

Seguridad MyQ X 10.x

Generado a partir de docs.myq-solution.com
octubre/2026
Copyright © 2026 MyQ spol. s r.o. Todos los derechos reservados.

ESPAÑOL

Aviso sobre la traducción

Esta traducción se creó con la ayuda de inteligencia artificial. En caso de discrepancia o ambigüedad, prevalecerá el documento original en inglés.

Tabla de contenido

1 Despliegue seguro de MyQ X 5
1.1 Servidor Central MyQ X 5
1.2 Servidor Print Server MyQ X 16
1.3 Cliente de escritorio MyQ X 29
2 Informe sobre la seguridad de MyQ X 33
2.1 Arquitectura de confianza cero 33
2.2 Marco de protección trifásico 34
2.3 Privacidad desde el diseño 34
2.4 Evolución continua de la seguridad 34
2.5 Principales mejoras de seguridad en 10.2 35
2.6 Valor empresarial de la gestión segura de la impresión 37
2.7 Conformidad 39
2.8 Implantación de la arquitectura de confianza cero 43
2.9 Gestión de identidades y accesos 46
2.10 Seguridad de las infraestructuras 50
2.11 Protección y cifrado de datos 53
2.12 Flujos de trabajo de impresión seguros 57
2.13 Seguridad de dispositivos y redes 60
2.14 Auditoría y control 63
2.15 Respuesta a incidentes y recuperación 66
3 MyQ X y NIS2 70
3.1 Áreas principales de la Directiva NIS2 70
4 Lista de materiales de software 77
5 Contactos comerciales 79

La seguridad siempre ha sido una **prioridad máxima para MyQ**. En esta sección, encontrarás una guía para la implementación segura de MyQ X, así como el informe técnico sobre seguridad de MyQ X:

- Implementación segura (see page 5)
- Documento técnico sobre seguridad (see page 33)

1 Despliegue seguro de MyQ X

Páginas OEM vinculadas
This ScriptRunner macro could not be rendered for export.

La confidencialidad de los datos de los clientes y su **seguridad** siempre han sido **la prioridad número uno de MyQ**. Sin embargo, **la seguridad es una responsabilidad compartida entre los proveedores y los clientes.** Aunque el objetivo de MyQ X es proporcionar una configuración segura por defecto, hay varias áreas que requieren medidas adicionales por parte del cliente. Entre ellas se incluyen, entre otras, la gestión de certificados, el uso de credenciales seguras, la delegación de permisos y la configuración del cortafuegos.

Este documento contiene listas de verificación prácticas para la implementación segura de MyQ X Central Server y MyQ X Print Server en entornos empresariales. Creemos firmemente que seguir estas directrices reducirá considerablemente la superficie de ataque de cualquier infraestructura de gestión de impresión. Huelga decir que las aplicaciones del servidor MyQ X son tan seguras como los sistemas operativos y los entornos de red subyacentes. Dado que la seguridad de Windows es un tema aparte, no se trata en este documento.

Los sistemas MyQ X se mejoran y actualizan constantemente, siguiendo la política de ciclo de vida de desarrollo seguro de MyQ. Asegúrese de **utilizar siempre la última versión compatible**. Las notas de la versión se pueden encontrar en cada guía del producto. Consulte también la política de[1] fin de vida útil (EOL)[2] para conocer los anuncios de fin de mantenimiento y los componentes sucesores.

Esta guía se ha elaborado junto con Mainstream Technologies, ahora Seyfor[3], durante auditorías de seguridad independientes periódicas.

1.1 Servidor Central MyQ X

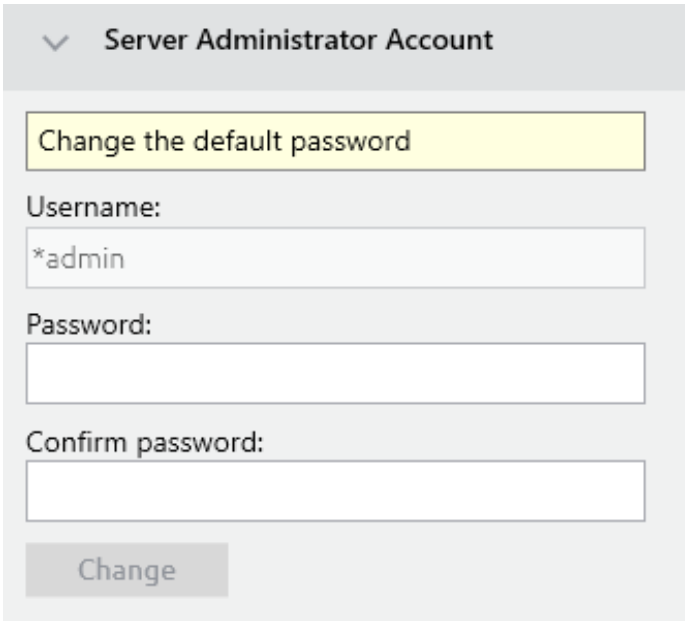
Páginas OEM vinculadas
This ScriptRunner macro could not be rendered for export.

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

1.1.1 Contraseñas predeterminadas

Cambiar la contraseña del administrador del servidor

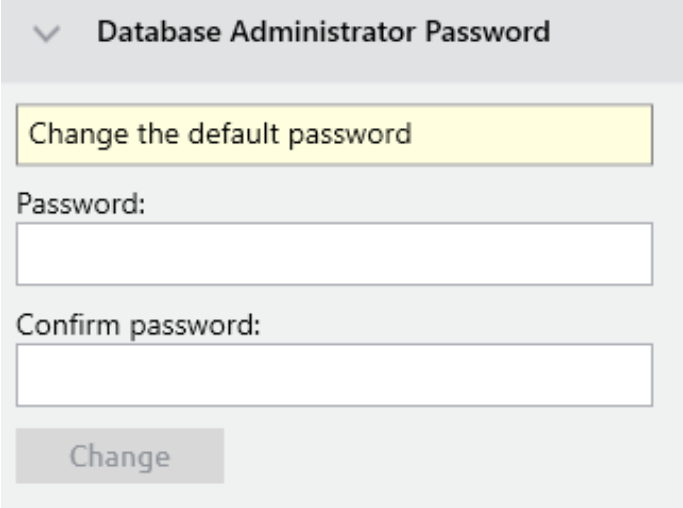
Uno de los primeros pasos debe ser cambiar la contraseña administrativa predeterminada, que es *1234*:



La contraseña se almacena en la base de datos en forma de hash.

Cambiar la contraseña del administrador de la base de datos

En caso de que se utilice la base de datos interna Firebird, cambie la contraseña predeterminada que utiliza MyQ Central Server para autenticarse en ella:



Esta contraseña se almacena en el archivo «C:\ProgramData\MyQ Central Server\setup.ini» en forma cifrada y está configurada como «*masterkey*» de forma predeterminada.

1.1.2 Seguridad de la conexión

Páginas OEM vinculadas
This ScriptRunner macro could not be rendered for export.

Configurar certificado HTTPS

Se debe configurar un certificado personalizado que sea de confianza para todos los equipos cliente y que contenga el nombre DNS del servidor para MyQ Central Server:

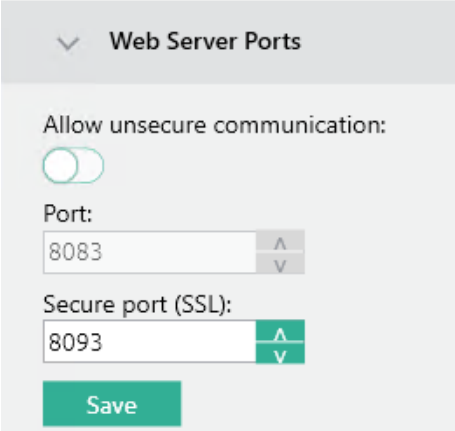
El certificado se almacena físicamente en el directorio «C:\ProgramData\MyQ Central Server\Cert» en los siguientes archivos:

- server.pfx: certificado con claves públicas y privadas
- server.cer: certificado con la clave pública
- server.key: clave privada

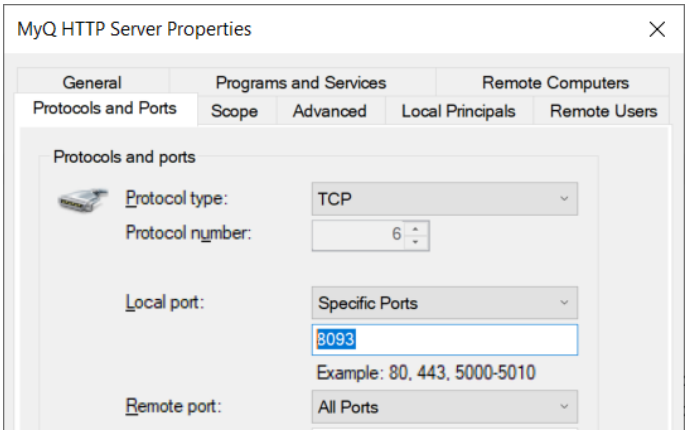
Se desaconseja el uso de certificados comodín, ya que suponen un riesgo de seguridad mucho mayor en caso de robo.

Bloquear el tráfico HTTP sin cifrar

El tráfico HTTP sin cifrar no debe habilitarse en la configuración del Central Server MyQ:

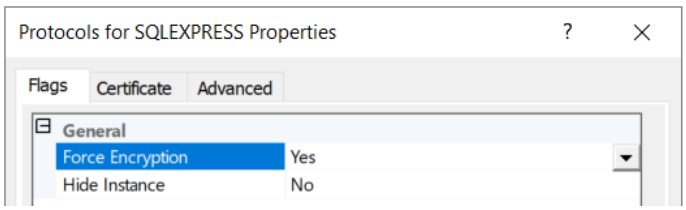


El firewall basado en host también debe configurarse para habilitar únicamente el tráfico HTTPS:

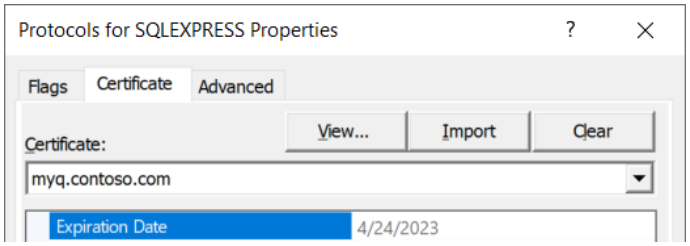


Cifrar las conexiones a la base de datos

Si se utiliza Microsoft SQL Server para almacenar la base de datos MyQ, asegúrese de que el cifrado TLS se aplique a través del Administrador de configuración de SQL Server:

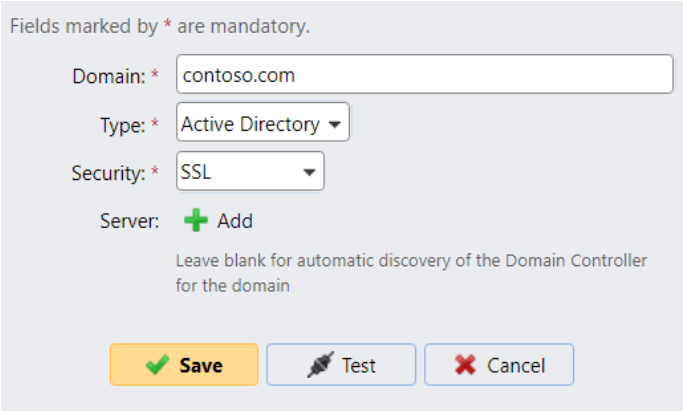


También se debe configurar un certificado emitido por una CA de confianza en SQL Server:



Aplicar tráfico LDAP cifrado

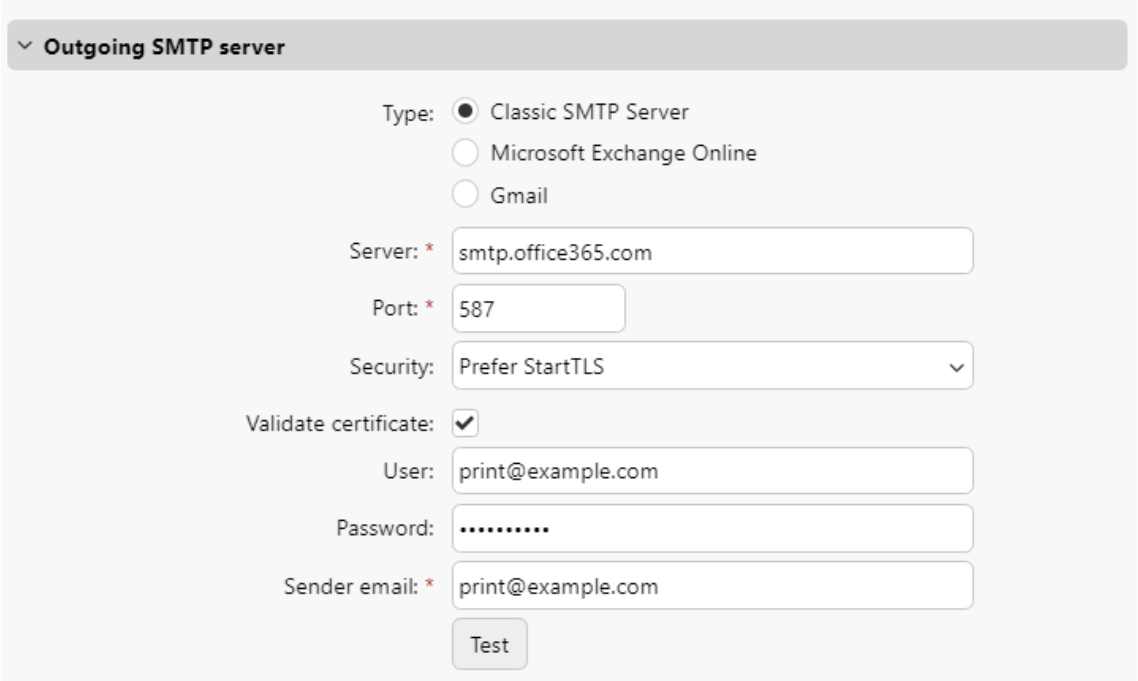
Si se utiliza la sincronización de cuentas de usuario a través del protocolo LDAP, establezca la seguridad de la conexión en SSL:



Por motivos de seguridad, no utilice START TLS, ya que es vulnerable a ataques MITM. Se debe configurar un certificado emitido por una CA de confianza en todos los servidores LDAP (controladores de dominio de Active Directory).

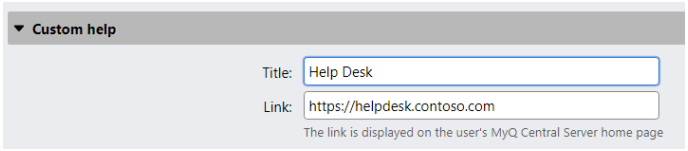
Proteger el tráfico SMTP

Si hay un servidor SMTP configurado en MyQ Central Server, aplique el uso de TLS con validación de certificados:



Utilice siempre FQDN

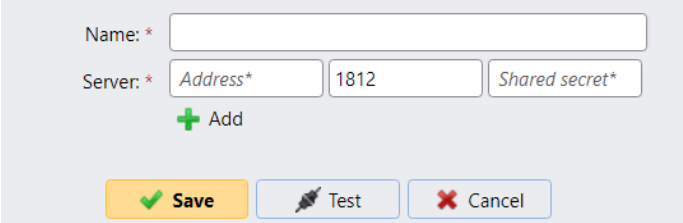
Para evitar ataques MITM, utilice estrictamente nombres de dominio completos en todas las ventanas de configuración:



Nunca se ponga en contacto con los servidores escribiendo únicamente direcciones IP o nombres de una sola etiqueta.

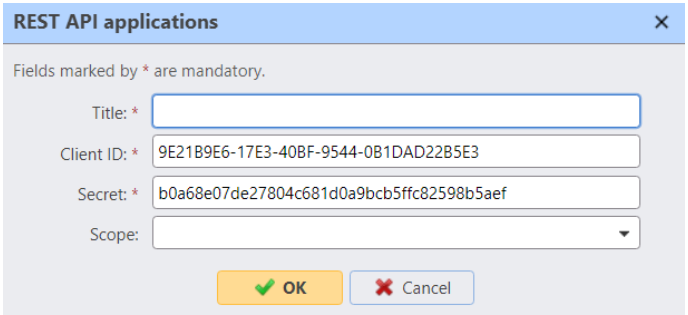
Tráfico RADIUS seguro

Si se utiliza la autenticación RADIUS, genere siempre secretos compartidos fuertes que sean específicos del Central Server MyQ:



Proteja las claves API REST

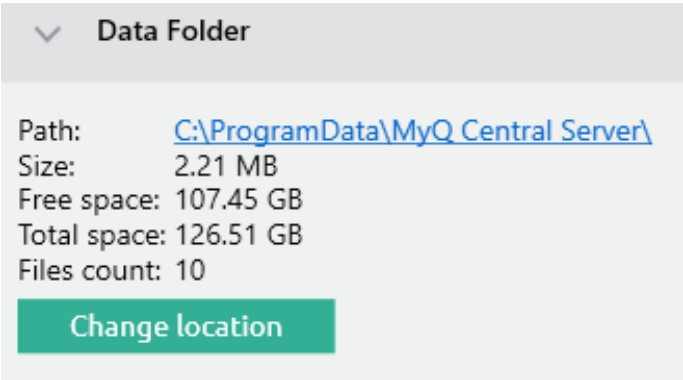
Cuando se utilicen API REST, proteja los secretos del cliente de una exposición innecesaria y realice renovaciones periódicas de los secretos:



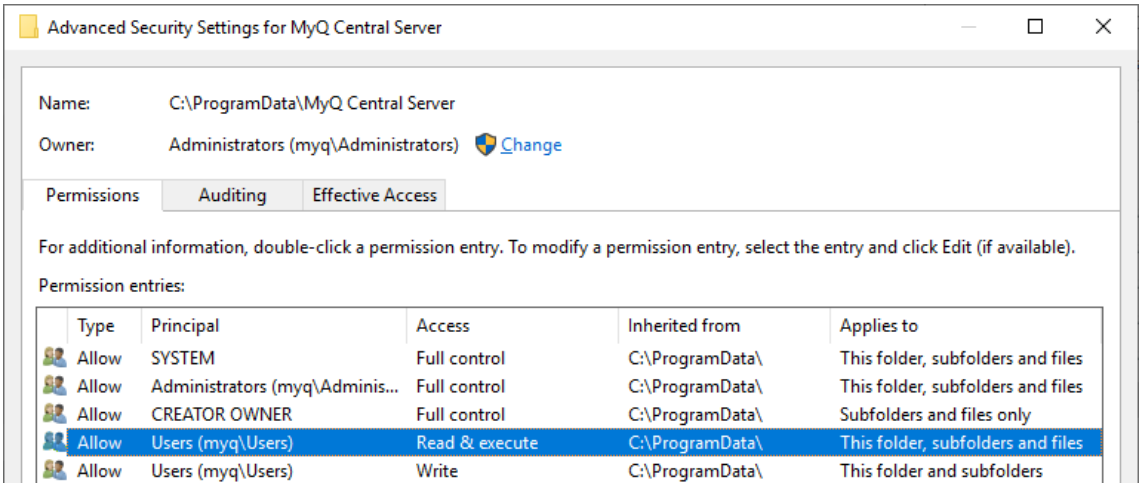
1.1.3 Seguridad de los datos

Restringir los permisos de la carpeta de datos

La carpeta de datos de MyQ Central Server contiene datos altamente confidenciales, como la base de datos de usuarios y la clave privada del certificado TLS. Su ubicación actual se muestra en la aplicación MyQ Central Server Easy Config:



Todos los usuarios (locales/de dominio) tienen acceso de lectura de forma predeterminada:



Solo los administradores, la cuenta «SYSTEM» y la cuenta de servicio de MyQ deben tener acceso a este directorio. A continuación se muestra un script por lotes de ejemplo que puede utilizarse para reforzar los permisos:

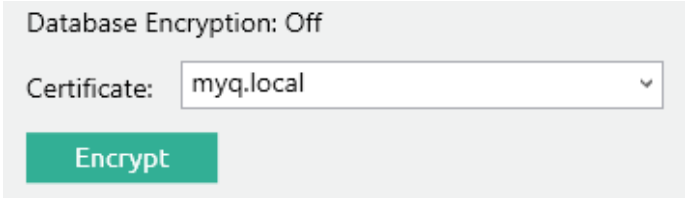
```
@ECHO OFF

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
```

Habilitar el cifrado de la base de datos

Cuando se utilice la base de datos integrada, cifrémosla siempre con un certificado personalizado para reducir el riesgo de fugas de datos:



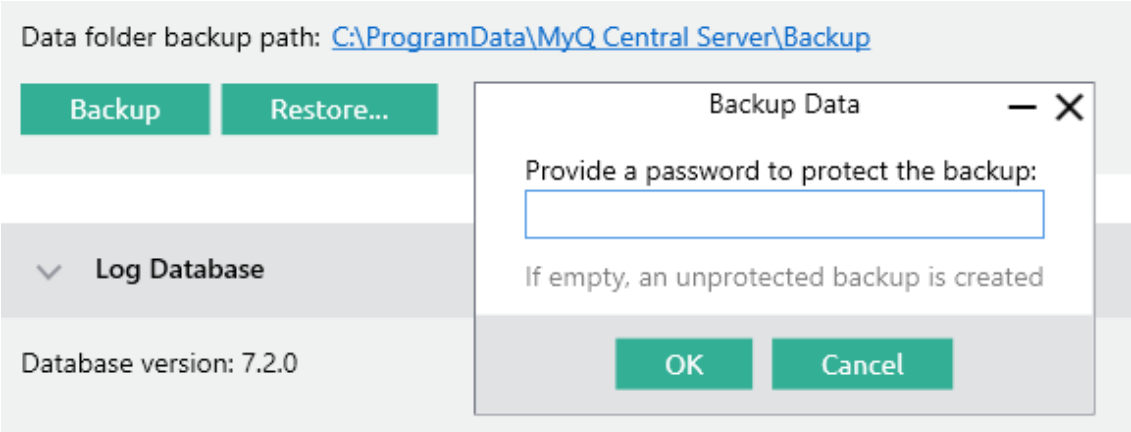
El certificado debe incluir el uso de clave mejorado (EKU) «Encrypting File System» y debe estar ubicado en uno de los siguientes almacenes de certificados del ordenador:

- Personal
- Editores de confianza
- Autoridades de certificación raíz de terceros
- Otras personas

El almacén «Personal» es el recomendado.

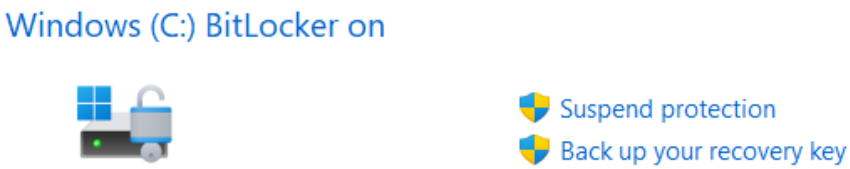
Cifrar las copias de seguridad

Las copias de seguridad de la base de datos deben protegerse con contraseñas seguras generadas aleatoriamente:



Habilitar el cifrado de disco

Si es posible, se debe habilitar una tecnología de cifrado completo del disco, como Microsoft BitLocker, en el Central Server de MyQ para proteger los datos en reposo:



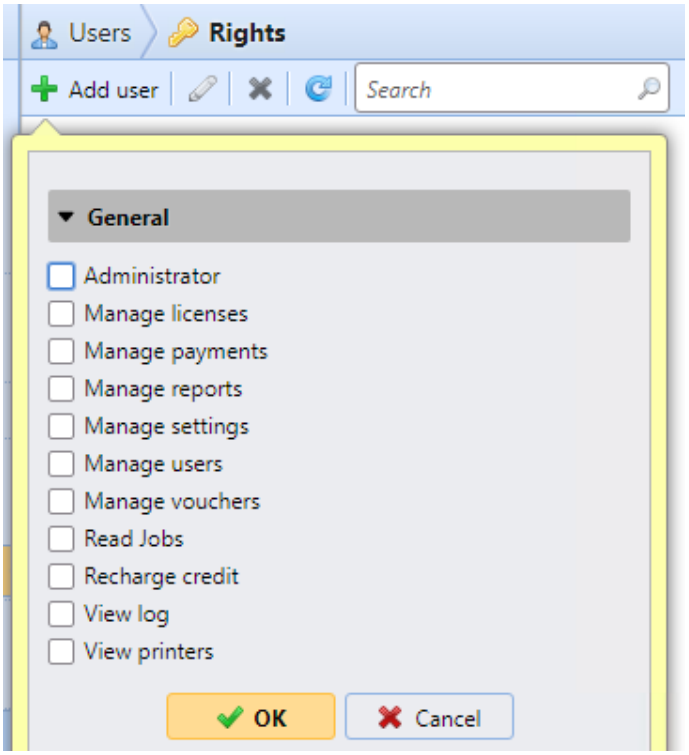
1.1.4 Recomendaciones adicionales

Páginas OEM vinculadas

This ScriptRunner macro could not be rendered for export.

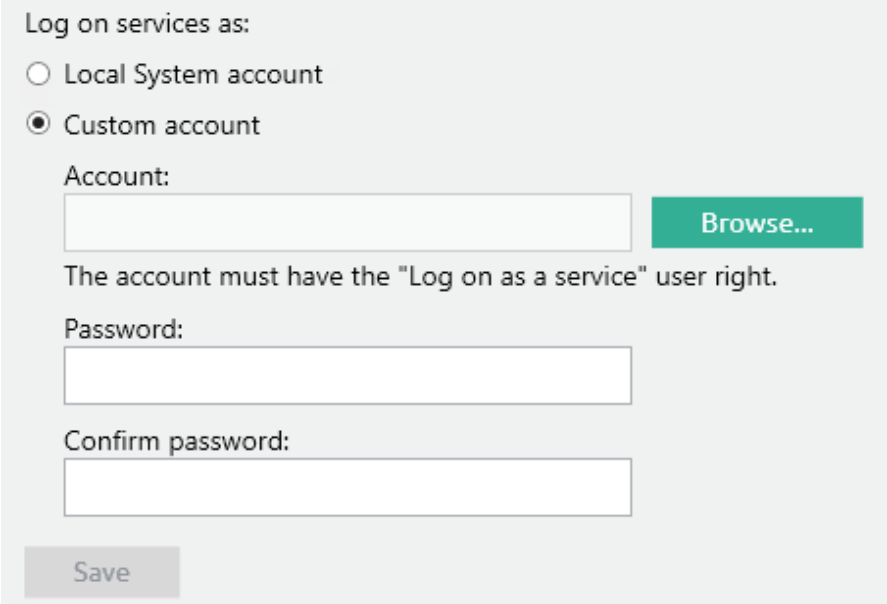
Implementar RBAC

No utilice la cuenta *admin predeterminada para operaciones habituales. En su lugar, utilice la delegación de privilegios, aplicando el principio del mínimo privilegio:



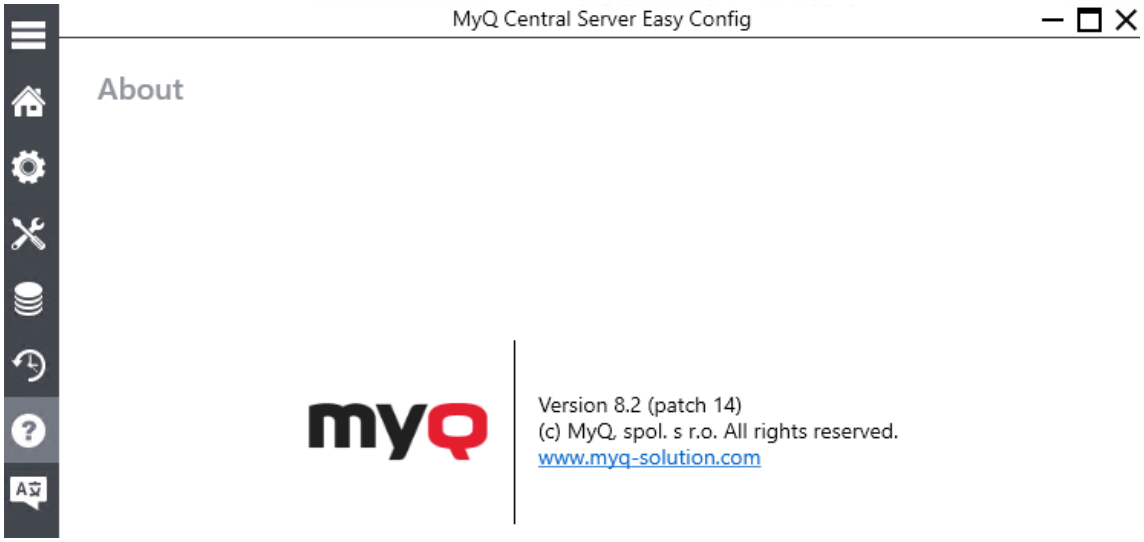
Configurar una cuenta de servicio personalizada

MyQ Central Server se ejecuta de forma predeterminada con la cuenta SYSTEM, que tiene privilegios elevados. Configure una cuenta de servicio personalizada con una contraseña segura:



Mantenga el servidor actualizado

Instale las actualizaciones de seguridad proporcionadas por MyQ tan pronto como estén disponibles. Puede comprobar la versión de la aplicación actualmente instalada en MyQ Central Server Easy Config:



Mantenga el sistema operativo seguro

MyQ Central Server es tan seguro como el sistema operativo subyacente. Manténgalo actualizado y aplique las políticas de seguridad recomendadas por Microsoft.

Actualice periódicamente su software para corregir vulnerabilidades de seguridad y mejorar el rendimiento. Consulte los requisitos del sistema para ver la lista de requisitos y recomendaciones.

Por ejemplo, .NET debe actualizarse con herramientas de administración o mediante Windows Updates de forma opcional[4].

Planifique la recuperación ante desastres

Cree periódicamente copias de seguridad del Central Server MyQ, incluyendo la base de datos, los certificados y los archivos de configuración. Pruebe el procedimiento de recuperación al menos una vez.

1.2 Servidor Print Server MyQ X

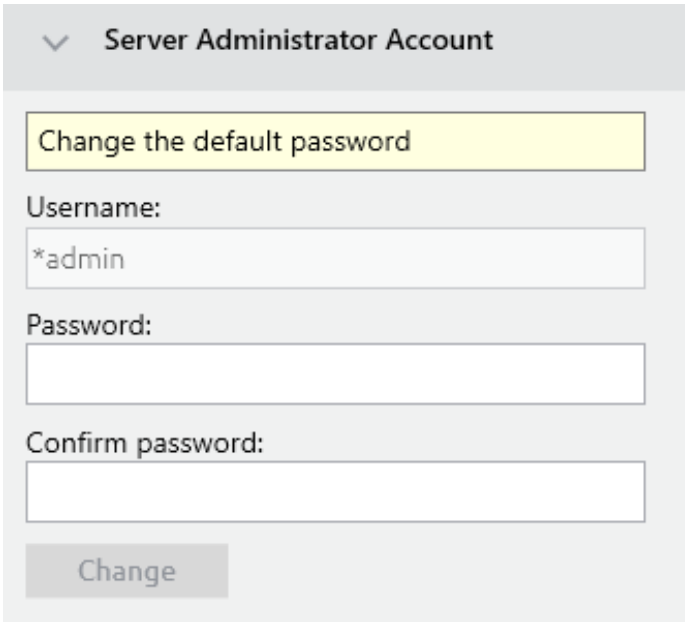
Páginas OEM vinculadas
This ScriptRunner macro could not be rendered for export.

1.2.1 Contraseñas predeterminadas de PS

Cambiar la contraseña del administrador del servidor

Uno de los primeros pasos debe ser cambiar la contraseña administrativa predeterminada, que es *1234*:

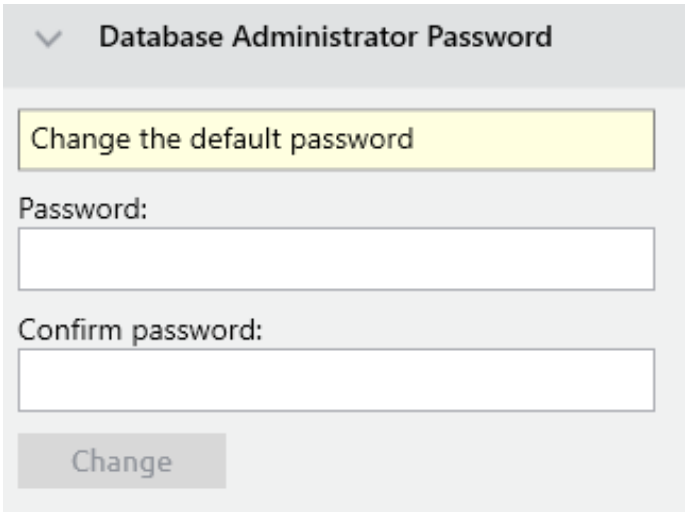
4. https://devblogs.microsoft.com/dotnet/server-operating-systems-auto-updates/



La contraseña se almacena en la base de datos en forma de hash.

Cambiar la contraseña del administrador de la base de datos

Cambie la contraseña predeterminada que utiliza MyQ Print Server para autenticarse en la base de datos interna Firebird:

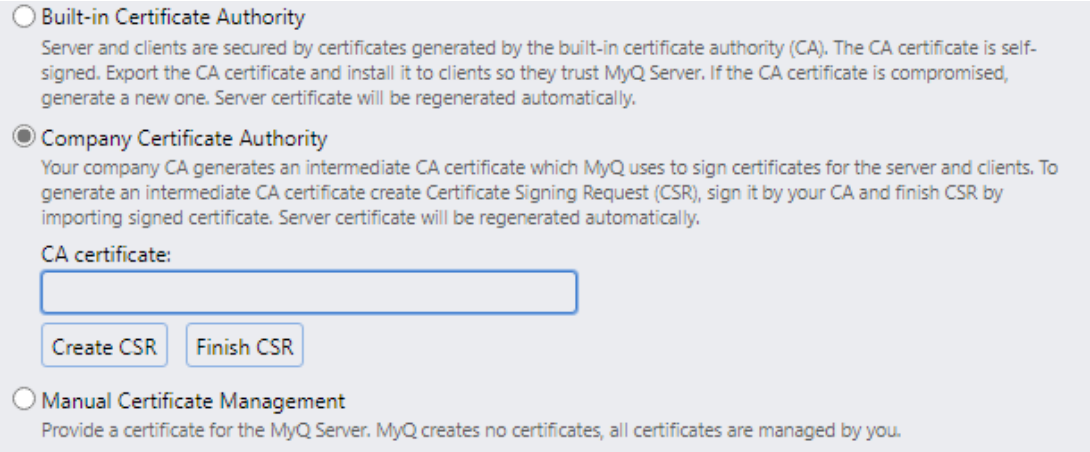


Esta contraseña se almacena en el archivo «C:\ProgramData\MyQ\setup.ini» en forma cifrada y está configurada como «*masterkey*» de forma predeterminada.

1.2.2 PS Seguridad de la conexión

Configurar el certificado HTTPS

Se debe configurar un certificado personalizado en el que confíen todos los equipos cliente para el Print Server de MyQ. Hay tres modos de gestión de certificados disponibles:



De forma predeterminada, MyQ Print Server crea su propio certificado de CA raíz y lo utiliza para firmar los certificados de servidor y de cliente. La parte pública de este certificado se puede exportar e implementar en el almacén de confianza de certificados del cliente, por ejemplo, mediante la Política de grupo o MDM.

Las organizaciones que ya cuenten con su propia PKI de confianza pueden preferir la segunda opción. MyQ Print Server utiliza su propia CA intermedia para emitir certificados de servidor y de cliente. El certificado de CA intermedia generado automáticamente debe estar firmado por la CA de la empresa para que los clientes lo consideren de confianza.

Si la política de seguridad corporativa no permite instalar un certificado de CA intermedia en el Print Server de MyQ, o si se va a utilizar un certificado emitido por una autoridad de certificación pública, se debe recurrir a la gestión manual de certificados.

Independientemente del modo de CA, los certificados se almacenan físicamente en el directorio «C:\ProgramData\MyQ\Cert», que puede contener los siguientes archivos:

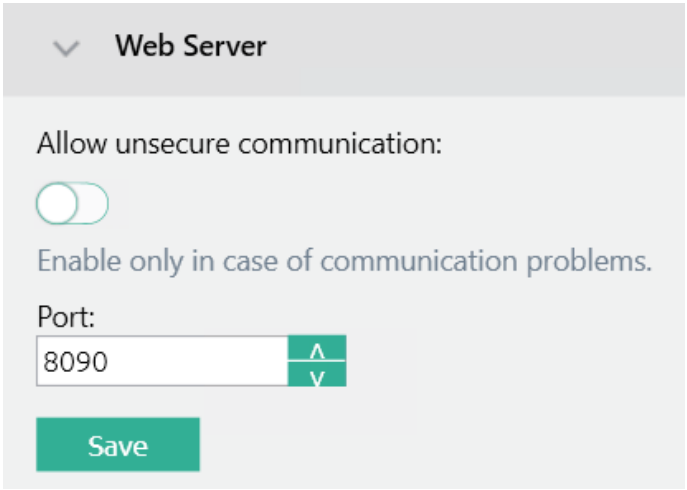
- server.pfx: certificado del servidor con claves pública y privada
- server.cer: certificado del servidor con clave pública
- server.key: clave privada del servidor
- ca-root.crt: certificado de CA raíz de la empresa con clave pública

- ca-myq.pfx: certificado de la CA emisora con claves pública y privada
- ca-myq.crt: certificado de la CA emisora con clave pública
- ca-myq.key: claves privadas de la CA emisora

Las claves privadas de la CA emisora local (utilizadas en los dos primeros modos de funcionamiento) están siempre protegidas por una contraseña generada aleatoriamente que se almacena en la base de datos interna de Firebird de forma cifrada.

Bloquear el tráfico HTTP sin cifrar

El tráfico HTTP sin cifrar no debe estar habilitado en la configuración de MyQ Print Server:



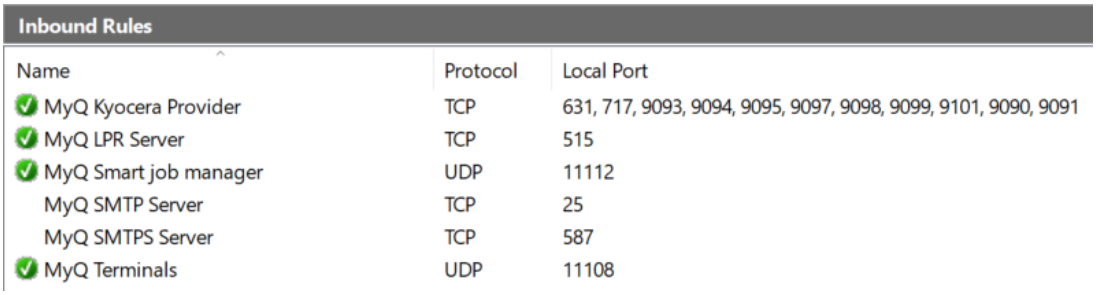
Revisar la configuración de seguridad de las comunicaciones

Compruebe las versiones mínimas de TLS configuradas en Ajustes – Red – Versión mínima de TLS. El valor predeterminado desde MyQ X 10.2 es TLS 1.2.

Para opciones más avanzadas, como cómo establecer el TLS mínimo requerido en 1.3, consulte Seguridadavanzada.

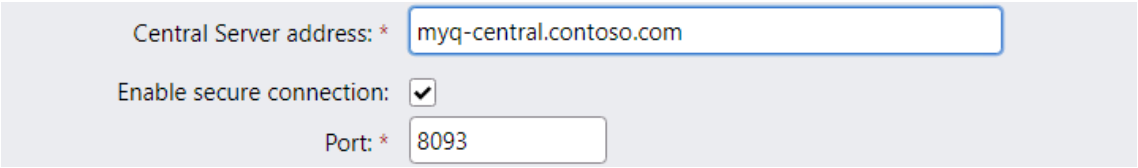
Bloquee los puertos no utilizados

Reduzca la superficie de ataque desactivando las reglas del cortafuegos para los protocolos que no utiliza MyQ Print Server:



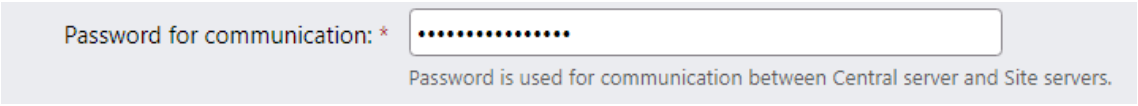
Cifre las conexiones al Central Server de MyQ

Utilice únicamente HTTPS para conectarse a MyQ Central Server:



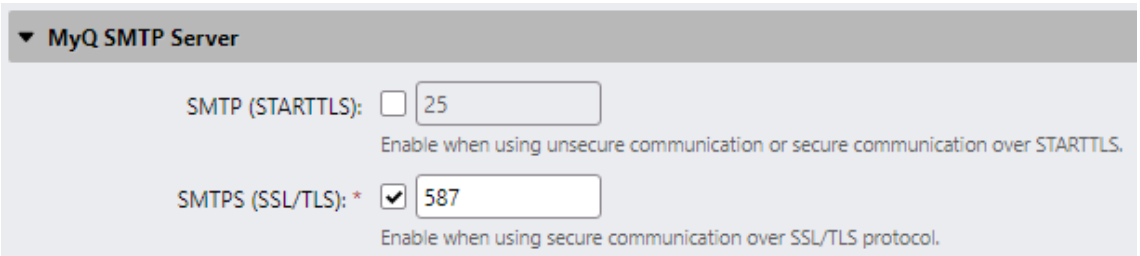
Utilice contraseñas seguras para la autenticación de servidor a servidor

La contraseña para la comunicación entre el Central Server y el sitio debe ser segura (complejidad de la contraseña):

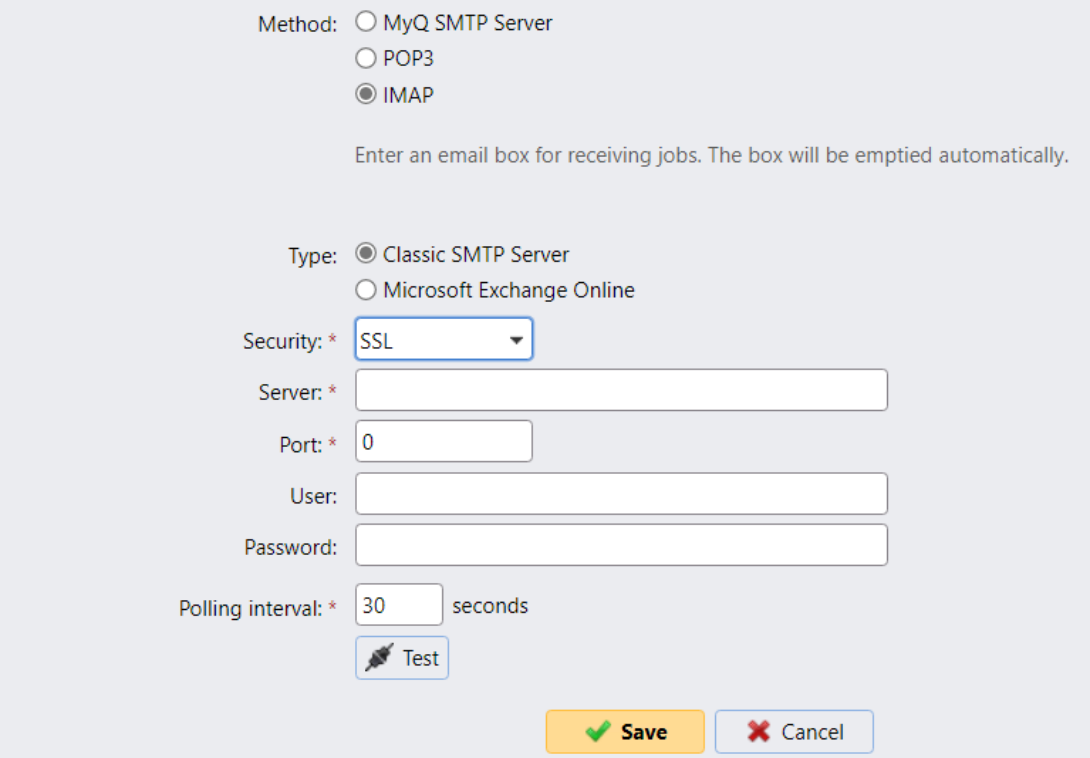


Proteja el tráfico SMTP

Cuando se utilice el protocolo SMTP para enviar correos electrónicos o recibir documentos de escáneres en red, siempre debe aplicarse el cifrado TLS para garantizar la confidencialidad de los datos.

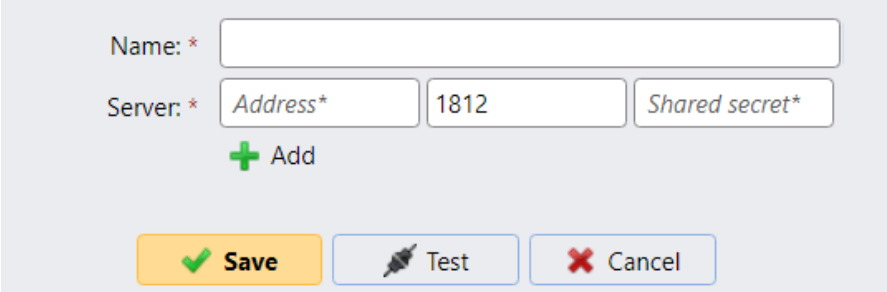


El cifrado TLS también debe aplicarse cuando se utilice el protocolo IMAP, mientras que debe evitarse el protocolo POP3 heredado:



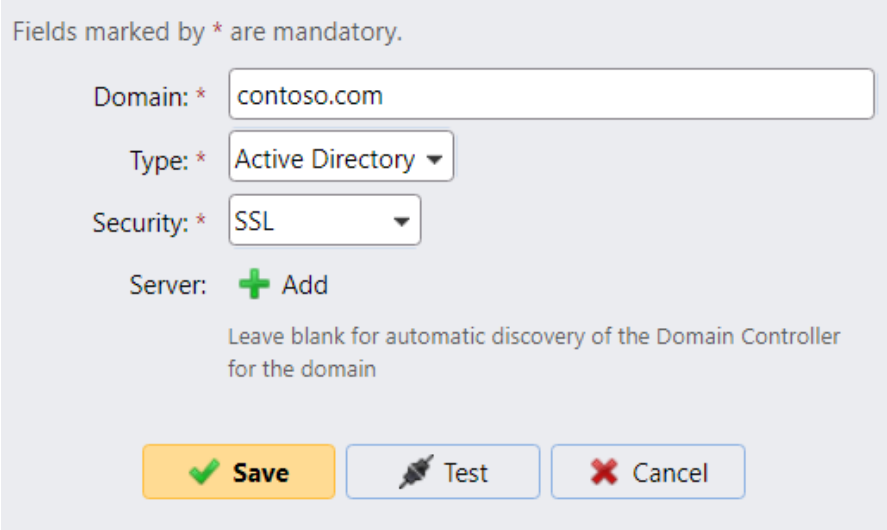
Utilice contraseñas RADIUS seguras y únicas

Si se utiliza la autenticación RADIUS, genere siempre secretos compartidos seguros que sean específicos del Print Server MyQ:



Cifre el tráfico LDAP

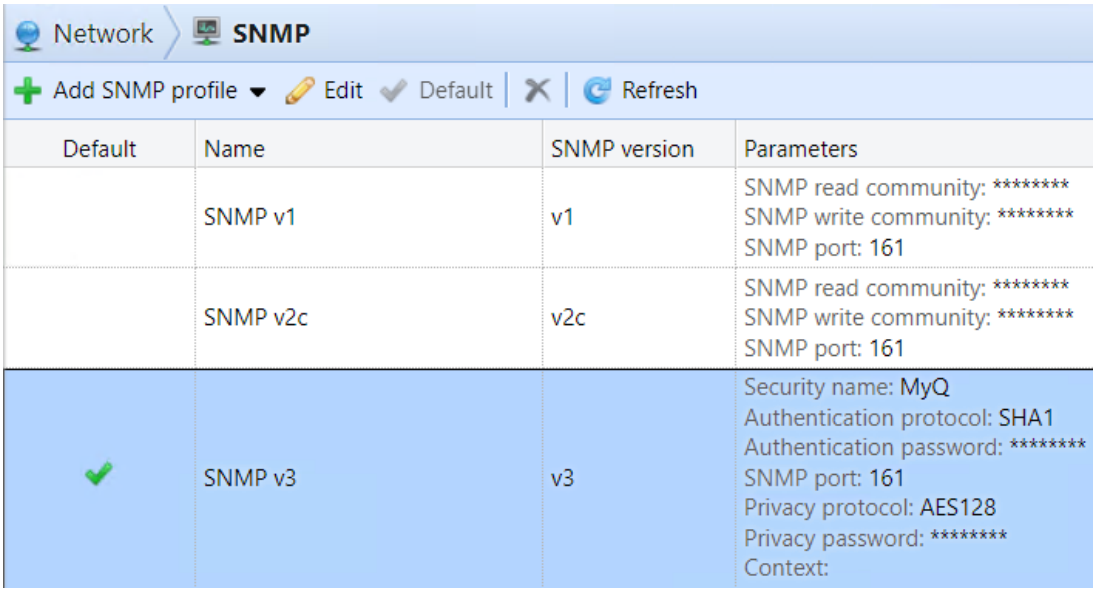
Se debe utilizar el cifrado TLS para proteger todo el tráfico LDAP:



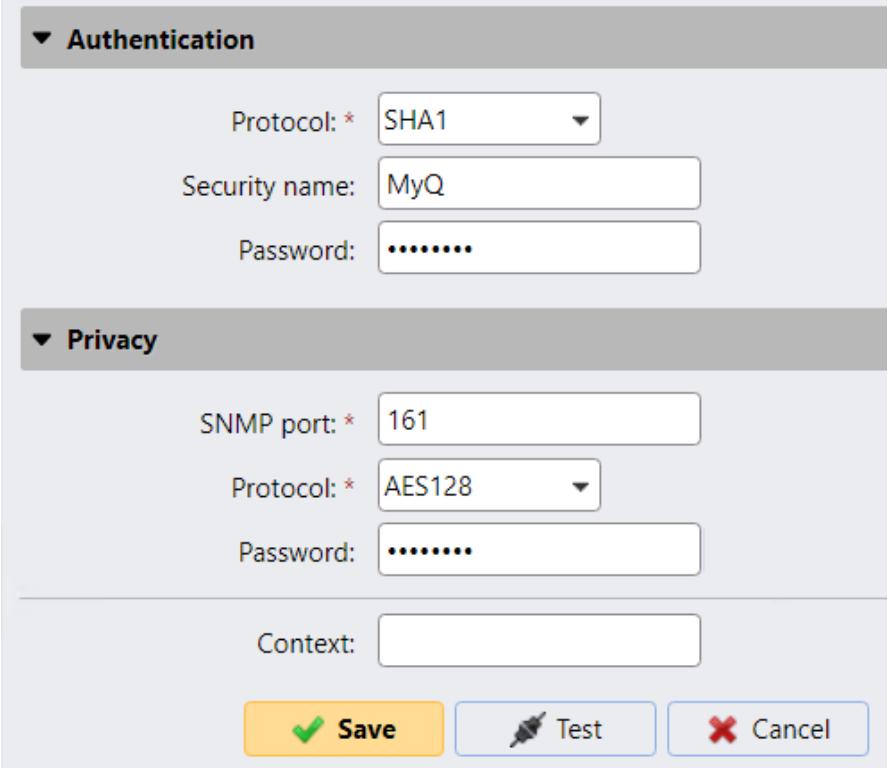
Por motivos de seguridad, no utilice START TLS, ya que es vulnerable a ataques MITM. Se debe configurar un certificado emitido por una CA de confianza en todos los servidores LDAP (controladores de dominio de Active Directory).

Proteja el tráfico SNMP

Se debe evitar la comunicación SNMPv1 no segura con los dispositivos:

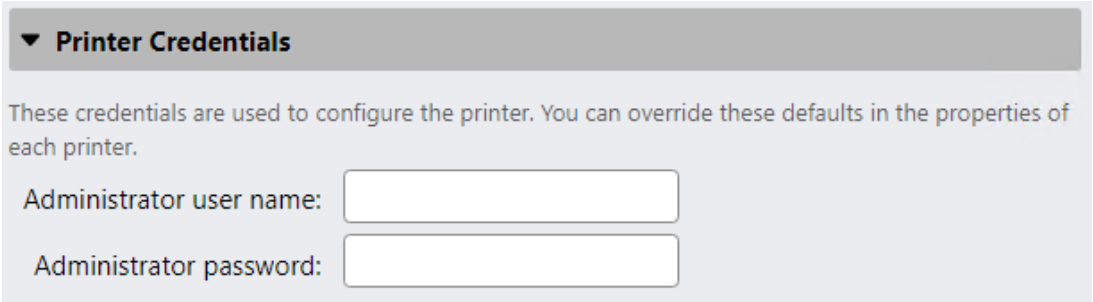


Utilice únicamente SNMPv3 con una contraseña segura y configure algoritmos criptográficos más seguros (SHA1 y AES):



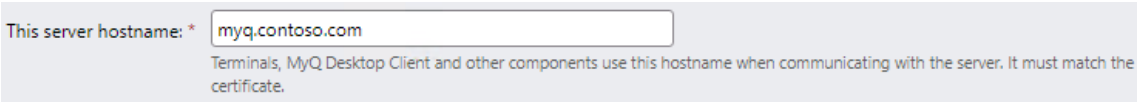
Credenciales seguras de la impresora

La gestión de credenciales de impresoras se realiza fuera del Print Server de MyQ y depende del proveedor. Si es posible, se deben utilizar contraseñas seguras y generadas aleatoriamente para gestionar las impresoras:



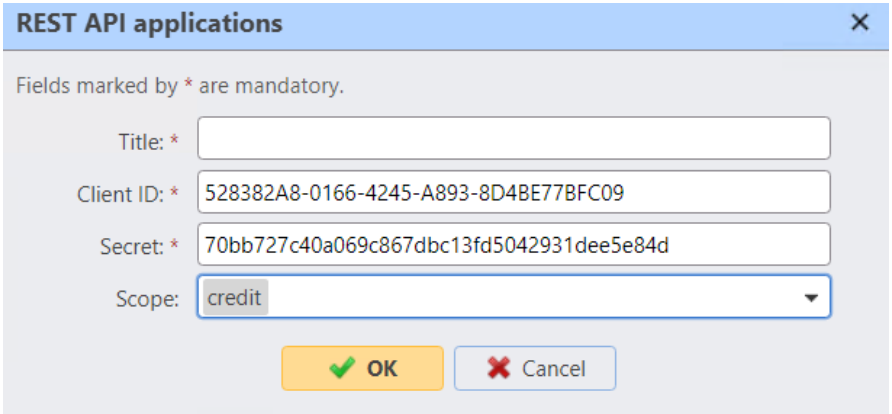
Utilice siempre el FQDN

Para prevenir ataques MITM, utilice estrictamente nombres de dominio completos en todas las ventanas de configuración:



Proteja las claves de la API REST

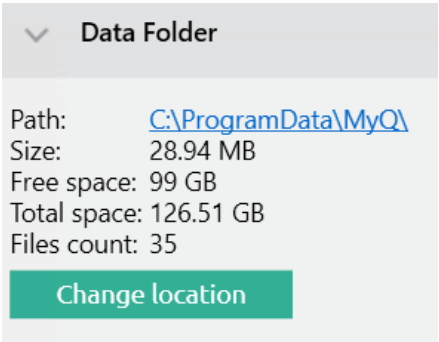
Cuando se utilicen API REST, proteja los secretos de cliente para evitar una exposición innecesaria y realice cambios periódicos de los secretos:



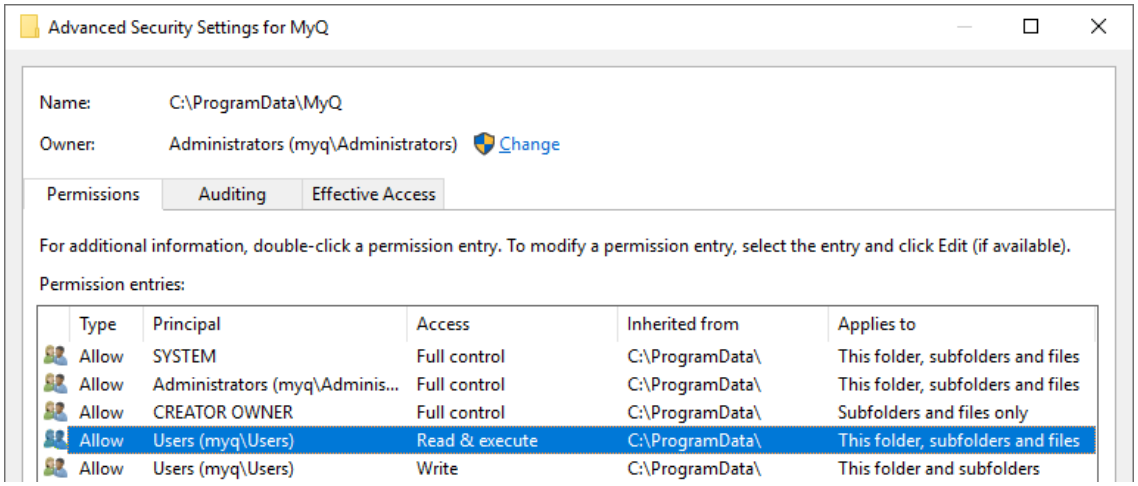
1.2.3 PS Seguridad de los datos

Restringir los permisos de la carpeta de datos

La carpeta de datos de MyQ Print Server contiene datos altamente confidenciales, como la base de datos de usuarios y la clave privada del certificado TLS. Su ubicación actual se muestra en la aplicación MyQ Easy Config:



Todos los usuarios (locales/del dominio) tienen acceso de lectura de forma predeterminada:



Solo los administradores, la cuenta «SYSTEM» y la cuenta de servicio de MyQ deben tener acceso a este directorio. A continuación se muestra un script por lotes de ejemplo que se puede utilizar para reforzar los permisos:

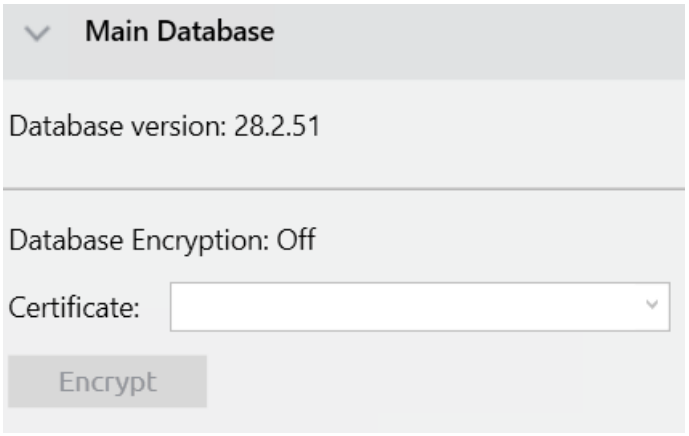
```
@ECHO OFF

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
```

Habilitar el cifrado de la base de datos

Cifra siempre la base de datos utilizando un certificado personalizado para reducir el riesgo de fugas de datos:



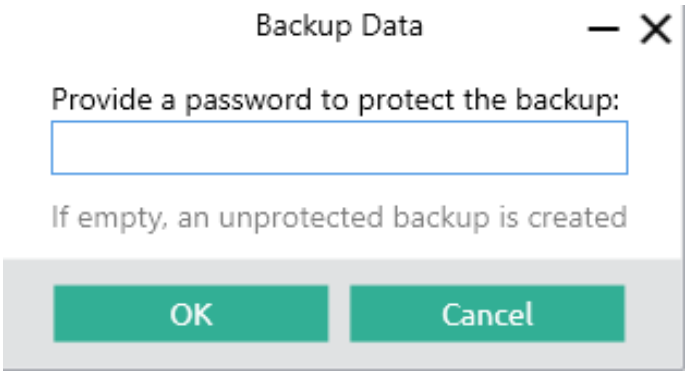
El certificado debe incluir el uso de clave mejorado (EKU) «Encrypting File System» y debe encontrarse en uno de los siguientes almacenes de certificados del ordenador:

- Personal
- Editores de confianza
- Autoridades de certificación raíz de terceros
- Otras personas

El almacén «Personal» es el preferido.

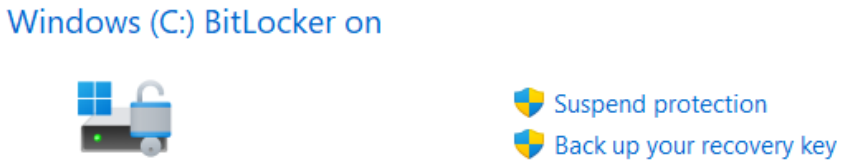
Cifrar las copias de seguridad

Las copias de seguridad de la base de datos deben protegerse con contraseñas seguras generadas aleatoriamente:



Habilitar el cifrado de disco

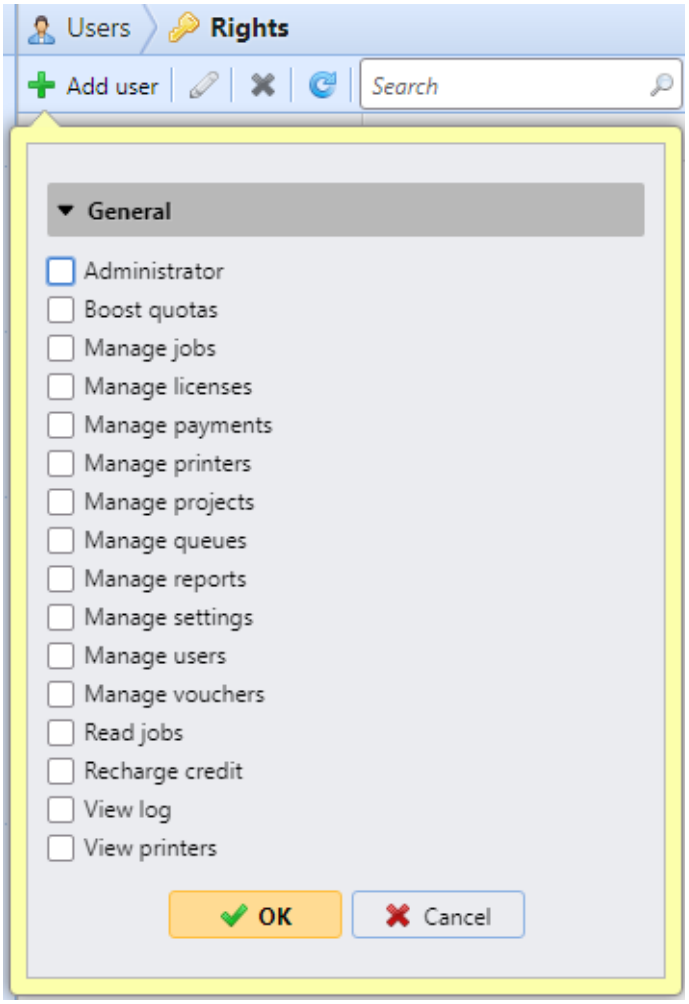
Si es posible, se debe habilitar una tecnología de cifrado completo del disco, como Microsoft BitLocker, en el Print Server de MyQ para proteger los datos en reposo:



1.2.4 PS Recomendaciones adicionales

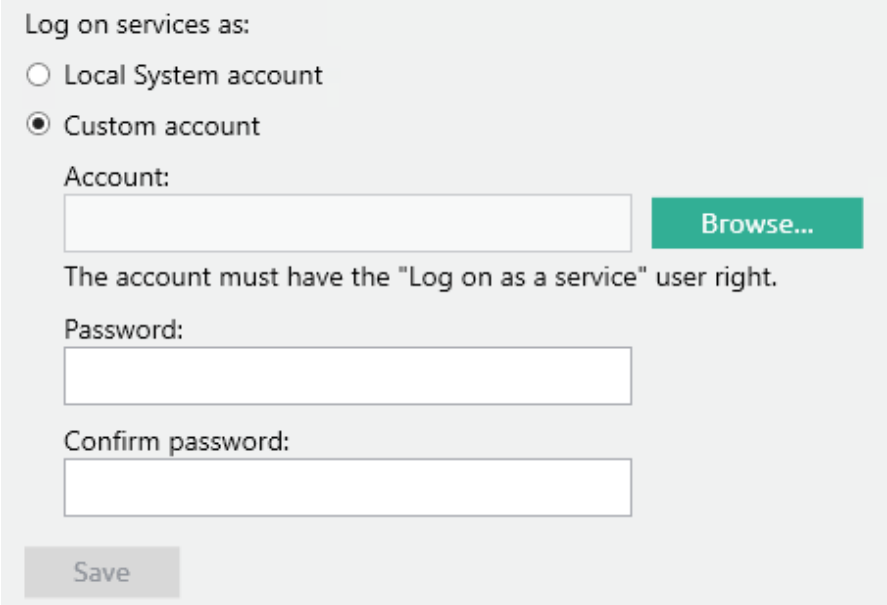
Implemente RBAC

No utilice la cuenta *admin predeterminada para operaciones habituales. Utilice en su lugar la delegación de privilegios, aplicando el principio del privilegio mínimo:



Configurar una cuenta de servicio personalizada

MyQ Print Server se ejecuta de forma predeterminada bajo la cuenta SYSTEM, que tiene privilegios elevados. En su lugar, configure una cuenta de servicio personalizada con una contraseña segura:



Mantenga el servidor actualizado

Instala las actualizaciones de seguridad proporcionadas por MyQ tan pronto como estén disponibles. Puedes comprobar la versión de la aplicación actualmente instalada en MyQ Easy Config:



Mantenga el sistema operativo seguro

MyQ Print Server es tan seguro como el sistema operativo subyacente. Manténgalo actualizado y aplique las políticas de seguridad recomendadas por Microsoft.

Actualice regularmente su software para corregir vulnerabilidades de seguridad y mejorar el rendimiento. Consulte los requisitosdel sistema para ver la lista de requisitos y recomendaciones.

Por ejemplo, .NET debe actualizarse mediante herramientas de gestión o a través de Windows Update, de forma opcional[5].

Planifique la recuperación ante desastres

Realice copias de seguridad periódicas del Print Server de MyQ, incluyendo la base de datos, los certificados y los archivos de configuración. Pruebe el procedimiento de recuperación al menos una vez.

1.3 Cliente de escritorio MyQ X

Páginas OEM vinculadas
This ScriptRunner macro could not be rendered for export.

El Desktop Client MyQ emplea mecanismos de seguridad robustos para garantizar la comunicación segura, la autenticación y la integridad de los datos en los entornos de impresión empresariales. Este documento detalla los protocolos, los métodos de autenticación y las prácticas recomendadas de configuración que sustentan la arquitectura de seguridad del Desktop Client, centrándose en el cifrado TLS, la autenticación integrada de Windows (IWA), Kerberos, NTLM y la integración de Entra ID. Se analizan implementaciones técnicas como el registro del nombre principal del servicio (SPN), la gestión de certificados y los flujos de inicio de sesión silencioso para demostrar el cumplimiento de las normas de seguridad modernas.

1.3.1 Arquitectura de comunicación segura

Cifrado TLS por defecto

Los servidores de impresión y Central Server aplican el cifrado TLS 1.2+ para todos los canales de comunicación, incluidas las interacciones con Desktop Client. Esto garantiza la confidencialidad y la integridad de los datos durante el almacenamiento

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

en cola de trabajos, la autenticación y la generación de informes. Los administradores deben configurar los puntos finales HTTPS utilizando nombres de dominio completos (FQDN) para evitar ataques de tipo «man-in-the-middle» (MITM).

Modos de validación de certificados

- **Modo estricto**: requiere que los certificados de servidor sean emitidos por una autoridad de certificación (CA) de confianza o añadidos manualmente al almacén de confianza del sistema. Los intentos de conexión fallan si la validación falla. Recomendamos utilizar el modo estricto siempre que sea posible.
- **Modo normal**: permite a los usuarios omitir las advertencias de certificados no fiables, con los certificados aceptados almacenados en `%ProgramData%\MyQ\Desktop Client\cert.store` para futuras sesiones.

1.3.2 Mecanismos de autenticación

Autenticación integrada de Windows (IWA)

La IWA permite una autenticación fluida en entornos unidos a un dominio mediante Kerberos o NTLM. El servidor aprovecha la API del servidor HTTP de Windows (`http.sys`) para gestionar las solicitudes HTTP entrantes y validar los nombres principales de servicio (SPN), lo que garantiza la integridad del protocolo.

Flujo de trabajo de Kerberos

1. **Adquisición de tickets de concesión de tickets (TGT)**: los clientes unidos al dominio obtienen un TGT del centro de distribución de claves (KDC).
2. **Solicitud de ticket de servicio**: el cliente solicita un ticket de servicio `HTTP/<FQDN>` al KDC.
3. **Validación del token**: El servidor MyQ valida el ticket de servicio con el SPN registrado.

Configuración crítica:

- El servidor debe tener un SPN correctamente configurado para que la autenticación Kerberos funcione correctamente.
- El acceso a través de direcciones IP omite Kerberos, lo que obliga a recurrir a NTLM.

Aplicación de Kerberos

Para entornos que requieren una seguridad más estricta, es posible configurar la aplicación para que **utilice exclusivamente Kerberos** y no permita el recurso a NTLM. Esto se hace a nivel de servidor, no exclusivamente para el Desktop Client.

1. Desactivar NTLM a través de `KerberosOnly=True` en `config.ini`.
2. Registrar SPN para todos los servidores MyQ utilizando `setspn`.
3. Utilice FQDN en lugar de direcciones IP para los puntos finales del servidor.

Recurso NTLM

NTLM sirve como alternativa en escenarios que no son de dominio o basados en IP. Aunque es menos seguro, utiliza un mecanismo de desafío-respuesta con hash con la contraseña del usuario. Para aplicar Kerberos de forma exclusiva, siga la sugerencia anterior.

Inicio de sesión silencioso de Entra ID

Para los dispositivos híbridos o unidos a Entra ID, Desktop Client utiliza la biblioteca de autenticación de Microsoft (MSAL) y el administrador de autenticación de Windows (WAM) para adquirir tokens de forma silenciosa a través de la cuenta del sistema operativo. El flujo implica:

1. **Adquisición de tokens**: MSAL recupera un token de identificación utilizando WAM.
2. **Intercambio de tokens**: el token de identificación se intercambia por un token de acceso MyQ para autenticar las llamadas a la API REST.

Flujo de código de autorización OAuth 2.0

Para entornos que no sean Windows, Desktop Client admite OAuth 2.0 a través de la `authorization_code` concesión:

1. **Redirección de usuario**: el cliente redirige a los usuarios a la página de inicio de sesión de MyQ.
2. **Intercambio de código**: Después de la autenticación, el código de autorización se intercambia por un token de acceso.

Configuración de Entra ID

- Habilite **el inicio de sesión con Microsoft** en la configuración del servidor MyQ para dispositivos híbridos.

- Asegúrese de que los dispositivos estén registrados en Entra ID para aprovechar la autenticación silenciosa.

Gestión de certificados

Certificados raíz de confianza

- **Modo estricto**: los certificados deben estar preinstalados en el almacén de confianza del sistema operativo (por ejemplo, a través de la política de grupo).
- **Modo normal**: los certificados aprobados por el usuario se almacenan en `cert.store` y se reutilizan para sesiones posteriores.

Flujo de trabajo de validación

1. La validación del certificado del servidor comprueba la cadena de confianza.
2. Si la validación falla, los usuarios reciben un mensaje para aceptar o rechazar el certificado (esto solo ocurre si se utiliza el modo de validación normal en lugar del estricto).
3. Los certificados aceptados se almacenan en caché para evitar que se repitan los mensajes (esto solo ocurre si se utiliza el modo de validación normal en lugar del estricto).

Prácticas recomendadas para certificados
Recomendamos implementar siempre certificados firmados por CA empresariales para los servidores MyQ.

Conclusión

MyQ Desktop Client integra autenticación y cifrado de nivel empresarial para mitigar riesgos como el robo de credenciales y el espionaje. Al aplicar Kerberos, TLS y la validación de certificados, las organizaciones pueden alinearse con los principios de Zero Trust y, al mismo tiempo, mantener la usabilidad a través de flujos de autenticación silenciosos.

2 Informe sobre la seguridad de MyQ X

Descripción general de las funciones de seguridad de MyQ X

MyQ X ofrece una serie de funciones que mejoran la seguridad y la privacidad tanto de los usuarios finales como de la empresa. Estas funciones comienzan con la impresión segura en el equipo multifunción, la personalización de la sesión de usuario y tienen un impacto continuo incluso después de imprimir un documento, gracias al uso de marcas de agua.

A continuación, se incluye un breve resumen de las funciones de seguridad de MyQ X:

- Cumplimiento del RGPD
- Impresión segura
- Sesiones de usuario con múltiples opciones de autenticación, incluida la autenticación de dos factores.
- Cierre de sesión manual y automático de las sesiones de usuario
- Cifrado de datos de extremo a extremo, incluido el cifrado de datos en reposo (base de datos, trabajos, registros).
- Carpetas de destino de escaneo fijas predefinidas por el administrador de MyQ.
- Colas privadas para eliminar trabajos de impresión inmediatamente después de su liberación.
- Modo de privacidad para anonimizar los nombres de los trabajos de impresión
- Acceso restringido a las opciones de configuración del Print Server en la interfaz web de MyQ X.
- Derechos personalizables para acceder a diferentes opciones de configuración.
- Múltiples niveles de complejidad de contraseñas
- Registro de auditoría para cambios en la configuración
- Soporte para la autoridad certificadora de la empresa
- Marcas de agua en documentos impresos
- Vista previa del trabajo
- Control de documentos escaneados mediante sistemas OCR y DMS
- Archivo de trabajos

El enfoque de seguridad de MyQ X se basa en el principio de que **La seguridad no es una cuestión secundaria, sino una parte integral de todo el ecosistema de gestión de impresión.**La plataforma implementa una estrategia de defensa integral que protege los datos y los flujos de trabajo en cada etapa del ciclo de vida de los documentos.

2.1 Arquitectura de confianza cero

Siguiendo la metodología «nunca confíe, siempre verifique», MyQ X asume que las amenazas pueden existir tanto dentro como fuera de una red. Cada conexión, usuario

y dispositivo debe ser autenticado y autorizado antes de acceder a los recursos de impresión, lo que garantiza una verificación continua en todas las interacciones.

2.2 Marco de protección trifásico

MyQ X aborda la seguridad a través de tres fases críticas:

2.2.1 Protección de la infraestructura de impresión

Toda la infraestructura de apoyo está debidamente protegida antes de imprimir cualquier documento, incluyendo estaciones de trabajo, dispositivos móviles, servidores, redes y dispositivos de impresión.

2.2.2 Protección de los flujos de trabajo de impresión

Los flujos de trabajo seguros y probados, que incluyen la liberación de impresión autenticada, el aislamiento de trabajos y la generación de informes completos, evitan vulnerabilidades que podrían dejar a las organizaciones expuestas.

2.2.3 Protección de la impresión

Protección continua mediante marcas de agua, firmas digitales y registros de auditoría exhaustivos que mantienen la trazabilidad y fomentan un comportamiento responsable por parte de los usuarios.

2.3 Privacidad desde el diseño

La protección de datos está integrada en la arquitectura de MyQ X desde el principio. El sistema minimiza la recopilación de datos, implementa un cifrado sólido y proporciona a los usuarios control sobre su información personal para garantizar el cumplimiento del RGPD y la protección de la privacidad.

2.4 Evolución continua de la seguridad

MyQ X mantiene su seguridad mediante actualizaciones periódicas, la corrección inmediata de vulnerabilidades, la integración de información sobre amenazas y evaluaciones y certificaciones de seguridad continuas realizadas por terceros.

Este enfoque centrado en la seguridad garantiza que las organizaciones puedan implementar MyQ X con confianza, sabiendo que su información confidencial, sus requisitos de cumplimiento normativo y su continuidad operativa están protegidos por medidas de seguridad líderes en el sector.

2.5 Principales mejoras de seguridad en 10.2

MyQ X 10.2 introduce importantes mejoras de seguridad diseñadas para reforzar la protección contra las amenazas cibernéticas en constante evolución, al tiempo que se mantiene la eficiencia operativa. Estas mejoras abordan vulnerabilidades críticas e implementan estándares de seguridad modernos.

2.5.1 Seguridad TLS mejorada

Versión mínima predeterminada de TLS 1.2: MyQ X 10.2 aumenta la versión mínima predeterminada de TLS de 1.1 a 1.2, con soporte para TLS 1.3. Esto elimina el soporte para protocolos SSL obsoletos y cifrados débiles que suponen riesgos de seguridad.

Validación de certificados mejorada: la validación de certificados mejorada impide el uso de certificados caducados o emitidos incorrectamente, lo que protege contra ataques de intermediarios y otras vulnerabilidades. El sistema ahora confía automáticamente en los certificados CA raíz del almacén de certificados del sistema del servidor.

2.5.2 Mejoras en la seguridad de la autenticación

Seguridad mejorada de contraseñas y PIN: los algoritmos de hash de contraseñas mejorados refuerzan la protección de las credenciales. El sistema introduce nuevas reglas de seguridad para los PIN, entre las que se incluyen una longitud mínima obligatoria de 6 dígitos y la prevención de combinaciones fáciles de adivinar, como «1234» o «1111».

Protección contra intentos de inicio de sesión: los intentos de autenticación fallidos ahora están limitados por razones de seguridad. De forma predeterminada, los clientes/dispositivos se bloquean durante 5 minutos después de más de 5 intentos de inicio de sesión no válidos en 60 segundos, con períodos de tiempo configurables.

Registro mejorado de eventos de inicio de sesión: el registro mejorado de los eventos de inicio de sesión, especialmente los intentos de autenticación fallidos, facilita a los administradores el filtrado y la supervisión de los eventos de seguridad en MyQ Log.

2.5.3 Actualizaciones de seguridad de la base de datos

Implementación de Firebird 4.0: la actualización al motor de base de datos Firebird 4.0 aporta funciones de seguridad mejoradas y un mayor rendimiento. Las

contraseñas de la base de datos ahora se ocultan en los archivos de registro para evitar la exposición de las credenciales.

Protección de datos mejorada: acceso limitado a los datos confidenciales a través de informes personalizados y cuentas de informes externas, lo que garantiza la confidencialidad de los datos en los diferentes niveles de acceso.

2.5.4 Resolución de vulnerabilidades

Correcciones críticas de CVE: MyQ X 10.2 aborda múltiples vulnerabilidades críticas, entre las que se incluyen:

- CVE-2024-28059: vulnerabilidad de ejecución remota de código no autenticado.
- CVE-2024-22076: Mejoras en la seguridad de los scripts PHP.
- CVE-2023-45853, CVE-2023-5678, CVE-2023-49316: vulnerabilidades de componentes de terceros.

Actualizaciones de seguridad de componentes: Las versiones actualizadas de componentes críticos, como OpenSSL 3.1.0, PHP 8.3.14 y Apache 2.4.57, solucionan vulnerabilidades de seguridad conocidas.

2.5.5 Seguridad de la API y la integración

Restricciones de la API REST: se han limitado los ámbitos de los clientes conocidos y se han eliminado las capacidades para operaciones sensibles, como el cambio de servidores de autenticación de usuarios, lo que refuerza la seguridad de la API.

Controles de scripts PHP: los nuevos ajustes de Easy Config permiten a los administradores bloquear/desbloquear el acceso a scripts PHP, lo que mejora la seguridad al mantener estos ajustes en modo de solo lectura.

2.5.6 Seguridad administrativa

Seguridad mejorada de la cuenta de administrador: se ha eliminado la contraseña de administrador predeterminada para las nuevas instalaciones. Los administradores ahora pueden desactivar las cuentas de administrador cuando no sean necesarias, lo que fomenta el uso de cuentas de usuario específicas con los derechos adecuados en lugar de cuentas administrativas compartidas.

Estas mejoras de seguridad demuestran el compromiso de MyQ X con el mantenimiento de los estándares de seguridad de nivel empresarial, al tiempo que abordan los retos actuales de ciberseguridad. Las actualizaciones de seguridad

periódicas y la gestión proactiva de las vulnerabilidades garantizan que las organizaciones puedan implementar MyQ X con confianza en su seguridad.

2.6 Valor empresarial de la gestión segura de la impresión

La gestión segura de la impresión ofrece un valor empresarial cuantificable al transformar la infraestructura de impresión de un posible pasivo en un activo estratégico de seguridad. MyQ X proporciona a las organizaciones una protección integral que aborda todo el espectro de riesgos relacionados con la impresión, al tiempo que mejora la eficiencia operativa.

2.6.1 Mitigación de riesgos y reducción de costes

Prevención de violaciones de datos: Secure Print Release garantiza que los documentos confidenciales nunca se dejen sin supervisión en las bandejas de las impresoras, lo que elimina el acceso no autorizado a información sensible. Los usuarios se autentican antes de que se liberen sus trabajos, lo que mantiene un control total sobre la seguridad de los documentos.

Evitar costes de cumplimiento normativo: las funciones integradas de cumplimiento de las normativas GDPR, HIPAA y SOX ayudan a las organizaciones a evitar sanciones reglamentarias y a reducir los costes de preparación de auditorías mediante controles de cumplimiento automatizados y registros de auditoría completos.

Continuidad operativa: la función Device Spooling de MyQ mantiene las capacidades de impresión durante las interrupciones del servidor, almacenando los trabajos cifrados localmente durante un máximo de una semana en 10 dispositivos, lo que evita la interrupción del negocio durante el mantenimiento del sistema o el tiempo de inactividad inesperado.

2.6.2 Principios de seguridad mejorados

Implementación de confianza cero: al exigir la autenticación para cada trabajo de impresión, MyQ X aplica los principios de «nunca confiar, siempre verificar» en todo el entorno de impresión, lo que refuerza la postura de seguridad general de la organización.

Trazabilidad de documentos: las marcas de agua y las firmas digitales permiten a las organizaciones realizar un seguimiento de los documentos confidenciales a lo largo

de su ciclo de vida, lo que proporciona responsabilidad y disuade del uso indebido de información sensible.

Cifrado completo: el cifrado de extremo a extremo de los datos de impresión, las bases de datos y los trabajos almacenados garantiza que la información confidencial permanezca protegida a lo largo de todo el flujo de trabajo documental, cumpliendo con los estrictos requisitos de seguridad.

2.6.3 Eficiencia operativa

Optimización del ancho de banda: el spooling de clientes reduce el tráfico de red al procesar los trabajos localmente, lo que mejora el rendimiento en entornos con ancho de banda limitado, como oficinas remotas y sucursales.

Autenticación flexible: las múltiples opciones de autenticación, que incluyen tarjetas de identificación, PIN, contraseñas y autenticación mediante aplicaciones móviles, proporcionan a los usuarios métodos de acceso cómodos y seguros que se adaptan a las diversas necesidades de la organización. También está disponible la autenticación multifactorial (MFA), que combina estos métodos.

Gestión centralizada: las políticas de seguridad unificadas en todos los dispositivos simplifican la administración y garantizan unos estándares de protección coherentes en toda la organización.

2.6.4 Ventajas estratégicas para el negocio

Ventaja competitiva: demostrar unas sólidas capacidades de seguridad de impresión puede diferenciar a las organizaciones en mercados competitivos, especialmente en sectores que manejan datos confidenciales o que prestan servicio a clientes preocupados por la seguridad.

Confianza de los empleados: los flujos de trabajo de impresión seguros dan a los usuarios la confianza de que sus documentos están protegidos, lo que mejora la productividad y reduce las preocupaciones relacionadas con la seguridad que pueden afectar a la eficiencia en el lugar de trabajo.

Infraestructura preparada para el futuro: el completo marco de seguridad de MyQ X permite a las organizaciones adaptarse a las amenazas de ciberseguridad y a los requisitos normativos en constante evolución sin necesidad de realizar grandes reformas en la infraestructura.

La gestión segura de la impresión con MyQ X transforma la impresión de una posible vulnerabilidad de seguridad en un proceso empresarial controlado, auditable y

conforme que respalda los objetivos de la organización al tiempo que protege los valiosos activos de información.

2.7 Conformidad

El completo marco de cumplimiento de MyQ X demuestra su compromiso con el cumplimiento de los más altos estándares internacionales de seguridad y requisitos normativos. Este enfoque multicapa garantiza que las organizaciones puedan implementar MyQ X con confianza, al tiempo que satisfacen los diversos requisitos de cumplimiento normativo de los distintos sectores y jurisdicciones.

2.7.1 Certificación e implementación de la norma ISO 27001:2022

MyQ ha obtenido **la certificación ISO/IEC 27001:2022**, lo que establece un enfoque sistemático para la gestión de la seguridad de la información que cumple con las mejores prácticas internacionales. La implementación abarca:

Marco de gestión de riesgos: procesos exhaustivos de evaluación de riesgos que identifican, evalúan y mitigan los riesgos de seguridad de la información en todas las operaciones comerciales y las implementaciones de los clientes.

Implementación de controles de seguridad: implementación estructurada de controles de seguridad técnicos, administrativos y físicos que protegen los activos de información a lo largo de su ciclo de vida.

Proceso de mejora continua: revisiones y actualizaciones periódicas de las políticas, procedimientos y controles de seguridad para hacer frente a las amenazas en constante evolución y mantener el cumplimiento de la certificación.

Compromiso de la dirección: supervisión a nivel ejecutivo que garantiza que la seguridad siga estando integrada en la estrategia empresarial y en los procesos de toma de decisiones operativas.

La certificación valida el enfoque sistemático de MyQ para proteger los datos de los clientes y mantener la confidencialidad, integridad y disponibilidad de los sistemas de información.

2.7.2 Marco de cumplimiento del RGPD y medidas de protección de datos

MyQ X implementa **un cumplimiento** integral **del RGPD** a través de principios de privacidad desde el diseño integrados en toda la arquitectura del sistema:

Minimización de datos: el sistema recopila solo los metadatos esenciales necesarios para el funcionamiento operativo, evitando el procesamiento innecesario de datos personales que podría aumentar los riesgos de cumplimiento.

Gestión de los derechos de los usuarios: implementación completa de los derechos de los usuarios del RGPD, incluyendo:

- Derecho de acceso a los datos personales
- Derecho a la rectificación de la información inexacta
- Derecho de supresión («derecho al olvido»)
- Derecho a la portabilidad de los datos
- Derecho a restringir el tratamiento

Evaluaciones de impacto en materia de protección de datos: evaluación sistemática de los riesgos para la privacidad de las nuevas funciones y despliegues, garantizando el cumplimiento del RGPD a lo largo de la evolución del sistema.

2.7.3 Requisitos de cumplimiento regionales (HIPAA, SOX)

MyQ X es compatible con marcos de cumplimiento específicos del sector mediante sólidas capacidades de protección de datos y auditoría:

Cumplimiento de la HIPAA para el sector sanitario:

- Cifrado de la información sanitaria protegida (PHI) en reposo y en tránsito.
- Registro de auditoría completo de todos los accesos a datos sanitarios confidenciales.
- Controles de acceso basados en roles que restringen el acceso a la PHI únicamente al personal autorizado.
- Procedimientos seguros de copia de seguridad y recuperación para los requisitos de retención de datos sanitarios.

Cumplimiento de la ley SOX para servicios financieros:

- Registros de auditoría detallados para el procesamiento y la impresión de documentos financieros.
- Controles de acceso que impiden la modificación no autorizada de los registros financieros.
- Funciones de archivo seguro que cumplen los requisitos normativos de conservación.
- Segregación de funciones mediante permisos basados en roles y flujos de trabajo de aprobación.

Controles de seguridad adicionales:

- Cifrado de bases de datos mediante algoritmos estándar del sector.
- Protocolos de comunicación seguros para todas las transmisiones de datos.

- Procedimientos de copia de seguridad automatizados con cifrado y verificación de integridad.
- Registro y supervisión de accesos para la elaboración de informes de cumplimiento.

2.7.4 Prácticas seguras del ciclo de vida del desarrollo de software (SSDLC)

MyQ implementa un ciclo de vida de desarrollo de software seguro alineado con los estándares del sector y los requisitos de la cadena de suministro **de SLSA**, lo que garantiza que las prácticas de seguridad se integren en todas las fases del ciclo de vida del software.

Análisis

MyQ realiza **un** riguroso **modelado de amenazas** y define **requisitos de seguridad** claros durante la fase de análisis inicial, lo que permite identificar los riesgos de forma temprana y establecer una base de seguridad sólida antes de comenzar el diseño.

Diseño

Todas las propuestas arquitectónicas se someten a **revisiones** formales **de la arquitectura de seguridad** para validar el cumplimiento de principios como **el privilegio mínimo**, **la confianza cero** y **la defensa en profundidad**, lo que garantiza que la seguridad se incorpore de forma sistemática en el diseño del sistema.

Desarrollo

Los desarrolladores siguen **prácticas de codificación segura** y procesos de revisión por pares, mientras que todas las compilaciones se ejecutan en **servidores de compilación** dedicados y aislados **que cumplen con SLSA**, lo que garantiza la protección de la integridad del código fuente y los artefactos de compilación.

Pruebas

Las pruebas de seguridad incluyen **SAST** automatizado y **escaneo de dependencias** integrados en los procesos de CI, lo que permite la detección temprana de vulnerabilidades tanto en el código personalizado como en los componentes de terceros.

Implementación

Todos los artefactos de lanzamiento están protegidos mediante **la firma de código** y se verifican durante la implementación, lo que garantiza **la integridad**, **la autenticidad** y la entrega controlada en los entornos de producción.

Mantenimiento

Tras la implementación, los sistemas se someten a **una supervisión** continua y a **una gestión** estructurada **de parches**, lo que garantiza una alineación constante con las amenazas en constante evolución y **las mejores prácticas de seguridad**.

2.7.5 Auditorías de seguridad y pruebas de penetración periódicas

MyQ mantiene una sólida validación de la seguridad mediante programas sistemáticos de pruebas y evaluación:

Pruebas de penetración automatizadas: la integración con la plataforma de seguridad Qualys proporciona una evaluación continua de vulnerabilidades y pruebas de penetración para todas las versiones de software.

Evaluaciones de seguridad de terceros: auditorías de seguridad independientes realizadas por organizaciones externas cualificadas para validar los controles de seguridad e identificar posibles mejoras.

Revisiones de seguridad internas: evaluaciones internas periódicas de las políticas, procedimientos y controles técnicos de seguridad para garantizar su eficacia y cumplimiento continuos.

Proceso de respuesta a vulnerabilidades: procedimientos estructurados para abordar los problemas de seguridad identificados, incluidos los requisitos de plazos para el desarrollo y la implementación de parches.

2.7.6 Lista de materiales de software y gestión de vulnerabilidades

MyQ implementa una seguridad integral de la cadena de suministro mediante un seguimiento detallado de los componentes y la gestión de vulnerabilidades:

Publicación de la SBOM: documentación completa de la lista de materiales de software que identifica todos los componentes, bibliotecas y dependencias de terceros utilizados en los sistemas MyQ X.

Escaneo automatizado de vulnerabilidades: supervisión continua de las bases de datos de componentes para detectar nuevas vulnerabilidades identificadas que afecten a las dependencias de MyQ X.

Gestión rápida de parches: proceso sistemático para evaluar, probar e implementar actualizaciones de seguridad para componentes de terceros, con priorización basada en la evaluación de riesgos.

Control de versiones de componentes: seguimiento detallado de todos los componentes de software, incluidos los números de versión, los niveles de parches de seguridad y los calendarios de actualización, tal y como se documenta en las notas de la versión.

Evaluación de la seguridad de los proveedores: evaluación de los proveedores de software de terceros para garantizar que mantienen los estándares de seguridad y los procesos de divulgación de vulnerabilidades adecuados.

Este completo marco de cumplimiento garantiza que MyQ X cumple diversos requisitos normativos, al tiempo que mantiene los más altos estándares de seguridad de la información y protección de datos en todos los entornos operativos.

2.8 Implantación de la arquitectura de confianza cero

MyQ X implementa la arquitectura Zero Trust como enfoque de seguridad fundamental que elimina la confianza implícita y valida continuamente cada transacción. Este marco integral garantiza que ningún usuario, dispositivo o conexión de red sea de confianza por defecto, independientemente de su ubicación o estado de autenticación anterior.

2.8.1 Principios de confianza cero en la gestión de la impresión

La implementación de confianza cero de MyQ X se basa en el principio de **«nunca confiar, siempre verificar»** en todo el sistema de gestión de impresión. El sistema requiere una verificación explícita para cada solicitud de acceso, lo que garantiza que:

Canales de comunicación cifrados: todo el tráfico de red utiliza el cifrado TLS obligatorio con una versión mínima de 1.2, lo que evita el espionaje y la manipulación durante la transmisión de datos. Los certificados HTTPS deben estar correctamente configurados y validados para evitar ataques de tipo «man-in-the-middle».

Aplicación de protocolos seguros: MyQ X bloquea el tráfico HTTP no cifrado y aplica protocolos de seguridad sólidos en todos los canales de comunicación, incluidas las conexiones SMTP, LDAP y SNMP. Los protocolos heredados como SNMPv1 están prohibidos en favor de SNMPv3 con autenticación sólida.

Controles de seguridad de la API: El acceso a la API REST requiere tokens de autenticación con filtrado de direcciones IP, lo que garantiza que las llamadas a la API estén autenticadas y procedan de fuentes fiables. Los secretos de los clientes se someten a una rotación periódica para mantener la integridad de la seguridad.

2.8.2 Metodología «Nunca confíes, siempre verifica»

La metodología Zero Trust impregna todos los aspectos de las operaciones de MyQ X a través de mecanismos de verificación continua:

Verificación de identidad: cada interacción del usuario requiere autenticación, independientemente de la ubicación de la red o del estado de confianza del dispositivo. Los usuarios deben autenticarse en cada dispositivo de impresión, incluso si ya han iniciado sesión en otro lugar de la organización.

Autenticación de dispositivos: los propios dispositivos de impresión deben autenticarse antes de acceder a los recursos de la red, con credenciales y certificados únicos que impiden la suplantación de dispositivos no autorizados.

Gestión de sesiones: las sesiones de los usuarios implementan una función de tiempo de espera y cierre de sesión automáticos, lo que garantiza que las sesiones abandonadas no puedan ser explotadas por personas no autorizadas.

2.8.3 Segmentación y aislamiento de la red

MyQ X implementa una segmentación completa de la red para limitar las superficies de ataque y contener posibles brechas de seguridad:

Controles de los límites de la red: el sistema aplica estrictas reglas de firewall que bloquean los puertos no utilizados y limitan el acceso a la red solo a los canales de comunicación necesarios. Las configuraciones predeterminadas desactivan los servicios y protocolos innecesarios.

Segmentación basada en certificados: MyQ X admite tres modos de gestión de certificados (autoridad de certificación integrada, autoridad de certificación de la empresa y gestión manual de certificados), lo que permite a las organizaciones implementar límites de confianza adecuados en función de sus políticas de seguridad.

Aplicación de FQDN: Todas las comunicaciones de red deben utilizar nombres de dominio completos (FQDN) en lugar de direcciones IP o nombres de una sola etiqueta, lo que evita los ataques de intermediarios basados en DNS y garantiza la validación adecuada de los certificados.

Gestión de puertos: el sistema gestiona automáticamente las reglas del cortafuegos y proporciona un control explícito sobre los puertos de red a los que se puede acceder, lo que reduce la superficie de ataque mediante el bloqueo sistemático de puertos.

2.8.4 Autenticación y verificación robustas

MyQ X mantiene una validación de seguridad continua a través de múltiples capas de autenticación y supervisión en tiempo real:

Autenticación multimétodo: el sistema admite diversos métodos de autenticación, incluidos LDAP, Microsoft Entra ID, RADIUS y la autenticación local de MyQ, con capacidades de conmutación automática por error que garantizan un control de acceso continuo.

Integración del servidor de autenticación: la integración segura con servidores de autenticación externos utiliza conexiones cifradas (TLS para LDAP, protocolos seguros para RADIUS) y aplica secretos compartidos sólidos específicos para cada implementación de MyQ.

Supervisión de inicio de sesión: el registro mejorado de los eventos de autenticación, en particular los intentos de inicio de sesión fallidos, permite a los administradores detectar y responder a posibles amenazas de seguridad. Los intentos de autenticación fallidos activan mecanismos de bloqueo automático: por defecto, los dispositivos se bloquean durante 5 minutos después de más de 5 intentos no válidos en 60 segundos.

Controles de persistencia de sesión: el sistema implementa políticas de tiempo de espera de sesión configurables y una función de cierre de sesión automático, lo que garantiza que las sesiones inactivas no puedan ser explotadas.

2.8.5 Verificación de dispositivos y puntos finales

MyQ X aplica estrictos protocolos de verificación de dispositivos para garantizar que solo los terminales autorizados puedan acceder a los recursos de impresión:

Gestión de certificados de dispositivos: Todos los dispositivos conectados deben presentar certificados válidos para la comunicación en red. El sistema mantiene un almacén de certificados completo con la validación adecuada de la cadena y admite la implementación automática de certificados a través de la política de grupo o la gestión de dispositivos móviles (MDM).

Controles de seguridad de terminales: Los dispositivos de impresión se someten a una validación de seguridad continua, que incluye la autenticación SNMP v3 con contraseñas seguras y algoritmos criptográficos (SHA1 y AES). Las credenciales de la impresora se gestionan a través de protocolos de seguridad específicos del proveedor con contraseñas seguras generadas aleatoriamente.

Autenticación de dispositivos móviles: MyQ X Mobile Client implementa la concesión de autorización de dispositivos OAuth 2.0 para una autenticación segura de los dispositivos móviles, sustituyendo los sistemas heredados basados en PIN por una seguridad moderna habilitada para la biometría.

Marco de seguridad BYOD: el sistema es compatible con entornos Bring-Your-Own-Device (BYOD) a través de la propagación segura de la impresión mediante AirPrint y Mopria, manteniendo los principios de confianza cero incluso en redes sin visibilidad directa del Print Server.

Gestión de tokens de acceso: se emiten tokens de acceso únicos para cada tipo de dispositivo, siendo obligatorio el uso de Transport Layer Security (TLS) para todas las comunicaciones. El sistema implementa controles de acceso Just-in-Time (JIT) que ajustan dinámicamente los privilegios en función del contexto y la evaluación continua de riesgos.

Esta implementación integral de confianza cero garantiza que MyQ X mantenga los más altos estándares de seguridad, al tiempo que da soporte a diversas necesidades organizativas y escenarios de implementación. La arquitectura proporciona una protección de defensa en profundidad que se adapta a los cambiantes escenarios de amenazas, al tiempo que mantiene la eficiencia operativa y la experiencia del usuario.

2.9 Gestión de identidades y accesos

MyQ X proporciona un marco completo de gestión de identidades y accesos que se integra perfectamente con los sistemas de autenticación empresariales existentes y es compatible con los estándares de seguridad modernos. La arquitectura IAM garantiza una autenticación de usuarios segura, escalable y flexible en diversos entornos organizativos.

2.9.1 Implementación de la autenticación multifactorial

MyQ X implementa sólidas capacidades **de autenticación multifactorial (MFA)** que mejoran significativamente la seguridad al requerir múltiples factores de verificación:

Autenticación de Embedded Terminal: los métodos MFA estándar incluyen combinaciones de tarjeta de identificación y PIN, en las que los usuarios primero presentan su tarjeta de identificación física y luego confirman su identidad con un código PIN. Alternativamente, la autenticación con tarjeta de identificación y contraseña proporciona una seguridad de dos factores similar con verificación de contraseña en lugar de PIN.

Autenticación basada en dispositivos móviles: MyQ X Mobile Client permite una MFA sofisticada mediante el escaneo de códigos QR combinado con la verificación biométrica. Los usuarios se autentican escaneando un código QR que se muestra en el Embedded Terminal, con seguridad adicional proporcionada a través de bloqueos biométricos (Face ID o huella dactilar) en sus dispositivos móviles.

Integración del Desktop Client: Las organizaciones que utilizan los servicios de Microsoft 365 se benefician de la MFA integrada a través de la autenticación Entra ID. A los usuarios que tienen habilitada la autenticación de dos factores en sus cuentas Entra ID se les solicita automáticamente que verifiquen su identidad mediante aplicaciones de autenticación cuando acceden al Desktop Client.

2.9.2 Concesión de autorización de dispositivos OAuth 2.0

MyQ X es compatible con el estándar **de concesión de códigos de autorización OAuth 2.0**, lo que permite una integración segura con proveedores de identidad modernos y aplicaciones de terceros:

Flujo OAuth estándar: el sistema implementa el marco de autorización OAuth 2.0 completo, incluida la presentación de la página de inicio de sesión, la generación de códigos de acceso únicos y la recuperación segura de tokens. Las aplicaciones cliente reciben tokens de portador con tiempos de caducidad configurables y ámbitos concedidos.

Seguridad de la integración de la API: se deben proporcionar tokens OAuth para todos los accesos a puntos finales de la API, lo que garantiza que las integraciones de terceros mantengan una autenticación adecuada. El sistema admite la validación del ID del cliente y el secreto del cliente con coincidencia segura de URI de redireccionamiento.

Gestión de tokens: los tokens de acceso incluyen controles de caducidad (por defecto, 1800 segundos) y restricciones de ámbito, lo que proporciona un control granular sobre los permisos de acceso a la API, al tiempo que se mantiene la seguridad mediante la rotación de tokens.

2.9.3 Capacidades de integración de inicio de sesión único

MyQ X proporciona una integración completa **de inicio de sesión único (SSO)** que agiliza la autenticación de usuarios en entornos empresariales:

Integración con Microsoft 365: la profunda integración con Microsoft Entra ID permite un SSO sin problemas para las organizaciones que utilizan los servicios de Microsoft 365. Los usuarios pueden autenticarse utilizando sus credenciales de Microsoft existentes, lo que elimina la necesidad de contraseñas MyQ independientes.

Servicios de directorio empresarial: las capacidades de SSO se extienden a varios servidores de autenticación, incluidos Active Directory, OpenLDAP y Novell eDirectory, lo que permite a los usuarios aprovechar las credenciales empresariales existentes para acceder al servidor MyQ.

Autenticación multiplataforma: la funcionalidad SSO funciona en todos los componentes de MyQ X, incluidos el Desktop Client, el cliente móvil y el Embedded Terminal, lo que proporciona experiencias de autenticación coherentes independientemente del método de acceso.

2.9.4 Control de acceso basado en roles (RBAC)

MyQ X implementa **un** sofisticado **control de acceso basado en roles** que se ajusta a los requisitos de seguridad de la empresa:

Gestión granular de permisos: el sistema proporciona un control detallado sobre los permisos de los usuarios, lo que permite a los administradores definir derechos de acceso específicos basados en las funciones y responsabilidades de la organización.

Administración basada en grupos: la implementación de RBAC admite tanto permisos de usuario individuales como control de acceso basado en grupos, lo que permite una gestión eficiente de grandes poblaciones de usuarios mediante asignaciones de grupos de seguridad.

Aplicación del privilegio mínimo: los controles de acceso siguen el principio del privilegio mínimo, lo que garantiza que los usuarios reciban solo los permisos mínimos necesarios para sus funciones laborales, al tiempo que se mantiene la eficiencia operativa.

2.9.5 Compatibilidad con Entra ID multitenant

MyQ X ofrece una sólida compatibilidad con **entornos multitenant de Microsoft Entra ID**:

Autenticación entre inquilinos: el sistema puede autenticar a los usuarios en varios inquilinos de Entra ID, lo que permite estructuras organizativas complejas con varias instancias de Azure AD.

Aislamiento de inquilinos: la compatibilidad con múltiples inquilinos incluye mecanismos de aislamiento adecuados que impiden el acceso a datos entre inquilinos, al tiempo que se mantienen las capacidades de gestión centralizada de MyQ.

Gestión híbrida de identidades: la integración admite tanto escenarios de identidades exclusivamente en la nube como híbridos, lo que permite adaptarse a organizaciones con Active Directory local sincronizado con Entra ID.

2.9.6 Integración con LDAP y Active Directory

MyQ X ofrece capacidades completas **de integración con LDAP y Active Directory**:

Opciones de sincronización flexibles: el sistema admite múltiples métodos de sincronización, incluyendo la sincronización completa, la sincronización selectiva de atributos y la sincronización condicional basada en filtros LDAP. Los administradores pueden elegir entre la sustitución completa, la adición exclusiva o las actualizaciones condicionales para las propiedades de la tarjeta y el PIN.

Funciones de filtrado avanzadas: la sincronización LDAP incluye sofisticadas opciones de filtrado que utilizan la sintaxis de filtro LDAP estándar, lo que permite la importación selectiva de usuarios basada en unidades organizativas, pertenencia a grupos o atributos personalizados.

Importación de la estructura de grupos: el sistema puede importar estructuras organizativas completas, incluidos grupos de seguridad, grupos de distribución y jerarquías de grupos anidados desde Active Directory, manteniendo las relaciones organizativas dentro de MyQ.

Autenticación segura: Todas las comunicaciones LDAP utilizan cifrado TLS para proteger las credenciales y los datos de los usuarios durante la sincronización. El sistema es compatible tanto con LDAP tradicional sobre TLS como con conexiones LDAP seguras.

2.9.7 Gestión de PIN temporales y políticas de seguridad

MyQ X implementa **políticas** integrales **de gestión de PIN y seguridad**:

Seguridad mejorada de los PIN: la versión 10.2 introduce una seguridad reforzada de los PIN, que incluye una longitud mínima obligatoria de 6 dígitos y la prevención de combinaciones fáciles de adivinar, como «1234» o «1111».

Emisión de PIN temporales: el sistema admite códigos PIN temporales que se pueden emitir para períodos de tiempo específicos o situaciones de un solo uso, lo que proporciona seguridad adicional para el acceso de invitados o empleados temporales.

Aplicación de políticas de PIN: las políticas de PIN configurables permiten a las organizaciones definir requisitos de complejidad, períodos de caducidad y restricciones de reutilización que se ajustan a las normas de seguridad corporativas.

Protección contra autenticaciones fallidas: la seguridad mejorada incluye el bloqueo automático de los intentos de autenticación tras repetidos fallos (por defecto: bloqueo de 5 minutos tras 5 intentos fallidos en 60 segundos).

2.9.8 Compatibilidad con la autenticación biométrica

MyQ X aprovecha **las** modernas **capacidades de autenticación biométrica** mediante la integración de dispositivos móviles:

Integración biométrica móvil: MyQ X Mobile Client es compatible con métodos de autenticación biométrica, como Face ID en dispositivos iOS y reconocimiento de huellas dactilares en dispositivos Android, lo que proporciona un control de acceso fluido y seguro.

Autenticación multimodal: la autenticación biométrica funciona junto con la seguridad basada en dispositivos, creando un sistema de autenticación multimodal que combina algo que el usuario tiene (dispositivo móvil) con algo que es (características biométricas).

2.10 Seguridad de las infraestructuras

MyQ X proporciona una sólida seguridad de infraestructura que protege todo el entorno de gestión de impresión de las amenazas cibernéticas en constante evolución. La plataforma incorpora múltiples capas de defensa para proteger los servidores, las bases de datos, las comunicaciones de red y la integridad del software, lo que garantiza la fiabilidad operativa y la confidencialidad de los datos.

2.10.1 Fortalecimiento de la seguridad del Print Server

Los servidores de impresión MyQ X se refuerzan utilizando las mejores prácticas de configuración de seguridad definidas en los ajustes **de config.ini**, entre las que se incluyen:

- Restricción de servicios y procesos para limitar la superficie de ataque.
- Habilitación de protocolos de comunicación seguros y deshabilitación de opciones heredadas inseguras.
- Asignación estricta de privilegios de usuario, evitando los privilegios de administrador cuando no sean necesarios.
- Actualizaciones automáticas periódicas y parches de seguridad para corregir las vulnerabilidades recién descubiertas.
- Configuración de reglas de firewall y restricciones de puertos para bloquear el tráfico de red no autorizado.

Estas medidas reducen el riesgo de explotación y mantienen la disponibilidad del sistema incluso en condiciones de ataque.

2.10.2 Cifrado de bases de datos (implementación de Firebird 4.0)

MyQ X utiliza el motor de base de datos **Firebird 4.0**, que proporciona capacidades de cifrado avanzadas para proteger los datos confidenciales en reposo y durante las operaciones de copia de seguridad. Las características clave del cifrado incluyen:

- Cifrado AES-256 de los archivos de la base de datos para impedir el acceso no autorizado a los datos.
- Almacenamiento cifrado de contraseñas y claves dentro del sistema de bases de datos.
- Ocultación del contenido confidencial de la base de datos en los registros y diagnósticos.

Esto garantiza el cumplimiento de las normativas de protección de datos y evita que se comprometa la contabilidad de los trabajos de impresión y la información de los usuarios.

2.10.3 Aplicación de TLS 1.2/1.3 y gestión de certificados

Para proteger los datos en tránsito, MyQ X aplica de forma predeterminada un protocolo **TLS 1.2** mínimo, con la posibilidad de actualizar opcionalmente a TLS 1.3 para mejorar la seguridad y el rendimiento. La plataforma admite modos de gestión de certificados flexibles:

- Generación automática de una autoridad de certificación (CA) raíz privada que firma los certificados del servidor y del cliente.
- Integración de CA intermedias gestionadas por la organización, lo que permite cadenas de confianza corporativas y un control centralizado de los certificados.
- Compatibilidad con la instalación manual de certificados, incluidos los certificados de CA públicos o de terceros.

Los certificados y las claves privadas se almacenan de forma segura con protección cifrada, y los clientes reciben certificados de confianza a través de la política de grupo o la gestión de dispositivos móviles.

2.10.4 Seguridad de las comunicaciones de red

MyQ X protege todos los canales de comunicación de red mediante:

- Bloquea todo el tráfico HTTP no cifrado y solo permite el HTTPS.
- Cifrar el tráfico SMTP, LDAP y RADIUS utilizando TLS para proteger la autenticación y el flujo de correo.
- Desactivar protocolos obsoletos y vulnerables, como los sustitutos de POP3 y STARTTLS.
- Emplea SNMPv3 con autenticación fuerte y algoritmos criptográficos para supervisar y gestionar los dispositivos de forma segura.

Estos controles evitan el espionaje, la suplantación de identidad y los ataques de intermediarios en toda la red.

2.10.5 Configuración del cortafuegos y gestión de puertos

MyQ X reduce las superficies de ataque mediante:

- Desactivar las reglas del firewall para los puertos y protocolos de red no utilizados.
- Permitir un control granular de los puertos que se exponen en función de las políticas de red de la organización.

Esto limita los puntos de entrada a solo aquellos esenciales para los servicios de impresión, lo que mejora las defensas perimetrales.

2.10.6 Seguridad de API y tokens de autenticación

Las API aplican múltiples capas de seguridad:

- El marco de concesión de códigos de autorización OAuth 2.0 protege el acceso a la API mediante tokens de portador de corta duración y restricciones de ámbito.

- Los tokens se validan con las direcciones IP de los clientes y requieren credenciales de cliente seguras.
- Las rotaciones periódicas de secretos protegen contra las fugas de credenciales.

Esto protege los puntos finales de la API contra solicitudes no autorizadas y abusos.

2.10.7 Aislamiento de procesos y sandboxing

Las aplicaciones de gestión de impresión MyQ X se ejecutan con **aislamiento de procesos** para evitar que los componentes comprometidos afecten a todo el sistema. Se emplea un entorno de pruebas virtual o contenedorizado cuando es posible para contener las brechas de seguridad y limitar el movimiento lateral dentro del entorno.

2.10.8 Firma de código y verificación de integridad

Todos los binarios e instaladores del software MyQ están **firmados con código** para garantizar su autenticidad e integridad. Esto garantiza que los clientes instalen versiones de software verificadas, libres de manipulaciones o modificaciones no autorizadas.

2.11 Protección y cifrado de datos

MyQ X implementa una protección y cifrado de datos completos a lo largo de todo el ciclo de vida del documento, lo que garantiza la confidencialidad y la integridad desde el envío inicial de la impresión hasta la salida final y el archivo.

2.11.1 Implementación de cifrado de extremo a extremo

MyQ X proporciona **cifrado de extremo a extremo** en todos los canales de comunicación y puntos de almacenamiento de datos:

Canales de comunicación cifrados: todo el tráfico de red utiliza cifrado TLS obligatorio con una versión mínima de 1.2 por defecto. Se aplica HTTPS para todas las interfaces web, la comunicación entre servidores y las conexiones de clientes.

Seguridad basada en certificados: los múltiples modos de gestión de certificados admiten los requisitos de la organización, desde la autoridad de certificación integrada hasta la integración de PKI corporativa y los certificados CA públicos. Las claves privadas están protegidas por contraseñas generadas aleatoriamente y almacenadas de forma cifrada en la base de datos Firebird.

Seguridad de protocolos: el cifrado TLS se aplica en los protocolos SMTP, LDAP, RADIUS y SNMP, lo que garantiza que no se transmitan datos confidenciales en texto claro.

2.11.2 Cifrado de datos en reposo

MyQ X protege los datos almacenados mediante múltiples capas de cifrado:

Cifrado de bases de datos: la base de datos Firebird 4.0 admite el cifrado mediante certificados personalizados con el uso mejorado de claves (EKU) del «sistema de cifrado de archivos». Los certificados deben ubicarse en almacenes de certificados informáticos designados, preferiblemente en el almacén personal.

Protección del sistema de archivos: los archivos de trabajos de impresión y escaneo almacenados en el Print Server MyQ X se pueden cifrar utilizando certificados personalizados proporcionados por los administradores, lo que añade una capa adicional de protección más allá de los permisos del sistema de archivos.

Cifrado completo del disco: MyQ X admite la integración con tecnologías de cifrado completo del disco, como Microsoft BitLocker, para proteger todos los datos en reposo en el Print Server, incluida la base de datos, los certificados y los archivos temporales.

2.11.3 Protección de datos en tránsito (cifrado TLS)

MyQ X aplica estrictas **normas de cifrado TLS** para todas las comunicaciones de red:

Mínimo TLS 1.2: la configuración predeterminada requiere como mínimo TLS 1.2, con una actualización opcional a TLS 1.3 para mejorar la seguridad y el rendimiento. Se bloquean los protocolos heredados, incluidos SSL y versiones anteriores de TLS.

Gestión de conjuntos de cifrado: el sistema implementa conjuntos de cifrado robustos y desactiva los algoritmos vulnerables para evitar ataques criptográficos. Las comunicaciones SNMPv3 utilizan cifrado SHA1 y AES.

Validación de certificados: todas las conexiones TLS requieren una validación adecuada de los certificados mediante nombres de dominio completos (FQDN) para evitar ataques de tipo «man-in-the-middle». Se evita START TLS debido a las vulnerabilidades MITM.

2.11.4 Cifrado de trabajos de impresión y almacenamiento seguro

MyQ X proporciona múltiples mecanismos para proteger los trabajos de impresión a lo largo de su ciclo de vida:

Liberación segura de impresiones: los trabajos de impresión se almacenan de forma segura en el servidor MyQ hasta que los usuarios se autentican en el dispositivo, lo que evita el acceso no autorizado a los documentos que se encuentran en las bandejas de salida de la impresora.

Cifrado de archivos de trabajo: los administradores pueden habilitar el cifrado de trabajos proporcionando certificados personalizados, lo que garantiza que los archivos de trabajo de impresión permanezcan cifrados mientras se almacenan en el servidor a la espera de su liberación.

Colas privadas: en el caso de documentos altamente confidenciales, las colas privadas eliminan automáticamente los trabajos de impresión inmediatamente después de su liberación, lo que elimina el riesgo de acceso no autorizado prolongado.

Modo de privacidad: cuando se habilita, el modo de privacidad oculta los nombres de los documentos a todos los usuarios excepto al propietario del documento, lo que evita la divulgación de información a través de los nombres de los trabajos. Ni siquiera los administradores pueden ver los nombres de los trabajos de otros usuarios.

2.11.5 Mejoras en el cifrado de bases de datos

La implementación de la base de datos **Firebird 4.0** proporciona capacidades de cifrado avanzadas:

Cifrado de certificados personalizados: los archivos de la base de datos se cifran utilizando certificados con EFS Extended Key Usage, lo que proporciona una sólida protección contra el acceso no autorizado a la base de datos.

Protección con contraseña: las contraseñas de la base de datos se ocultan en los archivos de registro, lo que evita la exposición de las credenciales durante las actividades de resolución de problemas y supervisión.

Fortalecimiento de permisos: la carpeta de datos de MyQ, que contiene la base de datos de usuarios y las claves privadas de los certificados TLS, está restringida únicamente a los administradores, al SISTEMA y a la cuenta de servicio de MyQ, lo que elimina el acceso de lectura predeterminado para todos los usuarios.

2.11.6 Cifrado de copias de seguridad y almacenamiento seguro

MyQ X garantiza que las copias de seguridad mantengan el mismo nivel de seguridad que los datos de producción:

Copias de seguridad cifradas: Las copias de seguridad de la base de datos están protegidas por contraseñas seguras generadas aleatoriamente que impiden la restauración o el acceso no autorizado a los archivos de copia de seguridad.

Almacenamiento seguro de copias de seguridad: los archivos de copia de seguridad deben almacenarse en ubicaciones seguras con controles de acceso adecuados y cifrado en reposo para mantener la confidencialidad de los datos durante el ciclo de vida de la copia de seguridad.

2.11.7 Políticas de gestión y rotación de claves

MyQ X implementa prácticas seguras de gestión de claves:

Rotación de certificados: los certificados se pueden rotar periódicamente de acuerdo con las políticas de seguridad de la organización, con soporte para la implementación automatizada a través de la política de grupo o la gestión de dispositivos móviles.

Protección de claves privadas: Todas las claves privadas para certificados y operaciones de CA están protegidas por contraseñas generadas aleatoriamente y almacenadas de forma cifrada en la base de datos.

Rotación de secretos de API: los secretos de cliente de la API REST deben someterse a una rotación periódica para mantener la seguridad. El sistema admite la renovación de secretos sin interrupción del servicio.

2.11.8 Minimización de datos y privacidad desde el diseño

MyQ X implementa **principios de privacidad desde el diseño que cumplen con el RGPD**:

Recopilación de datos limitada: el sistema recopila solo los metadatos esenciales necesarios para la funcionalidad operativa, evitando el procesamiento innecesario de datos personales que podría aumentar los riesgos de privacidad.

Eliminación automática: los administradores pueden configurar períodos de eliminación automática para los archivos de trabajos de impresión y escaneo, lo que

garantiza que los datos se conserven solo durante el tiempo necesario para fines comerciales.

Derechos de los datos de los usuarios: implementación completa de los derechos de los usuarios del RGPD, incluidos el acceso a los datos, la anonimización y el derecho al olvido, con avisos de privacidad personalizables en las interfaces de usuario.

Gestión de sesiones: la función de cierre de sesión automático garantiza que las sesiones de los usuarios se cierren correctamente, lo que evita el acceso no autorizado a través de sesiones abandonadas.

Este completo marco de protección y cifrado de datos garantiza que MyQ X mantenga los más altos estándares de confidencialidad e integridad de los datos, al tiempo que cumple con los requisitos normativos en diversos entornos organizativos.

2.12 Flujos de trabajo de impresión seguros

MyQ X proporciona flujos de trabajo de impresión seguros y completos que mantienen el control total del usuario sobre la liberación de documentos, al tiempo que evitan que la información confidencial quede expuesta en las bandejas de salida de la impresora. Estos flujos de trabajo son esenciales para las organizaciones que requieren una estricta seguridad de los documentos y la responsabilidad de los usuarios.

2.12.1 Implementación de la liberación segura de impresiones

Hold Print garantiza que los trabajos de impresión nunca se envíen inmediatamente a la impresora. Los documentos se almacenan de forma segura en el servidor MyQ y solo se imprimen después de que el usuario autorizado se autentique en el dispositivo de impresión, lo que evita que se dejen documentos sin supervisar en las bandejas de salida.

Pull Print amplía aún más esta función al permitir a los usuarios liberar sus trabajos en cualquier dispositivo compatible dentro del sistema de impresión, no solo en el dispositivo al que enviaron originalmente el trabajo. Esta flexibilidad es especialmente valiosa durante el mantenimiento de los equipos o cuando los usuarios necesitan imprimir desde diferentes ubicaciones.

Los métodos de autenticación múltiples son compatibles con Secure Print Release, incluidos los códigos PIN, las tarjetas de identificación, las contraseñas, los códigos QR con verificación biométrica y las combinaciones de autenticación de dos factores.

Esta flexibilidad se adapta a los diversos requisitos de seguridad de las organizaciones.

2.12.2 Flujos de trabajo de Pull Printing

Pull Print ofrece importantes ventajas tanto para los administradores como para los usuarios finales:

Ventajas administrativas:

- Elimina las pilas de documentos desatendidos en las impresoras de la oficina.
- Aplica un comportamiento de impresión responsable y políticas de seguridad de documentos.
- Gestionar todas las impresiones a través de una única cola de impresión unificada.
- Reducir el desperdicio de impresión y los costes asociados mediante opciones de vista previa y ajuste.
- Admite la impresión flexible en múltiples dispositivos

Ventajas para el usuario:

- Los documentos confidenciales permanecen seguros hasta que se liberan explícitamente
- Imprima en cualquier dispositivo autorizado de la organización
- Previsualice los documentos en el Embedded Terminal antes de liberarlos.
- Modifique las opciones de impresión (color, dúplex, acabado) incluso después de enviar el trabajo
- Cambiar los destinos de impresión en el dispositivo si la impresora original no está disponible.

2.12.3 Tiempo de espera del trabajo de impresión y eliminación automática

MyQ X implementa procedimientos de limpieza automática para evitar la exposición prolongada de los documentos:

Periodos de retención configurables: los administradores definen cuánto tiempo se almacenan los archivos de trabajos de impresión en el servidor MyQ antes de su eliminación automática, equilibrando los requisitos operativos con las necesidades de seguridad.

Gestión del tiempo de espera de los trabajos: los trabajos que no se liberan en los plazos especificados se eliminan automáticamente de la cola de espera, lo que evita que los documentos olvidados o abandonados se acumulen en los servidores.

Cierre de sesión automático: las sesiones del dispositivo caducan automáticamente tras los periodos definidos por el administrador, lo que evita el acceso no autorizado a los documentos en terminales abandonados.

2.12.4 Marcas de agua y firmas digitales

Las marcas de agua permiten la trazabilidad de los documentos añadiendo superposiciones personalizables a las páginas impresas que pueden incluir:

- Designaciones de confidencialidad
- Fechas de impresión y marcas de tiempo
- Nombre de la persona que imprime el documento
- Información de identificación de la impresora

Estas marcas de agua se pueden aplicar a todas las páginas o a páginas seleccionadas, creando un registro de auditoría que ayuda a identificar los documentos filtrados y rastrearlos hasta su origen.

2.12.5 Vista previa del trabajo y validación del contenido

El motor **de vista previa de trabajos** permite a los administradores revisar los trabajos de impresión antes de su liberación:

Formatos compatibles: la función de vista previa es compatible con los tres lenguajes de descripción de páginas más comunes: PCL 5, PCL 6 y PostScript.

Control preventivo: los administradores pueden rechazar los trabajos de impresión no autorizados antes de que lleguen al dispositivo de impresión, lo que evita el incumplimiento de las políticas y protege la información confidencial.

Filtrado basado en el contenido: la integración con sistemas de OCR y gestión de documentos permite aplicar políticas de escaneo basadas en el análisis del contenido de los documentos.

2.12.6 Gestión de errores y recuperación segura de trabajos

MyQ X implementa un sólido manejo de errores para mantener la seguridad durante los fallos del dispositivo:

Protección contra errores del dispositivo: cuando un dispositivo de impresión entra en estado de error (atascos de papel, falta de tóner), los documentos se retienen en lugar de imprimirse automáticamente cuando se resuelve el error, lo que mantiene el control del usuario sobre el momento de la liberación.

Conservación de la sesión: si un dispositivo deja de estar disponible en mitad de una sesión, el sistema MyQ conserva la sesión del usuario y permite continuar en dispositivos alternativos sin perder el estado del documento.

Cierre de sesión automático del dispositivo: cuando se producen errores en el dispositivo, el cierre de sesión automático borra la memoria del dispositivo para evitar el acceso no autorizado a los documentos por parte del personal de mantenimiento u otros usuarios.

Esta completa arquitectura de flujo de trabajo de impresión segura garantiza que las organizaciones mantengan un control estricto sobre la seguridad de los documentos a lo largo de todo el ciclo de vida de la impresión, al tiempo que favorece la flexibilidad operativa y la productividad de los usuarios.

2.13 Seguridad de dispositivos y redes

MyQ X proporciona controles de seguridad integrales para dispositivos y redes con el fin de proteger los dispositivos multifunción (MFD), las impresoras y la infraestructura de red contra el acceso no autorizado y la explotación.

2.13.1 Fortalecimiento de la seguridad de los dispositivos multifunción

Las organizaciones que implementan MyQ X con MFD deben aplicar las mejores prácticas de seguridad, entre las que se incluyen:

Controles de acceso a los dispositivos: restringir el acceso físico a las impresoras únicamente a las ubicaciones y al personal autorizados, reduciendo así la exposición a manipulaciones o robos.

Desactivación de protocolos no utilizados: desactive los protocolos y servicios innecesarios que no sean requeridos por MyQ X, reduciendo así la superficie de ataque de cada dispositivo.

Gestión de credenciales predeterminadas: cambie todas las contraseñas de administrador predeterminadas de los dispositivos por credenciales seguras generadas aleatoriamente. Los atacantes suelen conocer las contraseñas predeterminadas de fábrica.

Protección del disco duro interno: si los dispositivos admiten el almacenamiento interno de trabajos de impresión para su reimpresión, implemente funciones de cifrado (AES) y sobrescritura automática de datos para evitar el acceso no autorizado a los documentos almacenados.

2.13.2 Segmentación de red y configuración de VLAN

MyQ X admite estrategias de segmentación de red para contener posibles compromisos de los dispositivos:

Aislamiento de VLAN: separe el tráfico de red de las impresoras y los dispositivos de las redes generales de usuarios y administrativas mediante LAN virtuales, lo que limita el movimiento lateral si un dispositivo se ve comprometido.

Subredes y listas de control de acceso: implemente controles de acceso a nivel de red mediante listas de control de acceso (ACL) para garantizar que solo los sistemas autorizados puedan comunicarse con los dispositivos de impresión y los servidores.

Reglas de firewall: bloquee el tráfico entrante y saliente innecesario de las subredes de impresoras, limitando la conectividad solo a los servicios esenciales y evitando que los dispositivos infectados accedan a otros recursos de la red.

Aplicación de FQDN: Todas las comunicaciones de red deben utilizar nombres de dominio completos (FQDN) en lugar de direcciones IP o nombres de host cortos, lo que evita los ataques de intermediarios basados en DNS y garantiza la validación adecuada de los certificados.

2.13.3 Implementación de seguridad SNMP v3

MyQ X aplica los modernos protocolos **SNMPv3** con un cifrado sólido para la gestión de dispositivos:

Prohibición del SNMPv1 inseguro: La comunicación SNMPv1 heredada debe desactivarse por completo, ya que transmite las credenciales en texto claro y carece de cifrado.

Configuración SNMPv3: Todas las comunicaciones SNMP deben utilizar SNMPv3 con:

- Contraseñas seguras y generadas aleatoriamente para la autenticación
- Algoritmos hash SHA1 o más potentes
- Cifrado AES para la confidencialidad de los datos
- Credenciales únicas por dispositivo, específicas para cada implementación de MyQ

2.13.4 Gestión de credenciales de impresora

MyQ X reconoce que **la gestión de credenciales de impresora es específica del proveedor** y requiere la implementación por parte del cliente:

Requisitos de contraseñas seguras: todas las credenciales administrativas de la impresora deben utilizar contraseñas seguras generadas aleatoriamente, en lugar de credenciales predeterminadas o simples.

Rotación de credenciales: actualice periódicamente las contraseñas de las impresoras de acuerdo con las políticas de seguridad de la organización para reducir el riesgo de que las credenciales se vean comprometidas.

Restricciones de acceso: limitar el acceso a la gestión de la impresora solo al personal autorizado mediante reglas de firewall, controles de acceso físico y permisos basados en roles.

2.13.5 Seguridad del firmware y gestión de actualizaciones

Mantener actualizado el firmware del dispositivo es fundamental para la seguridad:

Actualizaciones automáticas: configure los dispositivos para que reciban y apliquen automáticamente las actualizaciones de firmware del fabricante que solucionen las vulnerabilidades de seguridad recién descubiertas.

Advertencias de seguridad de los proveedores: supervise las notificaciones de seguridad del fabricante sobre vulnerabilidades críticas que afecten a los dispositivos implementados y aplique los parches con prontitud.

Pruebas de actualización: pruebe las actualizaciones de firmware en entornos que no sean de producción antes de implementarlas en impresoras de producción para garantizar la compatibilidad y la funcionalidad.

2.13.6 Gestión y restricciones de los puertos USB

MyQ X admite controles administrativos para la conectividad USB de los dispositivos:

Desactivación de puertos USB: los administradores deben desactivar los puertos USB de entrada en los dispositivos multifunción para evitar:

- La impresión directa a través de USB, sin pasar por los controles de seguridad de MyQ.
- El acceso directo a los discos duros de los dispositivos y a los datos almacenados.
- Uso no autorizado de la funcionalidad del dispositivo

Alternativas seguras de impresión directa: habilite solo métodos de impresión seguros aprobados (IPP/S, AirPrint con integración MyQ) y bloquee el acceso USB directo no seguro.

Este completo marco de seguridad de dispositivos y redes garantiza que los dispositivos de impresión sigan siendo componentes seguros de la infraestructura MyQ X, al tiempo que se mantiene la eficiencia operativa y la postura de seguridad de la organización.

2.14 Auditoría y control

MyQ X ofrece funciones completas de auditoría y supervisión que permiten a los administradores mantener la visibilidad de las operaciones de impresión, detectar incidentes de seguridad y garantizar el cumplimiento de las políticas y normativas de la organización.

2.14.1 Supervisión y alertas en tiempo real

MyQ X supervisa todos los componentes de la infraestructura de impresión en tiempo real a través de múltiples canales de supervisión:

Supervisión del estado de los dispositivos: supervisión continua del estado de las impresoras y los dispositivos multifunción, incluidos los niveles de tóner, la disponibilidad de papel, las condiciones de error y la conectividad de los dispositivos. Los administradores reciben información inmediata sobre el estado y el funcionamiento de los dispositivos.

Gestión de alertas: las alertas automatizadas notifican a los administradores los eventos críticos, incluidos los errores de los dispositivos, los suministros bajos, los problemas de conectividad y otros problemas operativos. Las notificaciones de alerta se pueden enviar por correo electrónico o integrarse con el Visor de eventos de Windows.

Notificaciones de eventos: las notificaciones personalizables basadas en eventos activan acciones en respuesta a condiciones específicas del dispositivo o del sistema, lo que permite resolver los problemas de forma proactiva antes de que afecten a las operaciones.

2.14.2 Registro y análisis de la actividad de impresión

MyQ X mantiene **registros de auditoría detallados de todas las actividades de impresión, copia, escaneo y fax**:

Contabilidad basada en trabajos: la contabilidad avanzada realiza un seguimiento independiente de cada trabajo, lo que permite una atribución detallada a usuarios, dispositivos, proyectos y centros de coste específicos. Los trabajos realizados

durante una sola sesión de usuario se contabilizan por separado, lo que proporciona datos de uso precisos.

Metadatos de actividad: el registro completo captura la fecha de envío del trabajo, la fecha de liberación del trabajo, la identificación del dispositivo, el formato del papel, la configuración simplex/dúplex, la configuración de color y todos los demás parámetros relevantes del trabajo.

Registro MyQ: el registro del sistema en tiempo real muestra toda la actividad del servidor, incluidos los eventos del sistema, los errores, las advertencias, los intentos de autenticación, los cambios de configuración y las acciones administrativas. Los mensajes de registro se clasifican por gravedad (crítico, error, advertencia, información, aviso, depuración, seguimiento) y se pueden filtrar por período de tiempo y subsistema.

2.14.3 Análisis del comportamiento de los usuarios

MyQ X ofrece sofisticadas funciones de análisis para comprender los patrones de impresión y detectar anomalías:

Generación de informes personalizados: las funciones avanzadas de generación de informes permiten a los administradores crear informes personalizados basados en cualquier combinación de parámetros rastreados, lo que permite analizar el comportamiento de impresión por usuario, departamento, proyecto, dispositivo o período de tiempo.

Seguimiento de centros de coste: la atribución detallada de los trabajos de impresión a centros de coste, proyectos y grupos de usuarios permite la elaboración de informes de gastos transparentes y respalda la toma de decisiones informadas sobre las políticas de impresión.

Supervisión del comportamiento: los administradores pueden analizar los patrones de impresión para identificar actividades inusuales, usos excesivos o infracciones de las políticas que requieran una investigación más profunda.

2.14.4 Detección y respuesta a incidentes

MyQ X admite la supervisión centrada en la seguridad mediante registros y alertas estructurados:

Registro de **autenticación fallida**: el registro mejorado de los intentos de autenticación, en particular los intentos de inicio de sesión fallidos, permite a los administradores detectar y responder a posibles amenazas de seguridad. Desde la

versión 10.2, se han mejorado los registros de intentos de inicio de sesión para facilitar el filtrado en el registro de MyQ.

Reglas de notificación de registros: las reglas personalizables activan notificaciones automáticas basadas en tipos de eventos, subsistemas y patrones de mensajes específicos, lo que permite la detección rápida de eventos relevantes para la seguridad. Las reglas pueden utilizar expresiones regulares para buscar patrones específicos en los mensajes de registro.

Alertas de eventos críticos: el sistema avisa automáticamente a los administradores de eventos críticos, como violaciones de seguridad, fallos de autenticación, intentos de acceso no autorizados y cambios de configuración.

2.14.5 Políticas de retención y archivo de registros

MyQ X implementa una gestión flexible de registros para equilibrar las necesidades operativas con los requisitos de cumplimiento:

Períodos de retención configurables: los administradores definen el número de días antes de que los registros se eliminen automáticamente, alineando la retención con las políticas de gobernanza de datos de la organización y los requisitos normativos.

Exportación y archivo de registros: los registros se pueden exportar en formato Excel o CSV para su almacenamiento y análisis externos. Las exportaciones programadas permiten el archivo automatizado de registros a intervalos regulares.

Conservación a largo plazo: los registros exportados se pueden almacenar en repositorios seguros y cifrados para mantener registros históricos con fines de auditoría, verificación del cumplimiento normativo e investigación de incidentes.

2.14.6 Funciones avanzadas de filtrado y búsqueda

MyQ X proporciona herramientas sofisticadas para el análisis y la investigación de registros:

Búsquedas guardadas: los administradores pueden crear, guardar y compartir filtros de búsqueda de uso común para acceder rápidamente a los datos de registro relevantes. Las búsquedas guardadas se pueden organizar en carpetas para facilitar su gestión.

Filtrado por **periodo de tiempo**: filtre los registros por rangos de fechas específicos o periodos predefinidos para centrar el análisis en los intervalos de tiempo relevantes.

Filtrado por subsistema y contexto: busque por subsistemas MyQ específicos (interfaz de usuario web, terminal, servidor SMTP, etc.) y contextos (impresión directa, dispositivos específicos) para aislar los eventos relevantes.

Control de verbosidad: seleccione qué niveles de gravedad de los registros (crítico, error, advertencia, información, etc.) se muestran, reduciendo el ruido y centrándose en los eventos significativos.

2.14.7 Registro de auditoría para acciones administrativas

MyQ X realiza un seguimiento de todos los cambios administrativos a través de un **registro de auditoría** específico:

Cambios de configuración: registra todas las modificaciones de la configuración de MyQ, incluyendo quién realizó el cambio, cuándo se realizó y qué componente del sistema se vio afectado.

Gestión de derechos de usuario: seguimiento detallado de los cambios en los permisos de usuario, las pertenencias a grupos y los controles de acceso, con la posibilidad de ver información detallada sobre cada cambio.

Gestión de PIN y credenciales: seguimiento mejorado de las adiciones, eliminaciones y modificaciones de PIN para supervisar el ciclo de vida de las credenciales.

Capacidades de exportación: los registros de auditoría se pueden exportar bajo demanda o programarse para su exportación automática periódica, lo que permite cumplir con los requisitos de presentación de informes de cumplimiento y conservación de registros.

Este completo marco de auditoría y supervisión garantiza que MyQ X proporcione a los administradores la visibilidad necesaria para mantener la seguridad, detectar amenazas, garantizar el cumplimiento de las políticas y resolver eficazmente los problemas operativos.

2.15 Respuesta a incidentes y recuperación

MyQ X ofrece capacidades completas de respuesta y recuperación ante incidentes, diseñadas para mantener la continuidad del negocio durante interrupciones tanto planificadas como imprevistas. La plataforma combina procedimientos de copia de seguridad automatizados, funciones de alta disponibilidad y mecanismos de conmutación por error flexibles para garantizar que los servicios de impresión sigan funcionando incluso durante las interrupciones del sistema.

2.15.1 Procedimientos de respuesta a incidentes de seguridad

MyQ X admite una respuesta estructurada a incidentes a través de múltiples mecanismos de supervisión y alerta:

Detección de incidentes en tiempo real: la supervisión automatizada realiza un seguimiento continuo del estado del sistema, los fallos de autenticación, los cambios de configuración y los eventos de seguridad, lo que permite detectar rápidamente posibles incidentes de seguridad.

Escalado de alertas: las reglas configurables del notificador de registros activan notificaciones inmediatas a los administradores cuando se producen eventos de seguridad críticos, como intentos de autenticación fallidos, intentos de acceso no autorizados y anomalías del sistema.

Conservación del registro de auditoría: el registro completo de todas las actividades del sistema garantiza la disponibilidad de datos forenses completos para la investigación de incidentes. El registro de auditoría de MyQ realiza un seguimiento de todas las acciones administrativas, los cambios de configuración y las actividades de los usuarios.

Procedimientos de contención: en caso de incidente de seguridad, los administradores pueden aislar rápidamente los componentes afectados, desactivar las cuentas comprometidas e implementar controles de acceso de emergencia.

2.15.2 Procedimientos de recuperación y restauración

MyQ X implementa sólidas capacidades de copia de seguridad y restauración para garantizar una rápida recuperación ante fallos del sistema o pérdida de datos:

Copia de seguridad automatizada de la base de datos: Las copias de seguridad automatizadas periódicas de la base de datos de MyQ capturan todos los datos de configuración, la información de los usuarios y los ajustes del sistema. Las copias de seguridad están protegidas con cifrado de contraseña y se almacenan de forma segura.

Restauración completa del sistema: El proceso de restauración recupera todo el entorno MyQ, incluyendo la base de datos, los certificados, los archivos de configuración y los informes. Los administradores solo tienen que seleccionar el archivo de copia de seguridad y proporcionar la contraseña si está protegido.

Copia de seguridad y restauración con reconocimiento de clústeres: para implementaciones de alta disponibilidad que utilizan Microsoft Failover Clustering,

MyQ admite la copia de seguridad en el almacenamiento compartido del clúster y la restauración coordinada en todos los nodos del clúster.

2.15.3 Alta disponibilidad y conmutación por error

MyQ X ofrece múltiples estrategias de conmutación por error para mantener las operaciones de impresión durante el tiempo de inactividad del servidor:

Integración con Microsoft Failover Clustering: MyQ X se implementa en configuraciones activas-pasivas dentro de los clústeres de conmutación por error de Microsoft Windows Server. El software del clúster supervisa continuamente el estado de los nodos y cambia automáticamente a los nodos pasivos cuando el nodo activo deja de estar disponible.

Impresión de reserva: cuando el Desktop Client MyQ detecta una pérdida de conexión con el servidor, redirige automáticamente los trabajos de impresión a impresoras de reserva preconfiguradas. Una vez restablecida la conectividad del servidor, la contabilidad de los trabajos se actualiza automáticamente.

Cola de impresión **del dispositivo**: los trabajos de impresión se pueden almacenar cifrados en la memoria del dispositivo durante las interrupciones del servidor. Cuando se restablece la conectividad, los dispositivos transmiten automáticamente los datos de contabilidad al servidor.

Inicio de sesión sin conexión: los Embedded Terminal de MyQ X almacenan en caché las credenciales de autenticación de los usuarios, lo que les permite iniciar sesión y acceder a las funciones del dispositivo incluso cuando el servidor no está disponible.

Cola de impresión del cliente: los trabajos se procesan localmente en las estaciones de trabajo de los usuarios y se almacenan en sus ordenadores en lugar de en el servidor, lo que reduce significativamente los requisitos de ancho de banda y permite imprimir durante el mantenimiento del servidor o en caso de problemas de red.

2.15.4 Análisis y mejora posteriores al incidente

MyQ X permite la mejora continua de las capacidades de respuesta ante incidentes mediante herramientas de análisis completas:

Análisis del historial de registros: los administradores pueden revisar los registros exportados para comprender la secuencia de eventos que condujeron a un incidente, identificar las causas fundamentales y determinar las medidas correctivas adecuadas.

Revisión del registro de auditoría: el registro de auditoría proporciona una visibilidad completa de todas las acciones administrativas y los cambios de

configuración que pueden haber contribuido o precedido a los incidentes de seguridad.

Patrones de búsqueda guardados: los administradores pueden crear y guardar filtros de búsqueda dentro de los registros para patrones de incidentes comunes, lo que permite identificar rápidamente eventos similares en el futuro.

3 MyQ X y NIS2

La Directiva (UE) 2022/2555, más conocida como **NIS2**, supone un avance significativo hacia el establecimiento de un nivel común de ciberseguridad en toda la Unión Europea. Esta directiva, que entró en vigor el 16 de enero de 2023, tiene por objeto reforzar la **resiliencia de los servicios esenciales** y **de** los proveedores de servicios digitales frente a las ciberamenazas mediante la introducción de **normas y prácticas de ciberseguridad** coherentes.

El sector de la impresión, junto con muchos otros, entra dentro del ámbito de aplicación de la Directiva NIS2. Por lo tanto, las entidades del sector de la impresión deben comprender las implicaciones de la Directiva NIS2 y adoptar las medidas necesarias para cumplir con las normas de seguridad. Antes del 17 de octubre de 2024, los Estados miembros deben adoptar y publicar las medidas esenciales para cumplir con la Directiva NIS2.

En este artículo se analizan los detalles de la Directiva NIS2 y sus implicaciones para los distribuidores y clientes de MyQ X.

Si es usted un cliente final de MyQ X, comente los requisitos y recomendaciones de la Directiva NIS2 con su proveedor o distribuidor de MyQ X. Los socios de MyQ están capacitados para ofrecer un soporte de primer nivel y le ayudarán a implementar las medidas necesarias.

3.1 Áreas principales de la Directiva NIS2

3.1.1 Gestión de riesgos y ciberseguridad

Adopte un enfoque de gestión de riesgos en materia de ciberseguridad. Esto incluye identificar y evaluar los riesgos para la red y los sistemas de información, aplicar medidas para mitigar dichos riesgos y revisar periódicamente dichas medidas.

Asegúrese de que su servidor y el software asociado estén **actualizados con los últimos parches de seguridad** para mitigar las vulnerabilidades. Además, implemente y pruebe periódicamente planes de copia de seguridad y recuperación ante desastres para garantizar la disponibilidad e integridad de los datos. MyQ publica regularmente parches para sus productos. Se recomienda encarecidamente mantenerse informado, estar al tanto de estas publicaciones y diseñar con antelación

su estrategia y procedimiento de actualización. MyQ genera una **lista de materiales de software (SBOM)** para cada versión, que puede obtenerse a través de su proveedor o distribuidor de MyQ, lo que permite a las organizaciones analizar los componentes utilizados en el software en busca de vulnerabilidades de seguridad.

La segmentación de la red es una herramienta esencial para implementar en la práctica una política de «Zero Trust». Ofrece a las organizaciones formas de controlar sus redes con políticas de seguridad más granulares. Garantiza que, incluso si un atacante compromete una parte de la red, no pueda desplazarse lateralmente con facilidad a otras áreas. Sin embargo, las organizaciones con entornos segmentados se enfrentan a retos a la hora de garantizar la disponibilidad inmediata de la impresión.

Con MyQ X, las colas de impresión pueden propagarse en redes segmentadas mediante los Mobile Print Agents, y los documentos alojados en la nube pueden descargarse y liberarse inmediatamente desde la pantalla del dispositivo con Easy Print. La compatibilidad con Microsoft Universal Print o Application Proxy en el cliente móvil puede ayudar significativamente a las organizaciones a habilitar los servicios de impresión en todo su entorno, al tiempo que garantiza que el acceso a dichos recursos esté protegido.

Los certificados SSL para conexiones seguras ayudan a cumplir los requisitos de la norma NIS2 en materia de transmisión segura de datos a través de redes. MyQ X, de serie, incluye la comunicación segura habilitada gracias a la autoridad de certificación integrada. Las organizaciones que utilicen una PKI empresarial pueden alcanzar un nivel aún mayor de seguridad en las comunicaciones proporcionando certificados personalizados directamente.

Siempre que sea posible, **aplique el protocolo TLS** para la comunicación con otros sistemas. Proteja la conexión con Active Directory u otros directorios de usuarios mediante LDAPS. Asegúrese de que la transmisión de correo electrónico se realice a través de SMTPS y revise todos los ajustes de la página «Red» de MyQ X y de la pestaña «Seguridad» de Easy Config (por ejemplo, que el servidor web solo permita conexiones seguras).

MyQ también ofrece la posibilidad de **cifrar bases de datos, escaneos y trabajos de impresión**. El cifrado de datos es fundamental para garantizar la confidencialidad y la integridad de la información sensible, lo cual constituye un aspecto clave del cumplimiento de la norma NIS2.

En cuanto a la comunicación entre dispositivos, es esencial implementar protocolos de comunicación que ofrezcan el máximo nivel de seguridad. Se recomienda

encarecidamente utilizar **SNMPv3** en lugar de v1 o v2(c) para supervisar y gestionar el estado y la funcionalidad de los dispositivos en una red.

3.1.2 Continuidad del negocio y gestión de crisis

> Las organizaciones deben garantizar que sus operaciones puedan continuar en caso de una interrupción significativa.

Implemente **servidores redundantes o sistemas de conmutación por error** para garantizar que los servicios de impresión sigan estando disponibles durante un incidente. MyQ X permite la implementación de medidas de conmutación por error mediante varios métodos.

MyQ es compatible con **los clústeres de conmutación por error de Windows Server** para garantizar una alta disponibilidad: si el nodo activo falla, el clúster traslada los servicios de MyQ a un nodo en espera. Las implementaciones virtualizadas también pueden utilizar la alta disponibilidad (HA) del hipervisor para reiniciar la máquina virtual de MyQ en otro host.

Si se pierde la conexión con el servidor MyQ, la función **de impresión de reserva** del Cliente de Escritorio MyQ envía los trabajos de impresión directamente a un dispositivo de reserva configurado, de modo que los usuarios puedan seguir imprimiendo durante una interrupción del servidor. En los dispositivos compatibles de Kyocera y Ricoh, **la función «Device Spooling»,** combinada con **el inicio de sesión sin conexión,** permite a los usuarios iniciar sesión y liberar trabajos en el dispositivo mientras el servidor no está disponible. Las funciones que dependen del servidor, como los flujos de trabajo de escaneo de MyQ, el crédito y la cuota, no estarán disponibles hasta que se pueda volver a acceder al servidor.

Las copias de seguridad periódicas **de la base de datos** y la capacidad de restaurar los datos de MyQ cumplen con los requisitos de la norma NIS2 para garantizar la disponibilidad y la resiliencia de los datos ante ciberataques o fallos del sistema. Las copias de seguridad de la base de datos y de los registros se pueden programar con MyQ X y realizarse automáticamente, incluidas las copias de seguridad de la base de datos SQL del Central Server.

Para obtener más información, consulte:

- Resiliencia, planes de contingencia y alta disponibilidad
- Estrategia de spooling

3.1.3 Modelo de acceso con privilegios mínimos

> A los usuarios solo se les debe conceder el nivel mínimo de acceso o los permisos necesarios para realizar las operaciones requeridas.

NIS2 fomenta **la segregación de funciones** para evitar el acceso no autorizado a sistemas críticos.

Al asignar **derechos específicos de acceso** a la gestión del sistema y de los usuarios, la gestión de trabajos, la generación de informes o los registros, es posible conceder a determinados usuarios acceso con privilegios elevados a áreas concretas del entorno MyQ, al tiempo que se limitan los derechos de acceso de otros. Del mismo modo, los derechos pueden asignarse por Servidor de sitio, de modo que los administradores de un Servidor de sitio local no obtendrán acceso con privilegios elevados en otras ubicaciones y sucursales de la organización donde no sea deseable.

Cuando el administrador utiliza **la gestión** de usuarios **basada en grupos** (grupos de seguridad), puede reducir el número de pasos necesarios para configurar los derechos de acceso sin dejar de beneficiarse de la concesión y retirada de derechos de los usuarios. Para más información, consulte más adelante la sección *«Concesión y retirada de derechos de los usuarios»*.

Los permisos de acceso granulares deben aplicarse en toda la infraestructura de la organización, incluidos todos los componentes del ecosistema MyQ X. El acceso debe restringirse exclusivamente a los administradores y al personal autorizado, garantizando que solo quienes cuenten con los privilegios adecuados puedan gestionar e interactuar con estos sistemas. Esto incluye dispositivos físicos, servidores físicos y sus sistemas operativos (Windows Server), servidores SQL, almacenamiento y mucho más.

Más información:

- Implementación: derechos de usuario

3.1.4 Respuesta ante incidentes y auditoría

> Para gestionar los incidentes, establezca y ponga en práctica procedimientos de forma regular. En caso de actividad sospechosa, restrinja o suspenda el acceso del usuario para evitar daños mayores. La correcta aplicación de estas medidas puede mitigar el impacto de eventos inesperados.

Las funciones de registro y auditoría de MyQ (MyQ Logs y MyQ Audit Log) pueden resultar extremadamente útiles para la respuesta ante incidentes y su seguimiento. Estos registros ayudan a detectar, investigar y responder a actividades sospechosas, lo cual es un requisito obligatorio de la NIS2.

Los registros deben supervisarse periódicamente y deben activarse las notificaciones para los incidentes que la organización considere críticos. Para ello, la utilidad **Log Notifier** integrada en MyQ X puede configurarse para supervisar los eventos en el entorno de MyQ y notificar al personal responsable para que tome medidas inmediatas. Las tareas programadas en ejecución (como la sincronización de usuarios, la detección de impresoras y otras) también pueden enviar avisos a contactos predeterminados. Los administradores también pueden configurar MyQ X para que envíe alertas automáticas cuando fallen los trabajos de impresión o se produzcan errores críticos.

La gestión de registros puede centralizarse exportando y procesando los registros a través del Registro de eventos de Windows, y puede ser procesada posteriormente por sistemas SIEM cuando sea necesario. Asegúrese de que los períodos de conservación del historial, los registros y los registros de auditoría sean suficientes para sus necesidades. Esto se configura en **«Configuración»** – **«Gestión del sistema»**.

Establecer **acuerdos de nivel de servicio (SLA) sólidos** es esencial para servicios gestionados como MyQ, especialmente en el marco de la normativa NIS2. Para garantizar tiempos de respuesta rápidos ante incidentes, las organizaciones deberían plantearse optar por las ofertas de Soporte Premium.

Más información:

- Configuración de registros

3.1.5 Autenticación segura

> La autenticación segura garantiza que solo los usuarios autorizados accedan a los sistemas. La autenticación de dos factores (2FA) refuerza esta seguridad al exigir dos tipos de credenciales, lo que aumenta significativamente la seguridad.

Los requisitos de contraseña y PIN, **la autenticación de dos factores** en los terminales integrados o el uso de «Iniciar sesión con Microsoft» en las interfaces web

o en los terminales integrados (con el cliente móvil MyQ X) ofrecen alternativas para proteger el acceso al entorno MyQ X.

El cliente móvil MyQ X se puede configurar para que exija **una verificación biométrica**, lo que mejora aún más la seguridad de la cuenta de usuario de MyQ X al requerir un factor adicional durante la autenticación en los dispositivos.

La implementación de mecanismos de bloqueo de cuentas de usuario tras varios intentos fallidos de inicio de sesión mejora la seguridad y reduce el riesgo de ataques de fuerza bruta.

Más información:

- Implementación: Autenticación segura[6]
- Implementación: uso de la autenticación de dos factores[7]

3.1.6 Provisión y retirada de usuarios

El aprovisionamiento y el desaprovisionamiento garantizan que se deniegue inmediatamente el acceso de los usuarios al entorno MyQ en cuanto sean eliminados del directorio de usuarios de origen.

MyQ admite **la sincronización automática y programada de usuarios** con sistemas externos como LDAP, Microsoft Entra ID (antes Azure AD), Google Workspace y archivos CSV. Esto garantiza que los usuarios recién añadidos se importen automáticamente al entorno de MyQ X sin necesidad de intervención manual. Al sincronizar periódicamente los datos de los usuarios, MyQ X ayuda a mantener una lista actualizada de usuarios con los derechos de acceso correctos, lo que reduce el riesgo de acceso no autorizado.

La gestión basada en grupos y el uso de grupos de seguridad en el directorio de usuarios de origen pueden facilitar la **asignación y la retirada** automáticas **del acceso** a partes del entorno de MyQ X para los usuarios recién creados o eliminados.

MyQ X ofrece una función **de registro automático** que permite a los usuarios registrarse por sí mismos enviando trabajos de impresión, pasando una tarjeta de identificación o creando una cuenta a través de la interfaz web. Esta función resulta especialmente útil en entornos con usuarios externos frecuentes, como los empleados invitados. A los usuarios del sistema se les puede proporcionar un **PIN**

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

temporal que caduca tras el periodo establecido, lo que garantiza que el acceso se revoque automáticamente una vez que el usuario ya no lo necesite.

MyQ admite la anonimización de los datos de los usuarios para cumplir con la normativa de privacidad. Este proceso elimina de forma irreversible todos los identificadores personales, lo que hace que las cuentas de usuario sean inutilizables e imposibles de rastrear, al tiempo que permite la generación de informes y la auditoría del sistema sin comprometer la privacidad.

Más información:

- Implementación: gestión de usuarios basada en grupos

3.1.7 Sensibilización y formación

La normativa NIS2 hace hincapié en la necesidad de sensibilizar y formar al personal sobre las prácticas de ciberseguridad.

Se recomienda impartir sesiones de formación al personal de TI y a los administradores sobre la gestión segura del entorno MyQ X, haciendo hincapié en el cumplimiento de la normativa NIS2. La mejor opción es consultar la gestión del ecosistema MyQ X con su proveedor o distribuidor. Los socios de MyQ están capacitados para ofrecer un soporte de la máxima calidad.

Además, deben desarrollarse programas de sensibilización para ayudar a los usuarios finales a identificar amenazas e instruirles sobre el uso del ecosistema MyQ X, así como sobre los pasos a seguir en caso de incidentes de seguridad o de otro tipo.

Documento técnico sobre seguridad e implementación segura

Para obtener más información sobre cómo alcanzar los mejores estándares de seguridad con MyQ X, consulte el resto de esta guía, que trata sobre la seguridad de MyQ X (see page 4).

Actualizado el 6 de octubre de 2026

4 Lista de materiales de software

Páginas OEM vinculadas
This ScriptRunner macro could not be rendered for export.

Una lista de materiales de software (SBOM) es un registro detallado de todos los componentes, dependencias y bibliotecas incluidos en una aplicación de software, ya sean de código abierto o propietarios. Proporciona información clave, como nombres de componentes, versiones, licencias y ubicaciones de origen, lo que ofrece una visibilidad completa de la cadena de suministro del software.

Las SBOM se utilizan para rastrear y gestionar los riesgos del software, ya que permiten a las organizaciones identificar rápidamente los componentes vulnerables u obsoletos, garantizar el cumplimiento de las licencias y mejorar la seguridad general. El mantenimiento de una SBOM es especialmente importante en ecosistemas de software complejos, ya que ayuda a optimizar la gestión de vulnerabilidades y garantiza la transparencia en todo el ciclo de vida del desarrollo de software.

Mediante la generación, el análisis y el mantenimiento constantes de las SBOM, las organizaciones pueden gestionar mejor los riesgos del software y garantizar el cumplimiento de las normas de seguridad y reglamentarias.

Los formatos BOM (lista de materiales) se refieren a estructuras estandarizadas que representan y comparten los componentes de un sistema de software. En el contexto de las listas de materiales de software (SBOM), estos formatos proporcionan una forma legible por máquina de describir los componentes de software, sus relaciones y los metadatos. Los formatos SBOM más utilizados son:

- **CycloneDX**: un formato de BOM ligero y extensible diseñado específicamente para la seguridad de las aplicaciones. Proporciona información detallada sobre los componentes, las licencias, las vulnerabilidades y las dependencias. CycloneDX es popular por su flexibilidad y su compatibilidad con la automatización en los flujos de trabajo de seguridad y gestión de riesgos.

MyQ proporciona SBOM para los siguientes productos:

- MyQ X Central Server 10.2
- MyQ X Print Server 10.2
- MyQ Desktop Client (MDC) 10.2
- Mobile Print Agent (MPA) 1.3
- Reconocimiento óptico de caracteres (OCR) 3.1

Para recibir los SBOM de MyQ, póngase en contacto con nuestro servicio de asistencia.

5 Contactos comerciales

Fabricante de MyQ®	**MyQ® spol. s r.o.** Harfa Business Center, Ceskomoravska 2532/19b, 190 00 Praga 9, República Checa N.º de identificación 615 06 133 MyQ® spol. s r.o. está inscrita en el Registro Mercantil del Tribunal Municipal de Praga, con el número de expediente C 29842 (en lo sucesivo, «MyQ®»)
Información comercial	http://www.myq-solution.com info@myq-solution.com[8]
Soporte técnico	support@myq-solution.com[9]
Aviso	EL FABRICANTE NO SERÁ RESPONSABLE DE NINGUNA PÉRDIDA O DAÑO CAUSADO POR LA INSTALACIÓN O EL FUNCIONAMIENTO DEL SOFTWARE Y EL HARDWARE DE LA SOLUCIÓN DE IMPRESIÓN MyQ®. Este manual, su contenido, diseño y estructura están protegidos por derechos de autor. Queda prohibida y puede ser sancionada la copia o cualquier otra reproducción total o parcial de esta guía, o de cualquier material protegido por derechos de autor, sin el consentimiento previo por escrito de MyQ®. MyQ® no se hace responsable del contenido de este manual, en particular en lo que respecta a su integridad, actualidad y ocupación comercial. Todo el material aquí publicado tiene carácter exclusivamente informativo. Este manual está sujeto a cambios sin previo aviso. MyQ® no está obligado a realizar estos cambios periódicamente ni a anunciarlos, y no se hace responsable de que la información publicada actualmente sea compatible con la última versión de la solución de impresión MyQ®.

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

Marcas comerciales	«MyQ®», incluidos sus logotipos, es una marca comercial registrada de MyQ®. Queda prohibido cualquier uso de las marcas comerciales de MyQ®, incluidos sus logotipos, sin el consentimiento previo por escrito de MyQ® Company. La marca comercial y el nombre del producto están protegidos por MyQ® y/o sus filiales locales.

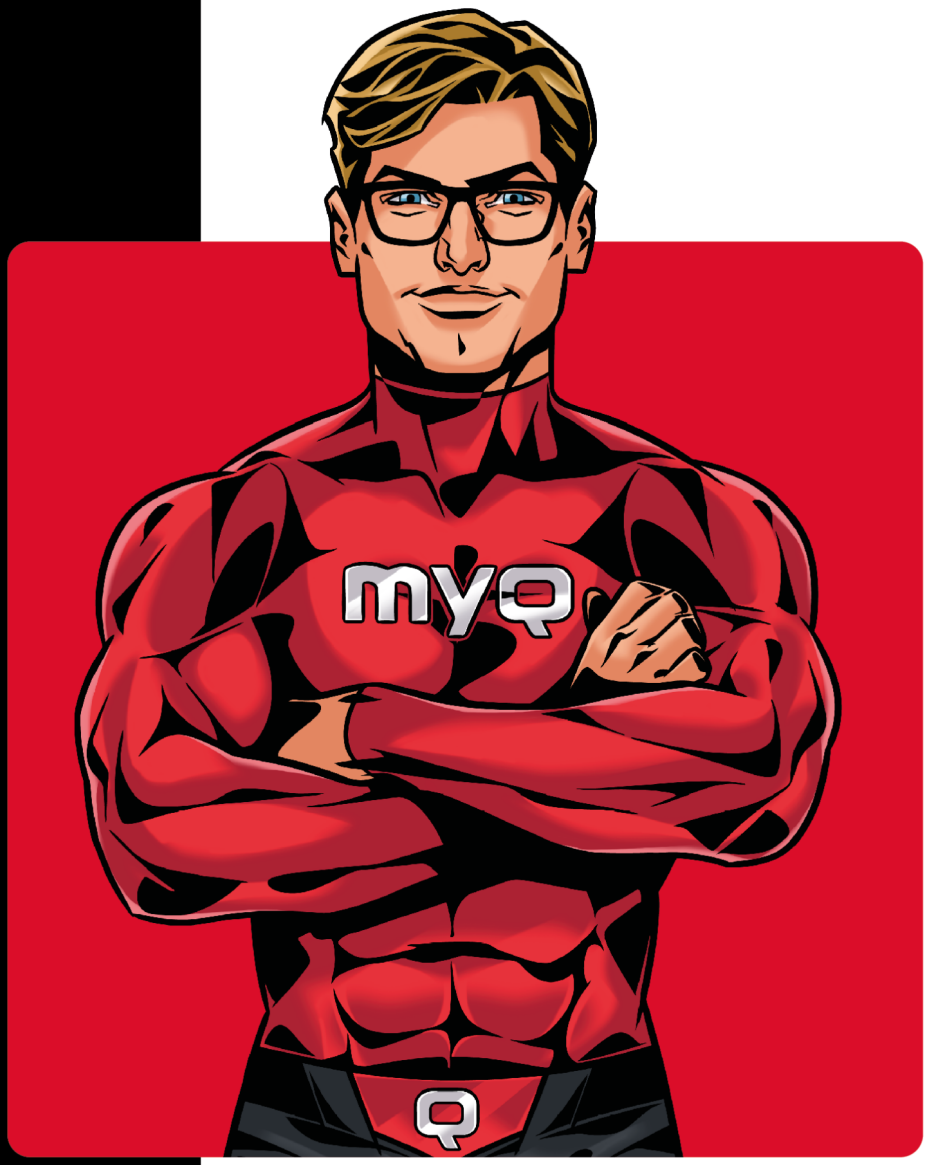
myQ X

AHORRE TIEMPO CON SOLUCIONES DE IMPRESIÓN PERSONALIZADAS

MyQ X es una solución de gestión de impresión galardonada, tanto local como en la nube privada, en la que confían millones de usuarios.

info@myq-solution.com

myq-solution.com



Más de 50 millones
de usuarios confiables

Más de 1 millón
de dispositivos activos

Más de 26
marcas compatibles

Más de 1000
socios certificados

Operando en más de **140** países

Premiado y certificado

BuyersLab PLATINUM TESTED SOLUTION 2023

BuyersLab PLATINUM TESTED SOLUTION 2022

BuyersLab PLATINUM TESTED SOLUTION 2021

ISO 9001 TÜV SÜD ISO 14001 ISO/IEC 27001