myQ X

Deployment v2

ENGLISH

Generated from docs.myq-solution.com
September/2026

Table of Contents

Use the Deployment guide to plan a MyQ X deployment before you start installing or configuring the system. This guide is intended for administrators, solution architects, consultants, and technical partners who are responsible for planning, preparing, or validating a MyQ deployment.

The guide helps you choose the right deployment model, prepare your infrastructure, and avoid common rollout issues. It focuses on recommendations, best practices, planning decisions, and deployment gotchas. For product-specific installation and configuration steps, use the relevant MyQ X Server guide.

You will learn how to plan:

- Deployment models, including standalone, multi-site, cloud, and hybrid scenarios.
- Server sizing, storage, network access, firewall rules, and certificates.
- User synchronization, authentication, print delivery, desktop clients, and mobile printing.
- Fallback, failover, backup, and other resilience measures.

---

1 Contents

2 Planning Your Deployment

Use this page to identify the main planning decisions for a MyQ deployment before you start installing or configuring the system.

During planning, evaluate the deployment model, expected capacity, network architecture, availability requirements, upgrade strategy, and long-term growth of the environment. These decisions affect server placement, infrastructure sizing, user authentication, print delivery, fallback options, and maintenance effort.

2.1 Before You Start

Consider these questions:

- Do you want to deploy MyQ on-premises, in a private or hybrid cloud, or use a public cloud print management solution?
- Do you need one standalone print server, or multiple servers across different locations?
- What is the expected size of the installation, and how quickly might it grow?
- How reliable is the network in each location where MyQ will be used?
- How often can you upgrade servers, embedded terminals, desktop clients, and other connected components?
- What fallback, failover, backup, and incident response measures do you need?

2.2 On-Premises vs Cloud

The right deployment model depends on your infrastructure, security requirements, administration model, and expected maintenance effort.

MyQ X is designed for on-premises and private or hybrid cloud environments. It can be deployed as a standalone Print Server, or as a multi-site environment with one Central Server and several connected Print Servers.

> **Tip!**
> For cloud-native environments, consider **MyQ Roger**. This public cloud print management solution designed for organizations that prefer a SaaS model, reduced infrastructure maintenance, and support for mobile, remote, and hybrid work.

2.3 MyQ X in Private Cloud

MyQ X servers can be deployed in a private or hybrid cloud environment, for example on an Azure virtual machine connected to your network.

Common deployment models include:

- A Central Server running in the cloud with on-premises Print Servers connected to it.
- Central Server and Print Servers running in a private cloud.
- Print Servers running close to local printer fleets, with a Central Server used for centralized management and reporting.

2.4 MyQ X Releases

MyQ X releases major and minor versions to deliver larger product changes, and patch versions to provide maintenance, security, compatibility, and stability updates.

For access to the latest features, improvements, security updates, and fixes, use the latest supported version and apply patches regularly. For many production environments, the latest Long-Term Support (LTS) version provides a more practical balance between stability, support lifecycle, and upgrade effort.

Before choosing or upgrading to a target version, review the release notes, product end-of-life policy, system requirements, and upgrade instructions for the relevant MyQ server and components. Also consider compatibility with embedded terminals, desktop clients, mobile clients, and other connected components when planning an upgrade.

Product versions are published on the MyQ Community Portal in the Downloads section.

2.5 Before Installation

After completing the deployment planning, confirm the following decisions before running the MyQ installers.

2.6 Central Server Database

Print Server, whether standalone or site, uses an integrated Firebird database. No database backend decision is required.

Central Server uses the integrated Firebird database by default, but can also use an external Microsoft SQL Server database. Decide the Central Server database

approach before installation, especially if you plan to use Microsoft SQL Server or deselect the integrated Firebird database during installation.

Use the integrated Firebird database unless your organization already uses Microsoft SQL Server for similar workloads, or has database management, backup, monitoring, or availability requirements that are better handled in SQL Server.

2.7 Installation Order in Multi-Site Environments

The Print Server and Central Server installers can be run in any order. However, starting with the Central Server is the recommended practice. User synchronization runs on the Central Server first, and site servers pull user data from it – synchronizing to a site before the Central Server has users will leave the site empty until the next sync cycle.

If you are adding new Site Servers to an existing Central Server, upgrade the Central Server to the target compatible version before installing the new sites. This allows new sites to be installed at the target version immediately, rather than requiring a second upgrade pass.

2.8 Version Compatibility

The Central Server version must be equal to or higher than the version of any connected Site Server. Always use the latest released patch of the version you are deploying. Before rollout, verify the exact supported version combinations in the current release notes and upgrade documentation.

Valid combinations:

Central Server	Site Server
10.3	10.3
10.3	10.2
10.2	10.2

A site server at a higher version than the Central Server is not supported.

See also:

- Product & Support End-of-Life Policy[1]

- https://community.myq-solution.com/
- Deployment in the Cloud (see page 30)
- https://roger.myq.cloud/
- (10.3) MyQ X Server

2.9 Standalone or Multi-Site

MyQ X can be deployed as a standalone Print Server for a single environment, or as a Central/Site architecture for larger or distributed environments. The right model depends on the number of locations, number of devices, user scale, network reliability, administration model, reporting needs, and expected growth.

2.9.1 Planning Limits and Terminology

In a standalone deployment, one **Print Server** manages users, devices, queues, jobs, reporting, and local system configuration.

A **Site Server** is a Print Server that is connected to a **Central Server**. The server component is functionally the same, but its role changes when it is managed as part of a Central/Site architecture.

In a Central/Site deployment, Central Server provides centralized licensing, consolidated reporting, user distribution, and selected shared configuration. Site Servers handle local print processing, scanning, device communication, embedded terminals, and other site-level operations. Site Servers still require some local configuration and maintenance.

MyQ X supports up to 30,000 managed devices across all connected sites. Use the current system requirements for per-server sizing, storage, and hardware recommendations.

2.9.2 Overview of Deployment Scenarios

Scenario	Best for	Advantages	Drawbacks

1. https://www.myq-solution.com/product-support-end-of-life-policy

1. Standalone Print Server	Small and medium environments with one main location	Simple architecture and maintenance, single administrative domain	Limited growth path if the environment expands across many sites or exceeds local server capacity
2. Multiple Print Servers at one site	Large single-location environments with many devices, high print volume, or local segmentation needs	Better distribution of print services, support for location-based printing, more flexible scaling	More servers to maintain; no centralized administration unless Central Server is added
3. Central/Site architecture	Distributed organizations that need local print processing and central management	Centralized reporting and management with local site operation	More complex architecture, more infrastructure, and more planning required
4. Small branches served by one Print Server	Main office with several small branches and reliable network connectivity	Lower infrastructure and administration overhead at remote sites	Branches depend on network connectivity to the Print Server

Tip!
Use a standalone Print Server for simple single-site deployments. Use a Central/Site architecture for multi-site environments that need local print processing with shared reporting or administration.

2.9.3 Decision Factors

When choosing a deployment model, consider the following factors:

- **Number of locations:** Decide whether one server can reasonably serve the whole environment, or whether local servers are needed at individual sites.

- **Device and user scale:** Estimate the number of printing devices, users, Desktop Clients, embedded terminals, and mobile clients at each location.
- **Network reliability and latency:** Consider whether print jobs, authentication, scanning, and device communication can depend on network links between locations.
- **Administration model:** Decide whether administration should be centralized, delegated per site, or separated by tenant or organizational unit.
- **Security boundaries:** Consider whether sites, departments, or tenants require separate administration, access control, reporting visibility, or data handling rules.
- **Reporting requirements:** Consider whether reporting must be consolidated across multiple locations.
- **Local print continuity:** Decide whether users must be able to print or release jobs during network outages or server maintenance.
- **Growth expectations:** Plan whether the environment is likely to expand to more locations, more devices, or higher print volume.
- **Data and reporting flow:** Consider which data must be consolidated centrally, how often reporting data must be available, and whether sites can tolerate delayed synchronization during network outages.
- **Upgrade and maintenance capacity:** Consider how often servers, embedded terminals, Desktop Clients, and related components can be upgraded.

Scenario 1: Standalone Print Server

Use this scenario for a single-location environment where one Print Server can manage the required users, devices, queues, jobs, and reporting.

This is typically the simplest MyQ X deployment model. It is suitable when the organization has centralized operations, one main administrative domain, and no requirement for site-level separation or centralized management across multiple Print Servers.

Key characteristics:

- One Print Server manages the environment.
- Suitable for environments up to the recommended standalone Print Server capacity.
- Simpler installation, maintenance, backup, and troubleshooting.
- No Central Server is required.

This model is often a good starting point for small and medium deployments. If the environment later grows across multiple sites or requires centralized management of several Print Servers, it can be migrated to a Central/Site architecture.

Scenario 2: Multiple Print Servers at one site

Use this scenario for a large single-location environment where one Print Server is not enough, or where print services need to be separated by building, department, device fleet, or availability requirement.

Multiple Print Servers can be managed independently. If you need unified reporting, licensing, or administration across them, plan a Central/Site architecture instead (Scenario 3).

This model can help distribute load, reduce local bottlenecks, and support location-based print services. It may also be useful when different parts of the organization require separate administration or maintenance windows.

Key characteristics:

- Multiple Print Servers operate within one physical location or campus.
- Print services can be separated by area, department, or device group.
- Useful for environments with high print volume, many devices, or many Desktop Clients.
- Can support proximity printing and local segmentation.

Consider Central Server if you need centralized reporting, licensing, administration, or coordination across the Print Servers.

Scenario 3: Central/Site Architecture

Use this scenario for distributed organizations that need local print processing at each site and centralized management across the whole environment.

In this architecture, Central Server provides central management, licensing, reporting, and selected shared configuration. Site Servers handle local print processing, scanning, device communication, embedded terminals, and user interaction with printers.

This model is suitable when sites are geographically distributed, have their own printer fleets, or require local operation for performance, security, or resilience reasons.

Key characteristics:

- Central Server provides consolidated administration and reporting.
- Each site runs a local Site Server for local print and device operations.
- Sites can be managed with site-level rights and responsibilities.
- The architecture can scale across many locations and large device fleets.
- Site Servers still require local configuration, monitoring, maintenance, and backup planning.

Use this model when central control is important, but print processing should remain close to users and devices.

Scenario 4: Small branches served by one Print Server

Use this scenario when one Print Server can serve a main office and several smaller branches without placing a server at each location.

This model reduces infrastructure and maintenance effort at remote locations. It can work well for small branches with reliable connectivity, limited local IT resources, and lower print volumes.

Key characteristics:

- One Print Server manages devices and users across multiple locations.
- Remote locations do not require their own local MyQ server.
- Administration, backup, and maintenance are simpler than in a full Central/Site architecture.
- The model depends on reliable network connectivity between remote locations and the Print Server.
- Print jobs, authentication, scanning, and device communication may be affected by network latency or outages.

Use this model when your branch locations have reliable network connectivity and modest print traffic. If a branch requires local print continuity, has unreliable network links, or grows significantly, plan a transition to a local Site Server managed by a Central Server.

2.9.4 Multi-Site Planning Considerations

Multi-site deployments require additional planning for job mobility, local spooling, storage connections, administration, and configuration management. Planning with the following features in mind can help support your deployment in distributed environments.

Job Roaming

Use **Job Roaming** when users need to release jobs across multiple Site Servers.

With Job Roaming, users can view and release jobs from different sites, and jobs can be transferred between sites when required. This improves flexibility for users who move between locations, but it can also affect network traffic, storage, and job transfer behavior between servers.

Plan Job Roaming when users regularly work across multiple locations, or when the organization needs a consistent pull-printing experience across sites.

Local Spooling

Use local spooling to reduce dependency on server-to-site network traffic and help maintain print availability during network or server disruptions.

Client Spooling keeps print data on the user's computer until release. This can reduce print data transfer through the server and may be useful when users print large jobs or when network links to the server are limited.

Device Spooling sends jobs directly to supported devices with embedded terminals. This can reduce server involvement during release, but support depends on the device vendor, model, and embedded terminal capabilities.

Plan to use local spooling when WAN traffic, server load, or outage tolerance are important deployment concerns.

Cloud Storage Connections

In multi-site environments, plan how users will connect to cloud storage services and whether those connections need to be available across sites.

If users move between locations, a consistent cloud storage experience can reduce repeated authentication and support effort. Before rollout, verify the required cloud integrations, authentication method, and site behavior for the target MyQ version.

Administrative Control

Use site-level administration when responsibilities need to be separated by location, tenant, department, or support team.

In Central/Site deployments, administration can be shared while still allowing selected responsibilities to be delegated at the site level. This supports least-privilege administration and can reduce operational dependency on a single admin team.

Plan the administration model before rollout, including who can manage users, devices, queues, reports, and site-specific settings.

Configuration Reuse

For deployments with many Site Servers, configure one Site Server as a reference server, then use the supported backup, restore, or settings-duplication features to reuse its configuration as a starting point for other Sites.

After restoring or duplicating settings, review site-specific settings such as printers, printer groups, IP addresses, network settings, authentication dependencies, local queues, certificates, and maintenance windows.

Before rollout, define which settings are part of the shared baseline, which settings are site-specific, and how updates to the baseline will be maintained.

See also:

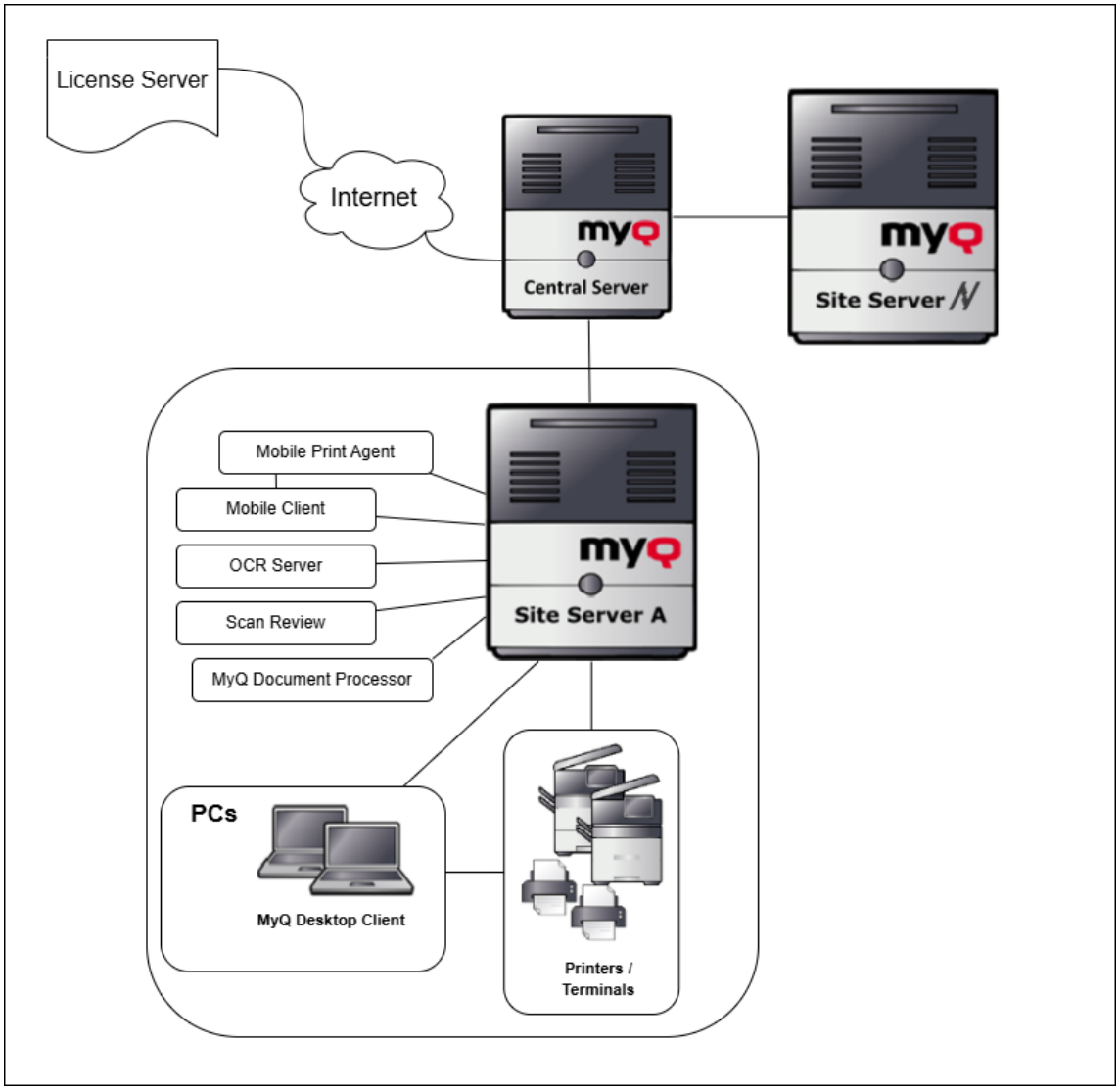
- Components Overview (see page 15)
- Infrastructure and Capacity (see page 22)
- Network Architecture (see page 19)
- (10.3) System Requirements
- Deployment in the Cloud (see page 30)
- (10.3) Main Communication Ports
- (10.3) Central & Site Administration

2.10 Components Overview

MyQ X is a distributed system consisting of servers, client applications, embedded terminal packages, and supporting services. Use the diagram below to identify the components required for your deployment.

Consider how users will print, scan, authenticate, release jobs, use mobile devices, and access MyQ services. The components you need depend on your deployment model, printer fleet, authentication requirements, scan workflows, mobile printing, reporting, and availability requirements.

This page provides a planning-level overview of the main MyQ components. For installation, configuration, ports, and detailed requirements, see the relevant MyQ Server and component documentation.



1 MyQ Server Architecture

2.10.1 Core Server Components

Print Server / Site Server

Print Server is the core MyQ X component. It manages print, scan, and device operations, including printers, queues, jobs, users, embedded terminal communication, reporting data, and local system configuration.

Every MyQ X deployment requires at least one Print Server. Consider whether one Print Server is sufficient or whether the environment requires multiple Print Servers for scale, location-based printing, local resilience, or separate administration.

A **Site Server** is the same component operating as part of a Central/Site deployment. It is connected to a Central Server while continuing to handle local print, scan, and device operations at its site.

Central Server

Central Server is used in Central/Site deployments with multiple Site Servers. It provides central licensing, consolidated reporting, user distribution, and selected shared configuration for connected Site Servers.

Use Central Server when multiple locations or Print Servers require shared reporting, administration, user distribution, or coordinated management.

Central Server does not replace local Site Server administration. Site Servers still require local setup, monitoring, maintenance, backup planning, and site-specific configuration.

2.10.2 User-Facing Components

Embedded Terminals

Embedded terminals are applications installed on supported multifunction devices. They let users authenticate and access supported MyQ functions directly from the device panel, including print release, copying, scanning, and other terminal actions.

Use embedded terminals when users require secure access to device functions, authenticated print release, user-specific scan workflows, or accounting directly at the device.

Available functions and behavior depend on the device vendor and model, terminal package, license, configuration, and MyQ version.

MyQ Desktop Client

MyQ Desktop Client is installed on user workstations. Depending on its configuration, it can provide user authentication, job metadata collection, project or cost-center selection, local printer monitoring, client spooling, fallback printing, and other workstation-side printing features.

Use MyQ Desktop Client when printing must be controlled or enriched on the user workstation, particularly for project accounting, client spooling, fallback printing, local printer monitoring, or prompts before job submission.

MyQ X Mobile Client

MyQ X Mobile Client gives users access to selected MyQ functions from mobile devices.

Use MyQ X Mobile Client when users need features such as mobile printing or interaction with their print environment without using a workstation.

2.10.3 Supporting Components

Mobile Print Agent

Mobile Print Agent supports mobile printing through protocols such as AirPrint and Mopria. It is typically deployed where mobile devices need to discover printers or MyQ queues on the local network, such as a Wi-Fi segment used by mobile users.

Use Mobile Print Agent to provide AirPrint or Mopria printing from iOS, macOS, or Android devices.

MyQ Document Processor

MyQ Document Processor is a supporting service that performs document-processing operations for MyQ scan workflows. It processes jobs received from MyQ X and returns the resulting documents for delivery to their configured destinations.

Use MyQ Document Processor for scan workflows that require supported document-processing functions, including OCR and conversion to searchable document formats.

Document processing can require significant CPU, memory, and storage resources. Consider installing MyQ Document Processor on a separate machine, particularly in environments with frequent scanning or large documents.

MyQ Scan Review

MyQ Scan Review adds a review and approval stage to Easy Scan workflows. Users scan documents at a device as usual, after which authorized reviewers can inspect the scanned images and record the result of the review before the paper originals are archived.

Use Scan Review when the organization requires a documented and auditable replacement-scanning process. It is intended to support compliance workflows such as those based on Germany's TR-RESISCAN guidelines.

Scan Review requires additional planning for reviewer access, workflow responsibilities, metadata, document retention, and integration with the

organization's archiving process. It supports the review workflow but does not by itself constitute a complete compliant archiving solution.

OCR Server (Deprecated)

OCR Server is a legacy supporting component used to perform optical character recognition in scan workflows, enabling output such as searchable PDFs and recognized text.

OCR Server is deprecated. For new deployments, use MyQ Document Processor where it supports the required document-processing workflow. Existing deployments should consider migration requirements when planning an upgrade.

Because OCR processing can require significant resources, OCR Server may need to run on a separate machine.

External Systems and Integrations

Depending on the deployment model and enabled features, MyQ X may depend on external systems such as identity providers, directory services, mail servers, cloud storage providers, licensing services, reporting tools, backup locations, monitoring systems, or BI tools.

Plan these dependencies early because they can affect authentication, user synchronization, scanning, notifications, reporting, firewall rules, certificates, availability, and support ownership.

See also:

- (10.3) MyQ X Server
- (10.2) MyQ Desktop Client
- (10.3) MyQ Scan Review
- (10.3) MyQ Document Processor
- (10.2) MyQ X Mobile Client
- (3.4) MyQ OCR Server
- (1.3) Mobile Print Agent

2.11 Network Architecture

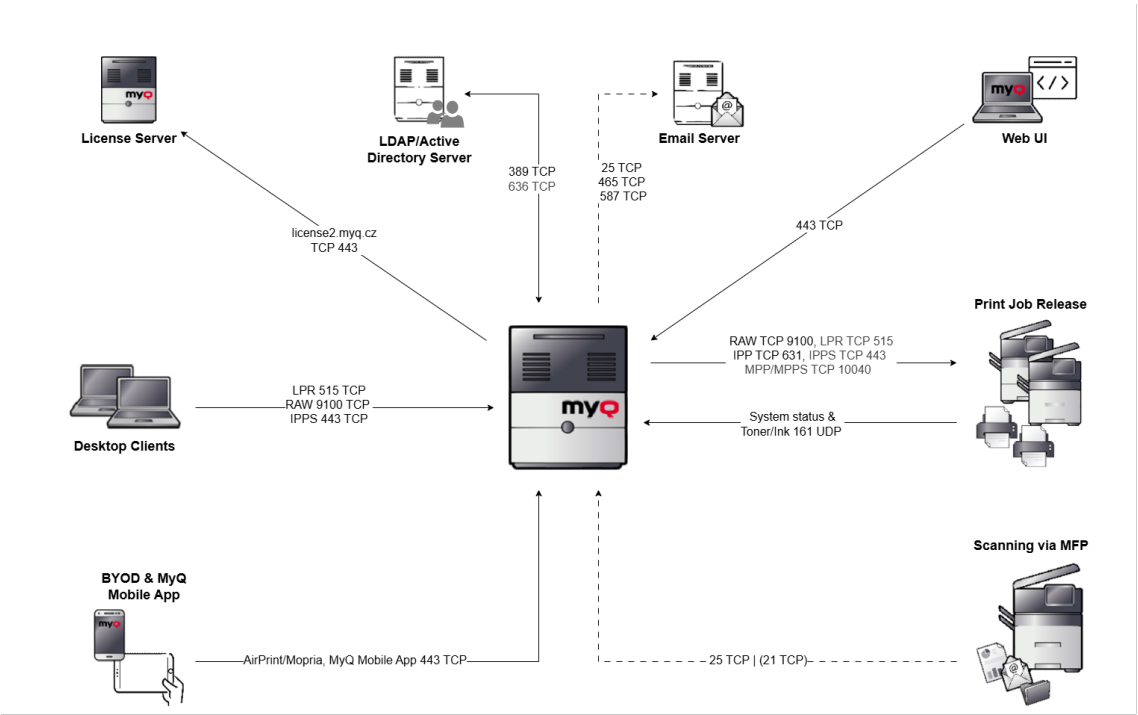
Network planning starts with identifying which MyQ components, clients, devices, and external services must communicate in your deployment. Focus on the paths

used for printing, scan reception and delivery, authentication, administration, reporting, licensing, and any enabled integrations.

Use the diagrams below as a reference map before completing the checklist. Focus on the connections that apply to your environment, especially traffic that crosses sites, network zones, or external services.

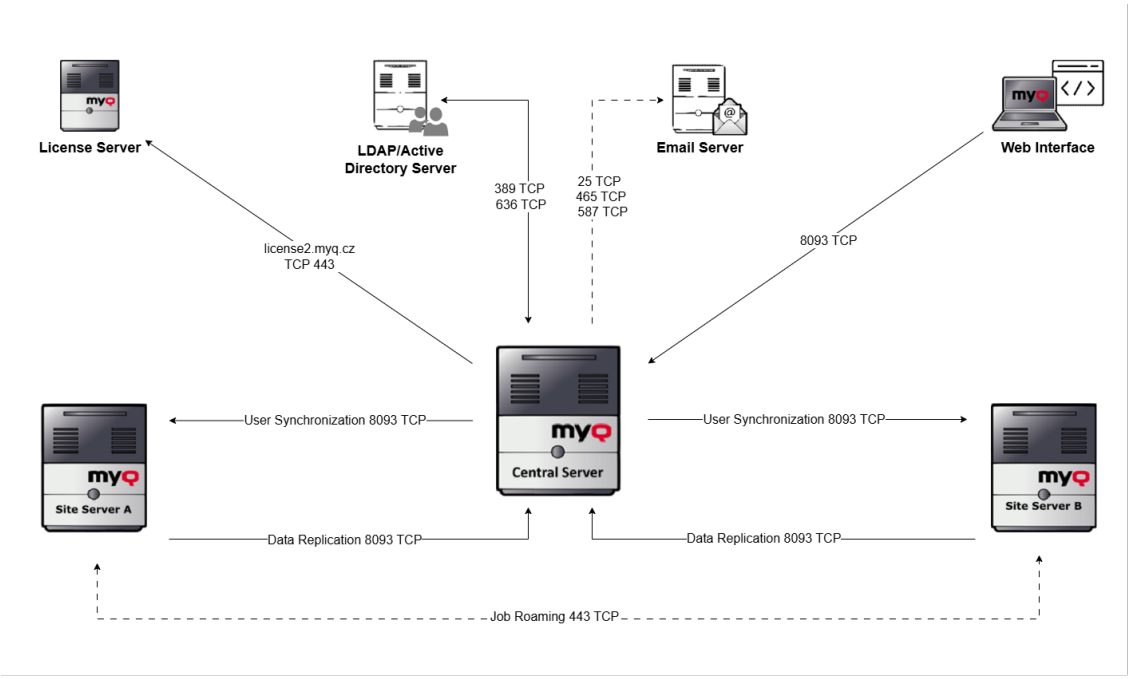
> ⚠ These diagrams are planning references, not a comprehensive port matrix. The current port, protocols and version-specific defaults are in the MyQ X Server guide:
>
> - (10.3) Main Communication Ports

2.11.1 Standalone Print Server



2 Print Server

2.11.2 Central/Site Environment



3 Central Server

2.11.3 Network Planning Checklist

Before deployment, confirm the main network paths that MyQ depends on.

1. **Server placement and site topology**

   Decide where each Print Server, Site Server, Central Server, OCR Server, and Mobile Print Agent will run. Place services close enough to users, printers, and required scan destinations to avoid unnecessary WAN dependency, especially where large print jobs or scan files would otherwise cross slow or unreliable links.

2. **Client, mobile, and user access**

   Confirm how users and workstations connect to MyQ, including MyQ Desktop Client, MyQ X Mobile Client, AirPrint, Mopria, and Mobile Print Agent where used. Consider users who move between sites and need access to jobs, printers, or cloud storage from different locations.

3. **Printer and embedded terminal communication**

   Confirm that MyQ servers can reach printers for monitoring, configuration, and print delivery. Also confirm the scan paths used in your deployment, including how scans are received from devices and how MyQ delivers scans to email, folders, cloud storage, FTP servers, or other configured destinations. Embedded terminals must be able to

communicate with the required MyQ server, and any vendor-specific terminal requirements should be checked before rollout.

4. **Central, site, and identity communication**
   Confirm reliable communication between Central Server and Site Servers, including DNS, routing, certificates, and firewall rules. In cloud and hybrid deployments, this does not necessarily require a VPN between the Central Server and Site Servers; check the current cloud deployment and port requirements for the selected model. Also confirm access to the user sources and authentication services used in your deployment, such as LDAP/LDAPS directories, Microsoft Entra ID, Google Workspace Secure LDAP, RADIUS, or other configured authentication providers.
5. **External services, mail, scan, storage, and certificates**
   Confirm access to the external services used in your deployment, such as mail servers, scan destinations, cloud storage, licensing services, Microsoft or Google endpoints, remote backup locations, and monitoring systems. Define stable DNS names and certificate requirements before production, rather than relying on temporary hostnames or IP addresses.
6. **WAN resilience and rollout validation**
   Identify sites with slow, weak, or unstable links and decide whether they need a local Site Server, Client Spooling, Device Spooling, Offline Login, or another fallback option. Verify each fallback option against the relevant MyQ X Server, Desktop Client, and embedded terminal documentation before rollout. Before rollout, test the paths used in your deployment, such as printing, scan reception and delivery, authentication, embedded terminal login, mobile printing, reporting, remote backups, and expected behavior during network restrictions or outages.

2.12 Infrastructure and Capacity

Use this page to plan infrastructure capacity before deploying MyQ X. For exact CPU, RAM, storage, operating system, software, and port requirements, see the current MyQ X Server system requirements.

Do not size production only from a small pilot or initial rollout. Early testing may not expose resource limits that appear later as more users, devices, terminals, and

features are added. Many deployments start small and grow as more users, printers, terminals, and features are added, so base your requirements on real and expected workloads:

- The operating system and Windows services
- MyQ X server components
- Database growth
- Print jobs waiting for release
- Scan files and scan delivery
- Logs and diagnostic data
- Reports and archived reports
- Job archiving and job preview, if enabled
- Replication data in Central/Site deployments
- Other applications running on the same server, if any

2.12.1 Standalone and Central/Site Deployments

In a standalone deployment, one Print Server handles the print, scan, device, user, queue, job, and reporting workload for its environment.

In a Central/Site deployment, Central Server and Site Servers have different roles. Central Server provides centralized licensing, consolidated reporting, user distribution, and selected shared configuration. Site Servers handle local print processing, scanning, printer communication, embedded terminals, and user interaction with devices.

Central/Site deployments usually require more infrastructure planning than standalone deployments. Site Servers still need enough resources for local operations, and Central Server needs enough resources for reporting, user distribution, replication, and coordination across connected sites.

Installing Central Server and a Site Server on the same machine is possible, but should be reserved for small installations and sized accordingly.

2.12.2 Server Sizing Considerations

Recommended system requirements are a baseline, not a guarantee for every environment. Actual resource usage depends on how MyQ is used.

Increase capacity planning when the environment includes:

- Many printers or embedded terminals
- High print volume or large print jobs
- Heavy scan delivery/storage requirements, or OCR workflows
- Job archiving or job preview

- Many Desktop Clients
- Credit, quota, projects, or detailed accounting
- Heavy API usage or external integrations
- Large user synchronization sources
- Central/Site replication and reporting

Do not size MyQ X only for the pilot phase. Use the pilot to validate behavior, but size the infrastructure for the expected production workload, including future users, devices, terminals, print volume, scan volume, reporting, and enabled features.

Signs of insufficient resources can include, for example, jobs not appearing or taking too long to print, slow authentication at devices, outgoing emails getting stuck, and slow loading of the Web Interface, mobile app, or desktop app.

2.12.3 Server Isolation

Install MyQ X on a dedicated server or virtual machine where possible.

Avoid sharing the server with other applications that use databases, web servers, PHP runtimes, mail services, or heavy background processing. Shared services can create resource or service conflicts and make troubleshooting harder. In some cases, conflicts can cause malfunctions in MyQ or in the other application.

2.12.4 Storage Planning

Plan storage before production use. MyQ storage usage can grow quickly depending on print volume, scan volume, job retention, reports, logs, job archiving, and job preview.

When planning storage, consider:

- Database growth
- Print jobs waiting for release
- Scan files and temporary scan data
- Job archive storage
- Job preview files
- Log data and log backups
- Report data and archived reports
- Database backups
- Replication data in Central/Site deployments

Use dedicated storage for MyQ data where appropriate, especially in larger environments. Also consider storage performance, not only available capacity.

Define retention policies before rollout. Decide how long jobs, history, reports, logs, and backups must be kept, and balance those requirements against storage growth and reporting needs. The job and history retention periods you set directly determine how far back reports can reach – once data is deleted, it can only be recovered from a backup that still contains it.

Do not leave debug logging enabled longer than necessary. Debug logs can grow quickly and should normally be used only for troubleshooting.

In Central/Site deployments, monitor replication health. If replication errors accumulate, the Site Server's replication log table can grow rapidly and cause significant database bloat.

2.12.5 Print, Scan, Archive, and Backup Destinations

In larger environments, do not assume that the operating system or application disk is the right place for all MyQ data. Plan which data should remain local and which should use dedicated or external storage.

For larger or fast-growing deployments, decide which data needs dedicated or external storage, such as MyQ data folders, job files, reports, databases, database backups, log backups, scan destinations, and archived jobs.

If users scan to network folders, FTP, cloud storage, or email, include those destinations in storage, network, and availability planning.

If Job Archiving or Job Preview is used, plan the storage impact carefully. These features can significantly increase disk usage. Define destination locations, retention limits, and any applicable size restrictions as part of the initial deployment design.

2.12.6 Network and Firewall Planning

Depending on the selected deployment model and enabled features, MyQ X may require communication between servers, printers, embedded terminals, user workstations, mobile devices, identity providers, mail servers, cloud services, licensing services, and optional supporting components.

Plan network access according to the selected deployment model and enabled features. Pay particular attention to communication between sites, terminal vendor requirements, print and scan traffic, identity providers, mail systems, cloud integrations, and mobile printing.

For exact ports and protocols, use the current MyQ X Server communication ports documentation.

2.12.7 Virtualization

MyQ X can run on virtual servers. When using virtualization, allocate resources according to the current MyQ X Server system requirements and expected workload.

For production deployments, avoid resource contention on the virtualization host, especially for CPU, memory, and storage performance. Monitor the virtual machine during peak usage and adjust resources if print, scan, authentication, reporting, or client operations become slow.

See also:

- (10.3) System Requirements
- (10.3) Main Communication Ports
- (10.3) Central & Site Administration
- (10.3) Site Server Data Replication
- (10.3) Easy Config Settings Tab

2.13 Security and Certificates

Proper configuration of security and certificates is essential for safeguarding sensitive data such as print jobs, user credentials, and administrative access.

2.13.1 General Security

MyQ X uses default security settings for encrypted communication between MyQ components, clients, devices, and external services. The exact TLS behavior depends on the communication layer and configuration, including web HTTPS, SMTP, IPP, LPR, WebSockets, and related settings in `config.ini`.

Recommended TLS Version

Keep the default minimum TLS version of 1.2, or increase it to TLS 1.3 where all connected clients and devices support it. Lower the minimum TLS version only for legacy compatibility cases, such as older devices that cannot use TLS 1.2 or later.

2.13.2 Certificates

Certificates are used to secure and validate communication between MyQ servers, print devices, user workstations, mobile clients, and external services. Administrators can manage the server certificates and certificate authority mode used by MyQ so that connecting clients and devices can trust the service. MyQ X supports the use of trusted third-party certificates, as well as internally issued certificates to enable flexible and scalable security configurations for different environments.

Trust Between MyQ X and Servers

To securely connect to external systems that MyQ X needs to interact with, you will need the MyQ server to trust the certificates of these remote servers and services. This is needed for HTTPS, SMTPS, LDAPS, and IPPS.

Since version 10.2, MyQ X is designed to automatically trust the Root CA certificates from the server's system certificate store.

Certificates in Certificate Management (`mmc.exe`) > **Trusted Root Certificate Authorities** are exported into the `cacert.pem` file that sits in the `ProgramData` folder of MyQ X.

The certificate synchronization is performed **during the Maintenance task run**. For this reason, if you encounter problems with certificates, and you confirm that the correct certs are installed in the system, run the Maintenance task, and try connecting MyQ X to the remote system again.

This allows MyQ X to automatically trust certificates issued by imported CAs, which is particularly helpful when they are published by Group Policy or from Active Directory.

> ⚠ **Before MyQ X 10.2 Update**
>
> For the majority of connections that were expected to be secured via SSL/TLS, it was already necessary that the remote server's certificate was trusted by the system MyQ X was running on, and thus also by MyQ X.
>
> For some operations, it could have been necessary to manually edit the `cacert.pem`, `ldap.conf` or `.ldaprc` files and include necessary (especially Enterprise) CA certificates. The reason was that certain connections and components utilized a different certificate store rather than the system one.

Trust Between MyQ X and Connecting Clients

Read how to select the server certificate that MyQ X presents to clients to secure communication.

Before deploying clients or enrolling devices, decide which hostnames or IP addresses they will use to connect to MyQ. Any hostname or IP address used by devices or MyQ Desktop Client must be included in the server certificate's Subject Alternative Name; otherwise, certificate validation can fail.

You will need this to:

- Serve your users the MyQ Web Interface on HTTPS.
- Communicate securely with printers and MFDs and the Embedded terminals installed on those devices.
- Connect to the server with the Desktop Client operating in the "Strict" mode.
- Print securely via IPPS.
- Connect and print with the Chromebook Extension.
- Connect securely from the Mobile Client for Android and iOS.

You can manage certificates on Print Server and Central Server. Go to **MyQ > Settings > Network**. The following modes are available:

Built-in Certificate Authority

MyQ creates a self-signed CA certificate and uses it to sign server and client certificates.

To use these certificates in production environments, you need to distribute the CA (which can be exported on the Network page) to all clients that will be connecting to the server. This is feasible for organization-managed devices where this certificate can be distributed with Group Policy or Intune.

To enable BYOD devices to connect, provide users with a way to download and install the MyQ Certificate Authority manually. Otherwise, users may see warnings that the server cannot be trusted.

Embedded terminals also need to trust the certificate presented by the MyQ server; if terminal-side certificate trust is not handled correctly, terminal communication may fail.

Company Certificate Authority

In Company Certificate Authority mode, MyQ uses an intermediate CA certificate from your company CA to sign certificates for the server and clients.

Since this certificate authority (CA) is probably a custom enterprise CA, similar conditions apply as for the built-in self-signed certificate. The CA will need to be distributed to devices that your organization can manage, or made available for end users to install themselves.

Manual Certificate Management

Provide a certificate for the MyQ Server. MyQ creates no certificates; all certificates are managed by you.

This mode is intended for administrators who already understand certificate chains, private keys, Subject Alternative Names (SANs), and trust distribution. In this mode, you provide the server certificate yourself. The certificate must be issued for the MyQ server and signed by a certificate authority that your clients and devices can trust, such as a publicly trusted CA or an internal CA created with Active Directory Certificate Services (AD CS).

Bring-Your-Own-Devices and Certificates

Compared to managed environments, such as a Windows domain, certificates for BYOD and devices not joined to a local domain or Entra tenant are a more complex issue.

If you expect to commonly serve printing services to guest users and visitors, or your organization is considered a public service (schools, libraries, traffic hubs, etc.), consider signing your server certificates by a publicly trusted CA that is already included in desktop and mobile operating systems and browsers out-of-the-box.

2.13.3 Certificates and Embedded Terminals

During remote setup when the Embedded terminals are installed, the MyQ X server uploads the CA certificate to the device, so that when MyQ X presents its certificate to the device, it is trusted. This is, however, possible only in the *Built-in Certificate Authority* and *Company Certificate Authority* modes.

In *Manual Certificate Management* mode, MyQ X does not get access to the CA certificate because it is not provided. Only the server certificate, which is signed by the CA, is uploaded. The CA certificate needs to be added to the devices manually.

Some vendors or devices might have stricter rules for certificate validation, e.g., they can require the certificate to contain the full FQDN (Fully Qualified Domain Name; such as `print.acme.com`), or the device might reject wildcard certificates (such as `*.acme.com`).

Follow the manual, instructions, and recommendations for each particular vendor. The certificate requirements may differ from device to device, and some devices may not support automatic upload. In case of problems, consult with your MyQ X provider.

See also:

- (10.3) Network Settings
- (10.3) Advanced Security
- (10.3) Main Communication Ports

2.14 Deployment in the Cloud

MyQ X can be deployed fully or partially in the cloud. This section covers the main cloud deployment models, network and communication requirements, and print delivery considerations specific to cloud environments.

2.14.1 Cloud Deployment Models

Hybrid Cloud – Central: The Central Server runs in a cloud-hosted virtual machine and acts as the central reporting and management point for site servers running in local on-premises networks. No VPN tunnel is required between the Central Server and site servers.

Hybrid Cloud – Combined: The Central Server and selected site servers run in the cloud, while the remaining site servers run on-premises. This model is common in organizations that prefer to keep large sites local while moving smaller or mid-sized sites to the cloud. On-premises site servers require no VPN tunnel to reach the Central Server. Cloud-hosted site servers require a VPN tunnel to communicate with printing devices and end-user devices on local networks.

Full Cloud: All MyQ X servers run in the cloud. VPN tunnels are required between each cloud-hosted site server and the local networks where printing devices and end-user devices are located.

2.14.2 Connection Requirements

A VPN tunnel is not required specifically for Site Server-to-Central Server communication. Since MyQ X 10.1, Site Servers can reach the Central Server through its public interface. Cloud-hosted Site Servers may still require a VPN or equivalent private connectivity to reach printers, end-user devices, and other services on local networks.

When reviewing port requirements, pay attention to embedded terminal vendor-specific ports. Kyocera and Kyocera Lite terminals require additional ports for the built-in PM Server component. On Print Server 10.2 and later, the FTP Server and SMTP Server can be disabled if the deployment does not require those incoming services.

2.14.3 Cloud-Friendly Printing

In cloud deployments, keeping print data local can reduce WAN traffic and avoid sending large print files to and from cloud-hosted servers. MyQ X supports two local spooling approaches:

- **Client Spooling**
  With the MyQ Desktop Client in Client Spooling mode, only job metadata is sent to the server. Print data stays on the user's workstation and is sent directly to the target device when the job is released.
- **Device Spooling**
  With Device Spooling, jobs are sent directly to supported devices with compatible embedded terminals and can be released after user authentication. Support depends on the device vendor, model, and embedded terminal package – see the embedded terminal documentation or consult your MyQ partner.

2.14.4 Microsoft Universal Print

MyQ X supports Microsoft Universal Print, which can let end users print without a client-side VPN connection by exposing MyQ-connected printers through Microsoft Universal Print. In cloud-hosted MyQ deployments, server-side connectivity between the MyQ server and the local network may still require a VPN or equivalent private connection, depending on where printers and services are located.

See also:

- (10.3) Main Communication Ports
- (10.3) Install MyQ in Private Cloud
- Spooling Strategy (see page 141)
- Set up Microsoft Universal Print (see page 137)

2.15 Microsoft Entra Apps and MyQ

Several MyQ X integrations use Microsoft Entra applications to authenticate MyQ and authorize access to Microsoft services:

- Microsoft Entra ID and Microsoft Graph
- OneDrive for Business
- SharePoint Online
- Exchange Online
- Universal Print

Depending on the integration and your organization's requirements, you can use automatic setup or register the application manually.

2.15.1 Automatic Setup

MyQ supports automatic setup for Microsoft Entra ID, OneDrive for Business, and SharePoint Online. This is the recommended option when the administrator performing the setup has the required Microsoft Entra permissions.

Automatic setup creates a **service principal**, displayed under **Enterprise applications** in the customer's Microsoft Entra tenant, and configures the credentials and permissions required by the integration.

See Automatic App Registration (see page 33).

2.15.2 Manual Setup

Use manual setup when your organization requires direct control over application registration, credentials, permissions, or administrator consent.

A manually registered application can be shared by **Microsoft Entra ID**, **OneDrive for Business**, and **SharePoint Online**, provided it includes the settings and permissions required by each enabled integration.

Exchange Online and **Universal Print** require dedicated application registrations because they use different application configurations. Do not add them to the shared registration.

See Manual App Registrations (see page 35) .

Before registering an application, determine:

- which integrations it will support
- whether it will be shared or dedicated
- the Microsoft Entra tenant in which it will be registered
- the MyQ server hostname and HTTPS port, where required
- whether it requires a client secret
- the required redirect URIs, API permissions, and authentication scopes

2.15.3 Complete the Integration in MyQ

Application registration prepares the Microsoft side of the integration. Complete the corresponding connection, synchronization, authentication, or service configuration in the relevant MyQ X Server settings.

See also:

- Automatic App Registration (see page 33)
- Manual App Registrations (see page 35)
- Single Sign-On with Entra ID (see page 108)
- Set up Microsoft Universal Print (see page 137)
- Set up Microsoft Exchange Online (see page 49)
- Microsoft Entra Application Reference (see page 41)

2.15.4 Automatic App Registration

MyQ can automatically create and configure the Microsoft Entra enterprise application required by the following integrations:

- Microsoft Entra ID and Microsoft Graph
- OneDrive for Business
- SharePoint Online

Automatic authorization is the recommended setup method when the administrator has the required Microsoft Entra permissions. MyQ creates the enterprise application, configures its credentials and permissions, and obtains administrator consent through a guided authorization process.

Exchange Online and Universal Print require manual application registration. For these and other manual setup scenarios, see **Microsoft Entra Application Reference for MyQ Integrations**.

Before You Begin

To complete automatic authorization, you need:

- a Microsoft Entra tenant
- access to the relevant integration settings in MyQ
- a Microsoft Entra account with the required administrator role

Required Administrator Roles

- **Application Administrator** or **Cloud Application Administrator** can create the service principal in the tenant.
- **Global Administrator** is required to grant administrator consent.
- Therefore, a **Global Administrator** can complete the entire authorization process without involving another administrator.

The administrator permissions used during setup are separate from the permissions that the resulting enterprise application uses at runtime.

How Automatic Authorization Works

Automatic authorization consists of three stages:

1. The administrator signs in to Microsoft Entra ID, and MyQ creates the service principal in the customer's tenant.
2. The administrator authorizes MyQ to configure the application.
3. MyQ assigns the runtime permissions required by the selected integration, and the administrator grants consent.

The service principal is displayed under **Enterprise applications** in the Microsoft Entra admin center.

The exact runtime permissions depend on the integrations enabled for the connection. For a complete list, see **Microsoft Entra Application Reference for MyQ Integrations**.

Application Credentials

Client secrets created by MyQ during automatic authorization are valid for **two years**.

When a secret is within **30 days of expiration**, MyQ reports a Health Check warning. Use **Re-authorize** before the secret expires to create a new secret for the existing connection.

Credentials created directly for service principals are not displayed in the Microsoft Entra admin center. They can be managed through Microsoft Graph or PowerShell.

Re-authorize a Connection

Use **Re-authorize** in MyQ to repeat the Microsoft authorization process for an existing connection.

Reauthorization can:

- complete administrator consent that was not granted during the initial setup
- create a new client secret
- recreate a deleted enterprise application
- change the connection between automatic and manual configuration

Reauthorization updates the existing enterprise application when it is still present. It does not normally create a duplicate.

Recreate a Deleted Enterprise Application

If the enterprise application has been deleted from Microsoft Entra ID, use **Re-authorize** in MyQ. The authorization process creates the service principal again and restores the connection.

Revoke Access

To revoke access for an automatically configured connection, delete its **enterprise application** in Microsoft Entra ID.

This removes the service principal and its credentials from the tenant. If the connection is later reauthorized in MyQ, MyQ creates the service principal again.

2.15.5 Manual App Registrations

Register an application in Microsoft Entra ID when you want to configure a Microsoft Entra ID, OneDrive for Business, or SharePoint Online connection in MyQ X manually.

You can use one application registration for multiple MyQ integrations, or create separate application registrations for each integration. Configure only the redirect URIs and permissions required for the integrations that you plan to use.

This procedure does not apply to Microsoft Exchange Online or Universal Print. These integrations use different application configurations.

Before you begin

Decide which MyQ integrations the application will support:

- Microsoft Entra ID / Microsoft Graph
- OneDrive for Business
- SharePoint Online

You also need the following information:

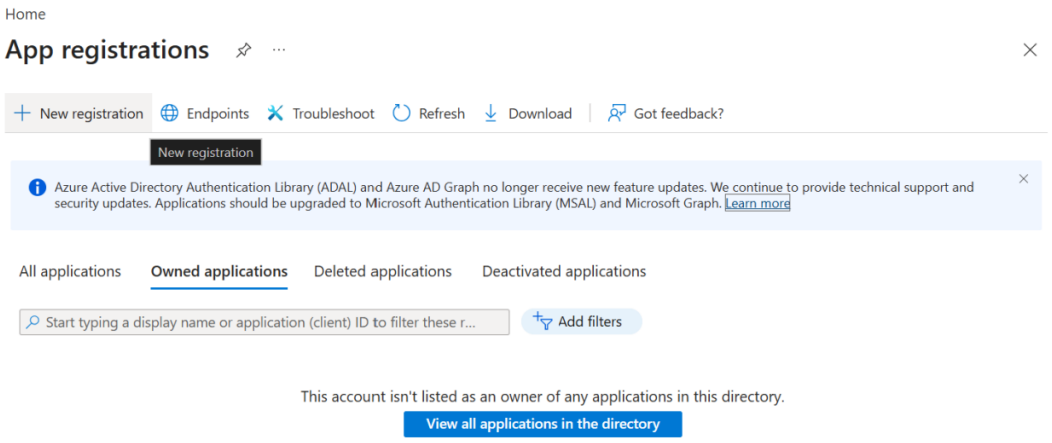
- the Microsoft tenant where the application will be registered
- the MyQ server hostname and HTTPS port, if the application will be used for Microsoft Entra ID authentication
- whether the deployment uses single-tenant or multitenant authentication
- whether MyQ Desktop Client Seamless SSO will be used

For the required redirect URIs, credentials, and permissions, see:

- Microsoft Entra application requirements for MyQ X

Register the application in Microsoft Entra ID

1. Sign in to the **Microsoft Entra admin center**.
2. Go to **Identity > Applications > App registrations**.
3. Select **New registration**.



4. In **Name**, enter a name for the application.

   Example: `MyQ X Connector`, `MyQ Universal Print`, `MyQ Sharepoint`

5. In **Supported account types**, select the account type required for your deployment.
6. Leave **Redirect URI** empty.

   You add the required redirect URIs later in this procedure.

7. Select **Register**.

The application is created.

In the Overview page of the application registration, copy and save the values:

- Application (client) ID
- Directory (tenant) ID

You enter these values when configuring the connection in MyQ.

Add redirect URIs

Add the platform configurations and redirect URIs required by the integrations that will use this application.

1. In the application registration, go to **Manage > Authentication**.
2. Select **Add a platform**.
3. Select the required platform type.
4. Enter the redirect URI.
5. Select **Configure**.
6. Repeat these steps for each additional platform or redirect URI required by the MyQ integrations that will use this application.

Use the following common redirect URI patterns:

Integration or feature	Setup method	Platform	Redirect URI
Microsoft Entra ID / Microsoft Graph	Manual	Web	`https://{hostname:port}/auth`
Microsoft Entra ID SSO helper	Manual	Single-page application	`https://helper.myq.cz/openid/`
MyQ Desktop Client Seamless SSO	Manual, when used	Mobile and desktop applications	`ms-appx-web://microsoft.aad.brokerplugin/{Application-client-ID}`
OneDrive for Business	Manual	Web	`https://helper.myq.cz/`

Integration or feature	Setup method	Platform	Redirect URI
SharePoint Online	Manual	Web	`https://helper.myq.cz/`
Microsoft Exchange Online	Manual	Mobile and desktop applications	`https://login.microsoftonline.com/common/oauth2/nativeclient`
Universal Print	Manual	Mobile and desktop applications	Select the mobile and desktop redirect URI in Microsoft Entra ID.

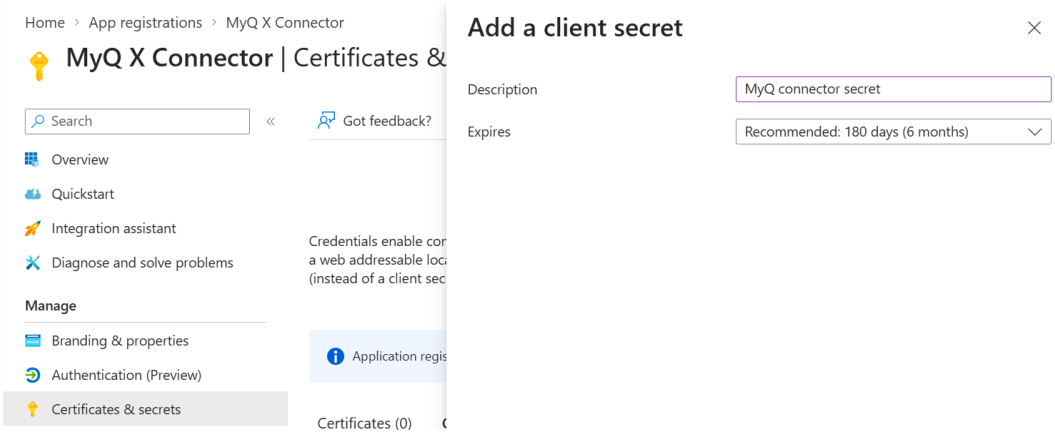
Replace:

- `{hostname:port}` with the hostname and HTTPS port of the MyQ server.
- `{Application-client-ID}` with the Application client ID of the application registration.

Create a Client Secret

Create a client secret for the application. MyQ uses this secret to authenticate to Microsoft Entra ID.

1. Go to **Manage > Certificates & secrets**.
2. Select **Client secrets**.
3. Select **New client secret**.

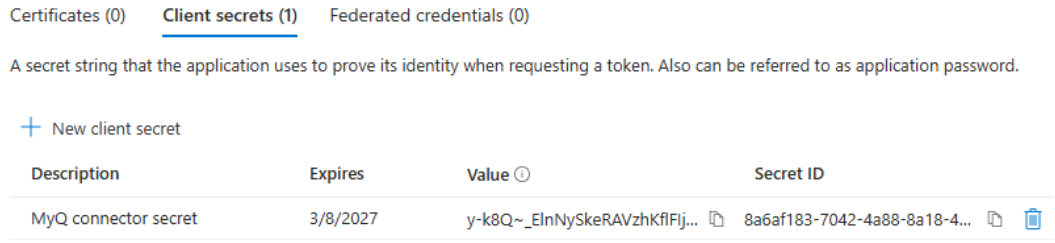


4 Add a client secret

4. Enter a description.

   Examples: `MyQ X Connector`, `MyQ X OneDrive`, `MyQ X SharePoint`

5. Select an expiration.
6. Select **Add**.
7. Copy and save the client secret **Value**.



5 Secret table with expiry, value and secret ID

Important: Copy the secret **Value**, not the Secret ID. The secret value is shown only when the secret is created.

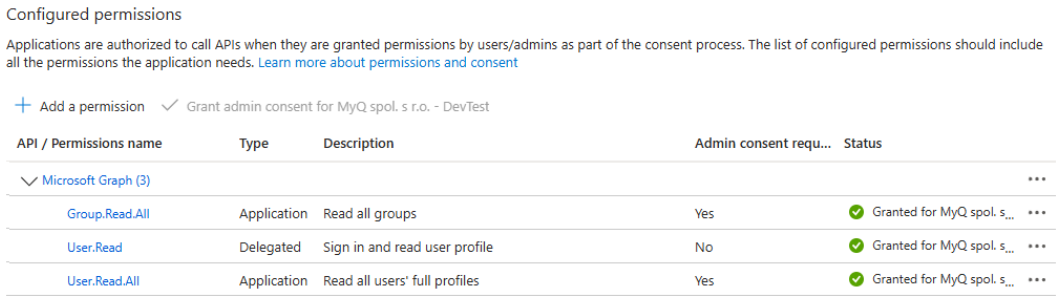
You enter the secret value in MyQ as the security key or client secret.

Add API permissions

Add only the permissions required by the MyQ integrations that will use this application.

1. Go to **Manage > API permissions**.
2. Select **Add a permission**.
3. Select **Microsoft Graph**.
4. Select the correct permission type for each permission, according to the table below:
   - **Delegated permissions**
   - **Application permissions**

5. Repeat these steps until all required permissions are added.
6. If administrator consent is required, select **Grant admin consent**.



6 Permissions granted

Permission	API	Type	Purpose
`Group.Read.All`	Microsoft Graph	Application	Read groups and group membership.
`User.Read.All`	Microsoft Graph	Application	Read users.
`User.Read`	Microsoft Graph	Delegated	Sign in and read the signed-in user's profile.

Next steps

Continue with the MyQ configuration for the integration that you want to use. Keep the following values available:

- Directory (tenant) ID
- Application (client) ID
- Client secret value

See also:

- (10.3) Connect to Microsoft Entra ID (Graph API)
- (10.3) Connect to OneDrive for Business
- (10.3) Connect to SharePoint Online
- (10.3) Synchronize Users from Microsoft Entra ID

2.15.6 Microsoft Entra Application Reference

This article summarizes the application registration models, authentication settings, redirect URIs, API permissions, and scopes used by MyQ integrations with Microsoft services.

Use this reference when:

- registering an application manually
- reviewing an automatically configured enterprise application
- planning whether integrations can share an application registration
- troubleshooting permissions, authentication, or consent

For the recommended automatic workflow, see Automatic App Registration (see page 33).

Registration Models

Some integrations can be configured automatically from MyQ. Other integrations require a manual application registration in Microsoft Entra ID.

For Microsoft Entra ID, OneDrive for Business, and SharePoint Online, manual setup can use one shared application registration or separate application registrations for each integration.

Do not use a shared application with Microsoft Exchange Online or Universal Print.

Integration	Setup	Registration model	Client Secret	Public client flow
Microsoft Entra ID / Microsoft Graph	Automatic or manual	Shared or dedicated	Yes	No
OneDrive for Business	Automatic or manual	Shared with Entra ID/ SharePoint, or dedicated	Yes	No
SharePoint Online	Automatic or manual	Shared with Entra ID/ OneDrive, or dedicated	Yes	No
Exchange Online	Manual	Dedicated	No	Yes
Universal Print	Manual	Dedicated	No	Yes

A manually registered application can be shared by Microsoft Entra ID, OneDrive for Business, and SharePoint Online, provided it contains all settings and permissions required by the enabled integrations.

Do not share this application registration with Exchange Online or Universal Print. These integrations require dedicated registrations with different authentication configurations.

Application Registration and Service Principal

A manually registered application is represented in two places in the Microsoft Entra admin center:

- **App registrations** contains the application definition, including its identifiers, authentication settings, credentials, redirect URIs, and requested API permissions.
- **Enterprise applications** contains the service principal representing the application in the customer's tenant. Access, consent, and tenant-specific permissions are managed here.

Automatic setup creates and configures the service principal used by MyQ.

Information Required by MyQ

For a manually configured integration, obtain the following information from the application's **Overview** page:

- **Application (client) ID**
- **Directory (tenant) ID**
- **Client secret**, when required

Redirect URIs

For Microsoft Entra ID, OneDrive for Business, and SharePoint Online, manual setup can use one shared application registration or separate application registrations for each integration.

Microsoft Exchange Online and Universal Print use different application configurations and should not use the shared manual registration procedure for Microsoft Entra ID, OneDrive for Business, and SharePoint Online.

Integration or feature	Setup method	Platform	Redirect URI
Microsoft Entra ID / Microsoft Graph	Manual	Web	`https://{hostname:port}/auth`
Microsoft Entra ID SSO helper	Manual	Single-page application	`https://helper.myq.cz/openid/`
MyQ Desktop Client Seamless SSO	Manual, when used	Mobile and desktop applications	`ms-appx-web://microsoft.aad.brokerplugin/{Application-client-ID}`
OneDrive for Business	Manual	Web	`https://helper.myq.cz/`
SharePoint Online	Manual	Web	`https://helper.myq.cz/`
Microsoft Exchange Online	Manual	Mobile and desktop applications	`https://login.microsoftonline.com/common/oauth2/nativeclient`
Universal Print	Manual	Mobile and desktop applications	Select the mobile and desktop redirect URI in Microsoft Entra ID.

Replace:

- `{hostname:port}` with the hostname and HTTPS port of the MyQ server.
- `{Application-client-ID}` with the Application client ID of the application registration.

Connecting to the Application from MyQ

If you use automatic registration, MyQ gets the client and tenant information silently.

If you configure any integration manually, get these details from your application registration Overview page:

- Application (client) ID
- Directory (tenant)
- Client secret (Entra ID, OneDrive for Business and SharePoint Online)

Permissions Used During Automatic Setup

The permissions used to create and configure the application are separate from the permissions that the resulting application uses at runtime.

Permission	API	Type	Purpose
`Application.ReadWrite.All`	Microsoft Graph	Delegated	Create or update the connector application credential.
`Directory.Read.All`	Microsoft Graph	Delegated	Read tenant information, including the default domain name.

Runtime Permissions

Microsoft Entra ID Permissions

Permission	API	Type	Purpose
`Group.Read.All`	Microsoft Graph	Application	Read groups and group membership.
`User.Read.All`	Microsoft Graph	Application	Read users.
`User.Read`	Microsoft Graph	Delegated	Sign in and read the signed-in user's profile.

OneDrive Permissions

Permission	API	Type	Purpose
`Files.ReadWrite`	Microsoft Graph	Delegated	Read and write files available to the signed-in user.
`User.Read`	Microsoft Graph	Delegated	Identify the signed-in user.
`Files.ReadWrite.All`	Microsoft Graph	Application	Access users' files without individual user authorization.

SharePoint Permissions

Permission	API	Type	Purpose
`User.Read`	Microsoft Graph	Delegated	Identify the signed-in user.
`Sites.ReadWrite.All`	Microsoft Graph	Delegated	Read and write SharePoint content available to the signed-in user.
`Sites.Read.All`	Microsoft Graph	Delegated	Read sites in the tenant.
`Sites.ReadWrite.All`	Microsoft Graph	Application	Read and write content without individual user authorization.

Microsoft Exchange Online Permissions

Permission	API	Type	Purpose
`User.Read`	Microsoft Graph	Delegated	Sign in and read the mailbox user's profile.

Permission	API	Type	Purpose
`IMAP.AccessAsUser.All`	Microsoft Graph	Delegated	Read, update, create, and delete email in the user's mailbox. This permission does not include sending mail.
`SMTP.Send`	Microsoft Graph	Delegated	Send email from the user's mailbox.

Microsoft Universal Print Permissions

Permission	API	Type	Purpose
`PrinterShare.ReadWrite.All`	Microsoft Graph	Delegated	Read and write printer shares.
`Printer.FullControl.All`	Microsoft Graph	Delegated	Register, read, update, and unregister printers.
`Printers.Create`	Universal Print	Delegated	Create and register printers.
`Printers.Read`	Universal Print	Application	Read printers without a signed-in user.
`PrinterProperties.ReadWrite`	Universal Print	Application	Read and write printer properties and attributes without a signed-in user.
`PrintJob.Read`	Universal Print	Application	Read print-job metadata and payload without a signed-in user.
`PrintJob.ReadWriteBasic`	Universal Print	Application	Read and write basic print-job metadata without a signed-in user.

Authentication Scopes

Entra ID / Microsoft Graph

Authentication scopes are used during OAuth or OpenID Connect authentication.

Integration	Scope	Scope ID	Purpose
Microsoft Entra ID / Microsoft Graph	`openid`	—	Sign in the user and request an ID token.
Microsoft Entra ID / Microsoft Graph	`email`	—	Request the user's email claim.
Microsoft Entra ID / Microsoft Graph	`profile`	—	Request basic profile claims.

Exchange Online

Integration	Scope	Scope ID	Purpose
Microsoft Exchange Online	`offline_access`	—	Allow MyQ to renew access without requiring the mailbox user to authenticate every time.

Universal Print

Integration	Scope	Scope ID	Purpose
Universal Print	`offline_access`	`7427e0e9-2fba-42fe-b0c0-848c9e6a8182`	Allow MyQ to use a refresh token to obtain new access tokens.

See also:

- Manual App Registrations (see page 35)
- (10.3) Configure Microsoft Entra ID Authentication
- (10.3) Synchronize Users from Microsoft Entra ID
- (10.3) Connect to Microsoft Entra ID (Graph API)

- (10.3) Connect to OneDrive for Business
- (10.3) Connect to SharePoint Online
- (10.3) Connect to Microsoft Exchange Online
- (10.3) Connect to Microsoft Universal Print

2.15.7 Customize your Registered MyQ App

After you register an application for MyQ, you can customize it.

Configure MyQ X branding for the application

Download the MyQ X logo to add it to the application branding.

7 Logo

1. On the application's **Properties & branding** page, adjust the following:
    a. **Name**: should be configured as **MyQ X** from the previous steps.
    b. **Upload new logo**: select the MyQ X logo downloaded earlier.
    c. **Home page URL**: provide the link the application will be pointing at when users click it in the My Apps portal, the options are:
        i. use the URL of the MyQ Web Interface of your Standalone or Site server (if this application will be used only by one site) or the Central Server.
        ii. use the MyQ's website: https://myq-solution.com[2].
        iii. fill in the URL of your Intranet site from which users can continue to MyQ X (optional).

2. https://myq-solution.com/

d. **Terms of service URL**: https://www.myq-solution.com/en/myq-legal-policies

e. **Privacy statement URL**: https://www.myq-solution.com/en/myq-legal-policies

2. Click **Save**.

MyQ X application visibility in the My Apps portal

Make the MyQ X application visible to users in My Apps

1. On the Azure Portal, type **Enterprise applications** in the search box, and open this section.
2. Find the application (i.e. **MyQ X**) you created previously in App registrations.
3. On the **Properties** page, configure the following:
   a. **Enabled for users to sign-in?**: No
   b. **Visible to users?**: Yes
4. Even here, you can configure the application's **Logo** (you can find it above in the Configure MyQ X branding for the application section of this article.
5. Click **Save**.

The application will be visible to your users in their My Apps portal. When they click it, they will be pointed to the URL defined in the **Homepage URL**.

Hide the MyQ X application from users

1. On Azure Portal, type **Enterprise applications** in the search box, and open this section.
2. Find the application you created previously in App registrations.
3. On the **Properties** page, configure the following:
   a. **Enabled for users to sign-in?**: No
   b. **Visible to users?**: No
4. Click **Save**.

The application will not be visible to your users in their My Apps portal.

2.16 Set up Microsoft Exchange Online

Configure Microsoft Exchange Online when you want MyQ to send email through Exchange Online using OAuth authentication.

After completing this procedure, continue with **Set up Exchange Online in MyQ**.

⚠ Important!

MyQ X sends email using SMTP with OAuth. SMTP AUTH must be enabled in Exchange Online for the tenant or mailbox used as the sender. If SMTP AUTH is disabled, MyQ cannot send email through Exchange Online.

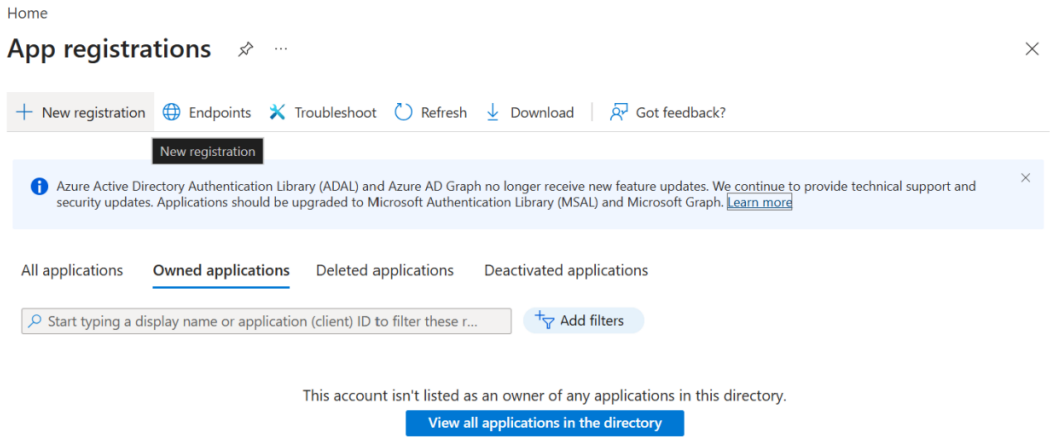
2.16.1 Prerequisites

- you can register applications in Microsoft Entra ID
- you can add Microsoft Graph API permissions
- SMTP AUTH is enabled for the Exchange Online tenant or sender mailbox
- you know which mailbox will be used as the sender address in MyQ

⚠ The mailbox user must complete Microsoft device-code authorization after the connection is added in MyQ.

2.16.2 Register the Application in Microsoft Entra ID

1. Sign in to the **Microsoft Entra admin center**.
2. Go to **Identity > Applications > App registrations**.
3. Select **New registration**.



4. In **Name**, enter a name for the application.

   Example: `MyQ X Connector`, `MyQ Universal Print`, `MyQ Sharepoint`

5. In **Supported account types**, select the account type required for your deployment.
6. Leave **Redirect URI** empty.

   You add the required redirect URIs later in this procedure.

7. Select **Register**.

The application is created.

In the Overview page of the application registration, copy and save the values:

- Application (client) ID
- Directory (tenant) ID

You enter these values when configuring the connection in MyQ.

2.16.3 Configure Authentication

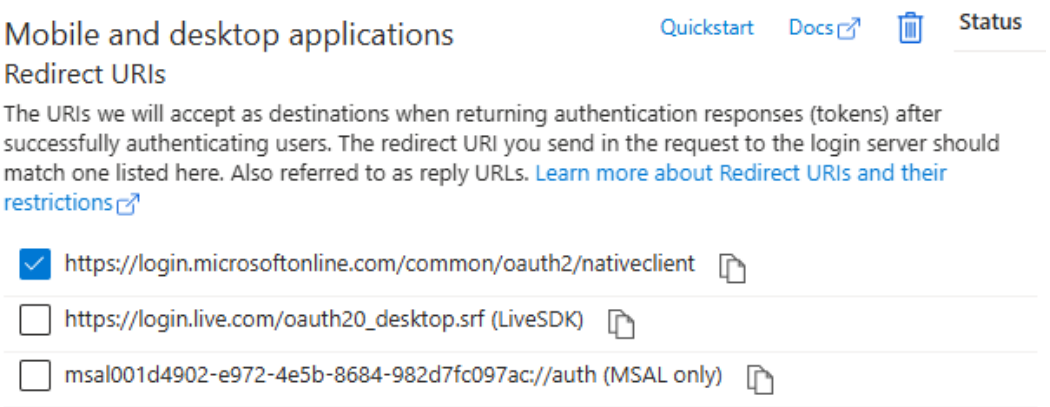
Configure the application as a public client.

No client secret is required.

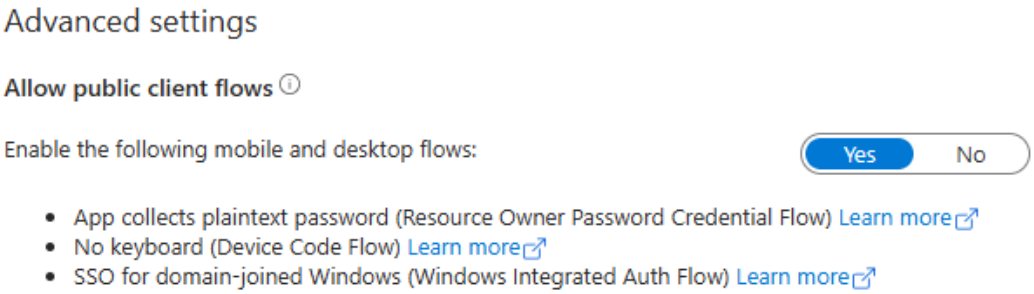
1. In the application registration, go to **Manage > Authentication**.
2. Select **Add a platform**.
3. Select **Mobile and desktop applications**.
4. Select the following redirect URI:

   ```
   https://login.microsoftonline.com/common/oauth2/nativeclient
   ```

5. Select **Configure**.



6. In **Advanced settings**, enable **Allow public client flows**.



7. Save the changes.

2.16.4 API Permissions

Add the permissions required by MyQ.

1. Go to **Manage > API permissions**.
2. Select **Add a permission**.
3. Select **Microsoft Graph**.
4. Add the permissions/scopes according to the tables below.

Permissions

Permission	API	Type	Purpose
`User.Read`	Microsoft Graph	Delegated	Sign in and read the mailbox user's profile.
`IMAP.AccessAsUser.All`	Microsoft Graph	Delegated	Read, update, create, and delete email in the user's mailbox. This permission does not include sending mail.
`SMTP.Send`	Microsoft Graph	Delegated	Send email from the user's mailbox.

Authentication Scope

Integration	Scope	Scope ID	Purpose
Microsoft Exchange Online	`offline_access`	—	Allow MyQ to renew access without requiring the mailbox user to authenticate every time.

Now you are ready to set up Exchange Online in MyQ. See (10.3) Connect to Microsoft Exchange Online

3 Users and Identity

User management in MyQ X involves three connected decisions that need to be made and implemented in order.

3.1 Decision 1. Job Detection Method

When a print job arrives at MyQ, the server needs to match it to a user. The attribute it uses to do this – the job sender name from the print driver, a PJL field, or the job filename – determines what value must exist in each user's MyQ account for jobs to authenticate successfully.

3.2 Decision 2. Map Synchronization Attributes

When users are imported from Active Directory, Entra ID, or another source, MyQ maps directory attributes to user properties. The username field – or the alias field – must be populated with the same value that job detection will look for. If job detection expects sAMAccountName but sync only populates UPN, jobs will not match.

3.3 Decision 3. Authentication Method

How users log in to terminals, the web interface, and client applications is a separate decision from how their print jobs are identified. However, it interacts with sync: ID card numbers, PINs, and aliases can all be imported from a directory source, and the choice of authentication method determines which of these need to be present and correctly mapped.

The practical consequence is that sync configuration should not be finalized until the job detection method is confirmed, and authentication configuration should be designed together with synchronization.

For step-by-step configuration of sync sources and authentication settings, see the MyQ X Server guide.

See also:

- (10.3) User Detection Methods
- (10.3) User Synchronization
- (10.3) User Authentication

3.4 Understanding Job Detection

When a print job arrives at MyQ, the server needs to match it to a user account. The value it uses for this match is extracted from the job itself, and must correspond to the username or an alias on the matching MyQ user account. Choosing the right detection method, and confirming that it works before configuring sync, helps prevent a common deployment problem: jobs arriving but not matching any user account.

3.4.1 Detection Methods

The main methods of identifying the user when a print job is received are:

- **Job sender:** MyQ reads the sender identity submitted with the print job. This is often the login name of the user on their workstation, typically `sAMAccountName` in Active Directory environments, though in some configurations it can be UPN. Use this method when the submitted job sender value matches the username or alias you synchronize into MyQ.
- **From PJL:** MyQ reads a field embedded in the print job by the driver, using a PJL command you define in the queue settings. Use this when the driver reliably embeds a consistent user identifier and you need more control over what value is extracted.
- **Job name:** MyQ reads the user identifier from the filename submitted with the job. This is used in specific application printing scenarios where the filename reliably encodes the sender.

Additional detection methods exist for edge cases. See the MyQ X Server guide for the full list.

3.4.2 How to Confirm Your Detection Method

It’s important to verify your detection method before you configure user synchronization. The easiest approach is to send a test job from a user account that does not yet exist in MyQ. MyQ will log the job as discarded with a message similar to this:

```
Job discarded. User "john.doe" not found.
```

The quoted value in this message is exactly what MyQ extracted and will try to match against. That is the value your synchronization job must place in the username or alias field.

In mixed-fleet environments with multiple driver types, test from each driver variant. Different drivers can embed different values in the same PJL field, and each combination may need its own queue configuration or alias mapping.

3.4.3 sAMAccountName, UPN, and Alias Strategy

For AD-synced users, MyQ always uses sAMAccountName as the username. There is no setting to change this. If your job detection returns UPN instead – common in environments where workstations are Entra-joined or where drivers are configured to use email-format identifiers – the match will fail unless UPN is also present as an alias on each user account.

The solution is to map `userPrincipalName` to the Alias field during LDAP synchronization. Once synced, MyQ will match jobs against both the username and all aliases, so UPN-identified jobs will authenticate correctly. The same approach can be used for other available and unique attributes, such as `mailNickname`, mail, or a custom attribute, if that is the identifier returned by job detection.

For Entra ID-synced users, UPN is always the username. If your print drivers send `sAMAccountName`-format identifiers, map `onPremisesSamAccountName` to the Alias field during Entra ID sync, where that attribute is available.

3.4.4 Mixed-Fleet Considerations

In environments with multiple print driver types – for example, a mix of Windows domain-joined workstations, macOS devices, and BYOD – it is common for different drivers to send different identifier formats. If different device or driver populations require different detection logic, use aliases to cover multiple identifier formats on each user account, or configure separate queues with the appropriate detection settings for each population.

Confirm the identifier sent by each driver type before finalizing the sync attribute mapping. Changing the detection method or alias configuration after users are already active in the system requires resyncing user accounts and may temporarily disrupt job authentication.

See also:
- (10.3) User Detection Methods

3.5 User Synchronization

User accounts in MyQ X can be created manually or imported from an external identity source. For most managed environments, synchronization is preferable because it keeps user data aligned with the organization's directory, supports group-based configuration, and reduces ongoing administration.

Plan synchronization together with job detection and user authentication. The username or alias imported into MyQ must match the identity detected in print jobs, while mapped cards, PINs, and other credentials must support the selected authentication methods.

Before configuring a synchronization source:

1. Confirm how MyQ identifies users in incoming print jobs.
2. Decide which users and groups should be imported.
3. Identify the attributes that will populate MyQ usernames, aliases, personal numbers, email addresses, credentials, and other properties.
4. Decide how users will authenticate to MyQ.
5. Determine which system will control user creation, updates, group membership, and deactivation.

See also:
- Understanding Job Detection (see page 54)
- (10.3) User Synchronization

3.5.1 Supported Synchronization Sources

MyQ X can import users from the following sources:

Source	Connection	Considerations
Active Directory Domain Services	LDAP or LDAPS	Standard method for on-premises Active Directory. Supports multiple domains. LDAPS is recommended.
Microsoft Entra ID	Microsoft Graph	Recommended for cloud-only and hybrid Entra environments. Does not require Microsoft Entra Domain Services.
Microsoft Entra Domain Services	LDAPS	Use only when LDAP access to Microsoft cloud identities is specifically required. Entra Domain Services is a separately licensed Microsoft service.
OpenLDAP	LDAP or LDAPS	Review server-side query and time limits before synchronizing large directories.
Google Workspace	Secure LDAP	Requires Secure LDAP to be enabled and MyQ to be configured as an LDAP client.
Novell	LDAP or LDAPS	Uses the standard LDAP synchronization workflow.
Lotus Domino	LDAP or LDAPS	Supported for legacy deployments only. It is not available for new deployments unless explicitly enabled.
CSV	File import	Suitable for one-time imports, scripted synchronization, or supplementing values unavailable from another source.

MyQ can communicate with up to five LDAP servers simultaneously. Consider this limit when planning multiple LDAP synchronization or authentication sources.

3.5.2 Active Directory

Active Directory synchronization uses LDAP or LDAPS.

MyQ uses `sAMAccountName` as the username for users synchronized from Active Directory. This mapping cannot be changed. The default mappings also include:

MyQ property	Active Directory attribute
Username	`sAMAccountName`
Full name	`cn`
Email	`mail`

Other properties, including aliases, personal numbers, notes, language, user storage, cards, and PINs, can be mapped where required.

If MyQ detects a user's print jobs by their user principal name rather than `sAMAccountName`, map `userPrincipalName` to the MyQ alias property. MyQ can then associate either identity with the same user account.

User Home Folders

If users have individual home folders, their storage path can be synchronized to the MyQ **User Storage** property. This allows supported terminal workflows to use the storage location associated with the signed-in user.

Map the appropriate Active Directory attribute containing the complete storage path. Confirm that the resulting path is reachable from the systems and accounts that will use it.

Transforming Attribute Values

Some organizations store several values in one directory attribute. For example, an attribute might contain both a card number and a personal number:

```
288373;736
```

MyQ can apply a regular expression transformation during synchronization to extract or reformat the required value.

See (10.3) Transform User Data with RegEx.

Sensitive Attributes

If cards, PINs, personal numbers, or other sensitive values are stored in Active Directory, review access to the source attributes before synchronizing them.

Standard Active Directory attributes may be readable by authenticated domain users. Where necessary, use appropriately protected attributes and grant read access only

to the directory account used by MyQ. Test directory schema or permission changes before applying them in production.

3.5.3 Microsoft Entra ID

MyQ supports two methods of synchronizing Microsoft Entra ID users:

- Microsoft Graph
- LDAPS through Microsoft Entra Domain Services

Use Microsoft Graph when users are managed in Entra ID and LDAP compatibility is not specifically required. This method supports cloud-only and hybrid identities without deploying Microsoft Entra Domain Services.

Use Entra Domain Services only when the deployment specifically requires LDAP access to Microsoft cloud identities. Entra Domain Services is a separate paid Microsoft service and must be configured for Secure LDAP before MyQ can connect to it.

Microsoft Graph Preparation

Before configuring Microsoft Graph synchronization, connect MyQ X to Microsoft Entra ID. The Entra application must have permission to read the required users, groups, and directory attributes.

See also:

- Microsoft Entra Apps and MyQ (see page 32)
- Manual App Registrations (see page 35)
- Microsoft Entra Application Reference (see page 41)

User Identity

For users synchronized through Microsoft Graph, MyQ uses the user principal name as the username. This cannot be changed.

In hybrid environments, additional on-premises attributes may also be available in Entra ID. If print jobs contain a `sAMAccountName`-style identity rather than the user's UPN, map `onPremisesSamAccountName` to the MyQ alias property.

The attributes available through Microsoft Graph depend on the user and the organization's identity configuration. Confirm that the required attributes are populated before relying on them for job detection or authentication.

Entra-Joined Devices

On Microsoft Entra-joined Windows devices, the identity submitted with a print job may not match the user's UPN.

MyQ can create a normalized alias from the user's Entra display name to help match these jobs. Consider using this option only when testing shows that jobs are identified by the normalized display name rather than by UPN.

Normalized aliases are limited to 20 characters. They may not uniquely identify users who have the same or similar display names. Test the resulting values before using them in production.

Synchronization and Authentication

Synchronization and authentication are separate functions.

Microsoft Entra ID can be used only as the source of user data while users authenticate through another method. Alternatively, the Entra connection can also be assigned as the authentication server for synchronized users.

When Entra ID is used for authentication, users authenticate with their Microsoft identities and are subject to the authentication policies configured for those accounts.

3.5.4 Other Sources

Google Workspace

Google Workspace synchronization uses Google's Secure LDAP service. Secure LDAP must be enabled in Google Admin, and MyQ must be configured as an LDAP client.

Each MyQ server instance requires the appropriate client certificate. Plan for certificate renewal and allow for possible delays while changes to LDAP client permissions propagate through Google Workspace.

OpenLDAP

OpenLDAP uses the standard LDAP synchronization source.

Default OpenLDAP limits may restrict a query to a maximum number of entries or impose a query time limit. Review these settings before synchronizing a large directory.

When OpenLDAP is also used for authentication, the full login identity required by the directory can be synchronized as an alias. If users require a shorter identity for terminal login, plan an additional alias mapping.

Novell and Lotus Domino

Novell uses the standard LDAP synchronization workflow.

Lotus Domino synchronization is intended for existing legacy deployments. It is not available for new deployments unless explicitly enabled.

CSV

CSV import can be used when:

- No supported directory connection is available.
- Users need to be imported once rather than synchronized regularly.
- An external system can generate a recurring import file.
- Additional values must be added to users synchronized from another source.

For example, a CSV import can supplement LDAP-synchronized accounts with aliases that are not available in the directory.

When combining CSV with another synchronization source, plan how existing users will be matched and which source will control each property. Incorrect matching can create duplicate accounts or update the wrong users.

3.5.5 Validate User Lifecycle Behavior

Synchronization can create and update users, change group membership, change default accounting groups, and deactivate accounts. Test these effects before treating an identity source as authoritative for MyQ users.

A user can disappear from synchronization results because:

- The account was deleted or disabled in the source.
- The user was moved outside the selected synchronization scope.
- A directory filter no longer matches the user.
- The synchronization account can no longer read the user or a required directory branch.
- A connection or directory query failed.
- The synchronization configuration was changed incorrectly.

A missing user in the synchronization result does not therefore always mean that the user has left the organization.

Synchronization-Source Ownership

When several sources are used, decide which source owns each user population and which source is allowed to update existing accounts.

Document:

- Which source creates each group of users.
- Which source controls usernames and aliases.
- Which source controls group membership.
- Which source controls cards, PINs, and other imported credentials.
- Which source is allowed to deactivate users.
- How users present in more than one source will be matched.

For complex environments, see Multi-domain and Multi-tenant Environments (see page 71).

Deactivating Missing Users

The **Deactivate missing users** option deactivates previously synchronized users who are no longer present in the source results.

Initially leave this option disabled. Enable it only after confirming that the Base DN, filters, permissions, connection, and imported population are correct.

Use particular caution when combining **Deactivate missing users** with **Ignore synchronization source**. With both options enabled, the synchronization can affect users created or imported by other sources when they are not present in the current synchronization result.

Use this combination only when the current source is intended to be authoritative for all affected users.

Username Changes

When a username changes in the source, MyQ must be able to associate the new identity with the existing account. Otherwise, synchronization can create a second user.

Where username changes are expected, map a stable and unique personal number and use it to pair users. Verify that the selected value:

- Is present for every synchronized user.
- Is unique across all sources.
- Does not change when the username changes.
- Is never reassigned to another person.

Test a representative username change before relying on this behavior in production.

3.5.6 Validate the Initial Synchronization

Test synchronization with a limited population before importing the complete production directory.

1. Use a test group, organizational unit, Base DN, or source filter.
2. Include representative users with the required attributes and group memberships.
3. Keep automatic deactivation of missing users disabled.
4. Run the synchronization manually.
5. Review the synchronization log and any reported conflicts.
6. Verify usernames, aliases, personal numbers, email addresses, cards, PINs, language, and user storage as applicable.
7. Verify imported groups, group memberships, and default accounting groups.
8. Send test jobs from representative client and driver environments.
9. Test user authentication if the identity source will also be used as an authentication server.
10. Test a username change, group-membership change, and removal from the synchronization scope.
11. Expand the synchronization scope only after the results are correct.

3.5.7 Schedule Synchronization

Directory synchronization is periodic rather than continuous. It can be run manually or scheduled using the MyQ task scheduler.

A daily synchronization is typical for most organizations. If user provisioning or deactivation must follow directory changes more quickly, choose a frequency that meets the organization’s operational and security requirements.

The **Delta synchronization** option enables you to run a lightweight Microsoft Entra ID (Graph API) synchronization periodically, to keep the user data up to date (default: every 10 minutes).

Before enabling a schedule:

- Complete the initial synchronization validation.
- Confirm which source controls user deactivation.
- Verify that the directory or application account will remain valid.
- Establish monitoring for failed or unexpected synchronization results.

- Consider the effect of directory maintenance or temporary connectivity failures.

See also:

- (10.3) User Synchronization
- Prepare for LDAP User Synchronization (see page 64)
- (10.3) Configure Microsoft Entra ID Authentication
- (10.3) Transform User Data with RegEx
- (10.3) Run and Schedule User Synchronization

3.5.8 Prepare for LDAP User Synchronization

Before configuring LDAP synchronization in MyQ X, determine which directory objects should be imported, which attributes and groups MyQ requires, and how the MyQ server will connect securely to the directory.

This preparation applies to:

- Active Directory Domain Services
- OpenLDAP
- Google Workspace Secure LDAP
- Novell
- Lotus Domino
- Microsoft Entra Domain Services using LDAPS

For help choosing between LDAP, Microsoft Graph, and other synchronization methods, see User Synchronization (see page 56).

Before You Start

Identify who will complete each part of the deployment. In smaller environments, one administrator may perform all the work. In larger organizations, coordination may be required between:

- The directory or identity administrator
- The network or security administrator
- The MyQ administrator

The directory administrator should provide the directory structure, required attributes, group information, and an account that MyQ can use to read them. The

network or security administrator may need to configure firewall access and certificate trust. The MyQ administrator uses this information to configure the authentication server and synchronization source.

Plan the Synchronization Scope

Determine which directory users MyQ should import.

Identify:

- The domains and organizational units containing the required users
- The Base DN or Base DNs from which MyQ should search
- Any users, contacts, service accounts, shared accounts, or disabled accounts that should be excluded
- The LDAP filter required to select the intended population
- Whether groups are stored within the same directory branch as users

A Base DN defines the starting point from which MyQ searches the directory. For example:

```
OU=Prague,DC=example,DC=com
```

This limits the search to the `Prague` organizational unit and its descendants.

An LDAP filter can restrict the results further. For example:

```
(&(objectCategory=person)(objectClass=user)(department=Sales))
```

The available attributes and correct filter syntax depend on the directory service. Test the intended Base DNs and filters against the directory before using them for production synchronization.

A user can appear to be missing when they are moved outside the selected Base DN or no longer match the filter. Consider this when planning user deactivation.

Plan Attribute Mapping

Identify which directory attributes will provide the MyQ user properties required by the deployment.

These can include:

MyQ property	Planning consideration
Username	Must support the identity strategy described in **Understanding Job Detection**.
Full name	Select an attribute containing a suitable display name.
Email	Required for features that send email to users.
Alias	Can store additional identities detected in print jobs or used during login.
Personal number	Must be unique and persistent if it is used to pair users.
Card	Can import one or several card identifiers.
PIN	Can import one or several PIN values.
Language	The source values must correspond to language codes supported by MyQ.
User storage	Must contain a complete storage path usable by the required scan workflows.
Notes	Can store additional directory information where required.

Confirm that the selected attributes:

- Exist in the directory schema.
- Are populated consistently for users in scope.
- Contain values in the format expected by MyQ.
- Are readable by the account used for synchronization.
- Are unique where MyQ relies on them to identify or pair users.

If a source attribute contains several values that must be separated or reformatted, MyQ can apply a regular expression transformation during synchronization.

Sensitive Attributes

Take particular care when synchronizing card numbers, PINs, personal numbers, or other sensitive values. Review who can read the source attributes in the directory. If necessary, store sensitive values in protected attributes and grant access only to the account used by MyQ.

Decide whether the directory or MyQ will be authoritative for cards and PINs. This determines whether synchronization should replace existing MyQ values, update them only when the directory value is populated, or add new values without removing existing ones.

Plan Group Synchronization

Synchronized groups can be used in MyQ for:

- Access control
- User policies
- Quotas and credit
- Projects and cost centers
- Reporting and accounting

Determine which directory groups MyQ requires and how they should be represented. MyQ can derive groups:

- From an attribute stored on each user object
- From one organizational unit in the user's distinguished name
- From an organizational-unit tree in the user's distinguished name
- From the user's `memberOf` attribute

Groups Derived from a Distinguished Name

Consider this user DN:

```
CN=Anna Novak,OU=Sales,OU=Prague,DC=example,DC=com
```

MyQ could derive only the `Sales` group or reproduce the hierarchy:

```
Prague > Sales
```

Before configuring this method, identify:

- Which DN component represents the user
- Which components represent organizational units
- Which domain components must be excluded
- Whether a single organizational unit or the complete hierarchy is required
- Which imported group should become the user's default accounting group

Groups Derived from `memberOf`

When importing groups from `memberOf`, identify a Groups Base DN that contains only the relevant groups. Without an appropriate scope, MyQ may import directory groups that have no purpose in the printing environment.

Determine whether MyQ should:

- Import only groups referenced by synchronized users
- Include empty groups
- Preserve the directory group hierarchy
- Import groups as a flat structure

Default Accounting Group

A user can belong to several groups, but only one group can be their default accounting group.

Decide:

- How the default group will be selected
- Whether synchronization may replace an existing default group
- What should happen when the user loses membership in their current default group

For guidance on using synchronized groups, see Group-Based User Management (see page 86).

Prepare a Directory Account

Create or select an account that MyQ can use to query the directory. A dedicated service account is recommended so that synchronization does not depend on an administrator's personal account.

The account requires read access to:

- Every directory branch included in the synchronization scope
- Every user attribute mapped to a MyQ property
- Group objects and membership attributes used for group synchronization

The account does not require permission to modify directory objects.

Apply the principle of least privilege and establish a process for managing the account throughout the deployment. Consider:

- Password expiration and rotation
- Account lockout
- Monitoring failed login attempts
- Ownership of the service account

- Updating MyQ when its credentials change

Use a username format accepted by the directory server. If the account belongs to a subdomain, a domain-qualified username may be required. For example:

```
Administrator@cz.example.local
```

Prepare Network Connectivity

The MyQ server must be able to connect to every LDAP server required by the deployment.

Confirm:

- DNS resolution from the MyQ server
- Firewall access between the MyQ server and the LDAP servers
- The hostname and port of each LDAP server
- Connectivity to servers required for directory availability or failover
- Any routing or firewall requirements between cloud-hosted MyQ servers and on-premises directories

LDAPS commonly uses TCP port `636`. LDAP commonly uses TCP port `389`, although a directory can use a different configured port.

LDAPS is recommended because it protects directory credentials and data in transit. Use unencrypted LDAP only when it is intentionally permitted by the organization's security policy.

For broader firewall and network planning, see

- Network Architecture (see page 19)
- Infrastructure and Capacity (see page 22)

Prepare Certificate Trust for LDAPS

For LDAPS, the certificate presented by the directory server must be trusted by the MyQ server.

Confirm that:

- The certificate is valid and has not expired.
- The certificate is suitable for server authentication.
- Its subject or subject alternative name matches the DNS hostname used by MyQ.
- The complete issuing CA chain is trusted by the MyQ server.
- Required certificate revocation services are reachable.
- The certificate-renewal process is understood.

Import the required root and intermediate CA certificates into the appropriate Windows certificate stores on the MyQ server.

Use the directory server's DNS hostname rather than its IP address when the certificate identifies the server by name. A hostname mismatch can prevent a secure connection even when the issuing CA is trusted.

Test the LDAPS connection from the MyQ server before configuring user synchronization.

For general certificate guidance, see Security and Certificates (see page 26).

Validate the Directory Preparation

Before continuing to MyQ configuration, confirm that:

- The synchronization scope contains the intended users.
- The Base DNs and LDAP filters return the expected results.
- Required user attributes are populated.
- Required attributes contain values in the expected format.
- Personal numbers and other identifiers that must be unique do not contain duplicates.
- Required groups and group relationships can be read.
- The intended default accounting-group strategy is defined.
- The directory account has the necessary read access.
- DNS resolution and network connectivity work from the MyQ server.
- The LDAP or LDAPS connection succeeds.
- The complete certificate chain is trusted when using LDAPS.
- Certificate and service-account renewal responsibilities are documented.

Continue in MyQ X Server

After preparing the directory, service account, network connection, and certificate trust:

1. Add the LDAP server under **MyQ > Settings > Authentication Servers**.
2. Create an LDAP synchronization source under **MyQ > Settings > User Synchronization**.
3. Configure the Base DNs, attribute mappings, options, filters, transformations, and group import.
4. Run the synchronization with a limited test population.
5. Review the results before expanding the synchronization scope.

For detailed configuration, see also:

- (10.3) Authentication Servers Settings
- (10.3) Synchronize Users from LDAP
- (10.3) Transform User Data with RegEx
- (10.3) Run and Schedule User Synchronization

3.6 Multi-domain and Multi-tenant Environments

A single MyQ X installation can manage users from multiple Active Directory domains, multiple Microsoft Entra ID tenants, or a combination of identity sources.

These environments are common in mergers, shared-service deployments, staged migrations, and organizations where separate identity systems share the same MyQ infrastructure.

The main deployment challenge is making sure that users remain uniquely identifiable across all sources, both when they are synchronized into MyQ and when MyQ identifies them from print jobs or authentication requests.

3.6.1 Choose Your Environment

Environment	Main consideration
Multiple Active Directory domains	The same `sAMAccountName` can exist in different domains. MyQ must preserve the domain when synchronizing users and identifying jobs.
Multiple Microsoft Entra ID tenants	Each tenant requires its own Entra connection and, where required, its own synchronization source and authentication server.
Active Directory and Entra ID together	Plan how usernames and aliases from the different sources map to MyQ users and to identities detected in print jobs.

3.6.2 Plan Unique User Identities

Before synchronizing users from multiple identity sources, determine which value MyQ will use as the username and which alternative identities should be stored as aliases.

Do not assume that usernames are unique across domains or tenants. A username that is unique within one source can conflict with a user imported from another source.

3.6.3 Plan Job Identification

Users must also be identifiable from incoming print jobs.

The identity included with a job can vary depending on the client environment, print driver, and authentication method. Before rollout, test representative jobs from each domain, tenant, and client type and confirm that the detected identity matches the corresponding MyQ username or alias.

See also Understanding Job Detection (see page 54).

3.6.4 Plan Authentication

If users from multiple domains or tenants authenticate against their source identity system, configure the corresponding authentication servers and make sure each MyQ user is assigned to the correct one.

In Microsoft Entra multi-tenant environments, users can be presented with multiple Microsoft sign-in options. In Active Directory multi-domain environments, authentication must resolve the user against the correct domain.

See also:

- Multiple Microsoft Entra ID Tenants (see page 72)
- Local Multi-domain Environments (Active Directory) (see page 76)
- Transition from Active Directory to Entra ID (see page 80)

3.6.5 Multiple Microsoft Entra ID Tenants

A single MyQ X environment can synchronize and authenticate users from multiple Microsoft Entra ID tenants.

This is useful in shared-service environments, mergers, subsidiaries with separate Microsoft tenants, or other deployments where users from several organizations share the same MyQ infrastructure.

Treat each Microsoft Entra tenant as a separate identity source in MyQ.

Plan the Tenant Configuration

For each tenant, create the MyQ components required by the services you use:

MyQ component	When required
Microsoft Entra ID connection	Always
User synchronization source	When users are synchronized from the tenant
Microsoft Entra ID authentication server	When users authenticate against the tenant

Give each connection, synchronization source, and authentication server a clear and unique name that identifies its tenant. For example:

- `Entra - Contoso`
- `Entra - Acme`

The authentication-server name is particularly important when users must choose between multiple Microsoft sign-in options.

Connect Each Tenant

Create a separate Microsoft Entra ID connection for each tenant.

Application registration and authorization can be managed automatically by MyQ or manually according to your organization's Microsoft Entra administration model.

Synchronize Users from Multiple Tenants

Create a separate Microsoft Entra ID synchronization source for each tenant that supplies users to MyQ. Each source can have its own:

- user scope
- group selection
- attribute mappings
- lifecycle settings
- authentication-server assignment

Microsoft Entra synchronization uses UPN-based usernames, which normally reduces the risk of username collisions because the tenant or domain suffix forms part of the identity. Still, review aliases and other identifiers when different tenants contain users with similar names or identities.

Authenticate Users from Multiple Tenants

Create a separate Microsoft Entra ID authentication server for each tenant whose users authenticate through Entra ID.

When **Sign in with Microsoft** is enabled for multiple authentication servers, users are presented with the available Microsoft tenant sign-in options.

Use descriptive authentication-server names so users can identify which organization they should use when signing in.

Central-Site Environments

In Central-Site deployments, configure Microsoft Entra authentication servers on the Central Server. The authentication servers are automatically distributed to connected Site Servers.

All Entra authentication servers configured on the Central Server are available on every Site Server. When **Sign in with Microsoft** is enabled, all corresponding tenant sign-in options are presented to users.

It is not currently possible to make a Microsoft Entra authentication server available only on selected Site Servers. Consider this limitation when planning shared environments containing many tenants or Sites.

Test the User Experience

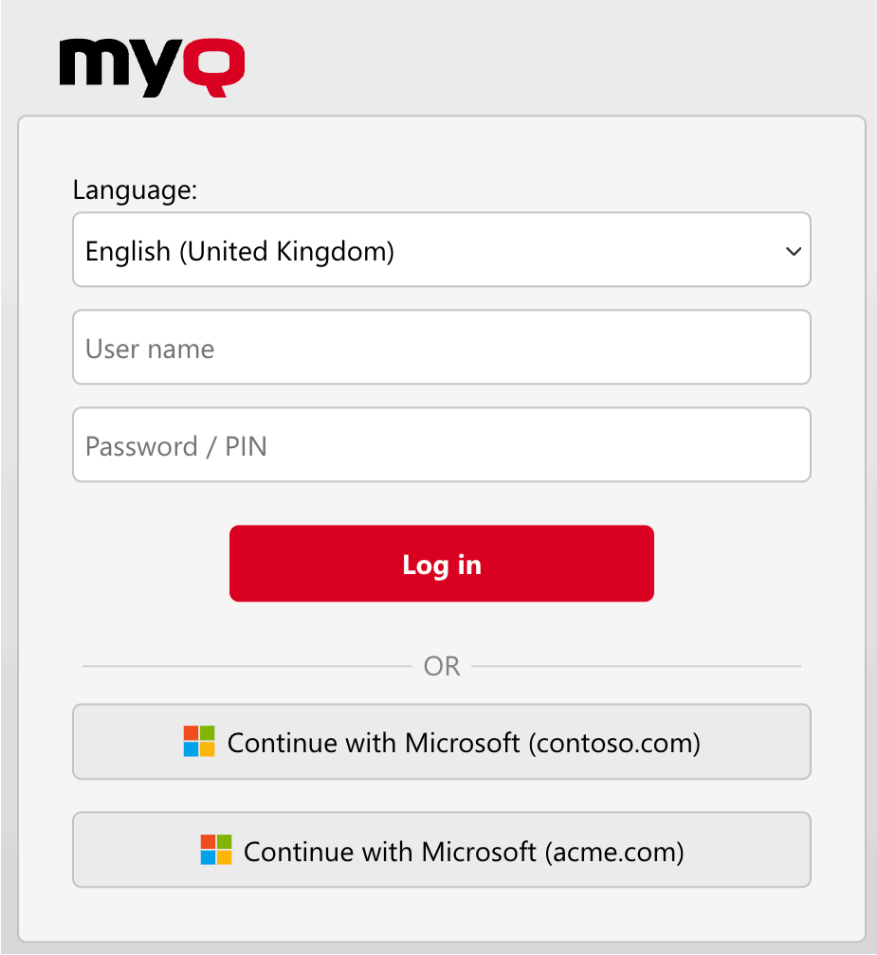
Before rollout, test:

- synchronization from each tenant
- authentication for users from each tenant
- the tenant choices presented during **Sign in with Microsoft**
- username and alias uniqueness
- job ownership for representative users and client devices

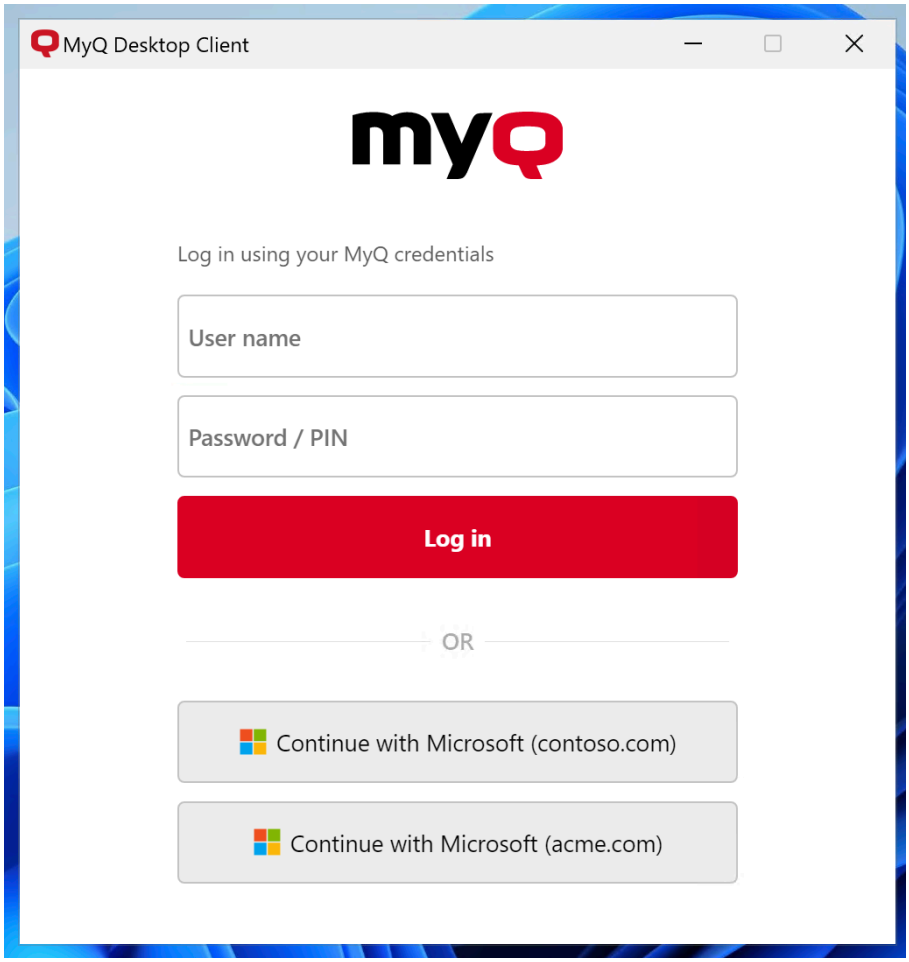
For deployments using Entra ID joined devices, also verify that the identity submitted with print jobs matches the username or alias stored for the synchronized user.

User Experience Preview

Users logging in to the Web UI see the following screen:



The login experience in the MyQ Desktop Client is similar.



See also:

- Manual App Registrations (see page 35)
- Microsoft Entra Application Reference (see page 41)
- (10.3) Connect to Microsoft Entra ID (Graph API)
- User Synchronization (see page 56)
- (10.3) Configure Microsoft Entra ID Authentication
- Understanding Job Detection (see page 54)

3.6.6 Local Multi-domain Environments (Active Directory)

A MyQ X installation can synchronize and authenticate users from multiple Active Directory domains.

Because the same `sAMAccountName` can exist in different domains, users must be represented in MyQ with identities that remain unique across all synchronized

domains. MyQ must also be able to determine the correct domain when assigning incoming print jobs.

Synchronize Users from Multiple Domains

Create a separate LDAP synchronization source for each Active Directory domain that supplies users to MyQ. For the synchronization procedure, see the Active Directory synchronization documentation in **MyQ X Server**.

Keep Usernames Unique

When synchronizing users from multiple domains, enable **Append the domain name to the username** for each relevant LDAP synchronization source.

Instead of:

`john.doe`

MyQ stores a domain-qualified username such as:

`john.doe@atlanta.example.com`

The appended domain is taken from the authentication server associated with the synchronization source.

For example, if two domains both contain a user with the `sAMAccountName` `john.doe`, MyQ can distinguish them as:

- `john.doe@atlanta.example.com`
- `john.doe@phoenix.example.com`

This prevents users with identical usernames in different domains from being treated as the same MyQ user.

Match Print Jobs to the Correct Domain

After domain-qualified usernames are created, incoming jobs must contain enough information for MyQ to identify both the user and their domain.

The identity information available in a print job depends on the print driver. Test the same driver vendor, model, and version that will be deployed to users.

To inspect the job:

1. Send a test job to MyQ from a computer in the relevant domain.
2. On the Print Server, open the job storage folder. The default location is:

   `C:\ProgramData\MyQ\Jobs`

If a different job folder is configured in MyQ Easy Config, use that location instead.

3. Find the corresponding `.prn` file.
4. Open the file and check whether the user's domain is present in the print data.

If the domain is available, configure MyQ to extract it so that the resulting identity matches the domain-qualified MyQ username.

See also Understanding Job Detection (see page 54).

Configure Multi-Domain Job Detection

To let MyQ distinguish users with the same username in different domains:

1. Make sure **Append the domain name to the username** is enabled for each relevant LDAP synchronization source.
2. In `C:\ProgramData\MyQ\config.ini`, add:

```
[ExtraFeatures]
multipleDomains=1
```

3. Save the file and restart the MyQ services using Easy Config.

Then configure how MyQ detects the domain in incoming print jobs.

Use the Default PJL Domain Information

Some print drivers include the Windows domain in the PJL header.

For example:

`@PJL COMMENT="USERDOMAIN:CustomerDomain.com"`

If the driver provides the domain in this format, MyQ can use it together with the detected username to assign the job to the corresponding domain-qualified user.

Configure Custom PJL Detection

If the print driver does not populate:

`@PJL COMMENT="USERDOMAIN:CustomerDomain.com"`

but includes the domain elsewhere in the PJL header, configure the queue to extract it from the available field.

1. Go to **MyQ > Queues** and open the queue used by these users.
2. In the **Job Receiving** settings, configure **PJL Detection** to identify the domain from the appropriate PJL command.

3. Specify the regular expression used to extract the domain value.
4. If necessary, configure PJL Detection for the username or other job properties in the same way.

Test the configuration with each print-driver family used in the deployment. Different drivers can use different PJL fields or formats.

Verify Job Ownership

After configuring multi-domain detection, test a user from each domain.

Where possible, include users with the same `sAMAccountName` in different domains. Confirm that:

- each user exists in MyQ with the expected domain-qualified username,
- the incoming job contains the expected domain,
- MyQ assigns the job to the correct user,
- a user with the same username in another domain cannot access the job.

Repeat the test for each print-driver family used in the deployment.

Authentication

Configure the appropriate Active Directory authentication server for users from each domain.

The authentication domain and the identity stored for the user in MyQ should be consistent with the domain-qualified username created during synchronization.

For authentication planning, see:

Legacy User Detection Script

For MyQ X 10.1 and earlier, multi-domain job detection can be implemented using a custom PHP user-detection script. This method is legacy. For current MyQ X versions, use the multi-domain and PJL Detection configuration described above.

For the legacy configuration procedure and downloadable script, see (v1) Local Multi-domain Environments (Active Directory).

See also:

- Multi-domain and Multi-tenant Environments (see page 71)
- Understanding Job Detection (see page 54)

- Integrated Windows Authentication (see page 110)
- User Synchronization (see page 56)

3.6.7 Transition from Active Directory to Entra ID

If your organization is moving identity management from on-premises Active Directory to Microsoft Entra ID, the sync transition in MyQ requires careful preparation. The core challenge is that AD-synced and Entra ID-synced users are identified by different attributes – sAMAccountName for AD, UPN for Entra ID – and these values are rarely identical. Without preparation, running an Entra ID sync against an existing AD-synced user population will create duplicate accounts rather than updating existing ones.

This article covers how to prevent that, and how to choose the right approach for your environment.

Why This Requires Preparation

MyQ uses sAMAccountName as the username for AD-synced users – for example, `tim.canterbury`. It uses userPrincipalName (UPN) as the username for Entra ID-synced users – for example, `tim.canterbury@acme.com`. These are two different values. By default, MyQ matches synchronized users by username and synchronization source. Because AD and Entra ID normally produce different usernames, an Entra ID sync cannot automatically match existing AD-synchronized users without additional preparation.

When you run an Entra ID sync against users already in MyQ with AD-sourced usernames, MyQ cannot match them – the usernames differ – and creates new accounts instead. The result is duplicate users, with the new accounts having no history: no credits, no quotas, no pending jobs.

The three options below each solve this by ensuring the identities can be matched before the Entra ID sync runs.

Understanding Synchronization Sources

Before choosing an option, it's important to understand how MyQ uses synchronization source names to match and update users.

Each synchronization source has a name. By default, MyQ will only update users that were imported by a source with the same name. If your AD source is named "AD" and your new Entra ID source is named "Entra ID", the Entra ID sync will not update the AD users – it will create new ones.

Two settings control this behavior:

Synchronization source name: acts as a marker identifying which users belong to which source. To allow an Entra ID source to update users previously imported by an AD source, either give both sources the same name, or use the option below.

Ignore synchronization source: when enabled, the sync source considers all users in MyQ, regardless of which source imported them. This allows any source to update any user when usernames match.

Determine Your Environment

Situation	Best fit
You want a method that works regardless of how AD usernames relate to Entra UPNs	**Option 1: CSV normalization**
Appending the configured domain to `sAMAccountName` produces the exact Entra UPN	**Option 2: Append domain**
AD and Entra share a unique, stable identifier for every user	**Option 3: Personal number matching**

Option 1 – Normalize Users With CSV and Update From Entra ID

This option works in all environments. It involves exporting existing users, rewriting their usernames to UPN format in a CSV file, re-importing to update them, and then running the Entra ID sync.

Prerequisites

Users must have personal numbers in MyQ before you start – these are used to pair the CSV import with existing accounts, since usernames will change. If users don't have personal numbers yet, either synchronize them from AD (via the Personal number mapping in the LDAP sync source) or add them manually. To add them manually: export users from the Users page (Tools – Export), add a unique value to the CODE column for each user, and re-import.

Steps

1. On the Users page, select Tools – Export and download the CSV.
2. In the CSV, rewrite all usernames to the UPN format used by Entra ID. For example, `timcanterbury` → `tim.canterbury@acme.com`. Leave personal numbers unchanged.
3. In Settings – User Synchronization, add the modified CSV as a new synchronization source.
    - Set the synchronization source name to match your existing AD source name, or enable Ignore synchronization source.
    - Enable Pair by the personal number.
4. Run the synchronization. Usernames in MyQ will now match UPNs in Entra ID.
5. Create the Entra ID synchronization source, setting its name to match the AD source or enabling Ignore synchronization source.
6. Run the Entra ID synchronization. Existing users will be updated, not duplicated.

Successful matches are logged as `Match via LOGIN`.

Option 2 – Append Domain to Usernames and Update From Entra ID

This option is available only when appending the configured domain to the AD `sAMAccountName` produces exactly the same value as the user's Entra ID UPN.

For example:
`tim.canterbury` → `tim.canterbury@acme.com`

Steps

1. In the AD synchronization source settings, enable Append domain to username and run the synchronization. Usernames will change from `tim.canterbury` to `tim.canterbury@acme.com`.
2. Create the Entra ID synchronization source, setting its name to match the AD source or enabling Ignore synchronization source.
3. Run the Entra ID synchronization. Users will be matched by the now-identical usernames and updated.
4. Once confirmed, remove the AD synchronization source and continue syncing from Entra ID only.

Option 3 – Match Users via Personal Number

This option uses the Personal number field as a shared identifier between AD and Entra ID, bypassing the username mismatch entirely.

Two common scenarios apply:

- Users in AD already have a personal number attribute (such as `employeeId`) that is also present in Entra ID.
- No personal number exists, but another **unique and stable** attribute that has the same value in both directories, such as an employee ID, email address, or UPN, can be mapped temporarily to Personal number for the transition.

Steps

1. In the AD synchronization source, map the chosen attribute to the Personal number field on the Users tab. If using `userPrincipalName`, this syncs the user's UPN from AD into MyQ's personal number field.
2. Run the AD synchronization to populate personal numbers.
3. Check a sample of users to confirm the Personal number field is populated correctly before proceeding.
4. Create the Entra ID synchronization source. Enable Pair by the personal number and map the same attribute to the Personal number field. Set the synchronization source name to match the AD source or enable Ignore synchronization source.
5. Run the Entra ID synchronization. Users will be matched via personal number and updated.

Note that the Personal number attribute in Entra ID does not need to be one of the listed options in the dropdown – you can type any attribute name manually and it will be used.

After the Transition

Once users are successfully updated from Entra ID, remove or disable the AD synchronization source to prevent it from overwriting Entra ID-managed users on subsequent runs. Monitor the User Synchronization log after the first few scheduled runs to confirm users are being updated as expected rather than duplicated.

See also:

- (10.3) Connect to Microsoft Entra ID (Graph API)

- (10.3) Synchronize Users from LDAP
- (10.3) Run and Schedule User Synchronization

3.7 User Self-Registration

Most deployments use directory synchronization for managed users. Self-registration is useful for users who are not already covered by the directory, such as guests, contractors, temporary staff, or BYOD users.

Plan the registration method, group assignment, and credential delivery before enabling user self-registration.

The following methods are available and can be enabled in combination:

- Web Interface registration
- Register by sending a job via LPR/IPPS/RAW
- Register by sending a job via email
- Register by Swiping an Unknown ID Card

3.7.1 Web Interface Registration

Users click **New Account** on the MyQ login screen, enter their name and email address, and receive account details by email. They must know the MyQ Web Interface URL before they can use this method.

This method works well where the Web Interface URL can be distributed to users before they need to print, for example during student, guest, or contractor onboarding.

3.7.2 Register by Sending a Job via LPR/IPPS/RAW

An unregistered user sends a print job and MyQ creates an account using the detected job sender name. No email address is captured, so MyQ cannot send account details automatically. In practice, an administrator usually needs to locate the new account and provide the credentials manually.

This method is occasionally useful in tightly controlled environments where an IT technician is present during onboarding and can hand off credentials in person. As a self-service method it falls short – users end up waiting for someone to find their new account and tell them their PIN, which defeats the purpose. It is not recommended as a primary registration path.

3.7.3 Register by Sending a Job via Email

If Jobs via Email is configured, a user who sends a job from an unrecognized email address is registered under that address and receives their account details automatically.

This method works best where Jobs via Email is already part of the normal print workflow and users know the print email address. If email printing is not familiar to users, this method may be overlooked or misunderstood.

Before enabling this method, check the group assigned to self-registered users and confirm that it has the rights needed for the expected email-printing workflow.

3.7.4 Register by Swiping an Unknown ID Card

When an unrecognized card is swiped, MyQ creates an account named `anonymX` and logs the user in automatically. The user can then edit their account details at the terminal if "Enable user profile editing" is active.

> This method works best where users already receive physical ID cards and can be instructed to complete their profile at the terminal after the first swipe. Because no automatic email is sent, users should be told what happens when they register with an unknown card.

New accounts created through self-registration can be added automatically to a selected group. Before enabling self-registration, decide which group these users should join and what access, quotas, terminal actions, and printing options that group should provide.

Self-registration introduces accounts that may be incomplete, duplicated, or created by accident. In environments where it is actively used, plan a periodic review of the Users tab to identify accounts with missing information or multiple registrations for the same person. The patterns you see will inform whether the enabled methods are working as intended or need adjustment.

See also

- (10.3) Users
- (10.3) Users Settings
- (10.3) Automatic User Registration

- (10.3) User Authentication

3.8 Group-Based User Management

In most organizations, users already exist in groups – by department, role, location, or access level. MyQ is designed to reflect and extend that structure rather than replace it. Getting group design right before rollout reduces per-user administration. When groups are synchronized and mapped to MyQ configuration, new users can receive the appropriate rights, queues, terminal actions, policies, and accounting rules through group membership.

Plan group-based rules before synchronizing users. If rights, queues, terminal actions, policies, quotas, and accounting rules are already assigned to groups, newly imported users can receive the correct configuration through their group membership instead of being configured one by one.

⚠ Changing group assignments after users are active can affect access, accounting, and reporting. For example, applying accounting rules after users have already started printing may leave earlier activity categorized differently than intended.

3.8.1 What Groups Control

Groups are a key unit of configuration across several areas of MyQ:

- **User Rights**
  Access levels – who can view logs, manage printers, run reports, administer queues – are assigned to groups, not just individuals. Decide which administrative roles exist in your organization and map them to groups before configuring rights.
- **Queue Access and Driver Provisioning**
  Access to specific print queues can be restricted by group. When MyQ Desktop Client printer provisioning is configured, queues can be assigned per user or group, reducing manual workstation configuration.
- **Terminal Actions**
  Terminal actions, such as Easy Scan, Easy Copy, access to device-native applications, and ID card registration, can be scoped to specific user groups. Plan these assignments together with your group structure so users see only the actions intended for their role.

- **Policies**
  Print option restrictions – duplex enforcement, color restrictions, page limits – are applied via policies assigned to groups. Define policies at the group level where possible, and verify the effective policy behavior where multiple policies or overlapping groups apply.
- **Accounting**
  Groups are the foundation of quota and cost management. See Accounting Groups and Cost Centers below.

3.8.2 Accounting Groups and Cost Centers

Tying accounting to group membership can reduce manual quota assignment. When group synchronization and quota rules are configured correctly, newly synchronized users can receive the appropriate group-based accounting rules as part of the sync process.

Accounting Groups

Accounting groups assign a shared quota to a set of users. All members draw from the same balance, which resets on a defined schedule. This model suits departments or organizational units with a collective print budget. Individual quota rules can still be applied on top of group quotas where exceptions are needed.

Cost Centers

Cost centers allow individual users to allocate activity across multiple budget lines. A user with access to several cost centers chooses which one to charge at the point of printing or scanning. This model suits organizations where individuals work across projects or departments and need to attribute usage accordingly.

3.8.3 Designing Your Group Structure

The most practical starting point is your existing directory structure. If your AD or Entra ID groups already reflect meaningful organizational divisions, synchronize them directly into MyQ and build your configuration on top of them.

Where the directory structure does not map cleanly to your MyQ requirements, you can create internal MyQ groups that are not present in the directory and populate them by combining multiple sync sources or using attribute filters during sync.

A useful pattern is to run AD or Entra ID sync first, export the result to CSV, modify group memberships programmatically – for example via PowerShell – and then run a

second CSV sync source to apply the adjustments. Scheduling the CSV sync to run after the directory sync finishes keeps it current automatically.

When configuring group synchronization, pay attention to the synchronization level. Full synchronization mirrors the directory exactly – users are added to and removed from groups as their directory membership changes. Add new only adds memberships and never removes them, which means a user who leaves a department in the directory retains their MyQ group membership until manually corrected – with accounting implications if quotas are group-based. Choose the level that matches how you want MyQ to respond to directory changes.

Example: A School Deployment

Consider a school where the print system administrator needs to manage two distinct user populations – teachers and students – each with different print entitlements and different terminal experiences.

The school's user directory organizes staff into departmental groups by grade and subject. Rather than syncing that granularity into MyQ, the administrator creates a single internal **Teachers** group and configures the LDAP sync sources to funnel all relevant AD groups into it. Students sync into a separate **Students** group.

With that structure in place, the administrator configures the following once:

- A shared monthly quota attached to the Teachers group, and a separate, more restrictive quota for the Students group.
- An Easy Scan action pointing to a SharePoint site where teachers distribute study materials, visible only to the Teachers group.
- An Easy Copy action preconfigured for 50 copies – adjustable at the terminal – also restricted to the Teachers group.

Students using the same devices see neither action.

When a new teacher joins mid-year, the administrator adds them to the relevant AD group. On the next sync, they appear in MyQ with the correct quota, the correct terminal actions, and access to the correct queues – without any further configuration. When a teacher leaves, removing them from AD revokes their MyQ access on the next sync.

See also:

- Granting User Rights (see page 90)

- (10.3) Rights
- Setting Policies (see page 93)
- (10.3) Policies

3.9 Managing Administrator Accounts

Plan administrator access before rollout. Grant administrative rights to as few accounts as possible, and give each account only the rights needed for its role.

3.9.1 Use Separate Admin and User Accounts

In most environments, the people who administer MyQ also use it as regular users – they print documents, scan files, and do everything other users do. Mixing administrative and everyday activity in a single account is a security risk. Instead, create two accounts for each administrator: one for daily use with standard user rights, and one strictly for administrative tasks.

For example, your IT administrator Tim would use the account `tim.canterbury` for printing and scanning, and `tim.canterbury.admin` for managing users, configuring queues, and adjusting settings. The everyday account carries no elevated rights. The admin account is used only when administrative work is required.

This reduces the attack surface of privileged accounts, makes stricter authentication controls easier to apply where available, and creates a clearer audit trail because administrative actions are not mixed with everyday print and scan activity.

3.9.2 The *admin Account

Every new MyQ installation includes a built-in `*admin` Server Administrator account for initial setup. It should not be used for ongoing administration after named administrator accounts are created. The recommended lifecycle is:

1. Set the `*admin` password in Easy Config immediately after installation.
2. Use it to complete initial setup – configure the system, synchronize or create users, assign rights.
3. Create at least one named administrator account with the minimum rights needed for ongoing administration.
4. Disable the `*admin` account in Easy Config once setup is complete.

Note that from MyQ X 10.2, if the `*admin` password is still set to the default `1234` at upgrade time, the account is automatically disabled and requires a password reset in Easy Config before it can be used again.

3.9.3 Least Privilege

Beyond the admin/user account separation, apply the same principle to every rights assignment: grant only what is needed for the task, and nothing more. MyQ rights can be assigned by task. For example, a user who recharges credit can be granted the relevant credit rights without full Administrator rights; a user who manages users does not necessarily need access to system-wide settings.

See also:

- (10.3) MyQ Easy Config
- (10.3) Rights
- (10.3) Policies
- Granting User Rights (see page 90)

3.10 Granting User Rights

Every user in MyQ operates within a defined rights scope that controls what they can see and do in MyQ. Most end users do not need explicit rights. A standard user account can still use normal print and scan workflows where the required queues, terminal actions, and policies are already configured. Rights become relevant for the people who need to administer or oversee some part of the environment.

The strategic goal is to match rights to roles, not to individuals. Design your rights model around the administrative roles that exist in your organization before go-live, assign those profiles to groups, and add individuals to the relevant group. This scales better as staff changes: when rights are assigned to groups, a new office administrator can receive the appropriate rights by joining the relevant group.

3.10.1 Available Rights

MyQ provides the following rights, each scoping a specific area of the system:

Right	Scope
Administrator	Administrator-level access. Delete Cards is assigned separately.
Manage Settings	Access to Settings management, excluding the Rights tab. Check the current Rights documentation for exact exceptions.
Manage Users	Access to user and group management, user settings, policies, and limited related accounting, credit, and quota areas.
Manage Printers	Monitor printers, device settings, terminals configuration.
Manage Queues	Create, edit, and manage queue status.
Manage Jobs	Edit other users' jobs.
Read Jobs	View other users' jobs without editing.
Manage Reports	Create, edit, and organize reports.
Manage Licenses	View and manage MyQ licenses.
Manage Payments	Access to the Payments tab.
Manage Projects	Project creation and management.
Manage Vouchers	Voucher batch management.
Boost Quotas	Access to Quota boosts.
Recharge Credit	Credit recharging, including the user's own.
View Log	Read-only access to Log and Audit Log.
View Printers	Read-only access to the Printers tab.
Delete Cards	Delete other users' ID cards from the User profile widget, where this right is available.

Rights accumulate – if a user has individual rights and is also a member of a group with additional rights, they hold all of them simultaneously.

3.10.2 Users With No Rights Assigned

A user with no explicit rights still has access to the Web UI – they are not locked out. Their access is limited compared with users who have administrative rights. They can use the standard user-facing areas of the Web UI, but they cannot access administrative settings or agendas unless rights are granted.

For the majority of end users – people who print, scan, and manage their own jobs – this default state is sufficient. Rights assignments are for people with an administrative or oversight role, not for the general user population.

3.10.3 Assigning Rights in Practice

The following examples show how rights can be matched to administrative roles.

Separating IT administration from user management

An IT administrator needs full system access to configure network settings, printers, and queues – grant them Administrator or Manage Settings. An office manager responsible for user administration and credit recharge may need **Manage Users** and **Recharge Credit**. Giving the office manager full Administrator rights is unnecessary and creates risk – they have access to infrastructure settings they are unlikely to understand and should not be changing.

Controlling reporting information

Manage Reports grants broad control over reports. Limit this right to users responsible for maintaining the report structure, otherwise report ownership and organization can become difficult to manage. Restrict **Manage Reports** to a small number of designated individuals responsible for maintaining a clean report structure. Other users can be left without **Manage Reports** unless they need to create or maintain shared reports.

Protecting confidential data while allowing administration

In environments where print or scan jobs can contain sensitive or personally identifiable information – legal documents, patient records, financial statements, HR correspondence, etc. – controlling who can see job content may be a compliance requirement. Under GDPR and similar frameworks, access to personal data should be limited to those with a legitimate need, and organizations must be able to

demonstrate that technical controls are in place to enforce that limitation. MyQ's rights model supports this directly.

Granting an IT specialist **Manage Settings** or **Manage Queues** gives them the access they need to configure and maintain the environment, while withholding **Read Jobs** and **Manage Jobs** means job content remains inaccessible to them. The same principle applies to log access: View Log exposes metadata about who printed what and when, which may itself constitute personal data under GDPR. Grant it only to roles with a documented need.

The Audit Log can help show which administrative actions were performed and by whom. Include Audit Log retention in your broader data retention policy where audit records are needed for operational, privacy, or compliance reasons.

See also:

- (10.3) Rights
- (10.3) Site Server Rights Management
- (10.3) MyQ Audit Log
- (10.3) Log Settings
- (10.3) Easy Config Log Tab

3.11 Setting Policies

MyQ uses two distinct policy types – print job policies and printer policies – and understanding the difference between them is essential before configuring either. Both types let you define and enforce desired print behavior across users and devices.

3.11.1 Print Job Policies

Print job policies control the attributes of the print job itself, including color, duplex, and stapling. They also control whether the user is permitted to change any of those settings before printing. A policy can enforce duplex while still allowing the user to switch to simplex when needed, or it can enforce duplex and deny any override.

Print job policies apply across all queues and all devices for the assigned users. There is no way to scope a print job policy to a specific printer – if a user has a print job policy enforcing mono, it applies everywhere they print.

Job Setting	Enforced Value	User Can Change
Keep jobs for reprint	Yes / No	Allow / Deny
Color	Do not change / Force mono / Revert force mono	Allow / Deny
Duplex	Do not change / Simplex / Duplex long edge / Duplex short edge	Allow / Deny
Staple	Do not change / Yes / No	Allow / Deny
Punch	Do not change / Yes / No	Allow / Deny
Toner saving	Do not change / Yes / No	Allow / Deny
Copies	–	Allow / Deny
Page range	–	Allow / Deny

3.11.2 Printer Policies

Printer policies control what a user can do on a specific device – whether they can print, copy, scan, or fax, and at what device access level. Unlike print job policies, printer policies are scoped to a combination of user or group and printer or printer group. Use printer policies when access varies by location or device rather than by job attribute.

Setting	Options
Print	Yes / No
Copy	Yes / No
Full-color copy	Yes / No
Scan	Yes / No
Fax	Yes / No
Device access level	User / Administrator

In most deployments, both types are used together – print job policies set the baseline behavior for all printing, and printer policies handle device-specific access.

3.11.3 Policy Priority

When a print job policy and a printer policy are in conflict for a particular user, the print job policy takes priority, because this policy operates at a more granular level and its settings are more specific to the job being submitted.

Where multiple policies of the same type apply to a user through overlapping group memberships, priority is determined by the order in which they are listed in settings. Policies higher in the list take precedence over those below them. Policies can also be temporarily disabled without being deleted, which is useful during testing or transitional periods.

The **Show Effective Policies** tool resolves the combined result for any user and printer combination. Before go-live, use it to verify that the policy configuration is producing the intended outcome for representative users across each group.

3.11.4 Practical Examples

Environmentally Friendly and Cost-Conscious Printing

Enforcing sustainable print behavior is most effective when policies do the work rather than relying on user awareness. The recommended approach uses two complementary policies.

The first applies to the majority of users – those with straightforward, day-to-day printing needs. This policy enforces mono, duplex, and toner saving, and denies the ability to change any of those settings. Color printing, single-sided output, and toner saving overrides are simply unavailable.

The second targets users with more complex or demanding print requirements – marketing materials, client-facing documents, legal forms that must be single-sided. This policy relaxes the constraints: color is permitted, duplex can be changed, toner saving can be overridden. These users are still expected to make sustainable choices where appropriate, but are not blocked when their work genuinely requires otherwise.

The same two-policy model applies directly to cost control. The standard policy keeps the majority of users on low-cost output settings; the permissive policy is granted selectively and reviewed periodically as printing needs change.

Differentiating Access by Printer

In some environments, who is printing matters less than where they are printing. A university is a good example – a student printing coursework on a public library printer needs basic access, but the same student working a part-time shift at the library office may need full device access on the office printer behind the counter.

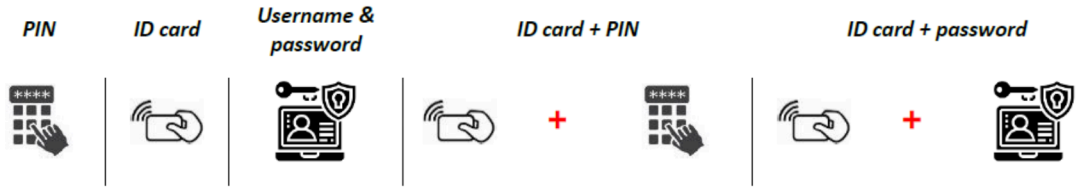
For this model, set the print job policy as permissively as possible – allow all job settings changes, apply no defaults. The printer policy of each device then defines what is actually available. Public printers are configured to allow printing and monochrome copying only. Office printers grant full access including administrator-level device functions.

This approach works well wherever access is naturally defined by physical location rather than by individual identity, and where the same person legitimately occupies different roles in different contexts.

See also:
- (10.3) Policies

4 Secure Authentication

MyQ supports a range of authentication methods across its different interfaces and client applications. The right combination for your organization depends on your infrastructure, your user population, and your security requirements.



4.1 Supported Authentication Methods

Method	Embedded Terminal	Desktop Client	Mobile Client	Web (Print Server)	Web (Central Server)
PIN	✓	✓	✓	✓	–
Username + password	✓	✓	✓	✓	✓
Username + PIN	–	✓	✓	✓	–
ID Card + PIN (2-step)	✓	–	–	–	–
ID Card + password (2-step)	✓	–	–	–	–
QR Code (Mobile Client)	✓	–	–	–	–
Sign in with Microsoft (Entra ID)	–	✓	✓	✓	✓
Entra ID SSO (silent, Windows only)	–	✓	–	–	–
Integrated Windows Authentication	–	✓	–	✓	✓

4.2 Choosing Your Authentication Strategy

No single authentication method suits every environment. The right choice depends on your infrastructure, your user population, and how much friction users can tolerate at the device. The following scenarios cover the most common deployment patterns.

4.2.1 Managed Domain, Windows-Joined Devices

If all users are on domain-joined Windows workstations and the MyQ server is also domain-joined, Integrated Windows Authentication is the lowest-friction option for Web Interface and Desktop Client access – users authenticate silently using their Windows identity without entering credentials. At embedded terminals, combine this with ID card authentication to avoid a separate manual login step: users are already identified by domain at their workstation, and tap their card at the device to release jobs.

4.2.2 Cloud-First and Entra ID Environments

Where your organization uses Entra ID as the primary identity provider and devices are Entra ID-joined, Entra ID SSO is usually the preferred silent-authentication option for client workstations. Users are authenticated silently at Desktop Client startup using their OS identity and a token from Entra ID. Sign in with Microsoft covers Web Interface and Mobile Client access for the same user population.

At embedded terminals, the MyQ X Mobile Client with QR code login continues the same pattern. Users sign in to the mobile app with their Microsoft account – including any Entra ID MFA step already in place – and authenticate at devices by scanning a QR code on the terminal panel.

4.2.3 Hybrid Environments

Many organizations run a mix of on-premises AD and Entra ID, with a combination of domain-joined and Entra ID-joined devices. One useful pattern is to layer the two silent authentication methods in the Desktop Client: Entra ID SSO and IWA. MyQ attempts Entra ID SSO first; IWA can be used as a fallback for domain-joined devices where Entra ID SSO is not available. Users who cannot use either silent method can fall back to a configured manual login method.

For the Web Interface, both IWA and Sign in with Microsoft can be enabled simultaneously, covering domain-joined and cloud-managed users respectively.

4.2.4 Mixed Device Fleet Including BYOD

Where some users are on managed devices and others are not – personal laptops, macOS, mobile devices – silent authentication cannot cover the whole population. IWA and Entra ID SSO both require specific device join conditions that BYOD devices will not meet. Ensure a manual fallback is always available: username + PIN or username + password for users who cannot authenticate silently. For users with Microsoft accounts, **Sign in with Microsoft** can provide a manual login option that does not depend on Windows domain membership. Note that this is different from Desktop Client Entra ID SSO, which has device and operating system prerequisites.

At embedded terminals, ID card + PIN 2-step authentication provides consistent security regardless of how the user authenticated at their workstation.

4.2.5 Guest and Contractor Access

Users without a permanent directory presence need a lightweight onboarding path. One practical pattern is self-registration via Jobs via Email combined with temporary PINs. When configured correctly, users can be created automatically after sending their first email print job and receive a time-limited PIN by email. The PIN expires automatically, reducing follow-up cleanup, but the account and group assignment still need to be planned.

4.2.6 High-Security Environments

Where print and scan content is sensitive two-factor authentication at embedded terminals is strongly recommended. A common implementation is **ID Card + PIN**: the card identifies the user account, and the PIN adds a second check before access is granted. PINs should be long enough relative to your user population to prevent guessable combinations.

For a stronger terminal-authentication model, consider the Mobile Client QR code model with biometric lock enabled. Users unlock the Mobile Client with Face ID or fingerprint recognition, then scan the terminal QR code to authenticate at the device.

4.3 Security Best Practices

The following recommendations apply across the user management and authentication configuration described in this section. Review them as a set before finalizing your deployment design.

4.3.1 Use Two-Factor Authentication for Sensitive Environments

Where print or scan content is sensitive, avoid relying on PIN-only terminal authentication as the only control. Consider **ID Card + PIN** or **ID Card + Password** as a stronger baseline. The Mobile Client QR code model with biometric lock can also be considered where users have suitable mobile devices and app access.

4.3.2 Protect Administrative Accounts

Create separate accounts for administrative and everyday use. Apply stricter authentication requirements to admin accounts – longer passwords, MFA where available – without impacting the daily experience of regular users. Disable the built-in `*admin` account once initial setup is complete.

4.3.3 Enforce LDAPS for Directory Communication

Configure directory authentication and synchronization to use encrypted LDAP wherever supported, such as LDAPS/TLS. For Active Directory authentication servers, configure TLS and use port 636. For LDAPS to work, the MyQ server must trust the certificate presented by the directory server. Install the issuing root CA certificate in the Windows certificate store on the MyQ server. If your organization distributes CA certificates via Group Policy, this may already be handled automatically.

4.3.4 Protect Sensitive Directory Attributes

If ID card numbers, PIN codes, or other sensitive user identifiers are stored in Active Directory and synced to MyQ, be aware that standard AD attributes are readable by any authenticated domain user by default. Before enabling sync of these values, review whether they need to be protected using confidential attributes – a mechanism that restricts read access to specified trustee accounts, such as the service account used by MyQ for synchronization.

For stronger protection, store these values in custom schema extension attributes rather than standard AD attributes. Custom attributes are less predictable to enumerate and can be flagged as confidential. If schema changes or confidential attribute configuration are required, test the approach in a lab environment before applying it to production.

4.3.5 Apply Least Privilege to the Sync Service Account

The service account used by MyQ for LDAP synchronization should have read-only access scoped to the organizational units being synced – nothing more. A sync account with broad directory read permissions is an unnecessary risk. If confidential attributes are used for card or PIN data, the service account must be explicitly granted trustee access to those attributes.

4.3.6 Control Access to Job Content

Manage Settings and Manage Queues rights give administrators access to system configuration without exposing job content. Withhold Read Jobs and Manage Jobs from anyone who does not have a documented need to view print or scan content. In environments subject to GDPR or similar privacy requirements, this separation is a technical control that should be documented and auditable.

4.3.7 Size PINs Appropriately for Your User Population

PIN codes are the most common authentication method at embedded terminals and carry the full authentication burden – no username is required. The security of PIN authentication is directly determined by the ratio of possible PIN combinations to the number of users. If every possible 4-digit combination is in use across 10,000 users, any 4-digit number will authenticate as someone.

Ensure the minimum PIN length is set so that possible combinations significantly exceed the number of users. MyQ will warn you when the user count approaches the point where uniqueness can no longer be guaranteed – act on that warning promptly by increasing the minimum length and regenerating PINs.

4.3.8 Define Account Lockout Policy

MyQ supports configuring the maximum number of failed login attempts before an account is locked, and the lockout duration. Define these values before go-live – the defaults may not meet your organization's security policy. For sensitive environments, a low attempt threshold with a meaningful lockout duration can help reduce brute-force attempts against PIN and password authentication.

See also:

- (10.x) MyQ X Security

- (10.3) Advanced Security

4.4 PIN and Password Authentication

PIN codes and passwords are widely used authentication methods in MyQ deployments – straightforward to set up and familiar to users. Both have security implications that are worth understanding before deciding how to use them.

4.4.1 PIN Codes

A PIN is entered without a username – unlike passwords, the PIN alone is sufficient to authenticate. This makes PIN authentication fast and frictionless, but means the PIN itself carries the full authentication burden. If PINs are too short or predictable, a user may be able to guess another user's PIN and authenticate as that user. If user storage is connected and folder browsing is enabled, this can also expose stored files.

The security of PINs in your environment is determined by two factors: the number of users and the minimum PIN length. The relationship between them is straightforward. For example, if 10,000 users all use unique 4-digit PINs, there are only 10,000 possible combinations. In that situation, every possible PIN can be assigned to a user, making random guessing far more likely to succeed. Increase the minimum PIN length so that the number of possible combinations significantly exceeds the number of users.

MyQ includes a built-in warning that triggers when the user count approaches the point where PIN uniqueness can no longer be guaranteed. Treat this as a signal to increase the minimum PIN length and regenerate PINs – not something to dismiss.

PINs can be generated by administrators in bulk and distributed to users by email, or users can generate their own if that option is enabled. Consider which model suits your environment: Bulk generation gives administrators central control over PIN generation and distribution. Self-generation reduces administrative overhead, but users must know how to generate or reset their PIN.

PIN authentication is available on embedded terminals, Desktop Client, Mobile Client, and the Print Server Web Interface. It is not available on the Central Server Web Interface, which accepts passwords only.

4.4.2 Temporary PINs

Temporary PINs expire after a defined period and are a useful tool in several specific deployment scenarios. Three use cases are worth planning for explicitly.

Use Temporary PINs for Guest and Visitor Access

Organizations that regularly host external visitors or contractors can configure a fully automated guest printing workflow using temporary PINs and self-registration via Jobs via Email.

When an unrecognized email address sends a print job, MyQ creates an account automatically and assigns it to the SELF-REGISTERED group. If that group is configured to receive only temporary PINs, the new user receives a PIN valid for a defined period – 24 hours is a common choice for day visitors. The PIN expires automatically; the next time the same person visits and sends a job, a new temporary PIN is issued. Regular employees in other groups are unaffected and continue to receive persistent PINs.

When all dependencies are configured correctly, this workflow can create the user account, assign a temporary PIN, and send the PIN by email without routine administrator action. The key configuration dependencies are: self-registration via email enabled, the SELF-REGISTERED group configured for temporary PINs only, and Send PIN via email enabled.

Use Temporary PINs for Organization-Wide PIN Rotation

Some organizations require all users – not just guests – to rotate their PINs regularly. MyQ supports this by generating all PINs as temporary with a defined validity period. For example, you might set a 30-day validity period if your organization requires monthly PIN rotation.

With this configuration, MyQ can generate temporary PINs for new users who meet the PIN-generation conditions, such as having an email address, and send the PIN by email when email notification is enabled. If **User can change PIN** is enabled, users can generate a new PIN from the Web Interface or Mobile Client before or after expiry. Ensure users are informed about this workflow before it goes live – unexpected PIN expiry at the device is a common source of helpdesk calls.

The following table summarizes the difference in PIN behavior between regular users and users in the SELF-REGISTERED group:

	Regular User	Self-Registered User (SELF-REGISTERED group)
PIN received when sending a job via email	Yes	Yes
PIN type	Persistent (never expires)	Temporary (expires after set period)
PIN change notifications	Sent by email	Sent by email
User can generate their own PIN	Yes – generates a persistent PIN	Yes – generates a temporary PIN

Note that the "User can change PIN" option in User Authentication – PIN applies globally. If disabled, no user – including self-registered guests – can regenerate their own PIN from the Web Interface or Mobile Client.

Use Temporary PINs during ID Card Registration

A short-lived temporary PIN is an effective onboarding tool for environments where ID cards are the primary authentication method. The administrator generates a temporary PIN for the new user – valid for a few days. The user swipes their card at a terminal, is prompted to register it, enters the temporary PIN once to confirm their identity, and the card is linked to their account. After the card is registered, the temporary PIN is no longer needed for regular card authentication and expires according to its validity period. This reduces cleanup compared with issuing persistent PINs for card onboarding.

For this to work, the terminal must be configured with "Allow the existing user to register the card" as the behavior when an unknown card is swiped.

4.4.3 Password Authentication

Passwords are always used in combination with a username – unlike PINs, they cannot authenticate a user on their own. This combination means a correctly guessed password is only useful if the attacker also knows the username, which provides a meaningful additional barrier.

Password authentication is available across all user-facing MyQ components:

- MyQ Web Interface (Print Server and Central Server)
- Embedded Terminals (if enabled in the configuration profile)
- MyQ Desktop Client (if enabled in the configuration profile)

- MyQ X Mobile Client (always available)

At embedded terminals, both the username and password must be entered. Note that an alias can be used in place of the username – useful in environments where the username format is not intuitive for users to type at a device screen.

Users set their own passwords via the Web Interface, subject to the complexity rules configured by the administrator. When defining password rules, consider favoring longer passwords or passphrases over short passwords with complex character requirements. Long passwords are usually easier to make resistant to guessing while remaining usable for users.

If your organization uses Entra ID for user authentication, consider **Sign in with Microsoft** instead of managing separate MyQ passwords. When users authenticate through Microsoft sign-in, the relevant Entra ID password and MFA policies apply through that identity flow.

4.4.4 Planning Checklist

Before finalizing your PIN and password configuration, confirm the following:

- Minimum PIN length is set so that possible combinations significantly exceed the number of users.
- Send PIN via email is enabled if PINs are the primary or sole authentication method. If this is disabled and new PINs are generated, users receive no email notification. If PIN is their only practical authentication method, they may be unable to use MyQ until an administrator provides or resets their PIN.
- If "User can change PIN" is disabled, users cannot generate a new PIN or reset a forgotten PIN from the Web Interface or Mobile Client. Administrators become the recovery path for PIN issues unless another authentication method is available.
- Temporary PIN validity periods are communicated to affected users before go-live.
- Password complexity policy favors length over character requirements.

See also:

- (10.3) User Authentication
- (10.3) ID Card Management
- (10.3) Users Settings
- (10.3) Generating PIN

4.5 Two-Factor Authentication

Two-Factor Authentication (2FA) combines two independent credentials – something the user has and something they know, or something they are – to verify identity before granting access. For print environments handling sensitive documents, 2FA at embedded terminals provides an important security control.

MyQ supports several stronger authentication patterns. At embedded terminals, users can authenticate with card-based 2FA methods or QR code login through the Mobile Client. For Desktop Client and Mobile Client sign-in, MFA can also be enforced by the external identity provider, such as Entra ID, when Microsoft sign-in is used.

4.5.1 Authentication at Embedded Terminals

Users can authenticate with 2FA at embedded terminals using one of two card-based methods, or by scanning a QR Code with the Mobile Client.

Configure embedded terminal login methods per terminal configuration profile in **Settings > Printers & Terminals**.

ID Card + PIN

The user presents their ID card to the reader, then enters their PIN to confirm. This is a common implementation. PIN codes can also be issued as temporary, which can reduce the risk of long-lived PIN misuse.

ID Card + Password

The user presents their ID card to the reader, then enters their password to confirm. This method is appropriate where your password policy already meets your security requirements and you prefer not to manage a separate PIN population.

QR Code Authentication with Mobile Client

The MyQ X Mobile Client can provide a stronger terminal-authentication option where users already have managed mobile devices and app access. Users sign in to the mobile app with their MyQ credentials – or via an authentication server such as Entra ID or Active Directory – and authenticate at the terminal by scanning a QR code displayed on the device screen.

Where biometric lock is enabled, the user must unlock the Mobile Client with Face ID or fingerprint recognition before using the app. This combines the enrolled mobile

device, biometric app unlock, and the terminal QR code, while avoiding the need to issue cards or PINs for that terminal-login workflow.

This model can fit Entra ID environments where users sign in to the Mobile Client with Microsoft accounts. If Entra ID MFA is enforced, users complete that MFA step during Microsoft sign-in. After that, the Mobile Client can act as the terminal login method, so users do not enter a MyQ-specific credential at the device for this workflow.

Where users authenticate to the Mobile Client against an LDAP authentication server, such as Active Directory or OpenLDAP, those credentials are validated against the remote identity provider and are not stored in MyQ. Document this behavior where credential-storage requirements are part of the deployment review.

4.5.2 Two-Factor Authentication in Desktop Client

Organizations using Microsoft 365 can enable **Sign in with Microsoft** in the Desktop Client configuration profile. When users authenticate through Microsoft sign-in, any MFA required by Entra ID is handled by Entra ID during the sign-in flow. No separate MyQ 2FA setting is required for that Microsoft sign-in step.

Configure Desktop Client login methods in **Settings > MyQ Desktop Client**, in the relevant configuration profile.

4.5.3 Planning Considerations

Stronger authentication can add steps to terminal use, such as a card tap, PIN entry, or phone unlock. For most users in most environments this is acceptable, but it is worth considering:

- In high-volume environments, card-only authentication with a longer session timeout may reduce friction, but it should be treated as a security/usability trade-off.
- The Mobile Client QR code model requires all users to have a compatible smartphone and the app installed. Plan the rollout and user communication accordingly.
- ID cards need to be issued, registered, and managed. Factor card provisioning into your deployment timeline, particularly in larger environments or those with high staff turnover.
- If cards are lost, define a fallback authentication method. Otherwise, users who rely only on card authentication may be unable to use devices until a replacement card is issued.

See also:

- (10.3) User Authentication
- (10.3) Users Settings
- (10.3) Configuration Profiles
- (10.3) MyQ Desktop Client Settings

4.6 Single Sign-On with Entra ID

Microsoft Entra ID Single Sign-On (SSO) provides silent authentication for **MyQ Desktop Client on Windows**. When Desktop Client starts on a supported joined device, it can use the signed-in Windows identity to obtain an Entra ID token and authenticate the user to MyQ without prompting for credentials.

Compared with Integrated Windows Authentication (IWA), Entra ID SSO is based on Microsoft cloud identity rather than Kerberos or NTLM. It is usually the preferred silent-authentication option for cloud-first or hybrid environments where Windows devices meet the required Entra ID join conditions.

Prerequisites:

Before deploying Entra ID SSO, make sure:

- MyQ Print Server 10.2 patch 6 or later is installed.
- MyQ Desktop Client is running Windows. Entra ID SSO is not supported on macOS.
- Windows devices are Entra ID joined, Active Directory joined, or hybrid joined.
- MyQ is connected to Microsoft Entra ID
- Sign in with Microsoft is enabled for the authentication server in **MyQ > Settings > Authentication Servers**.

4.6.1 Configure the Microsoft Entra Application

Entra ID SSO uses the Microsoft Entra application configured for the MyQ Entra ID connection. The application requires additional configuration for MyQ Desktop Client SSO, including the appropriate redirect URI and client configuration.

If MyQ manages the application automatically, the required configuration can be created or updated during authorization. If your organization manages the

application manually, configure the Desktop Client SSO settings in the existing MyQ application registration.

4.6.2 How Entra ID SSO Works

When MyQ Desktop Client starts:

1. Desktop Client requests an Entra ID token using the identity of the signed-in Windows user.
2. If the device and user meet the Entra ID authentication requirements, Microsoft issues the token without requiring user interaction.
3. Desktop Client uses the token to authenticate the user to MyQ.

When silent authentication succeeds, the user does not enter MyQ or Microsoft credentials in Desktop Client.

4.6.3 Authentication Fallback

If Entra ID SSO cannot authenticate the user, Desktop Client can fall back to other configured authentication methods:

1. **Integrated Windows Authentication (IWA)**, if enabled.
2. **Manual sign-in**, if enabled.

If both Entra ID SSO and IWA are enabled, Entra ID SSO is attempted first.

This combination can be useful in hybrid environments. Devices that meet the Entra ID SSO requirements can authenticate through Entra ID, other supported domain-joined Windows devices can use IWA, and remaining users can use a configured manual authentication method.

See also:

- Manual App Registrations (see page 35)
- Microsoft Entra Application Reference (see page 41)
- (10.3) Connect to Microsoft Entra ID (Graph API)
- (10.3) Configure Microsoft Entra ID Authentication

4.7 Integrated Windows Authentication

Integrated Windows Authentication (IWA) lets users authenticate to MyQ using their signed-in Windows identity without entering separate MyQ credentials.

IWA is designed for Active Directory environments with managed Windows devices. MyQ uses **Kerberos** where the required conditions are met and can fall back to **NTLM** unless Kerberos-only authentication is enforced.

IWA can be used for authentication to the MyQ Web Interface and MyQ Desktop Client.

This article covers the **deployment requirements and design considerations** for Integrated Windows Authentication.

For the configuration procedure, including MyQ settings, SPN registration, browser and Desktop Client configuration, Kerberos enforcement, domain mapping, and troubleshooting, see the MyQ X Server guide.

4.7.1 When to Use IWA

Consider IWA when:

- users and workstations are managed through Active Directory Domain Services (AD DS);
- client devices are joined to the same domain as the MyQ server or to a trusted domain;
- users should authenticate to MyQ using their existing Windows session;
- DNS, domain trust, and browser or client policies can be managed centrally.

IWA is primarily intended for managed domain environments. Users on BYOD devices, guest devices, or other computers outside the relevant domain or trust relationship need an alternative authentication method.

If your organization primarily uses Microsoft Entra ID for Windows identity, consider **Single Sign-On with Entra ID** instead.

4.7.2 Kerberos and NTLM

MyQ supports both Kerberos and NTLM for Integrated Windows Authentication.

	Kerberos	NTLM
Recommended use	Preferred for IWA	Compatibility fallback
Authentication	Ticket-based with mutual authentication	Challenge-response
Main dependencies	AD DS, DNS, correct SPN configuration, time synchronization	Fewer Kerberos infrastructure requirements
Deployment guidance	Use wherever possible	Retain only where required

Kerberos should be the primary protocol for IWA deployments. NTLM can provide compatibility where Kerberos cannot be used, but organizations that retain NTLM should consider their wider Windows security policy.

If your organization plans to restrict or disable NTLM, verify Kerberos authentication for MyQ and other affected services before applying the change.

4.7.3 Deployment Prerequisites

Before planning IWA for production use, confirm that:

- Active Directory Domain Services is available.
- The MyQ server and affected client computers are joined to the same domain or trusted domains.
- DNS reliably resolves the FQDN used by clients to access the MyQ server.
- Time synchronization is reliable between domain controllers, the MyQ server, and clients.
- Active Directory is configured as the authentication source for the affected MyQ users.
- Users are synchronized or otherwise mapped correctly to their Active Directory identities.
- Managed browsers and Desktop Clients can be configured to use Windows integrated authentication.
- The required HTTP Service Principal Name (SPN) can be registered in Active Directory.

MyQ uses Windows `http.sys` for Windows authentication. The HTTP SPN used for Kerberos authentication must therefore be associated with the **MyQ server computer account**.

For SPN registration, browser configuration, MyQ settings, and verification procedures, see **Configure Integrated Windows Authentication** in the MyQ X Server guide.

4.7.4 How Kerberos Authentication Reaches MyQ

When a domain user signs in to Windows, the client obtains a Ticket Granting Ticket (TGT) from Active Directory.

When the user subsequently accesses MyQ using the server FQDN:

1. The client requests a Kerberos service ticket for the MyQ HTTP service.
2. Active Directory uses the registered HTTP SPN to identify the MyQ server.
3. MyQ validates the service ticket and authenticates the user.

This flow depends on correct DNS resolution, SPN registration, domain trust, and time synchronization.

Using a hostname that does not correspond to the configured SPN can prevent Kerberos authentication and cause authentication to fall back to NTLM where fallback is permitted.

4.7.5 Where IWA Is Configured

Integrated Windows Authentication involves configuration in several places:

- **MyQ X Server** — enables Windows Authentication and controls Kerberos/ NTLM behavior.
- **Active Directory** — provides the domain trust and Service Principal Name (SPN) required for Kerberos.
- **Client browsers** — must allow integrated Windows authentication for the MyQ server.
- **MyQ Desktop Client** — Seamless Single Sign-On is enabled through Desktop Client configuration profiles where required.

For the configuration procedures, see **Configure Integrated Windows Authentication** in the MyQ X Server guide.

4.7.6 Web Interface Authentication

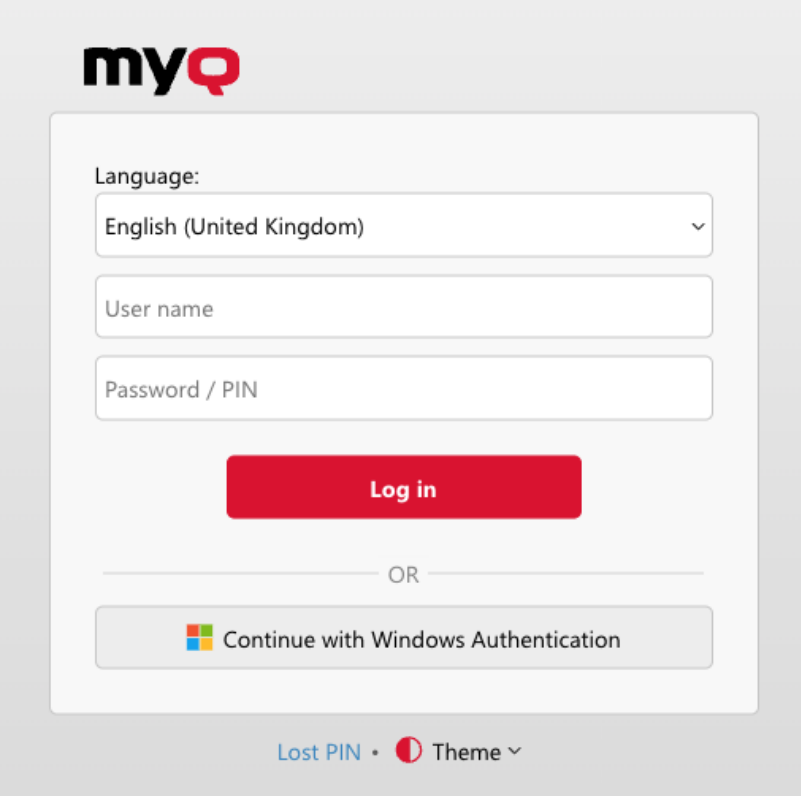
When Windows Authentication is enabled, it is available as an additional sign-in method in the MyQ Web Interface.

Domain users on correctly configured managed computers can authenticate using their current Windows identity. Other configured login methods remain available for

users who are outside the IWA environment or cannot authenticate through Windows.

Browser-based IWA also depends on the browser recognizing the MyQ server as an integrated-authentication destination and being permitted to send Windows credentials automatically.

In managed environments, plan to distribute the required browser configuration centrally rather than configuring individual workstations.



4.7.7 MyQ Desktop Client Authentication

MyQ Desktop Client can use Integrated Windows Authentication to authenticate the signed-in Windows user automatically.

Seamless authentication is configured through Desktop Client configuration profiles, allowing different workstation populations to use different authentication methods.

Where Microsoft Entra ID SSO and IWA are both configured, MyQ Desktop Client can use the following fallback sequence:

1. Microsoft Entra ID authentication

2. Integrated Windows Authentication
3. Manual sign-in

This allows Entra ID authentication to be used as the primary seamless method while retaining IWA for users or environments where cloud authentication is unavailable.

4.7.8 IWA and Microsoft Entra ID SSO

Integrated Windows Authentication and Microsoft Entra ID SSO both provide seamless authentication for Windows users, but they rely on different identity infrastructure.

	IWA	Microsoft Entra ID SSO
Identity source	Active Directory Domain Services	Microsoft Entra ID
Primary authentication	Kerberos	Microsoft cloud identity
Main client environment	AD domain-joined Windows devices	Entra ID, AD, or hybrid-joined supported Windows devices
Microsoft Entra application required	No	Yes
Typical deployment	On-premises AD environments	Cloud-first or hybrid identity environments

Use IWA where authentication is primarily based on on-premises Active Directory and Kerberos.

Use Microsoft Entra ID SSO where Microsoft Entra ID is the primary identity platform and the required Windows and MyQ configuration is available.

Hybrid environments can use both. When both methods are configured for MyQ Desktop Client, Entra ID authentication is attempted before IWA.

See also:

- (10.3) Configure Integrated Windows Authentication
- Single Sign-On with Entra ID (see page 108)
- (10.3) Configure Microsoft Entra ID Authentication

- User Synchronization (see page 56)
- Integrated Windows Authentication | Microsoft Learn[3]
- Kerberos Authentication Overview in Windows Server | Microsoft Learn[4]

3. https://learn.microsoft.com/en-us/aspnet/web-api/overview/security/integrated-windows-authentication
4. https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview

5 Devices & Embedded Terminals

Before users can print, scan, or authenticate at a device, the device needs to be added to MyQ, activated, and configured with the right terminal package and profile. For most deployments this is the most hands-on phase of the rollout – it involves physical devices, vendor-specific configuration, and coordination across network, licensing, and identity infrastructure that was set up in earlier phases.

This section covers the decisions and preparation required before devices go live, how to approach discovery and activation at scale, and how to manage terminal packages and upgrades over the lifetime of the deployment.

Work through these pages in order – device preparation depends on network and certificate decisions made earlier in the planning process, and terminal action design depends on the group and authentication configuration covered in the previous section.

5.1 Contents

5.2 Preparing Your Device Fleet

Before adding devices to MyQ, complete the preparation steps that affect discovery, activation, and embedded terminal installation. Missing preparation can cause activation failures or unexpected behavior after rollout.

5.2.1 Network Readiness

Devices must be connected to the network and reachable from the MyQ server before discovery or manual addition can proceed. Confirm the following:

- Devices are online, initialized, and idle – initial device setup must be complete before MyQ can manage them.

- The MyQ server can reach each device over the network. If the server and devices are on different subnets, confirm that the relevant ports are open between them.
- If devices use DHCP, use stable DNS names, DHCP reservations, or another stable addressing strategy. Avoid relying on changing IP addresses in configuration profiles.

5.2.2 TLS Compatibility

MyQ X 10.3 uses TLS 1.2 as the default minimum for secure communication. Older devices that support only TLS 1.0 or 1.1 may fail to connect or activate when secure communication requires TLS 1.2. Audit your device fleet for TLS support before starting activation – particularly relevant for older devices that may not have received firmware updates.

If legacy devices cannot be updated to support TLS 1.2, the minimum TLS version can be temporarily lowered via `config.ini`. This is not a recommended long-term configuration.

5.2.3 Clean Device State

Before installing a MyQ embedded terminal on a device, confirm the following:

- There is no previous MyQ installation on the device and no leftover MyQ applications.
- If the device has previously been used with another print management system, strongly consider a factory reset or resetting the web control panel settings to defaults before proceeding. Residual configuration from a previous system is a common source of terminal installation failures.

5.2.4 Licensing

There is no limit to the number of devices you can add to MyQ, but you can only activate as many embedded terminals as your license allows. Devices without an embedded terminal can be added and managed for free.

Terminal package updates, and server and component updates, require valid Software Assurance. If Software Assurance has expired, terminal activation will fail with the message "There is no free terminal license on the server." Confirm your license covers the number of terminals in scope and that Software Assurance is current before beginning activation.

Some functionality is licensed at half an Embedded Terminal license, for example Kyocera Lite Embedded Terminal. If your fleet includes devices using these lighter terminal variants, account for this when calculating the number of licenses required.

Consult your MyQ partner or reseller for licensing details.

5.2.5 Vendor-Specific Preparation

Embedded terminal installation varies by vendor. Some vendors require manual device-side configuration before MyQ can complete the remote installation. Common manual steps include:

- Configuring authentication settings on the device.
- Enabling specific functionality of the device's built-in platform.
- Installing the security certificate, if not done automatically by MyQ or when manual certificate management is selected in MyQ Network settings.
- Configuring the device to use MyQ as the primary login screen.
- Configuring settings related to accounting.

Not all steps apply to every vendor – refer to the embedded terminal documentation for your specific device before starting installation.

See also:

- MyQ Brother Embedded
- MyQ Canon Embedded
- MyQ Epson Embedded
- MyQ Fujifilm Embedded
- MyQ HP Embedded
- MyQ KATUN Embedded
- MyQ Kyocera Embedded
- MyQ Kyocera Embedded Lite
- MyQ Lexmark Embedded
- MyQ Ricoh SmartSDK Embedded
- MyQ Sharp Embedded
- MyQ Sharp Luna Embedded
- MyQ Toshiba Embedded
- MyQ Xerox Embedded

5.3 Adding Devices

Once devices are prepared, the next step is adding them to MyQ. There are two methods – Printer Discovery and manual addition – and the right choice depends on the size and complexity of your fleet.

5.3.1 Printer Discovery vs. Manual Addition

Printer Discovery scans your network and identifies reachable devices automatically. MyQ presents the discovered devices for review and allows you to add all or selected devices in a single operation. Printer Discovery is usually the fastest approach for initial onboarding of larger fleets. It reduces manual entry and lets administrators review discovered devices before adding them.

Manual addition gives granular control over each device and is useful for selective additions – a single new device, a device on an isolated network segment, or a device that Printer Discovery cannot reach for network topology reasons.

A common pattern is to use Printer Discovery for initial fleet onboarding and manual addition for individual devices added later.

For discovery and manual addition steps, see the MyQ X Server guide.

5.3.2 SNMP Strategy

MyQ uses SNMP to communicate with printing devices – to read counters, monitor status, and manage configuration. Three protocol versions are available:

- **SNMP v1**: default setting, widely supported but transmits community strings in cleartext.
- **SNMP v2c**: uses a community-string model similar to SNMP v1; do not treat it as a secure alternative to SNMP v3.
- **SNMP v3**: supports authentication and encryption when those options are configured on both the device and in MyQ. Consider SNMP v3 where device-management traffic requires stronger protection.

SNMP profiles are configured in MyQ and assigned per device. Create SNMP profiles for groups of devices that share the same SNMP configuration. This may align with vendor or model groups, but the deciding factor is the SNMP settings required by the devices. If all devices share the same SNMP configuration, a single profile is sufficient.

Define the required SNMP and configuration profiles before running Printer Discovery. Configuration profiles are needed for discovery, and the SNMP profile is selected through the configuration profile. Getting these profiles right upfront reduces reconfiguration after devices are added.

5.3.3 Configuration Profiles

Configuration profiles are used to apply shared settings across groups of devices, such as terminal type, login methods, SNMP profile, network settings, and related options. Many device and terminal settings are controlled through the assigned profile, while device-specific values may still need to be reviewed separately.

Plan your profile structure before discovery. One profile per device type or vendor is often practical when those devices require different terminal packages, credentials, network settings, or SNMP settings. Use the Clone feature to duplicate an existing profile as the starting point for a new one rather than building from scratch. Note that when cloning a profile, existing printers assigned to the original profile are not automatically reassigned to the new one. Printer assignments must be updated separately.

See also:

- (10.3) Printer Discovery
- (10.3) Configuration Profiles
- (10.3) SNMP Profiles

5.4 Plan and Roll Out Terminal Updates

MyQ supports running multiple terminal packages from the same vendor simultaneously, allowing different devices in the same fleet to run different versions of the terminal software.

Use this capability to roll out terminal updates gradually. Testing a new package on a limited group before broader deployment reduces the risk that compatibility issues or unexpected behavioral changes affect the entire fleet.

5.4.1 Plan a Staged Rollout

Avoid updating a large fleet in a single operation.

Start with a small, representative group of devices. Where possible, include each device model and important workflow used in the production environment. A low-traffic location can be useful for an initial pilot, provided it still represents the devices and workflows you need to validate.

Monitor the pilot for an appropriate period based on print volume and business risk. Once the package is stable, update additional groups in stages until the full fleet is covered.

Running multiple terminal versions during this period lets most devices remain on the known working version while the new package is validated.

5.4.2 Check Package Compatibility

Before starting the update:

- **Review the release notes.** Check for improvements, behavioral changes, known limitations, and compatibility requirements for the target terminal package.
- **Confirm device compatibility.** Verify that the target terminal package supports the device models in scope.
- **Verify TLS compatibility.** If the terminal update accompanies a MyQ server update, confirm that the devices support the TLS requirements of the target server version.
- **Confirm Software Assurance is current.** Terminal package updates can require valid Software Assurance. Verify the entitlement before scheduling the update window.

To run multiple terminal packages from the same vendor, at least one package normally needs to be version 10.2 or later. Some 10.1 terminal packages may also support this behavior. Check the Embedded Terminal documentation for the vendor and package versions in scope.

5.4.3 Check Settings Retention

When you update a terminal package using **Replace**, MyQ uploads and installs the new package and reactivates the affected devices.

Settings stored in the MyQ configuration profile are generally retained, but device-side settings and vendor-specific configuration might not be.

Before replacing a package, check the update and uninstallation documentation for the terminal vendor.

For HP terminals, see **HP Update and Uninstallation** and **HP Package Manager**, because package replacement and retained settings can differ from other vendors.

5.4.4 Test the Initial Group

Update a small, representative group first.

After updating the devices, verify:

- terminal activation and connectivity,
- configured authentication methods,
- terminal actions,
- scan destinations and workflows,
- any vendor-specific functionality used in your environment,
- the MyQ Main Log for relevant errors or warnings.

Pay particular attention to functionality identified as changed or limited in the release notes.

Resolve any issues before expanding the rollout.

5.4.5 Roll Out in Stages

After the initial group is confirmed stable, update additional batches.

Where possible, begin with lower-priority or lower-traffic devices. After each batch, review the MyQ Main Log and validate the updated devices before proceeding to the next group.

Avoid updating the entire fleet at once unless the fleet is small and you have an appropriate recovery or rollback plan.

5.4.6 After the Update

After each stage of the rollout:

- **Review the MyQ Main Log.** Check for errors or warnings related to the updated terminals and resolve them before continuing.
- **Test configured functionality.** Verify authentication methods, terminal actions, scan destinations, and other workflows used on the updated devices.
- **Monitor user feedback.** Issues reported after rollout can expose device-model, workflow, or usage combinations that were not covered during testing.

Continue to the next rollout stage only after the current group is operating as expected.

For terminal package upload, assignment, replacement, and update procedures, see the MyQ X Server guide and the Embedded Terminal documentation for your device vendor.

See also:

- (10.3) Printers and Terminals Settings
- (10.3) Configuration Profiles

5.5 Designing the Terminal Experience

The embedded terminal is the primary interface between MyQ and your users at the device. The look and feel of the terminal, including available actions, labels, ordering, icons, and colors, is highly configurable. A well-designed terminal experience can reduce training overhead, speed up device interactions, and help improve consistency across the device fleet.

Terminal experience design depends on group configuration (which users see which actions), authentication configuration (what the login screen looks like and how it behaves), and branding decisions (logos, colors, action names) that may involve stakeholders outside the IT team. Build it into your deployment timeline accordingly.

5.5.1 Terminal Actions

Terminal actions are the workflows available to authenticated users on the device panel – Easy Scan destinations, Easy Copy presets, access to device-native applications, ID card registration, and others. Terminal actions can be scoped to specific users or groups, ordered and organized into folders, and labelled in user-friendly language.

The key design decisions before go-live are:

- **Which actions does each user population need?**
  Map actions to groups as part of your group design process – the two are interdependent.
- **What should each action be called?**
  Default action names may not match the language that users expect. Use names that describe the task clearly, for example, "Scan to HR SharePoint" instead of "Easy Scan 3".

- **How should actions be ordered?**
  Frequently used actions should appear first. Consider whether folders are needed for users with many available actions, or whether a flat list is cleaner for users with only two or three.
- **Which actions should users be able to add to their Favorites?**
  Users can designate personal favorite actions for faster access. If this is enabled by default for your terminal package, make users aware of it during onboarding.

5.5.2 Branding and Custom Themes

MyQ supports visual customization of embedded terminals, including terminal themes and custom appearance for terminal actions. For organizations deploying across a multi-vendor fleet, consistent naming, icons, colors, and themes can help make the experience more predictable, even where terminal behavior differs by vendor or package.

Branding decisions, such as logo files, color choices, icons, and theme selection, should be planned before terminal configuration and may require input from your marketing or communications team.

See also:

- (10.3) Terminal Actions
- (10.3) Terminal Theme Editor

5.6 Terminal Upgrade Best Practices

Terminal upgrades are expected over the lifetime of a deployment. New MyQ releases can include updated terminal packages, and keeping terminals current can be important for security, compatibility, and access to new features. The recommendations here apply to any terminal upgrade, whether a minor patch or a major version change.

5.6.1 Before You Upgrade

- **Check the release notes**
  Before doing anything practical, read the release notes for the terminal version you are upgrading to. Release notes specify improvements, behavioral

changes, bug fixes, and – critically – known limitations and compatibility restrictions for the new package. Surprises during a terminal upgrade are almost always things that were documented in the release notes.

- **Verify TLS compatibility**
  If the upgrade involves a server-side update as well as a terminal package update, re-confirm that all devices in scope meet the TLS requirements of the new server version. See Preparing Your Device Fleet above.
- **Confirm Software Assurance is current**
  Terminal package updates require valid Software Assurance. Confirm this before scheduling the upgrade window, because an expired entitlement can block or delay terminal activation or updates.
- **Test on a limited group first**
  Before upgrading the full fleet, run the new package on a small, representative group of devices, ideally covering each device model in your fleet. Monitor the MyQ main log for errors and test all configured terminal actions on each device.

5.6.2 During the Upgrade

Start with batches of low-priority, low-traffic devices where possible. After testing the batch and reviewing logs, proceed to the next batch after a batch is confirmed stable. Avoid upgrading the full fleet in a single operation unless the fleet is small and you have a clear recovery or rollback plan.

When upgrading using the **Replace** option, some device-side configuration may not be retained. Check the upgrade or uninstallation guide for the terminal vendor before proceeding. For example, HP terminals have specific package-replacement limitations documented in **HP Update and Uninstallation**.

5.6.3 After the Upgrade

- **Check the Main Log**
  After each batch upgrade, review the MyQ Main Log for errors or warnings related to the upgraded terminals. Address any issues before proceeding to the next batch.
- **Test configured functionality**
  Verify that all terminal actions, authentication methods, and scan destinations are working as expected on upgraded devices. Pay particular attention to any functionality that was flagged as changed or limited in the release notes.
- **Monitor user feedback**
  In the days following a rollout, monitor helpdesk traffic for terminal-related issues. User-reported problems after rollout can reveal device-model, workflow, or usage issues that were not caught during testing.

For terminal package upload, assignment, and upgrade steps, see the MyQ X Server guide and the embedded terminal documentation for your device vendor.

See also:

- (10.3) Printers and Terminals Settings
- Plan and Roll Out Terminal Updates (see page 120)

6 Printing with MyQ

Before configuring queues or deploying drivers, decide how print jobs will move through your environment. This decision affects network load, server resource requirements, spooling infrastructure, accounting accuracy, and what happens when the server is unavailable.

The two fundamental models are server spooling and direct IP printing. Most deployments use one as the primary model, with the other available for specific use cases.

6.1 Server Spooling

In server spooling, jobs travel from the user's workstation to the MyQ Print Server, where they are processed, associated with the user, and handled according to the target queue type. The server applies policies, collects accounting data, and manages the release workflow.

This model gives you full control over the print environment – policies, quotas, job routing, reporting, and secure hold print all depend on jobs passing through the server. It is the right default for most deployments.

Consider server spooling when:

- You need centralized accounting, quota enforcement, or policy application.
- Users require secure hold print or pull print across multiple devices.
- You want automated printer provisioning and driver deployment.
- Your environment has reliable network connectivity between workstations and the Print Server.

The main constraint is network dependency. Every print job travels to the server and back to the device. In environments with limited WAN bandwidth, high print volume, or branches with unreliable links, this can become a bottleneck. Client Spooling and Device Spooling address this without abandoning the server model.

6.2 Direct IP Printing

In direct IP printing, jobs are sent from the workstation straight to the device, bypassing the server. MyQ can still monitor and account for direct print jobs when an appropriate monitoring method is used, such as MyQ Desktop Client, embedded terminal reporting, or counter checking. The print data itself is sent directly from the workstation to the device, not through the MyQ server.

This model suits environments where keeping print data local is a requirement, where network links to a central server are insufficient for print traffic, or where a small number of devices does not justify server-mediated spooling.

Consider direct IP printing when:

- Print data must not leave the local network segment.
- Network connectivity to the Print Server is unreliable or bandwidth-constrained.
- Users print to a small number of local devices with no requirement for pull print or hold print.

The main constraint is management overhead. Without the server in the job path, driver deployment, queue configuration, and print monitoring must be handled separately. MyQ Desktop Client in Client Spooling mode can reduce this overhead: jobs are delivered directly to the device while metadata is reported to the server, supporting accounting and selected MyQ controls without routing the full job data through the server. This is the recommended approach when direct printing is required for network or data-residency reasons.

6.3 Decision Factors

Factor	Favors Server Spooling	Favors Direct IP
Accounting and quota enforcement	Yes	Requires MDC
Secure hold print / pull print	Required	Not available
Policies and job modification	Full support	Limited
Automated driver deployment	Via MDC or GPO	Via MDC Client Spooling
Network bandwidth to server	Sufficient	Constrained
Print data residency	Flexible	Must stay local
Server availability dependency	Higher	Lower

In most environments these two models are combined: server spooling for the majority of users and queues, with Client Spooling enabled for sites or user groups where bandwidth or residency requirements apply.

See also:

- (10.3) Queues
- Spooling Strategy (see page 141)
- (10.2) Client Spooling
- (10.3) Jobs via LPR Protocol

6.4 Queue Types

MyQ X uses four queue types. Each has distinct behavior that determines how and when jobs are released, and which features are available to users. Choose queue types as part of your print environment design – the right combination depends on your security requirements, device fleet, user workflows, and accounting model.

6.4.1 Direct Queue

A direct queue is assigned to a single device. Jobs sent to a direct queue are forwarded to that device immediately and printed without user intervention.

Use a direct queue when:

- Immediate printing is acceptable and secure hold print is not required.
- A device is dedicated to a specific workgroup, department, or function.
- You need per-device accounting without requiring users to authenticate at the device.

A direct queue requires no embedded terminal for basic operation. If an embedded terminal is present, users can still log in and interact with the device, but jobs are not held waiting for release.

6.4.2 Pull Print Queue

A pull print queue holds jobs on the server until the user authenticates at a device and releases them. The queue can have multiple devices assigned to it, and users can release their jobs at any of those devices.

Pull print is the foundation of secure printing in MyQ X. Jobs are not printed until the user authenticates at a device and releases them, which reduces unattended output and helps prevent confidential documents from being printed before the user is present.

Use a pull print queue when:

- Secure hold print is required.
- Users need the flexibility to release jobs at any available device.
- You want to reduce waste from jobs that are sent but never collected.
- An embedded terminal or Mobile Client is available for authentication at the device.

Pull print typically requires an embedded terminal or hardware terminal for release at the device. In some scenarios, devices without an embedded terminal can participate by using a printed QR code with the MyQ X Mobile Client.

6.4.3 Tandem Queue

A tandem queue distributes jobs across multiple assigned devices. Incoming jobs are balanced among the available devices rather than queued for a single device.

> ⚠ Unlike pull print, tandem queues do not require the user to authenticate at the device before the job is printed. In this respect, they behave more like direct print: the job is sent to an available device and printed without user-directed release.

Use a tandem queue when:

- A group of users generates enough print volume to create bottlenecks at a single device.
- You want to reduce wait times without requiring users to choose a specific device.
- Load distribution across a device group is more important than user-directed device selection.

Tandem queues are suited to high-volume, time-sensitive printing where throughput matters more than document confidentiality. They are not a substitute for pull print where documents must be held until the user authenticates at the device.

6.4.4 Delegated Queue

A delegated queue extends pull print by allowing designated users – delegates – to release jobs on behalf of another user or group. Jobs sent to a delegated queue can be released by the configured delegates, and are accounted to the delegating user.

Use a delegated queue when:

- Users need to delegate print release to an assistant or a shared role.
- A group of users shares responsibility for releasing documents from a common workflow.

- You need delegated release while keeping jobs accounted to the originating user.

Delegated printing requires defining delegate relationships before go-live. Delegates are configured per user or per group, either by the administrator or by users themselves if self-management is enabled.

6.4.5 Queue Type Comparison

	Direct	Pull Print	Tandem	Delegated
Jobs held until release	No	Yes	No	Yes
Multiple devices per queue	No	Yes	Yes	Yes
User authentication required at device	No	Yes	No	Yes
Embedded terminal required	No	Yes*	No	Yes*
Load distribution	No	No	Yes	No
Delegate release	No	No	No	Yes
Accounting	Yes	Yes	Yes	Yes

*Or Mobile Client with QR code.

6.4.6 Planning Notes

Most deployments use more than one queue type. A common baseline is one pull print queue covering the majority of users and devices, one or more direct queues for dedicated or shared-access printers where immediate output is appropriate, and delegated queues for specific roles or workflows that require them.

Queue access can be restricted by user or group. When MyQ Desktop Client printer provisioning is configured, queues can be deployed to user workstations based on user or group assignment, so users receive the queues intended for them.

Queue design depends on group configuration and authentication decisions made earlier in the planning process. Finalize your queue structure after group configuration and authentication have been settled, not before.

See also

- (10.3) Queues
- (10.3) Printer Discovery
- (10.3) Printer Discovery General Configuration
- (10.2) Printer Profile Provisioning

6.5 Selecting Printing Methods

MyQ X supports multiple methods for submitting print jobs. The right combination depends on your user population, device types, network topology, and security requirements. Select methods during planning – some require infrastructure decisions (Mobile Print Agent placement, queue configuration, certificate trust) that need to be made before rollout.

6.5.1 Printing Methods

Method	Primary Use Case	Authentication	Requires	Supported Platforms	Network Reach
Server spooling via LPR/ IPPS	Managed workstations, primary print path	Job sender identity	Queue, print driver or IPPS	Windows, macOS	Local network
Client Spooling	Bandwidth-constrained sites, data residency	Job sender identity	MyQ Desktop Client	Windows, macOS	Local network
Device Spooling	Branch offices, offline resilience	At device	Supported embedded terminal	Windows, macOS	Local network
IPPS (driverless)	Managed and BYOD workstations, WPP environments	Job sender identity	IPPS queue, certificate trust	Windows, macOS, iOS (no auth), Android (no auth), Chromebook	Local network, multiple networks via DNS-SD

Method	Primary Use Case	Authentication	Requires	Supported Platforms	Network Reach
Mobile Client	iOS, Android – authenticated mobile printing	MyQ credentials or Entra ID	Mobile Client app, IPPS queue	iOS, Android, Chromebook (deprecated)	Local network, internet via Microsoft App Proxy
AirPrint / Mopria	iOS, macOS, Android – native mobile printing	MyQ credentials (first use)	Mobile Print Agent, IPPS queue	macOS (with auth), iOS (with auth), Android (with auth), Chromebook (without Chromebook Client)	Local network, multiple networks via DNS-SD
Web Upload	Any platform, driverless submission	MyQ Web Interface login	Web queue enabled	Any platform (primarily desktop)	Local network with access to Print Server
Jobs via Email	Guests, BYOD, remote users	Email address match	Email queue, SMTP configuration	Any platform	Any network with access to SMTP server; internet
Microsoft Universal Print	Cloud-managed devices, no-VPN scenarios	Microsoft identity	Azure app registration, Universal Print license	Windows (Entra ID-joined)	Internet

Method	Primary Use Case	Authentication	Requires	Supported Platforms	Network Reach
Chromebook / Chrome Extension	Google Workspace environments	Google identity	IPPS queue, Chromebook Client or Admin Console config	Chromebook	Local network, multiple networks via DNS-SD

6.5.2 About Printing Methods

Server spooling via LPR/IPPS is the standard path for managed Windows and macOS workstations. Jobs are submitted through a print driver pointing at a MyQ queue. IPPS is a strong choice for new deployments because it uses TLS, can support authenticated printing where the client platform supports it, and aligns with the Windows Protected Print mode transition.

Client Spooling keeps job data on the user's workstation and sends only metadata to the server. The job is delivered directly to the device at release. Use this where WAN bandwidth to the Print Server is limited, where print data should stay local, or where a cloud deployment should avoid transferring large print files through a cloud-hosted server. Requires MyQ Desktop Client.

Device Spooling sends jobs directly to the device where they are held for release. The server is not involved in job transfer – only metadata and release signals pass through. Use this at branch offices with limited connectivity, or as a resilience measure combined with Offline Login. Supported on Kyocera and Ricoh embedded terminals only.

IPPS (driverless) allows clients computers to submit jobs to MyQ through an IPP-based queue URL. Depending on the client platform and driver model, this can reduce or remove the need for vendor-specific print drivers. This is the path forward as Microsoft phases out third-party print drivers through Windows Protected Print Mode. IPP/IPPS-based queue access is also relevant for mobile and driverless printing methods such as Mobile Client, AirPrint, and Mopria. Plan certificate trust for IPPS – clients must trust the MyQ server certificate to connect without warnings.

Mobile Client gives iOS and Android users authenticated access to MyQ queues, job management, and QR code terminal login. Where Microsoft sign-in is configured,

users can sign in to the Mobile Client with their Microsoft account. If Entra ID MFA is enforced, that MFA step is handled during Microsoft sign-in. Requires an IPPS queue with mobile device access enabled. If remote Mobile Client access is required, verify the supported publishing method, such as Microsoft Entra Application Proxy, and test authentication, certificate trust, and queue access before rollout.

AirPrint and Mopria expose MyQ pull print queues as natively discoverable printers on the local network. Users on iOS, macOS, and Android can print without installing an app or configuring a queue URL. Requires Mobile Print Agent or DNS-SD configuration that allows mobile devices to discover the published MyQ queues on the relevant network. Queues must have mobile device access enabled. Plan Mobile Print Agent placement as part of your network architecture – it needs to be reachable from both the Print Server and the Wi-Fi segment used by mobile devices.

Web Upload is a driverless option for users who can reach the MyQ Web Interface, where Jobs via Web is enabled and the user has rights to the Web queue. Users log in, upload a supported file, and the job is queued for release. It is useful for guests, contractors, and platforms where driver installation is not practical.

Jobs via Email allows users to submit print jobs by sending email attachments to a designated MyQ address. Useful for guests, remote users, and BYOD scenarios where network access to the Print Server is not available. Can also drive automated guest account creation when combined with self-registration. Requires a configured inbound mail connection (POP3, IMAP, Exchange Online, or Gmail).

Microsoft Universal Print bridges MyQ queues to Microsoft's cloud print infrastructure. Users on Entra ID-joined devices can print without a VPN connection to the Print Server. MyQ retrieves jobs from Microsoft Universal Print and processes them through the configured MyQ printing workflow. Relevant primarily for cloud-first and hybrid deployments. Requires an Azure app registration and a Universal Print license.

Chromebook and Chrome Extension printing is supported via IPPS queues. Queues can be distributed to managed Chromebooks through Google Admin Console, or users can install the MyQ X Chromebook Client extension directly. The extension provisions IPPS queues automatically for signed-in users and works for both managed and BYOD Chromebooks.

6.5.3 BYOD and Guest Printing

For users who are not on managed workstations – personal laptops, mobile devices, guests, contractors – plan which methods are appropriate before rollout.

Pull print queues with a single well-known IPPS URL cover most BYOD workstations without requiring driver installation. The Mobile Client covers iOS and Android users who need authenticated access. AirPrint and Mopria cover native mobile printing without an app. Web Upload and Jobs via Email cover users who cannot join the network or install anything.

Platform coverage. Not all methods are available on all platforms, and authentication support varies. Standard IPP printing works on Windows, macOS, iOS, and Android, but authentication is not available on iOS and Android via this path. Mobile IPP (AirPrint/Mopria) adds authenticated access on macOS, iOS, and Android. For iOS and Android users who need authenticated access to MyQ functions, the Mobile Client is usually the clearest option. Validate the exact authentication behavior of IPP, AirPrint, Mopria, and Mobile Client for the platforms in scope before rollout.

Network reach. Several methods – Standard IPP, Mobile IPP, Mobile Client, and Web Upload – require the client device to reach the Print Server on the local network. Jobs via Email does not require the user device to reach the MyQ Print Server directly. Users only need to send email to the configured print mailbox, while the MyQ server must be able to retrieve jobs from that mailbox through the configured mail connection. The Mobile Client additionally supports internet access via Microsoft Entra Application Proxy, which extends authenticated mobile printing beyond the local network without requiring a VPN.

Certificate trust is a common BYOD pain point. If your server uses a certificate from a non-public CA, BYOD devices will receive trust warnings or fail to connect. For environments with significant BYOD usage, consider a publicly trusted certificate for the MyQ server.

Queue design for BYOD. A single pull print queue with a well-known IPPS URL can be enough for many BYOD scenarios. Where different user groups need different release options or restrictions, two or three queues – for example, one for employees and one for guests – provide flexibility without significantly increasing administrative overhead.

See also:

- Spooling Strategy (see page 141)
- Security and Certificates (see page 26)
- Deployment in the Cloud (see page 30)
- (10.3) Jobs via IPPS
- Set up Microsoft Universal Print (see page 137)
- (10.3) Jobs via Email
- (10.2) MyQ X Mobile Client
- (10.2) MyQ X Chromebook Client

6.6 Set up Microsoft Universal Print

Register a Microsoft Entra application for Universal Print before configuring Universal Print in MyQ.

This procedure creates the Microsoft-side application registration, configures public-client authentication, adds the required Microsoft Graph and Universal Print permissions, and enables document conversion in Universal Print.

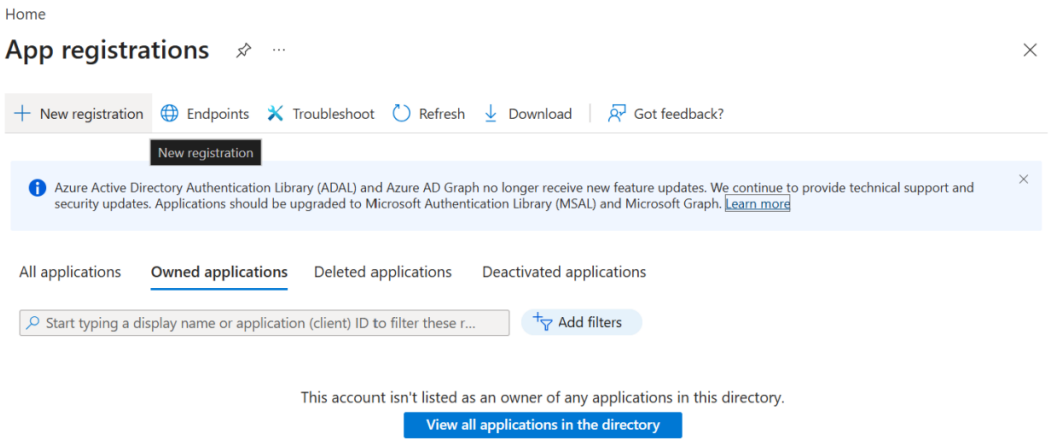
After completing this procedure, continue with (10.3) Connect to Microsoft Universal Print in the MyQ X Server guide.

6.6.1 Prerequisites

- Universal Print is available in the Microsoft tenant.
- You can register applications in Microsoft Entra ID.
- You can add API permissions and grant administrator consent.
- You can access **Universal Print > Settings** in the Microsoft Entra admin center or Azure portal.

6.6.2 Register the application in Microsoft Entra ID

1. Sign in to the **Microsoft Entra admin center**.
2. Go to **Identity > Applications > App registrations**.
3. Select **New registration**.



4. In **Name**, enter a name for the application.

   Example: `MyQ X Connector`, `MyQ Universal Print`, `MyQ Sharepoint`

5. In **Supported account types**, select the account type required for your deployment.
6. Leave **Redirect URI** empty.

   You add the required redirect URIs later in this procedure.

7. Select **Register**.

The application is created.

In the Overview page of the application registration, copy and save the values:

- Application (client) ID
- Directory (tenant) ID

You enter these values when configuring the connection in MyQ.

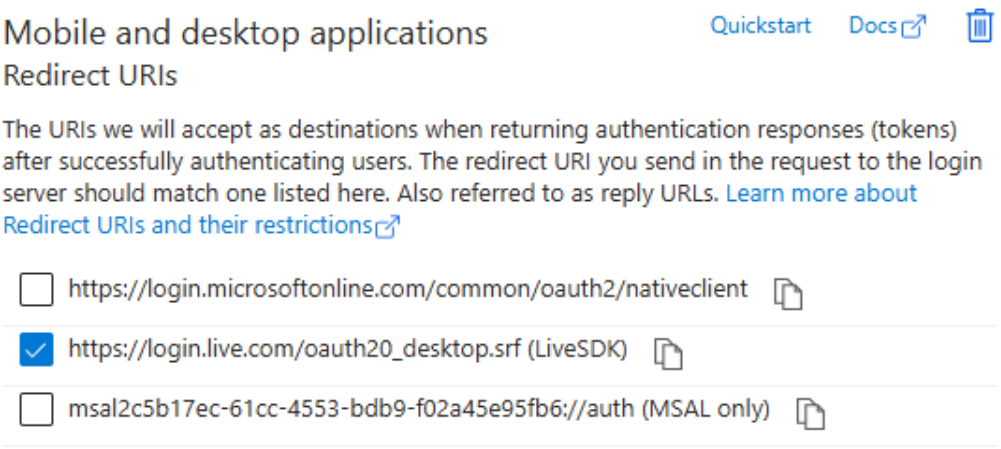
6.6.3 Configure Authentication

Configure the application as a public client.

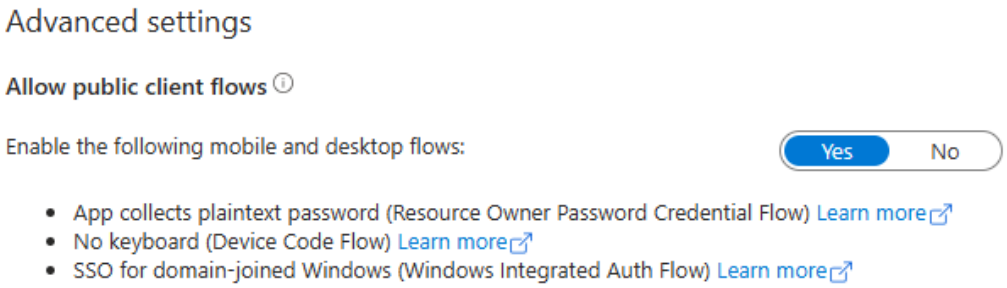
No client secret is required. The redirect URI ise:

1. In the application registration, go to **Manage > Authentication**.
2. Select **Add a platform**.
3. Select **Mobile and desktop applications**.
4. Select the following redirect URI:

   `https://login.live.com/oauth20_desktop.srf`



5. Select **Configure**.
6. In **Advanced settings**, enable **Allow public client flows.**



7. Save the changes.

6.6.4 Add API Permissions

Add the Microsoft Graph and Universal Print permissions required by MyQ.

1. Go to **Manage > API permissions**.
2. Select **Add a permission**.
3. Select **Microsoft Graph** or **Universal Print**, as appropriate.
4. Add the permissions according to the table.

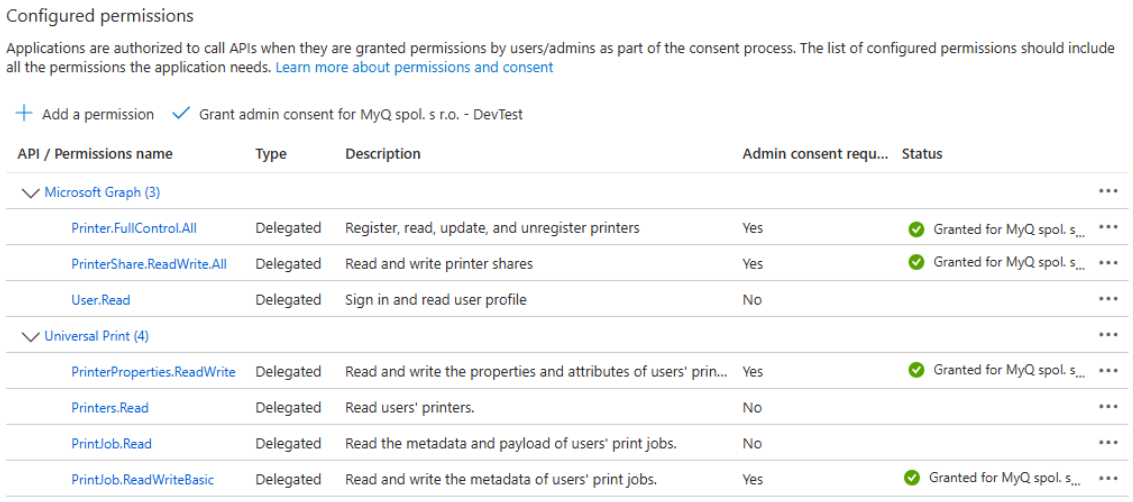
Permission	API	Type	Purpose
`PrinterShare.ReadWrite.All`	Microsoft Graph	Delegated	Read and write printer shares.
`Printer.FullControl.All`	Microsoft Graph	Delegated	Register, read, update, and unregister printers.

Permission	API	Type	Purpose
`Printers.Create`	Universal Print	Delegated	Create and register printers.
`Printers.Read`	Universal Print	Application	Read printers without a signed-in user.
`PrinterProperties.ReadWrite`	Universal Print	Application	Read and write printer properties and attributes without a signed-in user.
`PrintJob.Read`	Universal Print	Application	Read print-job metadata and payload without a signed-in user.
`PrintJob.ReadWriteBasic`	Universal Print	Application	Read and write basic print-job metadata without a signed-in user.

6.6.5 Grant Administrator Consent

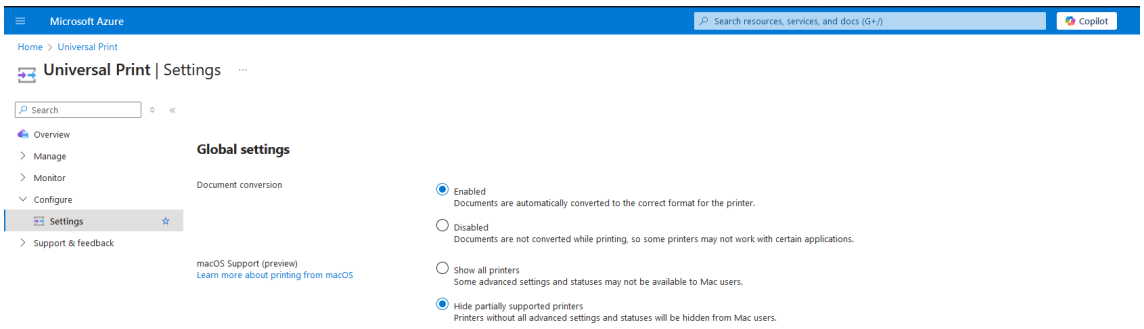
Grant administrator consent for the permissions added to the application.

1. Go to **Manage > API permissions**.
2. Review the configured Microsoft Graph and Universal Print permissions.
3. Select **Grant admin consent**.
4. Confirm the consent request.



6.6.6 Enable Document Conversion in Universal Print

Enable document conversion for Universal Print. In the Azure portal, go to **Universal Print > Settings** and set **Document Conversion** to *Enabled*.



Now you are ready to set up Universal Print in MyQ. See (10.3) Connect to Microsoft Universal Print.

6.7 Spooling Strategy

By default, MyQ X routes print jobs through the Print Server. Jobs travel from the workstation to the server and are then handled according to the target queue type, for example held for release or sent to a device. This works well when network connectivity is reliable and bandwidth is sufficient. When connectivity is limited, or when resilience during server downtime is required, MyQ X provides local spooling and offline-continuity features that keep jobs and authentication closer to where they are needed.

These mechanisms are also relevant in cloud deployments, where routing large print files to and from a cloud-hosted server can increase WAN traffic, latency, and storage requirements. Plan your spooling strategy alongside your network architecture and resilience requirements – the two are closely linked.

6.7.1 Client Spooling

With Client Spooling, the MyQ Desktop Client intercepts jobs on the user's workstation before they reach the server. Only job metadata is sent to the server; the job file itself stays on the workstation. When the user authenticates at a device

and releases the job, the Desktop Client sends the file directly from the workstation to the device.

From the user's perspective, the release experience can be similar to standard pull print in normal operation. The main difference is where the job data is stored and how it reaches the device. Accounting and selected MyQ controls can still be applied, depending on the configured workflow.

Use Client Spooling when:

- WAN bandwidth between the workstation and the Print Server is limited.
- Print data must not leave the local network segment or be routed through a central server.
- You are deploying in a cloud environment and want to avoid sending large print files over the WAN.
- You want to reduce server storage and processing load for print jobs.

To use Client Spooling, a user’s computer must have MyQ Desktop Client installed. If the user's computer is switched off or unreachable when a job is released, the job is paused on the server until the computer is available again – communicate this behavior to users and helpdesk staff before go-live.

Client Spooling is commonly paired with Fallback Printing. When the Print Server is unreachable and Fallback Printing is configured, the Desktop Client can redirect jobs to a configured fallback device.

6.7.2 Device Spooling

With Device Spooling, jobs are sent directly from the workstation to the device, where they are stored on the device's local storage and held for release. The print file is not transferred through the Print Server. Metadata, release coordination, and accounting synchronization still depend on the configured MyQ workflow and server connectivity.

Users release jobs by authenticating at the device in the normal way. If Device Spooling pull print is configured, jobs spooled on one device can be released from other supported devices on the same subnet. For this to work reliably, participating devices must have synchronized time.

Use Device Spooling when:

- Branch offices have limited or unreliable connectivity to the Print Server.
- You want print operations to continue independently of the server connection.
- Network traffic between branches and the central server must be minimized.

- You are combining with Offline Login for a fully server-independent print experience at a site.

Device Spooling has meaningful constraints that affect planning:

- Supported on Kyocera and Ricoh embedded terminals only. Verify support for your specific device models before including Device Spooling in your design.
- Project accounting is not supported – jobs are recorded without a project assignment.
- Job Roaming, favorite jobs, job archiving, and job preview are not supported.
- Pull print across devices is limited to the same subnet. Devices on different subnets cannot share spooled jobs.
- Device storage requirements are higher than in server-spooled deployments. Factor device storage capacity into your planning, particularly for sites with high print volume or large jobs.

6.7.3 Offline Login

Offline Login caches user credentials on the embedded terminal. When the terminal cannot reach the Print Server, users can still authenticate using their cached PIN or ID card and access device functions that do not require live server access.

Offline Login is not a spooling mechanism on its own – it handles authentication continuity, not job delivery. Its value is strongest in combination with Device Spooling: together, they can provide offline authentication and job release for supported Device Spooling workflows. Users can send jobs to a Device Spooling-enabled device, authenticate with cached credentials, and release those jobs while the server is unavailable.

Use Offline Login when:

- Sites must remain operational during server downtime or network outages.
- You are deploying Device Spooling and need authenticated job release to work offline.
- Users at a site must be able to use device-native functions (copy, scan) even when the server is unreachable.

Offline Login is currently supported on Kyocera, Ricoh, and Canon embedded terminals. PIN and ID card are the only supported login methods in offline mode – other authentication methods require a live server connection. Up to 100 users can be cached per device, and up to 3 ID cards and 3 PINs per user.

Plan the cache refresh interval as part of your configuration. Credentials are cached on a schedule; newly provisioned users or recently changed PINs will not be available for offline login until the next cache update runs.

Limitations

- Credit is not supported
- Quota is not supported
- Jobs using Projects are assigned **Without Project**

6.7.4 Combining Spooling Mechanisms

These features can be combined. For a branch office or site with unreliable connectivity, a strong continuity pattern is:

Client Spooling + Device Spooling + Offline Login

In this configuration, job data never travels to the central server. Jobs are intercepted by the Desktop Client, sent directly to the device, and held there. Users authenticate using cached credentials. Accounting data is stored locally and reported to the server when connectivity is restored, provided the relevant terminal and Desktop Client reporting paths reconnect successfully

This combination requires MyQ Desktop Client on workstations, a supported embedded terminal (Kyocera or Ricoh for the full combination), and coordination between the Client Spooling port configuration and the Device Spooling port on the device.

The Fallback Printing feature extends this further by allowing the Desktop Client to redirect jobs to an alternative device when the primary server path is unavailable.

6.7.5 Spooling and Cloud Deployments

In cloud deployments, Client Spooling is often the preferred option for reducing WAN traffic. Jobs stay on the user's workstation and are sent directly to the local device at release, while only metadata is sent to the cloud-hosted server. This can reduce latency, bandwidth use, and server-side storage compared with routing full print files through the cloud server.

Device Spooling can complement Client Spooling at sites where workstation availability cannot be guaranteed at release time, but the vendor and terminal support constraints apply equally in cloud environments.

See also:

- Resilience, Fallback & High Availability (see page 156)
- Deployment in the Cloud (see page 30)
- (10.2) Client Spooling

6.8 Printer Provisioning Strategy

Printer provisioning is the process of deploying print queues and drivers to user workstations. In a MyQ X deployment, this means ensuring that each user has the correct queues installed, pointing at the right server, with the right driver – automatically, and without per-workstation configuration.

Plan your provisioning approach before rollout. The method you choose affects how drivers are maintained over time, how BYOD and non-domain devices are handled, and how your environment responds to the Windows Protected Print Mode transition.

6.8.1 Provisioning Methods

MyQ Desktop Client provisioning is usually the strongest option for managed workstations, especially where queues should follow the signed-in user or workstation context. The Desktop Client can install or update provisioned queues and drivers automatically according to the applicable configuration and provisioning profiles. Profiles can target computers, users, and user groups, and can also use IP ranges or hostnames to apply different behavior to different workstation populations. This supports domain-joined, non-domain, and BYOD scenarios, and covers Windows and macOS.

Queue rights still apply. A user may receive a provisioned client printer but be unable to print through it if they do not have rights to the target queue.

MDC provisioning supports two modes. Legacy Printer Provisioning uses standard TCP/IP ports and vendor print drivers. Printer Provisioning Profiles, available from MyQ X 10.2 patch 21, support the transition to IPPS-based provisioning, including Universal IPP Printer Provisioning. Use them when MDC provisioning is used to deploy WPP-compatible IPPS queues to affected Windows workstations. Plan which provisioning mode is appropriate before WPP reaches managed workstations, especially where current profiles still deploy standard drivers or TCP/IP ports.

Group Policy provisioning is appropriate when workstations are domain-joined, a managed print infrastructure already exists, and the organization prefers to keep

printer deployment within existing GPO workflows. GPO provisioning does not depend on the Desktop Client and can be used where MDC is not deployed. The constraint is that GPO provisioning does not natively follow MyQ user or group assignment in the same way MDC provisioning can. Queues are typically assigned through AD, machine, OU, or policy targeting rather than MyQ provisioning rules.

Manual installation is suitable for small environments, one-off additions, or BYOD users who are not covered by an automated provisioning method. Users install queues by adding a printer via URL (IPPS) or by configuring a standard TCP/IP port manually. For BYOD users, an IPPS URL is often the lowest-friction manual option. It can reduce driver-management effort and is supported on Windows, macOS, Linux, and Chromebook, with platform-specific setup and driver behavior.

6.8.2 Choosing Your Approach

Factor	MDC Provisioning	GPO Provisioning	Manual / IPPS
Domain membership required	No	Yes	No
Adapts to user group membership	Yes	No	No
Covers BYOD and macOS	Yes	No	Yes (IPPS)
Removes queues when access revoked	Yes	Depends on GPO design	No
Requires Desktop Client deployment	Yes	No	No
WPP-compatible (IPPS mode)	Yes	Depends on port and driver	Yes

Most deployments combine methods: MDC provisioning for managed workstations, manual IPPS for BYOD and guest users, and GPO as a fallback or complement in large domain environments.

6.8.3 Dependencies and Recommendations

MDC provisioning requires the Desktop Client to be installed and running before queues are provisioned. Driver packages must be uploaded to the Print Server before

provisioning can deploy them. Allow time in your rollout plan for driver testing across each device model in your fleet. A driver that works correctly on one model may produce unexpected output on another, and provisioning will deploy it to all assigned users before the problem is discovered.

In Central/Site deployments, users who move between sites will have MDC attempt to install the queues configured for that site's server. If standard print drivers are configured and WPP is enabled on that workstation, the installation will fail silently from the user's perspective. Audit your provisioning profiles for non-IPPS drivers before enabling WPP in any part of the environment.

Use MDC configuration profiles and provisioning profile targeting to separate provisioning behavior where different sites, user groups, or workstation populations need different queues or IPPS-only provisioning during a WPP transition.

Printer Provisioning Profiles also depend on provisioning-profile licensing. In Central/Site deployments, check profile-license allocation before rollout. If the provisioning profile license limit is exceeded, some profiles may remain visible in the UI but not be deployed to Desktop Client.

6.8.4 Windows Protected Print Mode

Windows Protected Print Mode (WPP) requires IPP-based printing. When WPP is enabled, non-IPP drivers and standard TCP/IP ports are removed. When WPP is enabled, non-IPP drivers and standard TCP/IP ports are removed. Disabling WPP later does not automatically recreate the removed printers, drivers, or ports. Only IPPS ports and IPP-compatible drivers are preserved.

The planning implications for provisioning are:

Deploy IPPS queues before WPP is enforced. Users need a working IPPS-based print path in place before standard drivers are removed. If MDC provisioning is in use, switch affected profiles to Printer Provisioning Profiles with the built-in IPPS driver before WPP is enabled.

Audit your provisioning profiles for non-IPPS drivers and remove or reassign them before enabling WPP. Any profile still configured with a standard driver can generate repeated provisioning errors on WPP-enabled workstations, because the Desktop Client attempts to install drivers that Windows no longer allows.

In Central/Site environments, pay particular attention to roaming users. A user moving to a site whose server still has standard drivers configured will trigger failed provisioning attempts on a WPP-enabled workstation.

Test IPPS print output for each device model before the transition. IPPS printing may not expose all finishing options available through a vendor driver – duplex, stapling, tray selection, and other settings may require IPP attribute support on the device. Verify that the output your users need is achievable via IPPS before removing standard drivers.

See also:

- Selecting Printing Methods (see page 132)
- (10.2) Printer Profile Provisioning
- Windows Protected Print Mode (see page 148)

6.9 Windows Protected Print Mode

Windows Protected Print Mode (WPP) uses the modern IPP-based Windows print stack and removes support for non-IPP print drivers and standard TCP/IP print ports when enabled. When WPP is enabled, Windows removes non-IPP print drivers and standard TCP/IP ports. If WPP is later disabled, the removed printers, drivers, and ports are not automatically recreated. IPPS ports and IPP-compatible drivers are preserved.

WPP is already configurable via Group Policy and Windows Settings in current Windows releases. Plan the transition before WPP is enabled on managed workstations, especially where current printing depends on vendor drivers, LPR, RAW, or standard TCP/IP ports.

6.9.1 What WPP Changes

When WPP is enabled on a workstation:

- Non-IPP print drivers are removed. Vendor-specific drivers, such as PCL or PostScript drivers, cannot be used while WPP is active unless they are compatible with the IPP-based print model.
- Standard TCP/IP ports (LPR, RAW) are removed. Printers configured with these ports stop working.
- Only IPPS ports and the Windows built-in IPP class driver are preserved.
- Adding new printers is restricted to IPP-based devices only.

Disabling WPP later does not automatically recreate printers, drivers, or ports that were removed when WPP was enabled.

6.9.2 Impact on MyQ X

IPPS queues are preserved under WPP. Queues configured with IPPS ports on the MyQ Print Server can continue to work, but output behavior and finishing options must be tested for each device model. Planning IPPS queue deployment before WPP is enabled is one of the key transition tasks.

Device Spooling is affected by WPP because it uses RAW ports, such as 10010-10013, for direct job delivery to devices. WPP removes RAW/TCP/IP ports, so Device Spooling workflows can stop working on WPP-enabled workstations. If Device Spooling is part of your resilience or branch office strategy, you need an alternative before WPP is enforced in those environments. Assess affected sites and user populations as part of your WPP planning.

Standard driver provisioning via MDC fails under WPP. If MyQ Desktop Client provisioning profiles still deploy standard print drivers when WPP is active, Windows blocks the printer configuration. Users can see a **Configuring printers failed** error on each provisioning attempt, and the affected printer is not installed. Switch affected profiles to Printer Provisioning Profiles that deploy IPPS or Universal IPP printers before WPP reaches those workstations.

Finishing options may be reduced under IPPS. Vendor print drivers can expose device-specific finishing capabilities, such as duplex modes, tray selection, stapling, punch, or booklet printing. IPPS relies on IPP attributes reported by the device, and some capabilities available through a vendor driver may not be available or may behave differently through IPPS. Test print output for each device model in your fleet before removing standard drivers.

6.9.3 Transition Planning

Treat WPP as a migration with a defined completion target, not a future compatibility issue. The steps below give you a structured approach.

Inventory your current print paths. Identify which workstations use standard TCP/IP or LPR ports, which use vendor drivers, and which already use IPPS. This tells you the scope of work before WPP reaches any part of your environment.

Deploy IPPS queues before removing standard queues. Users need a working IPPS-based print path in place before their existing paths are removed. Configure IPPS

queues on the Print Server, verify certificate trust on target workstations, and confirm print output quality for each device model. Only then begin retiring standard queues.

Switch MDC provisioning profiles to IPPS. For environments using Desktop Client printer provisioning, update configuration profiles to use Printer Provisioning Profiles with the built-in IPPS driver. Disable or remove profiles that deploy standard drivers. Do this before WPP is enabled on any workstation covered by those profiles.

Address Device Spooling dependencies explicitly. Identify every site or use case that depends on Device Spooling. Determine whether Client Spooling is a viable substitute – it achieves similar network efficiency without RAW ports. Where Device Spooling is used for offline resilience in combination with Offline Login, assess whether that resilience model needs to be redesigned for affected sites.

Test finishing options per device model. For each device model in your fleet, print a test job via IPPS and verify that the finishing options your users need are available and function correctly. Document any gaps and decide whether they require firmware updates, device replacement, or workflow changes before standard drivers are removed.

Coordinate Central/Site environments carefully. In multi-site deployments, WPP may be enforced at different times across different workstation populations. A roaming user whose workstation has WPP enabled may visit a site whose MDC profiles still deploy standard drivers – this generates provisioning failures. Maintain a clear picture of which sites and profiles have been migrated and which have not, and restrict roaming users from receiving non-IPPS profiles during the transition period.

Communicate to users before the change. Removing a working print queue and replacing it with an IPPS queue is transparent if done correctly. Any gap in coverage can result in failed printing and additional support requests. Confirm replacement queues are working for representative users in each group before retiring standard queues fleet-wide.

See also:

- Printer Provisioning Strategy (see page 145)
- Spooling Strategy (see page 141)
- Selecting Printing Methods (see page 132)
- (10.3) Jobs via IPPS

- (10.2) Printer Profile Provisioning

7 Deploy MyQ Desktop Client

MyQ Desktop Client (MDC) is a software application installed on users' workstations. It provides user identification, server communication, print accounting, secure printing, print driver capture, and printer provisioning on supported Windows and macOS workstations.

This page covers the decisions to make before deploying MDC. Installation procedures, including Intune deployment where supported, are covered in the relevant MyQ Desktop Client guide for each platform.

7.1 Why Deploy MDC?

MDC deployment is optional, but useful in many environments, especially where workstation identification, printer provisioning, client spooling, fallback printing, or local print monitoring are required.

The main reasons to deploy MDC are:

7.1.1 User Convenience

MDC can be installed and preconfigured on users’ computers through Intune, or made available through Company Portal for self-service installation. Server connection parameters can also be included in the installer so that users do not need to configure the server connection manually.

7.1.2 Fallback Printing

MDC supports printing when the MyQ server is temporarily unavailable. To make fallback printing available broadly, install the client on all workstations that should be covered by the fallback printing plan, not only on workstations where users have already requested it.

7.1.3 Visibility and Control

Deploying MDC centrally helps you identify which devices have it installed, roll out updates consistently, and keep clients aligned with the intended configuration.

If your environment relies on embedded terminals for all print release and you have no requirement for client spooling, fallback printing, or workstation-level user identification, MDC may not be necessary. Where printing must continue during

temporary server unavailability, fallback printing can be enough reason to deploy MDC broadly.

7.2 Prerequisites for MDC

Before beginning deployment, confirm the following:

- **Certificates:** If your MyQ server uses a certificate issued by a certificate authority that is not automatically trusted by the client operating system, that certificate (or the issuing CA certificate) must be installed on client computers before MDC is deployed. Clients that cannot verify the server certificate may fail to connect or may show trust warnings, depending on the configured security mode and certificate state.
- **Dependencies:** Check the current Desktop Client system requirements before deployment. If the selected client version or deployment method requires additional components on target devices, deploy them before or alongside MDC. In Intune, required components can be handled as app dependencies.

7.3 Deployment Method

MDC can be deployed in two ways:

Intune (recommended for managed environments). MDC can be packaged and distributed through Microsoft Intune. This is the appropriate choice if your organization already manages endpoints through Intune and you want MDC installed and configured without user intervention. Use the platform-specific Desktop Client guide for Windows and macOS packaging details.

Manual installation. Users run the installer directly on their workstation. This is suitable for small deployments, pilots, or environments without MDM infrastructure. The installer filename can be customized to include the server address and port so that MDC connects automatically on first launch – otherwise users must configure the connection themselves.

7.4 Deploying MyQ Desktop Client with Intune

To deploy MDC to your managed endpoints without requiring user action, distribute it using Microsoft Intune. Both Windows and macOS are supported, though the packaging steps differ between platforms.

MDC can be deployed in two modes via Intune: pushed silently to all assigned devices without user involvement, or made available through Company Portal for users who prefer to install it themselves. Silent deployment is usually preferable for managed

fleets where MDC must be available without user action. It helps ensure MDC is installed on assigned workstations, subject to Intune deployment status and device eligibility.

Before you start, confirm that your Intune environment is configured – users, groups, devices, policies, and assignments should be in place in the Microsoft Intune admin center[5]. If you are new to Intune, review the Microsoft Intune Overview[6] and Win32 app management in Microsoft Intune[7] before proceeding.

7.5 Configuration Profiles

MDC configuration profiles are created and managed in MyQ X Settings. A profile defines the features and behavior of MDC for a set of client computers, matched by IP range or hostname.

If a client does not match any specific configuration profile, it uses the Default profile. If a client matches multiple profiles, the highest matching profile in the list is used.

Profiles can be prepared before deployment begins. Once MDC connects to the server after installation, it automatically downloads settings from the applicable profile. This means key configuration decisions, such as fallback printing behavior, client spooling, printer provisioning settings, and authentication mode, should be prepared in profiles before rollout where possible.

The default profile applies to any client not matched by a more specific profile. If you have multiple office locations or user populations with different printing requirements, plan your profile structure accordingly.

7.6 Personalization

Two settings in MyQ X affect how the Desktop Client appears to users. Both are configured in **Settings > Personalization** in the MyQ Web Interface, and both should be set before MDC is deployed – users see the client interface immediately after installation.

- **Custom Application Logo:** Replaces the default MyQ logo with your organization's logo. The logo appears in the Desktop Client, the Web UI, and reports. When no custom logo is configured, the MyQ logo is shown.

5. https://endpoint.microsoft.com
6. https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune
7. https://learn.microsoft.com/en-us/mem/intune/apps/apps-win32-app-management

- **Custom Link in the Desktop Client:** Adds a link to the Desktop Client interface that you can point to any URL – your intranet, a help page, the MyQ Web Interface, or any other resource useful to your users. The link title should not exceed 25 characters.

See also:

- (10.2) MyQ Desktop Client
- (10.2) Deploy with Intune
- (10.3) MyQ Desktop Client Settings
- (10.3) Personalization Settings

8 Resilience, Fallback & High Availability

MyQ X provides several features that can help keep printing operational during server downtime or degraded connectivity when they are enabled and configured before an outage. Choosing and configuring the right combination requires decisions that depend on your device fleet, your deployment of MyQ Desktop Client (MDC), and your availability requirements.

This article covers resilience and high-availability planning. For information about configuring Fallback Printing, spooling, Microsoft Failover Clustering, or VM high availability, see the relevant product documentation.

8.1 Feature Overview and Vendor Constraints

The available features divide into two categories: those that reduce server dependency during normal operation, and those that maintain print capability during complete server downtime.

Feature	What It Does	Requires	Vendor Constraint
Client Spooling	Stores jobs on the user's workstation; sends only metadata to the server. Job data travels to the device directly at release, not via the server.	MDC	None – any device
Device Spooling	Sends jobs directly to the device, where they wait for release. Server involvement at release is minimal.	MDC + embedded terminal	Kyocera and Ricoh only
Offline Login	Allows users to authenticate at a terminal when the server is unreachable, using cached credentials.	Embedded terminal	Kyocera, Ricoh, and Canon only

Feature	What It Does	Requires	Vendor Constraint
Fallback Printing	Routes jobs to a fallback printer via MDC when the server is unreachable.	MDC	No fixed vendor restriction, but device compatibility is not guaranteed. Test each fallback device or model before rollout.

8.1.1 Fallback Printing Compatibility

Whether a device will accept jobs routed via Fallback Printing depends on the device vendor and model. Some devices reject print jobs that do not originate from their configured accounting server. In some cases this can be overridden in the device's own settings – look for an option to accept unauthorized jobs or jobs from unknown sources. Always test Fallback Printing against your specific devices before rollout. Do not assume it works because it is configured.

8.1.2 Client Spooling vs. Device Spooling

These serve different purposes and are not alternatives to each other. Client Spooling reduces network load and keeps jobs off the server; Device Spooling enables printing directly to a device during server downtime. They can be used together.

8.2 Choosing the Right Features for Your Environment

The vendor constraints in the table above are the primary filter. If your fleet does not include Kyocera or Ricoh devices with embedded terminals, Device Spooling is not available. Offline Login may still be available on supported terminals, such as Canon, but it does not provide Device Spooling-based job release on its own. Plan around what your fleet actually supports.

If your fleet supports Device Spooling (Kyocera/Ricoh with embedded terminals):

The most complete MyQ continuity pattern for supported fleets combines Offline Login, Device Spooling, Client Spooling, and Fallback Printing. During normal operation, Client Spooling reduces server load. During server downtime, users can still authenticate via Offline Login, release jobs spooled to the device via Device Spooling, and fall back to a designated printer via MDC if needed. Accounting data can be reported after connectivity is restored: the embedded terminal reports Device Spooling job statistics to the server, and MDC reports fallback jobs when it reconnects.

This combination requires MDC to be deployed to user workstations and embedded terminals to be active on the target devices. Configure it before rollout.

If your fleet does not support Device Spooling:

If MDC is deployed, Fallback Printing is the main MyQ-managed print continuity option for fleets that do not support Device Spooling. Users whose jobs cannot reach the server are routed to a fallback printer. Authenticated pull print and delegated print are not available during the outage. Accounting is preserved once the server is reachable again.

If MDC is not deployed:

Neither Fallback Printing nor Client Spooling is available. Continuity depends entirely on whether your devices support Offline Login and Device Spooling. If they do not, MyQ-managed print continuity is not available during a server outage, except for any printing paths outside MyQ that the organization maintains separately.

8.3 Server Failover and Clustering

For environments where print server availability is a hard requirement, MyQ supports infrastructure-level approaches that go beyond print-and-device fallback features.

8.3.1 Microsoft Failover Clustering

MyQ can run in a Windows Server Failover Cluster using an active/passive configuration. The cluster manages MyQ services across multiple nodes; if the active node becomes unavailable, the cluster switches to a passive node automatically. Microsoft Failover Clustering primarily protects against node-level failure. Do not assume that every MyQ application or service failure will trigger cluster failover; include application-level monitoring and recovery in the operational design.

Microsoft Failover Clustering is appropriate when high availability of the MyQ server is a business requirement and your organization already has, or is prepared to

operate, Windows Server clustering infrastructure. It introduces greater infrastructure and operational complexity than a standalone MyQ server or VM-level high availability.

Before choosing this approach, verify the current MyQ system requirements, supported Windows Server versions, storage requirements, and cluster prerequisites in the MyQ X Server documentation.

8.3.2 Client Hostname Configuration

Client applications, such as MyQ Desktop Client and MyQ Mobile Client, should be configured to connect to the cluster hostname or IP address, not to an individual node. If clients are pointed at a node directly, they will lose connectivity when that node fails over, regardless of whether the cluster itself is functioning correctly. Confirm this before rollout.

8.3.3 Virtual Machine High Availability (VMHA)

When MyQ runs in a virtual machine, hypervisor high-availability features can provide infrastructure resilience by restarting or moving the VM after a host failure.

This approach is generally simpler than deploying MyQ in a Windows Failover Cluster because it does not require application-level Windows clustering. Recovery depends on the virtualization platform detecting the failure and restoring the VM, so the achievable recovery time depends on the HA platform and its configuration.

Consider VM-level HA when protection against host failure is required but the additional complexity of Microsoft Failover Clustering is not justified.

8.4 Choosing a Server HA Approach

	Microsoft Failover Clustering	**Virtual Machine HA**
Protection model	MyQ runs across active/passive Windows cluster nodes	The virtualization platform recovers the MyQ VM after host failure
Infrastructure	Windows Failover Clustering	Hypervisor HA
Complexity	Higher	Generally lower

	Microsoft Failover Clustering	Virtual Machine HA
Recovery	Failover to another cluster node	VM restart or relocation
Best suited to	Environments with stringent server-availability requirements and clustering expertise	Virtualized environments primarily protecting against host failure

Choose the approach according to the failures you need to tolerate, required recovery time, existing infrastructure, and operational expertise.

Server HA and print fallback address different failure scenarios and can be used together. HA restores the MyQ server service; Offline Login, Device Spooling, and Fallback Printing can preserve selected user workflows while the server is unavailable.

See also:

- (10.2) Fallback Printing
- (10.3) MyQ and MS Cluster
- (10.2) Fallback Printing
- (10.3) Device Spooling

myQ X

SAVE TIME WITH PERSONALIZED PRINT SOLUTIONS

MyQ X is an award-winning on-premise or private cloud print management solution trusted by millions of users.

info@myq-solution.com

myq-solution.com

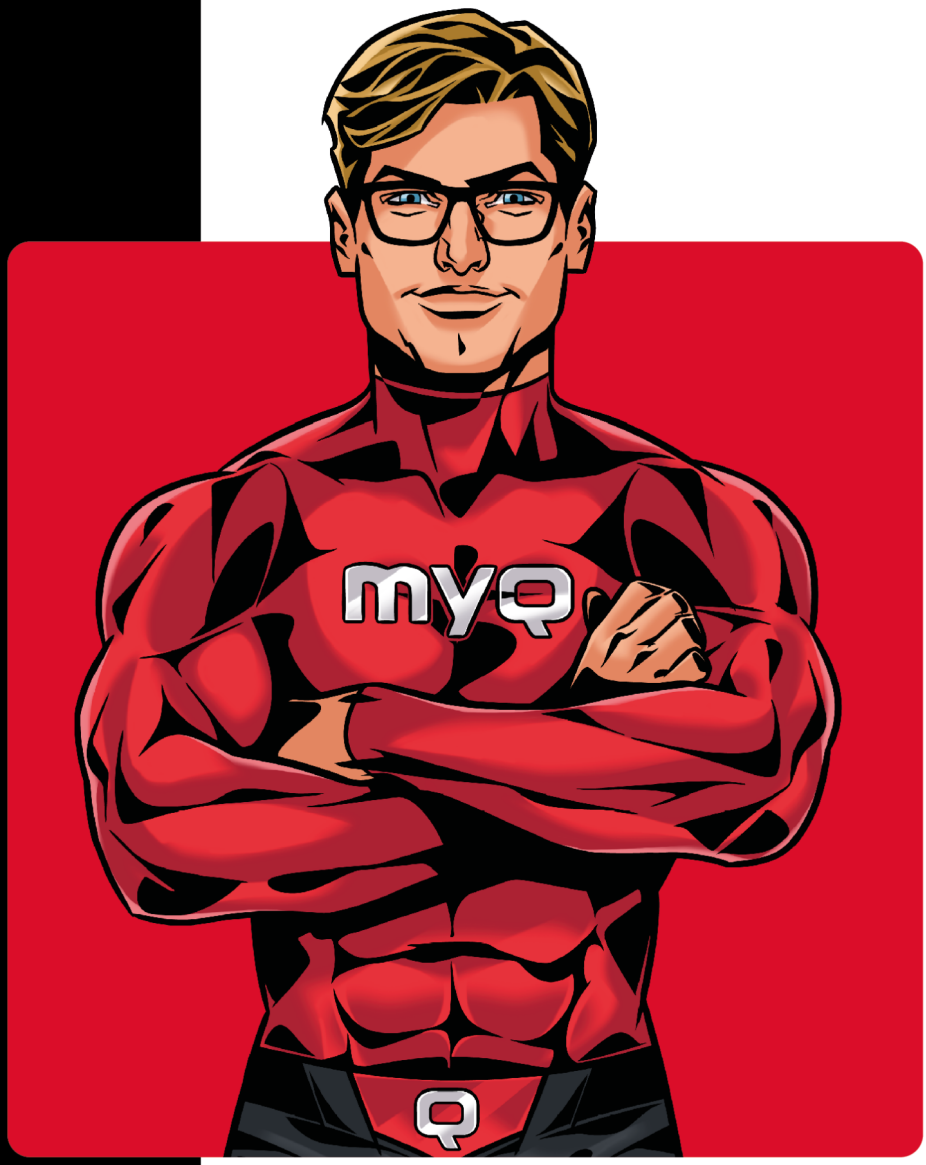
50+ million
Trusted users

1+ million
Active devices

26+
Brands supported

1000+
Certified partners

Operating in **140+** countries



Awarded and certified

BuyersLab PLATINUM TESTED SOLUTION 2023

BuyersLab PLATINUM TESTED SOLUTION 2022

BuyersLab PLATINUM TESTED SOLUTION 2021

ISO 9001 TÜV SÜD ISO 14001 ISO/IEC 27001