MyQ X Security 1.0

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

Table of Contents

Security has always been a **top priority for MyQ**. In this section, you will find a guide to the secure deployment of MyQ X, as well as the MyQ X security white paper:

1 MyQ X Secure Deployment

Confidentiality of customer data and customer **security** have always been **MyQ's number one priority**. However, **security is a responsibility shared between vendors and customers.** Although the goal of MyQ X is to provide secure configuration by default, several areas require extra steps on the customer's side. These include but are not limited to certificate management, usage of strong credentials, permission delegation, and firewall configuration.

This document contains actionable checklists for secure deployment of MyQ X Central Server and MyQ X Print Server in enterprise environments. We strongly believe that following these guidelines will considerably reduce the attack surface of any print management infrastructure. Needless to say, MyQ X server applications are only as secure as the underlying operating systems and network environments. As Windows security is a topic of its own, it is not covered by this document.

MyQ X systems are constantly being improved and patched, following the MyQ Secure Development Lifecycle policy. Please, make sure you **always use the latest supported release**. Release notes can be found in every product guide. Please also refer to the End Of Life (EOL) Policy[1] for the End of Maintenance announcements and successor components.

> This guide was prepared along with Mainstream Technologies, now Seyfor[2], during regular independent security audits.

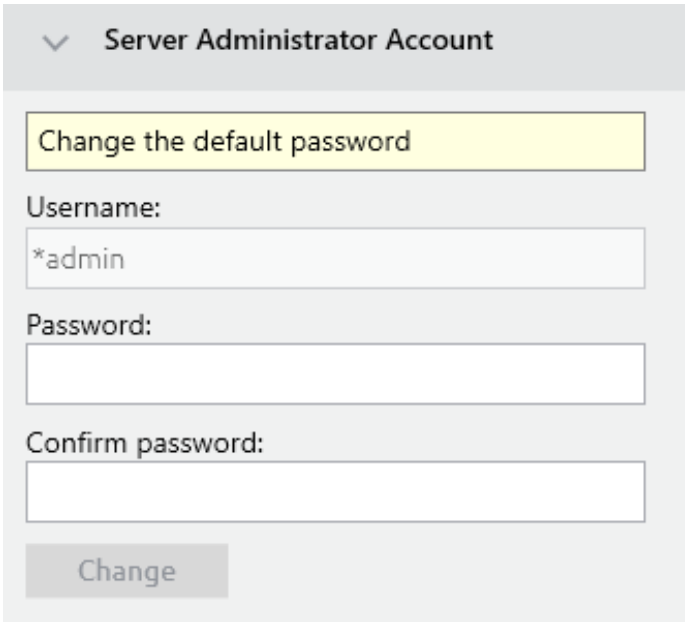
1.1 MyQ X Central Server

1.1.1 Default passwords

Change server administrator password

One of the first steps should be changing the default administrative password, which is *1234*:

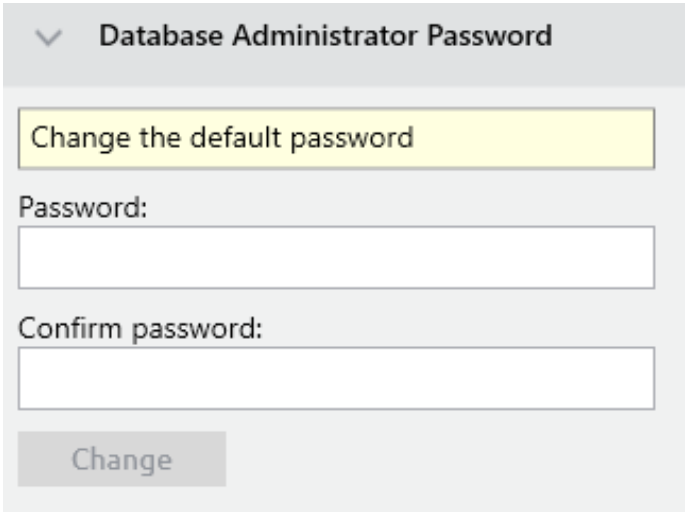
1. https://www.myq-solution.com/en/product-support-end-of-life-policy
2. http://www.seyfor.cz



The password is stored in the database in a hashed form.

Change database administrator password

In case the internal Firebird database is used, change the default password which is used by MyQ Central Server to authenticate against it:



This password is stored in the "C:\ProgramData\MyQ Central Server\setup.ini" file in an encrypted form and is set to "*masterkey*" by default.

1.1.2 Connection security

Configure HTTPS certificate

A custom certificate that is trusted by all client computers and contains the DNS name of the server should be configured for MyQ Central Server:

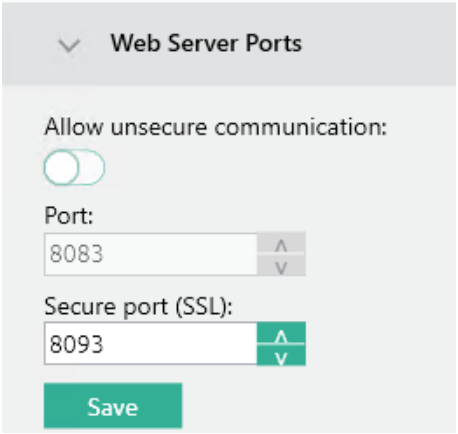
The certificate is physically stored in the “C:\ProgramData\MyQ Central Server\Cert” directory in the following files:

- server.pfx – certificate with both public and private keys
- server.cer – certificate with the public key
- server.key – private key

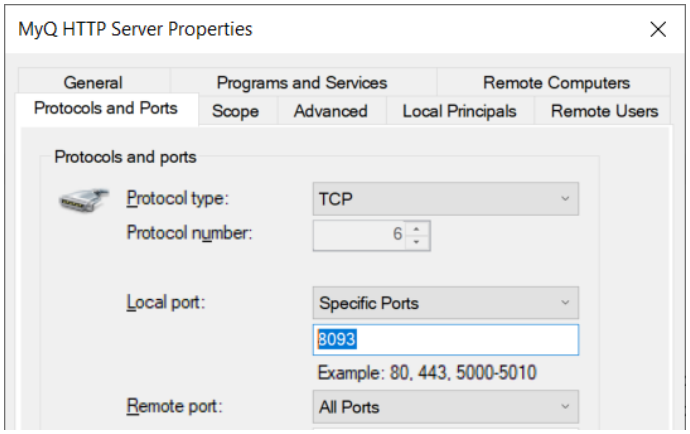
Usage of wildcard certificates is discouraged, as they pose a much higher security risk when stolen.

Block unencrypted HTTP traffic

Unencrypted HTTP traffic should not be enabled in the MyQ Central Server configuration:

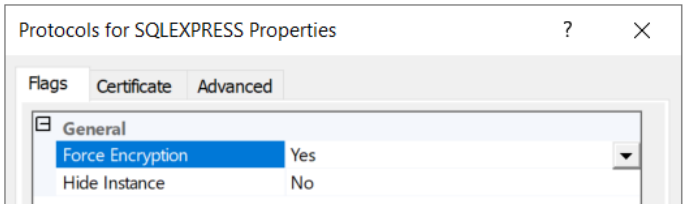


The host-based firewall should also be configured to only enable HTTPS traffic:

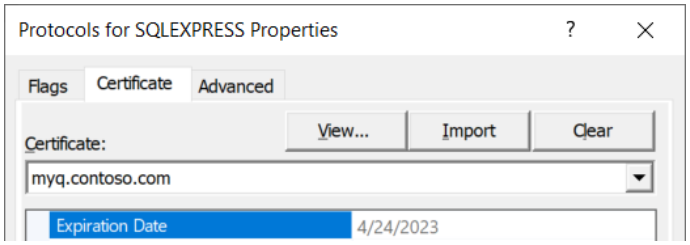


Encrypt database connections

If Microsoft SQL Server is used to store the MyQ database, ensure that TLS encryption is enforced through the SQL Server Configuration Manager:

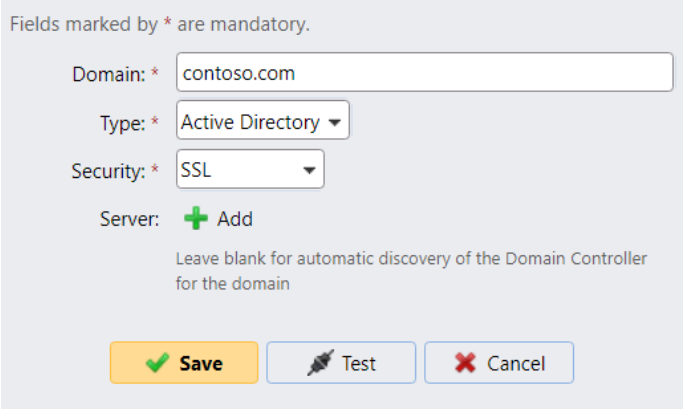


A certificate issued by a trusted CA should also be configured on the SQL Server:



Enforce encrypted LDAP traffic

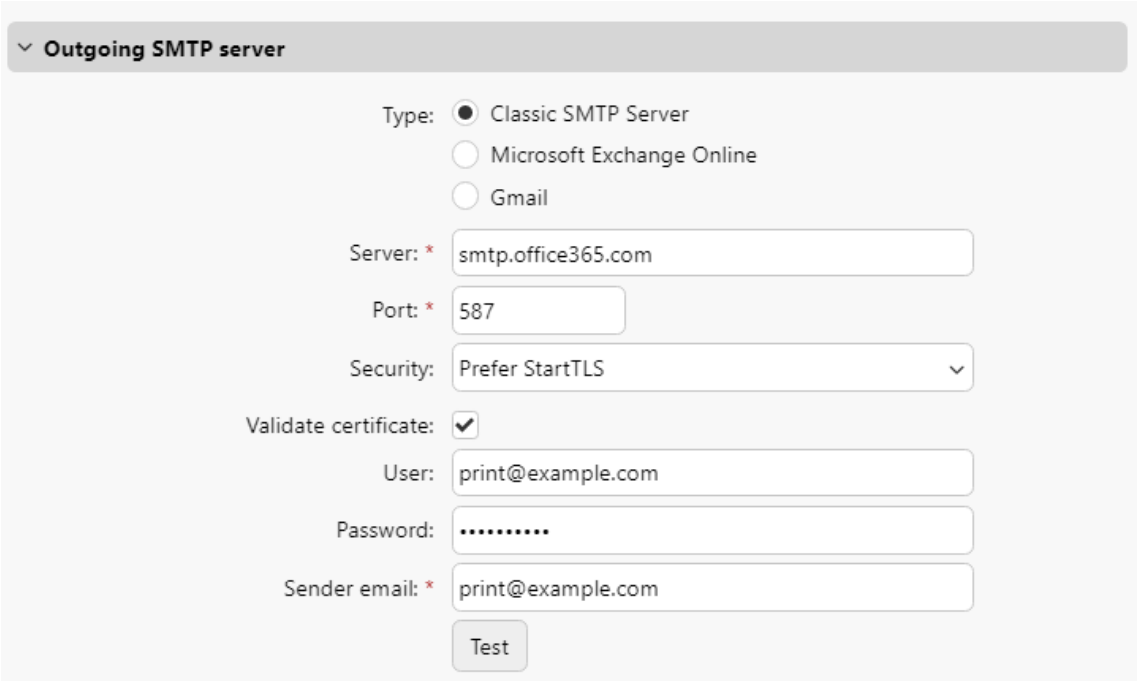
If synchronization of user accounts over the LDAP protocol is used, set the connection security to SSL:



For security reasons, do not use START TLS, as it is vulnerable to MITM attacks. A certificate issued by a trusted CA must be configured on all LDAP servers (Active Directory domain controllers).

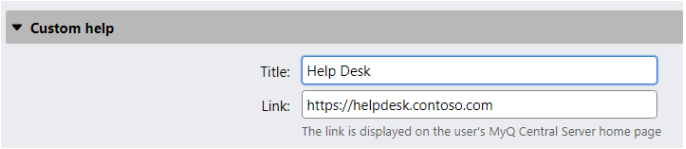
Secure SMTP traffic

If an SMTP server is configured in MyQ Central Server, enforce the usage of TLS with certificate validation:



Always use FQDN

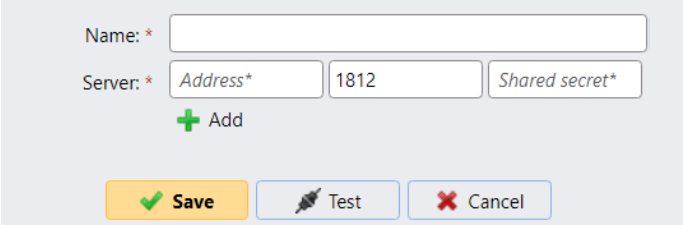
To prevent MITM attacks, strictly use fully qualified domain names in all configuration windows:



Never contact servers by only typing IP addresses or single-label names.

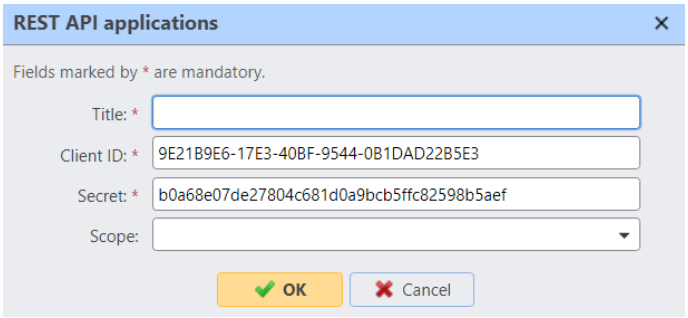
Secure RADIUS traffic

If RADIUS authentication is used, always generate strong shared secrets that are specific to the MyQ Central Server:



Protect REST API keys

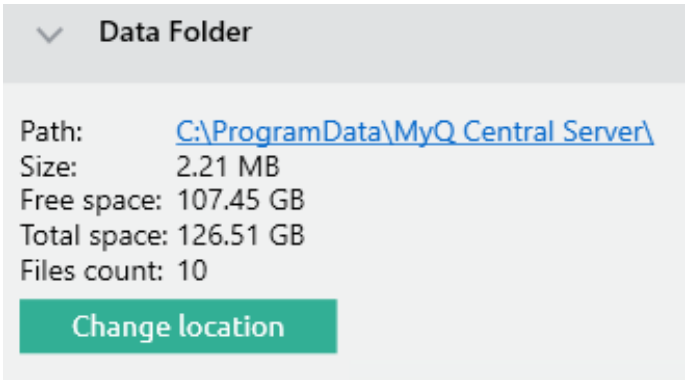
When REST APIs are used, protect the client secrets from unnecessary exposure and perform periodic secret rollover:



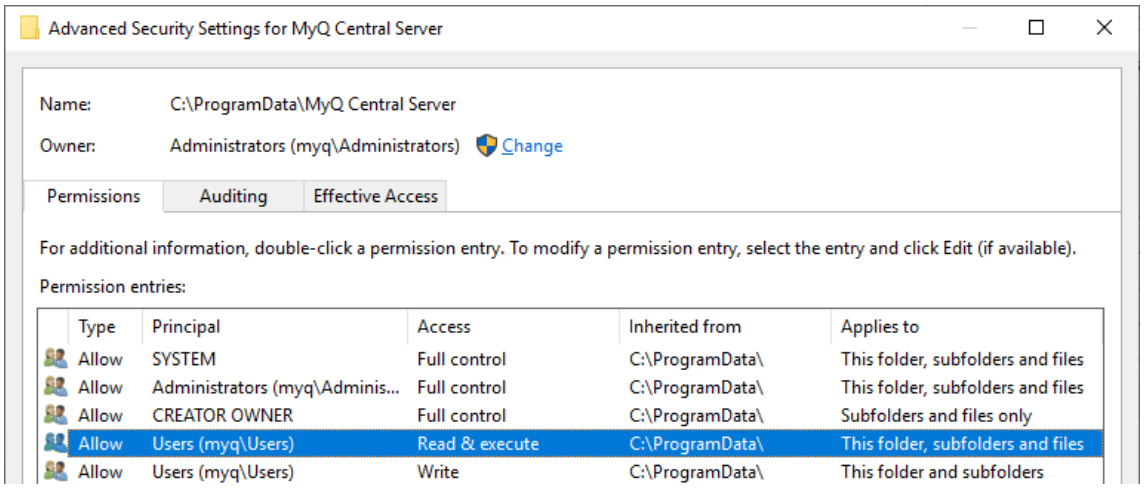
1.1.3 Data security

Restrict data folder permissions

The data folder of MyQ Central Server contains highly sensitive data, including the user database and TLS certificate private key. Its current location is displayed in the MyQ Central Server Easy Config application:



All users (local/domain) have read access by default:



Only Administrators, SYSTEM, and MyQ service account should have access to this directory. Here is a sample batch script that can be used for permission hardening:

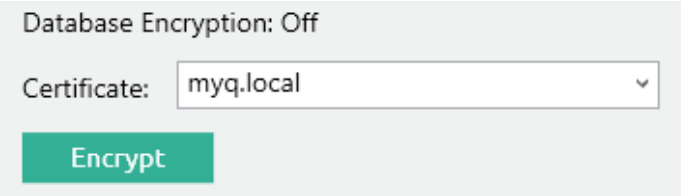
```
@ECHO OFF

REM Add the virtual account SIDs to all MyQ Central Server services:
sc sidtype myqm_platform unrestricted
sc sidtype myqm_apache unrestricted
sc sidtype traefik unrestricted
sc sidtype FirebirdServerMasterInstance unrestricted
```

```
REM Grant rights to the virtual service accounts:
icacls "%ProgramData%\MyQ Central Server" ^
  /grant:r "NT AUTHORITY\SYSTEM:(OI)(CI)F" ^
  /grant "BUILTIN\Administrators:(OI)(CI)F" ^
  /grant "NT SERVICE\myqm_platform:(OI)(CI)M" ^
  /grant "NT SERVICE\myqm_apache:(OI)(CI)M" ^
  /grant "NT SERVICE\FirebirdServerMasterInstance:(OI)(CI)M" ^
  /grant "NT SERVICE\traefik:(OI)(CI)M" ^
  /inheritance:r ^
  /Q
```

Enable database encryption

When using the embedded database, always encrypt it using a custom certificate to lower the risk of data leaks:



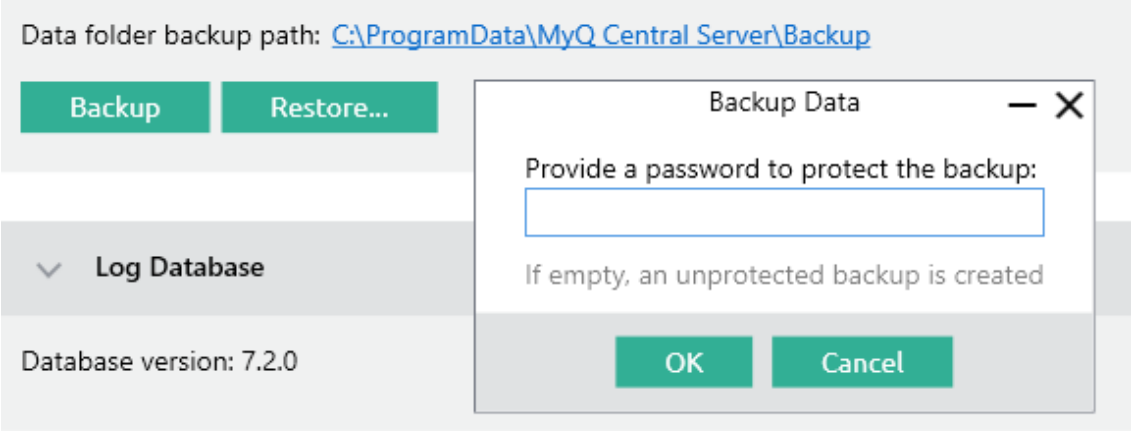
The certificate needs to have the “Encrypting File System” Enhanced Key Usage (EKU) and it must be located in one of the following computer certificate stores:

- Personal
- Trusted Publishers
- Third-Party Root Certification Authorities
- Other people

The Personal store is the preferred one.

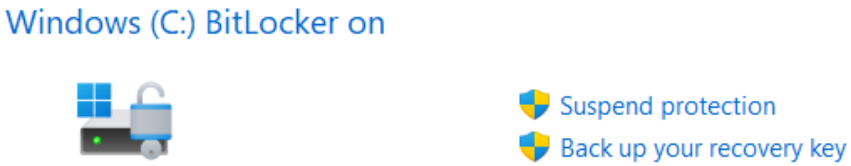
Encrypt backups

Database backups should be protected by secure, randomly generated passwords:



Enable disk encryption

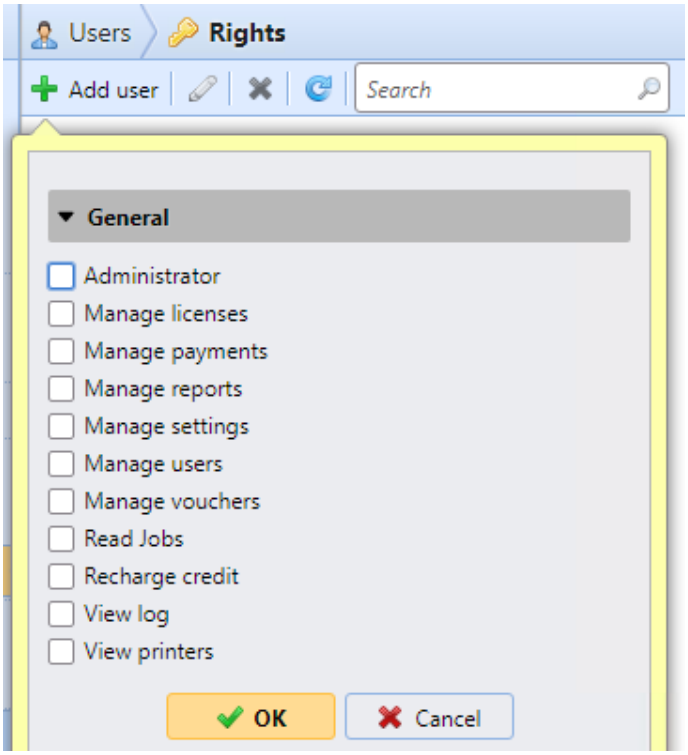
If possible, a full disk encryption technology like Microsoft BitLocker should be enabled on the MyQ Central Server to protect the data at rest:



1.1.4 Additional recommendations

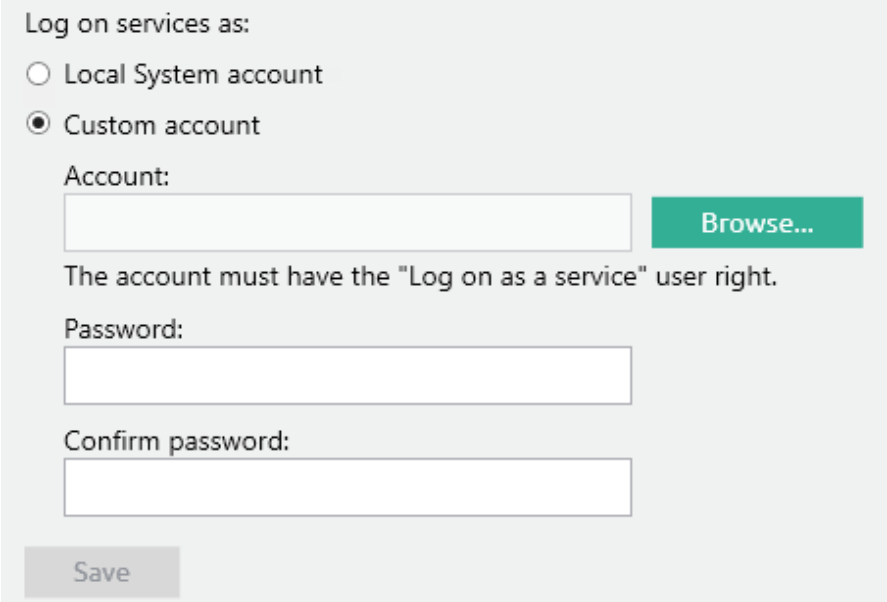
Deploy RBAC

Do not use the default *admin account for regular operations. Use privilege delegation instead, while applying the principle of least privilege:



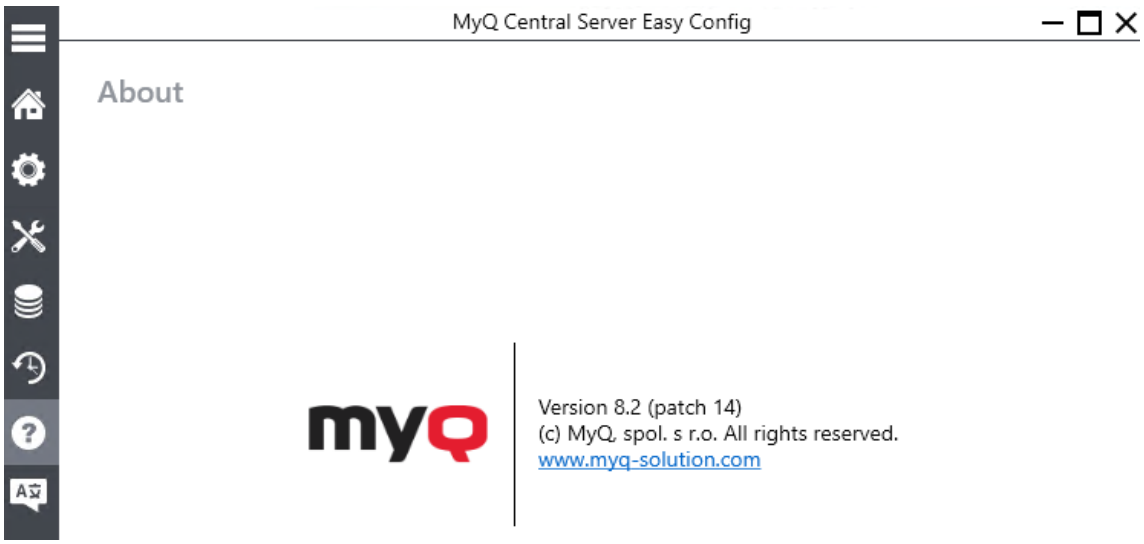
Configure a Custom Service Account

MyQ Central Server is by default running under the highly privileged SYSTEM account. Configure a custom service account with a strong password instead:



Keep the Server Updated

Install security updates provided by MyQ as soon as they are available. You can check the currently installed application version in MyQ Central Server Easy Config:



Keep the OS Secure

MyQ Central Server is only as secure as the underlying operating system. Keep it updated and apply security policies recommended by Microsoft.

Regularly update your software to fix security vulnerabilities and enhance performance. Check the System Requirements for the list of requirements and recommendations.

For example, .NET must be updated either with management tools or via Windows Updates on an opt-in basis[3].

Plan for Disaster Recovery

Periodically create backups of the MyQ Central Server, including the database, certificates, and configuration files. Test the recovery procedure at least once.

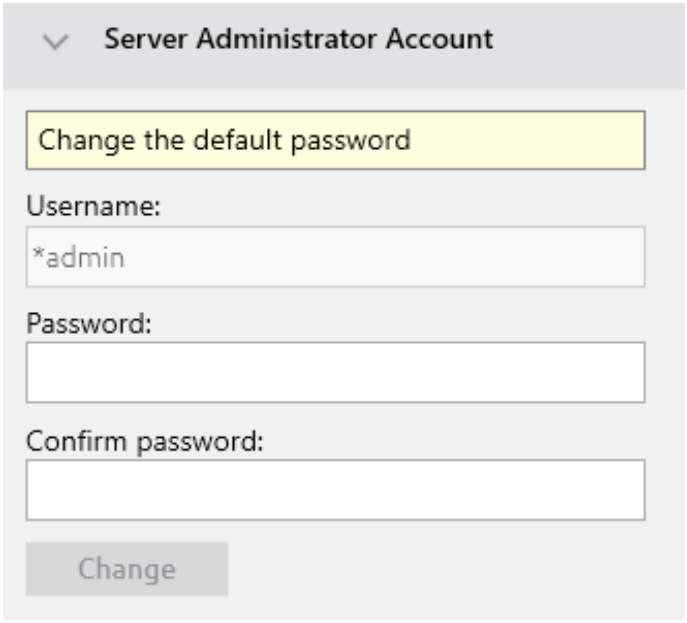
3. https://devblogs.microsoft.com/dotnet/server-operating-systems-auto-updates/

1.2 MyQ X Print Server

1.2.1 PS Default passwords

Change server administrator password

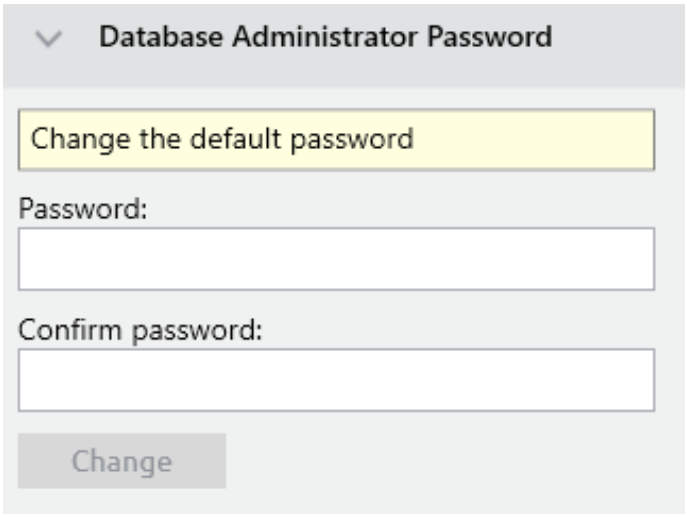
One of the first steps should be changing the default administrative password, which is *1234*:



The password is stored in the database in a hashed form.

Change database administrator password

Change the default password which is used by MyQ Print Server to authenticate against the internal Firebird database:

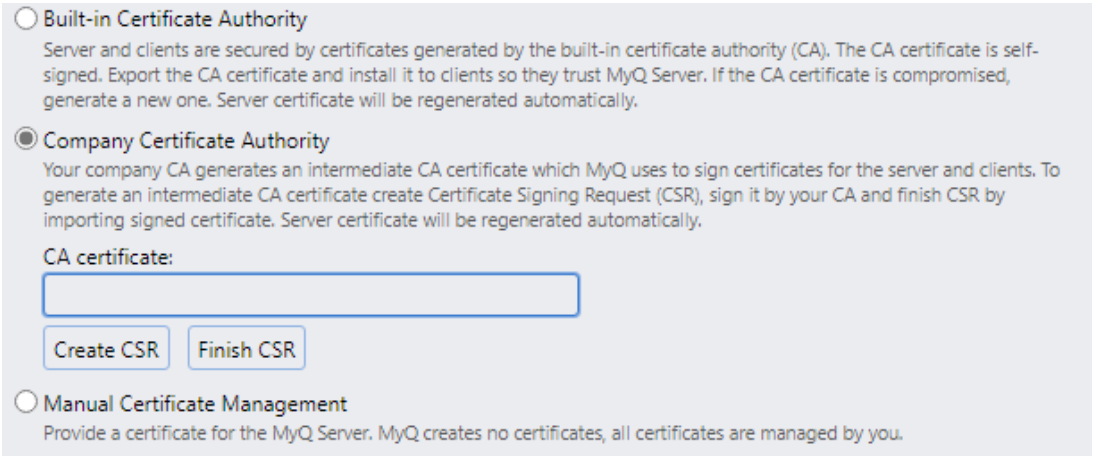


This password is stored in the "C:\ProgramData\MyQ\setup.ini" file in an encrypted form and is set to "*masterkey*" by default.

1.2.2 PS Connection security

Configure HTTPS certificate

A custom certificate that is trusted by all client computers should be configured for MyQ Print Server. Three modes of certificate management are available:



By default, MyQ Print Server creates its own root CA certificate and uses it to sign server and client certificates. The public portion of this certificate can be exported and deployed to the client certificate trust store, e.g., by using Group Policy or MDM.

Organizations with their own PKI already trusted might prefer the second option. MyQ Print Server uses its own intermediate CA to issue server and client certificates.

The autogenerated intermediate CA certificate must be signed by the company's CA so that it is trusted by clients.

If the corporate security policy does not allow for an intermediate CA certificate to be installed on MyQ Print Server, or a certificate issued by a public certificate authority is to be used, manual certificate management must be used instead.

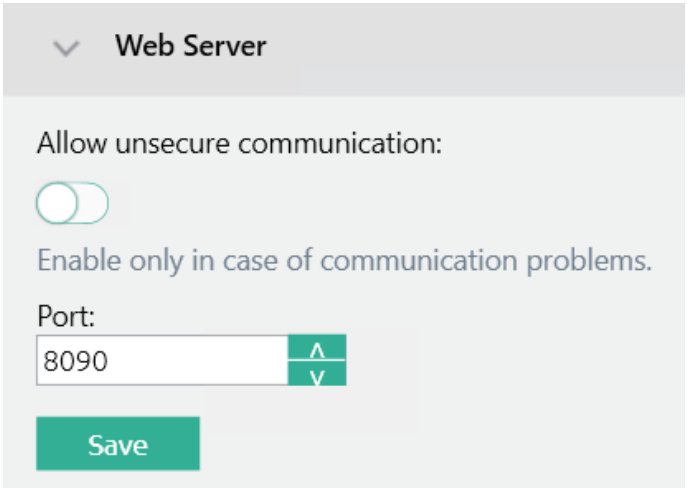
Regardless of the CA mode, certificates are physically stored in the "C:\ProgramData\MyQ\Cert" directory, which may contain the following files:

- server.pfx – server certificate with both public and private keys
- server.cer – server certificate with public key
- server.key – server private key
- ca-root.crt – company root CA certificate with public key
- ca-myq.pfx – issuing CA certificate with both public and private keys
- ca-myq.crt – issuing CA certificate with public key
- ca-myq.key– issuing CA private keys

Private keys of the local issuing CA (used in the first two modes of operation) are always protected by a randomly generated password that is stored in the internal Firebird database in an encrypted form.

Block unencrypted HTTP traffic

Unencrypted HTTP traffic should not be enabled in the MyQ Print Server configuration:



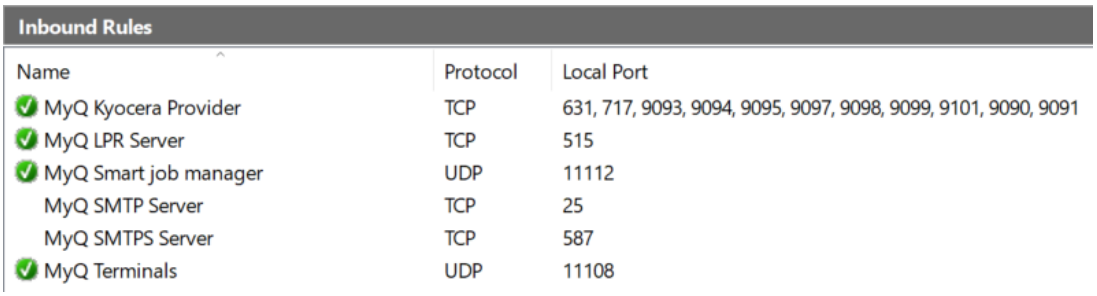
Review communication security settings

Check the minimum security TLS versions configured in Settings – Network – Minimum TLS version. The default since MyQ X 10.2 is TLS 1.2.

For more advanced options, such as how to set the minimum required TLS to 1.3 instead, check Advanced Security.

Block unused ports

Decrease the attack surface by disabling firewall rules for protocols not used by MyQ Print Server:

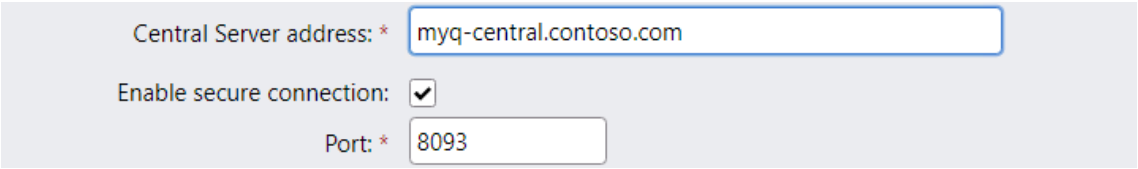


Inbound Rules

Name	Protocol	Local Port
MyQ Kyocera Provider	TCP	631, 717, 9093, 9094, 9095, 9097, 9098, 9099, 9101, 9090, 9091
MyQ LPR Server	TCP	515
MyQ Smart job manager	UDP	11112
MyQ SMTP Server	TCP	25
MyQ SMTPS Server	TCP	587
MyQ Terminals	UDP	11108

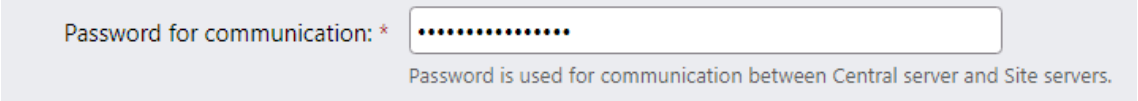
Encrypt connections to MyQ Central Server

Only use HTTPS to connect to MyQ Central Server:



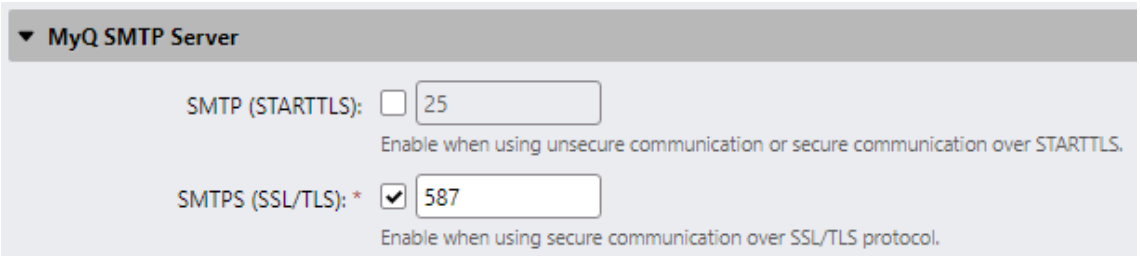
Use strong passwords for server-to-server authentication

Password for communication between central server and site should be strong (password complexity):

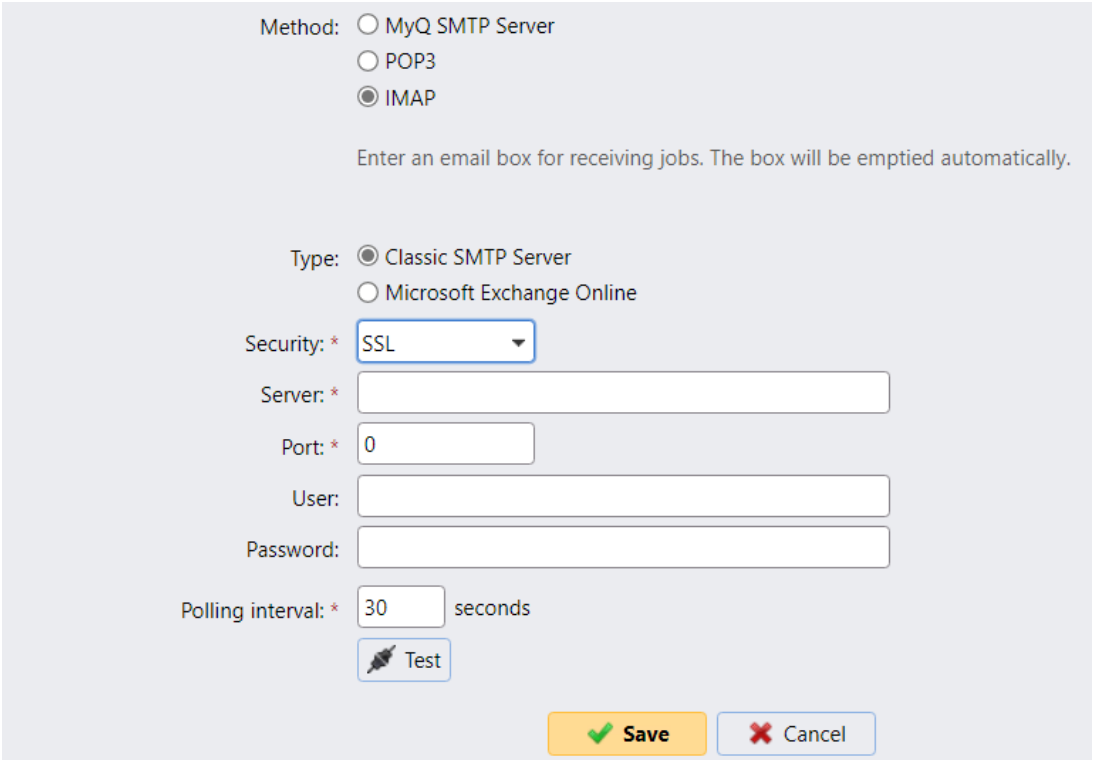


Secure SMTP traffic

When the SMTP protocol is used to send emails or to receive documents from network scanners, TLS encryption should always be enforced to ensure data confidentiality.

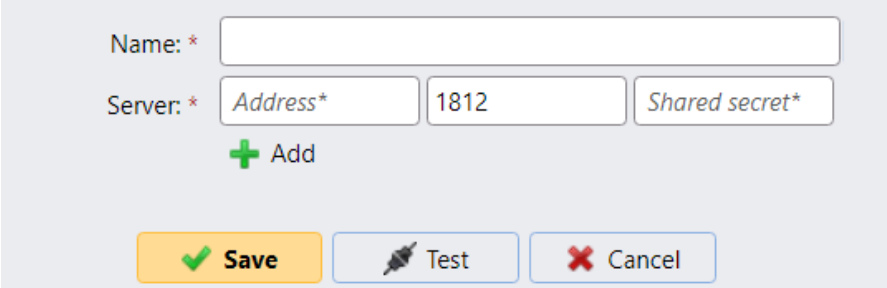


TLS encryption should also be enforced when the IMAP protocol is used, while the legacy POP3 protocol should be avoided:



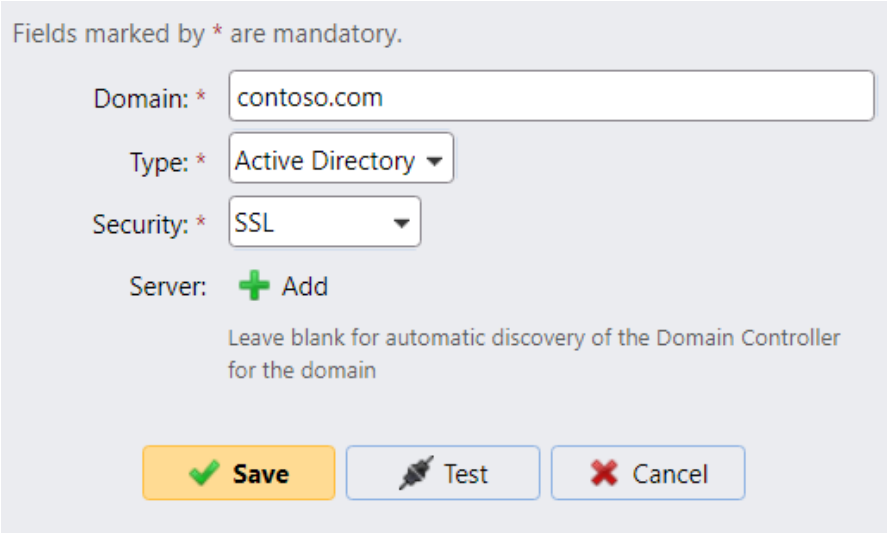
Use strong and unique RADIUS passwords

If RADIUS authentication is used, always generate strong shared secrets that are specific to the MyQ Print Server:



Encrypt LDAP traffic

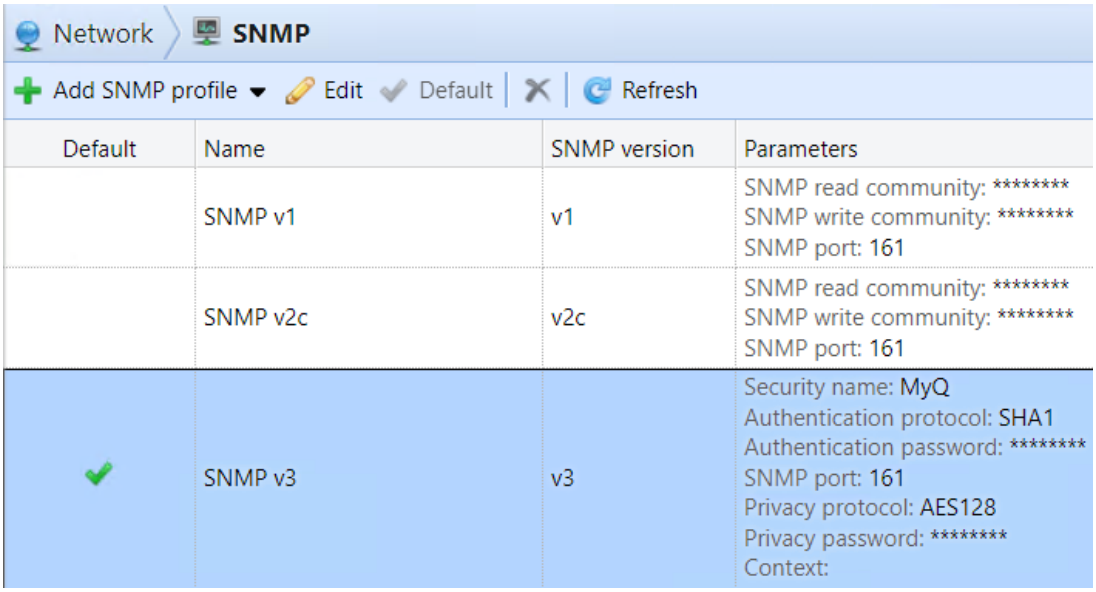
TLS encryption should be used to secure all LDAP traffic:



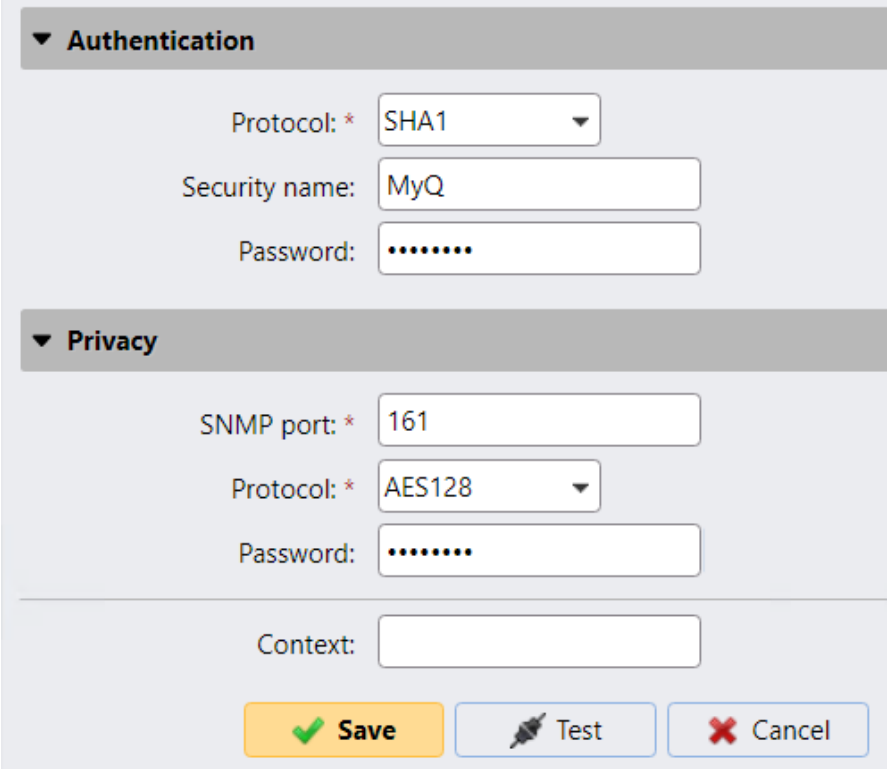
For security reasons, do not use START TLS, as it is vulnerable to MITM attacks. A certificate issued by a trusted CA must be configured on all LDAP servers (Active Directory domain controllers).

Secure SNMP traffic

Insecure SNMPv1 communication with devices should be avoided:

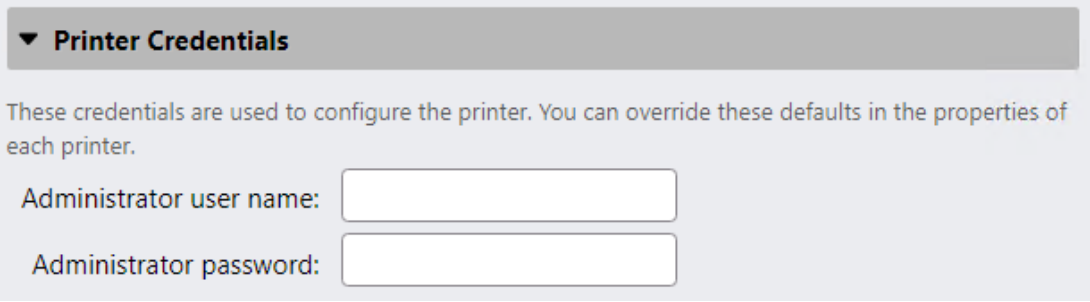


Only use SNMPv3 with a strong password and configure more secure cryptographic algorithms to be used (SHA1 and AES):



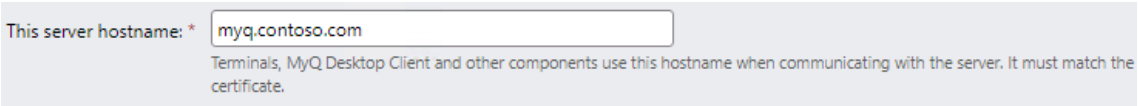
Secure printer credentials

Printer credential management is done outside of MyQ Print Server and is vendor specific. If possible, strong, randomly generated passwords should be used to manage printers:



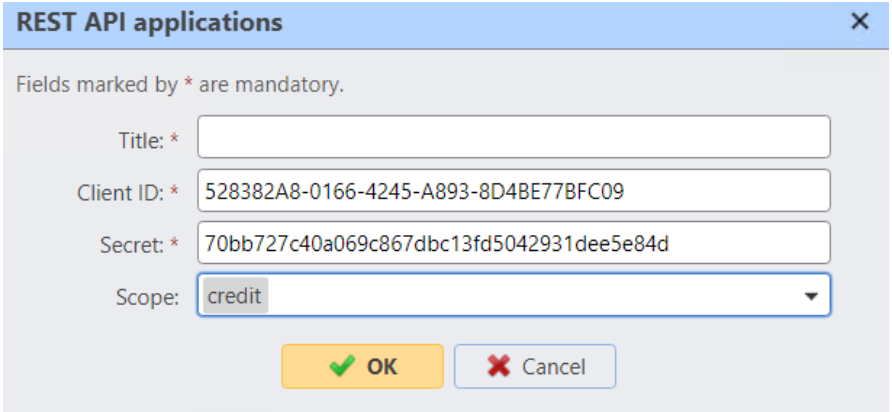
Always use FQDN

To prevent MITM attacks, strictly use fully qualified domain names in all configuration windows:



Protect REST API keys

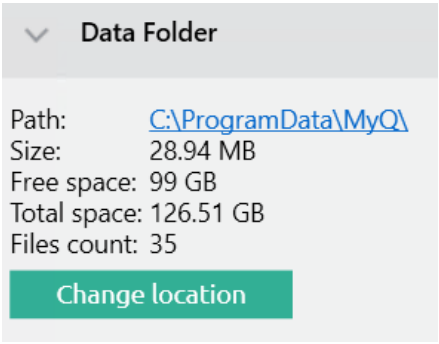
When REST APIs are used, protect the client secrets from unnecessary exposure and perform periodic secret rollover:



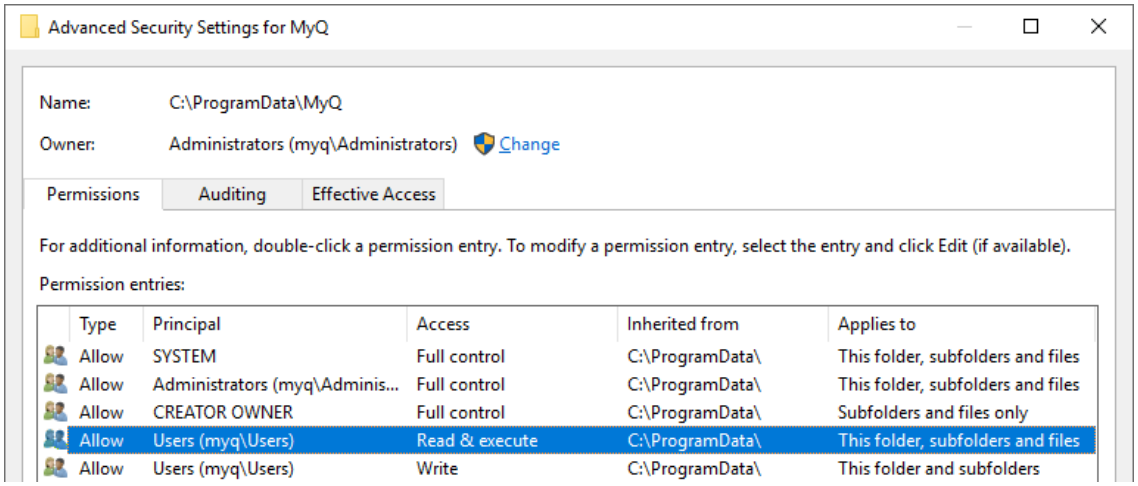
1.2.3 PS Data security

Restrict data folder permissions

The data folder of MyQ Print Server contains highly sensitive data, including the user database and TLS certificate private key. Its current location is displayed in the MyQ Easy Config application:



All users (local/domain) have read access by default:



Only Administrators, SYSTEM, and MyQ service account should have access to this directory. Here is a sample batch script that can be used for permission hardening:

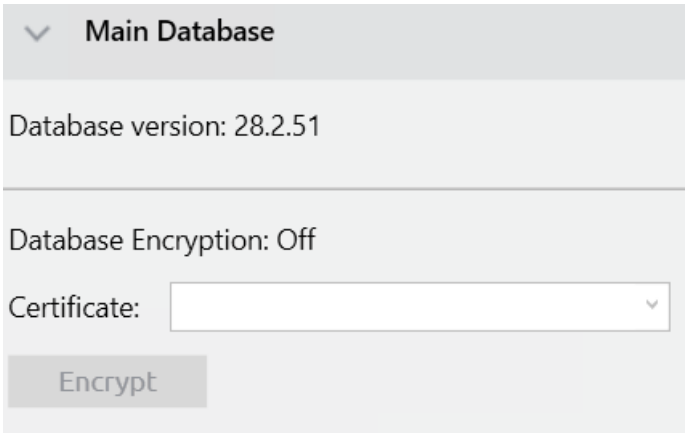
```
@ECHO OFF

REM Add the virtual account SIDs to all MyQ Print Server services:
sc sidtype Apache unrestricted
sc sidtype FirebirdServerDefaultInstance unrestricted
sc sidtype KNM_PM unrestricted
sc sidtype MyQ unrestricted
sc sidtype traefik unrestricted

REM Grant rights to the virtual service accounts:
icacls "%ProgramData%\MyQ" ^
  /grant:r "NT AUTHORITY\SYSTEM:(OI)(CI)F" ^
  /grant "BUILTIN\Administrators:(OI)(CI)F" ^
  /grant "NT SERVICE\MyQ:(OI)(CI)M" ^
  /grant "NT SERVICE\Apache:(OI)(CI)M" ^
  /grant "NT SERVICE\FirebirdServerDefaultInstance:(OI)(CI)M" ^
  /grant "NT SERVICE\KNM_PM:(OI)(CI)M" ^
  /grant "NT SERVICE\traefik:(OI)(CI)M" ^
  /inheritance:r ^
  /Q
```

Enable database encryption

Always encrypt the database using a custom certificate to lower the risk of data leaks:



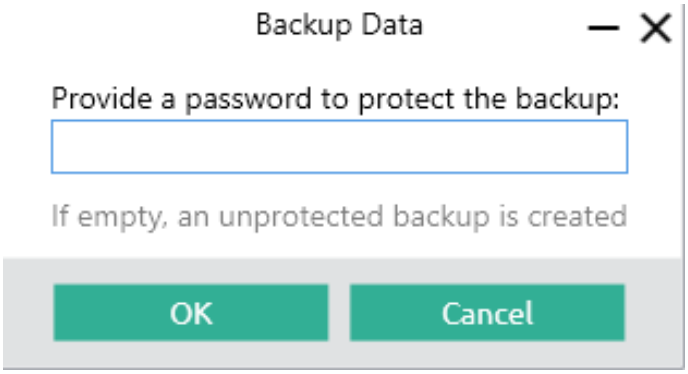
The certificate needs to have the “Encrypting File System” Enhanced Key Usage (EKU) and it must be located in one of the following computer certificate stores:

- Personal
- Trusted Publishers
- Third-Party Root Certification Authorities
- Other people

The Personal store is the preferred one.

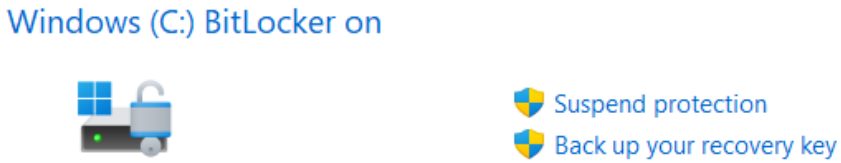
Encrypt backups

Database backups should be protected by secure, randomly generated passwords:



Enable disk encryption

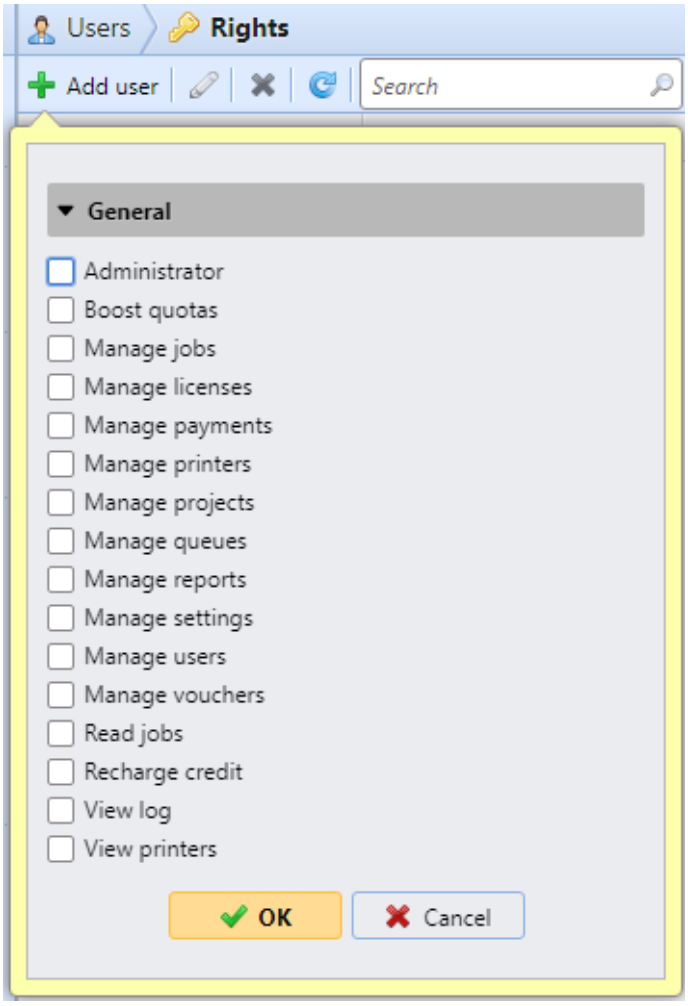
If possible, a full disk encryption technology like Microsoft BitLocker should be enabled on the MyQ Print Server to protect the data at rest:



1.2.4 PS Additional recommendations

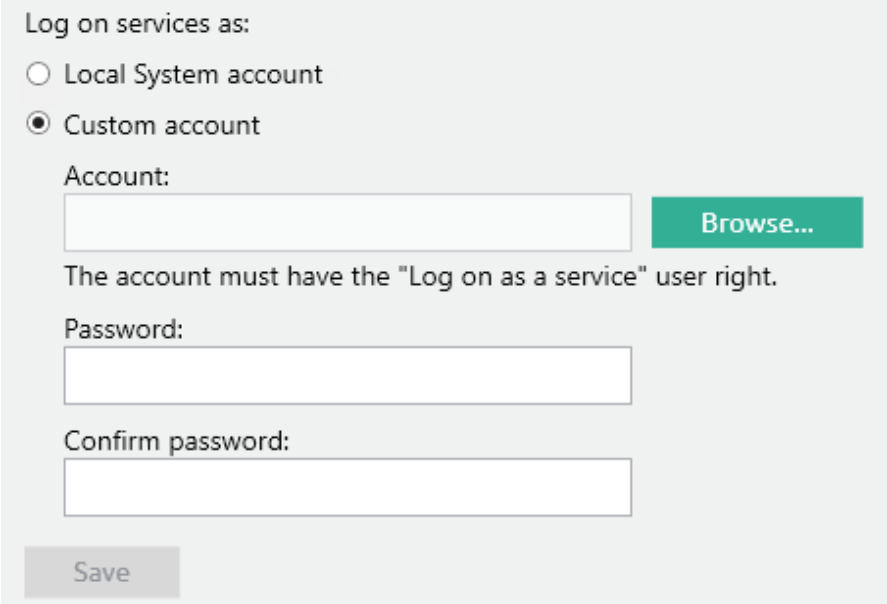
Deploy RBAC

Do not use the default *admin account for regular operations. Use privilege delegation instead, while applying the principle of least privilege:



Configure a Custom Service Account

MyQ Print Server is by default running under the highly privileged SYSTEM account. Configure a custom service account with a strong password instead:



Keep the Server Updated

Install security updates provided by MyQ as soon as they are available. You can check the currently installed application version in MyQ Easy Config:

Keep the OS Secure

MyQ Print Server is only as secure as the underlying operating system. Keep it updated and apply security policies recommended by Microsoft.

Regularly update your software to fix security vulnerabilities and enhance performance. Check the System Requirements for the list of requirements and recommendations.

For example, .NET must be updated either with management tools or via Windows Updates on an opt-in basis[4].

Plan for Disaster Recovery

Periodically create backups of the MyQ Print Server, including the database, certificates, and configuration files. Test the recovery procedure at least once.

1.3 MyQ X Desktop Client

The MyQ Desktop Client employs robust security mechanisms to ensure secure communication, authentication, and data integrity across enterprise printing environments. This document details the protocols, authentication methods, and configuration best practices that underpin the Desktop Client's security architecture, with a focus on TLS encryption, Integrated Windows Authentication (IWA), Kerberos, NTLM, and Entra ID integration. Technical implementations such as Service Principal Name (SPN) registration, certificate management, and silent login flows are analyzed to demonstrate compliance with modern security standards.

1.3.1 Secure Communication Architecture

TLS Encryption by Default

Print and Central Servers enforce TLS 1.2+ encryption for all communication channels, including interactions with the Desktop Client. This ensures data confidentiality and integrity during job spooling, authentication, and reporting. Administrators must configure HTTPS endpoints using Fully Qualified Domain Names (FQDNs) to prevent man-in-the-middle (MITM) attacks.

Certificate Validation Modes

- **Strict Mode**: Requires server certificates to be issued by a trusted Certificate Authority (CA) or manually added to the system's trust store. Connection attempts fail if validation fails. We recommend using Strict Mode whenever possible.
- **Normal Mode**: Allows users to bypass untrusted certificate warnings, with accepted certificates stored in `%ProgramData%\MyQ\Desktop Client\cert.store` for future sessions.

4. https://devblogs.microsoft.com/dotnet/server-operating-systems-auto-updates/

1.3.2 Authentication Mechanisms

Integrated Windows Authentication (IWA)

IWA enables seamless authentication in domain-joined environments using Kerberos or NTLM. The server leverages the Windows HTTP Server API (`http.sys`) to handle incoming HTTP requests and validate Service Principal Names (SPNs), ensuring protocol integrity.

Kerberos Workflow

1. **Ticket Granting Ticket (TGT) Acquisition**: Domain-joined clients obtain a TGT from the Key Distribution Center (KDC).
2. **Service Ticket Request**: The client requests a service ticket for `HTTP/<FQDN>` from the KDC.
3. **Token Validation**: MyQ Server validates the service ticket against the registered SPN.

Critical Configuration:

- The server must have a properly configured SPN for Kerberos authentication to function correctly.
- Access via IP addresses bypasses Kerberos, forcing fallback to NTLM.

> **Kerberos Enforcement**
> For environments requiring stricter security, it's possible to configure the application to **exclusively use Kerberos** and disallow NTLM fallback. This is done on a Server level basis, not exclusively for the Desktop Client.
>
> 1. Disable NTLM via `KerberosOnly=True` in `config.ini`.
> 2. Register SPNs for all MyQ servers using `setspn`.
> 3. Use FQDNs instead of IP addresses for server endpoints.

NTLM Fallback

NTLM serves as a fallback in non-domain or IP-based scenarios. While less secure, it uses a challenge-response mechanism hashed with the user's password. To enforce Kerberos exclusively, follow the suggestion above.

Entra ID Silent Login

For Entra ID-joined or hybrid devices, Desktop Client uses the Microsoft Authentication Library (MSAL) and Windows Authentication Manager (WAM) to acquire tokens silently via the OS account. The flow involves:

1. **Token Acquisition**: MSAL retrieves an ID token using WAM.
2. **Token Exchange**: The ID token is exchanged for a MyQ access token to authenticate REST API calls.

OAuth 2.0 Authorization Code Flow

For non-Windows environments, Desktop Client supports OAuth 2.0 via the `authorization_code` grant:

1. **User Redirection**: The client redirects users to the MyQ login page.
2. **Code Exchange**: After authentication, the authorization code is exchanged for an access token.

Entra ID Configuration

- Enable **Sign in with Microsoft** in the MyQ Server settings for hybrid-joined devices.
- Ensure devices are Entra ID-registered to leverage silent authentication.

Certificate Management

Trusted Root Certificates

- **Strict Mode**: Certificates must be preinstalled in the OS trust store (e.g., via Group Policy).
- **Normal Mode**: User-approved certificates are stored in `cert.store` and reused for subsequent sessions.

Validation Workflow

1. Server certificate validation checks the trust chain.
2. If validation fails, users receive a prompt to accept or reject the certificate (this is only the case if Normal rather than Strict Validation mode is in use).
3. Accepted certificates are cached to prevent repeated prompts (this is only the case if Normal rather than Strict Validation mode is in use).

Certificate Best Practices
We recommend always deploying enterprise CA-signed certificates for MyQ servers.

Conclusion

MyQ Desktop Client integrates enterprise-grade authentication and encryption to mitigate risks such as credential theft and eavesdropping. By enforcing Kerberos, TLS, and certificate validation, organizations can align with Zero Trust principles while maintaining usability through silent authentication flows.

2 MyQ X Security Whitepaper

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-factor 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

MyQ X's security approach is founded on the principle that **security is not an afterthought but an integral part of the entire print management ecosystem**. The platform implements a comprehensive defense strategy that protects data and workflows at every stage of the document lifecycle.

2.1 Zero Trust Architecture

Following the "never trust, always verify" methodology, MyQ X assumes that threats can exist both inside and outside of a network. Every connection, user, and device must be authenticated and authorized before accessing print resources, ensuring continuous verification throughout all interactions.

2.2 Three-Phase Protection Framework

MyQ X addresses security through three critical phases:

2.2.1 Securing Print Infrastructure

All supporting infrastructure is properly secured before any document is printed, including workstations, mobile devices, servers, networks, and printing devices.

2.2.2 Securing Print Workflows

Proven secure workflows including authenticated print release, job isolation, and comprehensive reporting prevent vulnerabilities that could leave organizations exposed.

2.2.3 Securing Printed Output

Continued protection through watermarking, digital signatures, and comprehensive audit logs that maintain traceability and encourage responsible user behavior.

2.3 Privacy by Design

Data protection is embedded into MyQ X's architecture from the ground up. The system minimizes data collection, implements strong encryption, and provides users with control over their personal information to ensure GDPR compliance and privacy protection.

2.4 Continuous Security Evolution

MyQ X maintains its security through regular updates, prompt vulnerability remediation, threat intelligence integration, and ongoing third-party security assessments and certifications.

This security-first approach ensures organizations can confidently deploy MyQ X knowing their sensitive information, compliance requirements, and operational continuity are protected by industry-leading security measures.

2.5 Key Security Improvements in 10.2

MyQ X 10.2 introduces significant security enhancements designed to strengthen protection against evolving cyber threats while maintaining operational efficiency. These improvements address critical vulnerabilities and implement modern security standards.

2.5.1 Enhanced TLS Security

Default TLS 1.2 Minimum Version: MyQ X 10.2 increases the default minimum TLS version from 1.1 to 1.2, with support for TLS 1.3. This eliminates support for deprecated SSL protocols and weak ciphers that pose security risks.

Improved Certificate Validation: Enhanced certificate validation prevents the use of expired or improperly issued certificates, protecting against man-in-the-middle attacks and other vulnerabilities. The system now automatically trusts Root CA certificates from the server's system certificate store.

2.5.2 Authentication Security Enhancements

Enhanced Password and PIN Security: Improved password hashing algorithms strengthen credential protection. The system introduces new PIN security rules, including mandatory 6-digit minimum length and prevention of easily guessable combinations like "1234" or "1111".

Login Attempt Protection: Unsuccessful authentication attempts are now limited for security reasons. By default, clients/devices are blocked for 5 minutes after more than 5 invalid login attempts within 60 seconds, with configurable time periods.

Improved Login Event Logging: Enhanced logging of login events, especially failed authentication attempts, makes filtering and monitoring security events in MyQ Log easier for administrators.

2.5.3 Database Security Upgrades

Firebird 4.0 Implementation: Upgrade to Firebird 4.0 database engine brings enhanced security features and improved performance. Database passwords are now obfuscated in log files to prevent credential exposure.

Enhanced Data Protection: Limited access to sensitive data through custom reports and external reporting accounts, ensuring data confidentiality across different access levels.

2.5.4 Vulnerability Resolution

Critical CVE Fixes: MyQ X 10.2 addresses multiple critical vulnerabilities including:

- CVE-2024-28059: Unauthenticated Remote Code Execution vulnerability.
- CVE-2024-22076: PHP Scripting security improvements.
- CVE-2023-45853, CVE-2023-5678, CVE-2023-49316: Third-party component vulnerabilities.

Component Security Updates: Updated versions of critical components including OpenSSL 3.1.0, PHP 8.3.14, and Apache 2.4.57 address known security vulnerabilities.

2.5.5 API and Integration Security

REST API Restrictions: Limited scopes for well-known clients and removed capabilities for sensitive operations like changing user authentication servers, strengthening API security.

PHP Scripting Controls: New Easy Config settings allow administrators to lock/unlock PHP scripting access, improving security by maintaining these settings in read-only mode.

2.5.6 Administrative Security

Enhanced Admin Account Security: Default admin password has been removed for new installations. Administrators can now disable admin accounts when not needed, promoting the use of specific user accounts with appropriate rights rather than shared administrative accounts.

These security improvements demonstrate MyQ X's commitment to maintaining enterprise-grade security standards while addressing contemporary cybersecurity challenges. Regular security updates and proactive vulnerability management ensure organizations can deploy MyQ X with confidence in their security.

2.6 Business Value of Secure Print Management

Secure print management delivers measurable business value by transforming print infrastructure from a potential liability into a strategic security asset. MyQ X provides organizations with comprehensive protection that addresses the full spectrum of print-related risks while enhancing operational efficiency.

2.6.1 Risk Mitigation and Cost Reduction

Data Breach Prevention: Secure Print Release ensures confidential documents are never left unsupervised in printer trays, eliminating unauthorized access to sensitive information. Users authenticate before their jobs are released, maintaining complete control over document security.

Compliance Cost Avoidance: Built-in GDPR, HIPAA, and SOX compliance capabilities help organizations avoid regulatory penalties and reduce audit preparation costs through automated compliance controls and comprehensive audit trails.

Operational Continuity: MyQ's Device Spooling feature maintains printing capabilities during server outages, storing encrypted jobs locally for up to one week across 10 devices, preventing business disruption during system maintenance or unexpected downtime.

2.6.2 Enhanced Security Principles

Zero Trust Implementation: By requiring authentication for every print job, MyQ X enforces "never trust, always verify" principles throughout the print environment, strengthening overall organizational security posture.

Document Traceability: Watermarking and digital signatures enable organizations to track confidential documents throughout their lifecycle, providing accountability and deterring misuse of sensitive information.

Comprehensive Encryption: End-to-end encryption of print data, databases, and stored jobs ensures sensitive information remains protected throughout the entire document workflow, meeting stringent security requirements.

2.6.3 Operational Efficiency

Bandwidth Optimization: Client Spooling reduces network traffic by processing jobs locally, improving performance in bandwidth-constrained environments such as remote offices and branch locations.

Flexible Authentication: Multiple authentication options including ID cards, PINs, passwords, and mobile app authentication provide users with convenient yet secure access methods that fit diverse organizational needs. Multi-Factor Authentication (MFA), combining these methods, is also available.

Centralized Management: Unified security policies across all devices simplify administration while ensuring consistent protection standards throughout the organization.

2.6.4 Strategic Business Benefits

Competitive Advantage: Demonstrating robust print security capabilities can differentiate organizations in competitive markets, particularly in industries handling sensitive data or serving security-conscious clients.

Employee Confidence: Secure print workflows give users confidence that their documents are protected, improving productivity and reducing security-related concerns that can impact workplace efficiency.

Future-Ready Infrastructure: MyQ X's comprehensive security framework positions organizations to adapt to evolving cybersecurity threats and regulatory requirements without major infrastructure overhauls.

Secure print management with MyQ X transforms printing from a potential security vulnerability into a controlled, auditable, and compliant business process that supports organizational goals while protecting valuable information assets.

2.7 Compliance

MyQ X's comprehensive compliance framework demonstrates its commitment to meeting the highest international security standards and regulatory requirements. This multi-layered approach ensures organizations can confidently deploy MyQ X while satisfying diverse compliance mandates across industries and jurisdictions.

2.7.1 ISO 27001:2022 Certification and Implementation

MyQ has achieved **ISO/IEC 27001:2022 certification**, establishing a systematic approach to information security management that meets international best practices. The implementation encompasses:

Risk Management Framework: Comprehensive risk assessment processes that identify, evaluate, and mitigate information security risks across all business operations and customer deployments.

Security Controls Implementation: Structured deployment of technical, administrative, and physical security controls that protect information assets throughout their lifecycle.

Continuous Improvement Process: Regular reviews and updates of security policies, procedures, and controls to address evolving threats and maintain certification compliance.

Management Commitment: Executive-level oversight ensuring security remains integrated into business strategy and operational decision-making processes.

The certification validates MyQ's systematic approach to protecting customer data and maintaining the confidentiality, integrity, and availability of information systems.

2.7.2 GDPR Compliance Framework and Data Protection Measures

MyQ X implements comprehensive **GDPR compliance** through privacy-by-design principles embedded throughout the system architecture:

Data Minimization: The system collects only essential metadata required for operational functionality, avoiding unnecessary personal data processing that could increase compliance risks.

User Rights Management: Complete implementation of GDPR user rights including:

- Right of access to personal data
- Right to rectification of inaccurate information
- Right to erasure ("right to be forgotten")
- Right to data portability
- Right to restrict processing

Data Protection Impact Assessments: Systematic evaluation of privacy risks for new features and deployments, ensuring GDPR compliance is maintained throughout system evolution.

2.7.3 Regional Compliance Requirements (HIPAA, SOX)

MyQ X supports critical industry-specific compliance frameworks through robust data protection and audit capabilities:

HIPAA Compliance for Healthcare:

- Encryption of Protected Health Information (PHI) at rest and in transit.
- Comprehensive audit logging of all access to sensitive health data.
- Role-based access controls restricting PHI access to authorized personnel only.
- Secure backup and recovery procedures for healthcare data retention requirements.

SOX Compliance for Financial Services:

- Detailed audit trails for financial document processing and printing.
- Access controls preventing unauthorized modification of financial records.
- Secure archival capabilities supporting regulatory retention requirements.
- Segregation of duties through role-based permissions and approval workflows.

Additional Security Controls:

- Database encryption using industry-standard algorithms.
- Secure communication protocols for all data transmission.
- Automated backup procedures with encryption and integrity verification.
- Access logging and monitoring for compliance reporting.

2.7.4 **Secure Software Development Lifecycle (SSDLC) Practices**

MyQ implements a Secure Software Development Life Cycle aligned with industry standards and **SLSA** supply-chain requirements, ensuring that security practices are embedded across all phases of the software lifecycle.

Analysis

MyQ performs rigorous **Threat Modeling** and defines clear **Security Requirements** during the initial analysis phase, enabling early risk identification and establishing a strong security baseline before design begins.

Design

All architectural proposals undergo formal **Security Architecture Reviews** to validate adherence to principles like **Least Privilege**, **Zero Trust**, and **Defense in Depth**, ensuring that security is systematically embedded into system design.

Development

Developers follow **Secure Coding Practices** and peer-review processes while all builds run on dedicated, isolated **SLSA-compliant Build Servers**, ensuring protection of source integrity and build artifacts.

Testing

Security testing includes automated **SAST** and **Dependency Scanning** integrated into CI pipelines, enabling early detection of vulnerabilities in both custom code and third-party components.

Deployment

All release artifacts are protected through **Code Signing** and verified during deployment, ensuring **Integrity**, **Authenticity**, and controlled delivery into production environments.

Maintenance

Post-deployment, systems undergo continuous **Monitoring** and structured **Patch Management**, ensuring ongoing alignment with evolving threats and **Security Best Practices**.

2.7.5 Regular Security Audits and Penetration Testing

MyQ maintains robust security validation through systematic testing and assessment programs:

Automated Penetration Testing: Integration with Qualys security platform provides continuous vulnerability assessment and penetration testing for all software releases.

Third-Party Security Assessments: Independent security audits conducted by qualified external organizations to validate security controls and identify potential improvements.

Internal Security Reviews: Regular internal assessments of security policies, procedures, and technical controls to ensure continued effectiveness and compliance.

Vulnerability Response Process: Structured procedures for addressing identified security issues, including timeline requirements for patch development and deployment.

2.7.6 Software Bill of Materials and Vulnerability Management

MyQ implements comprehensive supply chain security through detailed component tracking and vulnerability management:

SBOM Publication: Complete Software Bill of Materials documentation identifying all third-party components, libraries, and dependencies used in MyQ X systems.

Automated Vulnerability Scanning: Continuous monitoring of component databases for newly identified vulnerabilities affecting MyQ X dependencies.

Rapid Patch Management: Systematic process for evaluating, testing, and deploying security updates for third-party components, with prioritization based on risk assessment.

Component Version Control: Detailed tracking of all software components including version numbers, security patch levels, and update schedules as documented in release notes.

Supplier Security Assessment: Evaluation of third-party software suppliers to ensure they maintain appropriate security standards and vulnerability disclosure processes.

This comprehensive compliance framework ensures MyQ X meets diverse regulatory requirements while maintaining the highest standards of information security and data protection across all operational environments.

2.8 Zero Trust Architecture Implementation

MyQ X implements Zero Trust Architecture as a foundational security approach that eliminates implicit trust and continuously validates every transaction. This comprehensive framework ensures that no user, device, or network connection is trusted by default, regardless of their location or previous authentication status.

2.8.1 Zero Trust Principles in Print Management

MyQ X's Zero Trust implementation is built on the principle of **"never trust, always verify"** throughout the entire print management system. The system requires explicit verification for every access request, ensuring that:

Encrypted Communication Channels: All network traffic utilizes mandatory TLS encryption with minimum version 1.2, preventing eavesdropping and tampering during data transmission. HTTPS certificates must be properly configured and validated to prevent man-in-the-middle attacks.

Secure Protocol Enforcement: MyQ X blocks unencrypted HTTP traffic and enforces strong security protocols across all communication channels, including SMTP, LDAP, and SNMP connections. Legacy protocols like SNMPv1 are prohibited in favor of SNMPv3 with strong authentication.

API Security Controls: REST API access requires authentication tokens with IP address filtering, ensuring that API calls are both authenticated and originate from trusted sources. Client secrets undergo periodic rotation to maintain security integrity.

2.8.2 "Never Trust, Always Verify" Methodology

The Zero Trust methodology permeates every aspect of MyQ X operations through continuous verification mechanisms:

Identity Verification: Every user interaction requires authentication, regardless of network location or device trust status. Users must authenticate at each print device, even if they have previously logged in elsewhere in the organization.

Device Authentication: Print devices themselves must authenticate before accessing network resources, with unique credentials and certificates preventing unauthorized device spoofing.

Session Management: User sessions implement automatic timeout and logout functionality, ensuring that abandoned sessions cannot be exploited by unauthorized individuals.

2.8.3 Segmentation and Network Isolation

MyQ X implements comprehensive network segmentation to limit attack surfaces and contain potential security breaches:

Network Boundary Controls: The system enforces strict firewall rules that block unused ports and limit network access to only necessary communication channels. Default configurations disable unnecessary services and protocols.

Certificate-Based Segmentation: MyQ X supports three certificate management modes - Built-in Certificate Authority, Company Certificate Authority, and Manual Certificate Management - allowing organizations to implement appropriate trust boundaries based on their security policies.

FQDN Enforcement: All network communications must use fully qualified domain names (FQDN) rather than IP addresses or single-label names, preventing DNS-based man-in-the-middle attacks and ensuring proper certificate validation.

Port Management: The system automatically manages firewall rules and provides explicit control over which network ports are accessible, reducing the attack surface through systematic port blocking.

2.8.4 Robust Authentication and Verification

MyQ X maintains continuous security validation through multiple authentication layers and real-time monitoring:

Multi-Method Authentication: The system supports diverse authentication methods including LDAP, Microsoft Entra ID, RADIUS, and local MyQ authentication, with automatic failover capabilities ensuring continuous access control.

Authentication Server Integration: Secure integration with external authentication servers uses encrypted connections (TLS for LDAP, secure protocols for RADIUS) and enforces strong shared secrets specific to each MyQ deployment.

Login Monitoring: Enhanced logging of authentication events, particularly failed login attempts, enables administrators to detect and respond to potential security threats. Unsuccessful authentication attempts trigger automatic blocking mechanisms - by default, devices are blocked for 5 minutes after more than 5 invalid attempts within 60 seconds.

Session Persistence Controls: The system implements configurable session timeout policies and automatic logout functionality, ensuring that inactive sessions cannot be exploited.

2.8.5 Device and Endpoint Verification

MyQ X enforces strict device verification protocols to ensure only authorized endpoints can access print resources:

Device Certificate Management: All connected devices must present valid certificates for network communication. The system maintains a comprehensive certificate store with proper chain validation and supports automatic certificate deployment via Group Policy or Mobile Device Management (MDM).

Endpoint Security Controls: Print devices undergo continuous security validation, including SNMP v3 authentication with strong passwords and cryptographic algorithms (SHA1 and AES). Printer credentials are managed through vendor-specific security protocols with randomly generated strong passwords.

Mobile Device Authentication: MyQ X Mobile Client implements OAuth 2.0 Device Authorization Grant for secure mobile device authentication, replacing legacy PIN-based systems with modern biometric-enabled security.

BYOD Security Framework: The system supports Bring-Your-Own-Device (BYOD) environments through secure print propagation via AirPrint and Mopria, maintaining zero-trust principles even in networks with no direct print server visibility.

Access Token Management: Unique access tokens are issued for each device type, with Transport Layer Security (TLS) mandatory for all communications. The system implements Just-in-Time (JIT) access controls that dynamically adjust privileges based on context and continuous risk assessment.

This comprehensive Zero Trust implementation ensures that MyQ X maintains the highest security standards while supporting diverse organizational needs and deployment scenarios. The architecture provides defense-in-depth protection that adapts to evolving threat landscapes while maintaining operational efficiency and user experience.

2.9 Identity and Access Management

MyQ X provides a comprehensive Identity and Access Management framework that integrates seamlessly with existing enterprise authentication systems while supporting modern security standards. The IAM architecture ensures secure, scalable, and flexible user authentication across diverse organizational environments.

2.9.1 Multi-Factor Authentication Implementation

MyQ X implements robust **multi-factor authentication (MFA)** capabilities that significantly enhance security by requiring multiple verification factors:

Embedded Terminal Authentication: Standard MFA methods include ID Card and PIN combinations, where users first present their physical ID card and then confirm

their identity with a PIN code. Alternatively, ID Card and Password authentication provides similar two-factor security with password verification instead of PIN.

Mobile-Based Authentication: The MyQ X Mobile Client enables sophisticated MFA through QR code scanning combined with biometric verification. Users authenticate by scanning a QR code displayed on the embedded terminal, with additional security provided through biometric locks (Face ID or fingerprint) on their mobile devices.

Desktop Client Integration: Organizations using Microsoft 365 services benefit from integrated MFA through Entra ID authentication. Users with two-factor authentication enabled in their Entra ID accounts are automatically prompted to verify their identity using authenticator applications when accessing the Desktop Client.

2.9.2 OAuth 2.0 Device Authorization Grant

MyQ X supports the **OAuth 2.0 Authorization Code Grant** standard, enabling secure integration with modern identity providers and third-party applications:

Standard OAuth Flow: The system implements the complete OAuth 2.0 authorization framework including login page presentation, one-time access code generation, and secure token retrieval. Client applications receive bearer tokens with configurable expiration times and granted scopes.

API Integration Security: OAuth tokens must be provided for all API endpoint access, ensuring that third-party integrations maintain proper authentication. The system supports client ID and client secret validation with secure redirect URI matching.

Token Management: Access tokens include expiration controls (default 1800 seconds) and scope restrictions, providing granular control over API access permissions while maintaining security through token rotation.

2.9.3 Single Sign-On Integration Capabilities

MyQ X provides comprehensive **Single Sign-On (SSO)** integration that streamlines user authentication across enterprise environments:

Microsoft 365 Integration: Deep integration with Microsoft Entra ID enables seamless SSO for organizations using Microsoft 365 services. Users can authenticate using their existing Microsoft credentials, eliminating the need for separate MyQ passwords.

Enterprise Directory Services: SSO capabilities extend to various authentication servers including Active Directory, OpenLDAP, and Novell eDirectory, allowing users to leverage existing enterprise credentials for MyQ access.

Cross-Platform Authentication: SSO functionality works across all MyQ X components including Desktop Client, Mobile Client, and embedded terminals, providing consistent authentication experiences regardless of access method.

2.9.4 Role-Based Access Control (RBAC)

MyQ X implements sophisticated **Role-Based Access Control** that aligns with enterprise security requirements:

Granular Permission Management: The system provides detailed control over user permissions, allowing administrators to define specific access rights based on organizational roles and responsibilities.

Group-Based Administration: RBAC implementation supports both individual user permissions and group-based access control, enabling efficient management of large user populations through security group assignments.

Least Privilege Enforcement: Access controls follow the principle of least privilege, ensuring users receive only the minimum permissions necessary for their job functions while maintaining operational efficiency.

2.9.5 Entra ID Multi-Tenant Support

MyQ X provides robust support for **Microsoft Entra ID multi-tenant environments**:

Cross-Tenant Authentication: The system can authenticate users across multiple Entra ID tenants, supporting complex organizational structures with multiple Azure AD instances.

Tenant Isolation: Multi-tenant support includes proper isolation mechanisms that prevent cross-tenant data access while maintaining centralized MyQ management capabilities.

Hybrid Identity Management: Integration supports both cloud-only and hybrid identity scenarios, accommodating organizations with on-premises Active Directory synchronized to Entra ID.

2.9.6 LDAP and Active Directory Integration

MyQ X offers comprehensive **LDAP and Active Directory integration** capabilities:

Flexible Synchronization Options: The system supports multiple synchronization methods including full synchronization, selective attribute synchronization, and conditional synchronization based on LDAP filters. Administrators can choose between full replacement, add-only, or conditional updates for card and PIN properties.

Advanced Filtering Capabilities: LDAP synchronization includes sophisticated filtering options using standard LDAP filter syntax, enabling selective user import based on organizational units, group memberships, or custom attributes.

Group Structure Import: The system can import complete organizational structures including security groups, distribution groups, and nested group hierarchies from Active Directory, maintaining organizational relationships within MyQ.

Secure Authentication: All LDAP communications utilize TLS encryption to protect credentials and user data during synchronization. The system supports both traditional LDAP over TLS and secure LDAP connections.

2.9.7 Temporary PIN Management and Security Policies

MyQ X implements comprehensive **PIN management and security policies**:

Enhanced PIN Security: Version 10.2 introduces strengthened PIN security including mandatory 6-digit minimum length and prevention of easily guessable combinations such as "1234" or "1111".

Temporary PIN Issuance: The system supports temporary PIN codes that can be issued for specific time periods or single-use scenarios, providing additional security for guest access or temporary employees.

PIN Policy Enforcement: Configurable PIN policies allow organizations to define complexity requirements, expiration periods, and reuse restrictions that align with corporate security standards.

Failed Authentication Protection: Enhanced security includes automatic blocking of authentication attempts after repeated failures (default: 5 minutes blocking after 5 failed attempts within 60 seconds).

2.9.8 Biometric Authentication Support

MyQ X leverages modern **biometric authentication capabilities** through mobile device integration:

Mobile Biometric Integration: The MyQ X Mobile Client supports biometric authentication methods including Face ID on iOS devices and fingerprint recognition on Android devices, providing seamless yet secure access control.

Multi-Modal Authentication: Biometric authentication works in conjunction with device-based security, creating a multi-modal authentication system that combines something the user has (mobile device) with something they are (biometric characteristics).

2.10 Infrastructure Security

MyQ X provides robust infrastructure security that protects the entire print management environment from evolving cyber threats. The platform incorporates multiple layers of defense to safeguard servers, databases, network communication, and software integrity, ensuring operational reliability and data confidentiality.

2.10.1 Print Server Security Hardening

MyQ X print servers are hardened using best practice security configurations defined in the **config.ini** settings, including:

- Restriction of services and processes to limit attack surface.
- Enabling secure communication protocols and disabling legacy insecure options.
- Strict user privilege assignment, avoiding administrator privileges where unnecessary.
- Regular automatic updates and security patching to address newly discovered vulnerabilities.
- Configuration of firewall rules and port restrictions to block unauthorized network traffic.

These measures reduce the risk of exploitation and maintain system availability even under attack conditions.

2.10.2 Database Encryption (Firebird 4.0 Implementation)

MyQ X uses the **Firebird 4.0** database engine, which provides advanced encryption capabilities to protect sensitive data at rest and during backup operations. Key encryption features include:

- AES-256 encryption of database files to prevent unauthorized data access.
- Encrypted storage of passwords and keys within the database system.
- Obfuscation of sensitive database content in logs and diagnostics.

This ensures compliance with data protection regulations and prevents compromise of print job accounting and user information.

2.10.3 TLS 1.2/1.3 Enforcement and Certificate Management

To protect data in transit, MyQ X enforces a minimum **TLS 1.2** protocol by default, with optional upgrade to TLS 1.3 for enhanced security and performance. The platform supports flexible certificate management modes:

- Automatic generation of a private root Certificate Authority (CA) that signs server and client certificates.
- Integration of organization-managed intermediate CAs, allowing corporate trust chains and centralized certificate control.
- Support for manual certificate installation, including third-party/public CA certificates.

Certificates and private keys are securely stored with encrypted protection, and clients receive trusted certificates via Group Policy or Mobile Device Management.

2.10.4 Network Communication Security

MyQ X secures all network communication channels by:

- Blocking all unencrypted HTTP traffic, enforcing HTTPS only.
- Encrypting SMTP, LDAP, and RADIUS traffic using TLS to protect authentication and mail flow.
- Disabling deprecated and vulnerable protocols such as POP3 and STARTTLS replacements.
- Employing SNMPv3 with strong authentication and cryptographic algorithms to securely monitor and manage devices.

These controls prevent eavesdropping, spoofing, and man-in-the-middle attacks across the network.

2.10.5 Firewall Configuration and Port Management

MyQ X reduces attack surfaces by:

- Disabling firewall rules for unused network ports and protocols.
- Allowing granular control of which ports are exposed based on organizational network policies.

This limits ingress points to only those essential for print services, enhancing perimeter defenses.

2.10.6 API Security and Authentication Tokens

APIs enforce multiple layers of security:

- OAuth 2.0 Authorization Code Grant framework secures API access through short-lived bearer tokens and scope restrictions.
- Tokens are validated against client IP addresses and require secure client credentials.
- Periodic secret rotations protect against credential leaks.

This guards API endpoints against unauthorized requests and abuse.

2.10.7 Process Isolation and Sandboxing

MyQ X print management applications run with **process isolation** to prevent compromised components from affecting the entire system. Virtual machine or containerized sandboxing is employed where feasible to contain security breaches and limit lateral movement within the environment.

2.10.8 Code Signing and Integrity Verification

All MyQ software binaries and installers are **code signed** to guarantee authenticity and integrity. This ensures that customers install verified software versions free from tampering or unauthorized modification.

2.11 Data Protection and Encryption

MyQ X implements comprehensive data protection and encryption throughout the entire document lifecycle, ensuring confidentiality and integrity from initial print submission through final output and archival.

2.11.1 End-to-End Encryption Implementation

MyQ X provides **end-to-end encryption** across all communication channels and data storage points:

Encrypted Communication Channels: All network traffic utilizes mandatory TLS encryption with minimum version 1.2 by default. HTTPS is enforced for all web interfaces, server-to-server communication, and client connections.

Certificate-Based Security: Multiple certificate management modes support organizational requirements, from built-in Certificate Authority to corporate PKI integration and public CA certificates. Private keys are protected by randomly generated passwords stored in encrypted form within the Firebird database.

Protocol Security: TLS encryption is enforced across SMTP, LDAP, RADIUS, and SNMP protocols, ensuring no sensitive data is transmitted in clear text.

2.11.2 Data at Rest Encryption

MyQ X protects stored data through multiple encryption layers:

Database Encryption: The Firebird 4.0 database supports encryption using custom certificates with "Encrypting File System" Enhanced Key Usage (EKU). Certificates must be located in designated computer certificate stores, with the Personal store being preferred.

File System Protection: Print and scan job files stored on the MyQ X Print Server can be encrypted using custom certificates provided by administrators, adding an additional layer of protection beyond file system permissions.

Full Disk Encryption: MyQ X supports integration with full disk encryption technologies like Microsoft BitLocker to protect all data at rest on the print server, including the database, certificates, and temporary files.

2.11.3 Data in Transit Protection (TLS Encryption)

MyQ X enforces strict **TLS encryption standards** for all network communication:

Minimum TLS 1.2: Default configuration requires TLS 1.2 minimum, with optional upgrade to TLS 1.3 for enhanced security and performance. Legacy protocols including SSL and older TLS versions are blocked.

Cipher Suite Management: The system implements strong cipher suites and disables vulnerable algorithms to prevent cryptographic attacks. SNMPv3 communications use SHA1 and AES encryption.

Certificate Validation: All TLS connections require proper certificate validation using fully qualified domain names (FQDN) to prevent man-in-the-middle attacks. START TLS is avoided due to MITM vulnerabilities.

2.11.4 Print Job Encryption and Secure Storage

MyQ X provides multiple mechanisms to protect print jobs throughout their lifecycle:

Secure Print Release: Print jobs are stored securely on the MyQ Server until users authenticate at the device, preventing unauthorized access to documents sitting in printer output trays.

Job File Encryption: Administrators can enable job encryption by providing custom certificates, ensuring print job files remain encrypted while stored on the server awaiting release.

Private Queues: For highly confidential documents, private queues automatically delete print jobs immediately after release, eliminating the risk of prolonged unauthorized access.

Privacy Mode: When enabled, privacy mode masks document names from all users except the document owner, preventing information disclosure through job names. Even administrators cannot view job names from other users.

2.11.5 Database Encryption Enhancements

The **Firebird 4.0** database implementation provides advanced encryption capabilities:

Custom Certificate Encryption: Database files are encrypted using certificates with EFS Extended Key Usage, providing strong protection against unauthorized database access.

Password Protection: Database passwords are obfuscated in log files, preventing credential exposure during troubleshooting and monitoring activities.

Permission Hardening: The MyQ data folder, containing the user database and TLS certificate private keys, is restricted to Administrators, SYSTEM, and the MyQ service account only, removing default read access for all users.

2.11.6 Backup Encryption and Secure Storage

MyQ X ensures backups maintain the same security level as production data:

Encrypted Backups: Database backups are protected by secure, randomly generated passwords that prevent unauthorized restoration or access to backup files.

Secure Backup Storage: Backup files should be stored in secured locations with appropriate access controls and encryption at rest to maintain data confidentiality during the backup lifecycle.

2.11.7 Key Management and Rotation Policies

MyQ X implements secure key management practices:

Certificate Rotation: Certificates can be regularly rotated according to organizational security policies, with support for automated deployment via Group Policy or Mobile Device Management.

Private Key Protection: All private keys for certificates and CA operations are protected by randomly generated passwords stored in encrypted form within the database.

API Secret Rotation: REST API client secrets should undergo periodic rotation to maintain security. The system supports secret rollover without service interruption.

2.11.8 Data Minimization and Privacy by Design

MyQ X implements **GDPR-compliant privacy by design principles**:

Limited Data Collection: The system collects only essential metadata required for operational functionality, avoiding unnecessary personal data processing that could increase privacy risks.

Automatic Deletion: Administrators can configure automatic deletion periods for print and scan job files, ensuring data is retained only as long as necessary for business purposes.

User Data Rights: Complete implementation of GDPR user rights including data access, anonymization, and the right to be forgotten, with customizable privacy notices on user interfaces.

Session Management: Automatic logout functionality ensures user sessions are properly terminated, preventing unauthorized access through abandoned sessions.

This comprehensive data protection and encryption framework ensures MyQ X maintains the highest standards of data confidentiality and integrity while supporting regulatory compliance requirements across diverse organizational environments.

2.12 Secure Printing Workflows

MyQ X provides comprehensive secure printing workflows that maintain full user control over document release while preventing sensitive information from being exposed in printer output trays. These workflows are essential for organizations requiring strict document security and user accountability.

2.12.1 Secure Print Release Implementation

Hold Print ensures print jobs are never released immediately to the printer. Documents are stored securely on the MyQ Server and printed only after the authorized user authenticates at the printing device, preventing unattended documents from being left in output trays.

Pull Print extends this further by allowing users to release their jobs on any capable device within the print system, not just the device to which they originally sent the job. This flexibility is particularly valuable during equipment maintenance or when users need to print from different locations.

Multiple Authentication Methods support Secure Print Release including PIN codes, ID cards, passwords, QR codes with biometric verification, and two-factor authentication combinations. This flexibility accommodates diverse organizational security requirements.

2.12.2 Pull Printing Workflows

Pull Print offers significant benefits for both administrators and end users:

Administrative Benefits:

- Eliminate stacks of unattended documents on office printers
- Enforce responsible printing behavior and document security policies
- Manage all printing through a single unified print queue
- Reduce printing waste and associated costs through preview and adjustment options
- Support flexible printing across multiple devices

User Benefits:

- Confidential documents remain secure until explicitly released
- Print to any authorized device in the organization
- Preview documents on the embedded terminal before release
- Modify print options (color, duplex, finishing) even after job submission
- Change print destinations at the device if original printer is unavailable

2.12.3 Print Job Timeout and Automatic Deletion

MyQ X implements automatic cleanup procedures to prevent prolonged document exposure:

Configurable Retention Periods: Administrators define how long print job files are stored on the MyQ Server before automatic deletion, balancing operational requirements with security needs.

Job Timeout Management: Jobs not released within specified timeframes are automatically removed from the hold queue, preventing forgotten or abandoned documents from accumulating on servers.

Automatic Logout: Device sessions automatically timeout after administrator-defined periods, preventing unauthorized document access on abandoned terminals.

2.12.4 Watermarking and Digital Signatures

Watermarking enables document traceability by adding customizable overlays to printed pages that can include:

- Confidentiality designations
- Print dates and timestamps
- Name of the person printing the document
- Printer identification information

These watermarks can be applied to every page or selected pages, creating an audit trail that helps identify leaked documents and trace them to their source.

2.12.5 Job Preview and Content Validation

The **Job Preview** engine enables administrators to review print jobs before release:

Format Support: Preview functionality supports the three most common page description languages - PCL 5, PCL 6, and PostScript.

Preventive Control: Administrators can reject unauthorized print jobs before they reach the printing device, preventing policy violations and protecting sensitive information.

Content-Based Filtering: Integration with OCR and Document Management Systems allows scanning policies to be enforced based on document content analysis.

2.12.6 Error Handling and Secure Job Recovery

MyQ X implements robust error handling to maintain security during device malfunctions:

Device Error Protection: When a printing device enters an error state (paper jam, out of toner), documents are held rather than automatically printing when the error is resolved, maintaining user control over release timing.

Session Preservation: If a device becomes unavailable mid-session, the MyQ system preserves the user session and allows continuation on alternative devices without losing document state.

Automatic Device Logout: When device errors occur, automatic logout clears the device's memory to prevent unauthorized document access by maintenance personnel or other users.

This comprehensive secure printing workflow architecture ensures organizations maintain strict control over document security throughout the entire print lifecycle while supporting operational flexibility and user productivity.

2.13 Device and Network Security

MyQ X provides comprehensive device and network security controls to protect multifunction devices (MFDs), printers, and network infrastructure from unauthorized access and exploitation.

2.13.1 Multi-Function Device Security Hardening

Organizations deploying MyQ X with MFDs should implement security best practices including:

Device Access Controls: Restrict physical access to printers to authorized locations and personnel only, reducing exposure to tampering or theft.

Unused Protocol Disabling: Turn off unnecessary device protocols and services that are not required by MyQ X, reducing the attack surface of each device.

Default Credential Management: Change all default administrator passwords on devices to strong, randomly generated credentials. Factory defaults are commonly known to attackers.

Internal Hard Drive Protection: If devices support internal storage of print jobs for reprinting, implement encryption (AES) and automatic data overwrite features to prevent unauthorized access to stored documents.

2.13.2 Network Segmentation and VLAN Configuration

MyQ X supports network segmentation strategies to contain potential device compromises:

VLAN Isolation: Separate printer and device network traffic from general user and administrative networks using virtual LANs, limiting lateral movement if a device becomes compromised.

Subnetting and Access Control Lists: Implement network-level access controls using Access Control Lists (ACLs) to ensure only authorized systems can communicate with print devices and servers.

Firewall Rules: Block unnecessary inbound and outbound traffic from printer subnets, limiting connectivity to only essential services and preventing infected devices from accessing other network resources.

FQDN Enforcement: All network communications must use fully qualified domain names (FQDN) rather than IP addresses or short hostnames, preventing DNS-based man-in-the-middle attacks and ensuring proper certificate validation.

2.13.3 SNMP v3 Security Implementation

MyQ X enforces modern **SNMPv3** protocols with strong encryption for device management:

Insecure SNMPv1 Prohibition: Legacy SNMPv1 communication must be disabled entirely, as it transmits credentials in clear text and lacks encryption.

SNMPv3 Configuration: All SNMP communication must use SNMPv3 with:

- Strong, randomly generated passwords for authentication
- SHA1 or stronger hashing algorithms
- AES encryption for data confidentiality
- Per-device, unique credentials specific to each MyQ deployment

2.13.4 Printer Credential Management

MyQ X recognizes that **printer credential management is vendor-specific** and requires customer-side implementation:

Strong Password Requirements: All printer administrative credentials must use strong, randomly generated passwords rather than default or simple credentials.

Credential Rotation: Periodically update printer passwords according to organizational security policies to reduce the risk of compromised credentials.

Access Restrictions: Limit printer management access to authorized personnel only through firewall rules, physical access controls, and role-based permissions.

2.13.5 Firmware Security and Update Management

Maintaining current device firmware is critical for security:

Automatic Updates: Configure devices to automatically receive and apply manufacturer firmware updates that address newly discovered security vulnerabilities.

Vendor Security Advisories: Monitor manufacturer security notifications for critical vulnerabilities affecting deployed devices and apply patches promptly.

Update Testing: Test firmware updates in non-production environments before deploying to production printers to ensure compatibility and functionality.

2.13.6 USB Port Management and Restrictions

MyQ X supports administrative controls for device USB connectivity:

USB Port Disabling: Administrators should disable inbound USB ports on MFDs to prevent:

- Direct printing over USB, bypassing MyQ security controls
- Direct access to device hard drives and stored data
- Unauthorized use of device functionality

Secure Direct Print Alternatives: Enable only approved secure printing methods (IPP/S, AirPrint with MyQ integration) while blocking insecure direct USB access.

This comprehensive device and network security framework ensures that print devices remain secure components of the MyQ X infrastructure while maintaining operational efficiency and organizational security posture.

2.14 Audit and Monitoring

MyQ X provides comprehensive audit and monitoring capabilities that enable administrators to maintain visibility over print operations, detect security incidents, and ensure compliance with organizational policies and regulations.

2.14.1 Real-Time Monitoring and Alerting

MyQ X monitors all print infrastructure components in real-time through multiple monitoring channels:

Device Status Monitoring: Continuous monitoring of printer and multifunction device status including toner levels, paper availability, error conditions, and device connectivity. Administrators receive immediate insight into device health and operational status.

Alert Management: Automated alerts notify administrators of critical events including device errors, low supplies, connectivity issues, and other operational problems. Alert notifications can be sent via email or integrated with Windows Event Viewer.

Event Notifications: Customizable event-based notifications trigger actions in response to specific device or system conditions, enabling proactive problem solving before issues impact operations.

2.14.2 Print Activity Logging and Analysis

MyQ X maintains **detailed audit trails of all print, copy, scan, and fax activities**:

Job-Based Accounting: Advanced accounting tracks each job independently, allowing detailed attribution to specific users, devices, projects, and cost centers. Jobs performed during a single user session are separately accounted for, providing precise usage data.

Activity Metadata: Comprehensive logging captures date of job submission, date of job release, device identification, paper format, simplex/duplex settings, color settings, and all other relevant job parameters.

MyQ Log: Real-time system log displays all server activity including system events, errors, warnings, authentication attempts, configuration changes, and administrative actions. Log messages are categorized by severity (Critical, Error, Warning, Info, Notice, Debug, Trace) and filterable by time period and subsystem.

2.14.3 User Behavior Analytics

MyQ X provides sophisticated analytics capabilities to understand printing patterns and detect anomalies:

Custom Report Generation: Advanced reporting capabilities allow administrators to create custom reports based on any combination of tracked parameters, enabling analysis of printing behavior by user, department, project, device, or time period.

Cost Center Tracking: Detailed attribution of print jobs to cost centers, projects, and user groups enables transparent expense reporting and supports informed decisions regarding printing policies.

Behavior Monitoring: Administrators can analyze printing patterns to identify unusual activity, excessive usage, or policy violations that warrant further investigation.

2.14.4 Incident Detection and Response

MyQ X supports security-focused monitoring through structured logging and alerting:

Failed Authentication Logging: Enhanced logging of authentication attempts, particularly failed login attempts, enables administrators to detect and respond to potential security threats. Since version 10.2, login attempt records are improved for easier filtering in the MyQ Log.

Log Notifier Rules: Customizable rules trigger automated notifications based on specific event types, subsystems, and message patterns, enabling rapid detection of

security-relevant events. Rules can use regular expressions to search for specific patterns in log messages.

Critical Event Alerts: System automatically alerts administrators to critical events including security breaches, authentication failures, unauthorized access attempts, and configuration changes.

2.14.5 Log Retention and Archival Policies

MyQ X implements flexible log management to balance operational needs with compliance requirements:

Configurable Retention Periods: Administrators define the number of days before logs are automatically deleted, aligning retention with organizational data governance policies and regulatory requirements.

Log Export and Archival: Logs can be exported in Excel or CSV format for external storage and analysis. Scheduled exports enable automated log archival at regular intervals.

Long-Term Preservation: Exported logs can be stored in secure, encrypted repositories to maintain historical records for audit purposes, compliance verification, and incident investigation.

2.14.6 Advanced Filtering and Search Capabilities

MyQ X provides sophisticated tools for log analysis and investigation:

Saved Searches: Administrators can create, save, and share commonly used search filters for quick access to relevant log data. Saved searches can be organized into folders for easy management.

Time Period Filtering: Filter logs by specific date ranges or predefined periods to focus analysis on relevant timeframes.

Subsystem and Context Filtering: Search by specific MyQ subsystems (Web UI, Terminal, SMTP Server, etc.) and contexts (direct printing, specific devices) to isolate relevant events.

Verbosity Control: Select which log severity levels (Critical, Error, Warning, Info, etc.) are displayed, reducing noise and focusing on significant events.

2.14.7 Audit Log for Administrative Actions

MyQ X tracks all administrative changes through a dedicated **Audit Log**:

Configuration Changes: Records all modifications to MyQ settings, including who made the change, when it was made, and which system component was affected.

User Rights Management: Detailed tracking of changes to user permissions, group memberships, and access controls, with the ability to view detailed information about each change.

PIN and Credential Management: Enhanced tracking of PIN additions, removals, and modifications to monitor credential lifecycle.

Export Capabilities: Audit logs can be exported on-demand or scheduled for regular automated export, supporting compliance reporting and record retention requirements.

This comprehensive audit and monitoring framework ensures MyQ X provides administrators with the visibility needed to maintain security, detect threats, ensure policy compliance, and troubleshoot operational issues effectively.

2.15 Incident Response and Recovery

MyQ X provides comprehensive incident response and recovery capabilities designed to maintain business continuity during both planned and unplanned disruptions. The platform combines automated backup procedures, high-availability features, and flexible failover mechanisms to ensure print services remain operational even during system outages.

2.15.1 Security Incident Response Procedures

MyQ X supports structured incident response through multiple monitoring and alerting mechanisms:

Real-Time Incident Detection: Automated monitoring continuously tracks system health, authentication failures, configuration changes, and security events, enabling rapid detection of potential security incidents.

Alert Escalation: Configurable Log Notifier rules trigger immediate notifications to administrators when critical security events occur, including failed authentication attempts, unauthorized access attempts, and system anomalies.

Audit Trail Preservation: Comprehensive logging of all system activities ensures complete forensic data is available for incident investigation. The MyQ Audit Log tracks all administrative actions, configuration changes, and user activities.

Containment Procedures: In the event of a security incident, administrators can quickly isolate affected components, disable compromised accounts, and implement emergency access controls.

2.15.2 Recovery and Restoration Procedures

MyQ X implements robust backup and restoration capabilities to ensure rapid recovery from system failures or data loss:

Automated Database Backup: Regular automated backups of the MyQ database capture all configuration data, user information, and system settings. Backups are protected with password encryption and stored securely.

Full System Restoration: The restoration process recovers the complete MyQ environment including the database, certificates, configuration files, and reports. Administrators simply select the backup file and provide the password if protected.

Cluster-Aware Backup and Restore: For high-availability deployments using Microsoft Failover Clustering, MyQ supports backup to shared cluster storage and coordinated restoration across all cluster nodes.

2.15.3 High Availability and Failover

MyQ X provides multiple failover strategies to maintain printing operations during server downtime:

Microsoft Failover Clustering Integration: MyQ X deploys in active-passive configurations within Microsoft Windows Server Failover Clusters. The cluster software continuously monitors node health and automatically switches to passive nodes when the active node becomes unavailable.

Fallback Printing: When the MyQ Desktop Client detects lost connection to the server, it automatically redirects print jobs to pre-configured fallback printers. Once server connectivity is restored, job accounting is automatically updated.

Device Spooling: Print jobs can be stored encrypted in device memory during server outages. When connectivity is restored, devices automatically transmit accounting data to the server.

Offline Login: MyQ X embedded terminals cache user authentication credentials, allowing users to log in and access device functionality even when the server is unavailable.

Client Spooling: Jobs are processed locally on user workstations and stored on their computers rather than the server, significantly reducing bandwidth requirements and enabling printing during server maintenance or network issues.

2.15.4 Post-Incident Analysis and Improvement

MyQ X supports continuous improvement of incident response capabilities through comprehensive analysis tools:

Historical Log Analysis: Administrators can review exported logs to understand the sequence of events leading to an incident, identify root causes, and determine appropriate corrective actions.

Audit Trail Review: The Audit Log provides complete visibility into all administrative actions and configuration changes that may have contributed to or preceded security incidents.

Saved Search Patterns: Administrators can create and save search filters within logs for common incident patterns, enabling rapid identification of similar events in the future.

3 MyQ X and NIS2

The Directive (EU) 2022/2555, better known as the **NIS2**, is a significant stride towards establishing a common level of cybersecurity across the European Union. This directive, which came into force on January 16, 2023, aims to bolster the **resilience of essential services** and digital service providers against cyber threats by introducing consistent **cybersecurity standards and practices**.

The printing industry, alongside many others, falls under the scope of the NIS2 Directive. Therefore, entities in the printing industry must understand the implications of the NIS2 Directive and take the necessary steps to meet the security standards. By October 17, 2024, Member States are required to adopt and publish the measures essential for complying with the NIS2 Directive.

This article will explore the details of the NIS2 Directive and its implications for MyQ X distributors and customers.

If you are a MyQ X end customer, discuss the NIS2 Directive requirements and recommendations with your MyQ X provider/distributor. MyQ Partners are trained to deliver top-tier support and will assist you in implementing the necessary measures.

3.1 Main Areas of the NIS2 Directive

3.1.1 Risk Management and Cybersecurity

Adopt a risk management approach to cybersecurity. This includes identifying and assessing risks to network and information systems, implementing measures to mitigate these risks, and regularly reviewing these measures.

Ensure that your server and associated software are **up-to-date with the latest security patches** to mitigate vulnerabilities. Additionally, implement and regularly test backup and disaster recovery plans to ensure the availability and integrity of data. MyQ provides patch releases to its products regularly. It is highly recommended to stay informed, follow these releases, and design your update strategy and procedure ahead of time. MyQ generates a **Software Bill of Materials (SBOM)** for each release, which can be obtained through your MyQ provider/distributor, enabling organizations to analyze the components used in the software for security vulnerabilities.

Network segmentation is an essential tool for implementing a Zero Trust policy in practice. It gives organizations ways to control their networks with more granular security policies. It ensures that even if an attacker compromises one part of the network, they cannot easily move laterally to other areas. However, organizations with segmented environments face challenges in making print readily available.

With MyQ X, print queues can be propagated in segmented networks with Mobile Print Agents, and documents hosted in the cloud can be downloaded and released immediately from the device's screen with Easy Print. Support for Microsoft Universal Print or Application Proxy in the Mobile Client can significantly help organizations with the enablement of print services across their environment while making sure access to such resources is protected.

SSL certificates for secure connections help meet NIS2's requirement for secure data transmission across networks. MyQ X, out-of-the-box, comes with secure communication enabled with the built-in Certificate Authority. Organizations utilizing Enterprise PKI can achieve an even greater level of communication security by providing custom certificates directly.

Whenever possible, **enforce TLS** for communication with other systems. Secure the connection to the Active Directory or other user directories with LDAPS. Ensure that email transmission goes over SMTPS and review all settings on the MyQ X's Network page and the Easy Config's Security tab (e.g., that the Web Server allows only secure connections).

MyQ also provides the ability to **encrypt databases, scans, and print jobs**. Data encryption is vital for ensuring the confidentiality and integrity of sensitive information, which is a key aspect of NIS2 compliance.

For device communication, it is essential to implement communication protocols that provide the highest level of security. Using **SNMPv3** instead of v1 or v2(c) to monitor and manage device status and functionality on a network is strongly recommended.

3.1.2 Business Continuity and Crisis Management

> Organizations must ensure that their operations can continue in the event of a significant disruption.

Implement **redundant servers or failover systems** to ensure that printing services remain available during an incident. MyQ X allows for the implementation of failover measures using several methods.

MyQ supports a **Windows Server Failover Clustering** for high availability, ensuring that services are automatically transferred to a backup node in the event of a failure.

If the connection to the MyQ server is lost, the **Fallback Printing** feature allows users to continue printing via a backup device. MyQ Desktop Client sends print jobs directly to a backup device when server connectivity is down. This guarantees that printing operations can continue uninterrupted during server outages, which is crucial for maintaining business continuity. Similarly, the **Device Spooling** feature supported on selected vendors can be combined with **Offline Login** for offline operation, and further increases the uptime of printing services.

Regular **database backups** and the ability to restore MyQ data comply with NIS2's requirement for ensuring data availability and resilience in the face of cyberattacks or system failures. Database and log backups can be scheduled with MyQ X and performed automatically, including the backups of the Central Server's SQL database.

Read more:

- Overview: High Availability with MyQ X
- Deployment: High Availability, Fallback & Failover

3.1.3 Least-privilege Access Model

> Users should be granted only the minimum level of access or permissions needed to perform required operations.

NIS2 encourages **segregation of duties** to prevent unauthorized access to critical systems.

By assigning **specific rights for access** to system and user management, job management, reporting, or logs, it is possible to grant certain users high-privilege access to particular areas of the MyQ environment, while limiting the access rights of others. Similarly, rights can be assigned per a site server, and thus administrators of a local site server will not gain high-privilege access in other locations and branches of the organization where not desired.

When the administrator utilizes **group-based management** of users (security groups), they can decrease the number of steps needed to configure access rights while still benefiting from user provisioning and de-provisioning. Read more below in the *User Provisioning and Deprovisioning* section.

Granular access permissions should be enforced across the entire organizational infrastructure, including all components within the MyQ X ecosystem. Access should be restricted exclusively to administrators and authorized personnel, ensuring that only those with appropriate privileges can manage and interact with these systems. This involves physical devices, physical servers and their OS (Windows Server), SQL Servers, storage, and more.

Read more:

- Deployment: User Rights

3.1.4 Incident Response and Auditing

> To handle incidents, establish and practice procedures regularly. In case of suspicious activity, restrict or terminate user access to prevent further damage. Proper implementation of these measures can mitigate the impact of unexpected events.

MyQ's **logging and auditing capabilities** (MyQ Logs and MyQ Audit Log) can be extremely useful for incident response and tracking. These logs help detect, investigate, and respond to suspicious activities, which is a mandatory aspect of NIS2.

Logs should be monitored regularly, and notifications enabled for incidents that the organization deems critical. To achieve this, the **Log Notifier** utility built in MyQ X can be configured to monitor events in the MyQ environment and responsible personnel can be notified to take immediate action. Scheduled Tasks running (such as User Synchronization, Printer Discovery, and more) can also send warnings to predetermined contacts. Administrators can also configure MyQ X to send automated alerts when print jobs fail or critical errors occur.

Log management can be centralized by exporting and processing logs through the Windows Event Log and can be further processed by SIEM systems when required. Make sure that the periods for keeping history, log, and audit log are sufficient for your needs. This is configured in **Settings** – **System Management**.

Establishing **strong SLAs** is essential for managed services like MyQ, especially under NIS2 regulations. To guarantee swift incident response times, organizations should consider opting for Premium Support offerings.

Read more:

- Log Settings

3.1.5 Secure Authentication

Secure authentication ensures only authorized users access systems. Two-factor authentication (2FA) enhances this by requiring two types of credentials, increasing security significantly.

Password and PIN requirements, **two-factor authentication** on the Embedded terminals, or the use of Sign in with Microsoft on the Web interfaces or Embedded terminals (with the MyQ X Mobile Client) provide alternatives for securing access to the MyQ X environment.

The MyQ X Mobile Client can be configured to require **biometric verification**, further enhancing the security of the MyQ X user account by requiring an additional factor during authentication to devices.

Implementing user account lockout mechanisms after several failed login attempts enhances security and reduces the risk of brute-force attacks.

Read more:

- Deployment: Secure Authentication[5]
- Deployment: Using Two-Factor Authentication[6]

3.1.6 User Provisioning and Deprovisioning

Provisioning and deprovisioning guarantee that users are promptly denied access to the MyQ environment upon their removal from the source user directory.

MyQ supports **automatic schedule user synchronization** with external systems such as LDAP, Microsoft Entra ID (formerly Azure AD), Google Workspace, and CSV files. This ensures that newly added users are automatically imported into the MyQ X environment without manual input. By regularly syncing user data, MyQ X helps maintain an updated list of users with correct access rights, reducing the risk of unauthorized access.

Group-based management and the use of security groups in the source user directory can assist in **assigning and removing access** automatically to parts of the MyQ X environment for newly provisioned or removed users.

5. https://docs.myq-solution.com/deployment/v1/secure-authentication
6. https://docs.myq-solution.com/deployment/v1/using-two-factor-authentication

MyQ X provides an **automatic registration** feature, allowing users to self-register by sending print jobs, swiping an ID card, or creating an account through the web interface. This feature is particularly useful for environments with frequent external users, like guest employees. Users of the system can be provided with a **temporary PIN** that expires after the set period, ensuring that access is automatically revoked once the user no longer requires access.

MyQ supports the anonymization of user data to comply with privacy regulations. This process irreversibly removes all personal identifiers, making user accounts both unusable and untraceable, while still allowing for system reporting and auditing without compromising privacy.

Read more:

- Deployment: Group-Based User Management

3.1.7 Awareness and Training

NIS2 emphasizes the need for staff awareness and training on cybersecurity practices.

It is recommended you provide training sessions for IT personnel and administrators on the secure management of the MyQ X environment, with an emphasis on NIS2 compliance. The best choice is to consult the management of the MyQ X ecosystem with your provider/distributor. MyQ Partners are trained to provide the highest quality of support.

Additionally, awareness programs should be developed to help end-users identify threats and instruct them on the use of the MyQ X ecosystem, as well as the steps to take in the event of security and other incidents.

Security Whitepaper and Secure Deployment

To learn more about achieving the best security standards with MyQ X, continue to the rest of this guide that covers MyQ X Security (see page 3).

Updated 16/9/2024

4 Software Bill of Materials

A Software Bill of Materials (SBOM) is a detailed record of all the components, dependencies, and libraries included in a software application, whether they are open-source or proprietary. It provides key information such as component names, versions, licenses, and source locations, offering full visibility into the software's supply chain.

SBOMs are used to track and manage software risks by allowing organizations to quickly identify vulnerable or outdated components, ensuring compliance with licensing, and improving overall security. Maintaining an SBOM is especially critical in complex software ecosystems, as it helps streamline vulnerability management and ensures transparency across the software development lifecycle.

By consistently generating, analyzing, and maintaining SBOMs, organizations can better manage software risks and ensure compliance with security and regulatory standards.

BOM (Bill of Materials) formats refer to standardized structures that represent and share the components of a software system. In the Software Bill of Materials (SBOMs) context, these formats provide a machine-readable way to describe software components, their relationships, and metadata. The most widely used SBOM formats include:

- **CycloneDX**: A lightweight and extensible BOM format specifically designed for application security. It provides detailed information about components, licenses, vulnerabilities, and dependencies. CycloneDX is popular for its flexibility and support for automation in security and risk management workflows.

MyQ provides SBOM for the following products:

- MyQ X Central Server 10.2
- MyQ X Print Server 10.2
- MyQ Desktop Client (MDC) 10.2
- Mobile Print Agent (MPA) 1.3
- Optical Character Recognition (OCR) 3.1

To receive the SBOMs from MyQ, contact our support.

5 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[7]
Technical support	support@myq-solution.com[8]
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.

7. mailto:info@myq-solution.com
8. mailto:support@myq-solution.com

Trademarks	“MyQ®”, including its logos, is a registered trademark of MyQ®. Any use of trademarks of MyQ® including its logos without the prior written consent of MyQ® Company is prohibited. The trademark and product name are protected by MyQ® and/or its local affiliates.

myQ X

SAVE TIME WITH PERSONALIZED PRINT SOLUTIONS

MyQ X is an award-winning on-premise or private cloud print management solution trusted by millions of users.

info@myq-solution.com

myq-solution.com

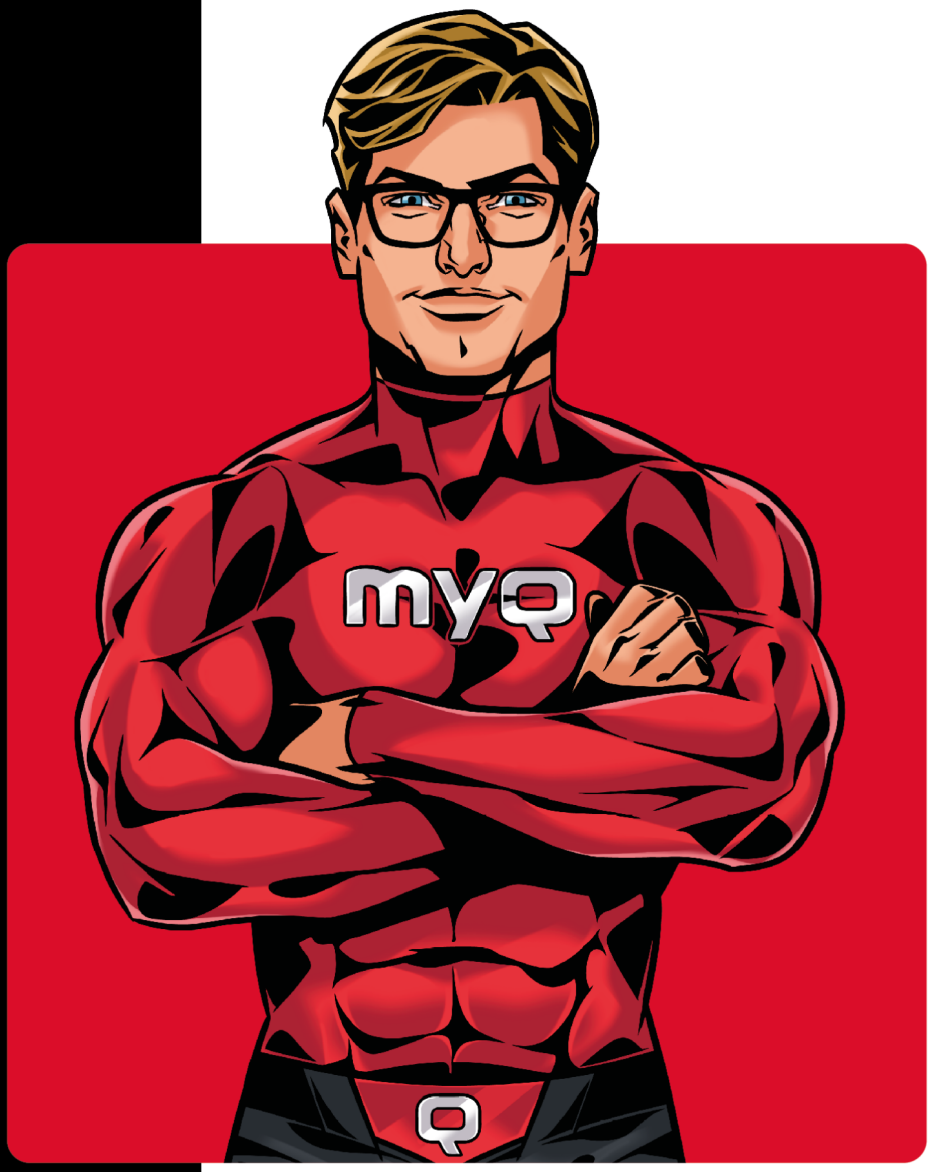
50+ million
Trusted users

1+ million
Active devices

26+
Brands supported

1000+
Certified partners

Operating in **140+** countries



Awarded and certified

BuyersLab PLATINUM TESTED SOLUTION 2023

BuyersLab PLATINUM TESTED SOLUTION 2022

BuyersLab PLATINUM TESTED SOLUTION 2021

ISO 9001 TÜV SÜD ISO 14001 ISO/IEC 27001