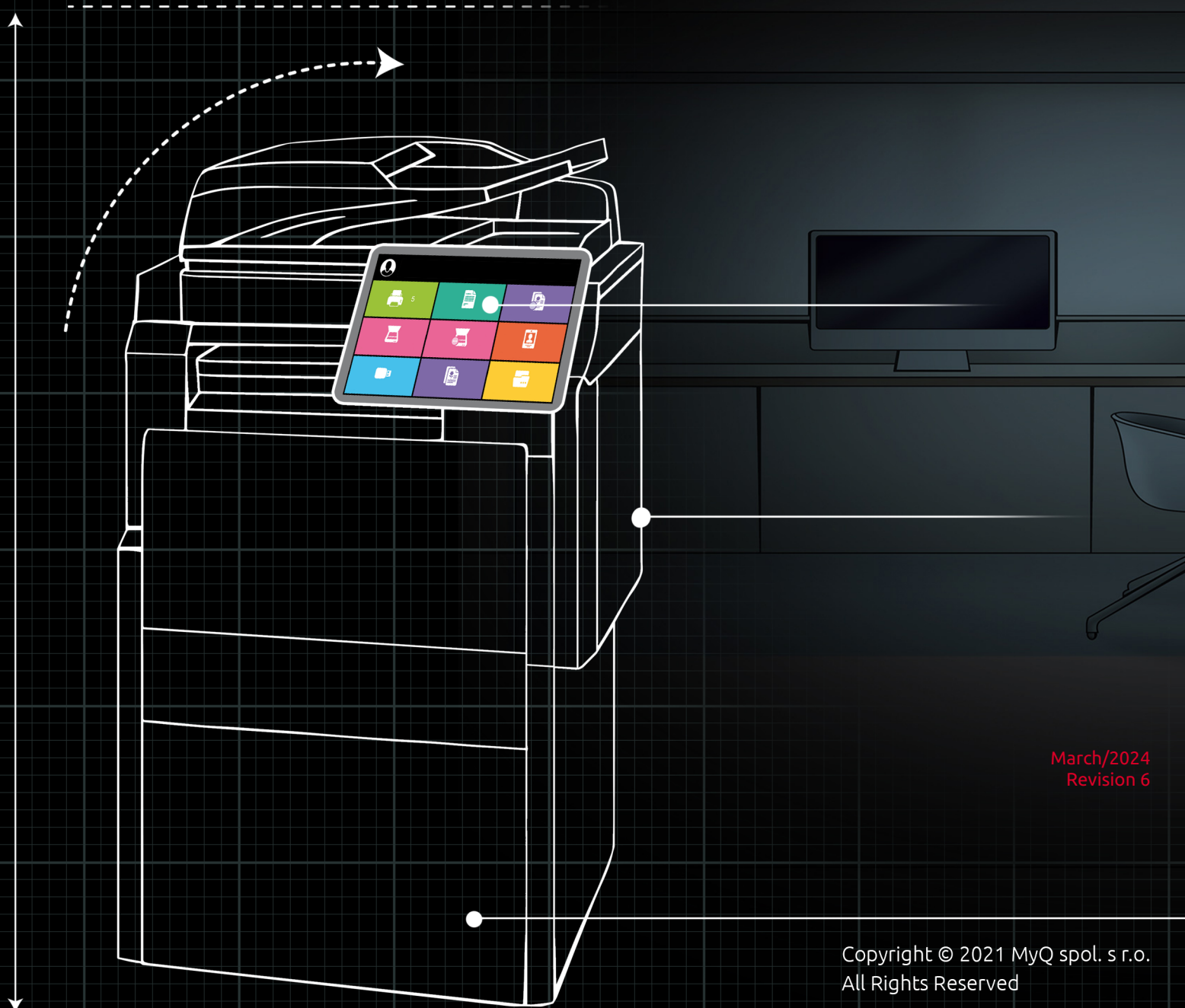


myq X

MyQ X Security Whitepaper



March/2024
Revision 6

Table of Contents

1	Security with MyQ	4
1.1	Your multifunctional printer is ground zero.....	4
1.2	Security is a three-way tug of war	4
1.3	Get the security balance right	4
1.4	With MyQ, the choice is yours	5
2	Securing the Privacy of MyQ users	6
2.1	GDPR compliance	6
2.2	MyQ X Secure Print.....	6
2.3	MyQ X Device Login/Logout.....	6
2.4	Document Security	7
2.5	Private Queues	7
2.6	Privacy Mode.....	7
3	Preventing Unauthorized Access.....	9
3.1	Secure Access to the MyQ X Server.....	9
3.2	Encrypting the MyQ Database, Log Database, and Jobs.....	9
3.3	Network Communication Security.....	9
3.4	Protocol Policies.....	10
4	Controlling the Printing Environment	11
4.1	Watermarking Printed Documents	11
4.2	Job Preview	11
4.3	Controlling Scanned Documents	11
4.4	Job Archiving	11
5	Compliance And Certifications.....	13
6	Security Wrap-up with MyQ	14

MyQ X Security Features Overview

MyQ X provides a range of features to enhance the security and privacy of end-users and of the company as well. These features start with secure printing at the MFD, customization of the user session, and have a continuous impact even after a document has been printed with the help of watermarks.

Here is a short summary of the MyQ X Security features:

- GDPR compliance
- Secure print
- User sessions with multiple authentication options including two-phase authentication
- Manual and automatic logout from user sessions
- End-to-end data encryption including data at rest encryption (database, jobs, logs)
- Fixed scan destination folders predefined by the MyQ administrator
- Private queues for deleting of print jobs immediately after release
- Privacy mode for anonymizing names of print job
- Restricted access to the setup options of the print server on the MyQ X Web Interface
- Customizable rights for access to different setup options
- Multiple levels of password complexity
- Audit log for changes of settings
- Support for [company certificate authority](#)
- Watermarking printed documents
- Job preview
- Controlling scanned documents via OCR and DMS systems
- Job archiving

1 Security with MyQ

Workflow security is a major concern for companies and individuals, regardless of whether documents are in physical or digital form. Misused or leaked data can result in substantial negative consequences from three major perspectives – for the individual employee, for the organization’s financial performance, and even for its competitive position in the marketplace.

1.1 Your multifunctional printer is ground zero

A multifunctional printer, with its always-on connection to company servers, has the central role in document distribution and reproduction – and overall data security. Done correctly, a print management software enhances your company’s ability to manage the new technological capabilities of its MFP, do this in a cost-effective way, and to enhance workflow security all the way from the individual workstation to printed documents as they pass outside of the company walls. Done incorrectly, you have extra financial costs, lose control over private and company data, and even face legal liabilities.

1.2 Security is a three-way tug of war

There is no single “one-size fits all” security setting. As each organization establishes its security and document privacy policies, there is a three-way struggle over how these settings can be formed. The three primary user groups and perspectives in this tug of war:

- End users/country legislation such as GDPR demanding a high level of individual data privacy.
- Administrator needing to secure the printing environment from external threats.
- Company wanting to control the printing environment to prevent its misuse.

1.3 Get the security balance right

Meeting the needs of the individual/legislation, the system administrator, and the company is a balancing act which has both legal and technical ramifications. While all three parties have a broad agreement over the primary security goals, each of these three perspectives brings its own particular set of problems and expectations.

Some privacy/security settings can be in direct opposition with one another. For example, if you select to anonymize print jobs (MyQ Job Privacy Mode) or to delete print jobs immediately after they are printed (MyQ Private Queues), you strengthen individual privacy but lose control over printing and increase the possibility of the printing environment being misused. On the other hand, if you decide to control printed jobs (MyQ Job Archiving) or scans (integration with OCR and DMS systems), user privacy might be compromised.

1.4 With MyQ, the choice is yours

This document discusses different aspects of workflow security within the printing environment and demonstrates how MyQ approaches a variety of security issues and threats throughout this process.

As the MyQ X system manages thousands of documents each day, we are aware of the critical importance of providing clients and users with the highest possible level of security. By using the best available data protection tools and by integrating security into every process, we can guarantee that the MyQ system fulfills the needs of companies and institutions with the highest possible security requirements.

At MyQ, we've developed a universal printing solution that incorporates best-in-class tools which give you the flexibility to create your own settings. The choice is yours to tailor settings to meet specific company needs, establish policies which can be simply enforced, and to have security and privacy settings in-line with the specific requirements of your country.

2 Securing the Privacy of MyQ users

Three basic measures are essential in every printing environment regardless of whether one is looking at security from the individual, administrator, or company perspective.

1. The secured print feature ensures that the printing end-user has full control over when and where their documents are printed.
2. Enclosed user sessions should include both user authentication and automatic logout.
3. Print files should be stored in a secured place on the MyQ X Print Server.

Beyond these basic security options, there are additional MyQ features which can further increase user privacy. To disable access to already printed documents, you can set up private queues where jobs are deleted immediately after they are released.

Once enabled, the MyQ privacy mode prevents everyone except for the printing user from knowing the name of the printed file.

2.1 GDPR compliance

MyQ X is compliant with GDPR and has implemented the necessary steps to make sure that all users' rights given by the regulation are secured in the MyQ X system. Three of the most important new features are the option to provide MyQ users with all their data, the option to anonymize user accounts, and a customizable message on users' MyQ Web Interface informing them about their rights.

2.2 MyQ X Secure Print

The importance of printer management has increased with the move away from small desktop printers to centralized high performance multifunctional printing devices.

Controlling access to documents as they come out of the printer is an essential and basic element in workflow security. In addition to security, restricting access to printed output is also part of managing office expenditures and project budgeting.

The MyQ Secure Print feature releases sent jobs only after the end-user reaches the multifunctional printer and authenticates themselves with an ID card, a PIN, or a username + password. This means that the printed copy is produced only under full physical control of the authorized person, preventing the accidental or malicious pickup of materials.

2.3 MyQ X Device Login/Logout

Requiring user authorization at the printing device enhances copying and scanning security in addition to enabling the release of individual print jobs.

One scenario which demonstrates the importance of this is when a user copies a sensitive document and the printing device runs out of paper or gets into error status.

In this case, some of the document is typically stored in the device's memory and can be released to anyone who refills the paper or resolves the device's issue, e.g. paper jam.

With MyQ Authentication activated, the user simply logs out of the device and the device's memory is automatically cleared.

Automatic logout from the printing device is another important security feature. Research shows that the human factor is often the weakest link in the security chain. Although users are instructed to always log out of the device after completing a project or in the event of an unexpected situation, they might not – and instead leave the device with an open session.

MyQ enables the administrator to trigger an automatic logout and set a time period after which the device is automatically locked.

In addition, MyQ enables two- level authentication as well as the choice of several authentication options such as an ID card and PIN or a combination of an ID card and password.

2.4 Document Security

All print jobs are stored at the MyQ X Server in a predefined folder and the MyQ administrator can set the period after which the files are automatically deleted. The MyQ administrator can [enable job encryption](#) by providing a custom certificate. Another option is to enable storage encryption on the operating system level.

Similar options are available for scan jobs. Further the MyQ administrator can limit where users can send documents.

2.5 Private Queues

By default, already released print jobs are stored on the print server for a period of time defined by the MyQ administrator. This way, users can reprint documents without the need to resend them to the server and the administrator can overview printed jobs.

Although this is generally useful, the prolonged access period can be a security threat for documents that are confidential or contain sensitive information. To protect these documents, the MyQ administrator can enable users or departments to use private queues, where print jobs are deleted immediately after they are released.

2.6 Privacy Mode

For companies needing a high level of personal data protection, MyQ can be switched to a special mode which does not save or display any personal data that would compromise the company's data protection policies.

In this mode, logged users can see only the names of their own jobs. The names of all other jobs are masked by ***. This rule is applied to all user roles, so that even system administrators cannot see names of the jobs from other users. Furthermore, this limits MyQ reporting to Printer and User Group related reports, disabling all Print Job and User-based reports.

3 Preventing Unauthorized Access

Administrators have the primary task of securing the print server, company data, and network communication against a range of external and internal threats. In addition, they have responsibility to implement and enforce the company's own security policies.

MyQ helps with this by providing extensive security options for the MyQ X Server, comprehensive network encryption, and clear protocol policies.

3.1 Secure Access to the MyQ X Server

To maximize print server security, restricting user access to the lowest necessary level is recommended. For this reason, access of common users to the MyQ X Web Interface is limited only to their profile, reports, and print jobs. Users' access rights can be extended according to their role and responsibilities in the MyQ system (user management, device management, credit recharge, etc.). The only accounts that have full access to the administration of MyQ are accounts with the system administrator role.

User login security to the MyQ Server can be increased by increasing the complexity level of passwords, PIN length, and by setting rules for locking an account in cases of repeated use of wrong credentials.

To detect misuse of the extended access rights, MyQ tracks all changes on the admin level and saves them to MyQ Audit Log together with information about when and by whom the MyQ settings were changed. This is particularly useful when users report problems with PIN or ID card access, or when the system stops working due to changes in the MyQ configuration.

3.2 Encrypting the MyQ Database, Log Database, and Jobs

To prevent unauthorized access to the company's data, the administrator can encrypt the data within the MyQ database. The data encryption feature was implemented in Firebird 3.0 and has been available in MyQ since MyQ X 7.6.

Print Jobs encryption, as well as Log Database encryption, can be turned on and off in MyQ Easy Config in the Security tab. Scan Jobs are encrypted by default. This feature was implemented in MyQ X 10.1.

3.3 Network Communication Security

MyQ security enables the encryption of all user authentication data and the content of print files on the network. This includes all TCP/IP communication between individual components of MyQ as well as all network connections to other services. Applications can be encrypted using either the MyQ default self-signed certificate or the customer's CA signed certificate, which is meant to prevent man-in-the-middle attacks.

3.4 Protocol Policies

MyQ X supports and uses the most recent protocols to support user security. Vulnerable protocols and ciphers are disabled by default.

The following communication protocols can be encrypted with MyQ:

- Communication among MyQ Servers — HTTPS
- Communication between the MyQ Server and a MyQ Terminal — HTTPS
- Communication between the MyQ client application and the MyQ Server — HTTPS
- Communication between the MyQ Server and AD/eDirectory/OpenLDAP — LDAPS
- Communication between the MyQ Server and a mail server — SMTPS
- Print from a workstation to the MyQ Server — LPR over SSL
- Print from the MyQ Server to a printing device — IPPS or MPPS (MyQ Print Protocol)
- Print from users computer to server can also be done using IPPS instead of the standard LPR.

See the following pages for detailed information on network usage:

- [MyQ X Print Server](#)
- [MyQ X Central Server](#)

4 Controlling the Printing Environment

With MyQ X, system administrators have the ability to directly monitor and enforce company workflow security policies. Optional MyQ X features enable control of the printing environment and more detailed information about individual activities with printed and scanned documents. These features minimize the risk of individuals misusing the company's printing environment and assist in the uncovering and tracking of unapproved activities. MyQ features enable the administrator or external systems to control print jobs and scan jobs. With selected models of printing devices, it is also possible to control copy jobs as well.

4.1 Watermarking Printed Documents

After a job is printed, it is impossible for a company to guarantee that it will not fall into wrong hands. However, MyQ can help uncover a leaked document and identify the user responsible for printing it. By applying variable PDL macros, MyQ enables administrators to add an overlay watermark which can identify the document as confidential, add the print date, and/or include the name of the person printing the document. These macros can be applied to every page of a printed document or only to selected pages.

4.2 Job Preview

To enable the administrator to control printing and subsequently prevent the release of unauthorized print jobs, MyQ utilizes a job preview engine. In this way, the administrator can preview print jobs that have been sent to MyQ in the three most common page description languages: PCL 5, PCL 6, and Postscript.

4.3 Controlling Scanned Documents

The MyQ administrator can restrict scanning to predefined folders and use an integrated OCR or DMS system to provide notifications and restrictions based on the scanned documents' content. By incorporating the best available tools to analyze documents, you can make sure that your company's scanning policy is properly implemented.

4.4 Job Archiving

The Job Archiving feature enables the administrator to keep track of what has been printed and scanned.

When it is enabled, MyQ stores all the documents in a special folder together with their XML metadata files. The data can then be used as a source for the detailed auditing of a document flow. The XML file contains the following information:

- Job's image data filename
- Type of job (print, copy, scan)
- Time stamp
- Username & user ID

- MyQ X Server's name & MyQ Server's version
- Printing device's model, network address (IP or hostname), serial number, MAC address
- Job parameters
- Project (if Project accounting is activated)

Deleting jobs from the MyQ X Server (automatically or manually) has no effect on files stored within the Job Archiving feature.

5 Compliance And Certifications

MyQ X is compliant with **ISO 27001:2017** — a well-known standard for information security management systems.

MyQ X is compliant with **GDPR** — a regulation for data protection and privacy for users.

MyQ X is built using the **Secure Development Life Cycle (SDLC)**. We think deeply about security and privacy at every step of the development lifecycle. We constantly monitor the state of the art in security. We use industry standards for secure communication, authentication and authorization, such as TLS or token-based authentication.

We apply security principles such as Least Privileges Principal or Zero Trust Architecture during design. We regularly train our employees on **OWASP Top 10** most critical security risks.

We perform **Static Application Security Testing (SAST)** and **secure code reviews**. We publish **Software Bill of Materials (SBOM)** for our products and automatically check the SBOM against vulnerability databases such as **CWE**.

All of our binaries are **signed with a code signing certificate**. We publish **hashes for each release** to ensure the integrity of installation packages.

MyQ X releases are automatically **penetration tested** with **Qualys**.




6 Security Wrap-up with MyQ

Multifunctional printers are ground zero when it comes to workflow security in the modern organization. MyQ X, as the print management solution, is focused on enhancing the security and privacy of data in a company network.

MyQ X features get all three competing demands – legislation protecting the privacy of the individual, the system administrator's task to protect the network from external attacks, and the company's management need to reduce costs and protect commercial secrets – all on the same page.

The core security features in MyQ such as encryption, user authentication, and session logout are just the beginning. MyQ also includes a wide range of policy options for giving companies greater control over their printing environment and workflow. The variety of security and privacy needs within each company demonstrates the importance of a print management solution which can be easily fine-tuned. With MyQ, you have a secure choice.

 Please note that MyQ is dedicated to increasing security for our customers on an ongoing basis.