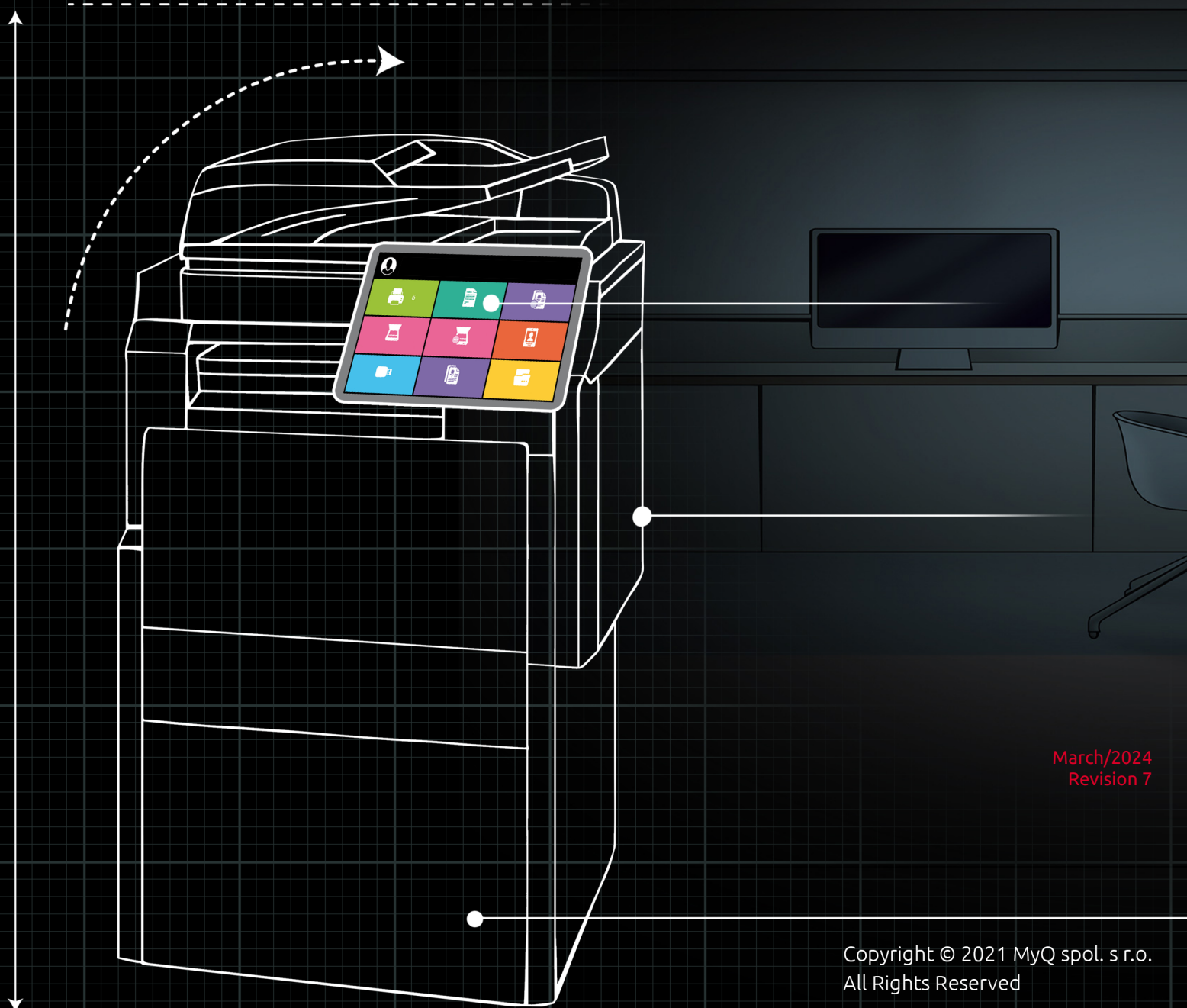


myQ X

MyQ X Secure Deployment



March/2024
Revision 7

Table of Contents


| | | |
|----------|--|-----------|
| 1 | MyQ X Central Server | 5 |
| 1.1 | Default passwords | 5 |
| 1.1.1 | Change server administrator password | 5 |
| 1.1.2 | Change database administrator password | 5 |
| 1.2 | Connection security | 6 |
| 1.2.1 | Configure HTTPS certificate | 6 |
| 1.2.2 | Block unencrypted HTTP traffic..... | 6 |
| 1.2.3 | Encrypt database connections | 7 |
| 1.2.4 | Enforce encrypted LDAP traffic..... | 7 |
| 1.2.5 | Secure SMTP traffic | 8 |
| 1.2.6 | Always use FQDN | 8 |
| 1.2.7 | Secure RADIUS traffic..... | 8 |
| 1.2.8 | Protect REST API keys | 9 |
| 1.3 | Data security | 9 |
| 1.3.1 | Restrict data folder permissions..... | 9 |
| 1.3.2 | Enable database encryption | 10 |
| 1.3.3 | Encrypt backups | 11 |
| 1.3.4 | Enable disk encryption..... | 11 |
| 1.4 | Additional recommendations | 11 |
| 1.4.1 | Deploy RBAC | 11 |
| 1.4.2 | Configure a custom service account | 12 |
| 1.4.3 | Keep the server updated | 13 |
| 1.4.4 | Keep the OS secure | 13 |
| 1.4.5 | Plan for disaster recovery | 13 |
| 2 | MyQ X Print Server | 14 |
| 2.1 | PS Default passwords..... | 14 |
| 2.1.1 | Change server administrator password | 14 |
| 2.1.2 | Change database administrator password | 14 |
| 2.2 | PS Connection security | 15 |
| 2.2.1 | Configure HTTPS certificate | 15 |
| 2.2.2 | Block unencrypted HTTP traffic..... | 16 |
| 2.2.3 | Block unused ports | 16 |
| 2.2.4 | Encrypt connections to MyQ Central Server | 16 |
| 2.2.5 | Use strong passwords for server-to-server authentication | 16 |
| 2.2.6 | Secure SMTP traffic | 17 |
| 2.2.7 | Use strong and unique RADIUS passwords..... | 17 |
| 2.2.8 | Encrypt LDAP traffic..... | 18 |
| 2.2.9 | Secure SNMP traffic..... | 18 |
| 2.2.10 | Secure printer credentials..... | 19 |
| 2.2.11 | Always use FQDN | 20 |

| | | |
|--------|---|-----------|
| 2.2.12 | Protect REST API keys | 20 |
| 2.3 | PS Data security..... | 20 |
| 2.3.1 | Restrict data folder permissions..... | 20 |
| 2.3.2 | Enable database encryption | 21 |
| 2.3.3 | Encrypt backups | 22 |
| 2.3.4 | Enable disk encryption..... | 22 |
| 2.4 | PS Additional recommendations | 23 |
| 2.4.1 | Deploy RBAC | 23 |
| 2.4.2 | Configure a custom service account | 23 |
| 2.4.3 | Keep the server updated..... | 24 |
| 2.4.4 | Keep the OS secure | 24 |
| 2.4.5 | Plan for disaster recovery | 24 |
| 3 | MyQ X Desktop Client..... | 25 |
| 3.1 | Secure communication..... | 25 |
| 3.1.1 | Encrypt communication with MyQ Print Server | 25 |
| 3.1.2 | Provide HTTPS links with FQDN..... | 25 |

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](#) for the End of Maintenance announcements and successor components.

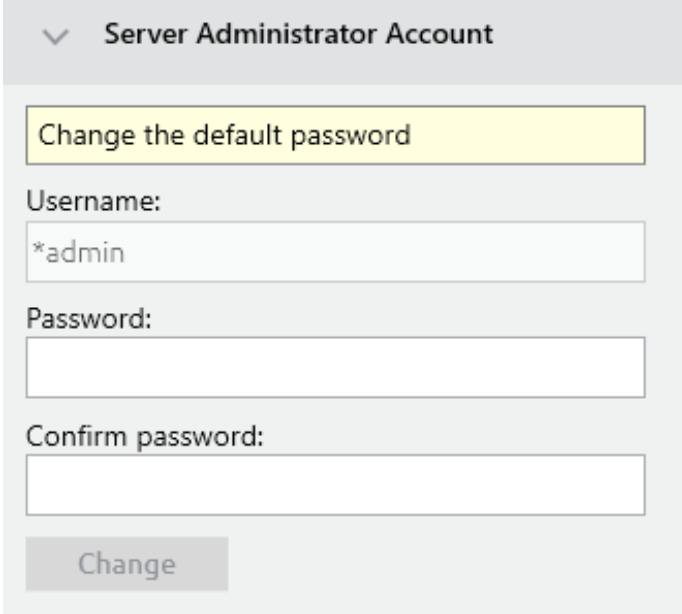
 This guide was prepared along with Mainstream Technologies, now [Seyfor](#), during regular independent security audits.

1 MyQ X Central Server

1.1 Default passwords

1.1.1 Change server administrator password

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



Server Administrator Account

Change the default password

Username:
*admin

Password:

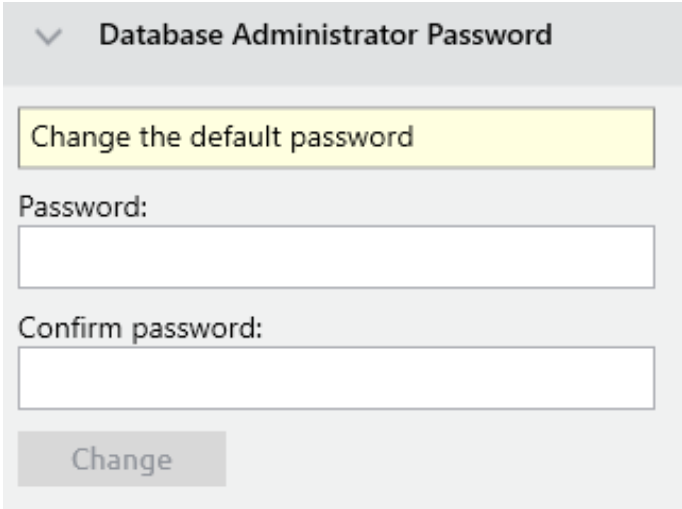
Confirm password:

Change

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

1.1.2 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:



Database Administrator Password

Change the default password

Password:

Confirm password:

Change

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.

1.2 Connection security

1.2.1 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:

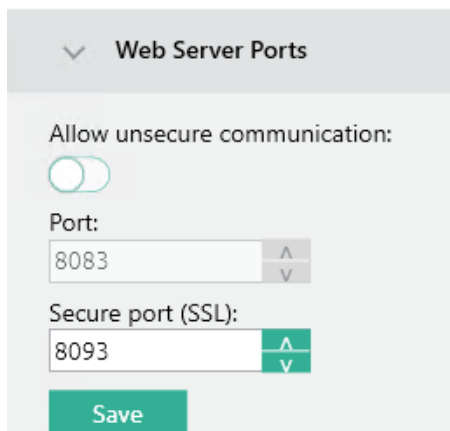
The certificate is physically stored in the "C:\ProgramData\MyQ Central Server\Cert" directory in the following files:

- 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.

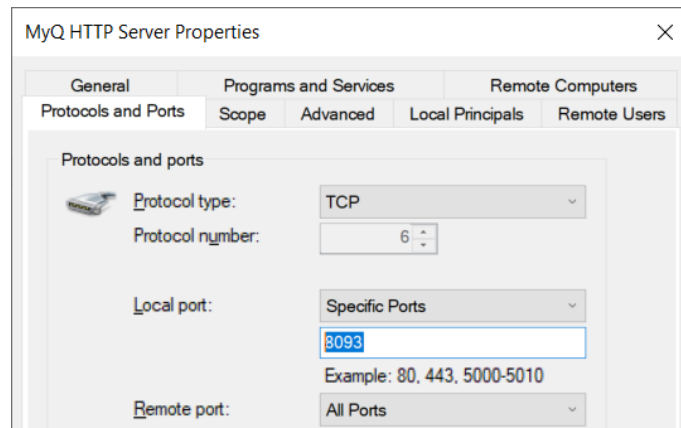
1.2.2 Block unencrypted HTTP traffic

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



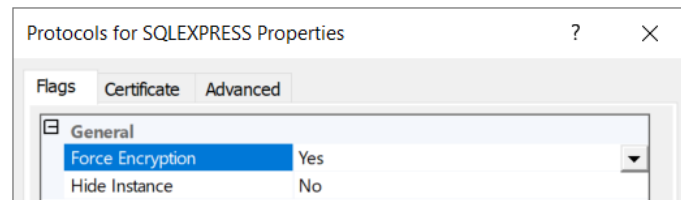
The screenshot shows the 'Web Server Ports' configuration window. It features a toggle switch for 'Allow unsecure communication' which is currently turned off. Below this, there are two input fields: 'Port:' with a value of 8083 and 'Secure port (SSL):' with a value of 8093. Each input field has up and down arrow buttons for navigation. A green 'Save' button is located at the bottom of the configuration area.

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

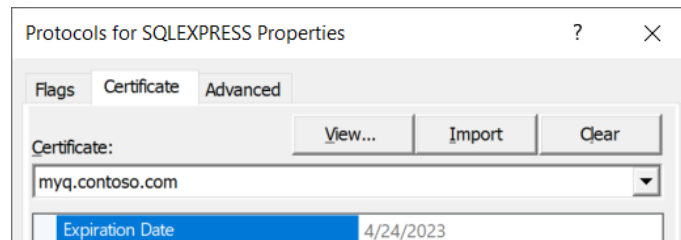


1.2.3 Encrypt database connections

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

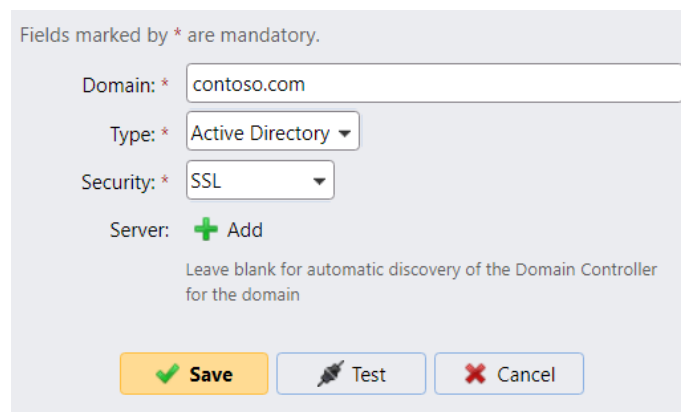


A certificate issued by a trusted CA should also be configured on the SQL Server:



1.2.4 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).

1.2.5 Secure SMTP traffic

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

▼ Outgoing SMTP server

Type: Classic SMTP Server
 Microsoft Exchange Online
 Gmail

Server: *

Port: *

Security: ▼

Validate certificate:

User:

Password:

Sender email: *

1.2.6 Always use FQDN

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

▼ Custom help

Title:

Link:

The link is displayed on the user's MyQ Central Server home page

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

1.2.7 Secure RADIUS traffic

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

Name: *

Server: * Address* 1812 Shared secret*

+ Add

Save Test Cancel

1.2.8 Protect REST API keys

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

REST API applications

Fields marked by * are mandatory.

Title: *

Client ID: * 9E21B9E6-17E3-40BF-9544-0B1DAD22B5E3

Secret: * b0a68e07de27804c681d0a9bcb5ffc82598b5aef

Scope:

OK Cancel

1.3 Data security

1.3.1 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:

▼ Data Folder

Path: [C:\ProgramData\MyQ Central Server\](#)

Size: 2.21 MB

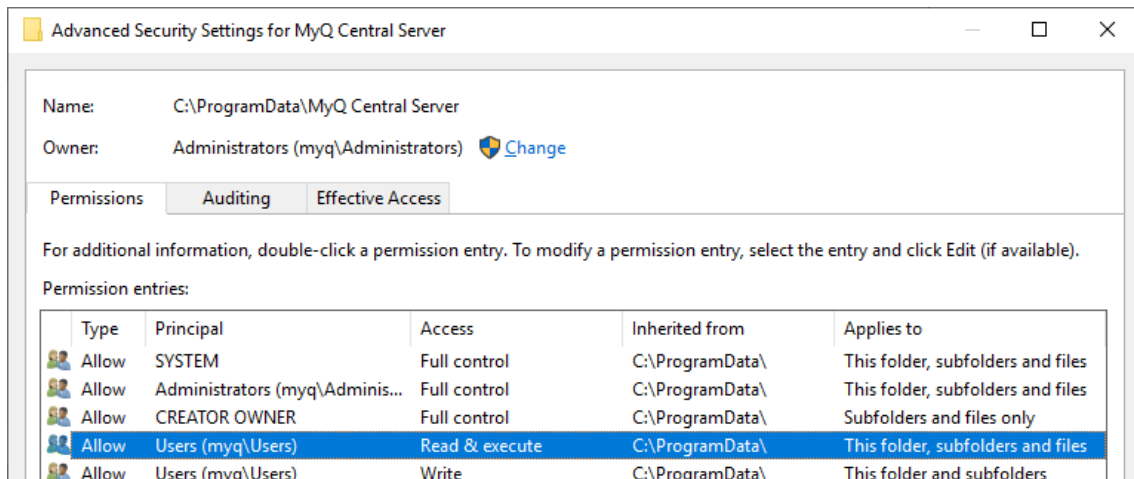
Free space: 107.45 GB

Total space: 126.51 GB

Files count: 10

Change location

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
```

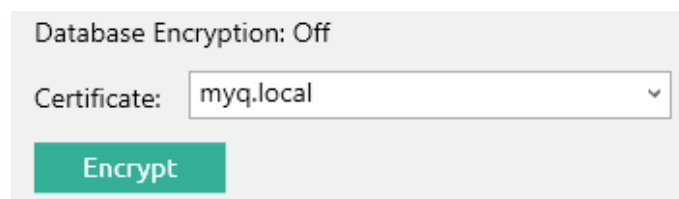
```
sc sidtype FirebirdServerMasterInstance unrestricted
```

```
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"
/inheritance:r /Q
```

1.3.2 Enable database encryption

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



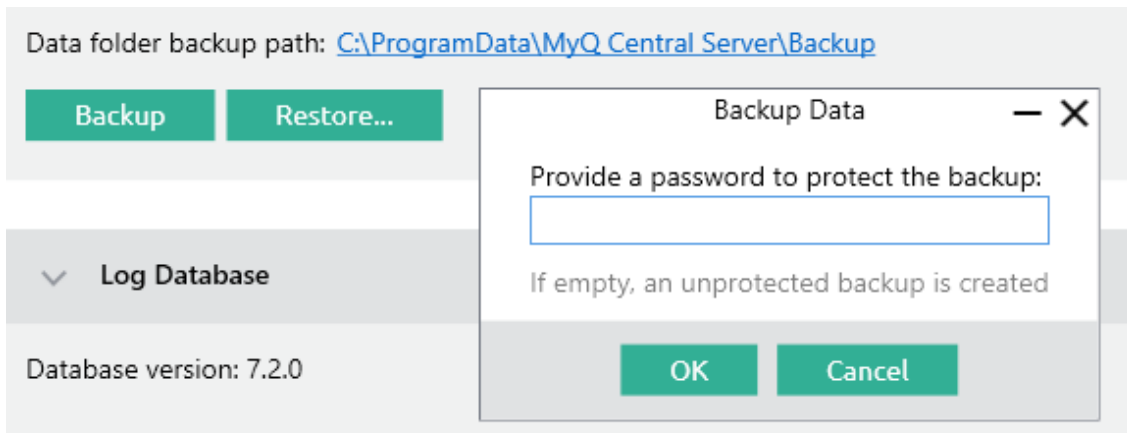
The certificate needs to have the "Encrypting File System" Enhanced Key Usage (EKU) and it must be located in one of the following computer certificate stores:

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

The Personal store is the preferred one.

1.3.3 Encrypt backups

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





1.3.4 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:

Windows (C:) BitLocker on

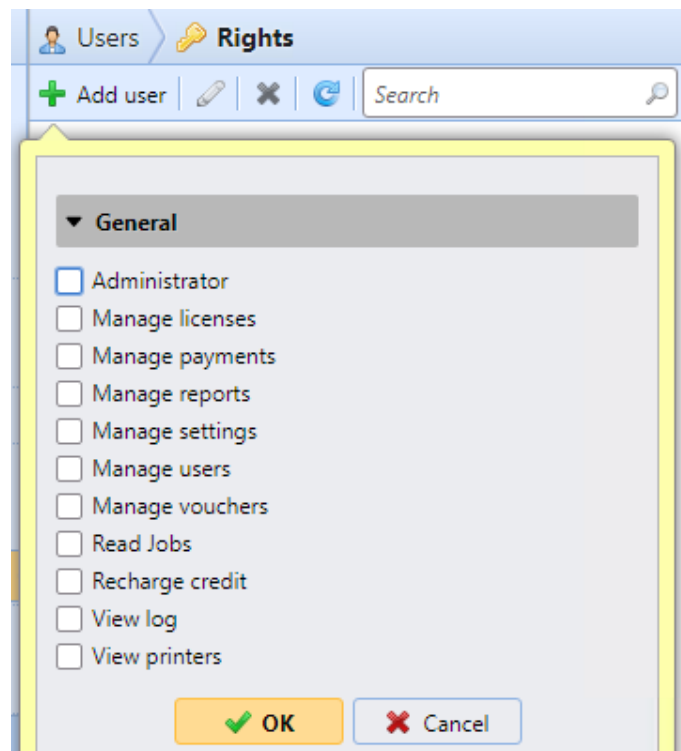


-  Suspend protection
-  Back up your recovery key

1.4 Additional recommendations

1.4.1 Deploy RBAC

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



1.4.2 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:

Log on services as:

Local System account

Custom account

Account:

[Browse...](#)

The account must have the "Log on as a service" user right.

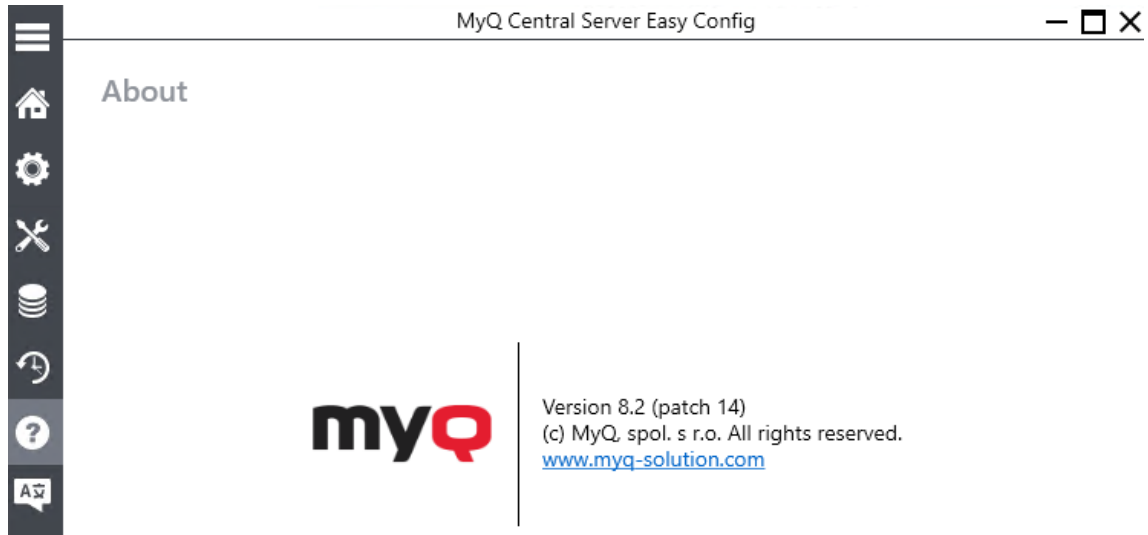
Password:

Confirm password:

[Save](#)

1.4.3 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:



1.4.4 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.

1.4.5 Plan for disaster recovery

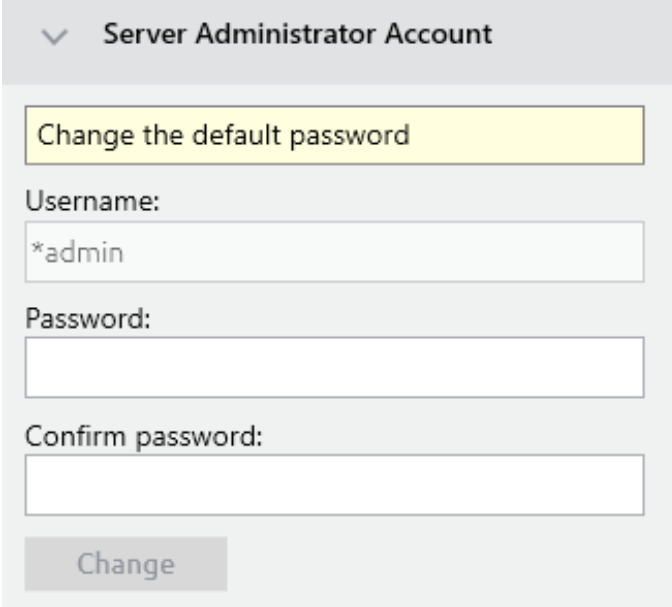
Periodically create backups of the MyQ Central Server, including the database, certificates, and configuration files. Test the recovery procedure at least once.

2 MyQ X Print Server

2.1 PS Default passwords

2.1.1 Change server administrator password

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



Server Administrator Account

Change the default password

Username:
*admin

Password:

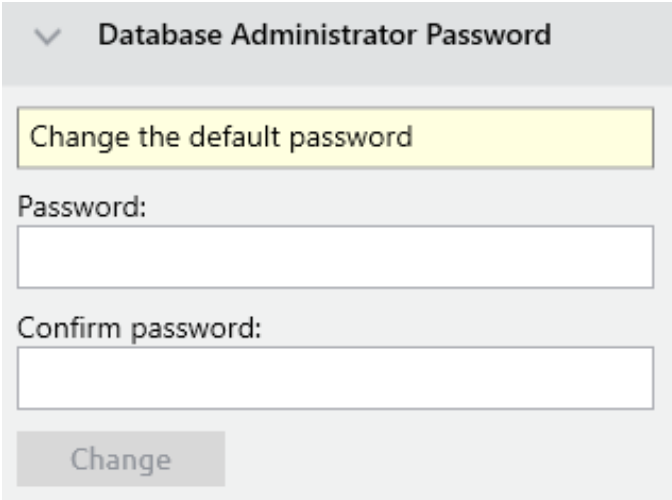
Confirm password:

Change

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

2.1.2 Change database administrator password

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



Database Administrator Password

Change the default password

Password:

Confirm password:

Change

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

2.2 PS Connection security

2.2.1 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:

Built-in Certificate Authority
Server and clients are secured by certificates generated by the built-in certificate authority (CA). The CA certificate is self-signed. Export the CA certificate and install it to clients so they trust MyQ Server. If the CA certificate is compromised, generate a new one. Server certificate will be regenerated automatically.

Company Certificate Authority
Your company CA generates an intermediate CA certificate which MyQ uses to sign certificates for the server and clients. To generate an intermediate CA certificate create Certificate Signing Request (CSR), sign it by your CA and finish CSR by importing signed certificate. Server certificate will be regenerated automatically.

CA certificate:

Manual Certificate Management
Provide a certificate for the MyQ Server. MyQ creates no certificates, all certificates are managed by you.

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.

2.2.2 Block unencrypted HTTP traffic

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

Web Server

Allow unsecure communication:

Enable only in case of communication problems.

Port:

8090

Save

2.2.3 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 |

2.2.4 Encrypt connections to MyQ Central Server

Only use HTTPS to connect to MyQ Central Server:

Central Server address: * myq-central.contoso.com

Enable secure connection:

Port: * 8093

2.2.5 Use strong passwords for server-to-server authentication

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

Password for communication: *

Password is used for communication between Central server and Site servers.

2.2.6 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.

▼ MyQ SMTP Server

SMTP (STARTTLS):
Enable when using unsecure communication or secure communication over STARTTLS.

SMTPS (SSL/TLS): *
Enable when using secure communication over SSL/TLS protocol.

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

Method: MyQ SMTP Server
 POP3
 IMAP

Enter an email box for receiving jobs. The box will be emptied automatically.

Type: Classic SMTP Server
 Microsoft Exchange Online

Security: *

Server: *

Port: *

User:

Password:

Polling interval: * seconds

2.2.7 Use strong and unique RADIUS passwords

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

Name: *

Server: *

Add

Save Test Cancel

2.2.8 Encrypt LDAP traffic

TLS encryption should be used to secure all LDAP traffic:

Fields marked by * are mandatory.

Domain: *

Type: *

Security: *

Server: Add

Leave blank for automatic discovery of the Domain Controller for the domain

Save Test Cancel

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).

2.2.9 Secure SNMP traffic

Insecure SNMPv1 communication with devices should be avoided:

| Default | Name | SNMP version | Parameters |
|---------|----------|--------------|--|
| | SNMP v1 | v1 | SNMP read community: ***** SNMP write community: ***** SNMP port: 161 |
| | SNMP v2c | v2c | SNMP read community: ***** SNMP write community: ***** SNMP port: 161 |
| ✓ | SNMP v3 | v3 | Security name: MyQ Authentication protocol: SHA1 Authentication password: ***** SNMP port: 161 Privacy protocol: AES128 Privacy password: ***** Context: |

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

Authentication

Protocol: * SHA1

Security name: MyQ

Password:

Privacy

SNMP port: * 161

Protocol: * AES128

Password:

Context:

Save Test Cancel

2.2.10 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:

Printer Credentials

These credentials are used to configure the printer. You can override these defaults in the properties of each printer.

Administrator user name:

Administrator password:

2.2.11 Always use FQDN

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

This server hostname: *

Terminals, MyQ Desktop Client and other components use this hostname when communicating with the server. It must match the certificate.

2.2.12 Protect REST API keys

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

REST API applications ✕

Fields marked by * are mandatory.

Title: *

Client ID: *

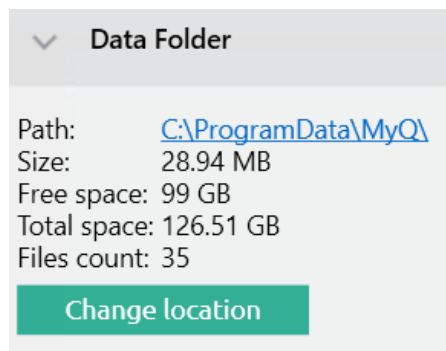
Secret: *

Scope:

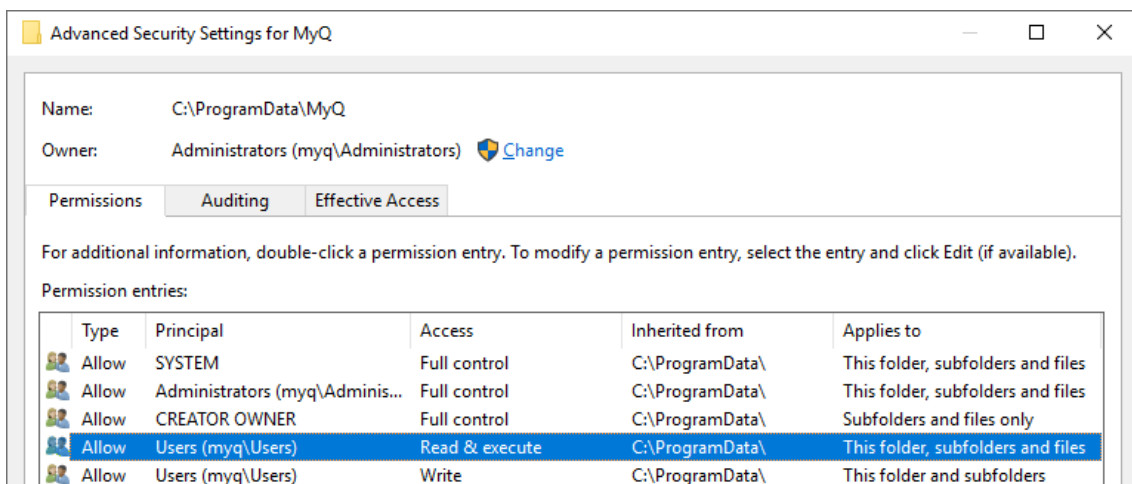
2.3 PS Data security

2.3.1 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\Apache:(OI)(CI)M" /grant "NT SERVICE\traefik:(OI)(CI)M" /

inheritance:r

/Q

2.3.2 Enable database encryption

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

Main Database
 Database version: 28.2.51
 Database Encryption: Off
 Certificate:
 Encrypt

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.

2.3.3 Encrypt backups

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

Backup Data
 Provide a password to protect the backup:

 If empty, an unprotected backup is created
 OK Cancel

2.3.4 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:

Windows (C:) BitLocker on

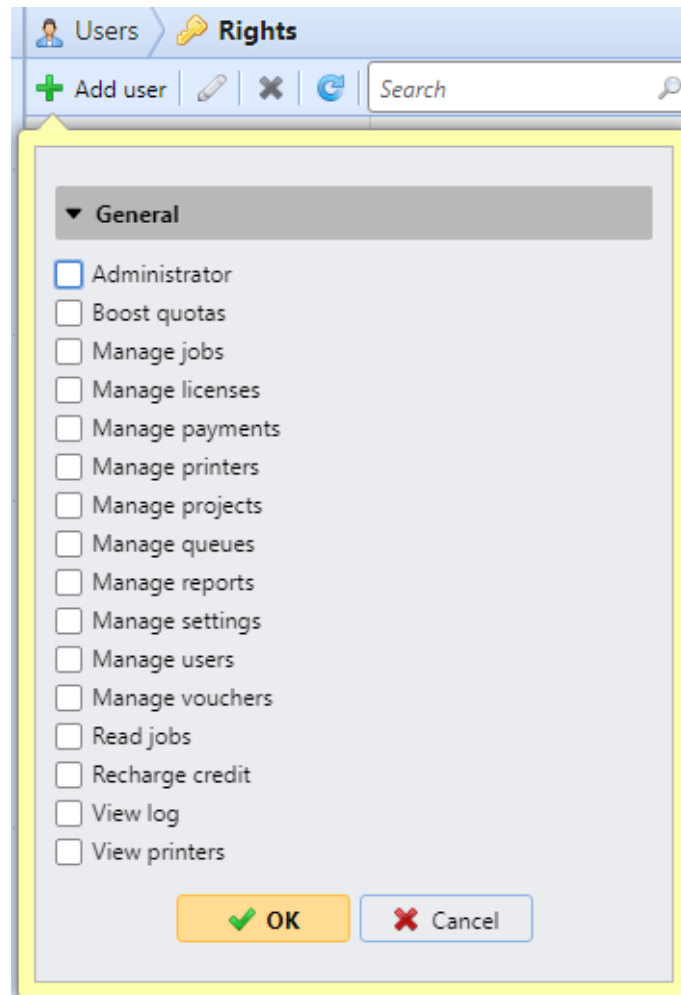


- Suspend protection
- Back up your recovery key

2.4 PS Additional recommendations

2.4.1 Deploy RBAC

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



2.4.2 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:

Log on services as:

Local System account

Custom account

Account:

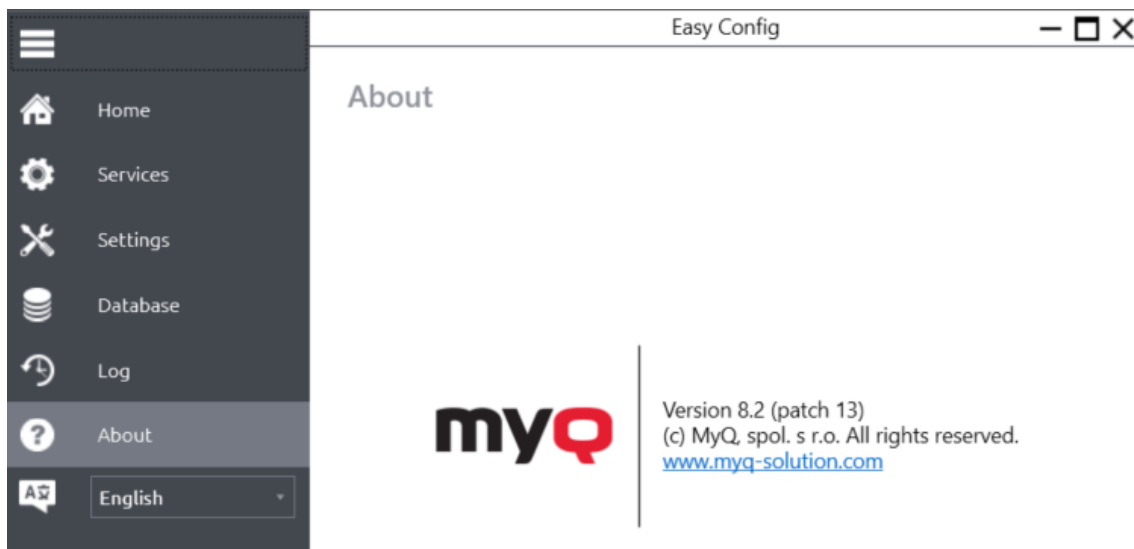
The account must have the "Log on as a service" user right.

Password:

Confirm password:

2.4.3 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:



2.4.4 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.

2.4.5 Plan for disaster recovery

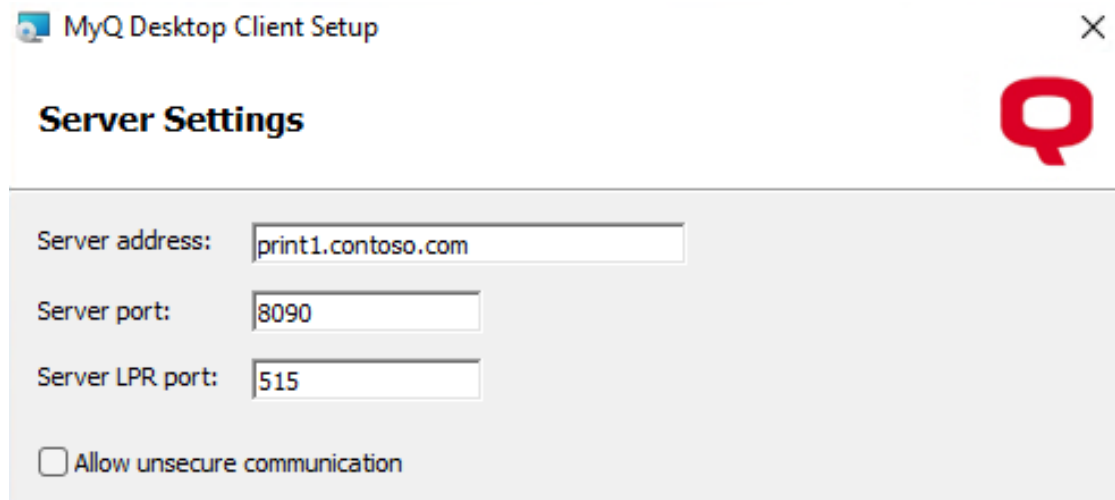
Periodically create backups of the MyQ Print Server, including the database, certificates, and configuration files. Test the recovery procedure at least once.

3 MyQ X Desktop Client

3.1 Secure communication

3.1.1 Encrypt communication with MyQ Print Server

MyQ X Desktop Client (MDC) is configured to use TLS encryption when communicating with MyQ Print server by default. Do not change this default behavior:



3.1.2 Provide HTTPS links with FQDN

When configuring custom links for MyQ Desktop Client, always use the server's DNS name prefixed with HTTPS, in order to prevent MITM attacks:

▼ Custom help

The link is displayed on the user's MyQ home page

Title:

Link:

▼ Custom link in the MyQ Desktop Client.

The link is displayed in the MyQ Desktop Client. It can be a weblink, a network path or a local path.

Title:

Link: