

Sécurité MyQ X 10.x

Généré à partir de docs.myq-solution.com
octobre/2026
Copyright © 2026 MyQ spol. s r.o. Tous droits réservés.

FRANÇAIS

Avis sur la traduction

Cette traduction a été réalisée avec l'aide de l'intelligence artificielle. En cas de divergence ou d'ambiguïté, le document source en anglais fait foi.

Table des matières

1 Déploiement sécurisé de MyQ X 5
1.1 MyQ X Central Server 5
1.2 Serveur d'impression MyQ X 16
1.3 MyQ X Desktop Client 29
2 Livre blanc sur la sécurité de MyQ X 33
2.1 Architecture Zero Trust 33
2.2 Cadre de protection en trois phases 34
2.3 Confidentialité dès la conception 34
2.4 Évolution continue de la sécurité 34
2.5 Principales améliorations de la sécurité dans la version 10.2 35
2.6 Valeur commerciale de la gestion sécurisée des impressions 37
2.7 Conformité 39
2.8 Mise en œuvre de l'architecture de confiance zéro 43
2.9 Gestion des identités et des accès 47
2.10 Sécurité des infrastructures 51
2.11 Protection des données et cryptage 54
2.12 Flux d'impression sécurisés 58
2.13 Sécurité des périphériques et des réseaux 61
2.14 Audit et suivi 63
2.15 Réponse aux incidents et récupération 67
3 MyQ X et NIS2 70
3.1 Principaux domaines de la directive NIS2 70
4 Nomenclature des logiciels 78
5 Contacts professionnels 79

La sécurité a toujours été une **priorité absolue pour MyQ**. Dans cette section, vous trouverez un guide pour le déploiement sécurisé de MyQ X, ainsi que le livre blanc sur la sécurité de MyQ X :

- Déploiement sécurisé (see page 5)
- Livre blanc sur la sécurité (see page 33)

1 Déploiement sécurisé de MyQ X

La confidentialité des données clients et **la sécurité** des clients ont toujours été **la priorité numéro un de MyQ**. Cependant, **la sécurité est une responsabilité partagée entre les fournisseurs et les clients.** Bien que l'objectif de MyQ X soit de fournir une configuration sécurisée par défaut, plusieurs domaines nécessitent des mesures supplémentaires de la part du client. Il s'agit notamment, mais sans s'y limiter, de la gestion des certificats, de l'utilisation d'identifiants forts, de la délégation des autorisations et de la configuration du pare-feu.

Ce document contient des listes de contrôle pratiques pour un déploiement sécurisé de MyQ X Central Server et MyQ X Print Server dans les environnements d'entreprise. Nous sommes convaincus que le respect de ces directives réduira considérablement la surface d'attaque de toute infrastructure de gestion d'impression. Il va sans dire que les applications serveur MyQ X ne sont aussi sécurisées que les systèmes d'exploitation et les environnements réseau sous-jacents. La sécurité Windows étant un sujet à part entière, elle n'est pas traitée dans ce document.

Les systèmes MyQ X sont constamment améliorés et corrigés, conformément à la politique MyQ Secure Development Lifecycle. Veuillez vous assurer de **toujours utiliser la dernière version prise en charge**. Les notes de mise à jour sont disponibles dans chaque guide produit. Veuillez également vous reporter à la politique de fin de vie (EOL)[1] pour les annonces de fin de maintenance et les composants de remplacement.

> Ce guide a été préparé en collaboration avec Mainstream Technologies, désormais Seyfor[2], lors d'audits de sécurité indépendants réguliers.

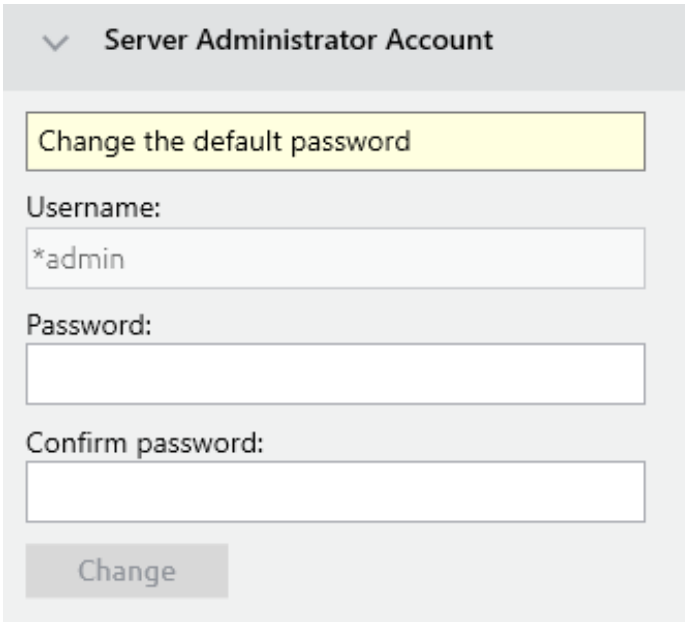
1.1 MyQ X Central Server

1.1.1 Mots de passe par défaut

Modifier le mot de passe administrateur du serveur

L'une des premières étapes consiste à modifier le mot de passe administratif par défaut, qui est *1234* :

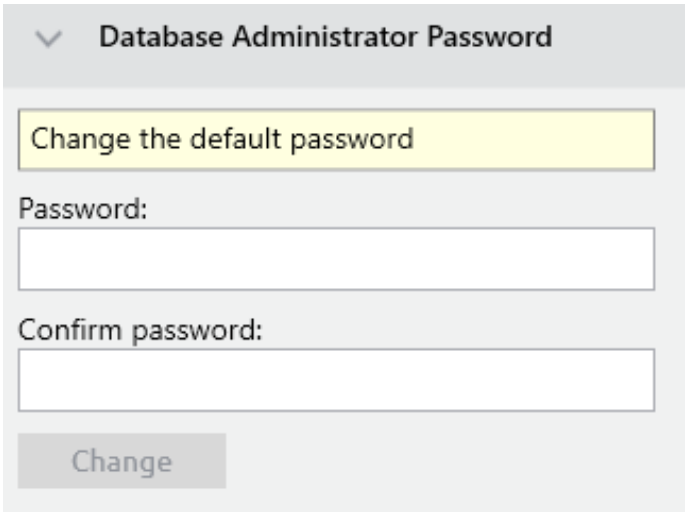
1. https://www.myq-solution.com/en/product-support-end-of-life-policy
2. http://www.seyfor.cz



Le mot de passe est stocké dans la base de données sous forme hachée.

Modifier le mot de passe administrateur de la base de données

Si la base de données interne Firebird est utilisée, modifiez le mot de passe par défaut utilisé par MyQ Central Server pour s'authentifier :



Ce mot de passe est stocké dans le fichier « C:\ProgramData\MyQ Central Server\setup.ini » sous forme cryptée et est défini par défaut sur *« masterkey »*.

1.1.2 Sécurité des connexions

Configurer le certificat HTTPS

Un certificat personnalisé qui est approuvé par tous les ordinateurs clients et qui contient le nom DNS du serveur doit être configuré pour MyQ Central Server :

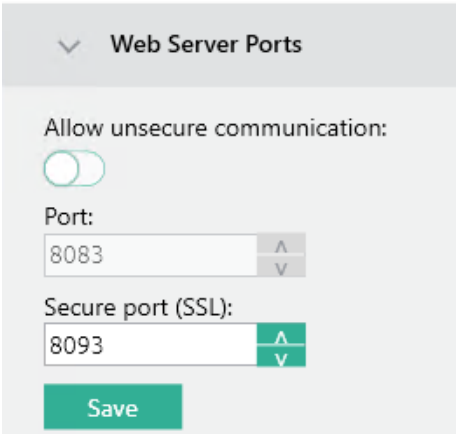
Le certificat est physiquement stocké dans le répertoire « C:\ProgramData\MyQ Central Server\Cert » dans les fichiers suivants :

- server.pfx – certificat avec clés publique et privée
- server.cer – certificat avec la clé publique
- server.key – clé privée

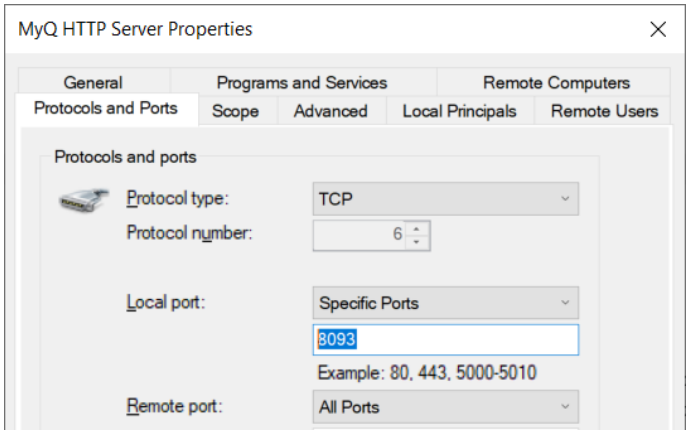
L'utilisation de certificats génériques est déconseillée, car ils présentent un risque de sécurité beaucoup plus élevé en cas de vol.

Bloquer le trafic HTTP non crypté

Le trafic HTTP non crypté ne doit pas être activé dans la configuration du Central Server MyQ :

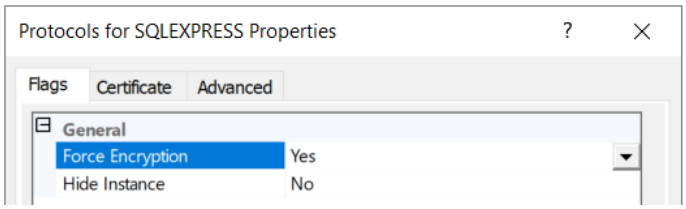


Le pare-feu basé sur l'hôte doit également être configuré pour n'autoriser que le trafic HTTPS :

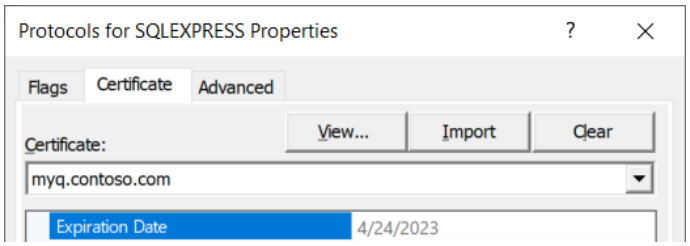


Chiffrer les connexions à la base de données

Si Microsoft SQL Server est utilisé pour stocker la base de données MyQ, assurez-vous que le cryptage TLS est appliqué via le Gestionnaire de configuration SQL Server :

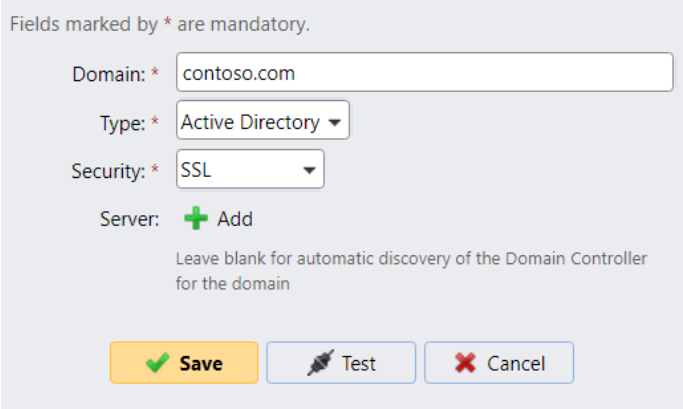


Un certificat émis par une autorité de certification de confiance doit également être configuré sur SQL Server :



Appliquer le trafic LDAP crypté

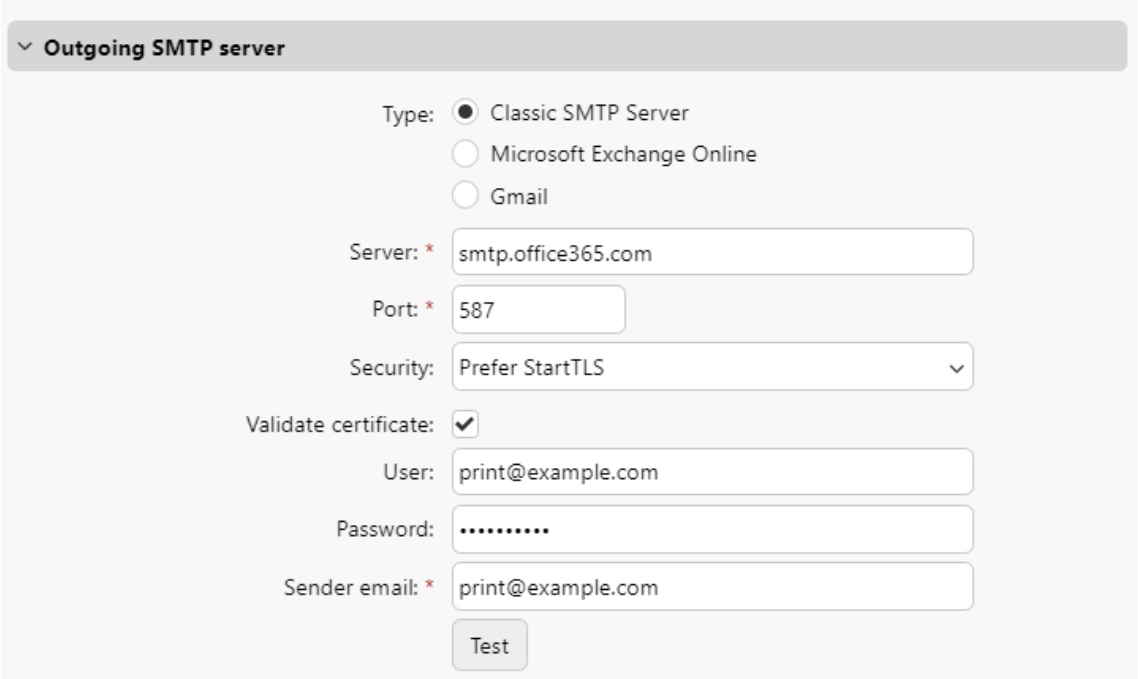
Si la synchronisation des comptes utilisateurs via le protocole LDAP est utilisée, définissez la sécurité de la connexion sur SSL :



Pour des raisons de sécurité, n'utilisez pas START TLS, car il est vulnérable aux attaques MITM. Un certificat émis par une autorité de certification de confiance doit être configuré sur tous les serveurs LDAP (contrôleurs de domaine Active Directory).

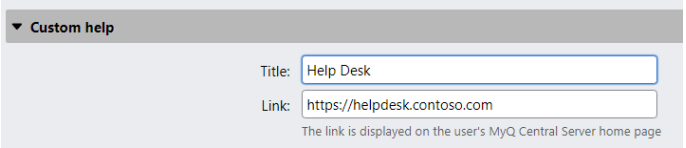
Sécuriser le trafic SMTP

Si un serveur SMTP est configuré dans MyQ Central Server, appliquez l'utilisation de TLS avec validation du certificat :



Toujours utiliser le nom de domaine complet

Pour éviter les attaques MITM, utilisez strictement des noms de domaine complets dans toutes les fenêtres de configuration :



Ne contactez jamais les serveurs en saisissant uniquement des adresses IP ou des noms à étiquette unique.

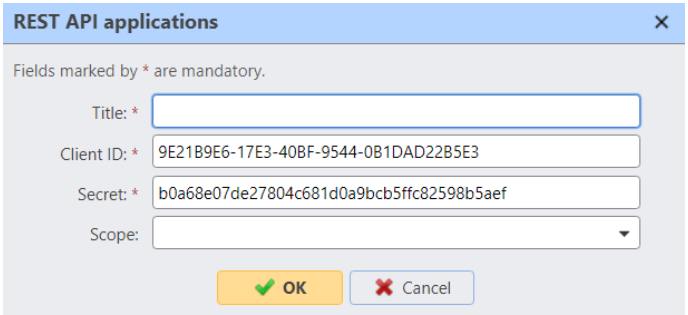
Sécurisation du trafic RADIUS

Si l'authentification RADIUS est utilisée, générez toujours des secrets partagés forts spécifiques au Central Server MyQ :



Protégez les clés API REST

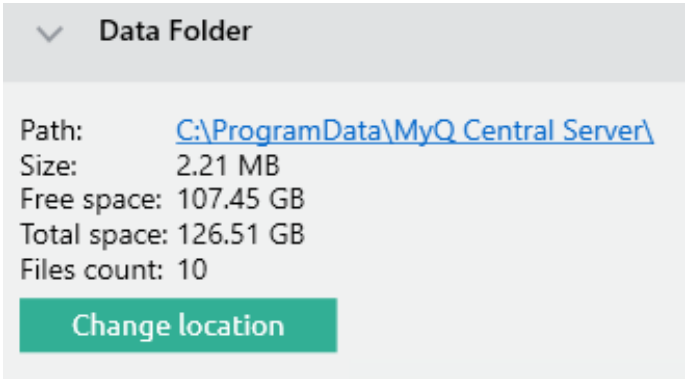
Lorsque des API REST sont utilisées, protégez les secrets clients contre toute exposition inutile et effectuez régulièrement un renouvellement des secrets :



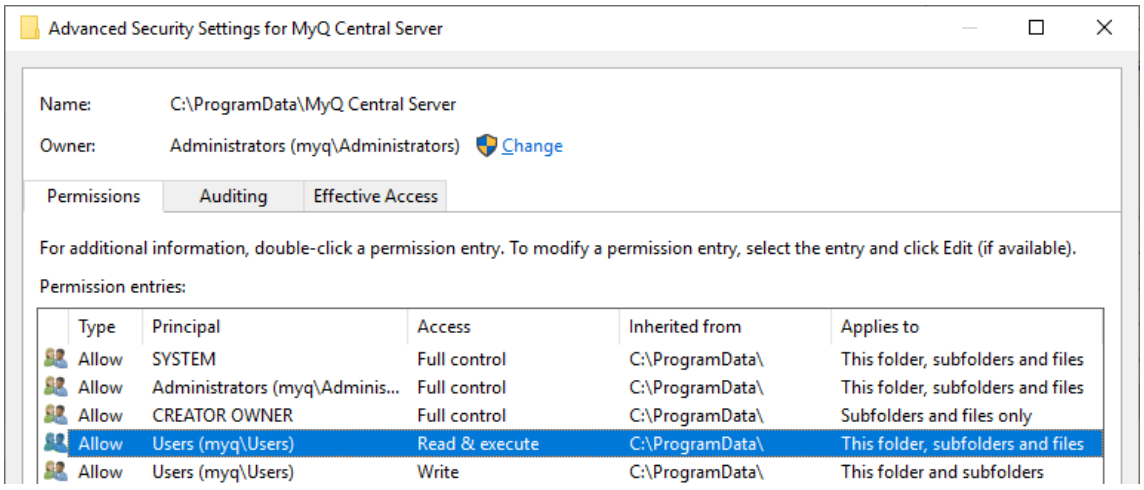
1.1.3 Sécurité des données

Restriction des droits d'accès au dossier de données

Le dossier de données de MyQ Central Server contient des données hautement sensibles, notamment la base de données des utilisateurs et la clé privée du certificat TLS. Son emplacement actuel est affiché dans l'application MyQ Central Server Easy Config :



Tous les utilisateurs (locaux/du domaine) disposent par défaut d'un accès en lecture :



Seuls les administrateurs, le compte SYSTEM et le compte de service MyQ doivent avoir accès à ce répertoire. Voici un exemple de script batch pouvant être utilisé pour renforcer les autorisations :

```
@ECHO OFF

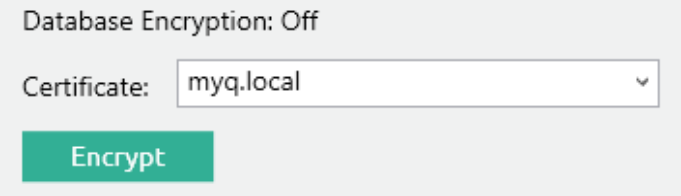
REM Add the virtual account SIDs to all MyQ Central Server services:
```

```
sc sidtype myqm_platform unrestricted
sc sidtype myqm_apache unrestricted
sc sidtype FirebirdServerMasterInstance unrestricted

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

Activer le chiffrement de la base de données

Lorsque vous utilisez la base de données intégrée, veillez à toujours la chiffrer à l'aide d'un certificat personnalisé afin de réduire le risque de fuites de données :



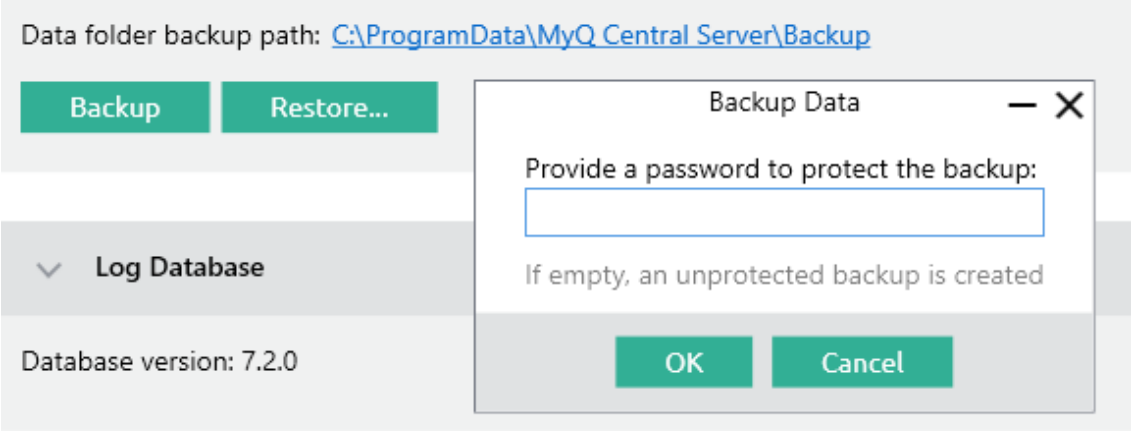
Le certificat doit disposer de l'utilisation de clé étendue (EKU) « Encrypting File System » et doit se trouver dans l'un des magasins de certificats suivants de l'ordinateur :

- Personnel
- Éditeurs de confiance
- Autorités de certification racines tierces
- Autres personnes

Le magasin « Personnel » est celui qui est recommandé.

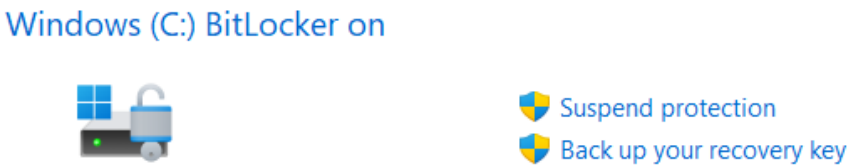
Chiffrer les sauvegardes

Les sauvegardes de bases de données doivent être protégées par des mots de passe sécurisés, générés de manière aléatoire :



Activer le chiffrement du disque

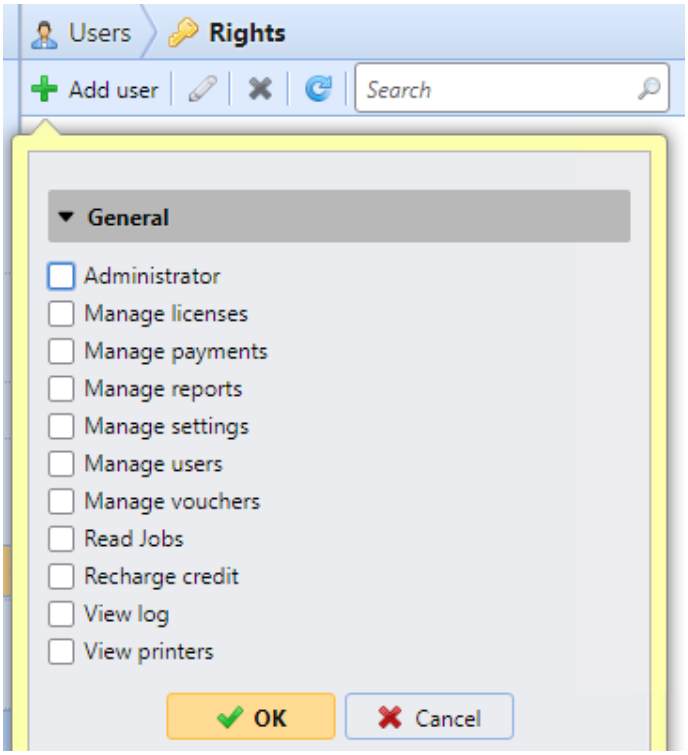
Si possible, une technologie de chiffrement complet du disque, telle que Microsoft BitLocker, doit être activée sur le Central Server MyQ afin de protéger les données au repos :



1.1.4 Recommandations supplémentaires

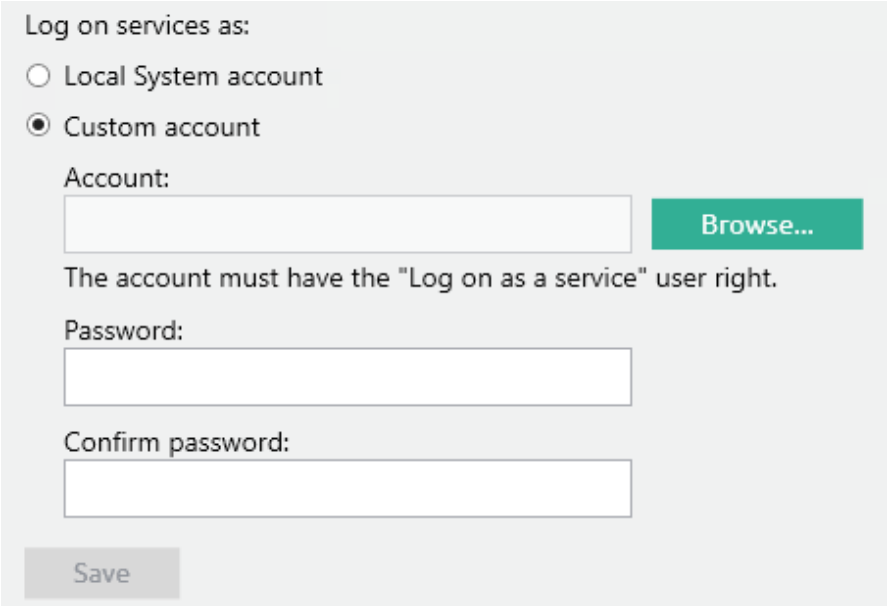
Déployer RBAC

N'utilisez pas le compte *admin par défaut pour les opérations courantes. Utilisez plutôt la délégation de privilèges, tout en appliquant le principe du moindre privilège :



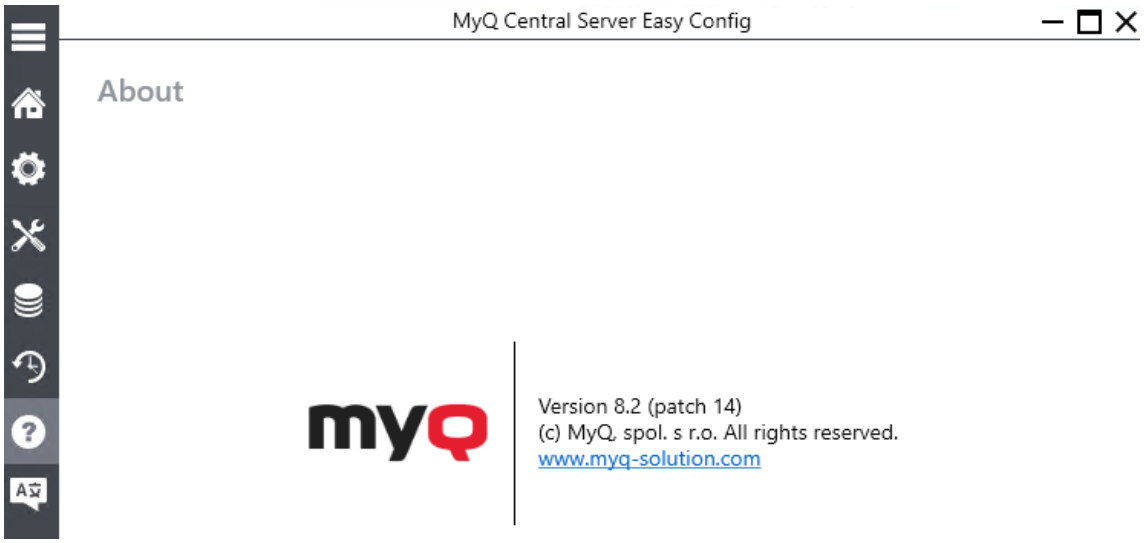
Configurer un compte de service personnalisé

MyQ Central Server s'exécute par défaut sous le compte SYSTEM hautement privilégié. Configurez plutôt un compte de service personnalisé avec un mot de passe fort :



Maintenir le serveur à jour

Installez les mises à jour de sécurité fournies par MyQ dès qu'elles sont disponibles. Vous pouvez vérifier la version actuellement installée de l'application dans MyQ Central Server Easy Config :



Assurez la sécurité du système d'exploitation

MyQ Central Server n'est aussi sécurisé que le système d'exploitation sous-jacent. Maintenez-le à jour et appliquez les politiques de sécurité recommandées par Microsoft.

Mettez régulièrement à jour vos logiciels afin de corriger les failles de sécurité et d'améliorer les performances. Consultez la configuration système requise pour connaître la liste des exigences et des recommandations.

Par exemple, .NET doit être mis à jour à l'aide d'outils de gestion ou via Windows Updates sur une base facultative[3].

Prévoyez une reprise après sinistre

Créez régulièrement des sauvegardes de MyQ Central Server, y compris la base de données, les certificats et les fichiers de configuration. Testez la procédure de reprise au moins une fois.

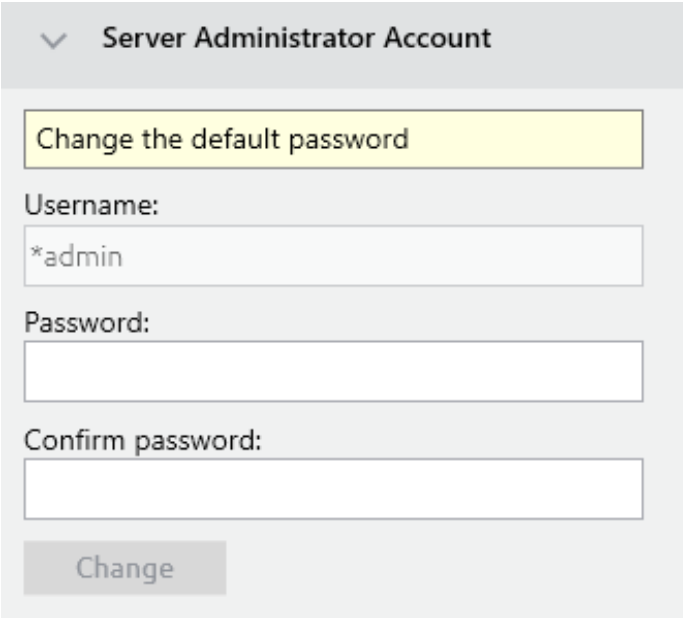
3. https://devblogs.microsoft.com/dotnet/server-operating-systems-auto-updates/

1.2 Serveur d’impression MyQ X

1.2.1 PS Mots de passe par défaut

Modifier le mot de passe administrateur du serveur

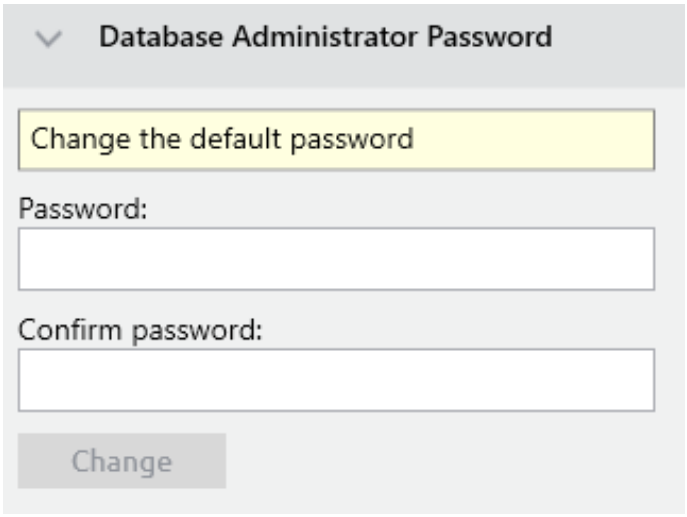
L'une des premières étapes consiste à modifier le mot de passe administratif par défaut, qui est *1234* :



Le mot de passe est stocké dans la base de données sous forme hachée.

Modifier le mot de passe administrateur de la base de données

Modifiez le mot de passe par défaut utilisé par MyQ Print Server pour s'authentifier auprès de la base de données Firebird interne :

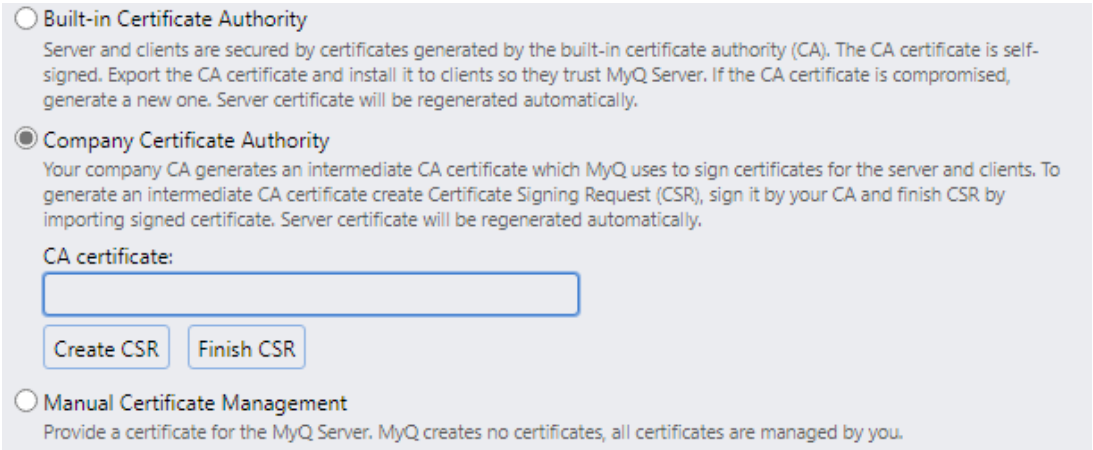


Ce mot de passe est stocké dans le fichier « C:\ProgramData\MyQ\setup.ini » sous forme cryptée et est défini par défaut sur *« masterkey »*.

1.2.2 PS Sécurité de la connexion

Configurer le certificat HTTPS

Un certificat personnalisé reconnu par tous les ordinateurs clients doit être configuré pour MyQ Print Server. Trois modes de gestion des certificats sont disponibles :



Par défaut, MyQ Print Server crée son propre certificat CA racine et l'utilise pour signer les certificats serveur et client. La partie publique de ce certificat peut être exportée et déployée dans le magasin de certificats de confiance du client, par exemple à l'aide de la stratégie de groupe ou d'un système MDM.

Les organisations disposant déjà d’une infrastructure PKI de confiance peuvent préférer la deuxième option. MyQ Print Server utilise sa propre autorité de certification intermédiaire pour émettre les certificats serveur et client. Le certificat d’autorité de certification intermédiaire généré automatiquement doit être signé par l’autorité de certification de l’entreprise afin d’être reconnu par les clients.

Si la politique de sécurité de l'entreprise n'autorise pas l'installation d'un certificat d'autorité de certification intermédiaire sur MyQ Print Server, ou si un certificat émis par une autorité de certification publique doit être utilisé, il faut alors recourir à la gestion manuelle des certificats.

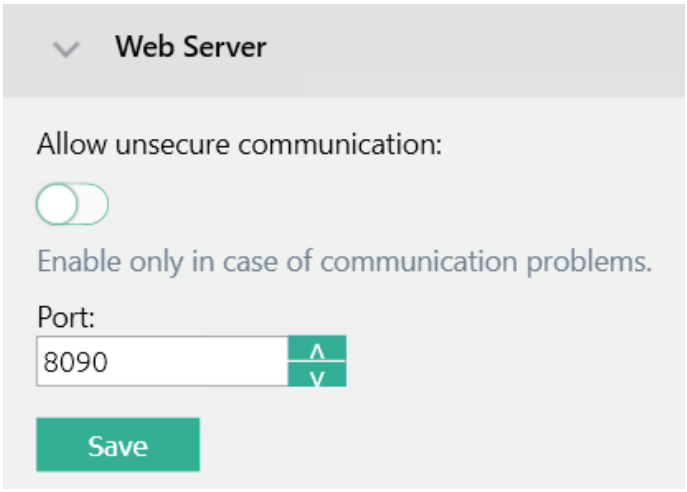
Quel que soit le mode CA, les certificats sont physiquement stockés dans le répertoire « C:\ProgramData\MyQ\Cert », qui peut contenir les fichiers suivants :

- server.pfx – certificat de serveur avec clés publique et privée
- server.cer – certificat de serveur avec clé publique
- server.key – clé privée du serveur
- ca-root.crt – certificat CA racine de l'entreprise avec clé publique
- ca-myq.pfx – certificat de l'autorité de certification émettrice avec clés publique et privée
- ca-myq.crt – certificat de l'autorité de certification émettrice avec clé publique
- ca-myq.key – clés privées de l'autorité de certification émettrice

Les clés privées de l'autorité de certification émettrice locale (utilisées dans les deux premiers modes de fonctionnement) sont toujours protégées par un mot de passe généré aléatoirement, qui est stocké sous forme chiffrée dans la base de données interne de Firebird.

Bloquer le trafic HTTP non chiffré

Le trafic HTTP non chiffré ne doit pas être activé dans la configuration de MyQ Print Server :



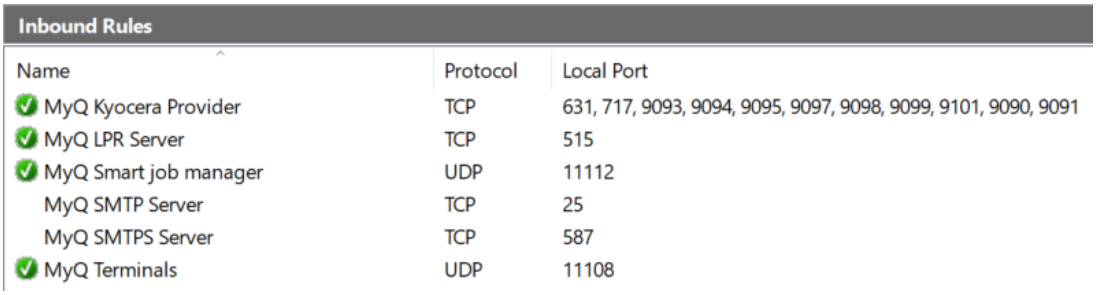
Vérifier les paramètres de sécurité des communications

Vérifiez les versions TLS minimales configurées dans Paramètres – Réseau – Version TLS minimale. La valeur par défaut depuis MyQ X 10.2 est TLS 1.2.

Pour des options plus avancées, telles que la configuration de la version TLS minimale requise à 1.3, consultez lasection Sécurité avancée.

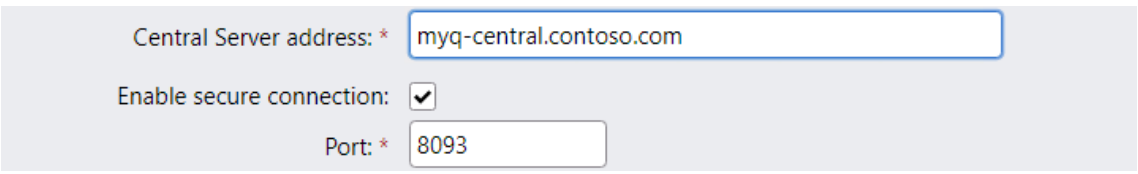
Bloquer les ports inutilisés

Réduisez la surface d'attaque en désactivant les règles de pare-feu pour les protocoles non utilisés par MyQ Print Server :



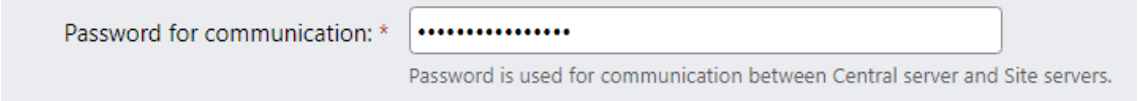
Cryptez les connexions au Central Server MyQ

Utilisez uniquement le protocole HTTPS pour vous connecter à MyQ Central Server :



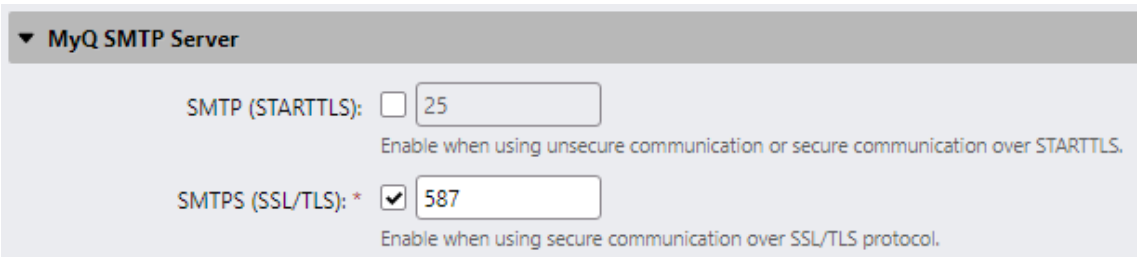
Utilisez des mots de passe forts pour l'authentification de serveur à serveur

Le mot de passe utilisé pour la communication entre le Central Server et le site doit être fort (complexité du mot de passe) :

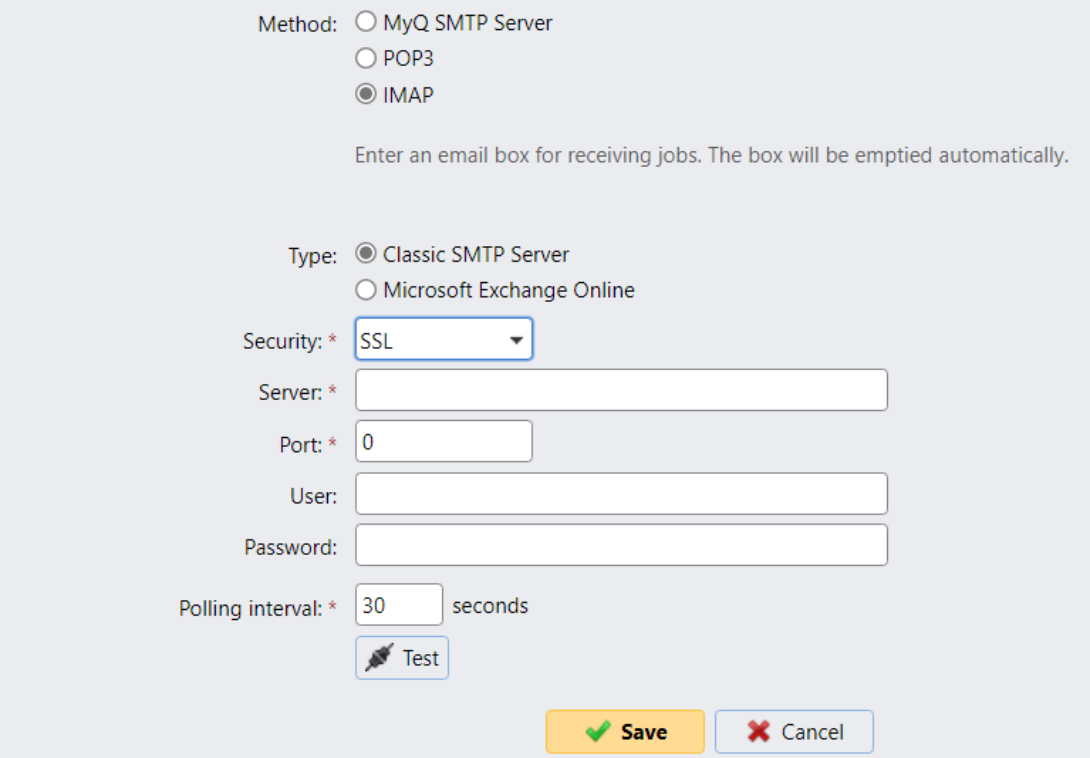


Sécurisez le trafic SMTP

Lorsque le protocole SMTP est utilisé pour envoyer des e-mails ou recevoir des documents provenant de scanners en réseau, le chiffrement TLS doit toujours être appliqué pour garantir la confidentialité des données.



Le chiffrement TLS doit également être appliqué lorsque le protocole IMAP est utilisé, tandis que l'ancien protocole POP3 doit être évité :



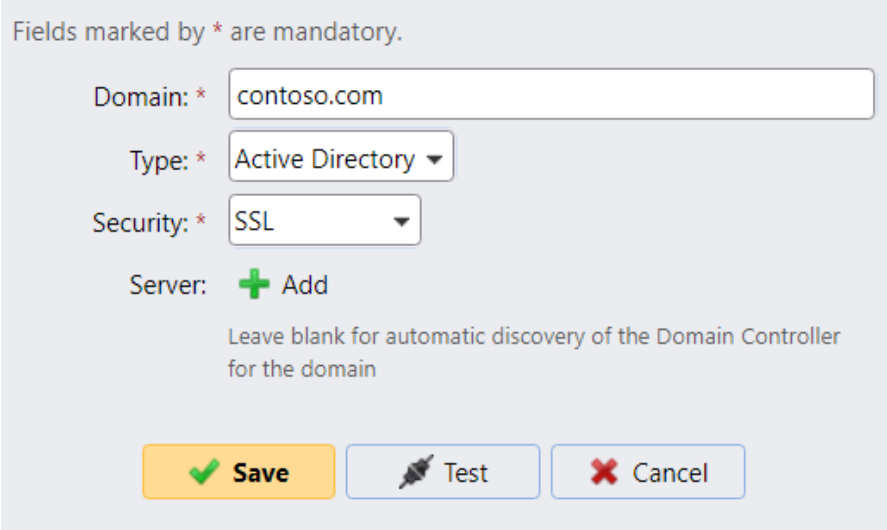
Utilisez des mots de passe RADIUS forts et uniques

Si l'authentification RADIUS est utilisée, générez toujours des secrets partagés forts spécifiques au Print Server MyQ :



Chiffrer le trafic LDAP

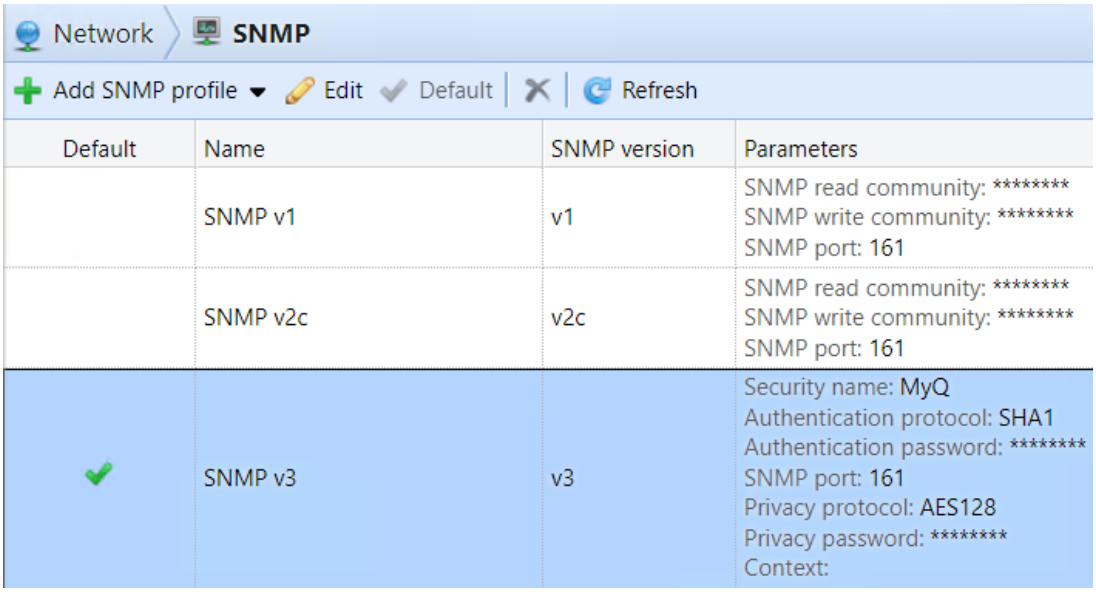
Le chiffrement TLS doit être utilisé pour sécuriser tout le trafic LDAP :



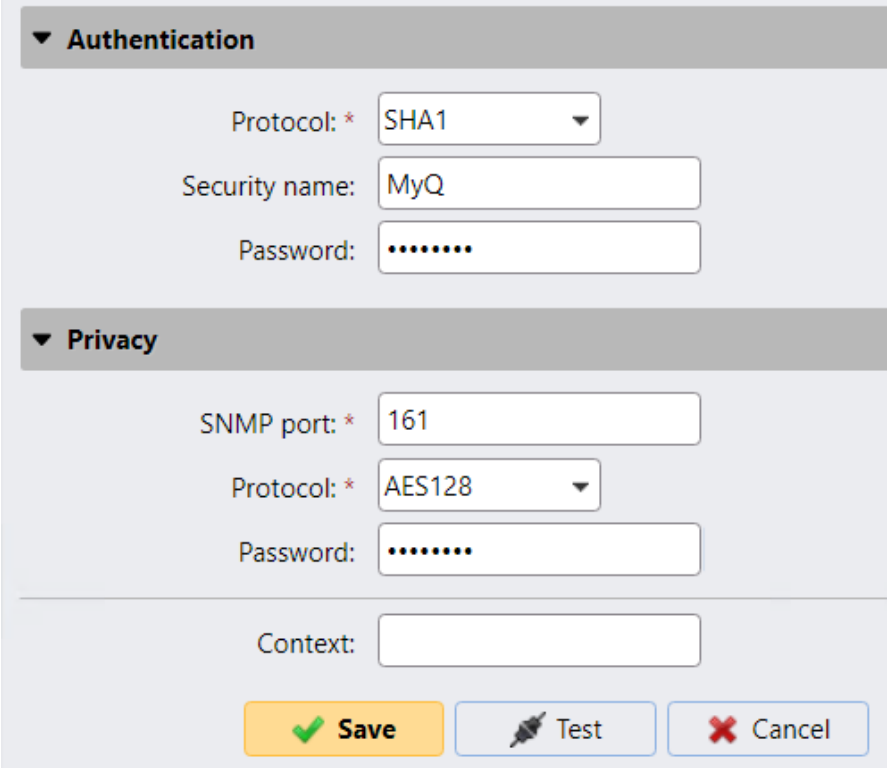
Pour des raisons de sécurité, n'utilisez pas START TLS, car il est vulnérable aux attaques de type « man-in-the-middle » (MITM). Un certificat émis par une autorité de certification (CA) de confiance doit être configuré sur tous les serveurs LDAP (contrôleurs de domaine Active Directory).

Sécurisez le trafic SNMP

Il convient d'éviter les communications SNMPv1 non sécurisées avec les périphériques :

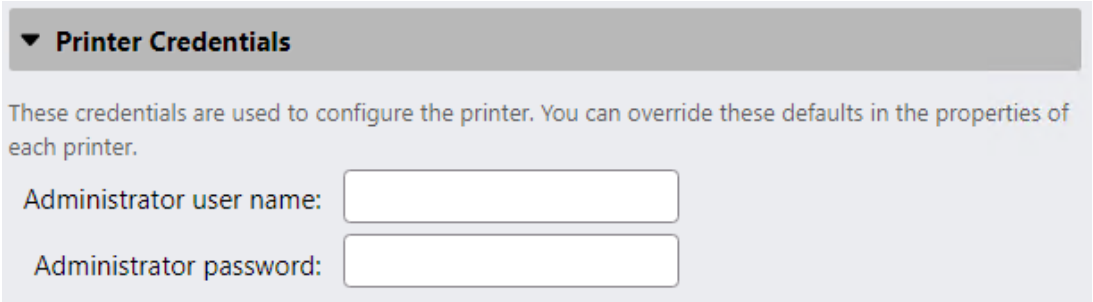


N'utilisez que le protocole SNMPv3 avec un mot de passe fort et configurez des algorithmes cryptographiques plus sécurisés (SHA1 et AES) :



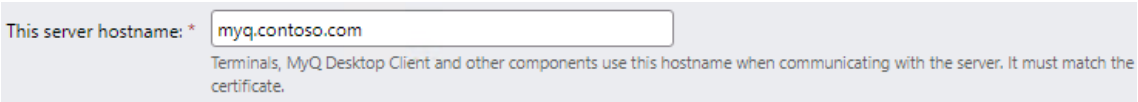
Sécurisation des identifiants d'imprimante

La gestion des identifiants d'imprimante s'effectue en dehors de MyQ Print Server et dépend du fournisseur. Dans la mesure du possible, utilisez des mots de passe forts générés de manière aléatoire pour gérer les imprimantes :



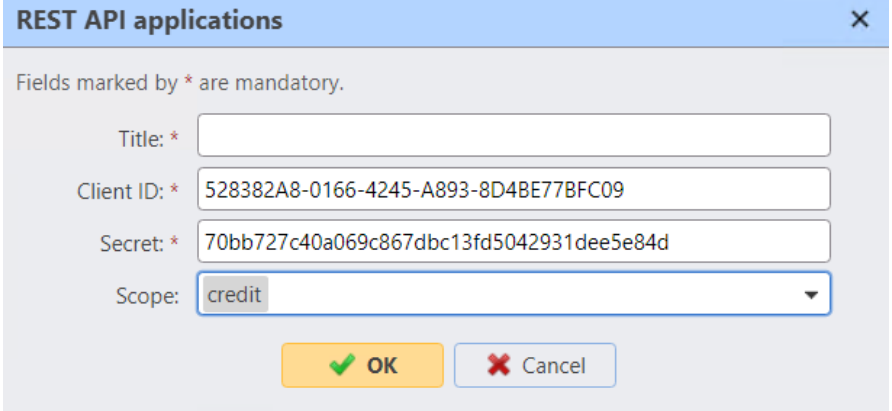
Utilisez toujours le nom de domaine complet (FQDN)

Pour prévenir les attaques de type MITM, utilisez strictement des noms de domaine complets dans toutes les fenêtres de configuration :



Protégez les clés API REST

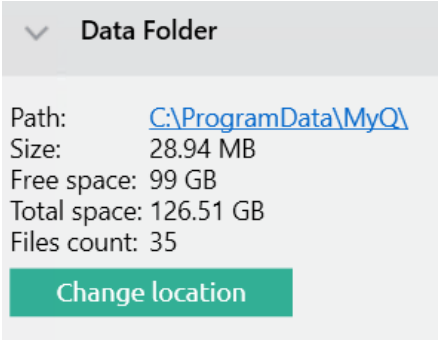
Lorsque des API REST sont utilisées, protégez les secrets client contre toute exposition inutile et procédez à un renouvellement périodique des secrets :



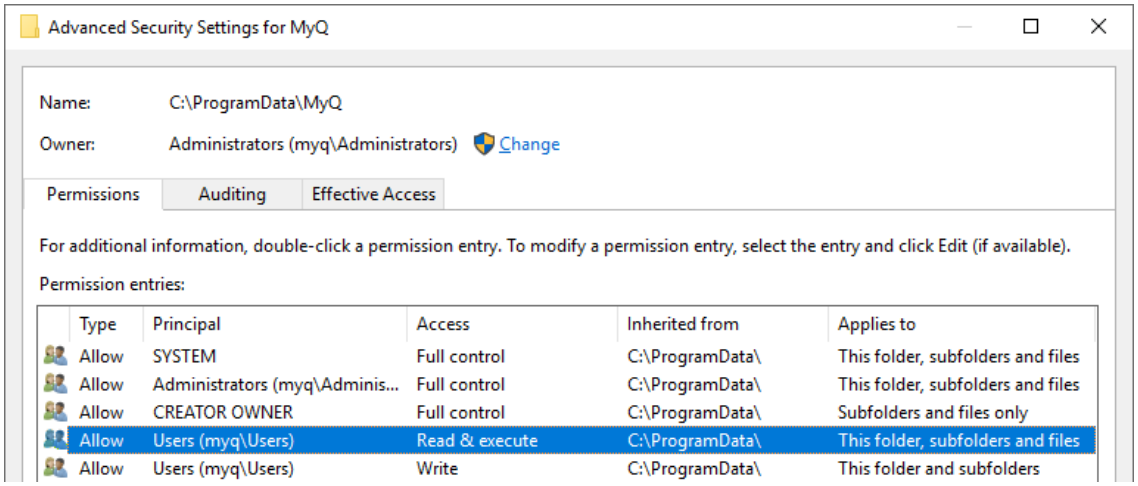
1.2.3 PS Sécurité des données

Restriction des droits d'accès au dossier de données

Le dossier de données de MyQ Print Server contient des données hautement sensibles, notamment la base de données des utilisateurs et la clé privée du certificat TLS. Son emplacement actuel est affiché dans l'application MyQ Easy Config :



Tous les utilisateurs (locaux/du domaine) disposent par défaut d'un accès en lecture :



Seuls les administrateurs, le compte SYSTEM et le compte de service MyQ doivent avoir accès à ce répertoire. Voici un exemple de script batch pouvant être utilisé pour renforcer les autorisations :

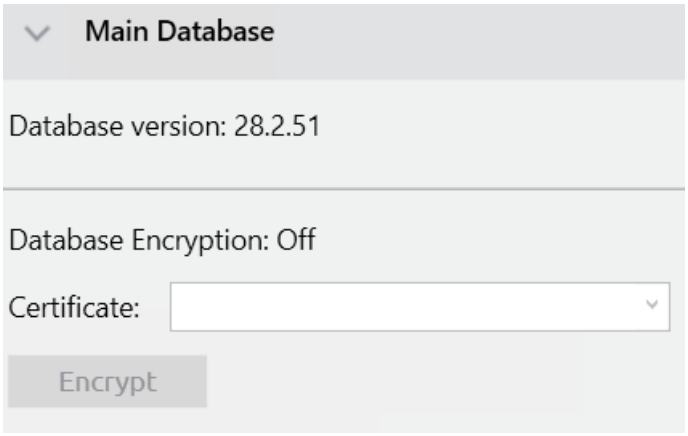
```
@ECHO OFF

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
```

Activer le chiffrement de la base de données

Chiffrez systématiquement la base de données à l'aide d'un certificat personnalisé afin de réduire le risque de fuites de données :



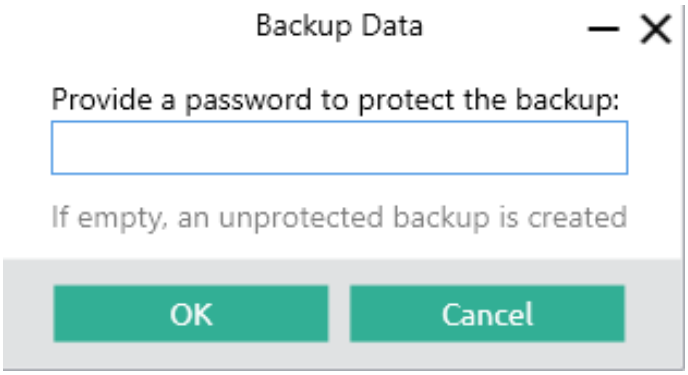
Le certificat doit disposer de l'utilisation de clé étendue (EKU) « Encrypting File System » et doit se trouver dans l'un des magasins de certificats suivants de l'ordinateur :

- Personnel
- Éditeurs de confiance
- Autorités de certification racines tierces
- Autres personnes

Le magasin « Personnel » est celui qui est recommandé.

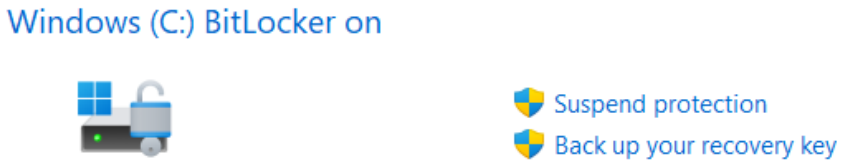
Chiffrer les sauvegardes

Les sauvegardes de bases de données doivent être protégées par des mots de passe sécurisés, générés de manière aléatoire :



Activer le chiffrement du disque

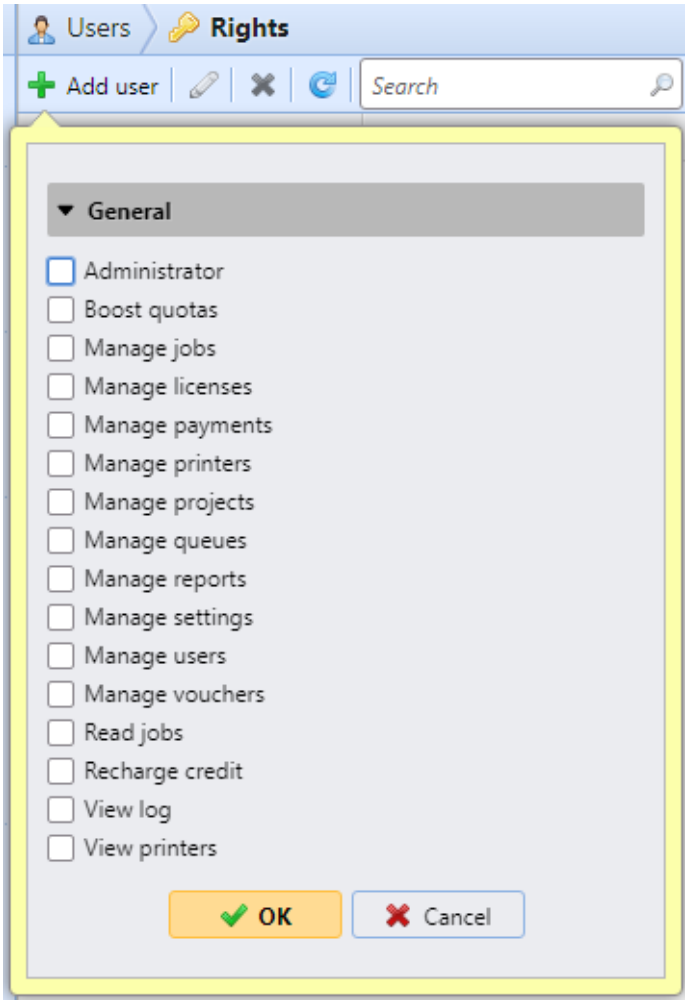
Si possible, une technologie de chiffrement complet du disque, telle que Microsoft BitLocker, doit être activée sur le Print Server MyQ afin de protéger les données au repos :



1.2.4 PS Recommandations supplémentaires

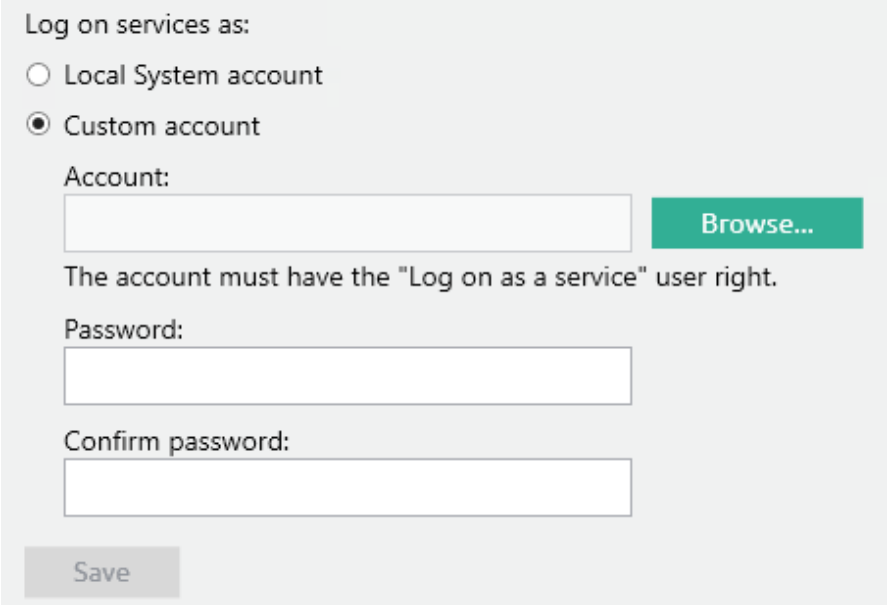
Déployez le RBAC

N'utilisez pas le compte *admin par défaut pour les opérations courantes. Utilisez plutôt la délégation de privilèges, tout en appliquant le principe du privilège minimal :



Configurer un compte de service personnalisé

MyQ Print Server s'exécute par défaut sous le compte SYSTEM, qui dispose de privilèges élevés. Configurez plutôt un compte de service personnalisé avec un mot de passe fort :



Maintenez le serveur à jour

Installez les mises à jour de sécurité fournies par MyQ dès qu'elles sont disponibles. Vous pouvez vérifier la version de l'application actuellement installée dans MyQ Easy Config :



Assurez la sécurité du système d'exploitation

La sécurité de MyQ Print Server dépend de celle du système d'exploitation sous-jacent. Maintenez-le à jour et appliquez les politiques de sécurité recommandées par Microsoft.

Mettez régulièrement à jour vos logiciels pour corriger les failles de sécurité et améliorer les performances. Consultez la (10.2-fr) Configuration requisesection « Configuration système requise » pour connaître la liste des exigences et des recommandations.

Par exemple, .NET doit être mis à jour soit à l'aide d'outils de gestion, soit via Windows Update, sur une base facultative[4].

Préparez-vous à la reprise après sinistre

Effectuez régulièrement des sauvegardes de MyQ Print Server, y compris la base de données, les certificats et les fichiers de configuration. Testez la procédure de reprise au moins une fois.

1.3 MyQ X Desktop Client

Le Desktop Client MyQ utilise des mécanismes de sécurité robustes pour garantir la sécurité des communications, l'authentification et l'intégrité des données dans les environnements d'impression d'entreprise. Ce document détaille les protocoles, les méthodes d'authentification et les meilleures pratiques de configuration qui sous-tendent l'architecture de sécurité du Desktop Client, en mettant l'accent sur le chiffrement TLS, l'authentification Windows intégrée (IWA), Kerberos, NTLM et l'intégration Entra ID. Les implémentations techniques telles que l'enregistrement du nom principal de service (SPN), la gestion des certificats et les flux de connexion silencieux sont analysées afin de démontrer la conformité aux normes de sécurité modernes.

1.3.1 Architecture de communication sécurisée

Chiffrement TLS par défaut

Les serveurs d'impression et Central Server appliquent le chiffrement TLS 1.2+ pour tous les canaux de communication, y compris les interactions avec le Desktop Client. Cela garantit la confidentialité et l'intégrité des données pendant la mise en file

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

d'attente des travaux, l'authentification et la création de rapports. Les administrateurs doivent configurer les points de terminaison HTTPS à l'aide de noms de domaine complets (FQDN) afin d'empêcher les attaques de type « man-in-the-middle » (MITM).

Modes de validation des certificats

- **Mode strict** : exige que les certificats de serveur soient émis par une autorité de certification (CA) de confiance ou ajoutés manuellement au magasin de confiance du système. Les tentatives de connexion échouent si la validation échoue. Nous recommandons d'utiliser le mode strict dans la mesure du possible.
- **Mode normal** : permet aux utilisateurs de contourner les avertissements relatifs aux certificats non fiables, les certificats acceptés étant stockés dans `%ProgramData%\MyQ\Desktop Client\cert.store` pour les sessions futures.

1.3.2 Mécanismes d'authentification

Authentification Windows intégrée (IWA)

L'IWA permet une authentification transparente dans les environnements joints à un domaine à l'aide de Kerberos ou NTLM. Le serveur exploite l'API Windows HTTP Server (`http.sys`) pour traiter les requêtes HTTP entrantes et valider les noms principaux de service (SPN), garantissant ainsi l'intégrité du protocole.

Workflow Kerberos

1. **Acquisition du ticket d'accès (TGT)** : les clients joints au domaine obtiennent un TGT auprès du centre de distribution de clés (KDC).
2. **Demande de ticket de service** : le client demande un ticket de service au `HTTP/<FQDN>` au KDC.
3. **Validation du jeton** : le serveur MyQ valide le ticket de service par rapport au SPN enregistré.

Configuration critique :

- Le serveur doit disposer d'un SPN correctement configuré pour que l'authentification Kerberos fonctionne correctement.
- L'accès via des adresses IP contourne Kerberos, ce qui oblige à revenir à NTLM.

Application de Kerberos

Pour les environnements nécessitant une sécurité plus stricte, il est possible de configurer l'application pour qu'elle **utilise exclusivement Kerberos** et interdise le repli vers NTLM. Cela se fait au niveau du serveur, et non exclusivement pour le Desktop Client.

1. Désactivez NTLM via `KerberosOnly=True` dans `config.ini`.
2. Enregistrer les SPN pour tous les serveurs MyQ à l'aide de `setspn`.
3. Utilisez les noms de domaine complets (FQDN) au lieu des adresses IP pour les points de terminaison du serveur.

Repli NTLM

NTLM sert de solution de secours dans les scénarios non basés sur un domaine ou sur IP. Bien que moins sécurisé, il utilise un mécanisme de défi-réponse haché avec le mot de passe de l'utilisateur. Pour appliquer exclusivement Kerberos, suivez la suggestion ci-dessus.

Connexion silencieuse Entra ID

Pour les périphériques hybrides ou connectés à Entra ID, Desktop Client utilise la bibliothèque d'authentification Microsoft (MSAL) et le gestionnaire d'authentification Windows (WAM) pour acquérir des jetons de manière silencieuse via le compte du système d'exploitation. Le flux comprend :

1. **Acquisition de jetons** : MSAL récupère un jeton d'identification à l'aide de WAM.
2. **Échange de jetons** : le jeton d'identification est échangé contre un jeton d'accès MyQ pour authentifier les appels API REST.

Flux de code d'autorisation OAuth 2.0

Pour les environnements non Windows, Desktop Client prend en charge OAuth 2.0 via le `authorization_code` autorisation :

1. **Redirection de l'utilisateur** : le client redirige les utilisateurs vers la page de connexion MyQ.
2. **Échange de code** : après authentification, le code d'autorisation est échangé contre un jeton d'accès.

Configuration Entra ID

- Activez **la connexion avec Microsoft** dans les paramètres du serveur MyQ pour les périphériques hybrides.
- Assurez-vous que les périphériques sont enregistrés avec Entra ID afin de bénéficier de l'authentification silencieuse.

Gestion des certificats

Certificats racine de confiance

- **Mode strict** : les certificats doivent être préinstallés dans le magasin de confiance du système d'exploitation (par exemple, via la stratégie de groupe).
- **Mode normal** : les certificats approuvés par l'utilisateur sont stockés dans `cert.store` et réutilisés pour les sessions suivantes.

Workflow de validation

1. La validation des certificats de serveur vérifie la chaîne de confiance.
2. Si la validation échoue, les utilisateurs reçoivent une invite leur demandant d'accepter ou de rejeter le certificat (ceci n'est le cas que si le mode de validation normal est utilisé plutôt que le mode strict).
3. Les certificats acceptés sont mis en cache afin d'éviter les invites répétées (ceci uniquement si le mode de validation normal est utilisé plutôt que le mode strict).

Meilleures pratiques en matière de certificats
Nous recommandons de toujours déployer des certificats signés par une autorité de certification d'entreprise pour les serveurs MyQ.

Conclusion

MyQ Desktop Client intègre une authentification et un chiffrement de niveau entreprise afin d'atténuer les risques tels que le vol d'identifiants et l'écoute clandestine. En imposant Kerberos, TLS et la validation des certificats, les organisations peuvent se conformer aux principes Zero Trust tout en conservant leur facilité d'utilisation grâce à des flux d'authentification silencieux.

2 Livre blanc sur la sécurité de MyQ X

Présentation des fonctionnalités de sécurité de MyQ X

MyQ X offre une gamme de fonctionnalités visant à renforcer la sécurité et la confidentialité des utilisateurs finaux ainsi que de l'entreprise. Ces fonctionnalités comprennent notamment l'impression sécurisée sur le multifonction, la personnalisation de la session utilisateur et ont un impact continu même après l'impression d'un document grâce à l'utilisation de filigranes.

Voici un bref résumé des fonctionnalités de sécurité de MyQ X :

- Conformité au RGPD
- Impression sécurisée
- Sessions utilisateur avec plusieurs options d'authentification, y compris l'authentification à deux facteurs
- Déconnexion manuelle et automatique des sessions utilisateur
- Chiffrement de bout en bout des données, y compris le chiffrement des données au repos (base de données, travaux, journaux)
- Dossiers de destination de numérisation prédéfinis par l'administrateur MyQ
- Files d'impression privées pour la suppression immédiate des travaux d'impression après leur libération
- Mode confidentialité pour anonymiser les noms des travaux d'impression
- Accès restreint aux options de configuration du Print Server sur l'interface Web MyQ X
- Droits personnalisables pour l'accès à différentes options de configuration
- Plusieurs niveaux de complexité des mots de passe
- Journal d'audit des modifications apportées aux paramètres
- Assistance pour l'autorité de certification d'entreprise
- Apposition d'un filigrane sur des documents imprimés
- Aperçu des travaux
- Contrôle des documents numérisés via les systèmes OCR et DMS
- Archivage des offres d'emploi

L'approche de MyQ X en matière de sécurité repose sur le principe suivant : **La sécurité n'est pas une considération secondaire, mais fait partie intégrante de l'ensemble de l'écosystème de gestion de l'impression.**La plateforme met en œuvre une stratégie de défense complète qui protège les données et les flux de travail à chaque étape du cycle de vie des documents.

2.1 Architecture Zero Trust

Conformément à la méthodologie « ne jamais faire confiance, toujours vérifier », MyQ X part du principe que des menaces peuvent exister tant à l'intérieur qu'à

l'extérieur d'un réseau. Chaque connexion, utilisateur et périphérique doit être authentifié et autorisé avant d'accéder aux ressources d'impression, garantissant ainsi une vérification continue tout au long des interactions.

2.2 Cadre de protection en trois phases

MyQ X aborde la sécurité à travers trois phases essentielles :

2.2.1 Sécurisation de l'infrastructure d'impression

Toutes les infrastructures de soutien sont correctement sécurisées avant l'impression de tout document, y compris les postes de travail, les périphériques mobiles, les serveurs, les réseaux et les imprimantes.

2.2.2 Sécurisation des flux de travail d'impression

Des flux de travail sécurisés éprouvés, comprenant la validation authentifiée des impressions, l'isolation des travaux et la génération de rapports complets, préviennent les vulnérabilités susceptibles d'exposer les organisations.

2.2.3 Sécurisation des impressions

Protection continue grâce au tatouage numérique, aux signatures numériques et aux journaux d'audit complets qui garantissent la traçabilité et encouragent un comportement responsable de la part des utilisateurs.

2.3 Confidentialité dès la conception

La protection des données est intégrée dès le départ dans l'architecture de MyQ X. Le système minimise la collecte de données, met en œuvre un cryptage puissant et offre aux utilisateurs le contrôle de leurs informations personnelles afin de garantir la conformité au RGPD et la protection de la vie privée.

2.4 Évolution continue de la sécurité

MyQ X assure sa sécurité grâce à des mises à jour régulières, une correction rapide des vulnérabilités, l'intégration de renseignements sur les menaces et des évaluations et certifications de sécurité continues par des tiers.

Cette approche axée sur la sécurité garantit aux organisations qu'elles peuvent déployer MyQ X en toute confiance, sachant que leurs informations sensibles, leurs

exigences de conformité et la continuité de leurs opérations sont protégées par des mesures de sécurité de pointe.

2.5 Principales améliorations de la sécurité dans la version 10.2

MyQ X 10.2 introduit des améliorations significatives en matière de sécurité, conçues pour renforcer la protection contre les cybermenaces en constante évolution tout en maintenant l'efficacité opérationnelle. Ces améliorations corrigent des vulnérabilités critiques et mettent en œuvre des normes de sécurité modernes.

2.5.1 Sécurité TLS améliorée

Version minimale TLS 1.2 par défaut : MyQ X 10.2 augmente la version TLS minimale par défaut de 1.1 à 1.2, avec prise en charge de TLS 1.3. Cela élimine la prise en charge des protocoles SSL obsolètes et des chiffrements faibles qui présentent des risques pour la sécurité.

Amélioration de la validation des certificats : la validation améliorée des certificats empêche l'utilisation de certificats expirés ou incorrectement émis, protégeant ainsi contre les attaques de type « man-in-the-middle » et d'autres vulnérabilités. Le système fait désormais automatiquement confiance aux certificats CA racine provenant du magasin de certificats système du serveur.

2.5.2 Améliorations de la sécurité de l'authentification

Sécurité améliorée des mots de passe et des codes PIN : les algorithmes de hachage des mots de passe améliorés renforcent la protection des identifiants. Le système introduit de nouvelles règles de sécurité pour les codes PIN, notamment une longueur minimale obligatoire de 6 chiffres et la prévention des combinaisons faciles à deviner telles que « 1234 » ou « 1111 ».

Protection contre les tentatives de connexion : les tentatives d'authentification infructueuses sont désormais limitées pour des raisons de sécurité. Par défaut, les clients/périphériques sont bloqués pendant 5 minutes après plus de 5 tentatives de connexion invalides en 60 secondes, avec des périodes configurables.

Amélioration de la journalisation des événements de connexion : la journalisation améliorée des événements de connexion, en particulier des tentatives d'authentification infructueuses, facilite le filtrage et la surveillance des événements de sécurité dans MyQ Log pour les administrateurs.

2.5.3 Mises à niveau de la sécurité de la base de données

Mise en œuvre de Firebird 4.0 : la mise à niveau vers le moteur de base de données Firebird 4.0 apporte des fonctionnalités de sécurité améliorées et des performances accrues. Les mots de passe de la base de données sont désormais masqués dans les fichiers journaux afin d'éviter toute exposition des identifiants.

Protection des données améliorée : accès limité aux données sensibles grâce à des rapports personnalisés et des comptes de rapport externes, garantissant la confidentialité des données à différents niveaux d'accès.

2.5.4 Résolution des vulnérabilités

Corrections CVE critiques : MyQ X 10.2 corrige plusieurs vulnérabilités critiques, notamment :

- CVE-2024-28059 : vulnérabilité d'exécution de code à distance non authentifiée.
- CVE-2024-22076 : améliorations de la sécurité des scripts PHP.
- CVE-2023-45853, CVE-2023-5678, CVE-2023-49316 : vulnérabilités des composants tiers.

Mises à jour de sécurité des composants : les versions mises à jour des composants critiques, notamment OpenSSL 3.1.0, PHP 8.3.14 et Apache 2.4.57, corrigent les vulnérabilités de sécurité connues.

2.5.5 Sécurité des API et de l'intégration

Restrictions de l'API REST : champs d'application limités pour les clients connus et suppression des capacités pour les opérations sensibles telles que la modification des serveurs d'authentification des utilisateurs, renforçant ainsi la sécurité de l'API.

Contrôles des scripts PHP : de nouveaux paramètres Easy Config permettent aux administrateurs de verrouiller/déverrouiller l'accès aux scripts PHP, améliorant ainsi la sécurité en conservant ces paramètres en mode lecture seule.

2.5.6 Sécurité administrative

Sécurité renforcée des comptes administrateur : le mot de passe administrateur par défaut a été supprimé pour les nouvelles installations. Les administrateurs peuvent désormais désactiver les comptes administrateur lorsqu'ils ne sont pas nécessaires, ce qui favorise l'utilisation de comptes utilisateur spécifiques dotés des droits appropriés plutôt que de comptes administratifs partagés.

Ces améliorations en matière de sécurité démontrent l'engagement de MyQ X à maintenir des normes de sécurité de niveau entreprise tout en répondant aux défis actuels en matière de cybersécurité. Des mises à jour de sécurité régulières et une gestion proactive des vulnérabilités garantissent aux organisations de pouvoir déployer MyQ X en toute confiance.

2.6 Valeur commerciale de la gestion sécurisée des impressions

La gestion sécurisée de l'impression apporte une valeur commerciale mesurable en transformant l'infrastructure d'impression, qui était auparavant un risque potentiel, en un atout stratégique en matière de sécurité. MyQ X offre aux organisations une protection complète qui couvre l'ensemble des risques liés à l'impression tout en améliorant l'efficacité opérationnelle.

2.6.1 Atténuation des risques et réduction des coûts

Prévention des violations de données : la fonction Secure Print Release garantit que les documents confidentiels ne sont jamais laissés sans surveillance dans les bacs d'impression, éliminant ainsi tout accès non autorisé aux informations sensibles. Les utilisateurs s'authentifient avant que leurs travaux ne soient lancés, ce qui leur permet de garder un contrôle total sur la sécurité des documents.

Éviter les coûts liés à la conformité : les fonctionnalités embarquées de conformité aux normes GDPR, HIPAA et SOX aident les organisations à éviter les sanctions réglementaires et à réduire les coûts de préparation aux audits grâce à des contrôles de conformité automatisés et des pistes d'audit complètes.

Continuité opérationnelle : la fonction Device Spooling de MyQ maintient les capacités d'impression pendant les pannes de serveur, en stockant localement les travaux cryptés pendant une semaine maximum sur 10 périphériques, ce qui évite toute interruption de l'activité pendant la maintenance du système ou les temps d'arrêt imprévus.

2.6.2 Principes de sécurité renforcés

Mise en œuvre du principe « Zero Trust » : en exigeant une authentification pour chaque travail d'impression, MyQ X applique le principe « ne jamais faire confiance, toujours vérifier » dans tout l'environnement d'impression, renforçant ainsi la sécurité globale de l'organisation.

Traçabilité des documents : les filigranes et les signatures numériques permettent aux organisations de suivre les documents confidentiels tout au long de leur cycle de vie, ce qui garantit la responsabilité et dissuade l'utilisation abusive d'informations sensibles.

Chiffrement complet : le chiffrement de bout en bout des données d'impression, des bases de données et des travaux stockés garantit la protection des informations sensibles tout au long du flux de travail documentaire, répondant ainsi à des exigences de sécurité strictes.

2.6.3 Efficacité opérationnelle

Optimisation de la bande passante : le spooling client réduit le trafic réseau en traitant les travaux localement, améliorant ainsi les performances dans les environnements à bande passante limitée, tels que les bureaux distants et les succursales.

Authentification flexible : plusieurs options d'authentification, notamment les badges, les codes PIN, les mots de passe et l'authentification par application mobile, offrent aux utilisateurs des méthodes d'accès pratiques et sécurisées qui répondent aux divers besoins des organisations. L'authentification multifactorielle (MFA), qui combine ces méthodes, est également disponible.

Gestion centralisée : des politiques de sécurité unifiées sur tous les périphériques simplifient l'administration tout en garantissant des normes de protection cohérentes dans toute l'organisation.

2.6.4 Avantages stratégiques pour l'entreprise

Avantage concurrentiel : la démonstration de solides capacités de sécurité d'impression peut permettre aux organisations de se démarquer sur les marchés concurrentiels, en particulier dans les secteurs qui traitent des données sensibles ou qui servent des clients soucieux de la sécurité.

Confiance des employés : les flux de travail d'impression sécurisés donnent aux utilisateurs l'assurance que leurs documents sont protégés, ce qui améliore la productivité et réduit les préoccupations liées à la sécurité qui peuvent avoir un impact sur l'efficacité au travail.

Infrastructure prête pour l'avenir : le cadre de sécurité complet de MyQ X permet aux organisations de s'adapter à l'évolution des menaces de cybersécurité et des

exigences réglementaires sans avoir à procéder à des révisions majeures de leur infrastructure.

La gestion sécurisée de l'impression avec MyQ X transforme l'impression, qui était auparavant une vulnérabilité potentielle en matière de sécurité, en un processus métier contrôlé, vérifiable et conforme qui soutient les objectifs de l'organisation tout en protégeant les précieuses ressources informationnelles.

2.7 Conformité

Le cadre de conformité complet de MyQ X démontre son engagement à respecter les normes de sécurité internationales et les exigences réglementaires les plus strictes. Cette approche à plusieurs niveaux garantit que les organisations peuvent déployer MyQ X en toute confiance tout en satisfaisant aux diverses exigences de conformité dans tous les secteurs et toutes les juridictions.

2.7.1 Certification et mise en œuvre de la norme ISO 27001:2022

MyQ a obtenu **la certification ISO/IEC 27001:2022**, établissant une approche systématique de la gestion de la sécurité de l'information qui répond aux meilleures pratiques internationales. La mise en œuvre comprend :

Cadre de gestion des risques : processus complets d'évaluation des risques qui identifient, évaluent et atténuent les risques liés à la sécurité de l'information dans toutes les opérations commerciales et tous les déploiements clients.

Mise en œuvre de contrôles de sécurité : déploiement structuré de contrôles de sécurité techniques, administratifs et physiques qui protègent les actifs informationnels tout au long de leur cycle de vie.

Processus d'amélioration continue : révisions et mises à jour régulières des politiques, procédures et contrôles de sécurité afin de faire face à l'évolution des menaces et de maintenir la conformité à la certification.

Engagement de la direction : supervision au niveau exécutif garantissant que la sécurité reste intégrée dans la stratégie commerciale et les processus décisionnels opérationnels.

La certification valide l'approche systématique de MyQ en matière de protection des données des clients et de maintien de la confidentialité, de l'intégrité et de la disponibilité des systèmes d'information.

2.7.2 Cadre de conformité au RGPD et mesures de protection des données

MyQ X met en œuvre **une conformité GDPR** complète grâce à des principes de confidentialité intégrés dans l'architecture du système :

Minimisation des données : le système ne collecte que les métadonnées essentielles nécessaires au fonctionnement opérationnel, évitant ainsi tout traitement inutile de données à caractère personnel qui pourrait augmenter les risques de non-conformité.

Gestion des droits des utilisateurs : mise en œuvre complète des droits des utilisateurs du RGPD, notamment

- Droit d'accès aux données personnelles
- Droit de rectification des informations inexactes
- Droit à l'effacement (« droit à l'oubli »)
- Droit à la portabilité des données
- Droit à la limitation du traitement

Évaluations d'impact sur la protection des données : évaluation systématique des risques liés à la confidentialité pour les nouvelles fonctionnalités et les nouveaux déploiements, afin de garantir le respect du RGPD tout au long de l'évolution du système.

2.7.3 Exigences de conformité régionales (HIPAA, SOX)

MyQ X prend en charge les cadres de conformité spécifiques à l'industrie grâce à des capacités robustes de protection des données et d'audit :

Conformité HIPAA pour les soins de santé :

- Chiffrement des informations médicales protégées (PHI) au repos et en transit.
- Journalisation complète de tous les accès aux données de santé sensibles.
- Contrôles d'accès basés sur les rôles limitant l'accès aux PHI au personnel autorisé uniquement.
- Procédures sécurisées de sauvegarde et de récupération pour répondre aux exigences de conservation des données de santé.

Conformité SOX pour les services financiers :

- Pistes d'audit détaillées pour le traitement et l'impression des documents financiers.
- Contrôles d'accès empêchant toute modification non autorisée des documents financiers.

- Fonctionnalités d'archivage sécurisées prenant en charge les exigences réglementaires en matière de conservation.
- Séparation des tâches grâce à des autorisations basées sur les rôles et des workflows d'approbation.

Contrôles de sécurité supplémentaires :

- Chiffrement des bases de données à l'aide d'algorithmes conformes aux normes de l'industrie.
- Protocoles de communication sécurisés pour toutes les transmissions de données.
- Procédures de sauvegarde automatisées avec chiffrement et vérification de l'intégrité.
- Journalisation et surveillance des accès pour les rapports de conformité.

2.7.4 Pratiques sécurisées du cycle de vie du développement logiciel (SSDLC)

MyQ met en œuvre un cycle de vie sécurisé du développement logiciel conforme aux normes industrielles et aux exigences de la chaîne d'approvisionnement **SLSA**, garantissant ainsi que les pratiques de sécurité sont intégrées à toutes les phases du cycle de vie du logiciel.

Analyse

MyQ effectue **une modélisation** rigoureuse **des menaces** et définit **des exigences de sécurité** claires lors de la phase d'analyse initiale, ce qui permet d'identifier rapidement les risques et d'établir une base de référence solide en matière de sécurité avant le début de la conception.

Conception

Toutes les propositions architecturales sont soumises à **des examens** formels **de l'architecture de sécurité** afin de valider le respect de principes tels que **le privilège minimal**, **la confiance zéro** et **la défense en profondeur**, garantissant ainsi que la sécurité est systématiquement intégrée dans la conception du système.

Développement

Les développeurs suivent **des pratiques de codage sécurisé** et des processus d'examen par les pairs, tandis que toutes les versions sont exécutées sur **des serveurs de compilation** dédiés et isolés, **conformes à la norme SLSA**, garantissant ainsi la protection de l'intégrité des sources et des artefacts de compilation.

Test

Les tests de sécurité comprennent **des analyses SAST** et **de dépendances** automatisées intégrées dans les pipelines CI, ce qui permet de détecter rapidement les vulnérabilités dans le code personnalisé et les composants tiers.

Déploiement

Tous les artefacts de publication sont protégés par **signature de code** et vérifiés lors du déploiement, ce qui garantit **leur intégrité**, **leur authenticité** et leur livraison contrôlée dans les environnements de production.

Maintenance

Après le déploiement, les systèmes font l'objet **d'une surveillance** continue et **d'une gestion** structurée **des correctifs**, ce qui garantit une adaptation permanente aux menaces en constante évolution et aux **meilleures pratiques en matière de sécurité**.

2.7.5 Audits de sécurité et tests de pénétration réguliers

MyQ maintient une validation de sécurité robuste grâce à des programmes de tests et d'évaluation systématiques :

Tests de pénétration automatisés : l'intégration avec la plateforme de sécurité Qualys permet une évaluation continue des vulnérabilités et des tests de pénétration pour toutes les versions logicielles.

Évaluations de sécurité par des tiers : des audits de sécurité indépendants sont menés par des organismes externes qualifiés afin de valider les contrôles de sécurité et d'identifier les améliorations potentielles.

Examens de sécurité internes : évaluations internes régulières des politiques, procédures et contrôles techniques de sécurité afin de garantir leur efficacité et leur conformité continues.

Processus de réponse aux vulnérabilités : procédures structurées pour traiter les problèmes de sécurité identifiés, y compris les délais requis pour le développement et le déploiement des correctifs.

2.7.6 Nomenclature logicielle et gestion des vulnérabilités

MyQ met en œuvre une sécurité complète de la chaîne d'approvisionnement grâce à un suivi détaillé des composants et à la gestion des vulnérabilités :

Publication de la nomenclature logicielle : documentation complète de la nomenclature logicielle identifiant tous les composants, bibliothèques et dépendances tiers utilisés dans les systèmes MyQ X.

Analyse automatisée des vulnérabilités : surveillance continue des bases de données des composants à la recherche de nouvelles vulnérabilités identifiées affectant les dépendances MyQ X.

Gestion rapide des correctifs : processus systématique d'évaluation, de test et de déploiement des mises à jour de sécurité pour les composants tiers, avec hiérarchisation basée sur l'évaluation des risques.

Contrôle des versions des composants : suivi détaillé de tous les composants logiciels, y compris les numéros de version, les niveaux de correctifs de sécurité et les calendriers de mise à jour, tels que documentés dans les notes de mise à jour.

Évaluation de la sécurité des fournisseurs : évaluation des fournisseurs de logiciels tiers afin de s'assurer qu'ils respectent les normes de sécurité et les processus de divulgation des vulnérabilités appropriés.

Ce cadre de conformité complet garantit que MyQ X répond à diverses exigences réglementaires tout en maintenant les normes les plus élevées en matière de sécurité de l'information et de protection des données dans tous les environnements opérationnels.

2.8 Mise en œuvre de l’architecture de confiance zéro

MyQ X met en œuvre l'architecture Zero Trust comme approche de sécurité fondamentale qui élimine la confiance implicite et valide en permanence chaque transaction. Ce cadre complet garantit qu'aucun utilisateur, périphérique ou connexion réseau n'est considéré comme fiable par défaut, quel que soit son emplacement ou son statut d'authentification précédent.

2.8.1 Principes Zero Trust dans la gestion de l'impression

La mise en œuvre de Zero Trust par MyQ X repose sur le principe **« ne jamais faire confiance, toujours vérifier »** dans l'ensemble du système de gestion d'impression. Le système exige une vérification explicite pour chaque demande d'accès, garantissant ainsi que :

Canaux de communication cryptés : tout le trafic réseau utilise le cryptage TLS obligatoire avec la version 1.2 minimum, empêchant ainsi l'écoute clandestine et la falsification pendant la transmission des données. Les certificats HTTPS doivent être

correctement configurés et validés afin d'empêcher les attaques de type « man-in-the-middle ».

Application de protocoles sécurisés : MyQ X bloque le trafic HTTP non crypté et applique des protocoles de sécurité rigoureux sur tous les canaux de communication, y compris les connexions SMTP, LDAP et SNMP. Les protocoles hérités tels que SNMPv1 sont interdits au profit de SNMPv3 avec authentification forte.

Contrôles de sécurité des API : l'accès à l'API REST nécessite des jetons d'authentification avec filtrage des adresses IP, garantissant que les appels API sont authentifiés et proviennent de sources fiables. Les secrets clients font l'objet d'une rotation périodique afin de maintenir l'intégrité de la sécurité.

2.8.2 Méthodologie « Ne jamais faire confiance, toujours vérifier »

La méthodologie Zero Trust imprègne tous les aspects des opérations MyQ X grâce à des mécanismes de vérification continue :

Vérification d'identité : chaque interaction utilisateur nécessite une authentification, quel que soit l'emplacement du réseau ou le statut de confiance du périphérique. Les utilisateurs doivent s'authentifier sur chaque périphérique d'impression, même s'ils se sont déjà connectés ailleurs dans l'organisation.

Authentification des périphériques : les périphériques d'impression eux-mêmes doivent s'authentifier avant d'accéder aux ressources du réseau, à l'aide d'identifiants et de certificats uniques empêchant l'usurpation d'identité non autorisée.

Gestion des sessions : les sessions utilisateur implémentent une fonctionnalité de déconnexion et de délai d'expiration automatique, garantissant que les sessions abandonnées ne peuvent pas être exploitées par des personnes non autorisées.

2.8.3 Segmentation et isolation du réseau

MyQ X met en œuvre une segmentation complète du réseau afin de limiter les surfaces d'attaque et de contenir les failles de sécurité potentielles :

Contrôles des limites du réseau : le système applique des règles de pare-feu strictes qui bloquent les ports inutilisés et limitent l'accès au réseau aux seuls canaux de communication nécessaires. Les configurations par défaut désactivent les services et protocoles inutiles.

Segmentation basée sur les certificats : MyQ X prend en charge trois modes de gestion des certificats (autorité de certification embarquée, autorité de certification d'entreprise et gestion manuelle des certificats), ce qui permet aux organisations de mettre en œuvre des limites de confiance appropriées en fonction de leurs politiques de sécurité.

Application des noms de domaine complets : toutes les communications réseau doivent utiliser des noms de domaine complets (FQDN) plutôt que des adresses IP ou des noms à étiquette unique, ce qui empêche les attaques de type « man-in-the-middle » basées sur le DNS et garantit une validation correcte des certificats.

Gestion des ports : le système gère automatiquement les règles de pare-feu et offre un contrôle explicite sur les ports réseau accessibles, réduisant ainsi la surface d'attaque grâce au blocage systématique des ports.

2.8.4 Authentification et vérification robustes

MyQ X maintient une validation de sécurité continue grâce à plusieurs couches d'authentification et à une surveillance en temps réel :

Authentification multi-méthodes : le système prend en charge diverses méthodes d'authentification, notamment LDAP, Microsoft Entra ID, RADIUS et l'authentification MyQ locale, avec des capacités de basculement automatique garantissant un contrôle d'accès continu.

Intégration du serveur d'authentification : l'intégration sécurisée avec des serveurs d'authentification externes utilise des connexions cryptées (TLS pour LDAP, protocoles sécurisés pour RADIUS) et applique des secrets partagés forts spécifiques à chaque déploiement MyQ.

Surveillance des connexions : la journalisation améliorée des événements d'authentification, en particulier des tentatives de connexion infructueuses, permet aux administrateurs de détecter les menaces potentielles pour la sécurité et d'y répondre. Les tentatives d'authentification infructueuses déclenchent des mécanismes de blocage automatiques. Par défaut, les périphériques sont bloqués pendant 5 minutes après plus de 5 tentatives invalides en 60 secondes.

Contrôles de persistance des sessions : le système met en œuvre des politiques de délai d'expiration des sessions configurables et une fonctionnalité de déconnexion automatique, garantissant que les sessions inactives ne peuvent pas être exploitées.

2.8.5 Vérification des périphériques et des terminaux

MyQ X applique des protocoles de vérification des périphériques stricts afin de garantir que seuls les terminaux autorisés peuvent accéder aux ressources d'impression :

Gestion des certificats des périphériques : tous les périphériques connectés doivent présenter des certificats valides pour communiquer sur le réseau. Le système gère un magasin de certificats complet avec une validation de chaîne appropriée et prend en charge le déploiement automatique des certificats via la stratégie de groupe ou la gestion des appareils mobiles (MDM).

Contrôles de sécurité des terminaux : les périphériques d'impression sont soumis à une validation de sécurité continue, notamment une authentification SNMP v3 avec des mots de passe forts et des algorithmes cryptographiques (SHA1 et AES). Les identifiants d'impression sont gérés via des protocoles de sécurité spécifiques aux fournisseurs avec des mots de passe forts générés de manière aléatoire.

Authentification des périphériques mobiles : MyQ X Mobile Client met en œuvre l'autorisation d'accès aux périphériques OAuth 2.0 pour une authentification sécurisée des périphériques mobiles, remplaçant les anciens systèmes basés sur des codes PIN par une sécurité moderne basée sur la biométrie.

Cadre de sécurité BYOD : le système prend en charge les environnements BYOD (Bring-Your-Own-Device) grâce à la propagation sécurisée des impressions via AirPrint et Mopria, en maintenant les principes de confiance zéro même dans les réseaux sans visibilité directe du Print Server.

Gestion des jetons d'accès : des jetons d'accès uniques sont émis pour chaque type de périphérique, la sécurité de la couche de transport (TLS) étant obligatoire pour toutes les communications. Le système met en œuvre des contrôles d'accès juste à temps (JIT) qui ajustent dynamiquement les privilèges en fonction du contexte et d'une évaluation continue des risques.

Cette mise en œuvre complète du principe « zero trust » garantit que MyQ X maintient les normes de sécurité les plus élevées tout en prenant en charge divers besoins organisationnels et scénarios de déploiement. L'architecture offre une protection approfondie qui s'adapte à l'évolution des menaces tout en maintenant l'efficacité opérationnelle et l'expérience utilisateur.

2.9 Gestion des identités et des accès

MyQ X fournit un cadre complet de gestion des identités et des accès qui s'intègre de manière transparente aux systèmes d'authentification d'entreprise existants tout en prenant en charge les normes de sécurité modernes. L'architecture IAM garantit une authentification des utilisateurs sécurisée, évolutive et flexible dans divers environnements organisationnels.

2.9.1 Mise en œuvre de l'authentification multifactorielle

MyQ X met en œuvre de solides capacités **d'authentification multifactorielle (MFA)** qui renforcent considérablement la sécurité en exigeant plusieurs facteurs de vérification :

Authentification par terminal intégré : les méthodes MFA standard comprennent des combinaisons de badge et de code PIN, où les utilisateurs présentent d'abord leur badge physique, puis confirment leur identité à l'aide d'un code PIN. L'authentification par badge et mot de passe offre une sécurité à deux facteurs similaire, avec une vérification par mot de passe au lieu d'un code PIN.

Authentification mobile : le client mobile MyQ X permet une MFA sophistiquée grâce à la lecture de codes QR combinée à une vérification biométrique. Les utilisateurs s'authentifient en scannant un code QR affiché sur le terminal intégré, avec une sécurité supplémentaire fournie par des verrous biométriques (Face ID ou empreinte digitale) sur leurs périphériques mobiles.

Intégration du Desktop Client : les organisations qui utilisent les services Microsoft 365 bénéficient d'une authentification multifactorielle intégrée grâce à l'authentification Entra ID. Les utilisateurs dont l'authentification à deux facteurs est activée dans leur compte Entra ID sont automatiquement invités à vérifier leur identité à l'aide d'applications d'authentification lorsqu'ils accèdent au Desktop Client.

2.9.2 Autorisation d'accès aux périphériques OAuth 2.0

MyQ X prend en charge la norme **d'octroi de code d'autorisation OAuth 2.0**, ce qui permet une intégration sécurisée avec les fournisseurs d'identité modernes et les applications tierces :

Flux OAuth standard : le système met en œuvre le cadre d'autorisation OAuth 2.0 complet, y compris la présentation de la page de connexion, la génération d'un code d'accès unique et la récupération sécurisée des jetons. Les applications clientes

reçoivent des jetons porteurs avec des durées d'expiration et des champs d'application configurables.

Sécurité de l'intégration API : des jetons OAuth doivent être fournis pour tous les accès aux points de terminaison API, afin de garantir que les intégrations tierces maintiennent une authentification appropriée. Le système prend en charge la validation de l'ID client et du secret client avec une correspondance URI de redirection sécurisée.

Gestion des jetons : les jetons d'accès comprennent des contrôles d'expiration (1800 secondes par défaut) et des restrictions de portée, offrant un contrôle granulaire des autorisations d'accès à l'API tout en maintenant la sécurité grâce à la rotation des jetons.

2.9.3 Capacités d'intégration de l'authentification unique

MyQ X offre une intégration complète **de l'authentification unique (SSO)** qui rationalise l'authentification des utilisateurs dans les environnements d'entreprise :

Intégration Microsoft 365 : l'intégration approfondie avec Microsoft Entra ID permet une authentification unique transparente pour les organisations utilisant les services Microsoft 365. Les utilisateurs peuvent s'authentifier à l'aide de leurs identifiants Microsoft existants, ce qui élimine le besoin de mots de passe MyQ distincts.

Services d'annuaire d'entreprise : les capacités SSO s'étendent à divers serveurs d'authentification, notamment Active Directory, OpenLDAP et Novell eDirectory, permettant aux utilisateurs d'utiliser leurs identifiants d'entreprise existants pour accéder à MyQ.

Authentification multiplateforme : la fonctionnalité SSO fonctionne sur tous les composants MyQ X, y compris Desktop Client, le client mobile et les terminaux intégrés, offrant une expérience d'authentification cohérente quelle que soit la méthode d'accès.

2.9.4 Contrôle d'accès basé sur les rôles (RBAC)

MyQ X met en œuvre **un contrôle d'accès basé sur les rôles** sophistiqué qui répond aux exigences de sécurité de l'entreprise :

Gestion granulaire des autorisations : le système offre un contrôle détaillé des autorisations des utilisateurs, permettant aux administrateurs de définir des droits

d'accès spécifiques en fonction des rôles et des responsabilités au sein de l'organisation.

Administration basée sur les groupes : la mise en œuvre du RBAC prend en charge à la fois les autorisations individuelles des utilisateurs et le contrôle d'accès basé sur les groupes, ce qui permet une gestion efficace d'un grand nombre d'utilisateurs grâce à l'attribution de groupes de sécurité.

Application du principe du moindre privilège : les contrôles d'accès suivent le principe du moindre privilège, garantissant que les utilisateurs ne reçoivent que les autorisations minimales nécessaires à leurs fonctions tout en maintenant l'efficacité opérationnelle.

2.9.5 Prise en charge multi-locataires Entra ID

MyQ X offre une prise en charge robuste des **environnements multi-locataires Microsoft Entra ID** :

Authentification inter-locataires : le système peut authentifier les utilisateurs sur plusieurs locataires Entra ID, prenant en charge des structures organisationnelles complexes avec plusieurs instances Azure AD.

Isolation des locataires : la prise en charge multi-locataires comprend des mécanismes d'isolation appropriés qui empêchent l'accès aux données entre locataires tout en conservant les capacités de gestion centralisée de MyQ.

Gestion hybride des identités : l'intégration prend en charge à la fois les scénarios d'identité exclusivement cloud et hybrides, s'adaptant aux organisations disposant d'un Active Directory sur site synchronisé avec Entra ID.

2.9.6 Intégration LDAP et Active Directory

MyQ X offre des capacités **d'intégration LDAP et Active Directory** complètes :

Options de synchronisation flexibles : le système prend en charge plusieurs méthodes de synchronisation, notamment la synchronisation complète, la synchronisation sélective des attributs et la synchronisation conditionnelle basée sur des filtres LDAP. Les administrateurs peuvent choisir entre le remplacement complet, l'ajout uniquement ou les mises à jour conditionnelles pour les propriétés des badges et des codes PIN.

Capacités de filtrage avancées : la synchronisation LDAP comprend des options de filtrage sophistiquées utilisant la syntaxe de filtre LDAP standard, permettant

l'importation sélective d'utilisateurs en fonction des unités organisationnelles, des appartenances à des groupes ou des attributs personnalisés.

Importation de la structure des groupes : le système peut importer des structures organisationnelles complètes, y compris des groupes de sécurité, des groupes de distribution et des hiérarchies de groupes imbriqués à partir d'Active Directory, tout en conservant les relations organisationnelles au sein de MyQ.

Authentification sécurisée : toutes les communications LDAP utilisent le cryptage TLS pour protéger les identifiants et les données utilisateur pendant la synchronisation. Le système prend en charge à la fois le LDAP traditionnel sur TLS et les connexions LDAP sécurisées.

2.9.7 Gestion des codes PIN temporaires et politiques de sécurité

MyQ X met en œuvre **des politiques** complètes **de gestion des codes PIN et de sécurité** :

Sécurité renforcée des codes PIN : la version 10.2 introduit une sécurité renforcée des codes PIN, notamment une longueur minimale obligatoire de 6 chiffres et la prévention des combinaisons faciles à deviner telles que « 1234 » ou « 1111 ».

Émission de codes PIN temporaires : le système prend en charge les codes PIN temporaires qui peuvent être émis pour des périodes spécifiques ou des scénarios à usage unique, offrant une sécurité supplémentaire pour l'accès des invités ou des employés temporaires.

Application des politiques relatives aux codes PIN : les politiques configurables relatives aux codes PIN permettent aux organisations de définir des exigences en matière de complexité, des périodes d'expiration et des restrictions de réutilisation conformes aux normes de sécurité de l'entreprise.

Protection en cas d'échec de l'authentification : la sécurité renforcée comprend le blocage automatique des tentatives d'authentification après des échecs répétés (par défaut : blocage de 5 minutes après 5 tentatives infructueuses en 60 secondes).

2.9.8 Prise en charge de l'authentification biométrique

MyQ X exploite **les capacités** modernes **d'authentification biométrique** grâce à l'intégration des appareils mobiles :

Intégration biométrique mobile : le client mobile MyQ X prend en charge les méthodes d'authentification biométrique, notamment Face ID sur les appareils iOS et

la reconnaissance d'empreintes digitales sur les périphériques Android, offrant un contrôle d'accès transparent et sécurisé.

Authentification multimodale : l'authentification biométrique fonctionne en conjonction avec la sécurité basée sur les appareils, créant ainsi un système d'authentification multimodal qui combine quelque chose que l'utilisateur possède (appareil mobile) avec quelque chose qu'il est (caractéristiques biométriques).

2.10 Sécurité des infrastructures

MyQ X offre une sécurité d'infrastructure robuste qui protège l'ensemble de l'environnement de gestion d'impression contre les cybermenaces en constante évolution. La plateforme intègre plusieurs niveaux de défense pour protéger les serveurs, les bases de données, les communications réseau et l'intégrité des logiciels, garantissant ainsi la fiabilité opérationnelle et la confidentialité des données.

2.10.1 Renforcement de la sécurité du Print Server

Les serveurs d'impression MyQ X sont renforcés à l'aide des meilleures pratiques en matière de configuration de sécurité définies dans les paramètres **config.ini**, notamment :

- Restriction des services et des processus afin de limiter la surface d'attaque.
- Activation de protocoles de communication sécurisés et désactivation des options héritées non sécurisées.
- Attribution stricte des privilèges aux utilisateurs, en évitant les privilèges d'administrateur lorsqu'ils ne sont pas nécessaires.
- Mises à jour automatiques régulières et correctifs de sécurité pour corriger les vulnérabilités nouvellement découvertes.
- Configuration de règles de pare-feu et de restrictions de ports pour bloquer le trafic réseau non autorisé.

Ces mesures réduisent le risque d'exploitation et maintiennent la disponibilité du système même en cas d'attaque.

2.10.2 Chiffrement de la base de données (implémentation Firebird 4.0)

MyQ X utilise le moteur de base de données **Firebird 4.0**, qui offre des capacités de chiffrement avancées pour protéger les données sensibles au repos et pendant les opérations de sauvegarde. Les principales fonctionnalités de chiffrement sont les suivantes :

- Chiffrement AES-256 des fichiers de base de données pour empêcher tout accès non autorisé aux données.
- Stockage crypté des mots de passe et des clés dans le système de base de données.
- L'obfuscation du contenu sensible de la base de données dans les journaux et les diagnostics.

Cela garantit la conformité aux réglementations en matière de protection des données et empêche la compromission de la comptabilité des travaux d'impression et des informations utilisateur.

2.10.3 Application de TLS 1.2/1.3 et gestion des certificats

Pour protéger les données en transit, MyQ X applique par défaut le protocole **TLS 1.2** minimum, avec une mise à niveau optionnelle vers TLS 1.3 pour une sécurité et des performances accrues. La plateforme prend en charge des modes de gestion des certificats flexibles :

- Génération automatique d'une autorité de certification (CA) racine privée qui signe les certificats serveur et client.
- Intégration d'autorités de certification intermédiaires gérées par l'organisation, permettant des chaînes de confiance d'entreprise et un contrôle centralisé des certificats.
- Prise en charge de l'installation manuelle de certificats, y compris les certificats d'autorité de certification tierce/publique.

Les certificats et les clés privées sont stockés de manière sécurisée avec une protection cryptée, et les clients reçoivent des certificats de confiance via la stratégie de groupe ou la gestion des appareils mobiles.

2.10.4 Sécurité des communications réseau

MyQ X sécurise tous les canaux de communication réseau en :

- Bloquant tout le trafic HTTP non crypté, en imposant uniquement le protocole HTTPS.
- Chiffrant le trafic SMTP, LDAP et RADIUS à l'aide du protocole TLS afin de protéger l'authentification et le flux de messagerie.
- Désactivant les protocoles obsolètes et vulnérables tels que les remplacements POP3 et STARTTLS.
- Utilisant SNMPv3 avec une authentification forte et des algorithmes cryptographiques pour surveiller et gérer les périphériques en toute sécurité.

Ces contrôles empêchent l'espionnage, l'usurpation d'identité et les attaques de type « man-in-the-middle » sur le réseau.

2.10.5 Configuration du pare-feu et gestion des ports

MyQ X réduit les surfaces d'attaque en :

- Désactivant les règles de pare-feu pour les ports et protocoles réseau inutilisés.
- Permettant un contrôle granulaire des ports exposés en fonction des politiques réseau de l'organisation.

Cela limite les points d'entrée à ceux qui sont essentiels pour les services d'impression, renforçant ainsi les défenses périmétriques.

2.10.6 Sécurité des API et jetons d'authentification

Les API appliquent plusieurs niveaux de sécurité :

- Le cadre d'octroi de codes d'autorisation OAuth 2.0 sécurise l'accès aux API grâce à des jetons porteurs à courte durée de vie et à des restrictions de portée.
- Les jetons sont validés par rapport aux adresses IP des clients et nécessitent des informations d'identification sécurisées.
- Des rotations secrètes périodiques protègent contre les fuites d'informations d'identification.

Cela protège les points de terminaison API contre les demandes non autorisées et les abus.

2.10.7 Isolation des processus et sandboxing

Les applications de gestion d'impression MyQ X fonctionnent avec **une isolation des processus** afin d'empêcher les composants compromis d'affecter l'ensemble du système. Une machine virtuelle ou un bac à sable conteneurisé est utilisé lorsque cela est possible afin de contenir les failles de sécurité et de limiter les mouvements latéraux au sein de l'environnement.

2.10.8 Signature de code et vérification de l'intégrité

Tous les binaires et programmes d'installation du logiciel MyQ sont **signés** afin de garantir leur authenticité et leur intégrité. Cela permet de s'assurer que les clients installent des versions vérifiées du logiciel, exemptes de toute altération ou modification non autorisée.

2.11 Protection des données et cryptage

MyQ X met en œuvre une protection et un cryptage complets des données tout au long du cycle de vie du document, garantissant la confidentialité et l'intégrité depuis la soumission initiale de l'impression jusqu'à la sortie finale et l'archivage.

2.11.1 Mise en œuvre du chiffrement de bout en bout

MyQ X assure **un chiffrement de bout en bout** sur tous les canaux de communication et tous les points de stockage des données :

Canaux de communication cryptés : tout le trafic réseau utilise par défaut le cryptage TLS obligatoire, avec une version minimale de 1.2. Le protocole HTTPS est appliqué à toutes les interfaces web, aux communications de serveur à serveur et aux connexions client.

Sécurité basée sur des certificats : plusieurs modes de gestion des certificats prennent en charge les exigences organisationnelles, de l'autorité de certification embarquée à l'intégration PKI d'entreprise et aux certificats CA publics. Les clés privées sont protégées par des mots de passe générés aléatoirement et stockés sous forme cryptée dans la base de données Firebird.

Sécurité des protocoles : le cryptage TLS est appliqué aux protocoles SMTP, LDAP, RADIUS et SNMP, garantissant qu'aucune donnée sensible n'est transmise en clair.

2.11.2 Chiffrement des données au repos

MyQ X protège les données stockées grâce à plusieurs couches de chiffrement :

Chiffrement de la base de données : la base de données Firebird 4.0 prend en charge le chiffrement à l'aide de certificats personnalisés avec l'utilisation de clés améliorée (EKU) « Encrypting File System ». Les certificats doivent être stockés dans des magasins de certificats informatiques désignés, le magasin personnel étant préféré.

Protection du système de fichiers : les fichiers de travaux d'impression et de numérisation stockés sur le Print Server MyQ X peuvent être cryptés à l'aide de certificats personnalisés fournis par les administrateurs, ajoutant ainsi une couche de protection supplémentaire au-delà des autorisations du système de fichiers.

Chiffrement complet du disque : MyQ X prend en charge l'intégration avec des technologies de chiffrement complet du disque telles que Microsoft BitLocker afin

de protéger toutes les données au repos sur le Print Server, y compris la base de données, les certificats et les fichiers temporaires.

2.11.3 Protection des données en transit (cryptage TLS)

MyQ X applique **des normes de chiffrement TLS** strictes pour toutes les communications réseau :

TLS 1.2 minimum : la configuration par défaut nécessite au minimum TLS 1.2, avec une mise à niveau optionnelle vers TLS 1.3 pour une sécurité et des performances accrues. Les protocoles hérités, notamment SSL et les anciennes versions de TLS, sont bloqués.

Gestion des suites de chiffrement : le système met en œuvre des suites de chiffrement robustes et désactive les algorithmes vulnérables afin de prévenir les attaques cryptographiques. Les communications SNMPv3 utilisent le chiffrement SHA1 et AES.

Validation des certificats : toutes les connexions TLS nécessitent une validation appropriée des certificats à l'aide de noms de domaine complets (FQDN) afin d'empêcher les attaques de type « man-in-the-middle ». START TLS est évité en raison des vulnérabilités MITM.

2.11.4 Chiffrement des travaux d'impression et stockage sécurisé

MyQ X fournit plusieurs mécanismes pour protéger les travaux d'impression tout au long de leur cycle de vie :

Libération sécurisée des impressions : les travaux d'impression sont stockés en toute sécurité sur le serveur MyQ jusqu'à ce que les utilisateurs s'authentifient sur l'appareil, ce qui empêche tout accès non autorisé aux documents se trouvant dans les bacs de sortie de l'imprimante.

Chiffrement des fichiers de travail : les administrateurs peuvent activer le chiffrement des travaux en fournissant des certificats personnalisés, garantissant ainsi que les fichiers de travail restent chiffrés lorsqu'ils sont stockés sur le serveur en attendant leur libération.

Files d'impression privées : pour les documents hautement confidentiels, les files d'impression privées suppriment automatiquement les travaux d'impression immédiatement après leur libération, éliminant ainsi le risque d'accès non autorisé prolongé.

Mode confidentialité : lorsqu'il est activé, le mode confidentialité masque les noms des documents à tous les utilisateurs, à l'exception du propriétaire du document, empêchant ainsi la divulgation d'informations par le biais des noms des travaux. Même les administrateurs ne peuvent pas voir les noms des travaux des autres utilisateurs.

2.11.5 Améliorations du chiffrement de la base de données

La mise en œuvre de la base de données **Firebird 4.0** offre des capacités de chiffrement avancées :

Chiffrement par certificat personnalisé : les fichiers de base de données sont chiffrés à l'aide de certificats avec EFS Extended Key Usage, offrant une protection solide contre les accès non autorisés à la base de données.

Protection par mot de passe : les mots de passe de la base de données sont masqués dans les fichiers journaux, ce qui empêche l'exposition des informations d'identification lors des activités de dépannage et de surveillance.

Renforcement des autorisations : le dossier de données MyQ, qui contient la base de données des utilisateurs et les clés privées des certificats TLS, est réservé aux administrateurs, au SYSTÈME et au compte de service MyQ, supprimant ainsi l'accès en lecture par défaut pour tous les utilisateurs.

2.11.6 Chiffrement des sauvegardes et stockage sécurisé

MyQ X garantit que les sauvegardes maintiennent le même niveau de sécurité que les données de production :

Sauvegardes cryptées : les sauvegardes de la base de données sont protégées par des mots de passe sécurisés générés de manière aléatoire qui empêchent toute restauration ou tout accès non autorisé aux fichiers de sauvegarde.

Stockage sécurisé des sauvegardes : les fichiers de sauvegarde doivent être stockés dans des emplacements sécurisés avec des contrôles d'accès appropriés et un chiffrement au repos afin de préserver la confidentialité des données pendant le cycle de vie de la sauvegarde.

2.11.7 Politiques de gestion et de rotation des clés

MyQ X met en œuvre des pratiques de gestion sécurisée des clés :

Rotation des certificats : les certificats peuvent être régulièrement renouvelés conformément aux politiques de sécurité de l'organisation, avec prise en charge du

déploiement automatisé via la stratégie de groupe ou la gestion des appareils mobiles.

Protection des clés privées : toutes les clés privées pour les certificats et les opérations CA sont protégées par des mots de passe générés de manière aléatoire et stockés sous forme cryptée dans la base de données.

Rotation des secrets API : les secrets client REST API doivent faire l'objet d'une rotation périodique afin de maintenir la sécurité. Le système prend en charge le renouvellement des secrets sans interruption de service.

2.11.8 Minimisation des données et confidentialité dès la conception

MyQ X met en œuvre **les principes de confidentialité dès la conception conformes au RGPD** :

Collecte de données limitée : le système ne collecte que les métadonnées essentielles nécessaires au fonctionnement opérationnel, évitant ainsi le traitement inutile de données personnelles qui pourrait augmenter les risques liés à la confidentialité.

Suppression automatique : les administrateurs peuvent configurer des périodes de suppression automatique pour les fichiers d'impression et de numérisation, garantissant ainsi que les données ne sont conservées que pendant la durée nécessaire à des fins professionnelles.

Droits des utilisateurs sur leurs données : mise en œuvre complète des droits des utilisateurs prévus par le RGPD, notamment l'accès aux données, l'anonymisation et le droit à l'oubli, avec des avis de confidentialité personnalisables sur les interfaces utilisateur.

Gestion des sessions : la fonctionnalité de déconnexion automatique garantit que les sessions des utilisateurs sont correctement terminées, empêchant ainsi tout accès non autorisé via des sessions abandonnées.

Ce cadre complet de protection et de cryptage des données garantit que MyQ X maintient les normes les plus élevées en matière de confidentialité et d'intégrité des données, tout en prenant en charge les exigences de conformité réglementaire dans divers environnements organisationnels.

2.12 Flux d’impression sécurisés

MyQ X fournit des flux de travail d'impression sécurisés complets qui permettent à l'utilisateur de contrôler entièrement la publication des documents tout en empêchant l'exposition d'informations sensibles dans les bacs de sortie des imprimantes. Ces flux de travail sont essentiels pour les organisations qui exigent une sécurité stricte des documents et une responsabilité des utilisateurs.

2.12.1 Mise en œuvre de la libération sécurisée des impressions

La **fonction Hold Print** garantit que les travaux d'impression ne sont jamais immédiatement transmis à l'imprimante. Les documents sont stockés en toute sécurité sur le serveur MyQ et ne sont imprimés qu'après authentification de l'utilisateur autorisé sur le périphérique d'impression, ce qui empêche que des documents sans surveillance ne soient laissés dans les bacs de sortie.

La fonction **impression sécurisée** va encore plus loin en permettant aux utilisateurs de libérer leurs travaux sur n'importe quel périphérique compatible du système d'impression, et pas seulement sur l'appareil auquel ils ont initialement envoyé le travail. Cette flexibilité est particulièrement utile lors de la maintenance des équipements ou lorsque les utilisateurs doivent imprimer à partir de différents endroits.

Plusieurs méthodes d'authentification prennent en charge la fonction Secure Print Release, notamment les codes PIN, les badges, les mots de passe, les codes QR avec vérification biométrique et les combinaisons d'authentification à deux facteurs. Cette flexibilité permet de répondre aux diverses exigences de sécurité des organisations.

2.12.2 Workflows d'impression sécurisée

Impression sécurisée offre des avantages significatifs tant pour les administrateurs que pour les utilisateurs finaux :

Avantages administratifs :

- Éliminez les piles de documents laissés sans surveillance sur les imprimantes de bureau
- Appliquez des comportements d'impression responsables et des politiques de sécurité des documents
- Gestion de toutes les impressions via une file d'impression unique et unifiée

- Réduction du gaspillage d'impression et des coûts associés grâce aux options de prévisualisation et de réglage
- Prise en charge de l'impression flexible sur plusieurs périphériques

Avantages pour l'utilisateur :

- Les documents confidentiels restent sécurisés jusqu'à leur publication explicite
- Imprimez sur n'importe quel périphérique autorisé au sein de l'organisation
- Prévisualisez les documents sur le terminal intégré avant leur publication
- Modification des options d'impression (couleur, recto verso, finition) même après l'envoi des travaux
- Modification des destinations d'impression sur les périphériques si l'imprimante d'origine n'est pas disponible

2.12.3 Délai d'expiration des travaux d'impression et suppression automatique

MyQ X met en œuvre des procédures de nettoyage automatique pour éviter l'exposition prolongée des documents :

Périodes de conservation configurables : les administrateurs définissent la durée de conservation des fichiers de travaux d'impression sur le serveur MyQ avant leur suppression automatique, en trouvant le juste équilibre entre les exigences opérationnelles et les besoins en matière de sécurité.

Gestion du délai d'expiration des travaux : les travaux qui ne sont pas lancés dans les délais spécifiés sont automatiquement supprimés de la file d'attente, ce qui empêche l'accumulation de documents oubliés ou abandonnés sur les serveurs.

Déconnexion automatique : les sessions sur les périphériques expirent automatiquement après des périodes définies par l'administrateur, ce qui empêche l'accès non autorisé aux documents sur les terminaux abandonnés.

2.12.4 Filigranes et signatures numériques

Le filigrane permet la traçabilité des documents en ajoutant des superpositions personnalisables aux pages imprimées, qui peuvent inclure :

- Des mentions de confidentialité
- Dates et horodatages d'impression
- Le nom de la personne qui imprime le document
- Informations d'identification de l'imprimante

Ces filigranes peuvent être appliqués à toutes les pages ou à certaines pages sélectionnées, créant ainsi une piste d'audit qui permet d'identifier les documents divulgués et de remonter jusqu'à leur source.

2.12.5 Aperçu avant impression et validation du contenu

Le moteur **d'aperçu avant impression** permet aux administrateurs de vérifier les travaux d'impression avant leur lancement :

Formats pris en charge : la fonctionnalité d'aperçu prend en charge les trois langages de description de page les plus courants : PCL 5, PCL 6 et PostScript.

Contrôle préventif : les administrateurs peuvent rejeter les travaux d'impression non autorisés avant qu'ils n'atteignent le périphérique d'impression, ce qui permet d'éviter les violations de politique et de protéger les informations sensibles.

Filtrage basé sur le contenu : l'intégration avec les systèmes OCR et de gestion de documents permet d'appliquer des politiques de numérisation basées sur l'analyse du contenu des documents.

2.12.6 Gestion des erreurs et récupération sécurisée des travaux

MyQ X met en œuvre une gestion robuste des erreurs afin de maintenir la sécurité en cas de dysfonctionnement des périphériques :

Protection contre les erreurs de périphériques : lorsqu'un périphérique d'impression entre en état d'erreur (bourrage papier, toner épuisé), les documents sont conservés plutôt que d'être automatiquement imprimés une fois l'erreur résolue, ce qui permet à l'utilisateur de contrôler le moment de la libération.

Préservation de la session : si un périphérique devient indisponible en cours de session, le système MyQ préserve la session utilisateur et permet de la poursuivre sur d'autres périphériques sans perdre l'état du document.

Déconnexion automatique du périphérique : en cas d'erreur du périphérique, la déconnexion automatique efface la mémoire du périphérique afin d'empêcher tout accès non autorisé aux documents par le personnel de maintenance ou d'autres utilisateurs.

Cette architecture complète de flux de travail d'impression sécurisée garantit aux organisations un contrôle strict de la sécurité des documents tout au long du cycle de vie de l'impression, tout en favorisant la flexibilité opérationnelle et la productivité des utilisateurs.

2.13 Sécurité des périphériques et des réseaux

MyQ X fournit des contrôles de sécurité complets pour les périphériques et les réseaux afin de protéger les appareils multifonctions (MFD), les imprimantes et l'infrastructure réseau contre tout accès et toute exploitation non autorisés.

2.13.1 Renforcement de la sécurité des périphériques multifonctions

Les organisations qui déploient MyQ X avec des MFD doivent mettre en œuvre les meilleures pratiques en matière de sécurité, notamment

Contrôles d'accès aux périphériques : limiter l'accès physique aux imprimantes aux seuls emplacements et personnels autorisés, afin de réduire les risques de falsification ou de vol.

Désactivation des protocoles inutilisés : désactivez les protocoles et services inutiles qui ne sont pas requis par MyQ X, afin de réduire la surface d'attaque de chaque périphérique.

Gestion des identifiants par défaut : remplacez tous les mots de passe administrateur par défaut des périphériques par des identifiants forts générés de manière aléatoire. Les paramètres d'usine par défaut sont généralement connus des pirates.

Protection du disque dur interne : si les périphériques prennent en charge le stockage interne des travaux d'impression pour les réimprimer, mettez en place un cryptage (AES) et des fonctions de réécriture automatique des données afin d'empêcher tout accès non autorisé aux documents stockés.

2.13.2 Segmentation du réseau et configuration VLAN

MyQ X prend en charge les stratégies de segmentation du réseau afin de limiter les risques de compromission des périphériques :

Isolation VLAN : séparez le trafic réseau des imprimantes et des périphériques des réseaux généraux des utilisateurs et des administrateurs à l'aide de réseaux locaux virtuels, limitant ainsi les mouvements latéraux si un périphérique est compromis.

Sous-réseaux et listes de contrôle d'accès : mettez en place des contrôles d'accès au niveau du réseau à l'aide de listes de contrôle d'accès (ACL) afin de garantir que seuls les systèmes autorisés peuvent communiquer avec les périphériques d'impression et les serveurs.

Règles de pare-feu : bloquez le trafic entrant et sortant inutile des sous-réseaux d'imprimantes, en limitant la connectivité aux seuls services essentiels et en empêchant les périphériques infectés d'accéder aux autres ressources du réseau.

Application des noms de domaine complets : toutes les communications réseau doivent utiliser des noms de domaine complets (FQDN) plutôt que des adresses IP ou des noms d'hôte courts, afin d'empêcher les attaques de type « man-in-the-middle » basées sur le DNS et de garantir une validation correcte des certificats.

2.13.3 Mise en œuvre de la sécurité SNMP v3

MyQ X applique les protocoles **SNMPv3** modernes avec un cryptage puissant pour la gestion des périphériques :

Interdiction du protocole SNMPv1 non sécurisé : les communications SNMPv1 héritées doivent être entièrement désactivées, car elles transmettent les informations d'identification en texte clair et ne sont pas cryptées.

Configuration SNMPv3 : toutes les communications SNMP doivent utiliser SNMPv3 avec :

- Des mots de passe forts, générés de manière aléatoire, pour l'authentification
- Algorithmes de hachage SHA1 ou plus puissants
- Un cryptage AES pour la confidentialité des données
- Des identifiants uniques par périphérique, spécifiques à chaque déploiement MyQ

2.13.4 Gestion des identifiants d'imprimante

MyQ X reconnaît que **la gestion des identifiants d'imprimante est spécifique au fournisseur** et nécessite une mise en œuvre côté client :

Exigences en matière de mots de passe forts : toutes les informations d'identification administratives des imprimantes doivent utiliser des mots de passe forts, générés de manière aléatoire, plutôt que des informations d'identification par défaut ou simples.

Rotation des identifiants : mettez régulièrement à jour les mots de passe des imprimantes conformément aux politiques de sécurité de l'organisation afin de réduire le risque de compromission des identifiants.

Restrictions d'accès : limitez l'accès à la gestion des imprimantes au personnel autorisé uniquement grâce à des règles de pare-feu, des contrôles d'accès physique et des autorisations basées sur les rôles.

2.13.5 Sécurité du micrologiciel et gestion des mises à jour

La mise à jour du micrologiciel des périphériques est essentielle pour la sécurité :

Mises à jour automatiques : configurez les périphériques pour qu'ils reçoivent et appliquent automatiquement les mises à jour du micrologiciel du fabricant qui corrigent les failles de sécurité récemment découvertes.

Avis de sécurité des fournisseurs : surveillez les notifications de sécurité des fabricants concernant les vulnérabilités critiques affectant les périphériques déployés et appliquez rapidement les correctifs.

Test des mises à jour : testez les mises à jour du micrologiciel dans des environnements hors production avant de les déployer sur les imprimantes de production afin de garantir leur compatibilité et leur fonctionnalité.

2.13.6 Gestion et restrictions des ports USB

MyQ X prend en charge les contrôles administratifs pour la connectivité USB des périphériques :

Désactivation des ports USB : les administrateurs doivent désactiver les ports USB entrants sur les imprimantes multifonctions afin d'empêcher :

- L'impression directe via USB, contournant les contrôles de sécurité MyQ
- L'accès direct aux disques durs des périphériques et aux données stockées
- L'utilisation non autorisée des fonctionnalités des périphériques

Alternatives d'impression directe sécurisée : n'autorisez que les méthodes d'impression sécurisées approuvées (IPP/S, AirPrint avec intégration MyQ) tout en bloquant l'accès USB direct non sécurisé.

Ce cadre complet de sécurité des périphériques et du réseau garantit que les périphériques d'impression restent des composants sécurisés de l'infrastructure MyQ X tout en maintenant l'efficacité opérationnelle et la sécurité de l'organisation.

2.14 Audit et suivi

MyQ X offre des fonctionnalités complètes d'audit et de surveillance qui permettent aux administrateurs de garder une visibilité sur les opérations d'impression, de détecter les incidents de sécurité et de garantir la conformité avec les politiques et réglementations de l'organisation.

2.14.1 Surveillance et alertes en temps réel

MyQ X surveille tous les composants de l'infrastructure d'impression en temps réel via plusieurs canaux de surveillance :

Surveillance de l'état des périphériques : surveillance continue de l'état des imprimantes et des périphériques multifonctions, y compris les niveaux de toner, la disponibilité du papier, les conditions d'erreur et la connectivité des périphériques. Les administrateurs reçoivent immédiatement des informations sur l'état de santé et le statut opérationnel des périphériques.

Gestion des alertes : des alertes automatisées informent les administrateurs des événements critiques, notamment les erreurs des périphériques, les niveaux de consommables bas, les problèmes de connectivité et autres problèmes opérationnels. Les notifications d'alerte peuvent être envoyées par e-mail ou intégrées à l'Observateur d'événements Windows.

Notifications d'événements : des notifications personnalisables basées sur les événements déclenchent des actions en réponse à des conditions spécifiques de l'appareil ou du système, permettant ainsi de résoudre les problèmes de manière proactive avant qu'ils n'aient un impact sur les opérations.

2.14.2 Enregistrement et analyse des activités d'impression

MyQ X conserve **des pistes d'audit détaillées de toutes les activités d'impression, de copie, de numérisation et de télécopie** :

Comptabilité basée sur les travaux : la comptabilité avancée suit chaque travail indépendamment, ce qui permet une attribution détaillée à des utilisateurs, des périphériques, des projets et des centres de coûts spécifiques. Les travaux effectués au cours d'une seule session utilisateur sont comptabilisés séparément, ce qui fournit des données d'utilisation précises.

Métadonnées d'activité : la journalisation complète enregistre la date de soumission du travail, la date de publication du travail, l'identification du périphérique, le format du papier, les paramètres recto/recto verso, les paramètres de couleur et tous les autres paramètres pertinents du travail.

Journal MyQ : le journal système en temps réel affiche toutes les activités du serveur, y compris les événements système, les erreurs, les avertissements, les tentatives d'authentification, les modifications de configuration et les actions administratives. Les messages du journal sont classés par gravité (critique, erreur,

avertissement, info, remarque, débogage, trace) et peuvent être filtrés par période et sous-système.

2.14.3 Analyse du comportement des utilisateurs

MyQ X offre des capacités d'analyse sophistiquées pour comprendre les habitudes d'impression et détecter les anomalies :

Génération de rapports personnalisés : des fonctionnalités de reporting avancées permettent aux administrateurs de créer des rapports personnalisés basés sur n'importe quelle combinaison de paramètres suivis, ce qui permet d'analyser le comportement d'impression par utilisateur, service, projet, périphérique ou période.

Suivi des centres de coûts : l'attribution détaillée des travaux d'impression aux centres de coûts, aux projets et aux groupes d'utilisateurs permet un reporting transparent des dépenses et facilite la prise de décisions éclairées concernant les politiques d'impression.

Surveillance du comportement : les administrateurs peuvent analyser les habitudes d'impression afin d'identifier les activités inhabituelles, les utilisations excessives ou les violations des politiques qui justifient une enquête plus approfondie.

2.14.4 Détection et réponse aux incidents

MyQ X prend en charge la surveillance axée sur la sécurité grâce à une journalisation et des alertes structurées :

Journalisation des échecs d'authentification : la journalisation améliorée des tentatives d'authentification, en particulier des échecs de connexion, permet aux administrateurs de détecter les menaces potentielles pour la sécurité et d'y répondre. Depuis la version 10.2, les enregistrements des tentatives de connexion ont été améliorés pour faciliter le filtrage dans le journal MyQ.

Règles de notification des journaux : des règles personnalisables déclenchent des notifications automatisées en fonction de types d'événements, de sous-systèmes et de modèles de messages spécifiques, ce qui permet une détection rapide des événements liés à la sécurité. Les règles peuvent utiliser des expressions régulières pour rechercher des modèles spécifiques dans les messages des journaux.

Alertes d'événements critiques : le système alerte automatiquement les administrateurs en cas d'événements critiques, notamment les violations de sécurité, les échecs d'authentification, les tentatives d'accès non autorisées et les modifications de configuration.

2.14.5 Politiques de conservation et d'archivage des journaux

MyQ X met en œuvre une gestion flexible des journaux afin d'équilibrer les besoins opérationnels et les exigences de conformité :

Périodes de conservation configurables : les administrateurs définissent le nombre de jours avant la suppression automatique des journaux, en alignant la conservation sur les politiques de gouvernance des données de l'organisation et les exigences réglementaires.

Exportation et archivage des journaux : les journaux peuvent être exportés au format Excel ou CSV pour être stockés et analysés en externe. Les exportations planifiées permettent l'archivage automatisé des journaux à intervalles réguliers.

Conservation à long terme : les journaux exportés peuvent être stockés dans des référentiels sécurisés et cryptés afin de conserver les enregistrements historiques à des fins d'audit, de vérification de la conformité et d'enquête sur les incidents.

2.14.6 Fonctionnalités avancées de filtrage et de recherche

MyQ X fournit des outils sophistiqués pour l'analyse et l'investigation des journaux :

Recherches enregistrées : les administrateurs peuvent créer, enregistrer et partager des filtres de recherche couramment utilisés pour accéder rapidement aux données de journal pertinentes. Les recherches enregistrées peuvent être organisées en dossiers pour faciliter leur gestion.

Filtrage par période : filtrez les journaux par plages de dates spécifiques ou périodes prédéfinies afin de concentrer l'analyse sur les périodes pertinentes.

Filtrage par sous-système et contexte : effectuez des recherches par sous-systèmes MyQ spécifiques (interface utilisateur Web, terminal, serveur SMTP, etc.) et contextes (impression directe, périphériques spécifiques) afin d'isoler les événements pertinents.

Contrôle de la verbosité : sélectionnez les niveaux de gravité des journaux (critique, erreur, avertissement, info, etc.) à afficher, afin de réduire le bruit et de vous concentrer sur les événements importants.

2.14.7 Journal d'audit pour les actions administratives

MyQ X suit toutes les modifications administratives grâce à un **journal d'audit** dédié :

Modifications de configuration : enregistre toutes les modifications apportées aux paramètres MyQ, y compris qui a effectué la modification, quand elle a été effectuée et quel composant du système a été affecté.

Gestion des droits des utilisateurs : suivi détaillé des modifications apportées aux autorisations des utilisateurs, aux appartenances à des groupes et aux contrôles d'accès, avec la possibilité de consulter des informations détaillées sur chaque modification.

Gestion des codes PIN et des identifiants : suivi amélioré des ajouts, suppressions et modifications de codes PIN afin de surveiller le cycle de vie des identifiants.

Capacités d'exportation : les journaux d'audit peuvent être exportés à la demande ou programmés pour une exportation automatisée régulière, ce qui facilite la conformité aux exigences en matière de rapports et de conservation des enregistrements.

Ce cadre complet d'audit et de surveillance garantit que MyQ X offre aux administrateurs la visibilité nécessaire pour maintenir la sécurité, détecter les menaces, assurer la conformité aux politiques et résoudre efficacement les problèmes opérationnels.

2.15 Réponse aux incidents et récupération

MyQ X offre des capacités complètes de réponse aux incidents et de récupération, conçues pour maintenir la continuité des activités pendant les interruptions prévues et imprévues. La plateforme combine des procédures de sauvegarde automatisées, des fonctionnalités de haute disponibilité et des mécanismes de basculement flexibles pour garantir le fonctionnement des services d'impression même en cas de panne du système.

2.15.1 Procédures de réponse aux incidents de sécurité

MyQ X prend en charge la réponse structurée aux incidents grâce à plusieurs mécanismes de surveillance et d'alerte :

Détection des incidents en temps réel : la surveillance automatisée suit en permanence l'état du système, les échecs d'authentification, les changements de configuration et les événements de sécurité, ce qui permet de détecter rapidement les incidents de sécurité potentiels.

Escalade des alertes : des règles de notification de journaux configurables déclenchent des notifications immédiates aux administrateurs lorsque des

événements de sécurité critiques se produisent, notamment des tentatives d'authentification échouées, des tentatives d'accès non autorisées et des anomalies du système.

Conservation des pistes d'audit : la journalisation complète de toutes les activités du système garantit la disponibilité de données d'analyse complètes pour les enquêtes sur les incidents. Le journal d'audit MyQ suit toutes les actions administratives, les modifications de configuration et les activités des utilisateurs.

Procédures de confinement : en cas d'incident de sécurité, les administrateurs peuvent rapidement isoler les composants affectés, désactiver les comptes compromis et mettre en œuvre des contrôles d'accès d'urgence.

2.15.2 Procédures de récupération et de restauration

MyQ X met en œuvre de solides capacités de sauvegarde et de restauration afin de garantir une récupération rapide en cas de panne du système ou de perte de données :

Sauvegarde automatisée de la base de données : des sauvegardes automatisées régulières de la base de données MyQ capturent toutes les données de configuration, les informations utilisateur et les paramètres système. Les sauvegardes sont protégées par un cryptage par mot de passe et stockées en toute sécurité.

Restauration complète du système : le processus de restauration récupère l'environnement MyQ complet, y compris la base de données, les certificats, les fichiers de configuration et les rapports. Les administrateurs sélectionnent simplement le fichier de sauvegarde et fournissent le mot de passe s'il est protégé.

Sauvegarde et restauration prises en charge par le cluster : pour les déploiements à haute disponibilité utilisant Microsoft Failover Clustering, MyQ prend en charge la sauvegarde vers un stockage partagé en cluster et la restauration coordonnée sur tous les nœuds du cluster.

2.15.3 Haute disponibilité et basculement

MyQ X propose plusieurs stratégies de basculement pour maintenir les opérations d'impression pendant les temps d'arrêt du serveur :

Intégration du clustering de basculement Microsoft : MyQ X se déploie dans des configurations actives-passives au sein des clusters de basculement Microsoft Windows Server. Le logiciel de cluster surveille en permanence l'état des nœuds et

bascule automatiquement vers les nœuds passifs lorsque le nœud actif devient indisponible.

Impression de secours : lorsque le client de bureau MyQ détecte une perte de connexion au serveur, il redirige automatiquement les travaux d'impression vers des imprimantes de secours préconfigurées. Une fois la connectivité du serveur rétablie, la comptabilité des travaux est automatiquement mise à jour.

Mise en file d'attente des périphériques : les travaux d'impression peuvent être stockés de manière cryptée dans la mémoire des périphériques pendant les pannes de serveur. Lorsque la connectivité est rétablie, les périphériques transmettent automatiquement les données de comptabilité au serveur.

Connexion hors ligne : les terminaux intégrés MyQ X mettent en cache les informations d'authentification des utilisateurs, ce qui leur permet de se connecter et d'accéder aux fonctionnalités des périphériques même lorsque le serveur n'est pas disponible.

Mise en file d'attente client : les travaux sont traités localement sur les postes de travail des utilisateurs et stockés sur leurs ordinateurs plutôt que sur le serveur, ce qui réduit considérablement les besoins en bande passante et permet d'imprimer pendant la maintenance du serveur ou en cas de problèmes réseau.

2.15.4 Analyse et amélioration après incident

MyQ X prend en charge l'amélioration continue des capacités de réponse aux incidents grâce à des outils d'analyse complets :

Analyse des journaux historiques : les administrateurs peuvent examiner les journaux exportés pour comprendre la séquence d'événements ayant conduit à un incident, identifier les causes profondes et déterminer les mesures correctives appropriées.

Examen de la piste d'audit : le journal d'audit offre une visibilité complète sur toutes les actions administratives et les modifications de configuration qui ont pu contribuer à des incidents de sécurité ou les avoir précédés.

Modèles de recherche enregistrés : les administrateurs peuvent créer et enregistrer des filtres de recherche dans les journaux pour les modèles d'incidents courants, ce qui permet d'identifier rapidement des événements similaires à l'avenir.

3 MyQ X et NIS2

La directive (UE) 2022/2555, plus connue sous le nom de **NIS2**, constitue une avancée significative vers la mise en place d'un niveau commun de cybersécurité dans l'ensemble de l'Union européenne. Cette directive, entrée en vigueur le 16 janvier 2023, vise à renforcer la **résilience des services essentiels** et **des** fournisseurs de services numériques face aux cybermenaces en instaurant **des normes et des pratiques** cohérentes **en matière de cybersécurité**.

Le secteur de l'imprimerie, à l'instar de nombreux autres, relève du champ d'application de la directive NIS2. Par conséquent, les entités du secteur de l'imprimerie doivent comprendre les implications de la directive NIS2 et prendre les mesures nécessaires pour se conformer aux normes de sécurité. D'ici le 17 octobre 2024, les États membres sont tenus d'adopter et de publier les mesures indispensables au respect de la directive NIS2.

Cet article examine en détail la directive NIS2 et ses implications pour les distributeurs et les clients de MyQ X.

Si vous êtes un client final de MyQ X, discutez des exigences et des recommandations de la directive NIS2 avec votre fournisseur ou distributeur MyQ X. Les partenaires MyQ sont formés pour offrir une assistance de haut niveau et vous aideront à mettre en œuvre les mesures nécessaires.

3.1 Principaux domaines de la directive NIS2

3.1.1 Gestion des risques et cybersécurité

Adoptez une approche de gestion des risques en matière de cybersécurité. Cela implique d'identifier et d'évaluer les risques pesant sur les réseaux et les systèmes d'information, de mettre en œuvre des mesures visant à atténuer ces risques et de réexaminer régulièrement ces mesures.

Assurez-vous que votre serveur et les logiciels associés sont **à jour avec les derniers correctifs de sécurité** afin de limiter les vulnérabilités. De plus, mettez en œuvre et testez régulièrement des plans de sauvegarde et de reprise après sinistre afin de garantir la disponibilité et l'intégrité des données. MyQ publie régulièrement des correctifs pour ses produits. Il est fortement recommandé de vous tenir informé, de suivre ces publications et de définir à l'avance votre stratégie et votre procédure de

mise à jour. MyQ génère une **liste des composants logiciels (SBOM)** pour chaque version, accessible via votre fournisseur/distributeur MyQ, ce qui permet aux organisations d'analyser les composants utilisés dans le logiciel afin de détecter d'éventuelles failles de sécurité.

La segmentation du réseau est un outil essentiel pour mettre en œuvre concrètement une politique « Zero Trust ». Elle offre aux organisations les moyens de contrôler leurs réseaux à l'aide de politiques de sécurité plus granulaires. Elle garantit que, même si un attaquant compromet une partie du réseau, il ne peut pas se déplacer latéralement vers d'autres zones. Cependant, les organisations disposant d'environnements segmentés sont confrontées à des défis pour rendre l'impression facilement accessible.

Avec MyQ X, les files d'impression peuvent être propagées dans des réseaux segmentés grâce aux Mobile Print Agents, et les documents hébergés dans le cloud peuvent être téléchargés et lancés immédiatement depuis l'écran du périphérique avec Easy Print. La prise en charge de Microsoft Universal Print ou d'Application Proxy dans le client mobile peut considérablement aider les organisations à mettre en place des services d'impression dans l'ensemble de leur environnement, tout en garantissant la protection de l'accès à ces ressources.

Les certificats SSL pour des connexions sécurisées permettent de répondre aux exigences de la norme NIS2 en matière de transmission sécurisée des données sur les réseaux. MyQ X est livré prêt à l'emploi avec une communication sécurisée activée grâce à l'autorité de certification embarquée. Les organisations utilisant une infrastructure PKI d'entreprise peuvent atteindre un niveau de sécurité des communications encore plus élevé en fournissant directement des certificats personnalisés.

Dans la mesure du possible, **imposez l'utilisation du protocole TLS** pour les communications avec d'autres systèmes. Sécurisez la connexion à Active Directory ou à d'autres annuaires d'utilisateurs à l'aide du protocole LDAPS. Assurez-vous que la transmission des e-mails s'effectue via SMTPS et vérifiez tous les paramètres de la page « Réseau » de MyQ X ainsi que de l'onglet « Sécurité » d'Easy Config (par exemple, que le serveur Web n'autorise que les connexions sécurisées).

MyQ offre également la possibilité de **chiffrer les bases de données, les numérisations et les travaux d'impression**. Le chiffrement des données est essentiel pour garantir la confidentialité et l'intégrité des informations sensibles, ce qui constitue un aspect clé de la conformité à la norme NIS2.

En ce qui concerne la communication entre les périphériques, il est essentiel de mettre en œuvre des protocoles de communication offrant le plus haut niveau de sécurité. Il est vivement recommandé d'utiliser **SNMPv3** plutôt que les versions v1 ou v2(c) pour surveiller et gérer l'état et les fonctionnalités des périphériques sur un réseau.

3.1.2 Continuité des activités et gestion de crise

> Les organisations doivent s'assurer que leurs opérations peuvent se poursuivre en cas de perturbation majeure.

Mettez en place **des serveurs redondants ou des systèmes de basculement** pour garantir la disponibilité des services d'impression en cas d'incident. MyQ X permet la mise en œuvre de mesures de basculement à l'aide de plusieurs méthodes.

MyQ prend en charge **le clustering de basculement Windows Server** pour une haute disponibilité : si le nœud actif tombe en panne, le cluster transfère les services MyQ vers un nœud de secours. Les déploiements virtualisés peuvent également utiliser la haute disponibilité (HA) de l'hyperviseur pour redémarrer la machine virtuelle MyQ sur un autre hôte.

En cas de perte de connexion au serveur MyQ, la fonctionnalité **d'impression de secours (Fallback Printing)** du Client Desktop MyQ envoie les travaux d'impression directement vers un périphérique de secours configuré, permettant ainsi aux utilisateurs de continuer à imprimer pendant une panne du serveur. Sur les périphériques Kyocera et Ricoh pris en charge, **la mise en file d'attente des travaux (Device Spooling),** combinée à **la connexion hors ligne (Offline Login),** permet aux utilisateurs de se connecter et de lancer des travaux directement sur le périphérique lorsque le serveur est indisponible. Les fonctionnalités qui dépendent du serveur, telles que les flux de travail de numérisation MyQ, le crédit et le quota, ne sont pas disponibles tant que le serveur n'est pas à nouveau accessible.

Les sauvegardes régulières **de la base de données** et la possibilité de restaurer les données MyQ sont conformes aux exigences de la norme NIS2 visant à garantir la disponibilité et la résilience des données face aux cyberattaques ou aux pannes du système. Les sauvegardes de la base de données et des journaux peuvent être planifiées avec MyQ X et effectuées automatiquement, y compris celles de la base de données SQL du Central Server.

Pour plus d'informations, consultez :

- Résilience, solution de secours et haute disponibilité
- Stratégie de mise en file d'attente

3.1.3 Modèle d'accès au principe du moindre privilège

> Les utilisateurs ne doivent se voir accorder que le niveau d'accès ou les autorisations minimales nécessaires pour effectuer les opérations requises.

NIS2 encourage **la séparation des tâches** afin d'empêcher tout accès non autorisé aux systèmes critiques.

En attribuant **des droits d'accès spécifiques** à la gestion du système et des utilisateurs, à la gestion des travaux, aux rapports ou aux journaux, il est possible d'accorder à certains utilisateurs un accès à privilèges élevés à des zones particulières de l'environnement MyQ, tout en limitant les droits d'accès des autres. De même, les droits peuvent être attribués par serveur de site ; ainsi, les administrateurs d'un serveur de site local ne bénéficieront pas d'un accès à privilèges élevés dans d'autres sites et succursales de l'organisation où cela n'est pas souhaité.

Lorsque l'administrateur utilise **la gestion** des utilisateurs **par groupes** (groupes de sécurité), il peut réduire le nombre d'étapes nécessaires à la configuration des droits d'accès tout en continuant à bénéficier des fonctionnalités de création et de suppression de comptes utilisateurs. Pour en savoir plus, consultez la section « *Création et suppression de comptes utilisateurs* » ci-dessous.

Des autorisations d'accès granulaires doivent être appliquées à l'ensemble de l'infrastructure de l'organisation, y compris tous les composants de l'écosystème MyQ X. L'accès doit être réservé exclusivement aux administrateurs et au personnel autorisé, afin de garantir que seules les personnes disposant des privilèges appropriés puissent gérer ces systèmes et interagir avec eux. Cela concerne les périphériques physiques, les serveurs physiques et leur système d'exploitation (Windows Server), les serveurs SQL, le stockage, etc.

Pour en savoir plus :

- Déploiement : droits des utilisateurs

3.1.4 Réponse aux incidents et audit

Pour gérer les incidents, mettez en place des procédures et entraînez-vous régulièrement à les appliquer. En cas d'activité suspecte, restreignez ou suspendez l'accès de l'utilisateur afin d'éviter tout dommage supplémentaire. Une mise en œuvre adéquate de ces mesures permet d'atténuer l'impact d'événements imprévus.

Les fonctionnalités de journalisation et d'audit de MyQ (MyQ Logs et MyQ Audit Log) peuvent s'avérer extrêmement utiles pour la réponse aux incidents et leur suivi. Ces journaux aident à détecter, enquêter et réagir face à des activités suspectes, ce qui constitue un aspect obligatoire de la norme NIS2.

Les journaux doivent être surveillés régulièrement, et les notifications doivent être activées pour les incidents que l'organisation juge critiques. Pour ce faire, l'utilitaire **Log Notifier** embarqué dans MyQ X peut être configuré pour surveiller les événements dans l'environnement MyQ, et le personnel responsable peut être averti afin de prendre des mesures immédiates. Les tâches planifiées en cours d'exécution (telles que la synchronisation des utilisateurs, la détection des imprimantes, etc.) peuvent également envoyer des alertes à des contacts prédéfinis. Les administrateurs peuvent également configurer MyQ X pour envoyer des alertes automatisées en cas d'échec des travaux d'impression ou d'erreurs critiques.

La gestion des journaux peut être centralisée en exportant et en traitant les journaux via le journal des événements Windows ; ceux-ci peuvent ensuite être traités par des systèmes SIEM si nécessaire. Assurez-vous que les durées de conservation de l'historique, des journaux et des journaux d'audit sont suffisantes pour vos besoins. Cette configuration s'effectue dans « **Paramètres** » – « **Gestion du système** ».

La mise en place de **SLA solides** est essentielle pour les services gérés tels que MyQ, en particulier dans le cadre de la réglementation NIS2. Afin de garantir des délais de réponse rapides en cas d'incident, les organisations devraient envisager d'opter pour les offres d'assistance Premium.

En savoir plus :

- Paramètres des journaux

3.1.5 Authentification sécurisée

L'authentification sécurisée garantit que seuls les utilisateurs autorisés accèdent aux systèmes. L'authentification à deux facteurs (2FA) renforce cette sécurité en exigeant deux types d'identifiants, ce qui augmente considérablement le niveau de sécurité.

Les exigences en matière de mot de passe et de code PIN, **l'authentification à deux facteurs** sur les Terminaux embarqués, ou l'utilisation de « Se connecter avec Microsoft » sur les interfaces Web ou les Terminaux embarqués (avec le client mobile MyQ X) offrent des alternatives pour sécuriser l'accès à l'environnement MyQ X.

Le client mobile MyQ X peut être configuré pour exiger **une vérification biométrique**, ce qui renforce encore la sécurité du compte utilisateur MyQ X en imposant un facteur supplémentaire lors de l'authentification sur les périphériques.

La mise en place de mécanismes de verrouillage des comptes utilisateur après plusieurs tentatives de connexion infructueuses renforce la sécurité et réduit le risque d'attaques par force brute.

En savoir plus :

- Déploiement : authentification sécurisée[5]
- Déploiement : utilisation de l'authentification à deux facteurs[6]

3.1.6 Provisionnement et déprovisionnement des utilisateurs

La création et la suppression de comptes garantissent que les utilisateurs se voient immédiatement refuser l'accès à l'environnement MyQ dès leur suppression du répertoire d'utilisateurs source.

MyQ prend en charge **la synchronisation automatique et programmée des utilisateurs** avec des systèmes externes tels que LDAP, Microsoft Entra ID (anciennement Azure AD), Google Workspace et les fichiers CSV. Cela garantit que les utilisateurs nouvellement ajoutés sont automatiquement importés dans l'environnement MyQ X sans intervention manuelle. En synchronisant régulièrement les données des utilisateurs, MyQ X permet de maintenir une liste à jour des utilisateurs disposant des droits d'accès appropriés, réduisant ainsi le risque d'accès non autorisé.

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

La gestion par groupes et l'utilisation de groupes de sécurité dans le répertoire utilisateur source peuvent faciliter l'**attribution et la suppression** automatiques **des droits d'accès** à certaines parties de l'environnement MyQ X pour les utilisateurs nouvellement créés ou supprimés.

MyQ X propose une fonctionnalité **d'enregistrement automatique**, permettant aux utilisateurs de s'enregistrer eux-mêmes en envoyant des travaux d'impression, en passant leur badge devant le lecteur ou en créant un compte via l'interface Web. Cette fonctionnalité est particulièrement utile dans les environnements accueillant fréquemment des utilisateurs externes, tels que des collaborateurs invités. Les utilisateurs du système peuvent se voir attribuer un code **PIN temporaire** qui expire après une période définie, garantissant ainsi que l'accès est automatiquement révoqué dès que l'utilisateur n'en a plus besoin.

MyQ prend en charge l'anonymisation des données utilisateur afin de se conformer aux réglementations en matière de confidentialité. Ce processus supprime de manière irréversible tous les identifiants personnels, rendant les comptes utilisateur à la fois inutilisables et intraçables, tout en permettant la génération de rapports et l'audit du système sans compromettre la confidentialité.

En savoir plus :

- Déploiement : gestion des utilisateurs par groupes

3.1.7 Sensibilisation et formation

> La norme NIS2 insiste sur la nécessité de sensibiliser et de former le personnel aux pratiques de cybersécurité.

Il est recommandé d'organiser des sessions de formation à l'intention du personnel informatique et des administrateurs sur la gestion sécurisée de l'environnement MyQ X, en mettant l'accent sur la conformité à la norme NIS2. La meilleure solution consiste à consulter votre fournisseur ou distributeur concernant la gestion de l'écosystème MyQ X. Les partenaires MyQ sont formés pour fournir un support de la plus haute qualité.

De plus, des programmes de sensibilisation doivent être mis en place pour aider les utilisateurs finaux à identifier les menaces et leur expliquer comment utiliser l'écosystème MyQ X, ainsi que les mesures à prendre en cas d'incidents de sécurité ou autres.

Livre blanc sur la sécurité et déploiement sécurisé

Pour en savoir plus sur la manière d'atteindre les meilleures normes de sécurité avec MyQ X, consultez la suite de ce guide consacré à la sécurité de MyQ X (see page 4).

Mis à jour le 6 octobre 2026

4 Nomenclature des logiciels

Une nomenclature logicielle (SBOM) est un registre détaillé de tous les composants, dépendances et bibliothèques inclus dans une application logicielle, qu'ils soient open source ou propriétaires. Elle fournit des informations clés telles que les noms des composants, les versions, les licences et les emplacements des sources, offrant une visibilité complète sur la chaîne d'approvisionnement du logiciel.

Les SBOM sont utilisées pour suivre et gérer les risques logiciels en permettant aux organisations d'identifier rapidement les composants vulnérables ou obsolètes, de garantir la conformité avec les licences et d'améliorer la sécurité globale. La maintenance d'une SBOM est particulièrement importante dans les écosystèmes logiciels complexes, car elle permet de rationaliser la gestion des vulnérabilités et d'assurer la transparence tout au long du cycle de vie du développement logiciel.

En générant, analysant et mettant à jour régulièrement des SBOM, les organisations peuvent mieux gérer les risques logiciels et garantir la conformité aux normes de sécurité et réglementaires.

Les formats BOM (Bill of Materials) font référence à des structures normalisées qui représentent et partagent les composants d'un système logiciel. Dans le contexte des nomenclatures logicielles (SBOM), ces formats fournissent un moyen lisible par machine pour décrire les composants logiciels, leurs relations et leurs métadonnées. Les formats SBOM les plus largement utilisés sont les suivants :

- **CycloneDX** : un format de nomenclature léger et extensible spécialement conçu pour la sécurité des applications. Il fournit des informations détaillées sur les composants, les licences, les vulnérabilités et les dépendances. CycloneDX est apprécié pour sa flexibilité et sa prise en charge de l'automatisation dans les workflows de sécurité et de gestion des risques.

MyQ fournit des SBOM pour les produits suivants :

- MyQ X Central Server 10.2
- MyQ X Print Server 10.2
- MyQ Desktop Client (MDC) 10.2
- Mobile Print Agent (MPA) 1.3
- Reconnaissance optique de caractères (OCR) 3.1

Pour recevoir les SBOM de MyQ, contactez notre service d'assistance.

5 Contacts professionnels

Fabricant MyQ®	**MyQ® spol. s r.o.** Harfa Business Center, Ceskomoravska 2532/19b, 190 00 Prague 9, République tchèque Numéro d'identification 615 06 133 MyQ® spol. s r.o. est inscrite au registre du commerce du tribunal municipal de Prague, sous le numéro C 29842 (ci-après dénommée « MyQ® »)
Informations commerciales	http://www.myq-solution.com info@myq-solution.com[7]
Assistance technique	support@myq-solution.com[8]
Avis	LE FABRICANT NE PEUT ÊTRE TENU RESPONSABLE DE TOUTE PERTE OU DOMMAGE RÉSULTANT DE L'INSTALLATION OU DU FONCTIONNEMENT DES COMPOSANTS LOGICIELS ET MATÉRIELS DE LA SOLUTION D'IMPRESSION MyQ®. Ce manuel, son contenu, sa conception et sa structure sont protégés par le droit d'auteur. La copie ou toute autre reproduction de tout ou partie de ce guide, ou de tout élément protégé par le droit d'auteur, sans l'accord écrit préalable de MyQ® est interdite et peut être punie par la loi. MyQ® n'est pas responsable du contenu de ce manuel, notamment en ce qui concerne son intégrité, sa monnaie et son occupation commerciale. Tout le matériel publié ici est exclusivement à titre informatif. Ce manuel est susceptible d'être modifié sans préavis. MyQ® n'est pas tenu d'effectuer ces modifications périodiquement ni de les annoncer, et n'est pas responsable de la compatibilité des informations actuellement publiées avec la dernière version de la solution d'impression MyQ®.

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

Marques commerciales	« MyQ® », y compris ses logos, est une marque déposée de MyQ®. Toute utilisation des marques commerciales de MyQ®, y compris ses logos, sans l'accord écrit préalable de MyQ® Company est interdite. La marque commerciale et le nom du produit sont protégés par MyQ® et/ou ses filiales locales.

myQ X

GAGNEZ DU TEMPS GRÂCE À DES SOLUTIONS D'IMPRESSION PERSONNALISÉES

MyQ X est une solution de gestion d'impression primée, disponible sur site ou dans un cloud privé, et à laquelle font confiance des millions d'utilisateurs.

info@myq-solution.com

myq-solution.com

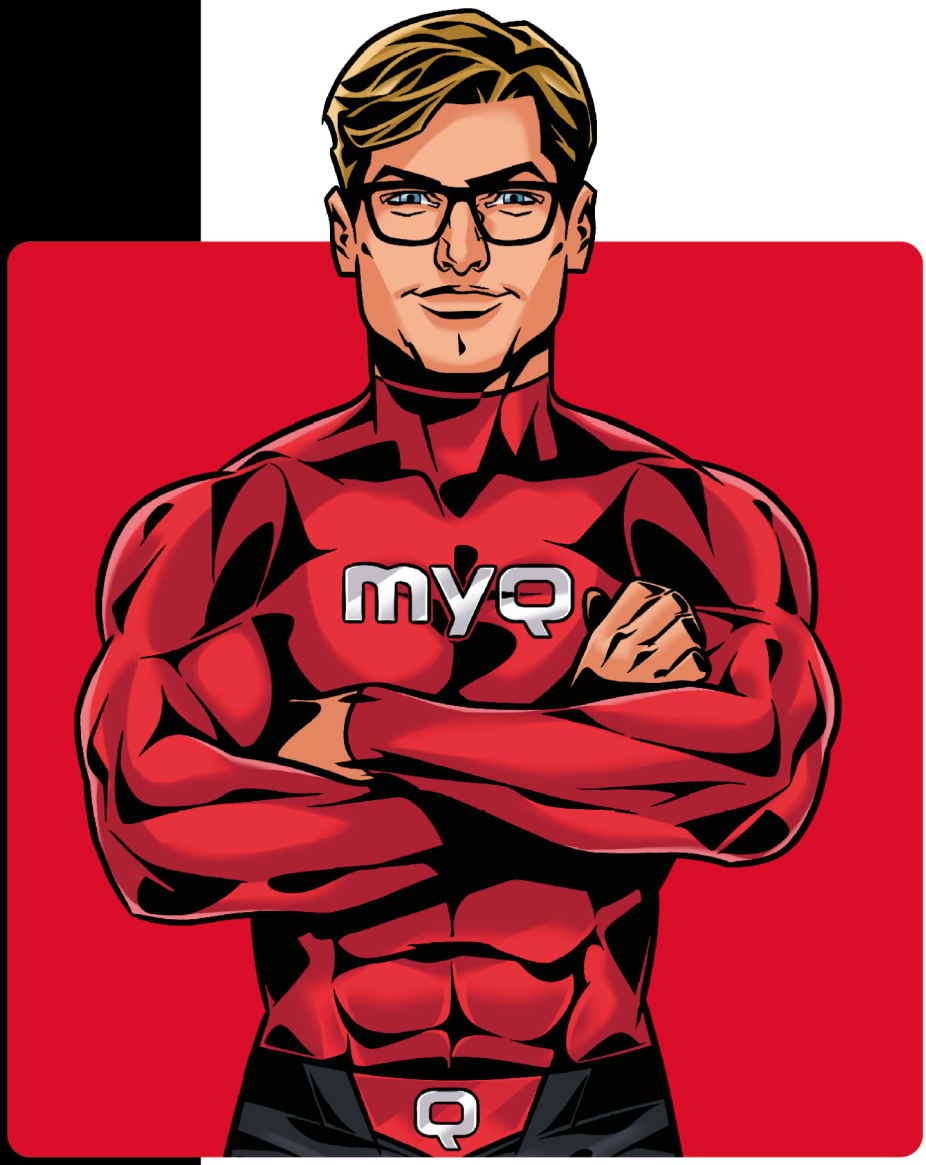
+ de 50 millions
d'utilisateurs nous font confiance

+d'1 million
d'équipements actifs

26+ marques
supportées

1000+
Partenaires certifiés

Présent dans
+ de 140 pays



Récompensé et certifié

BuyersLab PLATINUM TESTED SOLUTION 2023

BuyersLab PLATINUM TESTED SOLUTION 2022

BuyersLab PLATINUM TESTED SOLUTION 2021

ISO 9001 TÜV SÜD ISO 14001 ISO/IEC 27001