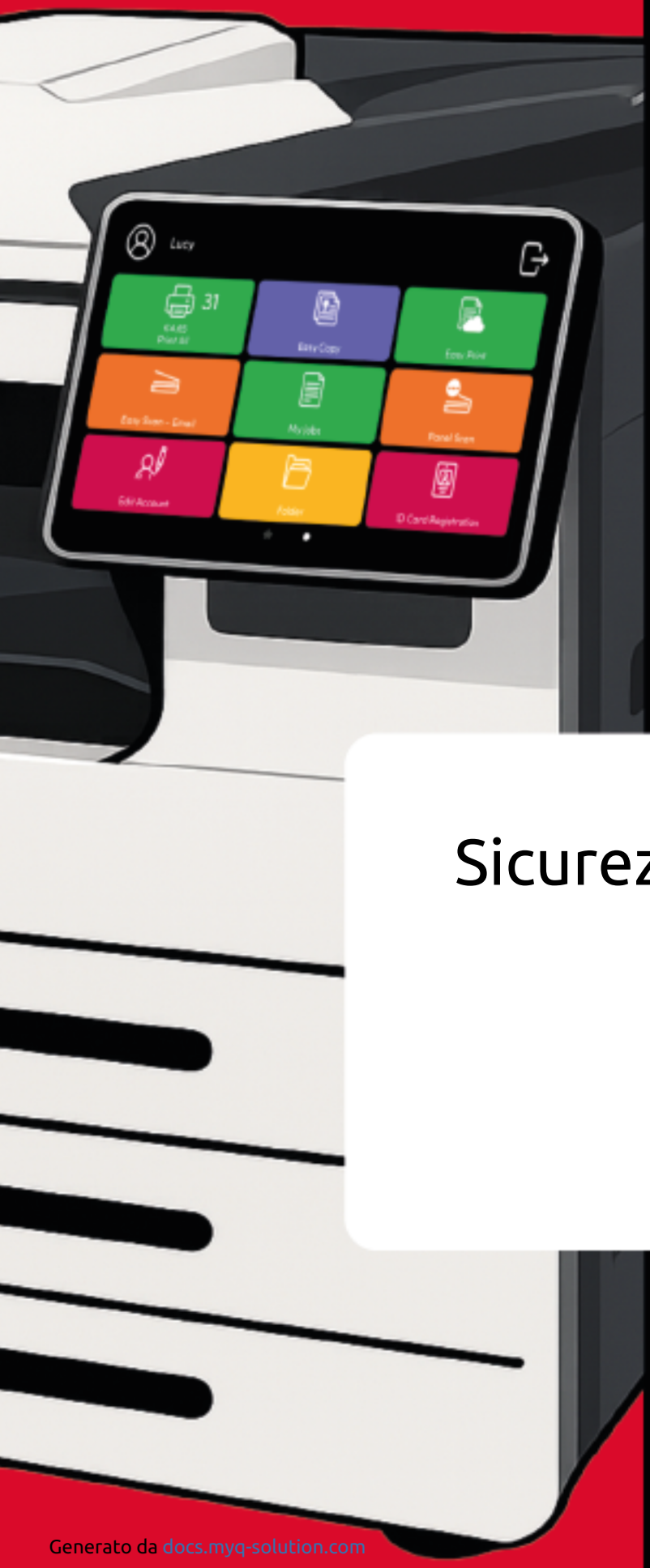


Sicurezza MyQ X 10.x

Generato da docs.myq-solution.com
ottobre/2026
Copyright © 2026 MyQ spol. s r.o. Tutti i diritti riservati.

ITALIANO

Avviso sulla traduzione

Questa traduzione è stata realizzata con l'assistenza dell'intelligenza artificiale. In caso di discrepanze o ambiguità, fa fede il documento originale in lingua inglese.

Indice

1 Distribuzione sicura di MyQ X 5
1.1 MyQ X Central Server 5
1.2 MyQ X Print Server 16
1.3 Desktop Client MyQ X 29
2 Carta bianca sulla sicurezza di MyQ X 33
2.1 Architettura Zero Trust 33
2.2 Struttura di protezione trifase 34
2.3 Privacy fin dalla progettazione 34
2.4 Evoluzione continua della sicurezza 34
2.5 Miglioramenti chiave per la sicurezza in 10.2 35
2.6 Valore aziendale della gestione sicura della stampa 37
2.7 Conformità 38
2.8 Implementazione dell’architettura Zero Trust 42
2.9 Gestione dell’identità e dell’accesso 46
2.10 Sicurezza dell’infrastruttura 49
2.11 Protezione e crittografia dei dati 52
2.12 Flussi di lavoro di stampa sicuri 55
2.13 Sicurezza dei dispositivi e della rete 58
2.14 Audit e monitoraggio 61
2.15 Risposta agli incidenti e recupero 64
3 MyQ X e NIS2 67
3.1 Principali ambiti della direttiva NIS2 67
4 Distinta base del software 74
5 Contatti commerciali 76

La sicurezza è sempre stata una **priorità assoluta per MyQ**. In questa sezione troverete una guida all'implementazione sicura di MyQ X, oltre al white paper sulla sicurezza di MyQ X:

- Implementazione sicura (see page 5)
- White paper sulla sicurezza (see page 33)

1 Distribuzione sicura di MyQ X

Pagine OEM collegate
This ScriptRunner macro could not be rendered for export.

La riservatezza dei dati dei clienti e **la** loro **sicurezza** sono sempre state **la priorità assoluta di MyQ**. Tuttavia, **la sicurezza è una responsabilità condivisa tra fornitori e clienti.** Sebbene l'obiettivo di MyQ X sia quello di fornire una configurazione sicura per impostazione predefinita, diverse aree richiedono misure aggiuntive da parte del cliente. Queste includono, a titolo esemplificativo ma non esaustivo, la gestione dei certificati, l'uso di credenziali sicure, la delega delle autorizzazioni e la configurazione del firewall.

Il presente documento contiene liste di controllo pratiche per l'implementazione sicura di MyQ X Central Server e MyQ X Print Server in ambienti aziendali. Siamo fermamente convinti che seguire queste linee guida ridurrà notevolmente la superficie di attacco di qualsiasi infrastruttura di gestione della stampa. Inutile dire che le applicazioni server MyQ X sono sicure solo quanto i sistemi operativi e gli ambienti di rete sottostanti. Poiché la sicurezza di Windows è un argomento a sé stante, non è trattata nel presente documento.

I sistemi MyQ X vengono costantemente migliorati e aggiornati, in conformità con la politica MyQ Secure Development Lifecycle. Assicurati di **utilizzare sempre l'ultima versione supportata**. Le note di rilascio sono disponibili in ogni guida del prodotto. Consulta anche la politica End Of Life (EOL)[1] per gli annunci di fine manutenzione e i componenti successivi.

Questa guida è stata preparata in collaborazione con Mainstream Technologies, ora Seyfor[2], durante regolari audit di sicurezza indipendenti.

1.1 MyQ X Central Server

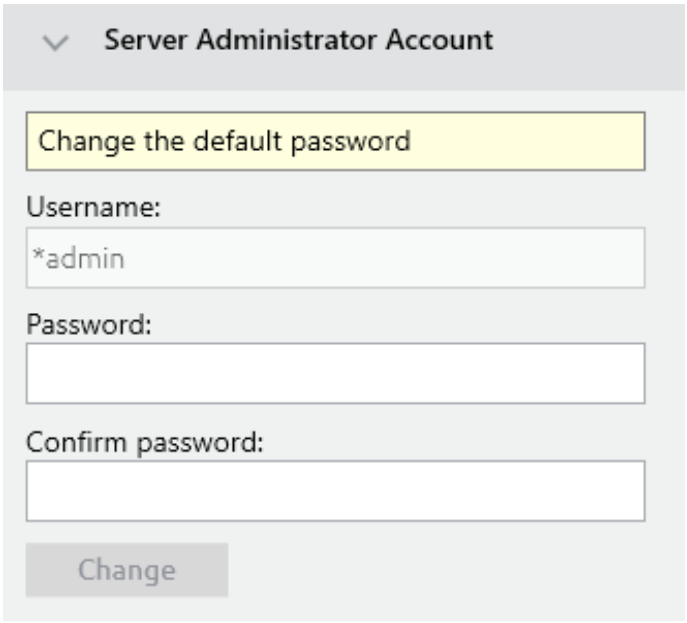
Pagine OEM collegate
This ScriptRunner macro could not be rendered for export.

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

1.1.1 Password predefinite

Modifica password amministratore server

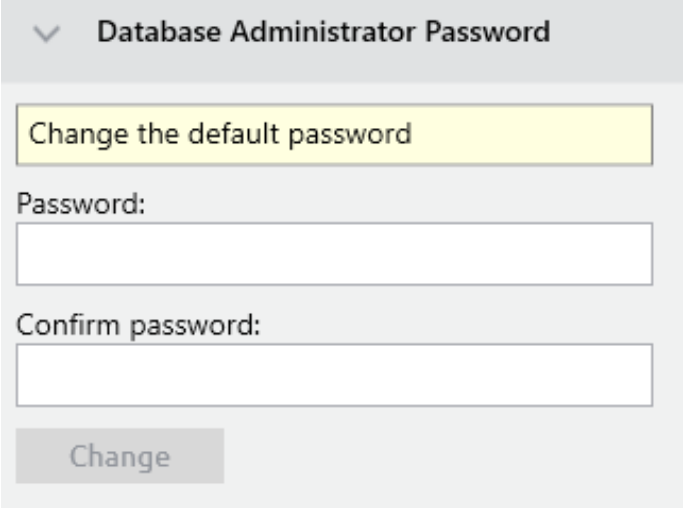
Uno dei primi passaggi dovrebbe essere la modifica della password amministrativa predefinita, che è *1234*:



La password è memorizzata nel database in forma hash.

Modifica della password dell'amministratore del database

Se si utilizza il database interno Firebird, modificare la password predefinita utilizzata da MyQ Central Server per l'autenticazione:



Questa password è memorizzata nel file "C:\ProgramData\MyQ Central Server\setup.ini" in forma crittografata ed è impostata su "*masterkey*" per impostazione predefinita.

1.1.2 Sicurezza della connessione

Pagine OEM collegate
This ScriptRunner macro could not be rendered for export.

Configurare il certificato HTTPS

Per MyQ Central Server è necessario configurare un certificato personalizzato che sia considerato attendibile da tutti i computer client e che contenga il nome DNS del server:

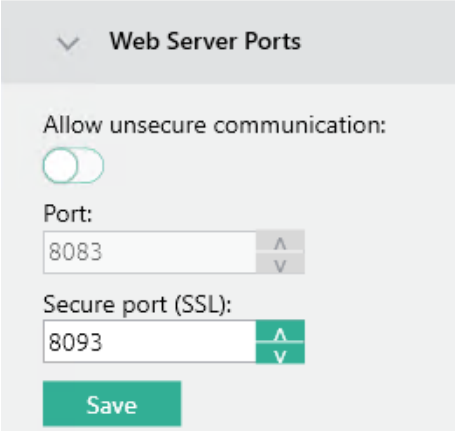
Il certificato è fisicamente memorizzato nella directory "C:\ProgramData\MyQ Central Server\Cert" nei seguenti file:

- server.pfx – certificato con chiavi pubbliche e private
- server.cer – certificato con chiave pubblica
- server.key – chiave privata

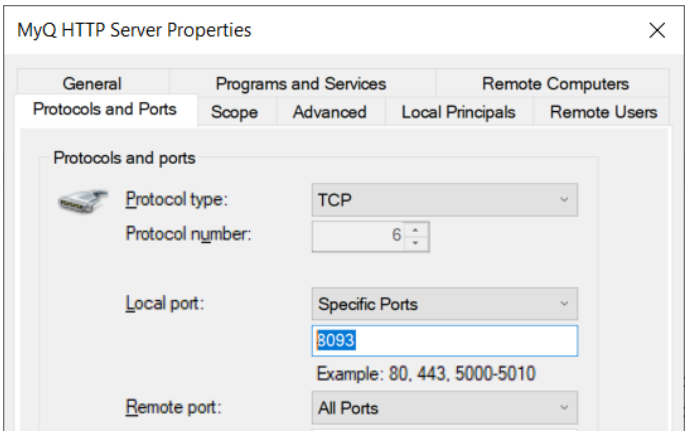
Si sconsiglia l'uso di certificati con caratteri jolly, poiché comportano un rischio molto più elevato per la sicurezza in caso di furto.

Bloccare il traffico HTTP non crittografato

Il traffico HTTP non crittografato non deve essere abilitato nella configurazione di MyQ Central Server:

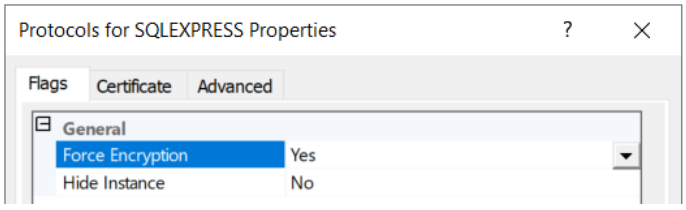


Il firewall basato su host dovrebbe inoltre essere configurato per abilitare solo il traffico HTTPS:

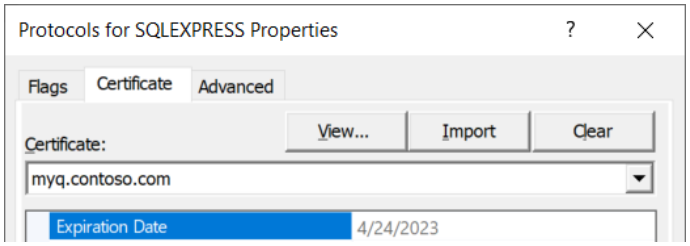


Crittografare le connessioni al database

Se si utilizza Microsoft SQL Server per archiviare il database MyQ, assicurarsi che la crittografia TLS sia applicata tramite SQL Server Configuration Manager:

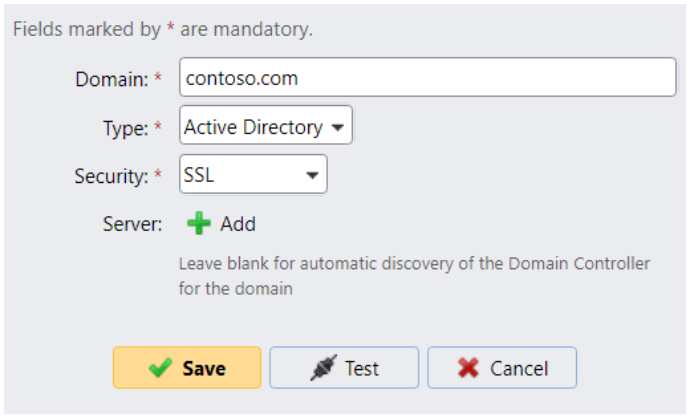


È inoltre necessario configurare un certificato emesso da una CA attendibile su SQL Server:



Applicare il traffico LDAP crittografato

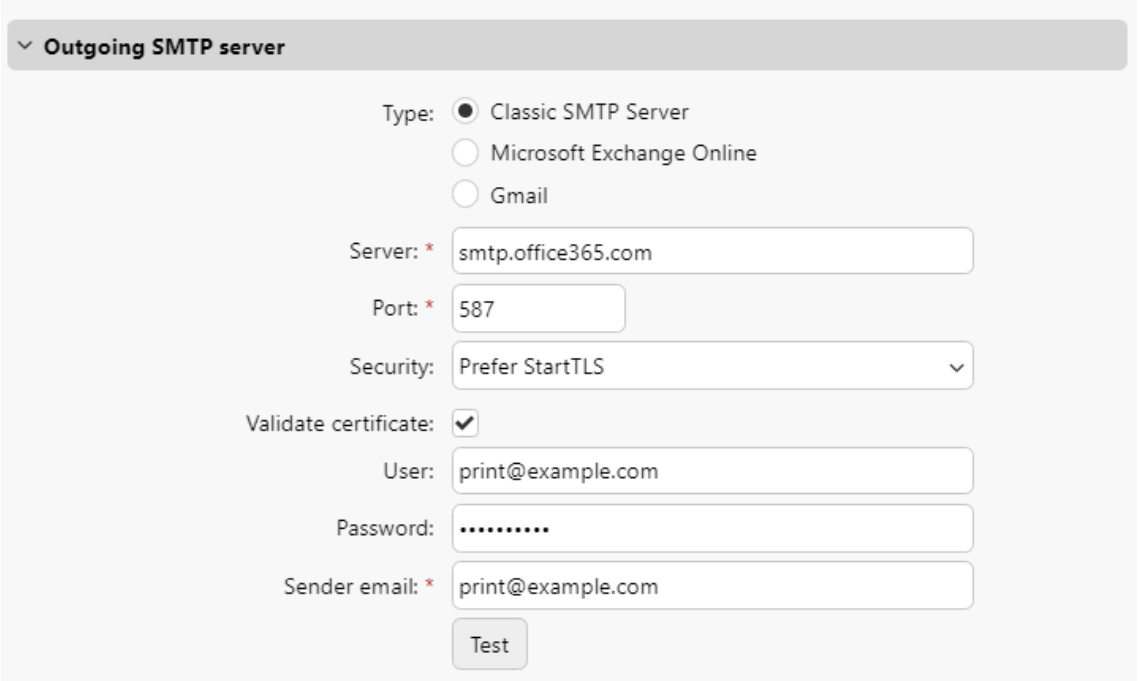
Se si utilizza la sincronizzazione degli account utente tramite il protocollo LDAP, impostare la sicurezza della connessione su SSL:



Per motivi di sicurezza, non utilizzare START TLS, poiché è vulnerabile agli attacchi MITM. Un certificato emesso da una CA attendibile deve essere configurato su tutti i server LDAP (controller di dominio Active Directory).

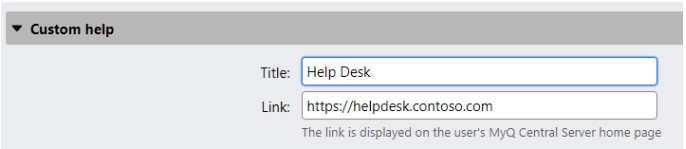
Proteggi il traffico SMTP

Se in MyQ Central Server è configurato un server SMTP, imporre l'uso di TLS con convalida del certificato:



Utilizzare sempre FQDN

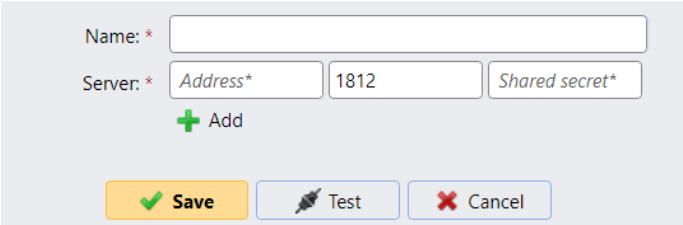
Per prevenire attacchi MITM, utilizzare rigorosamente nomi di dominio completi in tutte le finestre di configurazione:



Non contattare mai i server digitando solo indirizzi IP o nomi a etichetta singola.

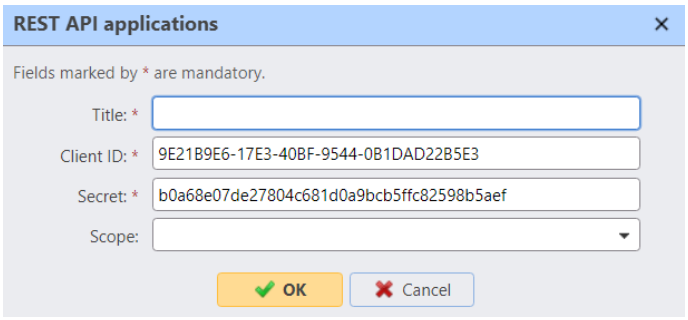
Traffico RADIUS sicuro

Se si utilizza l'autenticazione RADIUS, generare sempre segreti condivisi complessi specifici per MyQ Central Server:



Proteggere le chiavi API REST

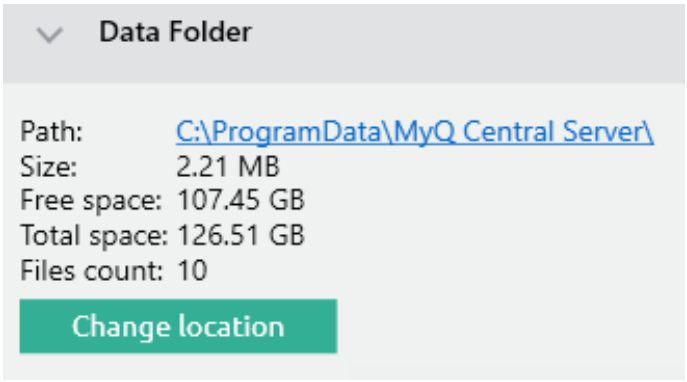
Quando si utilizzano le API REST, proteggere i segreti client da un'esposizione non necessaria ed eseguire periodicamente il rollover dei segreti:



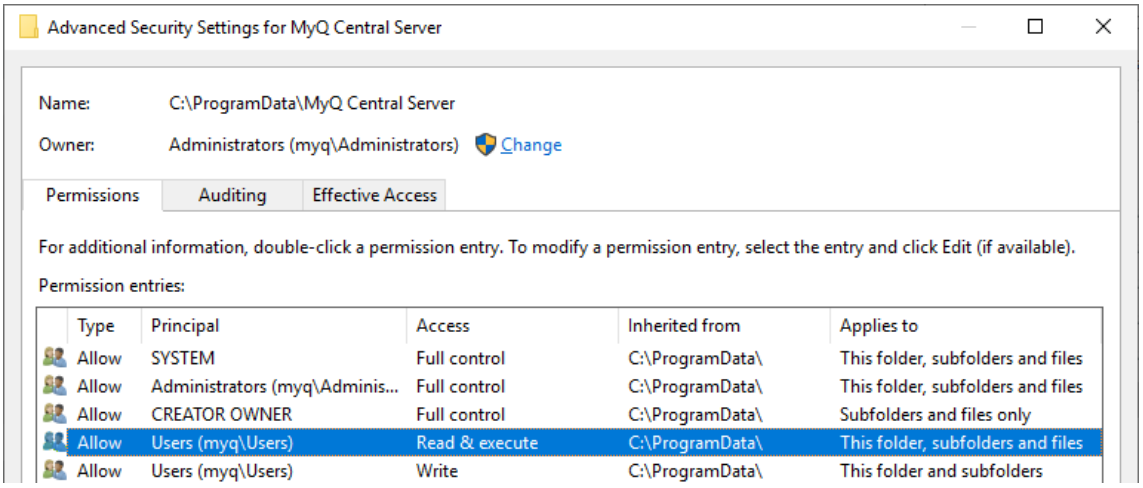
1.1.3 Sicurezza dei dati

Limitare i permessi della cartella dei dati

La cartella dei dati di MyQ Central Server contiene dati altamente sensibili, tra cui il database degli utenti e la chiave privata del certificato TLS. La sua posizione attuale è visualizzata nell'applicazione MyQ Central Server Easy Config:



Per impostazione predefinita, tutti gli utenti (locali/di dominio) dispongono di accesso in lettura:



Solo gli amministratori, l'account SYSTEM e l'account di servizio MyQ dovrebbero avere accesso a questa directory. Ecco uno script batch di esempio che può essere utilizzato per rafforzare le autorizzazioni:

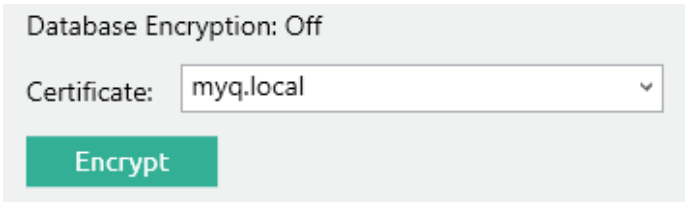
```
@ECHO OFF

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

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

Abilitare la crittografia del database

Quando si utilizza il database integrato, crittografarlo sempre utilizzando un certificato personalizzato per ridurre il rischio di fughe di dati:



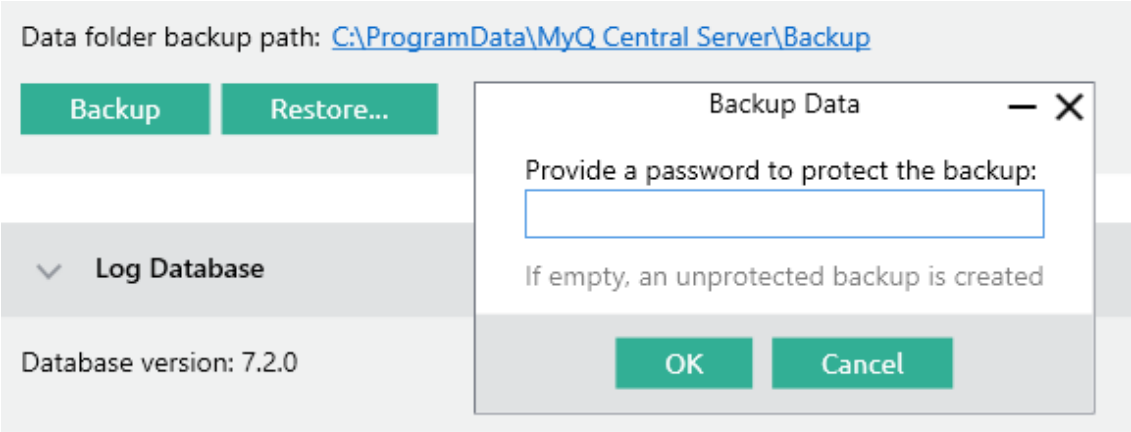
Il certificato deve avere l'uso avanzato della chiave (EKU) "Encrypting File System" e deve trovarsi in uno dei seguenti archivi di certificati del computer:

- Personale
- Editori attendibili
- Autorità di certificazione radice di terze parti
- Altre persone

L'archivio "Personale" è quello preferito.

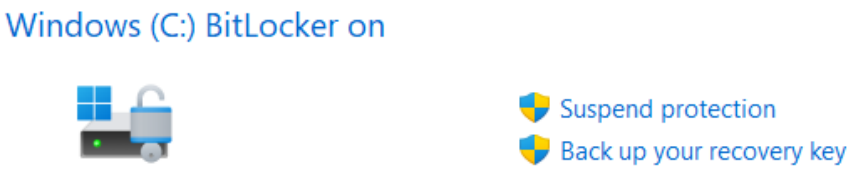
Crittografare i backup

I backup del database devono essere protetti da password sicure e generate in modo casuale:



Abilitare la crittografia del disco

Se possibile, è consigliabile abilitare una tecnologia di crittografia completa del disco, come Microsoft BitLocker, sul Central Server MyQ per proteggere i dati inattivi:

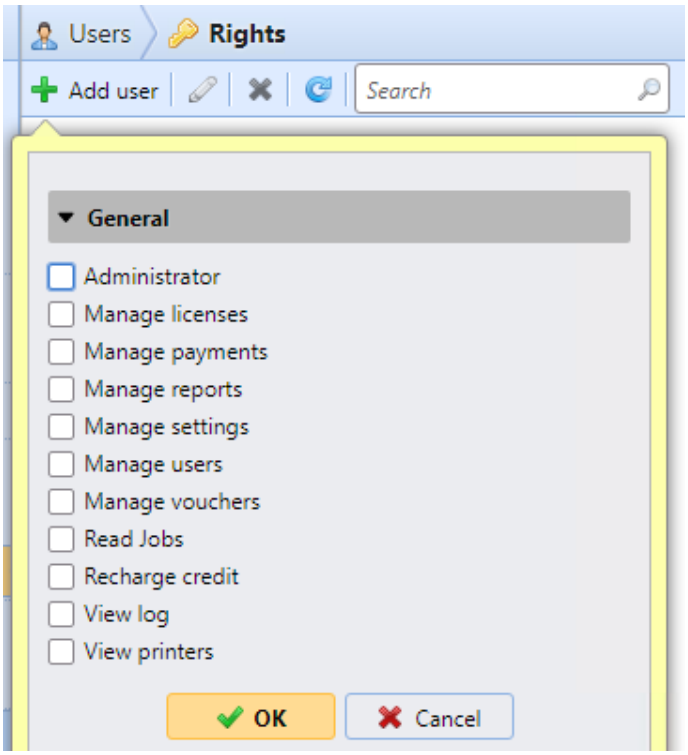


1.1.4 Ulteriori raccomandazioni

Pagine OEM collegate
This ScriptRunner macro could not be rendered for export.

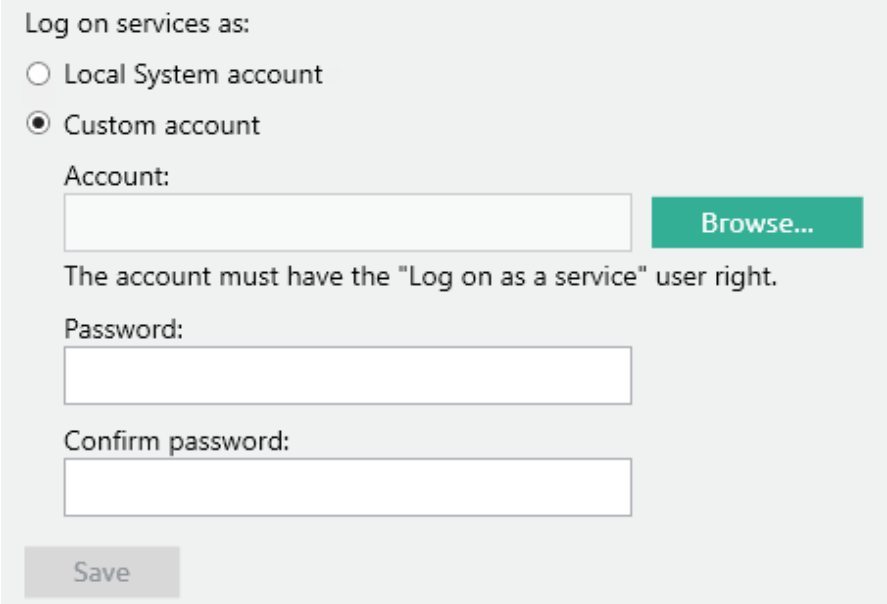
Implementare RBAC

Non utilizzare l'account *admin predefinito per le operazioni regolari. Utilizzare invece la delega dei privilegi, applicando il principio del privilegio minimo:



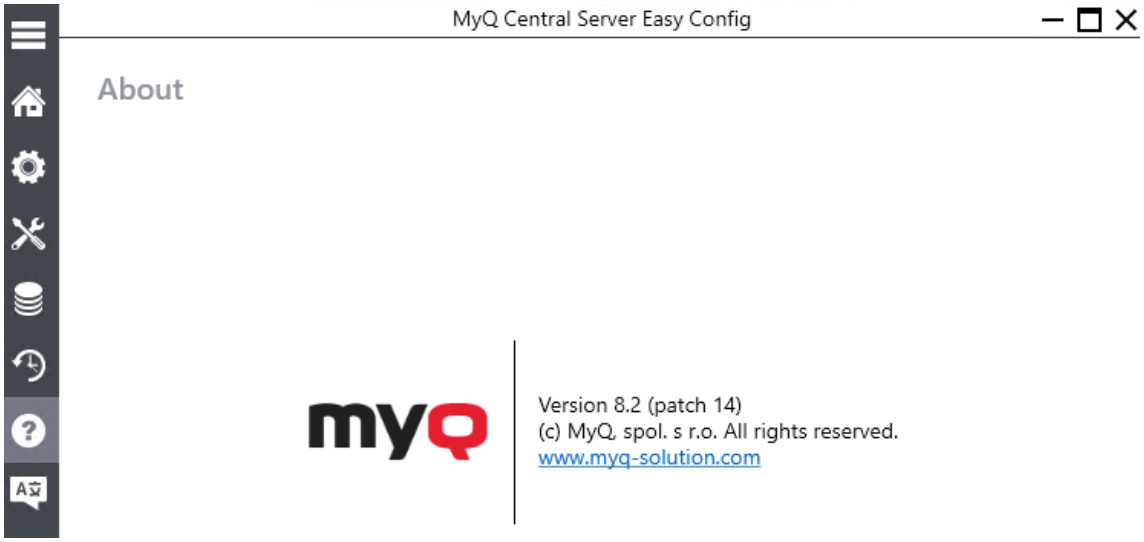
Configurare un account di servizio personalizzato

MyQ Central Server viene eseguito per impostazione predefinita con l'account SYSTEM altamente privilegiato. Configurare invece un account di servizio personalizzato con una password complessa:



Mantenere aggiornato il server

Installare gli aggiornamenti di sicurezza forniti da MyQ non appena disponibili. È possibile verificare la versione dell'applicazione attualmente installata in MyQ Central Server Easy Config:



Mantenere sicuro il sistema operativo

MyQ Central Server è sicuro solo quanto il sistema operativo sottostante. Mantenerlo aggiornato e applicare le politiche di sicurezza raccomandate da Microsoft.

Aggiornare regolarmente il software per correggere le vulnerabilità di sicurezza e migliorare le prestazioni. Controllare i requisiti di sistema per l'elenco dei requisiti e delle raccomandazioni.

Ad esempio, .NET deve essere aggiornato con strumenti di gestione o tramite Windows Updates su base opt-in[3].

Pianificare il ripristino di emergenza

Creare periodicamente backup di MyQ Central Server, inclusi database, certificati e file di configurazione. Testare la procedura di ripristino almeno una volta.

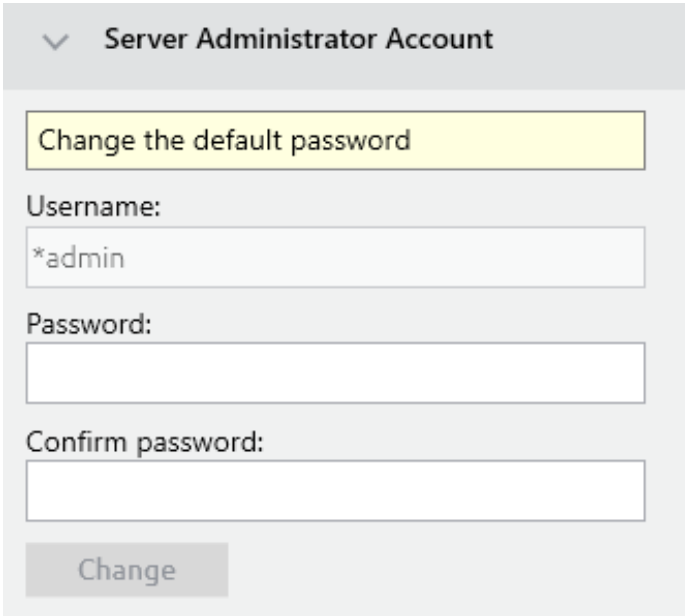
1.2 MyQ X Print Server

Pagine OEM collegate
This ScriptRunner macro could not be rendered for export.

1.2.1 PS Password predefinite

Modifica della password dell'amministratore del server

Uno dei primi passaggi dovrebbe essere la modifica della password amministrativa predefinita, che è *1234*:

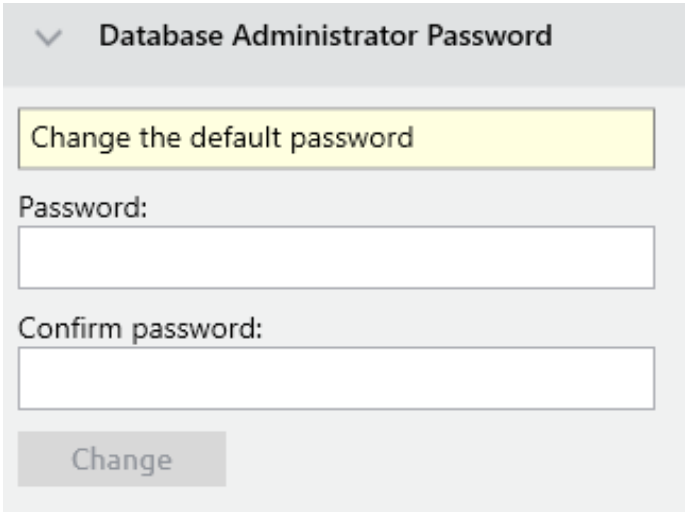


3. https://devblogs.microsoft.com/dotnet/server-operating-systems-auto-updates/

La password è memorizzata nel database in forma hash.

Modifica della password dell'amministratore del database

Modificare la password predefinita utilizzata da MyQ Print Server per l'autenticazione nel database interno Firebird:

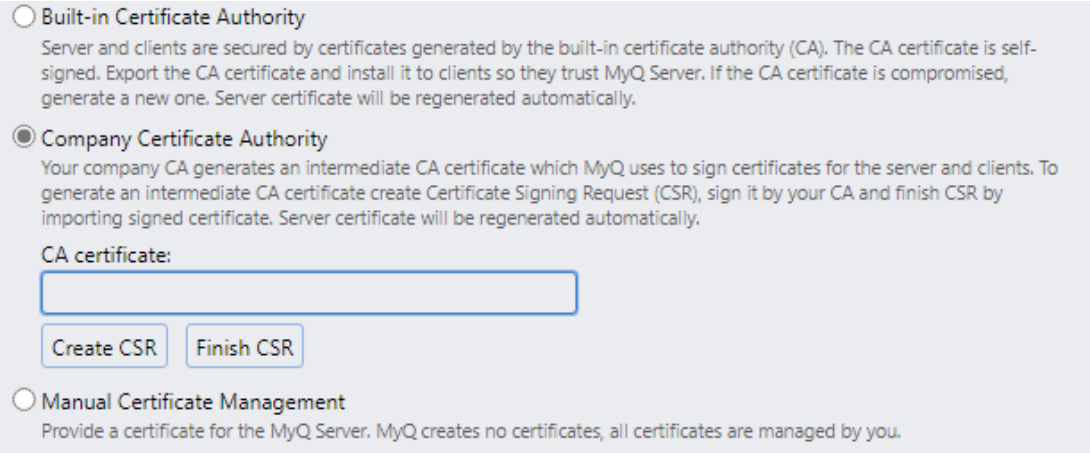


Questa password è memorizzata nel file "C:\ProgramData\MyQ\setup.ini" in forma crittografata ed è impostata su "*masterkey*" per impostazione predefinita.

1.2.2 PS Sicurezza della connessione

Configurare il certificato HTTPS

Per MyQ Print Server è necessario configurare un certificato personalizzato considerato attendibile da tutti i computer client. Sono disponibili tre modalità di gestione dei certificati:



Per impostazione predefinita, MyQ Print Server crea il proprio certificato CA radice e lo utilizza per firmare i certificati del server e dei client. La parte pubblica di questo certificato può essere esportata e distribuita nell'archivio di certificati attendibili del client, ad esempio utilizzando Criteri di gruppo o MDM.

Le organizzazioni che dispongono già di una propria PKI considerata attendibile potrebbero preferire la seconda opzione. MyQ Print Server utilizza la propria CA intermedia per emettere certificati server e client. Il certificato CA intermedio generato automaticamente deve essere firmato dalla CA aziendale affinché sia considerato attendibile dai client.

Se la politica di sicurezza aziendale non consente l'installazione di un certificato CA intermedio su MyQ Print Server, o se si deve utilizzare un certificato emesso da un'autorità di certificazione pubblica, è necessario ricorrere alla gestione manuale dei certificati.

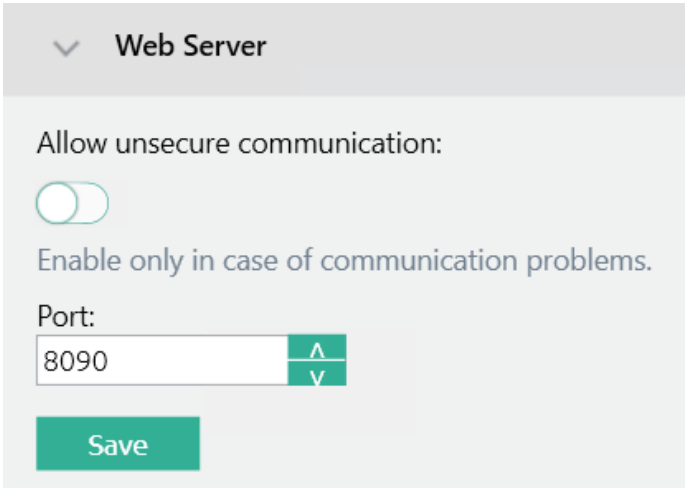
Indipendentemente dalla modalità CA, i certificati sono fisicamente memorizzati nella directory “C:\ProgramData\MyQ\Cert”, che può contenere i seguenti file:

- server.pfx – certificato del server con chiavi pubblica e privata
- server.cer – certificato del server con chiave pubblica
- server.key – chiave privata del server
- ca-root.crt – certificato CA radice aziendale con chiave pubblica
- ca-myq.pfx – certificato CA di emissione con chiavi pubblica e privata
- ca-myq.crt – certificato CA di emissione con chiave pubblica
- ca-myq.key – chiavi private della CA emittente

Le chiavi private della CA emittente locale (utilizzate nelle prime due modalità operative) sono sempre protette da una password generata in modo casuale che viene memorizzata nel database interno di Firebird in forma crittografata.

Blocca il traffico HTTP non crittografato

Il traffico HTTP non crittografato non deve essere abilitato nella configurazione di MyQ Print Server:



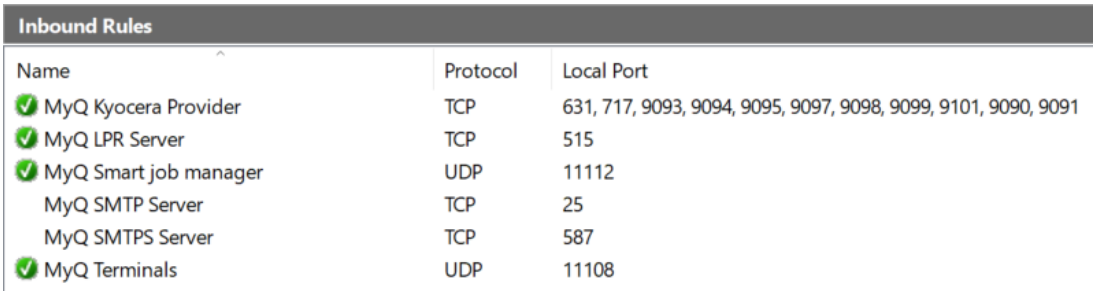
Verifica delle impostazioni di sicurezza delle comunicazioni

Controllare le versioni TLS minime di sicurezza configurate in Impostazioni – Rete – Versione TLS minima. L'impostazione predefinita a partire da MyQ X 10.2 è TLS 1.2.

Per opzioni più avanzate, come ad esempio come impostare invece la versione TLS minima richiesta a 1.3, consultare Sicurezzaavanzata.

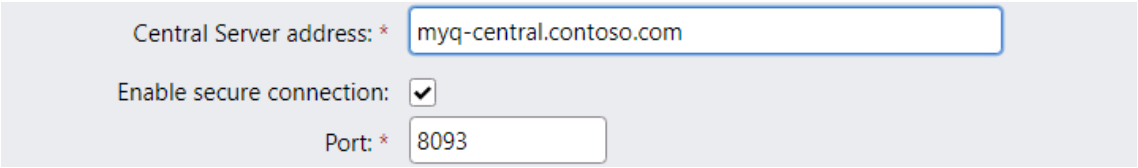
Bloccare le porte inutilizzate

Ridurre la superficie di attacco disabilitando le regole del firewall per i protocolli non utilizzati da MyQ Print Server:



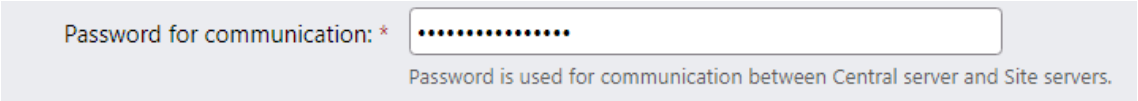
Crittografa le connessioni a MyQ Central Server

Utilizza solo HTTPS per connetterti a MyQ Central Server:



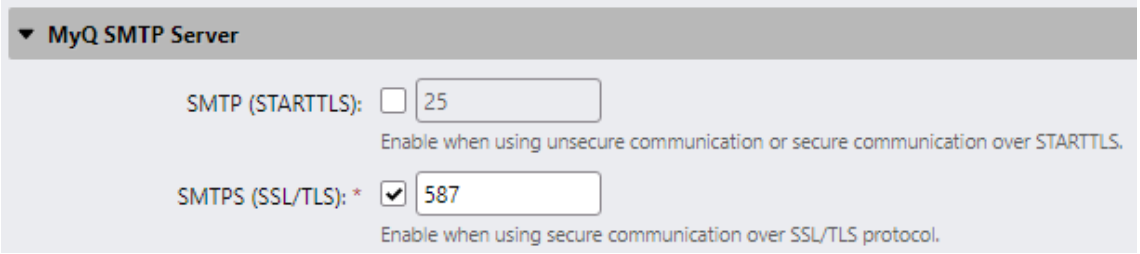
Utilizza password complesse per l'autenticazione da server a server

La password per la comunicazione tra il Central Server e il sito deve essere complessa (complessità della password):

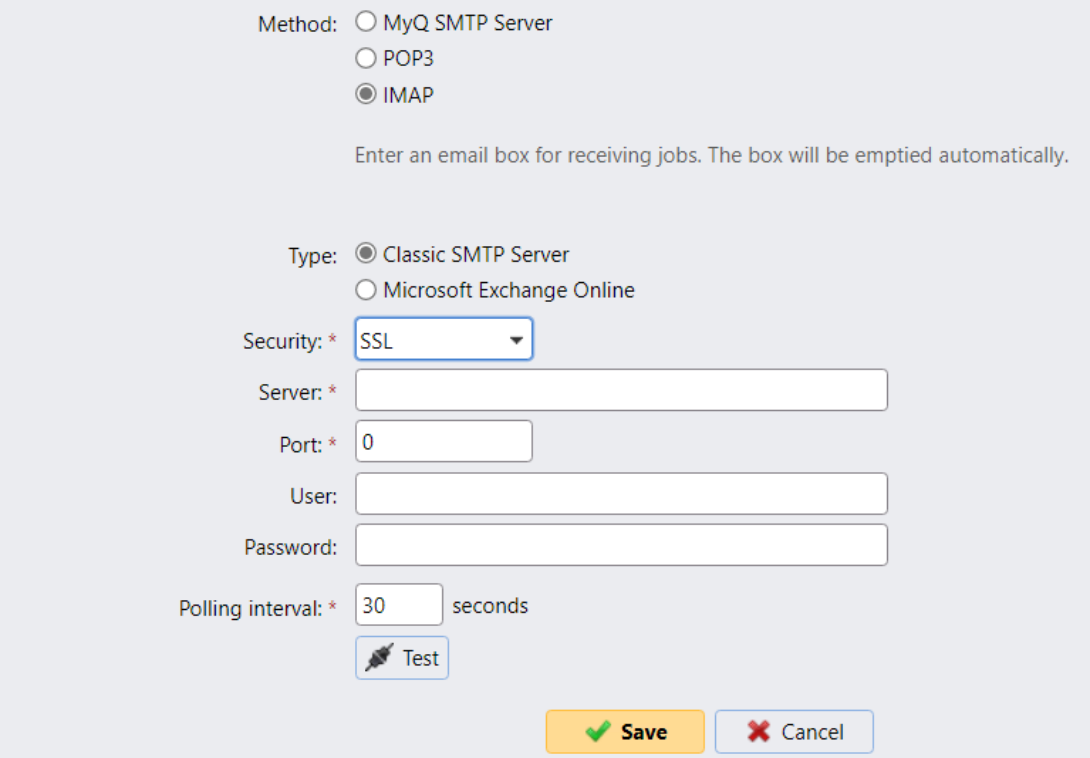


Proteggi il traffico SMTP

Quando si utilizza il protocollo SMTP per inviare e-mail o ricevere documenti dagli scanner di rete, è necessario applicare sempre la crittografia TLS per garantire la riservatezza dei dati.



La crittografia TLS deve essere applicata anche quando si utilizza il protocollo IMAP, mentre il protocollo POP3 legacy deve essere evitato:



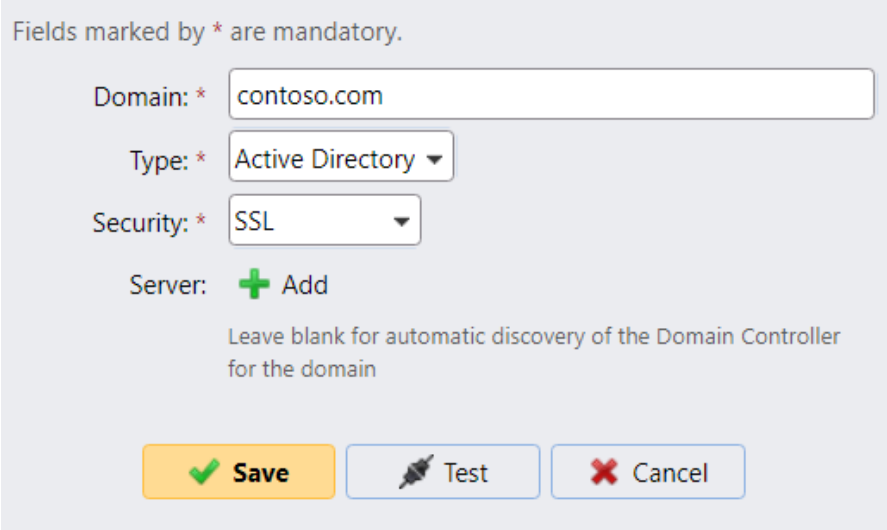
Utilizza password RADIUS complesse e uniche

Se si utilizza l'autenticazione RADIUS, generare sempre segreti condivisi forti specifici per MyQ Print Server:



Crittografare il traffico LDAP

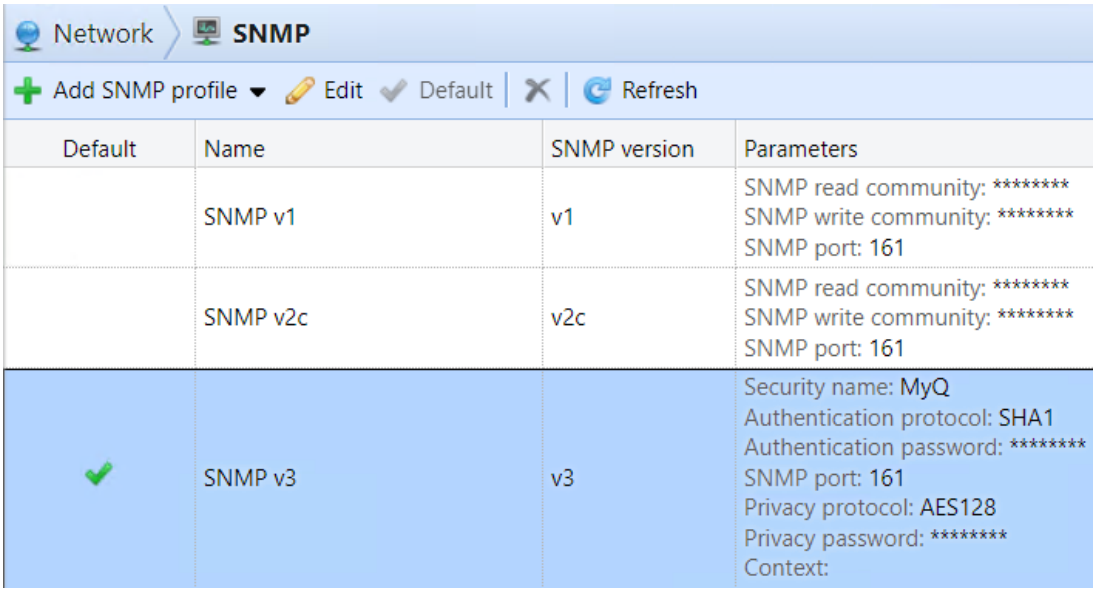
La crittografia TLS deve essere utilizzata per proteggere tutto il traffico LDAP:



Per motivi di sicurezza, non utilizzare START TLS, poiché è vulnerabile agli attacchi MITM. È necessario configurare un certificato emesso da una CA attendibile su tutti i server LDAP (controller di dominio Active Directory).

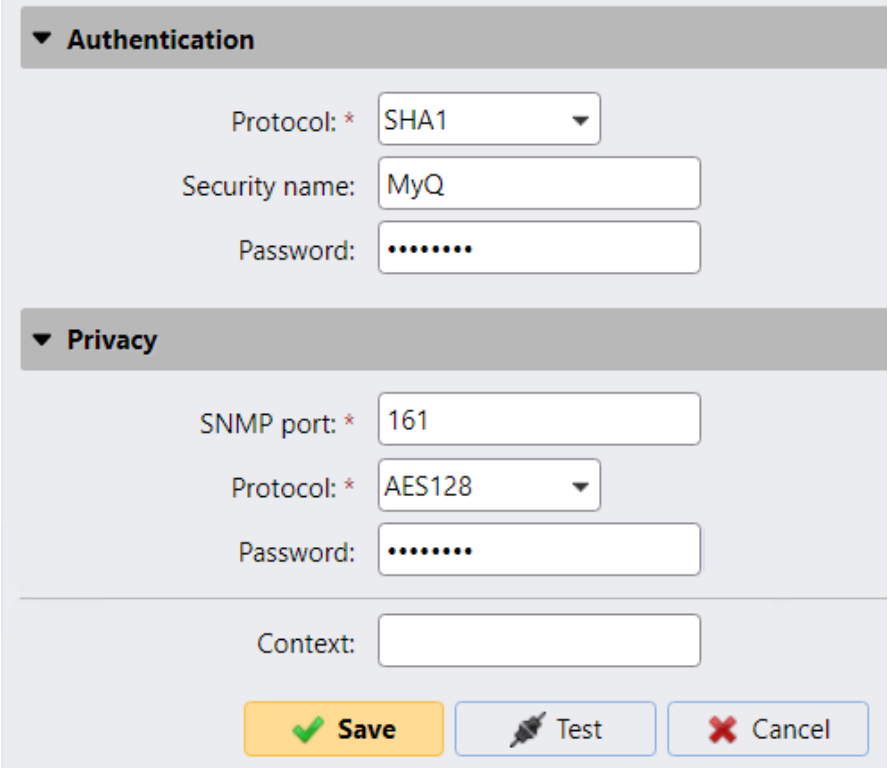
Proteggi il traffico SNMP

È necessario evitare comunicazioni SNMPv1 non sicure con i dispositivi:



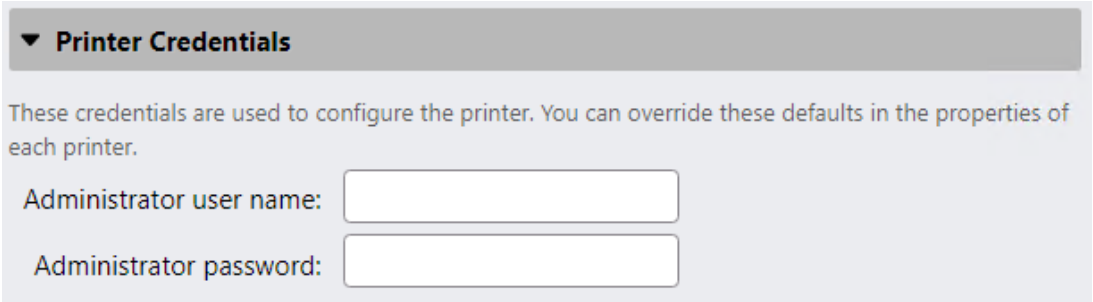
Default	Name	SNMP version	Parameters
	SNMP v1	v1	SNMP read community: ******** SNMP write community: ******** SNMP port: 161
	SNMP v2c	v2c	SNMP read community: ******** SNMP write community: ******** SNMP port: 161
✔	SNMP v3	v3	Security name: MyQ Authentication protocol: SHA1 Authentication password: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

Utilizzare solo SNMPv3 con una password complessa e configurare algoritmi crittografici più sicuri (SHA1 e AES):



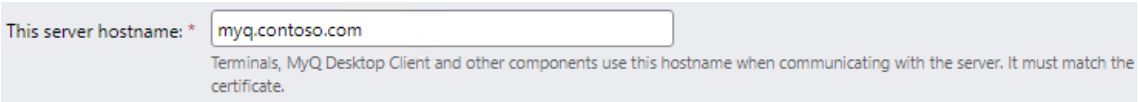
Proteggere le credenziali delle stampanti

La gestione delle credenziali delle stampanti avviene al di fuori di MyQ Print Server ed è specifica del fornitore. Se possibile, per la gestione delle stampanti si dovrebbero utilizzare password complesse generate in modo casuale:



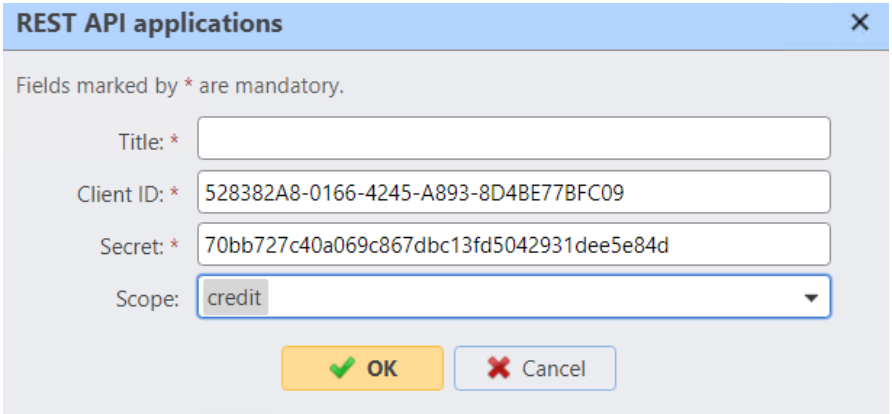
Utilizzare sempre FQDN

Per prevenire attacchi MITM, utilizzare rigorosamente nomi di dominio completi in tutte le finestre di configurazione:



Proteggere le chiavi API REST

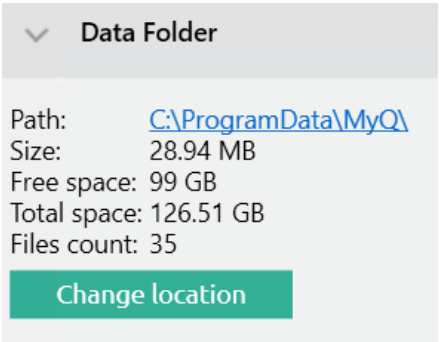
Quando si utilizzano le API REST, proteggere i segreti del client da un'esposizione non necessaria ed eseguire periodicamente il rollover dei segreti:



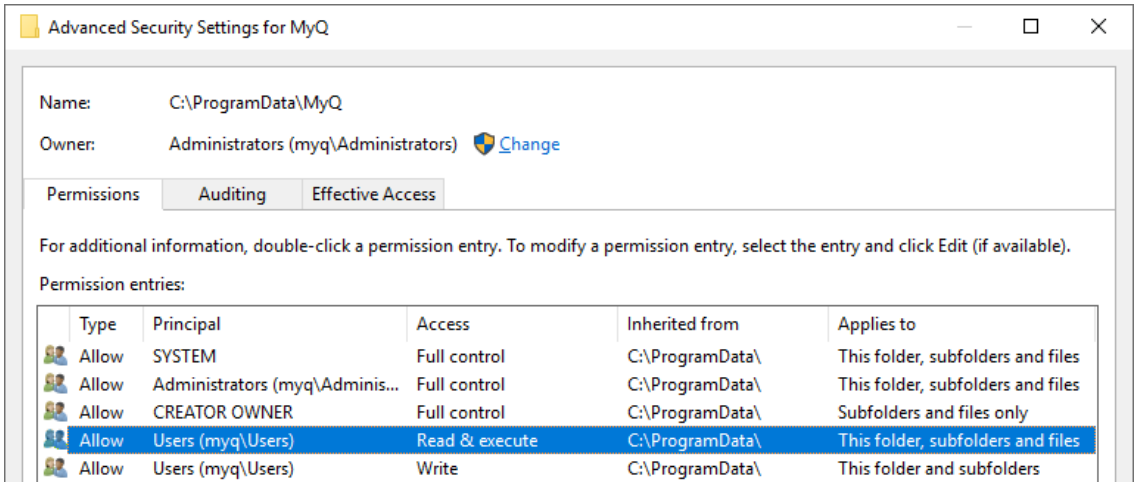
1.2.3 PS Sicurezza dei dati

Limitare i permessi della cartella dei dati

La cartella dei dati di MyQ Print Server contiene dati altamente sensibili, tra cui il database degli utenti e la chiave privata del certificato TLS. La sua posizione attuale è visualizzata nell'applicazione MyQ Easy Config:



Per impostazione predefinita, tutti gli utenti (locali/di dominio) dispongono di accesso in lettura:



Solo gli amministratori, l'account SYSTEM e l'account di servizio MyQ dovrebbero avere accesso a questa directory. Ecco uno script batch di esempio che può essere utilizzato per rafforzare le autorizzazioni:

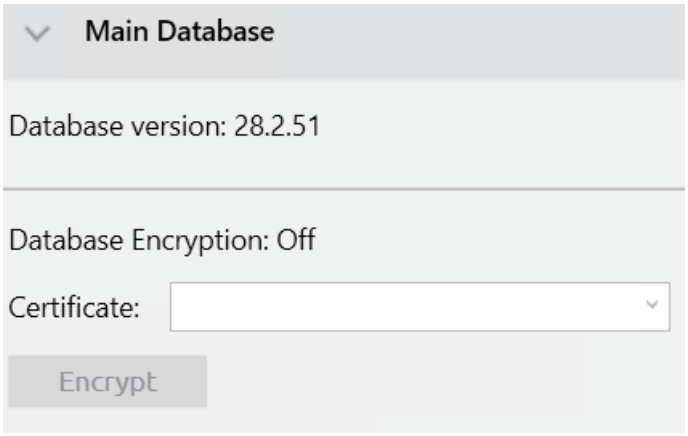
```
@ECHO OFF

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
```

Abilitare la crittografia del database

Crittografare sempre il database utilizzando un certificato personalizzato per ridurre il rischio di fughe di dati:



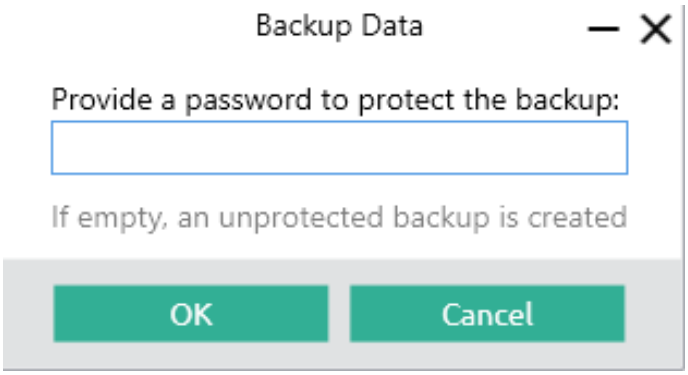
Il certificato deve avere l'uso avanzato della chiave (EKU) "Encrypting File System" e deve trovarsi in uno dei seguenti archivi di certificati del computer:

- Personale
- Emittenti attendibili
- Autorità di certificazione radice di terze parti
- Altre persone

L'archivio «Personale» è quello preferibile.

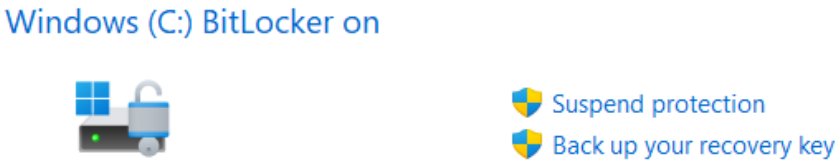
Crittografare i backup

I backup del database devono essere protetti da password sicure e generate in modo casuale:



Abilitare la crittografia del disco

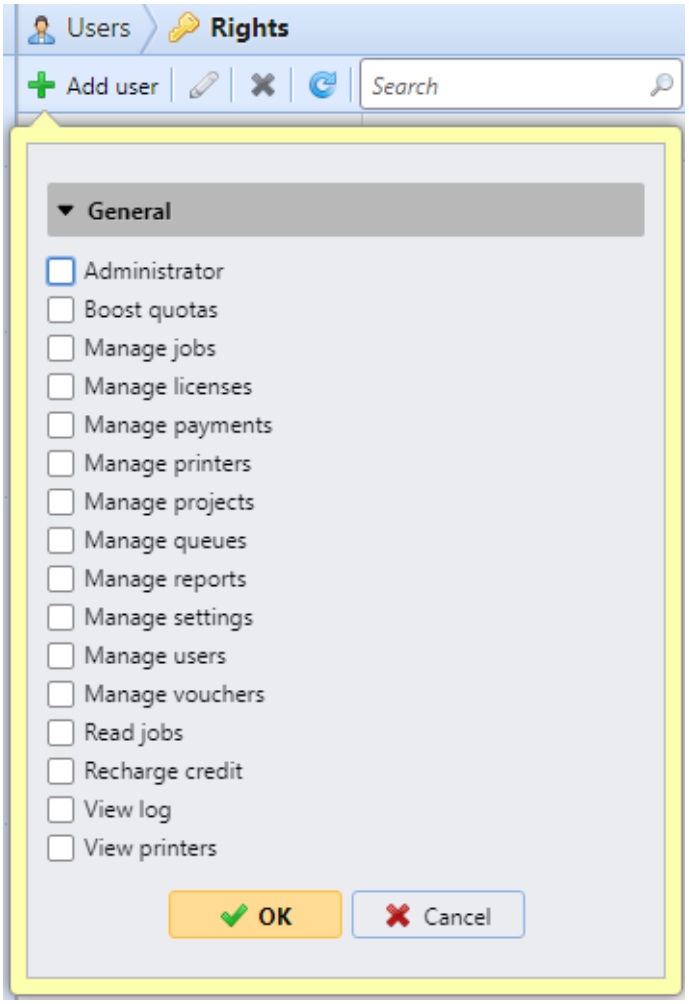
Se possibile, è consigliabile abilitare una tecnologia di crittografia completa del disco, come Microsoft BitLocker, sul Print Server MyQ per proteggere i dati inattivi:



1.2.4 PS Raccomandazioni aggiuntive

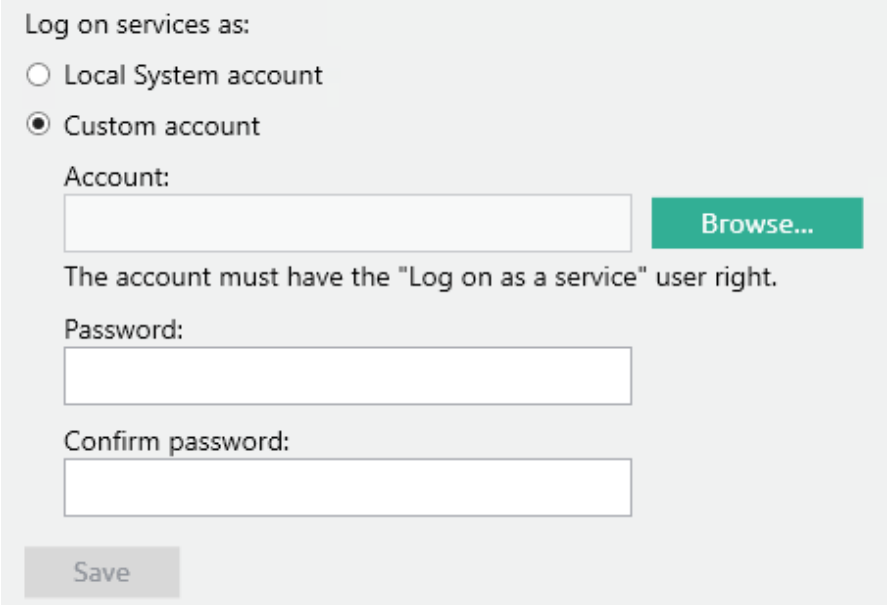
Implementare RBAC

Non utilizzare l'account *admin predefinito per le operazioni regolari. Utilizza invece la delega dei privilegi, applicando il principio del privilegio minimo:



Configurare un account di servizio personalizzato

MyQ Print Server viene eseguito per impostazione predefinita con l'account SYSTEM, che dispone di privilegi elevati. Configurare invece un account di servizio personalizzato con una password complessa:



Mantenere aggiornato il server

Installare gli aggiornamenti di sicurezza forniti da MyQ non appena disponibili. È possibile verificare la versione dell'applicazione attualmente installata in MyQ Easy Config:



Mantenere sicuro il sistema operativo

MyQ Print Server è sicuro solo quanto il sistema operativo sottostante. Mantenerlo aggiornato e applicare le politiche di sicurezza raccomandate da Microsoft.

Aggiornare regolarmente il software per correggere le vulnerabilità di sicurezza e migliorare le prestazioni. Controllare i Requisiti di sistema per l'elenco dei requisiti e delle raccomandazioni.

Ad esempio, .NET deve essere aggiornato tramite strumenti di gestione o tramite Windows Update su base facoltativa.[4]

Pianificare il ripristino di emergenza

Eseguire periodicamente il backup di MyQ Print Server, inclusi database, certificati e file di configurazione. Verificare la procedura di ripristino almeno una volta.

1.3 Desktop Client MyQ X

Pagine OEM collegate
This ScriptRunner macro could not be rendered for export.

Il Desktop Client MyQ utilizza robusti meccanismi di sicurezza per garantire comunicazioni sicure, autenticazione e integrità dei dati negli ambienti di stampa aziendali. Questo documento descrive in dettaglio i protocolli, i metodi di autenticazione e le best practice di configurazione alla base dell'architettura di sicurezza del Desktop Client, con particolare attenzione alla crittografia TLS, all'autenticazione integrata di Windows (IWA), a Kerberos, a NTLM e all'integrazione di Entra ID. Vengono analizzate implementazioni tecniche quali la registrazione del nome principale del servizio (SPN), la gestione dei certificati e i flussi di accesso silenzioso per dimostrare la conformità agli standard di sicurezza moderni.

1.3.1 Architettura di comunicazione sicura

Crittografia TLS predefinita

I server di stampa e Central Server applicano la crittografia TLS 1.2+ per tutti i canali di comunicazione, comprese le interazioni con Desktop Client. Ciò garantisce la riservatezza e l'integrità dei dati durante lo spooling dei lavori, l'autenticazione e la

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

reportistica. Gli amministratori devono configurare gli endpoint HTTPS utilizzando nomi di dominio completi (FQDN) per prevenire attacchi man-in-the-middle (MITM).

Modalità di convalida dei certificati

- **Modalità rigorosa**: richiede che i certificati server siano emessi da un'autorità di certificazione (CA) attendibile o aggiunti manualmente all'archivio di fiducia del sistema. I tentativi di connessione falliscono se la convalida non va a buon fine. Si consiglia di utilizzare la modalità rigorosa quando possibile.
- **Modalità normale**: consente agli utenti di ignorare gli avvisi relativi ai certificati non attendibili, con i certificati accettati memorizzati in `%ProgramData%\MyQ\Desktop Client\cert.store` per le sessioni future.

1.3.2 Meccanismi di autenticazione

Autenticazione Windows integrata (IWA)

L'IWA consente un'autenticazione senza interruzioni in ambienti collegati al dominio utilizzando Kerberos o NTLM. Il server sfrutta l'API del server HTTP di Windows (`http.sys`) per gestire le richieste HTTP in entrata e convalidare i nomi principali del servizio (SPN), garantendo l'integrità del protocollo.

Flusso di lavoro Kerberos

1. **Acquisizione del Ticket Granting Ticket (TGT)**: i client collegati al dominio ottengono un TGT dal Key Distribution Center (KDC).
2. **Richiesta di ticket di servizio**: il client richiede un ticket di servizio `HTTP/<FQDN>` dal KDC.
3. **Convalida del token**: MyQ Server convalida il ticket di servizio rispetto all'SPN registrato.

Configurazione critica:

- Il server deve disporre di un SPN correttamente configurato affinché l'autenticazione Kerberos funzioni correttamente.
- L'accesso tramite indirizzi IP bypassa Kerberos, costringendo il fallback a NTLM.

Applicazione di Kerberos

Per gli ambienti che richiedono una sicurezza più rigorosa, è possibile configurare l'applicazione in modo che **utilizzi esclusivamente Kerberos** e non consenta il fallback NTLM. Ciò viene eseguito a livello di server, non esclusivamente per il Desktop Client.

1. Disabilitare NTLM tramite `KerberosOnly=True` in `config.ini`.
2. Registrare gli SPN per tutti i server MyQ utilizzando `setspn`.
3. Utilizza FQDN invece di indirizzi IP per gli endpoint del server.

Fallback NTLM

NTLM funge da fallback in scenari non basati su dominio o IP. Sebbene meno sicuro, utilizza un meccanismo di challenge-response con hash della password dell'utente. Per applicare esclusivamente Kerberos, seguire il suggerimento sopra riportato.

Accesso silenzioso Entra ID

Per i dispositivi Entra ID o ibridi, Desktop Client utilizza Microsoft Authentication Library (MSAL) e Windows Authentication Manager (WAM) per acquisire i token in modo silenzioso tramite l'account del sistema operativo. Il flusso prevede:

1. **Acquisizione del token**: MSAL recupera un token ID utilizzando WAM.
2. **Scambio di token**: il token ID viene scambiato con un token di accesso MyQ per autenticare le chiamate API REST.

Flusso del codice di autorizzazione OAuth 2.0

Per gli ambienti non Windows, Desktop Client supporta OAuth 2.0 tramite la `authorization_code` concessione:

1. **Reindirizzamento utente**: il client reindirizza gli utenti alla pagina di accesso MyQ.
2. **Scambio di codici**: dopo l'autenticazione, il codice di autorizzazione viene scambiato con un token di accesso.

Configurazione Entra ID

- Abilita **Accedi con Microsoft** nelle impostazioni del server MyQ per i dispositivi con connessione ibrida.
- Assicurarsi che i dispositivi siano registrati con Entra ID per sfruttare l'autenticazione silenziosa.

Gestione dei certificati

Certificati radice attendibili

- **Modalità rigorosa**: i certificati devono essere preinstallati nell'archivio di fiducia del sistema operativo (ad esempio, tramite Criteri di gruppo).
- **Modalità normale**: i certificati approvati dall'utente vengono archiviati in `cert.store` e riutilizzati per le sessioni successive.

Flusso di lavoro di convalida

1. La convalida del certificato server verifica la catena di fiducia.
2. Se la convalida non va a buon fine, agli utenti viene chiesto di accettare o rifiutare il certificato (questo avviene solo se è in uso la modalità di convalida normale anziché quella rigorosa).
3. I certificati accettati vengono memorizzati nella cache per evitare richieste ripetute (solo se è in uso la modalità di convalida normale anziché quella rigorosa).

> **Best practice per i certificati**
> Si consiglia di implementare sempre certificati firmati da CA aziendali per i server MyQ.

Conclusione

MyQ Desktop Client integra autenticazione e crittografia di livello aziendale per mitigare rischi quali il furto di credenziali e l'intercettazione. Applicando Kerberos, TLS e la convalida dei certificati, le organizzazioni possono allinearsi ai principi Zero Trust mantenendo l'usabilità attraverso flussi di autenticazione silenziosi.

2 Carta bianca sulla sicurezza di MyQ X

Panoramica delle funzionalità di sicurezza di MyQ X

MyQ X offre una serie di funzionalità volte a migliorare la sicurezza e la privacy degli utenti finali e dell'azienda. Queste funzionalità includono la stampa sicura dal dispositivo multifunzione, la personalizzazione della sessione utente e continuano ad avere un impatto anche dopo la stampa del documento grazie all'utilizzo di filigrane.

Di seguito è riportato un breve riassunto delle funzionalità di sicurezza di MyQ X:

- Conformità al GDPR
- Stampa sicura
- Sessioni utente con diverse opzioni di autenticazione, compresa l'autenticazione a due fattori.
- Logout manuale e automatico dalle sessioni utente
- Crittografia dei dati end-to-end, compresa la crittografia dei dati inattivi (database, lavori, registri)
- Cartelle di destinazione della scansione predefinite dall'amministratore MyQ
- Code private per l'eliminazione immediata dei lavori di stampa dopo il rilascio
- Modalità privacy per l'anonimizzazione dei nomi dei lavori di stampa
- Accesso limitato alle opzioni di configurazione del Print Server sull'interfaccia web MyQ X
- Diritti personalizzabili per l'accesso a diverse opzioni di configurazione
- Livelli multipli di complessità delle password
- Registro di controllo delle modifiche alle impostazioni
- Supporto per l'autorità di certificazione aziendale
- Applicazione di filigrane ai documenti stampati
- Anteprima del lavoro
- Controllo dei documenti digitalizzati tramite sistemi OCR e DMS
- Archiviazione dei lavori di stampa

L'approccio alla sicurezza di MyQ X si basa sul principio che **La sicurezza non è un elemento secondario, ma parte integrante dell'intero ecosistema di gestione della stampa.**La piattaforma implementa una strategia di difesa completa che protegge i dati e i flussi di lavoro in ogni fase del ciclo di vita dei documenti.

2.1 Architettura Zero Trust

Seguendo la metodologia "non fidarti mai, verifica sempre", MyQ X parte dal presupposto che le minacce possano provenire sia dall'interno che dall'esterno di una rete. Ogni connessione, utente e dispositivo deve essere autenticato e autorizzato

prima di accedere alle risorse di stampa, garantendo una verifica continua durante tutte le interazioni.

2.2 Struttura di protezione trifase

MyQ X affronta la questione della sicurezza attraverso tre fasi fondamentali:

2.2.1 Protezione dell'infrastruttura di stampa

Tutte le infrastrutture di supporto sono adeguatamente protette prima della stampa di qualsiasi documento, comprese le workstation, i dispositivi mobili, i server, le reti e i dispositivi di stampa.

2.2.2 Protezione dei flussi di lavoro di stampa

Flussi di lavoro sicuri e comprovati, tra cui il rilascio di stampe autenticate, l'isolamento dei lavori e la reportistica completa, prevengono le vulnerabilità che potrebbero esporre le organizzazioni a rischi.

2.2.3 Protezione della stampa

Protezione continua tramite filigrana, firme digitali e registri di controllo completi che garantiscono la tracciabilità e incoraggiano un comportamento responsabile da parte degli utenti.

2.3 Privacy fin dalla progettazione

La protezione dei dati è integrata nell'architettura di MyQ X sin dalla sua concezione. Il sistema riduce al minimo la raccolta di dati, implementa una crittografia avanzata e offre agli utenti il controllo sulle proprie informazioni personali per garantire la conformità al GDPR e la protezione della privacy.

2.4 Evoluzione continua della sicurezza

MyQ X garantisce la sicurezza attraverso aggiornamenti regolari, risoluzione tempestiva delle vulnerabilità, integrazione delle informazioni sulle minacce e valutazioni e certificazioni di sicurezza continue da parte di terzi.

Questo approccio incentrato sulla sicurezza garantisce alle organizzazioni la possibilità di implementare MyQ X con la certezza che le loro informazioni sensibili, i requisiti di conformità e la continuità operativa siano protetti da misure di sicurezza leader nel settore.

2.5 Miglioramenti chiave per la sicurezza in 10.2

MyQ X 10.2 introduce significativi miglioramenti alla sicurezza progettati per rafforzare la protezione contro le minacce informatiche in continua evoluzione, mantenendo al contempo l'efficienza operativa. Questi miglioramenti risolvono vulnerabilità critiche e implementano standard di sicurezza moderni.

2.5.1 Sicurezza TLS migliorata

Versione minima TLS 1.2 predefinita: MyQ X 10.2 aumenta la versione TLS minima predefinita da 1.1 a 1.2, con supporto per TLS 1.3. Ciò elimina il supporto per i protocolli SSL obsoleti e i codici di cifratura deboli che comportano rischi per la sicurezza.

Convalida dei certificati migliorata: la convalida dei certificati migliorata impedisce l'uso di certificati scaduti o emessi in modo improprio, proteggendo dagli attacchi man-in-the-middle e da altre vulnerabilità. Il sistema ora si fida automaticamente dei certificati CA radice provenienti dall'archivio dei certificati di sistema del server.

2.5.2 Miglioramenti alla sicurezza dell'autenticazione

Maggiore sicurezza di password e PIN: gli algoritmi di hashing delle password migliorati rafforzano la protezione delle credenziali. Il sistema introduce nuove regole di sicurezza per i PIN, tra cui la lunghezza minima obbligatoria di 6 cifre e la prevenzione di combinazioni facilmente intuibili come "1234" o "1111".

Protezione dei tentativi di accesso: i tentativi di autenticazione non riusciti sono ora limitati per motivi di sicurezza. Per impostazione predefinita, i client/dispositivi vengono bloccati per 5 minuti dopo più di 5 tentativi di accesso non validi entro 60 secondi, con periodi di tempo configurabili.

Miglioramento della registrazione degli eventi di accesso: la registrazione avanzata degli eventi di accesso, in particolare dei tentativi di autenticazione non riusciti, semplifica il filtraggio e il monitoraggio degli eventi di sicurezza in MyQ Log per gli amministratori.

2.5.3 Aggiornamenti alla sicurezza del database

Implementazione di Firebird 4.0: l'aggiornamento al motore di database Firebird 4.0 offre funzionalità di sicurezza avanzate e prestazioni migliorate. Le password del database sono ora oscurate nei file di log per impedire l'esposizione delle credenziali.

Protezione dei dati migliorata: accesso limitato ai dati sensibili tramite report personalizzati e account di reporting esterni, garantendo la riservatezza dei dati a diversi livelli di accesso.

2.5.4 Risoluzione delle vulnerabilità

Correzioni CVE critiche: MyQ X 10.2 risolve diverse vulnerabilità critiche, tra cui:

- CVE-2024-28059: vulnerabilità di esecuzione di codice remoto non autenticato.
- CVE-2024-22076: Miglioramenti alla sicurezza dello scripting PHP.
- CVE-2023-45853, CVE-2023-5678, CVE-2023-49316: vulnerabilità dei componenti di terze parti.

Aggiornamenti di sicurezza dei componenti: le versioni aggiornate di componenti critici, tra cui OpenSSL 3.1.0, PHP 8.3.14 e Apache 2.4.57, risolvono vulnerabilità di sicurezza note.

2.5.5 Sicurezza API e integrazione

Restrizioni API REST: ambiti limitati per client noti e rimozione delle funzionalità per operazioni sensibili come la modifica dei server di autenticazione degli utenti, rafforzando la sicurezza delle API.

Controlli di scripting PHP: le nuove impostazioni Easy Config consentono agli amministratori di bloccare/sbloccare l'accesso allo scripting PHP, migliorando la sicurezza mantenendo queste impostazioni in modalità di sola lettura.

2.5.6 Sicurezza amministrativa

Maggiore sicurezza degli account amministrativi: la password amministrativa predefinita è stata rimossa per le nuove installazioni. Gli amministratori possono ora disabilitare gli account amministrativi quando non sono necessari, promuovendo l'uso di account utente specifici con diritti appropriati piuttosto che account amministrativi condivisi.

Questi miglioramenti alla sicurezza dimostrano l'impegno di MyQ X nel mantenere standard di sicurezza di livello aziendale, affrontando al contempo le sfide contemporanee della sicurezza informatica. Aggiornamenti di sicurezza regolari e una gestione proattiva delle vulnerabilità garantiscono alle organizzazioni di poter implementare MyQ X con fiducia nella propria sicurezza.

2.6 Valore aziendale della gestione sicura della stampa

La gestione sicura della stampa offre un valore aziendale misurabile trasformando l'infrastruttura di stampa da una potenziale responsabilità a una risorsa strategica per la sicurezza. MyQ X fornisce alle organizzazioni una protezione completa che affronta l'intera gamma di rischi legati alla stampa, migliorando al contempo l'efficienza operativa.

2.6.1 Mitigazione dei rischi e riduzione dei costi

Prevenzione della violazione dei dati: Secure Print Release garantisce che i documenti riservati non vengano mai lasciati incustoditi nei vassoi delle stampanti, eliminando l'accesso non autorizzato alle informazioni sensibili. Gli utenti effettuano l'autenticazione prima che i loro lavori di stampa vengano rilasciati, mantenendo il controllo completo sulla sicurezza dei documenti.

Evitare i costi di conformità: le funzionalità di conformità GDPR, HIPAA e SOX integrate aiutano le organizzazioni a evitare sanzioni normative e a ridurre i costi di preparazione degli audit attraverso controlli di conformità automatizzati e audit trail completi.

Continuità operativa: la funzione Device Spooling di MyQ mantiene le capacità di stampa durante le interruzioni del server, memorizzando i lavori crittografati localmente per un massimo di una settimana su 10 dispositivi, evitando interruzioni dell'attività durante la manutenzione del sistema o tempi di inattività imprevisti.

2.6.2 Principi di sicurezza avanzati

Implementazione Zero Trust: richiedendo l'autenticazione per ogni lavoro di stampa, MyQ X applica i principi "non fidarti mai, verifica sempre" in tutto l'ambiente di stampa, rafforzando la sicurezza complessiva dell'organizzazione.

Tracciabilità dei documenti: la filigrana e le firme digitali consentono alle organizzazioni di tracciare i documenti riservati durante tutto il loro ciclo di vita, garantendo la responsabilità e scoraggiando l'uso improprio delle informazioni sensibili.

Crittografia completa: la crittografia end-to-end dei dati di stampa, dei database e dei lavori di stampa memorizzati garantisce che le informazioni sensibili rimangano protette durante l'intero flusso di lavoro dei documenti, soddisfacendo i rigorosi requisiti di sicurezza.

2.6.3 Efficienza operativa

Ottimizzazione della larghezza di banda: il client spooling riduce il traffico di rete elaborando i lavori a livello locale, migliorando le prestazioni in ambienti con larghezza di banda limitata, come uffici remoti e filiali.

Autenticazione flessibile: diverse opzioni di autenticazione, tra cui carte d'identità, PIN, password e autenticazione tramite app mobile, offrono agli utenti metodi di accesso comodi ma sicuri che si adattano alle diverse esigenze aziendali. È disponibile anche l'autenticazione a più fattori (MFA), che combina questi metodi.

Gestione centralizzata: le politiche di sicurezza unificate su tutti i dispositivi semplificano l'amministrazione, garantendo al contempo standard di protezione coerenti in tutta l'organizzazione.

2.6.4 Vantaggi strategici per l'azienda

Vantaggio competitivo: dimostrare solide capacità di sicurezza di stampa può differenziare le organizzazioni nei mercati competitivi, in particolare nei settori che trattano dati sensibili o servono clienti attenti alla sicurezza.

Fiducia dei dipendenti: i flussi di lavoro di stampa sicuri danno agli utenti la certezza che i loro documenti sono protetti, migliorando la produttività e riducendo le preoccupazioni relative alla sicurezza che possono influire sull'efficienza sul posto di lavoro.

Infrastruttura pronta per il futuro: il framework di sicurezza completo di MyQ X consente alle organizzazioni di adattarsi alle minacce alla sicurezza informatica in continua evoluzione e ai requisiti normativi senza grandi revisioni dell'infrastruttura.

La gestione sicura della stampa con MyQ X trasforma la stampa da una potenziale vulnerabilità di sicurezza in un processo aziendale controllato, verificabile e conforme che supporta gli obiettivi organizzativi proteggendo al contempo le preziose risorse informative.

2.7 Conformità

Il quadro di conformità completo di MyQ X dimostra il suo impegno a soddisfare i più elevati standard di sicurezza internazionali e i requisiti normativi. Questo approccio multilivello garantisce alle organizzazioni di poter implementare MyQ X con fiducia, soddisfacendo al contempo i diversi requisiti di conformità in tutti i settori e giurisdizioni.

2.7.1 Certificazione e implementazione ISO 27001:2022

MyQ ha ottenuto **la certificazione ISO/IEC 27001:2022**, stabilendo un approccio sistematico alla gestione della sicurezza delle informazioni che soddisfa le migliori pratiche internazionali. L'implementazione comprende:

Quadro di gestione dei rischi: processi completi di valutazione dei rischi che identificano, valutano e mitigano i rischi per la sicurezza delle informazioni in tutte le operazioni aziendali e nelle implementazioni dei clienti.

Implementazione dei controlli di sicurezza: implementazione strutturata di controlli di sicurezza tecnici, amministrativi e fisici che proteggono le risorse informative durante tutto il loro ciclo di vita.

Processo di miglioramento continuo: revisioni e aggiornamenti regolari delle politiche, delle procedure e dei controlli di sicurezza per affrontare le minacce in evoluzione e mantenere la conformità alla certificazione.

Impegno della direzione: supervisione a livello esecutivo che garantisce che la sicurezza rimanga integrata nella strategia aziendale e nei processi decisionali operativi.

La certificazione convalida l'approccio sistematico di MyQ alla protezione dei dati dei clienti e al mantenimento della riservatezza, dell'integrità e della disponibilità dei sistemi informativi.

2.7.2 Quadro di conformità al GDPR e misure di protezione dei dati

MyQ X implementa **una conformità** completa **al GDPR** attraverso principi di privacy by design integrati nell'architettura del sistema:

Minimizzazione dei dati: il sistema raccoglie solo i metadati essenziali necessari per la funzionalità operativa, evitando il trattamento superfluo dei dati personali che potrebbe aumentare i rischi di conformità.

Gestione dei diritti degli utenti: implementazione completa dei diritti degli utenti GDPR, tra cui:

- Diritto di accesso ai dati personali
- Diritto di rettifica delle informazioni inesatte
- Diritto alla cancellazione ("diritto all'oblio")
- Diritto alla portabilità dei dati
- Diritto di limitazione del trattamento

Valutazioni d'impatto sulla protezione dei dati: valutazione sistematica dei rischi per la privacy relativi a nuove funzionalità e implementazioni, garantendo il mantenimento della conformità al GDPR durante l'evoluzione del sistema.

2.7.3 Requisiti di conformità regionali (HIPAA, SOX)

MyQ X supporta i framework di conformità specifici del settore attraverso solide funzionalità di protezione dei dati e di audit:

Conformità HIPAA per il settore sanitario:

- Crittografia delle informazioni sanitarie protette (PHI) inattive e in transito.
- Registrazione completa di tutti gli accessi ai dati sanitari sensibili.
- Controlli di accesso basati sui ruoli che limitano l'accesso alle PHI solo al personale autorizzato.
- Procedure di backup e ripristino sicure per i requisiti di conservazione dei dati sanitari.

Conformità SOX per i servizi finanziari:

- Audit trail dettagliati per l'elaborazione e la stampa di documenti finanziari.
- Controlli di accesso che impediscono la modifica non autorizzata dei registri finanziari.
- Funzionalità di archiviazione sicure che supportano i requisiti normativi di conservazione.
- Separazione dei compiti attraverso autorizzazioni basate sui ruoli e flussi di lavoro di approvazione.

Controlli di sicurezza aggiuntivi:

- Crittografia del database utilizzando algoritmi standard del settore.
- Protocolli di comunicazione sicuri per tutte le trasmissioni di dati.
- Procedure di backup automatizzate con crittografia e verifica dell'integrità.
- Registrazione e monitoraggio degli accessi per la reportistica di conformità.

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

MyQ implementa un ciclo di vita dello sviluppo software sicuro in linea con gli standard di settore e i requisiti della catena di fornitura **SLSA**, garantendo che le pratiche di sicurezza siano integrate in tutte le fasi del ciclo di vita del software.

Analisi

MyQ esegue **una** rigorosa **modellazione delle minacce** e definisce chiari **requisiti di sicurezza** durante la fase di analisi iniziale, consentendo l'identificazione precoce dei rischi e stabilendo una solida base di sicurezza prima dell'inizio della progettazione.

Progettazione

Tutte le proposte architetturali sono sottoposte a **revisioni** formali **dell'architettura di sicurezza** per convalidare l'aderenza a principi quali **il privilegio minimo**, **lo zero trust** e **la difesa in profondità**, garantendo che la sicurezza sia sistematicamente integrata nella progettazione del sistema.

Sviluppo

Gli sviluppatori seguono **pratiche di codifica sicure** e processi di revisione tra pari, mentre tutte le build vengono eseguite su **server di build** dedicati, isolati **e conformi allo standard SLSA**, garantendo la protezione dell'integrità del codice sorgente e degli artefatti di build.

Test

I test di sicurezza includono **SAST** automatizzato e **scansione delle dipendenze** integrati nelle pipeline CI, consentendo il rilevamento tempestivo delle vulnerabilità sia nel codice personalizzato che nei componenti di terze parti.

Distribuzione

Tutti gli artefatti di rilascio sono protetti tramite **la firma del codice** e verificati durante la distribuzione, garantendo **integrità**, **autenticità** e consegna controllata negli ambienti di produzione.

Manutenzione

Dopo la distribuzione, i sistemi sono sottoposti a **monitoraggio** continuo e **gestione** strutturata **delle patch**, garantendo un allineamento costante con le minacce in evoluzione e **le migliori pratiche di sicurezza**.

2.7.5 Audit di sicurezza regolari e test di penetrazione

MyQ mantiene una solida convalida della sicurezza attraverso programmi sistematici di test e valutazione:

Test di penetrazione automatizzati: l'integrazione con la piattaforma di sicurezza Qualys fornisce una valutazione continua delle vulnerabilità e test di penetrazione per tutte le versioni del software.

Valutazioni di sicurezza di terze parti: audit di sicurezza indipendenti condotti da organizzazioni esterne qualificate per convalidare i controlli di sicurezza e identificare potenziali miglioramenti.

Revisioni interne di sicurezza: valutazioni interne regolari delle politiche di sicurezza, delle procedure e dei controlli tecnici per garantire l'efficacia e la conformità continue.

Processo di risposta alle vulnerabilità: procedure strutturate per affrontare i problemi di sicurezza identificati, compresi i requisiti temporali per lo sviluppo e l'implementazione delle patch.

2.7.6 Distinta dei materiali software e gestione delle vulnerabilità

MyQ implementa una sicurezza completa della catena di fornitura attraverso il monitoraggio dettagliato dei componenti e la gestione delle vulnerabilità:

Pubblicazione SBOM: documentazione completa della distinta dei materiali software che identifica tutti i componenti, le librerie e le dipendenze di terze parti utilizzati nei sistemi MyQ X.

Scansione automatizzata delle vulnerabilità: monitoraggio continuo dei database dei componenti per individuare nuove vulnerabilità che interessano le dipendenze di MyQ X.

Gestione rapida delle patch: processo sistematico per la valutazione, il test e la distribuzione degli aggiornamenti di sicurezza per i componenti di terze parti, con priorità basata sulla valutazione dei rischi.

Controllo della versione dei componenti: tracciamento dettagliato di tutti i componenti software, inclusi i numeri di versione, i livelli delle patch di sicurezza e i programmi di aggiornamento, come documentato nelle note di rilascio.

Valutazione della sicurezza dei fornitori: valutazione dei fornitori di software di terze parti per garantire che mantengano standard di sicurezza e processi di divulgazione delle vulnerabilità adeguati.

Questo quadro di conformità completo garantisce che MyQ X soddisfi diversi requisiti normativi, mantenendo i più elevati standard di sicurezza delle informazioni e protezione dei dati in tutti gli ambienti operativi.

2.8 Implementazione dell’architettura Zero Trust

MyQ X implementa l'architettura Zero Trust come approccio di sicurezza fondamentale che elimina la fiducia implicita e convalida continuamente ogni transazione. Questo framework completo garantisce che nessun utente, dispositivo o

connessione di rete sia considerato affidabile per impostazione predefinita, indipendentemente dalla loro posizione o dallo stato di autenticazione precedente.

2.8.1 Principi Zero Trust nella gestione della stampa

L'implementazione Zero Trust di MyQ X si basa sul principio **"non fidarti mai, verifica sempre"** in tutto il sistema di gestione della stampa. Il sistema richiede una verifica esplicita per ogni richiesta di accesso, garantendo che:

Canali di comunicazione crittografati: tutto il traffico di rete utilizza la crittografia TLS obbligatoria con versione minima 1.2, impedendo l'intercettazione e la manomissione durante la trasmissione dei dati. I certificati HTTPS devono essere configurati e convalidati correttamente per prevenire attacchi man-in-the-middle.

Applicazione di protocolli sicuri: MyQ X blocca il traffico HTTP non crittografato e applica protocolli di sicurezza rigorosi su tutti i canali di comunicazione, comprese le connessioni SMTP, LDAP e SNMP. I protocolli legacy come SNMPv1 sono vietati a favore di SNMPv3 con autenticazione forte.

Controlli di sicurezza API: l'accesso all'API REST richiede token di autenticazione con filtraggio degli indirizzi IP, garantendo che le chiamate API siano autenticate e provengano da fonti affidabili. I segreti dei client vengono sottoposti a rotazione periodica per mantenere l'integrità della sicurezza.

2.8.2 Metodologia "Non fidarti mai, verifica sempre"

La metodologia Zero Trust permea ogni aspetto delle operazioni di MyQ X attraverso meccanismi di verifica continua:

Verifica dell'identità: ogni interazione dell'utente richiede l'autenticazione, indipendentemente dalla posizione di rete o dallo stato di affidabilità del dispositivo. Gli utenti devono autenticarsi su ogni dispositivo di stampa, anche se hanno già effettuato l'accesso altrove nell'organizzazione.

Autenticazione dei dispositivi: i dispositivi di stampa stessi devono autenticarsi prima di accedere alle risorse di rete, con credenziali e certificati univoci che impediscono lo spoofing non autorizzato dei dispositivi.

Gestione delle sessioni: le sessioni degli utenti implementano la funzionalità di timeout e logout automatici, garantendo che le sessioni abbandonate non possano essere sfruttate da persone non autorizzate.

2.8.3 Segmentazione e isolamento della rete

MyQ X implementa una segmentazione completa della rete per limitare le superfici di attacco e contenere potenziali violazioni della sicurezza:

Controlli dei confini di rete: il sistema applica rigide regole firewall che bloccano le porte inutilizzate e limitano l'accesso alla rete solo ai canali di comunicazione necessari. Le configurazioni predefinite disabilitano i servizi e i protocolli non necessari.

Segmentazione basata su certificati: MyQ X supporta tre modalità di gestione dei certificati - Autorità di certificazione integrata, Autorità di certificazione aziendale e Gestione manuale dei certificati - consentendo alle organizzazioni di implementare confini di fiducia appropriati in base alle loro politiche di sicurezza.

Applicazione FQDN: tutte le comunicazioni di rete devono utilizzare nomi di dominio completi (FQDN) anziché indirizzi IP o nomi a etichetta singola, impedendo attacchi man-in-the-middle basati su DNS e garantendo una corretta convalida dei certificati.

Gestione delle porte: il sistema gestisce automaticamente le regole del firewall e fornisce un controllo esplicito sulle porte di rete accessibili, riducendo la superficie di attacco attraverso il blocco sistematico delle porte.

2.8.4 Autenticazione e verifica robuste

MyQ X mantiene una convalida continua della sicurezza attraverso più livelli di autenticazione e monitoraggio in tempo reale:

Autenticazione multimodale: il sistema supporta diversi metodi di autenticazione, tra cui LDAP, Microsoft Entra ID, RADIUS e autenticazione MyQ locale, con funzionalità di failover automatico che garantiscono un controllo continuo degli accessi.

Integrazione del server di autenticazione: l'integrazione sicura con server di autenticazione esterni utilizza connessioni crittografate (TLS per LDAP, protocolli sicuri per RADIUS) e applica segreti condivisi forti specifici per ogni implementazione MyQ.

Monitoraggio degli accessi: la registrazione avanzata degli eventi di autenticazione, in particolare dei tentativi di accesso non riusciti, consente agli amministratori di rilevare e rispondere a potenziali minacce alla sicurezza. I tentativi di autenticazione non riusciti attivano meccanismi di blocco automatico: per impostazione predefinita, i dispositivi vengono bloccati per 5 minuti dopo più di 5 tentativi non validi entro 60 secondi.

Controlli di persistenza della sessione: il sistema implementa politiche di timeout della sessione configurabili e funzionalità di logout automatico, garantendo che le sessioni inattive non possano essere sfruttate.

2.8.5 Verifica dei dispositivi e degli endpoint

MyQ X applica rigorosi protocolli di verifica dei dispositivi per garantire che solo gli endpoint autorizzati possano accedere alle risorse di stampa:

Gestione dei certificati dei dispositivi: tutti i dispositivi collegati devono presentare certificati validi per la comunicazione di rete. Il sistema mantiene un archivio completo di certificati con una corretta convalida della catena e supporta la distribuzione automatica dei certificati tramite Group Policy o Mobile Device Management (MDM).

Controlli di sicurezza degli endpoint: i dispositivi di stampa sono sottoposti a una continua convalida della sicurezza, inclusa l'autenticazione SNMP v3 con password complesse e algoritmi crittografici (SHA1 e AES). Le credenziali della stampante sono gestite tramite protocolli di sicurezza specifici del fornitore con password complesse generate in modo casuale.

Autenticazione dei dispositivi mobili: MyQ X Mobile Client implementa OAuth 2.0 Device Authorization Grant per l'autenticazione sicura dei dispositivi mobili, sostituendo i sistemi legacy basati su PIN con una moderna sicurezza biometrica.

Struttura di sicurezza BYOD: il sistema supporta gli ambienti Bring-Your-Own-Device (BYOD) attraverso la propagazione sicura della stampa tramite AirPrint e Mopria, mantenendo i principi zero-trust anche nelle reti senza visibilità diretta del Print Server.

Gestione dei token di accesso: vengono emessi token di accesso univoci per ogni tipo di dispositivo, con Transport Layer Security (TLS) obbligatorio per tutte le comunicazioni. Il sistema implementa controlli di accesso Just-in-Time (JIT) che regolano dinamicamente i privilegi in base al contesto e alla valutazione continua del rischio.

Questa implementazione completa Zero Trust garantisce che MyQ X mantenga i più elevati standard di sicurezza, supportando al contempo diverse esigenze organizzative e scenari di implementazione. L'architettura fornisce una protezione approfondita che si adatta all'evoluzione delle minacce, mantenendo l'efficienza operativa e l'esperienza utente.

2.9 Gestione dell’identità e dell’accesso

MyQ X fornisce un framework completo per la gestione delle identità e degli accessi che si integra perfettamente con i sistemi di autenticazione aziendali esistenti, supportando al contempo i moderni standard di sicurezza. L'architettura IAM garantisce un'autenticazione degli utenti sicura, scalabile e flessibile in diversi ambienti organizzativi.

2.9.1 Implementazione dell'autenticazione a più fattori

MyQ X implementa solide funzionalità **di autenticazione a più fattori (MFA)** che migliorano significativamente la sicurezza richiedendo più fattori di verifica:

Autenticazione tramite Embedded Terminal: i metodi MFA standard includono combinazioni di carta d'identità e PIN, in cui gli utenti presentano prima la loro carta d'identità fisica e poi confermano la loro identità con un codice PIN. In alternativa, l'autenticazione tramite carta d'identità e password fornisce una sicurezza a due fattori simile con la verifica della password al posto del PIN.

Autenticazione basata su dispositivi mobili: MyQ X Mobile Client consente una sofisticata autenticazione MFA tramite la scansione di codici QR combinata con la verifica biometrica. Gli utenti si autenticano scansionando un codice QR visualizzato sul terminale integrato, con una sicurezza aggiuntiva fornita tramite blocchi biometrici (Face ID o impronta digitale) sui loro dispositivi mobili.

Integrazione del Desktop Client: le organizzazioni che utilizzano i servizi Microsoft 365 beneficiano dell'autenticazione MFA integrata tramite Entra ID. Agli utenti con l'autenticazione a due fattori abilitata nei propri account Entra ID viene automaticamente richiesto di verificare la propria identità utilizzando applicazioni di autenticazione quando accedono al Desktop Client.

2.9.2 Concessione dell'autorizzazione del dispositivo OAuth 2.0

MyQ X supporta lo standard **OAuth 2.0 Authorization Code Grant**, consentendo l'integrazione sicura con i moderni provider di identità e le applicazioni di terze parti:

Flusso OAuth standard: il sistema implementa il framework di autorizzazione OAuth 2.0 completo, compresa la presentazione della pagina di accesso, la generazione di codici di accesso monouso e il recupero sicuro dei token. Le applicazioni client ricevono token bearer con tempi di scadenza configurabili e ambiti concessi.

Sicurezza dell'integrazione API: i token OAuth devono essere forniti per tutti gli accessi agli endpoint API, garantendo che le integrazioni di terze parti mantengano un'autenticazione adeguata. Il sistema supporta la convalida dell'ID client e del segreto client con corrispondenza URI di reindirizzamento sicura.

Gestione dei token: i token di accesso includono controlli di scadenza (1800 secondi di default) e restrizioni di ambito, fornendo un controllo granulare sui permessi di accesso alle API e mantenendo la sicurezza attraverso la rotazione dei token.

2.9.3 Funzionalità di integrazione Single Sign-On

MyQ X fornisce un'integrazione **Single Sign-On (SSO)** completa che semplifica l'autenticazione degli utenti in tutti gli ambienti aziendali:

Integrazione con Microsoft 365: la profonda integrazione con Microsoft Entra ID consente un SSO senza soluzione di continuità per le organizzazioni che utilizzano i servizi Microsoft 365. Gli utenti possono autenticarsi utilizzando le loro credenziali Microsoft esistenti, eliminando la necessità di password MyQ separate.

Servizi di directory aziendali: le funzionalità SSO si estendono a vari server di autenticazione, tra cui Active Directory, OpenLDAP e Novell eDirectory, consentendo agli utenti di sfruttare le credenziali aziendali esistenti per l'accesso a MyQ.

Autenticazione multipiattaforma: la funzionalità SSO funziona su tutti i componenti MyQ X, inclusi Desktop Client, Mobile Client e Embedded Terminal, fornendo esperienze di autenticazione coerenti indipendentemente dal metodo di accesso.

2.9.4 Controllo degli accessi basato sui ruoli (RBAC)

MyQ X implementa **un** sofisticato **controllo degli accessi basato sui ruoli** che si allinea ai requisiti di sicurezza aziendali:

Gestione granulare delle autorizzazioni: il sistema fornisce un controllo dettagliato delle autorizzazioni degli utenti, consentendo agli amministratori di definire diritti di accesso specifici in base ai ruoli e alle responsabilità organizzative.

Amministrazione basata sui gruppi: l'implementazione RBAC supporta sia le autorizzazioni dei singoli utenti che il controllo degli accessi basato sui gruppi, consentendo una gestione efficiente di grandi popolazioni di utenti attraverso l'assegnazione di gruppi di sicurezza.

Applicazione del principio del privilegio minimo: i controlli di accesso seguono il principio del privilegio minimo, garantendo che gli utenti ricevano solo le

autorizzazioni minime necessarie per le loro funzioni lavorative, mantenendo al contempo l'efficienza operativa.

2.9.5 Supporto multi-tenant Entra ID

MyQ X fornisce un solido supporto per **gli ambienti multi-tenant Microsoft Entra ID**:

Autenticazione cross-tenant: il sistema è in grado di autenticare gli utenti su più tenant Entra ID, supportando strutture organizzative complesse con più istanze Azure AD.

Isolamento tenant: il supporto multi-tenant include adeguati meccanismi di isolamento che impediscono l'accesso ai dati tra tenant, mantenendo al contempo le funzionalità di gestione centralizzata di MyQ.

Gestione ibrida delle identità: l'integrazione supporta sia scenari di identità solo cloud che ibridi, adattandosi alle organizzazioni con Active Directory on-premise sincronizzato con Entra ID.

2.9.6 Integrazione LDAP e Active Directory

MyQ X offre funzionalità complete **di integrazione LDAP e Active Directory**:

Opzioni di sincronizzazione flessibili: il sistema supporta diversi metodi di sincronizzazione, tra cui la sincronizzazione completa, la sincronizzazione selettiva degli attributi e la sincronizzazione condizionale basata su filtri LDAP. Gli amministratori possono scegliere tra la sostituzione completa, l'aggiunta o gli aggiornamenti condizionali per le proprietà delle schede e dei PIN.

Funzionalità di filtraggio avanzate: la sincronizzazione LDAP include sofisticate opzioni di filtraggio che utilizzano la sintassi standard dei filtri LDAP, consentendo l'importazione selettiva degli utenti in base alle unità organizzative, all'appartenenza a gruppi o ad attributi personalizzati.

Importazione della struttura di gruppo: il sistema può importare strutture organizzative complete, inclusi gruppi di sicurezza, gruppi di distribuzione e gerarchie di gruppi nidificati da Active Directory, mantenendo le relazioni organizzative all'interno di MyQ.

Autenticazione sicura: tutte le comunicazioni LDAP utilizzano la crittografia TLS per proteggere le credenziali e i dati degli utenti durante la sincronizzazione. Il sistema supporta sia il tradizionale LDAP su TLS che le connessioni LDAP sicure.

2.9.7 Gestione dei PIN temporanei e politiche di sicurezza

MyQ X implementa **una gestione** completa **dei PIN e politiche di sicurezza**:

Sicurezza PIN migliorata: la versione 10.2 introduce una maggiore sicurezza dei PIN, tra cui la lunghezza minima obbligatoria di 6 cifre e la prevenzione di combinazioni facilmente intuibili come "1234" o "1111".

Emissione di PIN temporanei: il sistema supporta codici PIN temporanei che possono essere emessi per periodi di tempo specifici o scenari di utilizzo singolo, fornendo ulteriore sicurezza per l'accesso degli ospiti o dei dipendenti temporanei.

Applicazione delle politiche relative ai PIN: le politiche configurabili relative ai PIN consentono alle organizzazioni di definire requisiti di complessità, periodi di scadenza e restrizioni di riutilizzo in linea con gli standard di sicurezza aziendali.

Protezione in caso di autenticazione non riuscita: la sicurezza avanzata include il blocco automatico dei tentativi di autenticazione dopo ripetuti fallimenti (impostazione predefinita: blocco di 5 minuti dopo 5 tentativi non riusciti entro 60 secondi).

2.9.8 Supporto dell'autenticazione biometrica

MyQ X sfrutta **le** moderne **funzionalità di autenticazione biometrica** attraverso l'integrazione dei dispositivi mobili:

Integrazione biometrica mobile: il client mobile MyQ X supporta metodi di autenticazione biometrica, tra cui Face ID sui dispositivi iOS e riconoscimento delle impronte digitali sui dispositivi Android, fornendo un controllo degli accessi sicuro e senza interruzioni.

Autenticazione multimodale: l'autenticazione biometrica funziona in combinazione con la sicurezza basata sul dispositivo, creando un sistema di autenticazione multimodale che combina qualcosa che l'utente possiede (dispositivo mobile) con qualcosa che l'utente è (caratteristiche biometriche).

2.10 Sicurezza dell’infrastruttura

MyQ X fornisce una solida sicurezza dell'infrastruttura che protegge l'intero ambiente di gestione della stampa dalle minacce informatiche in continua evoluzione. La piattaforma incorpora più livelli di difesa per salvaguardare i server, i database, la comunicazione di rete e l'integrità del software, garantendo l'affidabilità operativa e la riservatezza dei dati.

2.10.1 Rafforzamento della sicurezza dei Print Server

I server di stampa MyQ X sono rafforzati utilizzando configurazioni di sicurezza basate sulle migliori pratiche definite nelle impostazioni del file **config.ini**, tra cui:

- Restrizione dei servizi e dei processi per limitare la superficie di attacco.
- Abilitazione di protocolli di comunicazione sicuri e disabilitazione delle opzioni legacy non sicure.
- Assegnazione rigorosa dei privilegi agli utenti, evitando i privilegi di amministratore quando non sono necessari.
- Aggiornamenti automatici regolari e patch di sicurezza per risolvere le vulnerabilità appena scoperte.
- Configurazione delle regole del firewall e delle restrizioni delle porte per bloccare il traffico di rete non autorizzato.

Queste misure riducono il rischio di sfruttamento e mantengono la disponibilità del sistema anche in condizioni di attacco.

2.10.2 Crittografia del database (implementazione Firebird 4.0)

MyQ X utilizza il motore di database **Firebird 4.0**, che fornisce funzionalità di crittografia avanzate per proteggere i dati sensibili inattivi e durante le operazioni di backup. Le principali funzionalità di crittografia includono:

- Crittografia AES-256 dei file del database per impedire l'accesso non autorizzato ai dati.
- Archiviazione crittografata di password e chiavi all'interno del sistema di database.
- Offuscamento dei contenuti sensibili del database nei log e nelle diagnostiche.

Ciò garantisce la conformità alle normative sulla protezione dei dati e impedisce la compromissione della contabilità dei lavori di stampa e delle informazioni degli utenti.

2.10.3 Applicazione TLS 1.2/1.3 e gestione dei certificati

Per proteggere i dati in transito, MyQ X applica di default un protocollo **TLS 1.2** minimo, con aggiornamento opzionale a TLS 1.3 per una maggiore sicurezza e prestazioni migliori. La piattaforma supporta modalità di gestione dei certificati flessibili:

- Generazione automatica di un'autorità di certificazione (CA) privata che firma i certificati del server e del client.

- Integrazione di CA intermedie gestite dall'organizzazione, che consentono catene di fiducia aziendali e controllo centralizzato dei certificati.
- Supporto per l'installazione manuale dei certificati, compresi i certificati CA di terze parti/pubblici.

I certificati e le chiavi private sono archiviati in modo sicuro con protezione crittografata e i clienti ricevono certificati affidabili tramite Criteri di gruppo o Gestione dispositivi mobili.

2.10.4 Sicurezza delle comunicazioni di rete

MyQ X protegge tutti i canali di comunicazione di rete:

- Bloccando tutto il traffico HTTP non crittografato, applicando solo HTTPS.
- Crittografando il traffico SMTP, LDAP e RADIUS utilizzando TLS per proteggere l'autenticazione e il flusso di posta.
- Disabilitazione dei protocolli obsoleti e vulnerabili come POP3 e STARTTLS.
- Utilizzando SNMPv3 con autenticazione forte e algoritmi crittografici per monitorare e gestire in modo sicuro i dispositivi.

Questi controlli impediscono intercettazioni, spoofing e attacchi man-in-the-middle sulla rete.

2.10.5 Configurazione del firewall e gestione delle porte

MyQ X riduce le superfici di attacco tramite:

- Disabilitando le regole del firewall per le porte e i protocolli di rete inutilizzati.
- Consentendo un controllo granulare delle porte esposte in base alle politiche di rete dell'organizzazione.

Ciò limita i punti di ingresso solo a quelli essenziali per i servizi di stampa, migliorando le difese perimetrali.

2.10.6 Sicurezza API e token di autenticazione

Le API applicano più livelli di sicurezza:

- Il framework OAuth 2.0 Authorization Code Grant protegge l'accesso alle API tramite token bearer di breve durata e restrizioni di ambito.
- I token vengono convalidati rispetto agli indirizzi IP dei client e richiedono credenziali client sicure.
- Le rotazioni periodiche dei segreti proteggono dalla fuga delle credenziali.

Ciò protegge gli endpoint API da richieste non autorizzate e abusi.

2.10.7 Isolamento dei processi e sandboxing

Le applicazioni di gestione della stampa MyQ X funzionano con **l'isolamento dei processi** per impedire che i componenti compromessi influenzino l'intero sistema. Laddove possibile, viene utilizzato il sandboxing con macchine virtuali o container per contenere le violazioni della sicurezza e limitare i movimenti laterali all'interno dell'ambiente.

2.10.8 Firma del codice e verifica dell'integrità

Tutti i file binari e gli installer del software MyQ sono **firmati** per garantirne l'autenticità e l'integrità. Ciò assicura che i clienti installino versioni del software verificate, prive di manomissioni o modifiche non autorizzate.

2.11 Protezione e crittografia dei dati

MyQ X implementa una protezione e una crittografia complete dei dati durante l'intero ciclo di vita del documento, garantendo la riservatezza e l'integrità dalla richiesta di stampa iniziale fino all'output finale e all'archiviazione.

2.11.1 Implementazione della crittografia end-to-end

MyQ X fornisce **una crittografia end-to-end** su tutti i canali di comunicazione e i punti di archiviazione dei dati:

Canali di comunicazione crittografati: tutto il traffico di rete utilizza la crittografia TLS obbligatoria con versione minima 1.2 per impostazione predefinita. HTTPS è applicato a tutte le interfacce web, alle comunicazioni da server a server e alle connessioni client.

Sicurezza basata su certificati: diverse modalità di gestione dei certificati supportano i requisiti organizzativi, dall'autorità di certificazione integrata all'integrazione PKI aziendale e ai certificati CA pubblici. Le chiavi private sono protette da password generate in modo casuale e memorizzate in forma crittografata nel database Firebird.

Sicurezza del protocollo: la crittografia TLS è applicata ai protocolli SMTP, LDAP, RADIUS e SNMP, garantendo che nessun dato sensibile venga trasmesso in chiaro.

2.11.2 Crittografia dei dati inattivi

MyQ X protegge i dati archiviati attraverso più livelli di crittografia:

Crittografia del database: il database Firebird 4.0 supporta la crittografia utilizzando certificati personalizzati con "Encrypting File System" Enhanced Key Usage (EKU). I certificati devono essere collocati in archivi di certificati designati, preferibilmente nell'archivio personale.

Protezione del file system: i file dei lavori di stampa e scansione archiviati sul Print Server MyQ X possono essere crittografati utilizzando certificati personalizzati forniti dagli amministratori, aggiungendo un ulteriore livello di protezione oltre alle autorizzazioni del file system.

Crittografia completa del disco: MyQ X supporta l'integrazione con tecnologie di crittografia completa del disco come Microsoft BitLocker per proteggere tutti i dati inattivi sul Print Server, inclusi database, certificati e file temporanei.

2.11.3 Protezione dei dati in transito (crittografia TLS)

MyQ X applica rigorosi **standard di crittografia TLS** per tutte le comunicazioni di rete:

TLS 1.2 minimo: la configurazione predefinita richiede almeno TLS 1.2, con aggiornamento opzionale a TLS 1.3 per una maggiore sicurezza e prestazioni migliori. I protocolli legacy, inclusi SSL e versioni TLS precedenti, sono bloccati.

Gestione delle suite di cifratura: il sistema implementa suite di cifratura avanzate e disabilita gli algoritmi vulnerabili per prevenire attacchi crittografici. Le comunicazioni SNMPv3 utilizzano la crittografia SHA1 e AES.

Convalida dei certificati: tutte le connessioni TLS richiedono una corretta convalida dei certificati utilizzando nomi di dominio completi (FQDN) per prevenire attacchi man-in-the-middle. START TLS viene evitato a causa delle vulnerabilità MITM.

2.11.4 Crittografia dei lavori di stampa e archiviazione sicura

MyQ X fornisce diversi meccanismi per proteggere i lavori di stampa durante il loro ciclo di vita:

Rilascio sicuro della stampa: i lavori di stampa vengono archiviati in modo sicuro sul server MyQ fino a quando gli utenti non effettuano l'autenticazione sul dispositivo, impedendo l'accesso non autorizzato ai documenti presenti nei vassoi di uscita della stampante.

Crittografia dei file di lavoro: gli amministratori possono abilitare la crittografia dei lavori fornendo certificati personalizzati, garantendo che i file dei lavori di stampa rimangano crittografati mentre sono archiviati sul server in attesa di essere rilasciati.

Code private: per i documenti altamente riservati, le code private eliminano automaticamente i lavori di stampa subito dopo il rilascio, eliminando il rischio di un accesso non autorizzato prolungato.

Modalità privacy: quando è abilitata, la modalità privacy nasconde i nomi dei documenti a tutti gli utenti tranne al proprietario del documento, impedendo la divulgazione di informazioni attraverso i nomi dei lavori. Anche gli amministratori non possono visualizzare i nomi dei lavori di altri utenti.

2.11.5 Miglioramenti alla crittografia del database

L'implementazione del database **Firebird 4.0** offre funzionalità di crittografia avanzate:

Crittografia con certificati personalizzati: i file del database vengono crittografati utilizzando certificati con EFS Extended Key Usage, fornendo una protezione efficace contro l'accesso non autorizzato al database.

Protezione con password: le password del database sono oscurate nei file di log, impedendo l'esposizione delle credenziali durante le attività di risoluzione dei problemi e monitoraggio.

Rafforzamento delle autorizzazioni: la cartella dati MyQ, contenente il database degli utenti e le chiavi private dei certificati TLS, è limitata solo agli amministratori, al SISTEMA e all'account di servizio MyQ, rimuovendo l'accesso di lettura predefinito per tutti gli utenti.

2.11.6 Crittografia dei backup e archiviazione sicura

MyQ X garantisce che i backup mantengano lo stesso livello di sicurezza dei dati di produzione:

Backup crittografati: i backup del database sono protetti da password sicure generate in modo casuale che impediscono il ripristino o l'accesso non autorizzato ai file di backup.

Archiviazione sicura dei backup: i file di backup devono essere archiviati in luoghi sicuri con controlli di accesso appropriati e crittografia a riposo per mantenere la riservatezza dei dati durante il ciclo di vita del backup.

2.11.7 Politiche di gestione e rotazione delle chiavi

MyQ X implementa pratiche di gestione sicura delle chiavi:

Rotazione dei certificati: i certificati possono essere ruotati regolarmente in base alle politiche di sicurezza dell'organizzazione, con supporto per la distribuzione automatizzata tramite Criteri di gruppo o Gestione dispositivi mobili.

Protezione delle chiavi private: tutte le chiavi private per i certificati e le operazioni CA sono protette da password generate in modo casuale e archiviate in forma crittografata all'interno del database.

Rotazione dei segreti API: i segreti dei client API REST devono essere sottoposti a rotazione periodica per mantenere la sicurezza. Il sistema supporta il rollover dei segreti senza interruzione del servizio.

2.11.8 Minimizzazione dei dati e privacy by design

MyQ X implementa **principi di privacy by design conformi al GDPR**:

Raccolta limitata dei dati: il sistema raccoglie solo i metadati essenziali necessari per la funzionalità operativa, evitando il trattamento superfluo dei dati personali che potrebbe aumentare i rischi per la privacy.

Cancellazione automatica: gli amministratori possono configurare periodi di cancellazione automatica per i file di stampa e scansione, garantendo che i dati vengano conservati solo per il tempo necessario alle finalità aziendali.

Diritti dei dati degli utenti: implementazione completa dei diritti degli utenti GDPR, inclusi l'accesso ai dati, l'anonimizzazione e il diritto all'oblio, con informative sulla privacy personalizzabili sulle interfacce utente.

Gestione delle sessioni: la funzionalità di logout automatico garantisce che le sessioni degli utenti vengano terminate correttamente, impedendo accessi non autorizzati attraverso sessioni abbandonate.

Questo quadro completo di protezione e crittografia dei dati garantisce che MyQ X mantenga i più elevati standard di riservatezza e integrità dei dati, supportando al contempo i requisiti di conformità normativa in diversi ambienti organizzativi.

2.12 Flussi di lavoro di stampa sicuri

MyQ X fornisce flussi di lavoro di stampa sicuri e completi che mantengono il pieno controllo dell'utente sul rilascio dei documenti, impedendo al contempo che le informazioni sensibili vengano esposte nei vassoi di uscita della stampante. Questi flussi di lavoro sono essenziali per le organizzazioni che richiedono una rigorosa sicurezza dei documenti e la responsabilità degli utenti.

2.12.1 Implementazione del rilascio sicuro della stampa

Hold Print garantisce che i lavori di stampa non vengano mai rilasciati immediatamente alla stampante. I documenti vengono archiviati in modo sicuro sul server MyQ e stampati solo dopo che l'utente autorizzato ha effettuato l'autenticazione sul dispositivo di stampa, impedendo che documenti incustoditi vengano lasciati nei vassoi di uscita.

Pull Print estende ulteriormente questa funzionalità consentendo agli utenti di rilasciare i propri lavori su qualsiasi dispositivo compatibile all'interno del sistema di stampa, non solo sul dispositivo a cui hanno originariamente inviato il lavoro. Questa flessibilità è particolarmente preziosa durante la manutenzione delle apparecchiature o quando gli utenti devono stampare da luoghi diversi.

I metodi di autenticazione multipli supportano il rilascio sicuro della stampa, inclusi codici PIN, tessere identificative, password, codici QR con verifica biometrica e combinazioni di autenticazione a due fattori. Questa flessibilità soddisfa i diversi requisiti di sicurezza delle organizzazioni.

2.12.2 Flussi di lavoro di Pull Printing

Pull Print offre vantaggi significativi sia per gli amministratori che per gli utenti finali:

Vantaggi amministrativi:

- Eliminazione delle pile di documenti incustoditi sulle stampanti dell'ufficio
- Applicazione di comportamenti di stampa responsabili e politiche di sicurezza dei documenti
- Gestione di tutte le stampe tramite un'unica coda di stampa unificata
- Riduzione degli sprechi di stampa e dei costi associati grazie alle opzioni di anteprima e regolazione
- Supporta la stampa flessibile su più dispositivi

Vantaggi per l'utente:

- I documenti riservati rimangono protetti fino al momento dell'esplicita autorizzazione alla stampa
- Stampa su qualsiasi dispositivo autorizzato nell'organizzazione
- Anteprima dei documenti sull'Embedded Terminal prima del rilascio
- Modifica delle opzioni di stampa (colore, fronte/retro, finitura) anche dopo l'invio del lavoro
- Modifica delle destinazioni di stampa sul dispositivo se la stampante originale non è disponibile

2.12.3 Timeout del lavoro di stampa ed eliminazione automatica

MyQ X implementa procedure di pulizia automatica per impedire l'esposizione prolungata dei documenti:

Periodi di conservazione configurabili: gli amministratori definiscono per quanto tempo i file dei lavori di stampa vengono conservati sul server MyQ prima della cancellazione automatica, bilanciando le esigenze operative con quelle di sicurezza.

Gestione del timeout dei lavori di stampa: i lavori di stampa non rilasciati entro i tempi specificati vengono automaticamente rimossi dalla coda di attesa, impedendo l'accumulo di documenti dimenticati o abbandonati sui server.

Logout automatico: le sessioni dei dispositivi scadono automaticamente dopo periodi definiti dall'amministratore, impedendo l'accesso non autorizzato ai documenti sui terminali abbandonati.

2.12.4 Filigrane e firme digitali

La filigrana consente la tracciabilità dei documenti aggiungendo sovrapposizioni personalizzabili alle pagine stampate che possono includere:

- Indicazioni di riservatezza
- Date di stampa e timestamp
- Nome della persona che stampa il documento
- Informazioni di identificazione della stampante

Queste filigrane possono essere applicate a tutte le pagine o solo a quelle selezionate, creando una traccia di controllo che aiuta a identificare i documenti trapelati e a risalire alla loro fonte.

2.12.5 Anteprima di stampa e convalida dei contenuti

Il motore **di anteprima del lavoro** consente agli amministratori di rivedere i lavori di stampa prima del rilascio:

Formati supportati: la funzionalità di anteprima supporta i tre linguaggi di descrizione pagina più comuni: PCL 5, PCL 6 e PostScript.

Controllo preventivo: gli amministratori possono rifiutare i lavori di stampa non autorizzati prima che raggiungano il dispositivo di stampa, prevenendo violazioni delle politiche e proteggendo le informazioni sensibili.

Filtraggio basato sul contenuto: l'integrazione con i sistemi OCR e di gestione dei documenti consente di applicare le politiche di scansione in base all'analisi del contenuto dei documenti.

2.12.6 Gestione degli errori e ripristino sicuro dei lavori di stampa

MyQ X implementa una solida gestione degli errori per mantenere la sicurezza durante i malfunzionamenti del dispositivo:

Protezione dagli errori del dispositivo: quando un dispositivo di stampa entra in uno stato di errore (inceppamento della carta, toner esaurito), i documenti vengono trattenuti anziché stampati automaticamente una volta risolto l'errore, mantenendo il controllo dell'utente sui tempi di rilascio.

Conservazione della sessione: se un dispositivo diventa indisponibile durante una sessione, il sistema MyQ conserva la sessione dell'utente e consente di continuare su dispositivi alternativi senza perdere lo stato del documento.

Logout automatico dal dispositivo: quando si verificano errori del dispositivo, il logout automatico cancella la memoria del dispositivo per impedire l'accesso non autorizzato ai documenti da parte del personale di manutenzione o di altri utenti.

Questa architettura completa e sicura del flusso di lavoro di stampa garantisce alle organizzazioni un controllo rigoroso sulla sicurezza dei documenti durante l'intero ciclo di vita della stampa, supportando al contempo la flessibilità operativa e la produttività degli utenti.

2.13 Sicurezza dei dispositivi e della rete

MyQ X fornisce controlli completi di sicurezza dei dispositivi e della rete per proteggere i dispositivi multifunzione (MFD), le stampanti e l'infrastruttura di rete da accessi non autorizzati e sfruttamento.

2.13.1 Rafforzamento della sicurezza dei dispositivi multifunzione

Le organizzazioni che implementano MyQ X con dispositivi multifunzione dovrebbero adottare le migliori pratiche di sicurezza, tra cui:

Controlli di accesso ai dispositivi: limitare l'accesso fisico alle stampanti solo alle sedi e al personale autorizzati, riducendo l'esposizione a manomissioni o furti.

Disattivazione dei protocolli inutilizzati: disattivare i protocolli e i servizi dei dispositivi non necessari e non richiesti da MyQ X, riducendo la superficie di attacco di ciascun dispositivo.

Gestione delle credenziali predefinite: modificare tutte le password amministratore predefinite sui dispositivi con credenziali complesse generate in modo casuale. Le impostazioni predefinite di fabbrica sono comunemente note agli aggressori.

Protezione del disco rigido interno: se i dispositivi supportano l'archiviazione interna dei lavori di stampa per la ristampa, implementare la crittografia (AES) e le funzioni di sovrascrittura automatica dei dati per impedire l'accesso non autorizzato ai documenti archiviati.

2.13.2 Segmentazione della rete e configurazione VLAN

MyQ X supporta strategie di segmentazione della rete per contenere potenziali compromissioni dei dispositivi:

Isolamento VLAN: separare il traffico di rete delle stampanti e dei dispositivi dalle reti generali degli utenti e amministrative utilizzando LAN virtuali, limitando il movimento laterale se un dispositivo viene compromesso.

Sottoreti e elenchi di controllo degli accessi: implementare controlli di accesso a livello di rete utilizzando elenchi di controllo degli accessi (ACL) per garantire che solo i sistemi autorizzati possano comunicare con i dispositivi di stampa e i server.

Regole firewall: blocca il traffico in entrata e in uscita non necessario dalle sottoreti delle stampanti, limitando la connettività solo ai servizi essenziali e impedendo ai dispositivi infetti di accedere ad altre risorse di rete.

Applicazione FQDN: tutte le comunicazioni di rete devono utilizzare nomi di dominio completi (FQDN) anziché indirizzi IP o nomi host abbreviati, impedendo attacchi man-in-the-middle basati su DNS e garantendo la corretta convalida dei certificati.

2.13.3 Implementazione della sicurezza SNMP v3

MyQ X applica i moderni protocolli **SNMPv3** con crittografia avanzata per la gestione dei dispositivi:

Divieto di SNMPv1 non sicuro: la comunicazione SNMPv1 legacy deve essere completamente disabilitata, poiché trasmette le credenziali in chiaro e non dispone di crittografia.

Configurazione SNMPv3: tutte le comunicazioni SNMP devono utilizzare SNMPv3 con:

- Password complesse generate in modo casuale per l'autenticazione
- Algoritmi di hashing SHA1 o più potenti
- Crittografia AES per la riservatezza dei dati
- Credenziali uniche per dispositivo specifiche per ogni implementazione MyQ

2.13.4 Gestione delle credenziali della stampante

MyQ X riconosce che **la gestione delle credenziali della stampante è specifica del fornitore** e richiede l'implementazione da parte del cliente:

Requisiti di password complesse: tutte le credenziali amministrative della stampante devono utilizzare password complesse generate in modo casuale anziché credenziali predefinite o semplici.

Rotazione delle credenziali: aggiornare periodicamente le password delle stampanti in base alle politiche di sicurezza dell'organizzazione per ridurre il rischio di compromissione delle credenziali.

Restrizioni di accesso: limitare l'accesso alla gestione della stampante al solo personale autorizzato tramite regole firewall, controlli di accesso fisico e autorizzazioni basate sui ruoli.

2.13.5 Sicurezza del firmware e gestione degli aggiornamenti

Mantenere aggiornato il firmware dei dispositivi è fondamentale per la sicurezza:

Aggiornamenti automatici: configurare i dispositivi in modo che ricevano e applichino automaticamente gli aggiornamenti del firmware del produttore che risolvono le vulnerabilità di sicurezza appena scoperte.

Avvisi di sicurezza dei fornitori: monitorare le notifiche di sicurezza del produttore relative a vulnerabilità critiche che interessano i dispositivi distribuiti e applicare tempestivamente le patch.

Test degli aggiornamenti: testare gli aggiornamenti del firmware in ambienti non di produzione prima di distribuirli alle stampanti di produzione per garantirne la compatibilità e la funzionalità.

2.13.6 Gestione e restrizioni delle porte USB

MyQ X supporta i controlli amministrativi per la connettività USB dei dispositivi:

Disabilitazione delle porte USB: gli amministratori devono disabilitare le porte USB in entrata sui dispositivi multifunzione per impedire:

- La stampa diretta tramite USB, aggirando i controlli di sicurezza MyQ
- Accesso diretto ai dischi rigidi dei dispositivi e ai dati memorizzati
- Uso non autorizzato delle funzionalità del dispositivo

Alternative di stampa diretta sicure: abilitare solo metodi di stampa sicuri approvati (IPP/S, AirPrint con integrazione MyQ) bloccando l'accesso USB diretto non sicuro.

Questo quadro completo di sicurezza dei dispositivi e della rete garantisce che i dispositivi di stampa rimangano componenti sicuri dell'infrastruttura MyQ X, mantenendo al contempo l'efficienza operativa e la sicurezza dell'organizzazione.

2.14 Audit e monitoraggio

MyQ X offre funzionalità complete di audit e monitoraggio che consentono agli amministratori di mantenere la visibilità sulle operazioni di stampa, rilevare incidenti di sicurezza e garantire la conformità alle politiche e alle normative aziendali.

2.14.1 Monitoraggio e avvisi in tempo reale

MyQ X monitora tutti i componenti dell'infrastruttura di stampa in tempo reale attraverso diversi canali di monitoraggio:

Monitoraggio dello stato dei dispositivi: monitoraggio continuo dello stato delle stampanti e dei dispositivi multifunzione, inclusi i livelli di toner, la disponibilità di carta, le condizioni di errore e la connettività dei dispositivi. Gli amministratori ricevono informazioni immediate sullo stato di salute e sullo stato operativo dei dispositivi.

Gestione degli avvisi: gli avvisi automatici informano gli amministratori di eventi critici, tra cui errori dei dispositivi, scorte in esaurimento, problemi di connettività e altri problemi operativi. Le notifiche di avviso possono essere inviate tramite e-mail o integrate con il Visualizzatore eventi di Windows.

Notifiche degli eventi: le notifiche personalizzabili basate sugli eventi attivano azioni in risposta a condizioni specifiche del dispositivo o del sistema, consentendo la risoluzione proattiva dei problemi prima che questi abbiano un impatto sulle operazioni.

2.14.2 Registrazione e analisi delle attività di stampa

MyQ X mantiene **registri di controllo dettagliati di tutte le attività di stampa, copia, scansione e fax**:

Contabilità basata sui lavori: la contabilità avanzata tiene traccia di ogni lavoro in modo indipendente, consentendo l'attribuzione dettagliata a utenti, dispositivi, progetti e centri di costo specifici. I lavori eseguiti durante una singola sessione utente vengono contabilizzati separatamente, fornendo dati di utilizzo precisi.

Metadati delle attività: la registrazione completa cattura la data di invio del lavoro, la data di rilascio del lavoro, l'identificazione del dispositivo, il formato della carta, le impostazioni simplex/duplex, le impostazioni del colore e tutti gli altri parametri rilevanti del lavoro.

Registro MyQ: il registro di sistema in tempo reale visualizza tutte le attività del server, inclusi eventi di sistema, errori, avvisi, tentativi di autenticazione, modifiche di configurazione e azioni amministrative. I messaggi di registro sono classificati in base alla gravità (critico, errore, avviso, informazione, notifica, debug, traccia) e filtrabili per periodo di tempo e sottosistema.

2.14.3 Analisi del comportamento degli utenti

MyQ X offre sofisticate funzionalità di analisi per comprendere i modelli di stampa e rilevare anomalie:

Generazione di report personalizzati: le funzionalità avanzate di reporting consentono agli amministratori di creare report personalizzati basati su qualsiasi combinazione di parametri tracciati, consentendo l'analisi del comportamento di stampa per utente, reparto, progetto, dispositivo o periodo di tempo.

Monitoraggio dei centri di costo: l'attribuzione dettagliata dei lavori di stampa ai centri di costo, ai progetti e ai gruppi di utenti consente una rendicontazione trasparente delle spese e supporta decisioni informate in merito alle politiche di stampa.

Monitoraggio del comportamento: gli amministratori possono analizzare i modelli di stampa per identificare attività insolite, utilizzi eccessivi o violazioni delle politiche che richiedono ulteriori indagini.

2.14.4 Rilevamento e risposta agli incidenti

MyQ X supporta il monitoraggio incentrato sulla sicurezza attraverso la registrazione strutturata e gli avvisi:

Registrazione delle autenticazioni non riuscite: la registrazione avanzata dei tentativi di autenticazione, in particolare dei tentativi di accesso non riusciti, consente agli amministratori di rilevare e rispondere a potenziali minacce alla sicurezza. A partire dalla versione 10.2, i registri dei tentativi di accesso sono stati migliorati per facilitare il filtraggio nel registro MyQ.

Regole di notifica dei registri: regole personalizzabili attivano notifiche automatiche basate su tipi di eventi, sottosistemi e modelli di messaggi specifici, consentendo il rilevamento rapido di eventi rilevanti per la sicurezza. Le regole possono utilizzare espressioni regolari per cercare modelli specifici nei messaggi di registro.

Avvisi di eventi critici: il sistema avvisa automaticamente gli amministratori in caso di eventi critici, tra cui violazioni della sicurezza, errori di autenticazione, tentativi di accesso non autorizzati e modifiche alla configurazione.

2.14.5 Politiche di conservazione e archiviazione dei log

MyQ X implementa una gestione flessibile dei log per bilanciare le esigenze operative con i requisiti di conformità:

Periodi di conservazione configurabili: gli amministratori definiscono il numero di giorni prima che i log vengano automaticamente eliminati, allineando la conservazione alle politiche di governance dei dati dell'organizzazione e ai requisiti normativi.

Esportazione e archiviazione dei log: i log possono essere esportati in formato Excel o CSV per l'archiviazione e l'analisi esterna. Le esportazioni pianificate consentono l'archiviazione automatica dei log a intervalli regolari.

Conservazione a lungo termine: i log esportati possono essere archiviati in repository sicuri e crittografati per conservare i registri storici a fini di audit, verifica della conformità e indagine sugli incidenti.

2.14.6 Funzionalità avanzate di filtraggio e ricerca

MyQ X fornisce strumenti sofisticati per l'analisi e l'investigazione dei log:

Ricerche salvate: gli amministratori possono creare, salvare e condividere filtri di ricerca di uso comune per un accesso rapido ai dati di log rilevanti. Le ricerche salvate possono essere organizzate in cartelle per una facile gestione.

Filtraggio per **periodo di tempo**: filtrare i log per intervalli di date specifici o periodi predefiniti per concentrare l'analisi su intervalli di tempo rilevanti.

Filtraggio per sottosistema e contesto: ricerca per specifici sottosistemi MyQ (interfaccia utente web, terminale, server SMTP, ecc.) e contesti (stampa diretta, dispositivi specifici) per isolare gli eventi rilevanti.

Controllo della verbosità: selezionare quali livelli di gravità dei log (critico, errore, avviso, informazioni, ecc.) vengono visualizzati, riducendo il rumore e concentrandosi sugli eventi significativi.

2.14.7 Registro di controllo per le azioni amministrative

MyQ X tiene traccia di tutte le modifiche amministrative attraverso un **registro di controllo** dedicato:

Modifiche alla configurazione: registra tutte le modifiche alle impostazioni MyQ, inclusi chi ha apportato la modifica, quando è stata effettuata e quale componente del sistema è stato interessato.

Gestione dei diritti utente: tracciamento dettagliato delle modifiche alle autorizzazioni utente, alle appartenenze ai gruppi e ai controlli di accesso, con la possibilità di visualizzare informazioni dettagliate su ogni modifica.

Gestione dei PIN e delle credenziali: monitoraggio avanzato delle aggiunte, delle rimozioni e delle modifiche dei PIN per monitorare il ciclo di vita delle credenziali.

Funzionalità di esportazione: i registri di controllo possono essere esportati su richiesta o programmati per l'esportazione automatica regolare, supportando i requisiti di conformità e conservazione dei dati.

Questo quadro completo di audit e monitoraggio garantisce che MyQ X fornisca agli amministratori la visibilità necessaria per mantenere la sicurezza, rilevare le minacce, garantire la conformità alle politiche e risolvere efficacemente i problemi operativi.

2.15 Risposta agli incidenti e recupero

MyQ X offre funzionalità complete di risposta agli incidenti e ripristino progettate per mantenere la continuità operativa durante le interruzioni pianificate e non pianificate. La piattaforma combina procedure di backup automatizzate, funzionalità ad alta disponibilità e meccanismi di failover flessibili per garantire che i servizi di stampa rimangano operativi anche durante le interruzioni del sistema.

2.15.1 Procedure di risposta agli incidenti di sicurezza

MyQ X supporta una risposta strutturata agli incidenti attraverso molteplici meccanismi di monitoraggio e allerta:

Rilevamento degli incidenti in tempo reale: il monitoraggio automatizzato tiene traccia in modo continuo dell'Integrità del sistema, degli errori di autenticazione, delle modifiche di configurazione e degli eventi di sicurezza, consentendo il rilevamento rapido di potenziali incidenti di sicurezza.

Escalation degli avvisi: regole configurabili di Log Notifier attivano notifiche immediate agli amministratori quando si verificano eventi di sicurezza critici, inclusi tentativi di autenticazione non riusciti, tentativi di accesso non autorizzati e anomalie di sistema.

Conservazione della traccia di audit: la registrazione completa di tutte le attività di sistema garantisce la disponibilità di dati forensi completi per l'indagine sugli incidenti. Il registro di audit MyQ tiene traccia di tutte le azioni amministrative, le modifiche di configurazione e le attività degli utenti.

Procedure di contenimento: in caso di incidente di sicurezza, gli amministratori possono isolare rapidamente i componenti interessati, disabilitare gli account compromessi e implementare controlli di accesso di emergenza.

2.15.2 Procedure di ripristino e recupero

MyQ X implementa solide funzionalità di backup e ripristino per garantire un rapido recupero da guasti del sistema o perdita di dati:

Backup automatico del database: i backup automatici regolari del database MyQ acquisiscono tutti i dati di configurazione, le informazioni sugli utenti e le impostazioni di sistema. I backup sono protetti con crittografia a password e archiviati in modo sicuro.

Ripristino completo del sistema: il processo di ripristino recupera l'intero ambiente MyQ, inclusi database, certificati, file di configurazione e report. Gli amministratori devono semplicemente selezionare il file di backup e fornire la password, se protetto.

Backup e ripristino cluster-aware: per le distribuzioni ad alta disponibilità che utilizzano Microsoft Failover Clustering, MyQ supporta il backup su storage cluster condiviso e il ripristino coordinato su tutti i nodi del cluster.

2.15.3 Alta disponibilità e failover

MyQ X offre diverse strategie di failover per mantenere le operazioni di stampa durante i periodi di inattività del server:

Integrazione con Microsoft Failover Clustering: MyQ X viene distribuito in configurazioni attive-passive all'interno dei cluster di failover di Microsoft Windows Server. Il software del cluster monitora continuamente lo stato dei nodi e passa automaticamente ai nodi passivi quando il nodo attivo non è disponibile.

Stampa di fallback: quando il Desktop Client MyQ rileva la perdita di connessione al server, reindirizza automaticamente i lavori di stampa a stampanti di fallback preconfigurate. Una volta ripristinata la connettività del server, la contabilità dei lavori viene aggiornata automaticamente.

Spooling dei dispositivi: i lavori di stampa possono essere memorizzati in modo crittografato nella memoria del dispositivo durante le interruzioni del server. Quando la connettività viene ripristinata, i dispositivi trasmettono automaticamente i dati di contabilità al server.

Accesso offline: i terminali Embedded Terminal MyQ X memorizzano nella cache le credenziali di autenticazione degli utenti, consentendo loro di accedere e utilizzare le funzionalità del dispositivo anche quando il server non è disponibile.

Spooling client: i lavori di stampa vengono elaborati localmente sulle workstation degli utenti e memorizzati sui loro computer anziché sul server, riducendo significativamente i requisiti di larghezza di banda e consentendo la stampa durante la manutenzione del server o in caso di problemi di rete.

2.15.4 Analisi post-incidente e miglioramento

MyQ X supporta il miglioramento continuo delle capacità di risposta agli incidenti attraverso strumenti di analisi completi:

Analisi dei registri storici: gli amministratori possono esaminare i registri esportati per comprendere la sequenza di eventi che hanno portato a un incidente, identificare le cause alla radice e determinare le azioni correttive appropriate.

Revisione dell'audit trail: il registro di audit fornisce una visibilità completa di tutte le azioni amministrative e le modifiche di configurazione che potrebbero aver contribuito o preceduto gli incidenti di sicurezza.

Modelli di ricerca salvati: gli amministratori possono creare e salvare filtri di ricerca all'interno dei registri per modelli di incidenti comuni, consentendo una rapida identificazione di eventi simili in futuro.

3 MyQ X e NIS2

La direttiva (UE) 2022/2555, meglio nota come **NIS2**, rappresenta un passo avanti significativo verso la definizione di un livello comune di sicurezza informatica in tutta l'Unione Europea. Questa direttiva, entrata in vigore il 16 gennaio 2023, mira a rafforzare la **resilienza dei servizi essenziali** e **dei** fornitori di servizi digitali contro le minacce informatiche, introducendo **standard e pratiche di sicurezza informatica** coerenti.

Il settore della stampa, insieme a molti altri, rientra nell'ambito di applicazione della direttiva NIS2. Pertanto, le entità del settore della stampa devono comprendere le implicazioni della direttiva NIS2 e adottare le misure necessarie per soddisfare gli standard di sicurezza. Entro il 17 ottobre 2024, gli Stati membri sono tenuti ad adottare e pubblicare le misure essenziali per conformarsi alla direttiva NIS2.

Questo articolo approfondirà i dettagli della direttiva NIS2 e le sue implicazioni per i distributori e i clienti di MyQ X.

Se sei un cliente finale di MyQ X, discuti i requisiti e le raccomandazioni della direttiva NIS2 con il tuo fornitore/distributore MyQ X. I partner MyQ sono formati per fornire un'assistenza di altissimo livello e ti aiuteranno ad attuare le misure necessarie.

3.1 Principali ambiti della direttiva NIS2

3.1.1 Gestione dei rischi e sicurezza informatica

Adottare un approccio di gestione del rischio alla sicurezza informatica. Ciò include l'identificazione e la valutazione dei rischi per la rete e i sistemi informativi, l'attuazione di misure volte a mitigare tali rischi e la revisione periodica di tali misure.

Assicuratevi che il vostro server e il software associato siano **aggiornati con le ultime patch di sicurezza** per mitigare le vulnerabilità. Inoltre, implementare e testare regolarmente piani di backup e di ripristino in caso di disastri per garantire la disponibilità e l'integrità dei dati. MyQ rilascia regolarmente patch per i propri prodotti. Si raccomanda vivamente di tenersi informati, seguire questi rilasci e definire in anticipo la propria strategia e procedura di aggiornamento. MyQ genera una **Software Bill of Materials (SBOM)** per ogni versione, ottenibile tramite il

proprio fornitore/distributore MyQ, consentendo alle organizzazioni di analizzare i componenti utilizzati nel software alla ricerca di vulnerabilità di sicurezza.

La segmentazione della rete è uno strumento essenziale per l'implementazione pratica di una politica Zero Trust. Offre alle organizzazioni la possibilità di controllare le proprie reti con politiche di sicurezza più granulari. Assicura che, anche se un aggressore compromette una parte della rete, non possa spostarsi facilmente in modo laterale verso altre aree. Tuttavia, le organizzazioni con ambienti segmentati devono affrontare delle sfide nel rendere la stampa prontamente disponibile.

Con MyQ X, le code di stampa possono essere propagate in reti segmentate tramite i Mobile Print Agent, mentre i documenti ospitati nel cloud possono essere scaricati e rilasciati immediatamente dallo schermo del dispositivo con Easy Print. Il supporto per Microsoft Universal Print o Application Proxy nel Mobile Client può aiutare significativamente le organizzazioni ad abilitare i servizi di stampa in tutto il loro ambiente, garantendo al contempo che l'accesso a tali risorse sia protetto.

I certificati SSL per connessioni sicure contribuiscono a soddisfare i requisiti della normativa NIS2 relativi alla trasmissione sicura dei dati attraverso le reti. MyQ X, fin da subito, offre comunicazioni sicure grazie all'Autorità di Certificazione integrata. Le organizzazioni che utilizzano una PKI aziendale possono raggiungere un livello ancora maggiore di sicurezza delle comunicazioni fornendo direttamente certificati personalizzati.

Ove possibile, **applicare il protocollo TLS** per la comunicazione con altri sistemi. Proteggere la connessione ad Active Directory o ad altre directory utenti tramite LDAPS. Assicurarsi che la trasmissione delle e-mail avvenga tramite SMTPS e verificare tutte le impostazioni nella pagina "Rete" di MyQ X e nella scheda "Sicurezza" di Easy Config (ad esempio, che il server Web consenta solo connessioni sicure).

MyQ offre inoltre la possibilità di **crittografare database, scansioni e lavori di stampa**. La crittografia dei dati è fondamentale per garantire la riservatezza e l'integrità delle informazioni sensibili, aspetto chiave della conformità alla normativa NIS2.

Per la comunicazione tra dispositivi, è essenziale implementare protocolli di comunicazione che garantiscano il massimo livello di sicurezza. Si raccomanda vivamente di utilizzare **SNMPv3** anziché v1 o v2(c) per monitorare e gestire lo stato e le funzionalità dei dispositivi in rete.

3.1.2 Continuità operativa e gestione delle crisi

> Le organizzazioni devono garantire che le proprie operazioni possano proseguire in caso di interruzioni significative.

Implementare **server ridondanti o sistemi di failover** per garantire che i servizi di stampa rimangano disponibili durante un incidente. MyQ X consente l'implementazione di misure di failover utilizzando diversi metodi.

MyQ supporta **il clustering di failover di Windows Server** per garantire l'alta disponibilità: se il nodo attivo si guasta, il cluster sposta i servizi MyQ su un nodo di standby. Le implementazioni virtualizzate possono inoltre utilizzare l'HA dell'hypervisor per riavviare la macchina virtuale MyQ su un altro host.

Se si interrompe la connessione al server MyQ, la funzione **"Stampa di riserva" (Fallback Printing)** di MyQ Desktop Client invia i lavori di stampa direttamente a un dispositivo di riserva configurato, in modo che gli utenti possano continuare a stampare durante un'interruzione del server. Sui dispositivi Kyocera e Ricoh supportati, la funzione **"Device Spooling"** combinata con **l'accesso offline (Offline Login)** consente agli utenti di effettuare l'accesso e rilasciare i lavori direttamente sul dispositivo mentre il server non è disponibile. Le funzionalità che dipendono dal server, come i flussi di lavoro di scansione MyQ, il credito e la quota, non sono disponibili finché il server non è nuovamente raggiungibile.

I backup regolari **del database** e la possibilità di ripristinare i dati MyQ sono conformi ai requisiti NIS2 volti a garantire la disponibilità e la resilienza dei dati in caso di attacchi informatici o guasti del sistema. I backup del database e dei log possono essere pianificati con MyQ X ed eseguiti automaticamente, compresi i backup del database SQL del Central Server.

Per ulteriori informazioni, consultare:

- Resilienza, fallback e alta disponibilità
- Strategia di spooling

3.1.3 Modello di accesso con privilegi minimi

> Gli utenti devono essere concessi solo il livello minimo di accesso o le autorizzazioni necessarie per eseguire le operazioni richieste.

NIS2 incoraggia **la separazione dei compiti** per impedire l'accesso non autorizzato ai sistemi critici.

Assegnando **diritti specifici per l'accesso** alla gestione del sistema e degli utenti, alla gestione dei lavori, alla reportistica o ai log, è possibile concedere a determinati utenti un accesso con privilegi elevati a particolari aree dell'ambiente MyQ, limitando al contempo i diritti di accesso degli altri. Analogamente, i diritti possono essere assegnati per ogni Server del sito; in questo modo, gli amministratori di un Server del sito locale non otterranno un accesso con privilegi elevati in altre sedi e filiali dell'organizzazione dove ciò non è desiderato.

Quando l'amministratore utilizza **la gestione** degli utenti **basata su gruppi** (gruppi di sicurezza), può ridurre il numero di passaggi necessari per configurare i diritti di accesso, continuando a beneficiare delle funzionalità di provisioning e deprovisioning degli utenti. Maggiori informazioni sono disponibili di seguito nella sezione *"Provisioning e deprovisioning degli utenti*".

Le autorizzazioni di accesso granulari devono essere applicate all'intera infrastruttura organizzativa, compresi tutti i componenti dell'ecosistema MyQ X. L'accesso deve essere limitato esclusivamente agli amministratori e al personale autorizzato, garantendo che solo chi dispone dei privilegi appropriati possa gestire e interagire con questi sistemi. Ciò riguarda i dispositivi fisici, i server fisici e il loro sistema operativo (Windows Server), i server SQL, lo storage e altro ancora.

Per saperne di più:

- Implementazione: diritti degli utenti

3.1.4 Risposta agli incidenti e auditing

> Per gestire gli incidenti, è necessario stabilire e mettere in pratica regolarmente delle procedure. In caso di attività sospette, limitare o interrompere l'accesso dell'utente per prevenire ulteriori danni. Una corretta implementazione di queste misure può mitigare l'impatto di eventi imprevisti.

Le funzionalità di registrazione e controllo di MyQ (MyQ Logs e MyQ Audit Log) possono rivelarsi estremamente utili per la risposta agli incidenti e il loro monitoraggio. Questi registri aiutano a individuare, indagare e rispondere alle attività sospette, aspetto obbligatorio previsto dalla normativa NIS2.

I registri devono essere monitorati regolarmente e le notifiche devono essere abilitate per gli incidenti che l'organizzazione ritiene critici. A tal fine, l'utilità **Log Notifier** integrata in MyQ X può essere configurata per monitorare gli eventi nell'ambiente MyQ e il personale responsabile può essere avvisato per intervenire

immediatamente. Anche le attività pianificate in esecuzione (come la sincronizzazione utente, il rilevamento delle stampanti e altro) possono inviare avvisi a contatti prestabiliti. Gli amministratori possono inoltre configurare MyQ X per l'invio di avvisi automatici in caso di fallimento dei lavori di stampa o di errori critici.

La gestione dei log può essere centralizzata esportando ed elaborando i log tramite il Registro eventi di Windows e, se necessario, può essere ulteriormente elaborata dai sistemi SIEM. Assicurarsi che i periodi di conservazione della cronologia, dei log e dei log di audit siano sufficienti per le proprie esigenze. Questa configurazione va effettuata in **Impostazioni** – **Gestione del sistema**.

Stabilire **SLA solidi** è essenziale per i servizi gestiti come MyQ, specialmente in conformità con le normative NIS2. Per garantire tempi di risposta rapidi agli incidenti, le organizzazioni dovrebbero prendere in considerazione la possibilità di optare per le offerte di Supporto Premium.

Per saperne di più:

- Impostazioni dei log

3.1.5 Autenticazione sicura

> L'autenticazione sicura garantisce che solo gli utenti autorizzati possano accedere ai sistemi. L'autenticazione a due fattori (2FA) rafforza questa protezione richiedendo due tipi di credenziali, aumentando significativamente la sicurezza.

I requisiti relativi a password e PIN, **l'autenticazione a due fattori** sugli Embedded Terminals o l'uso della funzione "Accedi con Microsoft" sulle interfacce web o sugli Embedded Terminals (con il MyQ X Mobile Client) offrono alternative per proteggere l'accesso all'ambiente MyQ X.

Il client mobile MyQ X può essere configurato per richiedere **la verifica biometrica**, migliorando ulteriormente la sicurezza dell'account utente MyQ X richiedendo un fattore aggiuntivo durante l'autenticazione ai dispositivi.

L'implementazione di meccanismi di blocco dell'account utente dopo diversi tentativi di accesso falliti migliora la sicurezza e riduce il rischio di attacchi di forza bruta.

Per saperne di più:

- Implementazione: Autenticazione sicura[5]

5. https://docs.myq-solution.com/deployment/v1/secure-authentication

- Implementazione: utilizzo dell'autenticazione a due fattori[6]

3.1.6 Provisioning e deprovisioning degli utenti

> La creazione e la rimozione degli account garantiscono che agli utenti venga immediatamente negato l'accesso all'ambiente MyQ una volta rimossi dalla directory utenti di origine.

MyQ supporta **la sincronizzazione automatica e programmata degli utenti** con sistemi esterni quali LDAP, Microsoft Entra ID (precedentemente Azure AD), Google Workspace e file CSV. Ciò garantisce che gli utenti appena aggiunti vengano importati automaticamente nell'ambiente MyQ X senza necessità di inserimento manuale. Sincronizzando regolarmente i dati degli utenti, MyQ X contribuisce a mantenere un elenco aggiornato di utenti con diritti di accesso corretti, riducendo il rischio di accessi non autorizzati.

La gestione basata sui gruppi e l'uso di gruppi di sicurezza nella directory utenti di origine possono facilitare l'**assegnazione e la revoca** automatica **dell'accesso** a parti dell'ambiente MyQ X per gli utenti appena creati o rimossi.

MyQ X offre una funzione **di registrazione automatica**, che consente agli utenti di registrarsi autonomamente inviando lavori di stampa, strisciando una scheda di identificazione o creando un account tramite l'interfaccia web. Questa funzione è particolarmente utile per ambienti con frequenti utenti esterni, come i collaboratori ospiti. Agli utenti del sistema può essere fornito un **PIN temporaneo** che scade dopo il periodo impostato, garantendo che l'accesso venga automaticamente revocato una volta che l'utente non ne ha più bisogno.

MyQ supporta l'anonimizzazione dei dati degli utenti per garantire la conformità alle normative sulla privacy. Questo processo rimuove in modo irreversibile tutti gli identificatori personali, rendendo gli account utente inutilizzabili e non rintracciabili, pur consentendo la generazione di report e l'audit del sistema senza compromettere la privacy.

Per saperne di più:

- Implementazione: gestione degli utenti basata su gruppi

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

3.1.7 Sensibilizzazione e formazione

La direttiva NIS2 sottolinea la necessità di sensibilizzare e formare il personale sulle pratiche di sicurezza informatica.

Si raccomanda di organizzare sessioni di formazione per il personale IT e gli amministratori sulla gestione sicura dell'ambiente MyQ X, con particolare attenzione alla conformità alla normativa NIS2. La scelta migliore è quella di consultare il proprio fornitore/distributore in merito alla gestione dell'ecosistema MyQ X. I partner MyQ sono formati per fornire un'assistenza di altissima qualità.

Inoltre, è opportuno sviluppare programmi di sensibilizzazione per aiutare gli utenti finali a identificare le minacce e istruirli sull'uso dell'ecosistema MyQ X, nonché sulle misure da adottare in caso di incidenti di sicurezza o di altro tipo.

White paper sulla sicurezza e implementazione sicura

Per ulteriori informazioni su come raggiungere i migliori standard di sicurezza con MyQ X, consultare il resto di questa guida dedicata alla sicurezza di MyQ X (see page 4).

Aggiornato il 6/10/2026

4 Distinta base del software

Pagine OEM collegate
This ScriptRunner macro could not be rendered for export.

Una distinta base del software (SBOM) è un registro dettagliato di tutti i componenti, le dipendenze e le librerie inclusi in un'applicazione software, sia essa open source o proprietaria. Fornisce informazioni chiave quali nomi dei componenti, versioni, licenze e posizioni delle fonti, offrendo piena visibilità sulla catena di fornitura del software.

Le SBOM vengono utilizzate per monitorare e gestire i rischi legati al software, consentendo alle organizzazioni di identificare rapidamente i componenti vulnerabili o obsoleti, garantendo la conformità alle licenze e migliorando la sicurezza complessiva. La gestione di una SBOM è particolarmente importante negli ecosistemi software complessi, poiché contribuisce a semplificare la gestione delle vulnerabilità e garantisce la trasparenza durante tutto il ciclo di vita dello sviluppo del software.

Generando, analizzando e mantenendo costantemente gli SBOM, le organizzazioni possono gestire meglio i rischi legati al software e garantire la conformità agli standard di sicurezza e normativi.

I formati BOM (Bill of Materials) si riferiscono a strutture standardizzate che rappresentano e condividono i componenti di un sistema software. Nel contesto delle Software Bill of Materials (SBOM), questi formati forniscono un modo leggibile da macchina per descrivere i componenti software, le loro relazioni e i metadati. I formati SBOM più utilizzati includono:

- **CycloneDX**: un formato BOM leggero ed estensibile progettato specificamente per la sicurezza delle applicazioni. Fornisce informazioni dettagliate su componenti, licenze, vulnerabilità e dipendenze. CycloneDX è apprezzato per la sua flessibilità e il supporto all'automazione nei flussi di lavoro di sicurezza e gestione dei rischi.

MyQ fornisce SBOM per i seguenti prodotti:

- MyQ X Central Server 10.2
- MyQ X Print Server 10.2
- MyQ Desktop Client (MDC) 10.2
- Mobile Print Agent (MPA) 1.3
- Riconoscimento ottico dei caratteri (OCR) 3.1

Per ricevere gli SBOM da MyQ, contattare il (see page 74) nostro supporto tecnico.

5 Contatti commerciali

Produttore MyQ®	**MyQ® spol. s r.o.** Harfa Business Center, Ceskomoravska 2532/19b, 190 00 Praga 9, Repubblica Ceca Numero identificativo 615 06 133 MyQ® spol. s r.o. è iscritta nel Registro delle Imprese presso il Tribunale Municipale di Praga, numero di registrazione C 29842 (di seguito denominata "MyQ®")
Informazioni commerciali	http://www.myq-solution.com info@myq-solution.com[7]
Assistenza tecnica	support@myq-solution.com[8]
Avviso	IL PRODUTTORE NON SARÀ RESPONSABILE DI EVENTUALI PERDITE O DANNI CAUSATI DALL'INSTALLAZIONE O DAL FUNZIONAMENTO DEL SOFTWARE E DELLE PARTI HARDWARE DELLA SOLUZIONE DI STAMPA MyQ®. Il presente manuale, il suo contenuto, il suo design e la sua struttura sono protetti da copyright. La copia o altra riproduzione totale o parziale della presente guida, o di qualsiasi oggetto protetto da copyright, senza il previo consenso scritto di MyQ® è vietata e può essere punibile. MyQ® non è responsabile del contenuto del presente manuale, in particolare per quanto riguarda la sua integrità, attualità e occupazione commerciale. Tutto il materiale qui pubblicato ha esclusivamente carattere informativo. Il presente manuale è soggetto a modifiche senza preavviso. MyQ® non è tenuta ad apportare tali modifiche periodicamente né ad annunciarle, e non è responsabile della compatibilità delle informazioni attualmente pubblicate con l'ultima versione della soluzione di stampa MyQ®.

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

Marchi commerciali	"MyQ®", compresi i relativi loghi, è un marchio registrato di MyQ®. È vietato qualsiasi utilizzo dei marchi commerciali di MyQ®, compresi i relativi loghi, senza il previo consenso scritto di MyQ® Company. Il marchio commerciale e il nome del prodotto sono protetti da MyQ® e/o dalle sue affiliate locali.

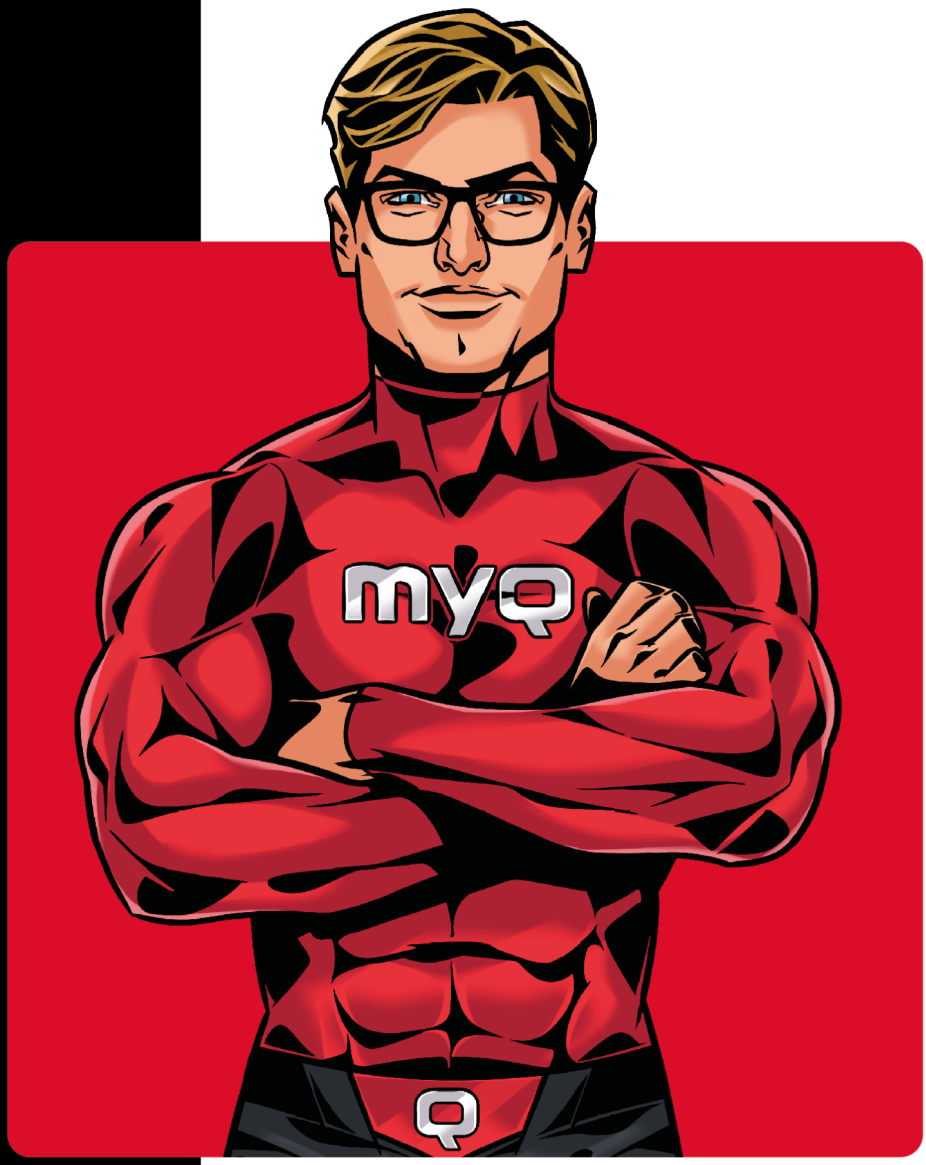
myQ X

RISPARMIA TEMPO CON SOLUZIONI DI STAMPA PERSONALIZZATE

MyQ X è una pluripremiata soluzione di gestione della stampa locale o su cloud privato, scelta da milioni di utenti.

info@myq-solution.com

myq-solution.com



50+ milioni
Utenti che si affidano a MyQ

1+ milione
Dispositivi attivi

26+
Marchi supportati

1000+
Partner certificati

Presente in **140+** paesi

Premi e certificazioni

BuyersLab PLATINUM TESTED SOLUTION 2023

BuyersLab PLATINUM TESTED SOLUTION 2022

BuyersLab PLATINUM TESTED SOLUTION 2021

ISO 9001 TÜV SÜD ISO 14001 ISO/IEC 27001