MyQ Security Whitepaper

REVISION 1

August 2018

Table Of Content

1. Overview of MyQ security features **1**

2. Security with MyQ **2**

2.1. Your multifunctional printer is ground zero 2

2.2. Security is a three-way tug of war 2

2.3. Get the security balance right 2

2.4. With MyQ, the choice is yours 3

3. Securing privacy of MyQ users **4**

3.1. Main security addition with MyQ 7.1 4

3.2. MyQ Secure Print 4

3.3. MyQ device login/logout 5

3.4. Document security 5

3.5. Private queues 6

3.6. Privacy mode 6

4. Preventing unauthorized access **7**

4.1. Secured access to the MyQ Server 7

4.2. Network communication security 7

4.3. Protocol policies 7

4.4. MyQ Server port requirements 8

5. Controlling the printing environment **11**

5.1. Watermarking printed documents 11

5.2. Job preview 11

5.3. Controlling scanned documents 11

5.4. Job archiving 12

6. **Security wrap-up with MyQ** **13**

7. **Business contact** **14**

1. Overview of MyQ security features

MyQ provides a range of features to enhance the security and privacy of end users and also that of the company. These features start with secure printing at the MFD, customization of the user session, and continue to have an impact even after a document has been printed with a watermark.

Here is a short summary of the MyQ security features:

- GDPR compliance
- Secure print
- User sessions with multiple authentication options [including two-level authentication]
- Manual and automatic logout from user sessions
- Secured folder for storing print jobs
- Fixed scan destination folders predefined by the MyQ administrator
- Private queues for deleting of print jobs immediately after release
- Privacy mode for anonymizing print jobs
- Restricted access to the setup options of the print server on the MyQ Web Interface
- Customizable rights for access to different setup options
- Multiple levels of password complexity
- Audit log for changes on the MyQ Print Server
- Self-signed and CA signed certificates
- Enforcing secured communication + Protocols for the secured communication
- Watermarking printed documents
- Job preview
- Controlling scanned documents via OCR and DMS systems
- Job archiving

2. 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.

2.1. 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.

2.2. 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.

2.3. 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 another. For example, if you select 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.

2.4. 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 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.

3. Securing 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 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.

3.1. Main security addition with MyQ 7.1

GDPR compliance - MyQ 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 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 the customizable message on users' MyQ Web Interface informing users about their rights.

3.2. MyQ 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 corridor multifunctional printer and has been authorized by 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.

3.3. MyQ 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 and enables the choice of several authentication options such as an ID card and PIN or a combination of an ID card and password.

3.4. Document security

All print files are stored at the MyQ Server in a predefined folder and the MyQ administrator can set the period after which the files are automatically deleted. By securing this folder, the administrator minimizes the risk of unauthorized access to the print data.

NOTICE: We recommend enabling OS level HDD encryption of the print folder.

INFO: The MyQ administrator can secure scanned files similar as with print files. A fixed destination can be set for every user, so that they can send documents only to approved destinations and restricts their ability to send sensitive data to any email address or shared folder.

3.5. 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.

3.6. 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.

4. 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 Server, comprehensive network encryption, and clear protocol policies.

4.1. Secured access to the MyQ 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 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 the case 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 who and when the MyQ settings were changed. This is particularly useful when users report problems with PIN or card access, or when the system stops working due to changes in MyQ configuration.

4.2. 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.

4.3. Protocol policies

MyQ 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 (Easy Job Manager) 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 (requires the Easy Job Manager) — LPR over SSL
- Print from the MyQ Server to a printing device — IPPS or MPPS (MyQ Print Protocol)

4.4. MyQ Server port requirements

The following table lists the receiving ports and protocols required for the operation of MyQ Server.

Receiving port	Sending application /device	Receiving application /device	Protocol	FW rule direction on MyQ Server	Description
21	Printer	MyQ Server	TCP	Inbound	FTP for opening a connection
49152-65535	Printer	MyQ Server	TCP	Inbound	FTP for actual file copy
25	Printer	MyQ Server	TCP	Inbound	Used by SMTP protocol to deliver scanned files from printer to MyQ
25/465/587	MyQ Server	SMTP Server	TCP	Outbound	Used by SMTP protocol for sending outgoing emails from MyQ. Port depends on SMTP server
80	MyQ Server	License activation server	TCP	Outbound	License activation server. IP address of the MyQ license server is 217.11.225.212 (license.myq.cz), running on standard http port 80
110	MyQ Server	POP3 server	TCP	Outbound	POP3
143	MyQ Server	IMAP server	TCP	Outbound	IMAP
161	MyQ Server	Printer	UDP	Outbound	Used by SNMP protocol for communication with printing devices. Answer from printer is returned on same dynamic port
389	MyQ Server	LDAP Server	TCP	Outbound	LDAP Server
443	MyQ Server	Printer	TCP	Outbound	Used by IPPS protocol for print job transmission from MyQ to printing devices

Receiving port	Sending application /device	Receiving application /device	Protocol	FW rule direction on MyQ Server	Description
515	EJM/User PC	MyQ Server	TCP	Inbound	Port used by LPR to accept print jobs
515	EJM/User PC	Printer	TCP		Used by LPR protocol to send a print job to the printer
631	MyQ Server	Printer	TCP	Inbound	Used by IPP protocol Mobile print via IPP. Kyocera Mobile Print (KMP)
631	MyQ Server	Printer	TCP	Outbound	Used by IPP protocol for print job transmission from MyQ to printing devices
636	MyQ Server	LDAP Server	TCP	Outbound	LDAPS Server
717	Mobile application	MyQ Server	TCP	Inbound	Mobile print via IPPS
993	MyQ Server	IMAPS Server		Outbound	IMPAS
3050	MyQ Master Server	MyQ Site Server	TCP	Inbound	Used by protocol for communication with Firebird database server and between master and site servers (replications)
8080	Various	MyQ Server	TCP	Inbound	Used by HTTP protocol for accessing MyQ web interface. Communication with Embedded Terminals, job roaming, REST API, Master-Site communication
8081-8089	Embedded Terminal	MyQ Server	TCP	Inbound	Port open after adding a terminal package
8090	Various	MyQ Server	TCP	Inbound	Same functions as the 8080 port except that MyQ runs in encrypted mode secured by SSL certificate on this port
9090	MyQ Server	Embedded Terminal	TCP	Outbound	Necessary for remote setup of Kyocera Embedded Terminals
9091	MyQ Server	Embedded Terminal	TCP	Outbound	Necessary for remote setup of Kyocera Embedded Terminals
9093	Terminal Lite	Kyocera Provider	TCP	Inbound	Needed for features of Kyocera provider - Authentication/Authorization
9094	Kyocera Provider	Terminal Lite	TCP	Outbound	Needed for features of Kyocera provider - Driver access, Mobile access (Kyocera mobile print app), port 9094 used for access to printing devices and cannot be changed!
9095	Kyocera Provider	Terminal Lite	TCP	Outbound	Needed for features of Kyocera provider - Spooler service

Receiving port	Sending application /device	Receiving application /device	Protocol	FW rule direction on MyQ Server	Description
9097	Kyocera Provider	Terminal Lite	TCP	Outbound	Needed for features of Kyocera provider - Log information event
9098	Kyocera Provider	Terminal Lite	TCP	Outbound	Needed for features of Kyocera provider - Job status event
9099	Kyocera Provider	MyQ Server	TCP		Needed for features of Kyocera provider - Thrift access. Only local communication
9100	MyQ Server	Printer	TCP	Outbound	Used by Raw protocol for print job transmission from MyQ to printing devices
9101	MyQ Server	Kyocera Provider	TCP	Outbound	Needed for features of Kyocera provider - User Session service
10010	User PC	Embedded Terminal	TCP		Port for direct print. The job is automatically printed after it is received by the printing device
10011	User PC	Embedded Terminal	TCP		Port for secured hold print. The job is spooled by the printer and waits there till the user logs in and prints it. It is not possible to print this job on other than this particular printing device
10012	User PC	Embedded Terminal	TCP		Port for Device Spool follow me. The job is spooled by the printing device. Once the user logs on any of the devices connected to the same subnet, information about this job is provided and the job is displayed in the list of the available jobs and can be printed
10013	User PC	Embedded Terminal	TCP		Port for Device Spool delegated print. Works same as the Device Spool follow me, except that the job can be printed by delegates of the sending user
10040	MyQ Server	Embedded Terminal	TCP	Outbound	MyQ Printing Protocol (Secured) - MPP (S)
11108	Embedded Terminal	MyQ Server	UDP	Inbound	Used for communication with terminals
11108	Terminal Manager	Embedded Terminal	TCP	Outbound	Communication between Terminal Manager and Terminals
11112	MyQ Server	Smart job manager	UDP/TCP	Inbound	Smart Job Manager and Smart Print Service communication with MyQ
11112	MyQ Server	Smart job manager	UDP/TCP	Outbound	MyQ sending data to Smart job manager

5. Controlling the printing environment

With MyQ, system administrators have the ability to directly monitor and enforce company workflow security policies. Optional MyQ features enable the 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.

5.1. 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 includes 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.

5.2. Job preview

To enable the administrator to control printing and subsequently prevent the release of unauthorized print jobs, MyQ can be integrated with a third-party job preview software. 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.

5.3. 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 content of the scanned documents. By incorporating the best available tools to analyze documents, you can make sure that your company's scanning policy is properly implemented.

5.4. 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. These 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 the job (print, copy, scan)
- Time stamp
- Username & user ID
- MyQ Server's name & MyQ Server's version
- Printing device's model, network address (IP or hostname), serial number MAC address
- Parameters of the job
- Project (if Project accounting is activated)

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

6. Security wrap-up with MyQ

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

MyQ features get all three competing demands – legislation protecting the privacy of the individual, the system administrator's task to protecting the network from external attack, and company 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 start. MyQ also includes a wide range of policy options for giving companies greater control over their printing environment and the workflow. The variable security and privacy needs within each company demonstrate the importance of a print management solution which can be easily fine-tuned. With MyQ, you have a secure choice.

NOTICE: Please note that MyQ is dedicated to increasing security for our customers on an ongoing basis. Our development roadmap includes several new features intended to enhance data protection.

7. Business contact

MyQ® Manufacturer	**MyQ® spol. s r.o.** Harfa Office Park, Ceskomoravska 2420/15, 190 93 Prague 9, Czech Republic MyQ® Company is registered in the Companies register at the Municipal Court in Prague, division C, no. 29842
Business information	www.myq-solution.com info@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® Company is prohibited and can be punishable. MyQ® is not responsible for information 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® Company 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 registered trademark of MyQ® company. Microsoft Windows, Windows NT and Windows Server are registered trademarks of Microsoft Corporation. All other brand and product names might be registered trademarks or trademarks of their respective companies. Any use of trademarks of MyQ® including its logos without the prior written consent of MyQ® Company is prohibited. The trademark and product name is protected by MyQ® Company and/or its local affiliates.