Show filters in the final report**: Mark the checkbox if you want filters to be visible in the final report.

Table

Here you can enable and disable the table option.

Table Add

Column	Width	Alignment	Summary	Aggregate
Group	Auto	Left	None	No
Date	Auto	Auto	None	No
B&W pages	Auto	Auto	Sum	No
Color pages	Auto	Auto	Sum	No
Total	Auto	Auto	Sum	No
Scans	Auto	Auto	Sum	No
Total price	Auto	Auto	Sum	No

You can also add and remove columns to the table, edit them and change their order. For each column, you can change the width, alignment and the type of summary that will be shown on the final (bottom) row (Sum, Average or None).

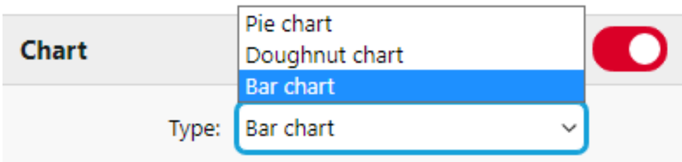
To add a new column, click **+Add**. To open the editing options of an existing column, double-click it (or select it, and then click **Edit**). To remove a column, select it and click **X**. To move a column up or down the order, select it, and then use the up/down arrows.

Period	B&W pages	Color Pages	Total	Scans	Total price
2017-3	5,621	9,189	14,810	5,506	$5,440.000
2017-4	1,211	569	1,780	1,234	$7,072.000
Period	**B&W pages**	**Color Pages**	**Total**	**Scans**	**Total price**
	6,832	**9,758**	**16,590**	**6,740**	**$12,512.000**

Some reports do not include the option to use tables and their data can be displayed only in the chart form.

Chart

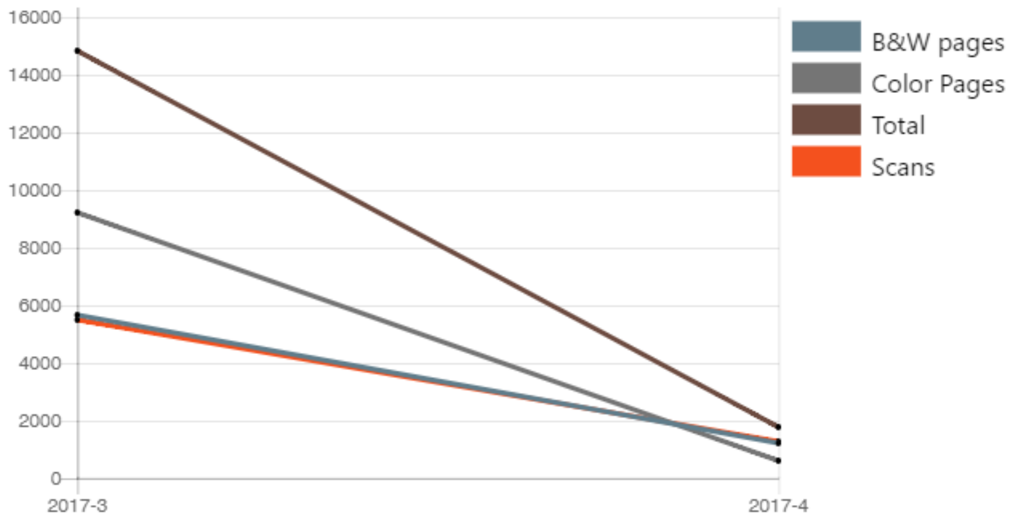
Here you can enable and disable the chart option.



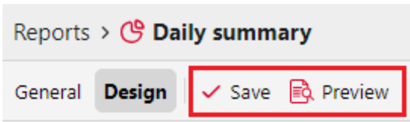
You can also select from the **Bar, Pie** and **Doughnut** chart types. Furthermore, you can add and remove data types to be shown on the chart and select colors for each data type (depending on the report type).

To add a data type, click **+Add**. To open editing options of a data type, double-click it (or select it, and then click **Edit**). To remove a data type, select it and click **X**. To move a data type up or down the order, select it, and then use the up/down arrows.

Some reports do not include the option to use charts and their data can be displayed only in the table form.

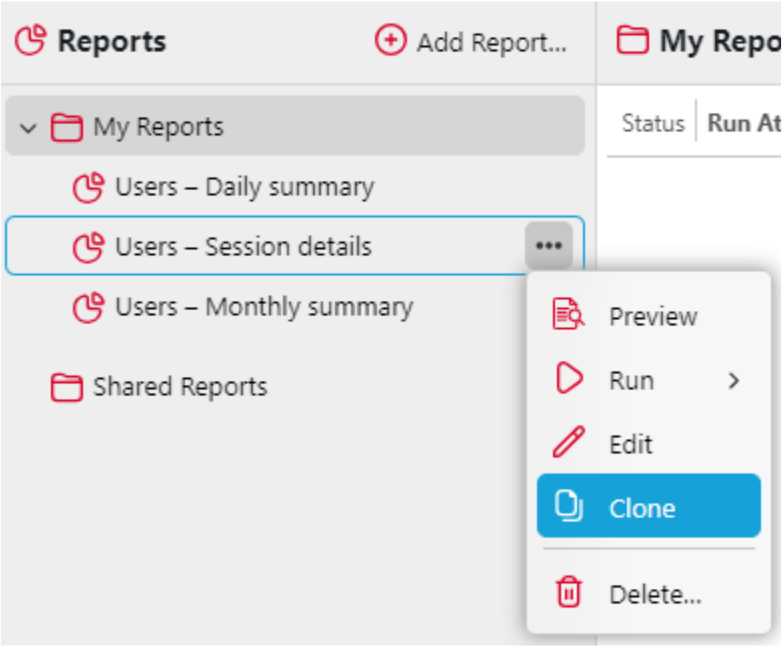


Designing your own reports can be a bit tricky, since it always depends on many factors - amount of data included (columns), length of column names and values, report orientation etc. To get the best result, you can click **Preview** anytime during the report's creation to check what the new design will look like. Only after you are satisfied with the layout, click **Save** to save the report.

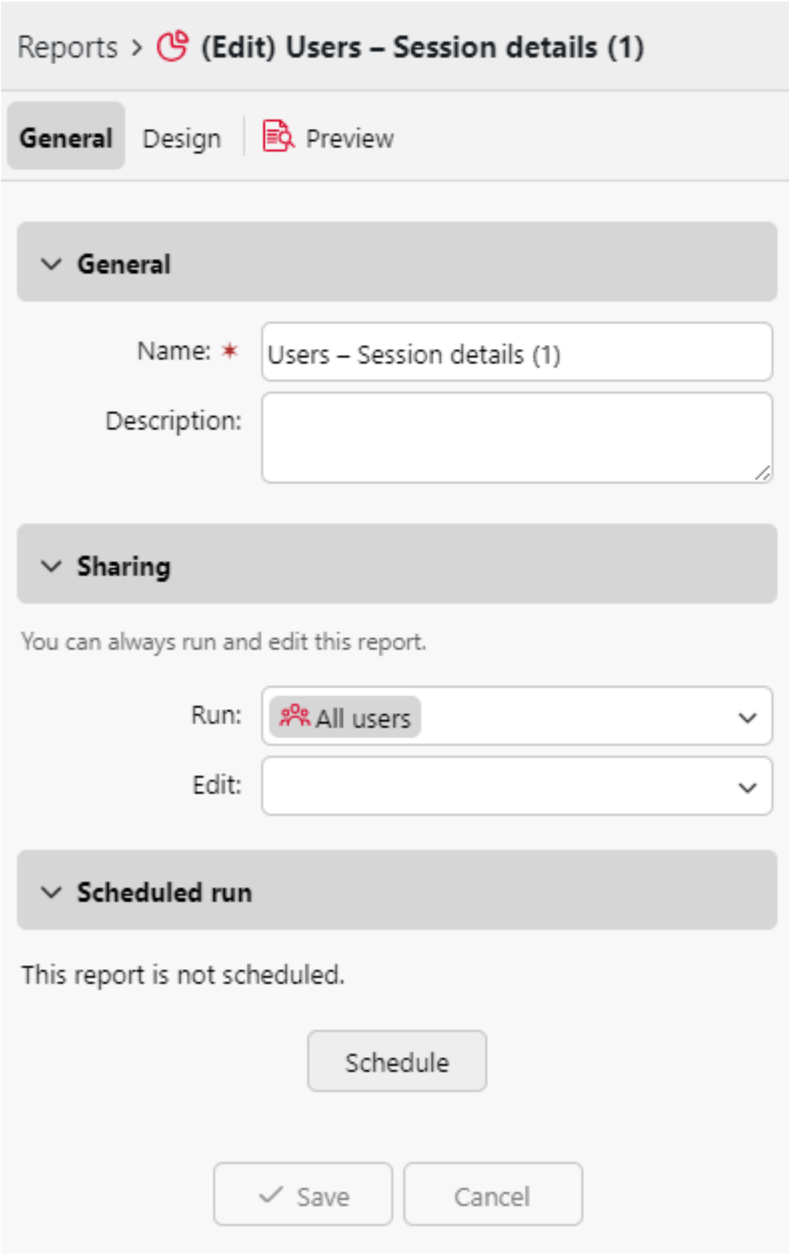


12.4.3 Cloning Reports

Any user can clone an existing report that they have access to, this copies the settings of the existing report and saves it with a modified title, for example, the clone of **Users - Session details** is automatically named **Users - Session details (1)**.



To clone a report, right-click its title or use its context menu and select **Clone**. The edit report options for the newly cloned report open automatically. Users can then change the title of the report or edit any other relevant settings and click **Save**. If a user does not edit any of the new report's settings, the clone is already automatically saved.



If the source folder of the report was not created by the user, a clone will be created in the My Reports folder.

12.5 Running and Scheduling Reports

Reports can be run on-demand or scheduled to run automatically at specified intervals. This section describes both approaches.

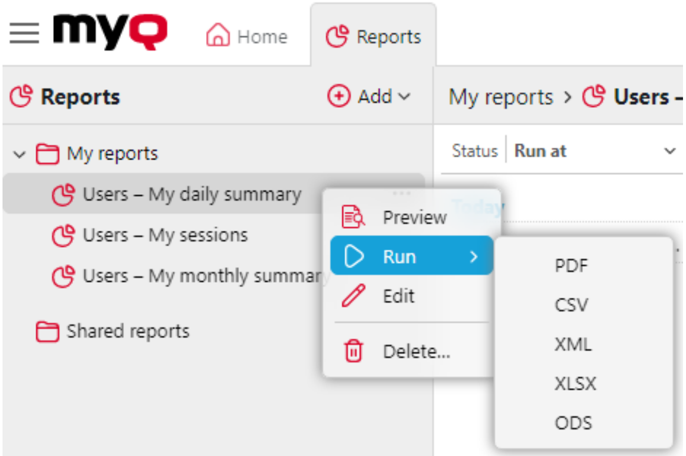
12.5.1 Running Reports On-Demand

Preview a report

Select the report and click **Preview**. The report is shown in HTML format, with a limited subset of data included. You can switch between Graphical and Grid views.

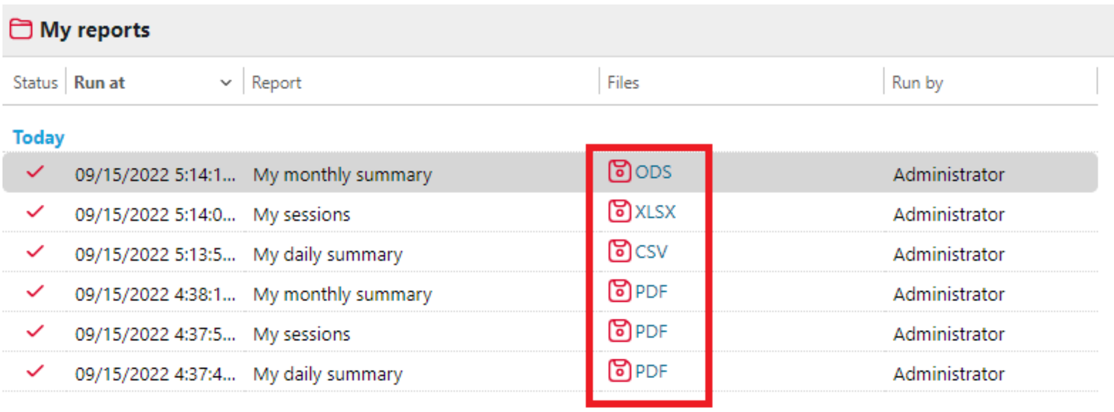
Run a report

Right-click the report and click **Run**. The report runs in the specified format (*PDF*, *CSV*, *XML*, *XLSX* or *ODS*) with no data limitation.



Export the displayed report

After the report is generated, click on the report's format link in the Files column to download it.

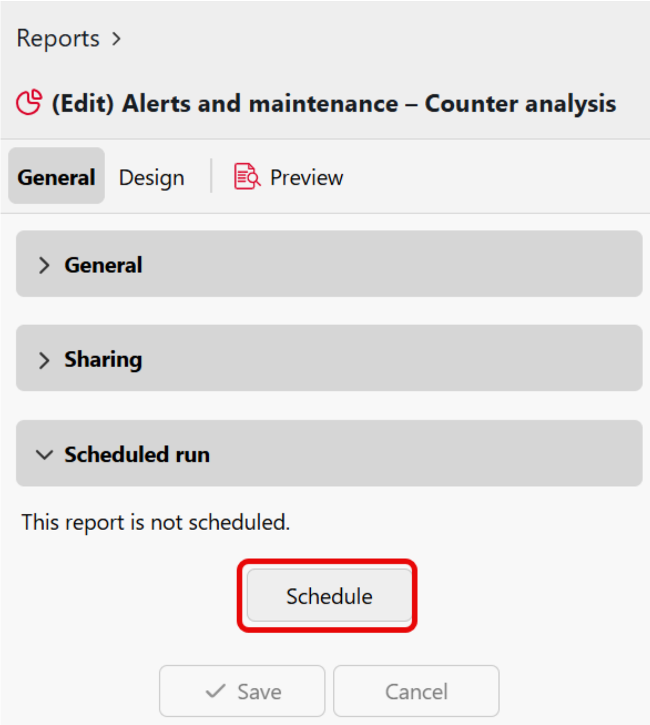


12.5.2 Scheduling Reports

You can schedule reports to run automatically at regular intervals. Scheduled reports are generated in the background and can be sent via email to specified recipients.

Schedule a report

1. In **MyQ > Reports**, click the three-dot menu for the report you want to schedule.
2. Click **Edit**. The report opens in edit mode.
3. On the **General** tab, in the **Scheduled run** section, click **Schedule**. The scheduled task editor opens.



4. Configure the scheduling options to your needs. For more information, see Task Scheduler Settings.
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.

13 Connection to BI Tools

Starting from version 8.2 (patch 16), MyQ Print Server exposes data to be analyzed with external BI tools (Business Intelligence tools).

The below information refers to the setup and use of Power BI by Microsoft, along with a MyQ setup.

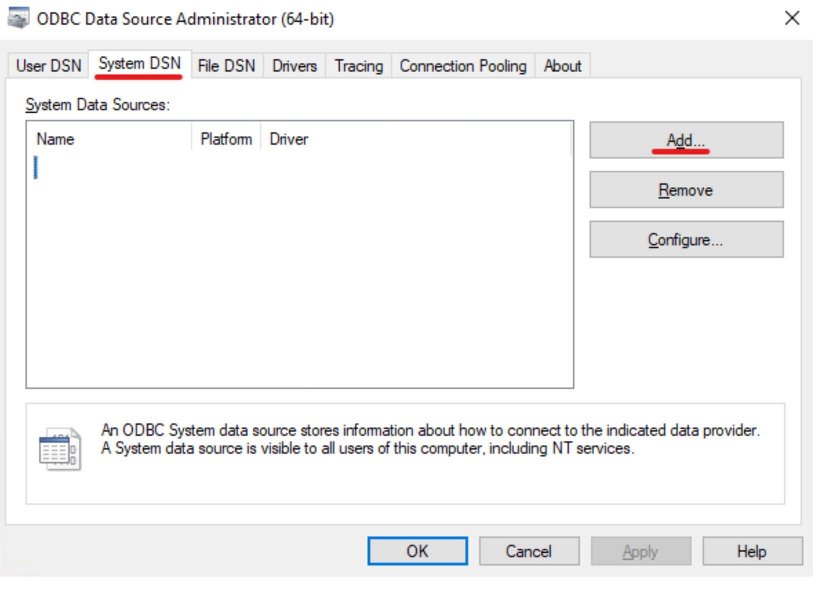
For further information about Power BI, visit:
https://docs.microsoft.com/en-us/power-bi/fundamentals/desktop-getting-started

13.1 Embedded Database Connection Configuration

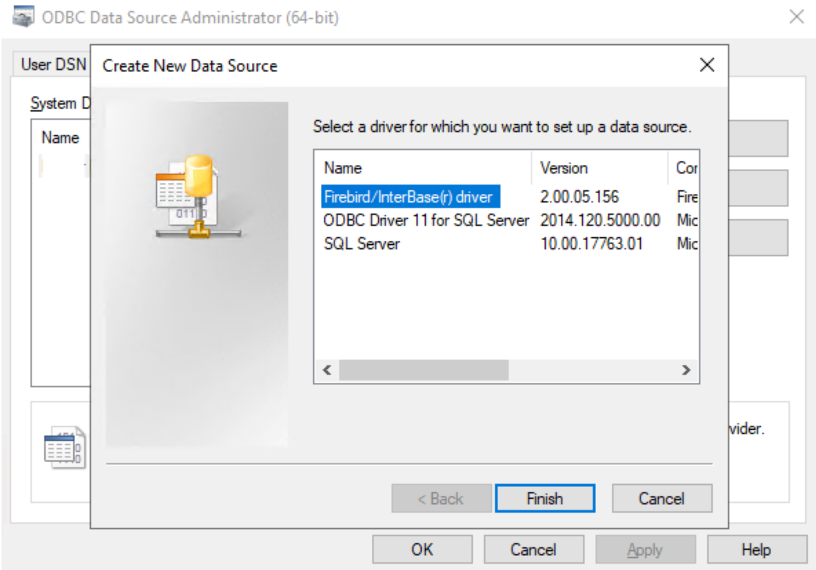
Power BI can access the MyQ Embedded Database via ODBC. In order to create an ODBC data source:

> 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.

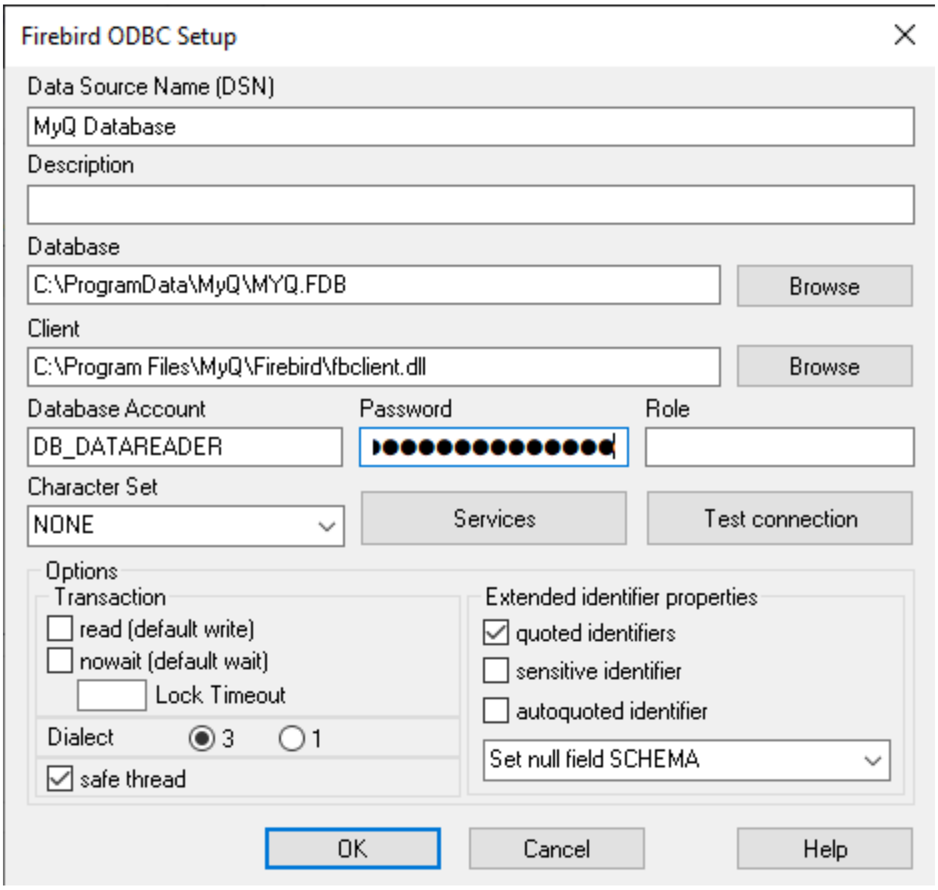
1. Download and install the latest ODBC driver for Firebird from: *https://firebirdsql.org/en/odbc-driver/*
2. Once installed, open the **ODBC Data Sources** application from the Windows Apps menu.
3. Go to the **System DSN** tab and click **Add**.



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:



1. **Data Source Name (DSN)**: Add a name as an identifier for the connection
    a. **Database**: Add the path to your database file (*C:\ProgramData\MyQ\MYQ.FDB* by default)

b. **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
c. **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.
d. **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*.
e. The rest of the fields can be left unchanged. Click **Test Connection** and if successful, click **OK**.

13.2 Creating Reports

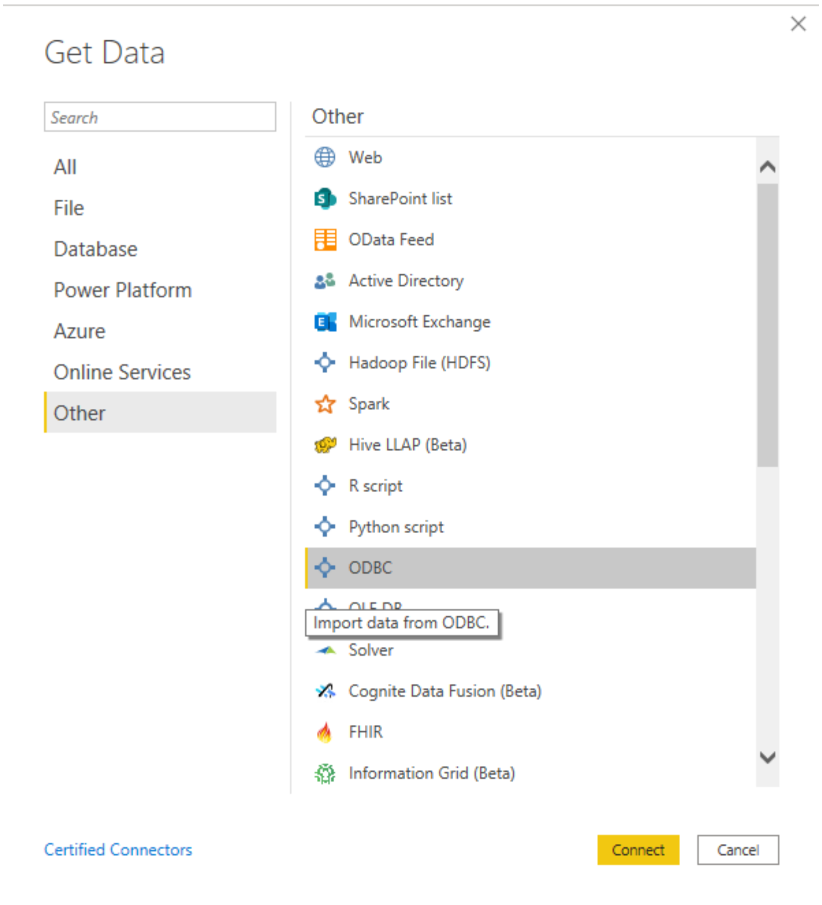
Reports can be created according to each customer's specific requirements. It is possible to create the reports manually, or use the Power BI template created by MyQ in order to generate reports quickly.

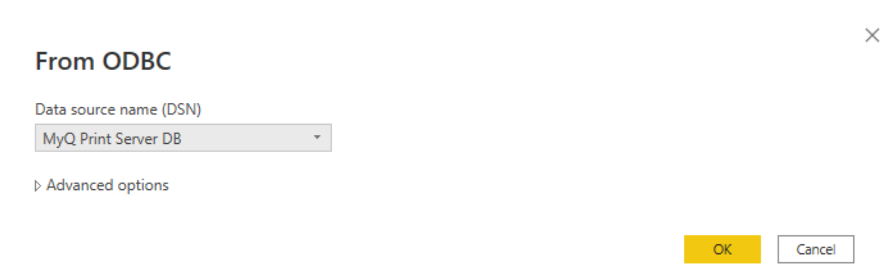
- Manual reports creation
- Reports creation via template import
- Report examples
- Database Views description

13.2.1 Manual Reports Creation

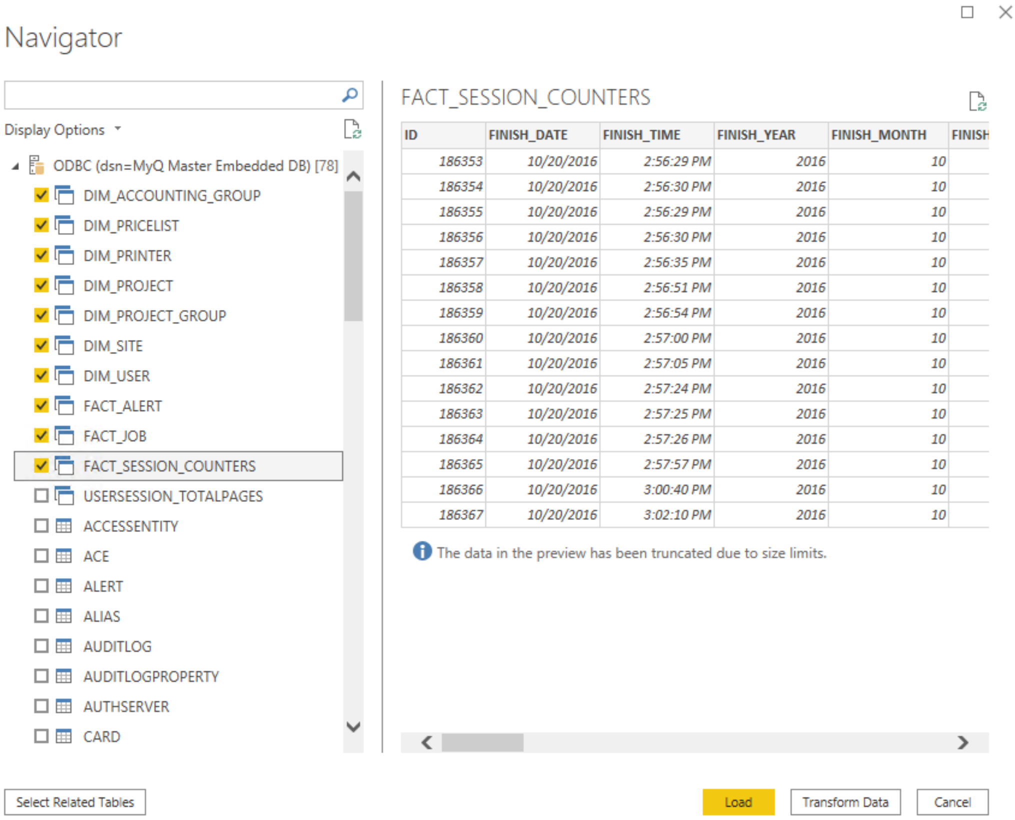
To manually create the reports, open Power BI and:

1. Establish the connection to your database:
    a. Click **Get data, More...**. In the new window, select **Other**, click on **ODBC** on the list, and click **Connect**. In the new prompt, select the Data source name (DSN) you created in the ODBC Data Sources app and click **OK**.

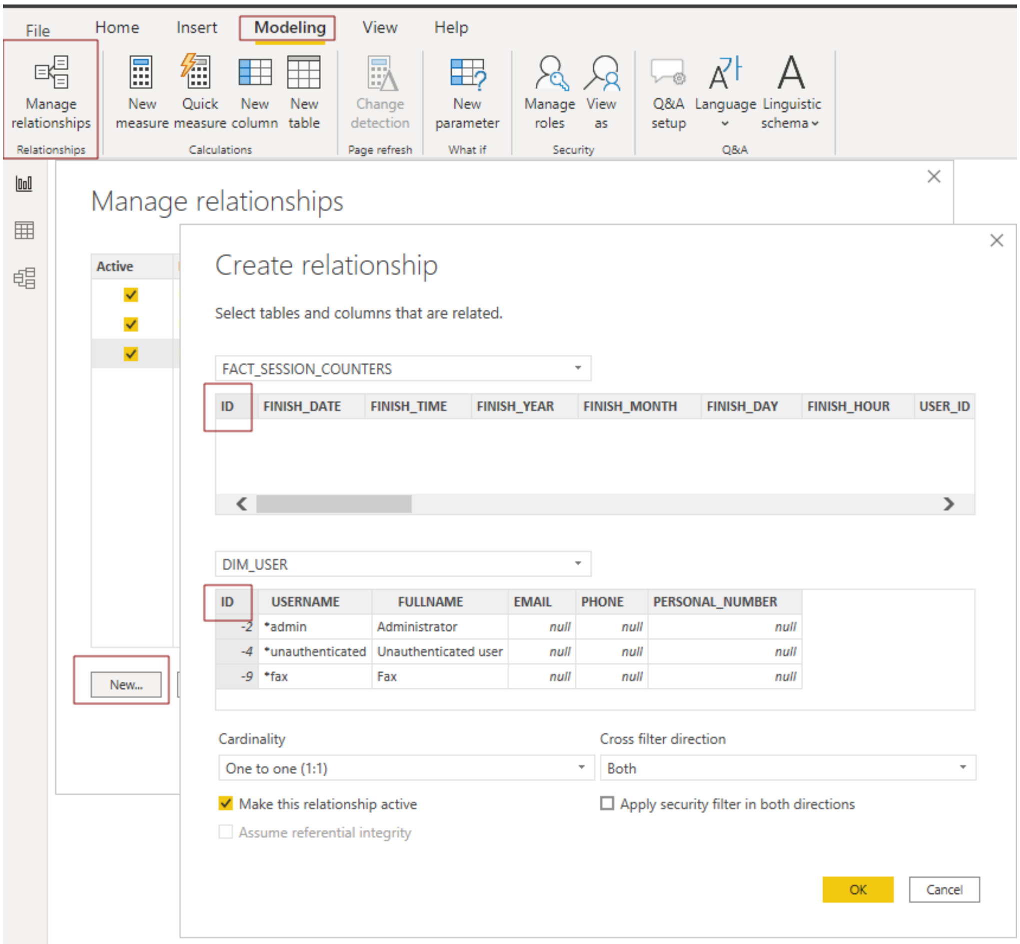




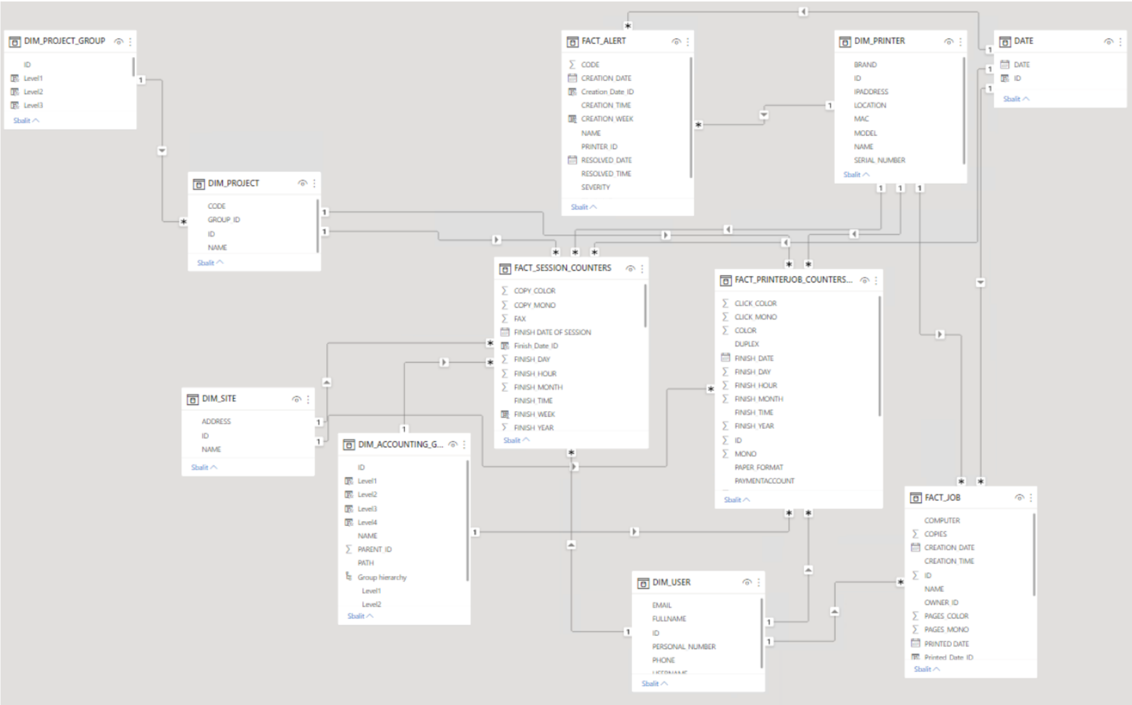
2. In the Navigator window, select all the options with the **DIM_** and **FACT_** prefixes and click **Load** (see Database Views description).



3. Power BI loads the data, however the relationships between them must be created manually, since Power BI cannot extract them:
   a. Go to the Modeling menu and click on **Manage relationships**.
   b. Click **New...** and create the relationships between the views, selecting the IDs in each of them. Click **OK** once done.



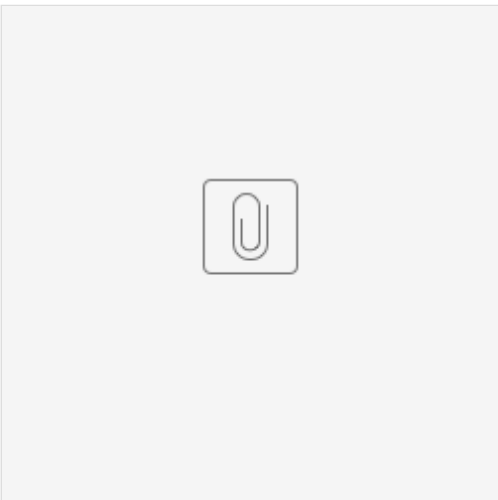
4. Your model has been created and you can add visualizations to the report.



13.2.2 Reports Creation via Template Import

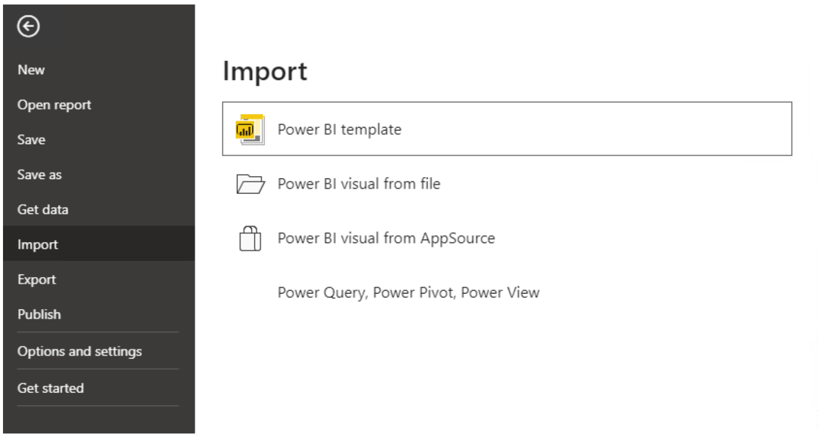
An ODBC DSN must be configured before using the template.

- ODBC template

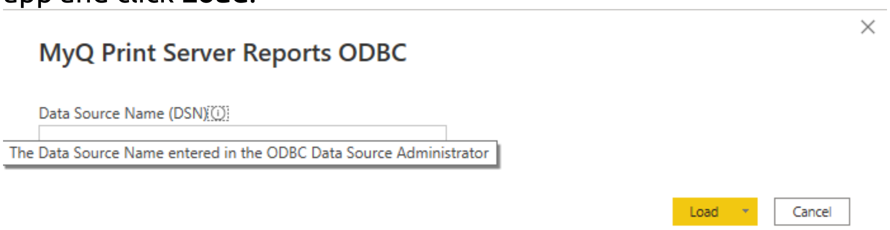


To import the template provided by MyQ , open Power BI and:

1. Open the **File** menu, select **Import**, and click on **Power BI template**. Find and open the correct template according to your database.



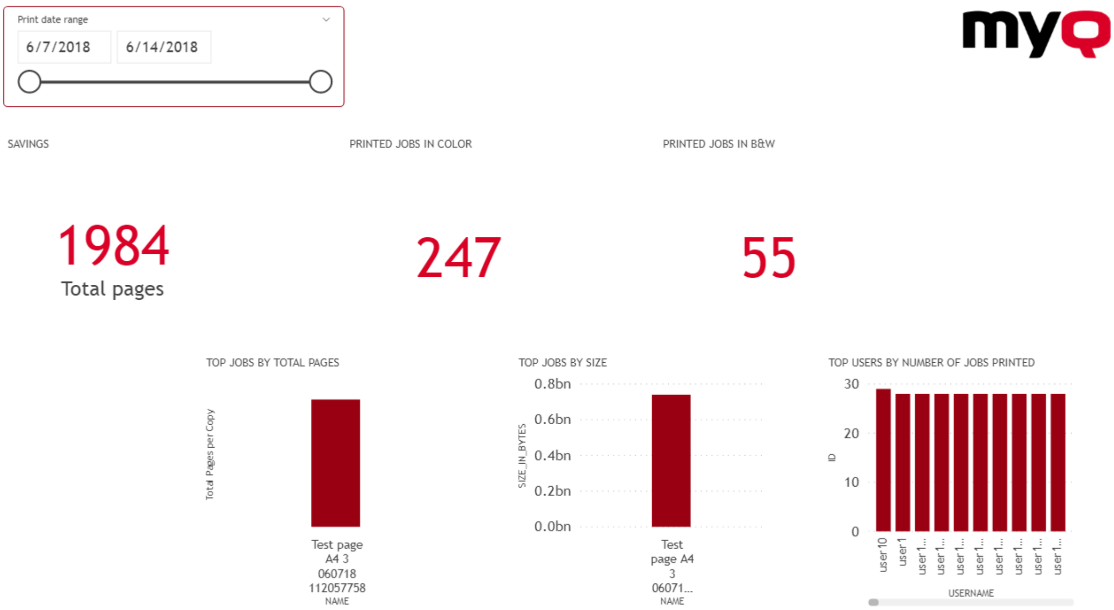
2. Establish the connection to your database:
   a. Add the **Data source name (DSN)** you created in the ODBC Data Sources app and click **Load**.

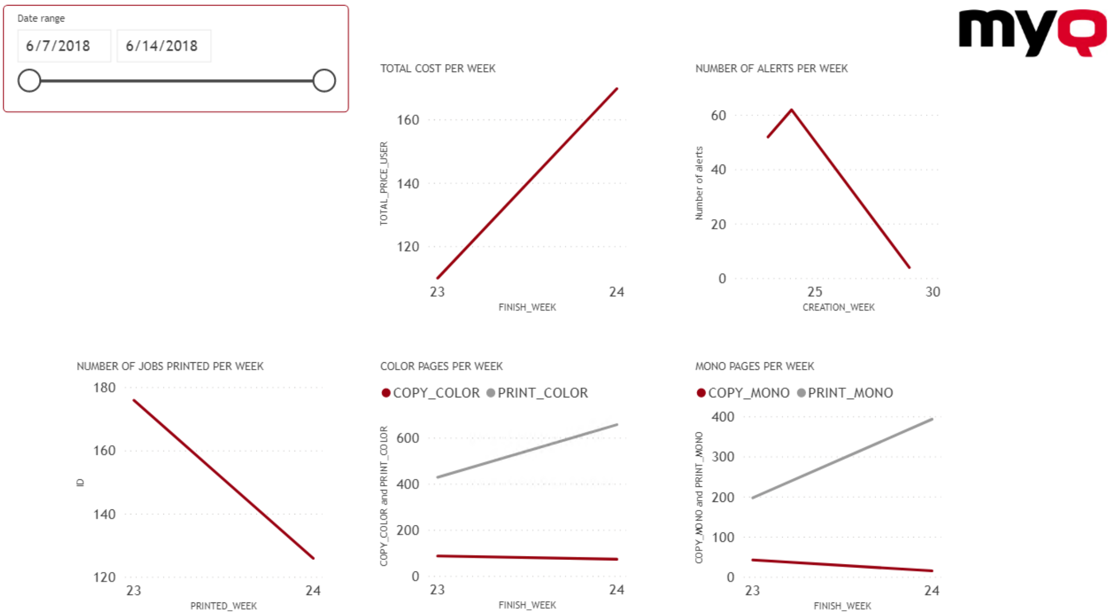


3. Power BI imports the data. The reports can be edited; the changes are saved in a different file so the template can be reused.

13.2.3 Report Examples

The examples below were generated using the MyQ template.





13.2.4 Database Views Description

There are two groups of views; **dimensions** and **facts**. The fact views contain measures, numeric data which can be used in calculations for reports. The dimension views contain descriptive information used for the measures in the facts. Dimension views have the **dim_** prefix and fact views have the **fact_** prefix.

The IDs in the views are internal MyQ IDs and can be used to establish relationships between views.

Printer Dimension (dim_PRINTER_V2) - Information about the printer

Field Name	Description
ID	Printer ID
Name	Printer name
IP_Address	Printer IP address
MAC	Printer MAC address
Brand	Printer brand
Model	Printer model
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**

Field Name	Description
COPIER_COLOR_COUNTER	Total counter of color copies
COPIER_MONO_COUNTER	Total counter of monochrome copies
PRINTER_COLOR_COUNTER	Total counter of printed color pages
PRINTER_MONO_COUNTER	Total counter of printed monochrome pages
SCANNER_COUNTER	Total counter of scanned pages
FAX_COUNTER	Total counter of fax pages

User Dimension (dim_User) - Information about the user

Field Name	Description
ID	User ID
USERNAME	MyQ username
FULLNAME	User's name and surname
EMAIL	User's email
PHONE	User's phone number
PERSONAL_NUMBER	User's MyQ personal number
CREDIT	Credit amount (`null` - if credit is disabled for user)
LANGUAGE	User language
NOTES	Notes (memo text) to users account

Printer Events Fact (fact_PRINTER_EVENTS) - Information about printer events.

Field name	Description
Name	Name of the event
Type	Type of the event (`alert` or `tonerLevel` or `totalCounter` or `tonerReplacement`)
Created	Date and time in which the event was created
Closed	Date and time in which the event was closed
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

Field name	Description
Type	Type of the toner (**cyan** or **magenta** or **yellow** or **black**)
Installed	Date and time in which the toner was installed
Replaced	Date and time in which the toner was replaced
Counters	Total number of pages printed with the toner type of the toner until the toner was replaced
Period	Number of days from the toner installation to the toner replacement
Pages	Number of pages printed by the toner
Printer_Id	ID of the printer where the toner was installed

V_TONERS_INSTALLED

Field name	Description
Name	Name of the toner
Type	Type of the toner (**cyan** or **magenta** or **yellow** or **black**)
Installed	Date and time in which the toner was installed
Replaced	NULL
Counters	Total number of pages printed with the toner type since the toner type installation
Period	Number of days since the toner installation
Pages	Number of pages printed by the toner
Printer_Id	ID of the printer where the toner was installed

Printer jobs counter fact (fact_PRINTERJOB_COUNTERS_V3) - Information about printer jobs counters

Field name	Description
PRINTERJOB_ID	Printer job Id
USER_ID	User Id
USER_GROUP_ID	Group of users
PRINTER_ID	Printer Id
PROJECT_ID	Project Id (-56 for jobs without project)
SITE_ID	Site id
TYPE	Job type. Values: `print`, `copy`, `scan`, `faxRx` (Incoming fax -print), `faxTx` (Outgoing fax - scan)
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

Field name	Description
DUPLEX	Duplex print. Values: `Yes`, `No`
SHEETS	Used sheets of paper
MONO	Monochrome print job
COLOR	Color print job
SINGLE	Single color print job
PRICE	Job price
CLICK_MONO	Click mono
CLICK_COLOR	Click color
SESSION_ID	User session id
JOB_ID	Job id (Reference to user's job)

Job Fact (fact_job) - Information about print jobs

Field Name	Description
ID	Job ID
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

Field Name	Description
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

Field Name	Description
FINISH_DAY	Day when session was finished
FINISH_HOUR	Hour when session was finished
USER_ID	User ID
PRINTER_ID	Printer id
PROJECT_ID	Project id
USER_GROUP_ID	User group id
TOTAL_PRICE_USER	Total price for the user
TOTAL_PRICE_ADMIN	Total price for the admin
TOTAL_PAGES	Total number of pages
PRINT_MONO	Printed pages in black and white
PRINT_COLOR	Printed pages in color
COPY_MONO	Copied pages in black and white
COPY_COLOR	Copied pages in color
COPY_SINGLECOLOR	Copied pages in single color
FAX	Faxed pages
SCAN	Scanned pages
PAPERA4	Pages in A4 paper format
PAPERA3	Pages in A3 paper format

Field Name	Description
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)

There is a limitation that even if you are using a Job Privacy license, the data in the database are not changed by this feature and are still readable.

14 Scanning and OCR

The MyQ system is able to automatically send scanned documents to the scanning user with the **Scan to Me** feature.

MyQ also allows you to use Optical Character Recognition (**OCR**) by either integrating the MyQ OCR server or using a custom 3rd-party application.

The first section of this topic shows you how to set up the **Scan to Me** feature on the MyQ server, how to use it, and how to limit the size of emails with scans.

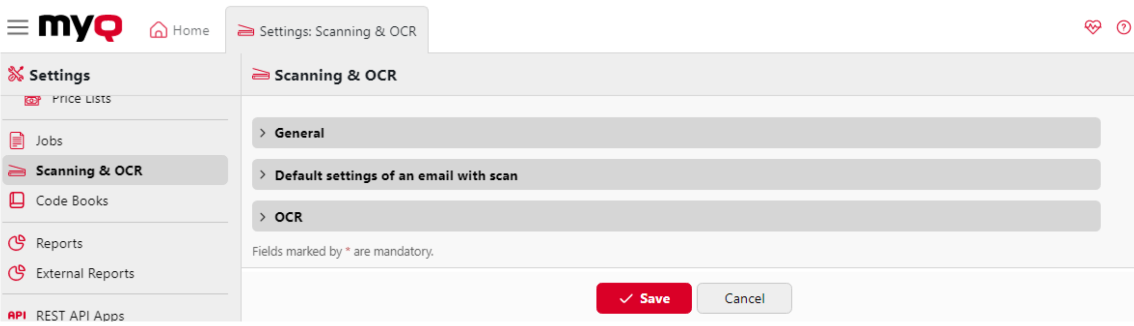
The second section shows you how to set up your **OCR** server.

14.1 Scan to Me

With the **Scan to Me** feature enabled, MyQ serves as an email server — it receives a scanned job from printing devices via the SMTP protocol, detects the device where the job is sent from, finds the user that is currently logged on the device and sends the job to their folder or email (depends on the user's settings).

Scan to Me is also one of the essential features of the MyQ Embedded terminals. Apart from it, the embedded terminals offer a large number of advanced destinations such as **Cloud** and **FTP servers**.

First, you need to set up the feature on the MyQ server and on the printing device to enable the MyQ users to use all of the scanning options. After that, you need to provide the users with an email addresses, where they can direct the scanned documents to.



The correct time and date must be set on the printing device to avoid issues with correct functionality.

14.1.1 Setting up the feature

To set up **Scan to Me**:

- Enable and setup scanning on the MyQ server
- Set SMTP on the printing device
- Set the destinations for the MyQ users on the MyQ server

Enable and setup scanning on the MyQ server

Go to the **Scanning & OCR** settings tab, under **General** and **Enable scanning**.

You can also change the subject and message of the email with the scanned document there. As the sender of the document, you can select either the email of the logged user or the default sender email set on the **Network** settings tab, under **Outgoing SMTP server**.

Set SMTP on the printing device

The scanning function requires enabling the SMTP protocol, setting the SMTP server address and entering a sender email on the printing device web interface. For information about how to enter the printing device web interface and find the particular settings, see the printing device manual.

To enable the scanning function, take the following steps on the printing device web interface:

- Enable SMTP protocol.
- Enter the MyQ server IP address or hostname.
- Ensure that the SMTP port is the same as the SMTP port in the **Network** settings tab, under MyQ SMTP server. The default port in MyQ is *25*.
- Enter sender email address. The address value is arbitrary.

14.1.2 Set the destinations for the MyQ users on the MyQ server

On the properties panel of each individual MyQ user (see Editing user accounts), you can set the destinations using these options: **Sending scans to the user's primary email, Storing scans to the user's scan folder**.

To provide a user with these options, set the appropriate fields on their properties panel, according to the following table.

Option	Parameter	Value
Sending scans to the user's primary email	Email	User's primary email address
Storing scans to the user's scan folder	User’s storage	Folder where the document should be stored

14.1.3 Using the Scan to Me Feature

To send the email to the desired destination, the scan needs to be directed to a specific receiver email address. There are two options to enable the MyQ users to send the scans there: provide them with the respective receiver email address, or predefine these email addresses on the printing device's Web User Interface.

Email addresses for Scan to Me

- **Sending scans to the user's primary email** - The scanned document is sent to the user email set in the email text box on the user properties panel.
  The receiver email address has to be *email@myq.local*.
- **Storing scans to the user's scan folder** - You have to create a shared folder and ensure that MyQ has access to this folder. After this, enter the folder's location to the **User's storage** text box. The scanned document is sent to MyQ, and then stored in the shared folder via the SMB protocol. The stored document file name consists of the user account name, and the date and the time when the scan was sent.
  The receiver email address has to be *folder@myq.local*.

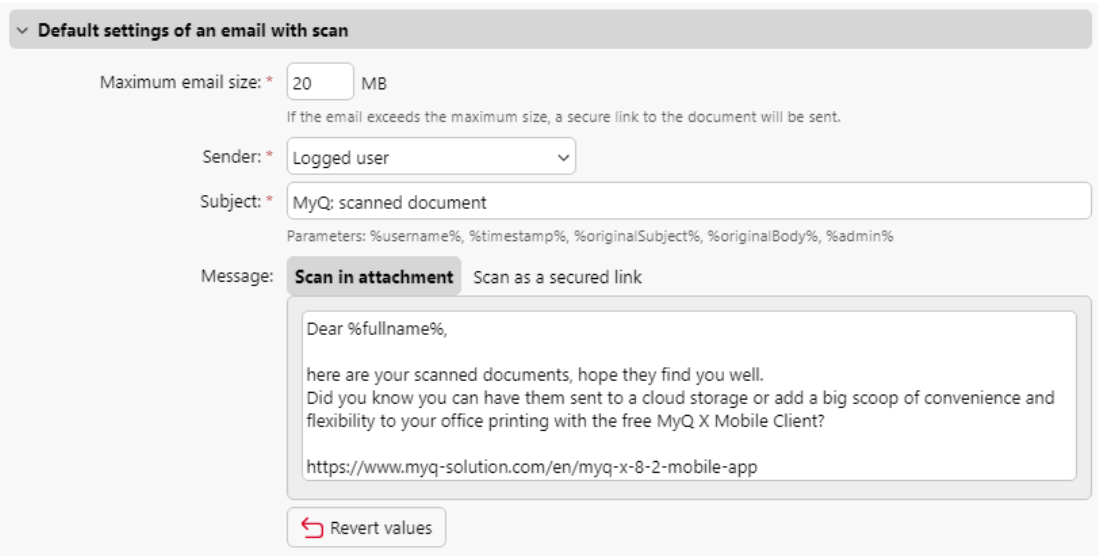
To enable MyQ to save the scan file in the user scan folder, you have to make sure that the folder is shared over your network and that the computer where you run MyQ has all the necessary access rights to this folder.

Predefined list of the MyQ destinations on the printing device

On the **Address List** on the printing device's web interface, you can predefine email addresses where the scanned documents are sent to.

14.1.4 Scan Email Size Limits

Due to email size restrictions in some email servers, users might not be able to send scans exceeding a certain size to their emails. To prevent such situations, you can set the maximum size of emails with scans on the MyQ Web Interface. Emails exceeding the limit are then replaced by emails with a secure link to the scan file, which is saved on the MyQ print server.



- **Maximum email size** - Set the maximum size limit (in MB) of the email with the scan. The default value is *20 MB*.
- If the scan is bigger than the above limit, it will be sent as an email with a secure link to the scan.

You can edit the email **Sender**, **Subject**, and **Message** as well.

You can use multiple parameters, such as *%username%, %timestamp%, %admin%, etc*.

The *%links%* parameter represents the actual link to the stored scan file.

14.2 OCR

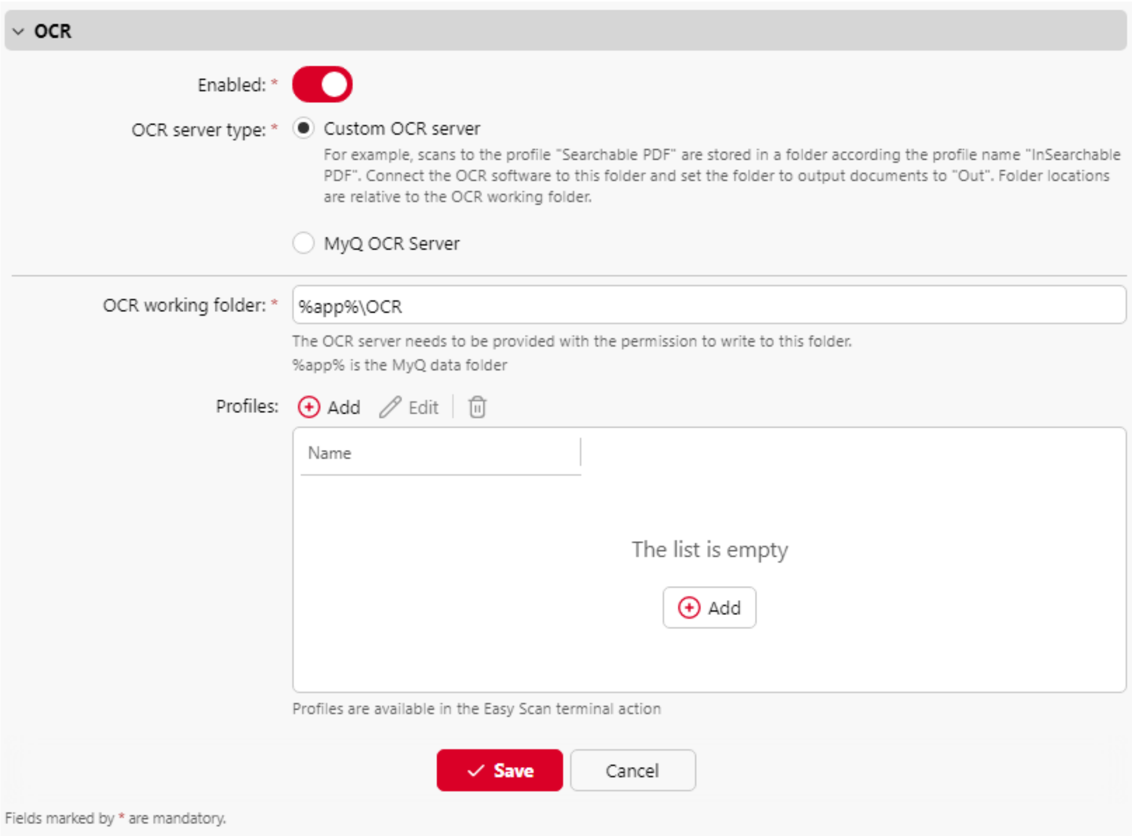
Optical Character Recognition (**OCR**) is a service that converts scanned documents to a searchable and editable format, such as a text document or a searchable PDF. To provide this functionality, you can either use the MyQ OCR server, which is a part of the MyQ solution, or you can employ a third-party application.

For more information, see the (3.2) MyQ OCR Server documentation.

MyQ Print Server 10+ requires MyQ OCR Server 3.0+.

14.2.1 Activation and setup

The OCR feature has to be enabled on the **Scanning & OCR** settings tab, under **OCR**.



Choose the **OCR server type**:

- *Custom OCR server* - select this option if you have your own Document Management System (DMS) for document processing or any other OCR-capable application.
- *MyQ OCR Server* - select this option if you already have the MyQ OCR Server set up and running.

You can change the folder where the scanned data is sent in the **OCR working folder** field. It is however, not recommended to change the default folder (*C:\ProgramData\MyQ\OCR*).

The OCR folder contains two sub-folders: **in** and **out**. In the **in** folder, the scanned documents are stored before being processed. In the **out** folder, the processed documents are saved by the OCR software and are ready to be sent.

In the **Profiles** section, you can set up OCR profiles to be used in the Easy Scan terminal action.

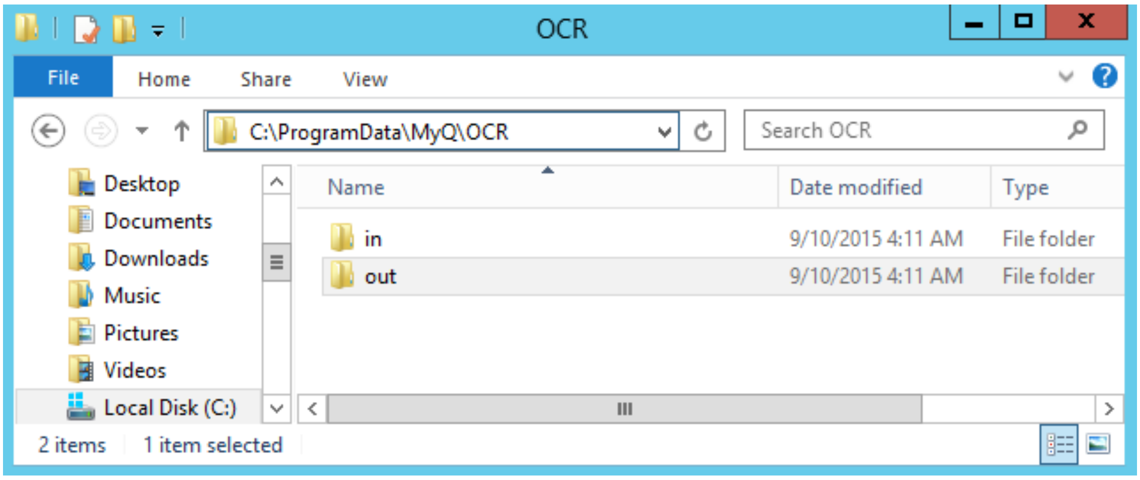
Click **Add**, set a **Name** for your new profile and select the **Output**, either *pdf*, *pdfa* or *text*, and click **Save**. You can now set this OCR profile as the **Default value** in the **Format** parameter of your Easy Scan terminal action.

A document sent to be processed by OCR is received with a certain delay, depending on the OCR software speed, and on the size of the document.

Running the OCR software on the same production server as MyQ may affect your system's performance.

14.2.2 OCR Processing

The OCR software should listen to the document sub-folders of the **in** folder (*in\pdf, in\txt,...*), process the file that was sent there, save the converted document to the **out** folder and delete the source file from the *in*folder** folder.



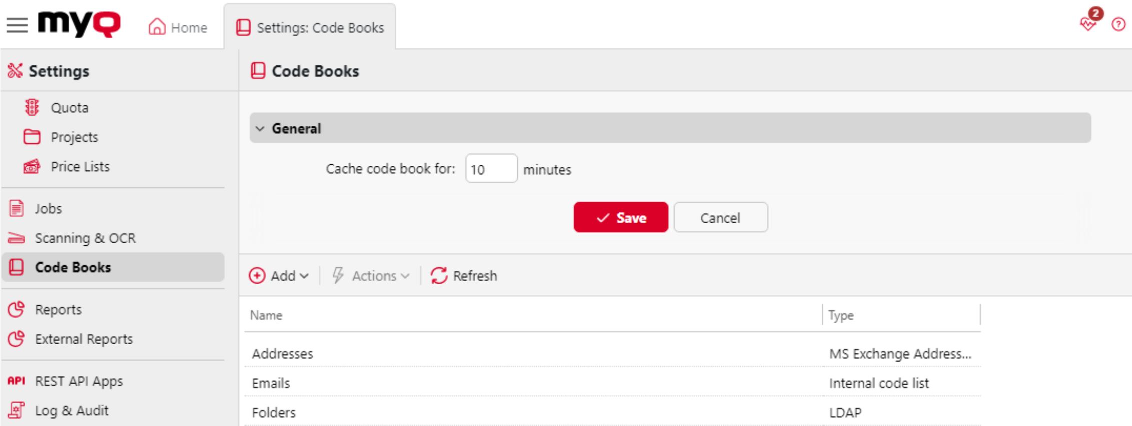
MyQ listens to the **out** folder, sends the converted file to the user and deletes it from the folder.

The converted file is sent to the folder listed in the **User's storage** text box, in the user properties panel.

The file sent to the **out** folder by the OCR software has to have the same name as the source file in the **in***** folder. If the name of the converted file differs from the source file, it is deleted without being sent to the user.

15 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 (available only when eGoldFax connections are enabled in *config.ini*.)

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.

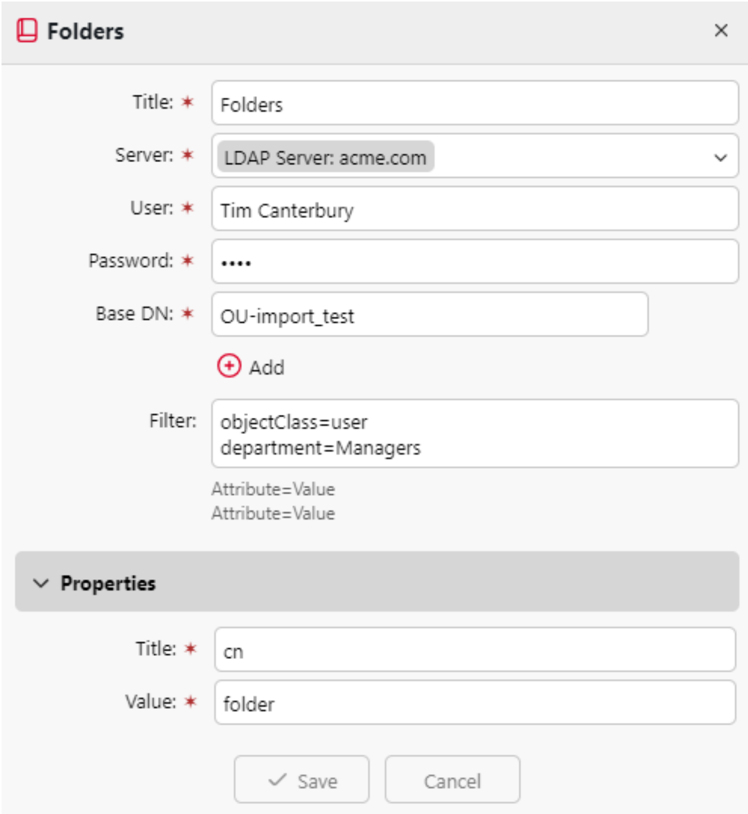
To delete a code book, select it, click **Actions**, and select **Delete**, or right-click on the code book and select **Delete**.

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.

15.1 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

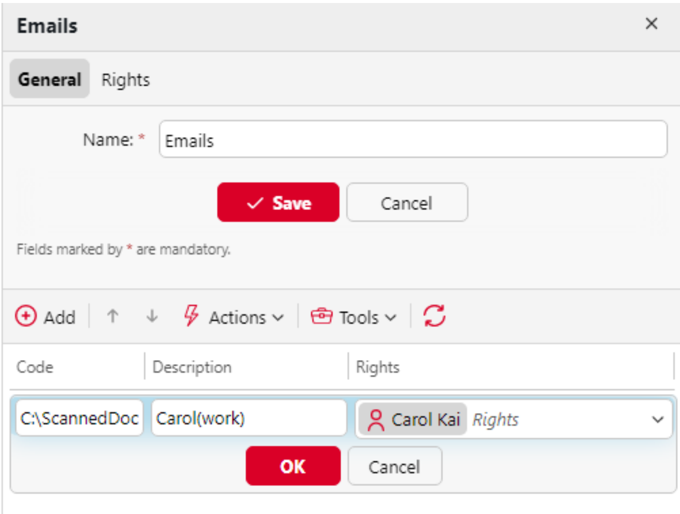
enter the *cn* attribute as the **Title** and the *folder* attribute as the **Value**. This way, each code will contain the user's folder and its title will be the user's full name.

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.

15.2 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.

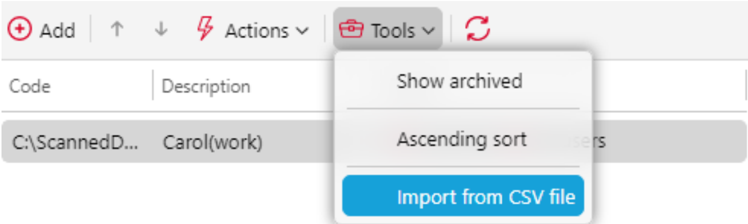
Add new codes to an existing code list

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**.

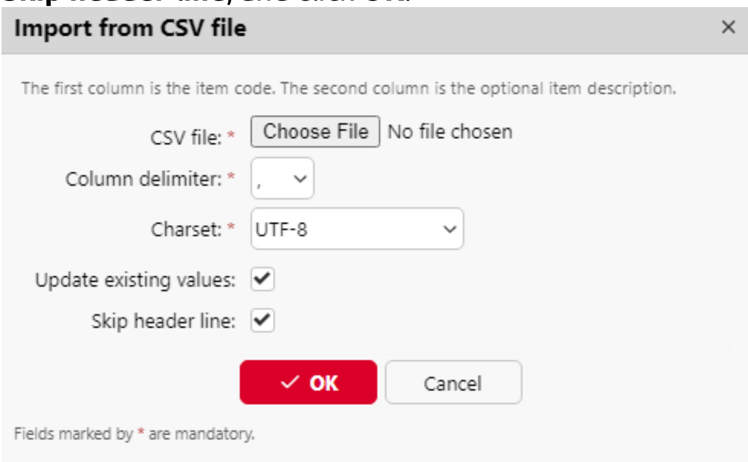
Import codes from a CSV file

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

15.3 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.

The following versions are supported:

- MS Exchange Server 2013 SP1 (from build 15.0.847.32)
- MS Exchange Server 2016
- MS Exchange Server 2019

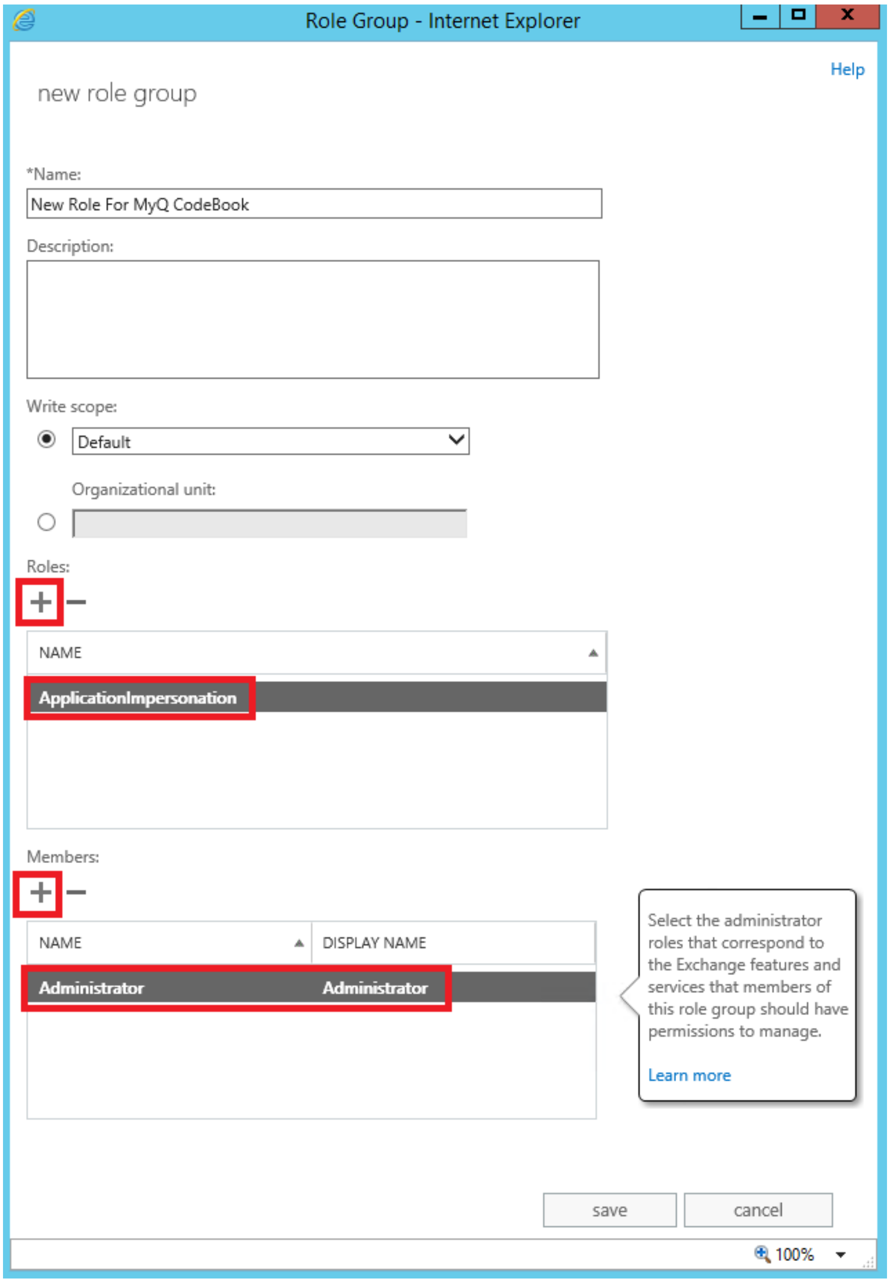
15.3.1 MS Exchange Server Configuration

All settings on IIS (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:

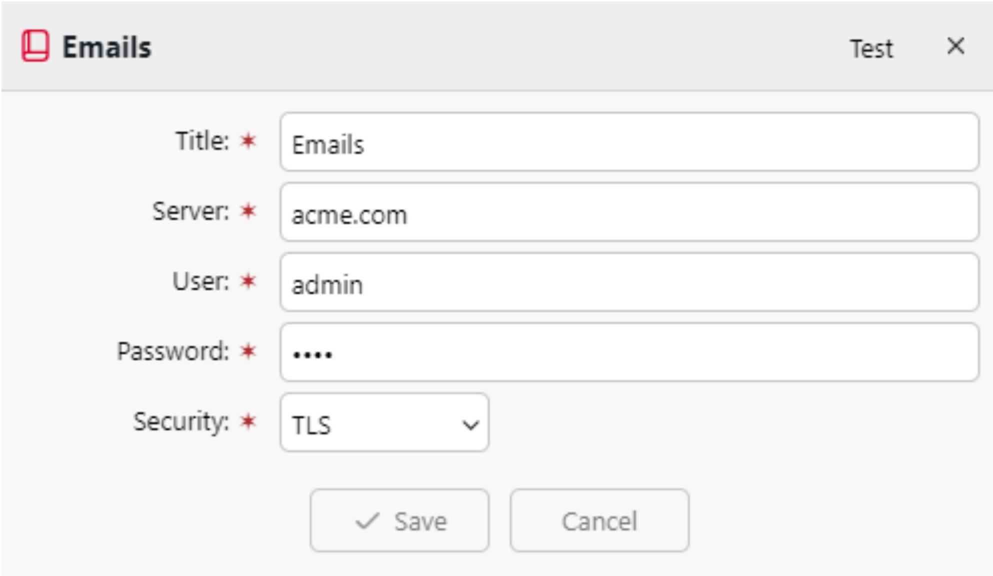
- Log in to your Exchange Admin Center.
- Go to the **permissions** tab, and Create (+) a new **Admin Role**.
- In this new role, add the **ApplicationImpersonation** right.
- In this new role, add user/admin account that you want to use in MyQ for accessing personal contacts of other users' mailboxes.



15.3.2 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:

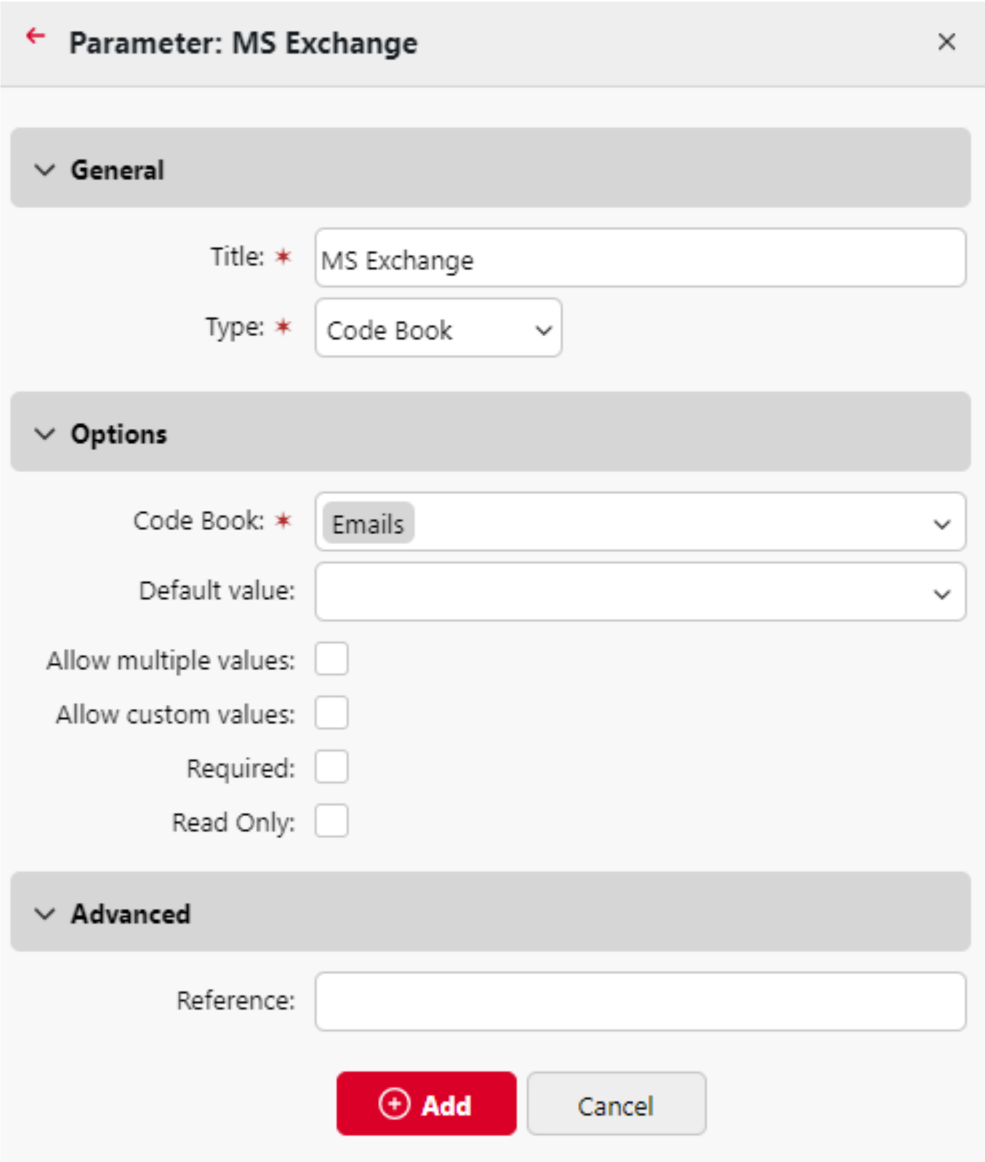


- **Name** - Add a name for the code book.
- **Server** - The host name or the IP address of the MS Exchange Server.
- **User** - The name of the user who has the required rights (*applicationImpersonation* to access other users' mailboxes) on the MS Exchange Server.
- **Password** - The above user's 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.

15.3.3 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.

16 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.

16.1 Credit Refund

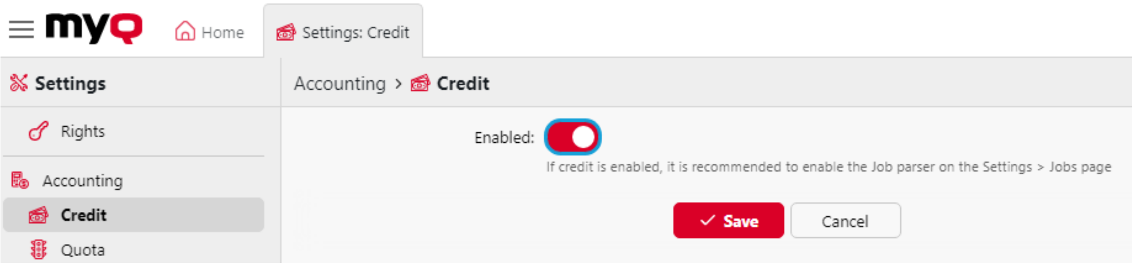
Direct credit refund from MyQ is not supported. If you need to reverse a transaction using any of the supported payment providers, you must then manually adjust the user’s credit balance in MyQ. This can be done by users with Administrator and Recharge credit roles.

16.2 Activation and Setup

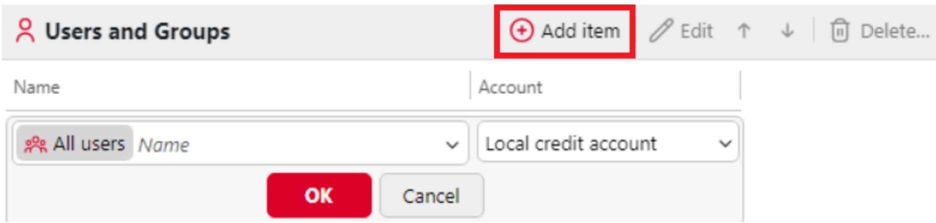
The activation and setup of credit accounting is managed on the **Credit** settings tab (**MyQ > Settings > Credit**).

To set up credit accounting:

Enable credit accounting on the **Credit** settings tab:



Activate credit for a user or for a group of users:



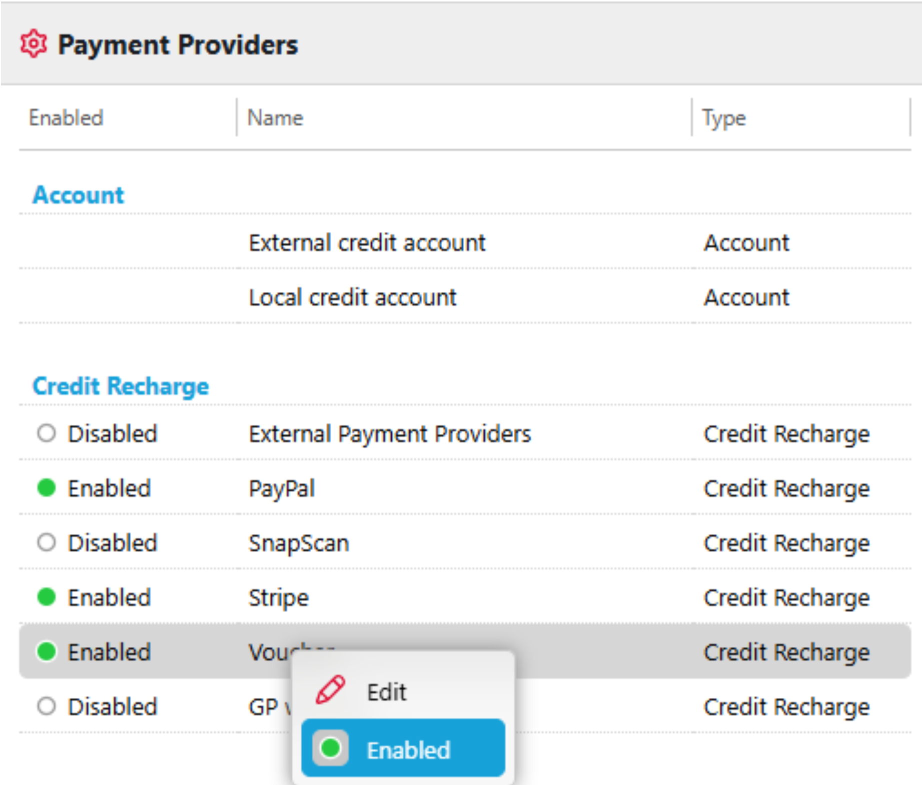
- Under **Users and Groups**, click **+Add item**. A new item appears on the list of users and groups on the **Credit** settings tab.
  - Select a **Name** from the drop-down list.
  - Select an **Account** from the drop-down list. The available options are:
    - Local credit account
    - External credit account
- Click **OK** to save the settings.

Enable/disable payment methods for credit recharge

Available payment methods:

- External Payment Providers
- PayPal
- SnapScan
- Stripe
- Voucher
- GP webpay

To enable any of these options (if disabled), select it in the **Payment providers** section, and then click **Enabled** on the bar at the top of the section (or right-click the item, and then click **Enabled** on the shortcut menu).



16.3 Manual Credit Recharge

The administrator (and users authorized to recharge credit) can manually recharge the credit of each user to a specific value. This can be done either on the **Credit Statement** main tab, or on the **Users** main tab in the MyQ Web administrator interface.

On the **Credit Statement tab**, you first open the credit recharge action, and subsequently select the users and groups to recharge credit.

On the **Users** tab, first select the users or group, and then recharge their credit.

Users' credit can be reduced by entering a negative number in the recharge credit dialog box. By entering *-100*, the credit is decreased by 100.

16.3.1 Providing Users with Rights to Recharge Credit

By default, the only person who can recharge credit is the administrator. However, the administrator can authorize a MyQ user to recharge credit as well. The user needs to be provided with the rights to access the credit settings and to recharge credit. This is done on the Rights settings tab of the MyQ Web Interface.

To authorize a user to recharge credit on the **Credit Statement** tab, you need to provide them with the right to **Recharge credit**.

To authorize a user to recharge credit on the **Users** tab, you need to provide them with the right to **Manage Users**.

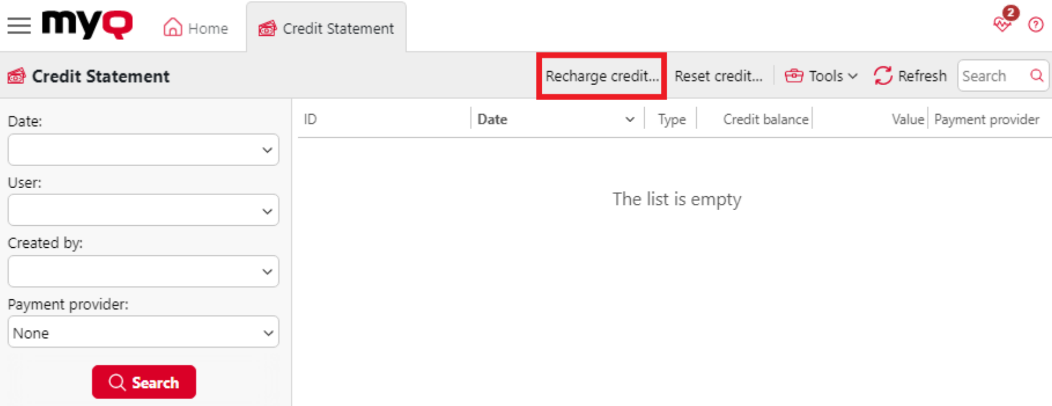
The authorized user can then recharge credit on their MyQ Web interface in the same way as the MyQ administrator.

16.3.2 Recharging Credit on the Credit Statement Tab

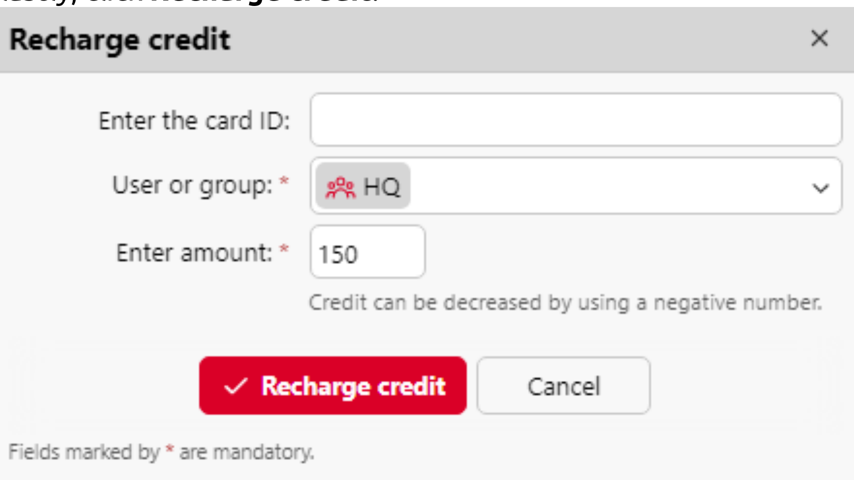
On the **Credit Statement** tab, you can overview the changes in the credit balance of MyQ users, and also recharge credit to users and groups. To open the tab on the MyQ Web administrator interface, go to **MyQ, Credit Statement**.

To recharge credit to users or groups:

1. Click **Recharge credit**. The Recharge credit dialog box appears on the tab.



2. In the dialog box, either **Enter the card ID** of a user card, or select the **User or group** to recharge the credit to, then **Enter amount** to be recharged, and lastly, click **Recharge credit**.



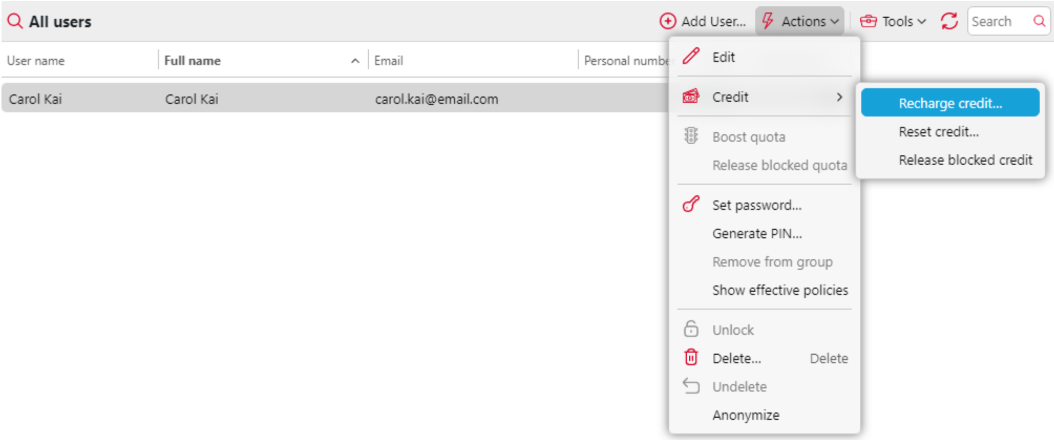
16.3.3 Recharging Credit on the Users Main Tab

To open the **Users** main tab on the MyQ Web administrator interface, go to **MyQ, Users**.

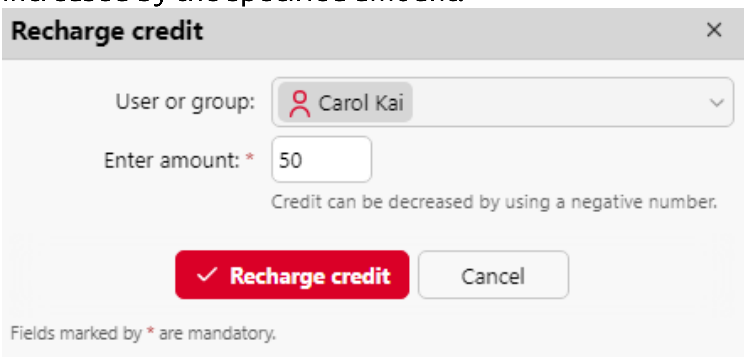
To recharge credit to selected users:

1. Select the users.
2. Click **Actions**.

3. Hover over **Credit** and click **Recharge credit** in the **Actions** drop-down. The Recharge credit dialog box opens.

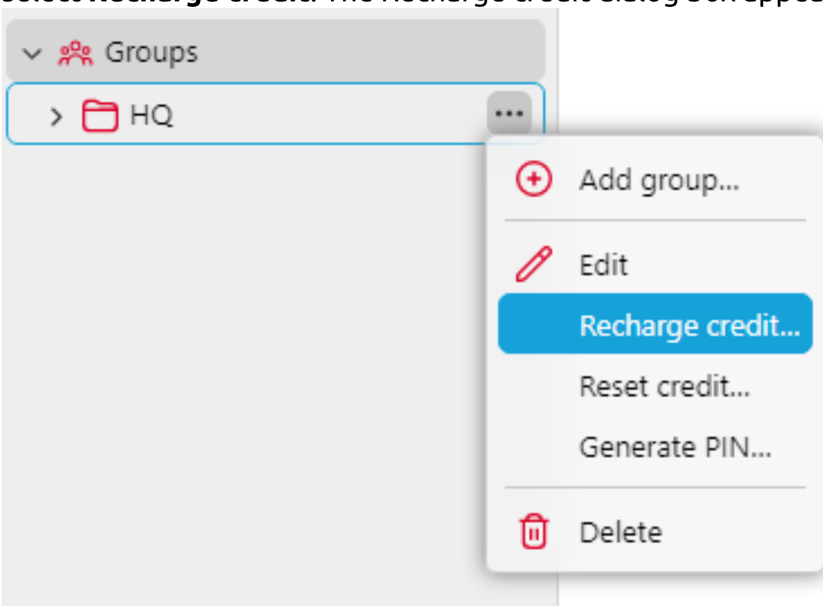


4. **Enter amount** to be recharged, and then click **Recharge credit**. The credit is increased by the specified amount.



To recharge credit to a group of users:

1. In the panel on the left side of the **Users** main tab, right-click the group, and select **Recharge credit**. The Recharge credit dialog box appears.



2. In the dialog box, **Enter amount** to be recharged, and click **Recharge credit**. The credit is increased by the specified amount.

16.4 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.

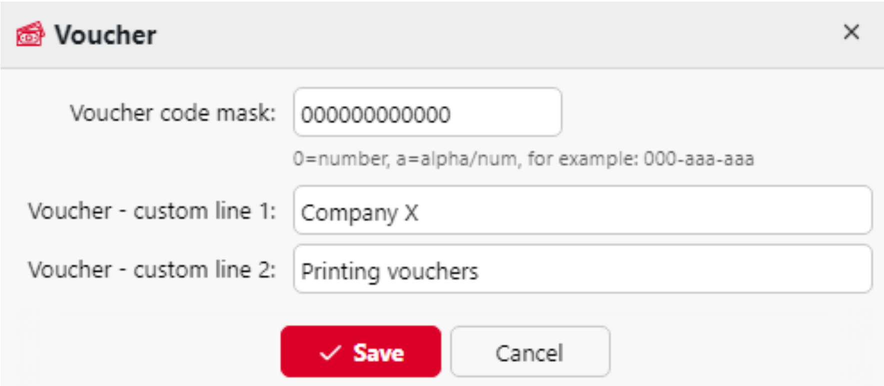
16.4.1 Setting the Voucher Format

Before the vouchers are generated, it is necessary to set the format of the voucher unique code and define the text printed on the voucher. These parameters can be set and modified on the **Credit** settings tab, under **Payment providers**. Select **Voucher** and mark it as **Enabled**. Then, double-click the **Voucher** item (or select the item and click **Edit**) to open the **Voucher** properties panel.

The unique code format can be defined by creating a **Voucher code mask** – a predefined code template consisting of zeroes and lower case a's. Zeroes are substituted by numbers and a's are substituted by upper case letters or numbers. For example, the *00a0000aaa* mask will generate numbers such as *86D9841POE, 03E8976E67,* etc.

Always set the code format adequate to the number of users and the frequency of the voucher generation process, to ensure a sufficient variety of codes. If the amount of the currently valid codes is large and the variety not sufficient, the chance of randomly guessing the valid code number is high and the credit system can be easily bypassed.

The text entered in the **Voucher-custom lines 1 and 2** fields is displayed on the printed vouchers. You
can enter, for example, the name of your company and additional information.



Do not forget to set the currency on the **General** settings tab, if you have not set it earlier. The currency on the printed voucher is the same as the one set in MyQ.

16.4.2 Custom Logo for Credit Vouchers

If you want to use your own logo on MyQ credit vouchers instead of the default MyQ logo, you can import the new logo on the Personalization Settings tab in the MyQ Web Administrator Interface.

The file with the logo has to be in the *JPG, JPEG, PNG* or the *BMP* format; the recommended size of the logo is *398px* x *92px*.

To import the logo:

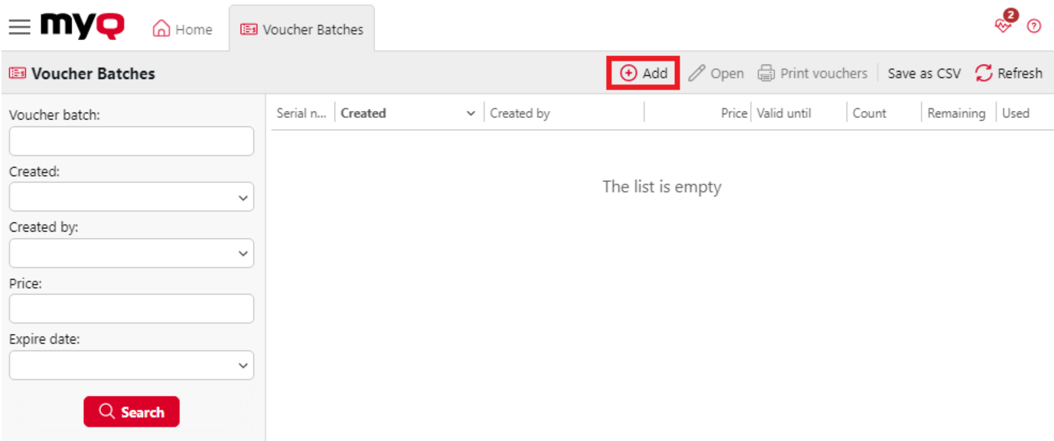
1. On the MyQ Web administrator interface, open the **Personalization** settings tab. (**MyQ, Settings, Personalization**).
2. On the tab, under **Custom application logo**, click **+Add**, browse and upload the file with the logo, and lastly click **Save** at the bottom of the tab. A preview of the new logo is displayed on the tab.

16.4.3 Voucher Batches

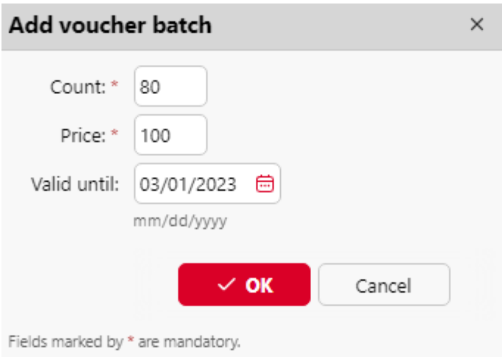
Vouchers can be generated on the **Voucher Batches** tab of the MyQ Web Interface. To open this tab, go to **MyQ, Voucher Batches**.

To generate new vouchers:

1. On the bar at top of the **Voucher Batches** tab, click **+Add**. The Add voucher batch dialog box appears.



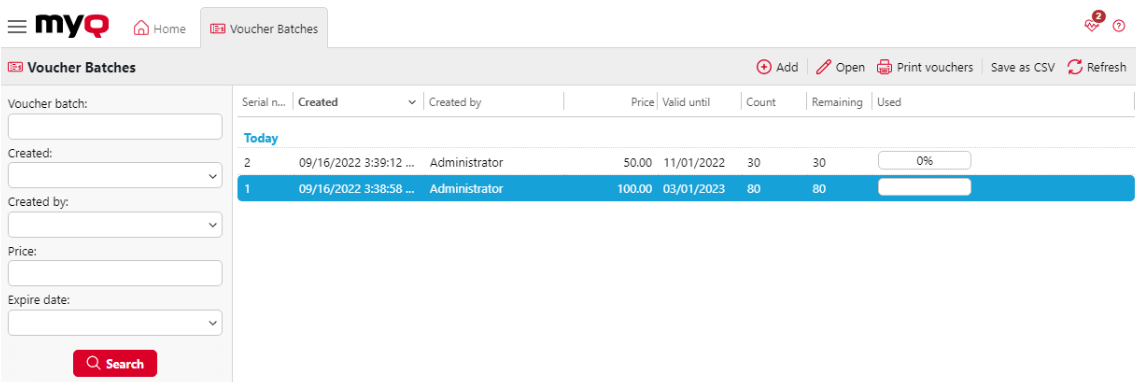
2. In the dialog box, enter the number of vouchers to be generated in the **Count** field, the **Price** of the vouchers, add the validity period in the **Valid until** field, and then click **OK**.



The new voucher batch record is displayed in the voucher batches list. You can overview all of the vouchers by double-clicking a record.

Managing Voucher Batches

Voucher batches can be filtered by serial number, date, creator, price, expiry date, etc. From the **Voucher Batches** main tab, you can export the list of voucher batches to a CSV, and display and print vouchers included in particular batches.



16.4.4 Providing Users with Rights to Manage Vouchers

To enable users to manage vouchers on the **Voucher Batches** main tab, provide them with the **Manage Vouchers** rights.

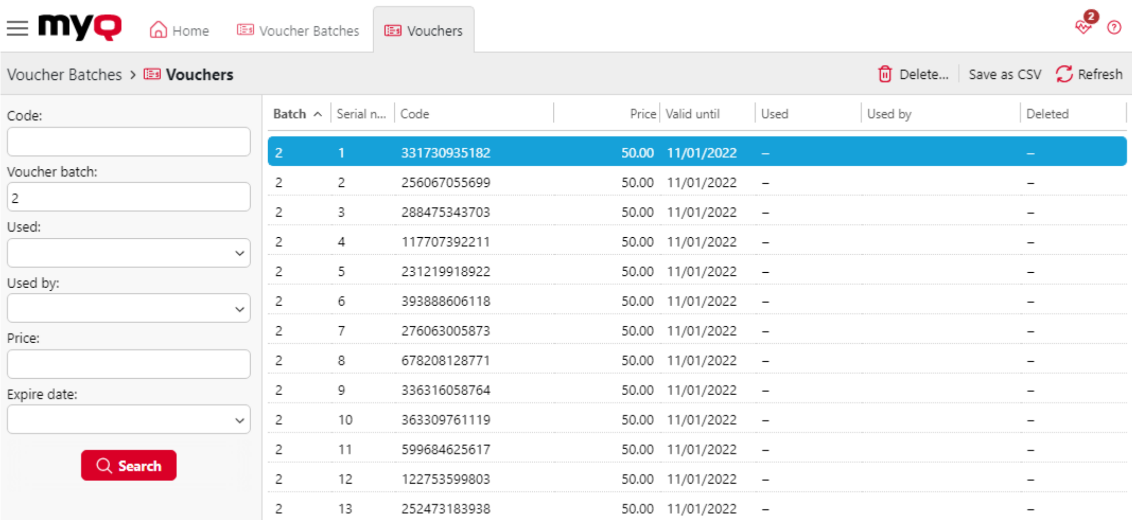
For more information about rights and how to provide them, see Rights.

16.4.5 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.



16.5 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.

16.5.1 Setting up PayPal Payments

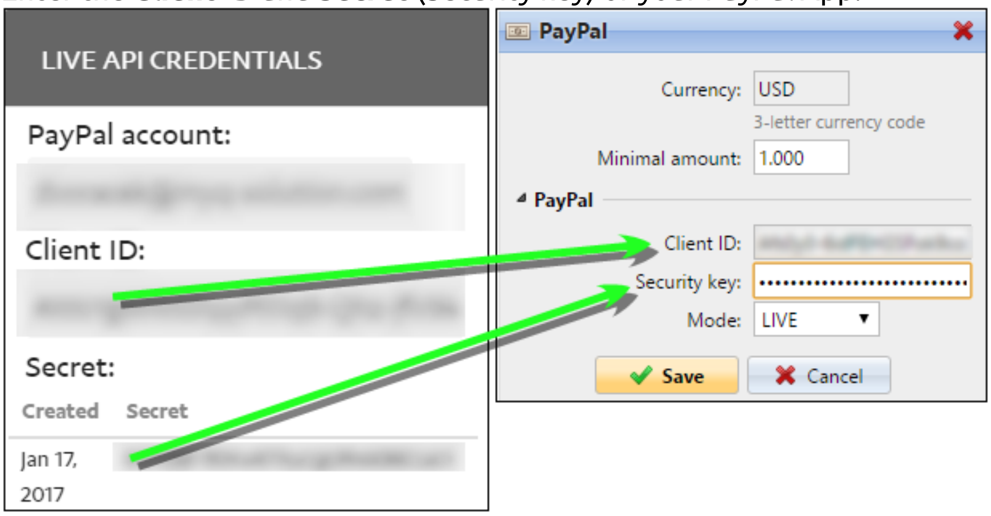
To integrate PayPal with MyQ, you first create a new App in your organization's PayPal Business account. Then you set up PayPal as a payment option in the MyQ server settings.

Create a new App in the PayPal Developer Environment

1. Log in to the PayPal developer portal (https://developer.paypal.com/) with your PayPal Business account.
2. On the **Dashboard**, under **MyApps & Credentials**, create a new REST API app.
3. In the App properties, select **Live** and remember (copy) the app **Client ID** and **Secret**. MyQ uses this information to register your PayPal account.

Set up PayPal Payments in MyQ

1. Go to **MyQ, Settings, Credit**.
2. Under **Payment providers**, double-click the **PayPal** payment provider. The **PayPal** properties panel opens.
3. Type the minimum amount that users must pay when they buy credit.
4. Enter the **Client ID** and **Secret** (Security key) of your PayPal App.



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**.

16.5.2 Recharge User Credit with PayPal

To update their credit with PayPal, the user completes these steps in the MyQ Web Interface.

1. Log in to the MyQ Web Interface.
2. Go to **Credit** and click **Recharge Credit**.
3. Select **PayPal** as the payment provider and type how much credit to recharge.
4. Click **Recharge Credit**.
   PayPal opens in a new window where the user completes the payment. PayPal

then redirects the user back to MyQ, where a **Payment successful** dialog box appears.

If you encounter errors with payment provider integration:

- **Check DNS settings -** Ensure your hostname resolves correctly from external DNS servers.
- **Verify redirection is not blocked -** Ensure that redirects between the payment provider and your server are not being blocked by firewalls, security settings, or network configurations.

16.6 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.

16.6.1 Setting up GP Webpay

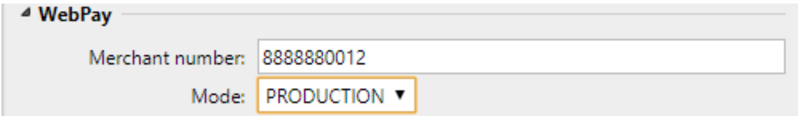
You need to have a GP webpay account, get a public and a private key; the public key has to be uploaded to the GP webpay server and the private one needs to be uploaded to MyQ. Also, you need to remember/copy the password of the private key. You can either use your own keys (for more information, see https://developers.mygp.global/en/p/webpay/) or use the GP webpay tools to create new ones.

MyQ needs the following data:

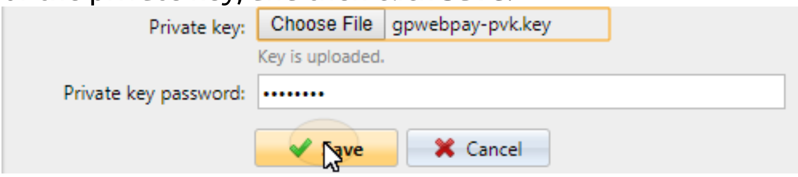
- **Merchant number**: The Merchant number can be found on the GP webpay portal, under **Key management**.
- **Private key**: The private key can be generated on the GP webpay portal, under **Key Management**. It can be in the *.key*, *.pem* or *.crt* format.
- **Private key password**: The private key 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*.

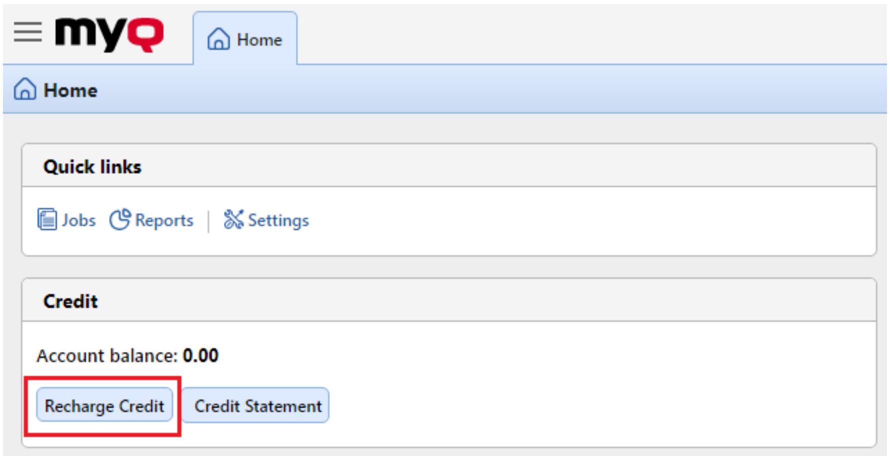


6. Upload the **Private key** from GP webpay (click **Choose File**, select the file, and then click **Open**), enter the **Private key password** provided during generating of the private key, and then click **Save**.

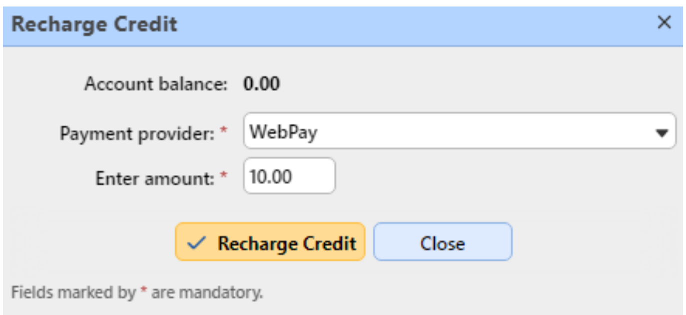


16.6.2 Recharging credit via GP webpay on the user's account on the MyQ Web Interface

First of all, the user needs to log in to their account on the MyQ Web Interface. To recharge the credit there, the user has to click **Recharge credit** under **Credit**. The Recharge credit dialog appears.



In the dialog box, the user has to select the **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.

16.7 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.

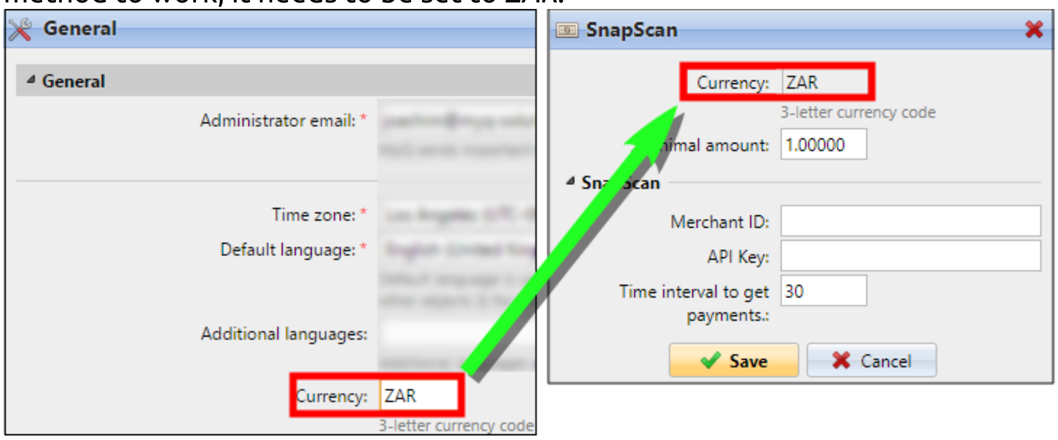
To be able to connect **SnapScan** to MyQ, you need to create a **Merchant Snapscan Account** and obtain the **Merchant Account API**. Within the setup of the connection on the MyQ Web Interface, you must enter the **Merchant ID** and the **API key** of the account.

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.

16.7.1 Setting up the SnapScan payment option

To set up the SnapScan payment option on the MyQ Web Interface:

1. Open the **Credit** settings tab (**MyQ, Settings, Credit**).
2. On the tab, under **Payment providers**, double-click the **SnapScan** payment provider. The **SnapScan** properties panel opens on the right side of the tab.
3. The value of the **Currency** setting corresponds to the currency set on the **General** settings tab of the MyQ Web Interface. For the SnapScan payment method to work, it needs to be set to *ZAR*.

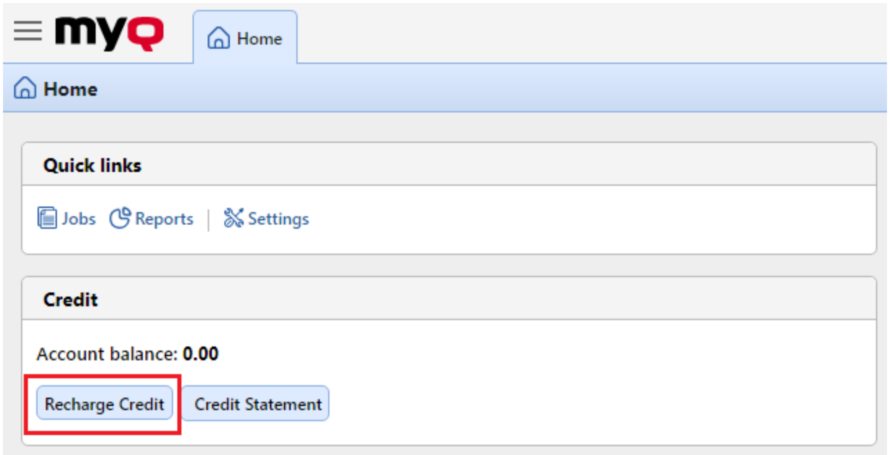


4. Type the **Minimal amount** of money that has to be paid when a user buys the credit.
5. Enter the **Merchant ID**(Company Name) and the **API key** provided by SnapScan.

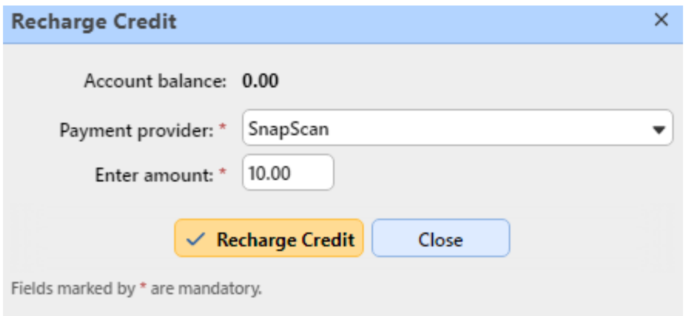
6. Set the **Time interval to get payments** (in seconds), and click **Save**. The **Time interval to get payments** setting limits the time for the recharge action; if MyQ does not receive confirmation of the payment within the interval, the credit recharge is canceled. If the payment is successful but MyQ does not receive the response within the time limit, the user has to contact the MyQ administrator, who can manually recharge the credit.

16.7.2 Recharging credit via SnapScan on the user's account on the MyQ Web Interface

First of all, the user needs to log in to their account on the MyQ Web Interface. To recharge the credit there, the user has to click **Recharge credit** under **Credit**. The Recharge credit dialog appears.



In the dialog box, the user has to select the **SnapScan** payment provider, **enter the amount** of credit that they want to buy, and then click **Recharge Credit**.



A window with the SnapScan payment options opens in the web browser; the rest of the steps correspond to the standard SnapScan payment process.

After the payment is successfully sent to MyQ, the **Payment successful** dialog box appears.

SnapScan tries to connect to the MyQ server via the hostname or IP address that is set on the Network Settings tab of the MyQ Web Interface. In case a hostname is set on the tab and paying users receive the "*This site can't be* *reached / XYZ's server DNS address could not be found. / DNS_PROBE_FINISHED_NXDOMAIN*" message, try to replace the hostname with the IP address of your server.

16.8 Recharging Credit via Stripe

Stripe is a payment provider that supports a range of payment methods, including credit and debit cards, and bank transfers, which you configure and manage from your Stripe dashboard.

With an activated Stripe account you can integrate with MyQ so that users can recharge their MyQ credit via Stripe payments from the MyQ Web Interface.

To avoid currency conversion fees, ensure that the 3-letter currency set in **MyQ > Settings > General** is also configured among your settlement currencies in Stripe.

16.8.1 Setting up Stripe Payments

To set up Stripe as a payment provider in MyQ, you simply need to generate a Stripe restricted key and enter it in MyQ. You don't need to create any special product catalog items – payments from MyQ are automatically processed in Stripe as **MyQ Credit.**

We recommend that you use use a unique restricted key for each of your Print Server instances.

Use a Stripe sandbox key to test MyQ integration. When you are ready, generate a restricted key from your live Stripe environment and set it in MyQ.

For more information, see the following resources in the Stripe documentation:

- https://docs.stripe.com/get-started
- https://docs.stripe.com/keys
- https://docs.stripe.com/testing

Create a Restricted Key in Stripe

You generate a restricted key through the Stripe Developers Dashboard.

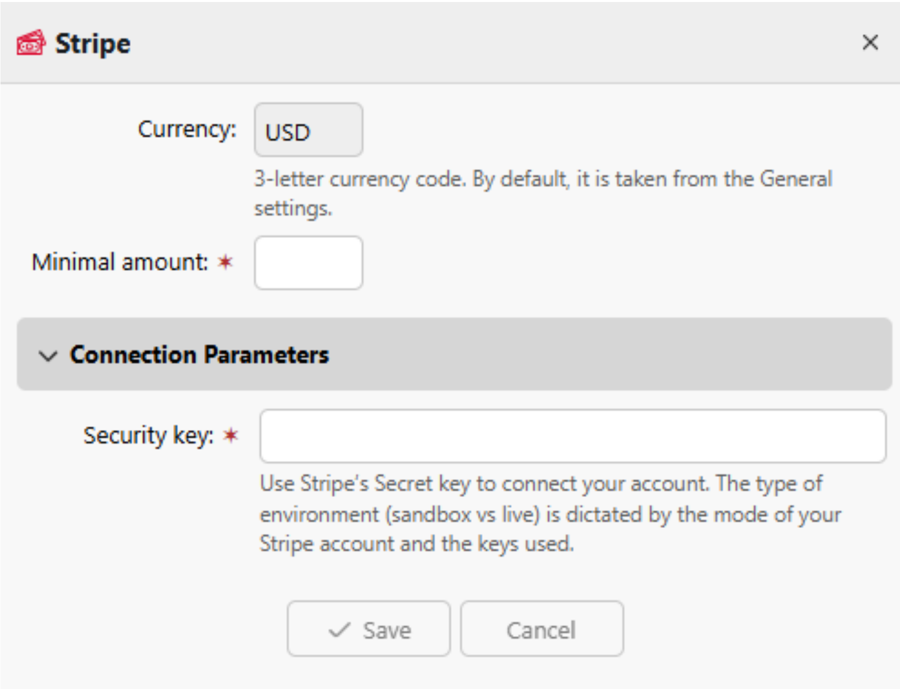
1. Log in to your Stripe account and select the environment that you want to use with MyQ.
2. Go to the **API keys** page in the Developers section of your Stripe Dashboard.
3. In the **Restricted keys** section, click **+ Create restricted key**.
4. Select **Building your own integration** and click **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 enter this token in MyQ.

Configure Stripe in MyQ

1. Log in to 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 users can buy.
4. Enter your Stripe **restricted key token** in the **Security key** field, and click **Save**.



16.8.2 Recharge User Credit with Stripe

To update their credit with Stripe, the user completes these steps in the MyQ Web Interface.

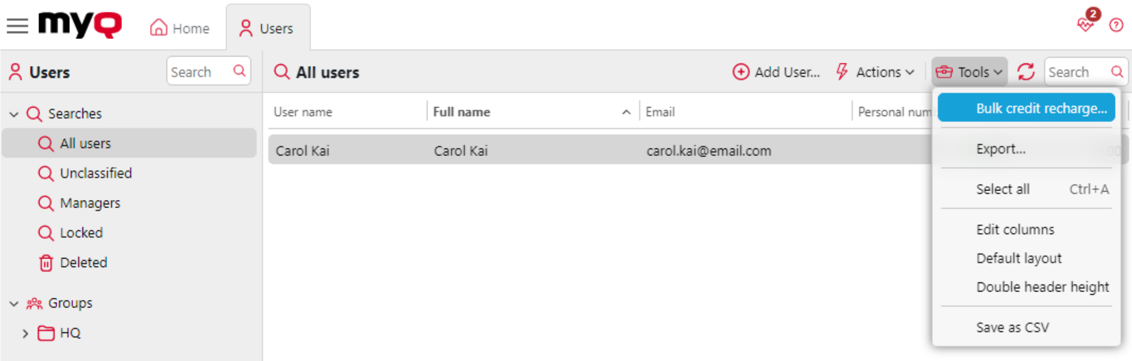
1. Log in to the MyQ Web Interface.
2. Go to **Credit** and click **Recharge Credit**.
3. Select *Stripe* as the payment provider and enter the desired amount of credit to purchase.
4. Click **Recharge Credit**.
   A Stripe checkout window opens, where you complete your payment. After successful payment, 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.

16.9 Bulk Credit Recharge

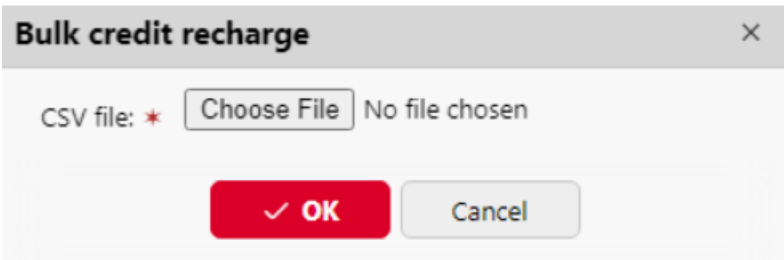
In MyQ, you can also import a bulk of credit from a CSV file.

The feature can be managed on the **Credit Statement** tab or on the **Users** main tab. To import a bulk of credit from CSV on either of the two tabs:

On the bar at the top of the tab (**Users** or **Credit Statement**), click **Tools**, and then click **Bulk credit recharge** in the **Tools** drop-down. The Bulk credit recharge dialog box opens.



In the dialog box, choose the **CSV file** to upload, and then click **OK**. You will be informed about the success of the operation and you can see the added amount of credit in the **Credit** columns on the user list.



Structure of the CSV file:

Each non-empty row has to consist of two entries separated by a delimiter:
*name of the user*delimiter*amount of credit*

The entered delimiter has to be the same as the delimiter set on the **General** settings tab, under **Column delimiter in CSV**.

16.10 Manual Reset of Users' Credit on the MyQ Web Interface

The administrator (and users authorized to recharge credit) can manually reset the credit of each user to a specific value. This can be done either on the **Credit Statement** main tab, or on the **Users** main tab if the MyQ Web interface.

On the **Credit Statement** tab, you first open the credit reset action, and subsequently select the users and groups whose credit is to be recharged. On the **Users** tab, you first select the users or the group, and then reset their credit.

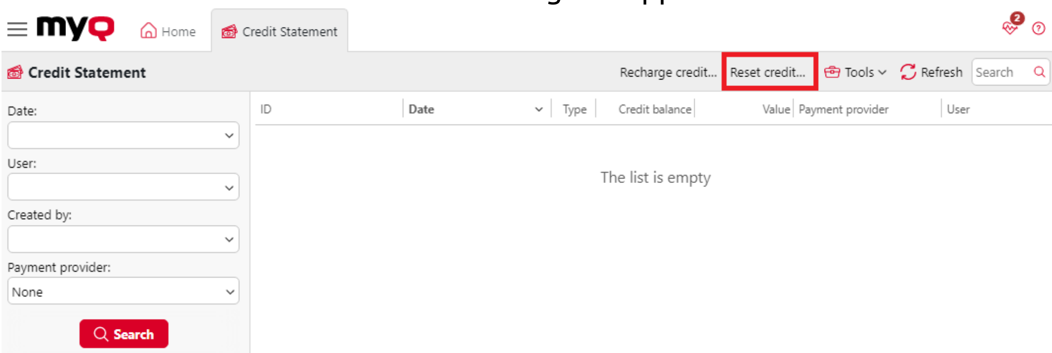
To authorize a user to reset credit on the **Credit Statement** tab, you need to provide them with the rights to **Recharge credit**. To authorize a user to reset credit on the **Users** tab, you need to provide them with the rights to **Recharge credit** and to **Manage Users**. The authorized user can reset the credit on their MyQ Web interface in the same way as the MyQ administrator.

16.10.1 Resetting Credit on the Credit Statement Tab

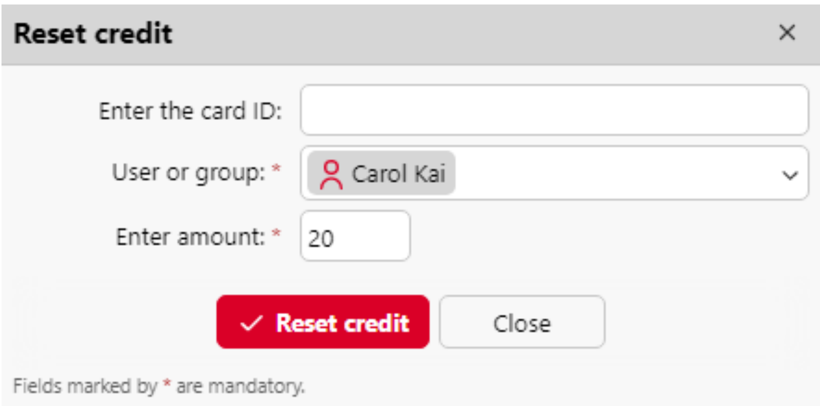
On the **Credit Statement** tab, you can overview the changes in the credit balance of MyQ users, and also reset credit to users and groups. To open the tab on the MyQ Web Interface, go to **MyQ, Credit Statement**.

To reset credit to users or groups:

1. Click **Reset credit**. The Reset credit dialog box appears on the tab.



2. In the dialog box, either **Enter the card ID** of a user, or select the **User or group** to reset the credit to, then **Enter amount** of the credit, and click **Reset credit**.

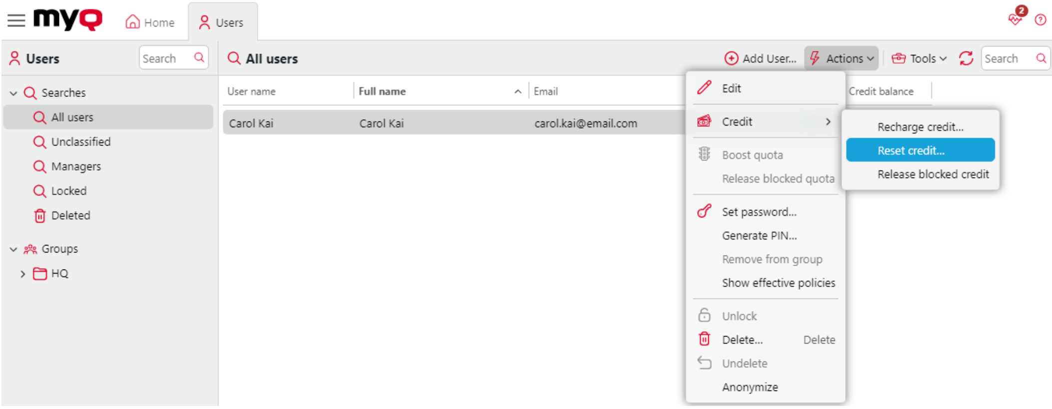


16.10.2 Resetting credit on the Users main tab

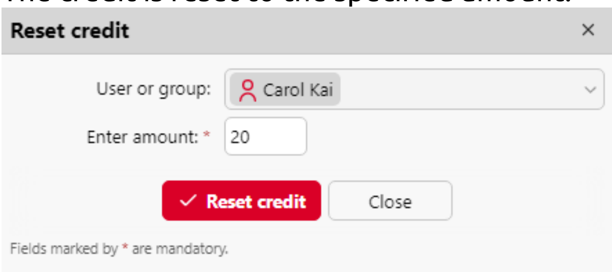
To open the **Users** main tab on the MyQ Web Interface, go to **MyQ, Users**.

To reset credit to a specific user:

1. Select the users, click **Actions**, hover over **Credit**, and then click **Reset credit** (or select the users, right click one of them, hover over **Credit**, and then click **Reset credit** on the shortcut menu.) The Reset credit dialog box opens.

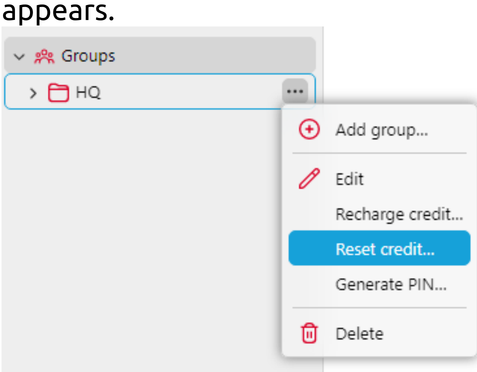


2. In the dialog box, **Enter amount** of the new credit, and then click **Reset credit**. The credit is reset to the specified amount.



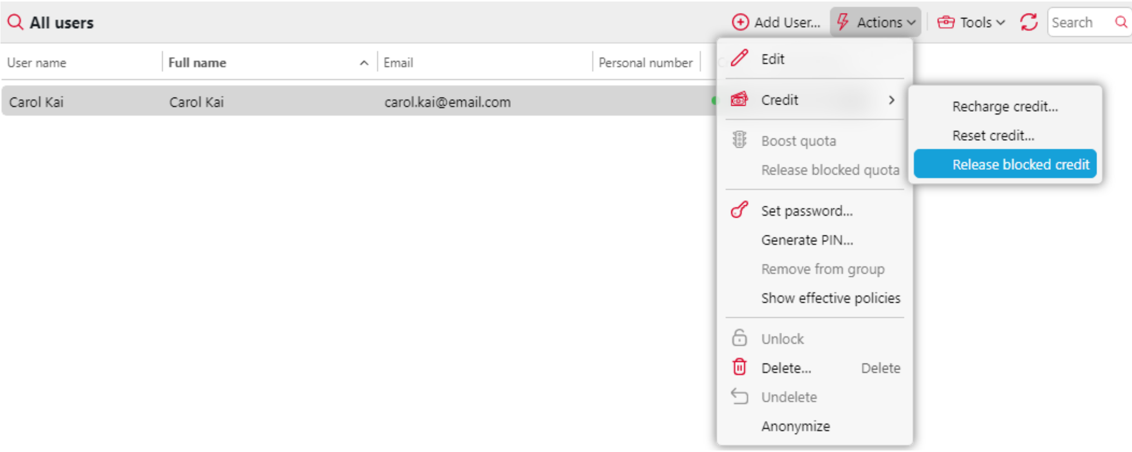
To reset credit to a group of users:

1. On the panel on the left side of the **Users** main tab, right-click the group, and then click **Reset credit** on the shortcut menu. The Reset credit dialog box appears.



2. In the dialog box, **Enter amount** of the new credit, and click **Reset credit**. The credit is reset to the specified amount.

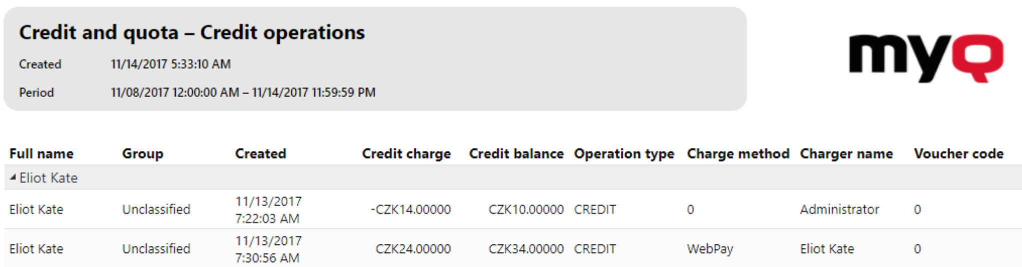
The administrator can also release blocked credit for a user by selecting the user, clicking **Actions**, hovering over **Credit**, and then clicking **Release blocked credit** (or by right-clicking the user, hovering over **Credit**, and selecting **Release blocked credit**).



16.11 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.



Credit and quota – Credit operations

Created 11/14/2017 5:33:10 AM

Period 11/08/2017 12:00:00 AM – 11/14/2017 11:59:59 PM

Full name	Group	Created	Credit charge	Credit balance	Operation type	Charge method	Charger name	Voucher code
Eliot Kate								
Eliot Kate	Unclassified	11/13/2017 7:22:03 AM	-CZK14.00000	CZK10.00000	CREDIT	0	Administrator	0
Eliot Kate	Unclassified	11/13/2017 7:30:56 AM	CZK24.00000	CZK34.00000	CREDIT	WebPay	Eliot Kate	0

17 Quota

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

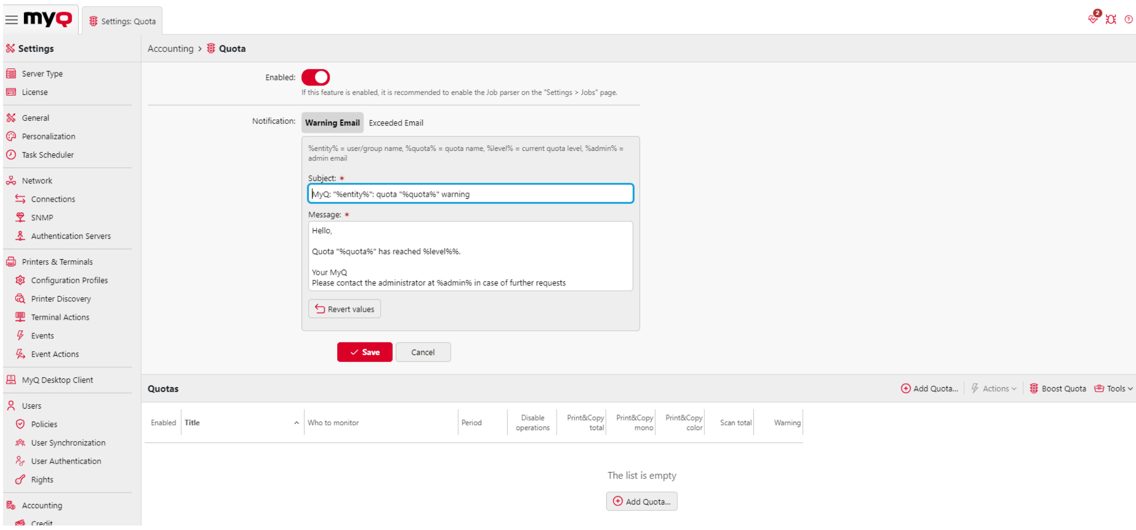
Quotas are active permanently until disabled and they reset after the specified interval. Users can check their quota status on their web user interface and in the MyQ mobile application. If a printing device is equipped with an embedded terminal, users can see the current percentage of their quota status 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.). For information about how to set the prices and how to activate the parser, see Price List and Jobs.

17.1 Activation and General Setup

You can enable the Quota feature by selecting the **Enabled** quota option at the top of the **Quota** settings tab (**MyQ, Settings, Quota**). Each quota can then be individually enabled or disabled on its properties panel.

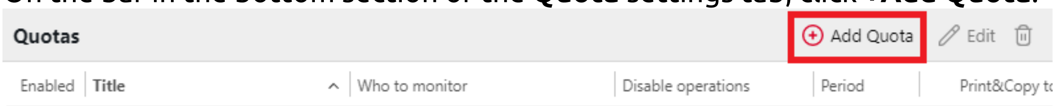
In the **Warning Email** tab you can type the subject and the body of the email that is sent after reaching the preset warning (e.g. 80% of the quota) and, on the **Exceeded Email** tab, the subject and the body of the email that is sent when the limit of a user or group is reached or exceeded.



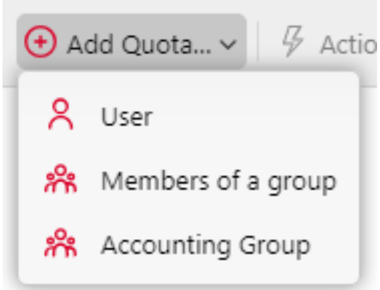
17.2 Creating Quotas

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. On the panel, enter the quota name, set its parameters, and then click **Save**.

The new quota is enabled and appears on the **Quota** overview list (**MyQ, Settings, Quota**).

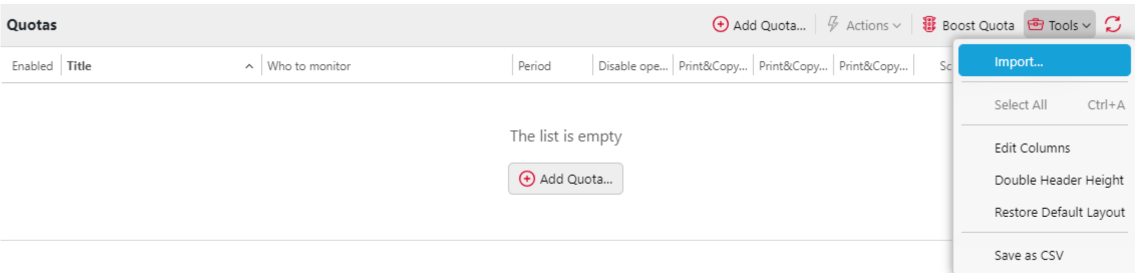
> A user can be assigned only one direct quota. This means you can create a quota specifically for an individual **User** and another for a broader category such as an **Accounting Group** or **Cost Center**. If the user belongs to an Accounting Group or Cost Center, they will inherit the shared quota 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.

17.2.1 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.

You can create several quotas at once by importing them from a CSV file. Click **Tools** and select **Import**, you can then select a CSV file to 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.

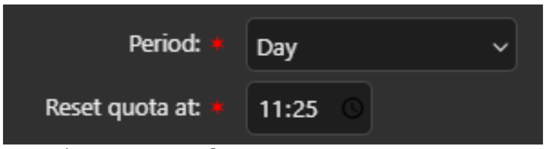
Column	Type	Required	Description
name	string	Yes	Name of quota

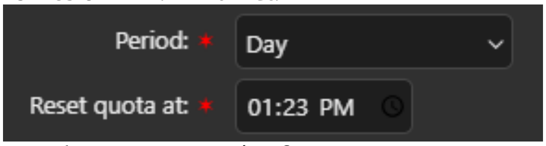
monitor	string • `user` • `group` • `members`	Yes	Who to monitor.
entity	string	Yes	User or Group When group used, full path must be specified. Example: `group level 1|target group`. Use same separator as for users import/export.
counter	Unique list of comma-separated values (at least one) from: • `cost` 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.

<table>
<tr>
<td>period start</td>
<td>One number, two numbers with comma or time of day. Exact format depends on Quota period type.</td>
<td>No</td>
<td>
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`.



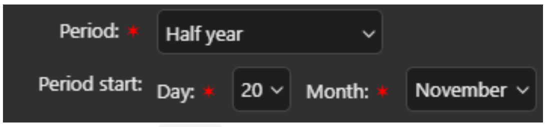
15 Web UI in HH:MM format.


16 Web UI in HH:MM am/pm format.
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



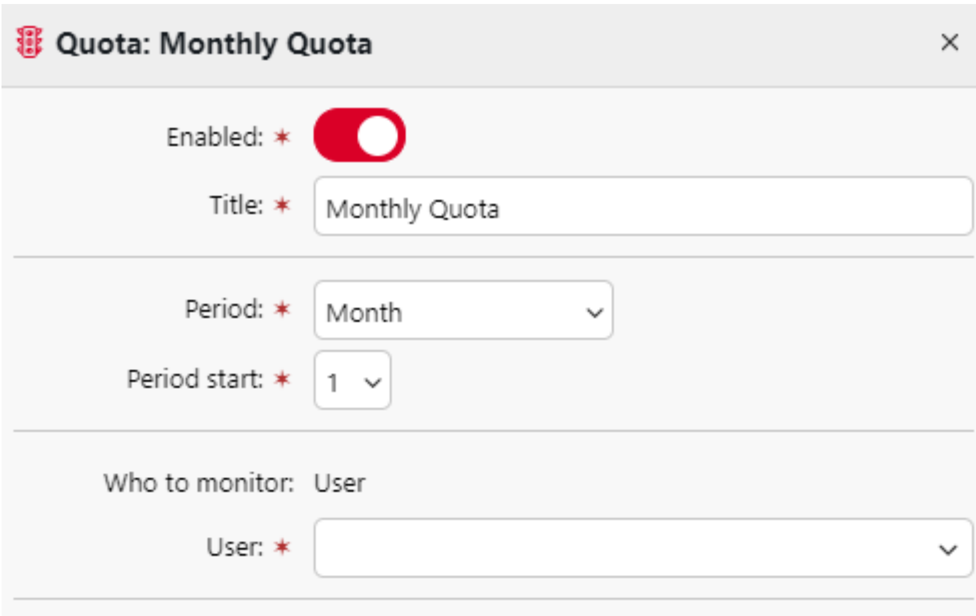
17 For example `20,11` is imported as 20th day of November.
Last X days: How many days from “now” will be counted into quota, 1 - 365, default is 30.
</td>
</tr>
</table>

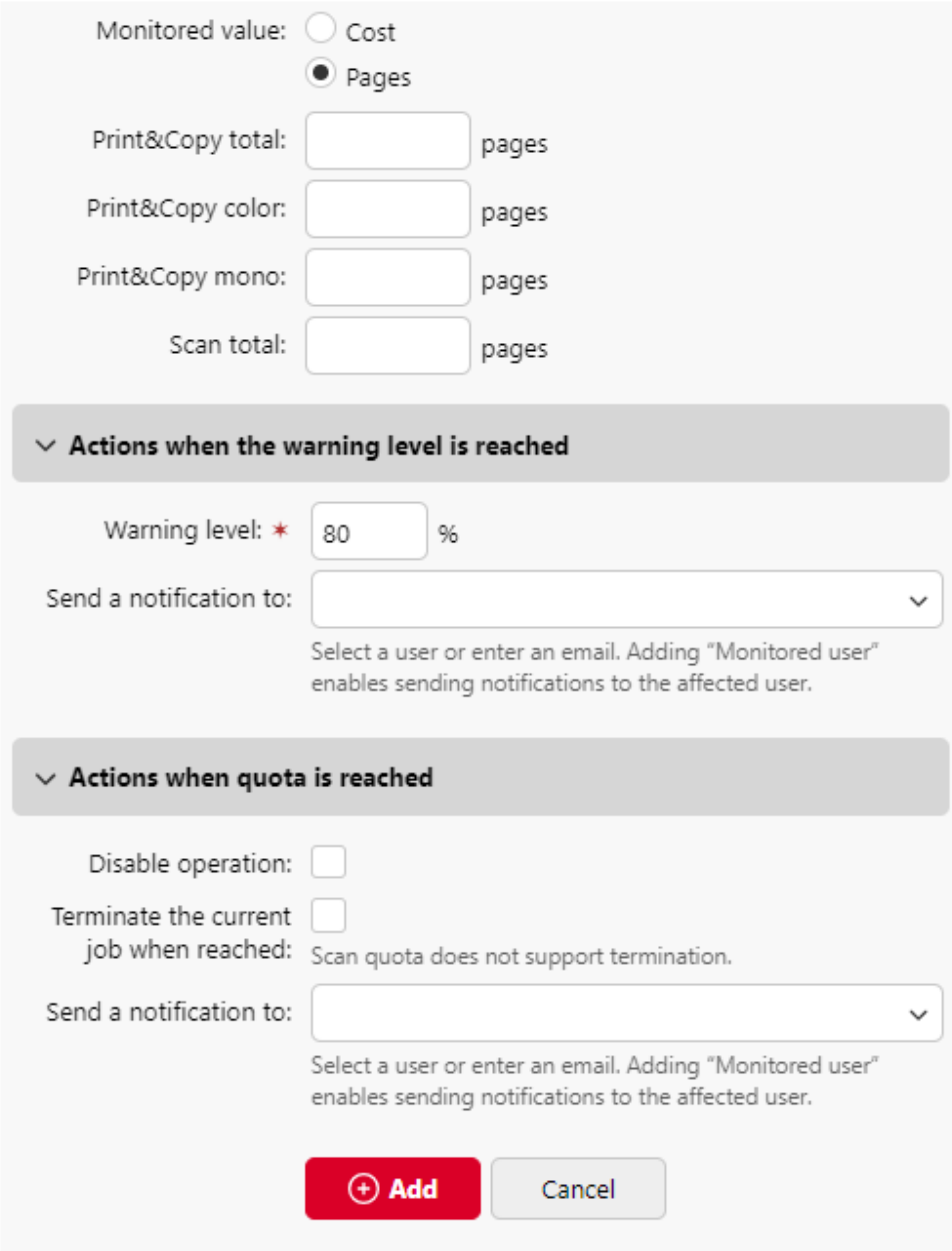
limit	List of comma-separated positive numbers (at least one).	Yes	If `counter` is type `cost`, a decimal value can be used to represent a currency amount. In other cases, `limit` represents pages. The list of values in `limit` corresponds to the values in `counter`. Examples: 1. Single value: `counter=cost` 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.

17.3 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:

Basic settings: enabling and naming 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**.

17.4 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.

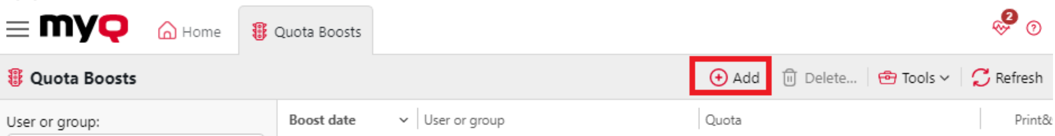
You can create Quota Boosts for the following quota types:

- User
- Accounting Group

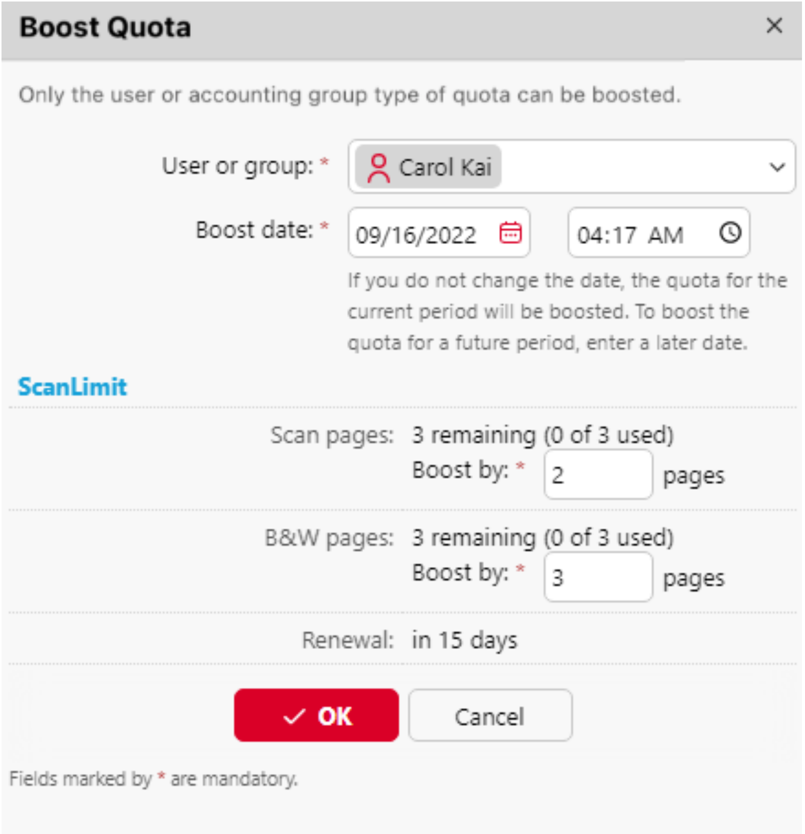
17.4.1 Boosting quotas on the Quota Boosts main tab

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).



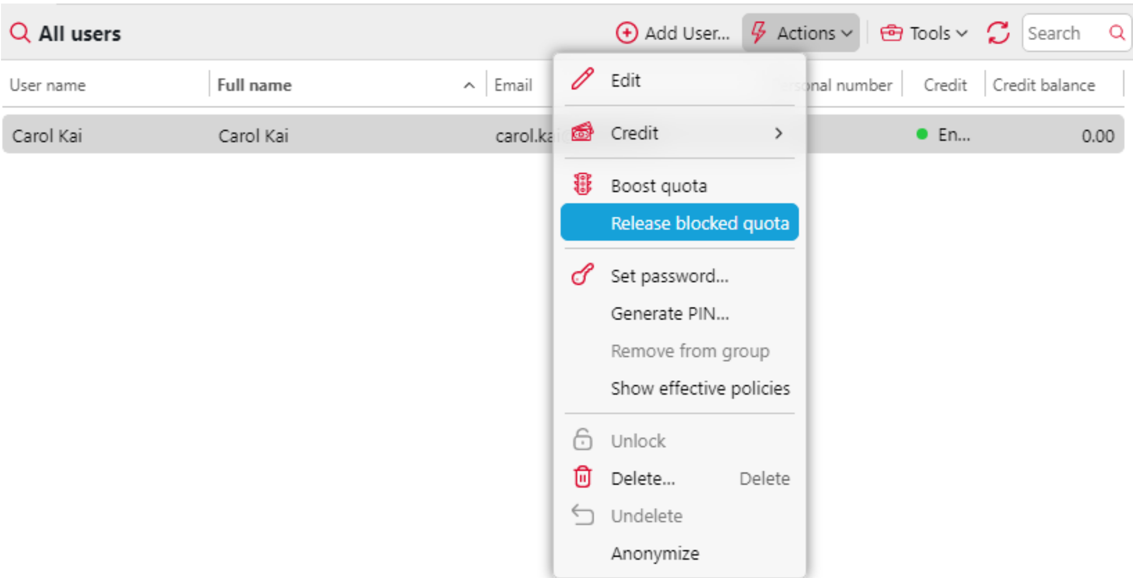
3. Enter the number of pages or the amount of money to the **Boost By** text box in the particular quotas sections (each quota has to be boosted separately), and then click **OK**.

17.4.2 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:

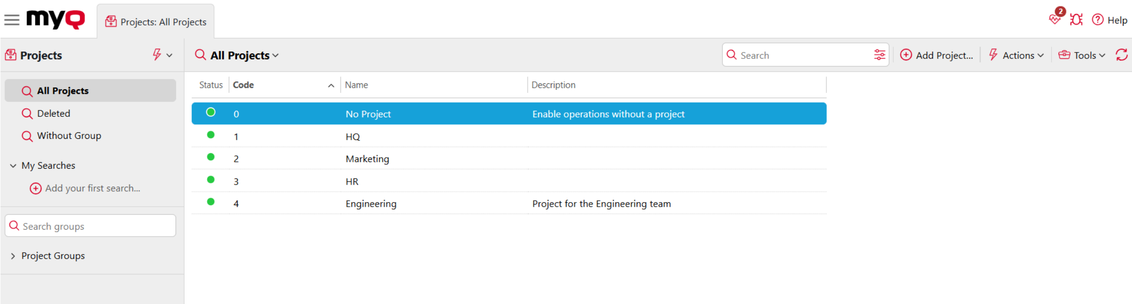
1. On the tab, select the user, click **Actions**, and then click **Boost quota** in the drop-down (or right-click the user, and then click **Boost quota** on the shortcut menu). The Boost quota dialog box appears with the user selected in the **User or group** drop-down.
2. Enter the number of pages 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**).


All users
Add User...
Actions
Tools
Search
User name
Full name
Email
rsonal number
Credit
Credit balance
Carol Kai
Carol Kai
carol.ka
En...
0.00
Edit
Credit
Boost quota
Release blocked quota
Set password...
Generate PIN...
Remove from group
Show effective policies
Unlock
Delete...
Delete
Undelete
Anonymize

18 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.

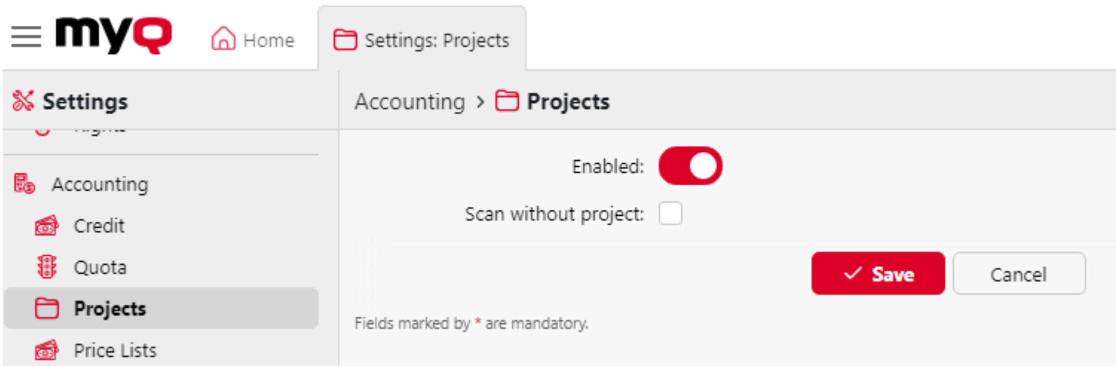


18.1 Projects Activation and Setup

On the **Projects** settings tab (**MyQ, Settings, Projects**), you can enable, or disable projects. Furthermore, you can change the global settings of the projects feature there.

Select the **Enabled** option to globally activate project accounting.

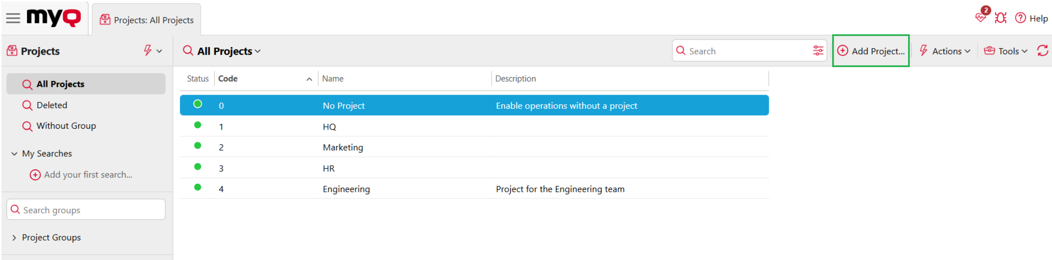
Scan without project: Users scan directly when this option is selected. They have to select a project when the option is not selected.



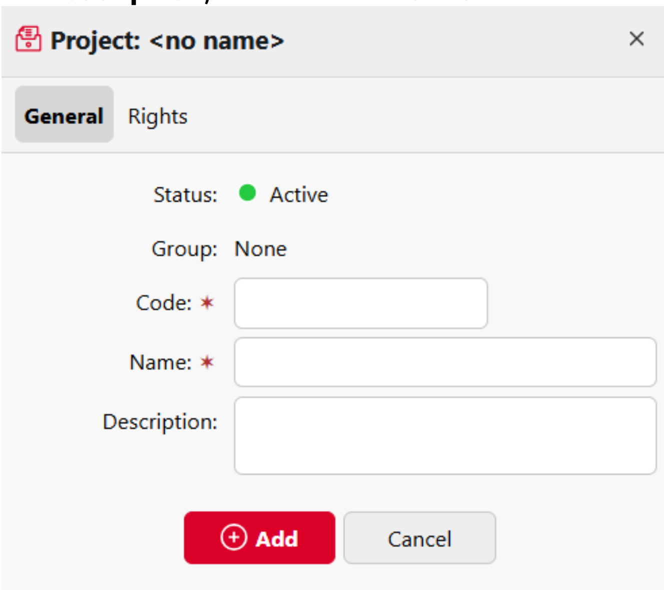
18.2 Creating Projects

To add new projects to MyQ, go to **MyQ, Projects** and:

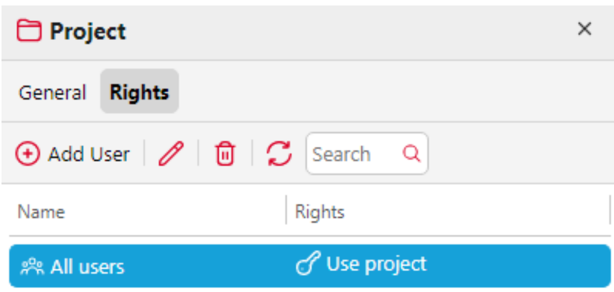
1. On the bar at the top of the **Projects** main tab, click **+Add project**. The new project properties panel opens on the right side of the screen.



2. On the **General** tab, enter a unique project **Code**, the project **Name**, optionally its **Description**, and then click **Save**.



3. 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. The user (or group of users) disappears from the **Rights** list.



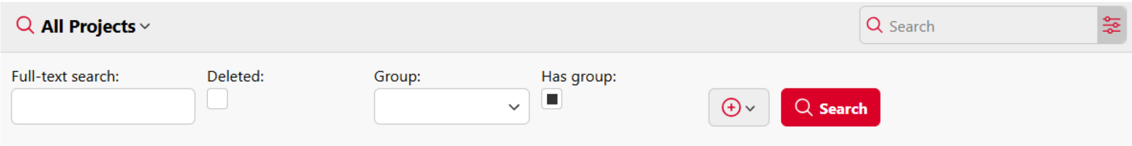
18.3 Project Management

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.

18.3.1 Searching Projects

You can use the search function to easily find particular projects:

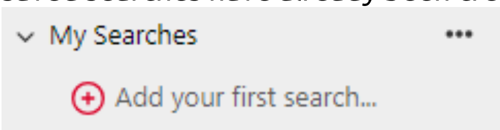
- **Full-text search** allows you to search a project's name or description.
- **Deleted** specifies whether or not deleted projects will be included.
- **Group** allows you to limit the search to projects in a particular group.
- **Has group** restricts the search to projects that have been added to any group.



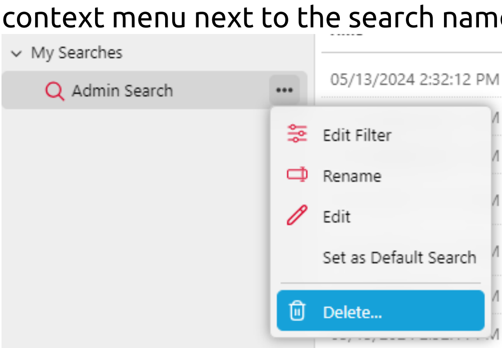
My Searches

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:

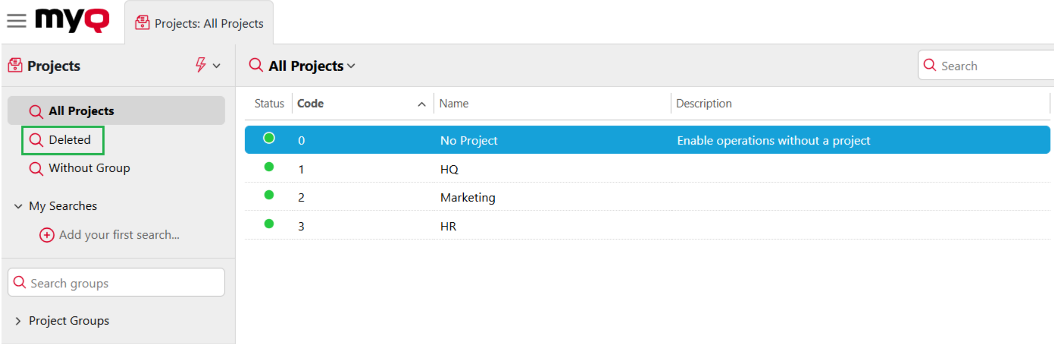


   - **Edit Filter:** displays the filter editor for the search.
   - **Rename:** allows the user to rename the search.
   - **Edit:** opens advanced properties in the right panel including sharing options.

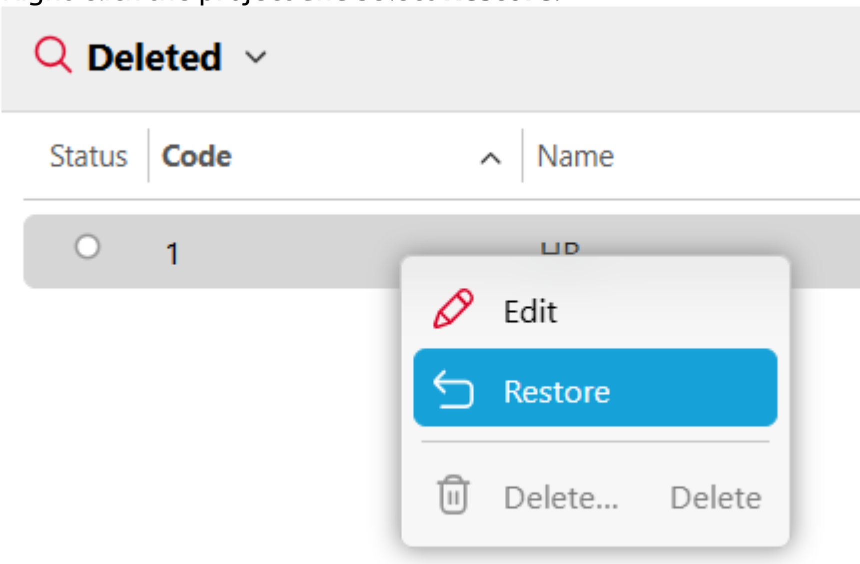
- **Set as Default Search:** sets the search as the default one.
- **Delete:** deletes the search.

18.3.2 Restoring deleted projects

1. Navigate to **Deleted** projects in the left-hand panel.



2. Right-click the project and select **Restore**.



18.3.3 Managing Project Groups

For bigger companies, it is easier to manage projects in groups on e.g. 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**.

18.4 Importing Projects from CSV Files

Another option of adding projects to MyQ is to import them from CSV files. This can be done manually and also as a scheduled task.

A sample CSV file called `Projects_example` is available in `ProgramData\MyQ\Data\Import`, this CSV can be populated with relevant information and imported.

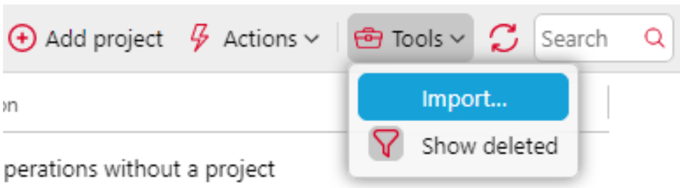
- The manual import is described in Manually importing projects.
- For information on how to set up the scheduled task, see Setting up the Project synchronization scheduled task.
- You can find the required syntax of the CSV file in Syntax of the projects' CSV file.

You can import projects with a hierarchy.

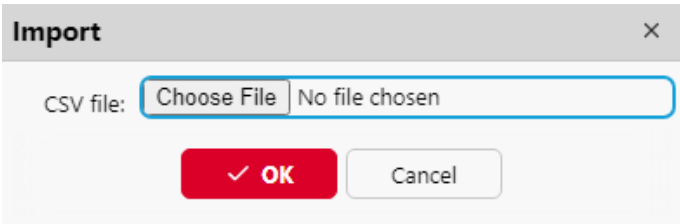
Within the CSV import, new projects are added and existing projects are updated. Projects already present in MyQ that are not listed in the CSV file are left untouched. Each project is recognized by the value of its code, and updated only if the CSV file contains a row with the same code.

18.4.1 Manually Importing Projects

On the bar at the top of the **Projects** main tab, click **Tools**, and select **Import**. The Import dialog box appears.



In the dialog box, 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.

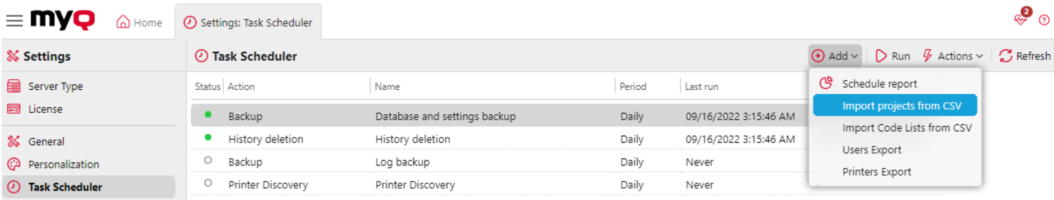


In addition, an information message appears at the top of the tab. By clicking log for details, you can display the import log.

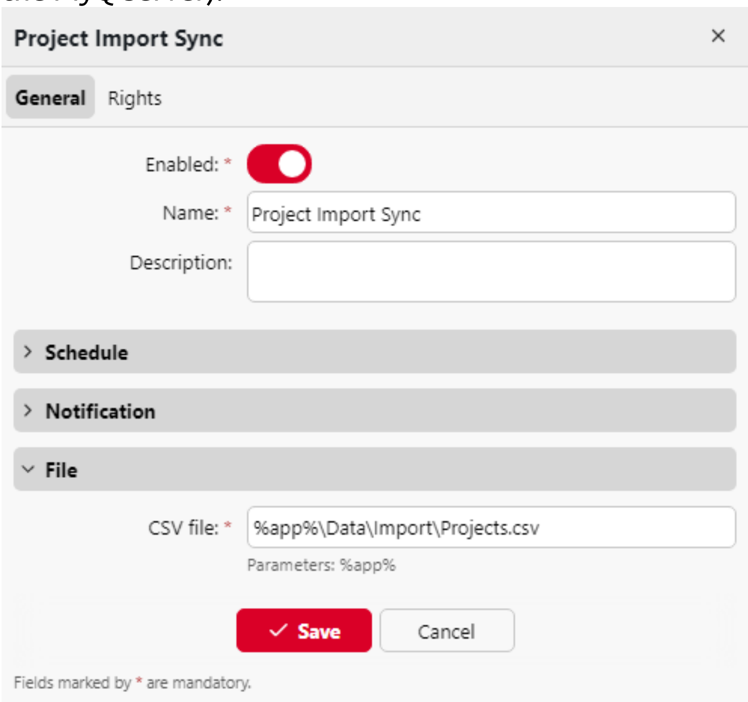
Any errors occurring during the import can be related to incorrect syntax or non-existing users or group of users listed in the CSV file.

18.4.2 Setting up the Project Synchronization Scheduled Task

1. On the **Task Scheduler** settings tab, 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, as described in Task Scheduler.
3. In the **File** section, add the path to the **CSV file** (the file should be stored on the MyQ server).



4. Click **Save**.

18.4.3 Syntax of the Projects' CSV File

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 (,).

active	code	name	groups	description	users
1	300	Project1	parent|child	Optional description	"All users"
0	400	Project 2			

18.5 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.

- How to assign projects in MyQ Desktop Client
- How to assign projects on the Jobs main tab

18.5.1 Assigning Projects in MyQ Desktop Client

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.

For information about MyQ Desktop Client, including installation, setup, and optional features of the application, see the *MyQ Desktop Client for Windows* or *macOS* manuals.

18.5.2 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**.

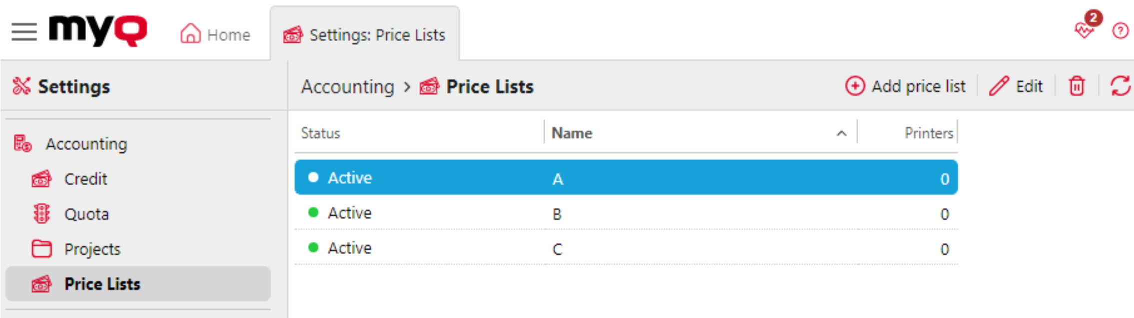
19 Price List

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**.

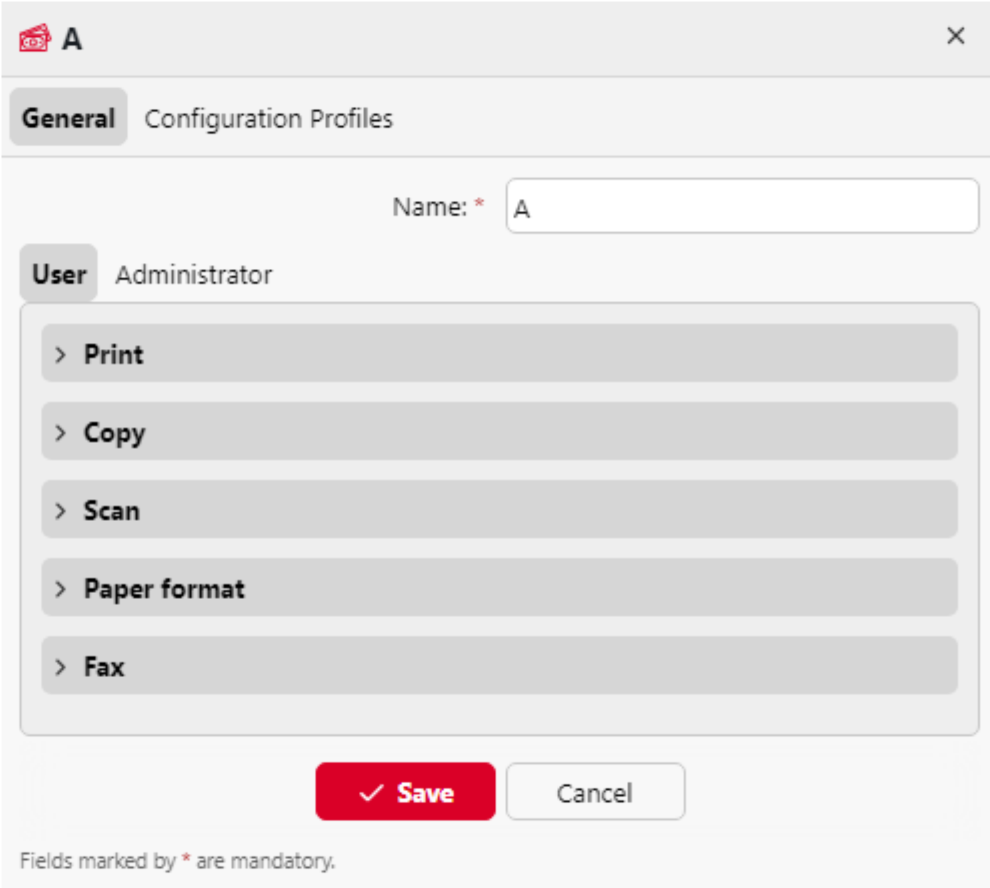


19.1 Adding Price Lists

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**.

19.2 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.



19.2.1 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.

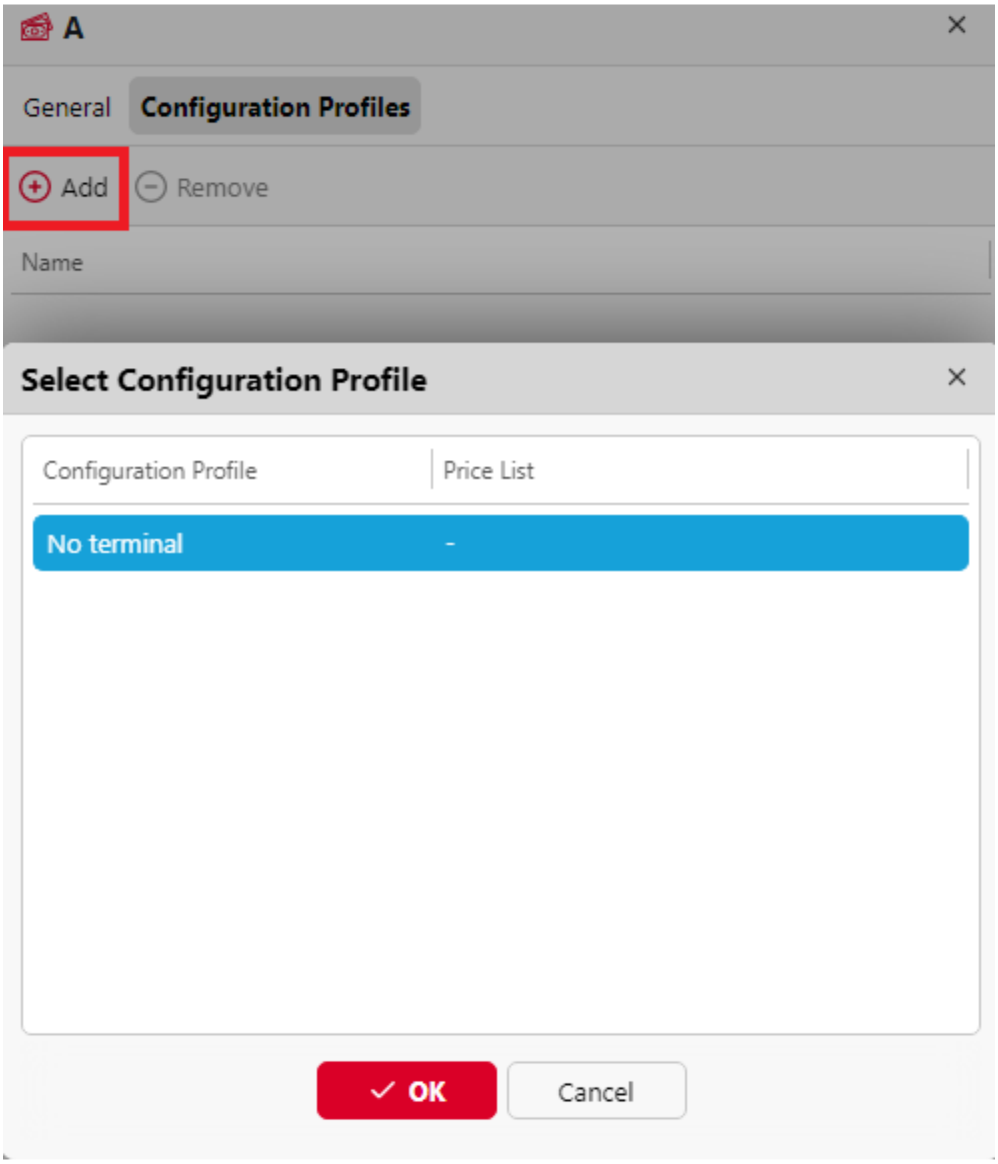
Some printing devices lack the counters necessary for obtaining information about some parameters, for example information about paper size. Those parameters are not counted in the final price of jobs that are carried out on these machines.

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.

19.2.2 Attaching Price Lists to Printing 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.

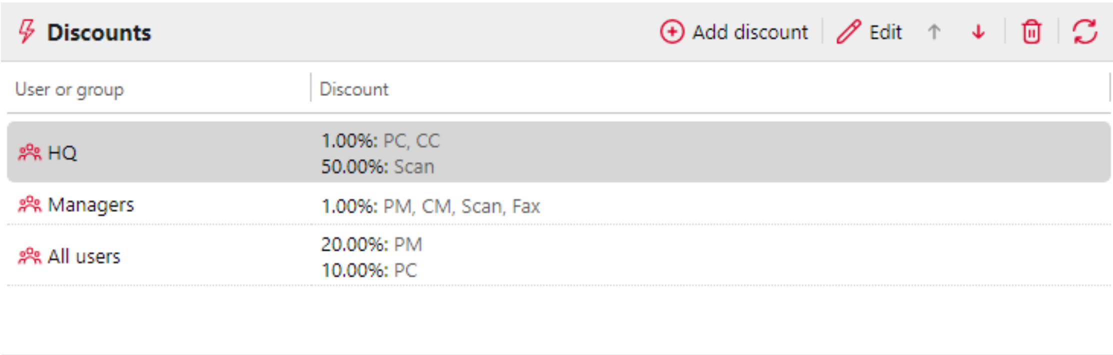
You cannot attach more than one price lists to a single configuration profile. If you add a price list to a configuration profile that already has a different price list attached to it, the old price list is replaced by the new one.

19.3 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.



19.3.1 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.

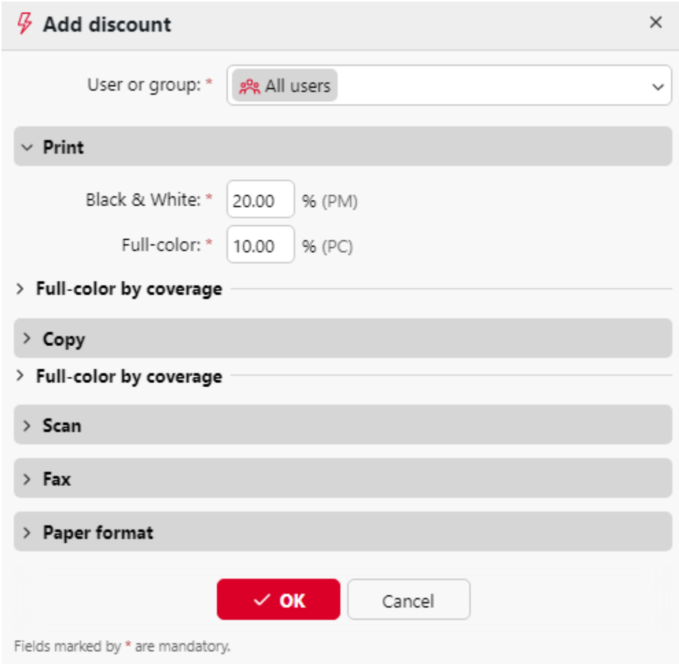
19.3.2 Editing a Discount

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.



19.3.3 Deleting a Discount

1. Select the discount.
2. Click the the trash can, or right-click and select **Delete**.

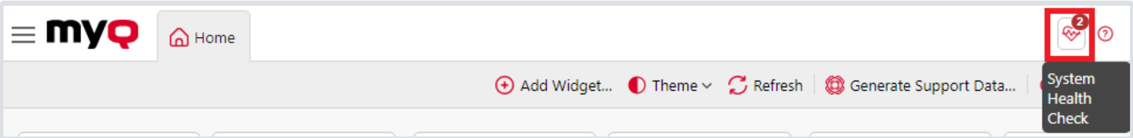
20 System Health Check

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.

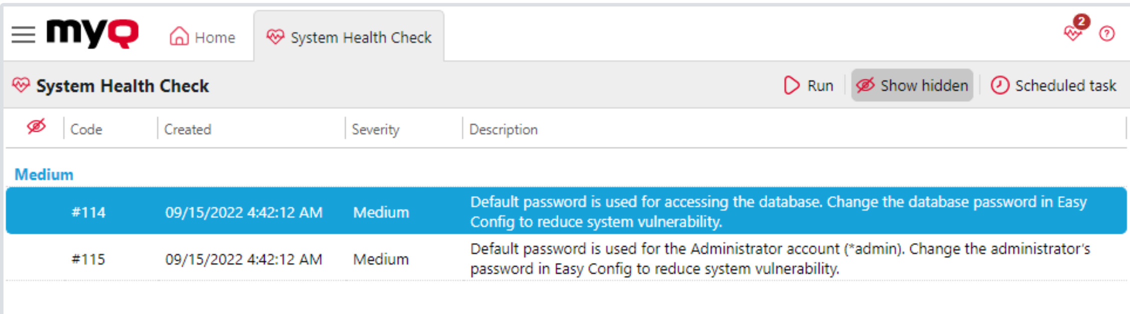
To access the system health check overview, log in as admin to MyQ and go to **MyQ**> **System Health Check** or click on the system health check button on the top-right side of the window.



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 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.

Error Code	Severity	Description	Troubleshooting Steps
102	High	Log database health issues	Check log database and clear outdated logs using scheduled tasks. Complete a database back-up and restore.
103	Medium	PIN length needs adjustment	Adjust PIN policies to enforce a higher minimum character count, learn more here.
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.
119	Medium	Connection secret keys expired/near expiry	Identify expiring keys. Generate new keys and update API configurations. Restart affected services.

Error Code	Severity	Description	Troubleshooting Steps
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.

21 Uninstalling MyQ

To uninstall MyQ:

1. Run **unins000.exe**. You can find this file in your MyQ program folder (The default folder is: *C:\Program Files\MyQ*). 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.

22 Available languages

Language	Abbreviation
Arabic (Saudi Arabia)	ar
Bosnian (Bosnia & Herzegovina)	bs
Bulgarian (Bulgaria)	bg
Chinese (China)	zh-CN
Chinese (Taiwan)	zh-TW
Croatian (Croatia)	hr
Czech (Czech Republic)	cs
Danish (Denmark)	da
Dutch (Belgium)	nl-BE
Dutch (The Netherlands)	nl
English (United Kingdom)	en
English (United States)	en-US
Estonian (Estonia)	et
Finnish (Finland)	fi
French (France)	fr
German (Germany)	de
Greek (Greece)	el
Hungarian (Hungary)	hu

Language	Abbreviation
Icelandic (Iceland)	is
Italian (Italy)	it
Japanese (Japan)	ja
Korean (South Korea)	ko
Latvian (Latvia)	lv
Lithuanian (Lithuania)	lt
Malay (Malaysia)	ms
Norwegian Nynorsk (Norway)	no
Polish (Poland)	pl
Portuguese (Brazil)	pt-BR
Portuguese (Portugal)	pt
Romanian (Romania)	ro
Russian (Russia)	ru
Serbian (Serbia)	sr
Slovak (Slovakia)	sk
Slovenian (Slovenia)	sl
Spanish (Spain)	es
Spanish (United States)	es-US
Swedish (Sweden)	sv

Language	Abbreviation
Thai (Thailand)	th
Turkish (Turkey)	tr
Ukrainian (Ukraine)	ua-UA
Vietnamese (Vietnam)	vn
Welsh (Wales)	cy

23 Business Contacts

MyQ® Manufacturer	**MyQ® spol. s r.o.** Harfa Business Center, Ceskomoravska 2532/19b, 190 00 Prague 9, Czech Republic ID no. 615 06 133 MyQ® spol. s r.o. is registered in the Commercial Register at the Municipal Court in Prague, file no. C 29842 (hereinafter as "MyQ®")
Business information	http://www.myq-solution.com info@myq-solution.com
Technical support	support@myq-solution.com
Notice	MANUFACTURER WILL NOT BE LIABLE FOR ANY LOSS OR DAMAGE CAUSED BY INSTALLATION OR OPERATION OF THE SOFTWARE AND HARDWARE PARTS OF THE MyQ® PRINTING SOLUTION. This manual, its content, design and structure are protected by copyright. Copying or other reproduction of all or part of this guide, or any copyrightable subject matter without the prior written consent of MyQ® is prohibited and can be punishable. MyQ® is not responsible for the content of this manual, particularly regarding its integrity, currency and commercial occupancy. All the material published here is exclusively of informative character. This manual is subject to change without notification. MyQ® is not obliged to make these changes periodically nor announce them, and is not responsible for currently published information to be compatible with the latest version of the MyQ® printing solution.
Trademarks	"MyQ®", including its logos, is a registered trademark of MyQ®. Any use of trademarks of MyQ® including its logos without the prior written consent of MyQ® Company is prohibited. The trademark and product name are protected by MyQ® and/or its local affiliates.