MyQ X Sicherheit 1.0

Generiert aus docs.myq-solution.com
August/2026

DEUTSCH

Hinweis zur Übersetzung

Diese Übersetzung wurde mithilfe künstlicher Intelligenz erstellt. Bei Abweichungen oder Unklarheiten ist das englischsprachige Quelldokument maßgeblich.

Inhaltsverzeichnis

Sicherheit hat **bei MyQ** seit jeher **höchste Priorität**. In diesem Abschnitt finden Sie einen Leitfaden zur sicheren Bereitstellung von MyQ X sowie das MyQ X-Sicherheits-Whitepaper:

- Sichere Bereitstellung (see page 5)
- Sicherheits-Whitepaper (see page 33)

1 Sichere Bereitstellung von MyQ X

Die Vertraulichkeit von Kundendaten und **die Sicherheit** der Kunden hatten **für MyQ** schon immer **oberste Priorität**. **Die Sicherheit ist** jedoch **eine gemeinsame Verantwortung von Anbietern und Kunden.** Obwohl das Ziel von MyQ X darin besteht, standardmäßig eine sichere Konfiguration bereitzustellen, erfordern einige Bereiche zusätzliche Maßnahmen seitens des Kunden. Dazu gehören unter anderem die Zertifikatsverwaltung, die Verwendung sicherer Anmeldedaten, die Vertretung von Berechtigungen und die Konfiguration der Firewall.

Dieses Dokument enthält umsetzbare Checklisten für die sichere Bereitstellung von MyQ X Central Server und MyQ X Print Server in Unternehmensumgebungen. Wir sind der festen Überzeugung, dass die Befolgung dieser Richtlinien die Angriffsfläche jeder Druckverwaltungsinfrastruktur erheblich verringert. Es versteht sich von selbst, dass MyQ X-Serveranwendungen nur so sicher sind wie die zugrunde liegenden Betriebssysteme und Netzwerkumgebungen. Da die Windows-Sicherheit ein eigenständiges Thema ist, wird sie in diesem Dokument nicht behandelt.

MyQ X-Systeme werden gemäß der MyQ Secure Development Lifecycle-Richtlinie ständig verbessert und gepatcht. Bitte stellen Sie sicher, dass Sie **immer die neueste unterstützte Version verwenden**. Die Versionshinweise finden Sie in jedem Produktleitfaden. Informationen zu Wartungsende und Nachfolgekomponenten finden Sie auch in der End-of-Life-Richtlinie (EOL)[1].

> Dieses Handbuch wurde zusammen mit Mainstream Technologies, jetzt Seyfor[2], im Rahmen regelmäßiger unabhängiger Sicherheitsaudits erstellt.

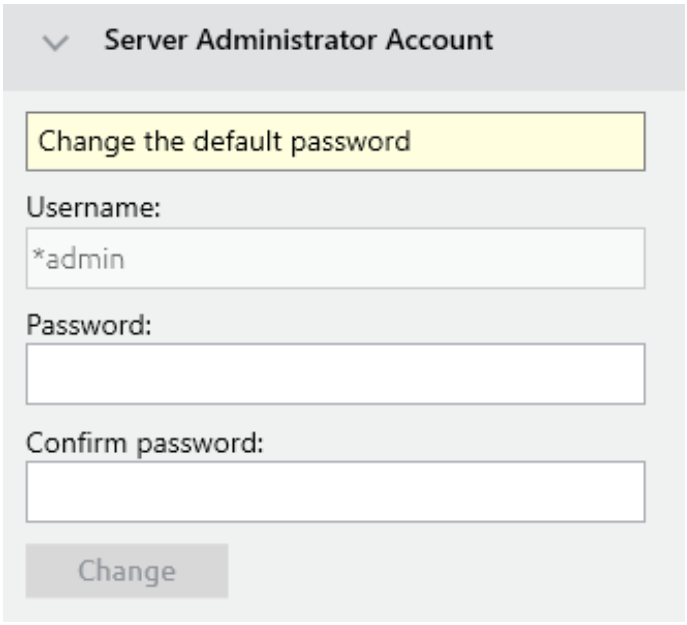
1.1 MyQ X Central Server

1.1.1 Standardpasswörter

Server-Administratorpasswort ändern

Einer der ersten Schritte sollte die Änderung des Standard-Administratorpassworts sein, das lautet: *1234*.

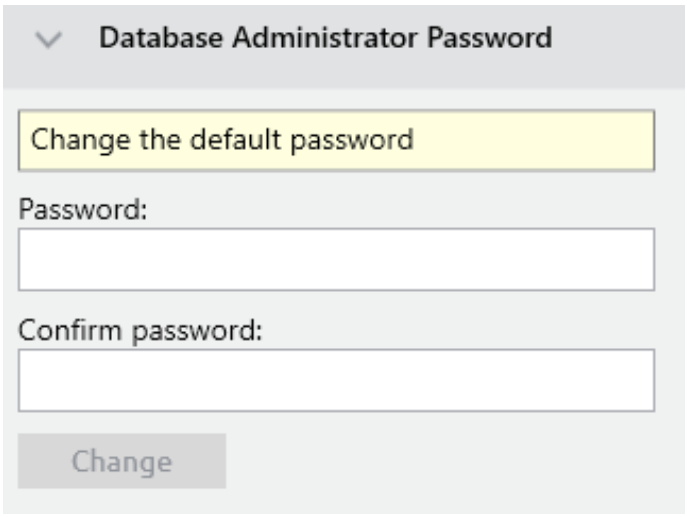
1. https://www.myq-solution.com/en/product-support-end-of-life-policy
2. http://www.seyfor.cz



Das Passwort wird in der Datenbank in gehashter Form gespeichert.

Ändern des Datenbankadministrator-Passworts

Falls die interne Firebird-Datenbank verwendet wird, ändern Sie das Standardpasswort, das von MyQ Central Server zur Authentifizierung verwendet wird:



Dieses Passwort wird in verschlüsselter Form in der Datei „C:\ProgramData\MyQ Central Server\setup.ini" gespeichert und ist standardmäßig auf *„masterkey*" gesetzt.

1.1.2 Sicherheit der Verbindung

HTTPS-Zertifikat konfigurieren

Für den MyQ Central Server sollte ein benutzerdefiniertes Zertifikat konfiguriert werden, das von allen Client-Computern als vertrauenswürdig eingestuft wird und den DNS-Namen des Servers enthält:

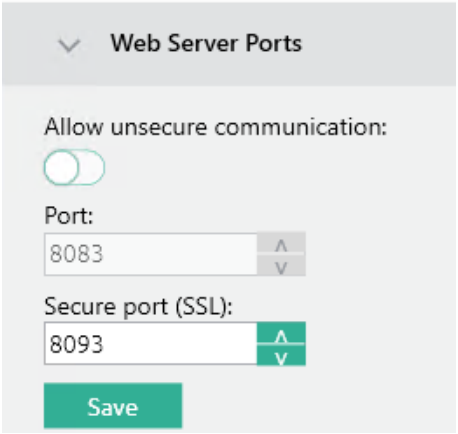
Das Zertifikat wird physisch im Verzeichnis „C:\ProgramData\MyQ Central Server\Cert" in den folgenden Dateien gespeichert:

- server.pfx – Zertifikat mit öffentlichen und privaten Schlüsseln
- server.cer – Zertifikat mit dem öffentlichen Schlüssel
- server.key – privater Schlüssel

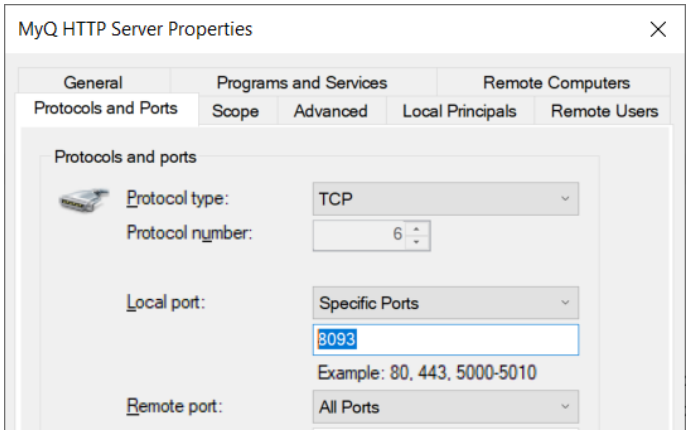
Von der Verwendung von Wildcard-Zertifikaten wird abgeraten, da sie bei Diebstahl ein viel höheres Sicherheitsrisiko darstellen.

Unverschlüsselten HTTP-Datenverkehr blockieren

Unverschlüsselter HTTP-Datenverkehr sollte in der Konfiguration des Central Server nicht aktiviert sein:

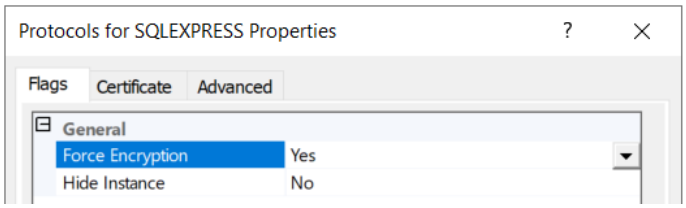


Die hostbasierte Firewall sollte ebenfalls so konfiguriert werden, dass nur HTTPS-Datenverkehr zugelassen wird:

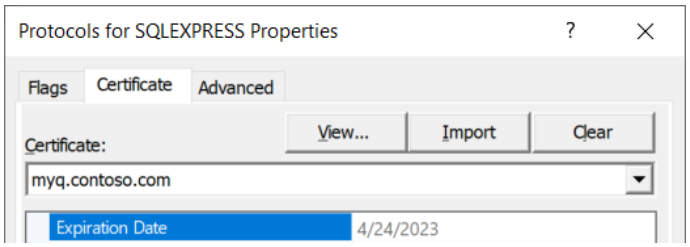


Datenbankverbindungen verschlüsseln

Wenn Microsoft SQL Server zum Speichern der MyQ-Datenbank verwendet wird, stellen Sie sicher, dass die TLS-Verschlüsselung über den SQL Server-Konfigurationsmanager erzwungen wird:

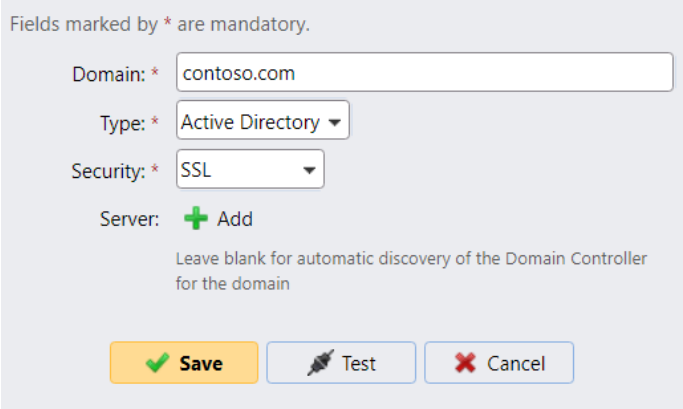


Ein von einer vertrauenswürdigen Zertifizierungsstelle ausgestelltes Zertifikat sollte ebenfalls auf dem SQL Server konfiguriert werden:



Verschlüsselten LDAP-Datenverkehr erzwingen

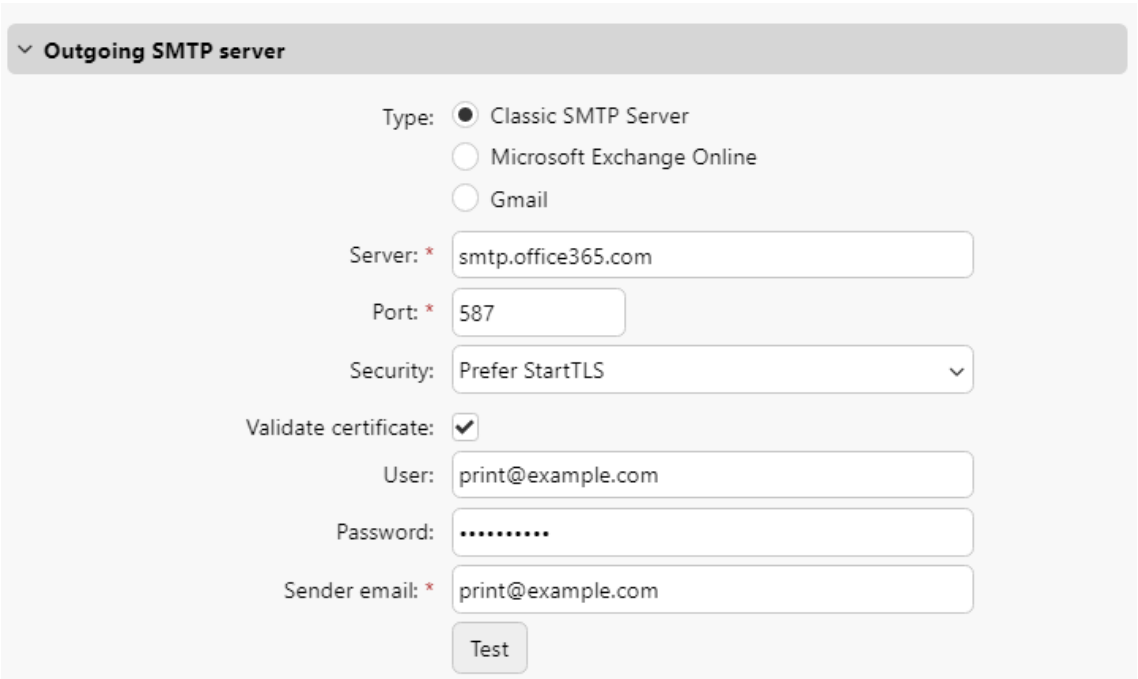
Wenn die Synchronisierung von Benutzerkonten über das LDAP-Protokoll verwendet wird, stellen Sie die Verbindungssicherheit auf SSL ein:



Verwenden Sie aus Sicherheitsgründen nicht START TLS, da es anfällig für MITM-Angriffe ist. Auf allen LDAP-Servern (Active Directory-Domänencontroller) muss ein von einer vertrauenswürdigen Zertifizierungsstelle ausgestelltes Zertifikat konfiguriert sein.

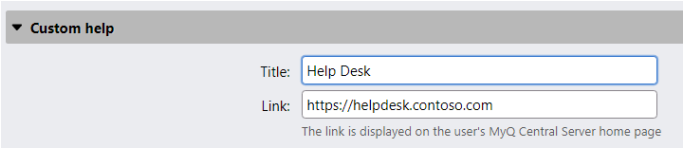
Sichern Sie den SMTP-Datenverkehr

Wenn ein SMTP-Server in MyQ Central Server konfiguriert ist, erzwingen Sie die Verwendung von TLS mit Zertifikatsvalidierung:



Verwenden Sie immer FQDN

Um MITM-Angriffe zu verhindern, verwenden Sie in allen Konfigurationsfenstern ausschließlich vollqualifizierte Domänennamen:



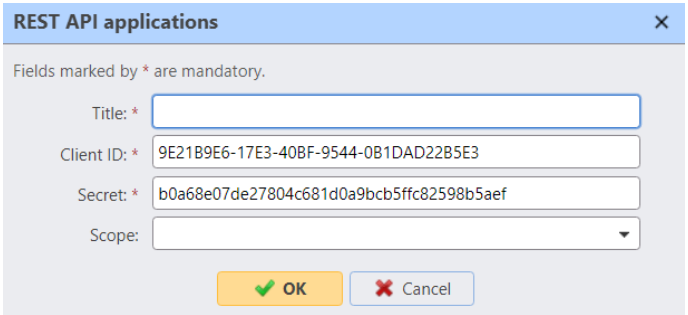
Kontaktieren Sie Server niemals, indem Sie nur IP-Adressen oder Namen mit einem einzigen Label eingeben.

Sicherer RADIUS-Datenverkehr

Wenn die RADIUS-Authentifizierung verwendet wird, generieren Sie immer starke gemeinsame Geheimnisse, die spezifisch für den MyQ Central Server sind:

Schützen Sie REST-API-Schlüssel

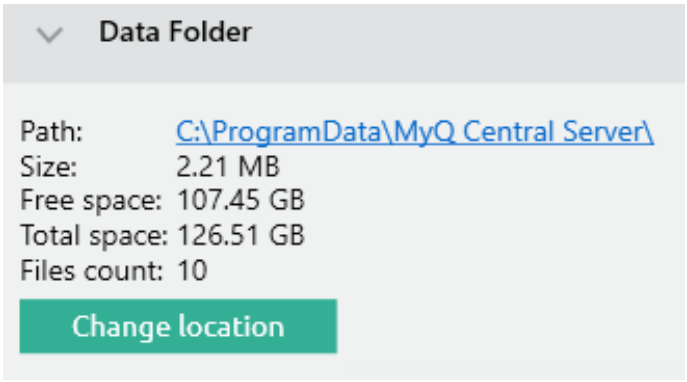
Wenn REST-APIs verwendet werden, schützen Sie die Client-Geheimnisse vor unnötiger Offenlegung und führen Sie regelmäßig eine Geheimniserneuerung durch:



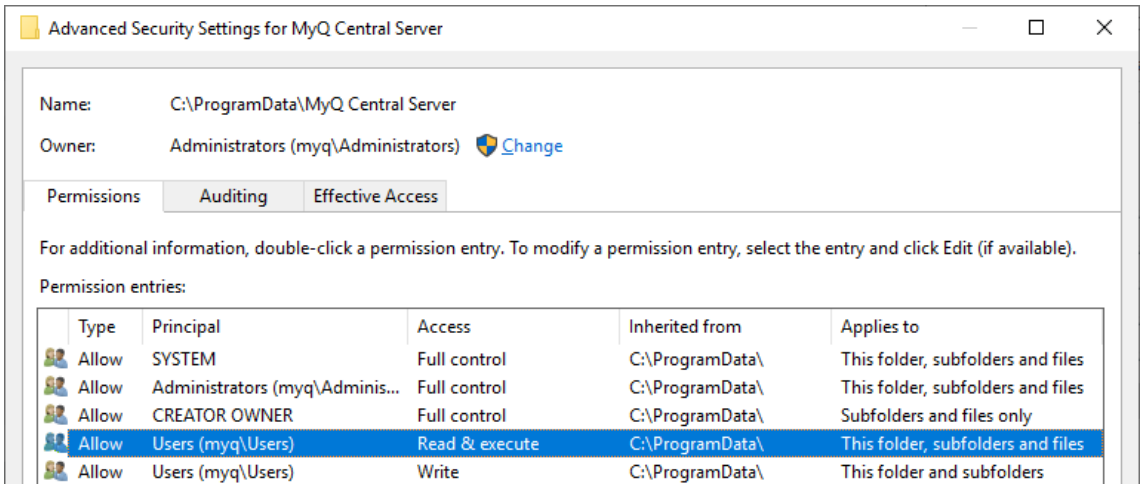
1.1.3 Sicherheit der Daten

Berechtigungen für den Datenordner einschränken

Der Datenordner von MyQ Central Server enthält hochsensible Daten, darunter die Benutzerdatenbank und den privaten Schlüssel des TLS-Zertifikats. Sein aktueller Speicherort wird in der Anwendung „MyQ Central Server Easy Config“ angezeigt:



Alle Benutzer (lokal/Domäne) verfügen standardmäßig über Lesezugriff:



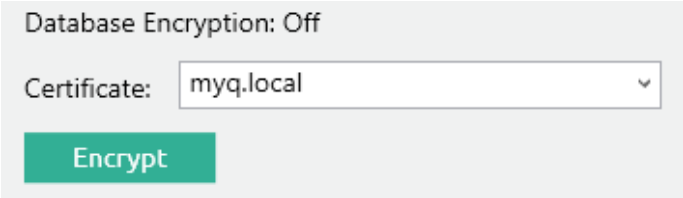
Nur Administratoren, das SYSTEM-Konto und das MyQ-Dienstkonto sollten Zugriff auf dieses Verzeichnis haben. Hier ist ein Beispiel für ein Batch-Skript, das zur Absicherung der Berechtigungen verwendet werden kann:

```
@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" ^
  /grant "NT SERVICE\traefik:(OI)(CI)M" ^
  /inheritance:r ^
  /Q
```

Datenbankverschlüsselung aktivieren

Wenn Sie die integrierte Datenbank verwenden, verschlüsseln Sie diese stets mit einem benutzerdefinierten Zertifikat, um das Risiko von Datenlecks zu verringern:



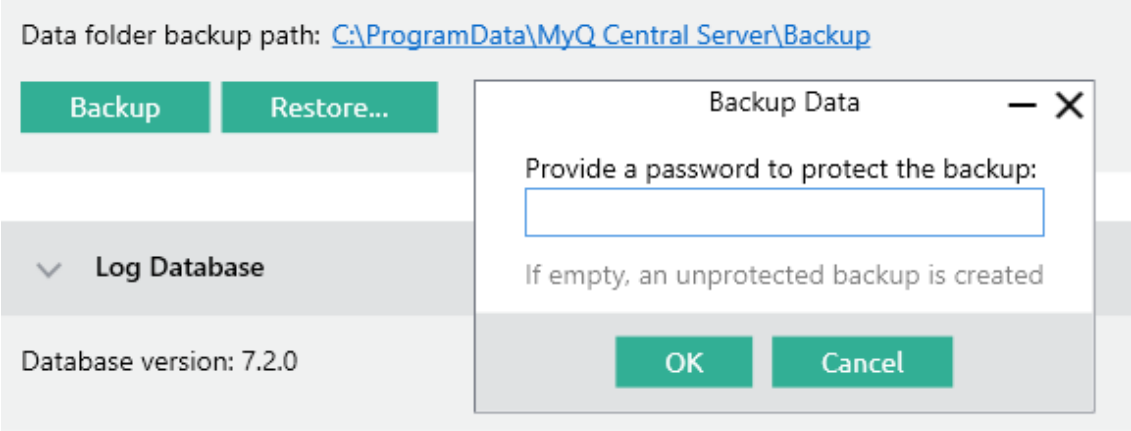
Das Zertifikat muss die erweiterte Schlüsselverwendung (EKU) „Encrypting File System“ aufweisen und sich in einem der folgenden Zertifikatsspeicher des Computers befinden:

- „Persönlich“
- Vertrauenswürdige Herausgeber
- Stammzertifizierungsstellen von Drittanbietern
- Andere Personen

Der Speicher „Persönlich“ wird bevorzugt.

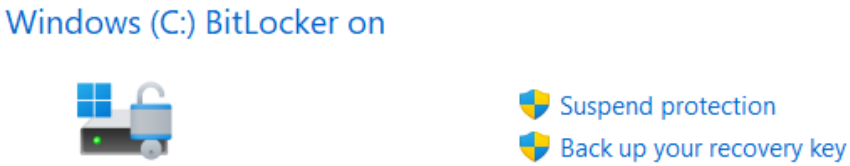
Sicherungen verschlüsseln

Datenbanksicherungen sollten durch sichere, zufällig generierte Passwörter geschützt werden:



Festplattenverschlüsselung aktivieren

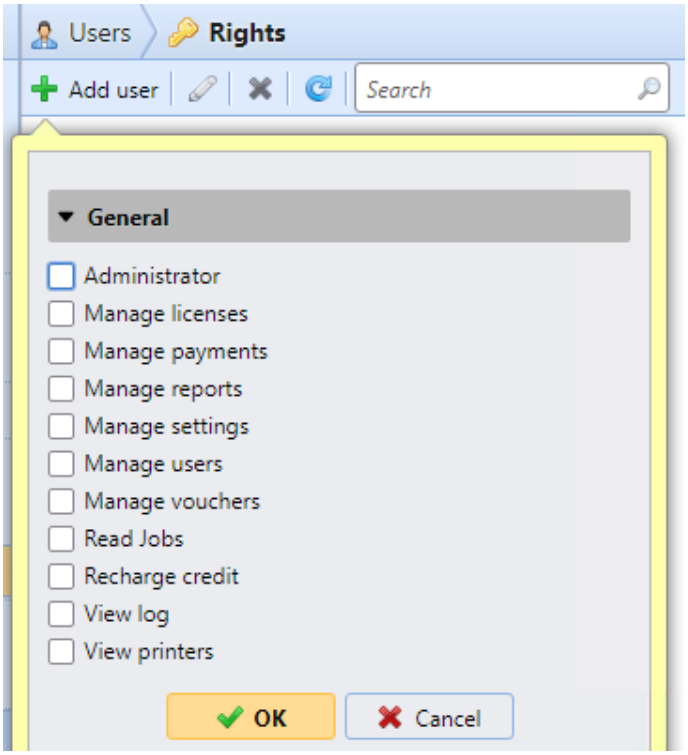
Wenn möglich, sollte auf dem MyQ Central Server eine Technologie zur vollständigen Festplattenverschlüsselung wie Microsoft BitLocker aktiviert werden, um die ruhenden Daten zu schützen:



1.1.4 Zusätzliche Empfehlungen

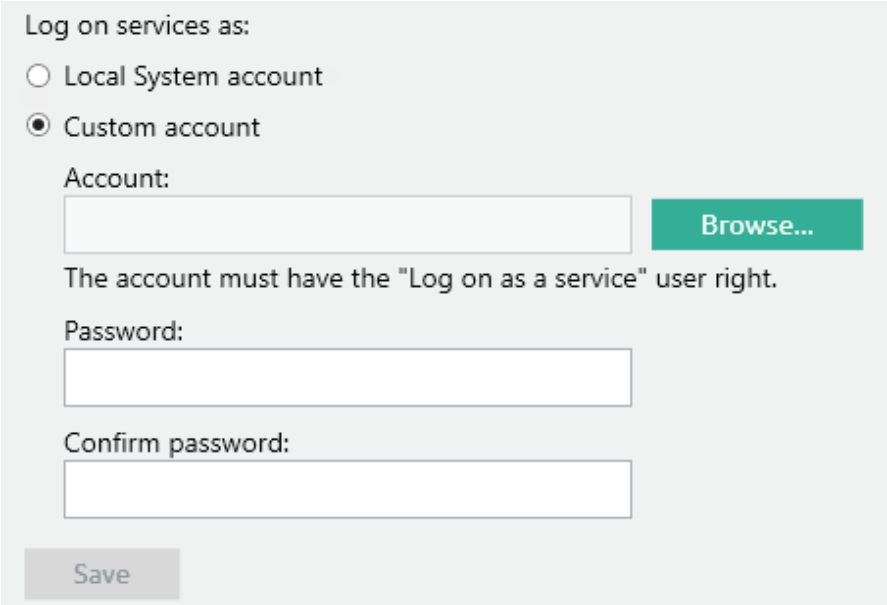
RBAC bereitstellen

Verwenden Sie das Standardkonto *admin nicht für reguläre Vorgänge. Verwenden Sie stattdessen die Vertretung von Berechtigungen und wenden Sie dabei das Prinzip der geringsten Berechtigungen an:



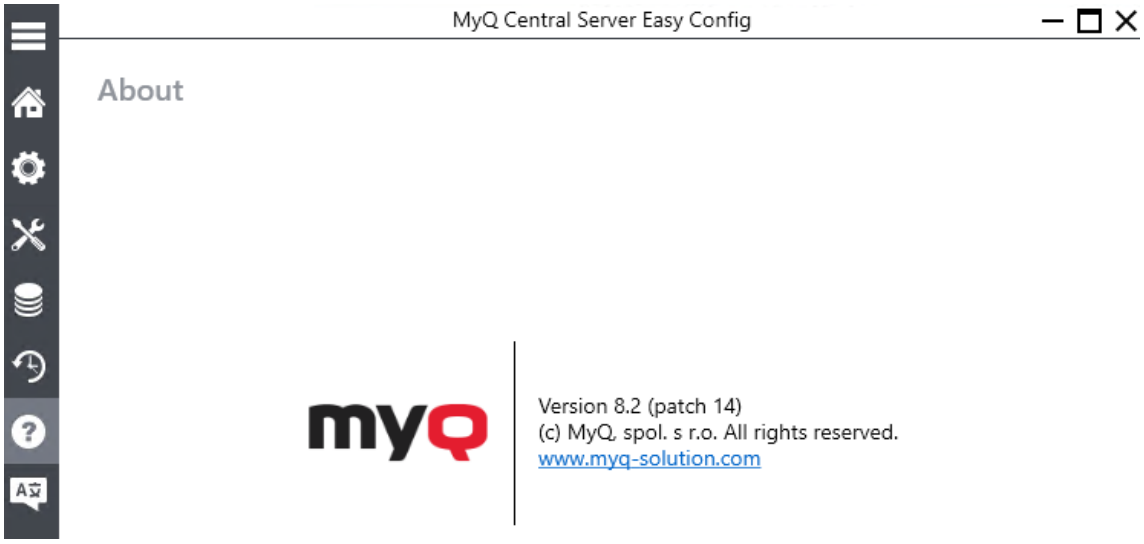
Konfigurieren Sie ein benutzerdefiniertes Dienstkonto

MyQ Central Server wird standardmäßig unter dem hochprivilegierten SYSTEM-Konto ausgeführt. Konfigurieren Sie stattdessen ein benutzerdefiniertes Dienstkonto mit einem starken Passwort:



Halten Sie den Server auf dem neuesten Stand

Installieren Sie die von MyQ bereitgestellten Sicherheitsupdates, sobald sie verfügbar sind. Sie können die aktuell installierte Anwendungsversion in MyQ Central Server Easy Config überprüfen:



Halten Sie das Betriebssystem sicher

MyQ Central Server ist nur so sicher wie das zugrunde liegende Betriebssystem. Halten Sie es auf dem neuesten Stand und wenden Sie die von Microsoft empfohlenen Sicherheitsrichtlinien an.

Aktualisieren Sie Ihre Software regelmäßig, um Sicherheitslücken zu schließen und die Leistung zu verbessern. Eine Liste der Anforderungen und Empfehlungen finden Sie unter Systemanforderungen.

Beispielsweise muss .NET entweder mit Verwaltungstools oder über Windows Updates auf Opt-in-Basis[3] aktualisiert werden.

Planen Sie die Notfallwiederherstellung

Erstellen Sie regelmäßig Backups des Central Server, einschließlich der Datenbank, Zertifikate und Konfigurationsdateien. Testen Sie das Wiederherstellungsverfahren mindestens einmal.

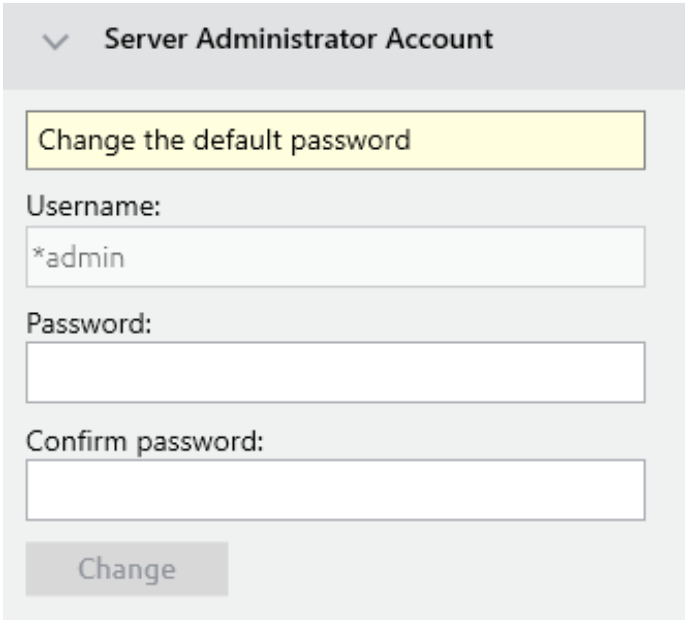
3. https://devblogs.microsoft.com/dotnet/server-operating-systems-auto-updates/

1.2 MyQ X Print Server

1.2.1 PS Standardpasswörter

Server-Administratorpasswort ändern

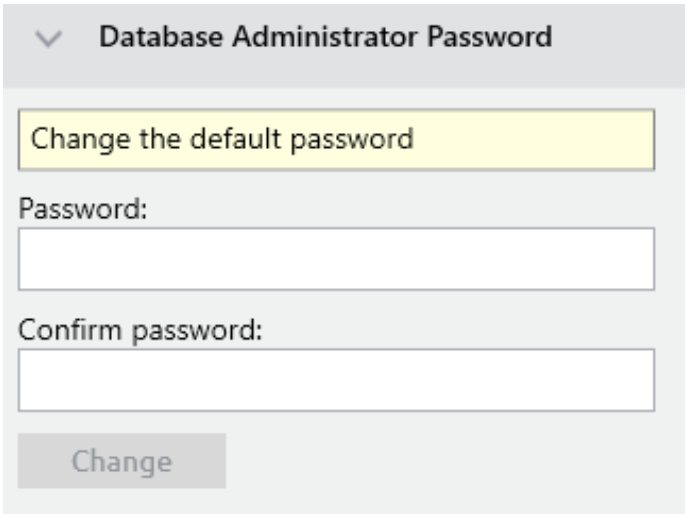
Einer der ersten Schritte sollte die Änderung des Standard-Administratorpassworts sein, das lautet: *1234*.



Das Passwort wird in der Datenbank in gehashter Form gespeichert.

Ändern des Datenbankadministrator-Passworts

Ändern Sie das Standardpasswort, das vom MyQ Print Server zur Authentifizierung gegenüber der internen Firebird-Datenbank verwendet wird:

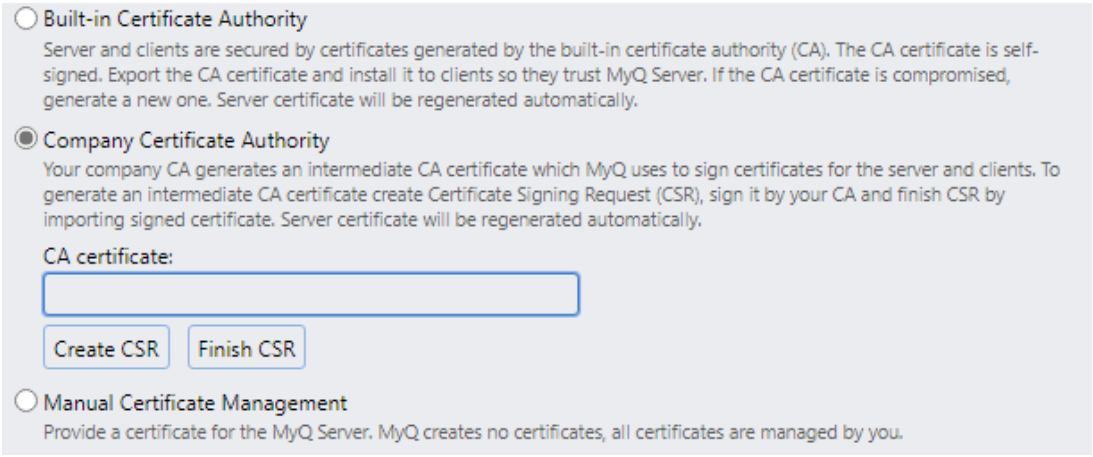


Dieses Passwort wird in verschlüsselter Form in der Datei „C:\ProgramData\MyQ\setup.ini“ gespeichert und ist standardmäßig auf „*masterkey*“ gesetzt.

1.2.2 PS Sicherheit der Verbindung

HTTPS-Zertifikat konfigurieren

Für den MyQ Print Server sollte ein benutzerdefiniertes Zertifikat konfiguriert werden, dem alle Client-Computer vertrauen. Es stehen drei Modi der Zertifikatsverwaltung zur Verfügung:



Standardmäßig erstellt MyQ Print Server ein eigenes Stamm-CA-Zertifikat und verwendet dieses zum Signieren von Server- und Client-Zertifikaten. Der öffentliche

Teil dieses Zertifikats kann exportiert und im Trust Store für Client-Zertifikate bereitgestellt werden, z. B. mithilfe von Gruppenrichtlinien oder MDM.

Unternehmen, deren eigene PKI bereits als vertrauenswürdig eingestuft ist, bevorzugen möglicherweise die zweite Option. MyQ Print Server verwendet eine eigene Zwischen-CA zur Ausstellung von Server- und Client-Zertifikaten. Das automatisch generierte Zwischen-CA-Zertifikat muss von der CA des Unternehmens signiert werden, damit es von den Clients als vertrauenswürdig eingestuft wird.

Wenn die Sicherheitsrichtlinie des Unternehmens die Installation eines Zwischen-CA-Zertifikats auf dem MyQ Print Server nicht zulässt oder ein von einer öffentlichen Zertifizierungsstelle ausgestelltes Zertifikat verwendet werden soll, muss stattdessen die manuelle Zertifikatsverwaltung verwendet werden.

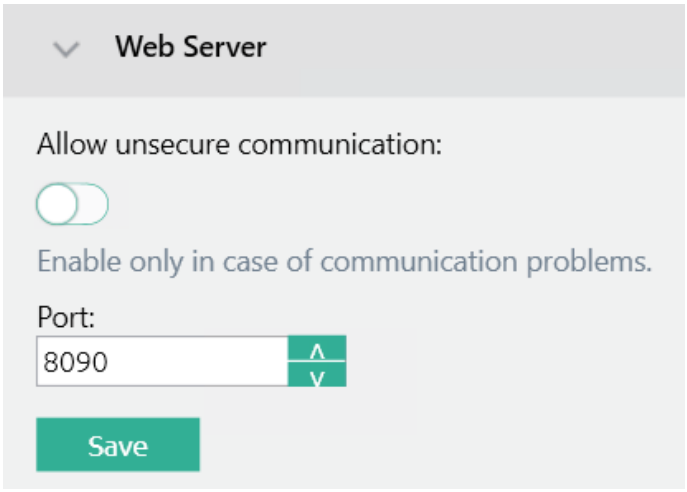
Unabhängig vom CA-Modus werden Zertifikate physisch im Verzeichnis „C:\ProgramData\MyQ\Cert“ gespeichert, das die folgenden Dateien enthalten kann:

- server.pfx – Serverzertifikat mit öffentlichem und privatem Schlüssel
- server.cer – Serverzertifikat mit öffentlichem Schlüssel
- server.key – privater Schlüssel des Servers
- ca-root.crt – Stamm-CA-Zertifikat des Unternehmens mit öffentlichem Schlüssel
- ca-myq.pfx – Zertifikat der ausstellenden CA mit öffentlichem und privatem Schlüssel
- ca-myq.crt – Zertifikat der ausstellenden Zertifizierungsstelle mit öffentlichem Schlüssel
- ca-myq.key – private Schlüssel der ausstellenden CA

Die privaten Schlüssel der lokalen ausstellenden CA (die in den ersten beiden Betriebsmodi verwendet wird) sind stets durch ein zufällig generiertes Passwort geschützt, das in verschlüsselter Form in der internen Firebird-Datenbank gespeichert ist.

Unverschlüsselten HTTP-Datenverkehr blockieren

Unverschlüsselter HTTP-Verkehr sollte in der Konfiguration des MyQ-Print Server nicht aktiviert sein:



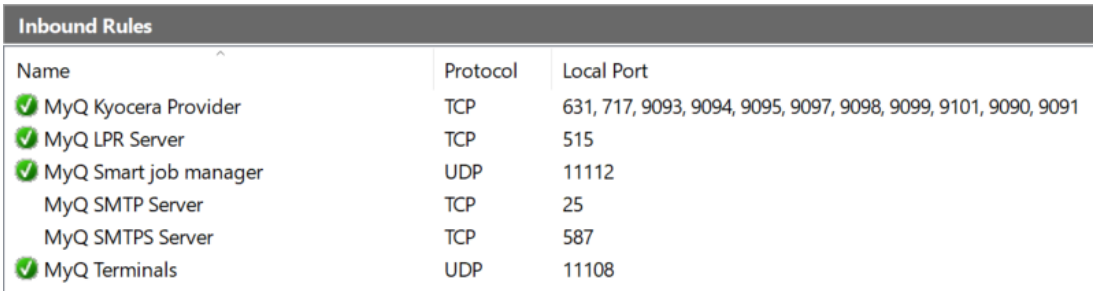
Überprüfen Sie die Sicherheitseinstellungen für die Kommunikation

Überprüfen Sie die unter „Einstellungen – Netzwerk – Mindest-TLS-Version“ konfigurierten Mindest-TLS-Versionen. Die Standardeinstellung seit MyQ X 10.2 ist TLS 1.2.

Weitere erweiterte Optionen, z. B. wie Sie die erforderliche Mindest-TLS-Version stattdessen auf 1.3 festlegen, finden Sie unter „Erweiterte Sicherheit“.

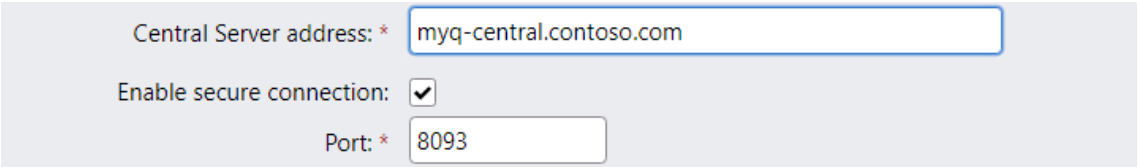
Nicht verwendete Ports blockieren

Verringern Sie die Angriffsfläche, indem Sie Firewall-Regeln für Protokolle deaktivieren, die vom MyQ Print Server nicht verwendet werden:



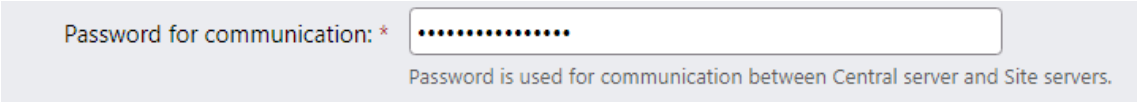
Verschlüsseln Sie Verbindungen zum MyQ Central Server

Verwenden Sie für die Verbindung zum MyQ Central Server ausschließlich HTTPS:



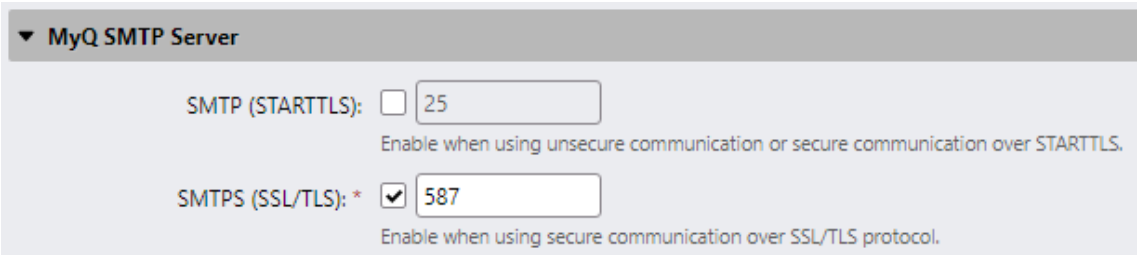
Verwenden Sie sichere Passwörter für die Server-zu-Server-Authentifizierung

Das Passwort für die Kommunikation zwischen dem Central Server und dem Standort sollte sicher sein (Passwortkomplexität):

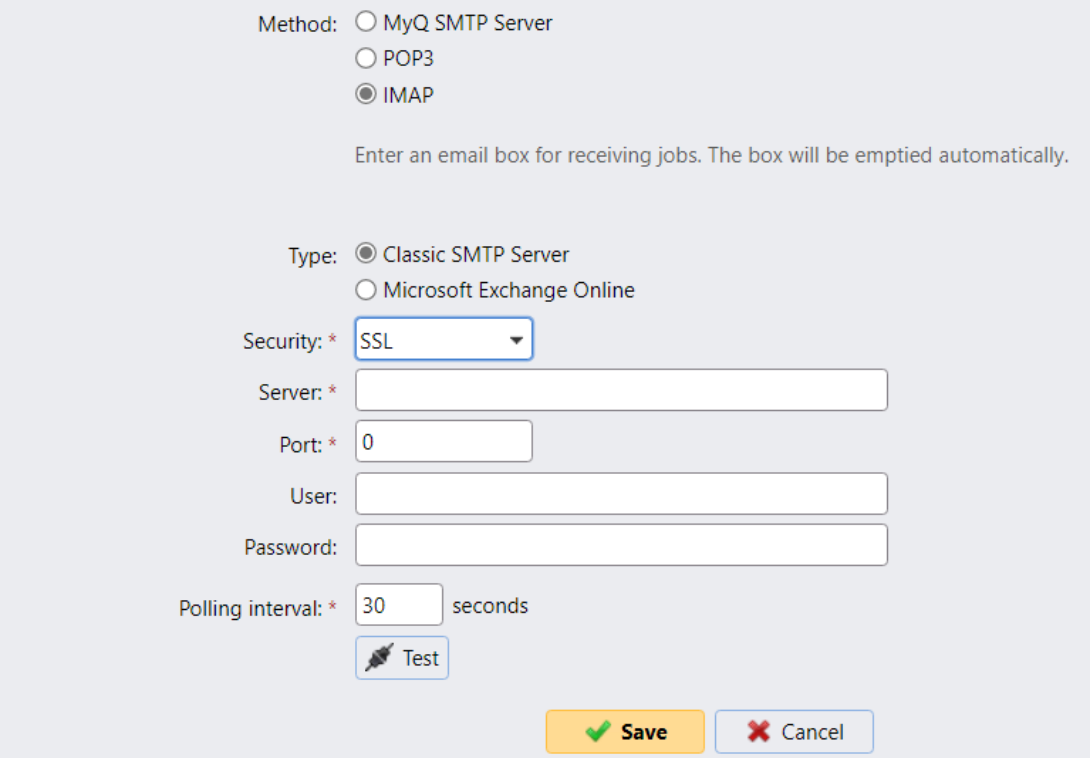


Sichern Sie den SMTP-Verkehr

Wenn das SMTP-Protokoll zum Versenden von E-Mails oder zum Empfangen von Dokumenten von Netzwerkscannern verwendet wird, sollte stets eine TLS-Verschlüsselung erzwungen werden, um die Vertraulichkeit der Daten zu gewährleisten.

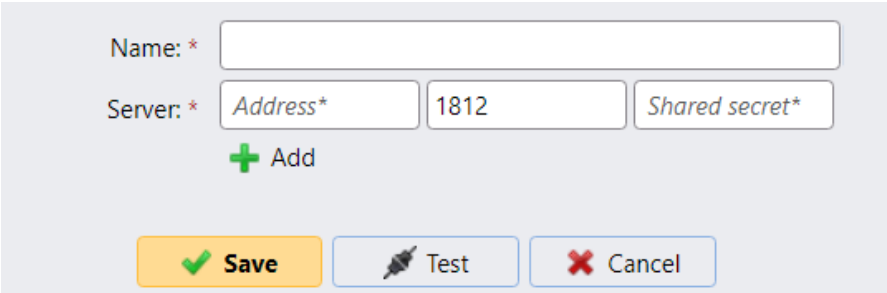


Die TLS-Verschlüsselung sollte auch bei Verwendung des IMAP-Protokolls erzwungen werden, während das veraltete POP3-Protokoll vermieden werden sollte:



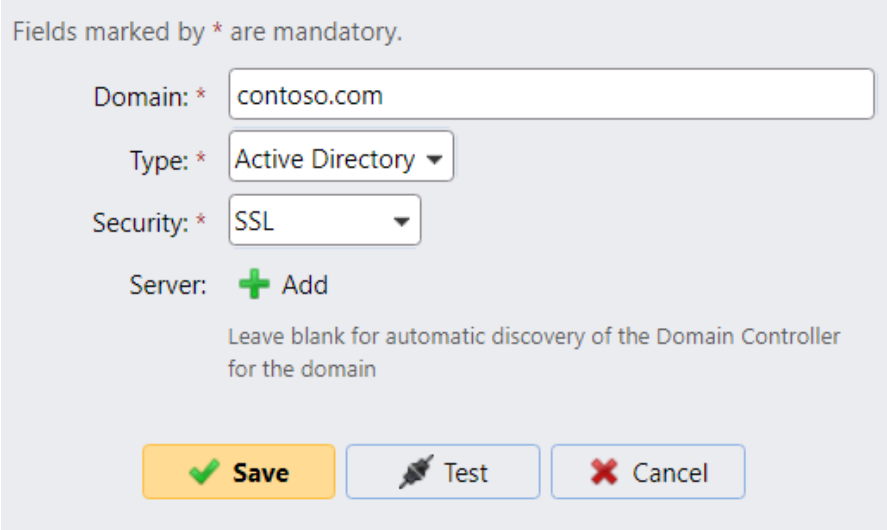
Verwenden Sie sichere und eindeutige RADIUS-Passwörter

Wenn die RADIUS-Authentifizierung verwendet wird, sollten stets sichere gemeinsame Geheimnisse generiert werden, die spezifisch für den MyQ Print Server sind:



Verschlüsseln Sie den LDAP-Verkehr

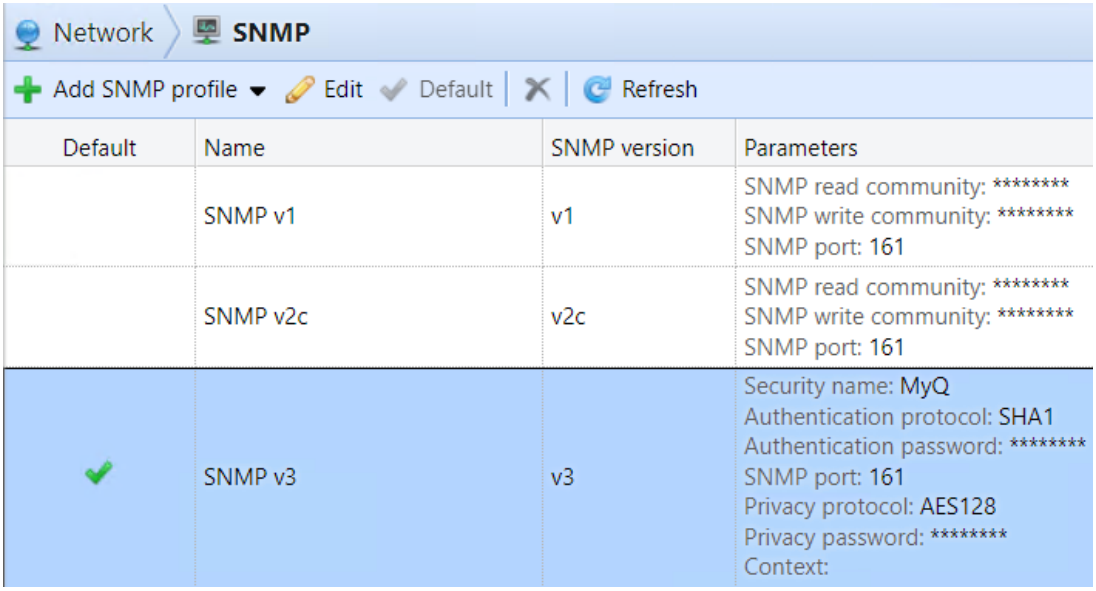
Zur Sicherung des gesamten LDAP-Datenverkehrs sollte TLS-Verschlüsselung verwendet werden:



Verwenden Sie aus Sicherheitsgründen kein START TLS, da dieses anfällig für MITM-Angriffe ist. Auf allen LDAP-Servern (Active Directory-Domänencontroller) muss ein von einer vertrauenswürdigen Zertifizierungsstelle ausgestelltes Zertifikat konfiguriert werden.

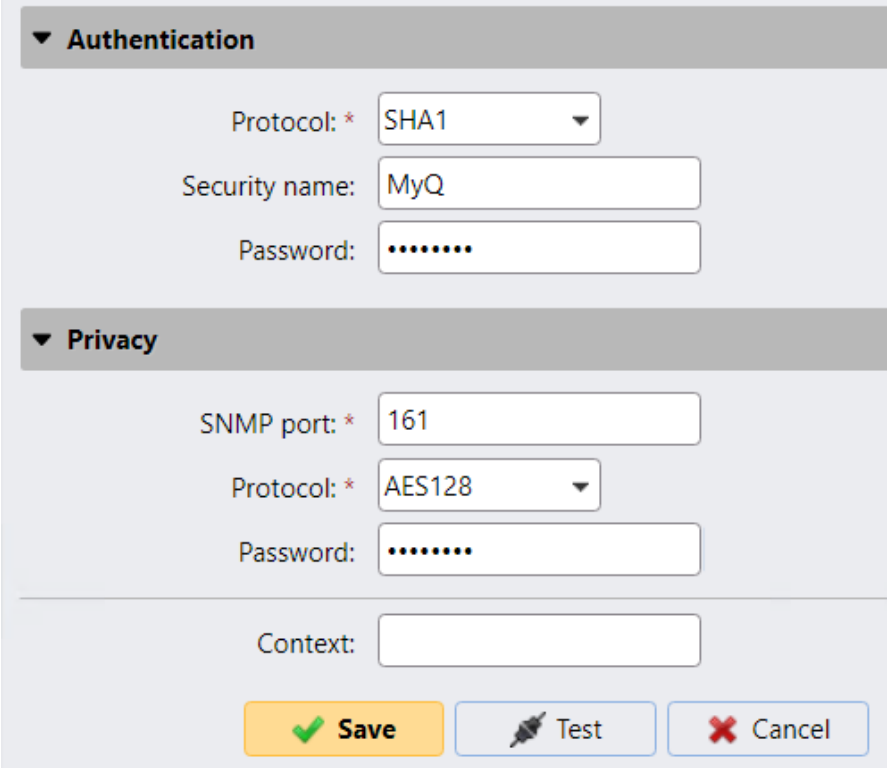
Sichern Sie den SNMP-Datenverkehr

Unsichere SNMPv1-Kommunikation mit Geräten sollte vermieden werden:



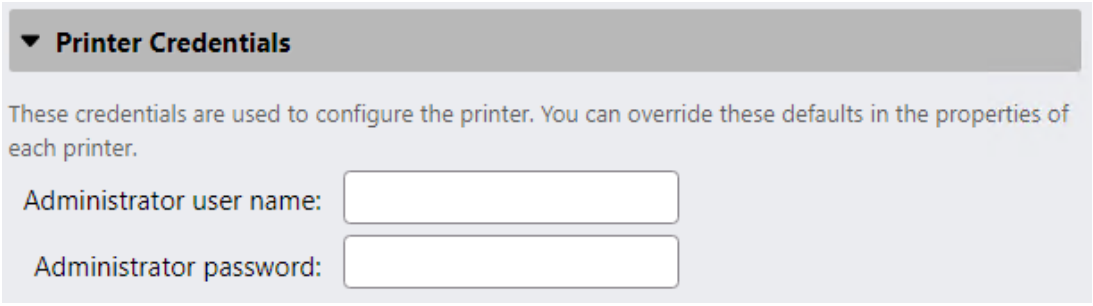
Default	Name	SNMP version	Parameters
	SNMP v1	v1	SNMP read community: ******** SNMP write community: ******** SNMP port: 161
	SNMP v2c	v2c	SNMP read community: ******** SNMP write community: ******** SNMP port: 161
✔	SNMP v3	v3	Security name: MyQ Authentication protocol: SHA1 Authentication password: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

Verwenden Sie nur SNMPv3 mit einem starken Passwort und konfigurieren Sie sicherere kryptografische Algorithmen (SHA1 und AES):



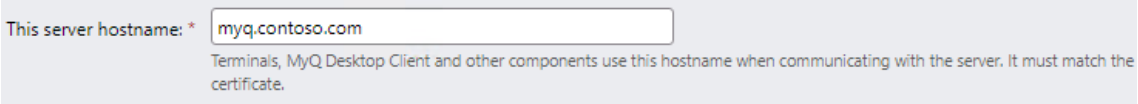
Sichere Drucker-Anmeldedaten

Die Verwaltung der Drucker-Anmeldedaten erfolgt außerhalb von MyQ Print Server und ist herstellerspezifisch. Wenn möglich, sollten starke, zufällig generierte Passwörter zur Verwaltung von Druckern verwendet werden:



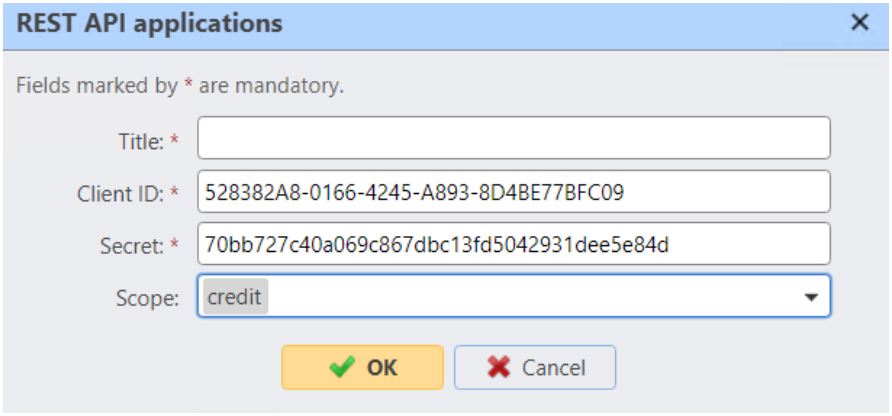
Verwenden Sie immer FQDN

Um MITM-Angriffe zu verhindern, verwenden Sie in allen Konfigurationsfenstern ausschließlich vollqualifizierte Domänennamen:



REST-API-Schlüssel schützen

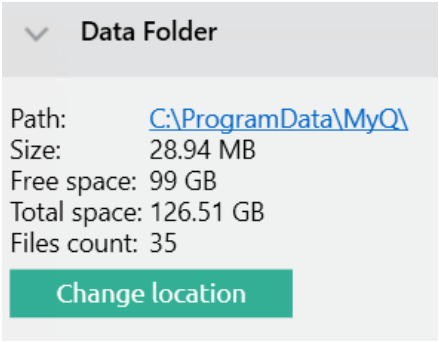
Wenn REST-APIs verwendet werden, schützen Sie die Client-Geheimnisse vor unnötiger Offenlegung und führen Sie regelmäßig einen Schlüsselwechsel durch:



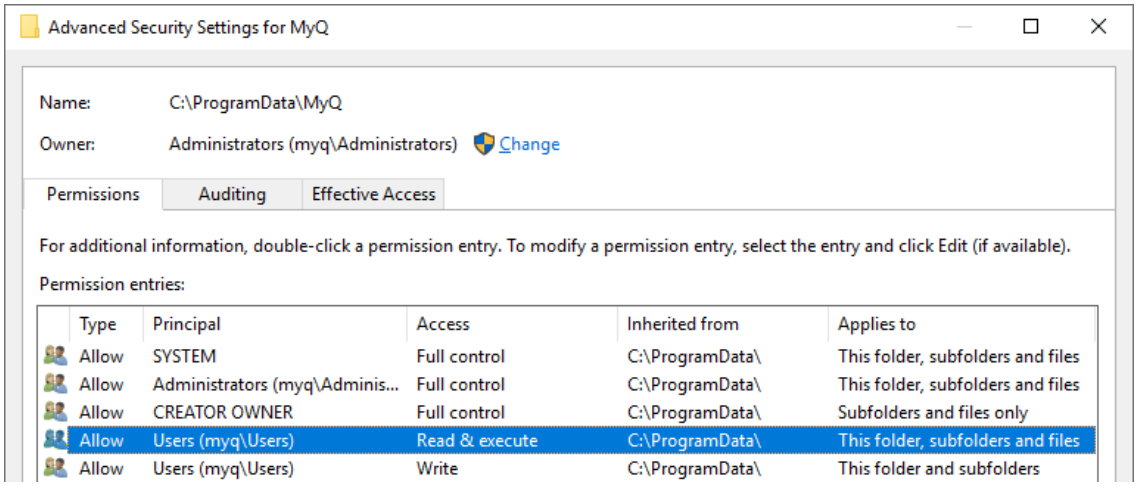
1.2.3 PS Datensicherheit

Berechtigungen für den Datenordner einschränken

Der Datenordner von MyQ Print Server enthält hochsensible Daten, darunter die Benutzerdatenbank und den privaten Schlüssel des TLS-Zertifikats. Sein aktueller Speicherort wird in der Anwendung „MyQ Easy Config“ angezeigt:



Alle Benutzer (lokal/Domäne) haben standardmäßig Lesezugriff:

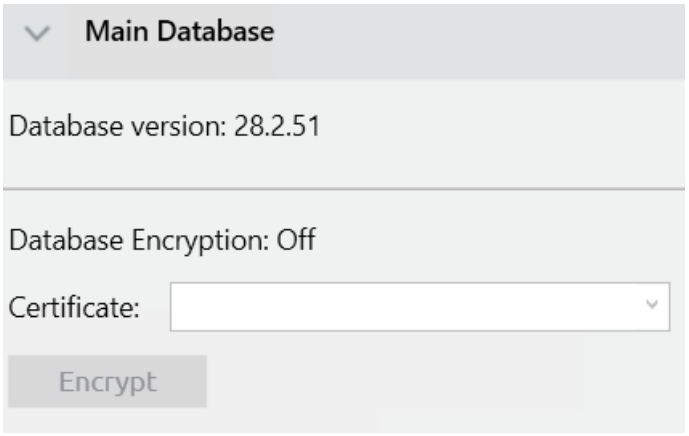


Nur Administratoren, das SYSTEM-Konto und das MyQ-Dienstkonto sollten Zugriff auf dieses Verzeichnis haben. Hier ist ein Beispiel für ein Batch-Skript, das zur Absicherung der Zugriffsrechte verwendet werden kann:

```
@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
```

Datenbankverschlüsselung aktivieren

Verschlüsseln Sie die Datenbank stets mit einem benutzerdefinierten Zertifikat, um das Risiko von Datenlecks zu verringern:



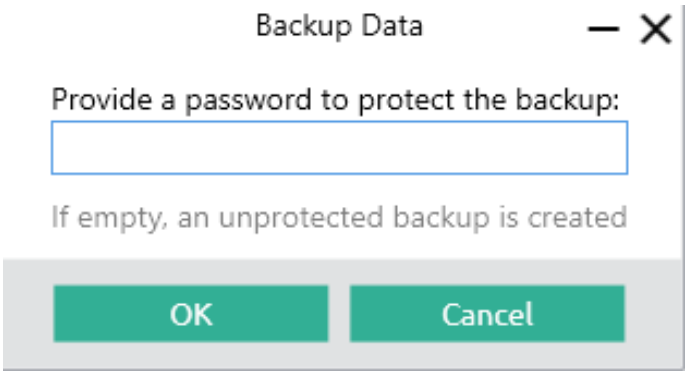
Das Zertifikat muss die erweiterte Schlüsselverwendung (EKU) „Encrypting File System“ aufweisen und sich in einem der folgenden Zertifikatsspeicher des Computers befinden:

- „Persönlich“
- Vertrauenswürdige Herausgeber
- Stammzertifizierungsstellen von Drittanbietern
- Andere Personen

Der Speicher „Persönlich“ wird bevorzugt.

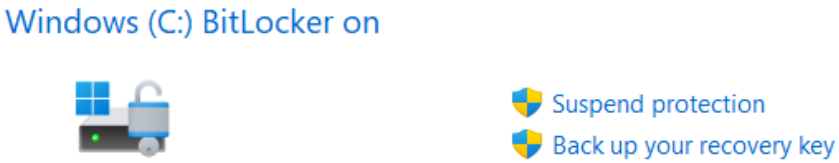
Sicherungen verschlüsseln

Datenbanksicherungen sollten durch sichere, zufällig generierte Passwörter geschützt werden:



Festplattenverschlüsselung aktivieren

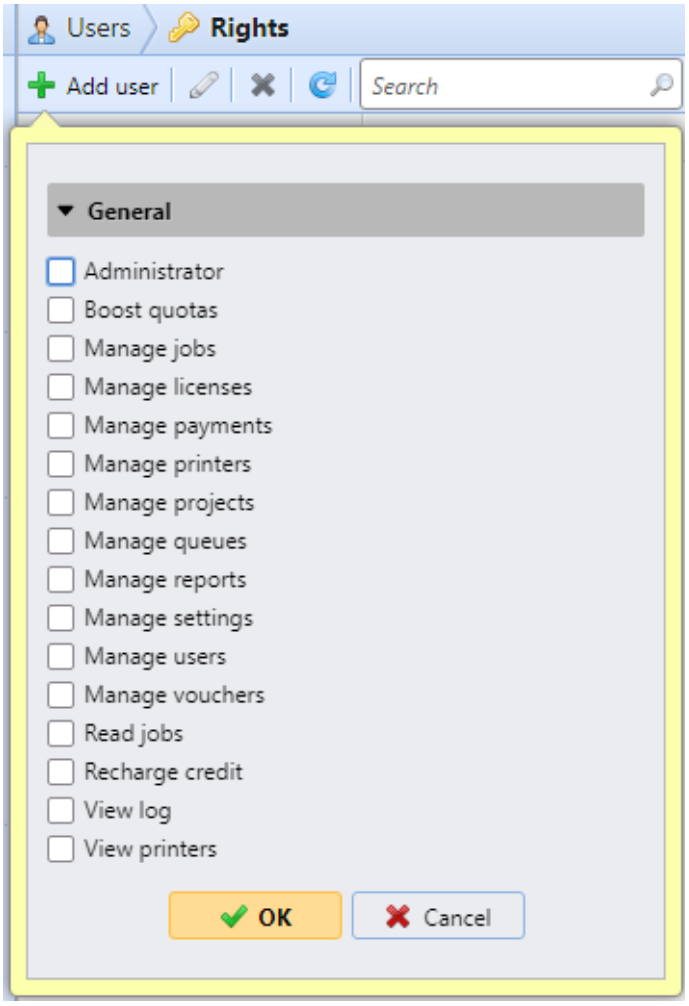
Wenn möglich, sollte auf dem MyQ-Print Server eine Technologie zur vollständigen Festplattenverschlüsselung wie Microsoft BitLocker aktiviert werden, um die ruhenden Daten zu schützen:



1.2.4 PS Zusätzliche Empfehlungen

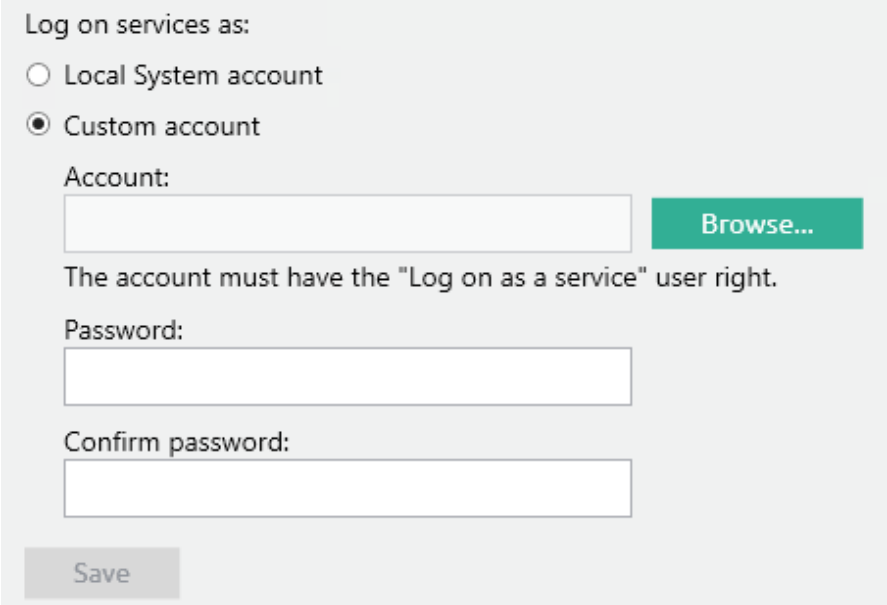
RBAC einsetzen

Verwenden Sie das Standard-*admin-Konto nicht für den regulären Betrieb. Nutzen Sie stattdessen die Delegierung von Berechtigungen und wenden Sie dabei das Prinzip der geringsten Berechtigungen an:



Konfigurieren Sie ein benutzerdefiniertes Dienstkonto für Dienste

MyQ Print Server läuft standardmäßig unter dem hochprivilegierten SYSTEM-Konto. Konfigurieren Sie stattdessen ein benutzerdefiniertes Dienstkonto mit einem sicheren Passwort:



Halten Sie den Server auf dem neuesten Stand

Installieren Sie die von MyQ bereitgestellten Sicherheitsupdates, sobald sie verfügbar sind. Sie können die aktuell installierte Anwendungsversion in MyQ Easy Config überprüfen:

Halten Sie das Betriebssystem sicher

MyQ Print Server ist nur so sicher wie das zugrunde liegende Betriebssystem. Halten Sie es auf dem neuesten Stand und wenden Sie die von Microsoft empfohlenen Sicherheitsrichtlinien an.

Aktualisieren Sie Ihre Software regelmäßig, um Sicherheitslücken zu beheben und die Leistung zu verbessern. Eine Liste der Anforderungen und Empfehlungen finden Sie in den Systemanforderungen.

Beispielsweise muss .NET entweder mit Verwaltungstools oder über Windows Updates auf Opt-in-Basis[4] aktualisiert werden.

Planen Sie die Notfallwiederherstellung

Erstellen Sie regelmäßig Backups des MyQ Print Servers, einschließlich der Datenbank, der Zertifikate und der Konfigurationsdateien. Testen Sie das Wiederherstellungsverfahren mindestens einmal.

1.3 MyQ X Desktop Client

Der MyQ Desktop Client verwendet robuste Sicherheitsmechanismen, um eine sichere Kommunikation, Authentifizierung und Datenintegrität in Unternehmensdruckumgebungen zu gewährleisten. Dieses Dokument beschreibt die Protokolle, Authentifizierungsmethoden und Konfigurationsbest Practices, die die Sicherheitsarchitektur des Desktop Client untermauern, mit Schwerpunkt auf TLS-Verschlüsselung, integrierter Windows-Authentifizierung (IWA), Kerberos, NTLM und Entra ID-Integration. Technische Implementierungen wie die Registrierung von Service Principal Names (SPN), die Zertifikatsverwaltung und stille Anmeldeabläufe werden analysiert, um die Einhaltung moderner Sicherheitsstandards zu demonstrieren.

1.3.1 Sichere Kommunikationsarchitektur

TLS-Verschlüsselung als Standard

Druck- und Central Server erzwingen die TLS 1.2+-Verschlüsselung für alle Kommunikationskanäle, einschließlich der Interaktionen mit dem Desktop Client. Dies gewährleistet die Vertraulichkeit und Integrität der Daten während des Job-Spoolings, der Authentifizierung und der Berichterstellung. Administratoren müssen

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

HTTPS-Endpunkte unter Verwendung von vollqualifizierten Domänennamen (FQDNs) konfigurieren, um Man-in-the-Middle-Angriffe (MITM) zu verhindern.

Zertifikatsvalidierungsmodi

- **Strenger Modus**: Erfordert, dass Serverzertifikate von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt oder manuell zum Vertrauensspeicher des Systems hinzugefügt werden. Verbindungsversuche schlagen fehl, wenn die Validierung fehlschlägt. Wir empfehlen, wann immer möglich den strengen Modus zu verwenden.
- **Normalmodus**: Ermöglicht es Benutzern, Warnungen zu nicht vertrauenswürdigen Zertifikaten zu umgehen, wobei akzeptierte Zertifikate für zukünftige Sitzungen gespeichert werden `%ProgramData%\MyQ\Desktop Client\cert.store` für zukünftige Sitzungen gespeichert werden.

1.3.2 Authentifizierungsmechanismen

Integrierte Windows-Authentifizierung (IWA)

IWA ermöglicht eine nahtlose Authentifizierung in Domänenumgebungen mit Kerberos oder NTLM. Der Server nutzt die Windows HTTP Server API (`http.sys`), um eingehende HTTP-Anfragen zu verarbeiten und Service Principal Names (SPNs) zu validieren, wodurch die Protokollintegrität gewährleistet wird.

Kerberos-Workflow

1. **Erwerb eines Ticket Granting Ticket (TGT)**: Mit der Domäne verbundene Clients erhalten ein TGT vom Key Distribution Center (KDC).
2. **Service Ticket Request**: Der Client fordert ein Service Ticket für `HTTP/<FQDN>` vom KDC an.
3. **Token-Validierung**: Der MyQ-Server validiert das Dienstticket anhand des registrierten SPN.

Kritische Konfiguration:

- Der Server muss über einen ordnungsgemäß konfigurierten SPN verfügen, damit die Kerberos-Authentifizierung korrekt funktioniert.
- Der Zugriff über IP-Adressen umgeht Kerberos und erzwingt einen Fallback auf NTLM.

Kerberos-Durchsetzung

Für Umgebungen, die strengere Sicherheitsanforderungen haben, kann die Anwendung so konfiguriert werden, dass **ausschließlich Kerberos verwendet wird** und ein NTLM-Fallback nicht zulässig ist. Dies erfolgt auf Serverebene und nicht ausschließlich für den Desktop Client.

1. Deaktivieren Sie NTLM über `KerberosOnly=True` in `config.ini`.
2. Registrieren Sie SPNs für alle MyQ-Server mit `setspn`.
3. Verwenden Sie FQDNs anstelle von IP-Adressen für Server-Endpunkte.

NTLM-Fallback

NTLM dient als Fallback in nicht domänen- oder IP-basierten Szenarien. Es ist zwar weniger sicher, verwendet jedoch einen Challenge-Response-Mechanismus, der mit dem Passwort des Benutzers gehasht wird. Um Kerberos ausschließlich zu erzwingen, befolgen Sie den obigen Vorschlag.

Entra ID Silent Login

Bei Entra ID-verbundenen oder hybriden Geräten verwendet Desktop Client die Microsoft Authentication Library (MSAL) und den Windows Authentication Manager (WAM), um Tokens stillschweigend über das Betriebssystemkonto zu erwerben. Der Ablauf umfasst:

1. **Token-Erwerb**: MSAL ruft mithilfe von WAM ein ID-Token ab.
2. **Token-Austausch**: Das ID-Token wird gegen ein MyQ-Zugriffstoken ausgetauscht, um REST-API-Aufrufe zu authentifizieren.

OAuth 2.0-Autorisierungscode-Ablauf

Für Nicht-Windows-Umgebungen unterstützt Desktop Client OAuth 2.0 über die `authorization_code` grant:

1. **Benutzerumleitung**: Der Client leitet Benutzer zur MyQ-Anmeldeseite um.
2. **Codeaustausch**: Nach der Authentifizierung wird der Autorisierungscode gegen einen Zugriffstoken ausgetauscht.

Entra ID-Konfiguration

- Aktivieren Sie **„Mit Microsoft anmelden"** in den MyQ-Server-Einstellungen für hybrid verbundene Geräte.

- Stellen Sie sicher, dass die Geräte bei Entra ID registriert sind, um die stille Authentifizierung nutzen zu können.

Zertifikatsverwaltung

Vertrauenswürdige Stammzertifikate

- **Strenger Modus**: Zertifikate müssen im Vertrauensspeicher des Betriebssystems vorinstalliert sein (z. B. über Gruppenrichtlinien).
- **Normalmodus**: Vom Benutzer genehmigte Zertifikate werden gespeichert `cert.store` und für nachfolgende Sitzungen wiederverwendet.

Validierungs-Workflow

1. Bei der Validierung von Serverzertifikaten wird die Vertrauenskette überprüft.
2. Wenn die Validierung fehlschlägt, werden Benutzer aufgefordert, das Zertifikat zu akzeptieren oder abzulehnen (dies ist nur der Fall, wenn der normale und nicht der strenge Validierungsmodus verwendet wird).
3. Akzeptierte Zertifikate werden zwischengespeichert, um wiederholte Aufforderungen zu vermeiden (dies ist nur der Fall, wenn der normale und nicht der strenge Validierungsmodus verwendet wird).

Bewährte Verfahren für Zertifikate
Wir empfehlen, für MyQ-Server immer von einer Unternehmens-CA signierte Zertifikate zu verwenden.

Fazit

Der MyQ Desktop Client integriert Authentifizierung und Verschlüsselung auf Unternehmensniveau, um Risiken wie den Diebstahl von Anmeldedaten und das Abhören von Daten zu minimieren. Durch die Durchsetzung von Kerberos, TLS und Zertifikatsvalidierung können Unternehmen die Zero-Trust-Prinzipien einhalten und gleichzeitig die Benutzerfreundlichkeit durch stille Authentifizierungsabläufe gewährleisten.

2 Whitepaper zur MyQ X-Sicherheit

Übersicht über die Sicherheitsfunktionen von MyQ X

MyQ X bietet eine Reihe von Funktionen, die die Sicherheit und den Datenschutz sowohl für Endbenutzer als auch für das Unternehmen verbessern. Diese Funktionen umfassen sicheres Drucken am Multifunktionsgerät, die Anpassung der Benutzersitzung und wirken sich mithilfe von Wasserzeichen auch nach dem Drucken eines Dokuments weiterhin aus.

Nachfolgend finden Sie eine kurze Zusammenfassung der Sicherheitsfunktionen von MyQ X:

- Einhaltung der DSGVO
- Sicheres Drucken
- Benutzersitzungen mit mehreren Authentifizierungsoptionen, einschließlich Zwei-Faktor-Authentifizierung
- Manuelles und automatisches Abmelden von Benutzersitzungen
- End-to-End-Datenverschlüsselung einschließlich Verschlüsselung ruhender Daten (Datenbank, Aufträge, Protokolle)
- Vom MyQ-Administrator vordefinierte feste Scan-Zielordner
- Private Warteschlangen zum sofortigen Löschen von Druckaufträgen nach der Freigabe
- Datenschutzmodus zur Anonymisierung von Namen in Druckaufträgen
- Eingeschränkter Zugriff auf die Einrichtungsoptionen des Print Servers über die MyQ X-Webschnittstelle
- Anpassbare Zugriffsrechte für verschiedene Einstellungsoptionen
- Mehrere Stufen der Passwortkomplexität
- Prüfprotokoll für Änderungen an den Einstellungen
- Unterstützung für Unternehmenszertifizierungsstellen
- Wasserzeichen auf gedruckten Dokumenten
- Stellenvorschau
- Steuerung gescannter Dokumente über OCR- und DMS-Systeme
- Stellenarchivierung

Der Sicherheitsansatz von MyQ X basiert auf dem Grundsatz, dass **Sicherheit ist kein nachträglicher Gedanke, sondern ein integraler Bestandteil des gesamten Druckmanagement-Ökosystems.**Die Plattform implementiert eine umfassende Verteidigungsstrategie, die Daten und Arbeitsabläufe in jeder Phase des Dokumentenlebenszyklus schützt.

2.1 Zero-Trust-Architektur

Gemäß der Methodik „Vertraue niemals, überprüfe immer“ geht MyQ X davon aus, dass Bedrohungen sowohl innerhalb als auch außerhalb eines Netzwerks existieren können. Jede Verbindung, jeder Benutzer und jedes Gerät muss vor dem Zugriff auf Druckressourcen authentifiziert und autorisiert werden, um eine kontinuierliche Überprüfung während aller Interaktionen zu gewährleisten.

2.2 Dreiphasiges Schutzkonzept

MyQ X gewährleistet Sicherheit in drei entscheidenden Phasen:

2.2.1 Sicherung der Druckinfrastruktur

Die gesamte unterstützende Infrastruktur wird vor dem Drucken von Dokumenten ordnungsgemäß gesichert, einschließlich Workstations, mobiler Geräte, Server, Netzwerke und Druckgeräte.

2.2.2 Sicherung von Druck-Workflows

Bewährte sichere Arbeitsabläufe, einschließlich authentifizierter Druckfreigabe, Auftragstrennung und umfassender Berichterstellung, verhindern Schwachstellen, die Unternehmen gefährden könnten.

2.2.3 Sichern von Druckausgaben

Kontinuierlicher Schutz durch Wasserzeichen, digitale Signaturen und umfassende Prüfprotokolle, die die Rückverfolgbarkeit gewährleisten und verantwortungsbewusstes Nutzerverhalten fördern.

2.3 Datenschutz durch Technikgestaltung

Der Datenschutz ist von Grund auf in die Architektur von MyQ X integriert. Das System minimiert die Datenerfassung, implementiert eine starke Verschlüsselung und bietet den Benutzern die Kontrolle über ihre persönlichen Daten, um die Einhaltung der DSGVO und den Schutz der Privatsphäre zu gewährleisten.

2.4 Kontinuierliche Weiterentwicklung der Sicherheit

MyQ X gewährleistet seine Sicherheit durch regelmäßige Updates, umgehende Behebung von Sicherheitslücken, Integration von Bedrohungsinformationen sowie fortlaufende Sicherheitsbewertungen und Zertifizierungen durch Dritte.

Dieser sicherheitsorientierte Ansatz gewährleistet, dass Unternehmen MyQ X vertrauensvoll einsetzen können, da sie wissen, dass ihre sensiblen Daten, Compliance-Anforderungen und die Betriebskontinuität durch branchenführende Sicherheitsmaßnahmen geschützt sind.

2.5 Wichtige Sicherheitsverbesserungen in 10.2

MyQ X 10.2 bietet erhebliche Sicherheitsverbesserungen, die den Schutz vor sich ständig weiterentwickelnden Cyber-Bedrohungen stärken und gleichzeitig die Betriebseffizienz aufrechterhalten. Diese Verbesserungen beheben kritische Schwachstellen und implementieren moderne Sicherheitsstandards.

2.5.1 Verbesserte TLS-Sicherheit

Standardmäßige Mindestversion TLS 1.2: MyQ X 10.2 erhöht die standardmäßige Mindestversion von TLS von 1.1 auf 1.2 und unterstützt TLS 1.3. Dadurch entfällt die Unterstützung für veraltete SSL-Protokolle und schwache Verschlüsselungen, die Sicherheitsrisiken darstellen.

Verbesserte Zertifikatsvalidierung: Die verbesserte Zertifikatsvalidierung verhindert die Verwendung abgelaufener oder nicht ordnungsgemäß ausgestellter Zertifikate und schützt so vor Man-in-the-Middle-Angriffen und anderen Schwachstellen. Das System vertraut nun automatisch Root-CA-Zertifikaten aus dem Systemzertifikatsspeicher des Servers.

2.5.2 Verbesserungen der Authentifizierungssicherheit

Verbesserte Passwort- und PIN-Sicherheit: Verbesserte Passwort-Hashing-Algorithmen stärken den Schutz von Anmeldedaten. Das System führt neue PIN-Sicherheitsregeln ein, darunter eine obligatorische Mindestlänge von 6 Ziffern und die Verhinderung leicht zu erratender Kombinationen wie „1234“ oder „1111“.

Schutz vor Anmeldeversuchen: Aus Sicherheitsgründen sind erfolglose Authentifizierungsversuche nun begrenzt. Standardmäßig werden Clients/Geräte nach mehr als 5 ungültigen Anmeldeversuchen innerhalb von 60 Sekunden für 5 Minuten gesperrt, wobei die Zeiträume konfigurierbar sind.

Verbesserte Protokollierung von Anmeldeereignissen: Die verbesserte Protokollierung von Anmeldeereignissen, insbesondere von fehlgeschlagenen Authentifizierungsversuchen, erleichtert Administratoren das Filtern und Überwachen von Sicherheitsereignissen im MyQ-Protokoll.

2.5.3 Verbesserungen der Datenbanksicherheit

Implementierung von Firebird 4.0: Das Upgrade auf die Datenbank-Engine Firebird 4.0 bietet erweiterte Sicherheitsfunktionen und eine verbesserte Leistung. Datenbankpasswörter werden nun in Protokolldateien verschleiert, um die Offenlegung von Anmeldedaten zu verhindern.

Verbesserter Datenschutz: Der Zugriff auf sensible Daten wird durch benutzerdefinierte Berichte und externe Berichtskonten eingeschränkt, wodurch die Vertraulichkeit der Daten über verschiedene Zugriffsebenen hinweg gewährleistet wird.

2.5.4 Behebung von Sicherheitslücken

Kritische CVE-Korrekturen: MyQ X 10.2 behebt mehrere kritische Sicherheitslücken, darunter:

- CVE-2024-28059: Sicherheitslücke bei der nicht authentifizierten Remote-Codeausführung.
- CVE-2024-22076: Sicherheitsverbesserungen für PHP-Skripte.
- CVE-2023-45853, CVE-2023-5678, CVE-2023-49316: Sicherheitslücken in Komponenten von Drittanbietern.

Sicherheitsupdates für Komponenten: Aktualisierte Versionen kritischer Komponenten, darunter OpenSSL 3.1.0, PHP 8.3.14 und Apache 2.4.57, beheben bekannte Sicherheitslücken.

2.5.5 API- und Integrationssicherheit

REST-API-Einschränkungen: Begrenzte Bereiche für bekannte Clients und entfernte Funktionen für sensible Vorgänge wie das Ändern von Benutzerauthentifizierungsservern, wodurch die API-Sicherheit erhöht wird.

PHP-Skriptsteuerung: Mit den neuen Easy Config-Einstellungen können Administratoren den Zugriff auf PHP-Skripte sperren/freigeben und so die Sicherheit verbessern, indem diese Einstellungen im schreibgeschützten Modus beibehalten werden.

2.5.6 Administrative Sicherheit

Verbesserte Sicherheit für Administratorkonten: Das Standard-Administratorpasswort wurde für neue Installationen entfernt. Administratoren können nun Administratorkonten deaktivieren, wenn sie nicht benötigt werden, und

so die Verwendung spezifischer Benutzerkonten mit entsprechenden Rechten anstelle von gemeinsam genutzten Administratorkonten fördern.

Diese Sicherheitsverbesserungen zeigen das Engagement von MyQ X für die Einhaltung von Sicherheitsstandards auf Unternehmensniveau und die Bewältigung aktueller Herausforderungen im Bereich der Cybersicherheit. Regelmäßige Sicherheitsupdates und proaktives Schwachstellenmanagement sorgen dafür, dass Unternehmen MyQ X mit Vertrauen in ihre Sicherheit einsetzen können.

2.6 Geschäftswert der sicheren Druckverwaltung

Sicheres Druckmanagement liefert messbaren geschäftlichen Nutzen, indem es die Druckinfrastruktur von einer potenziellen Belastung in einen strategischen Sicherheitsvorteil verwandelt. MyQ X bietet Unternehmen umfassenden Schutz, der das gesamte Spektrum der druckbezogenen Risiken abdeckt und gleichzeitig die betriebliche Effizienz steigert.

2.6.1 Risikominderung und Kostensenkung

Verhinderung von Datenverletzungen: Secure Print Release stellt sicher, dass vertrauliche Dokumente niemals unbeaufsichtigt in Druckerfachen liegen bleiben, wodurch der unbefugte Zugriff auf sensible Informationen verhindert wird. Benutzer authentifizieren sich vor der Freigabe ihrer Aufträge und behalten so die vollständige Kontrolle über die Dokumentensicherheit.

Vermeidung von Compliance-Kosten: Integrierte Funktionen zur Einhaltung der DSGVO, HIPAA und SOX helfen Unternehmen, Strafen aufgrund von Verstößen gegen Vorschriften zu vermeiden und die Kosten für die Vorbereitung von Audits durch automatisierte Compliance-Kontrollen und umfassende Prüfpfade zu senken.

Betriebskontinuität: Die Device Spooling-Funktion von MyQ gewährleistet die Druckfähigkeit auch bei Serverausfällen, indem sie verschlüsselte Aufträge bis zu einer Woche lang lokal auf bis zu 10 Geräten speichert und so Betriebsunterbrechungen während der Systemwartung oder unerwarteten Ausfallzeiten verhindert.

2.6.2 Verbesserte Sicherheitsprinzipien

Zero-Trust-Implementierung: Durch die Authentifizierungspflicht für jeden Druckauftrag setzt MyQ X das Prinzip „Vertraue niemals, überprüfe immer“ in der gesamten Druckumgebung durch und stärkt so die allgemeine Sicherheitslage des Unternehmens.

Rückverfolgbarkeit von Dokumenten: Wasserzeichen und digitale Signaturen ermöglichen es Unternehmen, vertrauliche Dokumente während ihres gesamten Lebenszyklus zu verfolgen, wodurch die Verantwortlichkeit gewährleistet und der Missbrauch sensibler Informationen verhindert wird.

Umfassende Verschlüsselung: Die End-to-End-Verschlüsselung von Druckdaten, Datenbanken und gespeicherten Aufträgen stellt sicher, dass sensible Informationen während des gesamten Dokumenten-Workflows geschützt bleiben und strenge Sicherheitsanforderungen erfüllt werden.

2.6.3 Betriebliche Effizienz

Bandbreitenoptimierung: Client-Spooling reduziert den Netzwerkverkehr durch lokale Verarbeitung von Aufträgen und verbessert so die Leistung in Umgebungen mit begrenzter Bandbreite, wie z. B. Remote-Büros und Zweigstellen.

Flexible Authentifizierung: Mehrere Authentifizierungsoptionen, darunter ID-Karten, PINs, Passwörter und die Authentifizierung über mobile Apps, bieten Benutzern bequeme und dennoch sichere Zugriffsmethoden, die den unterschiedlichen Anforderungen von Unternehmen gerecht werden. Eine Multi-Faktor-Authentifizierung (MFA), die diese Methoden kombiniert, ist ebenfalls verfügbar.

Zentrale Verwaltung: Einheitliche Sicherheitsrichtlinien für alle Geräte vereinfachen die Verwaltung und gewährleisten gleichzeitig konsistente Schutzstandards im gesamten Unternehmen.

2.6.4 Strategische Geschäftsvorteile

Wettbewerbsvorteil: Durch den Nachweis robuster Drucksicherheitsfunktionen können sich Unternehmen in wettbewerbsintensiven Märkten von anderen abheben, insbesondere in Branchen, die mit sensiblen Daten umgehen oder sicherheitsbewusste Kunden bedienen.

Vertrauen der Mitarbeiter: Sichere Druck-Workflows geben Benutzern die Gewissheit, dass ihre Dokumente geschützt sind, was die Produktivität verbessert und sicherheitsbezogene Bedenken verringert, die sich auf die Effizienz am Arbeitsplatz auswirken können.

Zukunftsfähige Infrastruktur: Das umfassende Sicherheitsframework von MyQ X versetzt Unternehmen in die Lage, sich ohne größere Infrastrukturüberholungen an

sich entwickelnde Cybersicherheitsbedrohungen und regulatorische Anforderungen anzupassen.

Sicheres Druckmanagement mit MyQ X verwandelt das Drucken von einer potenziellen Sicherheitslücke in einen kontrollierten, überprüfbaren und konformen Geschäftsprozess, der die Unternehmensziele unterstützt und gleichzeitig wertvolle Informationsressourcen schützt.

2.7 Einhaltung der Vorschriften

Das umfassende Compliance-Framework von MyQ X unterstreicht das Engagement des Unternehmens, die höchsten internationalen Sicherheitsstandards und regulatorischen Anforderungen zu erfüllen. Dieser mehrschichtige Ansatz stellt sicher, dass Unternehmen MyQ X vertrauensvoll einsetzen können und gleichzeitig die vielfältigen Compliance-Anforderungen verschiedener Branchen und Rechtsordnungen erfüllen.

2.7.1 ISO 27001:2022-Zertifizierung und -Implementierung

MyQ hat **die Zertifizierung nach ISO/IEC 27001:2022** erhalten und damit einen systematischen Ansatz für das Informationssicherheitsmanagement etabliert, der den internationalen Best Practices entspricht. Die Implementierung umfasst:

Risikomanagement-Rahmenwerk: Umfassende Risikobewertungsprozesse, die Informationssicherheitsrisiken in allen Geschäftsabläufen und Kundenimplementierungen identifizieren, bewerten und mindern.

Implementierung von **Sicherheitskontrollen**: Strukturierte Bereitstellung technischer, administrativer und physischer Sicherheitskontrollen, die Informationsressourcen während ihres gesamten Lebenszyklus schützen.

Kontinuierlicher Verbesserungsprozess: Regelmäßige Überprüfungen und Aktualisierungen von Sicherheitsrichtlinien, -verfahren und -kontrollen, um auf neue Bedrohungen zu reagieren und die Einhaltung der Zertifizierung zu gewährleisten.

Verpflichtung der Geschäftsleitung: Überwachung auf Führungsebene, um sicherzustellen, dass die Sicherheit in die Geschäftsstrategie und die operativen Entscheidungsprozesse integriert bleibt.

Die Zertifizierung bestätigt den systematischen Ansatz von MyQ zum Schutz von Kundendaten und zur Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationssystemen.

2.7.2 DSGVO-Konformitätsrahmen und Datenschutzmaßnahmen

MyQ X implementiert **eine** umfassende **DSGVO-Konformität** durch in die gesamte Systemarchitektur integrierte Privacy-by-Design-Prinzipien:

Datenminimierung: Das System erfasst nur die für die Betriebsfunktionalität erforderlichen Metadaten und vermeidet so die Verarbeitung unnötiger personenbezogener Daten, die die Compliance-Risiken erhöhen könnten.

Verwaltung von Benutzerrechten: Vollständige Umsetzung der GDPR-Benutzerrechte, darunter:

- Recht auf Zugang zu personenbezogenen Daten
- Recht auf Berichtigung unrichtiger Informationen
- Recht auf Löschung („Recht auf Vergessenwerden“)
- Recht auf Datenübertragbarkeit
- Recht auf Einschränkung der Verarbeitung

Datenschutz-Folgenabschätzungen: Systematische Bewertung der Datenschutzrisiken für neue Funktionen und Implementierungen, um sicherzustellen, dass die DSGVO-Konformität während der gesamten Systementwicklung gewährleistet ist.

2.7.3 Regionale Compliance-Anforderungen (HIPAA, SOX)

MyQ X unterstützt wichtige branchenspezifische Compliance-Rahmenwerke durch robuste Datenschutz- und Audit-Funktionen:

HIPAA-Konformität für das Gesundheitswesen:

- Verschlüsselung geschützter Gesundheitsdaten (PHI) im Ruhezustand und während der Übertragung.
- Umfassende Audit-Protokollierung aller Zugriffe auf sensible Gesundheitsdaten.
- Rollenbasierte Zugriffskontrollen, die den Zugriff auf PHI ausschließlich auf autorisiertes Personal beschränken.
- Sichere Sicherungs- und Wiederherstellungsverfahren für die Anforderungen an die Aufbewahrung von Gesundheitsdaten.

SOX-Konformität für Finanzdienstleistungen:

- Detaillierte Audit-Trails für die Verarbeitung und den Druck von Finanzdokumenten.
- Zugriffskontrollen, die eine unbefugte Änderung von Finanzunterlagen verhindern.
- Sichere Archivierungsfunktionen zur Unterstützung der gesetzlichen Aufbewahrungspflichten.

- Aufgabentrennung durch rollenbasierte Berechtigungen und Genehmigungsworkflows.

Zusätzliche Sicherheitskontrollen:

- Datenbankverschlüsselung unter Verwendung von Algorithmen nach Industriestandard.
- Sichere Kommunikationsprotokolle für die gesamte Datenübertragung.
- Automatisierte Sicherungsverfahren mit Verschlüsselung und Integritätsprüfung.
- Zugriffsprotokollierung und -überwachung für Compliance-Berichte.

2.7.4 Sichere Softwareentwicklungslebenszyklus-Praktiken (SSDLC)

MyQ implementiert einen sicheren Softwareentwicklungslebenszyklus, der den Industriestandards und **SLSA**-Anforderungen für die Lieferkette entspricht und sicherstellt, dass Sicherheitspraktiken in allen Phasen des Software-Lebenszyklus integriert sind.

Analyse

MyQ führt in der ersten Analysephase **eine** strenge **Bedrohungsmodellierung** durch und definiert klare **Sicherheitsanforderungen**, um Risiken frühzeitig zu erkennen und vor Beginn der Entwicklung eine solide Sicherheitsgrundlage zu schaffen.

Entwurf

Alle Architekturvorschläge werden **einer** formellen **Sicherheitsarchitekturprüfung** unterzogen, um die Einhaltung von Prinzipien wie **„Least Privilege“**, **„Zero Trust“** und **„Defense in Depth“** zu überprüfen und sicherzustellen, dass die Sicherheit systematisch in das Systemdesign integriert ist.

Entwicklung

Die Entwickler befolgen **sichere Codierungspraktiken** und Peer-Review-Prozesse, während alle Builds auf dedizierten, isolierten **SLSA-konformen Build-Servern** ausgeführt werden, um den Schutz der Quellintegrität und der Build-Artefakte zu gewährleisten.

Testen

Die Sicherheitsprüfungen umfassen automatisierte **SAST-** und **Dependency-Scans**, die in CI-Pipelines integriert sind und eine frühzeitige Erkennung von Schwachstellen sowohl in benutzerdefiniertem Code als auch in Komponenten von Drittanbietern ermöglichen.

Bereitstellung

Alle Release-Artefakte werden durch **Code Signing** geschützt und während der Bereitstellung überprüft, um **Integrität**, **Authentizität** und eine kontrollierte Bereitstellung in Produktionsumgebungen zu gewährleisten.

Wartung

Nach der Bereitstellung werden die Systeme **einer** kontinuierlichen **Überwachung** und **einem** strukturierten **Patch-Management** unterzogen, um eine kontinuierliche Anpassung an sich entwickelnde Bedrohungen und **bewährte Sicherheitsverfahren** zu gewährleisten.

2.7.5 Regelmäßige Sicherheitsaudits und Penetrationstests

MyQ gewährleistet eine robuste Sicherheitsvalidierung durch systematische Test- und Bewertungsprogramme:

Automatisierte Penetrationstests: Die Integration mit der Qualys-Sicherheitsplattform ermöglicht eine kontinuierliche Schwachstellenbewertung und Penetrationstests für alle Software-Releases.

Sicherheitsbewertungen durch Dritte: Unabhängige Sicherheitsaudits, die von qualifizierten externen Organisationen durchgeführt werden, um Sicherheitskontrollen zu validieren und potenzielle Verbesserungen zu identifizieren.

Interne Sicherheitsüberprüfungen: Regelmäßige interne Bewertungen von Sicherheitsrichtlinien, Verfahren und technischen Kontrollen, um die kontinuierliche Wirksamkeit und Compliance sicherzustellen.

Prozess zur Reaktion auf Schwachstellen: Strukturierte Verfahren zur Behebung identifizierter Sicherheitsprobleme, einschließlich zeitlicher Vorgaben für die Entwicklung und Bereitstellung von Patches.

2.7.6 Software-Stückliste und Schwachstellenmanagement

MyQ implementiert umfassende Sicherheit in der Lieferkette durch detaillierte Komponentenverfolgung und Schwachstellenmanagement:

SBOM-Veröffentlichung: Vollständige Dokumentation der Software-Stückliste, in der alle in MyQ X-Systemen verwendeten Komponenten, Bibliotheken und Abhängigkeiten von Drittanbietern aufgeführt sind.

Automatisierte Schwachstellenscans: Kontinuierliche Überwachung der Komponentendatenbanken auf neu identifizierte Schwachstellen, die sich auf MyQ X-Abhängigkeiten auswirken.

Schnelles Patch-Management: Systematischer Prozess zur Bewertung, Prüfung und Bereitstellung von Sicherheitsupdates für Komponenten von Drittanbietern, wobei die Priorisierung auf der Grundlage einer Risikobewertung erfolgt.

Versionskontrolle von Komponenten: Detaillierte Nachverfolgung aller Softwarekomponenten, einschließlich Versionsnummern, Sicherheitspatch-Levels und Update-Zeitplänen, wie in den Versionshinweisen dokumentiert.

Sicherheitsbewertung von Lieferanten: Bewertung von Drittanbietern von Software, um sicherzustellen, dass sie angemessene Sicherheitsstandards und Prozesse zur Offenlegung von Schwachstellen einhalten.

Dieses umfassende Compliance-Framework stellt sicher, dass MyQ X vielfältige regulatorische Anforderungen erfüllt und gleichzeitig die höchsten Standards für Informationssicherheit und Datenschutz in allen Betriebsumgebungen einhält.

2.8 Implementierung der Zero-Trust-Architektur

MyQ X implementiert die Zero-Trust-Architektur als grundlegenden Sicherheitsansatz, der implizites Vertrauen eliminiert und jede Transaktion kontinuierlich validiert. Dieses umfassende Framework stellt sicher, dass kein Benutzer, kein Gerät und keine Netzwerkverbindung standardmäßig als vertrauenswürdig eingestuft wird, unabhängig von ihrem Standort oder ihrem vorherigen Authentifizierungsstatus.

2.8.1 Zero-Trust-Prinzipien im Druckmanagement

Die Zero-Trust-Implementierung von MyQ X basiert auf dem Prinzip **„niemals vertrauen, immer überprüfen“** im gesamten Druckmanagementsystem. Das System erfordert eine explizite Überprüfung für jede Zugriffsanfrage und stellt sicher, dass:

Verschlüsselte Kommunikationskanäle: Der gesamte Netzwerkverkehr nutzt eine obligatorische TLS-Verschlüsselung mit mindestens Version 1.2, um Abhören und Manipulationen während der Datenübertragung zu verhindern. HTTPS-Zertifikate müssen ordnungsgemäß konfiguriert und validiert sein, um Man-in-the-Middle-Angriffe zu verhindern.

Durchsetzung sicherer Protokolle: MyQ X blockiert unverschlüsselten HTTP-Datenverkehr und setzt strenge Sicherheitsprotokolle für alle Kommunikationskanäle durch, einschließlich SMTP-, LDAP- und SNMP-Verbindungen. Ältere Protokolle wie SNMPv1 sind zugunsten von SNMPv3 mit starker Authentifizierung verboten.

API-Sicherheitskontrollen: Der Zugriff auf die REST-API erfordert Authentifizierungstoken mit IP-Adressfilterung, um sicherzustellen, dass API-Aufrufe authentifiziert sind und aus vertrauenswürdigen Quellen stammen. Client-Geheimnisse werden regelmäßig rotiert, um die Sicherheitsintegrität aufrechtzuerhalten.

2.8.2 „Never Trust, Always Verify"-Methodik

Die Zero-Trust-Methodik durchdringt jeden Aspekt des MyQ X-Betriebs durch kontinuierliche Verifizierungsmechanismen:

Identitätsprüfung: Jede Benutzerinteraktion erfordert eine Authentifizierung, unabhängig vom Standort im Netzwerk oder dem Vertrauensstatus des Geräts. Benutzer müssen sich an jedem Druckgerät authentifizieren, auch wenn sie sich zuvor an anderer Stelle in der Organisation angemeldet haben.

Geräteauthentifizierung: Druckgeräte selbst müssen sich vor dem Zugriff auf Netzwerkressourcen mit eindeutigen Anmeldedaten und Zertifikaten authentifizieren, um unbefugtes Gerätespoofing zu verhindern.

Sitzungsmanagement: Benutzersitzungen verfügen über eine automatische Zeitüberschreitungs- und Abmeldefunktion, die sicherstellt, dass verlassene Sitzungen nicht von unbefugten Personen ausgenutzt werden können.

2.8.3 Segmentierung und Netzwerkisolierung

MyQ X implementiert eine umfassende Netzwerksegmentierung, um Angriffsflächen zu begrenzen und potenzielle Sicherheitsverletzungen einzudämmen:

Netzwerkgrenzkontrollen: Das System erzwingt strenge Firewall-Regeln, die ungenutzte Ports blockieren und den Netzwerkzugriff auf die notwendigen Kommunikationskanäle beschränken. In den Standardkonfigurationen sind unnötige Dienste und Protokolle deaktiviert.

Zertifikatsbasierte Segmentierung: MyQ X unterstützt drei Zertifikatsverwaltungsmodi – integrierte Zertifizierungsstelle, Unternehmenszertifizierungsstelle und manuelle Zertifikatsverwaltung –, sodass Unternehmen entsprechend ihren Sicherheitsrichtlinien geeignete Vertrauensgrenzen implementieren können.

FQDN-Durchsetzung: Die gesamte Netzwerkkommunikation muss vollständig qualifizierte Domänennamen (FQDN) anstelle von IP-Adressen oder

Einfachbezeichnungen verwenden, um DNS-basierte Man-in-the-Middle-Angriffe zu verhindern und eine ordnungsgemäße Zertifikatsvalidierung sicherzustellen.

Portverwaltung: Das System verwaltet automatisch Firewall-Regeln und bietet eine explizite Kontrolle darüber, auf welche Netzwerkports zugegriffen werden kann, wodurch die Angriffsfläche durch systematische Portblockierung reduziert wird.

2.8.4 Robuste Authentifizierung und Verifizierung

MyQ X gewährleistet eine kontinuierliche Sicherheitsvalidierung durch mehrere Authentifizierungsebenen und Echtzeitüberwachung:

Multi-Method-Authentifizierung: Das System unterstützt verschiedene Authentifizierungsmethoden, darunter LDAP, Microsoft Entra ID, RADIUS und lokale MyQ-Authentifizierung, mit automatischen Failover-Funktionen, die eine kontinuierliche Zugriffskontrolle gewährleisten.

Integration von Authentifizierungsservern: Die sichere Integration mit externen Authentifizierungsservern nutzt verschlüsselte Verbindungen (TLS für LDAP, sichere Protokolle für RADIUS) und erzwingt starke gemeinsame Geheimnisse, die für jede MyQ-Bereitstellung spezifisch sind.

Anmeldeüberwachung: Eine verbesserte Protokollierung von Authentifizierungsereignissen, insbesondere fehlgeschlagenen Anmeldeversuchen, ermöglicht es Administratoren, potenzielle Sicherheitsbedrohungen zu erkennen und darauf zu reagieren. Fehlgeschlagene Authentifizierungsversuche lösen automatische Sperrmechanismen aus – standardmäßig werden Geräte nach mehr als 5 ungültigen Versuchen innerhalb von 60 Sekunden für 5 Minuten gesperrt.

Steuerung der Sitzungsdauer: Das System implementiert konfigurierbare Richtlinien für das Ablaufen von Sitzungen und eine automatische Abmeldefunktion, um sicherzustellen, dass inaktive Sitzungen nicht ausgenutzt werden können.

2.8.5 Geräte- und Endpunktüberprüfung

MyQ X erzwingt strenge Geräteüberprüfungsprotokolle, um sicherzustellen, dass nur autorisierte Endpunkte auf Druckressourcen zugreifen können:

Gerätezertifikatsverwaltung: Alle verbundenen Geräte müssen gültige Zertifikate für die Netzwerkkommunikation vorweisen. Das System unterhält einen umfassenden Zertifikatsspeicher mit ordnungsgemäßer Kettenvalidierung und unterstützt die automatische Zertifikatsbereitstellung über Gruppenrichtlinien oder Mobile Device Management (MDM).

Endpunkt-Sicherheitskontrollen: Druckgeräte werden einer kontinuierlichen Sicherheitsüberprüfung unterzogen, einschließlich SNMP v3-Authentifizierung mit starken Passwörtern und kryptografischen Algorithmen (SHA1 und AES). Die Anmeldedaten für Drucker werden über herstellerspezifische Sicherheitsprotokolle mit zufällig generierten starken Passwörtern verwaltet.

Authentifizierung mobiler Geräte: MyQ X Mobile Client implementiert OAuth 2.0 Device Authorization Grant für die sichere Authentifizierung mobiler Geräte und ersetzt damit ältere PIN-basierte Systeme durch moderne biometrische Sicherheitsfunktionen.

BYOD-Sicherheitsframework: Das System unterstützt Bring-Your-Own-Device (BYOD)-Umgebungen durch sichere Druckübertragung über AirPrint und Mopria und hält auch in Netzwerken ohne direkte Sichtbarkeit des Druckservers an den Zero-Trust-Prinzipien fest.

Zugriffstoken-Verwaltung: Für jeden Gerätetyp werden eindeutige Zugriffstoken ausgegeben, wobei Transport Layer Security (TLS) für die gesamte Kommunikation obligatorisch ist. Das System implementiert Just-in-Time-Zugriffskontrollen (JIT), die die Berechtigungen basierend auf dem Kontext und einer kontinuierlichen Risikobewertung dynamisch anpassen.

Diese umfassende Zero-Trust-Implementierung stellt sicher, dass MyQ X die höchsten Sicherheitsstandards einhält und gleichzeitig vielfältige organisatorische Anforderungen und Einsatzszenarien unterstützt. Die Architektur bietet einen umfassenden Schutz, der sich an die sich ständig weiterentwickelnde Bedrohungslandschaft anpasst und gleichzeitig die betriebliche Effizienz und Benutzerfreundlichkeit gewährleistet.

2.9 Identitäts- und Zugangsmanagement

MyQ X bietet ein umfassendes Identitäts- und Zugriffsmanagement-Framework, das sich nahtlos in bestehende Authentifizierungssysteme von Unternehmen integrieren lässt und moderne Sicherheitsstandards unterstützt. Die IAM-Architektur gewährleistet eine sichere, skalierbare und flexible Benutzerauthentifizierung in verschiedenen Unternehmensumgebungen.

2.9.1 Implementierung der Multi-Faktor-Authentifizierung

MyQ X implementiert robuste **Multi-Faktor-**Authentifizierungsfunktionen **(MFA),** die die Sicherheit durch die Anforderung mehrerer Verifizierungsfaktoren erheblich verbessern:

Embedded Terminal: Zu den Standard-MFA-Methoden gehören Kombinationen aus ID-Karte und PIN, bei denen Benutzer zunächst ihre physische ID-Karte vorlegen und dann ihre Identität mit einem PIN-Code bestätigen. Alternativ bietet die ID-Karten- und Passwortauthentifizierung eine ähnliche Zwei-Faktor-Sicherheit mit Passwortüberprüfung anstelle einer PIN.

Mobilgerätebasierte Authentifizierung: Der MyQ X Mobile Client ermöglicht eine ausgeklügelte MFA durch QR-Code-Scannen in Kombination mit biometrischer Verifizierung. Benutzer authentifizieren sich durch Scannen eines auf dem Embedded Terminal angezeigten QR-Codes, wobei zusätzliche Sicherheit durch biometrische Sperren (Face ID oder Fingerabdruck) auf ihren Mobilgeräten gewährleistet wird.

Desktop Client-Integration: Unternehmen, die Microsoft 365-Dienste nutzen, profitieren von einer integrierten MFA durch Entra ID-Authentifizierung. Benutzer, die in ihren Entra ID-Konten die Zwei-Faktor-Authentifizierung aktiviert haben, werden beim Zugriff auf den Desktop-Client automatisch aufgefordert, ihre Identität mithilfe von Authentifizierungsanwendungen zu überprüfen.

2.9.2 OAuth 2.0-Geräteautorisierung

MyQ X unterstützt den **OAuth 2.0 Authorization Code Grant**-Standard und ermöglicht so eine sichere Integration mit modernen Identitätsanbietern und Anwendungen von Drittanbietern:

Standard-OAuth-Ablauf: Das System implementiert das vollständige OAuth 2.0-Autorisierungsframework, einschließlich der Darstellung der Anmeldeseite, der Generierung von Einmal-Zugangscodes und der sicheren Token-Abrufung. Client-Anwendungen erhalten Bearer-Token mit konfigurierbaren Ablaufzeiten und gewährten Berechtigungsbereichen.

API-Integrationssicherheit: OAuth-Token müssen für alle API-Endpunktzugriffe bereitgestellt werden, um sicherzustellen, dass Integrationen von Drittanbietern eine ordnungsgemäße Authentifizierung aufrechterhalten. Das System unterstützt die Validierung von Client-IDs und Client-Geheimnissen mit sicherer URI-Umleitung.

Token-Verwaltung: Zugriffstoken umfassen Ablaufkontrollen (standardmäßig 1800 Sekunden) und Bereichsbeschränkungen, wodurch eine detaillierte Kontrolle über API-Zugriffsberechtigungen ermöglicht und gleichzeitig die Sicherheit durch Token-Rotation gewährleistet wird.

2.9.3 Single-Sign-On-Integrationsfunktionen

MyQ X bietet eine umfassende **Single-Sign-On**-Integration **(SSO),** die die Benutzerauthentifizierung in Unternehmensumgebungen optimiert:

Microsoft 365-Integration: Die tiefe Integration mit Microsoft Entra ID ermöglicht nahtloses SSO für Unternehmen, die Microsoft 365-Dienste nutzen. Benutzer können sich mit ihren bestehenden Microsoft-Anmeldedaten authentifizieren, sodass keine separaten MyQ-Passwörter erforderlich sind.

Unternehmensverzeichnis-Dienste: Die SSO-Funktionen erstrecken sich auf verschiedene Authentifizierungsserver, darunter Active Directory, OpenLDAP und Novell eDirectory, sodass Benutzer ihre vorhandenen Unternehmensanmeldedaten für den Zugriff auf MyQ verwenden können.

Plattformübergreifende Authentifizierung: Die SSO-Funktionalität funktioniert über alle MyQ X-Komponenten hinweg, einschließlich Desktop Client, Mobile Client und Embedded Terminal, und bietet unabhängig von der Zugriffsmethode ein einheitliches Authentifizierungserlebnis.

2.9.4 Rollenbasierte Zugriffskontrolle (RBAC)

MyQ X implementiert **eine** ausgeklügelte **rollenbasierte Zugriffskontrolle,** die den Sicherheitsanforderungen von Unternehmen entspricht:

Detaillierte Berechtigungsverwaltung: Das System bietet eine detaillierte Kontrolle über Benutzerberechtigungen, sodass Administratoren spezifische Zugriffsrechte basierend auf organisatorischen Rollen und Verantwortlichkeiten definieren können.

Gruppenbasierte Verwaltung: Die RBAC-Implementierung unterstützt sowohl individuelle Benutzerberechtigungen als auch gruppenbasierte Zugriffskontrolle und ermöglicht so eine effiziente Verwaltung großer Benutzergruppen durch die Zuweisung von Sicherheitsgruppen.

Durchsetzung des Prinzips der geringsten Privilegien: Die Zugriffskontrollen folgen dem Prinzip der geringsten Privilegien und stellen sicher, dass Benutzer nur die für ihre Aufgaben erforderlichen Mindestberechtigungen erhalten, während die betriebliche Effizienz erhalten bleibt.

2.9.5 Entra ID Multi-Tenant-Unterstützung

MyQ X bietet robuste Unterstützung für **Microsoft Entra ID-Mandantenumgebungen**:

Mandantenübergreifende Authentifizierung: Das System kann Benutzer über mehrere Entra ID-Mandanten hinweg authentifizieren und unterstützt so komplexe Organisationsstrukturen mit mehreren Azure AD-Instanzen.

Mandantenisolierung: Die Multi-Tenant-Unterstützung umfasst geeignete Isolierungsmechanismen, die den mandantenübergreifenden Datenzugriff verhindern und gleichzeitig die zentralisierten MyQ-Verwaltungsfunktionen aufrechterhalten.

Hybrides Identitätsmanagement: Die Integration unterstützt sowohl reine Cloud- als auch hybride Identitätsszenarien und eignet sich für Unternehmen mit lokalem Active Directory, das mit Entra ID synchronisiert ist.

2.9.6 LDAP- und Active Directory-Integration

MyQ X bietet umfassende **LDAP- und Active Directory-**Integrationsfunktionen:

Flexible Synchronisierungsoptionen: Das System unterstützt mehrere Synchronisierungsmethoden, darunter vollständige Synchronisierung, selektive Attributsynchronisierung und bedingte Synchronisierung basierend auf LDAP-Filtern. Administratoren können zwischen vollständigem Ersetzen, nur Hinzufügen oder bedingten Aktualisierungen für Karten- und PIN-Eigenschaften wählen.

Erweiterte Filterfunktionen: Die LDAP-Synchronisierung umfasst ausgefeilte Filteroptionen unter Verwendung der Standard-LDAP-Filtersyntax, die einen selektiven Benutzerimport basierend auf Organisationseinheiten, Gruppenmitgliedschaften oder benutzerdefinierten Attributen ermöglichen.

Import der Gruppenstruktur: Das System kann komplette Organisationsstrukturen einschließlich Sicherheitsgruppen, Verteilergruppen und verschachtelten Gruppenhierarchien aus Active Directory importieren und dabei die organisatorischen Beziehungen innerhalb von MyQ beibehalten.

Sichere Authentifizierung: Die gesamte LDAP-Kommunikation nutzt TLS-Verschlüsselung, um Anmeldedaten und Benutzerdaten während der Synchronisierung zu schützen. Das System unterstützt sowohl herkömmliches LDAP über TLS als auch sichere LDAP-Verbindungen.

2.9.7 Verwaltung temporärer PINs und Sicherheitsrichtlinien

MyQ X implementiert umfassende **PIN-Verwaltungs- und Sicherheitsrichtlinien**:

Verbesserte PIN-Sicherheit: Version 10.2 führt eine verbesserte PIN-Sicherheit ein, einschließlich einer obligatorischen Mindestlänge von 6 Ziffern und der Verhinderung leicht zu erratender Kombinationen wie „1234“ oder „1111“.

Ausgabe temporärer PINs: Das System unterstützt temporäre PIN-Codes, die für bestimmte Zeiträume oder Einmal-Szenarien ausgegeben werden können und zusätzliche Sicherheit für Gastzugänge oder Zeitarbeitskräfte bieten.

Durchsetzung von PIN-Richtlinien: Konfigurierbare PIN-Richtlinien ermöglichen es Unternehmen, Komplexitätsanforderungen, Ablaufzeiten und Wiederverwendungsbeschränkungen festzulegen, die den Sicherheitsstandards des Unternehmens entsprechen.

Schutz bei fehlgeschlagener Authentifizierung: Die verbesserte Sicherheit umfasst die automatische Sperrung von Authentifizierungsversuchen nach wiederholten Fehlversuchen (Standard: 5 Minuten Sperrung nach 5 fehlgeschlagenen Versuchen innerhalb von 60 Sekunden).

2.9.8 Unterstützung biometrischer Authentifizierung

MyQ X nutzt moderne **biometrische Authentifizierungsfunktionen** durch die Integration mobiler Geräte:

Integration mobiler Biometrie: Der MyQ X Mobile Client unterstützt biometrische Authentifizierungsmethoden wie Face ID auf iOS-Geräten und Fingerabdruckerkennung auf Android-Geräten und bietet so eine nahtlose und dennoch sichere Zugriffskontrolle.

Multimodale Authentifizierung: Die biometrische Authentifizierung funktioniert in Verbindung mit gerätebasierter Sicherheit und schafft so ein multimodales Authentifizierungssystem, das etwas, das der Benutzer hat (Mobilgerät), mit etwas, das er ist (biometrische Merkmale), kombiniert.

2.10 Sicherheit der Infrastruktur

MyQ X bietet eine robuste Infrastruktursicherheit, die die gesamte Druckverwaltungsumgebung vor sich ständig weiterentwickelnden Cyber-Bedrohungen schützt. Die Plattform umfasst mehrere Verteidigungsebenen zum Schutz von Servern, Datenbanken, Netzwerkkommunikation und Softwareintegrität und gewährleistet so Betriebssicherheit und Datenvertraulichkeit.

2.10.1 Sicherheit der Print Server

MyQ X-Print Server werden mithilfe von Best-Practice-Sicherheitskonfigurationen gehärtet, die in den Einstellungen **der Datei „config.ini“** definiert sind, darunter:

- Einschränkung von Diensten und Prozessen, um die Angriffsfläche zu begrenzen.
- Aktivierung sicherer Kommunikationsprotokolle und Deaktivierung veralteter unsicherer Optionen.
- Strenge Zuweisung von Benutzerrechten, Vermeidung von Administratorrechten, wo diese nicht erforderlich sind.
- Regelmäßige automatische Updates und Sicherheitspatches, um neu entdeckte Schwachstellen zu beheben.
- Konfiguration von Firewall-Regeln und Port-Beschränkungen, um unbefugten Netzwerkverkehr zu blockieren.

Diese Maßnahmen reduzieren das Risiko von Missbrauch und gewährleisten die Verfügbarkeit des Systems auch unter Angriffsbedingungen.

2.10.2 Datenbankverschlüsselung (Firebird 4.0-Implementierung)

MyQ X verwendet die Datenbank-Engine **Firebird 4.0**, die erweiterte Verschlüsselungsfunktionen zum Schutz sensibler Daten im Ruhezustand und während Sicherungsvorgängen bietet. Zu den wichtigsten Verschlüsselungsfunktionen gehören:

- AES-256-Verschlüsselung von Datenbankdateien, um unbefugten Datenzugriff zu verhindern.
- Verschlüsselte Speicherung von Passwörtern und Schlüsseln innerhalb des Datenbanksystems.
- Verschleierung sensibler Datenbankinhalte in Protokollen und Diagnosen.

Dies gewährleistet die Einhaltung der Datenschutzbestimmungen und verhindert die Gefährdung der Druckauftragsabrechnung und der Benutzerinformationen.

2.10.3 TLS 1.2/1.3-Durchsetzung und Zertifikatsverwaltung

Zum Schutz der Daten während der Übertragung erzwingt MyQ X standardmäßig mindestens das **TLS 1.2**-Protokoll, mit optionalem Upgrade auf TLS 1.3 für erhöhte Sicherheit und Leistung. Die Plattform unterstützt flexible Zertifikatsverwaltungsmodi:

- Automatische Generierung einer privaten Stammzertifizierungsstelle (CA), die Server- und Client-Zertifikate signiert.

- Integration von unternehmensverwalteten Zwischen-CAs, die vertrauenswürdige Ketten und eine zentralisierte Zertifikatskontrolle ermöglichen.
- Unterstützung für die manuelle Installation von Zertifikaten, einschließlich Zertifikaten von Drittanbietern/öffentlichen Zertifizierungsstellen.

Zertifikate und private Schlüssel werden sicher mit verschlüsseltem Schutz gespeichert, und Clients erhalten vertrauenswürdige Zertifikate über Gruppenrichtlinien oder die Verwaltung mobiler Geräte.

2.10.4 Sicherheit der Netzwerkkommunikation

MyQ X sichert alle Netzwerkkommunikationskanäle durch:

- den gesamten unverschlüsselten HTTP-Datenverkehr blockiert und ausschließlich HTTPS zulässt.
- Verschlüsselung von SMTP-, LDAP- und RADIUS-Datenverkehr mit TLS zum Schutz der Authentifizierung und des E-Mail-Flusses.
- Veraltete und anfällige Protokolle wie POP3 und STARTTLS-Ersatzprotokolle werden deaktiviert.
- SNMPv3 mit starker Authentifizierung und kryptografischen Algorithmen einsetzt, um Geräte sicher zu überwachen und zu verwalten.

Diese Kontrollen verhindern Abhören, Spoofing und Man-in-the-Middle-Angriffe im gesamten Netzwerk.

2.10.5 Firewall-Konfiguration und Port-Verwaltung

MyQ X reduziert Angriffsflächen durch:

- Deaktivierung von Firewall-Regeln für ungenutzte Netzwerkports und Protokolle.
- die detaillierte Kontrolle darüber ermöglicht, welche Ports basierend auf den Netzwerkrichtlinien des Unternehmens freigegeben werden.

Dadurch werden die Eingänge auf diejenigen beschränkt, die für Druckdienste unerlässlich sind, wodurch die Perimeterverteidigung verbessert wird.

2.10.6 API-Sicherheit und Authentifizierungstoken

APIs erzwingen mehrere Sicherheitsebenen:

- Das OAuth 2.0 Authorization Code Grant Framework sichert den API-Zugriff durch kurzlebige Bearer-Token und Bereichsbeschränkungen.
- Die Tokens werden anhand der IP-Adressen der Clients validiert und erfordern sichere Client-Anmeldedaten.

- Regelmäßige Geheimnisrotationen schützen vor dem Verlust von Anmeldedaten.

Dies schützt API-Endpunkte vor unbefugten Anfragen und Missbrauch.

2.10.7 Prozessisolierung und Sandboxing

MyQ X-Druckverwaltungsanwendungen werden mit **Prozessisolierung** ausgeführt, um zu verhindern, dass kompromittierte Komponenten das gesamte System beeinträchtigen. Soweit möglich, werden virtuelle Maschinen oder containerisierte Sandboxing-Lösungen eingesetzt, um Sicherheitsverletzungen einzudämmen und laterale Bewegungen innerhalb der Umgebung zu begrenzen.

2.10.8 Code-Signierung und Integritätsprüfung

Alle MyQ-Software-Binärdateien und Installationsprogramme sind **codesigniert,** um Authentizität und Integrität zu gewährleisten. Dadurch wird sichergestellt, dass Kunden verifizierte Softwareversionen installieren, die frei von Manipulationen oder unbefugten Änderungen sind.

2.11 Datenschutz und Verschlüsselung

MyQ X implementiert umfassenden Datenschutz und Verschlüsselung während des gesamten Dokumentlebenszyklus und gewährleistet so Vertraulichkeit und Integrität vom ersten Druckauftrag bis zur endgültigen Ausgabe und Archivierung.

2.11.1 End-to-End-Verschlüsselung

MyQ X bietet **eine End-to-End-Verschlüsselung** über alle Kommunikationskanäle und Datenspeicherpunkte hinweg:

Verschlüsselte Kommunikationskanäle: Der gesamte Netzwerkverkehr nutzt standardmäßig die obligatorische TLS-Verschlüsselung mit mindestens Version 1.2. HTTPS wird für alle Webschnittstellen, die Kommunikation zwischen Servern und Client-Verbindungen erzwungen.

Zertifikatsbasierte Sicherheit: Mehrere Zertifikatsverwaltungsmodi unterstützen organisatorische Anforderungen, von der integrierten Zertifizierungsstelle bis hin zur Integration von Unternehmens-PKI und öffentlichen CA-Zertifikaten. Private Schlüssel werden durch zufällig generierte Passwörter geschützt, die in verschlüsselter Form in der Firebird-Datenbank gespeichert sind.

Protokollsicherheit: Die TLS-Verschlüsselung wird für die Protokolle SMTP, LDAP, RADIUS und SNMP erzwungen, um sicherzustellen, dass keine sensiblen Daten im Klartext übertragen werden.

2.11.2 Verschlüsselung ruhender Daten

MyQ X schützt gespeicherte Daten durch mehrere Verschlüsselungsebenen:

Datenbankverschlüsselung: Die Firebird 4.0-Datenbank unterstützt die Verschlüsselung mit benutzerdefinierten Zertifikaten mit „Encrypting File System“ Enhanced Key Usage (EKU). Zertifikate müssen sich in bestimmten Zertifikatsspeichern des Computers befinden, wobei der persönliche Speicher bevorzugt wird.

Dateisystemschutz: Auf dem MyQ X Print Server gespeicherte Druck- und Scanauftragsdateien können mit benutzerdefinierten Zertifikaten verschlüsselt werden, die von Administratoren bereitgestellt werden und einen zusätzlichen Schutz über die Dateisystemberechtigungen hinaus bieten.

Vollständige Festplattenverschlüsselung: MyQ X unterstützt die Integration mit Technologien zur vollständigen Festplattenverschlüsselung wie Microsoft BitLocker, um alle auf dem Print Server gespeicherten Daten zu schützen, einschließlich der Datenbank, Zertifikate und temporären Dateien.

2.11.3 Schutz von Daten während der Übertragung (TLS-Verschlüsselung)

MyQ X erzwingt strenge **TLS-Verschlüsselungsstandards** für die gesamte Netzwerkkommunikation:

Mindestens TLS 1.2: Die Standardkonfiguration erfordert mindestens TLS 1.2, mit optionalem Upgrade auf TLS 1.3 für verbesserte Sicherheit und Leistung. Ältere Protokolle wie SSL und ältere TLS-Versionen werden blockiert.

Cipher Suite Management: Das System implementiert starke Verschlüsselungssuiten und deaktiviert anfällige Algorithmen, um kryptografische Angriffe zu verhindern. SNMPv3-Kommunikationen verwenden SHA1- und AES-Verschlüsselung.

Zertifikatsvalidierung: Alle TLS-Verbindungen erfordern eine ordnungsgemäße Zertifikatsvalidierung unter Verwendung vollqualifizierter Domänennamen (FQDN), um Man-in-the-Middle-Angriffe zu verhindern. START TLS wird aufgrund von MITM-Schwachstellen vermieden.

2.11.4 Verschlüsselung und sichere Speicherung von Druckaufträgen

MyQ X bietet mehrere Mechanismen zum Schutz von Druckaufträgen während ihres gesamten Lebenszyklus:

Sichere Druckfreigabe: Druckaufträge werden sicher auf dem MyQ-Server gespeichert, bis sich Benutzer am Gerät authentifizieren, wodurch unbefugter Zugriff auf Dokumente in den Ausgabefächern des Druckers verhindert wird.

Verschlüsselung von Auftragsdateien: Administratoren können die Auftragsverschlüsselung durch Bereitstellung benutzerdefinierter Zertifikate aktivieren, um sicherzustellen, dass Druckauftragsdateien während der Speicherung auf dem Server bis zur Freigabe verschlüsselt bleiben.

Private Warteschlangen: Bei streng vertraulichen Dokumenten löschen private Warteschlangen Druckaufträge automatisch unmittelbar nach der Freigabe, wodurch das Risiko eines längeren unbefugten Zugriffs ausgeschlossen wird.

Datenschutzmodus: Wenn der Datenschutzmodus aktiviert ist, werden Dokumentnamen für alle Benutzer außer dem Dokumentbesitzer maskiert, wodurch die Offenlegung von Informationen durch Auftragsnamen verhindert wird. Selbst Administratoren können die Auftragsnamen anderer Benutzer nicht einsehen.

2.11.5 Verbesserungen bei der Datenbankverschlüsselung

Die **Firebird 4.0**-Datenbankimplementierung bietet erweiterte Verschlüsselungsfunktionen:

Benutzerdefinierte Zertifikatsverschlüsselung: Datenbankdateien werden mit Zertifikaten mit EFS Extended Key Usage verschlüsselt, was einen starken Schutz vor unbefugtem Datenbankzugriff bietet.

Passwortschutz: Datenbankpasswörter werden in Protokolldateien verschleiert, wodurch die Offenlegung von Anmeldedaten während der Fehlerbehebung und Überwachung verhindert wird.

Verschärfte Berechtigungen: Der MyQ-Datenordner, der die Benutzerdatenbank und die privaten TLS-Zertifikatsschlüssel enthält, ist nur für Administratoren, SYSTEM und das MyQ-Dienstkonto zugänglich, wodurch der standardmäßige Lesezugriff für alle Benutzer aufgehoben wird.

2.11.6 Sicherheitsverschlüsselung und sichere Speicherung

MyQ X stellt sicher, dass Backups das gleiche Sicherheitsniveau wie Produktionsdaten aufweisen:

Verschlüsselte Backups: Datenbank-Backups werden durch sichere, zufällig generierte Passwörter geschützt, die eine unbefugte Wiederherstellung oder den Zugriff auf Backup-Dateien verhindern.

Sichere Speicherung von Backups: Backup-Dateien sollten an sicheren Orten mit geeigneten Zugriffskontrollen und Verschlüsselung im Ruhezustand gespeichert werden, um die Vertraulichkeit der Daten während des gesamten Backup-Lebenszyklus zu gewährleisten.

2.11.7 Richtlinien für die Schlüsselverwaltung und -rotation

MyQ X implementiert sichere Schlüsselverwaltungsverfahren:

Zertifikatsrotation: Zertifikate können gemäß den Sicherheitsrichtlinien des Unternehmens regelmäßig rotiert werden, wobei die automatisierte Bereitstellung über Gruppenrichtlinien oder die Verwaltung mobiler Geräte unterstützt wird.

Schutz privater Schlüssel: Alle privaten Schlüssel für Zertifikate und CA-Vorgänge werden durch zufällig generierte Passwörter geschützt, die in verschlüsselter Form in der Datenbank gespeichert sind.

Rotation von API-Geheimnissen: REST-API-Client-Geheimnisse sollten regelmäßig rotiert werden, um die Sicherheit zu gewährleisten. Das System unterstützt die Geheimnisrotation ohne Unterbrechung des Dienstes.

2.11.8 Datenminimierung und eingebauter Datenschutz

MyQ X implementiert **die Grundsätze des Datenschutzes durch Technikgestaltung gemäß der DSGVO**:

Begrenzte Datenerfassung: Das System erfasst nur die für die Betriebsfunktionalität erforderlichen Metadaten und vermeidet so die unnötige Verarbeitung personenbezogener Daten, die das Datenschutzrisiko erhöhen könnte.

Automatische Löschung: Administratoren können automatische Löschfristen für Druck- und Scan-Auftragsdateien konfigurieren, um sicherzustellen, dass Daten nur so lange aufbewahrt werden, wie es für geschäftliche Zwecke erforderlich ist.

Rechte der Nutzer: Vollständige Umsetzung der Nutzerrechte gemäß DSGVO, einschließlich Datenzugriff, Anonymisierung und Recht auf Vergessenwerden, mit anpassbaren Datenschutzhinweisen auf den Benutzeroberflächen.

Sitzungsmanagement: Die automatische Abmeldefunktion stellt sicher, dass Benutzersitzungen ordnungsgemäß beendet werden, und verhindert so unbefugten Zugriff über verlassene Sitzungen.

Dieses umfassende Datenschutz- und Verschlüsselungsframework stellt sicher, dass MyQ X die höchsten Standards für Datenvertraulichkeit und -integrität einhält und gleichzeitig die gesetzlichen Compliance-Anforderungen in verschiedenen Unternehmensumgebungen unterstützt.

2.12 Sichere Druck-Workflows

MyQ X bietet umfassende sichere Druck-Workflows, die dem Benutzer die vollständige Kontrolle über die Freigabe von Dokumenten ermöglichen und gleichzeitig verhindern, dass vertrauliche Informationen in den Ausgabefächern der Drucker sichtbar werden. Diese Workflows sind für Unternehmen unerlässlich, die strenge Dokumentensicherheit und Benutzerverantwortlichkeit benötigen.

2.12.1 Implementierung der sicheren Druckfreigabe

Hold Print stellt sicher, dass Druckaufträge niemals sofort an den Drucker freigegeben werden. Die Dokumente werden sicher auf dem MyQ-Server gespeichert und erst gedruckt, nachdem sich der autorisierte Benutzer am Druckgerät authentifiziert hat, wodurch verhindert wird, dass unbeaufsichtigte Dokumente in den Ausgabefächern zurückbleiben.

Pull Print erweitert dies noch weiter, indem es Benutzern ermöglicht, ihre Aufträge auf jedem geeigneten Gerät innerhalb des Drucksystems freizugeben, nicht nur auf dem Gerät, an das sie den Auftrag ursprünglich gesendet haben. Diese Flexibilität ist besonders wertvoll während der Wartung von Geräten oder wenn Benutzer von verschiedenen Standorten aus drucken müssen.

Mehrere Authentifizierungsmethoden unterstützen die sichere Druckfreigabe, darunter PIN-Codes, ID-Karten, Passwörter, QR-Codes mit biometrischer Verifizierung und Kombinationen aus Zwei-Faktor-Authentifizierung. Diese Flexibilität wird den unterschiedlichen Sicherheitsanforderungen von Unternehmen gerecht.

2.12.2 Pull-Printing-Workflows

Pull Print bietet sowohl Administratoren als auch Endbenutzern erhebliche Vorteile:

Vorteile für Administratoren:

- Keine Stapel unbeaufsichtigter Dokumente auf Bürodruckern mehr
- Durchsetzung verantwortungsbewussten Druckverhaltens und von Dokumentensicherheitsrichtlinien

- Verwalten Sie alle Druckaufträge über eine einzige einheitliche Druckwarteschlange
- Reduzierung von Druckabfällen und damit verbundenen Kosten durch Vorschau- und Anpassungsoptionen
- Unterstützung flexibler Druckvorgänge auf mehreren Geräten

Vorteile für den Benutzer:

- Vertrauliche Dokumente bleiben sicher, bis sie ausdrücklich freigegeben werden
- Drucken auf jedem autorisierten Gerät im Unternehmen
- Vorschau der Dokumente auf dem Embedded Terminal vor der Freigabe
- Ändern Sie die Druckoptionen (Farbe, Duplex, Finishing) auch nach der Auftragsübermittlung
- Ändern Sie die Druckziele am Gerät, wenn der ursprüngliche Drucker nicht verfügbar ist

2.12.3 Zeitlimit für Druckaufträge und automatisches Löschen

MyQ X implementiert automatische Bereinigungsverfahren, um eine längere Sichtbarkeit von Dokumenten zu verhindern:

Konfigurierbare Aufbewahrungsfristen: Administratoren legen fest, wie lange Druckauftragsdateien auf dem MyQ-Server gespeichert werden, bevor sie automatisch gelöscht werden, und gleichen so betriebliche Anforderungen mit Sicherheitsanforderungen ab.

Zeitüberschreitungsmanagement für Aufträge: Aufträge, die nicht innerhalb eines bestimmten Zeitraums freigegeben werden, werden automatisch aus der Warteschlange entfernt, wodurch verhindert wird, dass vergessene oder zurückgelassene Dokumente sich auf den Servern ansammeln.

Automatische Abmeldung: Gerätesitzungen werden nach vom Administrator festgelegten Zeiträumen automatisch beendet, wodurch unbefugter Zugriff auf Dokumente an verlassenen Terminals verhindert wird.

2.12.4 Wasserzeichen und digitale Signaturen

Wasserzeichen ermöglichen die Rückverfolgbarkeit von Dokumenten, indem sie gedruckten Seiten anpassbare Überlagerungen hinzufügen, die Folgendes enthalten können:

- Vertraulichkeitskennzeichnungen
- Druckdaten und Zeitstempel
- Name der Person, die das Dokument gedruckt hat

- Informationen zur Identifizierung des Druckers

Diese Wasserzeichen können auf jede Seite oder ausgewählte Seiten angewendet werden und schaffen so einen Prüfpfad, der dabei hilft, durchgesickerte Dokumente zu identifizieren und zu ihrer Quelle zurückzuverfolgen.

2.12.5 Auftragsvorschau und Inhaltsvalidierung

Mit der **Job-Vorschau**-Engine können Administratoren Druckaufträge vor der Freigabe überprüfen:

Unterstützte Formate: Die Vorschaufunktion unterstützt die drei gängigsten Seitenbeschreibungssprachen – PCL 5, PCL 6 und PostScript.

Präventive Kontrolle: Administratoren können nicht autorisierte Druckaufträge ablehnen, bevor sie das Druckgerät erreichen, wodurch Richtlinienverstöße verhindert und sensible Informationen geschützt werden.

Inhaltsbasierte Filterung: Durch die Integration mit OCR- und Dokumentenmanagementsystemen können Scan-Richtlinien auf der Grundlage einer Analyse des Dokumentinhalts durchgesetzt werden.

2.12.6 Fehlerbehandlung und sichere Auftragswiederherstellung

MyQ X implementiert eine robuste Fehlerbehandlung, um die Sicherheit bei Gerätefehlfunktionen aufrechtzuerhalten:

Gerätefehlerschutz: Wenn ein Druckgerät in einen Fehlerzustand gerät (Papierstau, Tonermangel), werden Dokumente zurückgehalten und nicht automatisch gedruckt, sobald der Fehler behoben ist, sodass der Benutzer die Kontrolle über den Zeitpunkt der Freigabe behält.

Sitzungserhaltung: Wenn ein Gerät während einer Sitzung nicht mehr verfügbar ist, behält das MyQ-System die Benutzersitzung bei und ermöglicht die Fortsetzung auf alternativen Geräten, ohne dass der Dokumentstatus verloren geht.

Automatische Geräteabmeldung: Bei Gerätefehlern löscht die automatische Abmeldung den Speicher des Geräts, um einen unbefugten Zugriff auf Dokumente durch Wartungspersonal oder andere Benutzer zu verhindern.

Diese umfassende Architektur für sichere Druck-Workflows gewährleistet, dass Unternehmen während des gesamten Drucklebenszyklus eine strenge Kontrolle über die Dokumentensicherheit behalten und gleichzeitig die betriebliche Flexibilität und die Produktivität der Benutzer unterstützen.

2.13 Geräte- und Netzwerksicherheit

MyQ X bietet umfassende Geräte- und Netzwerksicherheitskontrollen, um Multifunktionsgeräte (MFDs), Drucker und die Netzwerkinfrastruktur vor unbefugtem Zugriff und Missbrauch zu schützen.

2.13.1 Sicherheitshärtung für Multifunktionsgeräte

Unternehmen, die MyQ X mit MFDs einsetzen, sollten bewährte Sicherheitsverfahren implementieren, darunter:

Gerätezugriffskontrollen: Beschränken Sie den physischen Zugriff auf Drucker auf autorisierte Standorte und Personen, um das Risiko von Manipulationen oder Diebstahl zu verringern.

Deaktivierung nicht verwendeter Protokolle: Deaktivieren Sie unnötige Geräteprotokolle und Dienste, die von MyQ X nicht benötigt werden, um die Angriffsfläche jedes Geräts zu verringern.

Verwaltung der Standard-Anmeldedaten: Ändern Sie alle Standard-Administratorpasswörter auf Geräten in starke, zufällig generierte Anmeldedaten. Die Werkseinstellungen sind Angreifern in der Regel bekannt.

Schutz der internen Festplatte: Wenn Geräte die interne Speicherung von Druckaufträgen zum erneuten Drucken unterstützen, implementieren Sie Verschlüsselung (AES) und automatische Datenüberschreibungsfunktionen, um unbefugten Zugriff auf gespeicherte Dokumente zu verhindern.

2.13.2 Netzwerksegmentierung und VLAN-Konfiguration

MyQ X unterstützt Netzwerksegmentierungsstrategien, um potenzielle Gerätekompromittierungen einzudämmen:

VLAN-Isolierung: Trennen Sie den Netzwerkverkehr von Druckern und Geräten vom allgemeinen Benutzer- und Verwaltungsnetzwerk mithilfe virtueller LANs, um die seitliche Bewegung zu begrenzen, falls ein Gerät kompromittiert wird.

Subnetting und Zugriffskontrolllisten: Implementieren Sie Zugriffskontrollen auf Netzwerkebene mithilfe von Zugriffskontrolllisten (ACLs), um sicherzustellen, dass nur autorisierte Systeme mit Druckgeräten und Servern kommunizieren können.

Firewall-Regeln: Blockieren Sie unnötigen eingehenden und ausgehenden Datenverkehr aus Drucker-Subnetzen, beschränken Sie die Konnektivität auf nur wesentliche Dienste und verhindern Sie, dass infizierte Geräte auf andere Netzwerkressourcen zugreifen.

FQDN-Durchsetzung: Die gesamte Netzwerkkommunikation muss vollständig qualifizierte Domänennamen (FQDN) anstelle von IP-Adressen oder kurzen Hostnamen verwenden, um DNS-basierte Man-in-the-Middle-Angriffe zu verhindern und eine ordnungsgemäße Zertifikatsvalidierung sicherzustellen.

2.13.3 SNMP v3-Sicherheitsimplementierung

MyQ X erzwingt moderne **SNMPv3**-Protokolle mit starker Verschlüsselung für die Geräteverwaltung:

Verbot von unsicherem SNMPv1: Die veraltete SNMPv1-Kommunikation muss vollständig deaktiviert werden, da sie Anmeldedaten im Klartext überträgt und keine Verschlüsselung bietet.

SNMPv3-Konfiguration: Die gesamte SNMP-Kommunikation muss SNMPv3 mit folgenden Merkmalen verwenden:

- Starken, zufällig generierten Passwörtern für die Authentifizierung
- SHA1 oder stärkeren Hash-Algorithmen
- AES-Verschlüsselung für die Vertraulichkeit der Daten
- Gerätespezifische, eindeutige Anmeldedaten für jede MyQ-Bereitstellung

2.13.4 Verwaltung von Drucker-Anmeldedaten

MyQ X erkennt, dass **die Verwaltung von Drucker-Anmeldedaten herstellerspezifisch ist** und eine Implementierung auf Kundenseite erfordert:

Strenge Passwortanforderungen: Alle Administrator-Anmeldedaten für Drucker müssen starke, zufällig generierte Passwörter verwenden, anstatt Standard- oder einfache Anmeldedaten.

Rotation der Anmeldedaten: Aktualisieren Sie die Druckerpasswörter regelmäßig gemäß den Sicherheitsrichtlinien Ihres Unternehmens, um das Risiko einer Kompromittierung der Anmeldedaten zu verringern.

Zugriffsbeschränkungen: Beschränken Sie den Zugriff auf die Druckerverwaltung durch Firewall-Regeln, physische Zugriffskontrollen und rollenbasierte Berechtigungen auf autorisiertes Personal.

2.13.5 Firmware-Sicherheit und Update-Verwaltung

Die Aktualisierung der Geräte-Firmware ist für die Sicherheit von entscheidender Bedeutung:

Automatische Updates: Konfigurieren Sie Geräte so, dass sie automatisch Firmware-Updates des Herstellers erhalten und anwenden, die neu entdeckte Sicherheitslücken beheben.

Sicherheitshinweise des Herstellers: Überwachen Sie die Sicherheitshinweise des Herstellers auf kritische Schwachstellen, die sich auf eingesetzte Geräte auswirken, und wenden Sie Patches umgehend an.

Update-Tests: Testen Sie Firmware-Updates in Nicht-Produktionsumgebungen, bevor Sie sie auf Produktionsdruckern bereitstellen, um Kompatibilität und Funktionalität sicherzustellen.

2.13.6 Verwaltung und Einschränkungen von USB-Anschlüssen

MyQ X unterstützt administrative Kontrollen für die USB-Konnektivität von Geräten:

Deaktivierung von USB-Anschlüssen: Administratoren sollten eingehende USB-Anschlüsse an MFDs deaktivieren, um Folgendes zu verhindern:

- Direktes Drucken über USB unter Umgehung der MyQ-Sicherheitskontrollen
- Direkten Zugriff auf Gerätefestplatten und gespeicherte Daten
- unbefugte Nutzung von Gerätefunktionen

Sichere Alternativen zum direkten Drucken: Aktivieren Sie nur zugelassene sichere Druckmethoden (IPP/S, AirPrint mit MyQ-Integration) und blockieren Sie unsicheren direkten USB-Zugriff.

Dieses umfassende Rahmenwerk für Geräte- und Netzwerksicherheit stellt sicher, dass Druckgeräte sichere Komponenten der MyQ X-Infrastruktur bleiben und gleichzeitig die betriebliche Effizienz und die Sicherheitslage des Unternehmens gewahrt bleiben.

2.14 Prüfung und Überwachung

MyQ X bietet umfassende Audit- und Überwachungsfunktionen, mit denen Administratoren die Übersicht über Druckvorgänge behalten, Sicherheitsvorfälle erkennen und die Einhaltung von Unternehmensrichtlinien und Vorschriften sicherstellen können.

2.14.1 Echtzeitüberwachung und Warnmeldungen

MyQ X überwacht alle Komponenten der Druckinfrastruktur in Echtzeit über mehrere Überwachungskanäle:

Überwachung des Gerätestatus: Kontinuierliche Überwachung des Status von Druckern und Multifunktionsgeräten, einschließlich Tonerstand, Papierverfügbarkeit, Fehlerzustände und Gerätekonnektivität. Administratoren erhalten sofort Einblick in den Zustand und den Betriebsstatus der Geräte.

Warnungsmanagement: Automatische Warnmeldungen informieren Administratoren über kritische Ereignisse wie Gerätefehler, niedrige Verbrauchsmaterialvorräte, Verbindungsprobleme und andere Betriebsprobleme. Warnmeldungen können per E-Mail versendet oder in die Windows-Ereignisanzeige integriert werden.

Ereignisbenachrichtigungen: Anpassbare ereignisbasierte Benachrichtigungen lösen Aktionen als Reaktion auf bestimmte Geräte- oder Systembedingungen aus und ermöglichen so eine proaktive Problemlösung, bevor sich Probleme auf den Betrieb auswirken.

2.14.2 Protokollierung und Analyse von Druckaktivitäten

MyQ X führt **detaillierte Prüfprotokolle aller Druck-, Kopier-, Scan- und Faxaktivitäten**:

Auftragsbasierte Abrechnung: Die erweiterte Abrechnung verfolgt jeden Auftrag unabhängig voneinander und ermöglicht eine detaillierte Zuordnung zu bestimmten Benutzern, Geräten, Projekten und Kostenstellen. Aufträge, die während einer einzelnen Benutzersitzung ausgeführt werden, werden separat abgerechnet, wodurch präzise Nutzungsdaten bereitgestellt werden.

Aktivitätsmetadaten: Umfassende Protokollierung erfasst das Datum der Auftragsübermittlung, das Datum der Auftragsfreigabe, die Geräteidentifikation, das Papierformat, die Simplex-/Duplex-Einstellungen, die Farbeinstellungen und alle anderen relevanten Auftragsparameter.

MyQ-Protokoll: Das Echtzeit-Systemprotokoll zeigt alle Serveraktivitäten an, einschließlich Systemereignissen, Fehlern, Warnungen, Authentifizierungsversuchen, Konfigurationsänderungen und Verwaltungsaktionen. Protokollmeldungen werden nach Schweregrad (kritisch, Fehler, Warnung, Info, Hinweis, Debug, Trace) kategorisiert und können nach Zeitraum und Subsystem gefiltert werden.

2.14.3 Analyse des Benutzerverhaltens

MyQ X bietet ausgefeilte Analysefunktionen, um Druckmuster zu verstehen und Anomalien zu erkennen:

Erstellung benutzerdefinierter Berichte: Dank erweiterter Berichtsfunktionen können Administratoren benutzerdefinierte Berichte auf der Grundlage beliebiger Kombinationen von erfassten Parametern erstellen und so das Druckverhalten nach Benutzer, Abteilung, Projekt, Gerät oder Zeitraum analysieren.

Kostenstellenverfolgung: Die detaillierte Zuordnung von Druckaufträgen zu Kostenstellen, Projekten und Benutzergruppen ermöglicht eine transparente Spesenabrechnung und unterstützt fundierte Entscheidungen hinsichtlich der Druckrichtlinien.

Verhaltensüberwachung: Administratoren können Druckmuster analysieren, um ungewöhnliche Aktivitäten, übermäßige Nutzung oder Richtlinienverstöße zu identifizieren, die eine weitere Untersuchung rechtfertigen.

2.14.4 Erkennung und Reaktion auf Vorfälle

MyQ X unterstützt die sicherheitsorientierte Überwachung durch strukturierte Protokollierung und Warnmeldungen:

Protokollierung fehlgeschlagener Authentifizierungen: Eine verbesserte Protokollierung von Authentifizierungsversuchen, insbesondere fehlgeschlagenen Anmeldeversuchen, ermöglicht es Administratoren, potenzielle Sicherheitsbedrohungen zu erkennen und darauf zu reagieren. Seit Version 10.2 wurden die Aufzeichnungen von Anmeldeversuchen verbessert, um das Filtern im MyQ-Protokoll zu vereinfachen.

Protokollbenachrichtigungsregeln: Anpassbare Regeln lösen automatische Benachrichtigungen basierend auf bestimmten Ereignistypen, Subsystemen und Nachrichtenmustern aus und ermöglichen so die schnelle Erkennung sicherheitsrelevanter Ereignisse. Regeln können reguläre Ausdrücke verwenden, um nach bestimmten Mustern in Protokollmeldungen zu suchen.

Warnmeldungen zu kritischen Ereignissen: Das System benachrichtigt Administratoren automatisch über kritische Ereignisse wie Sicherheitsverletzungen, Authentifizierungsfehler, unbefugte Zugriffsversuche und Konfigurationsänderungen.

2.14.5 Richtlinien zur Protokollaufbewahrung und -archivierung

MyQ X implementiert eine flexible Protokollverwaltung, um betriebliche Anforderungen und Compliance-Anforderungen in Einklang zu bringen:

Konfigurierbare Aufbewahrungsfristen: Administratoren legen die Anzahl der Tage fest, nach denen Protokolle automatisch gelöscht werden, und passen die Aufbewahrung an die Datenverwaltungsrichtlinien und gesetzlichen Anforderungen des Unternehmens an.

Protokoll-Export und -Archivierung: Protokolle können im Excel- oder CSV-Format für die externe Speicherung und Analyse exportiert werden. Geplante Exporte ermöglichen eine automatisierte Protokollarchivierung in regelmäßigen Abständen.

Langfristige Aufbewahrung: Exportierte Protokolle können in sicheren, verschlüsselten Repositorys gespeichert werden, um historische Aufzeichnungen für Audit-Zwecke, Compliance-Überprüfungen und die Untersuchung von Vorfällen aufzubewahren.

2.14.6 Erweiterte Filter- und Suchfunktionen

MyQ X bietet ausgefeilte Tools für die Protokollanalyse und -untersuchung:

Gespeicherte Suchanfragen: Administratoren können häufig verwendete Suchfilter erstellen, speichern und freigeben, um schnell auf relevante Protokolldaten zugreifen zu können. Gespeicherte Suchanfragen können zur einfachen Verwaltung in Ordnern organisiert werden.

Zeitraumfilterung: Filtern Sie Protokolle nach bestimmten Datumsbereichen oder vordefinierten Zeiträumen, um die Analyse auf relevante Zeiträume zu konzentrieren.

Subsystem- und Kontextfilterung: Suchen Sie nach bestimmten MyQ-Subsystemen (Web-UI, Terminal, SMTP-Server usw.) und Kontexten (Direktdruck, bestimmte Geräte), um relevante Ereignisse zu isolieren.

Ausführlichkeitssteuerung: Wählen **Sie** aus, welche Protokollschweregrade (kritisch, Fehler, Warnung, Info usw.) angezeigt werden sollen, um Störsignale zu reduzieren und sich auf wichtige Ereignisse zu konzentrieren.

2.14.7 Audit-Protokoll für administrative Aktionen

MyQ X verfolgt alle administrativen Änderungen über ein spezielles **Audit-Protokoll**:

Konfigurationsänderungen: Zeichnet alle Änderungen an den MyQ-Einstellungen auf, einschließlich der Person, die die Änderung vorgenommen hat, des Zeitpunkts der Änderung und der betroffenen Systemkomponente.

Verwaltung von Benutzerrechten: Detaillierte Verfolgung von Änderungen an Benutzerberechtigungen, Gruppenmitgliedschaften und Zugriffskontrollen mit der Möglichkeit, detaillierte Informationen zu jeder Änderung anzuzeigen.

PIN- und Berechtigungsverwaltung: Verbesserte Nachverfolgung von PIN-Hinzufügungen, -Entfernungen und -Änderungen zur Überwachung des Lebenszyklus von Berechtigungen.

Exportfunktionen: Audit-Protokolle können bei Bedarf exportiert oder für einen regelmäßigen automatisierten Export geplant werden, wodurch die Anforderungen an die Compliance-Berichterstattung und die Aufbewahrung von Aufzeichnungen unterstützt werden.

Dieses umfassende Audit- und Überwachungsframework stellt sicher, dass MyQ X Administratoren die erforderliche Transparenz bietet, um die Sicherheit aufrechtzuerhalten, Bedrohungen zu erkennen, die Einhaltung von Richtlinien zu gewährleisten und Betriebsprobleme effektiv zu beheben.

2.15 Reaktion auf Zwischenfälle und Wiederherstellung

MyQ X bietet umfassende Funktionen für die Reaktion auf Vorfälle und die Wiederherstellung, die darauf ausgelegt sind, die Geschäftskontinuität sowohl bei geplanten als auch bei ungeplanten Unterbrechungen aufrechtzuerhalten. Die Plattform kombiniert automatisierte Sicherungsverfahren, Hochverfügbarkeitsfunktionen und flexible Failover-Mechanismen, um sicherzustellen, dass die Druckdienste auch bei Systemausfällen betriebsbereit bleiben.

2.15.1 Verfahren zur Reaktion auf Sicherheitsvorfälle

MyQ X unterstützt eine strukturierte Reaktion auf Vorfälle durch mehrere Überwachungs- und Warnmechanismen:

Echtzeit-Erkennung von Vorfällen: Die automatisierte Überwachung verfolgt kontinuierlich den Systemzustand, Authentifizierungsfehler, Konfigurationsänderungen und Sicherheitsereignisse und ermöglicht so die schnelle Erkennung potenzieller Sicherheitsvorfälle.

Eskalation von Warnmeldungen: Konfigurierbare Log Notifier-Regeln lösen sofortige Benachrichtigungen an Administratoren aus, wenn kritische Sicherheitsereignisse auftreten, darunter fehlgeschlagene Authentifizierungsversuche, unbefugte Zugriffsversuche und Systemanomalien.

Aufbewahrung von Prüfprotokollen: Eine umfassende Protokollierung aller Systemaktivitäten stellt sicher, dass vollständige forensische Daten für die Untersuchung von Vorfällen verfügbar sind. Das MyQ-Prüfprotokoll verfolgt alle administrativen Aktionen, Konfigurationsänderungen und Benutzeraktivitäten.

Eindämmungsmaßnahmen: Im Falle eines Sicherheitsvorfalls können Administratoren betroffene Komponenten schnell isolieren, kompromittierte Konten deaktivieren und Notfallzugriffskontrollen implementieren.

2.15.2 Wiederherstellungs- und Wiederaufbaumaßnahmen

MyQ X verfügt über robuste Sicherungs- und Wiederherstellungsfunktionen, um eine schnelle Wiederherstellung nach Systemausfällen oder Datenverlusten zu gewährleisten:

Automatisierte Datenbank-Sicherung: Regelmäßige automatisierte Sicherungen der MyQ-Datenbank erfassen alle Konfigurationsdaten, Benutzerinformationen und Systemeinstellungen. Die Sicherungen sind durch Passwortverschlüsselung geschützt und werden sicher gespeichert.

Vollständige Systemwiederherstellung: Der Wiederherstellungsprozess stellt die gesamte MyQ-Umgebung wieder her, einschließlich Datenbank, Zertifikate, Konfigurationsdateien und Berichte. Administratoren wählen einfach die Sicherungsdatei aus und geben das Passwort ein, falls diese geschützt ist.

Cluster-bewusste Sicherung und Wiederherstellung: Für Hochverfügbarkeitsbereitstellungen mit Microsoft Failover Clustering unterstützt MyQ die Sicherung auf einem gemeinsam genutzten Clusterspeicher und die koordinierte Wiederherstellung über alle Clusterknoten hinweg.

2.15.3 Hochverfügbarkeit und Failover

MyQ X bietet mehrere Failover-Strategien, um den Druckbetrieb während Serverausfällen aufrechtzuerhalten:

Integration von Microsoft Failover Clustering: MyQ X wird in Aktiv-Passiv-Konfigurationen innerhalb von Microsoft Windows Server Failover Clustern bereitgestellt. Die Cluster-Software überwacht kontinuierlich den Zustand der Knoten und wechselt automatisch zu passiven Knoten, wenn der aktive Knoten nicht mehr verfügbar ist.

Fallback-Druck: Wenn der MyQ Desktop Client eine unterbrochene Verbindung zum Server feststellt, leitet er Druckaufträge automatisch an vorkonfigurierte Fallback-

Drucker um. Sobald die Serververbindung wiederhergestellt ist, wird die Auftragsabrechnung automatisch aktualisiert.

Gerätespooling: Druckaufträge können während Serverausfällen verschlüsselt im Gerätespeicher gespeichert werden. Sobald die Verbindung wiederhergestellt ist, übertragen die Geräte die Abrechnungsdaten automatisch an den Server.

Offline-Anmeldung: MyQ X-Embedded Terminal speichern die Anmeldedaten der Benutzer zwischen, sodass sich Benutzer auch dann anmelden und auf die Gerätefunktionen zugreifen können, wenn der Server nicht verfügbar ist.

Client-Spooling: Aufträge werden lokal auf den Arbeitsplätzen der Benutzer verarbeitet und auf deren Computern statt auf dem Server gespeichert, wodurch der Bandbreitenbedarf erheblich reduziert wird und das Drucken während der Serverwartung oder bei Netzwerkproblemen möglich ist.

2.15.4 Analyse und Verbesserung nach Vorfällen

MyQ X unterstützt die kontinuierliche Verbesserung der Reaktionsfähigkeit bei Vorfällen durch umfassende Analyse-Tools:

Analyse historischer Protokolle: Administratoren können exportierte Protokolle überprüfen, um die Abfolge der Ereignisse zu verstehen, die zu einem Vorfall geführt haben, die Ursachen zu identifizieren und geeignete Korrekturmaßnahmen zu ermitteln.

Überprüfung des Prüfprotokolls: Das Prüfprotokoll bietet vollständige Transparenz über alle administrativen Maßnahmen und Konfigurationsänderungen, die zu Sicherheitsvorfällen beigetragen haben oder diesen vorausgegangen sind.

Gespeicherte Suchmuster: Administratoren können Suchfilter für häufige Vorfallmuster in Protokollen erstellen und speichern, um ähnliche Ereignisse in Zukunft schnell identifizieren zu können.

3 MyQ X und NIS2

Die Richtlinie (EU) 2022/2555, besser bekannt als **NIS2**, ist ein bedeutender Schritt zur Schaffung eines einheitlichen Niveaus der Cybersicherheit in der gesamten Europäischen Union. Diese Richtlinie, die am 16. Januar 2023 in Kraft trat, zielt darauf ab, die **Widerstandsfähigkeit kritischer Dienste** und digitaler Dienstleister gegen Cyberbedrohungen durch die Einführung einheitlicher **Cybersicherheitsstandards und -praktiken** zu stärken.

Die Druckindustrie fällt, neben vielen anderen Branchen, in den Anwendungsbereich der NIS2-Richtlinie. Daher müssen Unternehmen der Druckindustrie die Auswirkungen der NIS2-Richtlinie verstehen und die notwendigen Schritte unternehmen, um die Sicherheitsstandards zu erfüllen. Bis zum 17. Oktober 2024 sind die Mitgliedstaaten verpflichtet, die für die Einhaltung der NIS2-Richtlinie erforderlichen Maßnahmen zu erlassen und zu veröffentlichen.

Dieser Artikel befasst sich mit den Einzelheiten der NIS2-Richtlinie und ihren Auswirkungen auf MyQ X-Vertriebspartner und -Kunden.

Wenn Sie ein MyQ X-Endkunde sind, besprechen Sie die Anforderungen und Empfehlungen der NIS2-Richtlinie mit Ihrem MyQ X-Anbieter/Vertriebspartner. MyQ-Partner sind geschult, erstklassigen Support zu leisten, und werden Sie bei der Umsetzung der erforderlichen Maßnahmen unterstützen.

3.1 Hauptbereiche der NIS2-Richtlinie

3.1.1 Risikomanagement und Cybersicherheit

Verfolgen Sie einen risikobasierten Ansatz für die Cybersicherheit. Dazu gehören die Identifizierung und Bewertung von Risiken für Netzwerk- und Informationssysteme, die Umsetzung von Maßnahmen zur Minderung dieser Risiken sowie die regelmäßige Überprüfung dieser Maßnahmen.

Stellen Sie sicher, dass Ihr Server und die zugehörige Software **mit den neuesten Sicherheitspatches auf dem aktuellen Stand** sind, um Schwachstellen zu minimieren. Implementieren und testen Sie darüber hinaus regelmäßig Backup- und Notfallwiederherstellungspläne, um die Verfügbarkeit und Integrität der Daten sicherzustellen. MyQ stellt regelmäßig Patch-Releases für seine Produkte bereit. Es wird dringend empfohlen, sich auf dem Laufenden zu halten, diese Releases zu

verfolgen und Ihre Update-Strategie und -Prozedur im Voraus zu planen. MyQ erstellt für jedes Release eine **Software-Stückliste (SBOM)**, die Sie über Ihren MyQ-Anbieter/Vertriebspartner erhalten können und die es Unternehmen ermöglicht, die in der Software verwendeten Komponenten auf Sicherheitslücken zu analysieren.

Die Netzwerksegmentierung ist ein wesentliches Instrument für die praktische Umsetzung einer Zero-Trust-Richtlinie. Sie bietet Unternehmen Möglichkeiten, ihre Netzwerke mit detaillierteren Sicherheitsrichtlinien zu kontrollieren. Sie stellt sicher, dass ein Angreifer, selbst wenn er einen Teil des Netzwerks kompromittiert, nicht ohne Weiteres lateral in andere Bereiche vordringen kann. Unternehmen mit segmentierten Umgebungen stehen jedoch vor Herausforderungen, wenn es darum geht, den Druckzugang leicht verfügbar zu machen.

Mit MyQ X können Druckwarteschlangen in segmentierten Netzwerken mithilfe von Mobile Print Agents weitergeleitet werden, und in der Cloud gehostete Dokumente können mit Easy Print sofort vom Bildschirm des Geräts heruntergeladen und freigegeben werden. Die Unterstützung von Microsoft Universal Print oder Application Proxy im Mobile Client kann Unternehmen erheblich dabei helfen, Druckdienste in ihrer gesamten Umgebung bereitzustellen und gleichzeitig sicherzustellen, dass der Zugriff auf solche Ressourcen geschützt ist.

SSL-Zertifikate für sichere Verbindungen tragen dazu bei, die Anforderungen von NIS2 an eine sichere Datenübertragung über Netzwerke hinweg zu erfüllen. MyQ X verfügt standardmäßig über eine sichere Kommunikation dank der integrierten Zertifizierungsstelle. Unternehmen, die Enterprise PKI nutzen, können ein noch höheres Maß an Kommunikationssicherheit erreichen, indem sie direkt benutzerdefinierte Zertifikate bereitstellen.

Setzen Sie nach Möglichkeit **TLS** für die Kommunikation mit anderen Systemen **durch**. Sichern Sie die Verbindung zum Active Directory oder anderen Benutzerverzeichnissen mit LDAPS. Stellen Sie sicher, dass die E-Mail-Übertragung über SMTPS erfolgt, und überprüfen Sie alle Einstellungen auf der Netzwerkseite von MyQ X sowie auf der Registerkarte „Sicherheit“ in Easy Config (z. B. dass der Webserver nur sichere Verbindungen zulässt).

MyQ bietet zudem die Möglichkeit, **Datenbanken, Scans und Druckaufträge** zu **verschlüsseln**. Die Datenverschlüsselung ist unerlässlich, um die Vertraulichkeit und Integrität sensibler Informationen zu gewährleisten, was ein zentraler Aspekt der NIS2-Konformität ist.

Für die Gerätekommunikation ist es unerlässlich, Kommunikationsprotokolle zu implementieren, die ein Höchstmaß an Sicherheit bieten. Es wird dringend empfohlen**, SNMPv3** anstelle von v1 oder v2(c) zu verwenden, um den Status und die Funktionalität von Geräten in einem Netzwerk zu überwachen und zu verwalten.

3.1.2 Geschäftskontinuität und Krisenmanagement

> Unternehmen müssen sicherstellen, dass ihr Betrieb auch im Falle einer erheblichen Störung weiterlaufen kann.

Implementieren Sie **redundante Server oder Failover-Systeme,** um sicherzustellen, dass Druckdienste während eines Vorfalls verfügbar bleiben. MyQ X ermöglicht die Implementierung von Failover-Maßnahmen mithilfe verschiedener Methoden.

MyQ unterstützt **Windows Server Failover Clustering** für hohe Verfügbarkeit und stellt sicher, dass Dienste im Falle eines Ausfalls automatisch auf einen Backup-Knoten übertragen werden.

Wenn die Verbindung zum MyQ-Server unterbrochen wird, ermöglicht die **Fallback**-Druckfunktion den Benutzern, den Druckvorgang über ein Backup-Gerät fortzusetzen. Der MyQ Desktop Client sendet Druckaufträge direkt an ein Backup-Gerät, wenn die Serververbindung unterbrochen ist. Dies garantiert, dass Druckvorgänge während Serverausfällen unterbrechungsfrei fortgesetzt werden können, was für die Aufrechterhaltung der Geschäftskontinuität entscheidend ist. Ebenso kann die bei ausgewählten Anbietern unterstützte Funktion **„Device Spooling“** mit **der Offline-Anmeldung** für den Offline-Betrieb kombiniert werden und erhöht die Verfügbarkeit der Druckdienste zusätzlich.

Regelmäßige **Datenbank-Backups** und die Möglichkeit, MyQ-Daten wiederherzustellen, entsprechen den Anforderungen von NIS2 zur Gewährleistung der Datenverfügbarkeit und Ausfallsicherheit bei Cyberangriffen oder Systemausfällen. Datenbank- und Protokoll-Backups können mit MyQ X geplant und automatisch durchgeführt werden, einschließlich der Backups der SQL-Datenbank des Central Server.

Weiterlesen:

- Übersicht: Hochverfügbarkeit mit MyQ X
- Bereitstellung: Hochverfügbarkeit, Fallback und Failover

3.1.3 Zugriffsmodell mit geringsten Berechtigungen

> Benutzern sollten nur die minimalen Zugriffsrechte oder Berechtigungen gewährt werden, die zur Ausführung der erforderlichen Vorgänge notwendig sind.

NIS2 fördert **die Aufgabentrennung,** um unbefugten Zugriff auf kritische Systeme zu verhindern.

Durch die Zuweisung **spezifischer Rechte für den Zugriff** auf System- und Benutzerverwaltung, Auftragsverwaltung, Berichterstellung oder Protokolle ist es möglich, bestimmten Benutzern Zugriff mit erweiterten Berechtigungen auf bestimmte Bereiche der MyQ-Umgebung zu gewähren, während die Zugriffsrechte anderer eingeschränkt werden. Ebenso können Rechte pro Standortserver zugewiesen werden, sodass Administratoren eines lokalen Standortservers keinen Zugriff mit erweiterten Berechtigungen an anderen Standorten und Niederlassungen der Organisation erhalten, wo dies nicht gewünscht ist.

Wenn der Administrator **die gruppenbasierte Verwaltung** von Benutzern (Sicherheitsgruppen) nutzt, kann er die Anzahl der Schritte zur Konfiguration von Zugriffsrechten reduzieren und gleichzeitig von der Benutzerbereitstellung und -entfernung profitieren. Lesen Sie mehr dazu weiter unten im Abschnitt *„Benutzerbereitstellung und -entfernung*".

Detaillierte Zugriffsberechtigungen sollten in der gesamten Unternehmensinfrastruktur durchgesetzt werden, einschließlich aller Komponenten innerhalb des MyQ X-Ökosystems. Der Zugriff sollte ausschließlich auf Administratoren und autorisiertes Personal beschränkt sein, um sicherzustellen, dass nur Personen mit entsprechenden Berechtigungen diese Systeme verwalten und mit ihnen interagieren können. Dies umfasst physische Geräte, physische Server und deren Betriebssysteme (Windows Server), SQL-Server, Speicher und mehr.

Weiterlesen:

- Bereitstellung: Benutzerrechte

3.1.4 Reaktion auf Vorfälle und Überwachung

Legen Sie zur Bewältigung von Vorfällen Verfahren fest und üben Sie diese regelmäßig. Schränken Sie bei verdächtigen Aktivitäten den Benutzerzugriff ein oder sperren Sie ihn, um weiteren Schaden zu verhindern. Die ordnungsgemäße Umsetzung dieser Maßnahmen kann die Auswirkungen unerwarteter Ereignisse mindern.

Die Protokollierungs- und Überwachungsfunktionen von MyQ (MyQ Logs und MyQ Audit Log) können für die Reaktion auf Vorfälle und deren Nachverfolgung äußerst nützlich sein. Diese Protokolle helfen dabei, verdächtige Aktivitäten zu erkennen, zu untersuchen und darauf zu reagieren, was ein obligatorischer Aspekt von NIS2 ist.

Protokolle sollten regelmäßig überwacht und Benachrichtigungen für Vorfälle aktiviert werden, die das Unternehmen als kritisch einstuft. Zu diesem Zweck kann das in MyQ X integrierte Dienstprogramm **„Log Notifier“** so konfiguriert werden, dass es Ereignisse in der MyQ-Umgebung überwacht und das zuständige Personal benachrichtigt, um sofortige Maßnahmen zu ergreifen. Laufende geplante Aufgaben (wie Benutzersynchronisierung, Druckererkennung und mehr) können ebenfalls Warnungen an vorab festgelegte Kontakte senden. Administratoren können MyQ X zudem so konfigurieren, dass automatische Warnmeldungen gesendet werden, wenn Druckaufträge fehlschlagen oder kritische Fehler auftreten.

Die Protokollverwaltung kann durch den Export und die Verarbeitung von Protokollen über das Windows-Ereignisprotokoll zentralisiert und bei Bedarf durch SIEM-Systeme weiterverarbeitet werden. Stellen Sie sicher, dass die Aufbewahrungsfristen für Verlaufs-, Protokoll- und Audit-Protokolle Ihren Anforderungen entsprechen. Dies wird unter **„Einstellungen** – **Systemverwaltung“** konfiguriert.

Die Festlegung **solider SLAs** ist für Managed Services wie MyQ unerlässlich, insbesondere im Rahmen der NIS2-Vorschriften. Um schnelle Reaktionszeiten bei Vorfällen zu gewährleisten, sollten Unternehmen den Abschluss von Premium-Support-Angeboten in Betracht ziehen.

Weiterlesen:

- Protokoll-Einstellungen

3.1.5 Sichere Authentifizierung

Eine sichere Authentifizierung stellt sicher, dass nur autorisierte Benutzer auf Systeme zugreifen. Die Zwei-Faktor-Authentifizierung (2FA) verbessert dies, indem sie zwei Arten von Anmeldedaten erfordert, was die Sicherheit erheblich erhöht.

Passwort- und PIN-Anforderungen, **die Zwei-Faktor-Authentifizierung** auf den Embedded Terminals oder die Verwendung von „Anmelden mit Microsoft“ auf den Web-Schnittstellen oder Embedded Terminals (mit dem MyQ X Mobile Client) bieten Alternativen zur Sicherung des Zugriffs auf die MyQ X-Umgebung.

Der MyQ X Mobile Client kann so konfiguriert werden, dass **eine biometrische Verifizierung** erforderlich ist, wodurch die Sicherheit des MyQ X-Benutzerkontos weiter erhöht wird, da bei der Authentifizierung an Geräten ein zusätzlicher Faktor verlangt wird.

Die Implementierung von Mechanismen zur Sperrung von Benutzerkonten nach mehreren fehlgeschlagenen Anmeldeversuchen erhöht die Sicherheit und verringert das Risiko von Brute-Force-Angriffen.

Weiterlesen:

- Bereitstellung: Sichere Authentifizierung[5]
- Bereitstellung: Verwendung der Zwei-Faktor-Authentifizierung[6]

3.1.6 Benutzer-Provisioning und -Deprovisioning

Die Bereitstellung und Aufhebung der Bereitstellung stellen sicher, dass Benutzern sofort der Zugriff auf die MyQ-Umgebung verweigert wird, sobald sie aus dem Quellbenutzerverzeichnis entfernt werden.

MyQ unterstützt **die automatische, zeitgesteuerte Benutzersynchronisierung** mit externen Systemen wie LDAP, Microsoft Entra ID (ehemals Azure AD), Google Workspace und CSV-Dateien. Dadurch wird sichergestellt, dass neu hinzugefügte Benutzer automatisch und ohne manuelle Eingabe in die MyQ X-Umgebung importiert werden. Durch die regelmäßige Synchronisierung von Benutzerdaten hilft MyQ X dabei, eine aktuelle Liste von Benutzern mit korrekten Zugriffsrechten zu führen, wodurch das Risiko eines unbefugten Zugriffs verringert wird.

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

Die gruppenbasierte Verwaltung und die Verwendung von Sicherheitsgruppen im Quellbenutzerverzeichnis können dabei helfen, neu bereitgestellten oder entfernten Benutzern automatisch **Zugriff** auf Teile der MyQ X-Umgebung **zuzuweisen oder diesen zu entziehen.**

MyQ X bietet eine **automatische** Registrierungsfunktion, mit der sich Benutzer selbst registrieren können, indem sie Druckaufträge senden, eine ID-Karte durchziehen oder über die Weboberfläche ein Konto erstellen. Diese Funktion ist besonders nützlich für Umgebungen mit häufigen externen Benutzern, wie z. B. Gastmitarbeitern. Benutzern des Systems kann eine **temporäre PIN** zugewiesen werden, die nach einem festgelegten Zeitraum abläuft, wodurch sichergestellt wird, dass der Zugriff automatisch widerrufen wird, sobald der Benutzer keinen Zugriff mehr benötigt.

MyQ unterstützt die Anonymisierung von Benutzerdaten, um Datenschutzbestimmungen einzuhalten. Dieser Prozess entfernt unwiderruflich alle persönlichen Identifikatoren, wodurch Benutzerkonten sowohl unbrauchbar als auch nicht zurückverfolgbar werden, während Systemberichte und Audits weiterhin möglich sind, ohne die Privatsphäre zu beeinträchtigen.

Weiterlesen:

- Bereitstellung: Gruppenbasierte Benutzerverwaltung

3.1.7 Sensibilisierung und Schulung

NIS2 betont die Notwendigkeit der Sensibilisierung und Schulung der Mitarbeiter in Bezug auf Cybersicherheitspraktiken.

Es wird empfohlen, Schulungen für IT-Mitarbeiter und Administratoren zur sicheren Verwaltung der MyQ X-Umgebung anzubieten, wobei der Schwerpunkt auf der NIS2-Konformität liegen sollte. Am besten wenden Sie sich bezüglich der Verwaltung des MyQ X-Ökosystems an Ihren Anbieter/Vertriebspartner. MyQ-Partner sind geschult, um Support von höchster Qualität zu bieten.

Darüber hinaus sollten Sensibilisierungsprogramme entwickelt werden, um Endbenutzern dabei zu helfen, Bedrohungen zu erkennen, und sie in der Nutzung des MyQ X-Ökosystems sowie in den Maßnahmen zu unterweisen, die im Falle von Sicherheits- und anderen Vorfällen zu ergreifen sind.

Sicherheits-Whitepaper und sichere Bereitstellung

Um mehr darüber zu erfahren, wie Sie mit MyQ X die besten Sicherheitsstandards erreichen, lesen Sie den Rest dieses Leitfadens, der sich mit der Sicherheit von MyQ X (see page 69) befasst.

Aktualisiert am 16.9.2024

4 Software-Stückliste

Eine Software-Stückliste (SBOM) ist eine detaillierte Aufzeichnung aller Komponenten, Abhängigkeiten und Bibliotheken, die in einer Softwareanwendung enthalten sind, unabhängig davon, ob es sich um Open-Source- oder proprietäre Komponenten handelt. Sie enthält wichtige Informationen wie Komponentennamen, Versionen, Lizenzen und Quellstandorte und bietet vollständige Transparenz über die Lieferkette der Software.

SBOMs werden zur Verfolgung und Verwaltung von Software-Risiken verwendet, indem sie Unternehmen ermöglichen, anfällige oder veraltete Komponenten schnell zu identifizieren, die Einhaltung von Lizenzen sicherzustellen und die allgemeine Sicherheit zu verbessern. Die Pflege einer SBOM ist besonders in komplexen Software-Ökosystemen von entscheidender Bedeutung, da sie zur Rationalisierung des Schwachstellenmanagements beiträgt und Transparenz über den gesamten Softwareentwicklungszyklus hinweg gewährleistet.

Durch die konsequente Erstellung, Analyse und Pflege von SBOMs können Unternehmen Software-Risiken besser verwalten und die Einhaltung von Sicherheits- und Regulierungsstandards sicherstellen.

BOM-Formate (Bill of Materials) beziehen sich auf standardisierte Strukturen, die die Komponenten eines Softwaresystems darstellen und gemeinsam nutzen. Im Zusammenhang mit Software Bill of Materials (SBOMs) bieten diese Formate eine maschinenlesbare Möglichkeit, Softwarekomponenten, ihre Beziehungen und Metadaten zu beschreiben. Zu den am häufigsten verwendeten SBOM-Formaten gehören:

- **CycloneDX**: Ein leichtgewichtiges und erweiterbares BOM-Format, das speziell für die Anwendungssicherheit entwickelt wurde. Es bietet detaillierte Informationen zu Komponenten, Lizenzen, Schwachstellen und Abhängigkeiten. CycloneDX ist aufgrund seiner Flexibilität und Unterstützung für die Automatisierung von Sicherheits- und Risikomanagement-Workflows beliebt.

MyQ bietet SBOM für die folgenden Produkte:

- MyQ X Central Server 10.2
- MyQ X Print Server 10.2
- MyQ Desktop Client (MDC) 10.2
- Mobile Print Agent (MPA) 1.3
- Optische Zeichenerkennung (OCR) 3.1

Um die SBOMs von MyQ zu erhalten, wenden Sie sich bitte an unseren Support.

5 Geschäftskontakte

MyQ® Hersteller	**MyQ® GmbH** Harfa Business Center, Ceskomoravska 2532/19b, 190 00 Prag 9, Tschechische Republik ID-Nr. 615 06 133 MyQ® spol. s r.o. ist im Handelsregister des Stadtgerichts in Prag unter der Nummer C 29842 eingetragen (im Folgenden als „MyQ®“ bezeichnet)
Geschäftsinformationen	http://www.myq-solution.com info@myq-solution.com[7]
Technischer Support	support@myq-solution.com[8]

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

Hinweis	DER HERSTELLER ÜBERNIMMT KEINE HAFTUNG FÜR VERLUSTE ODER SCHÄDEN, DIE DURCH DIE INSTALLATION ODER DEN BETRIEB DER SOFTWARE- UND HARDWARE-KOMPONENTEN DER MyQ®-DRUCKLÖSUNG ENTSTEHEN. Dieses Handbuch, sein Inhalt, sein Design und seine Struktur sind urheberrechtlich geschützt. Das Kopieren oder sonstige Vervielfältigen dieses Handbuchs oder von Teilen davon sowie aller urheberrechtlich geschützten Inhalte ohne vorherige schriftliche Zustimmung von MyQ® ist untersagt und kann strafbar sein. MyQ® übernimmt keine Verantwortung für den Inhalt dieses Handbuchs, insbesondere hinsichtlich seiner Vollständigkeit, Aktualität und kommerziellen Verwertbarkeit. Alle hier veröffentlichten Materialien dienen ausschließlich zu Informationszwecken. Dieses Handbuch kann ohne vorherige Ankündigung geändert werden. MyQ® ist nicht verpflichtet, diese Änderungen regelmäßig vorzunehmen oder anzukündigen, und ist nicht dafür verantwortlich, dass die derzeit veröffentlichten Informationen mit der neuesten Version der MyQ®-Drucklösung kompatibel sind.
Markenzeichen	„MyQ®“, einschließlich seiner Logos, ist eine eingetragene Marke von MyQ®. Jede Verwendung von Marken von MyQ®, einschließlich seiner Logos, ohne vorherige schriftliche Zustimmung der MyQ® Company ist untersagt. Die Marke und der Produktname sind durch MyQ® und/oder seine lokalen Tochtergesellschaften geschützt.

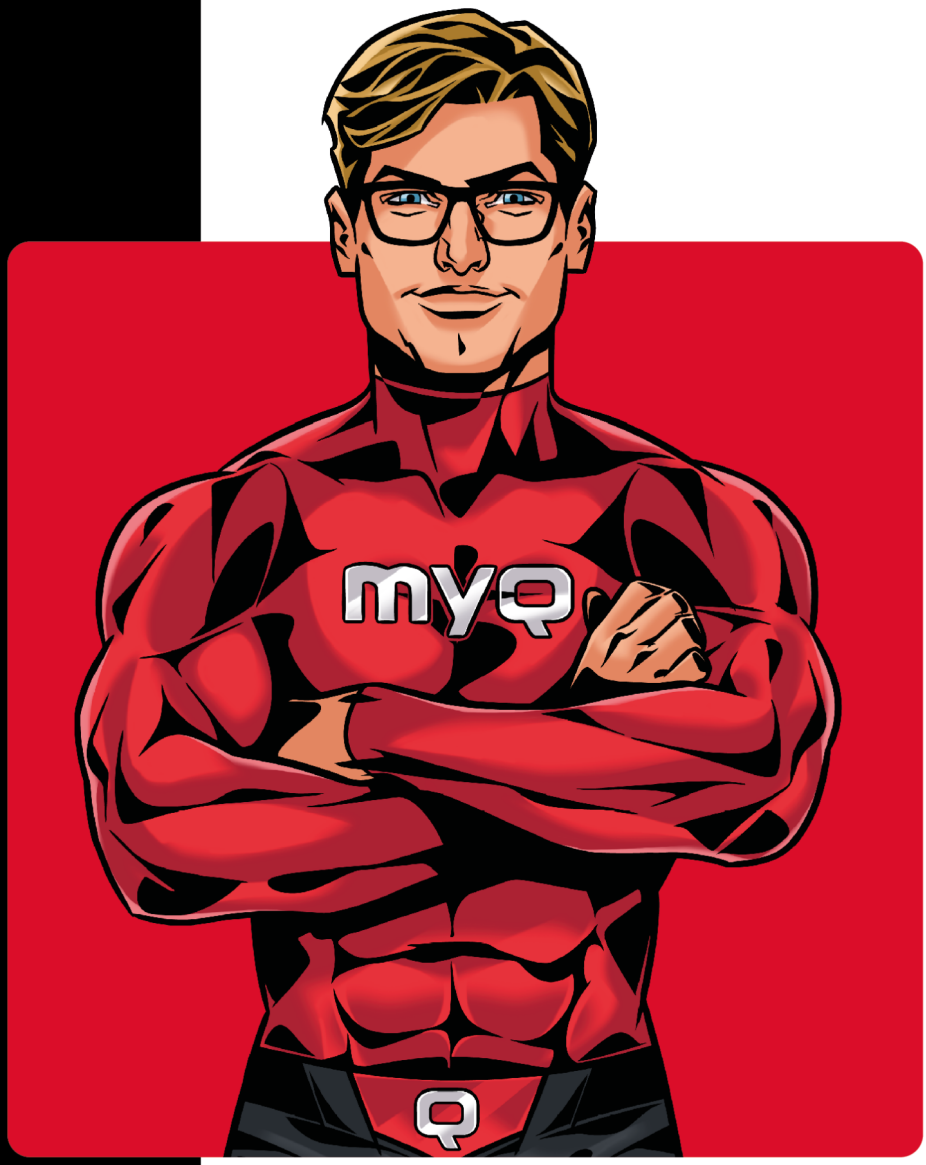
myQ X

SPAREN SIE ZEIT MIT PERSONALISIERTEN DRUCKLÖSUNGEN

MyQ X ist eine preisgekrönte Print-ManagementLösung für On-Premise- oder Private-CloudUmgebungen, der Millionen von Anwendern weltweit vertrauen.

info@myq-solution.com

myq-solution.com



50+ Millionen
Nutzer weltweit vertrauen auf MyQ

1+ Million
Aktive Geräte

26+
Unterstützte Hersteller

1000+
Zertifizierte Partner

Im Einsatz in über
140 Ländern

Ausgezeichnet und zertifiziert

BuyersLab PLATINUM TESTED SOLUTION 2023

BuyersLab PLATINUM TESTED SOLUTION 2022

BuyersLab PLATINUM TESTED SOLUTION 2021

ISO 9001 TÜV SÜD ISO 14001 ISO/IEC 27001